Lineare Algebra, WS 2002/2003

Adalbert Kerber

4. Oktober 2004

Inhaltsverzeichnis

Symbolverzeichnis

$\neg$	Junktor “nicht . . .”, 12
$\wedge$	Junktor “. . . und . . .”, 12
$\Rightarrow$	Junktor “wenn . . ., dann . . .”, 12
$\vee$	Junktor “. . . oder . . .”, 12
$\Longleftrightarrow$	Junktor “genau dann, wenn. . .”, 12
$\forall$	Quantor “für alle”, 14
$\exists$	Quantor “es gibt”, 14
$a \in b$	die Klasse a ist Element der Klasse b, 16
$a \notin b$	die Klasse a ist nicht Element der Klasse b, 16
$\mathrm{Mg}(x)$	die Klasse x ist eine Menge, 16
$\emptyset$	die leere Klasse, 17
$\mathcal{R}$	die Russellsche Klasse, 17
$\mathcal{A}$	die Allklasse, 17
$a \subseteq b$	a ist Teilklasse von b, 17
$a \cup b$	die Vereinigung der Klassen a und b, 18
$a \cap b$	der Durchschnitt der Klassen a und b, 18
$\overline{a}$	die Komplementärklasse von a, 19
$a \backslash b$	das Komplement von a in b, 19
$\bigcup_{x:\ A(x)} x$	die Vereinigung der Klassen mit Eigenschaft A, 19
$\bigcap_{x:\ A(x)} x$	der Schnitt der Klassen mit Eigenschaft A, 19
$V(a)$	die Vereinigung der Elemente von a, 19
$S(a)$	der Schnitt der Elemente von a, 19
$\{a\}$	die Einerklasse zu a, 19
$\mathbb{N}$	die (Menge der) natürlichen Zahlen, 20
a^+	der Nachfolger von a, 20
(a, b)	das geordnete Paar aus a und b, 23
(a, b, c)	das geordnete Tripel aus a, b und c, 23
$a \times b$	das cartesische Produkt aus a und b, 23

a^n	das n-fache cartesische Produkt von a mit sich selbst, 23
$\mathrm{Def}(R)$	der Definitionsbereich von R, 24
$\mathrm{Bild}(R)$	das Bild von R, 24
R^{-1}	die Umkehrrelation zu R, 24
$S \circ R$	die Komposition von S und R, 24
$\mathrm{Graph}(f)$	der Graph der Funktion f, 25
$\rightarrowtail$	injektiv, 25
$\twoheadrightarrow$	surjektiv, 25
$\rightarrowtail\!\!\!\!\twoheadrightarrow$	bijektiv, 25
$\lvert a \rvert$	die Ordnung, Kardinalität, Mächtigkeit von a, 26
$\mathbb{Q}_{\geq 0}$	die Menge der nicht negativen rationalen Zahlen, 28
$\times_{i \in I} a_i$	eine Klasse von Abbildungen, 28
$[m]_R$	die Äquivalenzklasse von m unter R, 30
R_f	die fon f induzierte Äquivalenzrelation, 31
M_R	die Menge der Äquivalenzklassen von R auf M, 31
ν_R	die natürliche Abbildung der Elemente auf ihre Restklassen, 35
L_I	die Lösungsgesamtheit eines inhomogenen linearen Gleichungssystems, 39
L_H	die Lösungsgesamtheit eines homogenen linearen Gleichungssystems, 39
$*$	eine Verknüpfung, 41
1_G	das neutrale Element, bei multiplikativer Schreibweise, 43
10_G	das neutrale Element, bei additiver Schreibweise, 43
$U \cdot U'$	das Komplexprodukt von U mit U', 45
$G \setminus\!\setminus M$	die Menge aller Bahnen von G auf M, 51
Ug	eine Rechtsnebenklasse von U, 53
$U \backslash G$	die Menge aller Rechtsnebenklassen von U in G, 53
gU	eine Linksnebenklasse von U, 53
G/U	die Menge aller Linksnebenklassen von U in G, 53
$\alpha(\pi)$	die Zykelpartition von π, 54
hom	Homomorphie, 61
$\overset{\sim}{\rightarrowtail}$	Monomorphie, 61
$\overset{\sim}{\twoheadrightarrow}$	Epimorphie, 61
$\simeq$	Isomorphie, 61
$U \trianglelefteq G$	U ist Normalteiler von G, 63
Δ_n	das Differenzenprodukt, 65

$\operatorname{sgn}(\pi)$	das Vorzeichen bzw. Signum von π, 66
A_n	die alternierende Gruppe, 66
$a_i(\pi)$	die Anzahl der zyklischen Faktoren der Länge i in π, 67
$a(\pi)$	der Zykeltyp von π, 67
$U(G)$	der Untergruppenverband von G, 68
$U \vee V$	das Erzeugnis von $U \cup V$, 68
$R[x]$	der Ring der Polynome über R, 73
$(\operatorname{End}(G), +, \circ)$	der Endomorphismenring der abelschen Gruppe G, 73
$I \trianglelefteq R$	I ist ein Ideal im Ring R, 74
$\mathbb{Z}_n$	der Restklassenring $\mathbb{Z}/(n)$, 75
$\operatorname{Char}(R)$	die Charakteristik von R, 76
${}_R M$	M ist R-Linksmodul, 80
M_R	M ist R-Rechtsmodul, 80
${}_R M R'$	M ist (R, R')-Bimodul, 80
$\simeq_R$	R-Isomorphie von R-Moduln, 81
$(a_{ik}) \in \mathbb{R}^{m \times n}$	(a_{ik}) ist eine $m \times n$-Matrix über $\mathbb{R}$, 82
${}_R\langle T \rangle$	Das R-erzeugnis von T, 82
$\sum_i U_i$	die Summe der Untermoduln U_i, 84
$\oplus_i U_i$	die direkte Summe der Untermoduln U_i, 85
$S = \{s_0, \ldots, s_m\}_{\neq}$	die angegebenen Elemente $s_i \in S$ sind paarweise verschieden, 87

Vorwort

Diesem Manuskript liegt eine viersemestrige, vierstündige Anfängervorlesung (mit zwei- bis vierstündigen Übungen) zugrunde, die ich in ähnlicher Form mehrfach an der RWTH Aachen und in Bayreuth gehalten habe (Lineare Algebra I, II sowie im Anschluß daran Algebra I und II).

Da ich weder in Aachen, noch in Bayreuth auf einer Vorlesung über die Grundlagen der Mathematik aufbauen konnte, wurden diese in die Vorlesung aufgenommen, soweit es notwendig erschien. (Leitfaden war mir dabei die Meinung, daß die Teilnehmer(innen) beim Vordiplom oder der Zwischenprüfung in der Lage sein sollten, für Mengen die Gültigkeit der Gleichung $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ zu beweisen, die Verwendung indirekter Beweise zu rechtfertigen, die vollständige Induktion zu begründen und die Definition einer Kategorie anzugeben.)

In der Linearen Algebra erschien mir — auch im Hinblick auf wichtige und anwendungsrelevante Konstruktionen — eine Erwähnung des Tensorbegriffs angezeigt.

Beim Aufbau der Algebra wurde das Gruppenkonzept in den Mittelpunkt gestellt, und zwar *nicht* wegen der Gruppentheorie um ihrer selbst willen, sondern wegen Ihrer Anwendungen in den konstruktiven Methoden computerunterstützter diskreter Mathematik in den Naturwissenschaften, der Technik und der Informatik.

Bayreuth, den 4. Oktober 2004, A. Kerber

Kapitel 1

Grundlagen

In diesem Kapitel werden die grundlegenden Begriffe der Aussagenlogik und der Mengenlehre eingeführt, die wir im folgenden benötigen.

Ziel des ersten Paragraphen ist eine kurze Beschreibung der logischen Grundlagen, die man kennen muß um im zweiten Abschnitt u.a. die folgende — Ihnen aus dem Schulunterricht bekannte — Eigenschaft von Schnitten bzw. Vereinigungen von Mengen zu beweisen: Für alle Mengen a, b, c gilt $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$.

Mengen werden im zweiten Abschnitt eingeführt zusammen mit einer Verallgemeinerung dieses Begriffs, den Klassen. Die wichtigsten Axiome aus dieser Theorie werden kurz angegeben, für detaillierte Einführung in die axiomatische Mengenlehre wird auf die angegebene Literatur verwiesen, insbesondere auf [**?**].

Im dritten Paragraphen betrachten wir Relationen und vor allem Funktionen, das wichtigste Handwerkszeug der Algebra. Zwei zentrale Sätze über die Faktorisierung von Abbildungen schließen sich an.

1.1 Aussagen

Mathematische Resultate sind in der Regel als *Aussagen* formuliert, also als Sprachgebilde, die je nach Inhalt entweder wahr (w) oder falsch (f) sind. Hier ist ein Beispiel:

> Die Anzahl der positiven Teiler einer positiven natürlichen Zahl ist genau dann ungerade, wenn die Zahl ein Quadrat ist.

Wir werden später zeigen, daß dies eine *wahre* Aussage ist. Aussagen können durch *Junktoren* zu neuen Aussagen verbunden werden:

$\neg$ (*Negation,* "nicht ..."), $\wedge$ (*Konjunktion,* "... und ..."),

sowie

$\vee$ (*Disjunktion,* "... oder ..."), $\Rightarrow$ (*Implikation,* "wenn ..., dann ...").

Den Gebrauch dieser Junktoren regelt die *Wahrheitswertetafel*:

1.1.1

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
w	w	f	w	w	w
w	f	f	f	w	f
f	w	w	f	w	w
f	f	w	f	f	w

.

Hier ist besonders die letzte Spalte zu beachten, weil diese Zuordnung von Wahrheitswerten zu $A \Rightarrow B$ vielleicht auf den ersten Blick ungewohnt erscheinen mag — hier wird nämlich festgelegt, daß "aus Falschem alles geschlossen werden kann". "Wenn der Mond aus grünem Käse besteht, dann haben alle Katzen Flügel" wird demnach als wahre Aussage angesehen, denn es ist bekanntlich wahr, daß der Mond nicht aus derlei Material zusammengesetzt ist. Aus dem Lateinunterricht ist Ihnen vielleicht der Satz "ex falso quodlibet" in Erinnerung, der diese Festlegung verbalisiert.

Die Spalte von $A \vee B$ zeigt, daß dieses durch $\vee$ abgekürzte "oder" nicht im ausschließenden Sinne zu verstehen ist, also *nicht* mit "entweder ... oder" verwechselt werden darf!

Darüberhinaus werden wir auch noch den folgenden Junktor:

$\Longleftrightarrow$ (*Äquivalenz,* "genau dann, wenn ...")

verwenden, der als Abkürzung für

$$(A \Rightarrow B) \wedge (B \Rightarrow A)$$

steht, dem also der folgende Wahrheitswerteverlauf zugeordnet wird:

A	B	$A \Longleftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

.

Es zeigt sich also, daß zwei Aussagen genau dann äquivalent sind, wenn beide wahr oder beide falsch sind, das heißt, Äquivalenz ist dasselbe wie *Werteverlaufsgleichheit.* Äquivalente Aussagen sind sozusagen *gleichwertig.* Festzuhalten ist demnach insbesondere:

> **Aussagen können durch werteverlaufsgleiche, durch *äquivalente* Aussagen, ersetzt werden.**

1.1.2 Beispiele Offensichtlich sind $A \wedge B$ und $B \wedge A$ äquivalent, da werteverlaufsgleich. Interessanter sind die folgenden Fälle:

i) Anhand des Werteverlaufs kann man leicht nachprüfen, daß die umgangssprachliche Formulierung "entweder A oder B" in folgender Weise formalisiert werden kann:

$$(A \vee B) \wedge \neg(A \wedge B),$$

denn

A	B	$A \vee B$	$\neg(A \wedge B)$	$(A \vee B) \wedge \neg(A \wedge B)$
w	w	w	f	f
w	f	w	w	w
f	w	w	w	w
f	f	f	w	f

zeigt, daß diese Aussage genau dann den Wahrheitswert w bekommt, wenn genau einer der beiden Bestandteile A und B diesen Wert hat.

ii) Werteverlaufsgleich — und damit äquivalent — sind auch $A \wedge (B \vee C)$ und $(A \wedge B) \vee (A \wedge C)$, wie man leicht nachprüft. Damit werden wir dann im nächsten Paragraphen die Mengengleichheit $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ beweisen können.

$\diamond$

Als weitere Anwendung lassen sich Beweisverfahren begründen:

1.1.3 Anwendungen (Beweisverfahren)

i) Man kann leicht nachweisen, daß $A \Rightarrow B$ und $\neg B \Rightarrow \neg A$ werteverlaufsgleich sind, anstelle eines Beweises von $A \Rightarrow B$ kann man demnach genausogut die Implikation $\neg B \Rightarrow \neg A$ (die sogenannte *Kontraposition* von $A \Rightarrow B$) herleiten, manchmal geht das einfacher.

ii) $\neg(A \Rightarrow B)$ und $A \wedge \neg B$ sind werteverlaufsgleich, woraus sich das Verfahren des *indirekten* Beweisens ergibt: Unter der Annahme, daß $\neg B$ wahr sei, leitet man, unter Zuhilfenahme von A, einen Widerspruch her und hat damit $\neg(\neg(A \Rightarrow B))$, also $A \Rightarrow B$ bewiesen.

$\diamond$

1.1.4 Bemerkung Man kann sich die Wahrheitswertetafel leichter merken, wenn man w durch 1 und f durch 0 ersetzt, denn dann genügt die folgende einzeilige Tafel:

$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
$1 - w(A)$	$\mathrm{Min}\{w(A), w(B)\}$	$\mathrm{Max}\{w(A), w(B)\}$	$\mathrm{Max}\{1 - w(A), w(B)\}$

Diese Version zeigt auch, daß man die "binäre" Aussagenlogik leicht z.B. dadurch verallgemeinern kann, daß man Wahrheitswerte *zwischen* 0 und 1 zuläßt. Sie wird beispielsweise in einem modernen Zweig der (besonders anwendungsrelevanten) Mathematik zugrunde gelegt, der Mathematik des Unscharfen (fuzzy mathematics). ◇

Es gibt auch Sprachgebilde, die *Variable* $x, y, \ldots$ enthalten und durch Einsetzen oder Quantifizieren von Werten für die Variablen in Aussagen übergehen. Solche Sprachgebilde werden als *Aussageformen* bezeichnet. Die Quantifizierung von Variablen erfolgt durch Einsetzen — beispielsweise wird $s < r$ durch Einsetzen von $s = 2$ und $r = 3$ zu einer wahren Aussage — oder mit Hilfe der *Quantoren,*

$\forall$ (*Allquantor,* "für alle") und $\exists$ (*Existenzquantor,* "es gibt").

Bei Quantoren muß man unbedingt *die Reihenfolge beachten*, das zeigt folgendes Beispiel:

$$\begin{array}{ll} \forall\, r \in \mathbb{R} & \exists\, s \in \mathbb{R} : \quad s < r \\ \exists\, s \in \mathbb{R} & \forall\, r \in \mathbb{R} : \quad s < r \end{array}$$

Die erste Aussage ist offenbar wahr, die zweite dagegen falsch!

1.1.5 Bemerkung Wichtig ist festzuhalten, daß die *Negation* einer Aussage mit Quantoren dadurch vorgenommen werden kann, daß man *die Quantoren umdreht und die Aussage negiert:*

$$\neg\, (\forall\, \ldots\, \exists\, \ldots\, : A) \iff \exists\, \ldots\, \forall\, \ldots\, : \neg A.$$

◇

Aufgabe 1.1.1
Zeigen Sie, daß die für die Junktoren $\wedge$ und $\vee$ die folgenden Eigenschaften haben:

1. *Kommutativität:* $A \wedge B \iff B \wedge A$, $A \vee B \iff B \vee A$.
2. *Assoziativität:* $A \wedge (B \wedge C) \iff (A \wedge B) \wedge C)$, $A \vee (B \vee C) \iff (A \vee B) \vee C)$.
3. *Adjunktivität:* $A \wedge (A \vee B) \iff A$, $A \vee (A \wedge B) \iff A$.
4. *Distributivität:* $A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C)$, $A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$.

Aufgabe 1.1.2
Drücken Sie die die Implikationen $A \Rightarrow B$ und $A \Leftrightarrow B$ jeweils durch einen werteverlaufsgleichen Ausdruck aus, in dem nur A, B (eventuell mehrfach), Klammern und die Junktoren $\neg$ und $\wedge$ auftreten.

Aufgabe 1.1.3
Formulieren Sie die oben erwähnte Aussage

> Die Anzahl der positiven Teiler einer positiven natürlichen Zahl ist genau dann ungerade, wenn die Zahl ein Quadrat ist.

mit Hilfe von Quantoren und bilden Sie danach deren Negation. Geben Sie auch die Kontraposition der Aussage an.

Aufgabe 1.1.4
Zeigen Sie, da das folgende Problem (aus "Die Zeit") eindeutig lösbar ist:
„Ich verstehe die Welt nicht mehr", klagt der pnümmige Bauzel, während er seine Hupalap sömmelt, „ich meine die Mömse. Jeder Möms ist entweder ein Drausenflutz oder ein Hersenknautz. Aber wer von den sechs Mömsen nun ein Drausenflutz und wer ein Hersenknautz ist, das weiß man leider nicht mehr".
„Das weißt *du* nicht mehr", verbessert ihn die teutelige Saginse, „ich zum Beispiel weiß das sehr wohl".
„Dann erklä re es mir doch bitte", fleht der pnümmige Bauzel. Doch die teutelige Saginse erwidert schnippisch: „Das könnte dir so passen, du denkfauler Bauzel du. Aber ich will dir sechs Hinweise geben". Also hub die teutelige Saginse an:

1. „Sowohl der Aknitzmöms als auch der Buffelmöms sind Hersenknautze.
2. Der Flüpomöms ist ein Drausenflutz, und wenn der Eikumöms ein Drausenflutz ist, dann ist auch der Chrïlduffmöms einer.
3. Der Dintelmöms ist ein Hersenknautz, und wenn der Flüpomöms ein Drausenflutz ist, dann ist auch der Aknitzmöms ein Drausenflutz.
4. Aknitzmöms und Eikumöms sind beide Drausenflutze.
5. Der Dintelmöms ist ein Drausenflutz und der Eikumöms ist ein Hersenknautz, und wenn der Chröllduffmöms ein Drausenflutz ist, dann ist der Buffelmöms ein Hersenknautz.
6. Der Dintelmöms und der Buffelmöms sind beide Drausenflutze".

Verwirrt schaut der pnümmige Bauzel drein. Wie sehr er auch sein Hupalap sömmelt, er kann sich die sechs Hinweise nicht zusammenreimen. Dabei ist es doch so einfach. Freilich muß man bedenken, daß die teutelige Saginse, wie allgemein bekannt, eine Lügnerin ist, und jeder ihrer sechs Hinweise unwahr ist. Wer nämlich dies berücksichtigt, dem wird ein wenig Nachdenken erschließen, welcher Möms was ist.

1.2 Klassen und Mengen

Als undefinierten Grundbegriff verwenden wir den Begriff der *Klasse.* Dieser ist allgemeiner als der Mengenbegriff und wird in der Algebra zur Definition sogenannter *Kategorien* — zum Beispiel der "Kategorie aller Mengen" (s.u.) — benötigt. Klassen bezeichnen wir mit kleinen Buchstaben: $a, b, c, \ldots$ Gegeben sei eine *Elementbeziehung* $\in$ ("... ist Element von ..."), und für je zwei Klassen a und b gelte entweder $a \in b$ oder $\neg(a \in b)$ (hierfür schreiben wir auch kurz: $a \notin b$). Mit ihrer Hilfe definieren wir jetzt den Mengenbegriff:

1.2.1 Definition (Menge, Unmenge) Die Klassen x, die als Elemente auftreten können, also die Klassen x mit der Eigenschaft $\exists\ a\colon\ x \in a$, heißen *Mengen.* Hierfür schreiben wir auch kurz $\mathrm{Mg}(x)$, d.h. wir definieren

$$\mathrm{Mg}(x) :\Longleftrightarrow\ \exists\ a\colon\ x \in a.$$

Klassen, die keine Mengen sind, heißen *Unmengen.* Dies sind also die Klassen x mit $\neg\mathrm{Mg}(x)$. •

Aussagen der speziellen Gestalt $a \in b$ heißen *einfache* Aussagen. Mittels Junktoren oder Quantoren erhält man aus diesen die sogenannten *einschlägigen* Aussagen bzw. Aussageformen. Ein Bespiel ist die oben erwähnte Aussage über die Zahlen mit einer ungeraden Anzahl von Teilern. Mit diesen Begriffen können wir jetzt einige *Axiome* formulieren, deren Gültigkeit wir im folgenden unterstellen wollen.

1.2.2 Das Klassenbildungsaxiom *Zu jeder einschlägigen Aussageform $A(x)$ gibt es eine Klasse a, welche genau diejenigen Mengen als Elemente enthält, die der Aussageform genügen:*

$$\exists\ a\ \forall\ x:\ (x \in a)\ \Longleftrightarrow\ (Mg(x) \wedge A(x)).$$

Diese Klasse ist also durch $A(x)$ vollständig bestimmt. Die Gleichheit zweier Klassen kann mit Hilfe der Elementbeziehung so definiert werden:

$$a = b :\Longleftrightarrow\ \forall\ x\colon\ (x \in a)\ \Longleftrightarrow\ (x \in b).$$

Zwei Klassen sind also genau dann gleich, wenn sie dieselben Elemente enthalten. Sie sollen dadurch auch vollständig bestimmt sein, d.h. sich *beide bzgl. Elementbeziehung gleich* verhalten. Wir fordern deshalb

1.2.3 Das Umfangsbestimmtheitsaxiom *Klassen sind durch ihre Elemente eindeutig bestimmt:*

$$\forall\ a, b, c:\ ((a = b) \wedge (a \in c)) \Longrightarrow (b \in c).$$

Mit anderen Worten: Zwei Klassen sind genau dann gleich, wenn sie dieselben Elemente enthalten! Die durch $A(x)$ bestimmte Klasse können wir deshalb auch so beschreiben:

$$a = \{x \mid \mathrm{Mg}(x) \wedge A(x)\}.$$

1.2.4 Beispiele

i) $\emptyset := \{x \mid \mathrm{Mg}(x) \wedge \neg\mathrm{Mg}(x)\}$, die *leere Klasse,* sie enthält kein einziges Element. Schon im nächsten Axiom werden wir fordern, daß $\emptyset$ eine Menge ist.

ii) $\mathcal{R} := \{x \mid \mathrm{Mg}(x) \wedge x \notin x\}$, die *Russellsche Klasse,* sie ist eine Unmenge. Diese Behauptung ist eine Implikation:

$$(a = \mathcal{R}) \Rightarrow \neg\mathrm{Mg}(a),$$

wir verwenden zum Nachweis ihrer Gültigkeit die Methode des indirekten Beweisens.

Beweis: Die (indirekte) Annahme $\mathrm{Mg}(\mathcal{R})$ ergibt wie folgt einen Widerspruch:

- Falls $\mathcal{R} \in \mathcal{R}$ ist ergibt sich, wegen $\mathcal{R} := \{x \mid \mathrm{Mg}(x) \wedge x \notin x\}$ und der indirekten Annahme $\mathrm{Mg}(\mathcal{R})$, daß $\mathcal{R} \notin \mathcal{R}$, im Widerspruch zu dem hier betrachteten Fall $\mathcal{R} \in \mathcal{R}$.
- Sei umgekehrt $\mathcal{R} \notin \mathcal{R}$. Wir erhalten dann — wiederum nach der Definition von $\mathcal{R}$ und wegen der indirekten Annahme $\mathrm{Mg}(\mathcal{R})$ — daß $\mathcal{R} \in \mathcal{R}$, also auch hier einen Widerspruch. □

iii) $\mathcal{A} := \{x \mid \mathrm{Mg}(x)\}$, die *Allklasse,* sie enthält alle Mengen als Elemente und ist ebenfalls eine Unmenge (s.u.).

◇

1.2.5 Das Axiom der leeren Menge *Die leere Klasse ist eine Menge:*

$$Mg(\emptyset).$$

Gilt für zwei Klassen a und $b : \forall\, x :\ (x \in a) \Rightarrow (x \in b)$, dann heißt a *Teilklasse* von b und wir schreiben

$$a \subseteq b.$$

Gilt darüber hinaus noch $a \neq b$, dann schreiben wir

$$a \subset b.$$

(Leider ist die Verwendung dieser beiden Bezeichnungen in der Literatur nicht einheitlich, $\subset$ wird oft auch geschrieben, wenn Gleichheit zugelassen wird!) Die leere Klasse liegt in jeder anderen, und jede Klasse liegt in der Allklasse:

$$\forall\, a\colon\ \emptyset \subseteq a \subseteq \mathcal{A}.$$

1.2.6 Das Axiom der Teilmenge *Teilklassen von Mengen sind Mengen:*

$$(Mg(a) \wedge (b \subseteq a)) \Longrightarrow Mg(b).$$

Hiermit kann man zeigen, daß die Allklasse eine Unmenge ist (Übungsaufgabe!). Für die *Vereinigung* und den *Durchschnitt* zweier Klassen verwenden wir die üblichen Symbole

$$a \cup b := \{x \mid \mathrm{Mg}(x) \wedge (x \in a \vee x \in b)\}$$

und

$$a \cap b := \{x \mid \mathrm{Mg}(x) \wedge x \in a \wedge x \in b\}.$$

1.2.7 Das Axiom der Vereinigungsmenge *Die Vereinigung zweier Mengen ist wieder eine Menge:*

$$(Mg(a) \wedge Mg(b)) \Longrightarrow Mg(a \cup b).$$

Zusammen mit 1.2.6 ergibt sich daraus

1.2.8 Folgerung *Der Schnitt zweier Mengen ist ebenfalls eine Menge:*

$$(Mg(a) \wedge Mg(b)) \Longrightarrow Mg(a \cap b).$$

□

Für diese *Verknüpfungen* $\cap$ und $\cup$ von Klassen gelten die für Mengen bekannten Gesetze:

1.2.9 Eigenschaften von $\cap$ und $\cup$ *Für alle Klassen a, b, c gilt:*

$$a \cap (b \cap c) = (a \cap b) \cap c,\ a \cup (b \cup c) = (a \cup b) \cup c,$$

d. h. $\cap$ und $\cup$ sind assoziativ. *Es gilt auch*

$$a \cap b = b \cap a,$$

$\cap$ und $\cup$ sind demnach kommutativ. *Sie sind auch* idempotent:

$$a \cap a = a,\ a \cup a = a,$$

und es gelten die beiden Distributivgesetze:

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c),\ a \cup (b \cap c) = (a \cup b) \cap (a \cup c).$$

Beweis: Diese Gleichungen beweist man mit Hilfe der Aussagenlogik. Wir sehen uns dies für eine dieser Gleichungen genau an, die andere folgen ganz analog und sind Ihnen sowieso aus dem Schulunterricht bekannt!
Als Aussage A nehmen wir die Aussage $x \in a$, und als Aussagen B und C eintsprechend $x \in B$ bzw. $x \in C$. Weil — wie man leicht nachprüft — $A \wedge (B \vee C)$ werteverlaufsgleich ist mit $(A \wedge B) \vee (A \wedge C)$, haben wir also beispielsweise

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c).$$

□

Als *Komplementärklasse* bezeichnen wir

$$\overline{a} := \{x \mid \mathrm{Mg}(x) \wedge x \notin a\},$$

als *relatives Komplement* bzgl. der Klasse b :

$$a \backslash b := \{x \mid \mathrm{Mg}(x) \wedge (x \in a) \wedge (x \notin b)\}.$$

Hierfür gelten (bitte nachprüfen)

1.2.10 Die de Morganschen Regeln *Für Klassen a, b und deren absolute Komplemente gilt:*

$$\overline{a \cup b} = \overline{a} \cap \overline{b},\ \overline{a \cap b} = \overline{a} \cup \overline{b}.$$

Für relative Komplemente gilt

$$\overline{a \backslash b} = \overline{(a \cap \overline{b})} = \overline{a} \cup b.$$

1.2.11 Definition (Vereinigung und Schnitt) Vereinigung und Schnitt zweier Klassen können noch deutlich verallgemeinert werden: Zu einer einschlägigen Aussage A definieren wir

$$\bigcup_{x:\ A(x)} x := \{y \mid \mathrm{Mg}(y) \wedge \exists x(A(x) \wedge y \in x)\}$$

und

$$\bigcap_{x:\ A(x)} x := \{y \mid \mathrm{Mg}(y) \wedge \forall x(A(x) \Rightarrow y \in x)\}.$$

•

1.2.12 Beispiele Spezialfälle einschlägiger Aussagen sind die einfachen Aussagen wie $x \in a$, wir erhalten also die Beispiele

$$V(a) := \bigcup_{x \in a} x = \{y \mid \mathrm{Mg}(y) \wedge (\exists\ x \in a:\ y \in x)\},$$

$$S(a) := \bigcap_{x \in a} x = \{y \mid \mathrm{Mg}(y) \wedge (\forall\ x \in a:\ y \in x)\}.$$

◇

1.2.13 Das große Axiom der Vereinigungsmenge

$$Mg(a) \iff Mg(V(a)).$$

1.2.14 Definition (Einerklasse) Wir definieren zunächst zu jeder Klasse a die sogenannte *Einerklasse*

$$\{a\} := \{x \mid \mathrm{Mg}(x) \wedge (\mathrm{Mg}(a) \Rightarrow x = a)\}.$$

•

Ist a eine Menge, dann ist $\{a\}$ eine Klasse, die ein einziges Element enthält, nämlich a. Ist dagegen a keine Menge, dann ist $\{a\}$ die Allklasse. Die Bildung der Einerklasse ist also eigentlich nur für Mengen interessant. Wir verwenden diese Klassenbildung auch zur Einführung der Klassen

$$\{a, b\} := \{a\} \cup \{b\}, \{a, b, c\} := \{a\} \cup \{b\} \cup \{c\}, \ldots$$

Als nächstes wird gefordert, daß die Einerklasse einer Menge ebenfalls Menge ist:

1.2.15 Das Axiom der Einermenge: $Mg(a) \Longrightarrow Mg(\{a\})$.

Diese Mengen werden entsprechend als *Einermengen* bezeichnet.

1.2.16 Beispiele (die natürlichen Zahlen) Wir haben bereits durch ein Axiom gefordert, daß die leere Klasse eine Menge sei. Diese definieren wir als *die natürliche Zahl* 0:

$$0 := \emptyset,$$

und wir erhalten daraus Mg(0), die natürliche Zahl Null *ist* die leere Menge.
Daraus ergibt sich die natürliche Zahl 1 als die vielleicht wichtigste Einermenge:

$$1 := \{\emptyset\} = \{0\}.$$

Nach dem Axiom der Einermenge ist also auch diese natürliche Zahl eine Menge! Ganz entsprechend wird dann

$$2 := \{0, 1\}$$

gesetzt, die natürliche Zahl n ist

$$n := \{0, 1, \ldots, n-1\}.$$

Nach dem gleich folgenden Prinzip der vollständigen Induktion sind damit alle natürlichen Zahlen definiert. ◇

1.2.17 Definition (die Klasse $\mathbb{N}$ der natürlichen Zahlen) Wir definieren zunächst zu jeder Klasse a deren *Nachfolger:*

$$a^+ := a \cup \{a\}.$$

Die Klasse $\mathbb{N}$ der natürlichen Zahlen wird als die kleinste Klasse definiert, welche die Null und zu jedem ihrer Elemente auch deren Nachfolger enthält:

$$\mathbb{N} := \bigcap_{0 \in a, \forall x (x \in a \Rightarrow x^+ \in a)} a.$$

•

Wir fordern schließlich, daß $\mathbb{N}$ eine Menge ist:

1.2.18 Axiom der Menge der natürlichen Zahlen: $Mg(\mathbb{N})$.

Eine unmittelbare Folgerung hieraus ist der nachstehende Satz, der ein weiteres sehr wichtiges Beweisprinzip beschreibt, die sogenannte *vollständige Induktion.* Sie besagt, daß jede Aussage $A(x)$ für *alle* natürlichen Zahlen x wahr ist, wenn man zeigen kann, daß $A(0)$ wahr ist und auch (für beliebiges n) die Implikation $A(n) \Rightarrow A(n^+)$. (Beim Beweis dieser Implikation kann man voraussetzen, daß $A(0), A(1), \ldots, A(n-1)$ wahr sind.)

1.2.19 Satz *(Prinzip der vollständigen Induktion)*

$$[(M \subseteq \mathbb{N}) \wedge (0 \in M) \wedge (\forall\ x\colon\ (x \in M) \Rightarrow (x^+ \in M))] \Longrightarrow (M = \mathbb{N})$$

Beweis: Wegen der Voraussetzung

$$(0 \in M) \wedge (\forall\ x\colon\ (x \in M) \Rightarrow (x^+ \in M))]$$

gilt $\mathbb{N} \subseteq M$. Da auch $M \subseteq \mathbb{N}$ gelten soll, folgt mit der Antisymmetrie von $\subseteq$ die Gleichheit $M = \mathbb{N}$. □

Schließlich definieren wir noch die *Potenzklasse* von a :

$$P(a) := \{x \mid \mathrm{Mg}(x) \wedge x \subseteq a\}.$$

Aufgabe 1.2.1
Zeigen Sie, daß es sich bei "Die Anzahl der positiven Teiler einer positiven natürlichen Zahl ist genau dann ungerade, wenn die Zahl ein Quadrat ist" um eine einschlägige Aussage handelt.

Aufgabe 1.2.2
Die durch das Umfangsbestimmtheitsaxiom definierte Gleichheit von Klassen hat die folgenden Eigenschaften: Sie ist

- *reflexiv:* $a = a$,
- *symmetrisch:* $(a = b) \Rightarrow (b = a)$,
- *transitiv:* $((a = b) \wedge (b = c)) \Rightarrow (a = c)$.

Aufgabe 1.2.3
Die Teilklassenbeziehung hat die folgenden Eigenschaften: Sie ist

- *reflexiv:* $a \subseteq a$,
- *antisymmetrisch:* $((a \subseteq b) \wedge (b \subseteq a)) \Rightarrow (a = b)$,
- *transitiv:* $((a \subseteq b) \wedge (b \subseteq c)) \Rightarrow (a \subseteq c)$.

Aufgabe 1.2.4
Zeigen Sie ausführlich, daß gilt $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$, und beweisen Sie die de Morgansche Regel $\overline{a \cup b} = \overline{a} \cap \overline{b}$.

Aufgabe 1.2.5
Spezialfälle der Distributivgesetze sind die Gesetze der *Absorption:*

$$a \cap (b \cup a) = a = a \cup (b \cap a).$$

Mathematische Strukturen mit zwei Verknüpfungen (genaue Definition folgt weiter unten) wie $\cup$ und $\cap$, die kommutativ, assoziativ, idempotent und absorptiv sind, heißen *Verbände.* Zeigen Sie deshalb, daß die Gesetze der Absorption gelten. (Sie haben dann bewiesen, daß die Klassen und auch die Mengen einen Verband bzgl. $\cup$ und $\cap$ bilden!)

Aufgabe 1.2.6
Zeigen Sie, da für drei Klassen a, b, c stets gilt:

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c).$$

1.3 Relationen und Funktionen

Es gibt eine Konstruktion (Übungsaufgabe!) einer Klasse (a, b) mit der Eigenschaft

$$(a, b) = (c, d) \iff a = c \wedge b = d.$$

Diese Klasse (a, b) heißt auch das *(geordnete) Paar* aus a und b. Es gilt

$$(\mathrm{Mg}(a) \wedge \mathrm{Mg}(b)) \iff \mathrm{Mg}((a, b)).$$

Entsprechend kann man *Tripel, Quadrupel, ... n-tupel* definieren:

$$(a, b, c) := ((a, b), c), \ldots$$

etc. Als *cartesisches Produkt* zweier Klassen definiert man die Klasse aus den geordneten Paaren ihrer Elemente:

$$a \times b := \{(x, y) \mid (x \in)a \wedge (y \in b)\}.$$

Hier gilt entsprechend

$$(\mathrm{Mg}(a) \wedge \mathrm{Mg}(b)) \iff \mathrm{Mg}(a \times b).$$

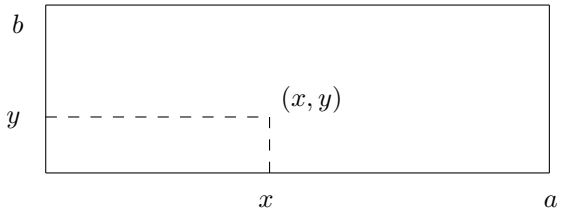
Diese Konstruktion kann natürlich iteriert werden, z.B. sei

$$a \times b \times c := (a \times b) \times c,$$

usw. Wir schreiben auch

$$a^n := \underbrace{a \times \ldots \times a}_{n \ Faktoren}.$$

Das cartesische Produkt $a \times b$ zweier Mengen veranschaulicht man sich gerne als Rechteck, wobei der linke Rand die Menge b, der untere Rand die Menge a bedeutet:



Prominenteste Beispiele sind die cartesischen Produkte $\mathbb{R} \times \mathbb{R}$ und $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$, die reelle Zahlenebene und der dreidimensionale reelle "Anschauungsraum". Aus schreibtechnischen Gründen erweist es sich später (bei der Verwendung von Vektoren) als zweckmäßig, geordnete Paare, Tripel, ... n-Tupel, nicht nur in *Zeilenschreibweise,* als $(a, b, \ldots)$ einzuführen, sondern gelegentlich auch in *Spaltenschreibweise* zu notieren, d. h. in der Form

$$\begin{pmatrix} a \\ b \\ \vdots \end{pmatrix}.$$

1.3.1 Definition (Relation, Funktion)

- Unter einer *(zweistelligen) Relation* verstehen wir eine Teilklasse R der Allklasse, also $R \subseteq \mathcal{A} \times \mathcal{A}$.
- Mit einer (zweistelligen) Relation *zwischen* zwei Klassen a und b meinen wir eine Teilklasse des cartesischen Produkts dieser beiden Klassen:

  $$R \subseteq a \times b.$$

  Für $(x, y) \in R$ schreiben wir auch kurz: xRy.
- Als *Definitionsbereich* von $R \subseteq a \times b$ bezeichnen wir

  $$\mathrm{Def}(R) := \{x \in a \mid \exists\, y \in b\colon\ xRy\}.$$
- Das *Bild* von $R \subseteq a \times b$ ist

  $$\mathrm{Bild}(R) := \{y \in b \mid \exists\, x \in a\colon\ xRy\}.$$
- Die *Umkehrrelation* zu $R \subseteq a \times b$ sei

  $$R^{-1} := \{(y, x) \mid xRy\} \subseteq b \times a.$$
- Die *Komposition* zweier Relationen $R, S \subseteq \mathcal{A} \times \mathcal{A}$ wird definiert als

  $$S \circ R := \{(x, z) \mid \exists\, y\colon (xRy \wedge ySz)\}.$$

  Gelesen wird die Komposition als "erst R, dann S", also *von rechts nach links.*
- Eine Relation R heißt *rechtseindeutig,* wenn gilt

  $$(xRy \wedge xRz) \Rightarrow y = z.$$

  Entsprechend ist die Definition von *linkseindeutig.*
- Rechtseindeutige Relationen heißen *Funktionen* oder (synonym) *Abbildungen.*

•

Beispiele solcher Relationen, die Sie kennen, sind die Gleichheitsrelation $=$, die Relation $\leq$ zwischen reellen Zahlen (d.h. $a = b = \mathbb{R}$), und auch die Teilerrelation zwischen natürlichen Zahlen (d.h. $a = b = \mathbb{N}$),

$$m \mid n :\Longleftrightarrow\ m \text{ teilt } n.$$

Unter einer Funktion *f von a nach b,* also einer rechtseindeutigen Relation $f \subseteq a \times b$, kurz: $f\colon a \to b$, versteht man demnach genau genommen das Tripel

$$(a, \{(x, y) \mid x \in \mathrm{Def}(f), y \in \mathrm{Bild}(f), (x, y) \in f\}, b).$$

Ist $(x, y) \in f$, dann schreibt man auch $f(x)$ anstelle von y, kürzt die mit $x \mapsto y$ ab und nennt y den *Wert von f an der Stelle x*. Man läßt jedoch bei der Beschreibung von Funktionen die beiden Klassen a und b gerne weg und betrachtet nur

$$\mathrm{Graph}(f) := \{(x, y) \mid (x \in a) \wedge (y \in b) \wedge ((x, y) \in f)\} \subseteq a \times b,$$

den sogenannten *Graphen* von f. Die Funktion wird also oft einfachheitshalber mit ihrem Graphen identifiziert. Zur Definition einer Funktion f dient meistens eine (weitgehend standardisierte) Schreibweise der folgenden Form:

$$f\colon\ a \to b,\ x \mapsto f(x),$$

also z.B.

$$f\colon\ \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$$

für die Ihnen aus der Schulzeit bekannte Funktion, deren Graph eine Parabel ist. Schließlich sei noch bemerkt, daß für die Komposition $f \circ g$ zweier Funktionen gilt:

$$(f \circ g)(x) = f(g(x)),$$

es folgt aus der Rechtseindeutigkeit.

Unter den Funktionen heben wir spezielle Typen durch Attribute hervor:

1.3.2 Definition (injektiv, surjektiv, bijektiv) Sei f eine Funktion zwischen a und b, wir sagen

- f sei *injektiv,* falls f^{-1} eine Funktion ist. Diese Forderung ist äquivalent zu
$$(f(x) = f(x')) \Rightarrow x = x'.$$
Wir werden dies auch so abkürzen:
$$f\colon a \rightarrowtail b.$$

- f ist *surjektiv,* wenn f eine Abbildung *auf* (=sur) b ist, also wenn
$$\forall\ y \in b\ \exists\ x \in a:\ f(x) = y.$$
Diese Forderung ist äquivalent zu
$$\mathrm{Bild}(f) = b,$$
kurz
$$f\colon a \twoheadrightarrow b.$$

- f sei *bijektiv,* wenn f sowohl injektiv als auch surjektiv ist. Als Abkürzung verwenden wir
$$f\colon a \rightarrowtail\!\!\!\!\!\twoheadrightarrow b.$$

- f heiße *Einbettung (von a in b),* wenn f injektiv ist und $\mathrm{Def}(f) = a$ gilt.

- f nennen wir die *identische* Abbildung oder *Identität,* wenn $b = a$ gilt und $f(x) = x$, für alle $x \in a$.

•

Mit Hilfe bijektiver Abbildungen werden wir jetzt den Begriff der *Ordnung* einer Klasse einführen. Man kann nämlich zeigen, daß es zu jeder Klasse a *höchstens ein* $n \in \mathbb{N}$ gibt mit $a \rightarrowtail\!\!\!\!\!\rightarrow n$ (eine Abkürzung für die Existenz einer Bijektion von a auf n). Dieses n nennt man (gegebenenfalls) die *Kardinalzahl, Mächtigkeit* oder *Ordnung* von a. Man nennt a dann *endlich* und kürzt dies mit $|a| = n$ ab, d. h. man definiert

1.3.3 $$(|a| = n) :\Longleftrightarrow\ (a \rightarrowtail\!\!\!\!\!\rightarrow n).$$

Andernfalls schreibt man $|a| = \infty$ und nennt a *unendliche* Klasse. Im Fall $a \rightarrowtail\!\!\!\!\!\rightarrow \mathbb{N}$ sagt man auch, die Klasse a sei *abzählbar* unendlich.

Funktionen mit geeigneten Eigenschaften sind wichtige *Werkzeuge* in der linearen Algebra und der Algebra. Betrachten wir ein ganz einfaches Beispiel hierfür, nämlich den Beweis der Aussage, die ganz am Anfang des ersten Paragraphen erwähnt wurde:

> Die Anzahl der positiven Teiler einer positiven natürlichen Zahl ist genau dann ungerade, wenn die Zahl ein Quadrat ist.

Betrachten wir dazu eine positive natürliche Zahl n und die Menge $T(n)$ ihrer positiven Teiler:

$$T(n) := \{t \in \mathbb{N} \mid t|n\}.$$

Auf dieser Menge betrachten wir die Abbildung f, die dem Teiler t den Teiler $\frac{n}{t}$ zuordnet. Sie gruppiert die Elemente von $T(n)$ in Teilmengen $\{t, \frac{n}{t}\}$, die offenbar aus 1 oder 2 Elementen bestehen. Maximal *eine* solche Teilmenge besteht aus einem einzigen Element, sie existiert genau dann, wenn es einen Teiler t gibt mit $t = \frac{n}{t}$, also genau dann, wenn n ein Quadrat ist: $n = t^2$. Das beweist die Behauptung!

Sehr hilfreich sind die folgenden Charakterisierungen von injektiv, surjektiv und bijektiv:

1.3.4 Satz *Sei f eine Abbildung zwischen einer nicht leeren Klasse a und einer (wegen $a \neq \emptyset$ ebenfalls nicht leeren) Klasse b, und es gelte* $\mathrm{Def}(f) = a$. *Dann gilt:*

- *f ist genau dann injektiv, wenn es eine Linksinverse gibt:*

$$\exists\ g :\ b \to a\ (g \circ f = \mathrm{id}_a).$$

- *f ist genau dann surjektiv, wenn es eine Rechtsinverse gibt:*

$$\exists\ g :\ b \to a\ (f \circ g = \mathrm{id}_b).$$

- *f ist genau dann bijektiv, wenn es sowohl eine Rechts- als auch eine Linksinverse gibt. Diese sind gleich.*
- *f ist genau dann injektiv, wenn f linkskürzbar ist, d. h. wenn gilt:*

$$(f \circ g = f \circ h) \Longrightarrow g = h.$$

- *f ist genau dann surjektiv, wenn f rechtskürzbar ist:*

$$(g \circ f = h \circ f) \Longrightarrow g = h.$$

Beweis: Wir beweisen die erste Behauptung, die restlichen werden analog bewiesen (Übungsaufgabe!):

a) Wir setzen zunächst voraus, f sei injektiv, und wir konstruieren eine Abbildung $g\colon b \to a$ mit den geforderten Eigenschaften: a ist nicht leer, es gibt also mindestens ein Element $x_0 \in a$. Hiermit setzen wir

1.3.5
$$g\colon b \to a,\ y \mapsto \begin{cases} x, & \text{falls } y = f(x), \\ x_0, & \text{falls } y \notin \mathrm{Bild}(f). \end{cases}$$

Hier ist es wichtig zu beachten, daß dies *noch genau begründet werden muß, denn so wie es da steht ist das keine Definition!* g ist nämlich nur dann eine Funktion, wenn jedem $y \in b$ auf diese Weise *eindeutig* ein Element aus a zugeordnet wird. Die Zuordnung "x, falls $y = f(x)$" ist aber nicht immer eindeutig, da es ja — ohne weitere Voraussetzungen an f — *mehrere* x geben kann mit $f(x) = y$! Hier ist das glücklicherweise nicht der Fall, denn f ist ja als injektiv vorausgesetzt. Man formuliert dies kurz und knapp so: Wegen der Injektivität von f ist g durch 1.3.5 *wohldefiniert.*

Es bleibt jetzt nur noch $g \circ f = \mathrm{id}_a$ nachzuprüfen, was sehr leicht ist. Aus der Injektivität folgt also tatsächlich die Existenz einer Linksinversen.

b) Existiert umgekehrt eine Linksinverse g, dann ist f injektiv, denn eine Anwendung von g auf beide Seiten einer Gleichung $f(x) = f(x')$ ergibt

$$x = (g \circ f)(x) = (g \circ f)(x') = x',$$

f ist also injektiv.

Damit ist die erste Behauptung bewiesen.

□

Das nächste Axiom ermöglicht den Nachweis, daß Bilder von Mengen ebenfalls Mengen sind:

1.3.6 Das Ersetzungsaxiom: *Ist f eine Funktion mit einer Menge als Definitionsbereich, dann ist auch das Bild eine Menge:*

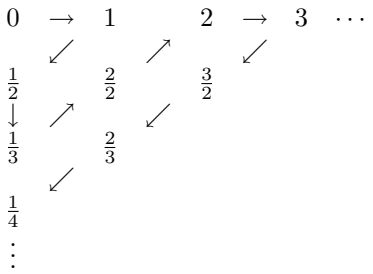
$$Mg(\mathrm{Def}(f)) \Longrightarrow Mg(\mathrm{Bild}(f)).$$

1.3.7 Anwendungen ($\mathbb{N}^n$ und $\mathbb{Q}$ sind Mengen)

- Das cartesische Produkt zweier Mengen ist ebenfalls eine Menge (Übungsaufgabe!) Daraus folgt unter anderem die Tatsache, daß die Menge der n-Tupel natürlicher Zahlen eine Menge ist:

$$\mathrm{Mg}(\mathbb{N}^n)$$

- Wir können $\mathbb{N}$ auf die Klasse $\mathbb{Q}_{\geq 0}$ der nicht negativen rationalen Zahlen abbilden, etwa mit Hilfe der im folgenden skizzierten Abbildung (die Pfeile deuten die Reihenfolge an, in der die rationalen Zahlen $\frac{i}{k}$ den natürlichen Zahlen $0, 1, 2, \ldots$ zugeordnet werden sollen, die ersten 10 Funktionswerte sind angegeben, daß einige Werte mehrfach auftreten macht nichts, es ist wegen der besseren Überschaubarkeit in Kauf genommen):



  Mit dem Ersetzungsaxiom ergibt sich hieraus $\mathrm{Mg}(\mathbb{Q}_{\geq 0})$, ganz analog folgt $\mathrm{Mg}(\mathbb{Q}_{\leq 0})$, insgesamt also mit dem Axiom der Vereinigungsmenge:

$$\mathrm{Mg}(\mathbb{Q}).$$

$\diamond$

Die n-te cartesische Potenz a^n einer Klasse a kann als Menge von Abbildungen aufgefaßt werden: $(x_0, \ldots, x_{n-1}) \in a^n$ wird dazu einfach als die folgende Abbildung interpretiert:

$$f\colon n \to a, i \mapsto x_i.$$

Die n-te cartesische Potenz a^n einer *Menge* a ist also eine Menge, beispielsweise auch $\mathbb{Q}^n$. Eine Verallgemeinerung des oben eingeführten cartesischen Produkts $a \times b$ zweier Klassen und der cartesischen Potenz a^n einer Klasse ist, für eine Menge I (eine sogenannte *Indexmenge*), und gegebene Klassen a_i, für alle $i \in I$, die Bildung von

$$\times_{i \in I} a_i := \{f\colon I \to \bigcup_{i \in I} a_i \mid \forall\, i \in I\colon\ f(i) \in a_i\}.$$

Schließlich führen wir noch ein letztes Axiom an, das die *Existenz* gewisser Funktionen, sogenannter *Auswahlen* fordert:

1.3.8 Das Auswahlaxiom: *Ist I eine nicht leere Indexmenge, $I \neq \emptyset$, und ist zu jedem Index $i \in I$ eine Klasse $a_i \neq \emptyset$ vorgegeben (kurz: eine* Folge, Familie *oder auch* indiziertes Klassensystem $(a_i)_{i\in I}$ *nicht leerer Klassen), dann gilt*

$$\times_{i\in I} a_i \neq \emptyset,$$

d.h. es gibt Auswahlen!

Es ist vielleicht auf den ersten Blick nicht einleuchtend, daß es ohne dieses Axiom Probleme geben könnte. Vergleichen Sie aber einmal die folgenden beiden Situtationen: Wenn die a_i Paare von Handschuhen sind, ist es leicht, eine Auswahl anzugeben, beispielsweise "die linken Handschuhe". Handelt es sich aber um Paare von Socken, dann wird es zumindest schwierig. Solche Fälle schließt man besser aus! Dieses Axiom wird selten herangezogen werden, es ist aber wichtig und kann auch scheinbar ganz anders formuliert werden. Die prominentesten, zum Auswahlaxiom äquivalenten, Forderungen sind die Gültigkeit des *Wohlordnungssatzes* und das *Zornsche Lemma.* Wir werden es beim Beweis des Satzes verwenden, daß alle Vektorräume Basen besitzen.

Aufgabe 1.3.1
Seien a und b Mengen. Zeigen Sie, daß durch $(a, b) := \{\{a\}, \{a, b\}\}$ das geordnete Paar definiert werden kann, d.h.: Zeigen Sie:
Sind a, b, c, d Mengen, dann gilt

$$(a, b) = (c, d) \quad \text{genau dann, wenn} \quad a = c \wedge b = d.$$

Aufgabe 1.3.2
Seien M, N nichtleere Mengen und $f\colon M \to N$ eine Abbildung. Zeigen Sie:
f ist genau dann surjektiv, wenn f eine Rechtsinverse $g\colon N \to M$ besitzt.

Aufgabe 1.3.3
Seien M, N nichtleere Mengen und $f\colon M \to N$ eine Abbildung. Zeigen Sie:

a) f ist genau dann surjektiv, wenn f rechtskürzbar ist, (d.h. wenn aus $g \circ f = h \circ f$ stets folgt $g = h$).

b) f ist genau dann injektiv, wenn f linkskürzbar ist, (d.h. wenn aus $f \circ g = f \circ h$ stets folgt $g = h$).

1.4 Äquivalenzrelationen

Nachdem nun die axiomatische Grundlage gelegt ist, können wir uns — bis zur Einführung der Kategorien — das Leben dadurch erleichtern, daß wir bis dorthin, also *bis auf weiteres, voraussetzen, alle betrachteten Klassen seien Mengen.* Um dies deutlich zu machen, verwenden wir für die betrachteten Mengen Großbuchstaben wie $L, M, N, \ldots$ Darüberhinaus unterstellen wir, daß $f\colon M \to N$ stets bedeute, *M sei der Definitionsbereich von f.*

1.4.1 Definition (Äquivalenzrelation) Sei $R \subseteq M \times M$, kurz: *eine Relation auf M*. Sie heißt genau dann *Äquivalenzrelation,* wenn sie reflexiv, symmetrisch und transitiv ist, also wenn, für alle $x, y, z \in M$, folgendes gilt:

$$xRx \text{ (Reflexivität)},$$

$$xRy \Rightarrow yRx \text{ (Symmetrie)},$$

$$((xRy) \wedge (yRz)) \Rightarrow xRz \text{ (Transitivität)}.$$

Die zu einem Element m von M äquivalenten Elemente bilden die sogenannte *Äquivalenzklasse* von m :

$$[m]_R := \{m' \mid mRm'\}.$$

•

Die wichtigste Eigenschaft von Äquivalenzrelationen ist die folgende:

1.4.2 Satz *Jede Äquivalenzrelation R auf einer Menge M ergibt eine* Partition *von M, das heißt eine* vollständige *Zerlegung von M,*

$$\bigcup_{m \in M} [m]_R = M,$$

in disjunkte *Teilmengen:*

$$([m]_R \neq [m']_R) \Rightarrow ([m]_R \cap [m']_R = \emptyset).$$

Beweis: Die Reflexivitätsbedingung garantiert, daß jedes m in mindestens einer Äquivalenzklasse liegt, z.B. in $[m]_R$. Mit Transitivität und Symmetrie folgt, daß verschiedene Klassen disjunkt sind:

$$[m]_R \neq [m']_R \Longrightarrow [m]_R \cap [m']_R = \emptyset.$$

Wir beweisen die Kontraposition hiervon: Sei $x \in [m]_R \cap [m']_R$. Es gilt hierfür nach der Definition der Äquivalenzklasse: $mRx \wedge m'Rx$. Mit der Symmetrieeigenschaft von R folgt $mRx \wedge xRm'$, was mit der Transitivität die Äquivalenz von m und m' liefert, mRm'. Hieraus ergibt nochmalige Anwendung von Transitivität und Symmetrie die beiden Inklusionen $[m]_R \subseteq [m']_R$ und $[m]_R \supseteq [m']_R$, woraus die Gleichheit der beiden Äquivalenzklassen folgt. □

1.4.3 Beispiele

- Die Gleichheit $=$ ist eine Äquivalenzrelation (auf jeder Menge M).
- Jede vollständige Zerlegung in disjunkte Teilmengen $M = \dot{\bigcup}_{i \in I} M_i$ liefert eine Äquivalenzrelation R :

$$mRm' :\Longleftrightarrow \exists\, i\colon\ m, m' \in M_i.$$

- Jede Funktion $f\colon M \to N$ (bzw. kurz: $f \in N^M$) induziert auf ihrem Definitionsbereich M die folgende Relation R_f :

$$mR_f m' :\Longleftrightarrow f(m) = f(m').$$

  Diese Äquivalenzrelation heißt auch die von f auf M *induzierte* Äquivalenzrelation.

$\diamond$

Zu einer gegebenen Äquivalenzrelation R auf M bezeichnen wir mit M_R die Menge ihrer Äquivalenzklassen:

$$M_R := \{[m]_R \mid m \in M\}.$$

Viele Strukturen der Mathematik können als solche Äquivalenzklassenmengen definiert werden, d.h. durch Wahl geeigneter Mengen M und geeigneter Äquivalenzrelationen auf diesen. Besonders prominente Beispiele sind die folgenden

1.4.4 Beispiele (Konstruktion von $\mathbb{Z}$ und $\mathbb{Q}$)

- Die Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$: Ihr liegt die Idee zugrunde, daß man jede ganze Zahl z als Differenz zweier natürlicher Zahlen n_1, n_2 schreiben kann: $z = n_1 - n_2$. Dabei ist allerdings zu beachten ist, daß diese Darstellung nicht eindeutig ist, man faßt deshalb die Paare (n_1, n_2), mit deren Hilfe man z als solche Differenz darstellen kann *zu einer Äquivalenzklasse zusammen:*

  Wir betrachten $\mathbb{N}$ und setzen die Addition natürlicher Zahlen als bekannt voraus (die man auch als mengentheoretische Operation formulieren kann: $n + m := (n + (m - 1))^+$). Auf $\mathbb{N} \times \mathbb{N}$ betrachten wir die folgende Äquivalenzrelation:

$$(n_1, n_2)R(n_3, n_4) :\Longleftrightarrow n_1 + n_4 = n_2 + n_3.$$

  Wir setzen dann

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})_R,$$

  und anstelle von $[(n_1, n_2)]_R$ schreiben wir $n_1 - n_2$, falls $n_1 > n_2$ bzw. $-(n_2 - n_1)$, falls $n_1 < n_2$, und 0 sonst.

- Die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$: Hier liegt — dem vorigen Punkt ganz entsprechend — die Idee zugrunde, daß jede rationale Zahl ja ein Quotient $r = \frac{z_1}{z_2}$ aus ganzen Zahlen ist, wobei der Nenner natürlich von Null verschieden sein muß. Diese Darstellung ist ebenfalls nicht eindeutig, so daß die entsprechende Äquivalenzrelation betrachtet wird:

  Gegeben sei $\mathbb{Z}$ und die Multiplikation ganzer Zahlen (auch diese läßt sich mengentheoretisch einführen, ähnlich wie die Addition!). Die Menge der von Null verschiedenen ganzen Zahlen sei mit $\mathbb{Z}^*$ bezeichnet, auf $\mathbb{Z} \times \mathbb{Z}^*$ wird die folgende Äquivalenzrelation betrachtet:

  $$(z_1, z_2)R(z_3, z_4) :\Longleftrightarrow\ z_1 \cdot z_4 = z_2 \cdot z_3.$$

  Wir setzen

  $$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)_R$$

  und bezeichnen die Äquivalenzklassen wie üblich in der folgenden Weise:

  $$\frac{z_1}{z_2} := [(z_1, z_2)]_R.$$

  Für diese *Brüche* gilt infolgedessen:

  $$\frac{z_1}{z_2} = \frac{z_3}{z_4} \iff z_1 \cdot z_4 = z_2 \cdot z_3.$$

- Viele Strukturen in Mathematik und Naturwissenschaften kann man bequem mit Hilfe von Äquivalenzrelationen auf Mengen von Abbildungen definieren. Ein interessantes Beispiel bilden die (unnumerierten) Graphen, die man als Äquivalenzklassen numerierter Graphen definiert, wie wir gleich sehen werden. Numerierte Graphen kann man nicht vermeiden, denn beispielsweise sind Computer "nur" zur Verarbeitung von Mengen in der Lage, deren Elemente Nummern tragen.

  Die *numerierten* Graphen mit n Punkten kann man wie folgt als Menge

  $$Y^X := \{f \mid f\colon X \to Y\}$$

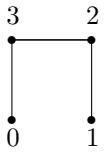
  aller Abbildungen von einer geeigneten Menge X in eine geeignete Menge Y definieren. Man numeriert zunächst die Punkte von 0 bis $n-1$ und identifiziert die Menge $n = \{0, \ldots, n-1\}$ der Nummern der Punkte mit der Punktemenge selbst. Dann betrachtet man die Menge der *Punktepaare,*

  $$\binom{n}{2} := \{\{i, j\} \mid i, j \in n, i \neq j\}.$$

  Für X nimmt man diese Menge, für Y die Menge $2 = \{0, 1\}$ und betrachtet die Menge von Abbildungen

  $$Y^X := 2^{\binom{n}{2}}$$

von der Menge der Punktepaare in die Menge $\{0,1\}$. Ist γ in dieser Menge, dann interpretiert man den Wert $\gamma(\{i,j\}) = 1$ als "die Punkte i und j sind durch eine Kante verbunden". Hier ist ein Beispiel:

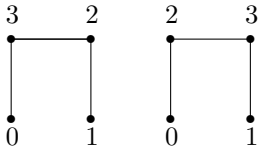


Dieser Graph wird auf diese Weise mit der folgenden Abbildung identifiziert:

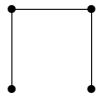
$$f\colon \binom{4}{2} \to \{0,1\},\ \begin{cases} \{0,1\} \mapsto 0, \\ \{0,2\} \mapsto 0, \\ \{0,3\} \mapsto 1, \\ \{1,2\} \mapsto 1, \\ \{1,3\} \mapsto 0, \\ \{2,3\} \mapsto 1. \end{cases}$$

Demnach kann die Menge der numerierten Graphen mit n Punkten mit dieser Menge von Abbildungen $\gamma\colon \binom{n}{2} \to \{0,1\}$ gleichgesetzt werden.

Die *unnumerierten* Graphen mit n Punkten definiert man — weil es bei ihnen auf die Nummern der Punkte nicht mehr ankommt — als die Äquivalenzklassen der folgenden Relation R : Zwei numerierte Graphen heißen *äquivalent* oder *isomorph,* wie man auch sagt, wenn sie durch Umnumerierung auseinander hervorgehen. Hier sind zwei äquivalente Graphen mit 4 Punkten:



Da beliebiges Umnumerieren zugelassen wird, kann man eine solche Äquivalenzklasse numerierter Graphen durch einen Graphen repräsentieren, den man durch Weglassen der Nummern aus irgendeinem Element der Klasse bekommt. Hier ist der unserem Beispiel auf diese Weise entsprechende *unnumerierte Graph:*



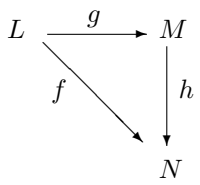
Solche unnumerierten Graphen dienen als *Wechselwirkungsmodelle* in Chemie, Physik und Wirtschaftswissenschaften, zum Beispiel zur Beschreibung von Molekülen (ein bekanntes Beispiel ist der Benzolring) oder von Schaltkreisen oder von Betriebsabläufen (Netzplantechnik) usw.

$\diamond$

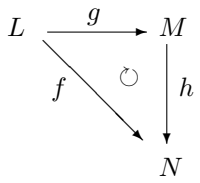
Es ist bereits erwähnt worden, daß Abbildungen ein wichtiges Werkzeug zur Untersuchung von algebraischen Strukturen sind. Oft sind diese Funktionen recht kompliziert, und man sucht nach Wegen, ihre Anwendung in kleine, möglichst übersichtliche Schritte zu zerlegen. Beispielsweise kann man oft eine gegebene Funktion $f\colon L \to N$ in zwei Faktoren $g\colon L \to M$ und $h\colon M \to N$ zerlegen, sie *faktorisieren:* $f = h \circ g$, als Komposition zweier Abbildungen schreiben. Zur Erinnerung:

$$f(x) = (h \circ g)(x) = h(g(x)).$$

Man drückt das gerne in Form eines *Diagramms* aus:

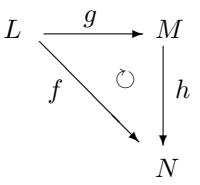


Man sagt, dieses Diagramm sei *kommutativ,* wenn $f = h \circ g$ gilt, und bezeichnet diesen Fall so:



Sehr wichtig ist die folgende *Charakterisierung* der Faktorisierbarkeit (d.h. die Angabe einer *notwendigen und hinreichenden* Bedingung hierfür):

1.4.5 Der Abbildungssatz *Ist L eine nicht leere Menge, f eine Abbildung von L nach N, g eine Abbildung von L nach M, dann ist f genau dann* über g faktorisierbar, *d.h. es gibt ein $h\colon M \to N$ mit $f = h \circ g$,*



,

wenn die induzierten Äquivalenzrelationen so ineinander liegen:

$$R_g \subseteq R_f.$$

Ist g surjektiv, dann ist h eindeutig bestimmt. Ist f surjektiv, dann ist auch h surjektiv, und ist g surjektiv sowie $R_f = R_g$, dann ist h injektiv.

Beweis:

i) Beweisen wir zunächst die Faktorisierbarkeit von f. Wegen $L \neq \emptyset$ sind M und N ebenfalls nicht leer. Wir können deshalb ein $n_0 \in N$ auswählen und damit die folgende Zuordnung treffen:

$$h\colon M \to N,\ m \mapsto \begin{cases} n_0, & \text{falls } m \notin \text{Bild}(g) \\ f(l), & \text{falls } m = g(l). \end{cases}.$$

Sie definiert eine Funktion, denn die Voraussetzung $R_g \subseteq R_f$ liefert die Implikation

$$g(l) = g(l') \Longrightarrow f(l) = f(l').$$

Für diese Abbildung gilt ganz offensichtlich $f = h \circ g$, sie faktorisiert also f.

ii) Sei umgekehrt $f = h \circ g$. Die Gleichheit $g(l) = g(l')$ impliziert dann

$$f(l) = h(g(l)) = h(g(l')) = f(l'),$$

also die Implikation $R_g \subseteq R_f$.

iii) Die übrigen Behauptungen sind ebenso leicht nachzuprüfen:

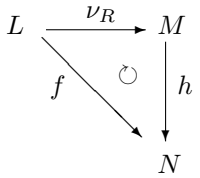
- Daß die Surjektivität von g die Abbildung h festlegt, ist klar (vgl. die Definition von h), ebenso, daß die Surjektivität von f die von h impliziert.
- Falls g surjektiv ist und $R_f = R_g$, dann ergibt sich die Injektivität von h wie folgt: Sei $h(m) = h(m')$. Wegen der Surjektivität von g gibt es l, l' mit $m = g(l)$ und $m' = g(l')$. Die Faktorisierung $f = h \circ g$ liefert $f(l) = f(l')$, was wegen der Gleichheit der Relationen die Identität $g(l) = g(l')$, also auch $m = m'$ impliziert, wie behauptet.

□

Ein Beispiel hierfür ist gegeben, wenn R eine Äquivalenzrelation ist mit $R \subseteq R_f$, denn dann läßt sich f über

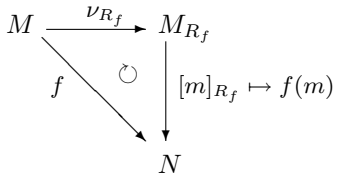
$$\nu_R\colon L \to M, l \mapsto [l]_R$$

faktorisieren:



.

Betrachten wir als erste Anwendung die natürliche Faktorisierung einer Abbildung mit Hilfe der von ihr induzierten Äquivalenzrelation:



Mit anderen Worten:*jede Abbildung* $f\colon M \to N$ *läßt sich mit Hilfe von*

$$\nu_{R_f}\colon M \twoheadrightarrow M_{R_f}, m \mapsto [m]_{R_f}$$

zerlegen:

1.4.6
$$\begin{array}{ccccccc} M & \twoheadrightarrow & M_{R_f} & \rightarrowtail & \mathrm{Bild}(f) & \hookrightarrow & N \\ m & \mapsto & [m]_{R_f} & \mapsto & f(m) & \mapsto & f(m) \end{array}.$$

(Dabei wird mit $\hookrightarrow$ wie meist üblich die sogenannte *Einbettung* bezeichnet, das ist, für $M \subseteq N$, die Abbildung $m \mapsto m$.)
Insbesondere gilt

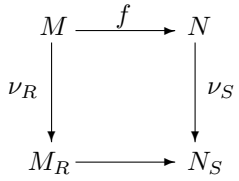
1.4.7
$$M_{R_f} \rightarrowtail \mathrm{Bild}(f),$$

d.h. M_{R_f} und $\mathrm{Bild}(f)$ "sind im wesentlichen dasselbe". Eine weitere Anwendung ist

1.4.8 Der Satz über induzierte Abbildungen *Ist* f *eine Abbildung von* M *nach* N *und sind* R *und* S *zwei Äquivalenzrelationen auf* M *bzw.* N*, die mit* f *wie folgt verträglich sind:*

$$mRm' \Longrightarrow f(m)Sf(m'),$$

dann gibt es genau eine Abbildung $h\colon M_R \to N_S$*, die das folgende Diagramm kommutativ ergänzt:*



.

Beweis: Übungsaufgabe!

Weitere Abbildungssätze werden wir bei Bedarf kennenlernen. Damit sind die grundlegenden Definitionen, Axiome und Resultate der Mengenlehre zusammengestellt, so daß wir uns jetzt den algebraischen Strukturen zuwenden können. Dabei werden wir über die bereits erwähnten Resultate hinaus die Grundeigenschaften von $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ als bekannt voraussetzen. $\mathbb{N}, \mathbb{Z}$ und $\mathbb{Q}$ wurden definiert, Konstruktionen von $\mathbb{R}$ und $\mathbb{C}$ werden Sie in der Analysis-Vorlesung kennenlernen.

Aufgabe 1.4.1
Sei R eine Äquivalenzrelation auf der nichtleeren Menge M. Zeigen Sie, daß durch

$$(x, y)S(u, v) \ :\Longleftrightarrow \ (xRu \ \wedge \ yRw)$$

eine Äquivalenzrelation S auf $M \times M$ definiert wird, und daß für die Äquivalenzklassen gilt:

$$[(x, y)]_S = [x]_R \times [y]_R := \{(u, v) \in M \times M \mid u \in [x]_R, v \in [y]_R\}.$$

Aufgabe 1.4.2
Beweisen Sie den Satz über induzierte Abbildungen.

Kapitel 2

Algebraische Strukturen

In diesem Kapitel werden die grundlegenden algebraischen Strukturen eingeführt. Als Aufhänger für ihre Verwendung dient die Behandlung linearer Gleichungssyteme

$$\begin{array}{rcccccccl} a_{00}x_0 & + & \dots & + & a_{0k}x_k & + & \dots & + & a_{0,n-1}x_n = b_0 \\ & & \vdots & & & & & & \\ a_{i0}x_0 & + & \dots & + & a_{ik}x_k & + & \dots & + & a_{i,n-1}x_n = b_i \quad . \\ & & \vdots & & & & & & \\ a_{m-1,0}x_0 & + & \dots & + & a_{m-1,k}x_k & + & \dots & + & a_{m-1,,n-1}x_n = b_{m-1}, \end{array}$$

Unter Benutzung des Summenzeichens $\sum$ können wir das auch kurz so schreiben:

2.0.9 $$\sum_{k\in n} a_{ik}x_k = b_i,\ i \in m.$$

Dabei sind die $a_{ik}, b_i \in \mathbb{R}$ gegeben, und gesucht sind *Lösungen*

$$x = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}, x_i \in \mathbb{R},$$

die 2.0.9 erfüllen. Um dieses Problem anpacken zu können, stellen wir die folgende Hilfsüberlegung an. Gleichzeitig mit 2.0.9 betrachten wir das zugehörige *homogene Gleichungssystem* (2.0.9 heißt *inhomogenes* System, da möglicherweise ein $b_i \neq 0$) :

2.0.10 $$\sum_{k} a_{ik}x_k = 0,\ i \in m.$$

Die zugehörigen *Lösungsgesamtheiten*, die wir ja suchen, bezeichnen wir so:

$$L_I := \{x \mid x \text{ erfüllt 2.0.9}\}, \quad L_H := \{x \mid x \text{ erfüllt 2.0.10}\}.$$

Ganz wichtig sind jetzt die folgenden Beobachtungen: Definieren wir

$$x+y=\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}+\begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix}:=\begin{pmatrix} x_0+y_0 \\ \vdots \\ x_{n-1}+y_{n-1} \end{pmatrix}, rx:=\begin{pmatrix} rx_0 \\ \vdots \\ rx_{n-1} \end{pmatrix},$$

dann gilt (nachrechnen!):

- $x, y \in L_H, r \in \mathbb{R} \Longrightarrow x+y, rx \in L_H$
- $x, y \in L_I \Longrightarrow x-y \in L_H$

Hieraus ergibt sich die

2.0.11 Folgerung *Ist $x \in L_I$, dann ist jede Lösung z von L_I von der Form $z = x + y$, mit einem geeigneten $y \in L_H$, kurz: $L_I = x + L_H$.*

Zur Bestimmung von L_I genügt also die Ermittlung *irgendeiner speziellen* Lösung des inhomogenen Systems und die Angabe der *Lösungsgesamtheit des homogenen Systems.*

2.1 Gruppen

Wir führen jetzt eine Hierarchie von algebraischen Strukturen ein, die für die weiteren Überlegungen sehr wichtig sind. Dabei betrachten wir zunächst diejenigen, die aus einer Menge zusammen mit lediglich einer einzigen Verknüpfung bestehen:

2.1.1 Definition (Gruppoide, Halbgruppen, Monoide, Gruppen)

i) Unter einem *Gruppoid* verstehen wir eine Menge G zusammen mit einer *Verknüpfung* "$*$", d. h. mit einer Abbildung

$$* : G \times G \to G, (g, g') \mapsto g * g'.$$

ii) Sei $(G, *)$ ein Gruppoid. Ein Element $e \in G$ heißt

$$\begin{aligned} \textit{linksneutral} &:\Longleftrightarrow \quad \forall\, g \in G\colon\ e * g = g, \\ \textit{rechtsneutral} &:\Longleftrightarrow \quad \forall\, g \in G\colon\ g * e = g, \\ \textit{neutral} &:\Longleftrightarrow \quad \forall\, g \in G\colon\ g * e = e * g = g. \end{aligned}$$

iii) Ist $(G, *)$ ein Gruppoid mit neutralem Element e, $g \in G$, dann heißt $g' \in G$

$$\begin{aligned} \textit{linksinvers zu } g &:\Longleftrightarrow \quad g' * g = e, \\ \textit{rechtsinvers zu } g &:\Longleftrightarrow \quad g * g' = e, \\ \textit{invers zu } g &:\Longleftrightarrow \quad g' * g = g * g' = e. \end{aligned}$$

iv) *Halbgruppen* heißen die Gruppoide mit *assoziativer* Verknüpfung:

$$\forall\, g, g', g'' \in G\colon \quad g * (g' * g'') = (g * g') * g''.$$

v) *Monoid* heißt jede Halbgruppe mit neutralem Element.

vi) *Gruppe* nennt man ein Monoid mit Inversen:

$$\forall\, g \in G \quad \exists\, g' \in G : \quad g * g' = g' * g = e.$$

vii) *Abelsche* Gruppen sind die Gruppen mit kommutativer Verknüpfung:

$$\forall\, g, g' \in G\colon \quad g * g' = g' * g.$$

•

2.1.2 Beispiele

- $(\mathbb{N}, +)$ ist ein Monoid, aber keine Gruppe, $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sind abelsche Gruppen, ebenso $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$, wenn $\mathbb{Q}^* := \mathbb{Q}\backslash\{0\}$ etc.

- Für Mengen X ist die Menge X^X aller Abbildungen von X nach X, zusammen mit der Komposition von Abbildungen, also das Paar $(X^X, \circ)$, ein Monoid.

- Die wichtigste Klasse von Beispielen ist die folgende. Sei X eine nicht leere Menge, $(G, *)$ Gruppoid, Halbgruppe, Monoid, oder Gruppe. Dann wird G^X zu Gruppoid, Halbgruppe, Monoid, Gruppe durch Einführung der *punktweisen* Verknüpfung $*'$ wie folgt:

$$\forall\ f, f' \in G^X\colon \quad (f *' f')(x) := f(x) * f'(x).$$

  Das Standardbeispiel ist hier $X := n = \{0, \ldots, n-1\}, G := \mathbb{R}$, also die Menge

$$\mathbb{R}^n = \{(x_0, \ldots, x_{n-1}) \mid x_i \in \mathbb{R}\}$$

  bei Zeilenschreibweise, bzw.

$$\mathbb{R}^n = \{\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \mid x_i \in \mathbb{R}\}$$

  bei Spaltenschreibweise, zusammen mit der punktweisen Addition

$$(x_0, \ldots, x_{n-1}) + (y_0, \ldots, y_{n-1}) = (x_0 + y_0, \ldots, x_{n-1} + y_{n-1}),$$

  bzw.

$$\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} + \begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} x_0 + y_0 \\ \vdots \\ x_{n-1} + y_{n-1} \end{pmatrix}.$$

- Die *symmetrische Gruppe* auf einer Menge X wird definiert als die Menge

$$S_X := \{\pi\colon X \rightarrowtail\!\!\!\!\!\rightarrow X\},$$

  zusammen mit der Hintereinanderausführung als Verknüpfung:

$$(S_X, \circ).$$

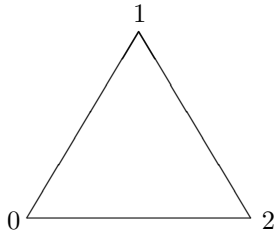
  Z. B. ist — in naheliegender Schreibweise, bei der die Bilder unter die Urbilder geschrieben werden —

$$S_3 = \{\begin{pmatrix} 012 \\ 012 \end{pmatrix}, \begin{pmatrix} 012 \\ 102 \end{pmatrix}, \begin{pmatrix} 012 \\ 210 \end{pmatrix}, \begin{pmatrix} 012 \\ 021 \end{pmatrix}, \begin{pmatrix} 012 \\ 120 \end{pmatrix}, \begin{pmatrix} 012 \\ 201 \end{pmatrix}\}.$$

  S_X ist leicht als Gruppe nachzuweisen, falls $|X| > 2$ ist diese Gruppe *nicht abelsch,* denn es gilt z. B.

$$\begin{pmatrix} 012 \\ 210 \end{pmatrix} \circ \begin{pmatrix} 012 \\ 021 \end{pmatrix} = \begin{pmatrix} 012 \\ 201 \end{pmatrix}, \text{aber } \begin{pmatrix} 012 \\ 021 \end{pmatrix} \circ \begin{pmatrix} 012 \\ 210 \end{pmatrix} = \begin{pmatrix} 012 \\ 120 \end{pmatrix},$$

und diese Nichtvertauschbarkeit ist natürlich nicht von der Numerierung der Elemente von X sondern nur von deren Anzahl abhängig. S_3 ist also eine nicht abelsche Gruppe. Man kann sie sich als *Symmetriegruppe* des regelmäßigen Dreiecks



vorstellen. Denn die Drehungen und Spiegelungen induzieren auf der Menge $\{0,1,2\}$ der Nummern der Ecken gerade die angegebenen Permutationen. Z.B. induziert die Drehung um 120 Grad *gegen den Uhrzeigersinn* die Permutation

$$\begin{pmatrix} 012 \\ 120 \end{pmatrix},$$

wenn wir $f(x) = y$ interpretieren als "y tritt an die Stelle von x".

$\diamond$

Es gelten die (echten!) Inklusionen

$$\text{Gruppoide} \supset \text{Halbgruppen} \supset \text{Monoide} \supset \text{Gruppen} \supset \text{abelsche Gruppen}.$$

In der Regel werden wir die *multiplikative Schreibweise* verwenden, also $*$ durch $\cdot$ ersetzen (und diesen Multiplikationspunkt oft einfachheitshalber sogar weglassen). Höchstens im kommutativen Fall werden wir die *additive Schreibweise* benutzen, also $+$ anstelle von $*$.
Es ist leicht zu zeigen, daß es in einem Gruppoid *höchstens ein neutrales Element* gibt: Für neutrale Elemente $e, e' \in G$ gilt nämlich $e = e * e'$, weil e' neutral ist, und die Neutralität von e ergibt daraus $e * e' = e'$. Bei multiplikativer Schreibweise werden wir dieses Element ggf. als 1 (oder genauer als 1_G) bezeichnen, bei additiver Schreibweise als 0 oder 0_G.
Ebenso mühelos zeigt man, daß Elemente von Monoiden *höchstens ein Inverses* besitzt, denn für zwei Inverse g' und g'' von g gilt offensichtlich

$$g' = e * g' = (g'' * g) * g' = g'' * (g * g') = g'' * e = g''.$$

Das Inverse wird ggf. mit g^{-1} bzw. $-g$ bezeichnet.

Hilfreich ist noch, daß man zum Nachweis der Gruppeneigenschaft von $(G, \cdot)$ manche Rechnung einsparen kann, wenn man folgendes Resultat berücksichtigt:

2.1.3 Satz *Halbgruppen $(G, \cdot)$ mit linksneutralem Element und diesbezüglichen Linksinversen sind Gruppen.*

Beweis: Sei e ein linksneutrales Element von G, g' linksinvers zu g bzgl. e.
i) Wir zeigen zunächst, daß g' auch rechtsinvers ist bzgl. e : Es gibt auch zu g' ein Linksinverses bzgl. e, es sei mit g'' bezeichnet. Hierfür gilt:

$$gg' = e(gg') = (g''g')(gg') = g''(g'g)g' = g''eg' = g''g' = e.$$

ii) Das Element e ist auch rechtsneutral:

$$ge = g(g'g) = (gg')g =_{i)} eg = g.$$

□

Die oben eingeführte *Verknüpfung* $*$ ist, genauer gesagt, eine *zweistellige* Abbildung:

$$G^2 \to G, (g, g') \mapsto g * g'.$$

Allgemeiner kann man *n-stellige* Verknüpfungen als Abbildungen $* : G^n \to G$ einführen und auf diese Weise dann die Existenz von Inversen als einstellige Abbildung auffassen:

$$G^1 \to G, g \mapsto g^{-1},$$

und die Existenz eines neutralen Elements mit der Existenz der folgenden nullstelligen Abbildung identifizieren: (denn $G^0 = G^\emptyset = \{\emptyset\}$):

$$G^0 \to G, \emptyset \mapsto e,$$

denn $G^0 = G^\emptyset = \{\emptyset\}$. Davon werden wir gleich anhand der nächsten Definition Gebrauch machen:

2.1.4 Definition (Unterstruktur) Ist G (genauer: die Menge G mit den vorgegebenen Verknüpfungen, der zweistelligen Verknüpfung $*$ und (gegebenenfalls) den ein- oder nullstelligen) ein Gruppoid, eine Halbgruppe ..., dann versteht man unter einem *Untergruppoid,* einer *Unterhalbgruppe,* ... eine Teilmenge $U \subseteq G$, so daß die Einschränkung der Verknüpfungen auf U^2 bzw. auf U^1 oder U^0 ihr Bild in U haben. Wir kürzen das mit

$$U \leq G$$

ab, wenn klar ist, welche Art algebraischer Struktur gemeint ist. •

2.1.5 Bemerkung *Zum Beweis von $U \leq G$ genügt der Nachweis, daß die Einschränkungen der die Struktur auf G definierenden Abbildungen auf U^2, U^1 bzw. auf U^0 nicht aus U hinausführen.*

Wir brauchen tatsächlich nicht mehr zu fordern, denn die geforderten Eigenschaften wie Assoziativität, Inversivität oder Neutralität übertragen sich automatisch von G nach U. Es folgt auch beispielsweise, daß Untergruppen ebenfalls nicht leer sind und dasselbe neutrale Element besitzen wie die Obergruppe! Wichtig ist vor allem diese unmittelbare Konsequenz:

2.1.6 Folgerung *Jeder Durchschnitt von Untergruppoiden, -halbgruppen, -monoiden oder -gruppen ist ebenfalls Untergruppoid, -halbgruppe, -monoid, -gruppe.*

Von besonderer Bedeutung ist es, ökonomische Verfahren zu entwickeln, mit denen eine Teilmenge $M \subseteq G$ daraufhin überprüft werden kann, ob sie eine Unterstruktur ist oder nicht. Zunächst einmal genügt natürlich die Überprüfung, ob die Einschränkungen der Verknüpfungen — von G^2, G^1, G^0 auf M^2, M^1, M^0 — aus M hinausführen oder nicht. Man kann dies bei Gruppen aber auch "in einem Aufwasch" verifizieren:

2.1.7 Satz *Sei $(G, \cdot)$ eine Gruppe, $\emptyset \neq U \subseteq G$. Dann gilt:*

i) $U \leq G \Longleftrightarrow [u, u' \in U \Longrightarrow u \cdot (u')^{-1} \in U]$.

ii) Ist U endlich, dann gilt $U \leq G \Longleftrightarrow [u, u' \in U \Longrightarrow u \cdot u' \in U]$.

iii) $U, U' \leq G \Longrightarrow [U \cdot U' \leq G \Longleftrightarrow U \cdot U' = U' \cdot U]$. *Dabei bedeutet $U \cdot U'$ das sogenannte* Komplexprodukt *von U mit U' :*

$$U \cdot U' := \{u \cdot u' \mid u \in U, u' \in U'\}.$$

Beweis: i) ist leicht nachzuprüfen:

a) Ist U eine Untergruppe, dann liegt mit u' auch dessen Inverses u'^{-1} in U und natürlich auch, zu jedem $u \in U$, das Produkt uu'^{-1}.

b) Liegt, umgekehrt, mit $u, u' \in U$ auch das Produkt uu'^{-1} in U, dann gilt das auch für $u' = u$, so daß $1_G = uu^{-1} \in U$ richtig ist. Setzen wir jetzt $u := 1_G$, dann folgt auch $u'^{-1} \in U$, die Inversen liegen also ebenfalls in U. Diese Teilmenge ist auch *multiplikativ abgeschlossen:* 1_G liegt in U, mit u' also auch u'^{-1} und deshalb, mit $u, u' \in U$, auch deren Produkt uu'. U ist demnach eine Untergruppe.

Für ii) beachten wir, daß es, wegen der Endlichkeit von G, für $u' \in U$ natürliche Zahlen $m \neq n$, etwa $m > n$, gibt mit $u'^n = u'^m$, also, wenn etwa $m > n$: $u'^{m-n} = e$, so daß eine Potenz von u' gleich dem Inversen von u' ist. Jetzt folgt aus i) die Behauptung.

iii) ist Übungsaufgabe.

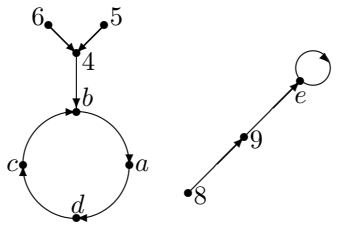
□

Sehen wir uns jetzt noch ein Beispiel etwas genauer an, die symmetrischen Gruppen auf endlichen Mengen, die bereits eingeführt worden sind. Es sollen einige Bezeichnungsweisen eingeführt werden, die den Umgang mit den Elementen symmetrischer Gruppen erleichtern.

2.1.8 Definition (Endofunktionen, Zyklen, disjunkte Zyklen)

- Bevor wir *bijektive* Abbildungen einer endlichen Menge X, also Elemente der symmetrischen Gruppe S_X, betrachten, wollen wir uns einmal *beliebige* Abbildungen $f \in X^X$ ansehen. Zunächst ein Beispiel, eine Abbildung

$f \in X^X$, wobei $X := \{4, 5, 6, 8, 9, a, b, c, d, e\}$, solche Funktionen heißen *Endofunktionen* auf X. Wir skizzieren uns diese Funktion durch einen *gerichteten Graphen,* die Pfeile geben an, welches Element von X worauf abgebildet wird. Hier ist ein Beispiel:

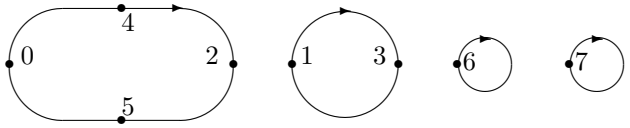


Es ist klar, daß eine Endofunktion einer *endlichen* Menge diese in zwei Teilmengen einteilt, von denen die eine Teilmenge aus den Elementen x besteht, die von einer geeigneten Potenz f^n auf sich selbst abgebildet werden: $f^n(x) = x$, für geeignetes n. Diese Punkte liegen also auf (gerichteten) *Kreisen* oder auch *Zyklen.*

- Ist die Abbildung dagegen *bijektiv,* dann müssen *alle* $x \in X$ auf solchen Kreisen liegen, hier ist ein Beispiel, ein Element π der symmetrischen Gruppe auf $X := \{0, 1, 2, 3, 4, 5, 6, 7\}$:

$$\pi := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 5 & 1 & 2 & 0 & 6 & 7 \end{pmatrix}.$$

Visualisierung durch Zyklen ergibt folgendes Bild (die Pfeilrichtung deutet die Abbildungsrichtung an):



- Elemente $\pi \in S_X$, die höchstens einen Kreis aus mehr als einem Element enthalten heißen *zyklisch, Zyklus* oder genauer $r-$*Zyklus,* wenn r die Anzahl der Elemente dieses Zyklus ist. Das ist genau dann der Fall, wenn es — bei geeigneter Numerierung der Elemente von X — $x_0, \ldots, x_{r-1} \in X$ gibt mit

$$\pi = \begin{pmatrix} x_0 & x_1 & \ldots & x_{r-2} & x_{r-1} & x_r & \ldots & x_{|X|-1} \\ x_1 & x_2 & \ldots & x_{r-1} & x_0 & x_r & \ldots & x_{|X|-1} \end{pmatrix}.$$

Wir schreiben dann auch kurz

$$\pi = (x_0 \ldots x_{r-1})(x_r) \ldots (x_{|X|-1}),$$

oder gar nur

$$\pi = (x_0 \ldots x_{r-1}),$$

wenn klar ist, auf welcher Gesamtmenge π wirkt.

- Zwei Zyklen $\pi = (x_{i_0} \dots x_{i_{r-1}})$ und $\rho = (x_{j_0} \dots x_{j_{s-1}})$ in S_X heißen *disjunkt*, wenn r oder s gleich 1 ist oder, bei $r, s \neq 1$,

$$\{x_{i_0}, \dots, x_{i_{r-1}}\} \cap \{x_{j_0}, \dots, x_{j_{s-1}}\} = \emptyset.$$

•

Schreiben wir als Beispiel erneut die Elemente der symmetrischen Gruppe auf der Menge 3 hin, diesmal unter Verwendung der gerade eingeführten Notation für Zyklen:

$$S_3 = \{1, (01), (02), (12), (012), (021)\}.$$

2.1.9 Hilfssatz

i) Disjunkte Zyklen sind vertauschbare Abbildungen.

ii) Ist X eine endliche Menge, dann ist jedes $\pi \in S_X$ darstellbar als Komposition verschiedener und bis auf die Reihenfolge eindeutig bestimmter disjunkter Zyklen.

iii) $(x_{i_0} \dots x_{i_{r-1}}) = (x_{i_1} \dots x_{i_{r-1}} x_{i_0}) = (x_{i_2} \dots x_{i_{r-1}} x_{i_0} x_{i_1}) = \dots$.

iv) $(x_{i_0} \dots x_{i_{r-1}})^{-1} = (x_{i_{r-1}} x_{i_{r-1}} \dots x_{i_0})$,

v) $(x_{i_0} \dots x_{i_{r-1}}) = (x_{i_0} x_{i_1})(x_{i_1} x_{i_2}) \dots (x_{i_{r-1}} x_{i_{r-1}})$.

Beweis: trivial.

□

2.1.10 Definition (Zyklenschreibweise, Listenschreibweise) Die Darstellung von $\pi \in S_X$ als Produkt disjunkter Zyklen nennt man die *Zyklenschreibweise,* bei Weglassen der 1-Zyklen auch die *verkürzte Zyklenschreibweise.* Ist $\pi \in S_n$ und

$$\pi = \prod_{\nu=0}^{z(\pi)-1} (j_\nu \pi j_\nu \dots \pi^{l_\nu - 1} j_\nu) \qquad (*)$$

die Zyklenschreibweise für π ($z(\pi)$ steht also für die Anzahl der zyklischen Faktoren, l_ν für deren Längen), dann wird diese eindeutig, wenn wir noch fordern

a) $\forall\, n \in \mathbb{N}$: $j_\nu \leq \pi^n j_\nu$,

b) $j_0 < j_1 < \dots$.

In diesem Fall heißt $(*)$ auch die *Standardzyklenschreibweise.*
Neben dieser Zyklenschreibweise wird noch die *Listenschreibweise* benutzt, insbesondere in Computerprogrammen. Hier schreibt man einfach für $\pi \in S_n$ die Folge der Funktionswerte:

$$\pi = [\pi 0, \pi 1, \dots, \pi(n-1)].$$

Bijektionen von Mengen auf sich selbst heißen *Permutationen,* Gruppen, die aus Permutationen einer Menge X bestehen, also Untergruppen von S_X, X geeignet, heißen entsprechend *Permutationsgruppen,* $|X|$ heißt dabei der *Grad* der Permutation $\pi \in S_X$ bzw. der Untergruppe $U \leq S_X$. •

Eine weitere Definition von grundlegender Bedeutung ist das sogenannte Erzeugnis einer Teilmenge:

2.1.11 Definition (Erzeugnis) Als *Erzeugnis* $\langle T\rangle$ einer Teilmenge T eines Gruppoids, einer Halbgruppe, eines Monoids, einer Gruppe G bezeichnet man die kleinste Unterstruktur von G, die T umfaßt, also, wegen 2.1.6, den Durchschnitt aller Untergruppoide, Unterhalbgruppen, Untermonoide, Untergruppen, die T enthalten:

$$\langle T\rangle := \bigcap_{U:T\subseteq U\leq G} U.$$

•

Weil das Erzeugnis von T als *kleinste* Unterstruktur definiert ist, die T umfaßt, geht man beim Nachweis, daß eine Teil*menge* U die von T erzeugte Unterstruktur ist, am besten wie folgt vor:

2.1.12 Hilfssatz *Ist G Gruppoid, Halbgruppe, Monoid oder Gruppe, $T\subseteq G$ und U eine Teilmenge von G, dann genügt zum Beweis von $\langle T\rangle = U$ der Nachweis von*

1. *U ist Unterstruktur von G,*
2. *T liegt in U,*
3. *U liegt in jeder Unterstruktur, die T umfaßt.*

□

2.1.13 Beispiele

- Das Erzeugnis von z in der abelschen Gruppe $(\mathbb{Z},+)$ wird kurz mit $\langle z\rangle$ (anstelle von $\langle\{z\}\rangle$) bezeichnet. Es gilt

  $$\langle z\rangle = \{0,\pm z,\pm 2z,\ldots\}.$$

  Das Erzeugnis von $\emptyset$ in dieser Gruppe ist

  $$\langle\emptyset\rangle = \{0\}.$$

- Ganz allgemein bezeichnet man das Erzeugnis eines Elements g in einer Gruppe G mit $\langle g\rangle$, es gilt offenbar

  $$\langle g\rangle = \{1, g^{\pm 1}, g^{\pm 2}, g^{\pm 3},\ldots\}.$$

  Diese Untergruppe heißt *die von g erzeugte zyklische Untergruppe von G.*

◇

Zur Untersuchung und Anwendung von Gruppen ist sehr oft die Kenntnis eines *möglichst kleinen* Erzeugendensystems hilfreich, wir wollen ein solches für die symmetrischen Gruppen S_n angeben.

2.1.14 Hilfssatz *Die symmetrische Gruppe S_n hat die Ordnung*

$$|S_n| = n! := 1 \cdot 2 \cdots n$$

(dabei ist zu beachten, daß das leere Produkt *als 1 definiert wird, also $|S_0| = 0! := 1$ behauptet wird) und die folgenden Erzeugendensysteme:*

$$S_n = \langle (01), (12), \ldots, (n-2, n-1) \rangle = \langle (01), (0, \ldots, n-1) \rangle.$$

Beweis: Die Behauptung über die Ordnung ergibt sich durch Induktion nach n :
i) Die Induktionsbasis ist $|S_0| = 1 = 0!$, was offensichtlich richtig ist, denn die einzige Bijektion auf der leeren Menge ist die leere Abbildung.
ii) Zum Vollzug des Induktionsschlusses von n auf $n+1$ betrachten wir die möglichen Bilder des Punktes n in der Menge $n+1 = \{0, \ldots, n\}$ unter Bijektionen auf der Menge $n+1$. Er kann die $n+1$ verschiedenen Werte $0, \ldots, n$ annehmen, wir erhalten also

$$|S_{n+1}| = (n+1) \cdot |S_n| = (n+1) \cdot n! = (n+1)!,$$

wie behauptet.
Es bleiben noch die Behauptungen über die Erzeugendensysteme nachzuweisen. Zunächst zeigen wir, daß alle zyklischen Permutationen als Produkte von *Transpositionen* (das sind die Bijektionen, die genau zwei Punkte vertauschen und alle anderen auf sich selbst abbilden) schreiben lassen:

$$(i_0 \ldots i_{r-1}) = (i_0 i_1)(i_1 i_2) \ldots (i_{r-2} i_{r-1}).$$

Jetzt braucht nur noch gezeigt zu werden, daß man von den Transpositionen eigentlich nur die von *benachbarten Punkten* benötigt, was sich aus folgender Gleichung ergibt:

$$(j, k+1) = (k, k+1)(j, k)(k, k+1).$$

Damit ist bewiesen, daß die symmetrische Gruppe von den Transpositionen $(i, i+1)$ benachbarter Ziffern erzeugt wird.
Es bleibt schließlich noch zu verifizieren, daß auch das angegeben System aus nur *zwei* Elementen genügt. Hierzu bemerken wir, daß

$$(i, i+1) = (0, \ldots, n-1)^i (01) (0, \ldots, n-1)^{-i}$$

gilt, also jede Transposition benachbarter Ziffern aus (01) mit Hilfe der Permutation $(0, \ldots, n-1)$ konstruiert werden kann.

□

Beispielsweise ist

$$S_4 = \langle (01), (12), (23) \rangle = \langle (01), (0123) \rangle.$$

Aufgabe 2.1.1
Sei $(G, *)$ eine Gruppe. Zeigen Sie, daß für jedes $g \in G$ die Abbildungen

a) $l_g: G \to G,\ x \mapsto g * x$, sowie

b) $\kappa_g: G \to G,\ x \mapsto g * x * g^{-1}$,

bijektiv sind. (Kennzeichnen Sie jeweils, an welcher Stelle Sie welches Gruppenaxiom verwenden!).

Aufgabe 2.1.2

Sei $\pi := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 10 & 4 & 1 & 7 & 8 & 9 & 11 & 2 & 3 & 0 & 5 & 6 \end{pmatrix} \in S_{12}$.

a) Schreiben Sie π als Produkt disjunkter Zykel.

b) Berechnen Sie $\pi^{-1}, \pi^3, \pi^4, \pi^{1997}$.

Aufgabe 2.1.3

Sei $(G, *)$ eine Gruppe und A, B zwei Untergruppen von G. Zeigen Sie:

Das Komplexprodukt $A * B$ ist genau dann eine Untergruppe von G, wenn gilt $A * B = B * A$.

Aufgabe 2.1.4

Geben Sie alle Untergruppen von S_3 an (keine Begründung)..

2.2 Operationen von Gruppen

In diesem Paragraphen wollen wir zeigen, wie Gruppen zur Definition, Abzählung und Konstruktion vieler Strukturen aus Mathematik und Naturwissenschaften benutzt werden können, wenn diese Strukturen als Äquivalenzklassen auf endlichen Mengen definiert sind. Ein Beispiel ist oben bereits erwähnt worden, die unnumerierten Graphen wurden als Äquivalenzklassen numerierter eingeführt. Die vorgesehene Anwendung von Gruppen auf Probleme dieser Art ermöglicht beispielsweise die *Abzählung* von Äquivalenzklassen, also u. a. die Bestimmung der Anzahl unnumerierter Graphen mit vorgegebener Punktezahl. Man kann mit Hilfe der Gruppenoperation sogar Repräsentanten der Äquivalenzklassen *konstruieren,* worauf aber zunächst nicht eingegangen werden kann.

2.2.1 Definition (Operationen von Gruppen auf Mengen) Sei G eine (multiplikativ geschriebene) Gruppe, M eine nicht leere Menge. Man sagt, G *operiere* auf M oder M sei eine $G-$*Menge,* wenn eine Abbildung

$$G \times M \to M\colon (g, m) \mapsto gm$$

gegeben ist mit

$$g(g'm) = (gg')m, 1m = m.$$

Dies, also die Vorgabe von G, M und einer solchen Abbildung, wird auch mit

$$_GM$$

abgekürzt, weil hier G *von links* auf M operiert. Ganz entsprechend kann man natürlich Operationen *von rechts* definieren. •

Wir bemerken zunächst, daß jede Operation $_GM$ eine Äquivalenzrelation auf M definiert:

$$m \sim_G m' :\Longleftrightarrow \quad \exists\, g \in G\colon\ gm = m'.$$

Daß dies tatsächlich eine Äquivalenzrelation ist, d.h. daß $\sim$ reflexiv, symmetrisch und transitiv ist, ergibt sich leicht mit Hilfe der folgenden Äquivalenz, die unmittelbar aus der Definition von $\sim$ folgt:

2.2.2 $$gm = m' \iff m = g^{-1}m'.$$

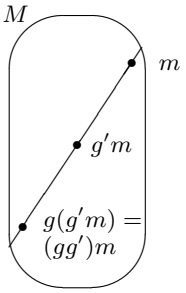
Die Klassen dieser Relation, also die Mengen

$$G(m) := \{gm \mid g \in G\}$$

heißen die *Bahnen* von G auf M. Als Äquivalenzklassen sind zwei Bahnen $G(m)$ und $G(m')$ entweder gleich oder disjunkt. Die Menge *aller* Bahnen wollen wir mit

$$G \setminus\setminus M := \{G(m) \mid m \in M\}$$

bezeichnen.



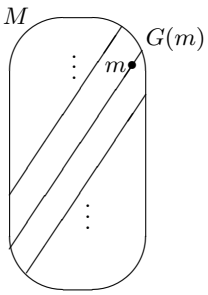
2.2.3 Beispiel Ist n eine positive natürliche Zahl und

$$T := \{t \in \mathbb{N} \mid t \text{ teilt } n\}$$

die Menge der Teiler von n, dann betrachten wir die Abbildung

$$\sigma\colon T \to T, t \mapsto n/t.$$

Für sie gilt $\sigma^2 = \mathrm{id}_T$, sie besitzt demnach Links- und Rechtsinverse, liegt also in S_T, und es folgt auch $\langle\sigma\rangle = \{1, \sigma\}$. Die Bahnen dieser Gruppe sind die Mengen $\{t, n/t\}$, sie sind also von der Ordnung oder *Länge* 2 oder 1. Und es gibt genau dann eine (und dann auch *nur* eine) Bahn der Länge 1, wenn es einen Teiler t gibt mit $t = n/t$, d.h. mit $n = t^2$, also wenn n eine Quadratzahl ist. Mit Hilfe dieser Operation und der Betrachtung ihrer Bahnen haben wir also die Aussage bewiesen, daß positive natürliche Zahlen genau dann ungeradzahlig viele Teiler besitzen, wenn sie Quadrate sind. ◇



Ein Repräsentantensystem T von $G \backslash\backslash M$, eine sogenannte *Transversale* von $G \backslash\backslash M$, liefert also eine vollständige Zerlegung von M in disjunkte Teilmengen, eine *Partition* von M :

$$M = \dot{\bigcup}_{m \in T} G(m).$$

Es gilt auch die Umkehrung: Jede Äquivalenzrelation bzw. partition einer Menge X kann als Bahnenmenge einer geeigneten Gruppenoperation beschrieben werden:

2.2.4 Folgerung *Besitzt eine Mengen M eine Partition in disjunkte, nicht leere Teilmengen $M_i, i \in I$, dann sind die M_i die Bahnen der Gruppe*

$$\bigoplus_{i \in I} S_{M_i} := \{\pi \in S_M \mid \forall\ i\colon\ \pi(M_i) = M_i\}.$$

Jede mathematische Struktur, die als Äquivalenzklasse definiert ist, kann also als Bahn einer Gruppe verstanden werden.

Neben diesen Bahnen der Elemente von M definiert die vorgegebene Operation noch *Untergruppen* von G, und zwar zu jedem $m \in M$:

$$G_m := \{g \in G \mid gm = m\}$$

heißt der *Stabilisator* von m. Die Untergruppeneigenschaft von G_m folgt aus leicht aus 10.2.2. Betrachten wir einige Beispiele wichtiger Strukturen aus der Algebra, die sich als Bahnen bzw. als Stabilisatoren erweisen:

2.2.5 Anwendungen (Nebenklassen, Konjugiertenklassen, Zentralisatoren)

- Ist U eine Gruppe von G, dann operiert diese per Linksmultiplikation auf G :
$$U \times G \to G, (u, g) \mapsto ug.$$
Bahnen sind hier die Mengen
$$U(g) = Ug = \{ug \mid u \in U\},$$
die sogenannten *Rechtsnebenklassen* von U in G (dabei haben wir einfachheitshalber Ug für das Komplexprodukt $U \cdot \{g\}$ geschrieben).
Die Menge aller Bahnen bzw. Rechtsnebenklassen bezeichnen wir mit
$$U\backslash G := \{Ug \mid g \in G\}.$$
Bei analoger Operation von U auf G per Rechtsmultiplikation ergeben sich als Bahnen die *Linksnebenklassen*
$$gU = \{gu \mid u \in U\}.$$
Entsprechend ist die Menge aller Bahnen bzw. Linksnebenklassen
$$G/U := \{gU \mid g \in G\}.$$
Bei der Linksmultiplikation ist der Stabilisator von g offenbar die Untergruppe $\{1\}$, ebenso bei der Rechtsmultiplikation.

Als erstes Ergebnis erhalten wir demnach, daß sowohl die Rechtsnebenklassen, als auch die Linksnebenklassen einer Untergruppe U von G eine Partition von G bilden.
Ein konkretes Beispiel ist übrigens die oben bereits erwähnte Beschreibung der Lösungsgesamtheit eines inhomogenen Systems linearer Gleichungen. Setzt man nämlich $G := \mathbb{R}^n$ und $U := L_H$, dann operiert diese (Untergruppe) L_H auf $\mathbb{R}^n$, und die Bahn (irgendeiner) speziellen Lösung x des inhomogenen Systems ist die Nebenklasse (Links- oder Rechts- braucht hier wegen der Kommutativität nicht unterschieden zu werden)
$$L_I = x + L_H.$$

- Eine interessante Operation von G auf sich selbst ist die sogenannte *Konjugation:*
$$G \times G \to G\colon (g', g) \mapsto g'gg'^{-1}.$$
Die Bahn von g ist die Menge
$$\{g'gg'^{-1} \mid g' \in G\},$$
die *Konjugiertenklasse* von g, wir bezeichnen sie mit $C^G(g)$.
Der Stabilisator von g ist die Untergruppe
$$\{g' \in G \mid g'gg'^{-1} = g\},$$
die wir mit $C_G(g)$ abkürzen, sie heißt auch der *Zentralisator* von g.

Wir erhalten daraus als weiteres Ergebnis, daß auch die Konjugiertenklassen von Elementen der Gruppe eine Partition der Gruppe bilden, und daß die Zentralisatoren Untergruppen sind. ◇

Einen wichtigen Spezialfall bilden die Konjugiertenklassen der symmetrischen Gruppe S_n. Zur Berechnung der Klasse von $\rho \in S_n$ bemerken wir, daß — unter Verwendung der Abkürzung $\binom{i}{\sigma(i)}$ für σ — die Gleichungen

$$\pi\rho\pi^{-1} = \binom{i}{\pi(i)}\binom{i}{\rho(i)}\binom{\pi(i)}{i} = \binom{i}{\pi(i)}\binom{\pi(i)}{\rho(i)}$$

$$= \binom{\rho(i)}{\pi(\rho(i))}\binom{\pi(i)}{\rho(i)} = \binom{\pi(i)}{\pi(\rho(i))}.$$

Hieraus folgt, daß $\pi\rho\pi^{-1}$ aus ρ durch Anwendung der Abbildung π auf die Ziffern in den zyklischen Faktoren von ρ entsteht: Aus

$$\rho = \ldots(\ldots i\ \rho(i)\ldots)\ldots,$$

der Zykelschreibweise für ρ, ergibt sich

$$\pi\rho\pi^{-1} = \ldots(\ldots \pi(i)\ \pi(\rho(i))\ldots)\ldots.$$

Die zyklischen Faktoren des zu ρ konjugierten Elements $\pi\rho\pi^{-1}$ haben also dieselben Längen wie die zyklischen Faktoren von ρ.

Umgekehrt sind zwei Permutationen mit denselben Längen der zyklischen Faktoren zueinander konjugiert: Ist nämlich

$$\rho = \ldots(\ldots i\ \rho(i)\ldots)\ldots,$$

$$\sigma = \ldots(\ldots j\ \sigma(j)\ldots)\ldots,$$

dann gilt, für

$$\pi := \begin{pmatrix} \ldots & \ldots & i & \rho(i) & \ldots & \ldots \\ \ldots & \ldots & j & \sigma(j) & \ldots & \ldots \end{pmatrix}$$

die Gleichung

$$\pi\rho\pi^{-1} = \sigma,$$

ρ und σ sind demnach konjugiert.

2.2.6 Folgerung *Bedeutet $\alpha(\pi) = (\alpha_0, \alpha_1, \ldots)$ die schwach monoton fallende Folge der Längen der zyklischen Faktoren von $\pi \in S_n$, dann sind ρ und σ genau dann konjugiert, wenn $\alpha(\rho) = \alpha(\sigma)$. Die schwach monoton fallenden Folgen $\alpha(\pi) = (\alpha_0, \alpha_1, \ldots)$ natürlicher Zahlen α_i mit $\sum_i \alpha_i = n$ charakterisieren demnach die Konjugiertenklassen von S_n. (Man nennt solche monoton fallenden Folgen natürlicher Zahlen, deren Summe n ergibt, auch* Partitionen *oder genauer* Zahlpartitionen *von n und $\alpha(\pi)$ die* Zykelpartition *von π.)* □

Beispielsweise sind (4), (3, 1), $(2^2) := (2, 2)$, $(2, 1^2)$ und (1^4) die Zykelpartitionen, die die Klassen von S_4 charakterisieren.
Mit Hilfe der — gerade als Bahnen beschriebenen — Linksnebenklassen von Untergruppen können wir jetzt ein grundlegendes Resultat über den Zusammenhang zwischen Bahnen und Stabilisatoren formulieren und beweisen:

2.2.7 Das Fundamentallemma *Ist*

$$G \times M \to M, (g, m) \mapsto gm$$

eine Operation von G auf M, dann ist, für jedes Element m von M, die Bahn von m auf natürliche Weise bijektiv zur Menge der Linksnebenklassen von G_m :

$$G(m) \rightarrowtail\!\!\!\!\!\rightarrow G/G_m, gm \mapsto gG_m.$$

Insbesondere gilt also, daß die Länge der Bahn von m gleich der Anzahl der Linksnebenklassen des Stabilisators von m ist,

$$|G(m)| = |G/G_m|,$$

wenn, wie üblich, G/G_m die Menge der Linksnebenklassen von G_m in G bezeichnet.

Beweis: Wir betrachten folgende Kette von Äquivalenzen:

$$gm = g'm \iff g^{-1}g'm = m \iff g^{-1}g' \in G_m \iff gG_m = g'G_m.$$

Liest man dies von links nach rechts, so ergibt sich die Wohldefiniertheit von $gm \mapsto gG_m$. Liest man von rechts nach links, so ergibt sich die Injektivität, die Surjektivität ist trivial.
Die einzelnen Äquivalenzen ergeben sich wie folgt:

i) Die erste folgt mit den beiden Bedingungen aus der Definition einer Operation.

ii) Die zweite Äquivalenz folgt aus der Definition des Stabilisators.

iii) Die dritte Äquivalenz benutzt eine einfache, aber sehr wichtige Überlegung, die im folgenden in vielen Fällen benutzt werden wird. Sie ist unmittelbar aus der Definition von Links- bzw. Rechtsnebenklassen ersichtlich: $g^{-1}g' \in G_m$ bedeutet die Existenz eines $g'' \in G_m$ mit $g^{-1}g' = g''$, was dasselbe ist wie $g' = gg''$ bzw. wie $g' \in gG_m$. Da verschiedene Linksnebenklassen disjunkt sind, ist das aber äquivalent zu $g'G_m = gG_m$. □

Die Anzahl der Links- oder Rechtsnebenklassen einer Untergruppe nennt man auch den *Index* der Untergruppe; es spielt dabei keine Rolle, ob es sich um Links- oder Rechtsnebenklassen handelt, denn beide Anzahlen sind gleich! Wir haben also u.a. gerade bewiesen, daß *die Länge der Bahn von m gleich dem Index des Stabilisators von m ist.*

Hieraus und aus den vorangegangenen Beispielen können wir viele wichtige Folgerungen ziehen: Bei der Operation von U auf G per Linksmultiplikation sind alle Stabilisatoren trivial, $U_g = \{1\}$, mit dem Fundamentallemma ergibt sich

2.2.8 Der Satz von Lagrange *Ist U eine Untergruppe von G, dann haben alle Links- und alle Rechtsnebenklassen von U in G dieselbe Ordnung:*

$$|U| = |Ug| = |gU|.$$

Ist G eine endliche *Gruppe, dann ist $|U|$ ein Teiler von $|G|$ und wir haben*

$$|G/U| = \frac{|G|}{|U|}.$$

Aus diesem Satz folgt zum Beispiel, daß Untergruppen von S_3 höchstens die Ordnungen 1,2,3 oder 6 haben können. Betrachten wir noch ein weiteres Beispiel einer Operation einer Gruppe mit einer Anwendung auf die Kombinatorik:

2.2.9 Anwendung (Binomialkoeffizienten) Die *natürliche* Operation der symmetrischen Gruppe S_n auf der Menge n, das ist die Operation

$$S_n \times n \to n, (\pi, i) \mapsto \pi(i),$$

induziert, zu jedem $k \leq n$, folgende Operation von S_n auf der Menge $\binom{n}{k}$ aller $k-$*Teilmengen* von n :

$$S_n \times \binom{n}{k} \to \binom{n}{k}, (\pi, K) \mapsto \pi(K) = \{\pi(x) \mid x \in K\}.$$

Es ist leicht einzusehen, daß jede k-Teilmenge K von n in jede andere k-Teilmenge K' von n übergeführt werden kann, durch Anwendung eines geeigneten $\pi \in S_n$. Mit dem Fundamentallemma und irgendeinem $K \in \binom{n}{k}$ bekommen wir also:

$$\left|\binom{n}{k}\right| = |S_n/(S_n)_K|\,.$$

Diese *Anzahl der k-Teilmengen* von n kürzt man einfachheitshalber mit demselben Symbol ab:

$$\binom{n}{k} := \left|\binom{n}{k}\right|,$$

diese Zahlen heißen bekanntlich *Binomialkoeffizienten.* Um sie genauer angeben zu können, brauchen wir uns jetzt nur noch zu überlegen, welche Ordnung der Stabilisator $(S_n)_K$ hat. Er besteht offenbar aus genau den $\pi \in S_n$, die sowohl K als auch den Rest $n\backslash K$ fest lassen, das sind die Permutationen der Form $\pi = \rho \cdot \sigma$, wobei ρ höchstens Elemente von K, σ höchstens Elemente der Restmenge vertauscht. Die Anzahl dieser Produkte ist aber $k! \cdot (n-k)!$, und wir erhalten deshalb das folgende interessante Ergebnis:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

$\diamond$

Das für die allgemeine Abzählung von Bahnen von Gruppenoperationen grundlegende Resultat ergibt sich jetzt, wenn wir noch den Begriff der *Fixpunkte* von $g \in G$ definieren:

$$M_g := \{m \mid gm = m\}.$$

2.2.10 Das Lemma von Cauchy-Frobenius *Ist G eine endliche Gruppe, M eine endliche G-Menge, dann ist die Anzahl der Bahnen von G auf M gleich der mittleren Fixpunktzahl der Elemente von G :*

$$|G \setminus\setminus M| = \frac{1}{|G|} \sum_g |M_g|.$$

Beweis:

$$\sum_{g \in G} |M_g| = \sum_{g \in G} \sum_{m \in M_g} 1 = \sum_{m \in M} \sum_{g \in G_m} 1$$

$$= \sum_{m \in M} |G_m| =_{2.2.7} |G| \sum_{m \in M} \frac{1}{|G(m)|} = |G| \cdot |G \setminus\setminus M|.$$

□

2.2.11 Bemerkung Die Anwendung dieser Abzählformel kann man sich mit Hilfe der Tatsache stark vereinfachen, daß die Anzahl der Fixpunkte $|M_g|$ konstant auf den Konjugiertenklassen ist (vgl. Übungsblatt). Man kann deshalb die Summe über alle Gruppenelemente durch die Summe über eine Transversale $\mathcal{C}$ der Konjugiertenklassen ersetzen, wenn man die Ordnungen der Konjugiertenklassen kennt,

$$|G \setminus\setminus M| = \frac{1}{|G|} \sum_{g \in \mathcal{C}} |C^G(g)| \cdot |M_g|.$$

Schließlich sei hierzu noch darauf hingewiesen, daß die Ordnung einer Konjugiertenklasse gleich dem Index des Zentralisators ist (nach dem Fundamentallemma):

$$|C^G(g)| = \frac{|G|}{|C_G(g)|}.$$

Beispielsweise zeigt eine kombinatorische Überlegung, daß der Zentralisator von $\sigma \in S_n$, also die Anzahl der $\pi \in S_n$, deren Anwendung auf die Ziffern in den zyklischen Faktoren von σ wieder σ ergibt, gleich

$$\prod_i i^{a_i(\sigma)} a_i(\sigma)!$$

ist, wenn $a_i(\sigma)$ die Anzahl zyklischer Faktoren von σ bezeichnet. Insgesamt erhalten wir also den folgenden Ausdruck für die Ordnung der Konjugiertenklasse von σ:

$$C^{S_n}(\sigma) = \frac{n!}{\prod_i i^{a_i(\sigma)} a_i(\sigma)!}.$$

◇

2.2.12 Beispiele

- Ist X eine endliche Menge, auf der die endliche Gruppe G von links operiert, Y irgendeine nicht leere endliche Menge, dann induziert die gegebene Operation ${}_GX$ von G auf X eine Operation ${}_G(Y^X)$ von G auf Y^X auf ganz natürliche Weise:
$$G \times Y^X \to Y^X, (g, f) \mapsto \tilde{f},$$
mit $\tilde{f}(x) := f(g^{-1}x)$. Ist jetzt $\bar{g}$ die Permutation von X, die durch $g \in G$ induziert wird: $\bar{g}\colon x \mapsto gx$, dann ist ein $f \in Y^X$ genau dann Fixpunkt, wenn f konstant auf den Bahnen (= Punktemengen in den zyklischen Faktoren) von $\bar{g}$ ist. Das schließt man direkt aus der folgenden Äquivalenz:
$$f \in (Y^X)_g \iff \forall\, x \in X:\ f(x) = f(g^{-1}x) = f(g^{-2}x) = \ldots$$
Wird die Anzahl dieser zyklischen Faktoren mit $z(\bar{g})$ bezeichnet, dann gilt also
$$\left|(Y^X)_g\right| = |Y|^{|\langle \bar{g}\rangle \setminus\setminus X|} = |Y|^{z(\bar{g})}.$$
Mit dem Lemma von Cauchy–Frobenius erhalten wir demnach
$$\left|G \setminus\setminus Y^X\right| = \frac{1}{|G|} \sum_{g \in G} |Y|^{z(\bar{g})}.$$

- Eine konkrete Anwendung hiervon ist die Ermittlung der Anzahl unnumerierter Graphen mit vorgegebener Punktezahl n, denn diese entsprechen ja, wie oben bereits beschrieben, der Bahnenmenge
$$S_n \setminus\setminus 2^{\binom{n}{2}}.$$
Mit dem Lemma von Cauchy–Frobenius ergibt sich demnach für die Anzahl aller unnumerierten Graphen mit n Punkten die Zahl
$$\left|S_n \setminus\setminus 2^{\binom{n}{2}}\right| = \frac{1}{n!} \sum_{\pi \in S_n} 2^{z(\bar{\pi})}.$$
(Es gibt natürlich auch eine explizite Formel für $z(\bar{\pi})$, ihre Herleitung ist aber länglich.)

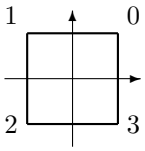
$\diamond$

Aufgabe 2.2.1
Sei (G, M) eine Gruppenoperation. Zeigen Sie:

a) Für $g \in G, m \in M$ ist $gG_mg^{-1} = G_{gm}$.

b) Sind G, M endlich und $g, h \in G$ konjugiert (in G), dann ist $|M_g| = |M_h|$.

Aufgabe 2.2.2



a) Geben Sie die Elemente der Symmetriegruppe D_4 des Quadrats, also die Gruppe der Drehungen und Spiegelungen, die das Quadrat in sich überführen, als Untergruppe der S_4 an.

b) Zeigen Sie, daß die Gruppe D_4 nicht von einem Element erzeugt werden kann, daß sie aber von einer Drehung und einer Spiegelung erzeugt wird.

Aufgabe 2.2.3
Im folgenden werde mit $a_r(\pi)$, $r \in \mathbb{N}^*$ und $\pi \in S_n$, die Anzahl der r-Zyklen in der kanonischen disjunkten Zyklenzerlegung von π bezeichnet. Zeigen Sie:

a) Sind $\pi \in S_n$ und $(i_1\ i_2 \dots\ i_r) \in S_n$ ein r-Zykel, dann gilt:

$$\pi\,(i_1 \dots i_r)\pi^{-1} = (\pi(i_1)\,\pi(i_2) \dots \pi(i_r)).$$

b) Sind $\sigma, \rho \in S_n$ konjugiert, dann ist $a_r(\sigma) = a_r(\rho)$ für alle $r \in \mathbb{N}^*$.

c) Sind $\sigma, \rho \in S_n$ gegeben mit $a_r(\sigma) = a_r(\rho)$ für alle $r \in \mathbb{N}^*$, dann sind σ und ρ konjugiert.

Aufgabe 2.2.4

a) Geben Sie aus jeder Konjugiertenklasse der S_4 genau ein Element an.

b) Die S_4 operiert auf der Menge $M := \binom{4}{2}$ der zweielementigen Teilmengen von 4 in natürlicher Weise (vgl. Vorlesung). Bestimmen Sie die auf M induzierte Zykelstruktur der in a) gewählten Elemente (Skizze).

c) Berechnen Sie die Anzahl der Graphen mit vier Punkten, d.i. die Anzahl der Bahnen von S_4 auf 2^M. (Hinweis: Beachten Sie Aufgabe 13b) und 16b).)

Aufgabe 2.2.5
Das Kohlenstoffgerüst eines Benzolmoleküls ist

a) Geben Sie (ohne Begründung) die sechs Elemente der Symmetriegruppe B des obigen Moleküls als Untergruppe der S_6 an.

b) Jede der freien Bindungen der sechs Kohlenstoffatome seien jeweils durch ein Wasserstoff- oder Chloratom abgesättigt. Dabei ändert sich die Struktur des Kohlenstoffgerüsts nicht. Man nennt nun zwei Moleküle äquivalent, wenn sie durch ein Element von B ineinander übergeführt werden können. Wieviele Äquivalenzklassen gibt es (Begründung)?

(Hinweis: Betrachten Sie die Bahnen von B auf 2^6.)

2.3 Homomorphismen

Algebraische Strukturen werden mit Hilfe *strukturverträglicher* Abbildungen untersucht, die wie folgt definiert werden:

2.3.1 Definition (Homomorphismus) $(G, *)$ und $(H, *')$ seien zwei Gruppoide, zwei Halbgruppen, zwei Monoide oder zwei Gruppen. Eine Abbildung $f : G \to H$ heißt dann *Homomorphismus,* kurz:

$$f : G\mathrm{hom}H, \text{ oder } f \in Hom(G, H),$$

wenn sie die algebraische Struktur auf G respektiert, d.h. wenn

$$f(g * g') = f(g) *' f(g'),$$

und, falls neutrales Element oder Inverse vorhanden sind,

$$f(e_G) = e_H, \ f(g^{-1}) = f(g)^{-1}.$$

Injektive (surjektive) Homomorphismen heißen *Monomorphismen (Epimorphismen)*, bijektive heißen *Isomorphismen.* In diesen Fällen schreibt man entsprechend: $f : G \overset{\sim}{\rightarrowtail} H$ ($f : G \overset{\sim}{\twoheadrightarrow} H$) bzw. $f : G \simeq H$. •

Man braucht dies jedoch meist nicht in allen Einzelheiten nachzuprüfen, denn es gilt

2.3.2 Hilfssatz *Sind G und H Gruppen, dann ist jede mit der Multiplikation verträgliche Abbildung $f: G \to H$ ein Homomorphismus.*

Beweis: Ist $f: G \to H$ eine Abbildung mit $f(g * g') = f(g) *' f(g')$, dann gilt

$$f(g) = f(g * e_G) = f(g) *' f(e_G),$$

also $f(e_G) = e_H$, da H ja eine Gruppe ist (so daß $f(g)$ ein Inverses besitzt). Bild des neutralen Elements ist demnach das neutrale Element. Ganz entsprechend weist man nach, daß das Bild des Inversen das Inverse des Bildes ist. □

2.3.3 Beispiele

- $exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot), x \mapsto \exp(x)$ ist Isomorphismus,
- $ln : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +), x \mapsto \ln(x)$.

Diese Isomorphismen — sie sind zueinander invers — ermöglichten die Konstruktion des Rechenschiebers, der das Multiplizieren reeller Zahlen, etwa x und y, durch das Addieren der Strecken $\ln(x)$ und $\ln(y)$ ersetzt:

$$\exp(\ln(x) + \ln(y)) = x \cdot y.$$

◇

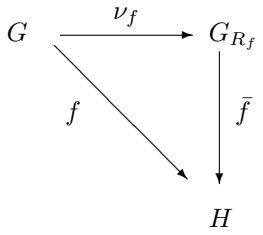
Ist $f \in \mathrm{Hom}(G, H)$ ein Homomorphismus zwischen zwei multiplikativ geschriebenen Gruppoiden, Halbgruppen, Monoiden oder Gruppen, dann bilden die Klassen $[g]_{R_f}$ der induzierten Äquivalenzrelation R_f mit der Multiplikation

$$[g]_{R_f} \cdot [g']_{R_f} := [gg']_{R_f}$$

das Gruppoid G_{R_f}, denn es ist leicht nachzuprüfen, daß diese Verknüpfung wohldefiniert ist. Die natürliche Abbildung von G hierauf bezeichnen wir mit

$$\nu_f \colon G \to G_{R_f}, g \mapsto [g]_{R_f}.$$

Aus dem Abbildungssatz folgt die Existenz einer Abbildung $\bar{f}$, die das Diagramm



kommutativ ergänzt, eindeutig bestimmt sowie injektiv ist und die folgende Form hat:

$$\bar{f} \colon G_{R_f} \to H, [g]_{R_f} \mapsto f(g).$$

Man prüft zudem leicht nach, daß es sich bei $\bar{f}$ um einen Homomorphismus handelt:

$$\bar{f}([g]_{R_f}[g']_{R_f}) = \bar{f}([gg']_{R_f}) = f(gg') = f(g)f(g') = \bar{f}([g]_{R_f})\bar{f}([g']_{R_f}).$$

Wenn wir ihren Wertebereich auf das *Bild* von f,

$$\mathrm{Bild}(f) := \{f(g) \mid g \in G\},$$

einschränken, erhalten wir demnach einen Isomorphismus zwischen den beiden Gruppoiden G_{R_f} und $\mathrm{Bild}(f)$. Dieses wichtige Resultat heißt

2.3.4 Der Homomorphiesatz für Gruppoide *Sind G und H zwei Gruppoide, dann gilt für jeden Homomorphismus $f \colon G \to H$, die davon induzierte Äquivalenzrelation R_f und das Gruppoid aus deren Äquivalenzklassen die folgende Isomorphie (zwischen Gruppoiden)*

$$G_{R_f} \simeq \mathrm{Bild}(f).$$

Das Bild eines Homomorphismus $f \colon G\mathrm{hom}H$ ist also im wesentlichen dasselbe wie G_{R_f}! Wir wollen deshalb dieses Gruppoid genauer beschreiben, insbesondere für den Fall, daß G und H Gruppen sind. (Eigentlich genügt sogar die Forderung, G sei eine Gruppe, weil man H ja durch $\mathrm{Bild}(f)$, d. h. durch Einschränkung des

Blickwinkels auf das Bild von f, ersetzen kann, und dieses Bild ist leicht als Gruppe nachgewiesen, s.u..) Seien also G und H Gruppen, $f \in \mathrm{Hom}(G, H)$. Wir bezeichnen die folgende Teilmenge von G als den *Kern* von f :

$$\mathrm{Kern}(f) := \{g \mid f(g) = 1_H\}.$$

$\mathrm{Kern}(f)$ und $\mathrm{Bild}(f)$ sind leicht als Untergruppen erkannt. Darüberhinaus ist der Kern eine Untergruppe mit speziellen Eigenschaften. Solche Untergruppen wollen wir jetzt einführen:

2.3.5 Definition Ist G eine Gruppe, dann heißt $T \subseteq G$ *normale* Teilmenge von G, wenn gilt:

$$\forall\ g \in G\colon\ gT = Tg,$$

oder, was dasselbe ist

$$\forall\ g \in G\colon\ gTg^{-1} = T.$$

Normale Untergruppen U heißen *Normalteiler*, hierfür schreiben wir kurz:

$$U \trianglelefteq G.$$

•

Wichtige Beispiele normaler Teilmengen sind die bereits erwähnten Konjugiertenklassen von Elementen:

$$C^G(g') = \{gg'g^{-1} \mid g \in G\},$$

es sind die *kleinsten* normalen Teilmengen von G, d. h. jede normale Teilmenge $T \subseteq G$ ist Vereinigung von Konjugiertenklassen $C^G(g')$. Die Umkehrung gilt ebenfalls: Jede Vereinigung von Konjugiertenklassen ist eine normale Teilmenge. Betrachten wir die normalen Untergruppen etwas genauer, es wird sich nämlich gleich zeigen, daß diese *genau die Kerne von Homomorphismen sind!*
Eine Untergruppe $U \leq G$ ist also genau dann ein Normalteiler, wenn die Linksnebenklassen auch Rechtsnebenklassen sind:

$$\forall\ g \in G\colon\ gU = Ug.$$

Genau bei Normalteilern braucht man demnach Links- und Rechtsnebenklassen nicht zu unterscheiden, man spricht dann einfachheitshalber von *Nebenklassen.*

2.3.6 Beispiele

- Als *triviale* Normalteiler bezeichnet man $\{1\}$ und G. Gruppen, die nur diese beiden Normalteiler besitzen, heißen *einfach.*
- Untergruppen vom Index 2 sind stets normal.
- In abelschen Gruppen sind sämtliche Untergruppen normal.

◇

2.3.7 Satz *Sind G und H Gruppen und $f \in Hom(G,H)$, dann gilt:*

i) Der Kern von f ist Normalteiler:

$$\mathrm{Kern}(f) \trianglelefteq G.$$

ii) Die von f auf G induzierte Äquivalenzrelation besteht gerade aus den Nebenklassen des Kerns:

$$G_{R_f} = G/\mathrm{Kern}(f).$$

iii) Die Nebenklassenmenge $G/\mathrm{Kern}(f)$ ist, zusammen mit der oben bereits eingeführten Multiplikation

$$(g\mathrm{Kern}(f)) \cdot (g'\mathrm{Kern}(f)) := (gg')\mathrm{Kern}(f),$$

eine Gruppe, die sogenannte Faktorgruppe *von G nach* $\mathrm{Kern}(f)$.

iv) Ist N ein Normalteiler in G, dann ist die Abbildung

$$\nu_N \colon G \to G/N, g \mapsto gN$$

ein Epimorphismus von G auf G/N, die Faktorgruppe von G nach N.

Insgesamt bedeutet das, daß genau die Normalteiler von G die Kerne von Homomorphismen auf G sind und die induzierten Äquivalenzrelationen gerade die jeweiligen Nebenklassenmengen.

Beweis: Wir beweisen zunächst i) und ii) gemeinsam:

$$[g]_{R_f} = [g']_{R_f} \iff f(g) = f(g') \iff f(gg'^{-1}) = 1_H$$

$$\iff gg'^{-1} \in \mathrm{Kern}(f) \iff \mathrm{Kern}(f)g = \mathrm{Kern}(f)g'.$$

Da f auf der Nebenklassen $\mathrm{Kern}(f)g$ den Wert $f(g)$ hat, folgt damit: Die Klassen von R_f sind gerade die Rechtsnebenklassen von $\mathrm{Kern}(f)$. Aus Symmetriegründen sind diese Klassen aber auch die Linksnebenklassen des Kerns. Links- und Rechtsnebenklassenmengen sind also gleich, nach obigem Hilfssatz folgt daraus die Normalteilereigenschaft. Damit sind i) und ii) bewiesen.

Zum Nachweis von iii) bemerken wir, daß die Nebenklassen des Kerns demnach das Gruppoid $G_{R_f} = G/\mathrm{Kern}(f)$ bilden, wie bereits weiter oben festgestellt wurde; dieses ist ganz offensichtlich eine Gruppe.

Ist schließlich umgekehrt N ein Normalteiler in G, dann ist ν_N eine Abbildung auf die Menge der Nebenklassen von N, und diese bilden eine Gruppe wie man leicht nachrechnet. Die Multiplikation in G/N zeigt sofort, daß diese Abbildung darüberhinaus ein Homomorphismus ist, insgesamt ist es also ein Epimorphismus, und damit ist auch iv) verifiziert. □

Aus all diesen Überlegungen halten wir insbesondere folgendes fest, was aus dem letzten Satz und dem allgemeinen Homomorphiesatz für Gruppoide folgt:

2.3.8 Der Homomorphiesatz für Gruppen *Sind G und H zwei Gruppen und ist $f \in \mathrm{Hom}(G,H)$, dann besteht folgender enge Zusammenhang zwischen Kern und Bild von f :*

$$G/\mathrm{Kern}(f) \simeq \mathrm{Bild}(f).$$

Das Bild von G unter f ist also im wesentlichen dasselbe wie die Faktorgruppe von G nach dem Kern von f.

2.3.9 Beispiele

- Das Problem der Lösbarkeit des linearen Gleichungssystems

$$\sum_{k=0}^{n-1} a_{ik}x_k = b_i, 0 \leq i \leq m-1,$$

kann als Frage nach dem Urbild von $b \in \mathbb{R}^m$ unter dem Homomorphismus

$$f\colon \mathbb{R}^n \to \mathbb{R}^m, x \mapsto \begin{pmatrix} \sum_k a_{0k}x_k \\ \vdots \\ \sum_k a_{ik}x_k \\ \vdots \\ \sum_k a_{m-1,k}x_k \end{pmatrix}$$

angesehen werden. Das Gleichungssystem ist nämlich ganz offenbar genau dann lösbar, wenn die rechte Seite, der Vektor b, in $\mathrm{Bild}(f)$ liegt. *Der Homomorphiesatz besagt, daß, bei Lösbarkeit, die Lösungsgesamtheit gerade eine Nebenklasse des Kerns des Homomorphismus ist:*

$$L_I = x + \mathrm{Kern}(f).$$

Und der Kern dieses Homomorphismus ist gerade die Lösungsgesamtheit L_H des homogenen Systems, insgesamt gilt also, falls $b \in \mathrm{Bild}(f)$:

$$L_I = x + L_H,$$

mit irgendeinem $x \in f^{-1}(b)$.

Das bestätigt die obigen Vorüberlegungen und zeigt, daß sich diese Lösungsmenge (gegebenenfalls, d. h. wenn sie nicht leer ist) als Nebenklasse erweist.

- Ein nichttrivialer Homomorphismus ist die Abbildung von Permutationen auf das sogenannte *Vorzeichen* bzw. das *Signum.* Sie spielt später, bei der Einführung der Determinanten, eine sehr wichtige Rolle:

  i) für $n \in \mathbb{N}$ sei das *Differenzenprodukt* Δ_n wie folgt definiert:

$$\Delta_n := \prod_{0 \leq i < j \leq n-1} (j-i) \in \mathbb{N}^*$$

(beachten Sie, daß das "leere Produkt"gleich 1 gesetzt wird, so daß $\Delta_0 = \Delta_1 = 1$ gilt).

ii) Für $\pi \in S_0$ sei $\pi\Delta_0 := 1$ und, für $\pi \in S_1, \pi\Delta_1 := 1$ gesetzt. Für $n > 1$ setzen wir

$$\pi\Delta_n := \prod_{0 \le i < j \le n-1} (\pi(j) - \pi(i)) \in \mathbb{Z}.$$

Beispielsweise ist $\Delta_2 = 1 - 0 = 1$, und $(01)\Delta_2 = 0 - 1 = -1$.

iii) Das *Signum* von $\pi \in S_n, n \in \mathbb{N}$, sei definiert als

$$\operatorname{sgn}(\pi) := \frac{\pi\Delta_n}{\Delta_n},$$

beispielsweise also $\operatorname{sgn}((01)) = -1$.

iv) Die Abbildung $\operatorname{sgn}\colon \pi \mapsto \operatorname{sgn}(\pi)$ ist ein Homomorphismus von S_n in die Gruppe $(\{1, -1\}, \cdot)$, und für $n \ge 2$ ist dieser ein Epimorphismus.

Beweis: Um die Homomorphie zu zeigen, bemerken wir

$$\operatorname{sgn}(\pi\rho) = \prod_{i<j} \frac{\pi\rho(j) - \pi\rho(i)}{\rho(j) - \rho(i)} \cdot \frac{\rho(j) - \rho(i)}{j - i} = \left(\prod_{i<j} \frac{\pi\rho(j) - \pi\rho(i)}{\rho(j) - \rho(i)} \right) \cdot \operatorname{sgn}(\rho)$$

Jetzt verwenden wir, daß die Anweisung $i < j$ unter dem Produktzeichen bedeutet, daß das Produkt über alle i und j aus den verschiedenen Zweiermengen $\{i, j\} \subseteq n$ zu bilden ist. Wegen der Bijektivität von ρ können wir diese "Laufanweisung" also durch die Anweisung $\rho(j) < \rho(i)$ ersetzen und wie folgt weiterfahren:

$$= \left(\prod_{\rho(j)<\rho(i)} \frac{\pi\rho(j) - \pi\rho(i)}{\rho(j) - \rho(i)} \right) \cdot \operatorname{sgn}(\rho) = \left(\prod_{i<j} \frac{\pi(j) - \pi(i)}{j - i} \right) \cdot \operatorname{sgn}(\rho)$$

$$= \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\rho).$$

Ist π Transposition benachbarter Ziffern, dann gilt offenbar $\operatorname{sgn}(\pi) = -1$. Weil die Transpositionen die symmetrische Gruppe erzeugen, beweist das die Behauptung, sgn sei ein Homomorphismus aus S_n.

$\diamond$

2.3.10 Definition Der Kern $A_n = \{\pi \in S_n \mid \operatorname{sgn}(\pi) = 1\}$ dieses Homomorphismus heißt die *alternierende Gruppe* in S_n. $\pi \in S_n$ heißt *gerade* Permutation, wenn $\pi \in A_n$, andernfalls heißt π *ungerade*. •

2.3.11 Folgerungen

i) $A_0 = S_0 = \{1\}$, ebenso $A_1 = S_1 = \{1\}$, dagegen ist, für $n \ge 2$, A_n Normalteiler vom Index 2 in S_n.

ii) Ein r–Zyklus ist genau dann gerade, wenn r ungerade ist.

iii) $\pi \in S_n$ liegt genau dann in A_n, wenn π (bezogen auf die Standardzyklenschreibweise oder jede andere Darstellung von π als Produkt von Zyklen) geradzahlig viele Zyklen gerader Länge enthält.

Um dieses Signum auf symmetrische Gruppen beliebiger endlicher Mengen zu verallgemeinern, überlegen wir uns noch:

2.3.12 Hilfssatz

i) Für $\pi \in S_n$ bedeute wieder $a_i(\pi)$ die Anzahl der zyklischen Faktoren der Länge i. Die Folge

$$a(\pi) = (a_1(\pi), \ldots, a_n(\pi))$$

dieser Vielfachheiten heißt der Zykeltyp *von π und bestimmt, genau wie die Zykelpartition, die Konjugiertenklasse von π. Aus ihm läßt sich wie folgt das Vorzeichen von π ermitteln,*

$$sgn(\pi) = (-1)^{n-z(\pi)},\ z(\pi) := \sum_i a_i(\pi).$$

Es ist leicht einzusehen, daß jede Folge $a = (a_1, \ldots, a_n)$ natürlicher Zahlen a_i mit $\sum_i i \cdot a_i = n$ als Zykeltyp von Elementen in S_n vorkommt.

ii) sgn ist, für $n \geq 2$, der einzige Homomorphismus von S_n in $(\mathbb{C}^*, \cdot)$, der nicht trivial ist, d.h. verschieden von $\pi \mapsto 1$.

iii) Für endliche Mengen X, Y gilt

$$S_X \simeq S_Y \Longleftrightarrow |X| = |Y|.$$

Beweis:

i) $\operatorname{sgn}(\pi) = (-1)^{\sum (i-1)a_i(\pi)} = (-1)^{n-z(\pi)}$, das ergibt sich aus iii) in 2.3.11.

ii) Sei $f \in Hom(S_n, \mathbb{C}^*)$. Da die Transpositionen S_n erzeugen, diese konjugiert sind, und ± 1 die einzigen Quadratwurzeln von 1 in $\mathbb{C}^*$ sind, ist f genau dann nicht trivial, wenn für jede Transposition τ gilt $f(\tau) = -1$.

iii) $|X| = |Y|$ heißt, daß es eine Bijektion $f: X \to Y$ gibt. Für ein solches f sei

$$\varphi: S_X \to Y^Y, \pi \mapsto f \circ \pi \circ f^{-1}.$$

Man sieht leicht, daß $\varphi(\pi) \in S_Y$ und φ ein Isomorphismus ist.

Umgekehrt gilt: $S_X \simeq S_Y$ ergibt $|X|! = |Y|!$, also wegen der Endlichkeit auch $|X| = |Y|$. □

2.3.13 Folgerung *Ist X eine endliche Menge, dann ist, für $|X| \geq 2$,*

$$sgn\colon \pi \mapsto (-1)^{|X|-z(\pi)}$$

der einzige nicht triviale Homomorphismus von S_n nach $(\mathbb{C}^*, \cdot)$, sein Kern

$$A_X = \{\pi \in S_X \mid sgn(\pi) = 1\}$$

also die einzige Untergruppe vom Index 2 in S_X.

Nachdem wir jetzt mit dem Signum einen nichttrivialen Homomorphismus auf einer ganzen Klasse nichttrivialer Gruppen — den endlichen symmetrischen Gruppen — kennengelernt haben, kehren wir nocheinmal zur allgemeinen Situtation zurück, also zur Untersuchung eines Homomorphismus $f\colon G\mathrm{hom}H$. Es gilt nämlich noch sehr viel mehr als "nur" die Isomorphie zwischen dem Bild von f und der Faktorgruppe nach dem Kern. Der Homomorphismus überträgt nämlich die gesamte sogenannte *Verbandsstruktur*. Um dies zu beschreiben, benötigen wir den folgenden Begriff:

2.3.14 Definition (geordnet, Verband) Eine Menge V, zusammen mit einer Relation $\preceq$, heißt *geordnet,* wenn $\preceq$ reflexiv, antisymmetrisch und transitiv ist. Eine geordnete Menge $(V, \preceq)$ heißt *Verband,* wenn zu je zwei Elementen $u, v \in V$ deren Supremum $u \vee v$ und deren Infimum $u \wedge v$ (also eine kleinste obere und eine größte untere Schranke) existieren. •

Beispiele sind die Klasse aller Mengen, mit Infimum $\wedge := \cap$ und Supremumsbildung $\vee := \cup$, natürlich auch die Potenzmenge einer Menge M.

Am meisten interessiert uns im Moment der *Untergruppenverband* einer Gruppe,

$$U(G) := \{U \mid U \leq G\},$$

zusammen mit $\subseteq$ als Ordnung. Hier ist das Infimum natürlich

$$U \wedge V := U \cap V,$$

denn der Schnitt von Untergruppen ist wieder eine Untergruppe und offenbar die größte Untergruppe, die in beiden liegt, also deren untere Schranke bzgl. $\subseteq$. Das Supremum ist das Erzeugnis der Vereinigung:

$$U \vee V := \langle U \cup V \rangle.$$

2.3.15 Satz *Ein Homomorphismus $f\colon G\mathrm{hom}H$ induziert einen Ordnungsisomorphismus zwischen dem Verband der Untergruppen von G, die* $\mathrm{Kern}(f)$ *enthalten und dem Verband der Untergruppen von* $\mathrm{Bild}(f)$.

(Vgl. Übungsblatt)

Übungen:

Ü 2.3.1 Zeigen Sie,daß eine Untergruppe $U \leq G$ genau dann ein Normalteiler ist, wenn jede Linksnebenklasse auch Rechtsnebenklasse ist:

$$\forall\, g \in G\ \exists\, g' \in G\colon\ gU = Ug'.$$

Ü 2.3.2 Sei G eine Gruppe. Zeigen Sie:

i) Für jedes $g \in G$ ist die Abbildung $\kappa_g\colon G \to G, \quad h \mapsto ghg^{-1}$ ein Gruppenisomorphismus.

ii) Bezeichnet man für jedes $g \in G$ mit $l_g\colon G \to G, \quad x \mapsto gx$, die Linkstranslation, dann ist $\phi\colon G \to S_G, g \mapsto l_g$, ein Gruppenmonomorphismus.

iii) Ist G abelsch, dann ist $\psi\colon G \to G, \quad g \mapsto g^{-1}$ ein Gruppenisomorphismus.

Ü 2.3.3 Betrachten Sie $\mathbb{Z}/3\mathbb{Z}$. Beschreiben Sie die Elemente von $\mathbb{Z}/3\mathbb{Z}$, und geben Sie die Multiplikationstafel des Gruppoids $(\mathbb{Z}/3\mathbb{Z}, \cdot)$ mit $a \cdot b := ab$ an.

Ü 2.3.4 Es sei $m \geq 3$ und $a := (1, m) \circ (2, m-1) \circ \ldots, \quad b := (1 \ldots m) \in S_m$. Setze $H :=< a >, \quad N :=< b >, \quad D_{2m} :=< a, b >$.

a) Zeigen Sie: $H^N = D_{2m}$, und bestimmen Sie die Mächtigkeit von D_{2m}.

b) Sei nun $m := 4$. Bestimmen Sie zwei Untergruppen U und V von $D_{2\cdot 4}$ mit $U \lhd V, \quad V \lhd D_{2\cdot 4}$, aber $U \not\lhd D_{2\cdot 4}$.

2.4 Strukturen mit Operatorenbereichen

Zu den Strukturen mit einer inneren Verknüpfung $*\colon G \times G \to G$ kommen jetzt Strukturen hinzu, die außerdem noch eine *äußere* Verknüpfung

$$\Delta\colon \Omega \times G \to G, (\omega, g) \mapsto \omega\Delta g$$

besitzen:

2.4.1 Definition (Operatorenbereiche, Operatorhomomorphismen) Sei $(G, *)$ Gruppoid, Ω eine Menge und $\Delta\colon \Omega \times G \to G$.

i) G, genauer: $(G, *, \Delta)$, heißt Gruppoid mit *Operatorenbereich* Ω oder auch $\Omega-$*Gruppoid,* wenn gilt

$$\omega\Delta(g * g') = (\omega\Delta g) * (\omega\Delta g'),$$

d. h. wenn l_ω, die Linksmultiplikation mit $\omega \in \Omega$, in $\mathrm{End}(G) := \mathrm{Hom}(G, G)$ liegt, also ein Endomorphismus von G ist.

ii) Sind $(G, *, \Delta)$ und $(G', *', \Delta')$ $\Omega-$Gruppoide, $f \in Hom(G, G')$, dann heißt f ein $\Omega-$*Homomorphismus* (kurz: $f \in Hom_\Omega(G, H)$), wenn gilt

$$f(\omega\Delta g) = \omega\Delta' f(g),$$

also wenn f mit der äußeren Verknüpfung vertauschbar ist.

iii) Ist $(G, *, \Delta)$ ein $\Omega-$Gruppoid, dann heißt ein Untergruppoid $U \subseteq G$ *zulässiges Untergruppoid,* wenn gilt

$$\omega\Delta u \in U,$$

also wenn U bzgl. der äußeren Verknüpfung abgeschlossen ist. Entsprechend sind *zulässige Unterhalbgruppe, ...*, *zulässige Untergruppe* und *zulässiger Normalteiler* definiert.

•

Man kann jeweils leicht nachprüfen, daß sich aus den voraufgegangenen Sätzen über Homomorphismen Sätze über $\Omega-$Gruppen und $\Omega-$Homomorphismen ergeben, wenn man jeweils "Homomorphismus"durch "$\Omega-$Homomorphismus", "Untergruppoid, ..." durch "zulässiges Untergruppoid, ..." und "Normalteiler" durch "zulässigen Normalteiler" ersetzt.

2.4.2 Beispiele

- $\mathbb{R}^n$ hat $\mathbb{R}$ als Operatorenbereich:

$$r \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} rx_1 \\ \vdots \\ rx_n \end{pmatrix}.$$

- Die Lösungsgesamtheit L_H eines homogenen linearen Gleichungssystems

$$\sum_{k=0}^{n-1} a_{ik}x_k = 0,\ 0 \leq i \leq m-1,$$

ist zulässige Untergruppe.

- $\mathbb{R}^n, \mathbb{R}^m$ sind abelsche $\mathbb{R}-$Gruppen, und die Abbildung

$$f\colon \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} \sum_k a_{0,k}x_k \\ \vdots \\ \sum_k a_{m-1,k}x_k \end{pmatrix}$$

ist ein $\mathbb{R}-$Homomorphismus.

$\diamond$

2.5 Ringe und Körper

Wir betrachten jetzt algebraische Strukturen mit *zwei* inneren Verknüpfungen.

2.5.1 Definition (Ring) Ist R eine Menge mit zwei inneren Verknüpfungen

$$+: R \times R \to R \text{ und } \cdot: R \times R \to R,$$

dann heißt R *Ring,* (mit Einselement) wenn gilt

- $(R, +)$ ist abelsche Gruppe,
- $(R, \cdot)$ ist Halbgruppe (Monoid)
- l_r, r_t, die Linksmultiplikation mit r bzw. die Rechtsmultiplikation mit t, liegen in $\mathrm{End}(R) := \mathrm{Hom}((R, +), (R, +))$, d.h. es gelten die sogenannten *Distributivgesetze*

$$r(s + t) = rs + rt, (r + s)t = rt + st.$$

•

Ein Ring $(R, +, \cdot)$ heißt *kommutativer Ring,* wenn $(R, \cdot)$ kommutativ ist. Das neutrale Element von $(R, +)$ wird mit 0_R oder kürzer mit 0 bezeichnet und *Null(element)* genannt. Das neutrale Element von $(R, \cdot)$ wird gegebenenfalls mit 1_R bzw. 1 bezeichnet und *Eins(element)* genannt. Das Inverse zu r in $(R, +)$ wird mit $-r$ bezeichnet, und statt $r + (-s)$ schreiben wir $r - s$.

2.5.2 Beispiele

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind kommutative Ringe, ebenso die *Restklassenringe*

  $$\mathbb{Z}_n := \{0, 1, \ldots, n - 1\}$$

  mit Addition und Multiplikation *modulo* n.

- Ist R ein Ring, M eine Menge, dann ist $(R^M, +, \cdot)$ ein Ring, wenn wir $+$ und $\cdot$ wieder *punktweise* definieren:

  $$(f + g)(m) := f(m) + g(m), (f \cdot g)(m) := f(m) \cdot g(m).$$

- Es gibt auch interessante *nicht punktweise* Verknüpfungen auf solchen Mengen R^M von Abbildungen, sogenannte *Faltungen,* bei denen eine Struktur auf M benutzt wird, z.B. beim Ring $R^{\mathbb{N}}$ der *Potenzreihen* über R : Hier ist die *Addition punktweise:*

  $$(f + g)(n) := f(n) + g(n),$$

  die *Multiplikation die Faltung,* bei der über alle Paare summiert wird, die eine Gleichung lösen:

  $$(f \cdot g)(n) := \sum_{(i,j):\ i+j=n} f(i) \cdot f(j).$$

Ein Unterring hiervon ist der *Polynomring,* der aus den $f \in R^{\mathbb{N}}$ besteht, die fast überall den Wert 0 haben. Die Potenzreihen und die Polynome schreibt man üblicherweise nicht als Abbildungen sondern als sogenannte *formale Summen:*

$$f = \sum_{n\in\mathbb{N}} a_n x^n.$$

x^n spielt dabei die Rolle des "Aufhängers" des Wertes a_n von f an der Stelle $n \in \mathbb{N}$. x nennt man dabei eine *Unbestimmte,*) und man bezeichnet diesen Ring auch mit

$$R[x].$$

Die Faltung ist dann gerade das bekannte "Ausmultiplizieren". Diese Schreibweise erspart die Anführung von Termen $a_n = 0$, sie ist also besonders sparsam und von den Polynomen her bekannt. Z.B. ist $1 + x^2 + 3,14x^3 \in \mathbb{R}[x] \subset \mathbb{R}^{\mathbb{N}}$.

- Ist $(G, *)$ eine abelsche Gruppe, dann ist $(\mathrm{End}(G), +, \circ)$ mit

  $$(f + f')(g) := f(g) * f'(g)$$

  ein (i.a. nicht kommutativer!) Ring, der *Endomorphismenring* von G.

◇

Weil Links- und Rechtsmultiplikationen mit Ringelementen Endomorphismen sind, gilt, da Endomorphismen das neutrale Element auf sich selbst und das Inverse eines Elements auf das Inverse des Bildes des Elements abbilden):

2.5.3 $$r \cdot 0 = 0 \cdot r = 0_R,\ (-r)s = r(-s) = -(rs),\ (-r)(-s) = rs.$$

Ist R ein vom *Nullring* $\{0\}$ verschiedener Ring mit Einselement, dann ist dieses von Null verschieden:

2.5.4 $$[R \neq \{0_R\} \wedge 1_R \in R] \Longrightarrow 0_R \neq 1_R.$$

Das beweisen wir indirekt, d.h. wir unterstelle $0 = 1$,

$$r \in R^* := R\backslash\{0\} \Longrightarrow 0 \neq r = r \cdot 1 = r \cdot 0 =_{2.5.3} 0,$$

ein Widerspruch. Per Induktion zeigt man schließlich noch die Gültigkeit der verallgemeinerten Distributivgesetze

2.5.5 $$r \sum_{i=1}^{n} s_i = \sum_{i=1}^{n} r s_i, (\sum_{i=1}^{n} s_i)\, r = \sum_{i=1}^{n} s_i r.$$

Eine Abbildung $f\colon R \to R'$ zwischen zwei Ringen heißt — gemäß der allgemeinen Homomorphismusdefinition — *Ringhomomorphismus,* wenn sie mit allen Verknüpfungen vertauschbar ist, also mit der Addition und der Multiplikation, sowie — bei Ringen mit Einselement — mit der Auswahl des Einselements. (Da

sie mit der Addition vertauschbar ist, gilt dies ja dann auch automatisch für die Auswahl des Nullelements und für die Inversenbildung!) Bei Ringen, für die eine Existenz eines Einselements nicht verlangt ist, genügt also die Forderung

$$f(r+r') = f(r) + f(r') \ \wedge f(rr') = f(r)f(r').$$

Entsprechend sind *Ringmonomorphismen, Ringepimorphismen, Ringisomorphismen, Ringendomorphismen* etc. definiert. Kerne von Ringhomomorphismus sind genau die sogenannten *Ideale,* das sind zulässige Untergruppen, mit R als Links- und Rechtsoperatorenbereich. Für Ideale benutzt man dasselbe Zeichen $\trianglelefteq$ wie für Normalteiler:

2.5.6 $$I \trianglelefteq R :\Longleftrightarrow \ \forall\, i, i' \in I, r \in R\colon\ i - i', ri, ir' \in I.$$

Ein Beispiel für ein Ideal in $\mathbb{Z}$ ist die Menge $\{z \cdot n \mid z \in \mathbb{Z}\}$ aller Vielfachen einer natürlichen Zahl n, denn diese Menge erfüllt offenbar 2.5.6. Darüberhinaus sieht man leicht ein, daß jedes Ideal, das n enthält, die Menge $\{z \cdot n \mid z \in \mathbb{Z}\}$ umfaßt, diese Menge ist also *das von n erzeugte Ideal!*
Die Nebenklassen

$$r + I = \{r + i \mid i \in I\} \subseteq R$$

eines solchen Ideals bilden den *Faktor-, Quotienten-* oder auch *Restklassenring* R/I von R nach I bzgl. den folgenden Verknüpfungen:

$$(r + I) + (r' + I) := (r + r') + I,\ \ (r + I) \cdot (r' + I) := (r \cdot r') + I.$$

Zusammenfassend ergibt sich

2.5.7 Der Homomorphiesatz für Ringe *Sind R und R' Ringe, und ist f ein Homomorphismus zwischen diesen, dann gilt*

$$\mathrm{Kern}(f) = \{r \in R \mid f(r) = 0_{R'}\} \trianglelefteq R,$$

und zwischen Bild und Kern besteht die folgende Beziehung:

$$\varphi\colon R/Kernf \simeq \mathrm{Bild}(f)\colon r + Kernf \mapsto f(r).$$

Ist umgekehrt I ein Ideal in R, dann ist dieses der Kern des folgenden Homomorphismus:

$$\nu_I\colon\ R \to R/I, r \mapsto r + I.$$

2.5.8 Beispiele

- Besonders interessant sind die von *einem einzigen Element* erzeugten Ideale, die sogenannten *Hauptideale.* Das von $r \in R$ erzeugte Ideal wollen wir mit

  $$(r)$$

  bezeichnen, damit keine Verwechslung mit $\langle r \rangle$, der von r erzeugten Untergruppe in $(R, +)$ unterlaufen kann.

Ein Beispiel eines solchen Ideals (in $\mathbb{Z}$) haben wir bereits kennengelernt. Der allgemeine Fall, das von $t \in R$ erzeugte Hauptideal, sieht allerdings erheblich komplizierter aus, es gilt nämlich (vgl. Übungsaufgabe!):

$$2.5.9 \qquad (r) = \mathbb{Z}r + Rr + rR + \left\{ \sum_{i=0}^{n} r_i r r_i' \;\middle|\; n \in \mathbb{N}, r_i, r_i' \in R \right\}.$$

Ist R ein Ring mit Einselement, dann vereinfacht sich diese Darstellung zu $(r) = \{\sum_{i=0}^{n} r_i r r_i' \mid n \in \mathbb{N}, r_i, r_i' \in R\}$, und wenn zusätzlich R auch noch kommutativ ist, dann haben wir $(r) = Rr = \{sr \mid s \in R\}$.

- Der oben bereits erwähnte Ring $\mathbb{Z}_n$ kann auch als Faktorring beschrieben werden:
$$n\mathbb{Z} := (n) = \{nz \mid z \in \mathbb{Z}\} \trianglelefteq \mathbb{Z}$$
ist das oben bereits beschriebene, von n erzeugte Hauptideal in $\mathbb{Z}$, für jedes $n \in \mathbb{N}$. Der Faktorring
$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$$
entsteht aus $\mathbb{Z}$ durch die Abbildung von $z \in \mathbb{Z}$ auf den Rest $\bar{z}$ von z modulo n. Addition bzw. Multiplikation sind die *Addition modulo n* bzw. die *Multiplikation modulo n*. So sind die Verknüpfungstafeln von $\mathbb{Z}_4$ beispielsweise

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Die Multiplikationstafel von $\mathbb{Z}_4$ zeigt, daß $\mathbb{Z}_4^*$ nicht multiplikativ abgechlossen ist ($\bar{2} \cdot \bar{2} = \bar{0} \ni \mathbb{Z}_4^*$), der Ring $\mathbb{Z}_4$ ist also kein Körper. Dagegen kann man zeigen, daß alle Restklassenringe $\mathbb{Z}_p$, p prim, Körper sind, beispielsweise also auch $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, der bekannte *binäre Zahlkörper.*

Aus gegebenen Zahlkörpern kann man — mit Hilfe der Polynomringe über diesen — weitere Zahlbereiche konstruieren. Zum Beispiel ist
$$\mathbb{Z}_2[x]/(1 + x + x^2)$$
ein Körper mit vier Elementen.

- Sei $\mathbb{R}[x]$ der Ring der Polynome in der Unbestimmten x und mit Koeffizienten in $\mathbb{R}$. Das vom Polynom $1 + x^2$ erzeugte Ideal ist
$$I = \{p \cdot (1 + x^2) \mid p \in \mathbb{R}[x]\},$$
es besteht also gerade aus den Vielfachen von $1 + x^2$. Der Restklassenring $\mathbb{R}[x]/I$ ist isomorph zum Körper (s. u.)
$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

der *komplexen Zahlen,* in dem wie folgt addiert und multipliziert wird:

$(a+bi)+(c+di) := (a+c)+(b+d)i, (a+bi)\cdot(c+di) := (ac-bd)+(ad+bc)i.$

Die Isomorphie zeigt sich durch Anwenden der Abbildung

$$\mathbb{C} \ni a + bi \mapsto a + bx + I \in \mathbb{R}[x]/I,$$

denn sie ist offenbar ein Homomorphismus bzgl. Addition, aber auch bzgl. Multiplikation, da

$$\begin{aligned}(a + bx + I)(c + dx + I) &= (a + bx)(c + dx) + I \\ &= (a + bx)(c + dx) + \underbrace{(-bd)(1 + x^2) + I}_{=I} \\ &= (ac - bd) + (ad + bc)x + I.\end{aligned}$$

Diese Abbildung ist surjektiv, da es für jedes $p \in \mathbb{R}[x]$ Zahlen $a, b \in \mathbb{R}$ gibt mit $p + I = a + bx + I$. Sie ist zudem offensichtlich injektiv, und $1 + I$ ist das neutrale Element.

Wir bemerken, daß die *Dividierbarkeit von Polynomen mit Rest* diese beiden Konstruktionen von Körpern ermöglicht hat! ◇

Ist R ein Ring mit Einselement 1_R, dann ist die von dem Einselement erzeugte Untergruppe $\langle 1_R\rangle \leq (R, +)$ abgeschlossen gegenüber allen Verknüpfungen, also ein Unterring, die spitzen Klammern entsprechen also sowohl dem Usus, damit die erzeugte *Untergruppe* (diesmal in $(R, +)$) anzugeben, als auch mit der Konvention damit die erzeugte Unterstruktur, in unserem Fall also den von 1_R erzeugten *Unterring,* den sogenannten *Primring,* zu bezeichnen. Die Ordnung dieses Teilrings hat große Bedeutung, wir geben ihr deshalb einen eigenen Namen:

2.5.10 Definition (Charakteristik) Ist $(R, +, \cdot)$ ein Ring mit Einselement, dann heißt

$$\mathrm{Char}(R) := |\langle 1_R\rangle|$$

die *Charakteristik* von R. (Ist diese nicht endlich, dann spricht man oft, anstelle von Charakteristik ∞, von Charakteristik 0, denn die Charakteristik wird oft auch als die kleinste *positive* natürliche Zahl n definiert mit $n1 := 1+\ldots+1 = 0$.)
•

2.5.11 Beispiele

- $\mathrm{Char}(\mathbb{Z}) = \mathrm{Char}(\mathbb{Q}) = \mathrm{Char}(\mathbb{R}) = \mathrm{Char}(\mathbb{C}) = \infty$,
- $\mathrm{Char}(\mathbb{Z}_n) = n$.

◇

2.5.12 Definition Ist $(R, +, \cdot)$ ein Ring, dann heißt R *Divisionsring* oder auch *Schiefkörper,* wenn $(R^*, \cdot)$ Gruppe ist, im abelschen Fall heißt R dann *Körper.*
•

2.5.13 Beispiel

- $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ sind Körper
- Ist R ein kommutativer Ring mit Einselement, I ein Ideal in R, dann ist R/I genau dann Körper, wenn I *maximal* ist in R, d.h. $I \neq R$ und für jedes Ideal J in R mit $I \subset J$ gilt $J = R$. Um das zu beweisen, rechnet man zuerst nach, daß für jedes $x \in R - I$ das von $I \cup \{x\}$ erzeugte Ideal J gerade die folgende Menge ist:

  $$J = \{i + rx \mid i \in I, r \in R\}.$$

  Wegen der Maximalität von I gilt also $J = R$, d. h.

  $$\forall x \in R - I \quad \exists r \in R \colon rx \in 1 + I.$$

  $((R/I)^*, \cdot)$ ist demzufolge abelsche Gruppe.

◇

Kapitel 3

Lineare Algebra

Wir kommen jetzt — nach der Bereitstellung der notwendigen algebraischen Strukturen — zur Linearen Algebra, in deren Mittelpunkt die linearen Gleichungssysteme und deren Auflösung stehen.

3.1 Moduln und Vektorräume

Im Zentrum der Untersuchungen in der Linearen Algebra stehen die Vektorräume, das sind abelsche Gruppen mit *Körpern* als Operatorenbereichen. In vielen Überlegungen und Anwendungen stehen aber auch abelsche Gruppen mit *Ringen* als Operatorenbereichen im Mittelpunkt, wir beginnen deshalb mit dieser etwas allgemeineren Definition. Hier müssen wir allerdings — wegen des Verzichts auf Kommutativität des Operatorenbereichs — genau unterscheiden, ob der Ring von rechts oder von links operiert:

3.1.1 Definition (Moduln) M sei eine abelsche Gruppe, R ein Ring. Dann heißt M *R-Linksmodul,* wenn R Linksoperatorenbereich ist:

$$r(m+m') = rm + rm',$$

und noch zusätzlich folgendes gilt;

$$(r+r')m = rm + r'm,\ r(r'm) = (rr')m, \text{ sowie } 1_R m = m, \text{ falls } 1_R \in R.$$

Hierfür schreiben wir kurz

$$_R M.$$

Entsprechend sind *$R-$Rechtsmoduln* M_R definiert. Ist M $R-$Linksmodul und $R'-$Rechtsmodul, dann nennt man M einen *$(R,R')-$Bimodul,* wenn gilt:

$$(rm)r' = r(mr').$$

Wir schreiben dann

$$_R M_{R'}.$$

•

3.1.2 Beispiele

- Jede abelsche Gruppe ist auf natürliche Weise $\mathbb{Z}-$Links-, $\mathbb{Z}-$Rechts- und $(\mathbb{Z},\mathbb{Z})-$Bimodul vermöge

$$z \cdot a := a \cdot z := \begin{cases} a + \ldots + a \ \ (z\text{-mal}), & \text{falls } z \geq 0 \\ -a - \ldots - a \ (|z|\text{-mal}), & \text{falls } z < 0. \end{cases}$$

- Jeder Ring R ist (R,R)-Bimodul.
- $\mathbb{R}^n$ ist $\mathbb{R}-$Linksmodul vermöge

$$r \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} := \begin{pmatrix} rx_0 \\ \vdots \\ rx_{n-1} \end{pmatrix}.$$

  $\mathbb{R}^n$ ist natürlich auch $\mathbb{R}$-Rechtsmodul vermöge

$$\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \cdot r := \begin{pmatrix} x_0 r \\ \vdots \\ x_{n-1} r \end{pmatrix}.$$

Das ergibt, wegen der *Assoziativität* der Multiplikation in $\mathbb{R}$ eine $(\mathbb{R},\mathbb{R})$-Bimodulstruktur auf $\mathbb{R}^n$. Wegen der *Kommutativität* der Multiplikation in $\mathbb{R}$ braucht man hier jedoch Links- und Rechts- und Bimoduln nicht zu unterscheiden, man kann einfach von einem $\mathbb{R}$-Modul sprechen.

Das gilt natürlich ganz allgemein für jeden *Körper* $\mathbb{K}$ und die abelsche Gruppe $\mathbb{K}^n$ und noch allgemeiner für beliebige $\mathbb{K}$-Moduln M, wenn $\kappa \cdot m = m \cdot \kappa$ gesetzt wird. Man kann also auch hier auf die Unterscheidung von Rechts- und Linksmoduln verzichten, spricht von $\mathbb{K}$-Moduln oder $\mathbb{K}$-*Vektorräumen,* ihre Elemente heißen *Vektoren.*

$\diamond$

Es sei zunächst bemerkt, daß unmittelbar aus der Definition folgt

$$r0_M = 0_R m = 0_M, (-r)m = r(-m) = -(rm).$$

Auch hier stellen sich — wie bei den anderen bisher eingeführten algebraischen Grundstrukturen, den Gruppen und Ringen — die Standardfragen nach dem Aussehen von Unterstrukturen, Erzeugnissen und Homomorphismen.
Eine Teilmenge $\emptyset \neq U \subseteq {}_R M$ ist genau dann Untermodul eines R-Linksmoduls M, kurz: $U \leq {}_R M$, wenn sie Untergruppe von $(M,+)$ ist und abgeschlossen gegenüber Linksmultiplikation mit Elementen von R :

$$\forall\ u,u' \in U, r \in R\colon\ u - u', ru \in U.$$

Ist R ein Ring mit Einselement, dann kann man diese Forderung zu *einer* Inklusion vereinfachen:

$$\forall\ u,u' \in U, r,r' \in R\colon\ ru - r'u' \in U.$$

Klar ist ebenfalls, daß $f\colon {}_R M \to {}_R N$ genau dann *R-(Linksmodul-)Homomorphismus* heißt, wenn

$$f(m+m') = f(m) + f(m'),\ \text{und}\ f(rm) = rf(m)$$

gelten. Solche Abbildungen nennen wir kurz auch *R-lineare* Abbildungen, und wir schreiben dafür $f \in \mathrm{Hom}_R(M,N)$, wenn klar ist, daß M und N als R-Linksmoduln verstanden werden sollen. $f \in \mathrm{Hom}_R(M,N)$ impliziert natürlich

$$f(0_M) = 0_N, f(-m) = -f(m).$$

Entsprechendes gilt für Rechts- und für Bimoduln, und es ergeben sich bei Existenz eines Einselements Vereinfachungen: Offenbar ist $f{:}_R M \to {}_R N$ *in diesem Fall* genau dann $R-$lineare Abbildung, wenn gilt

$$f(rm + r'm') = rf(m) + r'f(m').$$

Kerne und Bilder von R-Homomorphismen sind Unterstrukturen, also Links-, Rechts- oder Bimoduln, und es gilt die Isomorphie

$$M/\mathrm{Kern}(f)\ \simeq_R\ \mathrm{Bild}(f).$$

(Durch den Index R an $\simeq$ soll betont werden, daß über die Homomorphie der abelschen Gruppen hinaus noch Vertauschbarkeit mit der Multiplikation mit Elementen von R, mit der sogenannten *Skalarmultiplikation,* vorliegt.) Hierbei ist die Bildung des *Faktormoduls* natürlich die folgende: Ist $U \leq {}_RM$ ein Untermodul, dann wird die Faktorgruppe

$$M/U = \{m + U \mid m \in M\}$$

Zu einem R-Linksmodul vermöge $r(m+U) := rm+U$. Wir bezeichnen ihn kurz mit ${}_R(M/U)$.

3.1.3 Beispiel Erinnern wir erneut an unser Standardproblem, das lineare Gleichungssystem mit der *Koeffizientenmatrix*

$$A = \begin{pmatrix} a_{00} & \dots & a_{0,n-1} \\ \dots & \dots & \dots \\ a_{m-1,0} & \dots & a_{m-1,n-1} \end{pmatrix} =: (a_{ik}) \in \mathbb{R}^{m\times n}.$$

(Ganz allgemein heißen solche Tafeln aus m Zeilen und n Spalten mit Elementen aus einem Ring R, die man ja auch als Abbildungen von $m \times n$ nach R auffassen kann, $m \times n$-*Matrizen* über R.) Die bereits erwähnte Abbildung

$$f\colon \mathbb{R}^n \to \mathbb{R}^m, \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} \sum_k a_{0k}x_k \\ \vdots \\ \sum_k a_{m-1,k}x_k \end{pmatrix}$$

ist eine $\mathbb{R}$*-lineare Abbildung zwischen den* Vektorräumen $\mathbb{R}^n$ *und* $\mathbb{R}^m$. (Moduln über Körpern heißen *Vektorräume.*) ◇

Wir müssen jetzt noch das Erzeugnis einer Teilmenge $T \subseteq {}_RM$ diskutieren, es heißt auch die $R-$*lineare Hülle* von T : ${}_R\langle T\rangle$ besteht aus den endlichen Summen der Form

$$m = \sum_{i=0}^{n-1} r_i t_i + \sum_{j=0}^{n'-1} z_j t'_j,$$

mit $n, n' \in \mathbb{N}, r_i \in R, z_i \in \mathbb{Z}, t_i, t'_j \in T$. Enthält R ein Einselement, dann vereinfacht sich dies entsprechend zu

$${}_R\langle T\rangle = \left\{ \sum_{i=0}^{n-1} r_i t_i \;\middle|\; n \in \mathbb{N}, t_i \in T, r_i \in R \right\}.$$

Wir nehmen deshalb bis auf weiteres an, R enthalte ein Einselement!

3.1.4 Beispiele

- ${}_R\langle\emptyset\rangle = \{0_M\}$.
- ${}_R\left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} r \\ 0 \\ 0 \end{pmatrix} \;\middle|\; r \in \mathbb{R} \right\}$.

- $_R\left\langle e_0 := \begin{pmatrix}1\\0\\0\end{pmatrix}, e_1 := \begin{pmatrix}0\\1\\0\end{pmatrix}, e_2 := \begin{pmatrix}0\\0\\1\end{pmatrix}\right\rangle = \mathbb{R}^3$
- $_R\langle e_i \mid i \in n\rangle = \mathbb{R}^n$.

Den Vektor e_i nennt man den i-ten *Einheitsvektor.* ◇

Die Elemente $m \in M$ von der Form $\sum_{i=0}^{n-1} r_i t_i$, mit $n \in \mathbb{N}, r_i \in R, t_i \in T, i \in n$, heißen die *Linearkombinationen* aus Elementen von $T \subseteq {}_RM$. Das Erzeugnis von T besteht also (da wir ein Einselement voraussetzen!) genau aus den Linearkombinationen der Elemente von T. ${}_RM$ heißt *endlich erzeugt* oder *endlich erzeugbar,* wenn es eine endliche Teilmenge $T \subseteq M$ gibt mit ${}_R\langle T\rangle = {}_RM$. ${}_RM$ heißt *zyklisch,* wenn es $m \in M$ gibt mit ${}_RM = {}_R\langle m\rangle := {}_R\langle\{m\}\rangle$, d. h. wenn

$$_RM = \{rm \mid r \in R\} = Rm.$$

Beispielsweise ist $\mathbb{R}^n$ endlich erzeugbar, ${}_{\mathbb{R}}\mathbb{R}[x]$ jedoch nicht, denn im Erzeugnis ${}_{\mathbb{R}}\mathbb{R}[x]$ ist offensichtlich nicht zyklisch, aber ${}_{\mathbb{R}[x]}\mathbb{R}[x] = \mathbb{R}[x] \cdot 1$. Jeder Ring R mit Einselement ist zyklischer $R-$Linksmodul: ${}_RR = R \cdot 1$.
Wir kommen jetzt zur Definition der wichtigsten Begriffe aus der Linearen Algebra:

3.1.5 Definition (Lineare Unabhängigkeit, Basis) M sei ein R-Linksmodul über einem Ring mit Einselement.

i) Linearkombinationen der Form $0 = \sum_{i=0}^{n-1} r_i t_i$ heißen *lineare Beziehungen* zwischen den Elementen t von T (es gibt stets die *triviale* lineare Beziehung $0 = \sum_{t\in T} 0 \cdot t$).

ii) T heißt *linear unabhängig* oder *frei,* wenn es nur die triviale lineare Beziehung gibt. Andernfalls heißt T *linear abhängig.*

iii) Freie Erzeugendensysteme heißen *Basen.* Moduln mit Basen heißen *freie* Moduln.

•

Lineare Unabhängigkeit einer Teilmenge T bedeutet also, daß für irgendwelche *endlich vielen* $t_i \in T$ aus einer Gleichung $0_M = \sum_i r_i t_i \; r_i = 0_R$ folgt, für alle i. Und umgekehrt bedeutet lineare Abhängigkeit von T, daß es endlich viele $t_i \in T$ und $r_i \in R$ gibt, so daß $0_M = \sum_i r_i t_i$, aber nicht alle r_i sind gleich 0_R.

3.1.6 Beispiele

- Liegt 0_M in T, dann ist T linear abhängig, da wir ja $1_R \in R$ voraussetzen.
- $\mathbb{R}^n$ ist frei: $T := \{e_i \mid i \in n\}$ ist ein linear unabhängiges Erzeugendensystem. Analoges gilt für $\mathbb{K}^n$, $\mathbb{K}$ ein Körper.

- ${}_{\mathbb{R}}\mathbb{R}[x]$ ist frei, denn $\{1, x, x^2, \ldots\}$ ist ein linear unabhängiges Erzeugendensystem, da jedes Polynom Linearkombination aus *endlich vielen* Potenzen von x ist. Dieser Modul ist aber nicht endlich erzeugbar, denn im Erzeugnis von endlich vielen Polynomen kommen nur Polynome mit beschränktem Grad vor.

- Ist R ein kommutativer Ring mit $1, x \in R$ Nullteiler (d.h. es gibt $r \neq 0$ mit $rx = 0$) dann ist Rx ein Untermodul von ${}_RR$, der *nicht* frei ist. Zum Beweis verwenden wir die Hilfsüberlegung, daß $rM = \{0\}$, für einen freien Modul M, impliziert $r = 0 \vee M = \{0\}$. (Indirekter Beweis: $r \neq 0 \wedge M \neq \{0\}$ ergäbe, für jedes Element b aus einer Basis, den Widerspruch $rb = 0$.)

  Wir beweisen die Behauptung, Rx sei nicht frei, indirekt: $rRx = Rrx = 0$ impliziert — wenn wir annehmen, Rx sei frei — nach der Hilfsüberlegung und wegen $Rx \neq 0$ den Widerspruch $r = 0$.

- $\{e_i \mid 0 \leq i \leq n-1\} \subseteq \mathbb{K}^n, \mathbb{K}$ ein Körper, ist Basis.

- $\left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix} \right\} \subseteq \mathbb{R}^3$ ist linear abhängig: Setzen wir $r_0 := 1$, $r_1 := -2$, $r_2 := 1$, so erhalten wir eine nicht triviale lineare Beziehung.

◇

3.1.7 Definition $U_i \leq {}_RM$, dann heißt

$$\sum_{i \in I} U_i := {}_R\langle \bigcup_{i \in I} U_i \rangle$$

die *Summe* der Untermoduln U_i. •

Offensichtlich ist

3.1.8 $$\sum_{i \in I} U_i = \left\{ m \;\middle|\; \exists\, n \in \mathbb{N}\ \forall\, \nu \in n\ \exists\, u_{i_\nu} \in U_{i_\nu} \colon\ m = \sum_{\nu=1}^{n} u_{i_\nu} \right\}.$$

□

3.1.9 Folgerungen *Ist I eine endliche Indexmenge und $m_i \in {}_RM, i \in I$, dann sind äquivalent:*

i) ${}_RM = {}_R\langle m_i \mid i \in I \rangle$,

ii) $\forall\, m \in M\ \exists\, r_i \in R \colon\ m = \sum_{i \in I} r_i m_i$,

iii) ${}_RM = \sum_{i \in I} Rm_i$.

3.1.10 Definition Die Summe $\sum_{i\in I} U_i$ von Untermoduln $U_i \leq {}_RM$ heißt *direkt,* wenn für alle i gilt: $U_i \cap \sum_{j\neq i} U_j = \{0\}$. Wir schreiben dann für diese direkte Summe auch kurz:

$$\bigoplus_{i\in I} U_i.$$

•

3.1.11 Beispiele

- $\mathbb{R}^3 = \mathbb{R}\begin{pmatrix}1\\0\\0\end{pmatrix} \oplus \mathbb{R}\begin{pmatrix}0\\1\\0\end{pmatrix} \oplus \mathbb{R}\begin{pmatrix}0\\0\\1\end{pmatrix} = \mathbb{R}e_0 \oplus \mathbb{R}e_1 \oplus \mathbb{R}e_2.$
- $\mathbb{R}[x] = \mathbb{R}\cdot 1 \oplus \mathbb{R}\cdot x \oplus \mathbb{R}x^2 \oplus \ldots$

◇

3.1.12 Satz *${}_RM \geq U_i, i \in I$, dann sind äquivalent:*

i) $\sum_{i\in I} U_i = \bigoplus_{i\in I} U_i$,

ii) Die Null ist nur trivial kombinierbar *aus Elementen $u_i \in U_i$: Sind $u_i \in U_i, i \in I$, fast alle $u_i = 0$, dann gilt:*

$$\sum_{i\in I} u_i = 0 \Longrightarrow u_i = 0.$$

iii) Jedes $m \in \sum_{i\in I} U_i$ ist eindeutig darstellbar *in der Form*

$$m = \sum_{i\in I} u_i, u_i \in U_i, \ fast\ alle\ u_i = 0.$$

Beweis:
i) $\Longrightarrow$ *ii)* : Ist $\sum u_i = 0, i_o \in I$, dann gilt

$$-u_{i_o} = \sum_{j\neq i_o} u_j \in U_{i_o} \cap \sum_{j\neq i_o} U_j = \{0\},$$

also $u_{i_o} = 0$.
ii) $\Longrightarrow$ *iii)* : Indirekt. $m = \sum u_i = \sum u_i'$ ergibt $\sum(u_i - u_i') = 0$, also $u_i = u_i', i \in I$, wegen ii).
iii) $\Longrightarrow$ *i)* : $0 \neq m \in U_i \cap \sum_{j\neq i} U_j$ ergäbe zwei Darstellungen von m :

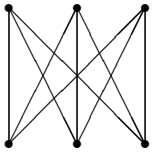
$$m = u_i = \sum_{j\neq i} u_j,$$

was $u_i = 0$ impliziert.

□

3.2 Unabhängigkeitsstrukturen

Unser Ziel ist der Nachweis, daß in Vektorräumen, also in Moduln über Körpern, Basen existieren und zwei endliche Basen gegebenenfalls von derselben Ordnung sind. (Basen sind sehr wichtig, weil jeder Vektor auf *eindeutige* Weise als Linearkombination der Elemente einer vorgegebenen Basis geschrieben werden kann. Beispielsweise besitzt auch L_H, die Lösungsgesamtheit eines homogenen Gleichungssystems, eine Basis, L_H besteht demnach *genau* aus den Linearkombinationen ihrer Elemente. L_H — eine Menge, die oft unendlich ist — kann deshalb mit Hilfe der *endlich vielen* Elemente einer solchen Basis vollständig beschrieben werden!)
Zum Beweis dieser Tatsache machen wir einen kurzen Ausflug in die sogenannte *Matroidtheorie,* das ist eine moderne kombinatorische Theorie, die sich als sehr anwendungsrelevant erwiesen hat und die aus der Fragestellung entstanden ist, weshalb diese Gleichheit der Basenordnungen gilt. Mit Hilfe dieser Theorie kann man beispielsweise zeigen, daß das bekannte Spiel, drei Punkte auf einem Blatt Papier jeweils mit drei weiteren Punkten kreuzungsfrei zu verbinden, nicht zum Ziel führen kann:



(In Worten der Graphentheorie: Mit Hilfe der Matroidtheorie kann man zeigen, daß der Graph $K_{3,3}$ *nicht planar* ist!)
Basen sind linear unabhängige Erzeugendensysteme, und man kann sie auch mit Hilfe nur einer dieser beiden Bedingungen definieren, linear unabhängig bzw. Erzeugendensystem zu sein: Basen sind *maximale linear unabhängige* Mengen, man kann sie aber auch als *minimale Erzeugendensysteme* charakterisieren.
Wir erinnern uns deshalb zunächst an den Begriff der Halbordnung. Eine Menge H zusammen mit einer Relation $\leq$ heißt *geordnet* bzw. das Paar $(H, \leq)$ heißt *Ordnung,* wenn $\leq$ reflexiv, antisymmetrisch und transitiv ist. Ein Beispiel hierfür ist in jedem R-Linksmodul M die Menge $\mathcal{U}$ der unabhängigen Teilmengen, zusammen mit der Inklusion:

$$(\mathcal{U}, \subseteq).$$

In einer Ordnung $(H, \leq)$ heißen diejenigen Elemente h *maximal,* für die $h' \geq h$ die Gleichheit $h = h'$ impliziert, und analog definiert man *minimal.* Ein Beispiel einer Ordnung ist $(\mathbb{N}\backslash\{0,1\}), |)$, also die Menge der natürlichen Zahlen > 1, mit der Teilbarkeit als Ordnung. Diese hat genau die Primzahlen als minimale Elemente, maximale Elemente gibt es nicht.
Es ist klar, daß Basen ggf. genau die maximalen Elemente von $(\mathcal{U}, \subseteq)$ sind. Dies erleichtert das Verständnis der folgenden Definition:

3.2.1 Definition (Matroide) Ist M eine Menge und $\mathcal{U} \neq \emptyset$ ein System von Teilmengen von M, dann heißt $\mathcal{U}$ eine *Unabhängigkeitsstruktur,* ein *Matroid* oder eine *Prägeometrie* auf M, wenn gilt:

i) $\mathcal{U}$ ist *erblich* oder *hereditär:* $S \subseteq T \in \mathcal{U} \Longrightarrow S \in \mathcal{U}$.

ii) Es gilt der (endliche) *Ergänzungssatz:*

$$S, T \in \mathcal{U},\ |S| = |T| + 1 \Longrightarrow \exists\ s \in S \backslash T :\ T \cup \{s\} \in \mathcal{U}.$$

•

Die Elemente $T \in \mathcal{U}$ heißen dann *unabhängige* Mengen, die $S \subseteq M$ mit $S \notin \mathcal{U}$ heißen *abhängige* Mengen.

3.2.2 Beispiele

i) Triviale Unabhängigkeitsstrukturen auf M sind $\{\emptyset\}$ und $P(M)$, die *universelle* Unabhängigkeitsstruktur von M.

ii) $M \subseteq {}_{\mathbb{K}}V, \mathbb{K}$ ein Körper, $\mathcal{U} := \{T \subseteq M \mid T \text{ linear unabhängig}\}$.

a) Die Erblichkeit ist trivial.

b) Der Ergänzungssatz wird indirekt bewiesen. Seien $S, T \in U, |S| = |T| + 1$, und $S = \{s_0, \ldots, s_m\}_{\neq}$ sowie $T = \{t_0, \ldots, t_{m-1}\}_{\neq}$.
Wir wollen also annehmen, es gebe kein $s \in S$ mit $T \cup \{s\}$ linear unabhängig bzw., äquivalent dazu: Für $0 \leq i \leq m$ gilt entweder $s_i \in \{t_0, \ldots, t_{m-1}\}$ oder $\{t_0, \ldots, t_{m-1}, s_i\}_{\neq}$ ist linear abhängig. Es gibt also nach dieser "indirekten Annahme" zwischen jedem $s_k \in S$ und den Elementen von T lineare Beziehungen der Form

$$s_k = \sum_{i=0}^{m-1} \kappa_{ik} t_i,\ 0 \leq k \leq m.$$

(Daß hierbei der Koeffizient von s_k gleich 1 gesetzt werden kann, verwendet die Annahme, daß der Koeffizientenbereich $\mathbb{K}$ ein Körper ist!) Mit diesen κ_{ik} bilden wir nun folgendes Gleichungssystem:

$$\begin{array}{rcl} \kappa_{00}x_0 \quad +\ldots+ \quad \kappa_{0,m}x_m & = & 0 \\ & \vdots & \\ \kappa_{m-1,0}x_0 \quad +\ldots+ \quad \kappa_{m-1,m}x_m & = & 0 \end{array} \tag{1}$$

Da $\mathbb{K}$ Körper ist, können wir dieses System durch Eliminieren lösen (z.B. können wir, falls $\kappa_{00} \neq 0$, die oberste Gleichung nach x_0 auflösen, das Ergebnis in die nächste Gleichung einsetzen, nach x_1 auflösen, die Ausdrücke für x_0 und x_1 in die dritte Gleichung einsetzen usw.). Vor allem aber gibt es, da es sich bei (1) um ein lineares Gleichungssystem mit *mehr Unbestimmten als Gleichungen* handelt, nicht triviale Lösungen

$$x = \begin{pmatrix} x_0 \\ \vdots \\ x_m \end{pmatrix}.$$

Für irgendeine dieser nicht trivialen Lösungen gilt aber

$$\sum_{k=0}^{m} x_k s_k = \sum_{k=0}^{m} x_k \sum_{i=0}^{m-1} \kappa_{ik} t_i = \sum_{i=0}^{m-1} (\underbrace{\sum_{k=0}^{m} \kappa_{ik} x_k}_{=0}) t_i = 0,$$

im Widerspruch zur linearen Unabhängigkeit von S.

iii) Ist $\mathcal{U}$ Unabhängigkeitsstruktur auf M, $T \subseteq M$, dann ist die *Einschränkung* von $\mathcal{U}$ auf T,

$$\mathcal{U} \downarrow T := \{S \in \mathcal{U} \mid S \subseteq T\},$$

offenbar eine Unabhängigkeitsstruktur auf T.

$\diamond$

3.2.3 Definition Ist $\mathcal{U}$ eine Unabhängigkeitsstruktur auf M, dann heißt jedes in der Ordnung $(\mathcal{U}, \subseteq)$ maximale $T \in \mathcal{U}$ (eine) *Basis.* •

3.2.4 Satz *Ist $\mathcal{U}$ eine Unabhängigkeitsstruktur auf M, dann gilt*

i) Keine echte Teilmenge einer Basis ist ebenfalls Basis.

ii) Gibt es endliche Basen, dann haben alle Basen dieselbe Ordnung.

iii) Gibt es endliche Basen, dann gilt der Austauschsatz: *Sind B, B' Basen, $T \subseteq B$, dann gibt es $T' \subseteq B'$, so daß $|T'| = |T|$ und $(B \backslash T) \cup T'$ eine Basis ist. D. h. jede Teilmenge T einer Basis B kann gegen eine Teilmenge T' von B' ausgetauscht werden, ohne daß die Basiseigenschaft verloren geht.*

Beweis:

i) ist trivial, ii) folgt aus dem Ergänzungssatz,

iii) folgt aus dem Ergänzungssatz mit vollständiger Induktion. □

3.2.5 Definition Gegebenenfalls heißt die endliche Ordnung $r(\mathcal{U})$ der Basen der *lineare Rang* der Unabhängigkeitsstruktur $\mathcal{U}$ bzw. deren *Dimension.* Andernfalls nennt man die Unabhängigkeitsstruktur *unendlichdimensional* und schreibt $r(\mathcal{U}) = \infty$. Der lineare Rang der Unabhängigkeitsstruktur aus allen linear unabhängigen Teilmengen eines Vektorraums V über einem Körper $\mathbb{K}$ heißt die $\mathbb{K}$-*Dimension* oder auch kurz die *Dimension* von V und wird mit

$$\dim_{\mathbb{K}}(V)$$

bezeichnet. •

3.2.6 Satz *Die Rangfunktion $r(-)$ hat auf Unabhängigkeitsstrukturen $\mathcal{U}$ auf M von endlichem Rang die folgenden Eigenschaften:*

i) $\forall\ S \subseteq T \subseteq M$:

$$0 \leq r(\mathcal{U} \downarrow S) \leq r(\mathcal{U} \downarrow T) \leq r(\mathcal{U}) \quad \textit{(Monotonie),}$$

ii) $\forall\ S, T \subseteq M$:

$$r(\mathcal{U} \downarrow S) + r(\mathcal{U} \downarrow T) \geq r(\mathcal{U} \downarrow S \cup T) + r(\mathcal{U} \downarrow S \cap T) \ \textit{(Submodularität).}$$

Beweis:

i) ist klar.

ii) Nach dem Ergänzungssatz kann man eine Basis B von $S \cap T$ ergänzen zu einer Basis $B \cup C$ von S und weiter zu einer Basis $B \cup C \cup D$ von $S \cup T$. Dabei gilt $C \subseteq S \backslash T$ und $D \subseteq T \backslash S$. Offensichtlich ist folgendes richtig:

$$r(\mathcal{U} \downarrow S \cap T) = |B|,$$

$$r(\mathcal{U} \downarrow S) = |B| + |C|,$$

$$r(\mathcal{U} \downarrow S \cup T) = |B| + |C| + |D|.$$

Wegen $B \cup D \in \mathcal{U}$ und $B \cup D \subseteq T$ gilt demnach

$$r(\mathcal{U} \downarrow T) \geq |B| + |D| = r(\mathcal{U} \downarrow S \cap T) + r(\mathcal{U} \downarrow S \cup T) - r(\mathcal{U} \downarrow S).$$

□

3.2.7 Beispiel Sei $M := \{1, 2, 3\}$.

$$\mathcal{U} := \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}\}$$

ist offenbar eine Unabhängigkeitsstruktur auf M, und es gilt, für $S := \{1\}$ und $T := \{3\}$:

$$2 = r(\mathcal{U} \downarrow S) + r(\mathcal{U} \downarrow T) > \underbrace{r(\mathcal{U} \downarrow S \cup T)}_{=1} + \underbrace{r(\mathcal{U} \downarrow S \cap T)}_{=0} = 1.$$

In 3.2.6 ii) kann " $\geq$ " also nicht durch " $=$ " ersetzt werden. ◇

In gewisser Weise dual zu den Basen, den maximalen unabhängigen Mengen, sind die *Kreise,* die minimalen abhängigen Mengen, also die $T \subseteq M$ mit

i) $T \notin \mathcal{U}$,

ii) $T \backslash \{t\} \in \mathcal{U}$, für alle $t \in T$.

Für Vektorräume ergibt sich jetzt:

3.2.8 Satz *Ist* ${}_{\mathbb{K}}V$ *im Vektorraum,* $B \subseteq V$*, dann sind die folgenden Bedingungen äquivalent:*

i) $V = \bigoplus_{b \in B} \mathbb{K}b$, *und alle* $b \neq 0_v$.

ii) B *ist linear unabhängiges Erzeugendensystem.*

iii) B *ist als Erzeugendensystem minimal.*

iv) B *ist als linear unabhängige Teilmenge maximal.*

Beweis:

i) $\Longrightarrow$ *ii)* :

a) Wäre B linear abhängig, dann gäbe es eine nicht triviale lineare Beziehung $0 = \sum_{b \in B} \kappa_b b$. Daraus folgte, wenn etwa $\kappa_{b_o} \neq 0$, da $\mathbb{K}$ Körper ist:

$$b_o = \sum_{b \neq b_o} -\kappa_{b_o}^{-1} \kappa_b b \in \mathbb{K}b_o \cap (\sum_{b \neq b_o} \mathbb{K}b)$$

im Widerspruch dazu, daß $\sum \mathbb{K}b$ als direkt vorausgesetzt ist.

b) Daß zudem noch B Erzeugendensystem sein muß , ist trivial.

ii) $\Longrightarrow$ *iii)* : Wäre B als Erzeugendensystem nicht minimal, könnte man ein Element $b_o \in B$ weglassen, dieses wäre dann aber $\neq 0$ und Linearkombination aus Elementen von $B \backslash \{b_o\}$, B also nicht linear unabhängig.

iii) $\Longrightarrow$ *iv)* : Minimale Erzeugendensysteme B sind linear unabhängig, das ist klar, man könnte ja sonst Elemente weglassen. Wären sie als linear unabhängige Teilmengen nicht maximal, dann könnte man ein von B unabhängiges $v \in V \backslash B$ hinzufügen, B wäre dann aber kein Erzeugendensystem.

iv) $\Longrightarrow$ *i)* : Ist B als linear unabhängige Menge maximal, dann gilt wegen der Maximalität, daß $V = \sum_{b \in B} \mathbb{K}b$, und wegen der linearen Unabhängigkeit von B ist diese Summe direkt. □

3.2.9 Folgerungen

i) Die Basen eines $\mathbb{K}-$ *Vektorraumes* V *(gemäß 3.1.5) sind genau die Basen der Unabhängigkeitsstruktur*

$$\mathcal{U} := \{T \subseteq V \mid T \text{ linear unabhängig}\}.$$

ii) Ist V *endlich erzeugbar, dann haben alle Basen von* V *dieselbe (endliche) Ordnung*

$$dim_{\mathbb{K}}(V) := r(\mathcal{U}),$$

die wir als $\mathbb{K}$-Dimension *von* V *bezeichnet haben.*

iii) In solchen endlichdimensionalen Vektorräumen gilt der (endliche) Basisergänzungssatz: *Ist* $T \subseteq V$ *linear unabhängig, dann kann man* T *zu einer Basis von* V *ergänzen.*

3.2.10 Satz *Jeder Vektorraum besitzt Basen.*

Beweis: Wir unterscheiden zwei Fälle:

i) Ist E ein endliches Erzeugendensystem, dann gibt es in E eine Teilmenge T, die als Erzeugendensystem minimal ist, T ist nach 3.2.8 Basis.

ii) Falls dagegen V nicht endlich erzeugbar ist, dann gibt es Ketten

$$T \subset T' \subset T'' \subset \ldots$$

linear unabhängiger Teilmengen $T^{(i)}$, die nicht abbrechen, da sonst V endlich erzeugbar wäre. Die Vereinigung

$$S := \bigcup_{i \in \mathbb{N}} T^{(i)}$$

aller Kettenglieder ist offensichtlich linear unabhängig. Also besitzt jede Kette in $\mathcal{U} := \{T \subseteq V \mid T \text{ l.u. }\}$ eine obere Grenze in $\mathcal{U}$. Die Menge der unabhängigen Teilmengen ist, wie man sagt, *strikt induktiv geordnet.* Nach dem *Lemma von Zorn,* das man aus dem Auswahlaxiom herleiten kann (vgl. Scheja/Storch: Lehrbuch der Algebra I, zweite Auflage), besitzen strikt induktiv geordnete Mengen maximale Elemente. □

Ist $B \subseteq V$ eine Basis von V, dann schreiben wir

$$V = {}_{\mathbb{K}} \ll B \gg .$$

Aus dem Beweis ergibt sich noch (wenn man anstelle *aller* unabhängigen Mengen in V nur die betrachtet, die eine vorgegebene unabhängige Teilmenge $T \subseteq V$ umfassen):

3.2.11 Folgerungen

i) Es gilt der (allgemeine) Basisergänzungssatz: Jede unabhängige Teilmenge $T \subseteq V$ läßt sich zu einer Basis von V ergänzen.

ii) Ist $W \leq {}_{\mathbb{K}}V$, dann gibt es $W' \leq {}_{\mathbb{K}}V$ mit $V = W \oplus W'$, d.h. jeder Unterraum W eines Vektorraums besitzt Komplemente.

□

Wegen 3.2.11 gilt

3.2.12 Satz *Sind $W, W' \leq {}_{\mathbb{K}}V$ und ist $dim_{\mathbb{K}}(V) \in \mathbb{N}$, dann gilt*

i) $dim_{\mathbb{K}}(W) < dim_{\mathbb{K}}(V) \Longleftrightarrow W \subset V$.

ii) $dim_{\mathbb{K}}(V/W) = dim_{\mathbb{K}}(V) - dim_{\mathbb{K}}(W)$.

iii) $dim_{\mathbb{K}}(W + W') + dim_{\mathbb{K}}(W \cap W') = dim_{\mathbb{K}}(W) + dim_{\mathbb{K}}(W')$.

Beweis:

i) Ist B_W eine Basis von W, dann läßt sich B_W zu Basis B von V ergänzen: $B = B_W \bigcup (B \backslash B_W)$, daraus folgt i).

ii) Nach 3.2.11 gibt es W' mit $V = W \oplus W'$. Dementsprechend sei $B = B_W \bigcup B_{W'}$ eine Basis von V und $f: W' \to V/W, w' \mapsto w' + W$. Man zeigt leicht, daß f ein $\mathbb{K}-$Isomorphismus ist.

iii) Wir erweitern eine Basis von $W \cap W'$ zu einer Basis von W und einer von W' :

$$B_W = B_{W\cap W'} \bigcup (B_W \backslash B_{W\cap W'}),\ B_{W'} = B_{W\cap W'} \bigcup (B_{W'} \backslash B_{W\cap W'}).$$

Diese Mengen erzeugen jedenfalls $W + W'$:

$$W + W' = {}_{\mathbb{K}}\left\langle \underbrace{B_{W\cap W'} \bigcup (B_W \backslash B_{W\cap W'})}_{=:B_1} \bigcup \underbrace{(B_{W'} \backslash B_{W\cap W'})}_{=:B_2} \right\rangle$$

B_1 und B_2 sind sogar disjunkt, und ihre Vereinigung ist linear unabhängig, denn eine lineare Relation

$$0 = \sum_{b_1 \in B_1} \kappa_{b_1} b_1 + \sum_{b_2 \in B_2} \kappa_{b_2} b_2$$

ergibt

$$\sum \kappa_{b_1} b_1 = -\sum \kappa_{b_2} b_2 \in W \cap W',$$

also $\kappa_{b_1} = 0$, falls $b_1 \notin B_{W\cap W'}$ und alle $\kappa_{b_2} = 0$. Da $B_{W\cap W'}$ aber Basis ist, folgt daraus sogar, daß *alle* $\kappa_{b_1} = 0$ sind. Die angesetzte lineare Beziehung muß also trivial sein, die beiden Mengen sind demnach disjunkt und ihre Vereinigung ist eine linear unabhängige Menge.

□

3.2.13 Beispiele

i) $\dim_{\mathbb{K}}(\{0_V\}) = \dim_{\mathbb{K}}(\langle\emptyset\rangle) = 0.$

ii) $\dim_{\mathbb{K}}(\mathbb{K}^n) = n.$

iii) $\dim_{\mathbb{K}}(\mathbb{K}^{m\times n}) = m \cdot n.$

iv) $\dim_{\mathbb{K}}(\mathbb{K}[x]) = \infty.$

v) $dim_{\mathbb{C}}(\mathbb{C}) = 1,\ aber\ dim_{\mathbb{R}}(\mathbb{C}) = 2.$

◇

3.3 Lineare Abbildungen und Matrizen

Wir wollen jetzt die *numerische Behandlung* linearer Abbildungen zwischen Vektorräumen beschreiben, bei der vorgegebene Basen die Hauptrolle spielen. Dazu sei daran erinnert, daß $f\colon {}_{\mathbb{K}}V \to {}_{\mathbb{K}}V'$ genau dann linear, also ein $\mathbb{K}$-Homomorphismus ist, kurz: $f \in Hom_{\mathbb{K}}(V, V')$, wenn $f(u+v) = f(u)+f(v)$ und $f(\kappa v) = \kappa f(v)$ gelten, für alle $u, v \in V$ und alle $\kappa \in \mathbb{K}$. Es ist bereits erwähnt worden, daß man diese beiden Bedingungen auch durch die einzige Bedingung

$$f(\kappa u + \lambda v) = \kappa f(u) + \lambda f(v)$$

ersetzen kann. Lineare Abbildungen sind also Abbildungen zwischen Vektorräumen mit demselben Grundkörper $\mathbb{K}$, wir können deshalb den Index $\mathbb{K}$ meistens weglassen.
Diese Definition der Linearität kann man auch mit Hilfe des Begriffs der linearen Beziehung formulieren, was den Durchblick verbessert: f ist genau dann linear, wenn

$$f(\sum_i \kappa_i v_i) = \sum_i \kappa_i f(v_i)$$

gilt, so daß aus $\sum_i \kappa_i v_i = 0$, wegen $f(0) = 0$, folgt $\sum_i \kappa_i f(v_i) = 0$. Lineare Abbildungen erhalten also lineare Beziehungen, genauer: eine lineare Beziehung zwischen Urbildern v_i überträgt sich auf deren Bilder $f(v_i)$:

$$\sum_i \kappa_i v_i = 0 \implies \sum_i \kappa_i f(v_i) = 0.$$

Es gilt auch die Umkehrung: Werden lineare Beziehungen erhalten, dann ist die Abbildung linear, denn aus $0 = w - u - v$ folgt dann $0 = f(w) - f(u) - f(v)$ und damit $f(u) + f(v) = f(w) = f(u + v)$. Analog ergibt sich $f(\kappa u) = \kappa f(u)$, denn $0 = w - \kappa u$ impliziert $0 = f(w) - \kappa f(u)$, so daß $\kappa f(u) = f(w) = f(\kappa u)$ folgt.
Wir fassen dies mit weiteren sehr wichtigen Eigenschaften solcher linearen Abbildungen zusammen in

3.3.1 Satz *Für $\mathbb{K}$-Vektorräume V, V' und eine Teilmenge T von V gilt:*

i) Genau diejenigen $f\colon V \to V'$ sind linear, die lineare Beziehungen erhalten (d.h. $0 = \sum \kappa_i v_i$ impliziert $0 = \sum \kappa_i f(v_i)$).

ii) Bilder linear unabhängiger Teilmengen unter injektiven linearen Abbildungen sind linear unabhängig.

iii) Ist $V = {}_{\mathbb{K}}\langle T\rangle$, $\bar{f}\colon T \to V'$, dann kann $\bar{f}$ genau dann zu einer linearen Abbildung $f\colon V \to V'$ fortgesetzt werden, wenn $\bar{f}$ lineare Beziehungen erhält. Eine solche lineare Abbildung ist gegebenenfalls eindeutig bestimmt.

iv) Auf linear unabhängigen Teilmengen T definierte Abbildungen sind linear fortsetzbar, auf Basen B definierte sogar eindeutig.

v) Ist $f \in Hom_{\mathbb{K}}(V, V')$, *dann gilt* $f(_{\mathbb{K}}\langle T\rangle) = {}_{\mathbb{K}}\langle f(T)\rangle$.

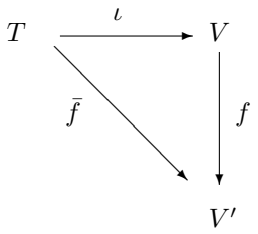
vi) Ist $T \subseteq {}_{\mathbb{K}}V$, *dann gilt:*

a) $f \in Epi_{\mathbb{K}}(V, V')$, $V = {}_{\mathbb{K}}\langle T\rangle \implies V' = {}_{\mathbb{K}}\langle f(T)\rangle$,

b) $f \in Mono_{\mathbb{K}}(V, V')$, $V = {}_{\mathbb{K}} \ll B \gg \implies f(V) = {}_{\mathbb{K}} \ll f(B) \gg$,

c) $f \in Iso_{\mathbb{K}}(V, V')$, $V = {}_{\mathbb{K}} \ll B \gg \implies V' = {}_{\mathbb{K}} \ll f(B) \gg$.

Beweis: i) wurde bereits bewiesen, ii) ist leicht nachzuprüfen. Zum Beweis von iii) betrachten wir das Diagramm



wobei $\iota: T \to V, t \mapsto t$ ist, die *Einbettung* von T in V. Wegen der Injektivität von ι gibt es — nach dem Abbildungssatz — eine Abbildung f, für welche dieses Diagramm kommutativ ist, die also $\bar{f}$ auf V fortsetzt. Darüberhinaus ist *jede* Fortsetzung von $\bar{f}$, d.h. jede Abbildung von V nach V' mit $f(t) = \bar{f}(t)$, eine kommutative Ergänzung des Diagramms, also auch die Abbildung

$$f: V \to V',\ \sum_t \kappa_t t \mapsto \sum_t \kappa_t \bar{f}(t),$$

wenn diese wohldefiniert ist, d.h. wenn sie lineare Beziehungen auf T erhält. Und dieses f ist ganz offensichtlich eine lineare Abbildung. Weil T ganz V erzeugt, ist sie sogar *eindeutig bestimmt.* Das beweist iii), iv) und v) und vi) folgen hieraus unmittelbar. □

Sind V und V' endlichdimensional und B, B' Basen, dann wird nach 3.3.1 jedes $f \in \mathrm{Hom}_{\mathbb{K}}(V, V')$ durch Angabe der Bilder $f(b), b \in B$, vollständig bestimmt. Zur systematischen numerischen Beschreibung von f ordnen wir deshalb B und B' zu *Basisfolgen* an:

$$\mathcal{B} = (b_0, \ldots, b_{n-1}), \mathcal{B}' = (b'_0, \ldots, b'_{m-1}).$$

f ist dann vollständig bestimmt durch die Koeffizienten a_{ik} aus den Gleichungen

3.3.2 $$f(b_k) = \sum_{i=0}^{m-1} a_{ik} b'_i.$$

Diese Koeffizienten a_{ik} (die von f, $\mathcal{B}$ und $\mathcal{B}'$ abhängen !) füllen die $m \times n-$Matrix

3.3.3 $$M(\mathcal{B}', f, \mathcal{B}) := (a_{ik}).$$

(Die dabei beachtete Konvention, *das Bild des $k-$ten Basisvektors in die $k-$te Spalte* zu schreiben (genauer: dessen Komponenten bzgl. $\mathcal{B}'$), heißt die *Spaltenkonvention.* Gelegentlich findet man auch Bücher, in denen die *Zeilenkonvention* benutzt wird.)

3.3.4 Beispiele Im folgenden bezeichnen wir mit $\mathcal{E}$ bzw. $\mathcal{E}_n$ stets die *Standardbasisfolge* $(e_0, \ldots, e_{n-1})$ von $\mathbb{K}^n$, wobei

$$e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Mit den Basisfolgen

$$\mathcal{B}_1 := (e_1, e_0), \mathcal{B}'_1 := (\begin{pmatrix} 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}), \mathcal{B}_2 := (\begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \end{pmatrix}), \mathcal{B}'_2 := (\begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \end{pmatrix})$$

von ${}_{\mathbb{R}}V := {}_{\mathbb{R}}\mathbb{R}^2 =: V'$ gilt dann für die lineare Abbildung

$$f\colon V \to V', \begin{pmatrix} \alpha \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ y \end{pmatrix}$$

folgendes:

$$M(\mathcal{E}, f, \mathcal{E}) = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, M(\mathcal{B}'_1, f, \mathcal{B}_1) = \begin{pmatrix} 1/3 & 0 \\ 0 & 0 \end{pmatrix},$$

$$M(\mathcal{B}'_2, f, \mathcal{B}_2) = \begin{pmatrix} -9/5 & -3 \\ 6/5 & 2 \end{pmatrix}.$$

◇

Die $m \times n$-Matrizen beschreiben also die linearen Abbildungen, aber es gilt noch mehr, denn auch die *Komposition zweier linearen Abbildungen* wird durch eine Matrix beschrieben, die das *Produkt der Matrizen der Kompositionsfaktoren* ist. Hierzu müssen wir aber erst einmal ein Produkt definieren. Zusammen mit der (kanonischen) Addition ergibt sich dabei sogar eine Ringstruktur auf den quadratischen Matrizen vorgegebener Zeilen und Spaltenzahl!

3.3.5 Definition Ist R ein Ring, $m, n \in \mathbb{N}^*$, dann heißen die Elemente von

$$R^{m\times n} = \{(a_{ik}) \mid a_{ik} \in R, i \in m, k \in n\}$$

die $m \times n-$*Matrizen* über R. Die *Elemente* oder *Einträge* a_{ik} von $A = (a_{ik}) \in R^{m\times n}$ werden wie folgt in Zeilen und Spalten angeordnet:

$$A = \begin{pmatrix} a_{00} & a_{12} & \ldots & a_{0,n-1} \\ a_{10} & a_{11} & \ldots & a_{1,n-1} \\ \ldots & \ldots & & \\ a_{m-1,0} & a_{m-1,1} & \ldots & a_{m-1,n-1} \end{pmatrix},$$

i ist also der *Zeilenindex,* k der *Spaltenindex.* •

3.3.6 Hilfssatz

i) $R^{m\times n}$ *ist* $R-$*Linksmodul mit der punktweisen Addition und Skalarmultiplikation:*

$$(a_{ik}) + (b_{ik}) := (a_{ik} + b_{ik}), r(a_{ik}) := (ra_{ik}).$$

ii) $R^{m\times m}$ *ist Ring mit der punktweisen Addition und folgender Multiplikation:*

$$(a_{ik})(b_{ik}) := (\sum_{j=0}^{m-1} a_{ij}b_{jk}).$$

Beweis: Nachrechnen. □

Diese Produktbildung läßt sich auf *nicht quadratische* Matrizen verallgemeinern, vorausgesetzt, *die Spaltenzahl des linken Faktors gleicht der Zeilenzahl des rechten Faktors:*

3.3.7 Hilfssatz *Für* $A \in R^{m\times n,}, B \in R^{n\times p}$ *definiert man als Produkt die Matrix*

$$AB := (\sum_{j=1}^{n} a_{ij}b_{jk}).$$

Die Produktbildung ist überall dort, wo sie definiert ist, assoziativ und distributiv:

$$A(BC) = (AB)C,\ A(B + C) = AB + AC,\ (A + B)C = AC + BC.$$

Beweis: Nachrechnen. □

Für $m > 1$ ist der Ring $R^{m\times m}$ i.a. nicht kommutativ, z.B. dann, wenn R ein Ring mit 1 ist:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Ist R ein Ring mit Eins, dann ist auch $R^{m\times m}$ ein Ring mit Einselement

$$E_m := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Diese Matrix heißt *Einheitsmatrix.* Eine Matrix $A \in R^{m\times m}$ heißt dann *invertierbar* oder *regulär,* wenn es $C \in R^{m\times m}$ gibt mit

$$AC = CA = E_m.$$

Die Matrix $D = (d_{ik}) \in R^{n\times m}$ mit $d_{ik} := a_{ki}$ heißt die zu $A \in R^{m\times n}$ *transponierte* Matrix und wird mit

$${}^tA$$

bezeichnet. Ist R kommutativ, dann gilt, für $A \in R^{m\times n}$, $B \in R^{n\times p}$:

$$^t(AB) = {}^tB\,{}^tA.$$

Sind $A, B \in R^{m\times m}$ invertierbar, dann gilt

$$(AB)^{-1} = B^{-1}A^{-1}.$$

3.3.8 Satz *Ist dim $V_{\mathbb{K}} = n$, dim $V'_{\mathbb{K}} = m$, so gilt, für Basisfolgen $\mathcal{B}$ von V, $\mathcal{B}'$ von V' :*

$$\varphi_{\mathcal{B},\mathcal{B}'}: Hom_{\mathbb{K}}(V,V') \simeq_{\mathbb{K}} \mathbb{K}^{m\times n}, f \mapsto M(\mathcal{B}', f, \mathcal{B}),$$

und die Abbildung

$$\varphi_{\mathcal{B},\mathcal{B}}: End_{\mathbb{K}}(V) \to \mathbb{K}^{n\times n}, f \mapsto M(\mathcal{B}, f, \mathcal{B})$$

ist ein Isomorphismus zwischen Ringen mit Eins.

Beweis:

i) Unmittelbar aus der Definition von $M(\mathcal{B}', f, \mathcal{B})$ und den Definitionen der Verknüpfungen in $\mathbb{K}^{m\times n}$ folgt, daß $\varphi_{\mathcal{B},\mathcal{B}'}$ Homomorphismus, linear und injektiv ist. Die Surjektivität ist ebenfalls offensichtlich: Jede $m\times n-$Matrix beschreibt eine lineare Abbildung.

ii) Die Homomorphie von $\varphi_{\mathcal{B},\mathcal{B}}$ bzgl. Addition folgt aus i). Für die Multiplikation haben wir zu zeigen, daß

$$M(\mathcal{B}, g\circ f, \mathcal{B}) = M(\mathcal{B}, g, \mathcal{B}) \cdot M(\mathcal{B}, f, \mathcal{B}).$$

Dies ergibt sich so:

$$\begin{aligned}(g\circ f)(b_k) &= g\sum_i a_{ik}b_i = \sum_i a_{ik}g(b_i)\\ &= \sum_{i,j} a_{ik}b_{ji}b_j = \sum_j(\sum_i b_{ji}a_{ik})b_j.\end{aligned}$$

Die Tatsache $\varphi_{\mathcal{B},\mathcal{B}}(id_V) = E_m$ ist trivial. □

Ganz analog folgt, für endlichdimensionale V, V', V'', lineare Abbildungen $f \in Hom_{\mathbb{K}}(V,V')$, $g \in Hom_{\mathbb{K}}(V',V'')$ und Basisfolgen $\mathcal{B}, \mathcal{B}'$ und $\mathcal{B}''$:

3.3.9 $$M(\mathcal{B}'', g, \mathcal{B}')M(\mathcal{B}', f, \mathcal{B}) = M(\mathcal{B}'', g\circ f, \mathcal{B}),$$

d.h. die Matrixmultiplikation ist gerade so eingerichtet, daß das Produkt der Matrizen die Komposition der entsprechenden linearen Abbildungen beschreibt!

Ist $V_{\mathbb{K}} = {}_{\mathbb{K}} \ll B \gg$ und $v = \sum_{b\in B} \kappa_b b$, dann heißen die κ_b die *Komponenten* von v bzgl. B.
Im endlichdimensionalen Fall (wenn $\mathcal{B} = (b_0, \ldots, b_{n-1})$ Basisfolge ist), ergibt sich der Isomorphismus

$$\varphi: V \simeq_{\mathbb{K}} \mathbb{K}^n, v \mapsto \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1}\end{pmatrix}, \; falls\; v = \sum_{i=0}^{n-1} v_i b_i.$$

3.3.10 Folgerung *Je zwei n-dimensionale $\mathbb{K}-$Vektorräume sind also zueinander isomorph, d.h. es gibt, zu vorgegebenem Körper $\mathbb{K}$ und vorgegebener natürlicher Zahl n, bis auf Isomorphie genau einen $\mathbb{K}$-Vektorraum mit dieser Dimension.*

Sehr wichtig ist noch, wie man mit Hilfe der $f \in Hom_{\mathbb{K}}(V, V')$ darstellenden Matrix $A = M(\mathcal{B}', f, \mathcal{B})$ die *Komponenten des Bildes* eines Vektors ermittelt. Ist $v = \sum_i v_i b_i$, dann gilt nämlich, wenn $f(v) = v' = \sum v'_i b'_i : \ v'_i = \sum_k a_{ik} v_k$, oder, in Matrixschreibweise:

3.3.11
$$\begin{pmatrix} v'_0 \\ \vdots \\ v'_{n-1} \end{pmatrix} = A \cdot \begin{pmatrix} v_0 \\ \vdots \\ v_{m-1} \end{pmatrix}.$$

Sehen wir uns noch an, wie sich die eine lineare Abbildung beschreibende Matrix bei einem *Basiswechsel* verhält: Sind $\mathcal{B}_1, \mathcal{B}_2$ bzw. $\mathcal{B}'_1, \mathcal{B}'_2$ Basisfolgen endlichdimensionaler Vektorräume, und sind $C = (c_{ik}), D = (d_{ik})$ die jeweiligen *Übergangsmatrizen,* d.h. es gilt

$$b^1_k = \sum_i c_{ik} b^2_i, \ b'^1_k = \sum_i d_{ik} b'^2_i,$$

dann folgt aus 3.3.9, wegen

$$C = (c_{ik}) = M(\mathcal{B}_2, \mathrm{id}, \mathcal{B}_1), \ D = (d_{ik}) = M(\mathcal{B}'_2, \mathrm{id}, \mathcal{B}'_1),$$

daß

$$M(\mathcal{B}'_2, f, \mathcal{B}_1) = M(\mathcal{B}'_2, f, \mathcal{B}_2) \cdot M(\mathcal{B}_2, \mathrm{id}, \mathcal{B}_1) = M(\mathcal{B}'_2, \mathrm{id}, \mathcal{B}'_1) \cdot M(\mathcal{B}'_1, f, \mathcal{B}_1),$$

insgesamt also die Gleichung

3.3.12
$$D \cdot M(\mathcal{B}'_1, f, \mathcal{B}_1) = M(\mathcal{B}'_2, f, \mathcal{B}_2) \cdot C.$$

Man sich das leicht auch so klarmachen:

$$\begin{array}{ccc} (V, \mathcal{B}_1) & \xrightarrow{\quad C \quad} & (V, \mathcal{B}_2) \\ \Big\downarrow {\scriptstyle M(\mathcal{B}'_1, f, \mathcal{B}_1)} & \circlearrowright & \Big\downarrow {\scriptstyle M(\mathcal{B}'_2, f, \mathcal{B}_2)} \\ (V', \mathcal{B}'_1) & \xrightarrow[\quad D \quad]{} & (V', \mathcal{B}'_2) \end{array}$$

Ein häufig vorkommender Spezialfall ist der eines Endomorphismus: $f \in \mathrm{End}_{\mathbb{K}}(V)$ und Basisfolgen $\mathcal{B}, \mathcal{B}'$: 3.3.9 liefert

3.3.13
$$M(\mathcal{B}', \mathrm{id}, \mathcal{B}) \cdot M(\mathcal{B}, f, \mathcal{B}) \cdot M(\mathcal{B}, \mathrm{id}, \mathcal{B}') = M(\mathcal{B}', f, \mathcal{B}'),$$

oder, explizit mit der Übergangsmatrix $C = (c_{ik})$, aus $b_k = \sum_i c_{ik} b'_i$, formuiert:

3.3.14 $$C \cdot M(\mathcal{B}, f, \mathcal{B}) \cdot C^{-1} = M(\mathcal{B}', f, \mathcal{B}').$$

Der Übergang von der Basisfolge $\mathcal{B}$ zur Basisfolge $\mathcal{B}'$ entspricht also der Konjugation der f beschreibenden Matrix mit der Übergangsmtrix C.

3.4 Der Gaußsche Algorithmus

Wir kommen jetzt zur expliziten numerischen Lösung des eingangs als eine Motivierung für die Lineare Algebra angegebenen linearen Gleichungssystems

3.4.1 $$\sum_{k=0}^{n-1} a_{ik}x_k = b_i, \quad 0 \leq i \leq m-1.$$

Wie bereits mehrfach erwähnt, ist zunächst herauszufinden, ob es überhaupt Lösungen gibt. Gegebenenfalls muß dann eine spezielle Lösung $x' \in L_I$ gesucht und eine Basis von L_H angegeben werden, denn $L_I = x + L_H$. All dies leistet der *Gaußsche Algorithmus,* der jetzt vorgeführt werden wird.
Wir gehen dazu von der *Matrixversion* des linearen Gleichungssystems aus:

3.4.2 $$A \cdot x = b, A \in \mathbb{K}^{m\times n}, b \in \mathbb{K}^m.$$

Außerdem benutzen wir, daß diese *Koeffizientenmatrix A* auch als lineare Abbildung f verstanden werden kann, so daß wir die Untersuchung auf Lösbarkeit des Gleichungssystems als Problem formulieren können festzustellen, ob die *rechte Seite b* in Bild(f) liegt. Diese Bedingung können wir mit Hilfe des folgenden Begriffs formulieren:

3.4.3 Definition (Spaltenrang einer Matrix) Die Dimension des Unterraumes U von $\mathbb{K}^m$, der von den Spalten einer Matrix $M \in \mathbb{K}^{m\times n}$ erzeugt wird, heißt der *Spaltenrang* von M. •

(Analog kann man den *Zeilenrang* definieren, und wir werden weiter unten zeigen, daß beide gleich sind!) Bedeutet jetzt

$$(A \mid b),$$

die um die rechte Seite des Gleichungssystem *erweiterte Matrix,* dann ergibt sich

3.4.4 Folgerung *Das lineare Gleichungssystem $Ax = b$ ist genau dann lösbar, wenn der Spaltenrang der* einfachen *Matrix A gleich dem Spaltenrang der erweiterten Matrix $(A \mid b)$ ist.*

Die Untersuchung des Gleichungssystems auf seine Lösbarkeit kann also mit Hilfe einer Rangbestimmung erfolgen. Um diese zu ermöglichen, bringen wir die erweiterte Matrix in eine übersichtliche Form, zu der ein Gleichungssystem *mit derselben Lösungsgesamtheit* gehört. Diese vereinfachte Form liefert uns den Rang, eine spezielle Lösung und schließlich sogar eine Basis von L_H. Diese Umformung heißt *Gaußscher Algorithmus* und wird jetzt beschrieben.

Zwecks Umformung können wir *invertierbare Matrizen C* auf beide Seiten der Gleichung $A \cdot x = b$ anwenden, denn das Gleichungssystem $CAx = Cb$ hat *dieselbe* Lösungsgesamtheit L_I. Wir listen deshalb zunächst diejenigen invertierbaren linearen Abbildungen und die ihnen entsprechenden Matrizen auf, die im Gaußschen Algorithmus Verwendung finden:

3.4.5 Hilfssatz *Ist E die Standardbasis von $\mathbb{K}^m$, dann sind die linearen Fortsetzungen f_i der folgenden Abbildungen $\bar{f}_i\colon E \to \mathbb{K}^m_{\mathbb{K}}$, $i = 1, 2, 3$, invertierbar:*

a) $\bar{f}_1$ vertauscht e_i mit e_j und läßt alle anderen e_k fest.

b) $\bar{f}_2$ multipliziert e_i mit $\kappa \neq 0$ von rechts und läßt alle anderen e_k fest.

c) $\bar{f}_3$ ersetzt e_i durch $e_i + e_j \cdot \kappa$ mit einem $j \neq i$ und läßt alle $e_k, k \neq i$, fest.

Die Matrizen $C_i := M(\mathcal{E}_m, f_i, \mathcal{E}_m)$ unterscheiden sich von der Einheitsmatrix E_m nur geringfügig:

α) C_1 geht aus E_m durch Vertauschen von $i-$ter Zeile und $j-$ter Spalte hervor.

β) C_2 unterscheidet sich von E_m nur durch den Eintrag κ (statt 1) in $i-$ter Zeile und $i-$ter Spalte.

γ) C_3 unterscheidet sich von E_m nur durch einen Eintrag k (statt 0) in $i-$ter Spalte, $j-$ter Zeile.

Diese Matrizen C_i können wir also von links an A sowie b multiplizieren ohne daß sich die Lösungsgesamtheit L_I ändert:

3.4.6 Folgerung *An der Koeffizientenmatrix A und der rechten Seite b des Gleichungssystems können wir folgende* Zeilenumformungen *anwenden, ohne die Lösungsgesamtheit zu verändern.:*

i) Vertauschen zweier Zeilen,

ii) Multiplizieren einer Zeile mit $\kappa \neq 0$,

iii) Addieren des $\kappa-$fachen der $j-$ten Zeile zur $i-$ten, wobei $i \neq j$.

□

Diese Art von Umformungen nennen wir *elementare Zeilemumformungen* und wenden sie in dem nun folgenden *Gauß–Algorithmus* zur Lösung linearer Gleichungssysteme an!

0. Schritt
(Aus bezeichnungstechnischen Gründen beschränken wir uns auf den "Spezialfall", bei dem die nullte Spalte der Ausgangsmatrix A nicht aus lauter Nullen besteht. Andernfalls läßt sich die Unbestimmte x_0 beliebig wählen.) Mit Hilfe von elementaren Zeilenumformungen bringt man das Ursprungsschema, die erweiterte Matrix,

$$(A \mid b) = \left(\begin{array}{ccc|c} a_{00} & \dots & a_{0,n-1} & b_0 \\ \vdots & & \vdots & \vdots \\ a_{m-1,0} & \dots & a_{m-1,n-1} & b_{m-1} \end{array}\right),$$

auf die Form

3.4.7
$$\left(\begin{array}{cccc|c} \boxed{1} & * & \dots & * & * & * \\ & & \boxed{1} & * \dots * & & * \\ & & & & \ddots & \vdots \\ & 0 & & & & * \end{array}\right)$$

Dabei hat man *spaltenweise* von *links* nach *rechts* vorzugehen! (Sterne im Schema 6.5.5 sollen nicht näher spezifizierte Elemente andeuten.) Ganz offensichtlich ist der Spaltenrang dieser (neuen) einfachen Matrix gleich der Anzahl dieser mit einer Eins beginnenden "Stufen". Und ebenso klar ist, daß die neue erweiterte Matrix genau dann denselben Spaltenrang wie die einfache hat, wenn die neue rechte Seite *unterhalb der letzten Stufe lauter Nullen enthält.* das ergibt folgendes wichtige Resultat:

3.4.8 Folgerung *Genau dann, wenn $A \cdot x = b$* lösbar *ist, geht, bei geeigneter Umformung, die erweiterte Matrix $(A \mid b)$ in eine Matrix der folgenden Form über:*

3.4.9
$$\left(\begin{array}{cccc|c} \boxed{1} & * & \dots & * & * & * \\ & & \boxed{1} & * \dots * & & \vdots \\ & & & & \ddots & \vdots \\ & & & & \boxed{1} * \dots * & * \\ & & & & & 0 \\ & & & & & \vdots \\ 0 & & & & & 0 \end{array}\right) \cdot$$

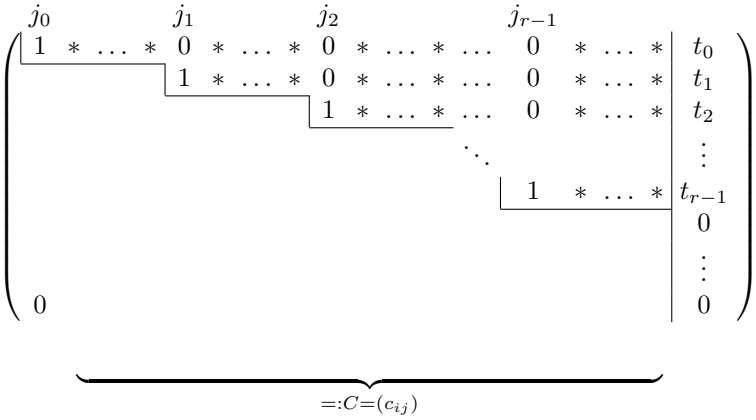
□

Nun sei das lineare Gleichungssystem als lösbar vorausgesetzt. Wir verabreden folgende Sprechweisen: Die Spalten im Schema 3.4.9, bei denen eine tiefer liegende "Treppenstufe"beginnt, nennen wir *Basisspalten,* die restlichen Spalten (ohne die letzte zusätzliche Spalte) heißen *Fehlspalten.* Basisspalten kennzeichnen wir durch Pfeile ↓, Fehlspalten durch Pfeile ↑:

$$\begin{array}{c} \textit{Basisspalten} \\ \downarrow \quad\quad \downarrow \quad\quad\quad \downarrow \\ \left(\begin{array}{cccc|c} \boxed{1} & * & \dots & * & * & * \\ & & \boxed{1} & * \dots * & & \vdots \\ & & & & \ddots & \vdots \\ & & & & \boxed{1} * \dots * & * \\ & & & & & 0 \\ & & & & & \vdots \\ 0 & & & & & 0 \end{array}\right) \\ \uparrow \dots \uparrow \quad \uparrow \dots \uparrow \quad\quad \uparrow \dots \uparrow \\ \textit{Fehlspalten} \end{array}$$

1. Schritt

Wieder nur mit elementaren Zeilenumformungen machen wir die in den Basisspalten von 3.4.9 oberhalb der 1 stehenden Elemente zu Null. Dabei fangen wir - im Gegensatz zum ersten Schritt - möglichst weit *rechts,* also mit der letzten Basisspalte an und arbeiten uns von rechts nach links spalten-, genauer: *basisspaltenweise* vor. Resultat ist ein Matrixschema der folgenden Form, bei dem wir in die erste Spalte zur Verdeutlichung die *Nummern* j_i der Basisspalten geschrieben haben:



Wir erhalten jetzt

i) eine spezielle Lösung des zugehörigen (und damit auch des urprünglichen) Systems, indem wir die Fehlvariablen (die Variablen x_i zu den Fehlspalten) sämtlich gleich 0 setzen und auflösen,

ii) und eine Basis von L_H ergibt sich, indem wir eine Fehlvariable gleich -1 und alle anderen Fehlvariablen gleich 0 setzen.

3.4.10 Satz *Ist die Spalte mit der Nummer p in der Matrix $C = (c_{ij})$ gleich*

$$\begin{pmatrix} c_{0p} \\ \vdots \\ c_{mp} \end{pmatrix}$$

und gleich der Fehl*spalte von C mit der Nummer k, so setze*

$$y^k := \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} p + \begin{pmatrix} c_{0p} \\ 0 \\ \vdots \\ 0 \\ c_{1p} \\ 0 \\ \vdots \\ 0 \\ c_{2p} \\ \vdots \\ \vdots \end{pmatrix} \begin{matrix} j_0 \\ \\ \\ \\ j_1 \\ \\ \\ \\ j_2 \\ \\ \end{matrix}, \quad x' := \begin{pmatrix} t_0 \\ 0 \\ \vdots \\ 0 \\ t_1 \\ 0 \\ \vdots \\ 0 \\ t_2 \\ \vdots \\ \vdots \end{pmatrix} \begin{matrix} j_0 - te\ Zeile \\ \\ \\ \\ j_1 - te\ Zeile \\ \\ \\ \\ j_2 - te\ Zeile \\ \\ \end{matrix}$$

Dann gilt:

1. *x' ist eine spezielle Lösung von $A \cdot x = b$.*
2. *Die $d = n - r$ Vektoren $y^0, \ldots, y^{d-1}$ bilden eine Basis des Vektorraumes $\{y \in \mathbb{R}^n \mid A \cdot y = 0\}$.*
3. *Die Lösungsgesamtheit von $A \cdot x = b$ ist (vgl. **??**):*

$$\{x' + \kappa_0 y^0 + \ldots + \kappa_{d-1} y^{d-1} \mid \kappa_i \in \mathbb{K}\}.$$

□

3.4.11 Beispiel Gegeben sei folgendes lineare Gleichungssystem über $\mathbb{R}$:

$$\begin{array}{rrrrrrrrr} -4x_1 & + 4x_2 & - 8x_3 & - 24x_4 & - 44x_5 & + 4x_6 & - 56x_7 & - 44x_8 & = -24 \\ 3x_1 & - 3x_2 & + 6x_3 & + 18x_4 & + 30x_5 & - 9x_6 & + 42x_7 & + 24x_8 & = 15 \\ 2x_1 & - 2x_2 & + 4x_3 & + 10x_4 & + 16x_5 & - 4x_6 & + 20x_7 & + 12x_8 & = 8\,. \\ -2x_1 & + 2x_2 & - 4x_3 & - 12x_4 & - 18x_5 & + 10x_6 & - 28x_7 & - 10x_8 & = -8 \\ 2x_1 & - 2x_2 & + 4x_3 & + 10x_4 & + 18x_5 & & + 20x_7 & + 18x_8 & = 10 \end{array}$$

Die dazugehörige erweiterte Matrix $(A \mid b)$ lautet:

$$\left(\begin{array}{rrrrrrrr|r} -4 & 4 & -8 & -24 & -44 & 4 & -56 & -44 & -24 \\ 3 & -3 & 6 & 18 & 30 & -9 & 42 & 24 & 15 \\ 2 & -2 & 4 & 10 & 16 & -4 & 20 & 12 & 8 \\ -2 & 2 & -4 & -12 & -18 & 10 & -28 & -10 & -8 \\ 2 & -2 & 4 & 10 & 18 & 0 & 20 & 18 & 10 \end{array}\right).$$

1. Wir bringen zunächst eine Eins an die Position $(0, 0)$, etwa durch die Division der nullten Zeile durch -4, kurz: $(Z_0 \| Z_0/(-4))$:

$$\left(\begin{array}{rrrrrrrr|r} \boxed{1} & -1 & 2 & 6 & 11 & -1 & 14 & 11 & 6 \\ 3 & -3 & 6 & 18 & 30 & -9 & 42 & 24 & 15 \\ 2 & -2 & 4 & 10 & 16 & -4 & 20 & 12 & 8 \\ -2 & 2 & -4 & -12 & -18 & 10 & -28 & -10 & -8 \\ 2 & -2 & 4 & 10 & 18 & 0 & 20 & 18 & 10 \end{array}\right).$$

2. Nun räumen wir die *unterhalb* von $\boxed{1}$ stehenden Elemente aus durch
$(Z_1 \| Z_1 - 3Z_0;\ Z_2 \| Z_2 - 2Z_0;\ Z_3 \| Z_3 + 2Z_0;\ Z_4 \| Z_4 - 2Z_0)$:

$$\left(\begin{array}{rrrrrrrr|r} 1 & -1 & 2 & 6 & 11 & -1 & 14 & 11 & 6 \\ 0 & 0 & 0 & 0 & -3 & -6 & 0 & -9 & -3 \\ 0 & 0 & 0 & -2 & -6 & -2 & -8 & -10 & -4 \\ 0 & 0 & 0 & 0 & 4 & 8 & 0 & 12 & 4 \\ 0 & 0 & 0 & -2 & -4 & 2 & -8 & -4 & -2 \end{array}\right).$$

3. Nachdem wir die nullte Spalte von A weitgehend ausgeräumt haben, suchen wir in dem neuen Zahlenschema die nächste Spalte, die *unterhalb* der nullten Zeile vom Nullvektor verschieden ist. (Hier ist das also die Spalte mit der Nummer 3.) Durch Zeilenvertauschungen bringen wir eine von 0 verschiedene Zahl an die oberste Position des Rechtecks (etwa durch die Vertauschung $(Z_1 \leftrightarrow Z_2)$):

$$\left(\begin{array}{rrrrrrrr|r} 1 & -1 & 2 & 6 & 11 & -1 & 14 & 11 & 6 \\ 0 & 0 & 0 & -2 & -6 & -2 & -8 & -10 & -4 \\ 0 & 0 & 0 & 0 & -3 & -6 & 0 & -9 & -3 \\ 0 & 0 & 0 & 0 & 4 & 8 & 0 & 12 & 4 \\ 0 & 0 & 0 & -2 & -4 & 2 & -8 & -4 & -2 \end{array}\right).$$

4. Durch Anwendung von $(Z_1 \| Z_1/(-2))$ erreichen wir, daß eine Eins an der Position $(1,3)$ steht. Um bequemer rechnen zu können, wenden wir noch

$(Z_2 \| Z_2/(-3);\ Z_3 \| Z_3/4;\ Z_4 \| Z_4/(-2))$

an und erhalten:

$$\left(\begin{array}{rrrrrrrr|r} 1 & -1 & 2 & 6 & 11 & -1 & 14 & 11 & 6 \\ 0 & 0 & 0 & \boxed{1} & 3 & 1 & 4 & 5 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 2 & -1 & 4 & 2 & 1 \end{array}\right).$$

5. Jetzt sind die unterhalb von $\boxed{1}$ stehenden Elemente zu 0 zu machen $(Z_4 \| Z_4 - Z_1)$:

$$\left(\begin{array}{rrrrrrrr|r} 1 & -1 & 2 & 6 & 11 & -1 & 14 & 11 & 6 \\ 0 & 0 & 0 & 1 & 3 & 1 & 4 & 5 & 2 \\ 0 & 0 & 0 & 0 & \boxed{1} & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & -1 & -2 & 0 & -3 & -1 \end{array}\right).$$

Nun ist diejenige Spalte zu suchen, die unterhalb der Zeile mit der Nummer 1 vom Nullvektor verschieden ist.

6. Da in unserem Beispiel bereits eine $\boxed{1}$ an der Position $(2,4)$ steht, müssen nur noch die Einträge unterhalb der Eins zu 0 gemacht werden ($Z_3 \| Z_3 - Z_2;\ Z_4 \| Z_4 + Z_2$):

$$\left(\begin{array}{cccccccc|c} 1 & -1 & 2 & 6 & 11 & -1 & 14 & 11 & 6 \\ 0 & 0 & 0 & 1 & 3 & 1 & 4 & 5 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \\ \mathrm{B} & \mathrm{F} & \mathrm{F} & \mathrm{B} & \mathrm{B} & \mathrm{F} & \mathrm{F} & \mathrm{F} & \end{array}\right)$$

(B= Basisspalte, F= Fehlspalte).

7. Damit ist der nullte Schritt durchgeführt, die Matrix besitzt Treppengestalt. Wir können folgende Eigenschaften direkt ablesen:

   - Das Gleichungssystem $Ax = b$ ist lösbar.
   - $\mathrm{Rang}(A) = 3$ (Anzahl der Basisspalten).
   - Der Vektorraum $\{y \in \mathbb{R}^8 \mid Ay = 0\}$ ist fünfdimensional (Anzahl der Fehlspalten).

8. Als nächstes sind die in den Basisspalten *oberhalb* der unteren 1 stehenden Elemente zu eliminieren. Dabei gehen wir von rechts nach links vor, beginnen also mit der Basisspalte mit der Nummer 2. Die Umformungen $(Z_1 \| Z_1 - 3Z_2;\ Z_0 \| Z_0 - 11Z_2)$ liefern:

$$\left(\begin{array}{cccccccc|c} 1 & -1 & 2 & 6 & 0 & -23 & 14 & -22 & -5 \\ 0 & 0 & 0 & 1 & 0 & -5 & 4 & -4 & -1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & \uparrow & & & & \end{array}\right).$$

9. Mit $(Z_0 \| Z_0 - 6Z_1)$ erreichen wir das entsprechende für die nächste Basisspalte:

$$\left(\begin{array}{cccccccc|c} 1 & -1 & 2 & 0 & 0 & 7 & -10 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & -5 & 4 & -4 & -1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & \uparrow & & & & & \end{array}\right).$$

Die nullte Basisspalte hat bereits die gewünschte Gestalt.

10. Erinnern wir uns, daß die Spalten von C den Komponenten $x_0, \ldots, x_7$ des Vektors x entsprechen. x_0, x_3, x_4 sind also Basisspaltenvariable, während x_1, x_2, x_5, x_6, x_7 Fehlspaltenvariable sind. Im Schema liest sich dies so:

$$x = \left(\begin{array}{|c|}\hline B \\ \hline F \\ \hline F \\ \hline B \\ \hline B \\ \hline F \\ \hline F \\ \hline F \\ \hline \end{array}\right).$$

Eine spezielle Lösung erhalten wir nun dadurch, daß wir die Einträge der rechten Spalte von oben nach unten auf die durch ein B gekennzeichneten Plätze verteilen und die F-Plätze mit 0 besetzen:

$$X_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Eine Basis $y^0, \ldots, y^4$ von $\{y \in \mathbb{R}^8 \mid Ay = 0\}$ erhalten wir so: Für die nullte Fehlspalte betrachten wir den nullten F-Platz im obigen Schema. Wir setzen an diese Stelle eine -1. Alle anderen F-Plätze werden mit 0 vorbesetzt. Nun verteilen wir die Einträge der nullten Fehlspalte von oben nach unten auf die B-Plätze und erhalten y^0. Entsprechend ergeben sich aus den anderen Fehlspalten die Vektoren $y^1, \ldots, y^4$.

$$y^0 = \begin{pmatrix} -1 \\ \boxed{\text{-1}} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad y^1 = \begin{pmatrix} 2 \\ 0 \\ \boxed{\text{-1}} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad y^2 = \begin{pmatrix} 7 \\ 0 \\ 0 \\ -5 \\ 2 \\ \boxed{\text{-1}} \\ 0 \\ 0 \end{pmatrix} \quad y^3 = \begin{pmatrix} -10 \\ 0 \\ 0 \\ 4 \\ 0 \\ 0 \\ \boxed{\text{-1}} \\ 0 \end{pmatrix} \quad y^4 = \begin{pmatrix} 2 \\ 0 \\ 0 \\ -4 \\ 3 \\ 0 \\ 0 \\ \boxed{\text{-1}} \end{pmatrix}$$

Wir bemerken vor allem, daß diese y^i linear unabhängig sind, das homogene System lösen und deshalb eine Basis von L_H besitzen, denn ihre Anzahl entspricht gerade der Dimension von L_H. Dieser Raum ist ja gerade der Kern der von A beschriebenen Abbildung, so daß gilt:

$$\dim(L_H) = \dim(\text{Kern}(f)) = n - \dim(\text{Bild}(f)) = n - \dim(\text{Spaltenraum von} A)$$

$$= n - \text{Anzahl der Basisspalten} = \text{Anzahl der Fehlspalten}.$$

Die *Lösungsgesamtheit* des linearen Gleichungssystems ist demnach:

$$\{x \in \mathbb{R}^8 \mid x = x' + \kappa_0 y^0 + \kappa_1 y^1 + \kappa_2 y^2 + \kappa_3 y^3 + \kappa_4 y^4 \text{ mit } \kappa_i \in \mathbb{R}\}.$$

$\diamond$

3.5 Duale Vektorräume und Abbildungen

Wir wollen im Folgenden auch geometrische Zusammenhänge mathematisch beschreiben und beginnen deshalb jetzt mit der Einführung hierfür geeigneter Begriffe.
Betrachten wir zunächst eine einzelne homogene lineare Gleichung

$$\sum_k a_{ik}x_k = 0$$

unter geometrischen Aspekten. Wenn nicht sämtliche Koeffizienten verschwinden, dann hat die (einzeilige) Koeffizientenmatrix den Rang 1, der Lösungsraum des einzeiligen homogenen Systems also die Dimension $n-1$, solche Unterräume heißen *Hyperebenen,* in Verallgemeinerung der Definition von Ebene als Raum der Dimension $2 = 3-1$, also als Hyperebene im Dreidimensionalen. Ein homogenes lineares Gleichungssystem hat also als Lösungsgesamtheit einen Schnitt von Hyperebenen. Wir werden bald zeigen können, daß auch umgekehrt zu vorgegebenen Hyperebenen leicht ein Gleichungssystem aufgestellt werden kann, das den Schnitt dieser Hyperebenen als Lösungsgesamtheit besitzt.
Wir verweisen deshalb zunächst auf die abbildungstheoretische Interpretation einer einzelnen linearen Gleichung: Zu ${}_{\mathbb{K}}V$ ergibt sich auf natürliche Weise der Vektorraum

$$L(V) := \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K})$$

der *Linearformen* λ auf V. Beispiele von Linearformen sind linke Seiten einzelner homogener linearer Gleichungen:

$$\lambda\colon \mathbb{K}^n \to \mathbb{K}, x \mapsto \sum_k a_{ik}x_k.$$

Eine Verallgemeinerung des Begriffs der Linearform ist der der *Bilinearform,* worunter man Abbildungen $\beta\colon V^* \times V \to \mathbb{K}$ versteht (für $\mathbb{K}$-Vektorräume V^*, V), die in beiden Komponenten linear sind, d.h. für alle $v^* \in V^*$ bzw. $v \in V$ ist $\beta(v^*, -)\colon v \mapsto \beta(v^*, v)$ bzw. $\beta(-, v)\colon v^* \mapsto \beta(v^*, v)$ Linearform. Die Menge *aller* solchen Bilinearformen sei mit

$$BLF(V^*, V)$$

bezeichnet.

3.5.1 Definition (Skalarprodukte) Sei $\beta \in BLF(V^*, V)$.

i) Als *Nullräume* von β bezeichnet man den Unterraum

$$N_{V^*}(\beta) := \{v^* \mid \forall\ v\colon\ \beta(v^*, v) = 0\}$$

von V^* und den analog definierten Unterraum $N_V(\beta)$ in V.

ii) β heißt *nicht ausgeartet,* wenn die Nullräume trivial sind: $N_{V^*}(\beta) = \{0_{V^*}\}$ und $N_V(\beta) = \{0_V\}$. Solche nicht ausgearteten Bilinearformen bezeichnen wir auch oft mit $\langle - \mid - \rangle$, schreiben also $\langle v^* \mid v \rangle$ statt $\beta(v^*, v)$.

iii) Ist $\langle - \mid - \rangle \in BLF(V^*, V)$ nicht ausgeartet, dann heißen V^* und V *dual* bzgl. $\langle - \mid - \rangle$. Die Bilinearform heißt dann *Skalarprodukt* und $\langle v^* \mid v \rangle$ das *skalare Produkt* von v^* und v.

•

3.5.2 Beispiele

i) $\langle - \mid - \rangle \colon \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}, (v^*, v) \mapsto \sum_{i=0}^{n-1} v_i^* v_i$ heißt das *Standardskalarprodukt* auf $\mathbb{K}^n$. $\mathbb{K}^n$ ist also diesbezüglich zu sich selbst dual.

ii) $\langle - \mid - \rangle \colon L(V) \times V \to \mathbb{K}, (\lambda, v) \mapsto \lambda(v)$ wird ebenfalls häufig herangezogen. Es zeigt, daß $L(V)$ dual ist zu V. Der Raum der Linearformen ist geradezu der *Prototyp* der zu V dualen Vektorräume!

iii) Sind $\mathcal{B}^*, \mathcal{B}$ Basisfolgen von $V^*, V, m = \dim_{\mathbb{K}}(V^*), n = \dim_{\mathbb{K}}(V)$, und $A \in \mathbb{K}^{m \times n}$, dann ist

$$\beta \colon V^* \times V \to \mathbb{K}, (v^*, v) \mapsto (v_0^*, \ldots, v_{m-1}^*) \cdot A \cdot \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} = {}^t v^* \cdot A \cdot v$$

eine Bilinearform. Für $A := E_m$, die Einheitsmatrix, ergibt sich so das Standardskalarprodukt. Umgekehrt gilt für $\beta \in BLF(V^*, V)$ mit $B := (\beta(b_i^*, b_k))$:

$$\beta(v^*, v) = (v_0^*, \ldots, v_{m-1}^*) \cdot B \cdot \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} = {}^t v^* B v.$$

iv) $\beta \in BLF(V^*, V)$ ergibt, für $U^* \leq_{\mathbb{K}} V^*, U \leq_{\mathbb{K}} V$, die Einschränkung

$$\beta \downarrow U^* \times U \in BLF(U^*, U).$$

Umgekehrt liefert $\beta' \in BLF(U^*, U)$, mit $f_1 \in \mathrm{Hom}_{\mathbb{K}}(V^*, U^*)$ und $f_2 \in \mathrm{Hom}_{\mathbb{K}}(V, U)$ die Bilinearform

$$\beta \colon V^* \times V \to \mathbb{K}, (v^*, v) \mapsto \beta'(f_1(v^*), f_2(v)).$$

v) Ist $\beta \in BLF(V^*, V)$, dann ergibt sich durch Ausfaktorisieren der Nullräume wie folgt eine nicht ausgeartete Bilinearform:

$$\bar{\beta} \colon (V^*/N_{V^*}(\beta)) \times (V/N_V(\beta)) \to \mathbb{K}, (v^* + N_{V^*}(\beta), v + N_V(\beta)) \mapsto \beta(v^*, v).$$

◇

3.5.3 Definition (orthogonal) Sei $\langle - \mid - \rangle \colon V^* \times V \to \mathbb{K}$ ein Skalarprodukt, $v^* \in V, v \in V$.

i) v^*, v heißen zueinander *orthogonal,* kurz: $v^* \perp v$, wenn gilt $\langle v^* \mid v\rangle = 0$.

ii) Als *orthogonales Komplement* von $U^* \leq_{\mathbb{K}} V^*$ bezeichnet man den Unterraum
$$U^{*\perp} := \{v \in V \mid \forall\ u^* \in U^*\colon\ \langle u^* \mid v\rangle = 0\}$$
von V. Analog ist das orthogonale Komplement $U^\perp$ von $U \leq_{\mathbb{K}} V$ definiert.

•

3.5.4 Beispiele Sei $\langle - \mid -\rangle \in BLF(V^*, V)$ ein Skalarprodukt. Es gilt:

i) $V^{*\perp} = \{0_V\}, V^\perp = \{0_{V^*}\}$, da $\langle - \mid -\rangle$ nicht ausgeartet ist.

ii) Offenbar gilt, für $U^* \leq_{\mathbb{K}} V^*$, $U^* \leq_{\mathbb{K}} U^{*\perp\perp}$.

iii) $U_i \leq_{\mathbb{K}} V \Rightarrow (U_1 + U_2)^\perp = U_1^\perp \cap U_2^\perp$.

◇

3.5.5 Definition (duale Abbildungen) Sind V^*, V und W^*, W Paare dualer $\mathbb{K}-$Vektorräume, dann heißen $f \in \mathrm{Hom}_{\mathbb{K}}(V, W)$ und $f^* \in \mathrm{Hom}_{\mathbb{K}}(W^*, V^*)$ zueinander *dual,* wenn gilt:
$$\langle f^*(w^*) \mid v\rangle = \langle w^* \mid f(v)\rangle.$$

•

3.5.6 Beispiele

i) $V^* := L(V)$ ist dual zu V. Ist außerdem W^* dual zu W bzgl. $\langle - \mid -\rangle$ sowie $f \in \mathrm{Hom}_{\mathbb{K}}(V, W)$, dann ist zu dieser Abbildung dual:
$$f^*\colon W^* \to L(V), w^* \mapsto \langle w^* \mid f(-)\rangle.$$

ii) Sind V^*, V zueinander dual und ist $U \leq_{\mathbb{K}} V$, dann sind $V^*/U^\perp$ und U zueinander dual bzgl. (vgl. 3.5.2 v))
$$\langle - \mid -\rangle'\colon (V^*/U^\perp) \times U \to \mathbb{K}, (v^* + U^\perp, u) \mapsto \langle v^* \mid u\rangle.$$
Dual zur Einbettung $\iota_U\colon U \to V, u \mapsto u$ ist die Abbildung
$$\nu_{U^\perp}\colon V^* \to V^*/U^\perp, v^* \mapsto v^* + U^\perp.$$

◇

3.5.7 Satz

i) Duale Abbildungen sind (gegebenenfalls) eindeutig bestimmt.

ii) Sind f^*, g^* dual zu $f, g \in Hom_{\mathbb{K}}(V, W)$, dann gilt
$$(f + g)^* = f^* + g^*, (\kappa \cdot f)^* = \kappa \cdot f^*.$$

iii) Sind f^*, g^* dual zu $f \in Hom_{\mathbb{K}}(U,V), g \in Hom_{\mathbb{K}}(V,W)$, dann ist

$$(g \circ f)^* = f^* \circ g^*.$$

iv) Sind f, f^* zueinander dual, dann gilt

$$\mathrm{Kern}(f^*) = \mathrm{Bild}(f)^\perp, \mathrm{Kern}(f) = \mathrm{Bild}(f^*)^\perp.$$

Beweis: i) gilt, da Skalarprodukte nicht ausgeartet sind, ii) und iii) sind leicht nachzurechnen. Zum Beweis von iv) bemerken wir:

$$w^* \in \mathrm{Kern}(f^*) \iff \forall\, v\colon\ 0 = \langle f^*(w^*) \mid v\rangle = \langle w^* \mid f(v)\rangle \iff w^* \in \mathrm{Bild}(f)^\perp.$$

Die zweite Identität $\mathrm{Kern}(f) = \mathrm{Bild}(f^*)^\perp$ ergibt sich ganz analog. □

3.5.8 Folgerungen *V^*, V und W^*, W seien Paare zueinander dualer $\mathbb{K}-$Vektorräume, und zu $f \in Hom_{\mathbb{K}}(V,W)$ sei $f^* \in Hom_{\mathbb{K}}(W^*, V^*)$ dual. Dann gilt:*

i) $W^*/\mathrm{Bild}(f)^\perp = W^*/\mathrm{Kern}(f^*)$ und $\mathrm{Bild}(f)$ sind dual bzgl.

$$\langle w^* + \mathrm{Bild}(f)^\perp \mid f(v)\rangle := \langle w^* \mid f(v)\rangle.$$

ii) $\mathrm{Bild}(f^*)$ und $V/\mathrm{Bild}(f^*)^\perp = V/\mathrm{Kern}(f)$ sind dual bzgl.

$$\langle f^*(w^*) \mid v + \mathrm{Kern}(f)\rangle := \langle f^*(w^*) \mid v\rangle.$$

Beweis: 3.5.6 ii).

□

Das Paradebeispiel für ein Paar dualer Vektorräume ist $L(V), V$ wir fassen zusammen, was wir darüber bereits wissen und zeigen noch einiges darüber hinaus:

3.5.9 Satz *Zu V ist $L(V)$ dual bzgl.*

$$\langle - \mid -\rangle\colon L(V) \times V \to \mathbb{K}, (\lambda, v) \mapsto \lambda(v).$$

Zu einer linearen Abbildung $f \in Hom_{\mathbb{K}}(V,W)$ dual ist

$$f^*\colon L(W) \to L(V), \mu \mapsto \mu \circ f.$$

Für die Kerne und Bilder dieser Abbildungen gilt:

$$\mathrm{Kern}(f) = \mathrm{Bild}(f^*)^\perp, \mathrm{Kern}(f^*) = \mathrm{Bild}(f)^\perp,$$

und analog

$$\mathrm{Bild}(f^*) = \mathrm{Kern}(f)^\perp, \mathrm{Bild}(f) = \mathrm{Kern}(f^*)^\perp.$$

Schließlich ist noch für orthogonale Komplemente folgendes richtig:

$$U^{\perp\perp} = U.$$

Beweis: Die Aussagen über die Dualität von V und $L(V)$ wie auch die Aussage über die Form der dualen Abbildung sind bereits bekannt. Wir wissen auch schon, daß

$$\mathrm{Kern}(f^*) = \mathrm{Bild}(f)^\perp,\ \mathrm{Kern}(f) = \mathrm{Bild}(f^*)^\perp.$$

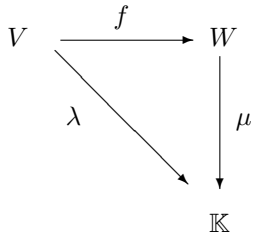
Es bleibt also noch zu zeigen, daß

$$\mathrm{Bild}(f^*) = \mathrm{Kern}(f)^\perp,\ \mathrm{Bild}(f) = \mathrm{Kern}(f^*)^\perp.$$

Zum Beweis der ersten Gleichung bemerken wir, daß

$$\lambda \in \mathrm{Kern}(f)^\perp \iff \mathrm{Kern}(f) \subseteq \mathrm{Kern}(\lambda).$$

Nach dem Abbildungssatz ist dies äquivalent zur Existenz einer kommutativen Ergänzung $\mu \in L(W)$ des folgenden Diagramms:



Hierfür gilt also $\lambda = \mu \circ f$ und damit ist $\lambda \in \mathrm{Kern}(f)^\perp$ äquivalent zu $\lambda \in \mathrm{Bild}(f^*)$, was zu zeigen war.
Vor dem Beweis von $\mathrm{Bild}(f) = \mathrm{Kern}(f^*)^\perp$ beweisen wir $U^{\perp\perp} = U$, für $U \leq_{\mathbb{K}} V$. Dazu betrachten wir die kanonische Projektion

$$\pi: V \to V/U, v \mapsto v + U.$$

Mit Hilfe des bereits Bewiesenen ergibt sich:

$$U = \mathrm{Kern}(\pi) = \mathrm{Bild}(\pi^*)^\perp = \mathrm{Kern}(\pi)^{\perp\perp} = U^{\perp\perp}.$$

Hiermit können wir jetzt den Beweis vervollständigen:

$$\mathrm{Kern}(f^*)^\perp = \mathrm{Bild}(f)^{\perp\perp} = \mathrm{Bild}(f).$$

□

Wir fragen nun nach Dimension und Basen von zueinander dualen Vektorräumen. Sind $\mathcal{B}, \mathcal{B}'$, endliche Basisfolgen für V und V', dann gilt offenbar

$$3.5.10 \mathrm{Hom}_{\mathbb{K}}(V, V') \simeq_{\mathbb{K}} \mathbb{K}^{m\times n} = {}_{\mathbb{K}}\left\langle\!\!\left\langle \begin{pmatrix} 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{pmatrix} \right\rangle\!\!\right\rangle,$$

denn $\mathbb{K}^{m\times n}$ hat (als $\mathbb{K}$-Vektorraum) diejenigen Matrizen als Basis, die — neben Nullen — nur eine Eins enthalten. Die von diesen Matrizen dargestellten Abbildungen bilden demnach eine Basis von $\mathrm{Hom}_{\mathbb{K}}(V,V')$:

3.5.11 $$\mathrm{Hom}_{\mathbb{K}}(V,V') = {}_{\mathbb{K}}\ll f_{ik}\colon b_j \mapsto \delta_{jk}b'_i \mid i\in m, j\in n \gg .$$

Dabei bezeichnet δ_{jk} das *Kroneckersymbol*

$$\delta_{jk} := \begin{cases} 1 & \text{falls } j=k \\ 0 & \text{sonst.} \end{cases}$$

Also folgt insbesondere

3.5.12 $$\dim_{\mathbb{K}}(\mathrm{Hom}_{\mathbb{K}}(V,V')) = \dim_{\mathbb{K}}(V)\cdot\dim_{\mathbb{K}}(V').$$

Für $V' := \mathbb{K}^1 = \mathbb{K}$ ergibt das die

3.5.13 Folgerung

i) $L(V) = {}_{\mathbb{K}}\ll \lambda_i\colon b_j \mapsto \delta_{ij}\cdot 1_{\mathbb{K}} \mid i\in m\gg$,

ii) $dim_{\mathbb{K}}(L(V)) = dim_{\mathbb{K}}(V)$.

Das legt die Vermutung nahe, daß endlichdimensionale zueinander duale Vektorräume V^*, V dieselbe Dimension haben und damit $V^* \simeq_{\mathbb{K}} L(V)$ gilt. Das ist tatsächlich richtig, weshalb $L(V)$ auch als *der* zu V duale Vektorraum bezeichnet werden kann. Genauer gilt:

3.5.14 Satz *Sind V^*, V dual bzgl. $\langle - \mid - \rangle$ und ist $dim_{\mathbb{K}}(V)\in\mathbb{N}$, dann gilt:*

i) $\varphi\colon V^* \simeq_{\mathbb{K}} L(V), v^* \mapsto \langle v^* \mid - \rangle$,

ii) $dim_{\mathbb{K}}(V^*) = dim_{\mathbb{K}}(V)$.

Beweis:

a) Offensichtlich ist $\varphi(v^*)\in L(V)$, und da $\langle - \mid - \rangle$ nicht ausgeartet ist, ist φ zudem injektiv.

b) Die Injektivität von φ ergibt $\dim_{\mathbb{K}}(V^*) \le \dim_{\mathbb{K}}(L(V)) =_{3.5.13} \dim_{\mathbb{K}}(V)$.

c) Betrachten von $\psi\colon V \to L(V^*), v\mapsto \langle - \mid v\rangle$ ergibt ganz analog $\dim_{\mathbb{K}}(V) \le \dim_{\mathbb{K}}(L(V^*)) =_{3.5.13} \dim_{\mathbb{K}}(V^*)$. Mit b) folgt also die Behauptung.

□

3.5.15 Definition (duale Basen) Sind V^*, V dual bzgl. $\langle - \mid - \rangle$, ist $\dim_{\mathbb{K}}(V)\in\mathbb{N}$ und sind $\mathcal{B}^*, \mathcal{B}$ Basisfolgen, dann heißen diese zueinander *dual,* wenn gilt

$$\langle b_i^* \mid b_k\rangle = \delta_{ik}\cdot 1_{\mathbb{K}} = \begin{cases} 1_{\mathbb{K}}, & \text{i=k,} \\ 0_{\mathbb{K}}, & \text{sonst.} \end{cases}$$

•

3.5.16 Beispiel
Die zur Basisfolge $\mathcal{B} = (b_0, \ldots, b_{m-1})$ von V oben bereits angegebene Basisfolge

$$\mathcal{L} := (\lambda_0, \ldots, \lambda_{m-1})$$

von $L(V)$ ist die zu $\mathcal{B}$ duale Basisfolge. $\diamond$

3.5.17 Satz *Ist V endlichdimensional, $\mathcal{B}$ Basisfolge, dann gibt es in jedem zu V dualen Vektorraum V^* eine zu $\mathcal{B}$ duale Basisfolge $\mathcal{B}^*$.*

Beweis: Ist $\mathcal{L}$ die zu $\mathcal{B}$ duale Basisfolge in $L(V)$, so ergibt die Abbildung $\varphi\colon V^* \simeq_{\mathbb{K}} L(V)$ vermöge

$$b_i^* \in \varphi^{-1}(\{\lambda_i\})$$

eine zu $\mathcal{B}$ duale Basisfolge $\mathcal{B}^* = (b_0^*, \ldots, b_{m-1}^*)$:

$$\langle b_i^* \mid b_k \rangle = \langle b_i^* \mid - \rangle(b_k) = \varphi(b_i^*)(b_k) = \lambda_i(b_k) = \delta_{ik}.$$

$\square$

3.5.18 Satz *Zueinander duale lineare Abbildungen zwischen endlichdimensionalen $\mathbb{K}-$Vektorräumen werden bzgl. dualer Basisfolgen durch zueinander transponierte Matrizen dargestellt.*

Beweis: V^*, V und W^*, W seien Paare endlichdimensionaler dualer $\mathbb{K}-$ Vektorräume mit zueinander dualen Basisfolgen $\mathcal{B}^*, \mathcal{B}$ und $\mathcal{C}^*, \mathcal{C}$. Weiter sei $f \in \mathrm{Hom}_{\mathbb{K}}(V, W)$ mit $A = (a_{ik}) := M(\mathcal{C}, f, \mathcal{B})$, und dazu dual $f^* \in \mathrm{Hom}_{\mathbb{K}}(W^*, V^*)$ mit $B = (b_{ik}) := M(\mathcal{B}^*, f^*, \mathcal{C}^*)$. Dann gilt:

$$\langle f^*(c_k^*) \mid b_j \rangle = \sum_i b_{ik} \langle b_i^* \mid b_j \rangle = b_{jk}.$$

Wegen der Dualität ergibt sich andererseits:

$$\langle f^*(c_k^*) \mid b_j \rangle = \langle c_k^* \mid f(b_j) \rangle = \sum_i \langle c_k^* \mid c_k \rangle a_{ij} = a_{kj},$$

also folgt insgesamt: $b_{jk} = a_{kj}$, wie behauptet. $\square$

3.5.19 Satz *Ist $U \leq V$, $dim_{\mathbb{K}}(V) \in \mathbb{N}$, dann gilt*

$$dim_{\mathbb{K}}(V) = dim_{\mathbb{K}}(U) + dim_{\mathbb{K}}(U^{\perp}).$$

Beweis: $L(V)$ und V sind zueinander dual, also auch $L(V)/U^{\perp}, U$, weshalb gilt

$$\dim_{\mathbb{K}}(U) = \dim_{\mathbb{K}}(L(V)) - \dim_{\mathbb{K}}(U^{\perp}) = \dim_{\mathbb{K}}(V) - \dim_{\mathbb{K}}(U^{\perp}).$$

$\square$

3.5.20 Satz *Sind V^*, V dual bzgl. $\langle - \mid - \rangle$, und ist $\beta \in BLF(V^*, V)$ sowie $dim_{\mathbb{K}}(V) \in \mathbb{N}$, dann gibt es genau ein $f_\beta \in End_{\mathbb{K}}(V)$ mit*

$$\beta(v^*, v) = \langle v^* \mid f_\beta(v) \rangle.$$

Beweis:

i) Die Existenz von f_β :

Sei $\psi: V \simeq L(V^*), v \mapsto \langle - \mid v \rangle$. Wegen $\beta(-, v) \in L(V^*)$ gibt es genau ein $v' \in V$ mit $\psi(v') = \beta(-, v)$, also ist

$$f_\beta: V \to V, v \mapsto v', \ mit \ \psi(v') = \beta(-, v),$$

wohldefiniert.

ii) f_β ist $\mathbb{K}-$ Endomorphismus:

$$f_\beta(\kappa_1 v_1 + \kappa_2 v_2) = (\kappa_1 v_1 + \kappa_2 v_2)' = \kappa_1 v_1' + \kappa_2 v_2',$$

letzteres wegen

$$\begin{aligned} \langle - \mid (\kappa_1 v_1 + \kappa_2 v_2)' \rangle &= \beta(-, \kappa_1 v_1 + \kappa_2 v_2) = \kappa_1 \beta(-, v_1) + \kappa_2 \beta(-, v_2) \\ &= \kappa_1 \langle - \mid v_1' \rangle + \kappa_2 \langle - \mid v_2' \rangle = \langle - \mid \kappa_1 v_1' + \kappa_2 v_2' \rangle, \end{aligned}$$

woraus sich $(\kappa_1 v_1 + \kappa_2 v_2)' = \kappa_1 v_1' + \kappa_2 v_2'$ ergibt, da $\langle - \mid - \rangle$ nicht ausgeartet ist.

iii) Die Eindeutigkeit:

$$\langle v^* \mid f_\beta(v) \rangle = \langle v^* \mid f(v) \rangle \Rightarrow \langle v^* \mid (f_\beta - f)(v) = 0 \rangle$$

ergibt $f_\beta = f$, da $\langle - \mid - \rangle$ nicht ausgeartet ist.

□

3.5.21 Folgerung $BLF(V^*, V) \simeq End_{\mathbb{K}}(V)$.

3.5.22 Anwendungen

i) Ist $f \in \mathrm{Hom}_{\mathbb{K}}(V, V')$, und sind V, V' endlichdimensional, dann heißt der Spaltenrang $Sr(A)$, für irgendeine Matrix A mit $M(\mathcal{B}', f, \mathcal{B})$, der *Rang* von f. Kurz: $Rg(f) := Sr(A)$. Wir wollen (nochmals) zeigen, daß der Spaltenrang dem Zeilenrang gleicht:

$$\begin{aligned} Rg(f) &= \dim_{\mathbb{K}}(\mathrm{Bild}(f)) \\ &= \dim_{\mathbb{K}}(V/\mathrm{Kern}(f)) \\ &= \dim_{\mathbb{K}}(V) - \dim_{\mathbb{K}}(\mathrm{Kern}(f)) \\ &= \dim_{\mathbb{K}}(V) - \dim_{\mathbb{K}}(\mathrm{Bild}(f^*)^\perp) \\ &= \dim_{\mathbb{K}}(V) - (\dim_{\mathbb{K}}(V^*) - \dim_{\mathbb{K}}(\mathrm{Bild}(f^*)) \\ &= \dim_{\mathbb{K}}(\mathrm{Bild}(f^*)) \\ &= Rg(f^*). \end{aligned}$$

Dies beweist, erneut, daß für Matrizen A gilt $Sr(A) = Zr(A)$, denn wir wissen ja, daß die duale Abbildung bzgl. der dualen Basis durch die Transponierte von A dargestellt wird.

ii) $Ax = b$ ist genau dann lösbar, wenn jede Lösung des *transponierten* homogenen Systems ${}^tA \cdot y = 0$ auf b senkrecht steht: $\sum y_i b_i = 0$.

$$Ax = b \text{ lösbar } \Leftrightarrow b \in \text{Kern}(f^*)^\perp.$$

iii) Ein numerisches Beispiel zu ii):

$$A := \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \\ 1 & 3 & 3 \end{pmatrix} \in \mathbb{R}^{3\times 3}, b := \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix} \in \mathbb{R}^3,$$

also

$${}^tA = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 3 \\ 1 & -1 & 3 \end{pmatrix}.$$

Dann ist

$$\mathbb{R}\left\langle\!\left\langle \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} \right\rangle\!\right\rangle = L_H({}^tA).$$

Wegen

$$\left\langle \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} \mid \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix} \right\rangle = -6 + 4 + 1 \neq 0$$

ist das System also nicht lösbar.

$\diamond$

3.6 Determinanten

Wir verallgemeinern jetzt den Begriff bilinear zu *multilinear*. Unser Ziel ist dabei insbesondere die Einführung der sogenannten Determinante.

3.6.1 Definition (alternierend, symmetrisch, schiefsymmetrisch) Seien V und V' $\mathbb{K}-$Vektorräume, $n \in \mathbb{N}^*$, $f\colon V^n \to V'$, dann heißt f

- *multilinear* $:\Longleftrightarrow\ f(v_0, \ldots, v_{i-1}, -, v_{i+1}, \ldots, v_{n-1}) \in \mathrm{Hom}_{\mathbb{K}}(V, V')$,
- *alternierend* $:\Longleftrightarrow\ [\ \exists\ i \neq k\colon\ v_i = v_k \Rightarrow f(v_0, \ldots, v_{n-1}) = 0\ ]$,
- *symmetrisch* $:\Longleftrightarrow\ \forall\ \pi \in S_n\colon\ f(v_0, \ldots, v_{n-1}) = f(v_{\pi(0)}, \ldots, v_{\pi(n-1)})$,
- *schiefsymmetrisch* $:\Longleftrightarrow\ f(v_0, \ldots, v_{n-1}) = \mathrm{sgn}(\pi) f(v_{\pi(0)}, \ldots, v_{\pi(n-1)})$.

•

3.6.2 Beispiele

i) Für $n = 2$ ist z.B.

$$f\colon \mathbb{K}^2 \times \mathbb{K}^2 \to \mathbb{K}, \left(\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \right) \mapsto x_0 y_1 - x_1 y_0$$

bilinear, alternierend und schiefsymmetrisch. Falls $\mathrm{char}(\mathbb{K}) \neq 2$ ist, ist f nicht symmetrisch.

ii) Bei $\mathrm{char}(\mathbb{K}) = 2$ fallen die Begriffe symmetrisch und schiefsymmetrisch zusammen.

iii) Ein für die Anwendungen in der euklidischen Geometrie und Physik sehr wichtiges Beispiel ist (für $n = 2$) das sogenannte *Kreuzprodukt* im $\mathbb{R}^3$:

$$\times\colon \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3, \left(\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} \right) \mapsto \begin{pmatrix} x_1 y_2 - x_2 y_1 \\ x_2 y_0 - x_0 y_2 \\ x_0 y_1 - x_1 y_0 \end{pmatrix} =: x \times y,$$

es ist bilinear und schiefsymmetrisch.

◇

3.6.3 Hilfssatz

i) Jede alternierende multilineare Abbildung ist schiefsymmetrisch.

ii) Bei char$(\mathbb{K}) \neq 2$ *sind die multilinearen schiefsymmetrischen Abbildungen alternierend.*

Beweis:

i) $f: V^n \to V'$ sei alternierend und multilinear, $i \in n$, dann gilt:

$$\begin{aligned} 0 &= f(\ldots, v_{i-1}, v_i + v_{i+1}, v_i + v_{i+1}, v_{i+2}, \ldots) \\ &= f(v_0, \ldots, v_{n-1}) + f(\ldots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \ldots). \end{aligned}$$

Für die Transposition $\tau := (i, i+1)$ gilt also

$$f(v_0, \ldots, v_{n-1}) = \operatorname{sgn}(\tau) f(v_{\tau(0)}, \ldots, v_{\tau(n-1)}).$$

Da diese Transpositionen aber S_n erzeugen, und sgn ein Homormophismus ist, folgt daraus die Behauptung.

ii) ist klar.

Von besonderer Bedeutung sind für uns nun gewisse *Multilinearformen,* also der Fall $V' = \mathbb{K}$, und dabei wiederum der Fall $n := \dim_{\mathbb{K}}(V)$.

3.6.4 Definition (Determinantenformen) Ist $n := \dim_{\mathbb{K}} V \in \mathbb{N}^*$, dann heißt $\Delta: V^n \to \mathbb{K}$ *Determinantenform* auf V, kurz: $\Delta \in DF(V)$, wenn Δ multilinear und alternierend ist. •

Nach 3.6.3 sind Determinantenformen also auch schiefsymmetrisch.

3.6.5 Beispiele $\Delta: V^n \to \mathbb{K}, (v_0, \ldots, v_{n-1}) \mapsto 0_{\mathbb{K}}$ heißt die *triviale* Determinantenform auf V. 3.6.2 i) ist eine nicht triviale Determinantenform, 3.6.2 iii) ist multilinear, alternierend und schiefsymmetrisch, aber keine Determinantenform, da weder $n = 3$ noch der Bildraum gleich $\mathbb{K}$ ist. ◇

3.6.6 Hilfssatz *Ist $\Delta \in DF(V)$ und $V = {}_{\mathbb{K}} \ll b_0, \ldots, b_{n-1} \gg$, dann gilt für $v_i = \sum_{\nu=0}^{n-1} v_{\nu,i} b_\nu \in V$:*

$$\begin{aligned} \Delta(v_0, \ldots, v_{n-1}) &= \Delta(b_0, \ldots, b_{n-1}) \sum_{\pi \in S_n} sgn(\pi) v_{\pi(0),0} \cdots v_{\pi(n-1),n-1} \\ &= \Delta(b_0, \ldots, b_{n-1}) \sum_{\pi \in S_n} sgn(\pi) v_{0,\pi(0)} \cdots v_{n-1,\pi(n-1)}. \end{aligned}$$

Beweis: Wegen der Multilinearität von Δ folgt zunächst:

$$\Delta(v_0, \ldots, v_{n-1}) = \sum_{\varphi: n \to n} v_{\varphi(0),0} \cdots v_{\varphi(n-1),n-1} \Delta(b_{\varphi(0)}, \ldots, b_{\varphi(n-1)}).$$

Da Δ alternierend ist, ergibt das einmal

$$\Delta(v_0, \ldots, v_{n-1}) = \sum_{\pi \in S_n} v_{\pi(0),0} \cdots v_{\pi(n-1),n-1} \Delta(b_{\pi(0)}, \ldots, b_{\pi(n-1)}),$$

und — weil alternierende Multilinearformen schiefsymmetrisch sind — auch noch

$$= \Delta(b_0, \ldots, b_{n-1}) \sum_{\pi \in S_n} \operatorname{sgn}(\pi) v_{\pi(0),0} \cdots v_{\pi(n-1),n-1},$$

insgesamt also die erste der behaupteten Gleichungen. Schließlich gilt, wegen der Kommutativität von $\mathbb{K}$,

$$v_{\pi(0),0} \cdots v_{\pi(n-1),n-1} = v_{0,\pi^{-1}(0)} \cdots v_{n-1,\pi^{-1}(n-1)},$$

so daß mit $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$ auch die zweite der behaupteten Gleichungen folgt, denn $\pi \mapsto \pi^{-1}$ ist eine Bijektion auf jeder Gruppe, insbesondere also auch auf S_n. □

3.6.7 Folgerungen

i) Jede Determinantenform $\Delta \in DF(V)$ ist durch den Wert $\Delta(b_0, \ldots, b_{n-1})$ auf irgendeiner Basisfolge $\mathcal{B}$ von V vollständig bestimmt.

ii) Nichttriviale Determinantenformen sind Vielfache voneinander.

iii) Zu jeder Basisfolge $\mathcal{B}$ von V gibt es höchstens ein $\Delta \in DF(V)$ mit $\Delta(b_0, \ldots, b_{n-1}) = 1$.

□

Daß es zu jeder Basisfolge $\mathcal{B} := (b_0, \ldots, b_{n-1})$ von V *genau eine* Determinantenform Δ mit $\Delta(b_0, \ldots, b_{n-1}) = 1$ gibt, folgt damit aus

3.6.8 Hilfssatz *Die Gleichung*

$$\Delta_{\mathcal{B}}(\ldots, \sum_{\nu=0}^{n-1} v_{\nu,i} b_\nu, \ldots) := \sum_{\pi \in S_n} sgn(\pi) v_{\pi(0),0} \cdots v_{\pi(n-1),n-1}$$

definiert eine nicht triviale Determinantenform $\Delta_{\mathcal{B}}$ auf V. Für diese gilt

$$\Delta_{\mathcal{B}}(b_0, \ldots, b_{n-1}) = 1.$$

Beweis: Die Abbildung $\Delta_{\mathcal{B}}$ ist offensichtlich multilinear, sie ist auch alternierend: Sei $i \neq k$ und $v_i = v_k$. Für die Transposition $\tau := (ik) \in S_n$ gilt dann zunächst einmal die folgende Zerlegung von S_n in Rechtsnebenklassen der alternierenden Gruppe $A_n = \{\pi \in S_n \mid \operatorname{sgn}(\pi) = 1\}$:

$$S_n = A_n \cup A_n \tau.$$

Damit ergibt sich, wegen $v_i = v_k$,

$$\begin{aligned} \Delta_{\mathcal{B}}(v_0, \ldots, v_{n-1}) &= \Delta_{\mathcal{B}}(v_{\tau(0)}, \ldots, v_{\tau(n-1)}) \\ &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) v_{\pi(0),\tau(0)} \cdots v_{\pi(n-1),\tau(n-1)} \end{aligned}$$

$$= \sum_{\rho \in A_n} (\operatorname{sgn}(\rho) v_{\rho(0),\tau(0)} \cdots v_{\rho(n-1),\tau(n-1)} + \operatorname{sgn}(\rho\tau) v_{\rho\tau(0),\tau(0)} \cdots v_{\rho\tau(n-1),\tau(n-1)})$$

$$= \sum_{\rho \in A_n} (\operatorname{sgn}(\rho) v_{\rho(0),0} \cdots v_{\rho(n-1),n-1} - \operatorname{sgn}(\rho) v_{\rho(0),0} \cdots v_{\rho(n-1),n-1}).$$

Jeder dieser Summanden ist aber, ganz unabhängig von char($\mathbb{K}$), gleich Null. Die Gleichung $\Delta_{\mathcal{B}}(b_0, \ldots, b_{n-1}) = 1.$ folgt unmittelbar aus der Definition von $\Delta_{\mathcal{B}}$.

□

Insgesamt ist damit folgendes bewiesen:

3.6.9 Folgerung *Ist $\mathcal{B} = (b_0, \ldots, b_{n-1})$ Basisfolge für V, dann gilt*

i) Die eindeutig bestimmte Determinantenform $\Delta_{\mathcal{B}}$ mit $\Delta_{\mathcal{B}}(b_0, \ldots, b_{n-1}) = 1$ wird definiert durch

$$\Delta_{\mathcal{B}}(\ldots, \sum_{\nu=0}^{n-1} v_{\nu,i} b_\nu, \ldots) := \sum_{\pi \in S_n} sgn(\pi) v_{\pi(0),0} \cdots v_{\pi(n-1),n-1} =$$

$$\sum_{\pi \in S_n} sgn(\pi) v_{0,\pi(0)} \cdots v_{n-1,\pi(n-1)}.$$

ii) Jede andere Determinantenform $\Delta \in DF(V)$ ist Vielfache von $\Delta_{\mathcal{B}}$:

$$\Delta(v_0, \ldots, v_{n-1}) = \Delta(b_0, \ldots, b_{n-1}) \cdot \Delta_{\mathcal{B}}(v_0, \ldots, v_{n-1}).$$

□

Es soll nun gezeigt werden, wie mit Hilfe einer Determinantenform $\Delta \in DF(V)$ einem Endomorphismus $f \in End_{\mathbb{K}}(V)$ ein Skalar, die sogenannte Determinante $\det(f)$ von f zugeordnet werden kann, die sehr nützliche Eigenschaften hat.

3.6.10 Hilfssatz *$\Delta \in DF(V)$ sei nicht trivial, $f \in End_{\mathbb{K}}(V)$, dann gilt:*

i) $\Delta_f(v_0, \ldots, v_{n-1}) := \Delta(f(v_0), \ldots, f(v_{n-1}))$ definiert eine Determinantenform Δ_f.

ii) Der Faktor κ_f aus $\Delta_f = \kappa_f \cdot \Delta$ ist unabhängig von der Wahl der (nicht trivialen) Determinantenform Δ.

Beweis: i) ist klar.

ii) Sei $\Delta' = \lambda \cdot \Delta, \lambda \neq 0$, dann folgt aus

$$\Delta'(b_0, \ldots, b_{n-1}) = \lambda \cdot \Delta(b_0, \ldots, b_{n-1})$$

die linke Seite der folgenden Sequenz von Gleichungen:

$$\begin{aligned} \Delta'_f(b_0, \ldots, b_{n-1}) &= \lambda \cdot \Delta_f(b_0, \ldots, b_{n-1}) = \lambda \cdot \kappa_f \cdot \Delta(b_0, \ldots, b_{n-1}) \\ &= \kappa_f \cdot \Delta'(b_0, \ldots, b_{n-1}), \end{aligned}$$

also gilt auch für Δ': $\Delta'_f = \kappa_f \cdot \Delta'$. □

3.6.11 Definition (die Determinante eines Endomorphismus) Der Faktor

$$\det(f) := \frac{\Delta_f(b_0, \ldots, b_{n-1})}{\Delta(b_0, \ldots, b_{n-1})},$$

$\mathcal{B}$ irgendeine Basisfolge von V, Δ irgendeine nicht triviale Determinantenfolge auf V, $f \in End_{\mathbb{K}}(V)$, heißt die *Determinante* von $f \in End_{\mathbb{K}}(V)$. •

Für diese Zahl gilt also die Gleichung:

3.6.12 $$\det(f) \cdot \Delta = \Delta_f.$$

3.6.13 Satz *Für $f, g \in End_{\mathbb{K}}(V), n := dim_{\mathbb{K}}(V), \kappa \in \mathbb{K}$ gilt:*

i) $f = \kappa \cdot id_V \Longrightarrow \det(f) = \kappa^n$,

ii) $f \in \mathrm{Aut}_{\mathbb{K}}(V) \iff \det(f) \neq 0$,

iii) $\det(g \circ f) = \det(g) \cdot \det(f) = \det(f \circ g)$,

iv) $f \in \mathrm{Aut}_{\mathbb{K}}(V) \Longrightarrow \det(f^{-1}) = \det(f)^{-1}$,

v) $V = V_0 \oplus V_1, f_i := f \downarrow V_i, f_i(V_i) \subseteq V_i, i = 0, 1 \Longrightarrow \det(f) = \det(f_0) \cdot \det(f_1)$.

Beweis: Sei $\Delta \in DF(V)$ nicht trivial, $\mathcal{B} = (b_0, \ldots, b_{n-1})$ eine Basisfolge.

i) Wegen $f = f = \kappa \cdot id_V$ gilt

$$\Delta(f(b_0), \ldots, f(b_{n-1})) = \Delta(\kappa b_0, \ldots, \kappa b_{n-1}) = \kappa^n \Delta(b_0, \ldots, b_{n-1}).$$

ii) Es ist

$$\begin{array}{rcl} f \in Aut_{\mathbb{K}}(V) & \iff & (f(b_0,), \ldots, f(b_{n-1})) \text{ Basisfolge} \\ & \iff & 0 \neq \Delta(f(b_0), \ldots, f(b_{n-1})) = \det(f) \cdot \Delta(b_0, \ldots, b_{n-1}) \\ & \iff & \det(f) \neq 0. \end{array}$$

iii) Wir haben

$$\begin{array}{rcl} \det(g \circ f)\Delta(b_0, \ldots, b_{n-1}) & = & \Delta(g(f(b_0)), \ldots, g(f(b_{n-1})) \\ & = & \det(g)\Delta(f(b_0), \ldots, f(b_{n-1})) \\ & = & \det(g) \cdot \det(f) \cdot \Delta(b_0, \ldots, b_{n-1}) \end{array}$$

iv) $f \in Aut_{\mathbb{K}}(V)$ impliziert $f^{-1} \in Aut_{\mathbb{K}}(V)$, die Determinanten dieser beiden Abbildungen sind also, nach ii), von Null verschieden, und wir können wie folgt schließen:

$$1 =_{i)} \det(f \circ f^{-1}) =_{iii)} \det(f) \cdot \det(f^{-1}).$$

Hieraus folgt $\det(f) = \det(f^{-1})^{-1}$.

v) Für $g_0 := f_0 \oplus id_{V_1} : v = v_0 + v_1 \mapsto f_0(v_0) + v_1$ und die entsprechend definierte Abbildung $g_1 := id_{V_0} \oplus f_1$ gilt $f = g_0 \circ g_1$, also, nach iii): $\det(f) = \det(g_0) \cdot \det(g_1)$, so daß $\det(f_i) = \det(g_i)$ zu zeigen bleibt. Wir wählen hierzu eine an die direkte Zerlegung $V = V_0 \oplus V_1$ *angepaßte Basisfolge* $\mathcal{B}$:

$$V_0 = \mathbb{K} \ll b_0, \ldots, b_{r-1} \gg,\ V_1 = \mathbb{K} \ll b_r, \ldots, b_{n-1} \gg,\ V = \mathbb{K} \ll b_0, \ldots, b_r \gg,$$

falls $V_1 \neq 0$, andernfalls ist nichts zu zeigen. Hiermit definieren wir

$$\Delta_0(v_0, \ldots, v_{r-1}) := \Delta_{\mathcal{B}}(v_0, \ldots, v_{r-1}, b_r, \ldots, b_{n-1}),$$

eine offenbar nicht triviale Determinantenform auf V_0. Für sie gilt

$$\begin{aligned} \det(f_0)\Delta_0(b_0, \ldots, b_{r-1}) &= \Delta_0(f(b_0), \ldots, f(b_{r-1})) \\ &= \Delta_{\mathcal{B}}(f(b_0), \ldots, f(b_{r-1}), b_r, \ldots, b_{n-1}) \\ &= \Delta_{\mathcal{B}}(g_0(b_0), \ldots, g_0(b_{n-1})) \\ &= \det(g_0) \cdot \Delta_{\mathcal{B}}(b_0, \ldots, b_{n-1}) \\ &= \det(g_0) \cdot \Delta_0(b_0, \ldots, b_{r-1}), \end{aligned}$$

also $\det(f_0) = \det(g_0)$. Analog folgt $\det(f_1) = \det(g_1)$.

□

Mit Hilfe der Determinante eines Endomorphismus kann nun eine Determinante für jede quadratische Matrix definiert werden. Dies geschieht so, daß für jede Basisfolge $\mathcal{B}$ von V gilt:

$$\det(A) = \det(f), \text{ falls } A = M(\mathcal{B}, f, \mathcal{B}).$$

Sei deshalb $A = (a_{ik}) = M(\mathcal{B}, f, \mathcal{B}) \in \mathbb{K}^{n \times n}$. Dann gilt

$$\det(f) \cdot \Delta_{\mathcal{B}}(b_0, \ldots, b_{n-1}) = \Delta_{\mathcal{B}}(f(b_0), \ldots, f(b_{n-1}))$$

$$= \Delta_{\mathcal{B}}(\ldots, \sum_{i=0}^{n-1} a_{ik} b_i, \ldots) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(0),0} \cdots a_{\pi(n-1),n-1}.$$

Wir sehen, daß dieser Ausdruck nicht von $\mathcal{B}$ und der hierzu passend zu wählenden Abbildung f abhängt, definieren deshalb wie folgt:

3.6.14 Definition (die Determinante einer Matrix) Ist $A = (a_{ik}) \in \mathbb{K}^{n \times n}$, dann sei

$$\det(A) := \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=0}^{n-1} a_{\pi(i),i} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=0}^{n-1} a_{i,\pi(i)}$$

die *Determinante* der Matrix A. •

3.6.15 Beispiele

i) $\det(a_{00}) = a_{00}$,

ii) $\det \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} = a_{00}a_{11} - a_{01}a_{10}$,

iii) $\det \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} = a_{00}a_{11}a_{22} - a_{10}a_{01}a_{22} + a_{20}a_{11}a_{02}$

$$-a_{00}a_{21}a_{12} + a_{10}a_{21}a_{02} + a_{20}a_{01}a_{12}.$$

◇

3.6.16 Folgerungen *Sind $A, B \in \mathbb{K}^{n\times n}, \kappa \in \mathbb{K}$, dann gilt:*

i) Ist $\mathcal{B}$ Basisfolge, $f \in End_{\mathbb{K}}(V), A = M(\mathcal{B}, f, \mathcal{B})$, so ist

$$\det(f) = \det(A).$$

ii) $\det(\kappa \cdot E_n) = \kappa^n$,

iii) A ist genau dann invertierbar, wenn $\det(A) \neq 0$,

iv) Die Abbildung einer Matrix auf ihre Determinante ist ein Homomorphismus *(ein Monoidhomomorphismus auf dem Ring $\mathbb{K}^{n\times n}$ der n-reihigen Matrizen, ein Gruppenhomomorphismus auf der Gruppe $GL_n(\mathbb{K})$ der invertierbaren n-reihigen Matrizen):*

$$\det(A \cdot B) = \det(A) \cdot \det(B) = \det(B \cdot A),$$

v) Ist B invertierbar, dann gilt

$$\det(BAB^{-1}) = det(A),$$

d.h. die Determinante ist invariant *unter der Transformation $A \mapsto BAB^{-1}$.*

vi) A ist invertierbar $\Longrightarrow \det(A^{-1}) = \det(A)^{-1}$,

vii) $\det(A) = \det({}^tA)$.

(Die Punkte i) bis v) folgen umnittelbar aus 3.6.13, der sechste Punkt ergibt sich aus $\prod_\nu a_{\pi(\nu),\nu} = \prod_\nu a_{\nu,\pi^{-1}(\nu)}$.) Für die konkrete Berechnung der Determinante einer Matrix A verwendet man zweckmäßigerweise *nicht* die oben angegebene explizite Formel, da diese aus $n!$ Summanden besteht. Vielmehr geht man in der Regel zu einer Matrix A' über, die dieselbe Determinante besitzt, bei der aber sichtlich weniger Summanden zu berechnen sind, da die anderen verschwinden. Die möglichen Umformungen ergeben sich aus 3.6.16 mit der Tatsache, daß Determinantenformen multilinear und alternierend sind:

3.6.17 Satz *Die Determinante* $\det(A)$ *ist multilinear, alternierend und schiefsymmetrisch in den Zeilen und in den Spalten von A. Es gilt also insbesondere:*

i) Das Vertauschen zweier Zeilen oder Spalten ändert am Wert der Determinante nur das Vorzeichen.

ii) Entsteht A' *aus A durch Multiplizieren einer Zeile oder einer Spalte mit* κ*, dann gilt* $\det(A') = \kappa \cdot \det(A)$.

iii) Addition eines Vielfachen einer Zeile (Spalte) zu einer anderen (!) Zeile (Spalte) ändert den Wert der Determinante nicht.

iv) Ist der Rang von A kleiner als die Zeilenzahl, dann gilt $\det(A) = 0$.

3.6.18 Beispiele
i)

$$\det \begin{pmatrix} a_{00} & & * \\ & \ddots & \\ 0 & & a_{n-1,n-1} \end{pmatrix} = \det \begin{pmatrix} a_{00} & & 0 \\ & \ddots & \\ * & & a_{n-1,n-1} \end{pmatrix} = a_{00} \cdots a_{n-1,n-1}$$

folgt unmittelbar aus der (wichtigen) Bemerkung, daß jeder Summand $\prod_i a_{\pi(i),i}$ aus jeder Zeile und Spalte von A genau ein Element enthält, bei oberen oder unteren Dreiecksmatrizen ist also maximal ein einziger Summand (der zu $\pi = \mathrm{id}$) von Null verschieden.
ii) Die *Vandermondesche Determinante:* Für paarweise verschiedene $\kappa_i \in \mathbb{K}^*$ gilt

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \kappa_0 & \kappa_1 & \dots & \kappa_{n-1} \\ \kappa_0^2 & \kappa_1^2 & \dots & \kappa_{n-1}^2 \\ \vdots & \vdots & & \vdots \\ \kappa_0^{n-1} & \kappa_1^{n-1} & \dots & \kappa_{n-1}^{n-1} \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & \kappa_1 - \kappa_0 & \dots & \kappa_{n-1} - \kappa_0 \\ 0 & \kappa_1^2 - \kappa_0\kappa_1 & \dots & \kappa_{n-1}^2 - \kappa_0\kappa_{n-1} \\ \vdots & \vdots & & \vdots \\ 0 & \kappa_1^{n-1} - \kappa_0\kappa_1^{n-2} & \dots & \kappa_{n-1}^{n-1} - \kappa_0\kappa_{n-1}^{n-2} \end{pmatrix},$$

da man von der $(i+1)-$ten Zeile das κ_0-fache der $i-$ten Zeile abziehen kann, ohne daß sich die Determinante ändert. Benutzt man jetzt die explizite Formel, so sieht man, daß (wegen der Nullen in der ersten Spalte) gilt

$$= \det \begin{pmatrix} \kappa_1 - \kappa_0 & \kappa_2 - \kappa_0 & \dots & \kappa_{n-1} - \kappa_0 \\ \kappa_1^2 - \kappa_0\kappa_1 & \kappa_2^2 - \kappa_0\kappa_2 & \dots & \kappa_n^2 - \kappa_0\kappa_{n-1} \\ \vdots & & & \\ \kappa_1^{n-1} - \kappa_0\kappa_1^{n-2} & \kappa_2^{n-1} - \kappa_0\kappa_2^{n-2} & \dots & \kappa_{n-1}^{n-1} - \kappa_0\kappa_{n-1}^{n-2} \end{pmatrix}$$

$$= (\kappa_1 - \kappa_0)(\kappa_2 - \kappa_0) \dots (\kappa_{n-1} - \kappa_0) \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \kappa_1 & \kappa_2 & \dots & \kappa_{n-1} \\ \vdots & \vdots & & \vdots \\ \kappa_1^{n-2} & \kappa_2^{n-2} & \dots & \kappa_{n-1}^{n-2} \end{pmatrix},$$

so daß per Induktion nach n folgt:

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \kappa_0 & \kappa_1 & \dots & \kappa_{n-1} \\ \vdots & \vdots & & \vdots \\ \kappa_0^{n-1} & \kappa_1^{n-1} & \dots & \kappa_{n-1}^{n-1} \end{pmatrix} = \prod_{0 \le i < j \le n-1} (\kappa_j - \kappa_i),$$

denn

$$\det(1) = 1.$$

◇

Zur Vorbereitung eines Satzes über die rekursive Berechnung von Determinanten definieren wir

3.6.19 Definition (Cofaktoren) Sei $A = (a_{ik}) \in \mathbb{K}^{n \times n}$ und a_i der i-te Zeilenvektor, a'_k der k-te Spaltenvektor dieser Matrix. Wir definieren mit Hilfe der Basisfolge $\mathcal{E} = (e_0, \dots, e_{n-1})$ aus den Einheitsvektoren den *Cofaktor* von a_{ik} durch

$$\mathrm{Cof}(a_{ik}) := \det(A_{ik}),$$

wobei A_{ik} aus A durch Ersetzen der $i-$ten Zeile durch den Einheitsvektor e_k und der k-ten Spalte durch den Einheitsvektor e_i entsteht:

$$A_{ik} = \begin{pmatrix} & & & 0 & & & \\ & * & & \vdots & & * & \\ & & & 0 & & & \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ & & & 0 & & & \\ & * & & \vdots & & * & \\ & & & 0 & & & \end{pmatrix}.$$

•

Es ist leicht einzusehen, daß diese Zahl auch mit Hilfe der Basisfolge $\mathcal{E}$ aus den Einheitsvektoren beschrieben werden kann, d.h. daß gilt

3.6.20 Bemerkung Die Cofaktoren lassen sich wie folgt auch mit Hilfe der Determinantenform $\Delta_{\mathcal{E}}$ ausdrücken:

$$\begin{aligned} \mathrm{Cof}(a_{ik}) &= \det(A_{ik}) \\ &= \Delta_{\mathcal{E}}(a_0, \dots, a_{i-1}, e_k, a_{i+1}, \dots, a_{n-1}) \\ &= \Delta_{\mathcal{E}}(a'_0, \dots, a'_{k-1}, e_i, a'_{k+1}, \dots, a'_{n-1}). \end{aligned}$$

◇

Weiterhin sei die *adjungierte Matrix* zu A definiert durch

$$\mathrm{Ad}(A) := {}^t(\mathrm{Cof}(a_{ik})).$$

3.6.21 Satz $A \cdot \mathrm{Ad}(A) = \det(A) \cdot E_n$.

Beweis:

$$\begin{aligned}(A \cdot \mathrm{Ad}(A))_{ik} &= \sum_\nu a_{i\nu}\mathrm{Cof}(a_{k\nu}) \\ &= \Delta_{\mathcal{E}}(a_0, \ldots, a_{k-1}, \sum_\nu a_{i\nu}e_\nu, a_{k+1}, \ldots, a_{n-1})) \\ &= \Delta_{\mathcal{E}}(a_0, \ldots, a_{k-1}, a_i, a_{k+1}, \ldots, a_{n-1})) \\ &= \delta_{ik}\det(A).\end{aligned}$$

□

3.6.22 Folgerung *Ist A invertierbar, dann gilt*

$$A^{-1} = \frac{\mathrm{Ad}(A)}{\det(A)} \ .$$

3.6.23 Beispiel

$$A := \begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} \Rightarrow \mathrm{Ad}(A) = {}^t(\mathrm{Cof}(a_{ik})) = {}^t\begin{pmatrix}\det\begin{pmatrix}1&0\\0&4\end{pmatrix} & \det\begin{pmatrix}0&1\\3&0\end{pmatrix}\\ \det\begin{pmatrix}0&2\\1&0\end{pmatrix} & \det\begin{pmatrix}1&0\\0&1\end{pmatrix}\end{pmatrix}$$

$$= {}^t\begin{pmatrix}4 & -3\\ -2 & 1\end{pmatrix} = \begin{pmatrix}4 & -2\\ -3 & 1\end{pmatrix} \Rightarrow A^{-1} = \frac{1}{4-6}\begin{pmatrix}4 & -2\\ -3 & 1\end{pmatrix} = \begin{pmatrix}-2 & 1\\ 3/2 & -1/2\end{pmatrix}.$$

◇

Als Anwendung auf lineare Gleichungssysteme mit *regulärer,* d.h. invertierbarer Koeffizientenmatrix A ergibt sich

3.6.24 Die Cramersche Regel *Ist $A \in \mathbb{K}^{n\times n}$ invertierbar, dann gilt für die Komponenten x_i der eindeutig bestimmten Lösung von $Ax = b$:*

$$x_i = \frac{1}{\det(A)} \cdot \det\begin{pmatrix}a_{00} & \ldots & a_{0,i-1} & b_1 & a_{0,i+1} & \ldots & a_{0,n-1}\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ a_{n-1,0} & \ldots & a_{n-1,i-1} & b_n & a_{n-1,i+1} & \ldots & a_{n-1,n-1}\end{pmatrix}.$$

Beweis:
Aus $x = A^{-1}b = \frac{1}{\det(A)}\mathrm{Ad}(A) \cdot b$ ergibt sich

$$\begin{aligned}x_i &= \frac{1}{\det(A)} \cdot (\sum_\nu \mathrm{Cof}(a_{\nu i}b_\nu)) \\ &= \frac{\Delta_{\mathcal{E}}(a'_0, \ldots, a'_{i-1}, b, a_{i+1}, \ldots, a'_{n-1})}{\det(A)}.,\end{aligned}$$

also die Behauptung.

□

Weiter erhalten wir jetzt die angekündigte Rekursionsformel

3.6.25 Der Laplacesche Entwicklungssatz *Ist* $A \in \mathbb{K}^{n\times n}$, *dann gilt, für jedes* $i, k \in n$:

$$\det(A) = \sum_{\nu}(-1)^{i+\nu} a_{i\nu} \det(A'_{i\nu}) = \sum_{\nu}(-1)^{\nu+k} a_{\nu k} \det(A'_{\nu k}),$$

d.h. man kann $\det(A)$ *sowohl* nach der $i-$ten Zeile *als auch* nach der $k-$ten Spalte entwickeln. A'_{ik} *bezeichnet dabei die* $(n-1)\times(n-1)$*-Matrix, die man aus* A *durch* Streichen *von* i*-ter Zeile und* k*-ter Spalte erhält.*

Beweis: Es gilt offenbar

$$\begin{aligned} \det(A) &= \Delta_{\mathcal{E}}(a'_0, \ldots, a'_{n-1}) = \sum_{\nu} a_{\nu k} \Delta_{\mathcal{E}}(a'_0, \ldots, a'_{k-1}, e_\nu, a'_{k+1}, \ldots, a'_{n-1}) \\ & \sum_{\nu} a_{\nu k} \mathrm{Cof}(a_{k\nu}) = \sum_{\nu} a_{\nu k} \det(A_{\nu k}). \end{aligned}$$

Entsprechendes gilt für die Entwicklung nach der $i-$ten Zeile. Schließlich gilt noch, wegen der Schiefsymmetrie der Determinante,

$$\det(A_{ik}) = (-1)^{i+k} \det(A'_{ik}).$$

□

3.7 Eigenwerte und Eigenvektoren

Wir wollen jetzt lineare Endomorphismen durch Matrizen besonders übersichtlicher Gestalt (u.a. mit möglichst vielen Nullen) beschreiben, was durch die Auswahl geeigneter Basen geschieht.
Zu einer besonders einfachen Form der $f \in \mathrm{End}_{\mathbb{K}}(V)$ darstellenden Matrix verhelfen gegebenenfalls natürlich solche Basisvektoren, die von f auf ein Vielfaches von sich selbst abgebildet werden. Wir bemerken zunächst, daß für solche Vektoren folgendes gilt:

$$f(v) = \kappa \cdot v \iff (f - \kappa \cdot \mathrm{id}_V)(v) = 0 \iff v \in \mathrm{Kern}(f - \kappa \cdot \mathrm{id}_V).$$

Wir führen deshalb die folgenden Bezeichnungen ein:

3.7.1 Definition (Eigenwerte, Eigenvektoren, Eigenräume) Ist $f \in \mathrm{End}_{\mathbb{K}}(V)$, dann heißt $\kappa \in \mathbb{K}$ *Eigenwert* von f genau dann, wenn

$$\mathrm{Kern}(f - \kappa \cdot \mathrm{id}_V) \neq \{0_V\}.$$

Die von Null verschiedenen Elemente des Kerns von $f - \kappa \cdot \mathrm{id}_V$ heißen ggf. *Eigenvektoren* zum Eigenwert κ, und als *Eigenraum* von f zum Eigenwert κ bezeichnen wir den gesamten Kern:

$$E(\kappa) := \{v \in V \mid f(v) = \kappa v\} = \mathrm{Kern}(f - \kappa \cdot \mathrm{id}_V).$$

•

Falls die Dimension von V endlich ist, gibt es weitere dazu äquivalente Formulierungen, denn wir können die Determinante von f heranziehen:

3.7.2 Hilfssatz *Ist $f \in \mathrm{End}_{\mathbb{K}}(V)$, $dim_{\mathbb{K}}(V) \in \mathbb{N}^*$, $\kappa \in \mathbb{K}$, dann sind äquivalent:*

1. *κ ist Eigenwert von f,*
2. $\mathrm{Kern}(f - \kappa \cdot \mathrm{id}_V) \neq \{0_V\}$,
3. $\det(f - \kappa \cdot \mathrm{id}_V) = 0$,
4. *$f - \kappa \cdot \mathrm{id}_V$ ist nicht injektiv,*
5. *$f - \kappa \cdot \mathrm{id}_V$ ist nicht surjektiv,*
6. $\exists\, v \in V \backslash \{0_V\}$: $f(v) = \kappa \cdot v$.

Die Gleichung $\det(f - \kappa \cdot \mathrm{id}_V) = 0$ zeigt, daß die Eigenwerte von f als Nullstellen eines Polynoms aufgefaßt werden können. Wir wollen dies präzisieren und beginnen dazu mit

3.7.3 Definition (Formale Potenzreihen, Polynome, Polynomabbildungen) $(R, +, \cdot)$ sei ein kommutativer Ring mit Einselement.

- Wir erinnern zunächst an den Ring $R^{\mathbb{N}}$ der *formalen Potenzreihen* über R in einer *Unbestimmten* x. Die Elemente $p \in R^{\mathbb{N}}$ schreibt man gern in der Form
$$p = \sum_{n=0}^{\infty} p_n x^n, \ \textit{wobei } p_n := p(n).$$
Dieser Ring wird meist mit $R[\![x]\!]$ bezeichnet, um die Bezeichnung der *Unbestimmten* x hervorzuheben. Er enthält — auch das wurde bereits erwähnt — den Teilring
$$R[x] := \{p \in R^{\mathbb{N}} \mid p(n) = 0, \ \textit{für fast alle } n\}$$
der *Polynome* über R in einer Unbestimmten x.

- Ist $p \in R[x]^*$ und $n \in \mathbb{N}$ maximal mit $p(n) \neq 0$, dann heißt $r_n = p(n)$ der *Leitkoeffizient* von p und n der *Grad* von p. Dem Nullpolynom wird kein Grad zugeordnet.

- Zu $p := \sum r_n x^n \in R[x]$ gehört die *Polynomabbildung*
$$P\colon R \to R, \rho \mapsto \sum r_n \rho^n.$$
Ganz allgemein heißt $f \in R^R$ *polynomiale Abbildung,* wenn es $p \in R[x]$ gibt mit $P = f$, d.h. $P(\rho) = f(\rho)$, für alle $\rho \in R$. Falls $\mathrm{Char}(R) \neq 0$ ist P *nicht notwendig eindeutig bestimmt,* z.B. ist $P = 0$, falls $p = x + x^2 \in \mathbb{Z}_2[x]$.

- $\rho \in R$ heißt *Wurzel* von p, wenn ρ *Nullstelle* von P ist, d.h. wenn $P(\rho) = 0$ gilt.

•

Wir definieren:

3.7.4 Definition (charakteristisches Polynom, charakteristische Koeffizienten) Ist $f \in \mathrm{End}_{\mathbb{K}}(V)$, $n := \dim_{\mathbb{K}}(V) \in \mathbb{N}^*$, $\mathcal{B}$ eine Basisfolge für V, $A := M(\mathcal{B}, f, \mathcal{B})$, dann heißt
$$p_A := \det(A - x \cdot E_n) = \sum \alpha_i x^i \ \in \ \mathbb{K}[x]$$
das *charakteristische Polynom* von A. Die α_i heißen die *charakteristischen Koeffizienten* von A. Wegen $\det(A - xE_n) = \det(TAT^{-1} - x \cdot E_n)$ ist dieses Polynom unabhängig von der Wahl der Basisfolge, wir können also
$$p_f := p_A$$
setzen und dieses Polynom auch als das charakteristische Polynom *von* f bezeichnen und die α_i als die charakteristischen Koeffizienten von f. •

Für

$$A := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

gilt beispielsweise

$$p_A = \det \begin{pmatrix} 1-x & 2 \\ 3 & 4-x \end{pmatrix} = x^2 - 5x - 2.$$

3.7.5 Hilfssatz *Ist* $f \in \mathrm{End}_{\mathbb{K}}(V)$, $n := dim_{\mathbb{K}}(V) \in \mathbb{N}^*$, $A = M(\mathcal{B}, f, \mathcal{B}) = (a_{ik})$, *dann gilt für die charakteristischen Koeffizienten von* f *bzw.* A *:*

$$\alpha_0 = \det(A),\ \alpha_{n-1} = (-1)^{n-1} \sum_i a_{ii},\ \alpha_n = (-1)^n.$$

□

Die Summe $\sum_i a_{ii}$ der Elemente in der *Hauptdiagonalen* von A heißt die *Spur* von A :

$$\mathrm{Spur}(A) := \sum_i a_{ii}.$$

Aus der Definition des charakteristischen Polynoms ergibt sich direkt:

3.7.6 Folgerung *Eigenwerte von* $f \in \mathrm{End}_{\mathbb{K}}(V)$ *bzw.* $A = M(\mathcal{B}, f, \mathcal{B})$ *sind, bei endlichdimensionalem* V*, gegebenenfalls (!) genau die Wurzeln (in* $\mathbb{K}$*!) des charakteristischen Polynoms* $p_f = p_A$*, also die Nullstellen der zugehörigen Polynomabbildung* $P_f = P_A$*.* □

Deshalb liefern u.a. auch Hilfsmittel aus der Analysis, nämlich Aussagen über Nullstellen von Polynomabbildungen, Existenzsätze für Eigenwerte. So sagt z.B. der *Fundamentalsatz der Algebra* — der meist in der Vorlesung über Funktionentheorie bewiesen wird — aus, daß jede Polynomabbildung $P\colon \mathbb{C} \to \mathbb{C}, p$ vom Grad n, n Nullstellen (die aber nicht paarweise verschieden sein müssen) in $\mathbb{C}$ hat. Das liefert, mit 4.3.9:

3.7.7 Satz *Jeder lineare Endomorphismus eines endlichdimensionalen Vektorraums* $V \neq \{0_V\}$ *über* $\mathbb{C}$ *besitzt Eigenwerte (und damit auch Eigenvektoren).*

□

Das gilt für $\mathbb{K} := \mathbb{R}$ dagegen nicht, z.B. hat das Polynom $p := 1 + x^2$ keine Wurzeln in $\mathbb{R}$, die lineare Abbildung $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$ mit

$$M(\mathcal{E}, f, \mathcal{E}) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

hat also *keine* Eigenwerte. Immerhin gilt noch

3.7.8 Satz *Ist* $n := dim_{\mathbb{R}}(V) \in \mathbb{N}^*, f \in \mathrm{End}_{\mathbb{R}}(V)$, *dann gilt:*

1. *Ist* n *ungerade, dann besitzt* f *Eigenwerte, und zwar mindestens einen positiven (negativen), falls* $\det(f)$ *positiv (negativ) ist.*

2. *Ist n gerade und $\det(f)$ negativ, dann besitzt f mindestens einen positiven und einen negativen Eigenwert.*

□

Beweis: Bei ungeradem n ist $a_n = (-1)^n = -1$, und nach Sätzen aus der Analysis ergibt sich, daß $P_f(x)$ mit $x \to -\infty$ gegen ∞ geht, mit $x \to \infty$ dagegen nach $-\infty$. Wegen der Stetigkeit von P_f folgt daraus mit dem Zwischenwertsatz die Behauptung. Analog folgt für gerade n die zweite Behauptung, da dann $\alpha_0 = P_f(0) = \det(f)$. □

Kehren wir wieder zu dem allgemeinen Fall zurück.

3.7.9 Satz *Jede Menge aus Eigenvektoren zu paarweise verschiedenen Eigenwerten ist linear unabhängig.*

Beweis: M bezeichne die gegebene Menge von Eigenvektoren. Wir haben zu zeigen, daß für jede endliche Teilmenge $\emptyset \neq N := \{v_0, \ldots, v_{n-1}\} \subseteq M$ gilt:

$$\sum_i \kappa_i v_i = 0 \Longrightarrow \ \forall\ i\colon\ \kappa_i = 0.$$

Der Beweis erfolgt per Induktion nach n :

I $n = 1$: Die Menge $\{v_0\}$ ist linear unabhängig, da $v_0 \neq 0$.

II $n \to n+1$: Wir schließen indirekt. Wäre $\{v_0, \ldots, v_n\}$ linear abhängig, dann gäbe es eine nicht triviale lineare Relation zwischen den Elementen dieser Menge. Ohne Einschränkung der Allgemeinheit können wir annehmen, sie sei von der Form $v_n = \sum_0^{n-1} \lambda_i v_i$, wobei nicht alle λ_i gleich Null sind. Daraus würde sich aber folgendes ergeben, wenn v_i Eigenvektor zum Eigenwert κ_i ist,

$$\begin{aligned} 0 &= f(v_n) - \kappa_n \cdot v_n \\ &= \sum_0^{n-1} \lambda_i f(v_i) - \kappa_n \sum_0^{n-1} \lambda_i v_i \\ &= \sum_0^{n-1} \lambda_i (\underbrace{\kappa_i - \kappa_n}_{\neq 0}) v_i, \end{aligned}$$

ein Widerspruch zur Induktionsannahme, der linearen Unabhängigkeit von $\{v_0, \ldots, v_{n-1}\}$. □

3.7.10 Folgerung *Ist f ein linearer Endomorphismus von V, $\dim_{\mathbb{K}}(V) \in \mathbb{N}^*$, mit $\dim_{\mathbb{K}}(V)$ paarweise verschiedenen Eigenwerten, dann besitzt V eine Basisfolge $\mathcal{B}$ aus Eigenvektoren. f wird also bezüglich dieser Basisfolge durch eine Diagonalmatrix $M(\mathcal{B}, f, \mathcal{B})$ beschrieben, in deren Hauptdiagonale die Eigenwerte von f stehen.*

□

3.7.11 Satz *Ist* $V = U \oplus W, n = dim_{\mathbb{K}}(V) \in \mathbb{N}^*, f \in \mathrm{End}_{\mathbb{K}}(V), f(U) \subseteq U, \pi_W\colon V \to W, u + w \mapsto w$ *(die kanonische Projektion von* V *auf* W*), dann gilt: Für* $g := \pi_W \circ f \downarrow W$ *haben wir*

$$p_f = p_{f\downarrow U} \cdot p_g.$$

□

Beweis: Wir wählen eine Basisfolge $\mathcal{B}$ von V, die an die Zerlegung "angepaßt" ist, d.h. $\mathcal{B} = (b_0, \ldots, b_{n-1})$, mit

$$U = \ll b_0, \ldots, b_{m-1} \gg, W = \ll b_m, \ldots, b_{n-1} \gg .$$

Dann gilt für $A := M(\mathcal{B}, f, \mathcal{B})$ und $\mathcal{B}_0 = (b_0, \ldots, b_{m-1}), \mathcal{B}_1 = (b_m, \ldots, b_{n-1})$:

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}, \text{ mit } B = M(\mathcal{B}_0, f \downarrow U, \mathcal{B}_0),$$

sowie, wegen $f(U) \subseteq U$, mit einer Nullmatrix 0 aus n Zeilen und m Spalten,

$$\begin{aligned} M(\mathcal{B}_1, g, \mathcal{B}_1) &= M(\mathcal{B}_1, \pi_w, \mathcal{B}) \cdot M(\mathcal{B}, f \downarrow W, \mathcal{B}_1) \\ &= (0 \mid E_{n-m}) \cdot \begin{pmatrix} C \\ D \end{pmatrix} = D. \end{aligned}$$

Damit erhalten wir:

$$p_f = \det(A - xE_n) = \det(B - xE_m) \cdot \det(D - xE_{n-m}) = p_{f\downarrow U} \cdot p_g.$$

□

3.7.12 Folgerung *Ist* U *Unterraum von* V *mit* $f(U) \subseteq U$*, dann teilt* $p_{f\downarrow U}$ *das Polynom* p_f*.* □

Heißt $\kappa \in \mathbb{K}$ ein *r−facher* Eigenwert von f, wenn $(x-\kappa)^r$ Teiler von p_f ist, und verstehen wir unter der *Vielfachheit* von κ das maximale dieser r, dann ergibt sich:

3.7.13 Satz *Die Dimension des Eigenraums von* $\kappa \in \mathbb{K}$ *ist höchstens gleich der Vielfachheit von* κ *als Eigenwert.*

Beweis: Man sieht sehr leicht, daß $f \downarrow E(\kappa) = \kappa \cdot \mathrm{id}_{E(\kappa)}$ gilt, also

$$p_{f\downarrow E(\kappa)} = (\kappa - x)^{dim(E(\kappa))}.$$

Dieses Polynom teilt aber, wegen $f(E(\kappa)) \subseteq E(\kappa)$ und 3.7.12 das charakteristische Polynom p_f, in dem der Faktor $\kappa - x$ genau mit dem Exponenten r steckt.

□

Der Grad des Produkts zweier Polynome $\neq 0$ ist die Summe der Grade der Faktoren. Also ist die Summe der Vielfachheiten der Eigenwerte von f höchstens $\dim_{\mathbb{K}}(V)$. Das, zusammen mit 4.3.16, ergibt:

3.7.14 Satz *Ist $f \in \mathrm{End}_{\mathbb{K}}(V)$ und $n := dim_{\mathbb{K}}(V) \in \mathbb{N}^*$, dann sind äquivalent:*

- *f läßt sich durch eine Diagonalmatrix beschreiben.*
- *V hat eine Basis aus Eigenvektoren.*
- *V ist direkte Summe der Eigenräume von f.*
- *p_f ist Produkt von Linearfaktoren (:=Polynome vom Grad 1) und die Vielfachheiten der Eigenwerte gleichen den Dimensionen der zugehörigen Eigenräume.*

□

Will man eine Matrix auf Diagonalisierbarkeit untersuchen, wird man sich also zuerst das charakteristische Polynom vorzunehmen. Läßt es sich in Linearfaktoren zerlegen, hat man noch die Dimensionen $n - Rg(A - \kappa E)$ der Eigenräume zu ermitteln und mit den Vielfachheiten zu vergleichen.

3.7.15 Beispiel

1. Die Matrix
$$A := \begin{pmatrix} -1 & 4 & 6 \\ 0 & -1 & 0 \\ 0 & 5 & 2 \end{pmatrix}$$
hat das charakteristische Polynom
$$\det(A - xE) = \det \begin{pmatrix} -1-x & 4 & 6 \\ 0 & -1-x & 0 \\ 0 & 5 & 2-x \end{pmatrix} = -(1+x)^2(2-x),$$
also die Eigenwerte $\kappa_0 = -1$ und $\kappa_1 = 2$. Wegen
$$A - \kappa_0 E_3 = \begin{pmatrix} 0 & 4 & 6 \\ 0 & 0 & 0 \\ 0 & 5 & 3 \end{pmatrix},$$
ist die Dimension des Eigenraums, also $3 - Rg(A - \kappa_0 E)$, gleich 1 und damit kleiner als die Vielfachheit des Eigenwerts κ_0. Die Matrix A besitzt demnach *keine* Basis aus Eigenvektoren.

2. Für die Matrix
$$A := \begin{pmatrix} -1 & 4 & 6 \\ 0 & 2 & 0 \\ 0 & 5 & 3 \end{pmatrix}$$
dagegen gilt $p_A = -(1+x)(2-x)(3-x)$. Die Eigenwerte sind also $\kappa_0 = -1$, $\kappa_1 = 2$ und $\kappa_2 = 3$. Nach 4.3.12 existiert also eine Basis aus Eigenvektoren.

3. Einen Eigenvektor b_i zum Eigenwert κ_i erhält man durch Lösen des Gleichungssystems $(A - \kappa_i E_n)b_i = 0$, für unser Beispiel erhält man beispielsweise (die Eigenvektoren sind nur bis auf Zahlenfaktoren eindeutig bestimmt!):
$$b_0 = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}, b_1 = \begin{pmatrix} 26/3 \\ -1 \\ 5 \end{pmatrix}, b_2 = \begin{pmatrix} -9 \\ 0 \\ -6 \end{pmatrix}.$$

$\diamond$

Eine deutlich schwächere Forderung an A als die Diagonalisierbarkeit ist die nach *Trigonalisierbarkeit:*

3.7.16 Satz *Ist $f \in \mathrm{End}_{\mathbb{K}}(V)$ und $n := dim_{\mathbb{K}}(V) \in \mathbb{N}^*$, dann sind äquivalent:*

- *f ist trigonalisierbar, d.h. es gibt eine Basisfolge $\mathcal{B}$, so daß $A := M(\mathcal{B}, f, \mathcal{B})$ eine obere Dreiecksmatrix ist.*
- *Es gibt eine Kette*
$$V_0 := \{0\} \subset V_1 \subset \ldots \subset V_{n-1} \subset V_n := V$$
f-invarianter Unterräume (d.h. $f(V_i) = V_i$) mit $dim_{\mathbb{K}}(V_i) = i$.
- *Das charakteristische Polynom zerfällt in Linearfaktoren:*
$$p_f = \prod_{i=0}^{n-1}(\lambda_i - x),\ \lambda_i \in \mathbb{K}.$$

Beweis:

a) Die Äquivalenz der ersten beiden Punkte ist klar: Eine an eine solche Kette von invarianten Unterräumen angepaßte Basis liefert eine obere Dreiecksmatrix und umgekehrt.

b) Ist $A := M(\mathcal{B}, f, \mathcal{B})$ eine obere Dreiecksmatrix, dann ist
$$\det(A - xE_n) = \prod_i (a_{ii} - x),$$
also Produkt von Linearfaktoren.

c) Zerfällt umgekehrt das charakteristische Polynom in Linearfaktoren, etwa $p_f = \prod_{i=0}^{n-1}(\lambda_i - x)$, dann können wir die Trigonalisierbarkeit wie folgt per Induktion nach n beweisen:

I $n = 1$: Dieser Fall ist trivial.

II $n > 1$: f besitzt Eigenvektoren zum Eigenwert λ_0. Wir nehmen einen von ihnen, v_0, als 0-tes Element der Basisfolge $\mathcal{B} = (v_0, \ldots, v_{n-1})$, so daß
$$A = M(\mathcal{B}, f, \mathcal{B}) = \begin{pmatrix} \lambda_0 & a_{01} & \ldots & a_{0,n-1} \\ 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{pmatrix}.$$

Nun gilt aber $V = \langle v_0 \rangle \oplus W$, wenn $W := \langle v_1, \ldots, v_{n-1} \rangle$. Aus 3.7.11 folgt demnach, wenn $U := \langle v_0 \rangle$,

$$p_f = p_{f\downarrow U} \cdot p_g,$$

mit $g = \pi_W \circ f \downarrow W$. Es folgt, weil $p_{f\downarrow U} = \lambda_0 - x$,

$$p_g = \prod_{i=1}^{n-1} (\lambda_i - x).$$

Nun ist aber p_g das charakteristische Polynom von $\tilde{A}$, so daß, nach Induktionsannahme, eine Kette

$$W_0 := \{0\} \subset W_1 \subset \ldots \subset W_{n-2} \subset W_{n-1} = W$$

aus g-invarianten Unterräumen W_i (der Dimension i) existiert.
Wir wollen zeigen, daß die Unterräume $V_i := U + W_{i-1}$ eine Kette f-invarianter Unterräume der gewünschten Dimensionen i bilden. Dazu bemerken wir, daß offenbar $f \downarrow W = h + k$, mit

$$h\colon W \to U, v_j \mapsto a_{0j} v_0, \text{ sowie } k\colon W \to W, v_j \mapsto \sum_{i=1}^{n-1} a_{ij} v_j.$$

Sei jetzt $v \in U + W_{i-1}$, etwa $v = u + w$, $u \in U, w \in W_{i-1}$. Es gilt dann

$$f(u+w) = f(u) + f(w) = f(u) + f \downarrow W(w) =$$
$$= f(u) + (h+k)(w) = \underbrace{f(u) + h(w)}_{\in U} + \underbrace{k(w)}_{=g(w)} \in U + W_{i-1}.$$

Demnach sind die V_i wirklich f-invariant. Die Aussage über die Dimension ist leicht nachzuvollziehen.

□

Dieser Beweis ergibt ein Verfahren zur sukzessiven Berechnung einer darstellenden Dreiecksmatrix anhand einer gegebenen Zerlegung

$$p_f = \pm \prod_{i=0}^{n-1} (\lambda_i - x)$$

des charakteristischen Polynoms in Linearfaktoren: Man geht von der Standardbasis $\mathcal{E}$ aus, ermittelt zunächst einen Eigenvektor v_0 zum Eigenwert λ_0 und nimmt diesen als 0-tes Element v_0 einer Basisfolge

$$\mathcal{B}_0 = (v_0, e_0, \ldots, e_{i-1}, \hat{e}_{i_0}, e_{i+1}, \ldots, e_{n-1}),$$

die aus v_0 und geeigneten $n-1$ Elementen der Standardbasis besteht (unter Verwendung des Austauschsatzes, die Schreibweise $\hat{e}_{i_0}$ bedeute, daß e_{i_0} ausgetauscht wurde). Die entsprechende Basistransformation T_0 ergibt

$$T_0 M(\mathcal{E}, f, \mathcal{E}) T_0^{-1} = \begin{pmatrix} \lambda_0 & * & \ldots & * \\ 0 & & & \\ \vdots & & \tilde{A}_0 & \\ 0 & & & \end{pmatrix}.$$

Jetzt betrachten wir den von der Basisfolge $(e_0, \ldots, e_{i-1}, \hat{e}_{i_0}, e_{i+1}, \ldots, e_{n-1})$ erzeugten Unterraum und auf diesem die durch $\tilde{A}_0$ dargestellte lineare Abbildung. Aus 3.7.12 folgt

$$p_{\tilde{A}_0} = \pm \prod_{i=1}^{n-1} (\lambda_i - x),$$

so daß man ganz analog zum vorherigen Schritt verfahren kann: Die Auswahl eines Eigenvektors v_1 zum Eigenwert λ_1 samt Anwendung des Austauschsatzes (mit $i_1 \neq i_0$) ergibt eine Basisfolge

$$(v_1, e_0, \ldots, \hat{e}_{i_0}, \ldots, \hat{e}_{i_1}, \ldots, e_{n-1}).$$

Die Transformation auf die Basisfolge

$$\mathcal{B}_1 := (v_0, v_1, e_0, \ldots, \hat{e}_{i_0}, \ldots, \hat{e}_{i_1}, \ldots, e_{n-1})$$

ergibt jetzt

$$T_1 M(\mathcal{E}, f, \mathcal{E}) T_1^{-1} = \begin{pmatrix} \lambda_0 & \lambda_1 & * & \ldots & * \\ 0 & \lambda_1 & * & \ldots & * \\ 0 & 0 & & & \\ \vdots & \vdots & & \tilde{A}_1 & \\ 0 & 0 & & & \end{pmatrix}$$

usw.

3.8 V als $\mathbb{K}[x]$-Linksmodul, das Minimalpolynom

Neben $f \in \mathrm{End}_{\mathbb{K}}(V)$ sind auch die "Polynome"

$$p(f) := \sum_{i=0}^{m} \kappa_i f^i, \text{ zu } p := \sum_{i=0}^{m} \kappa_i x^i \in \mathbb{K}[x],$$

Endomorphismen von V. Die Abbildung

$$\varphi_f \colon \mathbb{K}[x] \to \mathrm{End}_{\mathbb{K}}(V), p \mapsto p(f),$$

der *Einsetzungshomomorphismus* (bei dem f ja sozusagen in die Polynome *eingesetzt* wird) ist ein Ringhomomorphismus mit $\varphi(1) = \mathrm{id}_V$, also ein *Ring-mit-Eins-Homomorphismus.* Wir können damit V zu einem $\mathbb{K}[x]$-Linksmodul V_f machen,

$$V_f \text{ mit } pv := p(f)(v).$$

Diese induzierten $\mathbb{K}[x]$-Linksmodulstrukturen sind i.a. nicht alle verschieden. Ein vollständiges System paarweise verschiedener erhält man aus den Konjugiertenklassen der Endomorphismen von V unter der vollen linearen Gruppe:

3.8.1 Satz *Zu $f, g \in End_{\mathbb{K}}(V)$ sind V_f und V_g genau dann isomorph (als $\mathbb{K}[x]$-Linksmoduln), wenn es $h \in \mathrm{Aut}_{\mathbb{K}}(V)$ gibt mit*

$$hfh^{-1} = g.$$

Beweis: i) Wir beweisen zunächst, daß aus der Existenz eines solchen h die Isomorphie der induzierten Strukturen folgt. Dazu sei wieder $p = \sum_i \kappa_i x^i \in \mathbb{K}[x]$, wir haben dann (in V^V):

$$h \circ p(f) = \sum_i \kappa_i h f^i = \sum_i \kappa_i h f^i h^{-1} h = \sum_i \kappa_i g^i h = p(g) \circ h.$$

Ist jetzt $v \in V$, dann folgt

$$h(pv) = h(p(f)(v)) = (h \circ p(f))(v) = (p(g) \circ h)(v) = ph(v).$$

h induziert also auf V_f eine $\mathbb{K}[x]$-lineare bijektive Abbildung aus V_g, einen Isomorphismus zwischen $\mathbb{K}[x]$-Linksmoduln.

ii) Ist umgekehrt $\varphi \colon V_f \simeq V_g$ ein $\mathbb{K}[x]$-Isomorphismus, dann gilt, für $v \in V$ und $p \in \mathbb{K}[x]$,

$$(\varphi \circ p(f))(v) = \varphi(pv) = p\varphi(v) = (p(g) \circ \varphi)(v).$$

Da dies für alle v richtig ist, folgt

$$\varphi \circ p(f) \circ \varphi^{-1} = p(g),$$

und weil dies wiederum für alle p gilt, also auch für $p = x$, ergibt sich auch

$$\varphi \circ f \circ \varphi^{-1} = g.$$

Als $\mathbb{K}[x]$-lineare Abbildung ist φ insbesondere $\mathbb{K}$-linear (setze $p := \kappa$), liegt also, weil bijektiv, in $\mathrm{Aut}_{\mathbb{K}}(V)$.

□

Das Bild von φ_f bezeichnen wir so:

$$\mathbb{K}[f] := \varphi_f(\mathbb{K}[x]) = \{p(f) \mid p \in \mathbb{K}[x]\}.$$

Interessant ist der Kern dieser Einsetzung:

$$\mathrm{Kern}(\varphi_f) = \{p \mid p(f) = 0\},$$

also die Menge der Polynome, die beim Einsetzen von f die Nullabbildung ergeben. Als Kern eines Ringhomomorphismus ist er ein Ideal, und dieses wird von einem eindeutig bestimmten normierten Polynom erzeugt, das wir als Minimalpolynom von f bezeichnen werden. Der Grund für die Existenz eines solchen Polynoms ist die Tatsache, daß $\mathbb{K}[x]$ ein Hauptidealring ist, und daß man in solchen Ringen eine "Division mit Rest" durchführen kann. Um dies zu beschreiben, benötigen wir einiges über Teilbarkeit in kommutativen Ringen $R \neq \{0\}$ mit Eins und ohne Nullteiler, sogenannte *Integritätsbereiche.* Dabei werden wir bekannte Teilbarkeitseigenschaften der natürlichen und der ganzen Zahlen verallgemeinern, den Zusammenhang zwischen Teilbarkeit und Idealstruktur herstellen und sehen, daß die Eigenschaft einer ganzen Zahl, Primzahl zu sein, sich auf *zweierlei* Weise verallgemeinern läßt.

3.8.2 Definition (Teilbarkeit, ggT, kgV) Sei R ein Integritätsbereich mit Elementen $r, s \in R$ und einer nicht-leeren Teilmenge T. Wir sagen dann

- r *teilt* s, wenn es $t \in R$ gibt mit $rt = s$, kurz:

  $$r \mid s.$$

- r ist *assoziiert* zu s, wenn es eine Einheit $t \in R$ gibt, also ein Element der Einheitengruppe

  $$E(R) := \{x \in R \mid \exists\, y \in R\colon\ xy = 1\},$$

  mit $rt = s$, und das wird wie folgt abgekürzt:

  $$r \sim s.$$

- r ist ein *echter* Teiler von s, wenn folgendes gilt:

  $$r \mid s \ \wedge\ r \notin E(R) \ \wedge\ r \not\sim s.$$

- r heißt *unzerlegbar*, wenn r weder 0 noch Einheit ist und keine echten Teiler besitzt.

- r heißt *prim*, wenn r weder 0 noch Einheit ist und

$$r \mid st \Longrightarrow [\ r \mid s\ \vee\ r \mid t\ ]$$

  richtig ist, d.h. r teilt mit einem Produkt auch mindestens einen Faktor.

- r ist *ein größter gemeinsamer Teiler* von T, wenn folgende beiden Bedingungen erfüllt sind:
  - $\forall\ t \in T\colon r \mid t.$
  - $\forall\ s \in R\colon [\ \forall\ t \in T\colon\ s \mid t\ ] \Rightarrow s \mid r.$

  Dieses wird auch so geschrieben: $r \in ggT(T)$.

- r ist *ein kleinstes gemeinsames Vielfaches* von T, wenn es die folgenden Eigenschaften hat:
  - $\forall\ t \in T\colon\ t \mid r.$
  - $\forall\ s \in R\colon\ [\ \forall\ t \in T\colon\ t \mid s\ ] \Rightarrow r \mid s,$

  kurz: $r \in kgV(T)$.

- Die Elemente von T heißen genau dann *teilerfremd,* wenn

$$ggT(T) = E(R).$$

•

Beispiele für Einheitengruppen sind $E(\mathbb{Z}) = \{1, -1\}$ und $E(\mathbb{K}[x]) = \{\kappa \in \mathbb{K}^*\}$, die Menge der konstanten und vom Nullpolynom verschiedenen $p \in \mathbb{K}[x]$.

Teilbarkeitseigenschaften lassen sich sowohl mit Elementen als auch mit den davon erzeugten Idealen formulieren. Dabei verwenden wir die Kommutativität von R und die Existenz einer Eins, die für Hauptideale (r) die Gleichung

$$(r) = \{sr \mid s \in R\}$$

ergeben. Wie man leicht nachprüft gilt nämlich

3.8.3 Satz *In Integritätsbereichen R gilt für Elemente r, s und nicht-leere Teilmengen T:*

- $r \mid s \iff (s) \subseteq (r),$
- $r \in E(R) \iff (r) = R,$
- $r \sim s \iff [\ r \mid s\ \wedge\ s \mid r\ ] \iff (r) = (s),$
- *r ist echter Teiler von s* $\iff (s) \subset (r) \subset R,$
- $r \in ggT(T) \Longrightarrow ggT(T) = r \cdot E(R),$

- $r \in kgV(T) \Longrightarrow kgV(T) = r \cdot E(R)$.

□

Besonders interessant sind Integritätsbereiche, in denen eine Division mit Rest möglich ist, wie z.B. in $\mathbb{Z}$ und in $\mathbb{K}[x]$:

3.8.4 Definition (euklidischer Bereich) Ist R ein Integritätsbereich, dann heißt $\delta\colon R^* \to \mathbb{N}$ genau dann *euklidische Norm*, wenn folgendes gilt:

- $\forall\ r, s \in R^* :\ \delta(r) \leq \delta(rs)$,
- $\forall\ x \in R, y \in R^*\ \exists\ q, r \in R :\ [x = qy + r]\ \wedge\ [r = 0 \vee (\delta(r) < \delta(y))]$.

Der Ring R (genauer: das Paar (R, δ)) heißt dann *euklidischer Bereich*. •

Eine euklidische Norm auf $\mathbb{Z}$ ist die Betragsfunktion

$$\delta :\ \mathbb{Z}^* \to \mathbb{N},\ z \mapsto |z|.$$

Eine Norm auf dem Polynomring $\mathbb{K}[x]$ ist die Gradfunktion

$$\delta :\ \mathbb{K}[x]^* \to \mathbb{N},\ f \mapsto Grad(f),$$

denn es gilt:

3.8.5 Division mit Rest in $\mathbb{K}[x]$: *Ist $\mathbb{K}$ ein Körper, $f \in \mathbb{K}[x] \ni g \neq 0$, dann gibt es genau ein Paar (q, r) von Polynomen mit der Eigenschaft*

$$f = q \cdot g + r,\ \textit{und}\ [\ r = 0 \vee (Grad(r) < Grad(g))\ ].$$

Beweis: Der Fall $f = 0$ ist trivial, denn $q := r := 0$ erfüllen die Identität $f = qg + r$, und die Annahme $r \neq 0$ ergäbe $q \neq 0$ und damit

$$Grad(r) = Grad(gq) = Grad(g) + Grad(q) \geq Grad(g),$$

also einen Widerspruch.
Sei deshalb $f \neq 0$. Wir beweisen zunächst die Existenz eines Paares (q, r) per Induktion nach $Grad(f)$, danach die Eindeutigkeit.
Sei

$$f = a_0 + \ldots + a_n x^n,\ a_n \neq 0,\ g = b_0 + \ldots + b_m x^m,\ b_m \neq 0.$$

Wir unterscheiden drei Fälle:
Bei $n = 0 < m$ können wir $(q, r) := (0, f)$ setzen.
Falls $n = 0 = m$ wählen wir $(q, r) := (b_0^{-1} f, 0)$.
Ist dagegen $n > 0$, dann betrachten wir die beiden Fälle

- $n < m$: Wir nehmen $q := 0$ und $r := f$.
- Bei $n \geq m$ betrachten wir $f_1 := f - a_n b_m^{-1} x^{n-m} g$ und spalten erneut in zwei Teilfälle auf:

- Bei $f_1 = 0$ funktioniert $(q, r) := (a_n b_m^{-1} x^{n-m}, 0)$.
- Andernfalls ist $Grad(f_1) < Grad(f)$, und die Induktionsannahme liefert die Existenz eines Paare (q_1, r_1) mit

  $$f = q_1 g + a_n b_m^{-1} x^{n-m} g + r_1, \text{ mit } [r_1 = 0 \vee Grad(r_1) < Grad(g)],$$

  wir können also $(q, r) := (q_1 + a_n b_m^{-1} x^{n-m}, r_1)$ verwenden.

Zum abschließenden Beweis der Eindeutigkeit betrachten wir zwei Paare (q, r) und (q_1, r_1) mit $0 \neq f = gq + r = gq_1 + r_1$ und den Ungleichungen für die Grade. Da hierfür gilt $(q - q_1)g = r_1 - r$, folgt aus der Annahme $r \neq r_1$, daß $q \neq q_1$, und damit

$$0 \leq Grad(r - r_1) < Grad(g)$$

gelten müßte, im Widerspruch zu

$$Grad(r - r_1) = Grad((q - q_1)g) = Grad(q - q_1) + Grad(g) \geq Grad(g).$$

□

Die Division mit Rest kann man insbesondere zur sukzessiven Berechnung größter gemeinsamer Teiler endlicher Mengen mit Hilfe der folgenden Methode ermitteln:

3.8.6 Der Euklidische Algorithmus *Ist (R, δ) ein euklidischer Bereich, dann kann man ein Element aus der Menge $ggT(x_0, x_1)$ der größten gemeinsamen Teiler zweier Elemente $x_0, x_1 \in R$ durch sukzessives Dividieren berechnen (der Algorithmus terminiert, weil δ eine Abbildung in $\mathbb{Z}_{\geq 0}$ ist und die Werte $\delta(x_i)$ der Norm der Reste streng monoton fallen): Ist, ohne Einschränkung der Allgemeinheit, $\delta(x_0) \geq \delta(x_1)$, dann dividiert man wie folgt sukzessive und solange, bis der Rest Null wird:*

$$\begin{aligned} x_0 &= q_0 x_1 + x_2 \\ x_1 &= q_1 x_2 + x_3 \\ &\vdots \\ x_{n-1} &= q_{n-1} x_n + x_{n+1} \\ x_n &= q_n x_{n+1} \end{aligned}$$

Es ist dann $x_{n+1} \in ggT(x_0, x_1)$. Liest man nämlich diese Gleichungen von unten nach oben, so ergibt sich, daß x_{n+1} die Elemente $x_n, x_{n-1}, \ldots, x_1, x_0$ teilt. Liest man von oben nach unten, so erhält man, daß jeder Teiler von x_0 und x_1 auch in x_{n+1} aufgeht.
Hat man ein *solches Element aus $ggT(x_0, x_1)$ berechnet, dann ergibt sich die Menge* aller *größten gemeinsamen Teiler mit Hilfe der Einheitengruppe:*

$$ggT(x_0, x_1) = x_{n+1} \cdot E(R).$$

Vor allem aber gilt, daß jedes Ideal in einem euklidischen Bereich ein Hauptideal ist, d.h. von einzelnen Elementen erzeugt werden kann:

3.8.7 Satz *Jeder euklidische Bereich ist ein Hauptidealbereich.*

Beweis: Sei $I \trianglelefteq R$ und (R, δ) ein euklidischer Bereich. Das Nullideal ist trivialerweise ein Hauptideal, sei also $I \neq 0$ und $i_0 \in I$ ein Element $\neq 0$, dessen Norm $\delta(i_0)$ minimal ist unter den Normen der von Null verschiedenen Elemente in I (solche Elemente gibt es, denn δ ist eine Abbildung nach $\mathbb{N}$). Jedes von Null verschiedene $i \in I$ ist dann durch i_0 teilbar, denn die Division von i durch i_0 ergibt

$$i = q \cdot i_0 + r \ \wedge \ [r = 0 \vee (0 \leq \delta(r) < \delta(i_0))].$$

Dies ergibt, wegen der Minimalität der Norm von i_0, $r = 0$ und damit $i = q \cdot i_0$. Daraus folgt die Behauptung.

□

Teilbarkeit läßt sich in Hauptidealbereichen besonders gut mit den von den betrachteten Ringelementen erzeugten Hauptidealen formulieren:

3.8.8 Satz *Ist T nicht leere Teilmenge eines Hauptidealbereichs R, so gilt:*

- $r \in ggT(T) \iff (r) = \sum_{t \in T}(t)$,
- $r \in kgV(T) \iff (r) = \bigcap_{t \in T}(t)$.

Beweis:

i) Zum Beweis der Behauptung zum $ggT(T)$ nehmen wir zunächst an es sei $r \in ggT(T)$.
Dieses Ringelement r ist also Teiler aller $t \in T$ und demnach gilt für die davon erzeugten Ideale $(t) \subseteq (r)$, was

$$\sum_t (t) \subseteq (r)$$

impliziert, denn

$$\sum_t (t) = \{r_0 t_0 + \ldots r_{n-1} t_{n-1} \mid n \in \mathbb{N}, r_i \in R, t_i \in T\}.$$

(Die Idealeigenschaft ist leicht nachzuprüfen.)
Andererseits gilt für dieses r : Jedes $s \in R$, das alle $t \in T$ teilt, ist auch Teiler von r, was folgende Implikation ergibt:

$$\sum_t (t) = (s) \Longrightarrow (r) \subseteq (s).$$

Nun ist aber R als Hauptidealbereich vorausgesetzt, es gilt also $\sum_t (t) = (u)$, für geeignetes $u \in R$, so daß auch

$$(r) \subseteq (u) = \sum_t (t)$$

liefert. Insgesamt haben wir bewiesen, daß

$$\sum_t (t) = (r),$$

wie behauptet.

ii) Die Gültigkeit von $\sum_t(t) = (r)$ liefert $(t) \subseteq (r)$, r teilt also jedes $t \in T$. Hinzukommt, daß $\sum_t(t) \subseteq (s)$ die Implikation $(r) \subseteq (s)$ beinhaltet. Jedes $s \in R$, das alle $t \in T$ teilt, ist demnach ein Teiler von r :

i) zusammen mit ii) zeigt also die behauptete Äquivalenz

$$r \in ggT(T) \iff (r) = \sum_{t \in T} (t).$$

Die Äquivalenz zu $kgV(T)$ kann analog bewiesen werden (Übungsaufgabe!).

□

Für teilerfremde Elemente gilt insbesondere

3.8.9 Hilfssatz *Für nicht leere Teilmengen T von Hauptidealbereichen sind die folgenden Aussagen äquivalent:*

- *T ist teilerfremd,*
- *$\sum_t(t) = (1) = R$,*
- *Es gibt $a_t \in R$ mit $\sum_t a_t t = 1$.*

Beweis: T ist per definitionem teilerfremd, wenn jedes Element r von $ggT(T)$ Einheit ist. Nach dem letzten Satz ist das gleichbedeutend mit $\sum(t) = (1)$. Die beiden ersten Aussagen sind demnach äquivalent. Schließlich bedeutet die dritte Behauptung ganz offensichtlich dasselbe wie die zweite.

□

3.8.10 Satz *Für Elemente $r \neq 0$ in Hauptidealbereichen R sind die folgenden Eigenschaften äquivalent:*

- *r ist unzerlegbar,*
- *(r) ist maximales Ideal (d.h. $(r) \subset (s) \Rightarrow (s) = R$),*
- *(r) ist Primideal (d.h. $\emptyset \neq R \backslash (r)$ ist multiplikativ abgeschlossen),*
- *r ist Primelement.*

Beweis: r ist genau dann unzerlegbar, wenn (r) maximal ist, denn die Nichtexistenz echter Teiler ist (im Hauptidealbereich R!) äquivalent dazu, daß kein s existiert mit $(r) \subset (s) \subset R$.
r ist genau dann prim, wenn (r) Primideal ist, denn r prim bedeutet

$$r \mid st \Rightarrow r \mid s \vee r \mid t.$$

Die Kontraposition hiervon ist

$$r \nmid s \wedge r \nmid t \Rightarrow r \nmid st,$$

und dies ist dasselbe wie

$$s \in R\backslash(r) \wedge t \in R\backslash(r) \Rightarrow st \in R\backslash(r)$$

und bedeutet, daß (r) ein Primideal ist.

Es bleibt zu zeigen, daß r genau dann prim ist, wenn r unzerlegbar ist.

Angenommen, r sei prim und besitze einen echten Teiler t, etw $r = ta$, dann wäre r ein Teiler von a, etwa $a = br$. Das ergäbe $r = tbr$ und damit $(1-tb)r = 0$ bzw. $1 = tb$. t wäre Einheit, sollte aber echter Teiler sein.
Die Umkehrung können wir nach dem bereits Bewiesenen auch anhand der erzeugten Ideale verifizieren. Ist r ein Teiler von st, aber $r \nmid s$, dann haben wir $st \in (r)$ und $s \notin (r)$, also $(\{r, s\}) = R$, so daß $x, y \in R$ existieren mit $xr+ys = 1$. Diese Gleichung multiplizieren wir mit t und erhalten, wenn $st = ar$:

$$t = txr + yst = txr + yar,$$

und damit $t \in (r)$, was zu beweisen war.

□

3.8.11 Beispiele

- Ist $\mathbb{K}$ ein Körper, dann gilt in $\mathbb{K}[x, y] := \mathbb{K}[x][y]$:
  - x ist unzerlegbar,
  - $(x) \subset (x, y) \subset \mathbb{K}[x, y]$, also ist $\mathbb{K}[x, y]$, nach 3.8.10, kein Hauptidealbereich.
- $R := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ ist Integritätsbereich, 3 ist darin unzerlegbar (Nachweis?), wegen $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ aber nicht prim. R ist also *kein* Hauptidealbereich.

◇

Maximalität von Idealen muß also von der Eigenschaft Primideal zu sein bei allgemeinen kommutativen Ringen unterschieden werden. Das zeigt auch der folgende

3.8.12 Satz *Ist R ein kommutativer Ring mit 1, $I \lhd R$, dann ist I*

- *genau dann Primideal, wenn R/I Integritätsbereich ist, das heißt ein vom Nullring verschiedener kommutativer Ring mit Einselement und ohne Nullteiler.*
- *genau dann maximales Ideal, wenn R/I ein Körper ist.*

Beweis: Es gelten die folgenden Ketten von Äquivalenzen:

$$\begin{array}{lcl} I \text{ prim} & \iff & (R/I)^* \text{ komm. Monoid} \neq \{0\} \\ & \iff & R/I \text{ ist Integritätsbereich.} \end{array}$$

und

$$\begin{array}{lcl} I \text{ maximal} & \iff & [\ R\backslash I \neq \emptyset \wedge \forall\ x \in R\backslash I : I + (x) = R\ ] \\ & \iff & [\ R\backslash I \neq \emptyset \wedge \forall\ x \in R\backslash I\ \exists\ i \in I, r \in R\colon\ i + rx = 1_R\ ] \\ & \iff & ((R/I)^*, \cdot\ ) \text{ ist abelsche Gruppe.} \end{array}$$

□

Kehren wir damit zu den eingangs beschriebenen $\mathbb{K}[x]$-Linksmodulstrukturen V_f, zu $f \in \mathrm{End}_{\mathbb{K}}(V)$, zurück. Wir wissen jetzt, daß der Kern des Einsetzungshomomorphismus φ_f ein Hauptideal ist und von einem eindeutig bestimmten normierten Polynom m_f erzeugt wird:

$$\mathrm{Kern}(\varphi_f) = (m_f) \trianglelefteq \mathbb{K}[x],$$

wir nennen es das *Minimalpolynom* von f. Das Minimalpolynom von f ist also *das normierte Polynom m kleinsten Grades mit $m(f) = 0 \in End_{\mathbb{K}}(V)$.*

Ganz allgemein bezeichnet man, für einen R-Linksmodul M, mit

$$\mathrm{Ann}(M) := \{r \in R \mid \forall\ m \in M\colon rm = 0\}$$

das *Annihilatorideal* von M. Das Minimalpolynom erzeugt demnach das Annihilatorideal von V_f. Zur Berechnung des Minimalpolynoms kann man die Tatsache verwenden, daß das Annihilatorideal ganz offensichtlich der Schnitt der *Ordnungsideale* der Elemente von M ist:

$$\mathrm{Ann}(M) = \bigcap_{v \in M} \mathrm{Ord}(v),\ \mathrm{Ord}(v) := \{r \in R \mid rv = 0\}.$$

$v \in M$ heißt *Torsionselement,* wenn $\mathrm{Ord}(v) \neq \{0_R\}$, und M heißt *Torsionsmodul,* wenn jedes Element Torsionselement ist.
Ist E ein Erzeugendensystem von M, dann vereinfacht sich diese Gleichung zu

3.8.13 $$\mathrm{Ann}(M) = \bigcap_{e \in E} \mathrm{Ord}(e).$$

In dem uns interessierenden Beispiel gilt also, für einen $\mathbb{K}$-Vektorraum V mit Basisfolge $\mathcal{B} = (b_0, \ldots, b_{n-1})$:

$$\mathrm{Ann}(V_f) = (m_f) = \bigcap_{i=0}^{n-1} \mathrm{Ord}(b_i).$$

3.8.14 Folgerung *Das Minimalpolynom eines Endomorphismus eines endlichdimensionalen Vektorraums ist das normierte kleinste gemeinsame Vielfache der (normierten) Erzeugenden der Ordnungsideale einer Basis.*

3.8.15 Beispiel f sei der Endomorphismus von $\mathbb{R}^2$, der durch

$$A := \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = M(\mathcal{E}, f, \mathcal{E})$$

dargestellt wird. Wir wollen das Minimalpolynom von f berechnen, unter Verwendung der Standardbasis als Erzeugendensystem. Dazu sind also Erzeugende der Ordnungsideale der Einheitsvektoren zu berechnen.

i) Mit Hilfe von A und von

$$A^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$$

erhalten wir

$$f^0(e_0) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, f^1(e_0) = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, f^2(e_0) = \begin{pmatrix} 7 \\ 15 \end{pmatrix}.$$

Ganz entsprechend folgt

$$f^0(e_1) = e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, f^1(e_0) = \begin{pmatrix} 2 \\ 4 \end{pmatrix}, f^2(e_0) = \begin{pmatrix} 10 \\ 22 \end{pmatrix}.$$

ii) Erzeugende q_i, $i = 0, 1$, der Ordnungsideale $= (e_i)$ der Einheitsvektoren sind die normierten Polynome mit den Koeffizienten a_{ij} aus den Gleichungen

$$a_{00} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + a_{01} \begin{pmatrix} 1 \\ 3 \end{pmatrix} + \begin{pmatrix} 7 \\ 15 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

bzw.

$$a_{10} \begin{pmatrix} 0 \\ 1 \end{pmatrix} + a_{11} \begin{pmatrix} 2 \\ 4 \end{pmatrix} + \begin{pmatrix} 10 \\ 22 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Die Lösung ist

$$a_{00} = a_{10} = -2, a_{01} = a_{11} = -5.$$

iii) Die beiden Ordnungsideale, und damit auch den Annihilator von V_f, werden also von denselben normierten Polynomen erzeugt:

$$\mathrm{Ord}(e_0) = \mathrm{Ord}(e_1) = (-2 - 5x + x^2) = \mathrm{Ann}(\mathbb{R}^2_f).$$

(In der Regel werden die Ordnungsideale der Einheitsvektoren allerdings verschieden sein, so daß man, nach Ermittlung von Erzeugenden der Ordnungsideale noch das normierte kleinste gemeinsame Vielfache der Erzeugenden der Ordnungsideale ermitteln muss!) ◇

Es ist nützlich zu wissen, daß — weit über 3.8.13 hinaus — das Minimalpolynom gleich dem Erzeugnis eines *einzelnen* Ordnungideal ist: $\mathrm{Ann}(M) = \mathrm{Ord}(v)$, für ein geeignetes $v \in M$. Zur Vorbereitung der Herleitung dieses hilfreichen Resultats benötigen wir einige Erweiterungen der bisherigen Überlegungen, u.a. eine interessante Verfeinerung der Überlegungen zur Teilbarkeit (für weitere Details vgl. H. Lüneburg: Vorlesungen über Lineare Algebra).

3.8.16 Hilfssatz *(R, δ) sei ein euklidischer Bereich, $a \in R^*, b \in R$,*

$$T(a,b) := \{t \mid t \text{ teilt } a \text{ und ist zu } b \text{ teilerfremd}\}.$$

Es gilt:

- *$T(a,b)$ ist nicht leer, denn $1 \in T(a,b)$.*
- *Für $t \mid u \in T(a,b)$ gilt $t \in T(a,b)$.*
- *Für $u, v \in T(a,b)$ gilt $kgV(u,v) \subseteq T(a,b)$.*
- *Für $u \in T(a,b)$ gilt $\delta(u) \leq \delta(a)$.*
- *Es gibt Elemente $r \in T(a,b)$ mit maximaler Norm $\delta(r)$.*
- *Ist r ein solches Element mit maximaler Norm und $u \in T(a,b)$, dann haben alle Elemente in $kgV(r,u)$ dieselbe Norm $\delta(r)$, für alle $u \in T(a,b)$, die r teilen.*
- *Für $r \in ggT(a,b)$ gilt $T(a,b) = T(a \cdot r^{-1}, r)$.*

Beweis: Übungsaufgabe.

Wendet man das letzte item des Hilfsatzes wiederholt an, so ergibt sich nach endlich vielen Schritten eine Element maximaler Norm. Zum Beispiel bekommen wir

$$T(1080, 42) = T(180, 6) = T(30, 6) = T(5, 6) = T(5, 1),$$

also ist $5 \in T(1080, 42)$ ein Element maximaler Norm.

3.8.17 Hilfssatz *(R, δ) sei wieder ein euklidischer Bereich, $a, b \in R$, beide $\neq 0$. Für $t \in ggT(a,b)$ seien*

$$A \in T\left(a, \frac{b}{t}\right), \; B \in T\left(b, \frac{a}{t}\right)$$

Elemente maximaler Norm, und $T \in ggT(A,B)$. Es gilt dann

- *$ggT\left(A, \frac{B}{T}\right) = ggT\left(B, \frac{A}{T}\right) = E(R)$.*
- *$kgV(a,b) = kgV(A,B)$.*
- *$ggT\left(\frac{a}{A}, \frac{b}{B}T\right) = ggT\left(\frac{b}{B}, \frac{a}{A}T\right) = E(R)$.*

Beweis: Übungsaufgabe.

Mit Hife dieser Ergebnisse kann man das folgende Resultat beweisen:

3.8.18 Satz *Ist M ein R-Linksmodul über dem euklidischen Ring R, mit Elementen $u, v \in M$, für die gilt*

$$(a) := Ord(u) \neq Ord(v) = (b),$$

sowie t, A, B, T wie oben und $B' := \frac{B}{T}$, so gilt, für

$$w := \frac{a}{A} \cdot u + \frac{b}{B'} \cdot v$$

die Gleichung

$$Ord(w) = kgV(a, b) = Ord(u) \cap Ord(v).$$

Beweis: vgl. Lüneburg.

Hiermit kann man sukzessive — für endlichdimensionale Vektorräume V — ein *einzelnes* Element w berechnen mit

3.8.19 $$(m_f) = \mathrm{Ann}(V_f) = \mathrm{Ord}(w).$$

Auch das charakteristische Polynom $p_f = \det(f - x \cdot \mathrm{id}_V)$ liegt im Annihilatorideal, es gilt nämlich

3.8.20 Der Satz von Cayley-Hamilton *Für das charakteristische Polynom eines Endomorphismus f eines endlichdimensionalen Vektorraums gilt*

$$p_f(f) = 0 \in End_{\mathbb{K}}(V).$$

Beweis: Wir betrachten, für ein $v \neq 0$, die Vektoren $f^i(v)$ und verwenden die Existenz eines kleinsten Exponenten i, für den

$$\mathcal{B}_U := (b_0 := f^0(v), \ldots, b_{i-1} := f^{i-1}(v))$$

eine Folge linear unabhängiger Vektoren ist, $f^0(v), \ldots, f^i(v)$ dagegen eine Folge linear abhängiger, etwa

$$-f^i(v) + \sum_{j=0}^{i-1} \kappa_j f^j(v).$$

Offenbar ist

$$U :=\ll b_0 := f^0(v), \ldots, b_{i-1} := f^{i-1}(v) \gg$$

ein f-invarianter Unterraum, $f(U) \subseteq U$. Die Einschränkung $f \downarrow U$ ist also ein Endomorphismus von U. Er wird durch die folgende Matrix dargestellt:

$$A := \begin{pmatrix} 0 & 0 & \ldots & \ldots & 0 & \kappa_0 \\ 1 & 0 & \ldots & \ldots & 0 & \kappa_1 \\ 0 & 1 & \ldots & \ldots & 0 & \kappa_2 \\ \vdots & \vdots & \ddots & \ldots & \vdots & \vdots \\ 0 & 0 & \ldots & \ldots & 0 & \kappa_{i-2} \\ 0 & 0 & \ldots & \ldots & 1 & \kappa_{i-1} \end{pmatrix}.$$

Das charakteristische Polynom von $f \downarrow U$ ist also

$$p_{f\downarrow U} = \det(A - xE) = (-1)^i\Big(-x^i + \sum_{j=0}^{i-1} \kappa_j x^j\Big).$$

Dies impliziert

$$p_{f\downarrow U}(f)(v) = \pm\Big(-f^i(v) + \sum_{j=0}^{i-1} \kappa_j f^j(v)\Big) = 0.$$

Wählen wir eine an U angepaßte Basisfolge von V,

$$\mathcal{B} = (b_0, \ldots, b_{i-1}, b_i, \ldots, b_{n-1}),$$

dann ist

$$M(\mathcal{B}, f, \mathcal{B}) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix},$$

also, nach 3.7.11, $p_f = p_A \cdot p_C = p_{f\downarrow U} \cdot p_C$ und damit

$$p_f(f)(v) = p_{f\downarrow U}(f)(v) \cdot p_C(f)(v) = 0.$$

Da dies für alle v richtig ist, folgt die Behauptung.

□

Eine direkte Folgerung ist ein Ausdruck für die Inverse einer regulären Matrix A in den Potenzen von A und den Koeffizienten des charakteristischen Polynoms. Ist $p_A = \sum_{i=0}^{n-1} \kappa_i x^i$, dann folgt, wegen $p_A(A) = 0$ und $\kappa_0 = \det(A)$,

3.8.21
$$A^{-1} = -\frac{1}{\det(A)} \sum_{i=1}^{n-1} \kappa_i A^{i-1}.$$

Eine weitere Anwendung des Satzes von Cayley-Hamilton ist

3.8.22 Satz *Jeder Endomorphismus eines endlichdimensionalen reellen Vektorraums $V \neq \{0\}$ besitzt einen invarianten Unterraum der Dimension 1 oder 2.*

Beweis: Weil ein Polynom mit reellen Koeffizienten mit einer komplexen Wurzel $z \in \mathbb{C}$ auch die konjugiert komplexe Zahl $\bar{z}$ als Wurzel hat, ist das charakteristische Polynom eines Endomorphismus von V ein Polynom aus Linearfaktoren (zu den reellen Wurzeln) und quadratischen Faktoren (zu den Paaren $z, \bar{z}$ nicht reeller Wurzeln):

$$p_f = \pm \prod_{i=0}^{r-1} (x - \lambda_i) \cdot q_0 \cdots q_{t-1},$$

mit $q_i = x^2 + \alpha_i x + \beta_i$, und $\alpha_i^2 - 4\beta_i < 0$.

i) Ist $r > 0$, dann ist λ_0 Eigenwert mit einem Eigenvektor v_0, es gibt also mit $\langle v_0 \rangle$ einen invarianten Unterraum der Dimension 1.

ii) Ist $r = 0$, $0 \neq v \in V$, so gilt

$$0 = p_f(f)(v) = (q_0(f) \circ \ldots \circ q_{t-1}(f))(v).$$

Es gibt also $i \in t$ mit

$$(q_i(f) \circ \ldots \circ q_{t-1}(f))(v) = 0,\ w := (q_{i+1}(f) \circ \ldots \circ q_{t-1}(f))(v) \neq 0.$$

$U := \langle w, f(w)\rangle$ ist ein invarianter Unterraum, denn

$$0 = q_i(f)(w) = (f^2 + \alpha_i f + \beta_i)(w)$$

ergibt

$$f(f(w)) = f^2(w) = -\alpha_i f(w) - \beta_i w \in U.$$

□

Hieraus kann man herleiten (Übungsaufgabe), daß jeder Endomorphismus eines endlichen reellen Vektorraums bzgl. einer geeigneten Basis durch eine Matrix dargestellt wird, die unterhalb einer Hauptdiagonalen aus ein- und zweireihigen Kästchen nur Nullen enthält.

Der Satz von Cayley-Hamilton impliziert auch

3.8.23 Folgerung *Das Minimalpolynom m_f ist ein Teiler des charakteristischen Polynoms p_f.*

Man kann also in manchen Situationen vom charakteristischen Polynom auf das Minimalpolynom schließen. Sei beispielsweise

$$p_f = (-1)^n x^n,$$

etwa im Fall, daß

$$A = \begin{pmatrix} 0 & * & \ldots & * \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & * \\ 0 & \ldots & \ldots & 0 \end{pmatrix}.$$

Für solche Matrizen gibt es Exponenten m mit $A^m = 0$. Matrizen A mit dieser Eigenschaft bzw. die entsprechenden linearen Abbildungen, heißen *nilpotent.* Das Minimalpolynom hat dann die Form x^t, mit einem $t \leq n$.
Ein weiterer Fall, indem man, vom charakteristischen Polynom ausgehend, Aussagen über das Minimalpolynom gewinnen kann, sind die *Jordan-Matrizen,*

$$A = \begin{pmatrix} \lambda & 1 & \ldots & \ldots & 0 \\ 0 & \lambda & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \lambda & 1 \\ 0 & \ldots & \ldots & 0 & \lambda \end{pmatrix}.$$

Ihr charakteristisches Polynom ist $(\lambda - x)^n$, das Minimalpolynom also von der Form $(\lambda - x)^m$, mit $\leq n$.

Aufgabe 3.8.1
$v \in V_f$ ist genau dann ein Torsionselement, wenn der Unterraum

$$\sum_{n\in\mathbb{N}} \mathbb{K} f^n(v)$$

endlich erzeugbar ist.

3.9 Elementarteiler, die rationale Normalform

Wir suchen nach einem weiteren — am Minimalpolynom ablesbaren — Kriterium für die Isomorphie von V_f und V_g. Als ein Hilfsmittel verwenden wir eine Verallgemeinerung des Begriffes direkter Summand, indem wir einen Untermodul U eines R-Linksmoduls M als *rein* bezeichnen, wenn für alle $m \in M, r \in R$ gilt

$$rm \in U \Longrightarrow \exists\, u \in U\colon\ rm = ru.$$

3.9.1 Hilfssatz *Sei R ein euklidischer Bereich, M ein R-Linksmodul mit Untermoduln U und V, mit $U \subseteq V$. Dann gilt:*

- *Ist U direkter Summand, etwa $M = U \oplus W$, dann sind U und W reine Untermoduln von M.*
- *Ist U rein in M, V/U rein in M/U, dann ist V ebenfalls reiner Untermodul von M.*
- *Ist $Ann(M) \neq \{0\}$, sowie $u \in M$ mit $Ord(u) = Ann(M)$, dann ist Ru reiner Untermodul von M.*
- *Ist U rein, $m \in M$ mit $Ord(m+U) = (r)$, dann gibt es $u \in U$ mit $rm = ru$, und $Ord(m-u) = (r)$ sowie $U + Rm = U \oplus R(m-u)$.*

Beweis:

i) $M = U \oplus W$ impliziert, für jedes $m \in M$ die Existenz von $u \in U$ und $w \in W$ mit $m = u + w$. Es folgt $rm = ru + rw$ und damit, falls $rm \in U$,

$$rw = rm - ru \in U \cap W = \{0\},\ \text{also } rm = ru.$$

ii) $rm \in V$ impliziert, wegen der Reinheit von V/U in M/U, für die Nebenklasse von U : $rm + U \in V/U$, also

$$rm + U = r(m + U) = r(v + U),$$

für geeignete $v \in V$. Hierfür gilt aber $r(m-v) = rm - rv \in U$, also $r(m-v) = ru$, für geeignete $u \in U$. Diese Elemente haben die gewünschte Eigenschaft:

$$rm = rv + ru = r(v + u),$$

denn $u + v \in V$.

iii) Ist $rm \in Ru$, so gibt es $s \in R$ mit $rm = su$. Ist jetzt $\mathrm{Ann}(M) = \mathrm{Ord}(u) = (x)$, dann gilt $x \neq 0$, und wir erhalten, wenn $y \in ggT(r, u)$,

$$\frac{x}{y}su = \frac{x}{y}rm = x\frac{r}{y}m = 0,$$

also

$$\frac{x}{y}s \in \mathrm{Ord}(u) = (x),\ \text{etwa } \frac{x}{y}s = zx.$$

Dies impliziert $s = zy$, also $s \in z \cdot ggT(r, x)$ und damit $s = z(r\alpha + x\beta)$, für geeignete α, β. Es folgt

$$rm = su = z(r\alpha u + x\beta u) = r(z\alpha u).$$

Ru ist also tatsächlich ein reiner Untermodul.

iv) Sei $m \in M$ mit $\mathrm{Ord}(m + U) = (r)$, wir betrachten rm. Die Reinheit von U liefert die Existenz von $u \in U$ mit $rm = ru$.
Hierfür gilt $\mathrm{Ord}(m - u) = (r)$: Jedes $s \in \mathrm{Ord}(m - u)$ erfüllt $s(m - u) = 0$, also $sm = su \in U$, so daß auch $s \in \mathrm{Ord}(m + U) = (r)$. Die Umkehrung $(r) \subseteq \mathrm{Ord}(m - u)$ ist trivial, wegen $rm = ru$.
Jetzt beweisen wir, daß die Summe $U + (m - u)$ direkt ist: Sei $x \in U \cap (m - u)$, etwa $x = s[m-u] = \tilde{u}$. Wegen $sm - su \in U$ folgt $sm \in U$, also $s \in \mathrm{Ord}(m+U) = \mathrm{Ord}(m - u)$. Es folgt $\tilde{u} = 0$ und damit $x = 0$. Der Schnitt ist tatsächlich $\{0\}$.
Die Gleichheit $U + Rm = U \oplus R(m - u)$ ist leicht einzusehen, womit alles bewiesen ist.

□

Nach diesen Vorbemerkungen über die Reinheit von Untermoduln kommen wir jetzt zu den Elementarteilern:

3.9.2 Satz *Sei R weiterhin ein euklidischer Bereich, M ein R-Linksmodul, mit $Ann(M) \neq \{0\}$, und, für $m_1, \ldots, m_s \in M$, $U_0 := \{0\}$, $U_i := \sum_{j=1}^{i} Rm_j$, $i > 0$. Es gelte*

$$Ann(M/U_{i-1}) = Ord(m_i) = Ord(m_i + U_{i-1}).$$

Dann sind die U_i, $i = 1, \ldots, s$, reine Untermoduln und $U_s = \oplus_{j=1}^{s} Rm_j$. Darüberhinaus teilen die normierten Erzeuger r_i der Ordnungsideale der m_i einander:

$$(r_i) = Ord(m_i) \Longrightarrow r_{i+1} \mid r_i.$$

Beweis:

Zunächst zur Teilbarkeitsrelation zwischen den r_i. Wegen $r_i \in \mathrm{Ord}(m_i) = \mathrm{Ann}(M/U_{i-1})$ gilt $r_i M \subseteq U_{i-1} \subseteq U_i$ und damit $r_i \in \mathrm{Ann}(M/U_i) = \mathrm{Ord}(m_{i+1}) = (r_{i+1})$, was r_{i+1} als Teiler von r_i ausweist.

Die Reinheit der $U_i, i = 1, \ldots, U_s$ und die Behauptung, daß U_s *direkte* Summe der Rm_i sei, zeigen wir per Induktion nach s :

Für $s = 1$ ist die Summe natürlich direkt, $U_1 = Rm_1$. Die Reinheit von U_1 ergibt sich aus dem dritten Punkt von 3.9.1:

$$0 \neq \mathrm{Ann}(M) = \mathrm{Ann}(M/U_0) = \mathrm{Ord}(m_1)$$

impliziert die Reinheit von $Rm_1 = U_1$.

Sei jetzt $s > 1$, die Untermoduln $U_1, \ldots, U_{s-1}$ seien rein, und $U_{s-1} = \oplus_{i=1}^{s-1} Rm_i$.
Die Reinheit von ergibt sich wie folgt: Wegen $U_s/U_{s-1} = Rm_s + U_{s-1}$ ist

$$\mathrm{Ann}(U_s/U_{s-1}) = \mathrm{Ord}(m_s + U_{s-1}) = \mathrm{Ord}(m_s) = (r_s) \neq 0,$$

was, nach dem dritten Item von 3.9.1, die Reinheit von $R(m_s+U_{s-1})$ impliziert. U_s/U_{s-1} ist demnach rein in M/U_{s-1}. Der zweite Punkt aus 3.9.1 ergibt daraus die behauptete Reinheit von U_s.
Um schließlich zu zeigen, daß U_s wie angegeben direkte Summe ist, verwenden wir die Reinheit von U_{s-1} und

$$\mathrm{Ord}(m_s + U_{s-1}) = \mathrm{Ord}(m_s) = (r_s).$$

Dies impliziert nämlich, nach dem vierten Punkt von 3.9.1, die Existenz von $u \in U_{s-1}$ mit $U_{s-1} \oplus R(m_s - u)$, und diese direkte Summe gleicht $U_{s-1} \oplus Rm_s$. Damit ist alles bewiesen.

□

Tatsächlich kann man zeigen, daß endlich erzeugbare Torsionsmoduln Erzeugende diser Form besitzen. Die entscheidende Überlegung zu einer sukzessiven Berechnung solcher Elemente ist

3.9.3 Hilfssatz *Ist — unter den Voraussetzungen des letzten Satzes, d.h. nach Ermittlung von $m_1, \ldots, m_s$ — $m \in M$ ein weiteres Element, und gilt $Ord(m + U_s) = (r)$, dann teilt r alle r_i und $rm = \sum_i s_i m_i$, für geeignete $s_i \in R$. r teilt diese Koeffizienten, und*

$$u := \sum_i \frac{s_i}{r} m_i$$

genügt den Gleichungen

$$Ord(m - u) = (r),\ U_s + Rm = U_s \oplus R(m - u).$$

Beweis: Wegen $\mathrm{Ord}(m + U_s) = (r)$ gilt $rm \in U_s$, also $rm = \sum_{j=1}^{s} s_j m_j$, mit geeigneten $s_j \in R$. Die Teilbarkeit von r_i durch r folgt so: Weil $r_s \mid r_i$, etwa $r_s \cdot t_i = r_i$, gilt

$$r_i m = t_i r_s m \in U_s,$$

so daß $r_i \in \mathrm{Ord}(m + U_s) = (r)$, also $r \mid r_i$.
Dies liefert uns

$$r_i \cdot m = \frac{r_i}{r} \cdot r \cdot m = \sum_j \frac{r_i}{r} s_j m_j.$$

Mit

$$U_s = U_{i-1} \oplus Rm_i \oplus \ldots \oplus Rm_s,\ r_i \in \mathrm{Ord}(m + U_{i-1})$$

ist $r_i m \in U_{i-1}$, also $\frac{r_i}{r} s_j m_j = 0$, für $j = i, \ldots, s$, woraus wir auf

$$\frac{r_i}{r} s_i \in \mathrm{Ord}(m_i) = (r_i)$$

schließen können, was die Teilbarkeit von s_i durch r ergibt.
Wir können demnach folgendes Element definieren:

$$u := \sum_j \frac{s_j}{r} m_j.$$

Es gilt hierfür $rm = ru$, und die letzte Behauptung über die Direktheit der Summe folgt mit Punkt iv) aus 3.9.1.

□

Man kann hiermit und einigen weiteren Überlegungen (vgl. Lüneburg) das folgende Resultat beweisen:

3.9.4 Satz *Ist M ein endlich erzeugbarer R-Modul über einem euklidischen Bereich R mit $Ann(M) \neq (0)$, so gibt es $m_1, \ldots, m_s \in M$ mit*

$$M = \oplus_{i=1}^{s} Rm_i,$$

und die Erzeugenden r_i der Ordnungsideale $R \neq Ord(m_i) = (r_i) \neq 0$ genügen den Teilbarkeitsbedingungen

$$r_{i+1} \mid r_i, i = 1, \ldots, s-1.$$

Diese r_i sind, bis auf Assoziiertheit, eindeutig bestimmt, sie heißen die Elementarteiler *von M (bzw. von f, wenn $M = V_f$) und bestimmen M bis auf R-Isomorphie.*

Für unser Beispiel V_f bedeutet dies die Existenz einer Basisfolge $\mathcal{B}$, bezüglich der f durch eine Matrix dargestellt wird, die, bis auf Nullen, aus den *Begleitmatrizen*

$$C(r_i) := \begin{pmatrix} 0 & 0 & \ldots & 0 & -\kappa_0 \\ 1 & 0 & \ldots & 0 & -\kappa_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & -\kappa_{m-2} \\ 0 & 0 & \ldots & 1 & -\kappa_{m-1} \end{pmatrix}, \text{ wenn } r_i = \sum_{j=0}^{m-1} \kappa_i x^i,$$

der Elementarteiler besteht:

$$M(\mathcal{B}, f, \mathcal{B}) = \begin{pmatrix} C(r_1) & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & C(r_s) \end{pmatrix}.$$

Diese Matrix heißt die *rationale Normalform* der f darstellenden Matrizen.

3.9.5 Beispiel Betrachten wir das Beispiel aus Lüneburgs Vorlesung:

$$f: \mathbb{K}^4 \to \mathbb{K}^4, e_i \mapsto e_0 + \ldots + e_3,$$

also

$$M(\mathcal{E}, f, \mathcal{E}) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Wegen der linearen Unabhängigkeit von e_i und $f(e_i)$ sowie $f^2(e_i) = 4f(e_i)$ gilt $\mathrm{Ord}(e_i) = (x^2 - 4x)$ und damit $m_f = r_1 = x^2 - 4x$. Als Vektor m_1 können wir deshalb e_0 wählen, und der erzeugte Unterraum ist

$$U_1 = \mathbb{K}[x]m_1 = \mathbb{K}[x]e_0 = \mathbb{K}e_0 + \mathbb{K}(e_0 + \ldots + e_3).$$

In diesem Unterraum liegen weder e_1, noch e_2, noch e_3. Nehmen wir etwa $m := e_1$ zu m_1 hinzu und wenden wir darauf 3.9.3 an. Wegen $f(e_1) \in U_1$ ist $\mathrm{Ord}(e_1 + U_1) = (x) = (r_2)$. Wir erhalten also (vgl. 3.9.3) $rm = xm_1$, so daß sich $u = m_1$ und damit $m - u = e_0 - e_1$ ergibt, also $m_2 = e_0 - e_1$ und

$$U_2 = U_1 + \mathbb{K}[x](e_0 - e_1) = \mathbb{K}e_0 + \mathbb{K}(e_0 + e_1 + e_2 + e_3) + \mathbb{K}(e_0 - e_1).$$

Nehmen wir schließlich zu m_1, m_2 noch $m := e_3$ hinzu. Wir erhalten ganz analog $m_3 = e3 - e_1$, so daß sich

$$U_3 = \mathbb{K}e_0 + \mathbb{K}(e_0 + \ldots + e_3) + \mathbb{K}(e_3 - e_1)$$

als Zerlegung von V_f ergibt, mit den Elementarteilern

$$r_1 = x^2 - 4x,\ r_2 = x,\ r_3 = x.$$

Die Begleitmatrizen sind

$$C(r_1) = \begin{pmatrix} 0 & 0 \\ 1 & 4 \end{pmatrix},\ C(r_2) = C(r_3) = \begin{pmatrix} 0 \end{pmatrix}.$$

Insgesamt ergibt sich also, daß bezüglich der Basisfolge

$$\mathcal{B} := (e_0, e_0 + e_1 + e_2 + e_3, e_1 - e_0, e_2 - e_1)$$

wird f also durch die folgende Matrix dargestellt:

$$M(\mathcal{B}, f, \mathcal{B}) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$\diamond$

3.10 Die Jordansche Normalform

Eine noch übersichtlichere und ebenfalls sehr anwendungsrelevante Normalform einer darstellenden Matrix eines linearen Endomorphismus f ist die Jordansche, benannt nach Camille Jordan. Bevor wir diese herleiten können, müssen aber noch einige wichtige Sätze aus der Teilbarkeitstheorie bereitgestellt werden.
Der erste dieser Sätze ist der Chinesische Restesatz, dessen mengentheoretische Grundlage die folgende Aussage über die simultane Lösung von Äquivalenzen ist:

3.10.1 Chinesischer Restesatz, mengentheoretische Version *$R_0, \ldots, R_{t-1}$ seien Äquivalenzrelationen auf einer Menge M. Die Abbildung*

$$\varphi\colon M \to \times_{i\in t} M_{R_i}, m \mapsto ([m]_{R_0}, \ldots, [m]_{R_{t-1}})$$

ist genau dann surjektiv, wenn für alle $i \in t$ gilt

$$(R_0 \cap \ldots \cap R_{i-1}) \circ R_i = M \times M.$$

Die von φ induzierte Äquivalenzrelation auf M ist

$$R_\varphi = \bigcap_{i\in t} R_i.$$

Beweis: Ist φ surjektiv, $(m', m'') \in M \times M$, dann gibt es zu jedem $i \in t$ Elemente $m \in M$ mit

$$\varphi(m) = ([m']_{R_0}, \ldots, [m']_{R_{i-1}}, [m'']_{R_i}, \ldots, [m'']_{R_{t-1}}).$$

Es gilt also

$$(m', m) \in R_0 \cap \ldots \cap R_{i-1} \ \wedge \ (m, m'') \in R_i,$$

d.h.

$$(m', m'') \in (R_0 \cap \ldots \cap R_{i-1}) \circ R_i,$$

also

$$(R_0 \cap \ldots \cap R_{i-1}) \circ R_i = M \times M.$$

Sei umgekehrt

$$\forall\, i \in t : (R_0 \cap \ldots \cap R_{i-1}) \circ R_i = M \times M.$$

Wir beweisen die Surjektivität von φ per Induktion nach t.

Ist $t = 1$, dann ist φ die kanonische Abbildung der $m \in M$ auf ihre Äquivalenzklassen, also surjektiv.

Für $t \geq 2$ definieren wir, zu $i \in t - 1$, die Abbildung

$$\varphi_i(m) = ([m]_{R_0}, \ldots, [m]_{R_{i-1}}).$$

$\varphi_1, \ldots, \varphi_{t-1}$ sind dann nach Induktionsannahme surjektiv, und wir haben die Surjektivität von φ_t zu beweisen. Seien deshalb $m_0, \ldots, m_{t-1} \in M$. Wegen der Surjektivität von φ_{t-1} gibt es $x \in M$ mit

$$\varphi_{t-1}(x) = ([m_0]_{R_0}, \ldots, [m_{t-2}]_{R_{t-2}}).$$

Wegen

$$(x, m_{t-1}) \in (R_0 \cap \ldots \cap R_{t-2}) \circ R_{t-1} = M \times M$$

gibt es $y \in M$ mit

$$(x, y) \in R_0 \cap \ldots \cap R_{t-2} \ \wedge \ (y, m_{t-1}) \in R_{t-1}.$$

Hierfür gilt

$$\varphi(y) = \varphi_t(y) = ([y]_{R_0}, \ldots, [y]_{R_{t-1}})$$
$$= ([x]_{R_0}, \ldots, [x]_{R_{t-2}}, [m_{t-1}]_{R_{t-1}}) = ([m_0]_{R_0}, \ldots, [m_{t-1}]_{R_{t-1}}).$$

φ ist also tatsächlich surjektiv.
Die Aussage über R_φ ist offensichtlich gültig.

□

Für die Anwendung dieses Satzes auf die Teilbarkeit in Ringen R verwenden wir die von Idealen $I \trianglelefteq R$ induzierten Äquivalenzrelationen R_I, definiert durch

$$[r]_{R_I} = [s]_{R_I} :\Longleftrightarrow \quad r - s \in I.$$

Schließlich sei noch daran erinnert, daß das Produkt IJ zweier Ideale $I, J \trianglelefteq R$ das von den Elementen $ij, i \in I, j \in J$ *erzeugte* Ideal bezeichnet, während $I + J$ aus den Summen $i + j$, mit $i \in I, j \in J$ *besteht.*

3.10.2 Hilfssatz *Für Ideale I, J sowie $I_j, j \in t$, eines Rings R mit Einselement gilt*

- $R_I \circ R_J = R \times R \iff I + J = R.$
- $I_j + J = R$, *für alle* $j \in t$, *impliziert*

$$I_0 \cdots I_{t-1} + J = I_0 \cap \ldots \cap I_{t-1} + J = R.$$

Beweis:

i) Ist $R_I \circ R_J = R \times R$, dann liegt, zu jedem $r \in R$, $(r, 0)$ in $R_I \circ R_J$. Es gibt also $s \in R$ mit $(r, s) \in R_I$ und $(s, 0) \in R_J$ bzw. $r - s \in I$ und $s - 0 \in J$. Hierfür ist aber

$$r - s + s - 0 = r \in I + J.$$

Ist umgekehrt $I + J = R$, $r, s \in R$, $1 = i + j$, so gilt, für $t := rj + si$:

$$r - t = r(1 - j) - si = ri - si \in I,$$

sowie

$$t - s = rj + s(i - 1) = rj + sj \in J.$$

Wir haben demnach $(r,t) \in R_I$ und $(t,s) \in R_J$, so daß sich $(r,s) \in R_I \circ R_J$, d.h. $R_I \circ R_J = R \times R$ ergibt.

ii) Wegen $I_0 \cdots I_{t-1} \subseteq I_0 \cap \ldots \cap I_{t-1}$ genügt der Nachweis von $I_0 \cdots I_{t-1} + J = R$. Wir verwenden Induktion nach t. Der Fall $t = 1$ ist trivial.
Ist $t > 1$, dann gilt nach Induktionsannahme

$$I_0 \cdots I_{t-2} + J = R.$$

Es gibt also $x \in I_0 \cdots I_{t-2}$ und $y \in J$ mit $x + y = 1$. Nach Voraussetzung ist auch $I_{t-1} + J = R$, so daß auch $v \in I_{t-1}$ und $w \in J$ existieren mit $v + w = 1$. Multiplikation dieser beiden Gleichungen liefert

$$1 = (x+y)(v+w) = \underbrace{xv + xw}_{\in\ I_0 \cdots I_{t-1}} + \underbrace{yv + yw}_{\in\ J} \ \in\ I_0 \cdots I_{t-1} + J.$$

Dies impliziert was zu zeigen war:

$$I_0 \cdots I_{t-1} + J = R,$$

denn die linke Seite ist ja ein Ideal.

□

3.10.3 Der Chinesische Restesatz, ringtheoretische Version *Ist R ein Ring mit Einselement und Idealen $I_0, \ldots, I_{t-1} \trianglelefteq R$. Die Abbildung*

$$\varphi\colon R \to \times_{i \in t} R/I_i,\ r \mapsto (r + I_0, \ldots, r + I_{t-1})$$

der Ringelemente auf die Folge ihrer Nebenklassen ist ein Ringhomomorphismus (wenn $\times_{i \in t} R/I_i$ mit punktweiser Addition und Multiplikation versehen ist). Sein Kern ist

$$\mathrm{Kern}(\varphi) = \bigcap_{i \in t} I_i,$$

und φ ist genau dann surjektiv, wenn die Ideale paarweise teilerfremd sind:

$$\forall\ i, j \in t, i \neq j :\ I_i + I_j = R.$$

Diese Abbildung φ ist also genau dann ein Ringisomorphismus, *wenn der Schnitt der Ideale das Nullideal ist und je zwei von ihnen teilerfremd sind.*

Beweis: Die Homomorphieeigenschaft und die Aussage über den Kern sind klar. Ist φ surjektiv, $i, j \in t, i \neq j$, dann ist auch φ_{ij}, definiert durch $\varphi_{ij}(m) := ([m]_{R_i}, [m]_{R_j})$, eine surjektive Abbildung. Nach 3.10.1 ist also $R_{I_i} \circ R_{I_j} = R \times R$, und nach 3.10.2 ergibt sich daraus, wie behauptet, $I_i + I_j = R$.
Gilt umgekehrt, für alle $i, j \in t, i \neq j$, $I_i + I_j = R$, dann ist, nach 3.10.2, $I_0 \cap \ldots \cap I_{i-1} + I_i = R$. Mit 3.10.2 folgt daraus die Behauptung.

□

Hier ist eine Anwendung auf die Interpolation von Polynomen:

3.10.4 Anwendung Sind $\kappa_i \in \mathbb{K}, i \in n$, paarweise verschieden, $\lambda_i \in \mathbb{K}, i \in n$ beliebig, dann gibt es genau ein Polynom $p \in \mathbb{K}[x]$ mit

$$P(\kappa_i) = \lambda_i, i \in n, \text{ und } p = 0 \text{ oder } \mathrm{Grad}(p) < n.$$

Um dies zu zeigen verwenden wir, daß die Polynome $p_i := x - \kappa_i, i \in n$ teilerfremd sind. Die Abbildung

$$\varphi\colon \mathbb{K}[x] \to \times_i \mathbb{K}[x]/(p_i), p \mapsto (\ldots, p + (p_i), \ldots)$$

ist also nach dem Chinesischen Restesatz surjektiv. Es gibt demnach Polynome p mit

$$\varphi(p) = (\ldots, \lambda_i + (p_i), \ldots).$$

Hierfür gilt $p + (p_i) = \lambda_i + (p_i)$, was beinhaltet, daß $p - \lambda_i$ durch p_i teilbar ist, und das wiederum bedeutet $P(\kappa_i) = \lambda_i$.

Darüberhinaus ist der Kern dieser Abbildung

$$\mathrm{Kern}(\varphi) = \bigcap_i \big(p_i\big) = (r),$$

mit $r := \prod_i p_i \in \mathrm{kgV}\{p_i \mid i \in n\}$, also, nach dem Homomorphiesatz

$$\mathbb{K}[x]/\left(\prod_i [x - \kappa_i]\right) \simeq \times_i \big[\mathbb{K}[x]/(x - \kappa_i)\big].$$

Die linke Seite besteht aber — neben der Restklasse des Nullpolynoms — aus den Nebenklassen der Elemente vom Grad $< n$. Es gibt also genau ein Polynom p, welches das Nullpolynom oder vom Grad $< n$ ist, mit $P(\kappa_i) = \lambda_i$, für alle $i \in n$.

Die Berechnung eines solchen Polynoms p erfolgt mit der *Lagrangeschen Interpolationsformel.* Wir bilden das Produkt $r := \prod_i [x - \kappa_i]$ und setzen $r_i := r/[x - \kappa_i]$. Es gilt für die entsprechenden Polynomabbildungen $R_i(\kappa_i) \neq 0$, so daß wir $s_i := r_i/R_i(\kappa_i)$ setzen können. Das Polynom $p := \sum_i \lambda_i s_i$ hat die gewünschten Eigenschaften:

$$P(\kappa_j) = \sum_i \lambda_i S(\kappa_j) = \lambda_j.$$

Eine weitere Anwendung bietet sich in der Darstellung ganzer Zahlen durch Folgen von Resten modulo Primzahlen an:

3.10.5 Anwendung Sind $p_0, \ldots, p_{t-1}$ paarweise verschiedene Primzahlen, dann gibt es, zu vorgegebenen natürlichen Zahlen $r_i \in [0, p_i), i \in t$, genau eine natürliche Zahl n mit $0 \leq n < q := p_0 \cdots p_{t-1}$, mit

$$\varphi(n) = (r_0, \ldots, r_{t-1}),$$

wenn r_i den Rest von n bei Division durch p_i bezeichnet, $i \in t$, kurz:

$$n \equiv r_i \ (p_i), \ 0 \leq r_i < p_i.$$

Der Vorteil, den man durch diese Zahldarstellung gewinnt, ist leichte Parallelisierbarkeit arithmetischer Operationen, die aus $[0, q)$ nicht herausführen. Denn $\varphi(n \cdot n') = \varphi(n) \cdot \varphi(n')$, sowie $\varphi(n + n') = \varphi(n) + \varphi(n')$, und die Operationen auf diesen rechten Seiten sind punktweise auszuführen, können also parallel durchgeführt werden. Dabei ist wichtig, daß man mit Hilfe des euklidischen Algorithmus das Urbild n einer gegebenen Restefolge aus den Urbildern der "Einheitsvektoren" berechnen kann (vgl. Übungsblatt).

Neben dem Chinesischen Restesatz benötigen wir noch die Tatsache, daß die Zerlegung von Elementen aus Hauptidealbereichen in Primelemente (bzw. unzerlegbare Elemente) im wesentlichen, d.h. bis auf Faktoren aus der Einheitengruppe eindeutig ist.

3.10.6 Die Eindeutigkeit der Primfaktorzerlegung in euklidischen Bereichen *Ist R ein euklidischer Bereich, $r \in R^*$, dann gibt es eine Einheit $e \in E(R)$ sowie Primelemente r_λ, $\lambda \in L$, L endlich, mit*

$$r = e \prod_{\lambda \in L} r_\lambda.$$

Diese Darstellung von r als Produkt von Primelementen (und eine Einheit) ist im wesentlichen eindeutig, d.h. für jede weitere Darstellung

$$r = e \prod_{\lambda \in L} r_\lambda = f \prod_{\nu \in N} s_\nu,$$

f Einheit, N endlich, $s_\nu, \nu \in N$ Primelemente, gibt es eine Bijektion $\beta\colon L \rightarrowtail\!\!\!\!\!\rightarrow N$ mit

$$\forall\ \lambda \in L\colon\ r_\lambda \text{ ist assoziiert zu } s_{\beta(\lambda)},\ r_\lambda \sim s_{\beta(\lambda)}.$$

Beweis:

i) Wir zeigen zunächst, daß solche Zerlegungen gegebenenfalls im wesentlichen eindeutig sind, per Induktion nach $|L|$.

Ist $L = \emptyset$, dann ist $r = e = f \prod_\nu s_\nu$ und damit jedes Element auf der rechten Seite eine Einheit, N also ebenfalls leer und die Behauptung in diesem Fall richtig.
Sei jetzt L (und damit auch N) nicht leer, $\lambda \in L$. r_λ teilt, da Primelement, die rechte Seite, d.h. es gibt ein ν mit $r_\lambda \mid s_\nu$, etwa $r_\lambda t_\lambda = s_\nu$. s_ν ist aber auch unzerlegbar, t_λ demnach Einheit. Das ergibt

$$e \prod_{\kappa \neq \lambda} r_\kappa = f \cdot t_\lambda \prod_{\iota \neq \nu} s_\iota.$$

Hierauf ist die Induktionsannahme anwendbar, was die Behauptung ergibt.

ii) Jetzt zur Existenz einer solchen Zerlegung. Zu ihrem Nachweis verwenden wir Induktion nach $\delta(r)$.

Ist $\delta(r) = \delta(1)$, dann ist, wie man sich leicht überlegt (vgl. Übungsblatt), r eine Einheit, es existiert also eine Zerlegung der angegebenen Art: $r = r$.

Ist $\delta(r) > \delta(1)$ und r prim, dann ist wieder $r = r$ eine Zerlegung der gesuchten Form. Ist r jedoch nicht prim, dann ist r zerlegbar, besitzt also echte Teiler, etwa $a, b \in R^*$, mit $r = ab$ und $a, b \notin E(R)$. Hierfür gilt

$$\delta(a) < \delta(ab) = \delta(r) > \delta(b).$$

Die Induktionsannahme kann also sowohl auf a als auch auf b angewandt werden, aus deren Zerlegungen in Primelemente ergibt sich eine Zerlegung für r.

□

Wir können also in einem euklidischen Ring R mit

$$e(r, p)$$

den Exponenten bezeichnen, den das Primelement p oder dazu assoziierte Primelemente in einer Zerlegung von r in Primfaktoren hat. Sind dann r, s zwei Elemente in diesem euklidischen Bereich, dann gilt offenbar

3.10.7 $$\mathrm{ggT}\,(r, s) = \Big(\prod_{p \in \mathcal{P}} p^{\min\{e(r,p), e(s,p)\}}\Big) \cdot E(R),$$

sowie

3.10.8 $$\mathrm{kgV}(r, s) = \Big(\prod_{p \in \mathcal{P}} p^{\max\{e(r,p), e(s,p)\}}\Big) \cdot E(R),$$

wenn $\mathcal{P}$ ein Repräsentantensystem der Bahnen der Einheitengruppe auf der Menge der Primteiler bezeichnet.

Zur Herleitung der Jordanschen Normalform werden wir die folgende Konsequenz der eindeutigen Zerlegbarkeit verwenden:

3.10.9 Satz *Ist $I \neq (0)$ ein Ideal in einem euklidischen Ring R, dann gibt es nur endlich viele Ideale in R, die I enthalten.*

Beweis: Sei $I = (r)$, $r = e \prod_{\nu \in N} p_\nu$ die Zerlegung des erzeugenden Elements in Primfaktoren p_ν (N also eine endliche Menge), e eine Einheit. Ist jetzt $J = (s)$ ein weiteres Ideal, das I enthält, dann ist s ein Teiler von r und, wegen der Eindeutigkeit der Primfaktorzerlegung von der Form

$$s = e' \prod_{\nu \in T} p_\nu,$$

mit einer Teilmenge T von N und einer Einheit e'. Dies zeigt

$$J = \Big(\prod_{\nu \in T} p_\nu\Big),$$

so daß es nur endlich viele Ideale J oberhalb von I geben kann.

□

Wir wollen diese Überlegungen jetzt zur Herleitung der Jordanschen Normalform verwenden. Sei dazu M ein Linksmodul über einem euklidischen Bereich R, I ein maximales Ideal in R, erzeugt von r. Wir setzen

$$M_I := \{m \in M \mid \exists\, n \in \mathbb{N}\colon\ (r^n) = \mathrm{Ord}(m)\}.$$

3.10.10 Satz *Ist $Ann(M) \neq 0$, $\mathcal{M}$ die Menge der maximalen Ideale in R, dann gilt:*

- *Jedes M_I ist Untermodul.*
- *M ist die direkte Summe dieser Untermoduln:*

$$M = \bigoplus_{(0)\neq I\in\mathcal{M}} M_I.$$

- *Es gilt*

$$Ann(M) \subseteq I \iff M_I \neq \{0\}.$$

Beweis:

i) Die Eigenschaft von M_I, Untermodul zu sein, ergibt sich so: $0 \in M_I$ ist klar, denn $\mathrm{Ord}(0) = R = (r^0 = 1_R)$. Wenn $u, v \in M_I$, $s, t \in R$, $\mathrm{Ord}(u) = (r^m)$, $\mathrm{Ord}(v) = (r^n)$, und (ohne Einschränkung der Allgemeinheit) $m \geq n$, dann ist

$$r^m(su + tv) = sr^{m-n}r^n u + tr^m v = 0,$$

und damit $(r^m) \subseteq \mathrm{Ord}(su + tv)$. Nun ist aber $\mathrm{Ord}(su + tv) = (x)$, mit einem Teiler x von r^m. Weil r prim ist (I ist, als maximales Ideal, ja auch Primideal und von einem Primelement erzeugt), ist x eine Potenz von r und damit auch $su + tv \in M_I$.

ii) M ist Summe der M_I : Sei $m \in M$, $\mathrm{Ord}(m) = (s)$,

$$s = \prod_{p\in\mathcal{P}} p^{e(s,p)}$$

die Zerlegung in *verschiedene* Primfaktoren $p \in P$. Wir setzen $s_p := s/p^{e(s,p)}$. Diese s_p sind offenbar teilerfremd, so daß $t_p \in R$ existieren mit $1 = \sum_p t_p s_p$, also

$$m = \sum_{p\in\mathcal{P}} t_p s_p m.$$

Jeder der Summanden auf der rechten Seite liegt aber in einem der M_I, denn

$$0 = sm = t_p sm = p^{e(s,p)} t_p s_p m,$$

also $(p^{e(s,p)}) \subseteq \mathrm{Ord}(t_p s_p m)$ und demnach

$$t_p s_p m \in M_{(p)}.$$

Diese Summe ist direkt: Es genügt zu zeigen, daß die 0_M nur trivial als Summe von (endlich vielen) Elementen m_I der Summanden M_I dargestellt werden kann. Sei also

$$0 = \sum_{(0)\neq I\in\mathcal{N}} m_I,$$

$\mathcal{N}$ eine endliche Teilmenge von $\mathcal{M}$.

Wir bemerken zunächst, daß verschiedene Elemente I bzw. J aus $\mathcal{N}$ teilerfremd sind, denn ihre Erzeugenden, etwa r bzw. s, sind nicht assoziiert und prim. Die Ordnungsideale von m_I bzw. m_J werden von Potenzen von r bzw. s erzeugt, sind deshalb ebenfalls teilerfremd. Wir können demnach den Chinesischen Restesatz anwenden,

$$\varphi\colon R \to \times_{I\in\mathcal{N}} R/\mathrm{Ord}(m_I), r \mapsto (\ldots, r + \mathrm{Ord}(m_I), \ldots)$$

ist nach dem Restesatz surjektiv, es gibt also $t_I \in R$ mit

$$t_I - 1 \in \mathrm{Ord}(m_I), \text{ und } t_I \in \mathrm{Ord}(M_J), \text{ falls } J \neq I.$$

Wir schließen daraus auf

$$0 = t_I \cdot 0 = \sum_{J\in\mathcal{N}} t_I m_J = m_I.$$

iii) Es bleibt zu zeigen, daß $M_I \neq \{0\}$ genau dann gilt, wenn $\mathrm{Ann}(M) \subseteq I$.

Ist $0 \neq m \in M_I$, etwa $\mathrm{Ord}(m) = (r^n) \subseteq (r) = I$, so folgt

$$\mathrm{Ann}(M) \subseteq \mathrm{Ord}(m) \subseteq I,$$

wie behauptet.

Ist umgekehrt $\mathrm{Ann}(M) \subseteq I = (r)$, dann betrachten wir ein $m \in M$ mit $\mathrm{Ann}(M) = \mathrm{Ord}(m) = (s)$ (vgl. 3.8.19). Hierfür gilt $r \mid s$ und damit

$$\mathrm{Ord}(\frac{s}{r}m) = (r),$$

so daß gilt

$$0 \neq \frac{s}{r}m \in M_I,$$

was noch zu zeigen war.

□

Diese Untermoduln M_I heißen *Primärkomponenten* von M. Ist $M = M_I$, so heißt M *primär*. (Ist $\mathrm{Ann}(M) \neq 0$, dann gibt es, nach 3.10.10 iii) und 3.10.9, nur endlich viele Primärkomponenten $M_I \neq \{0\}$.) Tatsächlich bestimmen diese den Modul bis auf Isomorphie:

3.10.11 Satz *Sind M, N R-Linksmoduln über einem euklidischen Bereich R mit von Null verschiedenen Annihilatoren, dann sind sie genau dann isomorph, wenn dies auch für die Primärkomponenten gilt:*

$$M \simeq N \iff \forall\, I \in \mathcal{M}\colon\ M_I \simeq N_I.$$

Beweis:

Sei $f\colon M \simeq N$, $I \in \mathcal{M}$, $I = (r)$, $m \in M_I$ und $\mathrm{Ord}(m) = (r^n)$. Es gilt

$$r^n f(m) = f(r^n m) = f(0) = 0,$$

also $f(M_I) \subseteq N_I$. Aus Symmetriegründen gilt auch $f^{-1}(N_I) \subseteq M_I$. Insgesamt ergibt das den Isomorphismus

$$f \downarrow M_I\colon\ M_I \simeq N_I.$$

Sind umgekehrt die Primärkomponenten isomorph, $f_I\colon M_I \simeq N_I$, dann können wir, wegen 3.10.10, und weil es nur endlich viele Primärkomponenten $M_I \neq \{0\}$ gibt, eine Abbildung

$$f\colon \bigoplus_I M_I \to \bigoplus_I N_I, \sum_I m_I \mapsto \sum_I f_I(m_I)$$

definieren, die offensichtlich ein R-Isomorphismus von M auf N ist.

□

3.10.12 Satz *Ist $M = \oplus_{i\in t} Rm_i$ primär und Ord$(m_i) = (r_i)$, dann sind die r_i — bis auf Umnumerierung — die Elementarteiler von M.*

Beweis: Weil M primär ist, gilt $M = M_I$, für ein maximales Ideal I, d.h. $I = (r)$, für ein Primelement r. Darüberhinaus ist $\mathrm{Ord}(m_i) = (r^{e_i})$, für geeignete e_i. Bei geeigneter Numerierung haben wir

$$e_{t-1} \leq \ldots \leq e_0.$$

Die Erzeuger der Ornungsideale der m_i teilen sich also:

$$r^{e_{t-1}} \mid \ldots \mid r^{e_0}.$$

Weil die Elementarteiler durch den Isomorphietyp eindeutig bestimmt sind (vgl. Lüneburg, Satz 7, Kap. 14), folgt die Behauptung.

□

3.10.13 Satz *Sei V ein n-dimensionaler $\mathbb{K}$-Vektorraum, $f \in End_{\mathbb{K}}(V)$ mit $m_f = (x-\lambda)^n$. Ist $v \in V$ mit Ord$(v) = (m_f)$, dann bilden die Vektoren $b_0, \ldots, b_{n-1}$ mit $b_i := (x-\lambda)^i v$ eine Basisfolge für V mit*

$$f(b_i) = b_{i+1} + b_i\lambda,\ i \in n-1,\ f(b_{n-1}) = b_{n-1}\lambda.$$

f wird also durch folgende Matrix dargestellt:

$$M(\mathcal{B}, f, \mathcal{B}) = \begin{pmatrix} \lambda & & & & 0 \\ 1 & \lambda & & & \\ & 1 & \ddots & & \\ & & \ddots & \lambda & \\ 0 & & & 1 & \lambda \end{pmatrix} =: J(\lambda).$$

Beweis:

i) Die b_i bilden eine Basis: Sei

$$0 = \sum_{i=0}^{n-1} \kappa_i b_i = \sum_i \kappa_i (x-\lambda)^i v = \left(\sum_i \kappa_i (x-\lambda)^i \right) v.$$

Dies impliziert

$$(x-\lambda)^n = m_f \mid \sum_{i=0}^{n-1} \kappa_i (x-\lambda)^i,$$

und aus Gründen der Grade, ergibt das $\sum_{i=0}^{n-1} \kappa_i (x-\lambda)^i = 0$. Es folgt $\kappa_i = 0$, für alle i, die b_i sind also linear unabhängig.

ii) Zur Berechnung der Wirkung von f auf diese Basisvektoren bemerken wir, daß

$$(x-\lambda)^{i+1} v = (x-\lambda) b_i = f(b_i) - \lambda b_i,$$

was $f(b_i) = b_{i+1} + \lambda b_i$ liefert, für $i \in n-1$. Schließlich gilt noch

$$f(b_{n-1}) = f((x-\lambda)^{n-1} v) = x(x-\lambda)^{n-1} v - \lambda (x-\lambda)^{n-1} v + \lambda (x-\lambda)^{n-1} v$$

$$= (x-\lambda)^n v + \lambda b_{n-1} = \lambda b_{n-1}.$$

Die angegebene Form der darstellenden Matrix folgt hieraus unmittelbar.

□

In gewisser Weise eine Umkehrung enthält

3.10.14 Satz *Ist $\mathcal{B} = (b_0, \ldots, b_{n-1})$ eine Basisfolge von V und $f \in End_{\mathbb{K}}(V)$ mit $f(b_i) = b_{i+1} + \lambda b_i$, für $i \in n-1$, sowie $f(b_{n-1}) = \lambda b_{n-1}$, dann gilt:*

$$V_f = \mathbb{K}[x] b_0, \; m_f = (x-\lambda)^n.$$

Beweis: Nachrechnen!

Matrizen der Form $J(\lambda)$ heißen *Jordanmatrizen*, und wir erhalten jetzt durch Kombination dieser Überlegungen mit den Resultaten zur rationalen Normalform die gesuchte *Jordansche Normalform.*

3.10.15 Die Jordansche Normalform *Ist das Minimalpolynom von* $f \in End_{\mathbb{K}}(V)$ *von der Form*

$$m_f = \prod_{i \in t} (x - \lambda_i)^{e_i},$$

mit paarweise verschiedenen λ_i*, dann sind die Unterräume*

$$V_{f,i} := (V_f)_{(x-\lambda_i)}$$

die Primärkomponenten von V_f*, also*

$$V_f = \bigoplus_{i \in t} (V_f)_{(x-\lambda_i)}.$$

Die Berechnung der rationalen Normalform, angewandt auf die Primärkomponenten, liefert eine direkte Zerlegung dieser:

$$V_{f,i} = \bigoplus_{j=1}^{s(i)} \mathbb{K}[x] v_{ij},$$

mit

$$Ord(v_{ij}) = (x - \lambda_i)^{e_{ij}},\ e_i = e_{i1} \geq e_{i2} \geq \ldots e_{i,s(i)} \geq 1.$$

Dieser Zerlegung entspricht eine darstellende Matrix mit Jordanblöcken längs der Hauptdiagonalen:

$$\begin{pmatrix} \ddots & \cdots & 0 \\ \vdots & J(\lambda) & \vdots \\ 0 & \cdots & \ddots \end{pmatrix}.$$

Kapitel 4

Geometrische Aspekte

Weitere Begriffe der linearen Algebra, die jetzt eingeführt und diskutiert werden sollen, haben auch geometrische Bezüge. Sie ermöglichen u.a. die Definition von Winkeln, Längen, Orientierung usw.

4.1 Vektorräume mit innerem Produkt

In diesem Paragraphen sei stets V ein $\mathbb{R}-$Vektorraum, ohne daß dies noch gesondert erwähnt wird. Wir betrachten nun gewisse Skalarprodukte auf V, die die Einführung von Begriffen wie Länge, Winkel usw. erlauben.

4.1.1 Definition (inneres Produkt, Norm, orthogonal) $\langle - \mid - \rangle : V^2 \to \mathbb{R}$ sei Skalarprodukt (d.h. eine nicht ausgeartete Bilinearform, also eine bilineare Abbildung mit trivialen Nullräumen). Dann heißt $\langle - \mid - \rangle$ *inneres Produkt* wenn gilt:

i) $\langle - \mid - \rangle$ ist *symmetrisch:* $\langle v \mid w \rangle = \langle w \mid v \rangle$,

ii) $\langle - \mid - \rangle$ ist *positiv definit:* $\langle v \mid v \rangle \geq 0 \ \wedge \ [\langle v \mid v \rangle = 0 \Rightarrow v = 0_V]$.

In diesem Fall heißt das Paar $(V, \langle - \mid - \rangle)$ ein *Raum mit innerem Produkt.* Genau die endlichdimensionalen Vektorräume (über $\mathbb{R}$) mit innerem Produkt heißen *euklidische Vektorräume.*

iii) Die entsprechende Funktion $\| - \| : V \to \mathbb{R}, v \mapsto \sqrt{\langle v \mid v \rangle}$, heißt die *Norm.*

iv) u und w aus V heißen *orthogonal,* kurz: $u \perp w$, wenn $\langle u \mid w \rangle = 0$.

v) Unterräume $U, W \leq$ von V heißen *orthogonal,* kurz: $U \perp W$, wenn gilt: $\forall\, u \in U, w \in W : \langle u \mid w \rangle = 0$.

•

4.1.2 Beispiele

1. $\mathbb{R}^n$ mit $\langle v \mid w \rangle := \sum_{i=1}^{n} v_i w_i$.
2. Der Raum aller stetigen $f : [0,1] \to \mathbb{R}$ mit $\langle f \mid g \rangle := \int_0^1 f(t)g(t)dt$.

◇

4.1.3 Hilfssatz *In einem Raum mit innerem Produkt sind Teilmengen paarweise orthogonaler Vektoren $\neq 0_V$ linear unabhängig.* □

Beweis: Ist T eine solche Teilmenge, $v_0, \ldots, v_{r-1} \in T$, mit $\sum_i \kappa_i v_i = 0$, dann gilt:

$$\forall\, j \in r : \ 0_{\mathbb{R}} = \langle 0_V \mid v_j \rangle = \sum_{i=0}^{r-1} \kappa_i \langle v_i \mid v_j \rangle = \kappa_j \langle v_j \mid v_j \rangle.$$

(Die erste Gleichung folgt aus der Tatsache, daß $v \mapsto \langle v \mid w \rangle$ eine lineare Abbildung ist.) Wegen $\langle v_j \mid v_j \rangle \neq 0$ folgt daraus $\kappa_j = 0$.

□

Zwischen dem inneren Produkt und der zugehörigen Norm bestehen u.a. diese Zusammenhänge:

4.1.4 Hilfssatz *Ist* $(V, \langle - \mid - \rangle)$ *Raum mit innerem Produkt,* $v, w \in V$*, dann gilt:*

i) $\langle v \mid w \rangle = \frac{1}{2}(\|v+w\|^2 - \|v\|^2 - \|w\|^2)$

ii) $\langle v \mid w \rangle^2 \leq \|v\|^2\|w\|^2$ (Cauchy- Schwarzsche Ungleichung),
und dabei gilt Gleichheit genau dann, wenn $dim_{\mathbb{R}}\langle v, w\rangle \leq 1$.

iii) $\|v+w\| \leq \|v\| + \|w\|$ (Dreiecksungleichung)

Beweis:

i) $\|v+w\|^2 = \langle v+w \mid v+w\rangle = 2\langle v \mid w\rangle + \langle v \mid v\rangle + \langle w \mid w\rangle$ ergibt die erste Behauptung.

ii) Zum Beweis der Ungleichung verwenden wir die Tatsache, daß für beliebiges $r \in \mathbb{R}$ gilt

$$0 \leq \|v+rw\|^2 =_{i)} \|v\|^2 + r^2\|w\|^2 + 2r\langle v \mid w\rangle.$$

Für $w := 0_V$ gilt die Behauptung, im anderen Fall können wir r wie folgt wählen:

$$r := -\frac{\langle v \mid w\rangle}{\|w\|^2},$$

was folgendes ergibt:

$$0 \leq \|v\|^2 + \frac{\langle v \mid w\rangle^2}{\|w\|^2} - 2\frac{\langle v \mid w\rangle^2}{\|w\|^2} = \frac{\|v\|^2\|w\|^2 - \langle v \mid w\rangle^2}{\|w\|^2},$$

also $0 \leq \|v\|^2\|w\|^2 - \langle v \mid w\rangle^2$.

Ist dabei $\dim_{\mathbb{R}}(\langle v, w\rangle) \leq 1$, so gilt o.B.d.A.: $v = rw$, mit geeignetem $r \in \mathbb{R}$, und damit $\langle v \mid w\rangle^2 = r^2\|w\|^4 = \|v\|^2\|w\|^2$, es gilt also die behauptete Gleichheit.

Ist umgekehrt $\langle v \mid w\rangle^2 = \|v\|^2\|w\|^2$, so gilt in der obigen Ungleichung das Gleichheitszeichen, also

$$0 = \|v+rw\|^2 = \|v\|^2 + r^2\|w\|^2 + 2r\langle v \mid w\rangle,$$

zumindest für das angegebene $r \in \mathbb{R}$. Da $\langle - \mid - \rangle$ positiv definit ist, gilt $v + rw = 0$, also $\dim_{\mathbb{R}}(\langle v, w\rangle) \leq 1$.

iii) Die Dreiecksungleichung folgt schließlich so:

$$\|v+w\| = \sqrt{\|v\|^2 + \|w\|^2 + 2\langle v \mid w\rangle}$$

$$\leq_{ii)} \sqrt{\|v\|^2 + \|w\|^2 + 2\|v\|\,\|w\|} = \|v\| + \|w\|.$$

□

4.1.5 Folgerung *Ist* $(V, \langle - \mid - \rangle)$ *Raum mit innerem Produkt,* $v, w \in V \backslash \{0_V\}$, *dann gilt:*

$$-1 \leq \frac{\langle v \mid w \rangle}{\|v\|\|w\|} \leq 1,$$

es gibt also genau ein $\omega \in [0, \pi] \subseteq \mathbb{R}$ *mit:*

$$\cos(\omega) = \frac{\langle v \mid w \rangle}{\|v\|\|w\|}.$$

□

Wir sind demnach zur Einführung der folgenden Bezeichnung berechtigt:

4.1.6 Definition (Winkel) Das ω aus 4.1.5 heiße der *Winkel* zwischen v und w. (Offenbar ist $\omega \in \{0, \pi\}$ bei linearer Abhängigkeit von $\{v, w\}_{\neq}$, und gleich $\pi/2$ bei $v \perp w$.) •

Aus 4.1.5 folgt mit 4.1.4 i) noch:

4.1.7 Der Cosinussatz *Es gilt*

$$\|v - w\|^2 = \|v\|^2 + \|w\|^2 - 2\|v\|\|w\| \cos(w).$$

Der Winkelbegriff der anschaulichen Geometrie ist allerdings komplizierter, da es sich um *orientierte* Winkel handelt. Wir führen deshalb den Begriff der Orientierung ein.

4.1.8 Definition (orientierter Vektorraum) Ist $n := \dim_{\mathbb{R}} V \in \mathbb{N}^*$, so gibt es nichttriviale $\Delta \in DF(V)$ und auf diesen wegen 3.6.7 ii) folgende Äquivalenzrelation:

$$\Delta \sim \Delta' :\Longleftrightarrow \exists\, r \in \mathbb{R}_{>0} \colon\ \Delta = r\Delta'.$$

Die beiden Klassen von " $\sim$ " heißen die *Orientierungen* von V. V zusammen mit einer dieser beiden Klassen $[\Delta]_\sim$ heißt *orientierter Vektorraum.*
Ist $(V, [\Delta]_\sim)$ orientierter Vektorraum $\mathcal{B} = (b_1, \ldots, b_n)$ eine Basisfolge von V, dann heißt $\mathcal{B}$ *positive Basisfolge* genau dann, wenn $\Delta(b_1, \ldots, b_n) > 0$ gilt. •

4.1.9 Beispiel

$$\begin{aligned} \mathbb{R}^4 &= \ll e_0 + e_1, e_0 + e_1 + e_2, e_0 + e_1 + e_2 + e_3, e_0 - e_1 + e_3 \gg \\ &= \ll e_0 - 3e_2, e_1 + e_3, e_1 - e_0 - e_3, e_1 \gg . \end{aligned}$$

Diese Basen sind stets verschieden orientiert, da die beiden Determinanten mit diesen Basisfolgen als Spalten, also

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = -2, \ \det \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 1 \\ -3 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} = 3$$

verschiedene Vorzeichen haben. ◇

Jeder $\mathbb{R}-$Isomorphismus f induziert eine Orientierung im Bildraum, nämlich diejenige, bzgl. der f orientierungserhaltend ist:

4.1.10 Definition (orientierungserhaltend) Sind $(V, [\Delta]_\sim)$ und $(V', [\Delta']_\sim)$ orientierte Vektorräume, $f \in Iso_{\mathbb{R}}(V, V')$, dann heißt f *orientierungserhaltend,* wenn gilt

$$(\Delta')_f \in [\Delta]_\sim.$$

•

4.1.11 Satz *Ein $\mathbb{R}-$Automorphismus f eines orientierten $\mathbb{R}-$Vektorraums ist genau dann orientierungserhaltend, wenn* $\det(f) > 0$ *ist.*

Beweis: Ist $[\Delta]_\sim$ die Orientierung, dann gilt $\Delta_f = \det(f) \cdot \Delta$, also $\Delta_f \in [\Delta]_\sim$ genau dann, wenn $\det(f) > 0$. □

4.1.12 Definition (Orthonormalbasis) Ist wieder $(V, \langle - \mid - \rangle)$ ein Raum mit innerem Produkt, dann heißt eine Basis B *Orthonormalbasis* (kurz: ON-Basis) von V, wenn sie aus paarweise orthogonalen Vektoren der Norm 1 besteht. •

4.1.13 Satz *In jedem Vektorraum V mit innerem Produkt und abzählbarer Basis kann man jede endliche Basisfolge $(b_0, b_1, \ldots, b_{m-1})$ eines Unterraums* othonormalisieren, *d.h. eine Folge $(e_0, e_1, \ldots, e_{m-1})$ orthonormaler Vektoren e_i konstruieren, die Basis desselben Unterraums sind:*

$$\ll e_0, e_1, \ldots, e_{m-1} \gg = \ll b_0, b_1, \ldots, b_{m-1} \gg .$$

Beweis: Das *Orthonormalisierungsverfahren von E. Schmidt:*

Aus einer beliebigen vorgegebenen Basisfolge $\mathcal{B} = (b_0, b_1 \ldots, b_{m-1}, \ldots)$ wird eine ON-Basisfolge $(e_0, e_1, \ldots, e_{m-1}, \ldots)$ konstruiert, die denselben Unterraum erzeugt. Dazu zeigen wir per Induktion: Für $n \in \mathbb{N}$ und $U := \ll b_0, \ldots, b_{n-1} \gg$ existiert eine ON-Basisfolge $\mathcal{E}' = (e_0, \ldots, e_{n-1})$, die denselben Unterraum erzeugt.

I $n = 0$: Die leere Menge erzeugt den Nullraum, und die leere Folge ist offenbar eine ON-Basisfolge.

II $n \to n+1$: Entsprechend der Induktionsannahme sei $(e_0, \ldots, e_{n-1})$ eine ON-Basisfolge für $\ll b_0, \ldots, b_{n-1} \gg$. Wir setzen jetzt

$$a_n := b_n - \sum_{j=0}^{n-1} \langle b_n \mid e_j \rangle e_j.$$

Offenbar gilt damit

$$\ll b_0, \ldots, b_n \gg = \ll e_0, \ldots, e_{n-1}, a_n \gg,$$

zudem sind die Vektoren $e_0, \ldots, e_{n-1}, a_n$ paarweise orthogonal:

$$\langle a_n \mid e_i \rangle = \langle b_n \mid e_i \rangle - \sum_1^n \langle b_n \mid e_j \rangle \underbrace{\langle e_j \mid e_i \rangle}_{=\delta_{ij}} = 0.$$

Also ist $\mathcal{E}' := (e_0, \ldots, e_n)$, mit

$$e_n := \frac{a_n}{\|a_n\|}$$

eine ON-Basisfolge von $U = \ll b_0, \ldots, b_n \gg$.

□

4.1.14 Beispiel V sei der Raum der Polynomabbildungen $f: \mathbb{R} \to \mathbb{R}$ vom Grad ≤ 2 mit dem inneren Produkt

$$\langle f \mid g \rangle := \int_{-1}^{1} f(x)g(x)dx.$$

Aus der Basisfolge $(1, x, x^2)$ ergibt sich die ON-Folge

$$e_0 = \frac{1}{\sqrt{2}}, e_1 = \sqrt{\frac{3}{2}}x, e_2 = \sqrt{\frac{45}{8}}(x^2 - \frac{1}{3}).$$

$e_0, e_1, \ldots$ sind, bis auf Normierungsfaktoren, die sogenannten *Legendre-Polynome.*

◇

4.1.15 Definition (orthogonale Matrizen) $A \in \mathbb{R}^{n \times n}$ heißt *orthogonal,* wenn ${}^tA = A^{-1}$. •

4.1.16 Anwendung (Die QR-Zerlegung regulärer Matrizen) Jede reguläre Matrix über $\mathbb{R}$ kann als Produkt aus einer orthogonalen Matrix mit einer Dreiecksmatrix geschrieben werden.

Beweis: Übungsblatt.

4.1.17 Satz *Ist V endlichdimensional, dann wird der Übergang von einer ON-Basis zu einer anderen stets durch eine orthogonale Matrix beschrieben. Umgekehrt ergibt ein Basiswechsel, der durch eine orthogonale Matrix beschrieben wird, aus einer ON-Basis wieder eine solche.*

Beweis: Nachrechnen.

□

Als unmittelbare Folgerung aus der Orthonormalisierbarkeit von endlichen Basisfolgen ergibt sich: Ist V euklidischer Vektorraum, $U \leq V$, dann kann man eine an U angepaßte ON-Basisfolge finden. Es gilt also

4.1.18 $$V = U \oplus U^\perp,\ U^\perp := \{v \in V \mid \forall\ u \in U: \langle u \mid v \rangle = 0\}.$$

Demgemäß kann $v \in V$ zerlegt werden in $v = u + w, u \in U, w \in U^\perp$. Ist $(u_0, \ldots, u_{m-1})$ eine ON-Basis von U, dann gilt

4.1.19 $$u = \sum_0^{m-1} \langle u \mid u_i \rangle u_i.$$

u heißt die *Orthogonalprojektion* von v auf U, $\|w\|$ der *Abstand* von v zum Unterraum U. Wegen $\|v\|^2 = \|u\|^2 + \|w\|^2$ gilt

4.1.20 $$\|v\| \geq \|u\| \text{ (Besselsche Ungleichung).}$$

Sei jetzt $\Delta \in DF(V)$ nicht trivial, $(e_0, \ldots, e_{n-1})$ eine ON-Basisfolge. Die Funktion

$$\det(\langle - \mid - \rangle) \colon V^2 \to \mathbb{R}, (v, w) \mapsto \det(\langle v \mid w \rangle)$$

ist in beiden Komponenten multilinear, alternierend und nicht trivial. Es gibt deshalb $r \in \mathbb{R}^*$, so daß, für alle $v_i, w_i \in V$,

4.1.21 $$r \cdot \det(\langle v_i \mid w_k \rangle) = \Delta(v_0, \ldots, v_{n-1})\Delta(w_0, \ldots, w_{n-1}).$$

Wegen $\det(\langle e_i \mid e_k \rangle) = \det(I_n) = 1$ gilt insbesondere $r = \Delta(e_0, \ldots, e_{n-1})^2 > 0$. Für $\Delta' := \pm\Delta/\sqrt{r}$ gilt also

4.1.22 $$\Delta'(v_0, \ldots, v_{n-1})\Delta'(w_0, \ldots, w_{n-1}) = \det(\langle v_i \mid w_k \rangle).$$

4.1.23 Definition (normierte Determinantenform) Determinantenformen auf Räumen mit inneren Produkt, die 4.1.22 genügen, heißen *normiert.* •

$\pm\Delta/\sqrt{r}$ sind die beiden einzigen normierten Determinantenformen, genau eine von ihnen repräsentiert die Orientierung. Auf jedem euklidischen Vektorraum mit Orientierung gibt es also genau eine normierte Determinantenform, welche die Orientierung repräsentiert. Mit dieser die Orientierung repräsentierenden normierten Determinantenform Δ_0 können wir auch Winkel orientieren: In einem orientierten 2-dimensionalen Vektorraum V mit innerem Produkt $\langle - \mid - \rangle$ gilt nach 4.1.22:

4.1.24 $$\Delta_0(v, w)^2 = det \begin{pmatrix} \langle v \mid v \rangle & \langle v \mid w \rangle \\ \langle w \mid v \rangle & \langle w \mid w \rangle \end{pmatrix} = \|v\|^2\|w\|^2 - \langle v \mid w \rangle^2.$$

Für $v \neq 0_V \neq w$ ergibt dies

$$\frac{\langle v \mid w \rangle^2}{\|v\|^2\|w\|^2} + \frac{\Delta_0(v, w)^2}{\|v\|^2\|w\|^2} = 1.$$

Es gibt also — wegen $\sin^2(x) +$
$cos^2(x) = 1$ — genau ein $\omega \in (-\pi, \pi] \subseteq \mathbb{R}$ mit

4.1.25 $$\cos(\omega) = \frac{\langle v \mid w \rangle}{\|v\|\|w\|} \text{ und } \sin(\omega) = \frac{\Delta_0(v, w)}{\|v\|\|w\|}.$$

4.1.26 Definition (orientierter Winkel) Das ω aus 4.1.25 heißt der *orientierte Winkel* zwischen v und w. Er wechselt das Vorzeichen mit der Orientierung $[\Delta_0]_\sim$ und auch bei Vertauschen von v und w. •

4.1.27 Definition (die Gramsche Determinante) Ist $(V, \langle - \mid - \rangle)$ Vektorraum mit innerem Produkt und sind $v_0, \ldots, v_{m-1} \in V$, dann heißt

$$G(v_0, \ldots, v_{m-1}) := \det(\langle v_i \mid v_k \rangle)$$

die *Gramsche Determinante* der Vektorenfolge $(v_0, \ldots, v_{m-1})$. •

4.1.28 Hilfssatz *Für die Gramsche Determinante gilt*

i) $G(v_0, \ldots, v_{m-1}) \geq 0$

ii) $G(v_0, \ldots, v_{m-1}) = 0 \iff dim_{\mathbb{R}}(\langle v_0, \ldots, v_{m-1} \rangle) < m.$

Beweis: Die erste Behauptung ist für linear abhängige v_i natürlich richtig. Sind die v_i linear unabhängig, dann erzeugen sie einen m-dimensionalen Unterraum mit innerem Produkt. Auf diesem existiert eine normierte Determinantenfrom Δ_0, und hierfür ist

$$G(v_0, \ldots, v_{m-1}) = \Delta_0(v_0, \ldots, v_{m-1})^2 > 0.$$

Damit ist auch die Implikation von links nach rechts in der zweiten Behauptung bewiesen. Die Annahme $\dim(\langle v_0, \ldots, v_{m-1} \rangle) < m$ ergibt offensichtlich $G(v_0, \ldots, v_{m-1}) = 0$. □

4.1.29 Definition (Parallelepiped,Volumen) Ist $(V, \langle - \mid - \rangle)$ Raum mit innerem Produkt, $(v_0, \ldots, v_{r-1})$ linear unabhängig, Δ eine normierte Determinantenform auf $\ll v_0, \ldots, v_{r-1} \gg$, dann heißt

$$\{v \mid v = \sum_0^{r-1} \rho_i v_i, 0 \leq \rho_i \leq 1\}$$

das von den v_i aufgespannte r-dimensionale *Parallelepiped,* und

$$V(v_0, \ldots, v_{r-1}) := |\Delta(v_0, \ldots, v_{r-1})|$$

heißt dessen *Volumen.* •

Offenbar gilt dafür:

4.1.30 Satz

1. $V(v_0, \ldots, v_{r-1})^2 = \det(\langle v_i \mid v_k \rangle)$,
2. *Bei* $r = 2$ *haben wir* $V(v_0, v_1)^2 = \|v_0\|^2 \|v_1\|^2 \sin^2(\omega)$, *also*

$$V(v_0, v_1) = \|v_0\| \|v_1\| \cdot |\sin(\omega)|.$$

□

Auf euklidischen Vektorräumen definierte lineare Funktionale lassen sich mit Hilfe des inneren Produkts beschreiben:

4.1.31 Satz *Der Rieszsche Darstellungssatz: Ist* $(V, \langle - \mid - \rangle)$ *ein euklidischer Vektorraum,* $f \in L(V)$*, dann gibt es genau ein* $v \in V$ *mit*

$$f = \langle v \mid - \rangle.$$

□

Beweis: Die Abbildung $\varphi: v \mapsto \langle v \mid - \rangle$ ist injektiv, und, wegen der Endlichkeit der Dimension $\dim_{\mathbb{R}}(V) = \dim_{\mathbb{R}}(L(V))$ sogar bijektiv, also ein Isomorphismus.
□

Das benutzen wir jetzt zu folgender Definition:

4.1.32 Definition (Kreuzprodukt, Vektorprodukt) Sei $(V, \langle - \mid - \rangle)$ ein dreidimensionaler, euklidischer Vektorraum, Δ die normierte, eine Orientierung repräsentierende Determinantenform, $v, w \in V$. Dann ist $\Delta(v, w, -) \in L(V)$, nach dem Rieszschen Darstellungssatz gibt es also genau ein $u \in V$ mit

$$\Delta(v, w, -) = \langle u \mid - \rangle.$$

Dieses $u \in V$ heißt das *Kreuzprodukt* (oder auch *Vektorprodukt*) von v und w :

$$v \times w := u.$$

•

4.1.33 Eigenschaften des Kreuzprodukts *Für das Kreuzprodukt gilt:*

i) $(v, w) \mapsto v \times w$ *ist schiefsymmetrische Bilinearform,*

ii) $\langle v \times w \mid v \rangle = \langle v \times w \mid w \rangle = 0_{\mathbb{R}}$,

iii) $v \times w \neq 0 \iff dim_{\mathbb{R}}(\langle v, w \rangle) = 2$,

iv) $\Delta(v, w, v \times w) = \|v \times w\|^2$,

v) $dim_{\mathbb{R}}(\langle v, w \rangle) = 2 \Longrightarrow (v, w, v \times w)$ *ist positiv orientierte Basisfolge,*

vi) $\langle u \times v \mid w \times x \rangle = \langle u \mid w \rangle \langle v \mid x \rangle - \langle u \mid x \rangle \langle v \mid w \rangle$.

vii) Ist $v \neq 0 \neq w$ *und* ω *der Winkel zwischen* v *und* w*, dann gilt*

$$\|v \times w\| = \|v\| \cdot \|w\| \cdot |\sin(\omega)|,$$

viii) Für $u, v, w \in V$ *gilt:*

$$u \times (v \times w) = \langle u \mid w \rangle v - \langle u \mid v \rangle w.$$

ix) Es gilt die Jacobische Gleichung

$$u \times (v \times w) + v \times (w \times u) + w \times (u \times v) = 0.$$

x) Ist $\mathcal{B} = (b_0, b_1, b_2)$ *eine positiv orientierte Orthonormalbasisfolge, dann gilt, für den 3-Zyklus* $\pi := (ijk) \in S_3$ *und dessen Vorzeichen* $sgn((ijk))$,

- $b_i \times b_j = sgn((ijk))b_k$, *falls* $k \neq i \neq j \neq k$,
- $v \times w = (v_1w_2 - v_2w_1)b_0 + (v_2w_0 - v_0w_2)b_1 + (v_0w_1 - v_1w_0)b_2$.

Beweis: Aus der Gleichung

$$\Delta(v, w, -) = \langle v \times w \mid - \rangle$$

folgen Bilinearität und Schiefsymmetrie des Kreuzprodukts und auch die Tatsache, daß das Kreuzprodukt auf jedem seiner Faktoren senkrecht steht; i) und ii) sind damit bewiesen.
Zum Nachweis von iii) bemerken wir, daßs

$$v \times w \neq 0 \iff \Delta(v, w, -) \neq 0 \iff (v, w) \text{ linear unabhängig.}$$

Behauptung iv) ist ebenfalls offensichtlich richtig:

$$\Delta(v, w, v \times w) = \langle v \times w \mid v \times w \rangle = \|v \times w\|^2.$$

Ist, wie bei v) vorausgesetzt, $\dim(\langle v, w \rangle) = 2$, dann ist (v, w) linear unabhängig, nach iii) also $v \times w \neq 0$. Letzteres ergibt

$$0 < \|v \times w\|^2 = \Delta(v, w, v \times w).$$

Diese Ungleichung impliziert die positive Orientierung, weil Δ die vorgegebene Orientierung repräsentiert.
Zum Beweis von vi) betrachten wir, für später geeignet zu wählende u_i und v_i aus V, den Ausdruck

$$\begin{aligned}\langle u_0 \times u_1 \mid u_2 \rangle \langle v_0 \times v_1 \mid v_2 \rangle &= \Delta(u_0, u_1, u_2)\Delta(v_0, v_1, v_2) \\ &= \det(\langle u_i \mid v_k \rangle).\end{aligned}$$

Setzt man hier $v_2 := u_0 \times u_1$ und entwickelt nach der letzten Zeile, so bleibt von den drei Summanden nur der letzte übrig, und es ergibt sich die Gleichung

$$\langle u_0 \times u_1 \mid u_2 \rangle \langle v_0 \times v_1 \mid u_0 \times u_1 \rangle = \langle u_0 \times u_1 \mid u_2 \rangle (\langle u_0 \mid v_0 \rangle \langle u_1 \mid v_1 \rangle - \langle u_0 \mid v_1 \rangle \langle u_1 \mid v_0 \rangle).$$

Für $u_0 \times u_1 \neq 0$ gibt es u_2 mit $\langle u_0 \times u_1 \mid u_2 \rangle \neq 0$, durch diesen Faktor darf also dividiert werden, und es verbleibt

$$\langle u_0 \times u_1 \mid v_0 \times v_1 \rangle = \langle u_0 \mid v_0 \rangle \langle u_1 \mid v_1 \rangle - \langle u_0 \mid v_1 \rangle \langle u_1 \mid v_0 \rangle,$$

woraus die Behauptung vi) folgt.

Setzt man in dieser Gleichung vi) $u_0 = v_0 := v$ und $u_1 = v_1 := w$, dann erhält man die Gleichung

$$\|v \times w\|^2 = \|v\|^2\|w\|^2 - \langle v \mid w\rangle^2,$$

was mit der Definition des Winkels zwischen v und w die Behauptung vii) liefert. Zum Beweis von viii) verwenden wir

$$\begin{aligned}\langle u \times (v \times w) \mid x\rangle &= \Delta(u, v \times w, x)\\ &= -\Delta(u, x, v \times w)\\ &= -\langle u \times x \mid v \times w\rangle\\ &= -\langle u \mid v\rangle\langle x \mid w\rangle + \langle u \mid w\rangle\langle x \mid v\rangle\end{aligned}$$

Es gilt demnach, für alle $x \in V$,

$$\langle u \times (v \times w) \mid -\rangle = \langle\langle u \mid w\rangle \mid -\rangle - \langle\langle u \mid v\rangle w \mid -\rangle,$$

was die Behauptung beweist.
ix) folgt direkt aus viii).

□

Ist $(V, \langle - \mid -\rangle)$ ein Raum mit innerem Produkt, dann haben wir gemäß 4.1.1 eine Abbildung $\| - \|: V \to \mathbb{R}$ mit allen Eigenschaften einer Norm gemäß folgender

4.1.34 Definition (Norm) Eine Abbildung $\| - \|: V \to \mathbb{R}$ heißt *Norm,* wenn folgende Bedingungen erfüllt sind:

i) $\|v\| \geq 0$, mit Gleichheit genau dann, wenn $v = 0$.

ii) Es gilt die *Dreiecksungleichung* $\|v + w\| \leq \|v\| + \|w\|$.

iii) $\|\rho \cdot v\| = |\rho| \cdot \|v\|$.

Das Paar $(V, \| - \|)$ heißt dann *normierter Raum.* •

Jeder Raum $(V, \langle - \mid -\rangle)$ mit innerem Produkt ist demnach auf kanonische Weise auch ein normierter Raum. Die Umkehrung gilt aber nicht, denn nicht jede Norm ergibt anhand der Gleichung

$$\langle v \mid w\rangle = \frac{1}{2}(\|v + w\|^2 - \|v\|^2 - \|w\|^2)$$

ein inneres Produkt. Als Beispiel hierfür betrachten wir den Raum $\mathcal{C}$ der auf $[0, 1]$ stetigen reellwertigen Funktionen mit der bekannten und wichtigen *Maximumsnorm*

$$\|f\| := \max\{|f(x)| \mid x \in [0, 1]\}.$$

Die durch

$$\langle f \mid g\rangle := \frac{1}{2}(\|f + g\|^2 - \|f\|^2 - \|g\|^2)$$

definierte Abbildung ist nämlich nicht bilinear: $\langle x \mid x\rangle = 1$, $\langle 1 - x \mid x\rangle = -1/2$, aber $\langle 1 \mid x\rangle = 1$. (Mit zusätzlichen Forderungen an die Norm ergibt sich allerdings ein inneres Produkt, vgl. Übungsblatt.)

Mittels $\| - \|$ läßt sich auch eine *Distanzfunktion* $d_{\|-\|}$ (kurz auch: d) definieren durch

4.1.35 $$d_{\|-\|}\colon V \times V \to \mathbb{R},\ (v, w) \mapsto \|v - w\|.$$

Sie hat offenbar die folgenden Eigenschaften (vgl. 4.1.4):

4.1.36 Eigenschaften der Distanzfunktion *Für alle $u, v, w \in V$ gilt:*

1. *Distanzfunktionen d sind symmetrische Funktionen.*
2. *Distanzen sind nicht negativ:*

   $$d(v, w) \geq 0,$$

   mit Gleichheit genau dann, wenn $v = w$.
3. *Distanzfunktionen genügen der* Dreiecksungleichung,

   $$d(v, w) \leq d(v, u) + d(u, w).$$

4. *Distanzen sind* translationsinvariant:

   $$d(u + v, u + w) = d(v, w).$$

□

Die von Normen auf euklidischen Vektorräumen induzierten Funktionen $d = d_{\|-\|}$ sind also *Metriken,* d.h. symmetrische Funktionen, die der Dreiecksungleichung genügen und denau dann Null sind, wenn sich die beiden Argumente gleichen:

$$d(v, w) = 0 \iff v = w.$$

$(V, d_{\|-\|})$ ist also ein *metrischer Raum* im Sinne der Topologie.

4.1.37 Definition Sind V, W normierte Räume, dann heißt $f\colon V \to W$

1. *beschränkt,* wenn gilt

   $$\exists\ \rho \in \mathbb{R}\ \forall\ v \in V\colon\ \|f(v)\| \leq \rho \cdot \|v\|.$$

2. *stetig an der Stelle $v \in V$,* falls

   $$\forall\ \epsilon > 0\ \exists\ \delta > 0\ \forall\ v' \in V\colon\ \|v - v'\| < \delta\ \Rightarrow\ \|f(v) - f(v')\| < \epsilon.$$

3. *stetig,* wenn f an jeder Stelle stetig ist.

•

Schreibt man diese Bedingungen zur Verdeutlichung mit Hilfe der Distanzfunktion d um, dann ist zunächst die Beschränktheit von f äquivalent zu

$$\exists\ \rho \in \mathbb{R}\ \forall\ v \in V\colon\ d(f(0), f(v)) \leq \rho \cdot d(0, v).$$

Dies *zeigt zunächst, daß Beschränktheit die Stetigkeit an der Stelle* 0_V *impliziert.* Die Bedingung für Stetigkeit an der Stelle v sieht umformuliert so aus:

$$\forall\ \epsilon > 0\ \exists\ \delta > 0\ \forall\ v' \in V\colon\ d(v, v') < \delta\ \Rightarrow\ d(f(v), f(v')) < \epsilon.$$

Dies wiederum zeigt, daß sich — wegen der Translationsinvarianz — ggf. die Stetigkeit an der Stelle 0_V auf jede andere Stelle überträgt. Wir erhalten also den

4.1.38 Satz *Sind* V, W *normiert,* $f \in Hom_{\mathbb{R}}(V, W)$, *dann sind äquivalent:*

1. f *ist stetig,*
2. f *ist an der Stelle* 0_V *stetig,*
3. *es gibt eine Stelle* $v' \in V$, *an der* f *stetig ist.*

□

4.1.39 Satz *Unter den linearen Abbildungen zwischen normierten Räumen sind genau die beschränkten stetig.* □

Beweis: Ist f beschränkt, dann ist f an 0_V stetig ($\delta := \epsilon/(2\rho)$), also stetig.
Ist umgekehrt f stetig, dann insbesondere an der Stelle 0_V, es gibt also, zu $\epsilon := 1$, ein $\delta > 0$ mit:

$$\|v\| < \delta\ \Rightarrow\ \|f(v)\| < 1.$$

Zu $v \neq 0_V$ sei jetzt ein Vektor w definiert durch $w := \frac{\delta}{2}\frac{v}{\|v\|}$, dann ist $\|w\| = \frac{\delta}{2}$, also

$$1 > \|f(w)\| = \frac{\delta}{2}\frac{\|f(v)\|}{\|v\|},$$

und damit folgt

$$\|f(v)\| < \frac{2}{\delta}\|v\|. \qquad (*)$$

Da letzteres aber auch für $v := 0_V$ richtig ist, haben wir für *alle* $v \in V$ die Ungleichung $(*)$ bewiesen, f ist demnach beschränkt (mit $\rho = 2/\delta$).

□

4.1.40 Satz *Jede lineare Abbildung zwischen euklidischen Vektorräumen ist beschränkt und damit auch stetig.*

Beweis: Sei $\mathcal{B}$ eine Orthonormalbasisfolge von V, $\mathcal{C}$ eine Basisfolge von W, $f \in Hom_{\mathbb{R}}(V,W)$, V und W euklidisch, $A := M(\mathcal{C}, f, \mathcal{B})$. Dann gilt:

$$\begin{aligned}
&\|f(v)\| = \|A \cdot v\| = \|A \sum_i \langle v \mid b_i \rangle b_i\| = \|\sum_i \langle v \mid b_i \rangle A b_i\| \\
&\leq \sum_i |\langle v \mid b_i \rangle| \cdot \|A b_i\| \leq_{3.8.4} \sum_i \|v\| \cdot \|b_i\| \cdot \|A b_i\| \\
&\leq \|v\| \cdot \underbrace{n \cdot \max\{\|A b_i\| \mid i \in n\}}_{=:\rho}.
\end{aligned}$$

□

4.2 Die adjungierte Abbildung

Die Vektorräume dieses Paragraphen seien sämtlich euklidisch, die Norm kommt jetzt also vom inneren Produkt her,

$$\|v\| = \sqrt{\langle v \mid v\rangle}.$$

Zu $f \in Hom_{\mathbb{R}}(V,W)$ und $w \in W$ ist $\langle f(-) \mid w\rangle \in L(V)$, nach dem Rieszschen Darstellungssatz (4.1.31) gibt es also genau ein $v \in V$ mit

$$\langle f(-) \mid w\rangle = \langle - \mid v\rangle.$$

Die Zuordnung $w \mapsto v$ definiert also eine Abbildung $\tilde{f}$, und diese ist offenbar auch linear. Wir nennen sie die zu f *adjungierte* Abbildung, und sie erfüllt die folgende Gleichung, bzw. ist durch diese definiert:

4.2.1 $$\langle f(v) \mid w\rangle = \langle v \mid \tilde{f}(w)\rangle.$$

4.2.2 Hilfssatz *Die zu $f \in Hom_{\mathbb{R}}(V,W)$ adjungierte Abbildung $\tilde{f}$ hat die folgenden Eigenschaften:*

1. *f ist die adjungierte Abbildung zu $\tilde{f}$,*
2. *$W = \mathrm{Bild}(f) \oplus \mathrm{Kern}(\tilde{f})$,*
3. *Sind $\mathcal{B},\mathcal{C}$ Orthonormalbasisfolgen für V,W, dann gilt*
$$M(\mathcal{C}, f, \mathcal{B}) = {}^tM(\mathcal{B}, \tilde{f}, \mathcal{C}).$$
4. *Ist $V = W, g \in End_{\mathbb{R}}(V)$, dann ist $\widetilde{f \circ g} = \tilde{g} \circ \tilde{f}$, und irgend zwei Eigenvektoren v von f und $\tilde{v}$ von $\tilde{f}$ zu verschiedenen Eigenwerten κ und $\tilde{\kappa}$ sind orthogonal.*

Beweis:

1. $\langle f(v) \mid w\rangle = \langle v \mid \tilde{f}(w)\rangle = \langle \tilde{\tilde{f}}(v) \mid w\rangle$ ergibt $f = \tilde{\tilde{f}}$, da $\langle - \mid -\rangle$ nicht ausgeartet ist.
2. Folgt aus $\mathrm{Bild}(f)^\perp = \mathrm{Kern}(\tilde{f})$ mit 4.1.18.
3. Ist $A := M(\mathcal{C}, f, \mathcal{B})$, $\tilde{A} := M(\mathcal{B}, \tilde{f}, \mathcal{C})$, dann gilt
$$a_{jk} = \sum_i a_{ik}\langle c_i \mid c_j\rangle = \langle f(b_k) \mid c_j\rangle = \langle b_k \mid \tilde{f}(c_j)\rangle = \sum_i \tilde{a}_{ij}\langle b_k \mid b_i\rangle = \tilde{a}_{kj}.$$
4. $\langle (f \circ g)(v) \mid w\rangle = \langle g(v) \mid \tilde{f}(w)\rangle = \langle v \mid (\tilde{g} \circ \tilde{f})(w)\rangle$. Außerdem gilt für Eigenvektoren $v, \tilde{v}$ zu Eigenwerten $\kappa, \tilde{\kappa}$:
$$\begin{aligned}(\kappa - \tilde{\kappa})\langle v \mid \tilde{v}\rangle &= \langle \kappa v \mid \tilde{v}\rangle - \langle v \mid \tilde{\kappa}\tilde{v}\rangle \\ &= \langle f(v) \mid \tilde{v}\rangle - \langle v \mid \tilde{f}(\tilde{v})\rangle \\ &= \langle v \mid \tilde{f}(\tilde{v})\rangle - \langle v \mid \tilde{f}(v)\rangle \\ &= 0.\end{aligned}$$
Sind die beiden Eigenwerte verschieden, so folgt daraus $\langle v \mid \tilde{v}\rangle = 0$. □

4.2.3 Satz *Ist V euklidisch, dann gilt*

$$\varphi\colon End_{\mathbb{R}}(V) \simeq_{\mathbb{R}} BLF(V),\ f \mapsto \langle f(-) \mid - \rangle.$$

Beweis. Die Linearität von φ ist trivial. Die Injektivität folgt aus der Tatsache, daß $\langle f(-) \mid - \rangle\colon v \mapsto 0$ impliziert, daß f die Nullabbildung ist, denn dies bedeutet ja

$$\forall\ u, v \in V\colon\ \langle f(u) \mid v \rangle = 0,$$

also $f(u)$ im Nullraum und demnach $f(u) = 0$, für alle u, d. h. $f = 0$.
Die Surjektivität folgt so: Für $\Phi \in BLF(V), v \in V$, gibt es nach dem Rieszschen Darstellungssatz genau ein $u \in V$ mit

$$\Phi(v, -) = \langle u \mid - \rangle.$$

Damit ist $f\colon v \mapsto u$ wohldefiniert, und es gilt dafür offenbar $\varphi(f) = \Phi$. □

4.2.4 Beispiele
i) Ist $V := \mathbb{R}^n$ und $\langle - \mid - \rangle$ das Standardskalarprodukt, dann kann man die Werte von $\Phi := \langle f(-) \mid - \rangle \in BLF(V)$ mit Hilfe der Matrix $A := M(\mathcal{E}, f, \mathcal{E})$ berechnen:

$$\langle f(u) \mid v \rangle = \sum_i f(u)_i v_i = \sum_{i,k} a_{ik} u_k v_i = {}^t v \cdot A \cdot u.$$

Die Matrix A bezeichnen wir deshalb auch mit

$$M^{\Phi}_{\mathcal{E},\mathcal{E}}.$$

ii) Für $\tilde{\Phi} := \varphi(\tilde{f})$ (nach 4.2.3) gilt

$$\tilde{\Phi}(v, w) = \langle \tilde{f}(v) \mid w \rangle = \langle v \mid f(w) \rangle = \langle f(w) \mid v \rangle = \Phi(w, v).$$

Die zur adjungierten Abbildungen gemäß 4.6.3 gehörende Bilinearform erhält man also durch Vertauschen der Argumente. ◇
◇

4.2.5 Definition (normal) $f \in End_{\mathbb{R}}(V)$ heißt *normal,* wenn gilt

$$f \circ \tilde{f} = \tilde{f} \circ f.$$

•

4.2.6 Hilfssatz $f \in End_{\mathbb{R}}(V)$, *dann sind äquivalent.*

1. *f ist normal,*
2. $\langle f(v) \mid f(w) \rangle = \langle \tilde{f}(v) \mid \tilde{f}(w) \rangle$.
3. $\|f(v)\|^2 = \|\tilde{f}(v)\|^2$.

Beweis: Nachrechnen. □

4.2.7 Hilfssatz *Ist $f \in End_{\mathbb{R}}(V)$ normal, dann gilt*

1. $\mathrm{Kern}(f) = \mathrm{Kern}(\tilde{f})$,
2. $V = \mathrm{Bild}(f) \oplus \mathrm{Kern}(f)$,
3. $\forall\, n \in \mathbb{N}^*$: $\mathrm{Rang}(f) = \mathrm{Rang}(f^n)$,
4. $\widetilde{f - \rho \cdot id_V} = \tilde{f} - \rho \cdot \mathrm{id}_V$,
5. $f - \rho \cdot id_V$ *ist normal.*
6. f *und* $\tilde{f}$ *haben dieselben Eigenwerte und Eigenvektoren.*

Beweis:

1. Die erste Behauptung folgt unmittelbar aus 4.2.6 iii).
2. Die zweite Behauptung ergibt sich aus 4.2.2 ii) mit der gerade bewiesenen ersten Behauptung.
3. Aus 1. folgt, daß die Einschränkung $f \downarrow \mathrm{Bild}(f)$ regulär ist. Es folgt
$$\mathrm{Rang}(f^2) = \dim(f(\mathrm{Bild}(f))) = \dim(\mathrm{Bild}(f)) = \mathrm{Rang}(f),$$
und ganz analog ergibt sich $\mathrm{Rang}(f^3) = \mathrm{Rang}(f)$, usw.
4. Nachrechnen.
5. Nachrechnen.
6. Die Gleichungen
$$\mathrm{Kern}(f - \rho \cdot \mathrm{id}_V) = \mathrm{Kern}(\widetilde{f - \rho \cdot \mathrm{id}_V}) = \mathrm{Kern}(\tilde{f} - \rho \cdot \mathrm{id}_V)$$
ergeben die Identität der entsprechenden Eigenräume:
$$E_f(\rho) = E_{\tilde{f}}(\rho).$$

□

4.2.8 Satz *Sei $f \in End_{\mathbb{R}}(V)$ und $V = V_1 \oplus \ldots \oplus V_r$ mit paarweise orthogonalen V_i (d.h. $V_i \subseteq V_j^{\perp}$, falls $i \neq j$), kurz:*
$$V = V_1 \perp \ldots \perp V_r.$$
Sind zudem die V_i invariant unter f, d.h. $f(V_i) \subseteq V_i$, dann ist f genau dann normal, wenn die V_i auch unter den $\tilde{f}_i$ (zu $f_i := f \downarrow V_i$) invariant und die f_i normal sind. □

Beweis:
i) Sei f normal. Wir zeigen zunächst die Invarianz $\tilde{f}_i(V_i) \subseteq V_i$: Ist $v_j \in V_j, j \neq i$, dann gilt

$$\langle v_j \mid \tilde{f}(v_i)\rangle = \langle f(v_j) \mid v_i\rangle = 0,$$

also, für alle $j \neq i$: $\tilde{f}(v_i) = \tilde{f}_i(v_i) \in V_j^{\perp}$, und damit

$$\tilde{f}_i(v_i) \in \bigcap_{j\neq i} V_j^{\perp} = V_i.$$

Zum Nachweis der Normalität von f_i beachten wir, daß

$$\|f_i(v_i)\|^2 = \|f(v_i)\|^2 = \|\tilde{f}(v_i)\|^2 = \|\tilde{f}_i(v_i)\|^2.$$

Daraus folgt die Normalität von f_i nach 4.2.6.
ii) Jetzt seien umgekehrt die f_i normal und die V_i invariant unter den $\tilde{f}_i$. Ist $v = \sum_1^r v_i$, mit $v_i \in V_i$, dann gilt

$$\|f(v)\|^2 = \|\sum_i f_i(v_i)\|^2 = \sum_i \|f_i(v_i)\|^2,$$

letzteres wegen $f_i(v_i) \in V_i \perp V_j, j \neq i$. Da die f_i als normal vorausgesetzt sind, gilt weiter:

$$= \sum_i \|\tilde{f}_i(v_i)\|^2 = \|\tilde{f}(v)\|^2,$$

also ist auch f normal. □

Wir nennen $f \in End_{\mathbb{R}}(V)$ natürlich genau dann *selbstadjungiert,* wenn

$$\tilde{f} = f$$

gilt. Unmittelbar aus 4.2.2 ergibt sich für solche Abbildungen, daß sie bzgl. Orthonormalbasisfolgen $\mathcal{B}$ durch symmetrische Matrizen dargestellt werden:

$$M(\mathcal{B}, f, \mathcal{B}) = {}^tM(\mathcal{B}, f, \mathcal{B}).$$

Eines unserer Ziele ist der Nachweis der Tatsache, daß selbstadjungierte lineare Endomorphismen eines n-dimensionalen euklidischen Raumes n paarweise orthogonale Eigenvektoren besitzen. Dazu betrachten wir die Abbildung

$$\varphi\colon V\backslash\{0_V\} \to \mathbb{R}, v \mapsto \frac{\langle v \mid f(v)\rangle}{\langle v \mid v\rangle}.$$

4.2.9 Bemerkungen Diese Funktion φ hat die folgenden Eigenschaften:

- $\forall\ \rho \in \mathbb{R}^*, v \in V\colon\ \varphi(\rho v) = \varphi(v)$.
- Ist $\mathcal{B}$ eine ON-Basisfolge, $A := M(\mathcal{B}, f, \mathcal{B})$, dann gilt

  $$\langle v \mid f(v)\rangle = \sum_{i,k} a_{ik} v_i v_k,$$

  $v \mapsto \langle v \mid f(v)\rangle$ ist also eine Polynomabbildung und demnach stetig. Dies gilt natürlich insbesondere für $v \mapsto \langle v \mid v\rangle$.

- Als Quotient stetiger Funktionen nimmt φ auf der *Einheitssphäre,* d.h. auf der Menge $\{v \mid \|v\| = 1\}$, ein Minimum an, etwa bei $b_0 \in V$, d.h. es gilt

$$\|v\| = 1 \Longrightarrow \varphi(v) \geq \varphi(b_0).$$

- Mit dem ersten Punkt folgt dann weiter:

$$\forall\ v \in V \backslash \{0_V\}\colon\ \varphi(v) \geq \varphi(b_0).$$

$\diamond$

4.2.10 Hilfssatz *b_0 ist Eigenvektor von f zum Eigenwert $\langle b_0 \mid f(b_0)\rangle$.*

Beweis: Sei $v \in V$ und

$$\psi\colon \mathbb{R} \to \mathbb{R}, x \mapsto \varphi(b_0 + xv).$$

Nach 4.2.9 nimmt ψ an der Stelle $x = 0$ ein Minimum an, es gilt also $\psi'(0) = 0$. Einsetzen der Definition von φ und Differenzieren nach x ergibt

$$\psi'(0) = 2\langle b_0 \mid f(v)\rangle - 2\langle b_0 \mid f(b_0)\rangle\langle b_0 \mid v\rangle.$$

Setzen wir dies gleich Null, so folgt

$$0 = \langle f(b_0) - \langle b_0 \mid f(b_0)\rangle b_0 \mid v\rangle,$$

und zwar für *alle* $v \in V$. Das impliziert

$$f(b_0) = \langle b_0 \mid f(b_0)\rangle b_0,$$

wie behauptet.

$\square$

4.2.11 Satz *Zu jedem selbstadjungierten linearen Endomorphismus f eines euklidischen Vektorraums gibt es eine Orthonormalbasisfolge aus Eigenvektoren.*

Beweis: f besitzt nach 4.2.10 einen Eigenvektor b_0. Wir betrachten die orthogonale Zerlegung

$$V = \langle b_0\rangle \perp \langle b_0\rangle^\perp$$

und verwenden, daß $f\langle b_0\rangle^\perp \subseteq\ \langle b_0\rangle^\perp$:

$$\forall\ v \in \langle b_0\rangle^\perp\colon\ \langle b_0 \mid f(v)\rangle = \langle f(b_0) \mid v\rangle = \langle b_0 \mid f(b_0)\rangle \cdot \langle b_0 \mid v\rangle = 0.$$

Mit f ist auch die Einschränkung $f \downarrow \langle b_0\rangle^\perp$ selbstadjungiert, obige Überlegungen ergeben also einen Eigenvektor der Norm 1 in $\langle b_0\rangle^\perp$ usw. Die Behauptung folgt also per Induktion nach der Dimension von V.

$\square$

Selbstadjungierte lineare Abbildungen auf euklidischen Vektorräumen werden, wie wir wissen, durch symmetrische Matrizen beschrieben, es gilt aber auch die Umkehrung: Reell symmetrische Matrizen A beschreiben selbstadjungierte Abbildungen f, z.B. kann man f durch $M(\mathcal{B}, f, \mathcal{B}) := A$ definieren mit irgendeiner ON-Basisfolge $\mathcal{B}$. Man rechnet leicht nach, daß dieses f selbstadjungiert ist. Es ergeben sich also die

4.2.12 Folgerungen

1. *Reelle symmetrische Matrizen sind diagonalisierbar.*
2. *Ist $A \in \mathbb{R}^{n\times n}$ symmetrisch, dann hat A lauter reelle Eigenwerte λ_i, für diese gilt*
$$p_A = (-1)^n \prod_{i=0}^{n-1} (x - \lambda_i).$$
3. *Zu jeder symmetrischen Bilinearform auf einem euklidischen Vektorraum V gibt es eine Orthonormalbasisfolge $\mathcal{B}$ in V, bzgl. derer die Form durch eine Diagonalmatrix beschrieben wird.*

□

Die Transformation auf Diagonalgestalt bezeichnet man auch als *Hauptachsentransformation,* wir werden auf Anwendungen (wie z.B. die Klassifizierung von Kegelschnitten) noch zu sprechen kommen.

4.2.13 Definition (Projektion,Orthogonalprojektion) Ein linearer Endomorphismus $f \in \mathrm{End}_{\mathbb{K}}(V)$ eines Vektorraumes heißt *Projektion,* wenn $f^2 = f$ gilt. Ein Projektion heißt *Orthogonalprojektion,* wenn sie selbstadjungiert ist. •

4.2.14 Hilfssatz *Ist $f \in End_{\mathbb{R}}(V)$ ein Projektion, dann gilt*

$$V = \mathrm{Kern}(f) \oplus \mathrm{Bild}(f),$$

und

$$f = 0_{\mathrm{Kern}(f)} \oplus \mathrm{id}_{\mathrm{Bild}(f)}.$$

Ist f darüberhinaus selbstadjungiert, also eine Orthogonalprojektion, dann ist f normal. Umgekehrt ist jede normale Projektion eine Orthogonalprojektion.

Beweis:

i) Ist f Projektion, d.h. $f^2 = f$, dann ist zunächst die Summe $\mathrm{Kern}(f)+\mathrm{Bild}(f)$ direkt: $v \in \mathrm{Kern}(f)\cap\mathrm{Bild}(f)$, etwa $v = f(w)$, ergibt $0 = f(v) = f^2(w) = f(w) = v$. Diese direkte Summe ist darüberhinaus gleich V : Für $v \in V$ gibt es $w \in V$ mit $v = f(v) + w$, denn V ist eine additive Gruppe. Der Summand w liegt im $\mathrm{Kern}(f)$, da $f(v) = f^2(v) + f(w) = f(v) + f(w)$. Jedes $v \in V$ ist demnach als Summe aus einem Element des Kerns und einem Element des Bildes darstellbar. Damit ist der erste Teil der Behauptung bewiesen.

ii) Der zweite Teil, die Beschreibung von f als Summe aus der Nullabbildung auf dem Kern und der identischen Abbildung auf dem Bild von f folgt direkt aus dem ersten Teil, denn dieser liefert die Zerlegung in Nullabbildung auf dem Kern und der Einschränkung auf das Bild, und die Gleichung $f^2 = f$ zeigt noch, daß diese Einschränkung gleich der identischen Abbildung ist.

iii) Die Normalität jeder Othogonalprojektion f ist trivial:

$$\tilde{f} \circ f = f \circ f = f \circ \tilde{f},$$

da f selbstadjungiert ist.

iv) Ist umgekehrt f normale Projektion, $v \in V$ und wieder $v = f(v) + w, w \in \text{Kern}(f)$, dann gilt

$$\langle v \mid f(u)\rangle = \langle f(v) + w \mid f(u)\rangle = \langle f(v) \mid f(u)\rangle,$$

letzteres wegen $w \in \text{Kern}(f) = \text{Kern}(\tilde{f})$. Analog ergibt sich

$$\langle f(v) \mid u\rangle = \langle f(v) \mid f(u)\rangle,$$

also insgesamt

$$\langle v \mid f(u)\rangle = \langle f(u) \mid v\rangle.$$

Das liefert $\tilde{f} = f$, wie behauptet.

□

4.2.15 Hilfssatz

1. *Ist U ein Unterraum von V, dann gibt es genau eine Orthogonalprojektion $f \in End_{\mathbb{R}}(V)$ mit* $\text{Bild}(f) = U$, *nämlich* $f := \text{id}_U \oplus 0_{U^\perp}$.
2. *Sind $U_1, U_2 \leq_{\mathbb{R}} V$ und f_1, f_2 die zugehörigen Orthogonalprojeektionen gemäß i), dann gilt:*
   - $f_2 \circ f_1 = 0 \Longleftrightarrow U_1 \perp U_2$,
   - $f_1 + f_2$ *ist Orthogonalprojektion* $\Longleftrightarrow U_1 \perp U_2$,
   - $f_1 - f_2$ *ist Orthogonalprojektion* $\Longleftrightarrow U_2 \subseteq U_1$,
   - $f_1 \circ f_2$ *ist Orthogonalprojektion* $\Longleftrightarrow f_2 \circ f_1 = f_1 \circ f_2$.

Beweis: Übungsaufgabe. □

4.2.16 Definition (schiefsymmetrisch) $f \in End_{\mathbb{R}}(V)$ heißt *schiefsymmetrisch,* wenn $\tilde{f} = -f$ gilt. •

4.2.17 Folgerung *Ist f schiefsymmetrisch und $\mathcal{B}$ eine Orthogonalbasisfolge, dann gilt*

$$M(\mathcal{B}, f, \mathcal{B}) = -\,{}^t M(\mathcal{B}, f, \mathcal{B}),$$

d.h. die f darstellende Matrix ist schiefsymmetrisch.

□

Offensichtlich richtig ist

4.2.18 Hilfssatz

i) Ist $f \in End_{\mathbb{R}}(V)$, dann sind äquivalent:

1. *f ist schiefsymmetrisch,*
2. $\langle f(v) \mid w\rangle + \langle v \mid f(w)\rangle = 0$,

3. $\langle v \mid f(v)\rangle = 0$.

ii) Ist $f \in End_{\mathbb{R}}(V)$ schiefsymmetrisch, dann gilt:

1. *0 ist ggf. der einzige Eigenwert von f,*
2. $Spur f = 0$,
3. $\det(f) = (-1)^{dim(V)} \det(f)$,
4. $dim_{\mathbb{R}}(V)$ *ungerade* $\Longrightarrow \det(f) = 0$,
5. $Rg(f)$ *ist gerade.*

iii) Der Rang jeder schiefsymmetrischen Matrix ist gerade.

□

4.2.19 Satz *Ist $f \in End_{\mathbb{R}}(V)$ schiefsymmetrisch, dann gibt es eine Orthonormalbasisfolge $\mathcal{B}$ und reelle Zahlen κ_i mit*

$$M(\mathcal{B}, f, \mathcal{B}) = \begin{pmatrix} 0 & -\kappa_0 & & & & 0 \\ \kappa_0 & 0 & & & & \\ & & 0 & -\kappa_1 & & \\ & & \kappa_1 & 0 & & \\ & & & & \ddots & \\ 0 & & & & & \end{pmatrix}$$

□

Beweis: Die Abbildung $\varphi := f^2$ ist selbstadjungiert, es gibt also eine 0N-Basisfolge $\mathcal{C} = (c_0, \ldots, c_{n-1})$ aus Eigenvektoren von φ, sei etwa $\varphi(c_i) = \lambda_i c_i$.

Wir zeigen zunächst, daß $\lambda_i \leq 0$: Da die c_i Vektoren mit Norm 1 sind, gilt

$$\lambda_i = \langle c_i \mid \varphi(c_i)\rangle = \langle c_i \mid f^2(c_i)\rangle = -\langle f(c_i) \mid f(c_i)\rangle \leq 0.$$

Rang(φ) ist gerade, denn Rang(φ) = Rang(f^2) = Rang(f), und letzterer ist nach **??** gerade.

Die Anzahl der negativen Eigenwerte von φ gleicht dem Rang von φ, ist also gerade. $c_0, \ldots, c_{2s-1}$ seien die zugehörigen Eigenvektoren. Setzen wir jetzt

$$b_{2\nu+1} := c_\nu, b_{2\nu} := \sqrt{-\lambda_\nu^{-1}} \cdot f(c_\nu), 0 \leq \nu \leq s-1,$$

und

$$b_\nu := c_\nu, \nu \geq 2s,$$

dann hat die Basisfolge $\mathcal{B}$ offenbar die gewünschten Eigenschaften, mit $\kappa_i := \sqrt{-\lambda_\nu}$, wie man leicht nachrechnet:

$$f(b_{2\nu+1}) = f(c_\nu) = \sqrt{-\lambda_\nu} \cdot b_{2\nu} = \kappa_\nu b_{2\nu},$$

$$f(b_{2\nu}) = f(\sqrt{-\lambda_\nu^{-1}} \cdot f(c_\nu)) = \sqrt{-\lambda_\nu} \cdot f^2(b_{2\nu}) = -\kappa_\nu b_{2\nu+1},$$

□

4.3 Affine Punkträume

Es wird jetzt der Übergang von der linearen Algebra zur *analytischen Geometrie* beschrieben.

4.3.1 Definition (affiner Punktraum) Sei V ein $\mathbb{K}$-Vektorraum, A eine nicht leere Menge und

$$\overrightarrow{=}: A \times A \to V, (P, Q) \to \overrightarrow{PQ}$$

eine Abbildung. Dann heißt $(A, \overrightarrow{=})$ *affiner Punktraum* zu V, wenn gilt:

1. $\forall\ P \in A, v \in V\ \exists_1\ Q \in A:\ \overrightarrow{PQ} = v.$
   (Kurz: $Q = P + v$.)
2. $\forall\ P, Q, R \in A:\ \overrightarrow{PQ} + \overrightarrow{QR} = \overrightarrow{PR}.$

•

Die Elemente von A heißen *Punkte.* Ist V $n-$dimensional, so heißt auch A *$n-$dimensional:*

$$\dim_{\mathbb{K}}(A) := \dim_{\mathbb{K}}(V).$$

V wird zur Verdeutlichung auch mit $V(A)$ bezeichnet.

4.3.2 Beispiel Zu V sei $A := V$ und

$$\overrightarrow{=}: A \times A = V \times V \to V, (v_0, v_1) \mapsto \overrightarrow{v_0 v_1} := v_1 - v_0.$$

Dieser affine Punktraum zu V wird mit $D(V)$ bezeichnet. ◇

Leicht nachzuprüfen ist

4.3.3 Hilfssatz *Ist $(A, \overrightarrow{=})$ affiner Raum zu V und sind $P, Q, R, S \in A$, dann gilt:*

1. $\overrightarrow{PQ} = 0_V \iff P = Q,$
2. $\overrightarrow{PQ} = -\overrightarrow{QP},$
3. $\overrightarrow{PQ} = \overrightarrow{RS} \Longrightarrow \overrightarrow{PR} = \overrightarrow{QS}$ (Parallelogrammregel).

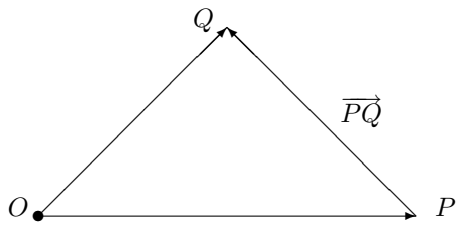
□

Greifen wir uns einen Punkt $0 \in A$ als *Ursprungspunkt* heraus, so ist nach 4.3.1 $P \in A$ eindeutig durch den Vektor $p := \overrightarrow{OP} \in V$ bestimmt, seinen *Ortsvektor.* P kann dann mit p *identifiziert* werden, d.h. wir haben die Bijektion

4.3.4 $$A \to V, P \mapsto p := \overrightarrow{OP}.$$

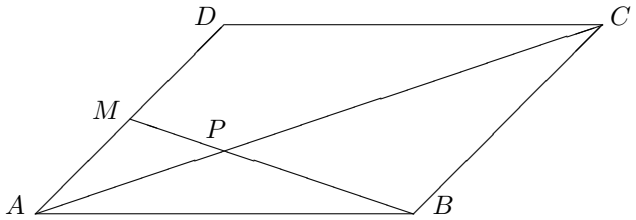
Der Differenzvektor $\overrightarrow{PQ}$ von P und Q genügt dann der Gleichung

4.3.5 $$\overrightarrow{PQ} = q - p.$$



Wie man nun damit die lineare Algebra auf die Elementargeometrie anwenden kann zeigt folgendes Beispiel:

4.3.6 Beispiel Wir wollen beweisen, daß die Diagonale und die Seitenhalbierende sich in nicht ausgearteten Parallelogrammen im Verhältnis 1:2 schneiden. Beweis: Wir betrachten das Parallelogramm, dessen Punkte wie skizziert bezeichnet seien:



Gesucht sind $\lambda, \mu \in \mathbb{R}$ mit $\overrightarrow{PM} = \lambda\overrightarrow{BM}$ und $\overrightarrow{AP} = \mu\overrightarrow{AC}$. Dazu betrachten wir das Dreieck AMP, für welches gilt:

$$\overrightarrow{AM} + \overrightarrow{MP} + \overrightarrow{PA} = 0,$$

bzw.

$$\frac{1}{2}\overrightarrow{AD} - \overrightarrow{\lambda BM} - \overrightarrow{\mu AC} = 0.$$

Das ist nach 4.3.1 ii) äquivalent zu

$$\frac{1}{2}\overrightarrow{AD} - \lambda(\overrightarrow{BA} + \overrightarrow{AM}) - \mu(\overrightarrow{AB} + \overrightarrow{BC}) = 0.$$

Da es sich um ein Parallelogramm handelt, gilt $\overrightarrow{BC} = \overrightarrow{AD}$, so daß sich hieraus folgendes ergibt:

$$(\frac{1}{2} - \frac{\lambda}{2} - \mu)\overrightarrow{AD} + (\lambda - \mu)\overrightarrow{AB} = 0.$$

Das Parallelogramm ist genau dann nicht ausgeartet, wenn $(\overrightarrow{AD}, \overrightarrow{AB})$ linear unabhängig ist, so daß wir schließlich folgendes Gleichungssystem für die gesuchten Parameter bekommen:

$$\begin{aligned} \lambda - \mu &= 0 \end{aligned}$$

$$\frac{1}{2} - \frac{\lambda}{2} - \mu \quad = \quad 0.$$

Die einzige Lösung ist $\lambda = \mu = \frac{1}{3}$, wie behauptet. $\diamond$

4.3.7 Definition (affine Koordinaten, Unterräume und Abbildungen) A sei ein affiner Punktraum zu V.

i) Ein Ursprungspunkt $O \in A$ ergibt zusammen mit irgendeiner Basisfolge $\mathcal{B} = (b_0, \ldots, b_{n-1})$ von $V = V(A)$ ein *affines Koordinatensystem*

$$(O; \mathcal{B}) = (O; b_0, \ldots, b_{n-1}).$$

Die diesbezüglichen Komponenten p_i des Ortsvektors $p = \overrightarrow{OP}$ von $P \in A$:

$$\overrightarrow{OP} = \sum_i p_i b_i$$

heißen die *affinen Koordinaten* von P bezüglich $(0; b_0, \ldots, b_{n-1})$.

ii) $B \subseteq A$ heißt *affiner Unterraum* von A, (kurz: $B \leq A$), wenn gilt:

$$\exists\, P_0 \in B : \ \{\overrightarrow{P_0 Q} \mid Q \in B\} \ \leq \ V(A).$$

Dieser Vektorraum $\{\overrightarrow{P_0 Q} \mid Q \in B\}$ ist offenbar unabhängig von der getroffenen Auswahl von $P_0 \in B$ und kann deshalb mit $V(B)$ bezeichnet werden, er heißt auch die *Richtung* von B.

In Anlehnung an die Elementargeometrie heißen eindimensionale affine Unterräume *Geraden,* zweidimensionale heißen *Ebenen.* $(n-1)-$dimensionale Unterräume — n die Dimension von A — heißen *Hyperebenen.*

iii) Sind $B_0, \ldots, B_m$ affine Unterräume von A, dann heißt der kleinste affine Unterraum, der $\cup_i B_i$ umfaßt, der *Verbindungsraum* der B_i. Er wird mit

$$B_0 \vee \ldots \vee B_m$$

bezeichnet. Beispielsweise sind Punkte $P, Q \in A$ (nulldimensionale) affine Unterräume. Der Verbindungsraum $P \vee Q$ heißt deren *Verbindungsgerade,* usw.

iv) Zwei Unterräume B_0, B_1 eines affinen Punktraumes A heißen *parallel,* kurz

$$B_0 \| B_1,$$

wenn die Richtung eines von ihnen in der Richtung des anderen enthalten ist:

$$\exists\, i\colon\ V(B_i) \subseteq V(B_j),\ j \neq i.$$

(B_0 und B_1 sind dann offenbar disjunkt oder einer ist im anderen enthalten.) Disjunkte und nicht zueinander parallele Unterräume heißen *windschief.*

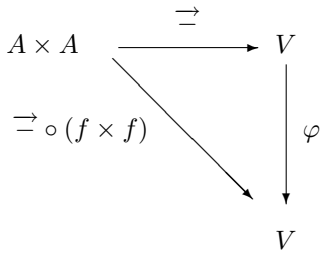
v) Eine Abbildung $f: A \to A, P \mapsto P'$ heißt *affine Abbildung*, wenn

$$\overrightarrow{P_1Q_1} = \overrightarrow{P_2Q_2} \Longrightarrow \overrightarrow{P_1'Q_1'} = \overrightarrow{P_2'Q_2'}$$

und die von f induzierte Abbildung

$$\varphi: V \to V, \overrightarrow{PQ} \mapsto \overrightarrow{P'Q'}$$

linear ist, also die Abbildung φ, die folgendes Diagramm kommutativ ergänzt:



•

4.3.8 Beispiele Für irgend zwei Punkte aus einem affinen Raum A zu einem Vektorraum V über $GF(2)$ gilt:

$$P \vee Q = \{P, Q\}.$$

Demnach enthält jede Teilmenge eines solchen affinen Unterraums mit zwei Punkten auch deren Verbindungsgerade. Es ist jedoch nicht jede Teilmenge eines affinen Raums zu $GF(2)^2$ ein affiner Unterraum. Das liegt an der Charakteristik von $GF(2)$, denn bei $\text{char}(\mathbb{K}) \neq 2$ folgt aus der Tatsache, daß $B \subseteq A$ nicht leer ist und mit je zwei Punkten auch deren Verbindungsgerade enthält, daß B ein affiner Unterraum ist (vgl. Übungsblatt). ◇

◇

4.3.9 Hilfssatz *Zu jedem $\varphi \in End_{\mathbb{K}}(V)$ und jedem Punktepaar $(O, O') \in A^2$ gibt es genau eine affine Abbildung $f: A \to A$, mit $f(O) = O'$, die gemäß 4.3.7 v) die lineare Abbildung φ induziert, nämlich*

$$f: P \mapsto P', \text{ mit } \overrightarrow{OP'} = \overrightarrow{OO'} + \varphi(\overrightarrow{OP}).$$

Mit Hilfe von Ortsvektoren $p = \overrightarrow{OP}$ läßt sich diese Abbildung auch wie folgt schreiben:

$$f: x \mapsto x' = \varphi(x) + t, \text{ mit } t := \overrightarrow{OO'}.$$

Affine Abbildungen $f: x \mapsto x' = \varphi(x) + t$ mit $\varphi = \text{id}_V$ heißen *Translationen.* Offenbar ist die affine Abbildung f genau dann injektiv, surjektiv, bijektiv, wenn dies für die induzierte lineare Abbildung φ gilt. Die Inverse f^{-1} einer affinen

Abbildung f induziert die Inverse φ^{-1} der von f induzierten linearen Abbildung φ. Die bijektiven affinen Abbildungen ergeben, zusammen mit der Komposition als Verknüpfung, eine Gruppe, die *affine Gruppe*

$$\mathrm{Aff}(A)$$

von A.
Unter den Teilmengen affiner Räume sind solche der folgenden Form besonders wichtig:

4.3.10 Definition (allgemeine Lage, Parallelepiped, Simplex) A sei ein affiner Raum, $P_0, \ldots, P_m \in A$.

i) Die P_ν heißen Punkte in *allgemeiner Lage,* wenn sie in keinem $(m-1)-$dimensionalen Unterraum liegen, d.h. wenn die Folge $(\overrightarrow{P_0P_1}, \ldots, \overrightarrow{P_0P_m})$ linear unabhängig ist, bzw. wenn

$$\dim(P_0 \vee P_1 \vee \ldots \vee P_m) = m.$$

ii) Sind $P_0, \ldots, P_m$, Punkte in allgemeiner Lage und ist $\mathbb{K} = \mathbb{R}$, dann heißt

$$\{P_0 + \sum_{i=1}^{m} \kappa_i \overrightarrow{P_0P_i} \mid 0 \leq \kappa_i \leq 1\}$$

das von den P_i aufgespannte *Parallelepiped.* Die Teilmenge

$$\{P_0 + \sum_{i=1}^{m} \rho_i \overrightarrow{P_0P_i} \mid 0 \leq \kappa_i \leq 1, \sum_i \kappa_i = 1\}$$

heißt das von den P_i aufgespannte *Simplex.*

•

Affine Räume A mit euklidischen Vektorräumen $V(A)$ nennt man *euklidische Räume.* Die hier definierte Metrik ergibt eine *Distanzfunktion*

$$\rho(P, Q) := \|\overrightarrow{PQ}\|,$$

und auch die anderen für euklidische Vektorräume behandelten metrischen Konzepte erfahren eine geometrische Interpretation. Affine Abbildungen, die die Distanzen erhalten, heißen *starre Bewegungen.* Die zugehörigen linearen φ gehören zu der folgenden Klasse linearer Abbildungen:

4.3.11 Definition (Isometrie) $f \in Hom_{\mathbb{R}}(V, W)$ heißt *Isometrie*, wenn f das innere Produkt *invariant läßt:* $\langle f(v_1) \mid f(v_2)\rangle = \langle v_1 \mid v_2\rangle$. •

Aus den vorangegangenen Überlegungen über lineare Abbildungen zwischen euklidischen Vektorräumen ergeben sich leicht die folgenden Eigenschaften von Isometrien:

4.3.12 Satz

i) Genau die die Norm erhaltenden linearen Abbildungen sind Isometrien.

ii) Isometrien sind injektiv.

iii) Isometrien f zwischen euklidischen Vektorräumen derselben Dimension sind Isomorphismen, und für sie gilt $\tilde{f} = f^{-1}$.

iv) Gilt für $f \in Hom_{\mathbb{R}}(V, W)$ die Gleichung $\tilde{f} = f^{-1}$, dann ist f Isometrie.

v) Isometrien zwischen euklidischen Vektorräumen derselben Dimension bilden Orthonormalbasisfolgen auf Orthonormalbasisfolgen ab, und umgekehrt sind Isomorphismen mit dieser Eigenschaft Isometrien.

vi) Ist $f \in \mathrm{End}_{\mathbb{R}}(V)$ eine Isometrie, dann ist

$$\det(f) \in \{1, -1\}$$

und Eigenwerte sind ggf. auch aus der Menge $\{1, -1\}$.

4.3.13 Definition (Rotation) $f \in End_{\mathbb{R}}(V)$ heißt *Rotation,* wenn f isometrisch ist. Die Rotationen f mit $\det(f) = 1$ heißen dabei *eigentliche,* die anderen *uneigentliche* Rotationen. •

Es gibt natürlich auch Rotationen, die überhaupt keine Eigenwerte im vorgegebenen Grundkörper haben, z. B. die Abbildung f mit

$$M(\mathcal{E}, f, \mathcal{E}) := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Sie beschreibt eine eigentliche Rotation des euklidischen Vektorraums $\mathbb{R}^2$ mit Standardskalarprodukt $\langle v \mid w \rangle := \sum v_i w_i$ und besitzt keinerlei Eigenwert in $\mathbb{R}$. Aus den Ergebnissen über die Existenz von Eigenwerten im Reellen, die mittels Zwischenwertsatz erzielt worden waren, erhalten wir (weil das Quadrat eines Eigenwerts λ einer Isometrie gleich 1 ist):

4.3.14 Folgerung *Eigentliche (uneigentliche) Rotationen von Räumen ungerader Dimension besitzen einen Eigenwert $1(-1)$. Uneigentliche Rotationen auf Räumen gerader Dimension besitzen die beiden Eigenwerte ± 1.*

Eine weitere leicht einzusehende Folgerung formuliert

4.3.15 Hilfssatz *Ist $U \leq V$ invariant unter der Rotation f, dann auch $U^{\perp}$.*

Sind $f, g \in End_{\mathbb{R}}(V)$ Rotationen, dann auch f^{-1} und $g \circ f^{-1}$. Die Rotationen bilden also eine Untergruppe $O(V)$ in der Gruppe $GL(V)$ der regulären linearen Automorphismen von V, sie heißt die *(volle) orthogonale Gruppe* von V, denn die Rotationen sind, wegen $\tilde{f} = f^{-1}$ orthogonale Abbildungen:

$$O(V) \leq GL(V).$$

Den Kern der Abbildungen det : $GL(V) \to \mathbb{R}^*$ bilden die eigentlichen Rotationen, er heißt die *spezielle orthogonale Gruppe* und wird mit $SO(V)$ bezeichnet:

$$SO(V) := \text{Kern}(\det \downarrow GL(V)) = \{A \in GL(V) \mid \det(A) = 1\}.$$

4.3.16 *Falls $V \neq \{0_V\}$ ist, gilt*

i) $SO(V) := \{f \in O(V) \mid \det(f) = 1\} \triangleleft O(V)$,

ii) $|O(V)/SO(V)| = 2$.

Es soll nun gezeigt werden, daß eine Rotation $f \in End_{\mathbb{R}}(V)$ eine direkte Zerlegung von V ergibt in invariante und orthogonale Unterräume der Dimension 1 oder 2.

4.3.17 Satz *Ist $f \in Aut_{\mathbb{R}}(V)$ eine Rotation, dann gibt es eine Orthonormalbasisfolge $\mathcal{B}$ von V mit*

$$M(\mathcal{B}, f, \mathcal{B}) = \begin{pmatrix} \epsilon_0 & & & & & & & 0 \\ & \ddots & & & & & & \\ & & \epsilon_{m-1} & & & & & \\ & & & \cos(\omega_1) & -\sin(\omega_1) & & & \\ & & & \sin(\omega_1) & \cos(\omega_1) & & & \\ & & & & & \ddots & & \\ & & & & & & \cos(\omega_r) & -\sin(\omega_r) \\ 0 & & & & & & \sin(\omega_r) & \cos(\omega_r) \end{pmatrix},$$

wobei $\epsilon_\nu \in \{1, -1\}, 0 \leq \nu \leq m-1$.

Beweis: i) Wir bemerken zunächst, daß die Summe der Eigenräume $E(1), E(-1)$ direkt ist:

$$U := E(1) + E(-1) = E(1) \oplus E(-1).$$

Nach dem letzten Hilfssatz ist die entsprechende Zerlegung

$$V = U \oplus U^\perp = E(1) \oplus E(-1) \oplus (E(1) \oplus E(-1))^\perp$$

eine Zerlegung in invariante Unterräume. Die Wahl einer an U und an die Zerlegung von U in die Eigenräume angepaßten Basisfolge $\mathcal{B}$ ergibt den ersten

diagonalen Teil der Matrix von f mit den Einträgen ϵ_i, wie behauptet:

$$M(\mathcal{B}, f, \mathcal{B}) = \left(\begin{array}{cccc|c} 1 & & & 0 & \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & 0 \\ & & & & \ddots \\ 0 & & & & -1 \\ \hline & & 0 & & * \end{array}\right).$$

ii) Da die Einschränkung $f \downarrow U^\perp = f \downarrow (E(1) \oplus E(-1))^\perp$ keinen Eigenwert besitzt, hat dieser Raum gerade Dimension. Wir zeigen, daß dieser Unterraum eine unter f invariante Ebene enthält:
Die Einschränkung F von $f + \tilde{f} = f + f^{-1}$ auf $(E(1) \oplus E(-1))^\perp$ ist selbstadjungiert, besitzt also einen Eigenvektor e, λ sei der zugehörige Eigenwert. Da f in $(E(1) \oplus E(-1))^\perp$ keinen Eigenvektor besitzt, sind e und $f(e)$ linear unabhängig:

$$W := \langle e, f(e) \rangle \Longrightarrow \dim_{\mathbb{R}}(W) = 2.$$

Diese Ebene ist invariant unter f, denn

$$F(e) = f(e) + f^{-1}(e) = \lambda \cdot e \Longrightarrow f^2(e) = \lambda \cdot f(e) - e.$$

Die Einschränkung von f auf W ist eine eigentliche Rotation, $W^\perp$ also ebenfalls invariant unter f, so daß wir eine verfeinerte Zerlegung von V in invariante Unterräume erhalten:

$$V = U \oplus W \oplus W^\perp.$$

Wir haben also von $U^\perp$ einen invarianten Unterraum der Dimension 2 abspalten können, so daß die Einschränkung von f auf diesen — wegen der geraden Dimension — eine *eigentliche* Rotation ist. Dies können wir iterieren und erhalten die Behauptung damit per Induktion und mit dem folgenden Hilfssatz. □

4.3.18 Hilfssatz *Ist W zweidimensional euklidisch, Δ_0 die normierte Determinantenform, die eine Orientierung repräsentiert, sowie $\varphi \in End_{\mathbb{R}}(W)$ definiert durch $\langle \varphi(v) \mid w \rangle = \Delta_0(v, w)$, dann ist φ eigentliche Rotation mit $\varphi^2 = -id$.*

Beweis: i) Wir beweisen als erste die Identität $\tilde{\varphi} = -\varphi$:

$$\langle v \mid \tilde{\varphi}(w) \rangle = \langle \varphi(v) \mid w \rangle = \Delta_0(v, w) = -\Delta_0(w, v) = -\langle \varphi(w) \mid v \rangle = -\langle v \mid \varphi(w) \rangle.$$

ii) Es zeigt sich jetzt, daß φ eine Isometrie ist:

$$\langle v \mid w \rangle^2 + \langle \varphi(v) \mid w \rangle^2 = \langle v \mid w \rangle^2 + \Delta_0(v, w)^2 =_{4.1.24} \|v\|^2 \|w\|^2.$$

Setzen wir jetzt $w := \varphi(v)$, so ergibt sich (mit $\langle v \mid \varphi(v)\rangle = 0$, nach i)):

$$\|\varphi(v)\|^4 = \langle \varphi(v) \mid \varphi(v)\rangle^2 = \|\varphi(v)\|^2\|v\|^2.$$

Das ergibt $\|\varphi(v)\| = \|v\|$, φ erhält also die Norm und ist demnach Isometrie.
iii) Zum Nachweis von $\varphi^2 = -id$:

$$\varphi^2 =_{i)} -\varphi \circ \tilde{\varphi} =_{ii)} -\varphi \circ \varphi^{-1} = -\mathrm{id}.$$

iv) Mit Hilfe von iii) erhalten wir schließlich

$$\det(\varphi) \cdot \Delta_0(v,w) = \Delta_0(\varphi(v),\varphi(w)) = \langle \varphi^2(v) \mid \varphi(w)\rangle = -\langle v \mid \varphi(w)\rangle = \Delta_0(v,w),$$

was $\det(\varphi) = 1$ ergibt und den Beweis vervollständigt.

□

Diese Abbildung φ heißt auch die *kanonische Komplexstruktur* der euklidischen Ebene W. Sei nun f eine eigentliche Drehung von W, $v \in W\backslash\{0_V\}$ und ω der orientierte Winkel zwischen v und $f(v)$. Für ihn gilt

$$\cos(\omega) = \frac{\langle v \mid f(v)\rangle}{\|v\|\|f(v)\|},\ \sin(\omega) = \frac{\Delta_0(v,f(v))}{\|v\|\|f(v)\|} = \frac{\langle \varphi(v) \mid f(v)\rangle}{\|v\|\|f(v)\|.}$$

Da, für jedes $v \in W$ der Norm 1, $(v, \varphi(v))$ eine ON-Basisfolge ist, gilt also für jede eigentliche Rotation f und die kanonische Komplexstruktur φ zu der Orientierung, bei der diese ON-Basisfolge positiv orientiert ist (beachte $\|v\| = \|f(v)\| = 1$):

$$v \cdot \cos(\omega) + \varphi(v) \cdot \sin(\omega) = v\langle v \mid f(v)\rangle + \varphi(v)\langle \varphi(v) \mid f(v)\rangle = f(v).$$

Mit $\varphi^2 = -\mathrm{id}_V$ ergibt sich daraus

$$f(\varphi(v)) = \varphi(v) \cdot \cos(\omega) - v \cdot \sin(\omega).$$

Das ergibt die behauptete Matrixform:

$$M((v,\varphi(v)), f, (v,\varphi(v))) = \begin{pmatrix} \cos(\omega) & -\sin(\omega) \\ \sin(\omega) & \cos(\omega) \end{pmatrix}$$

Tatsächlich sind diese Matrixelemente *unabhängig* von der Wahl von v :

4.3.19 $$\cos(\omega) = \frac{1}{2}\mathrm{Spur}(\varphi),\ \sin(\omega) = -\frac{1}{2}\mathrm{Spur}(f \circ \varphi).$$

Der Winkel ω kann deshalb als der *Drehwinkel von* f bezeichnet werden, kurz

$$\omega(f) := \omega.$$

Insbesondere haben wir $\omega(\mathrm{id}) = 0$, $\omega(-\mathrm{id}) = \pi$, $\omega(\varphi) = -\pi/2$. Für die Beschreibung von Rotationen in dreidimensionalen euklidischen Räumen gehen wir vom allgemeinen Satz über die Form von Rotationen f aus:

$$M(\mathcal{B},\varphi,\mathcal{B}) = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \cos(\omega) & -\sin(\omega) \\ 0 & \sin(\omega) & \cos(\omega) \end{pmatrix}.$$

Links oben steht ± 1, je nachdem ob f eine eigentliche oder eine uneigentliche Rotation beschreibt. Dabei ist $\mathcal{B} = (b_0, b_1, b_2)$ eine ON-Basisfolge, der Unterraum $\langle b_0 \rangle$ heißt *Drehachse* von f.

4.4 Symmetrische Bilinearformen

Alle betrachteten Vektorräume seien euklidisch. Wir betrachten Bilinearformen

$$\Phi\colon V \times V \to \mathbb{R},$$

von denen wir nur voraussetzen, daß sie symmetrisch sind. Ist $\mathcal{B} = (b_0, \ldots, b_{n-1})$ eine Basisfolge, dann können wir zur Beschreibung von Φ wieder die Matrix

$$A := M_{\mathcal{B}}^{\Phi} := (\Phi(b_i, b_k))$$

benutzen, sie heißt die *Formmatrix.* Wegen der Symmetrie von Φ ist sie symmetrisch, $A = {}^tA$, und es gilt (wenn $v = \sum v_i b_i, w = \sum w_i b_i$) :

$$\Phi(v, w) = {}^tv \cdot M_{\mathcal{B}}^{\Phi} \cdot w = \sum_{i,k} a_{ik} v_i w_k.$$

Zu $\Phi\colon V \times V \to \mathbb{R}$ sei die zugehörige *quadratische Form* $\varphi\colon V \to \mathbb{R}$ definiert durch

4.4.1 $$\varphi(v) := \Phi(v, v).$$

Hierfür gilt, da Φ bilinear und symmetrisch ist:

4.4.2 $$\Phi(v, w) = \frac{1}{2}[\varphi(v + w) - \varphi(v) - \varphi(w)],$$

Φ ist also durch φ eindeutig bestimmt. Es folgt die *Parallelogramm-Identität:*

4.4.3 $$\varphi(v + w) + \varphi(v - w) = 2[\varphi(v) + \varphi(w)].$$

Stetige Funktionen $\psi\colon V \to \mathbb{R}$ mit 4.4.3 heißen *quadratische Funktionen.* Jede symmetrische Bilinearform liefert eine quadratische Funktion, denn φ ist stetig (vgl. den Beweis von **??**). Es gilt aber auch die Umkehrung:

4.4.4 Satz *Jede quadratische Funktion ergibt gemäß 4.4.2 eine symmetrische Bilinearform.*

Beweis: Sei also $\varphi\colon V \to \mathbb{R}$ quadratische Funktion und, gemäß 4.4.2 eine Abbildung $\Phi\colon V \times V \to \mathbb{R}$ definiert. Sie soll als symmetrisch und bilinear nachgewiesen werden.

i) Die Symmetrie folgt unmittelbar aus 4.4.2.

ii) $\Phi(v_1+v_2, w) = \Phi(v_1, w)+\Phi(v_2, w)$ erhält man aus 4.4.2, 4.4.3 nach leichten Rechnungen.

iii) $\Phi(-v, w) = -\Phi(v, w)$ ergibt sich aus ii) und liefert

$$\forall\ z \in \mathbb{Z}, v, w\colon \quad \Phi(zv, w) = z\Phi(v, w),$$

woraus wir schließen, daß

$$\forall\ q \in \mathbb{Q}, v, w\colon \quad \Phi(qv, w) = q\Phi(v, w).$$

Jetzt ergibt sich mit der rationalen Approximierbarkeit reeller Zahlen aus der Stetigkeit von φ schließlich, daß

$$\forall\, r \in \mathbb{R}, v, w\colon \quad \Phi(rv, w) = r\Phi(v, w),$$

womit alles bewiesen ist, denn $\Phi(v, v) = \varphi(v)$. □

Insgesamt gilt also

4.4.5 Folgerung *4.4.1 und 4.4.2 definieren eine Bijektion zwischen den Mengen der symmetrischen Bilinearformen und der quadratischen Funktionen auf V.*

Für die zu Φ gehörige quadratische Funktion φ gilt natürlich

$$\varphi(v) = \sum_{i,k} a_{ik} v_i v_k.$$

Es soll nun gezeigt werden, daß V durch die Bilinearform Φ eine direkte Zerlegung $V = V_0 \oplus V_+ \oplus V_-$ erfährt in den Nullraum V_0 von Φ und die Unterräume $V_\pm$ wo Φ positiv bzw. negativ definit ist. Betrachten wir zunächst den Nullraum

$$V_0 := N_V = \{w \mid \forall\, v \in V\colon \Phi(v, w) = 0\} \leq V.$$

Die Differenz $\dim_{\mathbb{R}}(V) - \dim_{\mathbb{R}}(V_0)$ heißt auch der *Rang* von Φ. Ist V^* dual zu V bzgl. $\langle - \mid - \rangle\colon V \times V^* \to \mathbb{R}$ und $f\colon V \to V^*$ definiert durch

4.4.6 $$\Phi(v, w) = \langle v \mid f(w) \rangle,$$

dann gilt (nachrechnen) mit der zu $\mathcal{B}$ dualen Basisfolge $\mathcal{B}^*$:

4.4.7 Hilfssatz

i) $V_0 = \mathrm{Kern}(f)$,

ii) $\mathrm{Rang}(\Phi) = \mathrm{Rang}(f) = \mathrm{Rang}(M_{\mathcal{B}}^{\Phi})$,

iii) $M_{\mathcal{B}}^{\Phi} = M(\mathcal{B}^*, f, \mathcal{B})$,

iv) Φ *nicht ausgeartet* $\iff \det(M_{\mathcal{B}}^{\Phi}) \neq 0$.

4.4.8 Definition (definit, semidefinit, indefinit) Ist $\Phi\colon V \times V \to \mathbb{R}$ symmetrische Bilinearform, dann heißt Φ

i) *positiv definit,* wenn
$$\forall\, v \neq 0 :\ \varphi(v) > 0,$$

ii) *positiv semidefinit,* falls

$$\forall\, v :\ \varphi(v) \geq 0 \ \wedge\ \exists\, v \neq 0 :\ \varphi(v) = 0.$$

Entsprechend sind *negativ definit* und *negativ semidefinit* zu verstehen. Nimmt φ dagegen sowohl positive als auch negative Werte an, dann heißt Φ *indefinit.*

•

4.4.9 Hilfssatz *Semidefinite symmetrische Bilinearformen Φ sind ausgeartet.*

Beweis: Ist $v \neq 0$ und $\varphi(v) = 0$, dann gilt nach der Cauchy–Schwarzschen Ungleichung

$$\Phi(v, w)^2 \leq \varphi(v)\varphi(w) = 0,$$

also, für alle $w \in V$, $\Phi(v, w) = 0$.

□

4.4.10 Hilfssatz *Ist $\varphi(v) > 0$, dann ist Φ auf $\langle v\rangle^2$ positiv definit.*

Beweis:

$$\varphi(\rho v) = \Phi(\rho v, \rho v) = \rho^2\varphi(v) > 0,$$

falls $\rho \neq 0$.

□

Es gibt also, bei $\varphi(v) > 0$, ganze Unterräume U, so daß Φ auf U^2 positiv definit ist, und demnach auch Unterräume *maximaler Dimension* mit dieser Eigenschaft, etwa

$$V_+.$$

Wir setzen noch

$$V_- := V_+^{\perp}.$$

4.4.11 Hilfssatz *Ist Φ nicht ausgeartet, dann ist Φ auf V_-^2 negativ definit.*

Beweis:

i) Φ ist dort negativ semidefinit: Der Beweis erfolgt indirekt unter der Annahme eines $w \in V_-$ mit $\varphi(w) > 0$. Dazu betrachten wir

$$U := V_+ + \langle w\rangle \ \ni \ u = v + \rho w.$$

Wegen $v \perp w$ ergibt sich

$$\varphi(u) = \varphi(v) + \rho^2\varphi(w) > 0,$$

im Widerspruch zur Maximalität der Dimension von V_+.

ii) Φ ist dort sogar negativ definit: $w \in V_-$ mit $\varphi(w) = 0$ ergibt mit Hilfe der Cauchy–Schwarzschen Ungleichung:

$$\forall\ v \in V \ : \ \Phi(v, w) = 0,$$

also $w = 0$, denn Φ ist als nicht ausgeartet vorausgesetzt.

□

Wir können deshalb wie folgt zusammenfassen:

4.4.12 Satz *Ist Φ eine nicht ausgeartete symmetrische Bilinearform, dann ist*

$$V = V_+ \oplus V_-$$

und Φ ist auf V_+^2 positiv, auf V_-^2 negativ definit. Ist Φ ausgeartet, dann kommt noch der nicht triviale Nullraum hinzu:

$$V = V_+ \oplus V_- \oplus V_0.$$

Wählen wir eine an eine solche Zerlegung von V angepaßte ON-Basisfolge $\mathcal{B} = (b_0, \ldots, b_{n-1})$ so, daß $(b_0, \ldots, b_{s-1})$ Orthonormalbasisfolge von V_+ ist bzgl. Φ, $(b_s, \ldots, b_{s+r-1})$ Orthonormalbasisfolge von V_- bzgl. $-\Phi$ und $(b_{s+r}, \ldots, b_{n-1})$ eine Basisfolge für V_0, dann ist

$$M_{\mathcal{B}}^{\Phi} = \begin{pmatrix} 1 & & & & & & & & 0 \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ 0 & & & & & & & & 0 \end{pmatrix},$$

Hierbei sind die Anzahlen der Einsen s, der sogenannte Index *von Φ, und r, die Anzahl der Diagonalelemente -1, eindeutig bestimmt.*

□

$\mathbb{R}-$Vektorräume mit symmetrischen, nicht ausgearteten indefiniten Bilinearformen Φ treten u.a. in Untersuchungen im Rahmen der Relativitätstheorie auf, sie heißen *pseudo-euklidisch.* Hierbei heißen die Vektoren $v \in V$ mit $\Phi(v, v) > 0$ *raumartig,* solche mit $\Phi(v, v) < 0$ *zeitartig,* die mit $\Phi(v, v) = 0$ heißen *Lichtvektoren* (sie bilden den sogenannten *Lichtkegel.*

4.4.13 Beispiel Ist z.B. $\dim_{\mathbb{R}}(V) = 2$ und 1 der Index von Φ, dann hat die Bilinearform Φ eine Formmatrix der Gestalt

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

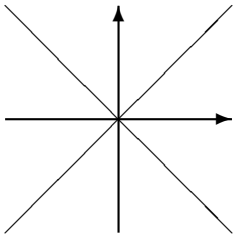
Die quadratische Form hat also die Werte

$$\varphi\left(\begin{pmatrix} \rho \\ \sigma \end{pmatrix}\right) = \rho^2 - \sigma^2.$$

Der Lichtkegel

$$L = \left\{ \begin{pmatrix} \pm\rho \\ \rho \end{pmatrix} \mid \rho \in \mathbb{R} \right\}.$$

dieser *pseudoeuklidischen Ebene* besteht also aus 2 Geraden:



L wird also erzeugt von den Vektoren

$$r_\pm := \begin{pmatrix} \pm\rho_0 \\ \rho_0 \end{pmatrix},$$

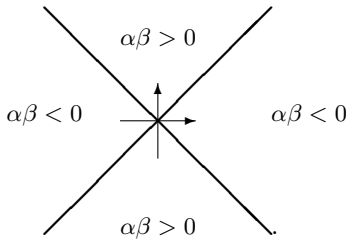
für ein festes $\rho_0 > 0$. Weil $\varphi(r_+) = \varphi(r_-) = 0$, Φ aber nicht ausgeartet ist, können wir annehmen, es sei

$$\Phi(r_+, r_-) = -1.$$

Es folgt

$$\varphi(\alpha \cdot r_+ + \beta \cdot r_-) = -2\alpha\beta.$$

Dies zeigt, daß die zeitartigen Vektoren wie auch die raumartigen Vektoren jeweils einen Kegel, bestehend zwei Sektoren bilden, die von den Geraden des Lichtkegels eingeschlossen werden:



Jeweils einer von diesen heißt *Zukunftskegel,* der andere *Vergangenheitskegel.* $\diamond$

Diese Konstruktionen dienen also der Unterscheidung von zeitlichem und räumlichem Abstand zweier Ereignisse. Die allgemeine Situation beschreibt

4.4.14 Definition (Minkowski-Raum, Lorentz-Transformation) Endlichdimensionale $\mathbb{R}-$Vektorräume zusammen mit nicht ausgearteten indefiniten Bilinearformen $\langle - \mid - \rangle$ heißen *pseudo-euklidisch,* die Bilinearform heißt dann ebenfalls das *innere Produkt,* ihr Index s der *Index* des pseudo-euklidischen Raums. Eine Basisfolge $\mathcal{B}$ heißt dabei *orthonormal,* wenn gilt

$$\langle b_i \mid b_k \rangle = \epsilon_i \delta_{ik}, \epsilon_i = \begin{cases} 1, & i \in s \\ -1, & i \in n \backslash s \end{cases}$$

Wir haben bereits gesehen, daß solche Orthonormalbasisfolgen stets existieren. Bezüglich einer solchen gilt

$$\langle v \mid w\rangle = \sum_{i=0}^{s-1} v_i w_i - \sum_{i=s}^{n-1} v_i w_i,$$

und die Gleichung des Lichtkegels ist

$$\sum_{i=0}^{s-1} v_i^2 - \sum_{i=s}^{n-1} v_i^2 = 0.$$

Interessant sind insbesondere die pseudo-euklidischen Räume V vom Index $n-1 := \dim_{\mathbb{R}}(V) - 1$. Unter diesen heißen die mit $n = 4$ *Minkowski-Räume,* deren Rotationen, also die Abbildungen $f \in End_{\mathbb{R}}(V)$ mit

$$\langle f(v) \mid f(w)\rangle = \langle v \mid w\rangle$$

heißen *Lorentz-Transformationen.* •

Eine Anwendung quadratischer Formen bzw. Funktionen in der klassischen Geometrie ist beispielsweise die Klassifizierung von Kegelschnitten und Verallgemeinerungen dieser. Wir wollen deshalb den Begriff des *Kegelschnitts* verallgemeinern und erinnern deshalb zunächst daran, daß Kegelschnitte in der euklidischen Ebene $\mathbb{E}^2 := \mathbb{R}^2$ mit $D(\mathbb{E}^2) = \mathbb{R}^2$ Mengen von Punkten $X \in \mathbb{E}^2$ sind, so daß die Koordinaten x_0, x_1 ihrer Ortsvektoren einer Gleichung der Form

$$\sum_{i,k=0}^{1} a_{ik} x_i x_k + 2 \sum_{i=0}^{1} b_i x_i = c$$

genügen.

4.4.15 Beispiele

- Die Gleichung
$$\frac{x_0^2}{a^2} + \frac{x_1^2}{b^2} = 1$$
beschreibt eine *Ellipse* bzw. einen *Kreis* (falls $a = b$).
- Die Gleichung
$$\frac{x_0^2}{a^2} - \frac{x_1^2}{b^2} = 1$$
beschreibt eine *Hyperbel.*
- Die Gleichung $x_1^2 = 2px_0$ beschreibt eine *Parabel.*

◇

Diese Kegelschnitte werden also durch quadratische Formen und Linearformen beschrieben. Wir verallgemeinern deshalb wie folgt:

4.4.16 Definition (Quadrik) Unter einer *Quadrik* im euklidischen Raum $\mathbb{E}^n$ mit $D(\mathbb{E}^n) = \mathbb{R}^n$ versteht man eine Menge Q von Punkten X, deren Ortsvektoren x die Lösungsmenge einer Gleichung der Gestalt

$$\varphi(x) + 2f(x) = \alpha$$

bilden, mit einer quadratischen Form φ, einer Linearform f und einem $\alpha \in \mathbb{R}$. •

4.4.17 Hilfssatz *Quadriken im $\mathbb{E}^n$ sind Mengen von Punkten X, deren Ortsvektoren x Lösungsmengen von Gleichungen der Form*

$$\langle F(x) \mid x\rangle + 2\langle a \mid x\rangle = \alpha$$

mit selbstadjungiertem $F \in End_{\mathbb{R}}(\mathbb{R}^n), a \in \mathbb{R}^n, \alpha \in \mathbb{R}$.

Beweis: Betrachten wir die Quadrik

$$Q := \{X \in \mathbb{E}^n \mid \varphi(x) + 2f(x) = \alpha\}.$$

Der Differenzenraum $\mathbb{R}^n$ ist euklidisch, $\langle - \mid -\rangle$ sei das innere Produkt. Dann kann nach 4.4.6 Φ, die symmetrische Bilinearform zu φ, mit einem geeigneten $F \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$ so ausgedrückt werden:

$$\Phi(x, y) = \langle F(x) \mid y\rangle.$$

Nun ist aber Φ symmetrisch, ebenso $\langle - \mid -\rangle$, und wir erhalten

$$\langle F(x) \mid y\rangle = \Phi(x, y) = \Phi(y, x) = \langle F(y) \mid x\rangle = \langle x \mid F(y)\rangle = \langle \tilde{F}(x) \mid y\rangle.$$

Das impliziert $F = \tilde{F}$. Zudem ist jede Linearform $f \in Hom_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R})$ von der Gestalt $f(-) = \langle - \mid a\rangle$, mit geeigneten $a \in \mathbb{R}^n$. Es folgt, wie behauptet, daß

$$Q = \{X \mid \langle F(x) \mid x\rangle + 2\langle a \mid x\rangle = \alpha\}.$$

Die Umkehrung ist trivial.

□

Wir unterscheiden jetzt zwei Fälle:

Fall 1: $\exists\ S \in Q$: $F(s) + a = 0$. In diesem Fall kann a durch $-F(s)$ ersetzt werden. Es ergibt sich

$$\langle F(x) \mid x\rangle - 2\langle F(s) \mid x\rangle = \alpha.$$

Einsetzen von $x := s$ ergibt noch $\alpha = -\langle F(s) \mid s\rangle$, so daß wir insgesamt erhalten:

$$0 = \langle F(x) \mid x\rangle - 2\langle F(s) \mid x\rangle + \langle F(s) \mid s\rangle = \varphi(x - s),$$

wobei für die letzte Gleichung die Selbstadjungiertheit von F benutzt wird. Eine solche Quadrik

4.4.18 $$Q = \{X \mid \varphi(x - s) = 0\}$$

heißt *Kegel* mit der *Spitze* S.

Fall 2: $\forall\ X \in Q\colon F(x) + a \neq 0$. Das hat u.a. die Konsequenz, daß für alle Quadrikpunkte $X \in Q$ das orthogonale Komplement von $F(x)+a$, dem sogenannten *Normalenvektor* im Punkt x, eine Hyperebene in $\mathbb{R}^n$ ist, der *Tangentialraum* zum Punkt x :

$$T(x) := \langle F(x) + a\rangle^{\perp} = \{y \mid \langle F(x) + a \mid y\rangle = 0\}.$$

Trägt man die Elemente des Tangentialraums $T(x)$ von x aus ab, dann erhält man die Vektoren (und daraus die Punkte) der *Tangentialhyperebene* in x :

$$H(x) := x + T(x).$$

Mit Φ und f formuliert lesen sich diese Gleichungen so:

4.4.19 $$T(x) = \{y \in \mathbb{R}^n \mid \Phi(x, y) + f(y) = 0\} \leq \mathbb{R}^n,$$

4.4.20 $$H(x) = \{y \in \mathbb{E}^n \mid \Phi(x, y) + f(x + y) = \alpha\} \subseteq \mathbb{R}^n.$$

4.4.21 Satz *Ist Z ein Punkt der Quadrik Q, dann ist der Schnitt von Q mit einer Ebene E durch Z ein Kegelschnitt.*

Beweis: Sei $\varphi(x) + 2f(x) = \alpha$ wieder die Bestimmungsgleichung von Q und sei die Ebene E definiert durch

$$E := \{x \mid x = z + \xi u + \eta v, \xi, \eta \in \mathbb{R}\}$$

für zwei linear unabhängige $u, v \in \mathbb{R}^n$. Durch Einsetzen in die Bestimmungsgleichung ergibt sich

$$\xi^2\varphi(u) + 2\xi\eta\Phi(u, v) + \eta^2\varphi(v) + 2\xi(\Phi(u, z) + f(u)) + 2\eta(\Phi(v, z) + f(v)) = 0.$$

Die Menge der Vektoren (ξ, η), die dieser Gleichung genügen, ist ein Kegelschnitt.

□

Verschiebt man den Koordinatenursprung im $\mathbb{E}^n$, d. h. ersetzt man x durch $z + x$, dann ergibt sich als neue Bestimmungsgleichung

4.4.22 $$Q = \{z + x \mid \varphi(x) + 2(\Phi(z, x) + f(x)) = \alpha - \varphi(z) - 2f(z)\}.$$

Um diese Bestimmungsgleichung zu vereinfachen, fragen wir, ob es solche z gibt, die die neue Linearform zum Verschwinden bringen, d. h. für die gilt

4.4.23 $$\Phi(z, x) + f(x) = \langle F(z) + a \mid x\rangle = 0,$$

für alle $x \in \mathbb{R}^n$. Solche $z \in \mathbb{E}^n$ heißen gegebenenfalls *Zentren.* Die Menge *aller* Zentren ist demnach

4.4.24 $$Z(Q) := \{z \in \mathbb{E}^n \mid F(z) = -a\}.$$

Zentren sind — als Lösungen der Gleichung $F(z) = -a$ — offenbar bis auf Vektoren aus $\mathrm{Kern}(F)$ eindeutig bestimmt. Die Menge der Zentren ist also leer oder ein affiner Unterraum von $\mathbb{E}^n$ mit $\mathrm{Kern}(F)$ als zugehörigem Differenzenraum. Ist Q *nicht degeneriert,* d. h. die Q beschreibende Bilinearform nicht ausgeartet (und damit F regulär), dann besitzt Q ggf. genau ein Zentrum. Hat Q ein Zentrum Z, dann ist diese Quadrik von der Form

4.4.25 $$Q = \{x \in \mathbb{E}^n \mid \varphi(x - z) = \beta\},$$

und dabei ist β genau dann gleich Null, wenn Q ein Kegel mit Spitze ist (die Spitze ist dann das Zentrum). Wegen $\beta \neq 0$, falls die Quadrik kein Kegel mit Spitze ist, kann (vgl. 4.4.22) — außer bei Kegeln mit Spitze — kein Zentrum auf der Quadrik liegen, es gilt sogar noch mehr:

4.4.26 Hilfssatz *Die Zentren von Quadriken Q, die keine Kegel mit Spitzen sind, liegen in keiner Tangentialhyperebene.*

Beweis: Indirekt. Ist Q eine Quadrik mit Zentrum $z \in Q$, aber kein Kegel mit Spitze, dann ist die Bestimmungsgleichung für die $y \in H(x)$ nach 4.4.20:

$$0 \neq \beta = \Phi(x, y) = \langle F(x) \mid y\rangle.$$

Wegen $a = 0$ ist aber $y \in Z(Q)$ genau dann, wenn $F(y) = 0$. Das ergibt den Widerspruch

$$0 = \langle x \mid F(y)\rangle = \langle F(x) \mid y\rangle.$$

□

Für die Lokalisierung von Zentren benutzt man zweckmäßig die Tatsache, daß jede Quadrik durch Punktspiegelung

$$\tau\colon x \mapsto 2z - x =: x'$$

an jedem ihrer Zentren in sich selbst übergeht:

$$\varphi(x' - z) = \varphi(2z - x - z) = \varphi(z - x) = \varphi(x - 1).$$

Aus dem Beweis des letzten Hilfssatzes ergibt sich noch mit **??** und durch Ersetzen von φ durch φ/β :

4.4.27 Folgerung *Eine Quadrik Q mit Zentrum, die kein Kegel mit Spitze ist, genügt einer Bestimmungsgleichung der Form $\varphi(x) = 1$, mit einer geeigneten quadratischen Form φ. Man nennt diese die* Normalform *der Bestimmungsgleichung. Wählt man noch eine Basisfolge $\mathcal{B}$ von $\mathbb{R}^n$ mit*

$$\Phi(b_i, b_k) = \epsilon_i \delta_{ik}, \epsilon_i := \begin{cases} 1, & 0 \leq i \leq s-1 \\ -1, & s \leq i \leq s+r-1 \\ 0, & s+r \leq i \leq n-1 \end{cases}$$

$s :=$ Index von φ, $r :=$ Rang von Φ, dann ist die Normalform der Bestimmungsgleichung von Q gerade diese:

$$\sum_{i=0}^{r-1} \epsilon_i x_i x_i = 1.$$

Beispiele solcher Normalformen von Quadriken mit Zentren in der Ebene sind:

Normalform	Typ
$x_0^2 + x_1^2 = 1$	Ellipse
$x_0^2 - x_1^2 = 1$	Hyperbel
$x_0^2 = 1$	zwei parallele Geraden

Im dreidimensionalen Anschauungsraum haben wir

Normalform	Typ
$x_0^2 + x_1^2 + x_2^2 = 1$	Ellipsoid
$x_0^2 + x_1^2 - x_2^2 = 1$	einschaliges Hyperboloid
$x_0^2 - x_1^2 - x_2^2 = 1$	zweischaliges Hyperboloid
$x_0^2 + x_1^2 = 1$	elliptischer Zylinder
$x_0^2 - x_1^2 = 1$	hyperbolischer Zylinder
$x_0^2 = 1$	zwei parallele Ebenen

Für Quadriken ohne Zentren kann man folgendes beweisen

4.4.28 Satz *Die Normalform einer Quadrik ohne Zentrum ist von der Form $\varphi(y) + 2\xi = 0$, bei Wahl einer Basis wie in 4.4.27 nimmt diese Bestimmungsgleichung die Form*

$$\sum_{i=1}^{r} \epsilon_i y_i y_i + 2\xi = 0$$

an.

4.5 Unitäre Räume

Es soll nun untersucht werden, wie man zweckmäßig vorzugehen hat, wenn der Grundkörper $\mathbb{K}$ der Körper

$$\mathbb{C} = \{\zeta := \rho + i\sigma \mid \rho, \sigma \in \mathbb{R}\}$$

der komplexen Zahlen ist, mit den bekannten Rechenregeln und der *Konjugation*

$$\overline{}: \mathbb{C} \to \mathbb{C}, \zeta \mapsto \overline{\zeta} := \rho - i\sigma.$$

4.5.1 Definition (Semibilinearformen) Ist V ein $\mathbb{C}$-Vektorraum, dann heißt $\Phi: V \times V \to \mathbb{C}$ *Semibilinearform,* wenn gilt

$$\Phi(\zeta_0 v_0 + \zeta_1 v_1, v_2) = \zeta_0 \Phi(v_0, v_2) + \zeta_1 \Phi(v_1, v_2)$$

und

$$\Phi(v_0, \zeta_1 v_1 + \zeta_2 v_2) = \overline{\zeta_1} \Phi(v_0, v_1) + \overline{\zeta_2} \Phi(v_0, v_2).$$

•

Die zugehörige quadratische Form φ ist wieder durch $\varphi(v) := \Phi(v, v)$ definiert, und auch hier gilt die Parallelogramm-Identität

$$\varphi(v + w) + \varphi(v - w) = 2[\varphi(v) + \varphi(w)].$$

Weiter haben wir, für $|\zeta| := \sqrt{\zeta\overline{\zeta}} = \sqrt{\rho^2 + \sigma^2}$:

4.5.2 $$\varphi(\zeta v) = |\zeta|^2 \varphi(v),$$

und auch hier im komplexen Fall läßt sich Φ aus der quadratischen Form φ wiedergewinnen:

4.5.3 $$2\Phi(v, w) = [\varphi(v + w) - \varphi(v) - \varphi(w)] + i \cdot [\varphi(v + iw) - \varphi(v) - \varphi(w)].$$

4.5.4 Definition (hermitesche Semibilinearform) Die Semibilinearform Φ heißt *hermitesch,* wenn $\Phi = \widetilde{\Phi}$ gilt, wobei

$$\widetilde{\Phi}(v, w) := \overline{\Phi(w, v)}.$$

($\widetilde{\Phi}$ ist offensichtlich ebenfalls hermitesche Semibilinearform.) •

Eine Semibilinearform ist also genau dann hermitesch, wenn die zugehörige quadratische Form reellwertig ist. Demnach kann man bei hermiteschen Semibilinearformen auch von positiv definiten sprechen, sie eigenen sich also zur Metrisierung!

4.5.5 Definition (hermitesche Matrix) $A \in \mathbb{C}^{n \times n}$ heißt *hermitesch,* wenn gilt

$$a_{ik} = \overline{a_{ki}}.$$

•

Ist z. B. Φ hermitesch, $\mathcal{B} = (b_0, \ldots, b_{n-1})$ eine Basisfolge, dann ist $M_{\mathcal{B}}^{\Phi}$ hermitesch.

4.5.6 Beispiele

- Ist $V := \mathbb{C}^n$, dann ist das *Standardskalarprodukt* Φ, definiert durch

$$\Phi(v, w) := \sum_{i=o}^{n-1} v_i \overline{w}_i,$$

  hermitesch.

- Ein $\mathbb{R}$-Vektorraum V ergibt den $\mathbb{C}-$Vektorraum $V \times V$ vermöge

$$(\rho + i\sigma)(v, w) := (\rho v - \sigma w, \rho w + \sigma v).$$

  Dieser Vektorraum heißt die *Komplexifizierung* von V. Wir bezeichnen ihn mit ${}_{\mathbb{C}}(V \times V)$. Jeder seiner Vektoren (v, w) ist eindeutig darstellbar als Summe

$$(v, w) = (v, 0) + (0, w) = (v, 0) + i(w, 0).$$

  Ist dabei ${}_{\mathbb{R}}V$ euklidisch, $\langle - \mid - \rangle$ das innere Produkt, dann definiert

$$\Phi((v, v'), (w, w')) := \langle v \mid w \rangle + \langle v' \mid w' \rangle + i \cdot [\langle v' \mid w \rangle - \langle v \mid w' \rangle]$$

  eine hermitesche Semibilinearform auf ${}_{\mathbb{C}}(V \times V)$.

$\diamond$

4.5.7 Definition (unitärer Raum, unitäre Matrix)

i) Ein endlichdimensionaler $\mathbb{C}-$Vektorraum zusammen mit einer positiv definiten hermiteschen Semibilinearform

$$\langle - \mid - \rangle \colon V \times V \to \mathbb{C}$$

heißt *unitärer Raum.* $\langle - \mid - \rangle$ heißt dann auch *hermitesches inneres Produkt.*

ii) $A \in \mathbb{C}^{n \times n}$ heißt *unitär,* wenn gilt:

$$A^{-1} = {}^t\overline{A} = (\overline{a_{ki}}).$$

$\bullet$

Natürlich ist $\mathbb{C}^n$ mit dem Standardskalarprodukt ein unitärer Nicht ganz so offensichtliches Beispiel ist die oben eingeführte Komplexifizierung ${}_{\mathbb{C}}(V \times V)$ eines reellen Vektorraums V mit der dort angegebenen hermiteschen Semibilinearform Φ.

Auf unitären Räumen kann, ganz wie für relle Vektorräume mit innerem Produkt, eine *Norm* definiert werden:

$$\|v\| := \sqrt{\langle v \mid v \rangle},$$

denn der Wert unter der Wurzel ist ja eine nicht negative reelle Zahl. Auch hier gilt die Cauchy-Schwarzsche Ungleichung

$$|\langle v \mid w\rangle| \leq \|v\| \, \|w\|.$$

mit Gleichheit genau dann, wenn die beiden Vektoren linear abhängig sind. Der Beweis verläuft hier völlig analog zum Beweis im Reellen.

4.5.8 Hilfssatz *Es gilt die Dreiecksungleichung*

$$\|v + w\| \leq \|v\| + \|w\|,$$

mit Gleichheit genau dann, wenn $v = \rho w, \rho \in \mathbb{R}_{\geq 0}$.

Beweis: Die Gültigkeit der Dreiecksungleichung folgt mit Hilfe der Cauchy-Schwarzschen Ungleichung. Bei Annahme der Gleichheit quadriert man beide Seiten von $\|v + w\| = \|v\| + \|w\|$ und erhält

4.5.9 $$\langle v \mid w\rangle + \overline{\langle v \mid w\rangle} = 2\sqrt{\langle v \mid v\rangle\langle w \mid w\rangle},$$

also für den Realteil von $\langle v \mid w\rangle$ die Gleichung

$$\mathrm{Re}(\langle v \mid w\rangle) = \|v\| \, \|w\|.$$

Aus der Cauchy-Schwarzschen Ungleichung folgt damit die Gleichheit

$$|\langle v \mid w\rangle| = \|v\| \, \|w\|,$$

die Vektoren v und w sind demnach linear abhängig, etwa $v = \zeta w$. Setzen wir dies in 4.5.9 ein, so folgt $\zeta + \overline{\zeta} = 2|\zeta|$, der Koeffizient ζ ist demnach reell.
Ist umgekehrt $v = \zeta w$, mit $\zeta \in \mathbb{R}_{\geq 0}$, dann wird aus der Dreiecksungleichung ganz offensichtlich eine Identität.

□

Auch im unitären Fall nennen wir zwei Vektoren v, w genau dann *orthogonal,* wenn ihr inneres Produkt verschwindet:

$$v \perp w \;:\Longleftrightarrow\; \langle v \mid w\rangle = 0.$$

Wir haben also einen Orthogonalitätsbegriff, Orthonormalbasisfolgen, orthogonale Komplemente usw.
Eine wichtige Konstruktion ist

4.5.10 Definition (der konjugierte Vektorraum) Der zu V *konjugierte* Vektorraum $\overline{V}$ hat dieselbe Grundmenge V von Vektoren, aber das Produkt eine $v \in \overline{V}$ mit einem Skalar $\zeta \in \mathbb{C}$ setzt man gleich dem Vektor $\overline{\zeta} \cdot v$ im Vektorraum V, kurz:

$$\zeta \cdot v := \overline{\zeta} \cdot v.$$

•

(Das sieht vielleicht auf den ersten Blick merkwürdig aus, wird aber dadurch erklärt, daß links ein Vektor aus $\overline{V}$, und rechts einer aus V steht!) Für die Abbildung

$$f\colon V \to \overline{V}, v \mapsto v$$

gilt

$$f(i \cdot v) = -i \cdot f(v).$$

Mit ihrer Hilfe definiert man dann zum unitären V (mit $\langle - \mid - \rangle$) die nicht ausgeartete Bilinearform (nachrechnen!)

$$[- \mid -]\colon V \times \overline{V} \to \mathbb{C}\colon (v, w) \mapsto \langle v \mid f^{-1}(w) \rangle.$$

V und $\overline{V}$ sind also bzgl. $[- \mid -]$ zueinander *duale* Vektorräume. Hiermit läßt sich auch der *Rieszsche Darstellungssatz* übertragen: Ist $G\colon V \to \mathbb{C}$ eine Linearform, dann folgt aus einem ganz analogen Beweis, daß $g(v) = [v \mid b]$, für ein geeignetes $b \in V$. Wegen $[v \mid b] = \langle v \mid f^{-1}(b) \rangle =: \langle v \mid a \rangle$ ergibt sich für g die folgende Darstellung mit Hilfe eines geeigneten $a \in V$ und des inneren Produkts auf V :

$$g(-) = \langle - \mid a \rangle.$$

usw.

Dies wird im kommenden Semester in der Vorlesung Algebra I ergänzt und fortgesetzt!

Inhalt von Kapitel 5: Tensoren, multilineare Algebra

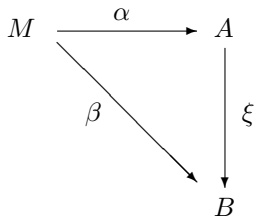
Kapitel 5

Multilineare Algebra

Viele Werte von Begriffen in der Mathematik und ihren Anwendungen werden durch *Zahlen* beschrieben, beispielsweise der Umfang eines Kreises vom Radius 1 durch die Zahl π. Zur Beschreibung anderer benötigt man den *Vektorbegriff,* also die Mittel der Linearen Algebra. Unter anderem hat eine physikalische Kraft über ihren Betrag hinaus auch eine Richtung. Bisher wissen wir aber "nur", wie man Vektoren addieren oder mit Skalaren multilizieren kann. In diesem Kapitel geht es jetzt um eine *Produktbildung* zwischen Vektoren, um *Tensoren,* das sind die Elemente von Tensorprodukten von Vektorräumen und Moduln.
Tensoren spielen eine wichtige Rolle in den Naturwissenschaften. Darüberhinaus ist das Tensorprodukt wegen seiner Universaleigenschaft von großer Bedeutung in der Algebra. Ein weiteres sehr wichtiges "universelles Element" werden wir mit der sogenannten Freien Gruppe im nächsten Kapitel kennenlernen.

5.1 Universelle Elemente

Analog zur Untersuchung der Lösbarkeit von Gleichungen der Form $b = x \cdot a$ in Halbgruppen, Gruppen, Ringen, Körpern usw., kann man die Auflösbarkeit von Gleichungen der Form $\beta = \xi \circ \alpha$ in vorgegebenen Klassen von *Abbildungen* betrachten. Mit anderen Worten: es geht jetzt um die Ergänzbarkeit von

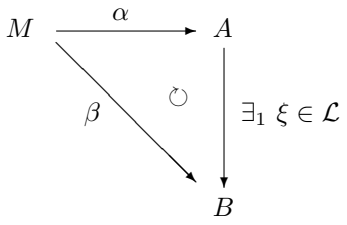


zu einem kommutativen Diagramm bei gegebenen α und β.

5.1.1 Definition (universell) Sei $\mathcal{F}$ eine vorgegebene Klasse von Funktionen mit Definitionsbereich M, sei $\alpha\colon M \to A$ in $\mathcal{F}$ und $\mathcal{L}$ eine weitere vorgegebene Klasse von Funktionen. $\mathcal{L}$ enthalte (zu den vorkommenden Definitionsbereichen) die Identitäten und sei abgeschlossen gegenüber Komposition (d.h. für $\gamma, \delta \in \mathcal{L}$ mit $Bild\ \delta \subseteq Def\ \gamma$ gilt $\gamma \circ \delta \in \mathcal{L}$). Dann heißt $\alpha\colon M \to A$ *universell bzgl.* $\mathcal{F}$ *und* $\mathcal{L}$, wenn gilt:

$$\forall\ \beta \in \mathcal{F}\ \exists_1\ \xi \in \mathcal{L}\colon\ \beta = \xi \circ \alpha.$$

In abkürzender Diagrammschreibweise:



Die Klasse $\mathcal{L}$ heißt dabei die Klasse der *zulässigen Lösungen*, und A heißt *universelles Element.* •

5.1.2 Beispiel Ist M eine Menge, $\sim$ eine Äquivalenzrelation auf M und

$$\alpha\colon M \to M/\sim,\ m \mapsto [m]_\sim$$

die Projektion der Elemente auf ihre Äquivalenzklasse. Dann ist die Abbildung $\alpha\colon M \to M/\sim$ universell bezüglich der Klasse $\mathcal{F}$ der Funktionen mit Defintionsbereich M, die konstant auf den Äquivalenzklassen sind, und der Klasse $\mathcal{L}$ aller Abbildungen. ◇

Von zentraler Bedeutung ist nun folgender Satz:

5.1.3 Die Eindeutigkeit universeller Elemente *Sind gegebene Abbildungen*

$$\alpha\colon M \to A \text{ und } \gamma\colon M \to C$$

universell bzgl. $\mathcal{F}$ und $\mathcal{L}$, dann gibt es eine Bijektion $\lambda \in \mathcal{L}$ mit $\lambda\colon A \to C$. Mit anderen Worten: Universelle Elemente sind im wesentlichen, d.h. bis auf zulässige Bijektionen, eindeutig bestimmt.

Beweis: Aus der Universalität von α und γ folgen die beiden Existenzaussagen

$$\exists_1\ \xi \in \mathcal{L}\colon \gamma = \xi \circ \alpha \text{ und } \exists_1\ \eta \in \mathcal{L}\colon \alpha = \eta \circ \gamma.$$

Daraus ergibt sich unmittelbar durch Einsetzen:

$$\gamma = \underbrace{\xi \circ \eta}_{\in \mathcal{L}} \circ \gamma \text{ und } \alpha = \underbrace{\eta \circ \xi}_{\in \mathcal{L}} \circ \alpha.$$

Nun gilt aber trivialerweise

$$\alpha = id_A \circ \alpha, \text{ und } \gamma = id_C \circ \gamma.$$

Wegen $id_A, id_C \in \mathcal{L}$ und der Eindeutigkeit der Ergänzungen zeigt also ein Vergleich, daß folgendes richtig ist:

$$\xi \circ \eta = id_C \text{ und } \eta \circ \xi = id_A,$$

woraus sich bekanntlich die Bijektivität von $\xi =: \lambda$ ergibt.

□

5.1.4 Anwendungen Ist G eine Gruppe, $\alpha\colon G \to H$ ein Epimorphismus, $\mathcal{F}$ die Klasse der Homomorphismen γ mit Definitionsbereich G und der Eigenschaft $\mathrm{Kern}(\alpha) \subseteq \mathrm{Kern}(\gamma)$, $\mathcal{L}$ die Klasse aller Homomorphismen zwischen Gruppen, dann ist α offenbar universell bzgl. $\mathcal{F}$ und $\mathcal{L}$. Demnach sind, wegen 5.1.3, alle epimorphen Bilder von G mit demselben Kern $Kern\ \alpha$ isomorph.
Ein weiteres, leicht einzusehendes Beispiel ist die Universalität von

$$\alpha\colon n \to \mathbb{K}^n, i \mapsto e_i,$$

bezüglich der Klasse $\mathcal{F}$ der Abbildungen von $n := \{0,\ldots,n\text{-}1\}$ in Vektorräume über $\mathbb{K}$ und der Klasse $\mathcal{L}$ aller $\mathbb{K}$-linearen Abbildungen. Hier ergibt die Eindeutigkeit universeller Elemente die Isomorphie aller n–dimensionalen Vektorräume über $\mathbb{K}$. ◇

5.2 Tensorprodukte von Moduln

Wir wollen ein Produkt $M \otimes_R N$ aus einem R-Rechtsmodul M und einem R-Linksmodul N bilden, dabei ist R ein Ring mit Einselement. Die Spezialisierung auf Vektorräume soll ein Vektorraum werden, dessen Dimension das *Produkt* der Dimensionen der beiden Faktoren ist.
Dieses Produkt wird als universelles Element eingeführt. Die Klasse $\mathcal{F}$ ist dabei die Klasse der Abbildungen f von $M \times N$ in abelsche Gruppen, die biadditiv sind, und für die gilt:

$$f(mr, n) = f(m, rn).$$

Solche Abbildungen heißen *ausgeglichen,* und wir definieren:

5.2.1 Definition (Tensorprodukt von Moduln) Ist T eine abelsche Gruppe, $\tau\colon M \times N \to T$, dann heißt T *ein Tensorprodukt* von M und N über R, wenn $\tau\colon M \times N \to T$ universell ist bzgl. der Klasse $\mathcal{F}$ der ausgeglichenen Abbildungen von $M \times N$ in abelsche Gruppen und der Klasse $\mathcal{L}$ aller Homomorphismen zwischen abelschen Gruppen. •

5.2.2 Satz *Es gibt Tensorprodukte von M und N über R.*

Beweis: Wir konstruieren ein Tensorprodukt. Dazu betrachten wir die *freie abelsche Gruppe* (additiv geschrieben) über $M \times N$, das ist

$$(\mathbb{Z}^{M\times N})' := \{f\colon M \times N \to \mathbb{Z} \mid \text{ fast alle } f(m,n) = 0\}$$

$$:= \{ \sum_{(m,n)\in M\times N} z_{mn}(m,n) \mid z_{mn} \in \mathbb{Z}\}.$$

(Beachte: Bei der letzten Schreibweise handelt es sich um eine *formale Summe*, nicht um Linearkombinationen o.ä.) Diese Gruppe enthält u.a. die folgenden Elemente (für alle m, m_i in M, und alle n, n_i in N, sowie alle $r \in R$):

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n),$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2),$$

$$(mr, n) - (m, rn).$$

Die von all diesen Elementen erzeugte Untergruppe heiße U, und wir setzen

$$T := (\mathbb{Z}^{M\times N})'/U,\ \tau\colon M \times N \to T\colon (m,n) \mapsto (m,n) + U.$$

Es bleibt jetzt zu zeigen, daß $\tau\colon M \times N \to T$ tatsächlich universell ist.

a) τ ist leicht als ausgeglichen nachgewiesen, z.B. gilt

$$\tau(m_1 + m_2, n) = (m_1 + m_2, n) + U$$

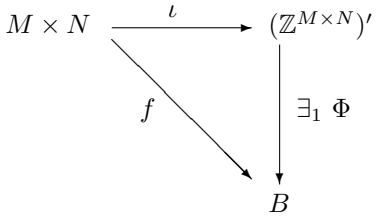
$$= (m_1 + m_2, n) \underbrace{-(m_1 + m_2, n) + (m_1, n) + (m_2, n)}_{\in U} + U$$

$$= (m_1, n) + (m_2, n) + U = \tau(m_1, n) + \tau(m_2, n).$$

b) Zum Beweis der Faktorisierbarkeit eines ausgeglichenen $f: M \times N \to B$ über τ (wobei B eine beliebige, i.a. wieder additiv geschriebene, abelsche Gruppe ist) bemerken wir zunächst, daß sich f trivialerweise und eindeutig über die Einbettung

$$\iota: M \times N \hookrightarrow (\mathbb{Z}^{M\times N})', (m,n) \mapsto 1_{\mathbb{Z}}(m,n)$$

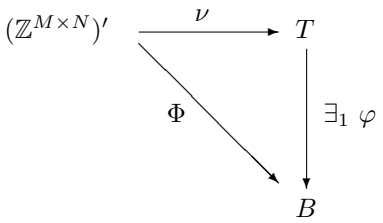
faktorisieren läßt:



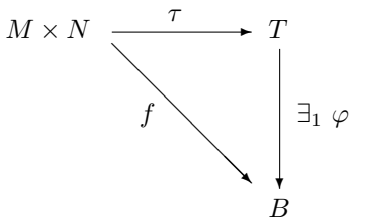
Die Eindeutigkeit von Φ folgt dabei aus der Tatsache, daß das Bild von $M \times N$ unter ι eine $\mathbb{Z}$-Basis von $(\mathbb{Z}^{M\times N})'$ als $\mathbb{Z}-$Modul ist. Φ ist dabei so zu definieren:

$$\Phi: (\mathbb{Z}^{M\times N})' \to B, \sum z_{mn}(m,n) \mapsto \sum z_{mn} f(m,n).$$

Da f ausgeglichen ist, gilt $U \subseteq Kern\ \Phi$, so daß wir noch folgendes kommutative Diagramm erhalten:



wobei $\nu: (\mathbb{Z}^{M\times N})' \to T$ der natürliche Epimorphismus auf die Faktorgruppe T ist. φ ist ebenfalls Homomorphismus (nachrechnen!). Insgesamt ergibt sich so das kommutative Diagramm



mit einem $\varphi \in \mathcal{L}$. Da die Elemente $\tau(m,n)$ ganz T erzeugen, ist zudem φ eindeutig bestimmt.

□

5.3 Eigenschaften von Tensorprodukten

Das im Beweis von 5.2.2 konstruierte Tensorprodukt von M und N über R bezeichnen wir so:

5.3.1 $$M \otimes_R N := (\mathbb{Z}^{M\times N})'/U,$$

und die Abbildung τ ersetzen wir durch das Symbol $\otimes$:

5.3.2 $$\otimes\colon\ M \times N \to M \otimes_R N, (m,n) \mapsto m \otimes n := (m,n) + U.$$

Aus dem Satz über die Eindeutigkeit universeller Elemente erhalten wir jetzt:

5.3.3 Folgerung *Jedes Tensorprodukt von M und N über R ist, als abelsche Gruppe, isomorph zu $M \otimes_R N$.*

Wir nennen deshalb $M \otimes_R N$ kurzerhand auch *das* Tensorprodukt von M und N über R. Es hat insbesondere die folgenden Eigenschaften:

5.3.4 Eigenschaften des Tensorprodukts *Für Tensorprodukte von Moduln gilt:*

$$M \otimes_R N = \left\{ \sum_{(m,n)\in M\times N} z_{mn} m \otimes n \;\middle|\; z_{mn} \in \mathbb{Z},\ \textit{fast alle } z_{mn} = 0 \right\}$$
$$= \langle m \otimes n \mid (m,n) \in M \times N \rangle,$$

außerdem gelten die Rechenregeln

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n,$$

$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2,$$

und

$$mr \otimes n = m \otimes rn.$$

Dabei ist es jedoch sehr wichtig zu beachten, daß

$$\{m \otimes n \mid (m,n) \in M \times N\}$$

i.a. *keine* $\mathbb{Z}$-Basis ist, denn in der Regel ist eine Darstellung

$$x = \sum z_{mn}(m \otimes n)$$

von $x \in M \otimes_R N$ als $\mathbb{Z}$-Linearkombination *nicht* eindeutig, gilt doch beispielsweise

$$3 \otimes 4 = \frac{3}{2} \otimes 8 \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}.$$

Bei der Interpretation eines Ausdruckes $m \otimes n$ ist noch weitere Vorsicht geboten. Es muß zweifelsfrei klar sein, *als Element welches Tensorprodukts* dieses $m \otimes n$

verstanden werden soll. Es kann nämlich sehr wohl sein, daß m in einem echten Untermodul M' von M liegt und $m \otimes n$ als Element von $M' \otimes_R N$ verschieden von 0 ist, obwohl $M \otimes_R N = \{0\}$ und damit $m \otimes n = 0$, als Element von $M \otimes_R N$. Z. B. gilt

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \simeq \mathbb{Z}_2, \text{ aber } \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2 = \{0\}.$$

Denn für alle $a \in \mathbb{Z}, b \in \mathbb{Z}_2$ gilt:

$$a \otimes b = 1 \otimes ab \in \{1 \otimes 0, 1 \otimes 1\} \simeq \mathbb{Z}_2,$$

während wir für $q \in \mathbb{Q}$ haben:

$$q \otimes b = q' \cdot 2 \otimes b = q' \otimes 2b = q' \otimes 0 = q' \cdot 0 \otimes 0 = 0 \otimes 0.$$

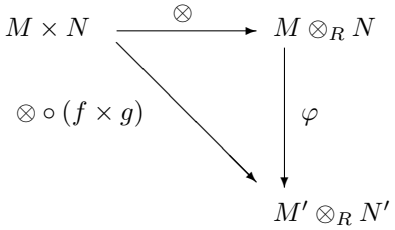
5.3.5 Satz *Sind $f\colon M_R \to M'_R$ und $g\colon {}_RN \to {}_RN'$ R-Homomorphismen, dann gilt: Es gibt genau einen Homomorphismus $f \otimes g$ zwischen (den abelschen Gruppen) $M \otimes_R N$ und $M' \otimes_R N'$ mit*

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

Beweis: Die Komposition

$$\otimes \circ (f \times g)\colon\ (m, n) \mapsto f(m) \otimes g(n)$$

ist nach den Rechenregeln 5.3.4 ausgeglichen. Es gibt deshalb genau ein $\varphi \in \mathcal{L}$, der Klasse aller Homomorphismen zwischen abelschen Gruppen, das folgendes Diagramm kommutativ ergänzt:



Für φ gilt offensichtlich $\varphi(m \otimes n) = f(m) \otimes g(n)$, so daß die Abbildung $f \otimes g := \varphi$ die Behauptung erfüllt.

□

Sei $A \dot{+} B$ die abelsche Gruppe über $A \times B$ mit komponentenweiser Verknüpfung, wobei A und B abelsch sind. Dann gilt der folgende sehr wichtige Satz über die Zerlegung des Tensorprodukts mit Hilfe von Untermoduln:

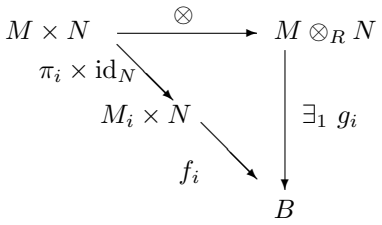
5.3.6 Satz *Ist $M = M_1 \oplus M_2$ (als R-Rechtsmodul), dann gilt*

$$M \otimes_R N \simeq M_1 \otimes_R N \dot{+} M_2 \otimes_R N.$$

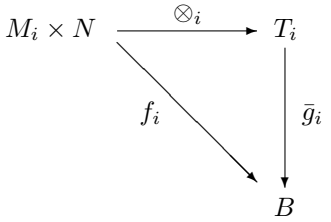
Beweis: π_i sei die Projektion von M auf M_i, $\theta_i := \pi_i \otimes id_N$, und

$$T_i := \theta_i(M \otimes_R N), i = 1, 2.$$

Es gilt: $M \otimes_R N = T_1 \oplus T_2 \simeq T_1 \dot{+} T_2$, so daß zu zeigen bleibt: $T_i \simeq M_i \otimes_R N$, d.h. T_i ist als *Tensorprodukt* von M_i und N, also als universell nachzuweisen. Sei dazu $f_i \colon M_i \times N \to B$ ausgeglichen und g_i definiert durch die Kommutativität von



Wir setzen $\bar{g}_i := g_i \downarrow T_i$ und $\otimes_i := \otimes \downarrow M_i \times N$. Es soll gezeigt werden, daß folgendes Diagramm kommutativ ist:



Dazu beachten wir, daß für alle $(m_i, n) \in M_i \times N$ gilt:

$$\overline{g}_i \circ \otimes_i(m_i, n) = \overline{g}_i \circ \otimes(m_i, n) = \overline{g}_i(m_i \otimes n) = g_i(m_i \otimes n)$$

$$= f_i \circ (\pi_i \times id_N)(m_i, n) = f_i(m_i, n).$$

Das Diagramm ist also tatsächlich kommutativ. Wegen

$$T_i = \langle \otimes_i(M_i \times N) \rangle$$

ist $\overline{g}_i$ zudem eindeutig bestimmt, $\otimes_i \colon M_i \times N \to T_i$ also universell. Demnach ist tatsächlich $T_i \simeq M_i \otimes_R N$.

Es bleibt noch nachzuweisen, daß $M \otimes_R N \simeq T_1 \dot{+} T_2$. Hierfür genügt der Beweis, daß

$$\mathrm{id}_{M \otimes_R N} = \theta_1 + \theta_2,\ \theta_i^2 = \theta_i,\ \theta_1\theta_2 = \theta_2\theta_1 = 0_{M \otimes_R N}.$$

Diese Eigenschaften der θ_i sind leicht nachzurechnen.

□

5.4 Tensorprodukte als Moduln

Ist S ein weiterer Ring mit Einselement und M sowohl R-Rechts- als auch S-Linksmodul, dann heißt M ein (S,R)-*Bimodul* (kurz: ${}_SM_R$), wenn gilt

$$(sm)r = s(mr).$$

Zu solchen Bimoduln werden z.B. $\mathbb{K}$-Linksvektorräume, $\mathbb{K}$ ein Körper, wenn man $v\kappa := \kappa v$ setzt, denn dann gilt, wegen der Kommutativität von $\mathbb{K}$,

$$(\lambda v)\kappa = \kappa(\lambda v) = (\kappa\lambda)v = (\lambda\kappa)v = \lambda(\kappa v) = \lambda(v\kappa).$$

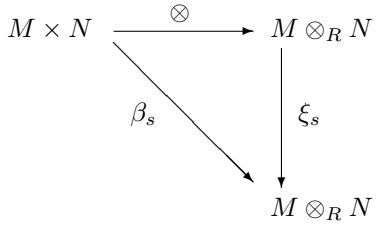
5.4.1 Satz *Ist M ein (S,R)-Bimodul, dann wird $M \otimes_R N$ zu einem S-Linksmodul vermöge*

$$s\left(\sum z_{mn}(m \otimes n)\right) := \sum z_{mn}(sm \otimes n).$$

Beweis: Für jedes $s \in S$ ist die Abbildung

$$\beta_s\colon\ M \times N \to M \otimes_R N,\ (m,n) \mapsto sm \otimes n$$

ausgeglichen, so daß genau ein Homomorphismus φ_s existiert mit kommutativem Diagramm



Für diese Abbildung ergibt sich aus der Kommutativität des Diagramms:

$$\xi_s(m \otimes n) = \beta_s(m,n) = sm \otimes n.$$

Die Homomorphieeigenschaft liefert, für $x, y \in M \otimes_R N$ und $sx := \xi_s(x)$,

$$s(x+y) = \xi_s(x+y) = \xi_s(x) + \xi_s(y) = sx + sy.$$

Die anderen Modulgesetze folgen entsprechend aus den Rechenregeln 5.3.4. □

Ist zudem noch $M = M_1 \oplus M_2$ als (S,R)-Bimodul, dann ist auch

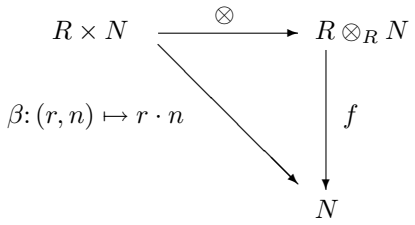
5.4.2 $$M \otimes_R N \simeq M_1 \otimes_R N \dot{+} M_2 \otimes_R N \quad \text{(als } S\text{-Linksmodul)}.$$

Schließlich ist noch folgendes Ergebnis wichtig:

5.4.3 Satz

$$R \otimes_R N \simeq N \quad \textit{(als } R\textit{-Linksmodul)}.$$

Beweis: Die Abbildung $\beta\colon (r,n) \mapsto r \cdot n$ ist ausgeglichen, es gibt also einen eindeutig bestimmten Homomorphismus f zwischen abelschen Gruppen, so daß



kommutativ ist. Dieser Homomorphismus

$$f\colon\ R \otimes_R N \to N,$$

die Fortsetzung der auf den Erzeugenden definierten Abbildung $r \otimes n \mapsto rn$, ist leicht als $R-$Isomorphismus zu erkennen, denn mit

$$g\colon\ N \to R \otimes_R N,\ n \mapsto 1 \otimes n$$

genügt sie den Gleichungen

$$f \circ g = id_N \wedge g \circ f = id_{R \otimes N}.$$

f besitzt also Rechts- und Linksinverse und ist demnach bijektiv. Außerdem ist leicht nachzurechnen, daß f R-Homomorphismus ist.

□

5.4.4 Satz *Diese Bildung des Tensorproduktes ist assoziativ, d.h.*

$$L \otimes_R (M \otimes_S N) \simeq (L \otimes_R M) \otimes_S N.$$

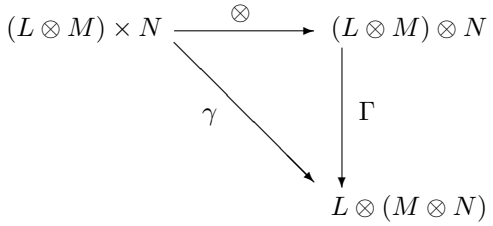
Beweis: Wir zeigen dazu, daß durch

$$l \otimes (m \otimes n) \mapsto (l \otimes m) \otimes n$$

ein Isomorphismus definiert wird. Deshalb betrachten wir die Abbildung

$$\gamma\colon (L \otimes M) \times N \to L \otimes (M \otimes N),$$

die $((l \otimes m), n) \mapsto l \otimes (m \otimes n)$ fortsetzt. Man rechnet leicht nach, daß γ ausgeglichen ist. Es gibt also genau einen Homomorphismus Γ mit kommutativem Diagramm



Γ genügt offenbar den Gleichungen

$$\Gamma((l \otimes m) \otimes n) = l \otimes (m \otimes n).$$

Entsprechend zeigt man die Existenz eines Homomorphismus

$$\Delta\colon L \otimes (M \otimes N) \to (L \otimes M) \otimes N$$

mit

$$\Delta(l \otimes (m \otimes n)) = (l \otimes m) \otimes n.$$

Für beide zusammen gilt somit

$$\Delta \circ \Gamma = id_{(L\otimes M)\otimes N}, \Gamma \circ \Delta = id_{L\otimes(M\otimes N)}.$$

Γ ist also Isomorphismus.

□

Statt $L \otimes_R (M \otimes_S N)$ können wir deshalb $L \otimes_R M \otimes_S N$ schreiben, entsprechend auch für endlich viele Faktoren

$$L \otimes_{R_1} M \otimes_{R_2} \ldots \otimes_{R_n} N.$$

Die Elemente solcher Tensorprodukte heißen *Tensoren.* Diejenigen unter ihnen, die von der Form $l \otimes m \otimes \ldots \otimes n$ sind, heißen *zerlegbare* Tensoren. Man nennt ein solches Element auch das *Tensorprodukt* von $l, m, \ldots, n$.

5.5 Tensorprodukte von Vektorräumen

$V_{\mathbb{K}}$ und ${}_{\mathbb{K}}W$ seien jetzt $\mathbb{K}$-Vektorräume, $\mathbb{K}$ ein Körper. Dann ist, wie bereits erwähnt, V auf natürliche Weise ein $\mathbb{K}$-Bimodul ($\kappa v := v\kappa$), und nach 5.4.1 wird deshalb $V \otimes_{\mathbb{K}} W$ zu einem $\mathbb{K}$-Vektorraum vermöge

$$\kappa \sum z_{vw}(v \otimes w) := \sum z_{vw}(\kappa v \otimes w) = \sum z_{vw}(v \otimes \kappa w).$$

5.5.1 Satz *Ist* $V = \langle\!\langle b_0, \ldots, b_{m-1} \rangle\!\rangle_{\mathbb{K}}, W = {}_{\mathbb{K}}\langle\!\langle c_0, \ldots, c_{n-1} \rangle\!\rangle$, *dann gilt*

$${}_{\mathbb{K}}(V \otimes_{\mathbb{K}} W) = {}_{\mathbb{K}}\langle\!\langle b_i \otimes c_k \mid i \in m, k \in n \rangle\!\rangle,$$

also ist insbesondere

$$dim_{\mathbb{K}}(V \otimes_{\mathbb{K}} W) = dim_{\mathbb{K}}(V) \cdot dim_{\mathbb{K}}(W).$$

Beweis: Aus $V = \oplus\, \mathbb{K}b_i, W = \oplus\, \mathbb{K}c_k$ folgt nach 5.3.6:

$$V \otimes_{\mathbb{K}} W \simeq_{\mathbb{K}} \dot{+}_{i,k}\ (\mathbb{K}b_i \otimes \mathbb{K}c_k).$$

Daraus folgt die Behauptung über die Dimension, denn

$$\mathbb{K}b_i \otimes \mathbb{K}c_k = \{\kappa(b_i \otimes c_k) \mid \kappa \in \mathbb{K}\} = \mathbb{K}(b_i \otimes c_k).$$

Zudem ergibt sich aus den Rechenregeln 5.3.4, daß die $b_i \otimes c_k$ das Tensorprodukt erzeugen, sie müssen also eine Basis bilden.

□

Wir betrachten jetzt lineare Abbildungen auf endlichdimensionalen $\mathbb{K}$-Vektorräumen und die davon auf dem Tensorprodukt induzierte lineare Abbildung. Sei also wieder $\mathcal{B} = (b_0, \ldots, b_{m-1})$ Basisfolge von V, $\mathcal{C} = (c_0, \ldots, c_{n-1})$ Basisfolge von W, und es sei $f \in Hom_{\mathbb{K}}(V, V')$, $g \in Hom_{\mathbb{K}}(W, W')$. Weiter sei $\mathcal{B}' = (b'_0, \ldots, b'_{m'})$ Basisfolge von V', $\mathcal{C}' = (c'_0, \ldots, c'_{n'})$ Basisfolge von W', und wir setzen $A = M(\mathcal{B}', f, \mathcal{B})$, $B = M(\mathcal{C}', g, \mathcal{C})$, die darstellenden Matrizen der linearen Abbildungen. Wegen 5.4.3 gilt

$$(f \otimes g)(b_j \otimes c_l) = \sum_{i,k} a_{ij} b_{kl} (b'_i \otimes c'_k),$$

also folgt für die Matrix $A \otimes B$, die $f \otimes g$ beschreibt bzgl. der doppelt lexikographisch geordneten Basisfolgen $(\ldots, b_i \otimes c_k, \ldots) = (b_0 \otimes c_0, b_0 \otimes c_1, \ldots, b_{m-1} \otimes c_{n-1})$ und die entsprechend angeordnete Folge $(\ldots, b'_i \otimes c'_k, \ldots)$:

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \ldots \\ a_{10}B & a_{11}B & \ldots \\ \ldots & \ldots & \ldots \end{pmatrix}$$

Diese Matrix heißt ein *Kroneckerprodukt* von A und B (die anderen Kroneckerprodukte von A und B gehören zu den anderen Numerierungen der Basiselemente). Es gilt (Übungsaufgabe):

5.5.2 Hilfssatz *Das Kroneckerprodukt von Matrizen bzw. linearen Abbildungen hat die folgenden Eigenschaften:*

- $Spur(A \otimes B) = Spur(A) \cdot Spur(B)$,
- $(A \otimes B)(A' \otimes B') = (AA') \otimes (BB')$, *bei geeigneten Zeilen- und Spaltenzahlen,*
- $\det\ (A \otimes B) = (\det(A))^n \cdot (\det(B))^m$, *falls A m-reihig, B n-reihig ist,*
- $\mathrm{Kern}(f \otimes g) = \mathrm{Kern}(f) \otimes W + V \otimes \mathrm{Kern}(g)$,
- $\mathrm{Rang}(f \otimes g) = \mathrm{Rang}(f) \cdot \mathrm{Rang}(g)$.

5.5.3 Satz *Ist $\mathbb{K}$ Teilkörper von $\mathbb{L}$, dann ist $\mathbb{L} \otimes_{\mathbb{K}} V$ ein $\mathbb{L}$-Vektorraum. Hat ${}_{\mathbb{K}}V$ die Basisfolge $\mathcal{B} = (b_0, \ldots, b_{m-1})$, dann gilt*

$$\mathbb{L} \otimes_{\mathbb{K}} V = {}_{\mathbb{L}} \ll 1_{\mathbb{L}} \otimes b_i \mid i \in m \gg .$$

Man sagt dazu, $\mathbb{L} \otimes_{\mathbb{K}} V$ entsteht aus V durch *Grundkörpererweiterung.*

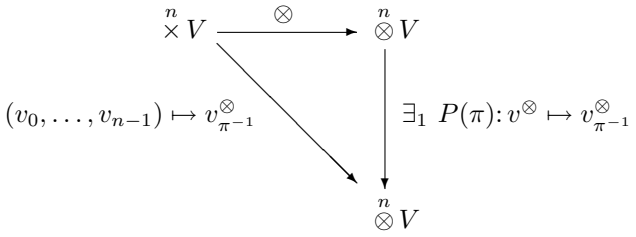
5.6 Symmetrieklassen von Tensoren

Wir betrachten jetzt, zu einem Körper $\mathbb{K}$, einem endlichdimensionalen $\mathbb{K}$-Vektorraum V und einem $n \in \mathbb{N}$, die n-fache Tensorpotenz von V:

$$\overset{n}{\otimes} V := V \otimes_{\mathbb{K}} \ldots \otimes_{\mathbb{K}} V\,,\ n\ Faktoren\,,\ \overset{0}{\otimes} V := \mathbb{K}.$$

Die Elemente von $\overset{n}{\otimes} V$ heißen *Tensoren $n-$ter Stufe.* Tensoren $0-$ter Stufe sind also die Skalare $\kappa \in \mathbb{K}$, Tensoren erster Stufe die Vektoren $v \in V$.
Unser Ziel ist die Beschreibung gewisser Unterräume von $\overset{n}{\otimes} V$, über die wir u.a. symmetrische und schiefsymmetrische Abbildungen faktorisieren können. Wir bemerken zunächst, daß folgendes gilt:

5.6.1 Hilfssatz *Zu $\pi \in S_n$ wird durch die Kommutativität des folgenden Diagramms der* Permutationsoperator $P(\pi)$ *definiert (wobei $v^{\otimes} := v_0 \otimes \ldots \otimes v_{n-1}$ und $v^{\otimes}_{\pi^{-1}} := v_{\pi^{-1}(0)} \otimes \ldots \otimes v_{\pi^{-1}(n-1)}$) :*



$P(\pi)$ ist ein $\mathbb{K}-$Automorphismus von $\overset{n}{\otimes} V$,

$$P(\pi) \in \mathrm{Aut}_{\mathbb{K}}(\overset{n}{\otimes} V),$$

und die Abbildung

$$P\colon S_n \to GL(\overset{n}{\otimes} V),\ \pi \mapsto P(\pi)$$

ist ein Homomorphismus von S_n in die volle lineare Gruppe $GL(\overset{n}{\otimes} V)$.

□

P ist also eine Darstellung von S_n auf $\overset{n}{\otimes} V$ im folgenden Sinn:

5.6.2 Definition (Darstellung einer Gruppe) Ist G eine Gruppe, $\mathbb{K}$ ein Körper, $W \neq \{0_W\}$ ein $\mathbb{K}$-Vektorraum, dann heißt jeder Homomorphismus $D\colon G \to GL(W)$ eine *(lineare) Darstellung* von G auf W. Dabei nennt man W den *Darstellungsraum.* Die Dimension von W heißt auch die *Dimension* von D, und die Funktion

$$\chi^D\colon G \to \mathbb{K}\,,\ g \mapsto \mathrm{Spur}(D(g))$$

heißt der *Charakter* der Darstellung. •

5.6.3 Beispiele Die Charaktere eindimensionaler Darstellungen, die sogenannten *eindimensionalen* Charaktere von G, sind genau die Homomorphismen χ von G in die multiplikative Gruppe $\mathbb{K}^* := (\mathbb{K}\backslash\{0\}, \cdot)$ von $\mathbb{K}$. Der *Einscharakter*

$$\iota\colon g \mapsto 1_{\mathbb{K}}$$

ist dabei ein trivialer Spezialfall. Neben ι hat die symmetrische Gruppe S_n, $n \geq 2$, $\mathrm{char}(\mathbb{K}) \neq 2$, noch genau einen weiteren eindimensionalen Charakter, nämlich

$$\epsilon\colon \pi \mapsto sgn(\pi),$$

den sogenannten *alternierenden* Charakter. ◇

5.6.4 Definition Sei $G \leq S_n$, $\mathrm{char}(\mathbb{K})$ teile die Ordnung von G nicht, χ sei ein Charakter von G. Dann heißt die lineare Abbildung

$$P_G^\chi := \frac{\chi(1)}{|G|} \sum_{\pi \in G} \chi(\pi^{-1}) P(\pi) \quad \in End_{\mathbb{K}}(\overset{n}{\otimes} V)$$

der *Symmetrisierungsoperator* zu (G, χ). •

5.6.5 Hilfssatz *Ist P_G^χ Symmetrisierungsoperator zu (G, χ), mit dem eindimensionalen Charakter χ von G, dann ist P_G^χ ein Projektionsoperator,*

$$(P_G^\chi)^2 = P_G^\chi.$$

Weiterhin gilt für diesen Operator:

$$Rang(P_G^\chi) = Spur(P_G^\chi) = \frac{1}{|G|} \sum_{\pi \in G} \chi(\pi^{-1}) m^{c(\pi)},$$

wenn $m := dim_{\mathbb{K}}(V)$ ist, und $c(\pi)$ die Anzahl der zyklischen Faktoren von $\pi \in G$ bezeichnet.

Beweis: Die Homomorphieeigenschaft von χ und P ergibt, wie man leicht nachrechnet, daß

$$P(\pi) \cdot P_G^\chi = \chi(\pi) \cdot P_G^\chi.$$

Das liefert $(P_G^\chi)^2 = P_G^\chi$, also ist P_G^χ ein Projektionsoperator. Hieraus wiederum folgt

$$P_G^\chi = 0_{Kern(P_G^\chi)} \oplus \mathrm{id}_{Bild(P_G^\chi)},$$

was $\mathrm{Rang}(P_G^\chi) = \dim_{\mathbb{K}}(\mathrm{Bild}(P_G^\chi)) = \mathrm{Spur}(P_G^\chi)$ liefert. Ist jetzt $\mathcal{B} = (b_0, \ldots, b_{m-1})$ eine Basisfolge von V, dann gilt

$$\overset{n}{\otimes} V = {}_{\mathbb{K}}\langle\!\langle\, b_\varphi := b_{\varphi(0)} \otimes \ldots \otimes b_{\varphi(n-1)} \mid \varphi \in m^n \,\rangle\!\rangle.$$

Da $P(\pi)$ diese Basiselemente nur permutiert, ist

$$\mathrm{Spur}(P(\pi)) = |\{\varphi \in m^n \mid \varphi = \varphi \circ \pi^{-1}\}|.$$

Nun gilt aber $\varphi = \varphi \circ \pi^{-1}$ genau dann, wenn

$$\forall\ i \in n\colon\ \varphi(i) = \varphi(\pi^{-1}(i)) = \varphi(\pi^{-2}(i)) = \ldots,$$

also genau dann, wenn φ auf den zyklischen Faktoren von π^{-1} konstant ist. Mit $c(\pi^{-1}) = c(\pi))$ ergibt das

$$\mathrm{Spur}(P(\pi)) = m^{c(\pi)},$$

woraus der Rest der Behauptung folgt.

□

Wir wollen nun zeigen, daß die Bilder von Symmetrisierungsoperatoren P_G^χ zu linearen Charakteren χ wichtige Universaleigenschaften haben und *setzen deshalb für den Rest des Kapitels voraus, daß die Charakteristik von $\mathbb{K}$ kein Teiler von $|G|$ ist.*

5.6.6 Definition (Symmetrieklassen) Sei $f\colon \overset{n}{\times} V \to W$ multilinear, $G \leq S_n, \chi\colon G \to \mathbb{K}^*$ ein eindimensionaler Charakter. f heißt dann $(G,\chi)-$*symmetrisch*, wenn gilt

$$\chi(\pi) f(v_{\pi(0)}, \ldots, v_{\pi(n-1)}) = f(v_0, \ldots, v_{n-1}).$$

Dafür schreiben wir kurz: $f \in M_n(V, W, G, \chi)$. Beispielsweise gilt $det \in M_n(V, \mathbb{K}, S_n, \epsilon)$. Wir setzen

$$V_G^\chi := P_G^\chi(\overset{n}{\otimes} V)$$

und nennen die Unterräume dieser Form von $\overset{n}{\otimes} V$ *(lineare) Symmetrieklassen von Tensoren.* Wir führen noch die folgende Bezeichnung ein:

$$v^\Delta := v_0 \Delta \ldots \Delta v_{n-1} := P_G^\chi(v_0 \otimes \ldots \otimes v_{n-1}) = P_G^\chi(v^\otimes).$$

•

5.6.7 Satz *Die Abbildung*

$$\Delta\colon \overset{n}{\times} V \to V_G^\chi\ ,\ (v_0, \ldots, v_{n-1}) \mapsto v^\Delta$$

ist universell bzgl.

$$\mathcal{F} := \{f \mid \exists\ U\colon f \in M_n(V, U, G, \chi)\}$$

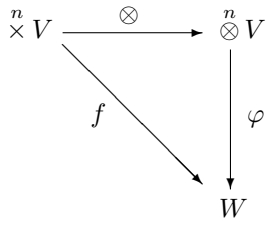
und der Klasse $\mathcal{L}$ der linearen Abbildungen zwischen $\mathbb{K}$- Vektorräumen.

Beweis: Δ liegt in $\mathcal{F}$, denn

$$\chi(\pi) v_\pi^\Delta = \chi(\pi) P_G^\chi(v_\pi^\otimes)$$

$$= \frac{1}{|G|} \sum_{\rho \in G} \chi(\pi\rho^{-1}) P(\rho\pi^{-1})(v^\otimes) = P_G^\chi(v^\otimes) = v^\Delta.$$

Die Faktorisierungseigenschaft zeigen wir wie folgt: Jedes $f \in M_n(V, W, G, \chi)$ ist multilinear, so daß genau ein lineares φ existiert mit kommutativem Diagramm

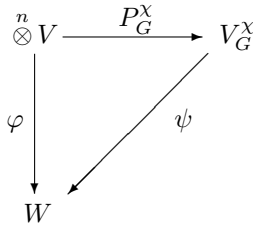


Dieses φ kann über P_G^χ faktorisiert werden, denn

$$\varphi \circ P_G^\chi(v^\otimes) = \frac{1}{|G|} \sum \chi(\pi^{-1}) \varphi(v^\otimes_{\pi^{-1}})$$

$$= \frac{1}{|G|} \sum \chi(\pi^{-1}) f(v_{\pi^{-1}(0)}, \ldots, v_{\pi^{-1}(n-1)}) = f(v_0, \ldots, v_{n-1}) = \varphi(v^\otimes).$$

Es gilt also $\varphi \circ P_G^\chi = \varphi$, und damit $Kern\ P_G^\chi \subseteq Kern\ \varphi$. Demnach gibt es lineare ψ mit kommutativem Diagramm



Da P_G^χ surjektiv ist, ist zudem ψ eindeutig bestimmt.

□

5.6.8 Bemerkung *Es gibt eine natürliche Verallgemeinerung des Begriffs der linearen Symmetrieklasse auf die Bilder von Projektionen von Symmetrieklassen P_G^χ zu nicht notwendig linearen Charakteren (den sogenannten* irreduziblen *Charakteren). Die Beschreibung von diesen setzt jedoch Resultate aus der Darstellungstheorie voraus.*

5.7 Basen und Beispiele von linearen Symmetrieklassen

Wir haben gesehen, daß die lineare Abbildung $P(\pi)$ die Basiselemente b_φ permutiert. Im Grunde handelt es sich dabei um die folgende Operation (vgl. 2.2.1) von $G \leq S_n$ auf der Indexmenge m^n der Basis $\{b_\varphi \mid \varphi \in m^n\}$ von $\overset{n}{\otimes} V$:

5.7.1 $$G \times m^n \to m^n\,,\ (\pi, \varphi) \mapsto \varphi \circ \pi^{-1}.$$

Die Untergruppe $G_\varphi := \{\pi \in G \mid \varphi = \varphi \circ \pi^{-1}\}$ heißt der Stabilisator von φ, und die Menge aller Bahnen $G(\varphi) := \{\varphi \circ \pi^{-1} \mid \pi \in G\}$ wird wie folgt bezeichnet:

$$G \setminus\!\setminus m^n := \{G(\varphi) \mid \varphi \in m^n\}.$$

Sei R_G ein Repräsentantensystem dieser Menge, eine sogenannte *Transversale.* Zu einem eindimensionalen $\chi\colon G \to \mathbb{K}^*$ sei R_G^χ die folgende Teilmenge:

$$R_G^\chi := \{\varphi \in R_G \mid G_\varphi \subseteq \mathrm{Kern}(\chi)\} = \{\varphi \in R_G \mid \forall\, \pi \in G_\varphi\colon \chi(\pi) = 1\}.$$

Unser Ziel ist der Nachweis, daß diese Menge eine Basis der Symmetrieklasse zu G und χ ist:

5.7.2 Satz $\quad V_G^\chi = \langle\!\langle\, b_\varphi^\Delta \mid \varphi \in R_G^\chi \,\rangle\!\rangle$.

Beweis:

i) Wir bemerken zunächst, daß wir unsere Untersuchung auf die b_φ^Δ beschränken können: Da die b_φ die Tensorpotenz $\overset{n}{\otimes} V$ erzeugen, spannen die $b_\varphi^\Delta = P_G^\chi(b_\varphi), \varphi \in m^n$, deren Bild unter P_G^χ auf.

ii) Bilder b_φ^Δ von Elementen b_φ aus derselben Bahn sind lineare Vielfache voneinander (mit von Null verschiedenen Koeffizienten):

$$b_{\varphi\circ\pi^{-1}}^\Delta = \frac{1}{|G|}\sum_{\rho\in G} \chi(\rho^{-1}) P(\rho\pi) b_\varphi = \chi(\pi) b_\varphi^\Delta, \qquad (*)$$

wir können wir uns demnach sogar auf die Elemente irgendeiner Transversale R_G beschränken: V_G^χ wird sogar schon von den $b_\varphi^\Delta, \varphi \in R_G$, erzeugt.

iii) Tatsächlich genügen sogar die $\varphi \in R_G^\chi$, denn die anderen Elemente aus der Transversale sind Null: Für $\varphi \in R_G \setminus R_G^\chi$ gibt es ein $\pi \in G_\varphi$ mit $\chi(\pi^{-1}) \neq 1$, so daß aus $(*)$ folgt:

$$b_\varphi^\Delta = \chi(\pi^{-1}) b_{\varphi\circ\pi^{-1}}^\Delta = \chi(\pi^{-1}) b_\varphi^\Delta,$$

was natürlich $b_\varphi^\Delta = 0$ impliziert.

iv) Zum abschließenden Nachweis der linearen Unabhängigkeit der $b_\varphi^\Delta, \varphi \in R_G^\chi$, benutzen wir die zu $(b_0, \ldots, b_{m-1})$ duale Basisfolge $(\lambda_0, \ldots, \lambda_{m-1})$, $\lambda_i \in Hom_{\mathbb{K}}(V, \mathbb{K})$, also die Linearformen mit der Eigenschaft $\lambda_i(b_j) = \delta_{ij}$. Aus ihnen

können wir leicht die zu $\{b_\varphi \mid \varphi \in m^n\}$ duale Basis gewinnen, es ist natürlich die Menge

$$\{\lambda_\varphi := \lambda_{\varphi(0)} \otimes \cdots \otimes \lambda_{\varphi(n-1)} \mid \varphi \in m^n\}.$$

Mit ihrer Hilfe können wir die Koeffizienten κ_φ aus jeder Linearkombination ermitteln. Ist etwa

$$x = \sum_{\psi \in R_G^\chi} \kappa_\psi b_\psi^\Delta,$$

dann gilt, für $\varphi \in R_G^\chi$,

$$\begin{aligned}
\lambda_\varphi(x) &= \sum_{\psi \in R_G^\chi} \kappa_\psi \lambda_\varphi(b_\psi^\Delta) \\
&= \sum_{\psi \in R_G^\chi} \kappa_\psi \lambda_\varphi P_G^\chi(b_\psi) \\
&= \sum_{\psi \in R_G^\chi} \kappa_\psi \lambda_\varphi \frac{1}{|G|} \sum_{\pi \in G} \chi(\pi^{-1}) P(\pi)(b_\psi) \\
&= \sum_{\psi \in R_G^\chi} \kappa_\psi \frac{1}{|G|} \sum_{\pi \in G} \chi(\pi^{-1}) \lambda_\varphi(b_{\psi \circ \pi^{-1}}).
\end{aligned}$$

Wegen

$$\lambda_\varphi(b_{\psi \circ \pi^{-1}}) = \delta_{\varphi, \psi \circ \pi^{-1}},$$

was zu

$$\varphi = \psi \ \wedge \ \pi \in G_\varphi \subseteq \mathrm{Kern}(\chi)$$

äquivalent ist, folgt insgesamt

$$\lambda_\varphi(x) = \kappa_\varphi \frac{|G_\varphi|}{|G|}.$$

Insgesamt erhalten wir demnach die interessante Gleichung

5.7.3
$$\kappa_\varphi = \frac{|G|}{|G_\varphi|} \lambda_\varphi(x).$$

Ist beispielsweise

$$0 = \sum_{\psi \in R_G^\chi} \kappa_\psi b_\psi^\Delta,$$

dann gilt für die Koeffizienten in dieser Linearkombination

$$\kappa_\varphi = \frac{|G|}{|G_\varphi|} \lambda_\varphi(0) = 0,$$

die Elemente aus R_G^χ sind also tatsächlich linear unabhängig, und der Beweis ist damit abgeschlossen.

□

5.7.4 Beispiele

i) $\bigvee^n V := V^\iota_{S_n}$, der Raum der *symmetrischen Tensoren n−ter Stufe.* Die Bahnen von S_n auf m^n sind offenbar die Teilmengen der Funktionen vom gleichen Gewicht:

$$S_n(\varphi) = S_n(\psi) \Longleftrightarrow \forall\ i \in m\colon\ |\varphi^{-1}(i)| = |\psi^{-1}(i)|.$$

Als ein Repräsentantensystem R_{S_n} der Bahnen können wir deshalb die (schwach) monoton wachsenden Funktionen φ wählen. Da wir den Einscharakter ι betrachten, gilt außerdem $R^\iota_{S_n} = R_{S_n}$. Es folgt also aus 5.7.2, wenn wir statt b^Δ_φ zur Verdeutlichung $b^\vee_\varphi := P^\iota_{S_n}(b_\varphi)$ schreiben:

$$\bigvee^n V := V^\iota_{S_n} = \langle\!\langle\, b^\vee_\varphi \mid \varphi \in m^n \textit{ schwach monoton wachsend} \,\rangle\!\rangle.$$

Die Dimension dieses Raumes erhalten wir aus der Tatsache, daß jedes *schwach* monoton wachsende n-Tupel $(\varphi(0), \ldots, \varphi(n-1))$ über m ein *streng* monoton waschsendes $n-$Tupel $(\varphi(0), \varphi(1)+1, \ldots, \varphi(n-1)+n-1)$ mit Werten in $m+n-1$ ergibt und umgekehrt. Die Anzahl all dieser streng monoton wachsenden $n-$Tupel ist aber gleich der Anzahl der Teilmengen der Ordnung n in $m+n-1$, also gleich

$$\binom{m+n-1}{n}.$$

Dieser Binomialkoeffizient ist demnach die gesuchte Dimension:

5.7.5 $$\dim_{\mathbb{K}} \left(\bigvee^n V \right) = \binom{m+n-1}{n}.$$

ii) $\bigwedge^n V := V^\epsilon_{S_n}$, der Raum der *schiefsymmetrischen Tensoren n−ter Stufe.* Wegen $\mathrm{Kern}(\epsilon) = A_n$ liegt $\varphi \in R_{S_n}$ liegt genau dann in $R^\epsilon_{S_n}$, wenn gilt

$$\forall\ i\colon\ |\varphi^{-1}(i)| \leq 1,$$

denn ein solches φ darf ja durch keine Transposition festgelassen werden. In $R^\epsilon_{S_n}$ liegen also genau die streng monoton wachsenden φ. Mit $b^\wedge_\varphi := P^\epsilon_{S_n}(b_\varphi)$ gilt demnach:

5.7.6 $$\bigwedge^n V = \langle\!\langle\, b^\wedge_\varphi \mid \varphi \in m^n \textit{ streng monoton wachsend} \,\rangle\!\rangle.$$

Für die Dimension ergibt sich also

5.7.7 $$\dim_{\mathbb{K}} \left(\bigwedge^n V \right) = \binom{m}{n}.$$

iii) Zur Berechnung der Komponenten von Elementen x aus $\bigvee^n V$ oder aus $\bigwedge^n V$ können wir 5.7.3 verwenden. Betrachten wir etwa $x := v^\wedge := v_0 \wedge \ldots \wedge v_{n-1} \in \bigwedge^n V$. Der Ansatz

$$v^\wedge = \sum_{\varphi \in R^\epsilon_{S_n}} \kappa_\varphi b^\wedge_\varphi$$

ergibt

$$\kappa_\varphi = \frac{n!}{1} \cdot \lambda_\varphi(v^\wedge),$$

wobei

$$\lambda_\varphi(v^\wedge) = \frac{1}{n!} \sum_{\pi \in S_n} \epsilon(\pi) \lambda_\varphi(v_{\pi^{-1}}) = \frac{1}{n!} \sum_\pi sgn(\pi) \prod_i v_{\pi^{-1}(i),\varphi(i)}$$

$$= \frac{1}{n!} \underbrace{\det(v_{i,\varphi(k)})}_{:=\det(A[id|\varphi])},$$

wenn $v_i = \sum v_{ij} b_j$ und $A[\mathrm{id} \mid \varphi]$ die Matrix bezeichnet, die in der i-ten Zeile und k-ten Spalte das Element $v_{i,\varphi(k)}$ enthält, für die vorgegebene Abbildung $\varphi \in m^n$. Wir erhalten also die folgende Darstellung von $v^\wedge$ als Linearkombination aus den Basiselementen:

5.7.8 $$v^\wedge = \sum_\varphi \det(A[id \mid \varphi]) b^\wedge_\varphi,$$

wobei über die streng monoton wachsenden $\varphi \in m^n$ zu summieren ist. $\diamond$

Interessante *Anwendungen* von Symmetrieklassen sind beispielsweise Herleitungen von Sätzen über Determinanten, z.B. der *Cauchy-Binet-Formel,* die abschließend bewiesen werden soll, als einer der vielen Determinantensätze aus der multilinearen Algebra. Der Beweis verwendet Koeffizientenvergleich bei einer Anwendung einer geeigneten Linearform auf einen geeigneten Tensor.
Die Anwendung der Linearformen $\mu := \mu^\otimes \in Hom_{\mathbb{K}}(\otimes^n V, \mathbb{K})$ mit den Faktoren

$$\mu_t := \sum_i b_{it} \lambda_i,$$

auf den Tensor $v^\wedge$ mit den Faktoren $v_i := \sum_k a_{i,k} b_k$ ergibt

$$\begin{aligned}
\mu(v^\wedge) &= \frac{1}{n!} \sum_\pi sgn(\pi) \mu(v_{\pi^{-1}}) \\
&= \frac{1}{n!} \sum_\pi sgn(\pi) \prod_t \mu_t(v_{\pi^{-1}(t)}) \\
&= \frac{1}{n!} \sum_\pi sgn(\pi) \prod_t \sum_i b_{i,t} \lambda_i \left(\sum_k a_{\pi^{-1}(t),k} b_k \right)
\end{aligned}$$

$$\begin{aligned} &= \frac{1}{n!}\sum_{\pi} sgn(\pi)\prod_t \sum_i b_{i,t}a_{\pi^{-1}(t),i} \\ &= \frac{1}{n!}\sum_{\pi} sgn(\pi)\prod_t \underbrace{\sum_i a_{\pi^{-1}(t),i}b_{i,t}}_{=(AB)_{\pi^{-1}(t),t}} \\ &= \frac{1}{n!}det(AB) \end{aligned}$$

Andererseits gilt, mit 5.7.8,

$$\begin{aligned} \mu(v^{\wedge}) &= \mu(\sum_{\varphi}\kappa_{\varphi}b_{\varphi}^{\wedge}) \\ &= \sum_{\varphi}\det(A[id \mid \varphi])\mu(b_{\varphi}^{\wedge}), \end{aligned}$$

und schließlich ist noch

$$\begin{aligned} \mu(b_{\varphi}^{\wedge}) &= \frac{1}{n!}\sum_{\pi} sgn(\pi)\prod_t \mu_t(b_{\varphi(\pi^{-1}(t))}) \\ &= \frac{1}{n!}\sum_{\pi} sgn(\pi)\prod_t \sum_i b_{i,t}\lambda_i(b_{\varphi\circ\pi^{-1}(t)}) \\ &= \frac{1}{n!}\sum_{\pi} sgn(\pi)\prod_t b_{\varphi\circ\pi^{-1}(t),t} \\ &= \frac{1}{n!}\sum_{\pi} sgn(\pi)\prod_t b_{\varphi(t),\pi^{-1}(t)} \\ &= \frac{1}{n!}\det(B[\varphi \mid id]) \end{aligned}$$

Insgesamt erhalten wir damit die gewünschte Formel zur Berechnung der Determinante eines Produkts von (evtl. rechteckigen) Matrizen, die

5.7.9 Die Formel von Cauchy–Binet

$$\det(AB) = \sum_{\varphi\in m^n, str.mon.w.} \det(A[id \mid \varphi])\det(B[\varphi \mid id]).$$

5.8 Die Tensoralgebra

Ist $\mathbb{K}$ jetzt ein *beliebiger Körper*, V ein $\mathbb{K}$-Vektorraum, dann können wir, wie im folgenden beschrieben wird, aus den Vektorräumen $\otimes^n V, n \in \mathbb{N}$, eine wichtige Algebra konstruieren.

5.8.1 Definition (graduierter Vektorraum) $(H, +)$ sei eine abelsche Halbgruppe. Ein $\mathbb{K}$-Vektorraum W heißt dann ein *H-graduierter Vektorraum*, wenn es zu jedem $h \in H$ einen Unterraum W_h gibt mit $W = \oplus_h W_h$. •

5.8.2 Beispiele

- Ist $(H, +)$ abelsche Halbgruppe und, für jedes $h \in H$, W_h ein $\mathbb{K}$-Vektorraum, dann heißt der $\mathbb{K}$-Vektorraum

$$\prod_{h\in H} W_h := \{f\colon H \to \bigcup_{h\in H} W_h \mid \forall\, h \in H\colon f(h) \in W_h\}.$$

  das *Produkt* der W_h, und

$$\coprod_{h\in H} W_h := \{f\colon H \to \bigcup_{h\in H} W_h \mid \forall\, h \in H\colon f(h) \in W_h,\ \text{fast alle } f(h) = 0\}$$

  das *Coprodukt* (oder auch die *äußere direkte Summe* der W_h). Es gilt $\coprod W_h = \oplus \overline{W}_h$, mit

$$\overline{W}_h := \{f \in \coprod W_h \mid \forall\, h' \neq h\colon f(h') = 0\} \simeq_{\mathbb{K}} W_h.$$

- Gemäß den vorangegangenen Beispielen haben wir zu V den $\mathbb{N}$-graduierten $\mathbb{K}$-Vektorraum

$$T_0(V) := \coprod_{n\in\mathbb{N}} \overset{n}{\otimes} V = \bigoplus_{n\in\mathbb{N}} \overline{\overset{n}{\otimes} V} = \overline{\mathbb{K}} \oplus \overline{V} \oplus (\overline{V \otimes V}) \oplus \ldots,$$

  das heißt:

$$T_0(V) = \{f\colon \mathbb{N} \to \bigcup_{n\in\mathbb{N}} \overset{n}{\otimes} V \mid \forall\, n \in \mathbb{N}\colon f(n) \in \overset{n}{\otimes} V,\ \text{fast alle } f(n) = 0\}.$$

- Der Polynomring $\mathbb{K}[x]$ enthält die Unterräume ${}_{\mathbb{K}}\langle\langle x^n \rangle\rangle$, für alle $n \in \mathbb{N}$, und es gilt

$$\mathbb{K}[x] = \bigoplus_{n\in\mathbb{N}} \langle\langle x^n \rangle\rangle,$$

  $\mathbb{K}[x]$ ist also ein $\mathbb{N}$-graduierter $\mathbb{K}$-Vektorraum.

◇

5.8.3 Definition (homogen, graduierte Algebra) $W = \bigoplus W_h$ sei H-graduierter $\mathbb{K}$-Vektorraum.

- $w \in W$ heißt *homogen vom Grad* h, wenn $w \in W_h$. $U \leq W$ heißt *homogen*, wenn U von homogenen Elementen erzeugt wird.
- Ist W zudem noch eine $\mathbb{K}$-Algebra, d.h. ist eine Multiplikation definiert, so daß $(W, +, \cdot)$ zu einem Ring wird und

$$\kappa(ww') = (\kappa w)w' = w(\kappa w')$$

gilt, für alle $\kappa \in \mathbb{K},\ w, w' \in W$, dann heißt W eine *H-graduierte $\mathbb{K}$-Algebra*, wenn

$$W_h \cdot W_{h'} \subseteq W_{h+h'}.$$

Ein Ideal I heißt dabei *homogenes Ideal*, wenn es (als $\mathbb{K}$-Algebra) von homogenen Elementen erzeugt wird, d.h. wenn es homogene Elemente gibt, so daß jedes $i \in I$ eine Linearkombination aus endlichen Produkten dieser homogenen Elemente ist.

•

5.8.4 Beispiele

- $\mathbb{K}[x]$ ist eine $\mathbb{N}$-graduierte Algebra.
- $\{f \in \mathbb{K}[x] \mid \text{ Polynomgrad } f \leq 5\} \cup \{0\}$ ist homogener Unterraum, jedoch kein Ideal.
- Die Polynome mit lauter geraden Koeffizienten bilden ein homogenes Ideal.

◇

5.8.5 Definition (homogene Abbildung) Seien $V = \bigoplus V_h$ und $W = \bigoplus W_h$, beide H-graduiert, $f \in Hom_{\mathbb{K}}(V, W)$. Dann heißt f *homogen vom Grad* h', wenn gilt

$$f(V_h) \subseteq W_{h+h'}.$$

•

5.8.6 Beispiele

- $f\colon \mathbb{K}[x] \to \mathbb{K}[x]\,,\ p \mapsto x^n \cdot p$ ist homogen vom Grad n.
- $\mathbb{K}[x]$ kann auch als $\mathbb{Z}$-graduierte $\mathbb{K}$-Algebra geschrieben werden:

$$\mathbb{K}[x] := \bigoplus_{z \in \mathbb{Z}} V_z,\ V_z := \langle\langle x^z \rangle\rangle,\ \text{falls } z \geq 0, V_z := \{0\},\ \text{falls } z < 0.$$

Die Differentiation $\frac{d}{dx}\colon\ \mathbb{K}[x] \to \mathbb{K}[x]$ ist, als lineare Abbildung auf diesem $\mathbb{Z}$-graduierten $\mathbb{K}$-Vektorraums, homogen vom Grad -1.

◇

Wir wollen nun aus folgenden Vektorräumen V_q^p (zu gegebenen $\mathbb{K}$) eine graduierte Algebra bilden:

5.8.7 Definition (Raum der gemischten Tensoren) Seien V ein $\mathbb{K}-$Vektorraum, p, q natürliche Zahlen, dann setzen wir:

$$V_q^p := \underbrace{V \otimes \ldots \otimes V}_{p} \otimes \underbrace{L(V) \otimes \ldots \otimes L(V)}_{q}.$$

Die Elemente dieses Tensorprodukts V_q^p heißen *p-fach kontravariante* und q-fache *kovariante* Tensoren. V_0^p heißt Raum der *p-fach kontravarianten*, V_q^0 der Raum der *$q-$fach kovarianten Tensoren*. Aus diesen Räumen bilden wir

$$T(V) := \coprod_{(p,q)} V_q^p = \bigoplus_{(p,q)} \overline{V_q^p},$$

den *Raum der gemischten Tensoren* über V. Er ist $\mathbb{N} \times \mathbb{N}$-graduiert. •

$T(V)$ soll nun zu einer $\mathbb{N}\times\mathbb{N}$-graduierten *Algebra* gemacht werden. Zu $(p, q), (p', q') \in \mathbb{N} \times \mathbb{N}$ sei zunächst

$$\nu\colon \overline{V_q^p} \times \overline{V_{q'}^{p'}} \to \overline{V_{q+q'}^{p+p'}}$$

definiert als bilineare Fortsetzung von

5.8.8 $$\nu(v^\otimes \otimes \lambda^\otimes, w^\otimes \otimes \mu^\otimes) := v^\otimes \otimes w^\otimes \otimes \lambda^\otimes \otimes \mu^\otimes.$$

Mit Hilfe dieser Abbildungen ν definieren wir die *Multiplikation*, also eine Abbildung

$$\nu\colon T(V) \times T(V) \to T(V)\,,\ (f, g) \mapsto \nu(f, g)$$

jetzt als distributive Fortsetzung, d.h. durch Angabe des Wertes von $\nu(f, g)$ an der Stelle $(m, n) \in \mathbb{N} \times \mathbb{N}$ wie folgt:

$$\nu(f, g)((m, n)) := \sum_{\substack{p+p'=m \\ q+q'=n}} \nu(f(p, q), g(p', q')).$$

(Die Summe auf der rechten Seite dieser definierenden Gleichung ist endlich!) $T(V)$ zusammen mit der durch ν definierten Multiplikation heißt *die (gemischte) Tensoralgebra über V*. Durch Einschränkung erhält man daraus eine Multiplikation auf dem Unterraum

$$T_0(V) = \bigoplus_{p\in\mathbb{N}} \overline{V_0^p},$$

der Algebra der *kontravarianten* Tensoren, bzw. auf

$$T^0(V) = \bigoplus_{q\in\mathbb{N}} \overline{V_q^0},$$

der Algebra der *kovarianten* Tensoren.

5.8.9 Bemerkungen

- *In 5.8.8 wird zu je zwei Paaren* $(p,q),(p',q') \in \mathbb{N}\times\mathbb{N}$ *ein* ν *definiert. Da* $T(V)$ *direkte Summe der* $\overline{V_q^p}$ *ist, wird dadurch eindeutig eine bilineare Abbildung* $\nu\colon T(V)\times T(V)\to T(V)$ *bestimmt.*
- $\nu(f,g)$ *hat höchstens endlich viele Werte* $\neq 0$.
- *Gilt* $x_i \in \overline{V_{q_i}^{p_i}}$, $i=1,2,3$, *dann haben wir*

$$\nu(x_1,\nu(x_2,x_3)) = \nu(\nu(x_1,x_2),x_3).$$

  Daraus folgt die Assoziativität von ν. *Die anderen Gesetze, z.B. die Distributivgesetze, folgen analog.*

- *Es gilt* $\nu(\overline{V_q^p}\times\overline{V_{q'}^{p'}}) \subseteq \overline{V_{q+q'}^{p+p'}}$. $T(V)$ *ist also eine* $\mathbb{N}\times\mathbb{N}$*-graduierte* $\mathbb{K}$*-Algebra.*

5.8.10 Beispiel

$$(2+v_1\otimes f_1+v_2\otimes v_3\otimes f_2)\otimes(v_4\otimes v_5\otimes f_3+f_4\otimes f_5) =$$

$$2(v_4\otimes v_5\otimes f_3)+2(f_4\otimes f_5)+v_1\otimes v_4\otimes v_5\otimes f_1\otimes f_3$$

$$+v_1\otimes f_1\otimes f_4\otimes f_5+v_2\otimes v_3\otimes v_4\otimes v_5\otimes f_2\otimes f_3+v_2\otimes v_3\otimes f_2\otimes f_4\otimes f_5.$$

◇

5.8.11 Definition Die Unteralgebren

$$T_0(V) := \bigoplus_{n\in\mathbb{N}} \overline{V_0^n}, \text{ bzw. } T^0(V) := \bigoplus_{n\in\mathbb{N}} \overline{V_n^0}.$$

heißen die Algebren der *kontravarianten* bzw. der *kovarianten* Tensoren über V.

•

5.9 Die Graßmann-Algebra

Wir betrachten in der Algebra

$$T_0(V) = \overline{\mathbb{K}} \oplus \overline{V} \oplus \overline{V \otimes V} \oplus \dots$$

der kovarianten Tensoren das Ideal I, das von den Tensoren $v \otimes v, v \in V$, erzeugt wird, also

$$I := \left\{ \sum u^{\otimes} \otimes v \otimes v \otimes w^{\otimes} \;\middle|\; u^{\otimes}, w^{\otimes} \in T_0(V), v \in V \right\}.$$

Ein Ideal in einer graduierten Algebra heißt *homogenes Ideal*, wenn es (als $\mathbb{K}$-Algebra) von homogenen Elementen erzeugt wird. Das gerade definierte Ideal I in der Algebra der kontravarianten Tensoren ist ein solches Ideal. Ein weiteres Beispiel bilden die Polynome mit lauter geraden Koeffizienten in $\mathbb{K}[x]$.

5.9.1 Hilfssatz *Ist $W = \bigoplus W_h$ H-graduiert, U ein homogener Unterraum dann gilt:*

- *$U = \bigoplus_h (U \cap W_h)$, ist also ebenfalls H-graduiert.*
- *$W/U = \bigoplus_h \nu_U(W_h) \simeq \coprod_h W_h/U_h$, mit $U_h := U \cap W_h$.*

Beweis:

i) Ist E ein Erzeugendensystem von U aus lauter homogenen Elementen $\neq 0$, dann ist $E = \bigcup(E \cap W_h)$, also

$$U = \sum_h U \cap W_h = \bigoplus_h (U \cap W_h).$$

ii) Wir betrachten $\alpha_h \colon W_h + U \to W_h/U_h, w_h + U \mapsto w_h + U_h$. Dafür gelten offensichtlich die folgen Äquivalenzen:

$$w_h + U = w'_h + U \Leftrightarrow w_h - w'_h \in U \Leftrightarrow w_h - w'_h \in U_h \Leftrightarrow w_h + U_h = w'_h + U_h.$$

Liest man diese von links nach rechts, so erweist sich α_h als wohldefiniert. Von rechts nach links gelesen ergibt sich die Injektivität. Die Surjektivität ist trivial. Es gilt demnach

$$\nu_U(W_h) \simeq_{\mathbb{K}} W_h/U_h.$$

iii) Es bleibt also nur noch zu zeigen, daß die Summe $\sum \nu_U(W_h)$ direkt ist. Ein Ansatz $0 = \sum_{h\in} \nu_U(w_h)$ ergibt aber

$$0 = \sum w_h + U \Longrightarrow \sum w_h \in U \Longrightarrow w_h \in U_h \Longrightarrow \nu_U(w_h) = 0.$$

□

5.9.2 Satz *Ist $A = \bigoplus A_h$ eine H-graduierte $\mathbb{K}$-Algebra, I ein homogenes Ideal, dann hat A/I die H-Graduierung*

$$A/I = \bigoplus \nu_I(A_h) \simeq_{\mathbb{K}} \coprod A_h/I_h, \;\; \textit{mit } I_h := I \cap A_h.$$

Beweis: Nach 5.9.1 gilt jedenfalls

$$A/I = \bigoplus \nu_I(A_h) \text{ (als } \mathbb{K}\text{-Vektorraum).}$$

Ist jetzt $x_h \in \nu_I(A_h), y_{h'} \in \nu_I(A_{h'})$, etwa

$$x_h = \nu_I(a_h), y_{h'} = \nu_I(b_{h'}),$$

dann gilt:

$$x_h \cdot y_{h'} = \nu_I(a_h \cdot b_{h'}) = \nu_I(c_{h+h'}) \in \nu_I(A_{h+h'}).$$

Die angegebene Zerlegung $A/I = \bigoplus \nu_I(A_h)$ ist also auch eine $H-$Graduierung für die Ringstruktur A/I.

□

5.9.3 Definition (Graßmann–Algebra) $T_0(V)/I$ ist, wie $T_0(V)$, $\mathbb{N}-$graduierte $\mathbb{K}-$Algebra, die sogenannte *Graßmann-Algebra* (oder auch: die äußere Algebra) über V:

$$\bigwedge V := T_0(V)/I = \bigoplus_{n\in\mathbb{N}} \nu_I(\overline{\otimes^n V}).$$

•

5.9.4 Satz *Der Unterraum $\nu_I(\overline{V_0^n})$ von $\bigwedge V$ ist isomorph zu $\bigwedge^n V$. Wir können also schreiben:*

$$\bigwedge V \simeq \coprod_{n\in\mathbb{N}} \overset{n}{\bigwedge} V = \bigoplus_{n\in\mathbb{N}} \overline{\overset{n}{\bigwedge} V}.$$

Beweis: Wir betrachten die Abbildungen

$$\mu_n \colon \overset{n}{\times} V \to \nu_I(\overline{\overset{n}{\otimes} V}), (v_0, \ldots, v_{n-1}) \mapsto \nu_I(v^{\otimes}).$$

i) $\mu_n \in M_n(\times^n V, \nu_I(\overline{\overset{n}{\otimes} V}), S_n, \epsilon)$: Aus der Definition von I folgt

$$\mu_n(v_0, \ldots, v_{i-1}, v_i + v_{i+1}, v_i + v_{i+1}, v_{i+2}, \ldots, v_{n-1}) = 0,$$

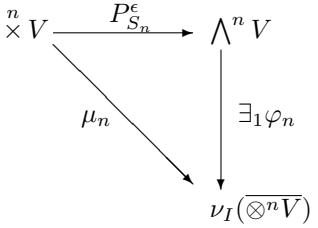
also gilt

$$\mu_n(v_0, \ldots, v_{n-1}) = -\mu_n(v_0, \ldots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \ldots, v_{n-1}),$$

und das wiederum impliziert

$$\mu(v_0, \ldots, v_{n-1}) = \epsilon(\pi)\mu_n(v_{\pi(0)}, \ldots, v_{\pi(n-1)}).$$

ii) Nach i) kann μ_n über $\bigwedge^n V$ faktorisiert werden:



es bleibt zu zeigen, daß φ_n Isomorphismus ist. Nach dem Abbildungssatz genügt — wegen der Surjektivität von $P^{\epsilon}_{S_n}$ — der Nachweis der Gleichheit der Kerne.

ii) Wir zeigen deshalb, daß $I \cap \overline{\overset{n}{\otimes} V} = \mathrm{Kern}(P^{\epsilon}_{S_n})$:

a) $\mathrm{Kern}(P^{\epsilon}_{S_n}) \subseteq I \cap \overline{\overset{n}{\otimes} V}$: Weil $P^{\epsilon}_{S_n}$ Projektionsoperator ist, gilt

$$\mathrm{Kern}(P^{\epsilon}_{S_n}) = \mathrm{Bild}(\mathrm{id} - P^{\epsilon}_{S_n}) = {}_{\mathbb{K}}\langle (\mathrm{id} - P^{\epsilon}_{S_n}) v^{\otimes} \mid v_i \in V \rangle$$

und beachten, daß

$$(\mathrm{id} - P^{\epsilon}_{S_n}) v^{\otimes} = \frac{1}{n!} \sum_{\pi} (v^{\otimes} - \epsilon(\pi) v^{\otimes}_{\pi}) \in I \cap \overline{\overset{n}{\otimes} V},$$

denn

$$\nu_I(v^{\otimes} - \epsilon(\pi) v^{\otimes}_{\pi}) = \mu_n(v_0, \ldots, v_{n-1}) - \epsilon(\pi) \mu_n(v_{\pi(0)}, \ldots, v_{\pi(n-1)}) =_{i)} 0.$$

b) Die Umkehrung $I \cap \overline{\overset{n}{\otimes} V} \subseteq \mathrm{Kern}(P^{\epsilon}_{S_n})$ ist trivial, da jedes $u^{\otimes} \otimes v \otimes v \otimes w^{\otimes}$ aus $\overline{\overset{n}{\otimes} V}$ im Kern von $P^{\epsilon}_{S_n}$ liegt.

□

Die Graßmann-Algebra ist also direkte Summe der Symmetrieklassen $\bigwedge^n V$, und diese wiederum haben, wie wir bereits seit langer Zeit wissen, als Basen die Mengen

$$\{ b^{\Delta}_{\varphi} \mid \varphi \text{ streng monoton wachsend} \}.$$

Streng monoton wachsende Abbildungen von n nach m gibt es aber nur für $n \leq m$. Wir schließen daraus, mit Hilfe der Dimensionsformel

$$\dim_{\mathbb{K}}(\bigwedge^n V) = \binom{m}{n},$$

daß folgendes richtig ist, weil $2^m = (1+1)^m = \sum_{n \leq m} \binom{m}{n}$:

5.9.5 Folgerung

- $\bigwedge V = \bigoplus_{n \leq m} \overline{\bigwedge^n V}$,
- $dim_{\mathbb{K}}(\bigwedge V) = 2^{dim_{\mathbb{K}}(V)}$.

□

Wir benutzen im folgenden auch für die Multiplikation in $\bigwedge V$ das Symbol $\wedge$ anstelle von $\cdot$, schreiben also z.B. $v^{\wedge} \wedge w^{\wedge}$ anstelle von $v^{\wedge} \cdot w^{\wedge}$.

5.9.6 Anwendungen

i) $v \wedge v = 0$.

ii) Man kann auch die Cramersche Regel mit diesen Mitteln herleiten: Ist $Ax = b$ ein vorgegebenes lineares Gleichungssystem mit regulärer Koeffizientenmatrix $A \in \mathbb{K}^{n\times n}$ und Spaltenvektoren a_k, dann setzt man

$$v_t := a_0 \wedge \ldots \wedge a_{t-1} \wedge a_{t+1} \wedge \ldots \wedge a_{n-1}, t \in n.$$

Statt $Ax = b$ können wir auch schreiben

$$\sum_k x_k a_k = b.$$

um daraus x_k zu ermitteln, multiplizieren wir (in $\bigwedge V$) mit v_t. Es ergibt sich dabei einerseits

$$v_t \wedge b = \sum x_k(v_t \wedge a_k) = x_t(v_t \wedge a_t).$$

Andererseits gilt aber auch (beachte 5.7.8):

$$v_t \wedge b = (-1)^{n-t+1} a_0 \wedge \ldots \wedge a_{t-1} \wedge b \wedge a_{t+1} \wedge \ldots \wedge a_{n-1}$$

$$= (-1)^{n-t+1} \det(a_0, \ldots, a_{t-1}, b, a_{t+1}, \ldots, a_{n-1}) b_0 \wedge \ldots \wedge b_{n-1},$$

während 5.7.8 auch noch folgendes hergibt:

$$v_t \wedge a_t = (-1)^{n-t} \cdot \det(A) \cdot b_0 \wedge \ldots \wedge b_{n-1}.$$

Also ergibt sich insgesamt

$$x_t = \frac{det(a_0, \ldots, a_{t-1}, b, a_{t+1}, \ldots, a_{n-1})}{\det(A)};$$

das ist die *Cramersche Regel.*

$\diamond$

Kapitel 6

Gruppentheorie

Wir setzen in diesem Kapitel die Theorie und Anwendung der Gruppentheorie fort. Gruppen sind die wichtigsten Grundstrukturen der Algebra. Sie spielen in Anwendungen u.a. bei Symmetriebetrachtungen eine zentrale Rolle, auch bei klassischen Problemen aus der Geometrie, bei der Auflösbarkeit von Gleichungen usw.
Gruppen sind auch das zentrale Hilfsmittel zur Untersuchung von mathematischen Strukturen, die als Äquivalenzklassen definiert sind (wie beispielsweise unnumerierte Graphen), wenn man diese abzählen oder gar konstruieren will. Mit Hilfe von Mitteln aus der Gruppentheorie kann man sogar eine gleichverteilte Zufallserzeugung solcher Strukturen organisieren.

6.1 Präsentationen von Gruppen

Es geht jetzt um die Beschreibung von Gruppen durch Erzeugende und Relationen, also z. B. um die genaue Beschreibung dessen, was Zeilen wie die folgende bedeuten:

$$G := \langle x, y \mid x^2 = y^2 = (xy)^3 = 1 \rangle.$$

Aus dieser Zeile erhält man durch naives Rechnen die folgende Multiplikationstafel:

	1	x	y	xy	yx	xyx
1	1	x	y	xy	yx	xyx
x	x	1	xy	y	xyx	yx
y	y	yx	1	xyx	x	xy
xy	xy	xyx	x	yx	1	y
yx	yx	y	xyx	1	xy	x
xyx	xyx	xy	yx	x	y	1

eine zu S_3 isomorphe Gruppe. Diese ist aber, im Gegensatz zu der Definition der S_3 als Menge von Bijektionen auf der Menge $\{0, 1, 2\}$, eine sogenannte *abstrakte Gruppe*, die gegeben ist durch die Erzeugenden x und y und durch die drei Gleichungen, die em definierenden Relationen $x^2 = 1$, $y^2 = 1$ sowie $(xy)^3 = 1$. Ein Isomorphismus zwischen beiden Gruppen ist offenbar die Fortsetzung von $x \mapsto (01), y \mapsto (12)$. Es stellt sich also die Frage, ob man jede Gruppe so beschreiben, und wie man mit abstrakten Gruppen rechnen kann.

6.1.1 Definition (freie Gruppen) Ist M eine Menge, $\varphi\colon M \to G$ eine Abbildung von M in eine Gruppe G, dann heißt G eine von M *frei erzeugte Gruppe*, wenn

$$\varphi\colon M \to G$$

universell ist bzgl. der Klasse $\mathcal{F}$ der Abbildungen von M in Gruppen und der Klasse $\mathcal{L}$ der Homomorphismen zwischen Gruppen. •

6.1.2 Satz *Zu jeder Menge M existieren von ihr frei erzeugte Gruppen, je zwei von ihnen sind isomorph.*

Beweis: Wir konstruieren eine Gruppe $F(M)$, die die gewünschten Eigenschaften hat.

- Zu M nehmen wir eine bijektive, aber zu M *disjunkte* Menge M^{-1} hinzu, einem $m \in M$ entspreche dabei das Element $m^{-1} \in M^{-1}$. Diese beiden Mengen fassen wir zum *Alphabet* $A := M \cup M^{-1}$ zusammen und bilden die Halbgruppe A^* aus den endlichen Wörtern w über A, einschließlich des *leeren Worts* ϵ, mit dem Anfügen ("Concatenation") als Verknüpfung:

  $$ww' = (a_{i_0} \cdots a_{i_{k-1}})(a_{j_0} \cdots a_{j_{l-1}}) := a_{i_0} \cdots a_{i_{k-1}} a_{j_0} \cdots a_{j_{l-1}}.$$

  Das leere Wort ist hier offenbar das neutrale Element, die Halbgruppe A^* ist also ein *Monoid*.

- Auf A^* definieren wir eine *Reduktion* ρ wie folgt: Aus $w \in A^*$ streichen wir, von links beginnend, alle Teilfolgen der Form mm^{-1} oder $m^{-1}m$, und wiederholen dies, bis keine derartige Teilfolge mehr auftritt. Die Menge $F(M)$ dieser *reduzierten Worte* $\rho(w)$ versehen wir mit der folgenden Verknüpfung:

$$*\colon F(M) \times F(M) \to F(M)\,,\ (w, w') \mapsto \rho(ww').$$

- Das Paar $(F(M), *)$ ist eine Gruppe, und die Einbettung

$$M \hookrightarrow F(M)\,,\ m \mapsto m$$

  hat die gewünschte Universaleigenschaft, denn eine Abbildung f von M in eine Gruppe H läßt sich offenbar mittels folgender Abbildung γ von $F(M)$ nach H faktorisieren:

$$\gamma\colon F(M) \to H\,,\ \underbrace{m_{i_0}^{b_0} \cdots m_{i_{k-1}}^{b_{k-1}}}_{oBdA\colon\ b_i \in \{-1,+1\}} \mapsto f(m_{i_0})^{b_0} \cdots f(m_{i_{k-1}})^{b_{k-1}}.$$

  Außerdem ist γ offensichtlich Homomorphismus und eindeutig bestimmt, da $F(M)$ von M erzeugt wird.

- Die Isomorphie folgt nach 5.1.3.

□

Wegen der Isomorphie zweier von M frei erzeugter Gruppen können wir $F(M)$ auch als *die* von M frei erzeugte Gruppe bezeichnen. Die Elemente $m \in M$ heißen *freie Erzeugende* dieser Gruppe. Das Attribut *frei* bedeutet dabei insbesondere, daß zwischen den Elementen aus M keine nichttrivialen *Relationen* bestehen, das sind Gleichungen der Form

$$\underbrace{m_{i_0}^{b_0} \cdots m_{i_{k-1}}^{b_{k-1}}}_{reduziert\ !} = \epsilon.$$

Weil M ganz $F(M)$ erzeugt, heißt $F(M)$ auch die freie Gruppe *über* M.

6.1.3 Beispiele Für die freie Gruppe über einem einzigen Element gilt offenbar

$$F(\{m\}) \simeq \mathbb{Z}\,,\ m \mapsto 1,$$

während alle anderen freien Gruppen nicht kommutativ sind:

$$1 < |M| \Longrightarrow F(M) \text{ ist nicht abelsch.}$$

◇

Aus der Existenz und Isomorphie zwischen den freien Gruppen über M ergibt sich noch

6.1.4 Folgerung *Für Gruppen und freie Gruppen gilt:*

- *Jede Gruppe G mit Erzeugendensystem M ist auf eindeutige Weise epimorphes Bild von $F(M)$.*
- *Jede Gruppe G ist homomorphes Bild einer freien Gruppe und damit isomorph zu einer Faktorgruppe einer freien Gruppe.*

□

6.1.5 Definition (definierender Kern, definierende Relationen) Wird G von M erzeugt und ist γ der (eindeutig bestimmte) Epimorphismus von $F(M)$ auf G, dann heißt der Kern

$$K_M := \mathrm{Kern}(\gamma)$$

der definierende Kern von G bzgl. M. Ist E *Normalteilererzeugendensystem* von K_M (d. h. K_M ist der kleinste Normalteiler in $F(M)$, der E enthält), dann heißt das System der Gleichungen

$$\gamma(e) = 1_G,\ e \in E,$$

ein System *definierender Relationen* von G bzgl. M. Gibt es endliche E mit dieser Eigenschaft, dann heißt G *endlich präsentierbar*, und

$$\langle E \mid \gamma(e) = 1, e \in E\rangle = G$$

heißt eine *endliche Präsentation* von G. •

6.1.6 Beispiel Die zyklische Gruppe der Ordnung 5 kann offenbar wie folgt präsentiert werden:

$$G := \langle a \mid a^5 = 1\rangle.$$

◇

Es stellt sich jetzt natürlich die Frage, wie man eine Präsentation einer vorgegebenen Gruppe berechnen kann. Sei deshalb G eine Gruppe mit einem Erzeugendensystem $M = \{m_0, \ldots, m_{n-1}\}$, sowie Relationen

$$R_0(m_0, \ldots, m_{n-1}) = 1_G, \ldots, R_{s-1}(m_0, \ldots, m_{n-1}) = 1_G.$$

Wir fragen, ob dies schon eine Präsentation von G ist, d. h. ob folgendes gilt:

$$G' := \langle M \mid R_0 = \ldots = R_{s-1} = 1\rangle \simeq G.$$

Um dies zu entscheiden, kann nun im endlichen Fall wie folgt argumentiert werden:

- Nach 6.1.4 ist G homomorphes Bild von G', es gilt also insbesondere $|G'| \geq |G|$.

- Die Isomorphie ist somit bewiesen, wenn $|G'| = |G|$ verifiziert werden kann. Dazu genügt es, eine Untergruppe $U' \leq G'$ zu finden, für die $|U'|$ und $|G'/U'|$ ermittelt werden können.

6.1.7 Beispiel Betrachten wir als Beispiel den eingangs aufgeführten Fall der Präsentation

$$G := \langle x, y \mid x^2 = y^2 = (xy)^3 = 1 \rangle.$$

Wir wollen zeigen, daß dies tatsächlich eine Präsentation der symmetrischen Gruppe S_3 ist. Dazu schließen wir wie folgt:

- S_3 ist jedenfalls homomorphes Bild von G, also ist 3! ein Teiler von $|G|$.
- Die von y erzeugte Untergruppe U hat die Ordnung 2, zum Nachweis der vermuteten Isomorphie genügt also allein die Verifizierung von $|G/U| = 3$.
- Zur Berechnung des gewünschten Index beachten wir, daß U, xU und yxU Linksnebenklassen sind (ob sie verschieden sind brauchen wir hier nicht einmal zu wissen!). Bei Linksmultiplikation mit Erzeugenden ergeben sich daraus *keine weiteren* Linksnebenklassen, der Index ist also tatsächlich ≤ 3.

Zusammenfassend haben wir daraus die folgende Präsentation ermittelt:

$$S_3 \simeq \langle x, y \mid x^2 = y^2 = (xy)^3 = 1 \rangle.$$

◇

6.1.8 Definition (Diedergruppen) Die Gruppen

$$D_m := \langle x, y \mid x^2 = y^2 = (xy)^m = 1 \rangle$$

heißen *Diedergruppen.* •

6.1.9 Hilfssatz *D_m hat die Ordnung $2m$ und enthält mit $\langle xy \rangle$ einen Normalteiler der Ordnung m.*

Beweis: Sei $z := xy$. D_m wird erzeugt von $\{x, z\}$, und die Gleichungen

$$yx = y^{-1}x^{-1} = z^{-1}$$

zeigen, daß sich jedes Element von D_m in der Form $x^r z^s$ schreiben läßt, mit $0 \leq r \leq 1$ und $0 \leq s \leq m-1$. Es gilt demnach $|D_m| = 2m$. Die Normalteilereigenschaft von $\langle z \rangle$ ergibt sich aus $xzx = yzy$.

□

6.1.10 Definition (semidirektes Produkt) Sind G und H Gruppen und ist $h \mapsto \bar{h}$ ein Homomorphismus von H in die Gruppe $Aut(G)$ der Automorphismen von G, dann wird $G \times H$ zu einer Gruppe durch die Setzung

$$(g, h)(g', h') := (g \cdot \bar{h}(g'), hh').$$

Diese Gruppe heißt das *semidirekte Produkt von G mit H bzgl. $h \mapsto \bar{h}$.* •

Der Beweis von 6.1.9 zeigt, daß die Diedergruppe semidirektes Produkt einer zyklischen Gruppe der Ordnung m mit einer zyklischen Gruppe der Ordnung 2 ist.

Ü 6.1.1 Zeigen Sie, daß die oben definierte Abbildung $*$ auf $F(M) \times F(M)$ wohldefiniert ist.

6.2 Gruppenoperationen, der Satz von Sylow

Erinnern wir uns jetzt an die im Paragraphen 2 bereits eingeführten *Gruppenoperationen*

$$G \times M \to M\colon (g,m) \mapsto gm, \text{ mit } g(g'm) = (gg')m, \text{ und } 1m = m.$$

Wir schrieben dafür abkürzend auch ${}_GM$, da G von *links* auf M operiert, und wir hatten festgestellt, daß eine solche Operation wichtige Teilstrukturen auf M und auf G definiert:

- Zu jedem $m \in M$ gehört seine *Bahn*

  $$G(m) := \{gm \mid g \in G\}.$$

  Je zwei Bahnen $G(m)$ und $G(m')$ sind entweder gleich oder disjunkt. Eine Transversale T der Menge

  $$G \setminus\setminus M := \{G(m) \mid m \in M\}$$

  aller Bahnen liefert also eine Partition von M:

  $$M = \dot{\bigcup}_{t \in T} G(t).$$

  Umgekehrt kann man zu jeder Partition $\dot{\cup}_{i\in I} M_i$ von M leicht eine Gruppe konstruieren, die als Bahnen die Teile der Partition hat:

  $$\bigoplus_{i\in I} S_{M_i} := \{\pi \in S_M \mid \forall\, i \in I\colon \pi M_i = M_i\}$$

  hat als Bahnenmenge

  $$\bigoplus_i S_{M_i} \setminus\setminus M = \{M_i \mid i \in I\}.$$

- Andererseits gehört zu $m \in M$ sein *Stabilisator*

  $$G_m := \{g \in G \mid gm = m\},$$

  eine Untergruppe von G. Die Abbildung

  $$\varphi\colon G(m) \to G/G_m\,,\ gm \mapsto gG_m$$

  ist eine Bijektion zwischen der Bahn $G(m)$ und der Menge

  $$G/G_m := \{gG_m \mid g \in G\}$$

  der Linksnebenklassen des Stabilisators von m. φ ist sogar ein *G–Isomorphismus* ist, d.h. eine mit der Operation vertauschbare Bijektion, gilt doch

  $$g'\varphi(gm) = \varphi(g'(gm)).$$

Wir wollen Operationen ${}_GM$ und ${}_GN$ als *ähnlich* bezeichnen, wenn solche G–Isomorphismen zwischen M und N existieren, und wir wollen diese Situation so abkürzen: ${}_GM \simeq {}_GN$. Es gilt also insbesondere

$$6.2.1 \qquad {}_G(G(m)) \simeq {}_G(G/G_m).$$

- Zu jedem $g \in G$ gehört die Menge seiner *Fixpunkte*:

$$M_g := \{m \in M \mid gm = m\}.$$

Man kann dies natürlich auf Teilmengen $\subseteq G$ verallgemeinern:

$$M_K := \{m \in M \mid \forall\, g \in K\colon gm = m\}.$$

Die Elemente m von M_G heißen auch die *Invarianten* von G in M.

Viele Strukturen aus Mathematik und Naturwissenschaften lassen sich als Bahnen, Stabilisatoren oder Fixpunktmengen definieren und werden dadurch einer Untersuchung mit Hilfe der im folgenden beschriebenen Methoden zugänglich.

6.2.2 Anwendungen (bilaterale Klassen) Ist wieder G eine Gruppe, dann operiert jede Untergruppe U von $G \times G$ in folgender Weise kanonisch auf G:

$$U \times G \to G\,,\ ((u,u'),g) \mapsto ugu'^{-1}.$$

Die Bahnen dieser Operation heißen *bilaterale Klassen* von U auf G. Beispiele sind:

- Die Konjugiertenklassen von Elementen $g \in G$, sind die bilateralen Klassen der *Diagonalen*

$$U := \Delta(G \times G) := \{(g,g) \mid g \in G\}.$$

Wir bezeichnen sie so:

$$C^G(g') := \Delta(G \times G)(g) = \{gg'g^{-1} \mid g \in G\}.$$

Für die entsprechenden Stabilisatoren schreiben wir:

$$C_G(g') := \Delta(G \times G)_g = \{g \in G \mid gg'g^{-1} = g'\}.$$

Sie heißen auch *Zentralisatoren*.

- Die *Links-* bzw. *Rechtsnebenklassen* von Untergruppen $H \leq G$ sind die Bahnen von $U := 1 \times H$ bzw. $U := H \times 1$:

$$(1 \times H)(g) = gH \text{ bzw. } (H \times 1)(g) = Hg.$$

- Die (H,K)-*Doppelnebenklassen* in G sind die Bahnen der Untergruppe $U := H \times K$ von $G \times G$, mit $H, K \leq G$:

$$(H \times K)(g) = HgK = \{hgk \mid h \in H, k \in K\}.$$

$\diamond$

Als konkretes Beispiel wollen wir die Konjugiertenklassen von Elementen π der symmetrischen Gruppe S_n beschreiben. Dazu erinnern wir uns an die *Zyklenschreibweise* für Permutationen, π kann als Produkt disjunkter zyklischer Faktoren geschrieben werden:

$$\pi = \prod_{\nu=0}^{z(\pi)-1} (j_\nu, \pi j_\nu, \ldots, \pi^{l_\nu - 1} j_\nu).$$

Wenn wir mit ρ konjugieren, erhalten wir

$$\rho\pi\rho^{-1} = \prod_{\nu=0}^{z(\pi)-1} (\rho j_\nu, \rho\pi j_\nu, \ldots, \rho\pi^{l_\nu - 1} j_\nu),$$

beim Konjugieren bleiben also die Längen der zyklischen Faktoren erhalten. Umgekehrt sind Permutationen mit zyklischen Faktoren derselben Längen zueinander konjugiert: Für

$$\pi = \prod_{\nu=0}^{z(\pi)-1} (j_\nu, \pi j_\nu, \ldots, \pi^{l_\nu - 1} j_\nu)$$

und

$$\sigma = \prod_{\nu=0}^{z(\pi)-1} (k_\nu, \pi k_\nu, \ldots, \pi^{l_\nu - 1} k_\nu)$$

gilt mit

$$\rho = \prod_{\nu=0}^{z(\pi)-1} \begin{pmatrix} j_\nu, \pi j_\nu, \ldots, \pi^{l_\nu - 1} j_\nu \\ k_\nu, \pi k_\nu, \ldots, \pi^{l_\nu - 1} k_\nu \end{pmatrix}$$

die Gleichung

$$\sigma = \rho\pi\rho^{-1}.$$

6.2.3 Folgerung *Zwei Permutationen aus $\pi, \sigma \in S_n$ sind genau dann konjugiert, wenn die schwach monoton fallende Folge*

$$\alpha(\pi) := (\alpha_0(\pi), \alpha_1(\pi), \ldots)$$

der Längen der zyklischen Faktoren von π gleich der entsprechenden Folge $\alpha(\sigma)$ ist.

Solche schwach monoton fallenden Folgen $\alpha = (\alpha_0, \alpha_1, \ldots)$ natürlicher Zahlen mit $\sum \alpha_i = n$ heißen *Partitionen* der Zahl n, wir kürzen dies wie folgt ab:

$$\alpha \vdash n.$$

Die Konjugiertenklasse der Elemente mit Zykellängenpartition α bezeichnen wir wie folgt:

$$C^\alpha := \{\pi \in S_n \mid \alpha(\pi) = \alpha\}.$$

Sind sowohl G als auch M endlich, dann nennen wir ${}_GM$ eine endliche Operation. Für diese zeigt 6.2.1, daß die Länge der Bahn eines Gruppenelementes dem Index seines Stabilisators gleicht:

6.2.4 $$|G(m)| = \frac{|G|}{|G_m|}.$$

Beispielsweise gilt, für $\pi \in C^\alpha$,

$$|C^\alpha| = \frac{n!}{|C_{S_n}(\pi)|},$$

und man kann sich leicht überlegen, wie man die Ordnung $|C_{S_n}(\pi)|$ dieses Zentralisators erhält: Bezeichnet a_i die Anzahl der i-Zyklen von π, dann heißt $a(\pi) := (a_1(\pi), \ldots, a_n(\pi))$ der *Zykeltyp* von π. Allgemeiner heißen n-Tupel $a = (a_1, \ldots, a_n)$ mit $a_i \in \mathbb{N}$ und $\sum_i i \cdot a_i = n$ Zykeltypen von n, und man kann das wie folgt abkürzend bezeichnen:

$$a \vdash n.$$

Der Zykeltyp $a(\pi)$ der Permutationen mit Zykelpartition $\alpha(\pi)$ charakterisiert also ebenfalls die Konjugiertenklasse

$$C^a = C^\alpha = \{\pi \mid a(\pi) = a\}.$$

Eine Permutation $\rho \in S_n$ liegt genau dann im Zentralisator von π, wenn sie jeden i-Zyklus von π wieder in einen i-Zyklus von π transformiert. Die Anzahl solcher ρ ist

$$|C_{S_n}(\pi)| = \prod_{i=1}^{n} i^{a_i(\pi)} a_i(\pi)!.$$

Insgesamt gilt also

$$|C^a| = \frac{n!}{\prod_{i=1}^n i^{a_i(\pi)} a_i(\pi)!}.$$

Die Gleichung 6.2.4 ist eine sehr einschneidende Bedingung an die Bahnlängen, wie die folgende Anwendung zeigt, H. Wielandts berühmter Beweis (Archiv d. Math. 1959) für die Existenz von Untergruppen von Primzahlpotenzordnung p^r, wenn p^r in $|G|$ aufgeht.

6.2.5 Anwendung(der Satz von Sylow) Wir betrachten die natürliche Operation von G auf der Menge ihrer Teilmengen K der Ordnung p^r:

$$G \times \binom{G}{p^r} \to \binom{G}{p^r},\ (g, K) \mapsto gK.$$

Ist jetzt $|G| = p^r p^s q$, mit zu p teilerfremdem q, dann sieht man leicht, daß die exakte Potenz von p, die in der Anzahl der p^r–Teilmengen von G aufgeht, gerade p^s ist:

$$\left|\binom{G}{p^r}\right| = \frac{|G| \cdot (|G| - 1) \cdots (|G| - (p^r - 1))}{p^r \cdot 1 \cdots (p^r - 1)},$$

und alle im Nenner stehenden Potenzen von p können gekürzt werden. Es muß also eine Bahn $G(K)$ geben, deren Länge nicht durch p^{s+1} teilbar ist. Der Stabilisator G_K ist dann eine Untergruppe der Ordnung p^r, wie man leicht durch Abschätzung der Ordnung dieses Stabilisators nach oben und unten beweist:

i) Aus 6.2.4 folgt
$$|G(K)| = \frac{|G|}{|G_K|}.$$
Diese Zahl ist nicht durch p^{s+1} teilbar, in $|G_K|$ steckt also mindestens die p-Potenz p^r als Faktor, d. h. $|G_K| \geq p^r$.

ii) Ist $\kappa \in K$, dann liegt $G_K \cdot \kappa$ ganz in K. Dieses Komplexprodukt besteht aber aus genau $|G_K|$ verschiedenen Elementen, es muß also $|G_K| \leq p^r$ gelten.

□

Es gibt also, unter anderem, Untergruppen von G, deren Ordnung der *maximalen* p-Potenz gleicht, die in $|G|$ aufgeht. Diese heißen *p-Sylowuntergruppen.* Insgesamt haben wir damit den folgenden sehr wichtigen Existenzsatz bewiesen:

6.2.6 Der Satz von Sylow, Teil I: *Ist G eine endliche Gruppe, p eine Primzahl, dann gibt es zu jeder p-Potenz p^r, die in $|G|$ aufgeht, eine Untergruppe $U \leq G$ von dieser Ordnung.*

Es gibt weitere Teile dieses Satzes, die ebenfalls mit Hilfe von Gruppenoperationen bewiesen werden können, insbesondere mit Hilfe von Doppelnebenklassen.

6.2.7 Hilfssatz *Sind H und K Untergruppen einer endlichen Gruppe G, dann gilt für die Bahnen von $H \times K$ auf G, also für die (H,K)-Doppelnebenklassen HgK auf G :*

- $(H \times K)_g \simeq H \cap gKg^{-1}$,
- $|HgK| = |H||K|/|H \cap gKg^{-1}|$,
- *Für jede Transversale T der Doppelnebenklassenmenge $H\backslash G/K$ ist*
$$|G| = \sum_{t \in T} |HtK| = \sum_{t \in T} |H||K|/|H \cap tKt^{-1}|.$$

Beweis: Der Stabilisator von g in $H \times K$ ist

$$(H \times K)_g = \{(h,k) \in H \times K \mid h = gkg^{-1}\}$$
$$= \{(gkg^{-1}, k) \mid k \in K, gkg^{-1} \in H\} \simeq H \cap gKg^{-1}.$$

Aus dem hiermit bewiesenen ersten Teil der Behauptung folgen die beiden anderen Punkte direkt mit dem Fundamentallemma.

□

Damit können wir den zweiten Teil des Satzes von Sylow über $p-$Untergruppen, d.h. über Untergruppen von $p-$Potenz-Ordnung, beweisen

6.2.8 Der Satz von Sylow, Teil II: *Jede $p-$Untergruppe einer endlichen Gruppe liegt in einer $p-$Sylowuntergruppe von G, und je zwei $p-$Sylowuntergruppen von G sind zueinander konjugiert.*

Beweis: Sei H eine $p-$Untergruppe von G, K eine $p-$Sylowuntergruppe. Es gilt dann, nach dem Hilfssatz:

$$|G|/|K| = \sum_{t \in T} |H|/|H \cap tKt^{-1}|.$$

Weil die linke Seite dieser Gleichung nicht durch p teilbar ist und alle Summanden rechts Potenzen von p, muß mindestens ein Summand gleich $p^0 = 1$ sein und damit, für mindestens ein t, $H \subseteq tKt^{-1}$ gelten. Mit K ist natürlich auch tKt^{-1} eine $p-$Sylowuntergruppe. Das beweist zunächst den ersten Teil der Behauptung. Der zweite folgt aber auch, denn wenn sowohl H als auch K (verschiedene) $p-$Sylowuntergruppen sind, gilt für ein solches t ja aus Ordnungsgründen $H = tKt^{-1}$.

□

Schließlich ist es noch nützlich zu wissen, daß die Gesamtzahl der Untergruppen der Ordnung p^r kongruent 1 modulo p ist. Hierzu analysiert man die oben betrachtete Operation von G auf ihren p^r-Teilmengen noch etwas genauer. Wir hatten gesehen, daß der Stabilisator jeden Elements einer Bahn, deren Länge nicht durch p^{s+1} teilbar ist, die Ordnung p^r besitzt. Die Umkehrung gilt natürlich auch, genau die Elemente solcher Bahnen haben Stabilisatoren dieser Ordnung, die Länge dieser Bahnen ist natürlich $p^s \cdot q$.

6.2.9 Hilfssatz *Die Untergruppen der Ordnung p^r bilden eine Transversale der Bahnen der Länge $p^s \cdot q$.*

Beweis: Jede dieser Bahnen $G(M)$ enthält eine Untergruppe U der Ordnung p^r. Ist nämlich $m \in M$, dann gilt

$$U := m^{-1} \cdot G_M \cdot m = m^{-1} \cdot M \in G(M).$$

Dies ist das einzige Element dieser Bahn, das Untergruppe ist, denn weil U Stabilisator eines Elements dieser Bahn ist, besteht diese Bahn aus den Linksnebenklassen von U, und von diesen ist ja genau eine Untergruppe.

□

6.2.10 Der Satz von Sylow, Teil III: *Die Anzahl der Untergruppen der Ordnung p^r in G ist kongruent 1 modulo p.*

Beweis: Diese Gruppen bilden, nach dem letzten Hilfssatz, eine Transversale der Menge Bahnen von G auf den p^r-Teilmengen, deren Länge nicht durch p^{s+1} teilbar, oder, äquivalent dazu, gleich $p^s \cdot q$ ist. Es gibt also, wenn wir mit n die Anzahl solcher Untergruppen bezeichnen, eine natürliche Zahl t mit

$$\left| \binom{G}{p^r} \right| = n \cdot p^s \cdot q + t \cdot p^{s+1}.$$

Ist G eine zyklische Gruppe der Ordnung $p^{r+s} \cdot q$, dann gilt eine entsprechende Gleichung, mit einem $\widetilde{t}$ und, vor allem, mit $n = 1$, denn in zyklischen Gruppen gibt es zu jedem Teiler der Gruppenordnung genau eine Untergruppe von diese Ordnung. Es gilt also auch

$$\left|\binom{G}{p^r}\right| = p^s \cdot q + \widetilde{t} \cdot p^{s+1}.$$

Vergleichen wir die beiden rechten Seiten, so erhalten wir, nach Division durch p^s :

$$n \cdot q + t \cdot p = q + \widetilde{t} \cdot p,$$

woraus, wegen $p \nmid q$, die behauptete Kongruenz $n \equiv 1$ modulo p folgt.

□

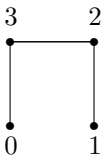
6.2.11 Folgerung *Insbesondere gilt also für die Anzahl der $p-$Sylowuntergruppen jeder endlichen Gruppe:*

- *sie ist kongruent 1 modulo p,*
- *und sie teilt $|G|$.*

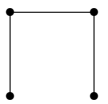
□

6.3 Symmetrieklassen von Abbildungen

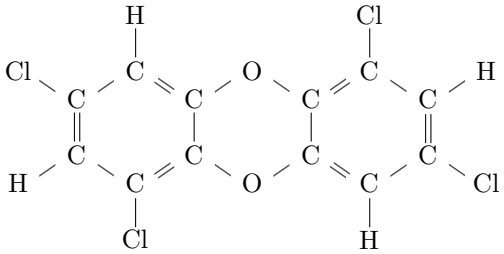
Wir kommen jetzt zu Anwendungen von Gruppenoperationen *außerhalbder Gruppentheorie.* Hier ist insbesondere die Behandlung *unnumerierter Strukturen* hervorzuheben, das sind Strukturen, die als Äquivalenzklassen *numerierter Strukturen* definiert sind. Ein besonders einfaches und einleuchtendes Beispiel bilden die *Graphen.* Hier ist zunächst ein *numerierter Graph:*



und hier ein *unnumerierter Graph:*



Unnumerierte Graphen sind von gr0ßer Bedeutung, denn sie können als *Wechselwirkungsmodelle* interpretiert werden. Beispiele aus den Naturwissenschaften sind die chemischen Strukturformeln. Hier ist die Situation allerdings noch etwas komplizierter, weil es sich um *kolorierte* Graphen handelt, die Knoten sind noch mit Atomnamen $C, H, O, \ldots$ koloriert. Hier ist ein Beispiel:



eines der 22 *Permutationsisomere* des Dioxin. Es stellt sich jetzt natürlich die Frage, wie man diese Zahl 22 berechnen oder, noch besser, diese konstruieren kann. Ein interessanter und vielseitig verwendbarer Ansatz zur Lösung solcher Probleme soll jetzt diskutiert werden.

Wir hatten bereits erwähnt, daß jede Äquivalenzrelation mit Hilfe einer Gruppenoperation modelliert werden kann, welche die Klassen der Relation als Bahnen hat. Wir werden also Gruppenoperationen eingehender betrachten und anwenden. Im folgenden seien alle betrachteten Operationen endlich. Der angekündigte allgemeine Ansatz wird in der folgenden Definition beschrieben.

6.3.1 Definition (Symmetrieklassen von Abbildungen) Aus gegebenen Operationen ${}_GX$ und ${}_HY$ erhält man auf natürliche Weise die folgenden Operationen von $G, H, H \times G, H \wr_X G$ auf $Y^X := \{f\colon X \to Y\}$:

$$G \times Y^X \to Y^X\,,\ (g,f) \mapsto f \circ g^{-1},$$

$$H \times Y^X \to Y^X\,,\ (h,f) \mapsto h \circ f,$$

$$(H \times G) \times Y^X \to Y^X\,,\ ((h,g),f) \mapsto h \circ f \circ g^{-1}.$$

Die Gruppe $H \wr_X G$, das *Kranzprodukt* von H mit G, hat als Grundmenge $H^X \times G$, besteht also aus den Paaren $(\varphi; g)$ mit $\varphi\colon X \to H$ und $g \in G$. Die Verknüpfung ist

$$(\varphi; g)(\psi; g') := (\varphi\psi_g; gg'),$$

wobei $\varphi\psi_g(x) := \varphi(x) \cdot \psi(g^{-1}x)$. Diese Gruppe operiert auf Y^X wie folgt:

$$(H \wr_X G) \times Y^X \to Y^X\,,\ ((\varphi; g), f) \mapsto \widetilde{f},\ \text{mit } \widetilde{f}(x) := \varphi(x) f(g^{-1}x).$$

Die Bahnen dieser Operationen heißen *Symmetrieklassen von Abbildungen.* •

6.3.2 Bemerkung *Man sieht leicht, daß das Kranzprodukt $H \wr_X G$ Untergruppen enthält, die isomorph zu $G, H, H \times G$ sind, so daß die zunächst definierten Operationen von $G, H, H \times G$ aus der Operation von $H \wr_X G$ durch Einschränkung auf diese Untergruppen entstehen:*

$$\{(\varphi; g) \mid \forall\, x \in X\colon \varphi(x) = 1_H, g \in G\} \simeq G,$$

$$\{(\varphi; 1_G) \mid \varphi \textit{ konstant}\} \simeq H,$$

$$\{(\varphi; g) \mid \varphi \textit{ konstant, } g \in G\} \simeq H \times G.$$

□

Viele unnumerierte Strukturen können als Symmetrieklassen von Abbildungen beschrieben werden, hier einige einfache Fälle:

6.3.3 Beispiele (Graphen) Zur Beschreibung von Graphen kann man wie folgt vorgehen:

i) Ist P eine Menge von Punkten, dann bezeichnet

$$X := \binom{P}{2} = \{\{x, y\} \mid x, y \in P, x \neq y\}$$

die Menge der Punktepaare. Auf dieser Menge operiert die symmetrische Gruppe $G := S_P$ wie folgt:

$$S_P \times \binom{P}{2} \to \binom{P}{2}, (\pi, \{x, y\}) \mapsto \{\pi x, \pi y\}.$$

Diese Operation der symmetrischen Gruppe ist offenbar die *Umnumerierung* der Punkte!

ii) Betrachten wir die Abbildungen der Menge der Punktepaare in die Menge $Y := 2 = \{0, 1\}$, also

$$Y^X := 2^{\binom{P}{2}} = \left\{ f \colon \binom{P}{2} \to \{0, 1\} \right\}.$$

Sie kann mit der Menge aller *numerierten Graphen* auf P identifiziert werden, wenn $f(\{x, y\}) = 1$ interpretiert wird als Existenz einer Kante zwichen den Punkten x und y. Genauer handelt es sich dabei um schlichte Graphen, d.h. es kommen keine Mehrfachkanten oder Schleifen vor.

iii) Die Operation von S_P faßt die numerierten Graphen zu einer Bahn zusammen, die auseinander durch Umnumerierung hervorgehen. Diese Bahnen werden also durch einen Graphen repräsentiert, den man aus irgendeinem ihrer Elemente durch Wegwischen der Numerierung erhält. Sie "sind" also die unnumerierten Graphen mit $|P|$ Punkten. Die Menge all dieser Graphen kann demnach mit der Bahnenmenge

$$S_P \backslash\backslash 2^{\binom{P}{2}}$$

identifiziert werden.

iv) Will man Mehrfachkanten zulassen, etwa bis zu einer maximalen Vielfachheit v, dann braucht man den Bildbereich nur entsprechend zu erweitern:

$$S_P \backslash\backslash (v+1)^{\binom{P}{2}}$$

sind dann die unnumerierten Graphen mit dieser Eigenschaft. Will man beliebige Vielfachheiten zulassen, dann geht es um

$$S_P \backslash\backslash \mathbb{N}^{\binom{P}{2}}.$$

v) Um *gerichtete Graphen* zu modellieren, braucht man nur die Menge der Punktepaare durch die Menge der geordneten Paare aus verschiedenen Punkten zu ersetzen, nimmt also einfach P^2 und läßt die Diagonale weg:

$$X := P^2 - \Delta(P^2) = \{(x, y) \mid x, y \in P, x \neq y\}.$$

Die Menge der gerichteten Graphen (ohne Schleifen oder Parallelkanten) mit $|P|$ Punkten kann demnach mit

$$S_P \backslash\backslash 2^{P^2 - \Delta(P^2)}$$

identifiziert werden

Diese Bahnenmengen sind sämtlich Bahnen von Operationen der Form ${}_G(Y^X)$.

vi) Bahnenmenge einer Operation der Form ${}_{H \times G}(Y^X)$ ist

$$S_2 \times S_P \backslash\backslash 2^{\binom{P}{2}}.$$

Hier sind unnumerierte Graphen mit ihrem Komplementen in einer Bahn zusammengefaßt.

vii) Faßt man dies zusammen, so ergibt sich beispielsweise die folgenden Formel für die Anzahl unnumerierter schlichter selbstkomplementärer Graphen:

$$2 \cdot \left| S_2 \times S_P \wr 2^{\binom{P}{2}} \right| - \left| S_P \wr 2^{\binom{P}{2}} \right|.$$

$\diamond$

Eine Operation von der Form ${}_{H\wr_X G}(Y^X)$ liefert eine wichtige Klassifizierung fehlerkorrigierender linearer Codes:

6.3.4 Beispiel (Isometrieklassen linearer Codes)

i) Lineare Codes C sind endliche Vektorräume, etwa $C \leq GF(q)^n$. Auf $GF(q)^n$ ist die *Hammingmetrik* definiert durch

$$d(u,v) := |\{i \mid u_i \neq v_i\}|,$$

und die *Minimaldistanz* von C ist definiert durch

$$d(C) := \min\{d(c,c') \mid c,c' \in C, c \neq c'\}.$$

Die Grundidee zur Verwendung linearer Codes ist die folgende: Sendet man einen Codevektor c über einen störanfälligen Kanal, und ist u der empfangene Vektor, dann gibt es, falls $d(u,c) \leq \lfloor d(C)/2 \rfloor$, genau einen zu u nächstgelegenen Codevektor, und dieser ist c. Dekodiert man einen empfangenen Vektor u also in einen der nächstgelegenen Codevektoren, dann werden also alle Fehler korrigiert, vorausgesetzt es sind weniger als $\lfloor d(C)/2 \rfloor$.

ii) Solche Codes C, C' sind demnach gleichwertig, wenn sie *isometrisch* sind, d.h. wenn es eine Isometrie zwichen ihnen gibt, eine reguläre lineare Abbildung $A \in GL(GF(q)^n)$ mit $AC = C'$ und

$$d(u,v) = d(Au, Av),$$

für alle $u, v \in GF(q)^n$.

iii) $A \in GL(GF(q)^n)$ ist offenbar genau dann eine Isometrie, wenn sie jeden Einheitsvektor e_k in ein Vielfaches eines Einheitsvektors überführt, also wenn es eine Permutation $\pi \in S_n$ und von Null verschiedene Elemente κ_k des Grundkörper gibt mit

$$Ae_k = \kappa_k e_{\pi^{-1}k}.$$

A ist demnach von der Form

$$(\varphi; g) = (\kappa_0, \ldots, \kappa_{n-1}; \pi) \in GF(q)^* \wr_n S_n.$$

Die Matrix, die A beschreibt, ist eine Matrix, die in jeder Zeile und Spalte genau ein Element aus der multiplikativen Gruppe des Grundkörpers enthält.

iv) Die Gruppe aller Isometrien auf $Y^X := GF(q)^n$ ist also

$$H \wr_X G := GF(q)^* \wr_n S_n,$$

und die *Isometrieklassen linearer Codes der Länge n* sind die Bahnen dieses Kranzprodukts auf der Menge der Unterräume. ◇

Die Beschreibung von Strukturen, die als Äquivalenzklassen auf endlichen Mengen definiert sind, als Bahnen endlicher Gruppen auf endlichen Mengen eröffnet den Zugang zu deren Untersuchung, insbesondere zu ihrer Abzählung und Konstruktion. Dies motiviert zur detaillierten Untersuchung der Abzählung von Bahnen und — was natürlich erheblich schwieriger ist — der Konstruktion von Transversalen.
Erinnern wir uns zunächst an das Lemma von Cauchy-Frobenius zur Bestimmung der Anzahl der Bahnen einer endlichen Gruppe G auf einer endlichen Menge M :

$$|G \backslash\backslash M| = \frac{1}{|G|} \sum_{g \in G} |M_g|.$$

Bei Anwendungen dieses Lemmas sollte man beachten, daß die Summation über die ganze Gruppe wesentlich vereinfacht werden kann, weil die Anzahl der Fixpunkte konstant auf den Konjugiertenklassen ist:

6.3.5 $$|M_g| = |M_{g'gg'^{-1}}|,$$

denn $m \mapsto g'm$ ist eine Bijektion zwischen M_g und $M_{g'gg'^{-1}}$. Kurz: Die Abbildung

$$\chi\colon g \mapsto |M_g|,$$

der *Charakter* der Operation ${}_G M$, ist eine *Klassenfunktion,* d.h. konstant auf den Konjugiertenklassen der Elemente von G. Man kann sich demnach bei Anwendung des Lemmas von Cauchy-Frobenius auf die Summation über die Elemente einer Transversalen T der Konjugiertenklassen beschränken,

6.3.6 $$|G \backslash\backslash M| = \frac{1}{|G|} \sum_{t \in T} |C^G(t)| \cdot |M_t| = \sum_{t \in T} \frac{|M_t|}{|C_G(t)|} \ .$$

Das Lemma von Cauchy-Frobenius soll jetzt auf die Abzählung von Symmetrieklassen angewandt werden! Wir berechnen dazu die Anzahl der Fixpunkte eines $(\varphi; g) \in H \wr_X G$ auf Y^X. Daraus ergibt sich die Anzahl der $H \wr_X G-$Bahnen, die anderen Anzahlen ergeben sich daraus durch Einschränkung auf entsprechende Untergruppen.

Ist

$$\overline{g} = \prod_{\nu \in z(\overline{g})} (j_\nu \dots g^{l_\nu - 1} j_\nu)$$

die Standardzykelschreibweise von $\overline{g} \in S_X$, dann ordnen wir dem ν-ten zyklischen Faktor von $\overline{g}$ mit Hilfe von $\varphi\colon X \to H$ das folgende Element von H zu:

6.3.7 $$h_\nu(\varphi; g) := \varphi(j_\nu)\varphi(g^{-1}j_\nu)\cdots\varphi(g^{-l_\nu+1}j_\nu) = \varphi\cdots\varphi_{g^{l_\nu-1}}(j_\nu),$$

das *ν-te Zykelprodukt von* $(\varphi; g)$.

6.3.8 Hilfssatz *$f \in Y^X$ ist genau dann ein Fixpunkt von $(\varphi; g) \in H \wr_X G$, wenn die folgenden Bedingungen erfüllt sind:*

- *Jedes $f(j_\nu)$ ist Fixpunkt des Zykelprodukts $h_\nu(\varphi; g)$:*
$$f(j_\nu) \in Y_{h_\nu(\varphi;g)}.$$
- *Die anderen Werte von f ergeben sich aus den Werten $f(j_\nu)$ gemäß den folgenden Gleichungen:*
$$f(j_\nu) = \varphi(j_\nu)f(g^{-1}j_\nu) = \varphi(j_\nu)\varphi(g^{-1}j_\nu)f(g^{-2}j_\nu) = \dots\ .$$

Beweis: 6.3.7 besagt, daß f genau dann Fixpunkt von $(\varphi; g)$ ist, wenn die Werte $f(x)$ den folgenden Gleichungen genügen:

$$f(x) = \varphi(x)f(g^{-1}x) = \psi(x)\varphi(g^{-1}x)f(g^{-2}x)\dots$$
$$\dots = \varphi(x)\varphi(g^{-1}x)\dots\varphi(g^{-l+1}x)f(x),$$

wenn l die Länge des zyklischen Faktors von $\bar{g}$ bezeichnet, der den Punkt $x \in X$ enthält. Es muss also insbesondere folgendes richtig sein:

$$f(x_\nu) = h_\nu(\varphi; g)f(x_\nu),$$

d.h. $f(x_\nu)$ ist Fixpunkt von $h_\nu(\psi, g)$, wie behauptet. Demnach hat jeder Fixpunkt $f \in Y^X$ die geforderten Eigenschaften, und umgekehrt.

□

Zusammen mit dem Lemma von the Cauchy-Frobenius ergibt sich jetzt die Anzahl der $H \wr_X G$-Bahnen auf Y^X, und die Einschränkung auf die oben erwähnten Untergruppen isomorph zu G, H und $H \times G$ liefern daraus die gesuchten Anzahlen der G–, H– und $H \times G$–Klassen auf Y^X:

6.3.9 Folgerung *Sind ${}_GX$ und ${}_HY$ endliche Gruppenoperationen, dann gilt für die Anzahl der Bahnen der induzierten Operation von $H \wr_X G$ auf Y^X:*

$$|H \wr_X G \setminus\!\setminus Y^X| = \frac{1}{|H|^{|X|}|G|} \sum_{(\varphi;g)\in H\wr_X G} \prod_{\nu\in z(\bar{g})} |Y_{h_\nu(\varphi;g)}|.$$

Die Einschränkung auf die entsprechenden Untergruppen isomorph G, H und $H \times G$ liefert:

$$|G \setminus\!\setminus Y^X| = \frac{1}{|G|}\sum_{g\in G}|Y|^{z(\bar{g})},\ |H \setminus\!\setminus Y^X| = \frac{1}{|H|}\sum_{h\in H}|Y_h|^{|X|},$$

sowie

$$|(H \times G) \setminus\!\setminus Y^X| = \frac{1}{|H||G|} \sum_{(h,g)\in H\times G} \prod_i |Y_{h^i}|^{a_i(\bar{g})}.$$

□

6.3.10 Anwendung (Anzahl unnumerierter Graphen) Eine konkrete Anwendung ist die Berechnung der Anzahl unnumerierter Graphen mit p Punkten. Diese gleicht

6.3.11
$$|S_p \setminus\!\setminus 2^{\binom{p}{2}}| = \sum_{a\vdash p} \frac{2^{z(\bar{a})}}{\prod_i i^{a_i} a_i!},$$

wenn $z(\bar{a})$ die Anzahl der von einer Permutation $\pi \in S_P$ vom Zykeltyp $a(\pi) = a$ induzierten zyklischen Faktoren ist. Man kann das übrigens auch als Bahnenanzahl formulieren:

$$z(\bar{a}) = \left| \langle \pi \rangle \setminus\!\setminus \binom{P}{2} \right|.$$

Ist beispielsweise $|P| = 4$, so stellt man folgendes fest:

Die symmetrische Gruppe hat 5 Konjugiertenklassen, die Zykelpartitionen dieser Klassen sind

$$(4), (3,1), (2^2), (2,1^2), (1^4),$$

die entsprechenden Zykeltypen sind

$$(0,0,0,1), (1,0,1,0), (0,2,0,0), (2,1,0,0), (4,0,0,0).$$

Die Ordnungen $\prod_i i^{a_i} a_i!$ der Zentralisatoren von Elementen dieser Klassen sind

$$4, 3, 8, 4, 16.$$

Repräsentanten dieser Klassen sind die Permutationen

$$(0123), (012), (01)(23), (01), 1,$$

und die Anzahlen $z(\overline{a})$ der Zyklen, die von diesen Repräsentanten auf den 6 Punktepaaren (!) induziert werden, sind

$$2, 2, 4, 4, 6.$$

Setzt man diese Zahlen in 6.3.11 ein, so ergibt sich 11 als deren Anzahl.

◇

Das Lemma von Cauchy–Frobenius läßt mehrere Verfeinerungen zu und findet zahlreiche Anwendungen. Zum Beispiel folgen zahlentheoretische Kongruenzen:

6.3.12 Anwendung (Kongruenzen) Aus dem Lemma von Cauchy–Frobenius ergibt sich direkt, daß für jede endliche Operation ${}_GM$ die folgende Kongruenz richtig ist:

$$\sum_{g\in G} |M_g| \equiv 0 \ (|G|).$$

Hiermit kann man, durch Betrachtung geeigneter Operationen, viele zahlentheoretische Kongruenzen herleiten, zum Beispiel aus

$$|C_p \setminus\setminus m^p| = \frac{1}{p}(m^p + (p-1)m),$$

den sogenannten *kleinen Satz von Fermat,*

$$m^p \equiv m \ (p).$$

$\diamond$

Neben solchen Anwendungen, wie der Herleitung von Kongruenzen, kann man aber auch das Lemma von Cauchy-Frobenius selbst verfeinern, so daß sich beispielsweise über die Zahl der Graphen mit $|P|$ Punkten hinaus die Anzahl der Graphen mit $|P|$ Punkten *und* k *Kanten* ermitteln läßt. Tatsächlich läßt sich dies mit folgender Verfeinerung des Lemmas bewerkstelligen:

6.3.13 Das Lemma von Cauchy–Frobenius, gewichtete Form: *Ist* ${}_GM$ *eine endliche Operation und* $w\colon M \to R$ *eine auf den Bahnen konstante Abbildung von* M *in einen kommutativen Ring* R*, der den Körper* $\mathbb{Q}$ *der rationalen Zahlen als Teilring enthält. Dann gilt, für eine Transversale* T *der Menge* $G \setminus\setminus M$ *der Bahnen:*

$$\sum_{t\in T} w(t) = \frac{1}{|G|} \sum_{g\in G} \sum_{m\in M_g} w(m).$$

Der Beweis dieser Verfeinerung ist im wesentlichen derselbe wie der der ursprünglichen Version, der sogenannten *konstanten Form* des Cauchy-Frobenius Lemmas.

6.3.14 Anwendung (Abzählung von $G-$Symmetrieklassen nach Gewicht) Ist ${}_GX$ wieder eine endliche Operation, ${}_G(Y^X)$ die davon induzierte Operation auf Y^X, zu einer gegebenen endlichen Menge Y.
Wir können Y als eine Menge von Unbestimmten auffassen und folgende Gewichtsfunktion auf Y^X betrachten, die offenbar konstant auf den Bahnen ist:

$$w\colon Y^X \to \mathbb{Q}[Y]\,,\ f \mapsto \prod_{x\in X} f(x).$$

Weil f genau dann Fixpunkt ist, wenn f auf den zyklischen Faktoren von $\bar{g}$ konstant ist, gilt entsprechend für die Summe aller Fixpunkte von g :

$$\sum_{f\in(Y^X)_g} w(f) = \prod_i \Big(\sum_{y\in Y} y^i\Big)^{a_i(\bar{g})}.$$

Mit der gewichteten Form des Lemmas von Cauchy-Frobenius erhalten wir demnach die

6.3.15 Folgerung *Die Anzahl der Bahnen von G auf Y^X mit vorgegebenem Gewicht*

$$\prod_{y\in Y} y^{b_y}$$

ist der Koeffizient dieses Monoms in dem Polynom

$$\frac{1}{|G|}\sum_{g\in G}\prod_i\Big(\sum_{y\in Y} y^i\Big)^{a_i(\bar g)}.$$

□

Wir können diese Abzählung nach Gewicht sofort anwenden. Unser konkretes Standardbeispiel sind wieder die Graphen. Wir wollen die Anzahl der Graphen mit p Punkten *und mit k Kanten* bestimmen.
Hier war $Y = 2 = \{0, 1\}$, wir ersetzen diese Menge zur Verdeutlichung durch

$$Y = \{y_0, y_1\}.$$

Ist jetzt $f \in Y^{\binom{p}{2}}$ wieder ein numerierter Graph, dann ist sein Gewicht bei der oben eingeführten Gewichtsfunktion w gleich

$$w(f) = y_0^{\binom{p}{2}-k} y_1^k,$$

wenn k die Kantenzahl ist. Die erzeugende Funktion für die Abzählung der Graphen mit p Punkten nach Kantenzahl ist, entsprechend der gewichteten Form des Lemmas von Cauchy-Frobenius, gleich

6.3.16
$$\frac{1}{p!}\sum_{\pi\in S_p}\prod_{i=1}^{\binom{p}{2}}(y_0^i + y_1^i)^{a_i(\bar\pi)}.$$

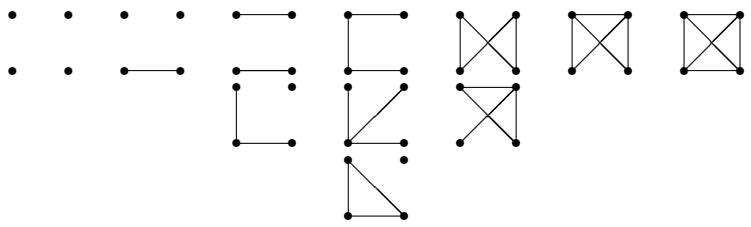
Man kann sich hierbei ganz offenbar das Leben noch dadurch erleichtern, daß man y_0 durch 1 und y_1 durch y ersetzt, es ergibt sich dann als erzeugende Funktion das Polynom

6.3.17
$$\frac{1}{p!}\sum_{\pi\in S_p}\prod_{i=1}^{\binom{p}{2}}(1+y^i)^{a_i(\bar\pi)} = \sum_{a\vdash p}\frac{1}{\prod_{i=1}^p i^{a_i}a_i!}\prod_{j=1}^{\binom{p}{2}}\big(1+y^i\big)^{\overline{a_i}}.$$

Der Koeffizient von y^k in diesem Polynom ist die Anzahl der Graphen mit p Punkten und k Kanten! Für $p = 4$ erhält man das Polynom

$$1 + y + 2y^2 + 3y^3 + 2y^4 + y^5 + y^6.$$

Das entspricht der folgenden Skizze dieser Graphen:



$\diamond$

6.4 Abzählen nach Stabilisatorklasse, Inversionsmethoden

Eine andere Verfeinerung der Abzählung der Bahnen von G auf M geht von folgender Bemerkung aus:

$$G_{gm} = gG_mg^{-1}.$$

Sie impliziert, daß die Stabilisatoren der Elemente $m' \in G(m)$ die Klasse der zu G_m konjugierten Untergruppen, die *Konjugiertenklasse von* G_m bilden:

6.4.1 $$\widetilde{G_m} := \{gG_mg^{-1} \mid g \in G\} = \{G_{gm} \mid g \in G\}.$$

Die Bahnen, deren Elementstabilisatoren die Konjugiertenklasse $\widetilde{U}$ bilden, heißen Bahnen *vom Typ* $\widetilde{U}$. Man kann also die Frage stellen, wie groß die Anzahl der Bahnen vom Typ $\widetilde{U}$ ist, zu vorgegebener Untergruppe U von G. Diese Menge nennen wir das *Stratum von* U und bezeichnen sie so:

$$G \setminus\setminus_{\widetilde{U}} M := \{G(m) \mid G_m \in \widetilde{U}\}.$$

Zur Berechnung ihrer Ordnung bringen wir sie mit der Menge der Fixpunkte von U in Zusammenhang:

$$M_U := \{m \in M \mid \forall\ g \in U : gm = m\}.$$

Es gilt, wenn wieder T eine Transversale von $G \setminus\setminus M$ bezeichnet:

$$|M_U| = \sum_{m:U\le G_m} 1 = \sum_{V:U\le V\le G} \sum_{m:V=G_m} 1 = \sum_{V:U\le V\le G} \frac{1}{|\widetilde{V}|} \sum_{m:G_m\in\widetilde{V}} 1$$

$$= \sum_{V:U\le V\le G} \frac{|G/V|}{|\widetilde{V}|} \sum_{t\in T:G_t\in\widetilde{V}} 1 = \sum_{V:U\le V\le G} \frac{|G/V|}{|\widetilde{V}|} |G \setminus\setminus_{\widetilde{V}} M|.$$

Wir haben also folgendes bewiesen:

6.4.2 $$|M_U| = \sum_{V:U\le V\le G} \frac{|G/V|}{|\widetilde{V}|} |G \setminus\setminus_{\widetilde{V}} M|.$$

Diese Gleichung soll nach $|G \setminus\setminus_{\widetilde{V}} M|$ aufgelöst, sie soll *invertiert* werden. Dazu verwenden wir ein ganz allgemeingültiges Inversionsverfahren für Halbordnungen, die *Möbiusinversion:*

6.4.3 Inversion auf Halbordnungen Wir beginnen mit der Einführung der *Inzidenzalgebra* zu einer Halbordnung.

i) Sei $(P, \le)$ eine *Halbordnung*, d.h. $\le$ sei reflexiv, antisymmetrisch und transitiv. Die gegebene Relation $\le$ erlaubt die Definition von *Intervallen*

$$[p, q] := \{r \in P \mid p \le r \le q\}.$$

Sind alle diese Intervalle endlich, dann heißt $(P, \leq)$ *lokal endlich.* Im folgenden sei das stets erfüllt, und es sei ein Körper $\mathbb{K}$ vorgegeben. Die Menge

$$I_{\mathbb{K}}(P) := \{\varphi\colon P^2 \to \mathbb{K} \mid \varphi(p,q) = 0 \text{ falls } p \not\leq q\}$$

aller sogenannten *Inzidenzfunktionen* ist eine $\mathbb{K}$–Algebra: die folgende Addition und Skalarmultiplikation definieren nämlich eine Vektorraumstruktur:

$$(\varphi + \psi)(p,q) := \varphi(p,q) + \psi(p,q)\ ,\ (\rho\varphi)(p,q) := \rho \cdot \varphi(p,q),\ \rho \in \mathbb{K},$$

während die lokale Endlichkeit die folgende *Convolution* als Multiplikation einzuführen erlaubt:

$$(\varphi \star \psi)(p,q) := \sum_{r \in [p,q]} \varphi(p,r)\psi(r,q).$$

Dies macht $I_{\mathbb{K}}(P)$ zu einem Ring. Einselement ist die *Kroneckersche δ–Funktion*

$$\delta(p,q) := \begin{cases} 1 & \text{falls } p = q \\ 0 & \text{sonst.} \end{cases}$$

Skalarmultiplikation und Convolution erfüllen

$$\rho(\varphi \star \psi) = (\rho\varphi) \star \psi = \varphi \star (\rho\psi),$$

dieser Ring ist demnach sogar eine $\mathbb{K}$–*Algebra*, die *Inzidenzalgebra* von $(P, \leq)$ über $\mathbb{K}$.

ii) Von großer Bedeutung ist die Charakterisierung der invertierbaren Elemente, also der φ in $I_{\mathbb{K}}(P)$, für die es $\psi \in I_{\mathbb{K}}(P)$ gibt mit $\psi \star \varphi = \delta$ und $\varphi \star \psi = \delta$. Man erhält diese Funktionen mit einem einfachen Argument aus der linearen Algebra, das die Inzidenzfunktionen mit oberen Dreiecksmatrizen identifiziert, wie folgt. Bei endlichem P können wir die Halbordnung bekanntlich in eine Totalordnung einbetten, eine sogenannte *topologische Numerierung,* d.h. wir können die $p \in P$ so numerieren, daß

$$p_i < p_k \Longrightarrow i < k.$$

Eine solche Numerierung ergibt die Einbettung

$$\varphi \mapsto \Phi := (\varphi(p_i, p_k))$$

von $I_{\mathbb{K}}(P)$ in die Menge der oberen Dreiecksmatrizen über $\mathbb{K}$. Diese Einbettung respektiert Addition und Skalarmultiplikation, und die Convolution entspricht dem Matrixprodukt. Demnach ist φ genau dann invertierbar, wenn die Werte $\varphi(p,p) \neq 0$ sind. Dies gilt auch im allgemeinen Fall solange $(P, \leq)$ lokal endlich ist, denn man kann leicht zeigen, daß die Inzidenzfunktion, die im zweiten Punkt des Hilfssatzes rekursiv definiert wird, tatsächlich eine Inverse bzgl. Convolution ist:

6.4.4 Hilfssatz *In jeder Inzidenzalgebra einer lokal endlichen Halbordnung $(P, \leq)$ gilt für $\varphi \in I_{\mathbb{K}}(P)$:*

- *φ ist genau dann invertierbar, wenn für jedes $p \in P$ gilt*

$$\varphi(p,p) \neq 0.$$

- *Ist φ invertierbar, dann gilt für φ^{-1}*

$$\varphi^{-1}(p,p) = \varphi(p,p)^{-1},$$

und

$$\begin{aligned}\varphi^{-1}(p,q) &= -\varphi(q,q)^{-1} \sum_{r\in[p,q)} \varphi^{-1}(p,r)\varphi(r,q) \\ &= -\varphi(p,p)^{-1} \sum_{r\in(p,q]} \varphi(p,r)\varphi^{-1}(r,q),\end{aligned}$$

wobei, wie üblich, $[p,q)$ und $(p,q]$ halb offene Intervalle bezeichnen.

□

Eine besonders wichtige invertierbare Inzidenzfunktion ist die *Zetafunktion.* Sie bechreibt nämlich die Halbordnung P, ist mit dieser identifizierbar:

$$\zeta(p,q) := \begin{cases} 1 & \text{falls } p \leq q, \\ 0 & \text{sonst.} \end{cases}$$

Ihre Inverse heißt die *Möbiusfunktion* von $(P,\leq)$: $\mu := \zeta^{-1}$, für die, nach dem Hilfssatz, folgende Rekursionen gelten: $\mu(p,p) = 1$, und für $p < Q$ gilt

6.4.5 $$\mu(p,q) = -\sum_{r\in[p,q)} \mu(p,r) = -\sum_{r\in(p,q]} \mu(r,q).$$

Diese enge Verbindung zwichen Zeta- und Möbiusfunktion liefert uns ein sehr wichtiges Inversionstheorem, das jetzt angegeben werden soll. In $(P,\leq)$ heißen die Teilmengen $\{q \in P \mid q \leq p\}$ *Hauptideale,* während die Teilmengen $\{q \in P \mid q \geq p\}$ *Hauptfilter* genannt werden.

6.4.6 Die Möbiusinversion *Sei $(P,\leq)$ eine lokal endliche Halbordnung, F und G Abbildungen von P in einen Körper $\mathbb{K}$. Es gilt dann:*

- *Sind alle Hauptideale von P endlich, dann gilt die folgende Äquivalenz zwischen Gleichungssystemen:*

$$\forall\ p:\ G(p) = \sum_{q\leq p} F(q) \iff \forall\ p:\ F(p) = \sum_{q\leq p} G(q)\mu(q,p).$$

- *Sind alle Hauptfilter von P endlich, dann gilt*

$$\forall\ p:\ G(p) = \sum_{q\geq p} F(q) \iff \forall\ p:\ F(p) = \sum_{q\geq p} \mu(p,q)G(q).$$

Beweis: $I_{\mathbb{K}}(P)$ operiert (von rechts) linear auf dem Vektorraum $\mathbb{K}^P$:

$$(F \cdot \varphi)(p) := \sum_{q \leq p} F(q)\varphi(q,p).$$

Die Gültigkeit von $G(p) = \sum_{q \leq p} F(q)$, für alle $p \in P$, bedeutet unter diesem Aspekt, daß $G = F \cdot \zeta$, was offensichtlich äquivalent ist zu $F = G \cdot \mu$, bzw. zu der Gültigkeit von $F(p) = \sum_{q \leq p} G(q)\mu(q,p)$, für alle $p \in P$.
Das beweist die erste Äquivalenz, die zweite folgt ganz analog, mit der entsprechenden Operation der Inzidenzalgebra von links.

□

Eine spezielle lokal endliche Halbordnung ist $(\mathbb{N}^*, |)$, die Menge der positiven natürlichen Zahlen zusammen mit der Teilbarkeit als Relation. Diese Halbordnung ist der Untersuchungsgegenstand der *Zahlentheorie,* ihre Funktion μ heißt deshalb auch die *zahlentheoretische Möbiusfunktion.* Um ihre Werte explizit angeben zu können, verwendet man folgende Beobachtungen:

- Man kann anstelle von $\mu(p,q)$ kurz $\mu(q/p)$ schreiben, denn die Intervalle $[p,q]$ und $[r,s]$ sind ordnungsisomorph, wenn $q/p = s/r$, so daß nach obiger Rekursion gilt $\mu(p,q) = \mu(r,s)$. Man kann deshalb anstelle von $\mu(p,q)$ auch $\mu(q/q)$ schreiben, falls p q teilt.

- Weil ζ allein durch die Halbordnung bestimmt ist, gilt dasselbe für die Möbiusfunktion, sie ist also "dieselbe" für ordnungsisomorphe Halbordnungen.

- Man kann die Werte der Möbiusfunktion auf $(\mathbb{N}^*, |)$ demnach unter Ausnutzung der Tatsache berechnen, daß sie multiplikativ ist:

6.4.7 Hilfssatz *Aus den Möbiusfunktionen μ_P und μ_Q zweier lokal endlicher Halbordnungen gewinnt man die Möbiusfunktion $\mu_{P\times Q}$ von $P \times Q$ mit*

$$(p_1,q_1) \leq (p_2,q_2) \iff p_1 \leq p_2, \text{ und } q_1 \leq q_2,$$

in folgender Weise:

$$\mu_{P\times Q}((p_1,q_1),(p_2,q_2)) = \mu_P(p_1,p_2) \cdot \mu_Q(q_1,q_2).$$

(vgl. Übungsblatt) Um das auf die Möbiusfunktion von $(\mathbb{N}^*, |)$ anzuwenden bemerkt man noch, daß das Intervall $[d,n]$, mit $d \mid n$, ordnungsisomorph ist zu dem cartesischen Produkt

6.4.8 $$[1, p_0^{k_0}] \times \ldots \times [1, p_{r-1}^{k_{r-1}}],$$

wenn n/d die folgende Primzahlzerlegung hat:

$$n/d = p_0^{k_0} \cdot \ldots \cdot p_{r-1}^{k_{r-1}},$$

wobei die p_i paarweise verschiedene Primzahlen sind und $k_i \geq 1$. Es folgt jetzt insgesmt:

$$\mu(n/d) := \mu(d,n) = \mu(1,n/d) = \prod_{i=0}^{r-1} \mu(1,p_i^{k_i}).$$

Zusätzlich bekommen wir noch aus 6.4.5, daß $\mu(1) = 1, \mu(p) = -1$, wenn p prim ist, und $\mu(p^r) = 0$, falls $r > 1$. Dies liefert die gesuchte explizite Formel für die Werte der zahlentheoretischen Möbiusfunktion:

6.4.9 $$\mu(n) = \begin{cases} 1 & \text{falls } n = 1, \\ (-1)^r & \text{falls } n \text{ Produkt von } r \text{ verschiedenen Primzahlen ist,} \\ 0 & \text{sonst.} \end{cases}$$

◇

Kehren wir damit zu einer endlichen Gruppenoperation ${}_GM$ und zur Bestimmung der Anzahl der Bahnen vom Typ $\widetilde{U}$ zurück. Wir hatten bewiesen, daß

$$|M_U| = \sum_{V:U\leq V\leq G} \frac{|G/V|}{|\widetilde{V}|} |G \setminus\!\setminus_{\widetilde{V}} M|$$

gilt. Mit Hilfe der Zetafunktion auf der Halbordnung

$$(L(G), \subseteq),\ L(G) := \{U^i \mid U^i \leq G\},$$

liest sich diese Gleichung so:

$$|M_U| = \sum_{V\leq G} \zeta(U,V) \frac{|G/V|}{|\widetilde{V}|} |G \setminus\!\setminus_{\widetilde{V}} M|.$$

In $L(G)$ gibt es zu je zwei Elementen U^i und U^k ein eindeutig bestimmtes Infimum $U^i \wedge U^k$ und ein eindeutig bestimmtes Supremum $U^i \vee U^k$, nämlich

$$U^i \wedge U^k = U^i \cap U^k, \text{ bzw. } U^i \vee U^k = \langle U^i \cup U^k \rangle.$$

Das Quadrupel

$$(L(G), \subseteq, \wedge, \vee)$$

ist also ein *Verband,* der *Untergruppenverband von G*. Die Werte der Möbiusfunktion auf dem Untergruppenverband von G sind nach obiger Argumentation ganze Zahlen. Die Matrix $\mu(G)$ heißt die *Möbiusmatrix* von G, und $\zeta(G) = (\zeta(U^i, U^k))$ heißt die *Zetamatrix* von G.

Die gewünschte Auflösung nach der Anzahl der Untergruppen vorgegebenen Typs gelingt mit Hilfe der Möbiusinversion, unter Verwendung der Möbiusfunktion des Untergruppenverbandes:

6.4.10 Folgerung *Ist ${}_GM$ eine endliche Operation und ist U eine Untergruppe von G, dann gilt für die Anzahl der Bahnen vom Typ $\widetilde{U}$:*

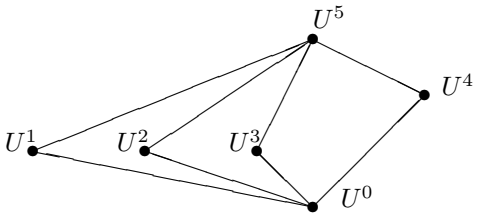
$$|G \setminus\!\setminus_{\widetilde{U}} M| = \frac{|\widetilde{U}|}{|G/U|} \sum_{V\leq G} \mu(U,V) |M_V|.$$

□

Dieses Resultat war im wesentlichen bereits Burnside bekannt, ihm fehlte nur noch der Begriff der Möbius–Inversion. Ein interessanter Spezialfall ist die Anzahl der Bahnen vom Typ $\widetilde{1}$, also der Bahnen der (maximalen) Länge $|G|$ von G auf M, die Anzahl der *asymmetrischen Bahnen:*

$$|G \setminus\!\setminus_{\widetilde{1}} M| = \frac{1}{|G|} \sum_{U \leq G} \mu(1, U)|M_U|.$$

Betrachten wir als ein einfaches Beispiel die symmetrische Gruppe S_3. Ihren Untergruppenverband zeigt



wobei

$$U^0 = \langle 1 \rangle,\ U^1 = \langle (01) \rangle,\ U^2 = \langle (02) \rangle,\ U^3 = \langle (12) \rangle,\ U^4 = \langle (012) \rangle,\ U^5 = S_3.$$

Es gilt also für die *Zetamatrix*

$$\zeta(S_3) := (\zeta(U^i, U^k)) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 1 \\ & & & 1 & 0 & 1 \\ & & & & 1 & 1 \\ & & & & & 1 \end{pmatrix},$$

und ihr Inverse, die *Möbiusmatrix,*

$$\mu(S_3) := (\mu(U^i, U^k)) = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & 3 \\ & 1 & 0 & 0 & 0 & -1 \\ & & 1 & 0 & 0 & -1 \\ & & & 1 & 0 & -1 \\ & & & & 1 & -1 \\ & & & & & 1 \end{pmatrix}.$$

Der Untergruppenverband der symmetrischen Gruppe ist im allgemeinen Fall allerdings sehr kompliziert und bisher nicht explizit beschrieben. Dagegen ist $L(C_n)$ leicht anzugeben: Ist $C_n = \langle x \mid x^n = 1 \rangle$, dann gibt es zu jedem Teiler d von n genau eine Untergruppe $C(d)$ der Ordnung d in C_n, und es gilt für diese:

$$C(d_1) \leq C(d_2) \iff d_2 \mid d_1.$$

6.4.11 Folgerung *Die Halbordnung der Untergruppen der zyklischen Gruppe C_n ist antiisomorph zur Halbordnung der Teiler von n.*

□

Die Identität

$$|G \setminus\!\setminus_{\widetilde{U}} M| = \frac{|\widetilde{U}|}{|G/U|} \sum_{V \leq G} \mu(U,V)|M_V|.$$

kann man noch durch Zusammenfassen von Koeffizienten nach Konjugiertenklassen von Untergruppen vereinfachen, denn die Fixpunkteanzahl $|M_V|$ ist konstant auf den Konjugiertenklassen von Untergruppen von G. Wir betrachten dazu die Menge $\widetilde{L}(G)$ der Konjugiertenklassen von Untergruppen in G:

$$\widetilde{L}(G) := \{\widetilde{U}_0, \ldots, \widetilde{U}_{d-1}\}, \text{ mit Repräsentanten } U_i \in \widetilde{U}_i.$$

Diese Menge ist ebenfalls eine Halbordnung (im allgemeinen aber *kein* Verband):

$$\widetilde{U}_i \leq \widetilde{U}_k \ :\Longleftrightarrow\ \exists\, U \in \widetilde{U}_i, V \in \widetilde{U}_k : U \leq V.$$

Mit ihrer Hilfe definieren wir jetzt die rationalen Zahlen

$$b_{ik} := \frac{|\widetilde{U}_i|}{|G/U_i|} \sum_{V \in \widetilde{U}_k} \mu(U_i, V), \text{ und } B(G) := (b_{ik}).$$

Diese Matrix ist die Inverse der sogenannten *Markentafel*, die bereits Burnside eingeführt hat: $B(G) = M(G)^{-1}$, mit $M(G) := (m_{ik})$, und

$$m_{ik} := \frac{|G/U_k|}{|\widetilde{U}_k|} \sum_{V \in \widetilde{U}_k} \zeta(U_i, V).$$

Mit Hilfe dieser Matrix $B(G)$, die wir als *Burnsidematrix* von G bezeichnen wollen, liest sich jetzt obiges Resultat wie folgt:

6.4.12 Burnsides Lemma: *Ist ${}_GM$ eine endliche Operation, dann gilt:*

$$\begin{pmatrix} \vdots \\ |G \setminus\!\setminus_{\widetilde{U}_i} M| \\ \vdots \end{pmatrix} = B(G) \cdot \begin{pmatrix} \vdots \\ |M_{U_i}| \\ \vdots \end{pmatrix}.$$

Ganz analog ergibt sich auch hier eine Möglichkeit, Bahnen nach Gewicht und Typ abzuzählen:

6.4.13 Burnsides Lemma, gewichtete Form: *Ist ${}_GM$ eine endliche Operation, $w\colon M \to R$, R ein kommutativer Ring, der $\mathbb{Q}$ als Teilring enthält, w konstant auf den Bahnen, dann gilt, wenn T_i eine Transversale des Stratums vom Typ $\widetilde{U}_i$ ist:*

$$\begin{pmatrix} \vdots \\ \sum_{t \in T_i} w(t) \\ \vdots \end{pmatrix} = B(G) \cdot \begin{pmatrix} \vdots \\ \sum_{m : U_i \leq G_m} w(m) \\ \vdots \end{pmatrix}.$$

Der Beweis ist im wesentlichen derselbe wie obige Herleitung der konstanten Form.

Beispielsweise bilden die bereits erwähnten 6 Untergruppen von S_3 vier Konjugiertenklassen:

$$\widetilde{U}_0 = \{U^0\},\ \widetilde{U}_1 = \{U^1, U^2, U^3\},\ \widetilde{U}_2 = \{U^4\},\ \widetilde{U}_3 = \{U^5\}.$$

Als Markentafel ergibt sich

$$M(S_3) = \begin{pmatrix} 6 & 3 & 2 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

und die Burnsidematrix hat die folgende Form:

$$B(S_3) = \begin{pmatrix} 1/6 & -1/2 & -1/6 & 1/2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1/2 & -1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

6.5 Konstruktion und Zufallserzeugung von Repräsentanten

Hat man mit Hilfe einer Bahnenabzählung eine Übersicht über die Anzahl unnumerierter Strukturen, wie z.B. unnumerierter Graphen mit n Punkten, gewonnen, dann entsteht sofort die Frage, wie man diese Strukturen *konstruieren* kann. Hierzu ebenfalls einige (aus Zeitgründen kurze) Bemerkungen.

Zunächst ein Hinweis, daß auch hier Doppelnebenklassen verwendet werden können. Eine unmittelbare Konsequenz der Bijektivität

$$G(m) \rightarrowtail\!\!\!\!\!\rightarrow G/G_m, gm \mapsto gG_m$$

ist nämlich die

6.5.1 Folgerung *Ist ${}_GM$ gegeben, $U \leq G$ und $m \in M$, dann ist die folgende Abbildung eine Bijektion:*

$$\alpha\colon U \backslash\!\backslash G(m) \to U\backslash G/G_m\,,\ U(gm) \mapsto UgG_m.$$

Aus jeder Transversalen von $U\backslash G/G_m$ erhält man also, durch Anwendung von α^{-1}, eine Transverale von $U \backslash\!\backslash G(m)$.

6.5.2 Anwendung (Transversalen von $G \backslash\!\backslash Y^X$) Betrachten wir, als vielseitiges Anwendungsbeispiel, die Ermittlung einer Transversalen der Symmetrieklassen von G auf Y^X. Ohne Einschränkung der Allgemeinheit können wir $G \leq S_X$ voraussetzen.

i) Aus der Folgerung gewinnen wir die Bijektion

$$\alpha\colon G \backslash\!\backslash S_X(f) \rightarrowtail\!\!\!\!\!\rightarrow G\backslash S_X/(S_X)_f\,,\ G(gf) \mapsto Gg(S_X)_f.$$

Darüberhinaus können wir ohne Einschränkung annehmen, daß

$$Y^X = m^n,$$

also $G \leq S_n$ und entsprechend

$$\alpha\colon G \backslash\!\backslash S_n(f) \rightarrowtail\!\!\!\!\!\rightarrow G\backslash S_n/(S_n)_f\,,\ G(gf) \mapsto Gg(S_n)_f.$$

ii) Die nächste Beobachtung, die wir machen, betrifft die Bahn $S_n(f)$. Sie besteht offenbar aus den Abbildungen $f' \in m^n$ desselben Inhalts $\lambda(f')$ wie f. Dabei verstehen wir unter dem *Inhalt* von f die Zahlenfolge

$$\lambda(f) = (\lambda_0(f), \ldots, \lambda_{m-1}(f)),\ \ \lambda_i(f) := |f^{-1}(i)|,$$

der Vielfachheiten, mit denen f die Werte $i \in m$ annimmt. Ist $\lambda = (\lambda_0, \ldots, \lambda_{m-1})$ eine Folge der Länge m aus natürlichen Zahlen $\lambda_i, i \in m$, mit $\sum_i \lambda_i = n$, dann kürzen wir dies auch so ab:

$$\lambda \models_m n.$$

Die Bahn $S_n(f)$ einer Abbildung f vom Inhalt λ enthält also insbesondere die *kanonische Abbildung* mit diesem Inhalt:

$$f_\lambda := (f_\lambda(0), \ldots, f_\lambda(n-1)) := (\underbrace{0, \ldots, 0}_{\lambda_0(f)}, \underbrace{1, \ldots, 1}_{\lambda_1(f)}, \ldots, \underbrace{m-1, \ldots, m-1}_{\lambda_{m-1}(f)}).$$

Die Bahn von f mit Inhalt λ ist also die Menge

$$m^n_\lambda := \{\pi f_\lambda = f_\lambda \circ \pi^{-1} \mid \pi \in S_n\},$$

und wir haben damit folgendes bewiesen:

6.5.3 $$G \setminus\setminus S_n(f) = G \setminus\setminus m^n_{\lambda(f)}.$$

Die Berechnung einer Transversale von $G \setminus\setminus m^n$ können wir also schrittweise vornehmen, indem wir sukzessive Transversalen der Teilmengen m^n_λ ermitteln:

$$G \setminus\setminus m^n = \dot{\bigcup_{\lambda \models_m n}} G \setminus\setminus m^n_\lambda.$$

Die Menge der Bahnen aus Elementen vom Inhalt λ wollen wir so bezeichnen:

$$G \setminus\setminus_\lambda m^n := G \setminus\setminus m^n_\lambda.$$

iii) $f \in m^n_\lambda$ kann durch das λ–*Tabloid* der Urbildmengen $f^{-1}(i), i \in m$, veranschaulicht werden:

$$\begin{array}{l} \underline{i_0 \ldots i_{\lambda_0 - 1}} \\ \underline{j_0 \cdots j_{\lambda_1 - 1}} \\ \cdots \end{array},$$

wobei die $i-$te Zeile aus den Elementen von $f^{-1}(i)$ besteht, in natürlicher Reihenfolge, also $i_0 < \ldots < i_{\lambda_0 - 1}$. Die verschiedenen $\lambda-$Tabloide sind also gerade die Elemente der Bahn $S_n(f_\lambda)$. Es geht also um die Ermittlung der Transversalen der Bahnen von G auf den Mengen der $\lambda-$Tabloide, für alle $\lambda \models_m n$.

iv) Der kanonische Repräsentant f_λ aus der Bahn von f wird durch folgendes Tabloid visualisiert:

$$\begin{array}{l} \underline{0 \ldots \lambda_0 - 1} \\ \underline{\lambda_0 \ldots \lambda_0 + \lambda_1 - 1} \\ \cdots \end{array}.$$

Der Stabilisator dieser Abbildung ist

$$(S_n)_{f_\lambda} = S_{\{0, \ldots, \lambda_0 - 1\}} \oplus S_{\{\lambda_0, \ldots, \lambda_0 + \lambda_1 - 1\}} \oplus \ldots =: S_\lambda,$$

die Untergruppe aller Permutationen $\pi \in S_n$, die jede Zeile des Tabloids in sich selbst überführen. Wir können unser Problem also wie folgt präzisieren: Es geht um die Bestimmung einer Transversalen von (einer der folgenden bijektiven Mengen):

6.5.4 $$G \setminus\!\setminus m_\lambda^n \rightarrowtail G\backslash S_n/S_\lambda \twoheadrightarrow G \setminus\!\setminus (S_n/S_\lambda).$$

v) Betrachten wir als Beispiel erneut die Graphen mit 4 Punkten und genau 2 Kanten, d.h. $n = \binom{4}{2} = 6$, $m = 2$, $\lambda = (4,2)$. Bevor wir alle 15 $(4,2)$–Tabloide en detail hinschreiben, ist es zweckmäßig zu bemerken, daß von jedem Tabloid eine Zeile weggelassen werden kann, weil diese eindeutig durch die übrigen bestimmt ist, d.h. es genügt, die *verkürzten* Tabloide hinzuschreiben. Im vorliegenden Fall der Graphen mit 4 Punkten und 2 Kanten schreiben wir deshalb nur die zweiten Zeilen hin, weil diese die kürzeren sind:

$$\underline{\overline{01}},\ \underline{\overline{02}},\ \underline{\overline{03}},\ \underline{\overline{04}},\ \underline{\overline{05}},\ \underline{\overline{12}},\ \underline{\overline{13}},\ \underline{\overline{14}},\ \underline{\overline{15}},\ \underline{\overline{23}},\ \underline{\overline{24}},\ \underline{\overline{25}},\ \underline{\overline{34}},\ \underline{\overline{35}},\ \underline{\overline{45}}.$$

vi) Gemäß obiger Argumentation sind die Bahnen von $G = \bar{S}_4$ auf der Menge dieser 15 verkürzten Tabloide zu berechnen. Dabei ist aber wieder zu beachten, daß die 6 Einträge $0, \ldots, 5 \in 6$ dieser Tabloide, auf denen $S_n = S_6$ operiert für die $6 = \binom{4}{2}$ Paare $\{0,1\}, \ldots, \{2,3\}$ von Punkten stehen!
Die Untergruppe

$$G = \bar{S}_4 \hookrightarrow S_6$$

ist die Permutationsgruppe induziert von $S_4 = \langle (01), (0123) \rangle$ auf der Menge der Punktepaare. Es gilt also

$$G = \bar{S}_4 = \langle (13)(24), (0352)(14) \rangle.$$

Eine der beiden Bahnen von $\bar{S}_4$ auf der Menge der 15 $(4,2)$–Tabloide ist

$$\omega_1 := \{\underline{\overline{05}}, \underline{\overline{14}}, \underline{\overline{23}}\},$$

die andere Bahn ω_0 besteht au den übrigen 12 Tabloiden. (Dabei verwenden wir, daß in einer vorbereitenden Abzählung die Anzahl 2 der Graphen mit 4 Punkten und 2 Kanten ermittelt werden konnte!)

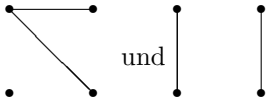
vii) Repräsentanten dieser Bahnen ω_0, ω_1 sind die verkürzten Tabloide zu $\underline{\overline{45}} \in \omega_0$ und $\underline{\overline{23}} \in \omega_1$. Daraus ergeben sich die vollständigen Tabloide

$$\begin{array}{|c|c|}\hline 0123 \\ \hline 45 \\ \hline \end{array} \quad \text{und} \quad \begin{array}{|c|c|}\hline 0145 \\ \hline 23 \\ \hline \end{array}\ .$$

Ihnen entsprechen die folgenden Abbildungen $f, f' \in 2^6_{(4,2)}$:

$$f = (0,0,0,0,1,1), \text{ und } f' = (0,0,1,1,0,0).$$

viii) Insgesamt haben wir gezeigt, daß die folgenden beiden Graphen die *sämtlichen* unnumerierten Graphen mit 4 Punkten und 2 Kanten:



Diese Methode erscheint mühsam. Mit ihrer Hilfe kann man vollständige Listen aller dieser Graphen mit bis zu ca. 8 Punkten berechnen. Es bedarf also noch einiger Verfeinerungen, um solche Kataloge mit bis zu 12 Punkten, beispielsweise, zu erstellen. Eine solche ist das *Leiterspiel,* das die sukzessive Berechnung nach ansteigender Kantenzahl erlaubt (vgl. Übungsblatt).

◇

Viele mathematische Strukturen wie Graphen, Schaltfunktionen, physikalische Zustände usw. können als Bahnen endlicher Gruppen auf endlichen Mengen definiert und damit auch abgezählt werden. Natürlich kann man sie auch auf diese Weise konstruieren, solange die Gruppe und die Menge, auf der die Gruppe operiert, einigermaßen klein sind. Bei Graphen kann man z.B. einen Katalog aller Graphen mit 10 Punkten herstellen (das sind etwa 12 Millionen Graphen). Man will aber oft auch Graphen mit wesentlich größeren Punktezahlen untersuchen, etwa eine *Hypothese* über Graphen *testen.* Hierbei hilft die folgende Methode weiter, die eine *gleichverteilte Zufallserzeugung* von Repräsentanten der Bahnen ermöglicht. Sie eröffnet gleichzeitig ein weites Feld für die *experimentelle Mathematik*, kann man hiermit doch immer dann Strukturen gleichverteilt zufallserzeugen, wenn sie als Bahnen endlicher Gruppen auf endlichen Mengen definierbar sind.

6.5.5 Der Algorithmus von Dixon und Wilf: *Ist ${}_GM$ eine endliche Operation, dann erhält man wie folgt Elemente $m \in M$, die über die Bahnen gleichverteilt sind (d.h. für jede Bahn $\omega \in G \setminus\!\setminus M$ ist die Wahrscheinlichkeit für $m \in \omega$ gleich $|G \setminus\!\setminus M|^{-1}$):*

- *Zuerst wählt man eine Konjugiertenklasse C von Elementen aus G mit der Wahrscheinlichkeit*

$$p(C) := \frac{|C||M_g|}{|G||G \setminus\!\setminus M|},$$

  für irgendein $g \in C$.

- *Dann entnimmt man C irgendein Element g.*

- *Schließlich wählt man aus der Menge M_g der Fixpunkte von g gleichverteilt ein Element m.*

Beweis: Seien $C_1, \ldots, C_r$ die Konjugiertenklassen von G, mit Repräsentanten $g_i \in C_i$. Dann gilt, nach dem Cauchy-Frobenius Lemma:

$$\sum_{i=1}^{r} p(C_i) = \frac{\sum_i |C_i||M_{g_i}|}{\sum_g |M_g|} = 1,$$

so daß $p(-)$ tatsächlich eine Wahrscheinlichkeitsverteilung definiert. Ist jetzt $\omega \in G \setminus\!\setminus M$, dann haben wir

$$p(m \in \omega) = \sum_i p(C_i) p(m \in M_{g_i} \cap \omega)$$

$$= \sum_i p(C_i) \frac{|M_{g_i} \cap \omega|}{|M_{g_i}|} = \sum_i \frac{|C_i||M_{g_i}|}{|G||G \setminus\setminus M|} \frac{|M_{g_i} \cap \omega|}{|M_{g_i}|}$$

$$= \frac{1}{|G||G \setminus\setminus M|} \sum_i |C_i||M_{g_i} \cap \omega| = \frac{1}{|G||G \setminus\setminus M|} \sum_g |M_g \cap \omega|.$$

Nun gilt zudem

$$\sum_g |M_g \cap \omega| = \sum_{g \in G} \sum_{m \in M_g \cap \omega} 1 = \sum_{m \in \omega} \sum_{g \in G_m} 1 = \sum_{m \in \omega} |G_m|,$$

das ist aber gleich $|G_y||\omega| = |G|$, für jedes $y \in \omega$, und wir sind fertig.

□

Die Anwendung dieser Methode zur Erzeugung von Repräsentanten von G-Klassen auf Y^X ist recht einfach, da wir die Fixpunkte für diesen Fall genau kennen.

6.5.6 Folgerung *Für endliche ${}_GX$ und Y liefert der folgende Algorithmus Elemente $f \in Y^X$, die gleichverteilt über die G-Klassen sind:*

- *Zuerst wählt man eine Konjugiertenklasse C von G mit der Wahrscheinlichkeit*
$$p(C) := \frac{|C||Y|^{z(\bar{g'})}}{\sum_g |Y|^{z(\bar{g})}}, g' \in C.$$
- *Dann nimmt man irgendein $g \in C$, berechnet dessen Zykeltyp und konstruiert ein $f \in Y^X$, das konstant auf diesen Zykeln ist, und wobei die Werte auf diesen Zykeln gleichverteilt über Y sind.*

6.5.7 Beispiel Wir wollen nun die Graphen mit vier Punkten zufällig gleichverteilt erzeugen. Die Konjugiertenklassen werden durch die Partitionen (4), $(3,1)$, (2^2), $(2,1^2)$ und (1^4) von 4 charakterisiert. Die Ordnungen dieser Klassen sind 6,8,3,6 und 1. Die Anzahl zyklischer Faktoren der auf der Menge $\binom{4}{2}$ der Punktepaare induzierten Permutationen sind 2,2,4,4 und 6, so daß die Zahl der Fixpunkte auf der Menge $2^{\binom{4}{2}}$ der numerierten Graphen 4,4,16,16 und 64 beträgt. Damit erhält man für die Wahrscheinlichkeiten die Werte (mit $|S_4 \setminus\setminus 2^{\binom{4}{2}}| = 11$)

$$\frac{1}{11}, \frac{4}{33}, \frac{2}{11}, \frac{4}{11}, \frac{8}{33}.$$

Dies liefert uns nach der Multiplikation mit dem Hauptnenner 33 die natürlichen Zahlen 3,4,6,12,8, aus denen sich nach Aufaddieren $3, 7, 13, 25, 33$ ergibt. Ein Zufallsgenerator, der gleichverteilt natürliche Zahlen zwischen 1 und 33 liefert, wird nun verwendet, um C zu wählen. Wird 1, 2 oder 3 erzeugt, so bedeutet dies, daß die erste Konjugiertenklasse gewählt ist. Erhalten wir 4, 5, 6 oder 7, fahren wir mit der zweiten Klasse fort usw. Nehmen wir an, der Generator würde uns 12 ausgeben. Damit ist die Klasse C_2 der Elemente mit Zykelpartition (2^2)

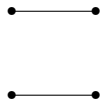


Abbildung 6.1: Der zufallserzeugte Graph

ausgewählt; sie enthält z.B. die Permutation (01)(23). Diese induziert auf der Menge

$$\{a = \{0,1\}, b = \{0,2\}, c = \{0,3\}, d = \{1,2\}, e = \{1,3\}, f = \{2,3\}\}$$

der Punktepaare die Permutation

$$\overline{(01)(23)} = (a)(be)(cd)(f).$$

Ein Zufallsgenerator für Nullen und Einsen wird jetzt eingesetzt, um den zyklischen Faktoren $(a)(be)(cd)(f)$ die Werte 0 oder 1 zuzuordnen. Erzeugt er beispielsweise die Folge 1,0,0,1, so erhalten wir den numerierten Graphen, bei dem nur die Elemente der Paare a und f verbunden sind. Seine Bahn wird durch einen Graphen repräsentiert, wie ihn Abb. 6.1 zeigt.

$\diamond$

6.6 Normal- und Kompositionsreihen

Es geht jetzt um die innere Struktur von Gruppen, soweit diese mit Ketten von ineinandergeschachtelten Normalteilern beschrieben werden kann. Erinnern wir uns deshalb zunächst daran, daß *Normalteiler* genau die selbstkonjugierten Untergruppen $N \leq G$ sind, also die Untergruppen mit

$$\forall\ g \in G:\ gNg^{-1} = N.$$

Dies kürzen wir so ab: $N \trianglelefteq G$. Beispiele sind sämtliche Untergruppen vom Index ≤ 2, also z. B. die alternierende Gruppe $A_n \trianglelefteq S_n$. Wir wissen auch, daß genau die Kerne von Homomorphismen Normalteiler sind, und wir haben gesehen, daß die Nebenklassen eines solchen Normalteilers eine Gruppe bilden, die sogenannte *Faktorgruppe*

$$G/N := \{gN \mid g \in G\}.$$

Sie ist das Bild des Homomorphismus

$$\nu_N : G \to G/N\ ,\ g \mapsto gN,$$

und wir erinnern uns, daß diese Abbildung $\nu_N : G \to G/N$ *universell* ist bzgl. der Klasse $\mathcal{F}$ der auf G definierten Epimorphismen ist, deren Kern N umfaßt, sowie der Klasse $\mathcal{L}$ der Homomorphismen zwischen Gruppen.

Für jeden Homomorphismus $\varphi : G \to H$ von G in eine Gruppe H ist das Bild isomorph zur Faktorgruppe nach dem Kern:

$$\mathrm{Bild}(\varphi) \simeq G/\mathrm{Kern}(\varphi).$$

Dieses Resultat wurde als *Homomorphiesatz* bezeichnet (2.3.8). Hierbei ist die Bemerkung wichtig, daß der Homomorphismus φ eine Bijektion zwischen der Menge der Untergruppen von G, die oberhalb $\mathrm{Kern}(\varphi)$ liegen und der Menge der Untergruppen von $\mathrm{Bild}(\varphi)$ stiftet. Diese Bijektion erhält Durchschnitte und Erzeugnisse, ist also ein sogenannter *Verbandsisomorphismus*

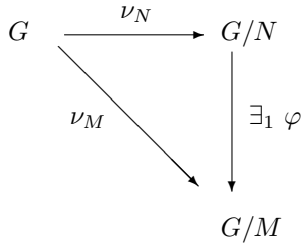
6.6.1 $$(\{U \leq G \mid \mathrm{Kern}(\varphi) \leq U\}, \wedge, \vee) \simeq (\{W \leq \mathrm{Bild}(\varphi)\}, \wedge, \vee).$$

Hat man zwei Normalteiler M und N in G mit $N \subseteq M$, dann gilt

6.6.2 Der erste Isomorphiesatz

$$(G/N)/(M/N) \simeq G/M.$$

Beweis: Wir betrachten das durch einen eindeutig bestimmten Epimorphismus (Universalität von ν_N!) kommutativ ergänzte Diagramm



Wegen $\varphi(gN) = gM$ ist der Kern von φ offenbar M/N, die Behauptung folgt deshalb aus dem Homormorphiesatz.

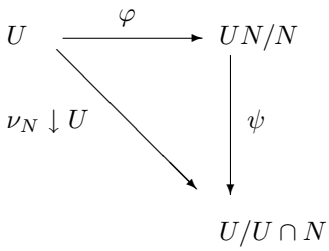
□

Hat man in G einen Normalteiler N und eine Untergruppe U, dann ist UN ebenfalls Untergruppe und es gilt

6.6.3 Der Noethersche Isomorphiesatz

$$U/U \cap N \simeq UN/N.$$

Beweis: Ist ι die Einbettung $U \hookrightarrow UN$ von U in UN, dann hat $\varphi := \nu_N \circ \iota$ als Kern die Untergruppe $U \cap N$, diese ist also ein Normalteiler. Wir haben demnach das eindeutig durch einen Homomorphismus kommutativ ergänzbare Diagramm



Die Abbildung ψ ist injektiv und surjektiv, also ein Isomorphismus.

□

Wir betrachten jetzt, für eine Gruppe G, sogenannte *Normalketten*, das sind Ketten von Untergruppen, bei denen jedes Glied der Kette Normalteiler des Nachbarn ist:

$$\gamma\colon G = G_0 \trianglerighteq G_1 \trianglerighteq \dots.$$

Sind hier Nachbarn G_i, G_{i+1} stets verschieden, dann spricht man von einer *eigentlichen* Normalkette. Die Kettenglieder G_i heißen auch die *Elemente* der Kette, die Faktorgruppen G_i/G_{i+1} heißen ihre *Faktoren*. Normalketten der Form

$$\gamma\colon G = G_0 \trianglerighteq \dots \trianglerighteq G_k = 1$$

heißen *Normalreihen*. Sind γ, γ' Normalketten, dann heißt γ *Verfeinerung* von γ', wenn alle Elemente G'_i von γ' auch in γ vorkommen.

6.6.4 Definition (Äquivalenz von Normalketten) Zwei Normalketten

$$\gamma\colon G = G_0 \trianglerighteq \dots \trianglerighteq G_k$$

und

$$\gamma'\colon G = G'_0 \trianglerighteq \dots \trianglerighteq G'_l$$

heißen *äquivalent*, wenn $k = l$ und

$$\exists\, \pi \in S_k\colon\ G_i/G_{i+1} \simeq G'_{\pi(i)}/G'_{\pi(i)+1}.$$

•

6.6.5 Beispiele

- $S_4 \rhd A_4 \rhd V_4 := \{1, (01)(23), (02)(13), (03)(12)\} \rhd \{1, (01)(23)\} \rhd 1$.
- $S_n \rhd A_n \rhd 1$, ist für $n \neq 4$ nicht verfeinerbar (s.u.).

$\diamond$

6.6.6 Definition (Kompositionsreihen) Eine eigentliche Normalreihe

$$\gamma\colon G = G_0 \rhd G_1 \rhd \ldots \rhd G_{k-1} \rhd G_k = 1$$

heißt *Kompositionsreihe*, wenn alle Faktoren *einfach* sind, d.h. wenn jedes G_i maximaler Normalteiler in G_{i-1} ist. Die Zahl k heißt dabei die *Länge* der Kompositionsreihe. •

Kompositionsreihen sind also *nicht mehr verfeinerbare Normalreihen*. Offensichtlich sind eigentliche Normalreihen mit Faktoren von Primzahlordnung Kompositionsreihen, insbesondere also auch die obige Reihe der symmetrischen Gruppe vom Grad 4:

$$S_4 \rhd A_4 \rhd V_4 \rhd C_2 \rhd 1.$$

Jede Gruppe besitzt Normalreihen, z.B. $G \trianglerighteq 1$, jedoch nicht immer Kompositionsreihen, was sich an der Gruppe $\mathbb{Z}$ zeigen wird. Endliche Gruppen besitzen Kompositionsreihen.

6.6.7 Hilfssatz *Hat G eine Kompositionsreihe der Länge r, so hat jede eigentliche Normalreihe von G höchstens diese Länge.*

Beweis: Sei

$$\gamma\colon G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = 1$$

eine Kompositionsreihe von G und

$$\gamma'\colon G = G_0 \rhd G_1' \rhd \ldots \rhd G_s' = 1$$

sei eine Normalreihe. Wir führen eine Induktion nach r durch.

$r = 1$: G ist einfach, also auch $s = 1$ und damit die Behauptung richtig.

$r > 1$: Wir unterscheiden drei Fälle:

a. Ist $G_1 = G_1'$, dann gilt nach Induktionsannahme $s - 1 \leq r - 1$, woraus die Behauptung folgt.

b. Ist $G_1' < G_1$, dann ist auch

$$G_1 \rhd G_1' \rhd \ldots \rhd G_s' = 1$$

eine eigentliche Normalreihe, nach der Induktionsannahme gilt also $s \leq r - 1$ und damit auch $s \leq r$.

c. Es bleibt der Fall $G_1' \not\leq G_1$ zu diskutieren. Da G_1 maximal in G ist, ergibt diese Annahme, daß $G = G_1G_1'$ gilt. Wir betrachten den Schnitt $G_1 \cap G_1'$. Er ist Normalteiler sowohl in G_1 als auch in G_1'. Nach dem Noetherschen Isomorphiesatz gilt

$$\begin{array}{ll} G/G_1 = G_1G_1'/G_1 \simeq G_1'/G_1 \cap G_1', & \text{und} \\ G/G_1' = G_1G_1'/G_1' \simeq G_1/G_1 \cap G_1'. & \end{array} \tag{6.6.8}$$

Es ergeben sich also die beiden Normalketten

$$G \rhd G_1 \rhd G_1 \cap G_1' \text{ sowie } G \rhd G_1' \rhd G_1 \cap G_1', \tag{6.6.9}$$

und beide sind äquivalent.

Daraus folgt auch, daß $G_1 \cap G_1'$ ein maximaler Normalteiler in G_1' ist. Aus der Induktionsannahme folgt aber, daß jede eigentliche Normalreihe von G_1 eine Länge $\leq r-1$ hat. Jede eigentliche Normalreihe von $G_1 \cap G_1'$ ist also, wegn 6.6.9, von einer Länge $\leq r-2$, dieser Schnitt besitzt also Kompositionsreihen (so wie jede Gruppe mit eigentlichen Normalreihen von beschränkter Länge), und deren Längen sind zudem $\leq r-2$. Daraus schließen wir, mit Hilfe der zweiten der angegebenen eigentlichen Normalketten 6.6.9, daß auch G_1' eine Kompositionsreihe besitzt und deren Länge $\leq r-1$ ist. Zusammen mit der Induktionsannahme ergibt das die Behauptung.

□

6.6.10 Folgerung *Besitzt G Kompositionsreihen, dann gilt:*

- *Je zwei von diesen sind gleichlang.*
- *Jede eigentliche Normalreihe kann zu einer Kompositionsreihe verfeinert werden.*

Wir können damit den Satz von Jordan und Hölder beweisen.

6.6.11 Satz von Jordan und Hölder *Je zwei Kompositionsreihen derselben Gruppe sind äquivalent.*

Beweis: Seien

$$\gamma\colon G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = 1 \text{ und } \gamma'\colon G = G_0 \rhd G_1' \rhd \ldots \rhd G_r' = 1$$

Kompositionsreihen. Wir induzieren nach r. Da der Fall $r = 1$ klar ist (G ist dann ja einfach), können wir gleich $r > 1$ annehmen und die folgenden Fälle unterscheiden:

a. $G_1 = G_1'$, hier folgt die Behauptung direkt aus der Induktionsannahme.

b. Ist $G_1 \neq G_1'$, dann gilt wieder $G = G_1 G_1'$. Wir betrachten Reihen, die durch Verfeinerung von $G_1 \trianglerighteq G_1 \cap G_1' \trianglerighteq 1$ bzw. von der entsprechenden Reihe für G_1', zu Kompositionsreihen führen:

$$G_1 \rhd G_1 \cap G_1' \rhd G_3'' \rhd \ldots \rhd G_r'' = 1,$$

$$G_1' \rhd G_1 \cap G_1' \rhd G_3'' \rhd \ldots \rhd G_r'' = 1.$$

Nun folgt, aus der Induktionsannahme, daß

$$G \rhd G_1 \rhd G_1 \cap G_1' \rhd G_3'' \rhd \ldots \rhd G_r'' = 1$$

äquivalent ist zu γ, und daß

$$G \rhd G_1' \rhd G_1 \cap G_1' \rhd G_3'' \rhd \ldots \rhd G_r'' = 1$$

äquivalent ist zu γ'. Das ergibt schon die Behauptung, denn nach 6.6.8 ist

$$G/G_1 \simeq G_1'/G_1 \cap G_1', \text{ und } G/G_1' \simeq G_1/G_1 \cap G_1'.$$

□

6.6.12 Satz *Eine Gruppe $G \neq 1$ besitzt genau dann eine Kompositionsreihe, wenn folgende beiden Bedingungen erfüllt sind:*

- *Jede absteigende eigentliche Normalkette ist von endlicher Länge.*
- *Jede aufsteigende eigentliche Normalkette eines Elements G' einer Normalreihe von G hat endliche Länge.*

Beweis: Die Notwendigkeit der beiden angegebenen Bedingungen für die Existenz einer Kompositionsreihe ist klar. Zum Beweis der Umkehrung betrachten wir ein Element $G' \neq 1$ einer Normalreihe von G. Aus der zweiten der angegebenen Bedingungen folgt die Existenz eines maximalen Normalteilers von G', woraus mit der ersten Bedingung die Existenz einer Kompositionsreihe von G' folgt. Setzt man jetzt $G' := G$, dann ergibt sich die Existenz einer Kompositionsreihe auch für die Gruppe G.

□

6.6.13 Folgerung *Eine abelsche Gruppe besitzt genau dann Kompositionsreihen, wenn sie die* aufsteigende–Ketten–Bedingung *und die* absteigende–Ketten–Bedingung *für Untergruppen erfüllt (d.h. daß solche (eigentlichen) Untergruppenketten stets von endlicher Länge sind).*

$\mathbb{Z}$ besitzt diese Eigenschaften *nicht,* verfügt daher auch nicht über Kompositionsreihen. Eine nicht abbrechende Kette von Untergruppen bilden beispielsweise die von den Potenzen einer Primzahl p erzeugten Ideale:

$$(p) \supset (p^2) \supset (p^3) \supset \ldots$$

6.6.14 Satz *Ist G eine Gruppe mit Kompositionsreihen der Länge r und ist G' ein Normalteiler von G, dann besitzen sowohl G' als auch G/G' Kompositionsreihen, deren Längen sich zu r addieren.*

Beweis: Ist $G' = 1$ oder $G' = G$, dann gilt die Behauptung offenbar. Andernfalls verfeinern wir $G \rhd G' \rhd 1$ zu einer Kompositionsreihe:

$$G \rhd G_1 \rhd \ldots \rhd G_s = G' \rhd H_1 \rhd \ldots \rhd H_t = 1.$$

Aus ihr ergibt sich $r = s + t$, sowie die Reihe

$$G/G' \rhd G_1/G' \rhd \ldots \rhd G_s/G' = 1.$$

Diese Reihe ist eine Kompositionsreihe von G/G', denn $\nu_{G'}$ ist ein Isomorphismus zwischen dem Verband der Obergruppen von G' in G und dem Verband der Untergruppen in G/G'. Weil G_{i+1} maximaler Normalteiler in G_i ist, ist demnach auch G_{i+1}/G' maximaler Normalteiler in G_i/G'.
Natürlich ist

$$G' \rhd H_1 \rhd \ldots \rhd H_t = 1$$

eine Kompositionsreihe von G'.

□

Eine wichtige Klasse von Gruppen ist dadurch charakterisiert, daß die Faktoren ihrer Kompositionsreihen von Primzahlordnung sind, wir wollen diese aber anders definieren und später die Äquivalenz der verlangten Eigenschaften nachweisen.

6.6.15 Definition (Kommutatorgruppe) G sei eine Gruppe.

i) Eine Untergruppe $U \leq G$ heißt *charakteristische* Untergruppe, wenn für alle Elemente α der Automorphismengruppe $Aut(G)$ von G gilt

$$\alpha(U) = U.$$

ii) Zu zwei Elementen $g, h \in G$ heißt

$$[g, h] := g^{-1}h^{-1}gh$$

ihr *Kommutator*.

iii) Die von allen Kommutatoren erzeugte Untergruppe

$$G^{(1)} := [G, G] := \langle g^{-1}h^{-1}gh \mid g, h \in G \rangle$$

heißt die *Kommutatorgruppe* von G.

iv) Die *höheren Kommutatorgruppen* $G^{(i)}$ werden rekursiv so definiert:

$$\forall\, i > 1 \colon G^{(i)} := [G^{(i-1)}, G^{(i-1)}],$$

dabei sei $G^{(0)} := G$.

•

6.6.16 Hilfssatz *Die Kommutatorgruppe ist die kleinste Untergruppe mit abelscher Faktorgruppe in G. Sie ist charakteristische Untergruppe.*

Beweis:

i) Ein Automorphismus α bildet einen Kommutator auf einen Kommutator ab,

$$\alpha([g,h]) = [\alpha(g), \alpha(h)],$$

das ist ganz leicht nachzurechnen. Die Kommutatorgruppe ist also charakteristisch, insbesondere also normal.

ii) Ihre Faktorgruppe $G/G^{(1)}$ ist abelsch, denn

$$(gG^{(1)}) \cdot (hG^{(1)}) = gG^{(1)}hG^{(1)} = h \underbrace{h^{-1}gG^{(1)}g^{-1}h}_{=G^{(1)}} \underbrace{h^{-1}ghh^{-1}g^{-1}hgG^{(1)}}_{=gG^{(1)}}.$$

iii) Ist andererseits N ein Normalteiler mit abelscher Faktorgruppe, dann gilt, für alle $g, h \in G$,

$$(gh)N = (gN) \cdot (hN) = (hN) \cdot (gN) = (hg)N,$$

also $(gh)N = (hg)N$, was

$$g^{-1}h^{-1}gh \in N$$

und damit $G^{(1)} \subseteq N$ impliziert.

□

Ein Beispiel ist die Kommutatorgruppe der symmetrischen Gruppe:

6.6.17 $$S_n^{(1)} = A_n.$$

Tatsächlich ist sogar jedes Element der alternierenden Gruppe ein Kommutator (vgl. Übungsblatt).

6.6.18 Definition (auflösbar) Eine Gruppe heißt *auflösbar*, wenn G Kompositionsreihen besitzt und diese nur Faktoren von Primzahlordnung haben. •

Man kann zeigen, daß eine endliche Gruppe G genau dann auflösbar ist, wenn es ein $k \in \mathbb{N}$ gibt mit $G^{(k)} = 1$. Ebenfalls äquivalent ist, eine Gruppe als auflösbar zu bezeichnen, wenn die Faktoren ihrer Kompositionsreihen abelsch sind (denn eine abelsche Gruppe $G \neq 1$ ist genau dann einfach, wenn sie zyklisch von Primzahlordnung ist, und Gruppen von Primzahlordnung sind zyklisch, insbesondere also abelsch).

6.6.19 Satz *Die symmetrische Gruppe S_n ist für $n > 4$ nicht auflösbar, da*

$$S_n \rhd A_n \rhd 1$$

eine Kompositionsreihe ist (A_n ist für $n \neq 4$ einfach).

Diesen auflösbaren Gruppen werden wir im nächsten Semester wieder begegnen, wenn wir Gleichungen nichtlineare Gleichungen im Hinblick auf ihre Lösbarkeit durch Anwendung arithmetischer Operationen und Wurzelziehen auf die Koeffizienten der Gleichung untersuchen (daher haben diese Gruppen nämlich ihren Namen).
All diese Struktursätze, insbesondere der Satz von Jordan und Hölder, lassen sich auf $\Omega-$Gruppen übertragen, wie man leicht nachprüfen kann!

Kapitel 7

Aus der Ringtheorie

Wir kehren jetzt zur Ringtheorie zurück, die verfeinert werden soll. Es geht dabei zunächst um das Verhältnis zwischen Ringen und Idealen, insbesondere Primidealen und maximalen Idealen, denn die entsprechenden Faktorringe sind Integritätsbereiche bzw. Körper. Sie dienen also auch der *Konstruktion* solcher Strukturen. Danach diskutieren wir euklidische Ringe und zeigen, daß diese Hauptidealbereiche sind und daß demnach ihre Elemente eine im wesentlichen eindeutige Zerlegung in unzerlegbare besitzen, in analogie zu den ganzen Zahlen, die im wesentlichen eindeutig in Primfaktoren zerlegt werden können.

7.1 Ringe und Ideale

Erinnern wir uns zunächst an die Definition von Ringen, es sind Mengen R mit zwei Verknüpfungen $+$ und $\cdot$, so daß $(R,+)$ eine abelsche Gruppe, $(R,\cdot)$ eine Halbgruppe ist, und die beiden Distributivgesetze gelten:

$$r(s+t) = rs + rt,\ (r+s)t = rt + st.$$

Diese Distributivgesetze formuliert man eigentlich besser gleich strukturtheoretisch: Links- und Rechtsmultiplikation mit einem Ringelement ist ein Endomorphismus von $(R,+)$. Das liefert nämlich sofort, daß $0r = r0 = 0$ und $r(-s) = (-r)s = -(rs)$ gelten!

7.1.1 Beispiele

- Ringe, die wir bereits kennengelernt haben sind die Zahlbereiche $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- Weitere uns bereits bekannte Beispiele sind die Matrixringe über diesen, also z.B. der Ring $\mathbb{Z}^{n\times n}$, der aus den n-reihigen Matrizen über $\mathbb{Z}$ besteht, mit der Matrixaddition und der Matrizenmultiplikation als Verknüpfungen.
- Allgemeiner gilt: man kann mit einem Ring R und einer nicht leeren Menge M die Menge
$$R^M := \{f \mid f\colon M \to R\}$$
aller Abbildungen von M nach R bilden, die mit punktweiser Addition und Multiplikation,
$$(f+g)(m) := f(m) + g(m),\ (f\cdot g)(m) := f(m)\cdot g(m)$$
offenbar einen Ring bildet.
- Auf solchen Mengen von Abbildungen hat man aber auch Verknüpfungen verwenden, die nicht die punktweisen sind, z.B. ist $R^{\mathbb{N}}$ mit punktweiser Addition und der *Faltung*
$$(f\cdot g)(n) := \sum_{(i,j):i+j=n} f(i)\cdot g(j)$$
identifizierbar mit dem Ring $R[\![x]\!]$ der formalen Potenzreihen über R, in der Unbestimmten x. Der Teilring
$$\left(R^{\mathbb{N}}\right)' := \{f \in R^{\mathbb{N}} \mid \text{ fast alle } f(n) = 0\}$$
ist identifizierbar mit dem Polynomring $R[x]$.
- Daneben bieten die *Endomorphismenringe* abelscher Gruppen eine Fülle an Beispielen: Ist $(A,*)$ abelsche Gruppe, $End(A)$ die Menge ihrer Endomorphismen, dann ist $(End(A),+,\cdot)$ ein Ring mit
$$(f+g)(a) := f(a) * g(a),\ (f\cdot g)(a) := (f\circ g)(a) = f(g(a)).$$

- Wegen der Distributivgesetze ist offensichtlich jeder Ring mit Einselement isomorph zu einem Ring von Endomorphismen von sich selbst, denn man braucht ja nur $r \in R$ auf die Linksmultiplikation mit r abzubilden.

$\diamond$

Ist R ein Ring mit Einselement — und die meisten in der Vorlesung vorkommenden Ringe besitzen ein solches Element —, dann heißt $r \in R$ *Einheit*, wenn es ein $s \in R$ gibt mit $rs = sr = 1$. Die Menge aller Einheiten wird so bezeichnet:

$$E(R) := \{r \in R \mid r \text{ Einheit}\},$$

sie ist eine (multiplikative) Gruppe, die *Einheitengruppe* von R. Einfache Beispiele sind

$$E(\mathbb{Z}) = \{1, -1\},\ E(\mathbb{Z}^{2\times 2}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1 \right\}.$$

Die tragende Rolle, die in der Gruppentheorie die Normalteiler spielen, übernehmen, wie wir bereits wissen, die Ideale: Eine nicht-leere Teilmenge L von R heißt *Linksideal*, wenn für alle $l, l' \in L$ und alle $r \in R$ gilt:

$$l - l' \in L,\ rl \in L.$$

Analog wurde der Begriff des *Rechtsideals* definiert. Ideale, die sowohl Rechts- als auch Linksideale sind, heißen *(zweiseitige) Ideale,* und wir schreiben hierfür auch

$$I \trianglelefteq R.$$

Ideale sind somit Untermoduln.

Schnitte von Idealen sind ebenfalls Ideale, so daß wir von dem Ideal sprechen können, das von einer Teilmenge $M \subseteq R$ *erzeugt* wird; wir bezeichnen es mit (M). Besteht M aus einem einzigen Element r, dann schreiben wir kurz (r) statt $(\{r\})$. Solche Ideale (r) heißen *Hauptideale*, Ringe, deren Ideale sämtlich Hauptideale sind, dementsprechend *Hauptidealringe*.

7.1.2 Beispiele Ist R ein Ring, dann enthält

- R die *trivialen* Ideale $0 := \{0\}$ und R.
- Für das von $r \in R$ erzeugte Hauptideal gilt:

$$(r) = \left\{ x = \sum_{i=1}^{n} s_i r t_i + rt + ur + zr \;\middle|\; s_i, t_i, u, t \in R, z \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

  Enthält R ein Einselement, dann reduziert sich dies zu

$$(r) = \left\{ x = \sum_{i=1}^{n} s_i r t_i \;\middle|\; n \in \mathbb{N}, s_i, t_i \in R \right\}.$$

  Ist R zusätzlich kommutativ, dann gilt entsprechend

$$(r) = \{x = sr \mid s \in R\}.$$

- Sind $I, I' \trianglelefteq R$, dann ist deren Summe

$$I + I' = \{x = i + i' \mid i \in I, i' \in I'\}$$

ein Ideal, das *Summenideal*. Analog definieren wir

$$(II') := \left\{ x = \sum_{\nu=1}^{n} i_\nu i'_\nu \;\middle|\; i_\nu \in I, i'_\nu \in I', n \in \mathbb{N} \right\},$$

das *Produktideal*.

- Summen- und Produktideal genügen den folgenden Ungleichungen:

$$(II') \subseteq I \cap I' \subseteq I + I'.$$

◇

Für Ringhomomorphismen, also für Abbildungen $f\colon R \to R'$ zwischen Ringen, mit

$$f(r_0 + r_1) = f(r_0) + f(r_1) \quad \text{und} \quad f(r_0 \cdot r_1) = f(r_0) \cdot f(r_1),$$

sowie $f(1_R) = 1_{R'}$, falls beide Ringe Einselemente besitzen (f nennt man dann manchmal auch genauer einen Ring-mit-Eins-Homomorphismus), gilt, wie wir wissen, der *Homomorphiesatz für Ringe* 2.5.7, welcher insbesondere folgendes impliziert:

- Der Kern ist ein Ideal:

$$\mathrm{Kern}(f) = \{r \in R \mid f(r) = 0_{R'}\} \trianglelefteq R,$$

und zwischen $\mathrm{Bild}(f)$ (einem Ring!) und $\mathrm{Kern}(f)$ besteht die folgende Beziehung:

$$\varphi\colon R/\mathrm{Kern}(f) \simeq \mathrm{Bild}(f)\,,\; r + \mathrm{Kern}(f) \mapsto f(r).$$

- Ist umgekehrt I ein Ideal in R, dann ist dieses der Kern des folgenden Homomorphismus:

$$\nu_I\colon\; R \to R/I, r \mapsto r + I.$$

Ideale sind also genau die Kerne von Ringhomomorphismen!

- Ist I ein Ideal in R, dann erhält man demnach aus der Faktorgruppe $(R/I, +)$ den Faktorring $(R/I, +, \cdot)$ vermöge

$$[r]_I \cdot [s]_I := [rs]_I, \text{ wobei } [r]_I := r + I.$$

Die I entsprechende kanonische Abbildung $\nu_I\colon r \mapsto [r]_I$ auf die Faktorgruppe R/I ist ein Ringepimorphismus mit I als Kern.

7.1.3 Beispiele

- Als *Restklassenring von $\mathbb{Z}$ modulo n* bezeichnen wir den Faktorring
$$(\mathbb{Z}_n, +, \cdot) := (\mathbb{Z}/(n), +, \cdot) = (\mathbb{Z}/n \cdot \mathbb{Z}, +, \cdot).$$
- Ein Ringhomomorphismus zwischen solchen Restklassenringen ist beispielsweise
$$f\colon \mathbb{Z}_{12} \to \mathbb{Z}_3\ ,\ z + (12) \mapsto z + (3).$$
Der Kern ist $(3 + (12))$; da f zusätzlich surjektiv ist, gilt also
$$\mathbb{Z}_{12}/(3 + (12)) \simeq \mathbb{Z}_3.$$
Schreiben wir kurz $n\mathbb{Z}_m$ für das Ideal
$$(n + (m)) = \{0 + (m), n + (m), 2n + (m), \ldots\} \trianglelefteq \mathbb{Z}_m,$$
dann gilt also
$$\mathbb{Z}_{12}/3\mathbb{Z}_{12} \simeq \mathbb{Z}_3.$$

◇

7.1.4 Anwendungen

i) Eine ganz einfache Anwendung der Abbildung von Ringen auf Restklassenringe ermöglicht eine erhebliche Vereinfachung und Parallelisierung beim *Rechnen mit großen ganzen Zahlen:* Der *Chinesische Restesatz* besagt:

- Ist R ein Ring mit Einselement und Idealen $I_0, \ldots, I_{t-1} \trianglelefteq R$. Die Abbildung
$$\varphi\colon R \to \times_{i\in t} R/I_i,\ r \mapsto (r + I_0, \ldots, r + I_{t-1})$$
der Ringelemente auf die Folge ihrer Nebenklassen ist ein Ringhomomorphismus (wenn $\times_{i\in t} R/I_i$ mit punktweiser Addition und Multiplikation versehen ist).
- Sein Kern ist
$$\mathrm{Kern}(\varphi) = \bigcap_{i\in t} I_i,$$
und φ ist genau dann surjektiv, wenn die Ideale paarweise teilerfremd sind:
$$\forall\ i, j \in t, i \neq j\ :\ I_i + I_j = R.$$
- Diese Abbildung φ ist also genau dann ein *Ringisomorphismus,* wenn der Schnitt der Ideale das Nullideal ist und je zwei von ihnen teilerfremd sind.

Nehmen wir beispielsweise $R := \mathbb{Z}$ und $I := (n)$, $I' := (n')$, mit teilerfremden natürlichen Erzeugenden n, n', dann gilt also
$$\mathbb{Z}_{n\cdot n'} \simeq \mathbb{Z}_n \times \mathbb{Z}_{n'}.$$
Das bedeutet: Anstatt in $\mathbb{Z}_{nn'}$ rechnen zu müssen, können wir demnach auch in dem kartesischen Produkt der beiden Restklassenringe rechnen.

ii) Eine Anwendung in der *Analysis* ergibt sich bei der Untersuchung von Nullstellenvarietäten multivariater Polynome:

- Sind $f_0, \ldots, f_{m-1} \in \mathbb{K}[x_0, \ldots, x_{n-1}$ dann bezeichnen wir das von diesen Polynomen erzeugte Ideal mit

$$I(f_0, \ldots, f_{m-1}) := (f_0, \ldots, f_{m-1}).$$

- In der Analysis, genauer: in der algebraichen Geometrie, betrachtet man die zugehörigen polynomialen Funktionen

$$F_i \colon \mathbb{K}^n \to \mathbb{K}\,,\ (x_0, \ldots, x_{n-1}) \mapsto f_i(x_0, \ldots, x_{n-1})$$

  und die zugehörige Varietät

$$V(F_0, \ldots, F_{m-1}) := \{(x_0, \ldots, x_{n-1}) \mid \forall\, i \in m \colon F_i(x_0, \ldots, x_{n-1}) = 0\}.$$

- Man sieht ehr leicht, daß

$$(f_0, \ldots, f_{m-1}) = (g_0, \ldots, g_{l-1}) \Longrightarrow V(F_0, \ldots, F_{m-1}) = V(G_0, \ldots, G_{l-1}).$$

- Zur Varietät $V \subseteq \mathbb{K}^n$ betrachtet man das Ideal (nachprüfen!)

$$I(V) := \{f \in \mathbb{K}[x_0, \ldots, x_{n-1}] \mid \forall\, (x_0, \ldots, x_{n-1}) \in V \colon F(x_0, \ldots, x_{n-1}) = 0\}.$$

- Es gilt ganz offensichtlich

$$(f_0, \ldots, f_{m-1}) \subseteq I(V(f_0, \ldots, f_{m-1})),$$

  aber nicht immer Gleichheit, was allerhand Fragen aufwirft. Beispielsweise gilt

$$(x_0^2, x_1^2) \subset I(V(x_o^2, x_1^2)) = (x, y).$$

Man verwendet dabei insbesondere Gröbnerbasen, das sind Mengen von Polynomen, deren höchste Terme $HT(f_i)$ ein vorgegebenes Ideal erzeugen:

$$(HT(f_0), \ldots, HT(f_{m-1})) = (HT(I)),$$

wobei

$$HT(I) := \{\kappa x^\alpha \mid \exists\, f \in I \colon HT(f) = \kappa x^\alpha\}.$$

Diese Definition hängt allerdings von dem Verständnis ab, was mit *höchster Term* von f gemeint ist, es braucht die Vorgabe einer *Termordnung* (vgl. Übungsblatt). ◇

Besonders interessant sind die beiden folgenden Klassen von Idealen:

- $I \lhd R$ ist *maximales Ideal*, wenn I als Ideal maximal in R ist:

$$\forall\ I' \trianglelefteq R \colon\ [I \subset I' \Rightarrow I' = R]\,.$$

- $I \lhd R$ heißt *Primideal*, wenn $R\backslash I$ multiplikativ abgeschlossen ist, d.h.:

$$(R\backslash I, \cdot) \text{ ist nicht leere Halbgruppe.}$$

Für solche Ideale gilt, wie wir bereits wissen (3.8.10), der wichtige Satz:

- Ist R ein kommutativer Ring mit 1, $I \trianglelefteq R$, dann ist I
  - genau dann Primideal, wenn R/I Integritätsbereich ist,
  - genau dann maximales Ideal, wenn R/I ein Körper ist.

In kommutativen Ringen mit Einselement sind demnach maximale Ideale auch Primideale. In $\mathbb{Z}$ gilt auch die Umkehrung. In vielen Ringen ist das anders, dort klaffen diese Begriffe auseinander, was wiederum heißt, daß die maximalen Ideale und auch die Primideale als *verschiedene* Verallgemeinerungen des Primzahlbegriffs angesehen werden können.

Der gerade wiederholte Satz ist die strukturtheoretische Grundlage für die *Konstruktion von Integritätsbereichen und Zahlkörpern* — auf die wir noch genauer eingehen werden. Maximale Ideale in Polynomringen $\mathbb{K}[x]$ über Körpern $\mathbb{K}$ sind die von irreduziblen Polynomen f erzeugten Hauptideale (f). Alle Restklassenringe $\mathbb{K}[x]/(f)$ sind demnach Erweiterungskörper von $\mathbb{K}$. Wir werden zeigen, daß man auf diese Weise beispielweise alle endlichen Körper aus den sogenannten Primkörpern $\mathbb{Z}_p$, p eine Primzahl, *konstruieren* kann!

Die Existenz maximaler Ideale folgt — ähnlich wie die Existenz von Basen von Vektorräumen — mit dem Lemma von Zorn.

7.2 Ringe von Brüchen, Lokalisierung, Quotientenkörper

Wir verallgemeinern zunächst die Bildung von $\mathbb{Q}$ aus $\mathbb{Z}$ als Menge der Äquivalenzklassen von Brüchen ganzer Zahlen. Dazu bemerken wir, daß folgendes leicht nachgerechnet werden kann:

7.2.1 Satz *Ist $0 \neq R$ ein kommutativer Ring mit Eins und $N \subseteq R$ ein Teilmonoid von $(R^*, \cdot)$ (d. h. N ist multiplikativ abgeschlossen, also eine Unterhalbgruppe, und N enthält das Einselement von R), dann gilt:*

- *Folgende Relation auf $R \times N$ ist eine Äquivalenzrelation:*

$$(r,n) \sim (r',n') :\Longleftrightarrow \exists\, n'' \in N : n''(rn' - r'n) = 0.$$

- *Die Menge $[R \times N]_\sim$ der entsprechenden Äquivalenzklassen $[r,n]_\sim := [(r,n)]_\sim$, ist zusammen mit den Verknüpfungen*

$$[r,n]_\sim + [r',n']_\sim := [rn' + r'n, nn']_\sim$$

und

$$[r,n]_\sim \cdot [r',n']_\sim := [rr', nn']_\sim$$

ein kommutativer Ring mit dem Einselement $[n,n]_\sim$ und dem Nullelement $[0,n]_\sim$, sowie mit den additiven Inversen

$$-[r,n]_\sim = [-r,n]_\sim.$$

Die Teilmenge N heißt dabei die Nennermenge.

7.2.2 Beispiele Ist $R \neq 0$ ein kommutativer Ring mit Einselement, dann sind R^*, $E(R)$ und $R\backslash I$, für jedes Primideal I geeignete Nennermengen. Beispiele sind also $\mathbb{Z}^*$, $\{1,-1\}$, und $\mathbb{Z}\backslash(p)$, für Primzahlen p. ◇

7.2.3 Hilfssatz *N sei eine Nennermenge gemäß 7.2.1. Es gilt:*

- *Die Abbildung*

$$f : R \to [R \times N]_\sim\,,\ r \mapsto [rn,n]_\sim$$

ist ein Ringhomomorphismus mit $f(N) \subseteq E([R \times N]_\sim)$.

- *Ist R ein Integritätsbereich, dann ist f sogar injektiv, und wir haben eine Einbettung*

$$R \hookrightarrow [R \times N]_\sim\,,\ r \mapsto [rn,n]_\sim$$

von R. Wir können in diesem Fall das Element $[rn,n]_\sim$ durch r ersetzen. Die oben angegebene Äquivalenzrelation vereinfacht sich zu

$$(r,n) \sim (r',n') :\Longleftrightarrow\ rn' - r'n = 0,$$

das Element $[r,n]_\sim$ ist demnach durch den Bruch $\frac{r}{n}$ *ersetzbar. Der so aus $[R\times N]_\sim$ entstandene Ring heißt* Ring der Brüche *von R mit* Nennermenge *N. Wir bezeichnen ihn mit*

$$B(R,N).$$

Beweis:Übungsaufgabe.

Das bekannteste Beispiel ist natürlich

$$\mathbb{Q} := B(\mathbb{Z}, \mathbb{Z}^*),$$

der *Körper der rationalen Zahlen*. Die herausragende Eigenschaft dieses Ringes der Brüche ist seine Universalität (Übungsaufgabe):

7.2.4 Satz *Ist R ein Integritätsbereich, N eine Nennermenge in R, dann ist die Einbettung*

$$R \hookrightarrow B(R, N)$$

universell bzgl. der Klasse $\mathcal{F}$ der (Ring mit 1)-Homomorphismen von R in Ringe R' mit Einselement und der Eigenschaft $f(N) \subseteq E(R')$, sowie der Klasse $\mathcal{L}$ der Ring-mit-Eins-Homomorphismen.

7.2.5 Definition (lokale Ringe) Ein Ring R heißt *lokaler Ring*, wenn R genau ein maximales Ideal besitzt. •

7.2.6 Satz *Ist R ein Integritätsbereich, P ein Primideal in R, dann ist der Ring der Brüche*

$$B(R, R\backslash P)$$

ein lokaler Ring.

Beweis: Wir zeigen daß das Ideal (nachprüfen!)

$$I := \left\{ \frac{p}{n} \;\middle|\; p \in P, n \in R\backslash P \right\}$$

genau aus den Nichteinheiten von $B(R, R\backslash P)$ besteht:

a. $\frac{a}{n} \notin I \Rightarrow a \notin P \Rightarrow \frac{n}{a} \in B(R, R\backslash P) \Rightarrow \frac{a}{n}$ Einheit.

b. $I \ni \frac{p}{n}$ Einheit, etwa $\frac{p}{n} \cdot \frac{a}{n'} = 1 \Rightarrow \underbrace{pa}_{\in P} = \underbrace{nn'}_{\in R\backslash P}$, ein Widerspruch.

Als Menge aller Nichteinheiten ist dieses Ideal maximal. Umgekehrt besteht jedes maximale Ideal aus Nichteinheiten, liegt also in I und ist deshalb *gleich* I. □

7.2.7 Beispiel Der Ring der Brüche

$$B(\mathbb{Z}, \mathbb{Z}\backslash(p))$$

ist lokal, falls p eine Primzahl ist. ◇

7.2.8 Satz *Ist R Integritätsbereich, dann ist der Ring der Brüche*

$$B(R, R^*)$$

ein Körper, der sogenannte Quotientenkörper *von R.*

Beweis: Das Nullideal ist Primideal, also ist, nach 7.2.6, $B(R, R^*)$ lokal und dessen Nullideal ist maximal, enthält also alle Nichteinheiten. Demnach ist $B(R, R^*)$ Schiefkörper und wegen der Kommutativität auch ein Körper.

□

Das klassische Beispiel hierfür ist natürlich wieder

$$\mathbb{Q} := B(\mathbb{Z}, \mathbb{Z}^*),$$

der *Körper der rationalen Zahlen*. Ein weiteres Beispiel ist — für jeden Körper $\mathbb{K}$ — der *Körper*

$$\mathbb{K}(x) := B(\mathbb{K}[x], \mathbb{K}[x]^*)$$

der rationalen Funktionen in einer Unbestimmten x. Entsprechendes gilt für mehrere Variable $x_0, x_1, \ldots x_{n-1}$.

7.3 Euklidische Bereiche, Hauptideal- und Gaußbereiche

Wir wissen bereits, daß in Integritätsbereichen R eine Division mit Rest möglich ist, wenn dort eine *euklidische Norm* existiert, d.h. eine Abbildung $\delta\colon R^* \to \mathbb{N}$ mit

- $\forall\ r, s \in R^* :\ \delta(r) \leq \delta(rs)$,
- $\forall\ x \in R, y \in R^*\ \exists\ q, r \in R :\ [x = qy + r]\ \wedge\ [r = 0 \vee (\delta(r) < \delta(y))]$.

Der Ring R (genauer: das Paar (R, δ)) heißt dann *euklidischer Bereich*.

Eine euklidische Norm auf $\mathbb{Z}$ ist die Betragsfunktion

$$\delta :\ \mathbb{Z}^* \to \mathbb{N},\ z \mapsto |z|,$$

eine Norm auf dem Polynomring $\mathbb{K}[x]$ ist die Gradfunktion

$$\delta :\ \mathbb{K}[x]^* \to \mathbb{N},\ f \mapsto Grad(f).$$

Jeder euklidische Bereich ist ein Hauptidealbereich, denn jedes Element $0 \neq i \in I \trianglelefteq R$ ist durch jedes Element $\neq 0$ und von kleinster Norm teilbar! Demnach ist beispielsweise $\mathbb{Z}$ und jeder Polynomring $\mathbb{K}[x]$ über einem Körper ein Hauptidealring.

Als nächstes wollen wir zeigen, daß in Hauptidealbereichen so etwas wie die im wesentlichen eindeutige Zerlegung ganzer Zahlen in Primfaktoren existiert. Es sei aber gleich betont, daß es zwei wesentlich verschiedene Möglichkeiten gibt, den Begriff Primzahl zu verallgemeinern: Dazu wiederholen wir zunächst die folgenden beiden Bezeichnungen:

- r ist *assoziiert* zu s, wenn es eine Einheit $t \in E(R)$ gibt mit $rt = s$, und das wird wie folgt abgekürzt:

  $$r \sim s.$$

- r ist ein *echter* Teiler von s, wenn folgendes gilt:

  $$r \mid s\ \wedge\ r \notin E(R)\ \wedge\ r \not\sim s.$$

Die beiden Verallgemeinerungen des Begriffs Primzahl sind jetzt:

- r heißt *unzerlegbar*, wenn r weder 0 noch Einheit ist und keine echten Teiler besitzt.
- r heißt *prim*, wenn r weder 0 noch Einheit ist und

  $$r \mid st \Rightarrow [\ r \mid s\ \vee\ r \mid t\ ]$$

  richtig ist, d.h. r teilt mit einem Produkt auch mindestens einen Faktor.

Schließlich sei auch noch betont, daß, für $\emptyset \neq T \subseteq R$, die *Mengen* $\mathrm{ggT}\,(T)$ und $\mathrm{kgV}(T)$ wie folgt definiert wurden: $r \in ggT(T)$, in Worten: r ist *ein größter gemeinsamer Teiler* von T, wenn folgende beiden Bedingungen erfüllt sind:

- $\forall\ t \in T\colon r \mid t$.
- $\forall\ s \in R\colon [\ \forall\ t \in T\colon\ s \mid t\ ] \Rightarrow s \mid r$,

und die Elemente von T heißen genau dann *teilerfremd,* wenn

$$\mathrm{ggT}\,(T) = E(R).$$

$r \in \mathrm{kgV}(T)$, also r ist *ein kleinstes gemeinsames Vielfaches* von T, bedeute, daß

- $\forall\ t \in T\colon\ t \mid r$.
- $\forall\ s \in R\colon\ [\ \forall\ t \in T\colon\ t \mid s\ ] \Rightarrow r \mid s$.

In Integritätsbereichen sind Primelemente stets unzerlegbar. Und wir wissen bereits, daß in Hauptidealbereichen genau die Primelemente unzerlegbar sind. Wir hatten aber auch Beispiele von Integritätsbereichen, wie $\mathbb{K}[x,y] := \mathbb{K}[x][y]$ und $R := \{a + b\sqrt{-5} \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$, die *keine* Hauptidealbereiche sind.

7.3.1 Definition (Gaußbereich) R sei ein Integritätsbereich mit dem Element r und Nichteinheiten $r_0, \ldots, r_{m-1}$ sowie Nichteinheiten $s_0, \ldots, s_{n-1}$.

- r heißt *streng zerlegbar*, wenn gilt:

$$0 \neq r \notin E(R) \wedge\ r \text{ besitzt echte Teiler.}$$

- $\prod_{i\in m} r_i$ heißt *äquivalent* zu $\prod_{i\in n} s_i$ (kurz: $\prod_i r_i \approx \prod_i s_i$), wenn gilt:

$$m = n\ \wedge\ \exists\ \pi \in S_n\colon\ r_i \sim s_{\pi(i)}.$$

- R heißt *Gaußbereich*, wenn jedes streng zerlegbare Element bis auf Äquivalenz eindeutig als Produkt unzerlegbarer Elemente geschrieben werden kann.

•

Alle Körper sind Gaußbereiche, denn es gibt dort keine streng zerlegbaren Elemente. Unser Ziel ist der Beweis der Tatsache, daß alle Hauptidealbereiche Gaußbereiche sind.

7.3.2 Definition (Kettenbedingungen) Sei $(M, \leq)$ eine angeordnete Menge.

- $(M, \leq)$ genügt der *Maximal-* bzw. der *Minimalbedingung*, wenn jede nichtleere Teilmenge maximale bzw. minimale Elemente enthält.
- $(M, \leq)$ genügt der *Aufsteigende-Ketten-Bedingung* bzw. der *Absteigende-Ketten-Bedingung*, wenn alle aufsteigenden bzw. alle absteigenden Ketten von Elementen stationär werden.

•

7.3.3 Satz *Die Maximalbedingung ist äquivalent zur Aufsteigende-Ketten-Bedingung, die Minimalbedingung ist äquivalent zur Absteigende-Ketten-Bedingung.*

Beweis: Zu einer aufsteigenden Kette

$$m_0 \leq m_1 \leq \dots$$

betrachten wir $\cup_i \{m_i\}$. Gilt die Maximalbedingung, dann gibt es darin maximale Elemente, die Kette muß also stationär werden. Umgekehrt gibt es, wenn keine maximalen Elemente existieren, offensichtlich aufsteigende Ketten, die nicht stationär werden. Entsprechend argumentiert man bei absteigenden Ketten und der Minimalbedingung.

□

7.3.4 Satz *Ist R ein Hauptidealbereich, dann gilt die Aufsteigende-Ketten-Bedingung für die Menge $(\mathcal{I}, \subseteq)$ seiner Ideale.*

Beweis: Ist $I_0 \leq I_1 \leq \dots$ eine aufsteigende Kette von Idealen, dann ist die Vereinigung $I := \cup I_\nu$ ihrer Elemente ein Ideal. R ist Hauptidealbereich, es gibt also $i \in R$ mit $I = (i)$. Dieses i liegt in einem der I_ν, nach diesem Element bleibt die Kette demnach konstant.

□

7.3.5 Satz *Jeder Hauptidealbereich ist Gaußbereich.*

Beweis:

i) Wir beweisen zunächst die *Existenz* der Zerlegung streng zerlegbarer Elemente in unzerlegbare. Sei $r \in R$ streng zerlegbar, R ein Hauptidealbereich. Es gibt also echte Teiler r_0 von r, etwa $r = r_0 r_1$, r_1 ist dann ebenfalls echter Teiler. Wir haben also die beiden Ketten

$$(r) \subset (r_0) \subset R,\ (r) \subset (r_1) \subset R.$$

Der Teiler r_0 von r ist nun entweder unzerlegbar oder streng zerlegbar, in welchem Falle $r_0 = r_{00} r_{01}$ gilt, mit echten Teilern, also insgesamt

$$(r) \subset (r_0) \subset (r_{00}) \subset R,\ (r) \subset (r_0) \subset (r_{01}) \subset R$$

usw., und entsprechend mit r_1. Nun ist aber R ein Hauptidealbereich, so daß (nach 7.3.4) all diese Ketten stationär werden. Die jeweils vorletzten Kettenglieder sind von unzerlegbaren Faktoren von r erzeugt, und das Produkt dieser endlich vielen (!) Faktoren ergibt r.

ii) Um noch die Äquivalenz dieser Faktorisierungen nachzuweisen, betrachten wir zwei Zerlegungen

$$r = p_0 \cdots p_s = q_0 \cdots q_t$$

von r in unzerlegbare Elemente aus R. Da die unzerlegbaren Faktoren auch prim sind, gibt es j mit $p_0 \mid q_j$. Nun ist aber R kommutativ, demnach können wir ohne Einschränkung annehmen, daß $j = 0$ gilt, also, weil auch q_0 unzerlegbar ist,

$$p_0 \sim q_0, \text{ etwa } q_0 = e \cdot p_0, \text{ mit } e \in E(R).$$

Es folgt

$$r' = p_1 \cdots p_s = (e \cdot q_1) \cdots q_t.$$

Ist $s = 1$, dann folgt $t = 1$, und wir sind fertig. Andernfalls argumentieren wir mit p_1 wie oben mit p_0 und erhalten schließlich per Induktion, daß $s = t$ gilt und die beiden Faktorisierungen äquivalent sein müssen.

□

7.3.6 Folgerung *Ist $\mathbb{K}$ ein Körper, dann ist $\mathbb{K}[x]$ ein Gaußbereich.*

Wir haben also insgesamt die folgende Kette von Implikationen (mit den Abkürzungen EB für Euklidischer Bereich, HIB für Hauptidealbereich, GB für Gaußbereich, IB für Integritätsbereich):

7.3.7 Satz *Für Integritätsbereiche R gelten die folgenden Implikationen:*

$$EB(R) \Rightarrow HIB(R) \Rightarrow GB(R) \Rightarrow IB(R).$$

Keine dieser Implikationen ist umkehrbar, das sieht man an:

7.3.8 Beispiele

- Die Menge $\{a + b(\frac{1+\sqrt{-19}}{2}) \mid a, b \in \mathbb{Z}\}$ ist ein Hauptidealbereich, aber kein Euklidischer Bereich. (s. T. Motzkin, *Bull. Amer. Math. Soc.* **55** (1949), 1142-1146)
- Der Polynomring $\mathbb{K}[x, y] := \mathbb{K}[x][y]$ ist ein Gaußbereich (s.u.), aber kein Hauptidealbereich (s. 3.8.11).
- $\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ist ein Integritätsbereich, aber kein Gaußbereich:

  $$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

  die Darstellung als Produkt unzerlegbarer Elemente ist also nicht bis auf Äquivalenz eindeutig (s. 3.8.11).

◇

7.3.9 Satz *In Gaußbereichen sind genau die primen Elemente unzerlegbar.*

Beweis: Primelemente sind unzerlegbar, das haben wir bereits gesehen. Die Umkehrung folgt (indirekter Beweis) so: Sei r unzerlegbar und Teiler von $s \cdot t$, etwa $r \cdot p = s \cdot t$. Nehmen wir an, $r \nmid s$ und $r \nmid t$. Da R Gaußbereich ist, existieren Zerlegungen $s \cdot t = \prod r_i$ und $r \cdot p = r \prod p_i$ in unzerlegbare Elemente, und es gilt: $r \nmid r_i$, also $r \not\sim r_i$, und damit $r \prod p_i \not\approx \prod r_i$, ein Widerspruch.

□

7.3.10 Satz *Sind r, s Elemente eines Gaußbereichs R mit Produktdarstellungen*

$$r \sim \prod_{i=1}^{m} p_i^{m_i},\ s \sim \prod_{i=1}^{m} p_i^{n_i},\ p_i \text{ unzerlegbar},$$

dann besitzen diese Elemente größte gemeinsame Teiler und kleinste gemeinsame Vielfache, es gilt nämlich

$$\prod_{i=1}^{m} p_i^{\min\{m_i,n_i\}} \in ggT(r,s),\ \prod_{i=1}^{m} p_i^{\max\{m_i,n_i\}} \in kgV(r,s).$$

Insgesamt gilt also

$$ggT(r,s) = E(R) \cdot \prod_{i=1}^{m} p_i^{\min\{m_i,n_i\}}$$

und

$$kgV(r,s) = E(R) \cdot \prod_{i=1}^{m} p_i^{\max\{m_i,n_i\}}.$$

Beweis: Übungsaufgabe.

□

7.3.11 Definition (primitive Polynome) Ist R Integritätsbereich, so heißt $f \in R[x]$ genau dann *primitiv*, wenn $Grad(f) > 0$ und die Menge der gemeinsamen Teiler *aller* Koeffizienten von f die Einheiten sind, d.h. wenn

$$E(R) = \text{ggT}\,\{\text{Koeffizienten von } f\}.$$

•

7.3.12 Hilfssatz *Ist R ein Integritätsbereich, $f \in R[x]$ und $r \in R$, dann gilt:*

- $r \mid f \iff r$ *teilt jeden Koeffizienten.*
- $f \in E(R[x]) \iff f \in E(R)$.
- *Ist R Gaußbereich, $Grad(f) > 0$, dann gibt es ein primitives Polynom $g \in R[x]$ und $s \in R$ mit $f = sg$.*
- *Ist $f = r_1 g_1 = r_2 g_2$ mit $r_i \in R$ und primitiven g_i, dann gilt $r_1 \sim r_2$ und $g_1 \sim g_2$.*

Beweis: Übungsaufgabe.

7.3.13 Hilfssatz *Ist R Gaußbereich, dann sind Produkte primitiver Polynome in $R[x]$ primitiv.*

Beweis: Übungsaufgabe.

7.3.14 Satz *Ist R ein Gaußbereich, $\mathbb{K} = B(R, R^*)$ der Quotientenkörper, $f \in R[x]$ primitiv, dann gilt:*

$$f \text{ unzerlegbar in } \mathbb{K}[x] \iff f \text{ unzerlegbar in } R[x].$$

Beweis:

i) Sei $f \in R[x]$ in $\mathbb{K}[x]$ unzerlegbar, es gebe also keinen Teiler $g \in \mathbb{K}[x]$ von f mit $0 < Grad(g) < Grad(f)$. Jeder echte Teiler t von f in $R[x]$ ist also vom Grad 0: $t \in R$. Da f nach Voraussetzung primitiv ist, und t alle Koeffizienten teilt, gilt $t \in E(R)$, d.h. f ist auch in $R[x]$ unzerlegbar.

ii) Sei jetzt f unzerlegbar in $R[x]$ und Produkt $f = gh$ zweier Polynome in $\mathbb{K}[x]$, die echte Teiler seien. Da $\mathbb{K}$ der Quotientenkörper von R ist, gibt es $a, b \in R^*$ mit $ag, bh \in R[x]$. Es gibt demnach primitive $h_1, g_1 \in R[x]$ mit

$$abf = abgh = a_1 b_1 g_1 h_1.$$

Nach 7.3.13 ist deren Produkt $g_1 h_1$ primitiv. Weil f als primitiv vorausgesetzt ist, folgt $f \sim g_1 h_1$, in $R[x]$. Es ergibt sich

$$g_1 \mid f \wedge 0 < Grad(g) = Grad(g_1) < Grad(f).$$

Dies impliziert aber den Widerspruch, g_1 sei ein echter Teiler von f in $R[x]$.

□

7.3.15 Hilfssatz *Ist R Gaußbereich mit Quotientenkörper $\mathbb{K}$ und primitiven Polynomen $f, g \in R[x]$, so gilt*

$$f \sim g \text{ in } R[x] \iff f \sim g \text{ in } \mathbb{K}[x].$$

Beweis:

i) Ist $f \sim g$ in $\mathbb{K}[x]$, etwa $f = eg, e \in E(\mathbb{K}[x]) = \mathbb{K}^*$, dann gibt es $s, t \in R^*$ mit $e = s/t$, also $tf = sg$, was $f \sim g$ impliziert, in $R[x]$.

ii) Die Umkehrung ist trivial.

□

7.3.16 Satz *Polynomringe über Gaußbereichen sind ebenfalls Gaußbereiche.*

Beweis:

i) Ist R Gaußbereich, dann ist R mindestens Integritätsbereich. Bezeichnen wir mit $\mathbb{K}$ den Quotientenkörper, dann ist $\mathbb{K}[x]$ Hauptidealbereich, also Gaußbereich.

ii) Wir beweisen zunächst die *Existenz* von Faktorisierungen streng zerlegbarer Polynome f in unzerlegbare.

1. Sei f ein *primitives* streng zerlegbares Polynom in $R[x]$. Wegen 7.3.14 ist es auch in $\mathbb{K}[x]$ streng zerlegbar, und es gelte dort:

   $$f = \overline{p_1} \cdots \overline{p_s},$$

   mit unzerlegbaren $\overline{p_i}$. Wir wählen $a_i \in R^*$ mit $a_i\overline{p_i} \in R[x]$ und dann $b_i \in R^*$ mit

   $$a_i\overline{p_i} = b_i p_i \in R[x], p_i \text{ primitiv.}$$

   Es gilt dann, für $a := \prod a_i, b := \prod b_i$:

   $$af = bp_1 \cdots p_s.$$

   Nun sind aber auch die p_i unzerlegbar in $\mathbb{K}[x]$. Da sie primitiv sind, sind diese Polynome nach 7.3.14 auch unzerlegbar in $R[x]$. Nach 7.3.13 ist auch deren Produkt primitiv. Da f zu diesem Produkt in $\mathbb{K}[x]$ assoziiert ist, gilt das auch in $R[x]$, nach 7.3.15. Demnach ist f selbst Produkt unzerlegbarer Polynome aus $R[x]$.

2. Sei $f \in R[x]$ jetzt *irgendein* streng zerlegbares Polynom in $R[x]$. Wir unterscheiden zwei Fälle:

   a) Ist $f \in R$, dann gibt es, da R Gaußbereich ist, unzerlegbare a_i mit $f = a_1 \cdots a_h$. Eine solche Zerlegung ist in R bis auf Äquivalenz eindeutig, also auch in $R[x]$. Bei $f \in R$ gilt also die Behauptung.

   b) Ist $f \notin R$, dann gibt es $d \in R^*$ mit $f = dg$ und einem primitiven $g \in R[x]$. Wie unter 1. ergeben sich Zerlegungen $g = p_1 \cdots p_s,\ d = d_1 \cdots d_h$, also auch Faktorisierungen von f:

   $$f = d_1 \cdots d_h p_1 \cdots p_s.$$

iii) Zum Beweis der *Äquivalenz* zweier solcher Zerlegungen betrachten wir

$$f = d_1 \cdots d_h p_1 \cdots p_s = e_1 \cdots e_k q_1 \cdots q_t,$$

mit unzerlegbaren $d_i, e_i \in R$, und unzerlegbaren $p_i, q_i \in R[x]\backslash R$, von denen wir ohne Einschränkung annehmen können, sie seien zusätzlich auch primitive Polynome. Es gilt dann

$$d_1 \cdots d_h \sim e_1 \cdots e_k, \text{ in } R.$$

Da R Gaußbereich ist, impliziert dies die Äquivalenz dieser beiden Produkte. Die Produkte $d_1 \cdots d_h$ und $e_1 \cdots e_k$ sind dann auch in $R[x]$ äquivalent, insbesondere gilt $h = k$.
Auch die polynomialen Faktoren $p_1 \cdots p_s$ und $q_1 \cdots q_t$ sind assoziiert in $R[x]$, also auch in $\mathbb{K}[x]$, dies ist aber ein Gaußbereich, also sind sie dort sogar äquivalent, und insbesondere gilt $s = t$. Geeignete Paare sind also assoziiert in $\mathbb{K}[x]$, nach 7.3.15 auch assoziiert in $R[x]$, so daß diese beiden Produkte sogar in $R[x]$ äquivalent sind. Insgesamt ergibt sich daraus die Äquivalenz der beiden Faktorisierungen von f.

□

Wiederholte Anwendung dieses Satzes ergibt

7.3.17 Folgerung *Ist R ein Gaußbereich, $n \in \mathbb{N}$, dann ist der Polynomring*

$$R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$$

ein Gaußbereich.

7.3.18 Unzerlegbarkeitskriterien *Sei R ein Integritätsbereich, dann gilt im Polynomring $R[x]$:*

- *Die linearen Polynome $f = r + sx, s \in E(R)$, sind sämtlich unzerlegbar.*
- *Für alle $r \in R$ ist $f(x) \in R[x]$ genau dann unzerlegbar, wenn $f(x + r)$ unzerlegbar ist.*
- *Ist R sogar Gaußbereich, $f \in R[x]$ primitiv, dann ist f, als Polynom über $\mathbb{K} = B(R, R^*)$, genau dann unzerlegbar, wenn f auch über R unzerlegbar ist.*
- *Ist $R = \mathbb{Z}$, $f \in \mathbb{Z}[x]$ primitiv und unzerlegbar über $\mathbb{Z}_p$ (genauer: $\overline{f}$, das aus f durch Reduktion der Koeffizienten modulo p hervorgeht) und teilt p den Leitkoeffizienten nicht, dann ist f auch in $\mathbb{Z}[x]$ unzerlegbar.*
- Kriterium von Eisenstein: *Ist R Gaußbereich, $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ primitives Polynom, $p \in R$ ein Primelement, für das in R gilt:*

  $$p \nmid a_n, p \mid a_{n-1}, p \mid a_{n-2}, \ldots, p \mid a_0, p^2 \nmid a_0,$$

  dann ist f über R unzerlegbar.

Beweis: Das Eisensteinkriterium zeigen wir indirekt: Ist $f = \sum a_i x^i = gh$, mit $g = \sum b_i x^i, h = \sum c_i x^i$, dann teilt p entweder b_0 nicht oder c_0 nicht, o.E. $p \nmid c_0$. Da p kein Teiler von a_n ist, gibt es einen kleinsten Index i mit $p \nmid b_i$. Nun ist aber

$$a_i = b_i c_0 + (b_{i-1} c_1 + \ldots + b_0 c_i),$$

wobei p den eingeklammerten Summanden auf der rechten Seite teilt, aber nicht $b_i c_0$, also auch nicht a_i. Damit ist $i = n$, und der Grad von h ist Null. Da f als primitiv vorausgesetzt war, ist $h \in E(R)$.

□

Das Eisensteinkriterium veranlaßt uns zu folgender

7.3.19 Definition (irreduzible Polynome) Ein Polynom $f \in R[x]^*$, R Gaußbereich, heißt *irreduzibel*, wenn für $g, h \in R[x]$ gilt:

$$[f = gh \;\Rightarrow\; Grad(g) = 0 \;\vee\; Grad(h) = 0]$$

•

Im Falle, daß f primitiv oder R ein Körper ist, sind Unzerlegbarkeit und Irreduzibilität gleichwertig.

7.3.20 Beispiele

- $f(x) := 2+4x+6x^2+4x^3+x^4 = (x+1)^4+1$ ist über $\mathbb{Z}$ unzerlegbar nach dem Eisensteinkriterium, damit ist y^4+1 unzerlegbar über $\mathbb{Q}$.
- $f := -135 + 17x - 8x^2 + x^3$ ergibt, modulo $p = 2$, das Polynom $\overline{f} = 1 + x + x^3 \in \mathbb{Z}_2[x]$, das dort unzerlegbar ist, denn eine Zerlegung müßte einen Linearfaktor enthalten, $1 + x + x^3$ also eine Nullstelle besitzen, was offensichtlich nicht der Fall ist. Also ist $f \in \mathbb{Z}[x]$ irreduzibel.
- Mit Hilfe einer Kombination des Eisensteinkriteriums mit dem Transformationskriterium ergibt sich auch die Unzerlegbarkeit der wichtigen *Kreisteilungspolynome*

  $$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1 \in \mathbb{Z}[x],$$

  für Primzahlen p. Denn

  $$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-1}$$

  ist unzerlegbar nach dem Eisensteinkriterium.

$\diamond$

7.4 Zerlegung von Ringen und Moduln

Die Struktur eines Ringes R wirkt sich auch auf die Struktur von R-Moduln aus, insbesondere gewisse direkte Zerlegung von R in Ideale. Zu deren Beschreibung dienen insbesondere Ringelemente der folgenden Form:

7.4.1 Definition (Idempotente) *Idempotente* in R sind die Elemente $e \in R$ mit

$$0 \neq e = e^2.$$

Sie heißen *zentral,* wen sie im *Zentrum* von R liegen, d. h. wenn $er = re$, für alle $r \in R$. Zwei Idempotente $e, f \in R$ heißen *orthogonal,* wenn

$$ef = fe = 0.$$

•

Demnach gilt für Idempotente e und alle $n \in \mathbb{N}^* : e^n = e \neq 0$. Idempotenten stehen deshalb diejenigen $r \in R$ gegenüber, für die es $n \in \mathbb{N}^*$ gibt mit $r^n = 0$, solche Elemente heißen *nilpotent.*

7.4.2 Beispiele

i) In einem Ring R mit Einselement ist mit einem Idempotent e auch $1-e$ ein Idempotent, und diese beiden Idempotente sind orthogonal. Sie ergeben eine direkte Zerlegung von R in Linksideale, die sogenannte *Piercesche Zerlegung*

$$R = Re \oplus R(1-e).$$

ii) Ist $n > 1$ eine natürliche Zahl mit Primfaktorzerlegung

$$n = \prod_{i=1}^{r} p_i^{a_i}$$

(also $p_i \neq p_j$, für $i \neq j$, und $a_i > 0$), dann sind die Quotienten $n_i := n/p_i^{a_i}$, $i = 1, \ldots, r$ teilerfremd, es gibt also $z_i \in \mathbb{Z}^*$ mit

$$\sum_{i=1}^{r} n_i z_i = 1.$$

Die Restklassen dieser Summanden in $\mathbb{Z}_n$, also die

$$\bar{e_i} := n_i z_i + (n) \in \mathbb{Z}_n$$

sind orthogonale Idempotente: Die Orthogonalität folgt aus der Teilbarkeit von $n_i n_j$ durch n. Die Idempotenz ergibt sich aus der Tatsache, daß die $\bar{e_i}$ eine *Zerlegung der Eins* ergeben:

$$\bar{1} = \sum_i \bar{e_i},$$

denn hieraus folgt durch Multiplikation mit $\bar{e_j}$ und mit der Orthogonalität: $\bar{e_j} = \bar{e_j}^2$.

iii) Dreiecksmatrizen mit Nullen auf der Hauptdiagonalen sind nilpotent.

iv) In Integritätsbereichen ist nur das Einselement idempotent und nur das Nullelement nilpotent.

◇

Das letzte Beispiel läßt sich leicht verallgemeinern: Jede Zerlegung $1 = \sum_i e_i$ der Eins in paarweise orthogonale Idempotente ergibt eine direkte Zerlegung von R in Linksideale:

7.4.3 $$R = \oplus_i Re_i.$$

Wenn die Idempotente zusätzlich noch zentral sind ergibt sich daraus ein sehr wichtiges Resultat über Zerlegungen von R-Moduln:

7.4.4 Satz *R sei ein Ring mit 1, $1 = \sum_i e_i$ eine Zerlegung der Eins in zentrale und paarweise orthogonale Idempotente, M ein R-Linksmodul. Dann gilt:*

- *Aus der Zerlegung der Eins des Ringes ergibt sich eine eine direkte Zerlegung von M in R-Linksmoduln:*

  $$_RM = \oplus_i e_iM.$$

  (Entsprechendes gilt natürlich für Rechtsmoduln!)

- *Das zweiseitige Ideal $Re_i = e_iRe_i$ ist ein Unterring von R mit Einselement e_i, es gilt*

  $$R = \oplus_i e_iRe_i.$$

- *e_iM ist ein e_iRe_i-Linksmodul. Jede direkte Zerlegung*

  $$e_iM = L_1 \oplus \ldots \oplus L_k$$

  von e_iM in e_iRe_i-Untermoduln L_j kann als Zerlegung in R-Untermoduln aufgefaßt werden.

Beweis:

i) Wegen $re_im = e_irm$ ist e_iM ein Untermodul. Die Summe $\sum_i e_iM$ dieser Untermoduln ist $M : m = 1m = \sum_i e_im$, und sie ist direkt: $0 = \sum_i e_im_i$ ergibt, durch Multiplikation von links mit e_j, daß $0 = e_jm_j$.
ii) e_iRe_i ist additiv und multiplikativ abgeschlossen, also Unterring. e_i ist offenbar das Einselement, und die angegebene direkte Zerlegung folgt unmittelbar aus 7.4.3.
iii) Die L_j sind, nach Definition, e_iRe_i-Untermoduln. Sie sind aber auch R-Untermoduln, bzw. können als solche aufgefaßt werden. Jedes $l \in L_j$ ist ja von der Form e_im, so daß wegen der Orthogonalität folgt

$$rl = re_im = \big(\sum_\nu re_\nu\big)e_im = \big(\sum_\nu e_\nu re_\nu\big)e_im = e_ire_ie_im = e_ire_il \in L_j.$$

Die Setzung $rl := (e_i r e_i)l$ definiert also eine $R-$Linksmodulstruktur auf L_j. □

Die Isomorphiesätze übertragen sich von Gruppen auf Moduln, wenn man "Normalteiler" durch "zulässige Normalteiler", d.h. durch "Untermoduln" ersetzt. Es gilt vor allem

7.4.5 Der Satz von Jordan und Hölder *Besitzt ein R-Linksmodul Kompositionsreihen, dann sind diese paarweise äquivalent.*

7.4.6 Beispiele

i) Kompositionsreihen n-dimensionaler Vektorräume V sind von der Form

$$V = V_0 > V_1 > \ldots > V_n = 0,$$

mit $\dim(V_i) = n - i$.

ii) Ist R ein euklidischer Bereich, $p \in R$ prim, dann ist

$$R/(p^n) \supset (p)/(p^n) \supset (p^2)/(p^n) \supset \ldots \supset (p^{n-1})/(p^n) \supset (p^n)/(p^n) = 0$$

die einzige Kompositionsreihe des Faktorrings $R/(p^n)$. Um das einzusehen, betrachtet man den kanonischen Epimorphismus

$$\nu_{(p^n)}: r \mapsto r + (p^n),$$

von R auf den Faktorring. Ein Ideal I im Faktorring ist Bild eines Ideals J aus R, welches (p^n) umfaßt. R ist Hauptidealring, es gibt also $q \in R$ mit $J = (q)$. Ist jetzt p^m die maximale Potenz von p, die in q aufgeht (R ist Gaußbereich!), also $q \sim p^m$, und damit $I = (p^m)/(p^n)$.

iii) Dagegen besitzen Moduln, die direkte Summe $M = M_1 \oplus M_2$ von nicht trivialen Untermoduln M_i sind, mehr als eine Kompositionsreihe, da andernfalls $M \supset M_1 \supset 0$ und $M \supset M_2 \supset 0$ eine gemeinsame Verfeinerung besitzen müßten, was nicht sein kann, da keiner dieser Untermoduln im anderen liegt. ◇

Wir heben Moduln mit eindeutig bestimmter Kompositionsreihe hervor, sie sollen *einreihig* heißen. Moduln, die von einem Element erzeugt werden, also $M = {}_R\langle m\rangle = Rm$, nennen wir *zyklisch.* Unser Ziel ist der Beweis der Tatsache, daß jeder endlich erzeugbare R-Linksmodul M *direkte Summe von zyklischen Untermoduln* ist, wenn die beiden Moduln ${}_RR$ und R_R einreihig sind. Der Beweis erfolgt über zwei Hilfssätze:

7.4.7 Hilfssatz *Ist R ein Ring mit Eins und besitzt ${}_RR$ Kompositionsreihen, dann auch jeder zyklische $R-$Linksmodul Rm.*

Bewei: Rm ist isomorph $R/\mathrm{Kern}(\nu)$, wenn ν der folgende $R-$Epimorphismus ist:

$$\nu: R \to Rm\,,\ r \mapsto rm.$$

Als Faktormodul von R besitzt Rm mit ${}_RR$, nach 6.6.14, Kompositionsreihen. (Der Kern des $R-$Homomorphismus ν ist übrigens das Ordnungsideal $\mathrm{Ord}(m)$.) □

7.4.8 Hilfssatz *Ist R ein Ring mit Einselement, M ein endlich erzeugbarer $R-$Linksmodul, ${}_RR$ und R_R einreihig, dann gibt es $n \in \mathbb{N}, m_i \in M, i \in n$, mit*

$$M = \bigoplus_{i \in n} Rm_i.$$

Beweis:

i) Wir zeigen, daß diese Bedingung von jedem Erzeugendensystem $\{m_i \mid i \in n\}, n \in \mathbb{N}$, erfüllt wird, für das die Summe $\sum_i l(Rm_i)$ der Längen $l(Rm_i)$ der Kompositionsreihen der erzeugten zyklischen Moduln *minimal* ist. Ist ein solches Erzeugendensystem $\{m_i \mid i \in n\}$ gegeben und gilt $0 = \sum_i r_i m_i$, dann ist zu zeigen, daß alle $r_i m_i = 0$. Wir führen einen indirekten Beweis.

ii) Nehmen wir also an, es gäbe Indizes i mit $r_i m_i \neq 0$. Weil R_R einreihig ist, gibt es ein größtes Rechtsideal $r_i R$ zu diesen Koeffizienten r_i mit $r_i m_i \neq 0$, und wir können ohne Einschränkung der Allgemeinheit annehmen, dieses sei $r_0 R$. In $r_0 R$ liegen alle r_i mit $r_i m_i \neq 0$, es gibt demnach $q_i \in R$ mit $r_0 q_i = r_i$, falls $r_i m_i \neq 0$. Sei $q_0 = 1$ und noch $q_i := 0$ gesetzt, falls $r_i m_i = 0$. Wir haben dann

$$0 = \sum_{i=0}^{n-1} r_i m_i = r_0 \Big(m_0 + \sum_{i=1}^{n-1} q_i m_i \Big) =: r_0 m_0'.$$

iii) Wir führen jetzt einen Widerspruch herbei durch Nachweis von $l(Rm_0') < l(Rm_0)$. Dazu betrachten wir die kanonischen Epimorphismen ν bzw. ν' von ${}_RR$ auf Rm_0 bzw. auf Rm_0'. Wegen der Einreihigkeit von ${}_RR$ liegt einer der beiden Kerne im anderen. Weil $r_0 m_0 \neq 0$, aber $r_0 m_0' = 0$, gilt, haben wir demnach

$$\mathrm{Ord}(m_0) = \mathrm{Kern}(\nu) \subset \mathrm{Kern}(\nu') = \mathrm{Ord}(m').$$

Es folgt $l(\mathrm{Ord}(m_0)) < l(\mathrm{Ord}(m_0'))$ und damit

$$l(Rm_0') = l({}_RR) - l(\mathrm{Ord}('_0)) < l({}_RR) - l(\mathrm{Ord}(m_0)) = l(Rm_0).$$

Da, mit $\{m_0, m_1, \ldots, m_{n-1}\}$ auch $\{m_0', m_1, \ldots, m_{n-1}\}$ Erzeugendensystem ist:

$$m_0 = m_0' - \sum_{i=1}^{n-1} q_i m_i,$$

nach der Definition von m_0', steht also $l(Rm_0') < l(Rm_0)$ im Widerspruch zur angenommenen Minimalität der Längensumme $\sum l(Rm_i)$. Es muß also auch $r_i m_i = 0$ gelten.

□

7.4.9 Folgerung *Ist R ein Ring mit Einselement, und sind die beiden Moduln ${}_RR$ und R_R einreihig, dann ist jeder endlich erzeugbare R-Linksmodul M direkte Summe von zyklischen, also einreihigen, Untermoduln.*

□

7.5 Abelsche Gruppen, Normalform von Matrizen

Wie wir bereits gesehen haben, kann man solche direkten Zerlegungen, deren Existenz in 7.4.9 nachgewiesen wurde, ggf. aus Zerlegungen der Eins in zentrale orthogonale Idempotente bekommen. Es folgen zwei sehr wichtige Anwendungsbeispiele. Interessant ist insbesondere, daß die Herleitungen der beiden Resultate im wesentlichen die gleichen Argumente verwenden!

7.5.1 Der Hauptsatz über endliche abelsche Gruppen *Jede endliche abelsche Gruppe ist direkte Summe zyklischer Untergruppen von Primzahlpotenzordnung.*

Beweis: $(A,+)$ seieine endliche abelsche Gruppe, $n := |A| > 1$. A ist, wie bereits erwähnt, ein $\mathbb{Z}$-Modul,

$$za := \begin{cases} a+\ldots+a, & z\text{-mal, falls } z \geq 0, \\ -a-\ldots-a, & (-z)\text{-mal, falls } z < 0. \end{cases}$$

Wegen $na = 0$ kann A auch als $\mathbb{Z}_n$-Modul aufgefaßt werden, vermöge

$$\bar{z}a := za, \text{ falls } \bar{z} = z + (n) \in \mathbb{Z}_n, 0 \leq z < n.$$

Nun sei wieder $n = \prod_i p_i^{a_i}$ die Primfaktorzerlegung von n, $n_i := n/p_i^{a_i}$, $z_i \in \mathbb{Z}^*$ mit $\sum_i n_i z_i = 1$, $e_i := n_i z_i$, $\bar{e_i} := e_i + (n) \in \mathbb{Z}_n$. Wie oben bereits diskutiert, sind die $\bar{e_i}$ zentrale orthogonale Idempotente, die eine Zerlegung der Eins in $\mathbb{Z}_n$ bilden, $\sum_i \bar{e_i} = \bar{1}$, und wir erhalten daraus direkte Zerlegungen $\mathbb{Z}_n = \oplus_i \bar{e_i}\mathbb{Z}_n$ sowie

$$A = \oplus_i e_i A = \oplus_i \bar{e_i} A.$$

Die erste der beiden direkten Summen ist eine Zerlegung von A als $\mathbb{Z}$-Modul, die zweite ist eine Zerlegung von A als $\mathbb{Z}_n$-Modul. Die Summanden sind dabei, als Teilmengen von A, gleich: $e_i A = \bar{e_i} A$.
Die $e_i A$ sind sogar $\mathbb{Z}_{p_i^{a_i}}$-Moduln, denn $p_i^{a_i} e_i A = n z_i A = 0$. Die Ringe $\mathbb{Z}_{p_i^{a_i}}$ sind einreihig, nach 7.4.9 ist also $e_i A$ eine direkte Summe zyklischer Untermoduln. Diese haben, als Faktormoduln von $\mathbb{Z}_{p_i^{a_i}}$, als Ordnung eine Potenz von p_i.

□

Analog verläuft der Beweis von

7.5.2 Die Jordansche Normalform einer quadratischen Matrix *Jede quadratische Matrix endlicher Reihenzahl über einem algebraisch abgeschlossenen Zahlkörper kann auf Blockdiagonalgestalt transformiert werden, wobei die Blöcke die folgende Form haben*

$$\begin{pmatrix} \lambda & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda \end{pmatrix},$$

mit einem Eigenwert λ der betrachteten Matrix.

Beweis: A sei eine $n \times n$-matrix über $\mathbb{K}$, einem algebraisch abgeschlossenen Körper (d. h. jedes Polynom in $\mathbb{K}[x]$ zerfällt in Linearfaktoren.

i) Der Vektorraum $\mathbb{K}^n$ wird zu einem $\mathbb{K}[x]$-Modul, wenn wir die Operation eines Polynoms $\sum_i \kappa_i x^i$ als Anwendung der linearen Abbildung definieren, die durch Einsetzen der Matrix in das Polynom entsteht:

$$\big(\sum_i \kappa_i x^i\big) \cdot v := \sum_i \kappa_i A^i \cdot v.$$

ii) Ist jetzt E_j der j-te Einheitsvektor, $0 \leq j \leq n-1$, dann hat (aus Dimensionsgründen) der Epimorphismus

$$\mathbb{K}[x] \to \mathbb{K}[x]E_j\ ,\ \big(\sum_i \kappa_i x^i\big) \mapsto \big(\sum_i \kappa_i x^i\big) \cdot E_j = \sum_i \kappa_i A^i \cdot E_j$$

einen nicht trivialen Kern, also ein Ideal, das von einem normierten Polynom vom Grad > 0 erzeugt wird. Es folgt

$$\mathbb{K}[x]E_j \simeq \mathbb{K}[x]/(q_j).$$

iii) Der Vektorraum $\mathbb{K}^n$ wird vom Produkt $q = q_0 \cdots q_{n-1}$ der diese Kerne erzeugenden Polynome q_i annulliert und kann deshalb als $\mathbb{K}[x]/(q)$-Modul aufgefaßt werden. Ist jetzt $q = \prod_i p_i^{a_i}$ die Primfaktorzerlegung von q, mit normierten unzerlegbaren und paarweise verschiedenen Polynomen p_i, dann erhalten wir — ganz wie im Beweis des Hauptsatzes über abelsche Gruppen — aus den teilerfremden $r_i := q/p_i^{a_i}$ eine Zerlegung der Eins:

$$1 = \sum_i r_i s_i,\ \ s_i \in \mathbb{K}[x]^*.$$

Die Restklassen $\bar{e_i}$ der Summanden e_i, also

$$\bar{e_i} := r_i s_i + (q),$$

sind zentrale orthogonale Idempotente mit

$$\mathbb{K}^n = \oplus_i \bar{e_i}\mathbb{K}^n = \oplus_i e_i \mathbb{K}^n,$$

sowie $\bar{e_i}\mathbb{K}^n = e_i\mathbb{K}^n$.
Der Unterraum $e_i\mathbb{K}^n$ ist $\mathbb{K}[x]/(p_i^{a_i})$-Modul also Modul über einem einreihigen Ring und deshalb Summe von Unterräumen U_{ij}, die zyklische $\mathbb{K}[x]/(p_i^{a_i})$-Moduln sind, d. h. isomorph zu Faktormoduln nach den Idealen dieses Rings:

$$U_{ij} = \mathbb{K}[x]u_{ij} \simeq \mathbb{K}[x]/(p_i^{a_i})/(p_i^{b_{ij}})/(p_i^{a_i}) \simeq \mathbb{K}[x]/(p_i^{b_{ij}}).$$

Insgesamt haben wir also die folgende Zerlegung von $\mathbb{K}^n$ als direkte Summe erhalten:

$$\mathbb{K}^n = \oplus_i \oplus_j \mathbb{K}[x]u_{ij}.$$

Es bleibt die Wirkung der Matrix A auf Basen dieser Unterräume $\mathbb{K}[x]u_{ij}$ zu berechnen.
Wir verwenden dazu die Voraussetzung, daß $\mathbb{K}$ algebraisch abgeschlossen ist, die unzerlegbaren Polynome, insbesondere auch die p_i, sind also linear: $p_i = x - \lambda_i$, für ein geeignetes $\lambda_i \in \mathbb{K}$. Die Potenzen p_i^k, $0 \leq k \leq b_{ij} - 1$, bilden also eine Basis von $\mathbb{K}[x]/(p_i^{b_{ij}}) \simeq U_{ij}$. Es gilt also

$$U_{ij} = \ll u_{ij}, p_i u_{ij}, p_i^2 u_{ij}, \ldots, p_i^{b_{ij}-1} u_{ij} \gg .$$

Wir brauchen jetzt nur noch zu bemerken, daß

$$A p_i^k u_{ij} = x p_i^k u_{ij} = \lambda_i p_i^k u_{ij} + p_i^{k+1} u_{ij},$$

Die Matrix der Einschränkung von A auf den Unterraum U_{ij} hat also wirklich die Form

$$\begin{pmatrix} \lambda_i & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda_i \end{pmatrix}.$$

Dabei zeigt die letzte Spalte dieser Matrix, daß λ_i tatsächlich ein Eigenwert von A ist.

□

Kapitel 8

Aus der Körpertheorie

Wir kommen jetzt — nach der Einführung in die Ringtheorie — zu einer Einführung in die Körpertheorie. Die Schilderung der Grundbegriffe dieser Theorie wird mit dem Ziel betrieben, ein paar der klassischen Probleme aus der griechischen Geometrie zu behandeln, deren Lösung die Entwicklung dieser Theorie benötigte und deshalb erst in den letzten beiden Jahrunderten gelungen ist. Es sind dies insbesondere die folgenden Probleme aus der Theorie der von den Griechen seit dem siebten Jahrundert vor Christus entwickelten Geometrie der *Konstruktionen mit Zirkel und Lineal:*

- Sind beliebige Winkel auf diese Weise, das heißt unter ausschließlicher Zuhilfenahme von Zirkel und Lineal, drittelbar?
- Kann man einen vorgegebenen Würfel verdoppeln, d. h. aus einer vorgegebenen Strecke der Länge r mit ausschließlicher Hilfe von Zirkel und Lineal eine Strecke der Länge $\sqrt[3]{2} \cdot r$ konstruieren?
- Ist die Quadratur des Kreises möglich, d.h. kann man aus einer vorgegebenen Strecke r eine Strecke der Länge $r\sqrt{\pi}$ mit Zirkel und Lineal konstruieren, also die Seitenlänge eine Quadrats mit dem Flächeninhalt $\pi \cdot r^2$?

8.1 Primkörper, Körpererweiterungen

Körper sind insbesondere Ringe, wir erinnern uns deshalb zunächst an einige wichtige Begriffe aus der Ringtheorie. Ist R ein Ring mit Eins, dann heißt $\mathrm{Char}(R) := |\langle 1_R \rangle|$, also die Ordnung der von der Eins erzeugten Untergruppe der additiven Gruppe von R, die *Charakteristik* von R. Ist diese nicht endlich, dann spricht man oft, anstelle von Charakteristik ∞, von Charakteristik 0, denn die Charakteristik definiert man oft auch als den nicht negativen Erzeuger des Kerns von

$$f_R \colon \mathbb{Z} \to R\,,\ z \mapsto z \cdot 1_R.$$

Einen Unterschied macht das genau dann, wenn f_R injektiv ist; dann ergibt sich bei der ersten Definition ∞ als Charakteristik, im anderen Fall 0. Ist R ein Integritätsbereich, dann ist seine Charakteristik 0 (bzw. ∞) oder eine Primzahl. Ist T ein Teilring von R (also auch $1_T = 1_R$), dann hat T dieselbe Charakteristik wie R.

8.1.1 Definition (Primkörper) Ist $\mathbb{K}$ ein Körper, dann heißt der kleinste Teilkörper $P_{\mathbb{K}}$, also

$$P_{\mathbb{K}} := \bigcap_{\mathbb{L} \leq \mathbb{K}} \mathbb{L},$$

der *Primkörper* von $\mathbb{K}$. •

Ein wichtiges Beispiel ist $\mathbb{Q}$, ein Körper, der sein eigener Primkörper ist (denn $P_{\mathbb{Q}}$ enthält $\mathbb{Z}$ und $\mathbb{Q} = B(\mathbb{Z}, \mathbb{Z}^*)$, der Quotientenkörper von $\mathbb{Z}$):

$$\mathbb{Q} = P_{\mathbb{Q}} = P_{\mathbb{R}} = P_{\mathbb{C}}.$$

8.1.2 Satz *Ist $\mathbb{K}$ ein Körper, dann hat $\mathbb{K}$ entweder die Charakteristik 0 oder p, mit einer Primzahl p. Dementsprechend ist der Primkörper $P_{\mathbb{K}}$ von $\mathbb{K}$ entweder isomorph zu $\mathbb{Q}$ oder zu $\mathbb{Z}_p$.*

Beweis: Die Abbildungen $f_{\mathbb{Q}}$ bzw $f_{\mathbb{Z}_p}$ sind universell bzgl. der Klassen

$$\mathcal{F}_0 := \{f_{\mathbb{K}} \mid \mathrm{Char}(\mathbb{K}) = 0\},$$

bzw.

$$\mathcal{F}_p := \{f_{\mathbb{K}} \mid \mathrm{Char}(\mathbb{K}) = p\},$$

sowie der Klasse $\mathcal{L}$ der Körpermonomorphismen. $\mathbb{K}$ enthält also entweder $\mathbb{Q}$ oder $\mathbb{Z}_p$.
Enthält $\mathbb{K}$ den Körper $\mathbb{Z}_p$, dann ist p die Charakteristik. Sie muß eine Primzahl sein, denn andernfalls gäbe es Nullteiler. □

8.1.3 Definition (Erweiterungskörper, Zwischenkörper, Körpergrad) Sind $\mathbb{K}, \mathbb{L}$ und $\mathbb{M}$ Körper, dann heißt

- $\mathbb{L}$ *Erweiterungskörper* von $\mathbb{K}$, wenn $\mathbb{K}$ Teilkörper von $\mathbb{L}$ ist (ganz genau ist ein Erweiterungskörper eigentlich ein Paar $(\mathbb{L}, \epsilon)$, mit einem Monomorphismus $\epsilon \colon \mathbb{K} \to \mathbb{L}$.) Wir schreiben dafür auch kurz $\mathbb{L} : \mathbb{K}$, und wir identifizieren $\mathbb{K}$ mit $\epsilon(\mathbb{K})$.

- $\mathbb{M}$ heißt *Zwischenkörper* von $\mathbb{L} : \mathbb{K}$, wenn gilt $\mathbb{K} \leq \mathbb{M} \leq \mathbb{L}$.
- Als *Grad* der Körpererweiterung $\mathbb{L} : \mathbb{K}$ bezeichnen wir die $\mathbb{K}$–Dimension von $\mathbb{L}$:
$$[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}}(\mathbb{L}).$$
Dementsprechend unterscheiden wir *endliche* und *unendliche* Körpererweiterungen.

•

8.1.4 Beispiele Bekannte Beispiele von Körpererweiterungen bzw. von Zwischenkörpern sind:

- Der Körper $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$ der komplexen Zahlen ist ein Erweiterungskörper des Körpers $\mathbb{R}$ der reellen Zahlen:
$$\epsilon\colon \mathbb{R} \to \mathbb{C}\,,\ a \mapsto a + 0 \cdot i.$$
Ganz analog ergibt sich die Körpererweiterung $\mathbb{C} : \mathbb{Q}$.
- $\mathbb{R}$ ist Zwischenkörper von $\mathbb{C} : \mathbb{Q}$, und für die Grade gilt:
$$[\mathbb{R} : \mathbb{Q}] = \infty,\ [\mathbb{C} : \mathbb{R}] = 2.$$
(Die erste Gleichung gilt, weil andernfalls $\mathbb{R}$ abzählbar wäre.)
- Jeder endliche Körper $\mathbb{K}$ hat einen endlichen Primkörper, also einen Primkörper isomorph $\mathbb{Z}_p$, mit $p := char(\mathbb{K})$. $\mathbb{K}$ ist zudem endliche Erweiterung seines Primkörpers und hat deshalb die Ordnung p^n, für geeignetes $n \in \mathbb{N}^*$.

◇

8.1.5 Der Gradsatz *Ist* $\mathbb{K} \leq \mathbb{M} \leq \mathbb{L}$ *und* $[\mathbb{L} : \mathbb{K}] \in \mathbb{N}$*, dann gilt:*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}].$$

Beweis: Wir wissen, daß — nach dem Lemma von Zorn — jeder Vektorraum Basen besitzt. Sei etwa

$$\mathbb{L} =_{\mathbb{M}} \ll b_i \mid i \in \mathcal{I} \gg,\ \mathbb{M} =_{\mathbb{K}} \ll c_j \mid j \in \mathcal{J} \gg .$$

Die Menge
$$\{b_i c_j \mid i \in \mathcal{I}, j \in \mathcal{J}\}$$
ist linear unabhängig über $\mathbb{K}$: Sind nämlich I bzw. J endliche Teilmengen von $\mathcal{I}$ bzw. von $\mathcal{J}$, dann gilt

$$0 = \sum_{i \in I, j \in J} \kappa_{ij} b_i c_j = \sum_{i \in I} b_i \sum_{j \in J} \kappa_{ij} c_j.$$

Wegen der linearen Unabhängigkeit der b_i (über $\mathbb{M}$) ist $\sum_{j\in J}\kappa_{ij}c_j = 0$, wegen der Unabhängigkeit der c_j (über $\mathbb{K}$) ergibt sich daraus $\kappa_{ij} = 0$, für alle $i \in I, j \in J$.
Wegen der vorausgesetzten Endlichkeit der $\mathbb{K}-$Dimension von $\mathbb{L}$ sind demnach $\mathcal{I}$ und $\mathcal{J}$ endlich.
Die c_ib_j erzeugen $\mathbb{L}$, denn jedes $\lambda \in \mathbb{L}$ ist eine $\mathbb{M}-$Linearkombination der $b_i, i \in \mathcal{I}$, etwa $\lambda = \sum_i \mu_i b_i$, und jedes μ_i eine $\mathbb{K}-$Linearkombination der $c_j, j \in \mathcal{J}$: $\mu_i = \sum_j \kappa_{ij}c_j$. Insgesamt folgt

$$\lambda = \sum_{i,j} \kappa_{ij} b_i c_j.$$

Die $\mathbb{K}-$Dimension von $\mathbb{L}$ ist also $|\mathcal{I}| \cdot |\mathcal{J}| = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}]$, wie behauptet.

□

8.1.6 Definition Für Teilmengen $T \subseteq \mathbb{L}$ und Erweiterungen $\mathbb{L} : \mathbb{K}$ bezeichnen wir als den *von T erzeugten Teilkörper* den kleinsten Zwischenkörper, der T enthält:

$$\mathbb{K}(T) := \bigcap_{\mathbb{M}:T\subseteq\mathbb{M}\leq\mathbb{L},\mathbb{K}\leq\mathbb{M}} \mathbb{M}.$$

Statt $\mathbb{K}(\{t\})$ schreiben wir kurz $\mathbb{K}(t)$, Zwischenkörper dieser Form heißen *einfache* Erweiterungen. •

Das Standardbeispiel für eine einfache Erweiterung ist $\mathbb{C} = \mathbb{R}(i)$. Leicht nachzuweisen ist, daß für sukzessives Erweitern folgendes gilt:

8.1.7 $$(\mathbb{K}(T_0))(T_1) = (\mathbb{K}(T_1))(T_0) = \mathbb{K}(T_0 \cup T_1) =: \mathbb{K}(T_0, T_1).$$

8.1.8 Definition (Polynomfunktion, Wurzel) Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung.

- Zu $f = \sum a_i x^i \in \mathbb{K}[x]$ ist

  $$F\colon \mathbb{L} \to \mathbb{L}\,,\ \lambda \mapsto \sum_i a_i \lambda^i$$

  die *zugehörige Polynomfunktion.*

- Unter einer *Wurzel* von f versteht man eine Nullstelle von F, also ein $\lambda \in \mathbb{L}$ mit $F(\lambda) = 0$.

•

Es sei erneut daran erinnert, daß die Zuordnung $f \mapsto F$ im allgemeinen nicht injektiv ist, daß also f nicht immer aus F rekonstruiert werden kann. Z.B. ist über $\mathbb{Z}_2$ die Polynomfunktion zu $f_1 = x^2 + x$ wie die zu $f_2 = 0$ die Nullfunktion! Polynomfunktionen und Polynome müssen also streng auseinandergehalten werden! Der folgende Satz über die Existenz von Wurzeln in Erweiterungskörpern ermöglicht gleichzeitig die Konstruktion derartiger Erweiterungen und ist von entsprechend großer Bedeutung:

8.1.9 Satz *Ist $\mathbb{K}$ ein Körper, $f \in \mathbb{K}[x]$ mit $Grad(f) > 0$, dann ist gibt es Erweiterungskörper $\mathbb{L} : \mathbb{K}$, in denen f Wurzeln besitzt.*

Beweis: Da $\mathbb{K}[x]$ Gaußbereich ist, gibt es Polynome g, h mit $f = gh$ und h irreduzibel. (h) ist maximales Ideal, $\mathbb{L} := \mathbb{K}[x]/(h)$ also ein Körper. Die Einschränkung der natürlichen Abbildung $\nu_{(h)}$ auf $\mathbb{K}$, also

$$\nu_{(h)} \downarrow \mathbb{K} \colon \mathbb{K} \to \mathbb{K}[x]/(h)$$

ist injektiv, denn h ist nicht konstant. $\mathbb{L} = \mathbb{K}[x]/(h)$ ist also ein Erweiterungskörper von $\mathbb{K}$. Außerdem gilt, wenn $f = \sum_i a_i x^i$,

$$\sum a_i (\nu_{(h)}(x))^i = \nu_{(h)}(f) = \nu_{(h)}(gh) = 0_{\mathbb{K}[x]/(h)}.$$

$\nu_{(h)}(x)$ ist demnach eine Nullstelle von F. □

8.1.10 Folgerung *Ist $\mathbb{K}$ ein Körper, $f \in \mathbb{K}[x]$, $Grad(f) > 0$, und $f = gh$ mit einem irreduziblen $h \in \mathbb{K}[x]$, dann ist die Restklasse $\nu_{(h)}(x)$ eine Wurzel von f in dem Erweiterungskörper $\mathbb{L} := \mathbb{K}[x]/(h)$.*

8.1.11 Beispiele Der Übergang von einem Körper $\mathbb{K}$ zu einem Erweiterungskörper $\mathbb{K}[x]/(h)$ ist ein wichtiges Konstruktionsverfahren, wie die folgenden Beispiele zeigen:

- Das Polynom $1+x^2 \in \mathbb{R}[x]$ ist irreduzibel, der Körper $\mathbb{R}[x]/(1+x^2)$ enthält also Wurzeln von $1 + x^2$. Man rechnet leicht nach, daß

  $$\varphi \colon \mathbb{R}[x]/(1 + x^2) \to \mathbb{C}\,,\ a + bx + (1 + x^2) \mapsto a + bi$$

  ein Isomorphismus ist (dabei ist i das Bild von $x + (1 + x^2)$).

- Das Polynom $1 + x + x^2 \in \mathbb{Z}_2[x]$ ist ebenfalls irreduzibel, hat also eine Wurzel in $\mathbb{Z}_2[x]/(1 + x + x^2)$, einem Körper, der aus 4 Elementen besteht:

  $$\mathbb{Z}_2[x]/(1 + x + x^2) = \{\overline{0}, \overline{1}, \overline{x}, \overline{1 + x}\},$$

  wobei die folgende Abkürzung benutzt wurde: $\overline{f} := f + (1 + x + x^2)$.

◇

8.2 Ring- und Körperadjunktion

8.2.1 Definition (Ringadjunktion, Körperadjunktion) Sei jetzt $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung.

- Als *Einsetzung* von $\lambda \in \mathbb{L}$ oder auch als *Auswertung* an der Stelle λ bezeichnen wir den Ringhomomorphismus

$$\varphi_{\mathbb{K},\lambda}\colon \mathbb{K}[x] \to \mathbb{L}\,,\ f \mapsto F(\lambda).$$

- Sein Bild heißt *Ringadjunktion* von λ an $\mathbb{K}$:

$$\mathbb{K}[\lambda] := \varphi_{\mathbb{K},\lambda}(\mathbb{K}[x]) \simeq \mathbb{K}[x]/\mathrm{Kern}(\varphi_{\mathbb{K},\lambda}).$$

- Unter der *Körperadjunktion* von λ an $\mathbb{K}$ verstehen wir die bereits erwähnte einfache Körpererweiterung

$$\mathbb{K}(\lambda) = \bigcap_{\mathbb{M}:\lambda\in\mathbb{M},\mathbb{K}\leq\mathbb{M}\leq\mathbb{L}} \mathbb{M}.$$

•

Mit Hilfe dieser Begriffe werden nun die Elemente einer Körpererweiterung in die zwei Klassen der algebraischen und der transzendenten Elemente eingeteilt:

8.2.2 Definition (algebraisch, transzendent, Minimalpolynom) Sei wieder $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, $\lambda \in \mathbb{L}$.

- Ist $Kern(\varphi_{\mathbb{K},\lambda}) \neq 0$, dann heißt λ *algebraisch*, andernfalls *transzendent* über $\mathbb{K}$. In Worten: λ ist genau dann algebraisch über $\mathbb{K}$, wenn es in $\mathbb{K}[x]$ Polynome mit λ als Wurzel gibt.

- Ist λ algebraisch, dann heißt das eindeutig bestimmte normierte Polynom kleinsten Grades $f_{\mathbb{K},\lambda}$, das λ als Wurzel hat, *Minimalpolynom* von λ. Der Grad dieses (irreduziblen) Polynoms heißt auch der *Grad* von λ:

$$Grad(\lambda) := Grad(f_{\mathbb{K},\lambda}).$$

- $\mathbb{L} : \mathbb{K}$ heißt *algebraische Erweiterung*, falls alle $\lambda \in \mathbb{L}$ algebraisch sind, andernfalls heißt sie *transzendente* Erweiterung.

•

8.2.3 Beispiele

- $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, $f_{\mathbb{R},i} = 1 + x^2$.

- $\mathbb{K}(x) = B(\mathbb{K}[x], \mathbb{K}[x]^*)$ heißt der *Körper der rationalen Funktionen über* $\mathbb{K}$, $x \in \mathbb{K}(x)$ ist transzendent über $\mathbb{K}$.

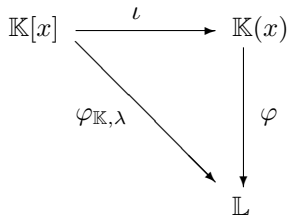
- $e, \pi \in \mathbb{R} : \mathbb{Q}$ sind transzendent, der Beweis übersteigt allerdings den momentanten Stand der Vorlesung.

$\diamond$

8.2.4 Satz *Sei $\lambda \in \mathbb{L}$ transzendent, $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung. Dann gilt:*

- $\mathbb{K}(\lambda) \simeq \mathbb{K}(x)$,
- $[\mathbb{K}(\lambda) : \mathbb{K}] = \infty$,
- $\lambda^n,\ n > 0$, *ist ebenfalls transzendent über* $\mathbb{K}$,
- $\mathbb{K}(\lambda) \supset \mathbb{K}(\lambda^2) \supset \mathbb{K}(\lambda^4) \supset \ldots$ *ist eine unendliche Kette, die nicht stationär wird.*

Beweis:
i) Die Einbettung $\iota : \mathbb{K}[x] \hookrightarrow \mathbb{K}(x)$ ist universell bzgl. der Klasse $\mathcal{F}$ der Einsetzungshomomorphismen $\varphi_{\mathbb{K},\lambda}$ und der Klasse $\mathcal{L}$ der Körpermonomorphismen. Es gibt demnach genau einen Homomorphismus φ, der folgendes Diagramm kommutativ ergänzt:



Diese Abbildung φ ist ein Körpermonomorphismus und hat als Bild gerade $\mathbb{K}(\lambda)$.

ii) Die Potenzen $1, \lambda, \lambda^2, \ldots$ von λ sind linear unabhängig, denn andernfalls gäbe es ein Polynom f mit $F(\lambda) = 0$.

iii) Wäre λ^n algebraisch, dann gäbe es a_i mit $\sum_i a_i \lambda^{n \cdot i} = 0$, also ein Polynom mit Wurzel λ.

iv) Die Ungleichung $\mathbb{K}(\lambda^2) \leq \mathbb{K}(\lambda)$ ist klar. Gleichheit ergäbe $\lambda \in \mathbb{K}(\lambda^2)$, also existierten nach i) $f \in \mathbb{K}[x],\ g \in \mathbb{K}[x]^*$ mit $\lambda \cdot G(\lambda^2) = F(\lambda^2)$. Ist $f = \sum a_i x^i$ und $g = \sum b_i x^i$, dann würde also gelten

$$\sum b_i \lambda^{2i+1} = \sum a_i \lambda^{2i}.$$

Mit ii) ergäbe das $f = g = 0$, im Widerspruch zu $g \in \mathbb{K}[x]^*$.

$\square$

8.2.5 Folgerung *Der Körper $\mathbb{K}(x)$ der rationalen Funktionen über $\mathbb{K}$ ist im wesentlichen die einzige einfache transzendente Erweiterung von $\mathbb{K}$.*

8.2.6 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine Körpererweiterung,* $\lambda \in \mathbb{L}$ *algebraisch, dann gilt:*

- $\text{Kern}(\varphi_{\mathbb{K},\lambda}) = (f_{\mathbb{K},\lambda})$,
- $\mathbb{K}(\lambda) = \mathbb{K}[\lambda]$,
- $[\mathbb{K}(\lambda) : \mathbb{K}] = [\mathbb{K}[\lambda] : \mathbb{K}] = Grad(f_{\mathbb{K},\lambda})$,
- $\mathbb{K}[\lambda] = \mathbb{K}(\lambda) =_{\mathbb{K}} \ll 1, \lambda, \ldots, \lambda^{Grad(\lambda)-1} \gg$.

Beweis:
i) $f_{\mathbb{K},\lambda}$ liegt im Kern von $\varphi_{\mathbb{K},\lambda}$ und ist das normierte Polynom kleinsten Grades mit dieser Eigenschaft, erzeugt also dieses Ideal.

ii) $\mathbb{K}[\lambda]$ ist isomorph zu $\mathbb{K}[x]/(f_{\mathbb{K},\lambda})$, also Körper. Als Körper zwischen $\mathbb{K}$ und $\mathbb{K}(\lambda)$ ist er, wegen der Minimalität von $\mathbb{K}(\lambda)$ gleich diesem.

iii) Die Potenzen $1, \lambda, \ldots, \lambda^{Grad(\lambda)-1}$ sind linear unabhängig, denn $f_{\mathbb{K},\lambda}$ ist ein Polynom mit *minimalem Grad* und λ als Wurzel. Wegen

$$\mathbb{K}(\lambda) = \mathbb{K}[\lambda] \simeq \mathbb{K}[x]/(f_{\mathbb{K},\lambda})$$

gilt aber auch $[\mathbb{K}(\lambda) : \mathbb{K}] = \text{Grad}(f_{\mathbb{K},\lambda})$, insgesamt ergibt das die beiden letzten Punkte der Behauptung.

□

Zusammen mit 8.2.4 ergibt das die folgende wichtige Äquivalenz:

8.2.7 Folgerung *Für Körpererweiterungen* $\mathbb{L} : \mathbb{K}$ *gilt:*

$$\lambda \in \mathbb{L} : \mathbb{K} \text{ algebraisch} \iff [\mathbb{K}(\lambda) : \mathbb{K}] \in \mathbb{N}.$$

8.2.8 Satz

- $[\mathbb{L} : \mathbb{K}] \in \mathbb{N} \Longrightarrow \mathbb{L} : \mathbb{K}$ *algebraisch.*
- $[\mathbb{L} : \mathbb{K}] \in \mathbb{N} \iff \exists\, \lambda_i \in \mathbb{L}\colon \lambda_i$ *algebraisch* $\wedge\, \mathbb{L} = \mathbb{K}(\lambda_0, \ldots, \lambda_{n-1})$.

Beweis:
i) Ist $[\mathbb{L} : \mathbb{K}]$ endlich, dann gilt, wegen 8.1.5, für jedes $\lambda \in \mathbb{L}$:

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L}\colon \mathbb{K}(\lambda)][\mathbb{K}(\lambda)\colon \mathbb{K}],$$

also ist λ algebraisch nach 8.2.7.

ii) Ist $[\mathbb{L} : \mathbb{K}]$ endlich, dann gibt es eine endliche $\mathbb{K}$–Basis von $\mathbb{L}$, etwa

$$\mathbb{L} =_{\mathbb{K}} \ll \lambda_0, \ldots, \lambda_{n-1} \gg .$$

Diese λ_i erzeugen endliche Erweiterungen, sind also algebraisch, und sie erzeugen $\mathbb{L}$.

iii) Ist umgekehrt

$$\mathbb{L} = \mathbb{K}(\lambda_0, \ldots, \lambda_{n-1}),$$

mit algebraischen λ_i, die $\mathbb{L}$ erzeugen, dann ist jedes λ_i natürlich auch algebraisch über $\mathbb{K}(\lambda_0, \ldots, \lambda_{i-1})$, also (mit $\mathbb{K}(\emptyset) := \mathbb{K}$)

$$[\mathbb{L} : \mathbb{K}] = \prod_{i=0}^{n-1} [\mathbb{K}(\lambda_0, \ldots, \lambda_i) : \mathbb{K}(\lambda_0, \ldots, \lambda_{i-1})],$$

und damit endlich.

□

8.2.9 Hilfssatz *Ist* $\mathbb{L} = \mathbb{K}(\lambda)$ *eine einfache algebraische Erweiterung,* $\mathbb{K} \leq \mathbb{M} \leq \mathbb{L}$ *und* $f_{\mathbb{M},\lambda} = \sum_0^n a_i x^i$*, dann gilt*

$$\mathbb{M} = \mathbb{K}(a_0, \ldots, a_n).$$

D. h. der Zwischenkörper $\mathbb{M}$ *ist durch (die Koeffizienten von)* $f_{\mathbb{M},\lambda}$ *bestimmt.*

Beweis: Für $\mathbb{M}' := \mathbb{K}(a_0, \ldots, a_n) \leq \mathbb{M}$ gilt:

$$f_{\mathbb{M},\lambda} = f_{\mathbb{M}',\lambda}.$$

Das impliziert die Gleichheit der Grade der entsprechenden Erweiterungen:

$$[\mathbb{M}(\lambda) : \mathbb{M}] = [\mathbb{M}'(\lambda) : \mathbb{M}'].$$

Nun gilt aber $\mathbb{L} = \mathbb{K}(\lambda) = \mathbb{M}(\lambda) = \mathbb{M}'(\lambda)$, also folgt nach dem Gradsatz die Gleichheit

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M}' : \mathbb{K}],$$

was mit $\mathbb{M}' \subseteq \mathbb{M}$ die behauptete Identität von $\mathbb{M}$ und $\mathbb{M}'$ liefert.

□

8.2.10 Satz *Genau die einfachen algebraischen Körpererweiterungen besitzen nur endlich viele Zwischenkörper.*

Beweis:
i) Sei $\mathbb{L} : \mathbb{K}$ einfache algebraische Körpererweiterung, etwa $\mathbb{L} = \mathbb{K}(\lambda)$, $\mathbb{M}$ ein Zwischenkörper. Nach 8.2.9 ist dieser Zwischenkörper durch das Minimalpolynom von λ über $\mathbb{M}$ vollständig bestimmt. Dieses Minimalpolynom teilt aber das Minimalpolynom von λ über $\mathbb{K}$, und es gibt nur endlich viele solcher normierten und unzerlegbaren Teiler.

ii) Sei jetzt umgekehrt $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung mit nur endlich vielen Zwischenkörpern $\mathbb{M}$. $\mathbb{L} : \mathbb{K}$ ist nach 8.2.4 (vierter Punkt) algebraisch, und jede Kette

$$\mathbb{K}(\lambda_0) \subseteq \mathbb{K}(\lambda_0, \lambda_1) \subseteq \ldots$$

wird stationär, es gibt also λ_i mit

$$\mathbb{K}(\lambda_0, \ldots, \lambda_m) = \mathbb{L}.$$

Es bleibt also zu zeigen, daß $\mathbb{K}(\lambda_0, \ldots, \lambda_m)$ eine *einfache* Erweiterung von $\mathbb{K}$ ist.

- Ist $\mathbb{K}$ ein endlicher Körper, dann ist, wegen $[\mathbb{L}:\mathbb{K}] \in \mathbb{N}$, $\mathbb{L}$ endlich. Weiter unten werden wir zeigen, daß also $\mathbb{L}^*$ zyklisch ist, d.h. von einem Element λ erzeugt wird (s. 9.1.2).

- Ist $\mathbb{K}$ unendlich, dann betrachten wir zu den $\kappa \in \mathbb{K}$ die Zwischenkörper

$$\mathbb{K}_\kappa := \mathbb{K}(\lambda_0 + \kappa\lambda_1).$$

  Von diesen können nur endlich viele verschieden sein. Da $\mathbb{K}$ unendlich ist, gibt es also $\kappa_1, \kappa_2 \in \mathbb{K}^*$ mit $\kappa_1 \neq \kappa_2$, aber $\mathbb{K}_{\kappa_1} = \mathbb{K}_{\kappa_2}$. Für diese gilt

$$\lambda_0 + \kappa_1\lambda_1 - (\lambda_0 + \kappa_2\lambda_1) = \lambda_1 \underbrace{(\kappa_1 - \kappa_2)}_{\neq 0} \in \mathbb{K}_{\kappa_2} \Rightarrow \lambda_1 \in \mathbb{K}_{\kappa_2},$$

$$\lambda_0 = \underbrace{(\lambda_0 + \kappa_2\lambda_1)}_{\in \mathbb{K}_{\kappa_2}} - \underbrace{\kappa_2\lambda_1}_{\in \mathbb{K}_{\kappa_2}} \Rightarrow \mathbb{K}(\lambda_0, \lambda_1) \leq \mathbb{K}_{\kappa_2}.$$

  Also ist $\mathbb{K}(\lambda_0, \lambda_1) = \mathbb{K}(\lambda_0 + \kappa_2\lambda_1)$, und durch Induktion zeigt man, daß auch $\mathbb{K}(\lambda_0, \ldots, \lambda_m)$ eine einfache Erweiterung ist.

□

8.2.11 Satz *Ist* $\mathbb{M}$ *ein Zwischenkörper von* $\mathbb{L} : \mathbb{K}$*, dann ist* $\mathbb{L} : \mathbb{K}$ *genau dann algebraisch, wenn dies sowohl für* $\mathbb{L} : \mathbb{M}$ *als auch für* $\mathbb{M} : \mathbb{K}$ *gilt.*

Beweis: Ist $\mathbb{L} : \mathbb{K}$ algebraisch, dann sind alle $\lambda \in \mathbb{L}$ algebraisch über $\mathbb{K}$ und damit erst recht über $\mathbb{M}$, also ist $\mathbb{L} : \mathbb{M}$ algebraisch, was natürlich auch für $\mathbb{M} : \mathbb{K}$ gilt. Sei umgekehrt $\lambda \in \mathbb{L}$ algebraisch über $\mathbb{M}$, etwa $f_{\mathbb{M},\lambda} = \sum_0^n a_i x^i$. Da auch $\mathbb{M} : \mathbb{K}$ als algebraisch vorausgesetzt wird, ist $\mathbb{M}' := \mathbb{K}(a_0, \ldots, a_n)$ eine endliche Erweiterung: $[\mathbb{M}' : \mathbb{K}] \in \mathbb{N}$. Wegen $f_{\mathbb{M},\lambda} \in \mathbb{M}'[x]$ ist λ auch über $\mathbb{M}'$ algebraisch, also $[\mathbb{M}'(\lambda) : \mathbb{M}'] \in \mathbb{N}$, insgesamt ist

$$[\mathbb{M}'(\lambda) : \mathbb{K}] = [\mathbb{M}'(\lambda) : \mathbb{M}'][\mathbb{M}' : \mathbb{K}] \ \in \mathbb{N}.$$

λ ist demnach auch über $\mathbb{K}$ algebraisch.

□

8.2.12 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine Körpererweiterung, dann ist auch*

$$\mathcal{A}(\mathbb{L} : \mathbb{K}) := \{\lambda \in \mathbb{L} \mid \lambda \textit{ algebraisch über } \mathbb{K}\}$$

ein algebraischer Erweiterungskörper von $\mathbb{K}$*. Dieser heißt* Körper der algebraischen Zahlen *von* $\mathbb{L} : \mathbb{K}$*.*

Beweis: Wir haben die Körpereigenschaften für $\mathcal{A}(\mathbb{L} : \mathbb{K})$ nachzuprüfen. Sind $\lambda_1, \lambda_2 \in \mathcal{A}(\mathbb{L} : \mathbb{K})$, dann liegen diese beiden Elemente in der algebraischen (vgl. 8.2.8) Erweiterung $\mathbb{K}(\lambda_1, \lambda_2)$, also auch deren Summe, Differenz, Produkt und Quotient (letzteres, falls $\lambda_2 \neq 0$) und sind deshalb algebraisch.

□

Im Spezialfall $\mathcal{A}(\mathbb{C} : \mathbb{Q})$ spricht man auch einfach von *dem* Körper der algebraischen Zahlen. Dieser ist abzählbar, es gibt also überabzählbar viele komplexe Zahlen, die transzendent über $\mathbb{Q}$ sind.

8.3 Konstruktionen mit Zirkel und Lineal

Eine Anwendung der Theorie der algebraischen Zahlkörper ist die Beantwortung der Frage, welche Strecken man in der Zeichenebene $\mathbb{R}^2$ ausschließlich mit Hilfe von Zirkel und (unmarkiertem) Lineal konstruieren kann.
Zur Präzisierung dessen, was hiermit gemeint ist, nehmen wir an, in der Zeichenebene $\mathbb{R}^2$ seien zwei Punkte gegeben, den einen identifizieren wir mit $(0,0)$, den anderen mit $(1,0)$. Es geht um die Frage, welche weiteren Punkte der Zeichenebene man in endlich vielen Schritten aus diesen beiden vorgegebenen Punkten konstruieren kann. Dabei sind folgende Schritte zur Konstruktion weiterer Punkte sind zugelassen:

- **Verwendung des Lineals:** Durch zwei vorgegebene oder bereits konstruierte Punkte kann man eine Gerade ziehen.

- **Benutzung des Zirkels:** Um einen vorgegebenen oder bereits konstruierten Punkt kann man einen Kreis mit der Länge einer zuvor bereits konstruierten Verbindungsstrecke als Radius schlagen.

Als *konstruierbare Punkte* bezeichnen wir Punkte von $\mathbb{R}^2$, die man in endlich vielen Schritten mit Hilfe dieser beiden Methoden erhalten kann. Neu hinzukommende Punkte sind also Schnittpunkte von Geraden mit Geraden, von Geraden mit Kreisen, oder auch von Kreisen mit Kreisen, ausgehend von den beiden vorgegebenen Punkten.
Die Konstruierbarkeit von Punkten der Zeichenebene formulieren wir zunächst um in die Konstruierbarkeit ihrer Koordinaten bzw. in die Konstruierbarkeit reeller Zahlen: Wir nennen die Zahl $r \in \mathbb{R}$ *konstruierbar*, wenn der Punkt $(r,0)$ auf die gerade beschriebene Weise konstruierbar ist. Es gilt natürlich:

8.3.1 $$r, s \in \mathbb{R} \text{ konstruierbar } \iff (r,s) \in \mathbb{R}^2 \text{ konstruierbar.}$$

Offenbar sind die natürlichen Zahlen konstruierbar, also auch die ganzen Zahlen und damit die rationalen Zahlen. Es gibt aber auch irrationale Zahlen, die leicht konstruiert werden können. Ein Beispiel ist $\sqrt{2}$, da $(0,1)$ und $(1,0)$ konstruierbar sind. Die Länge der Verbindungsstrecke dieser beiden Punkte ist nämlich $\sqrt{2}$. Allgemeiner kann man aus konstruiertem $r \in \mathbb{R}$ die Quadratwurzel $\sqrt{r}$ konstruieren.

8.3.2 Satz *Die konstruierbaren reellen Zahlen bilden einen Zwischenkörper von* $\mathbb{R} : \mathbb{Q}$.

Beweis: Die aus der Schule bekannten Konstruktionen für Summe, Differenz, Produkt und Quotienten zeigen die Abgeschlossenheit der Menge konstruierbarer $r \in \mathbb{R}$ gegenüber den arithmetischen Operationen, sie bilden demnach einen Körper. Daß dieser Körper $\mathbb{Q}$ enthält, ist oben bereits erwähnt worden.

□

8.3.3 Hilfssatz *Ist* $\mathbb{L}$ *der Zwischenkörper von* $\mathbb{R} : \mathbb{Q}$*, der die Koordinaten bereits konstruierter Punkte enthält, aus denen* r *bzw.* $(r, 0)$ *in* einem *Schritt konstruiert werden kann, dann gilt:*

$$r \in \mathbb{L}(\sqrt{s}),\ 0 \leq s \in \mathbb{L} \text{ geeignet.}$$

Beweis: Die Koordinaten von Schnittpunkten zweier Geraden sind Lösungen von linearen Gleichungen mit Koeffizienten in $\mathbb{L}$. Die Koordinaten von Schnittpunkten von Geraden mit Kreisen sind Lösungen von quadratischen Gleichungen mit Koeffizienten in $\mathbb{L}$, dies gilt auch für die Schnittpunkte von Kreisen mit Kreisen. Es bleibt deshalb nur noch zu bemerken, daß die Lösungen von $x^2 + px + q = 0$, mit $p, q \in \mathbb{L}$, bekanntlich die Zahlen

$$x_{1,2} = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}$$

sind, also von der Form $a + b\sqrt{s}$, mit $a, b, s \in \mathbb{L}$.

□

8.3.4 Satz *Eine reelle Zahl* r *ist genau dann konstruierbar, wenn es eine endliche Kette*

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_n \subseteq \mathbb{R}$$

von Zwischenkörpern von $\mathbb{R} : \mathbb{Q}$ *gibt mit*

$$\mathbb{K}_i = \mathbb{K}_{i-1}(\sqrt{r_i}),\ 0 \leq r_i \in \mathbb{K}_{i-1},$$

so daß insbesondere gilt:

$$r \in \mathbb{K}_n = \mathbb{Q}(\sqrt{r_1}, \ldots, \sqrt{r_n}).$$

Beweis:
i) Die Existenz einer solchen endlichen Kette von Zwischenkörpern folgt induktiv aus dem Hilfssatz 8.3.3.
ii) Haben wir umgekehrt eine Kette

$$\mathbb{Q} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \ldots \subseteq \mathbb{K}_{n-1} \subseteq \mathbb{K}_n \subseteq \mathbb{R},$$

mit $\mathbb{K}_i = \mathbb{K}_{i-1}(\sqrt{r_i})$ und $r_i \in \mathbb{K}_{i-1}$, so folgt (per Induktion nach n) aus der Konstruierbarkeit der Elemente von $\mathbb{K}_{i-1}$ die Konstruierbarkeit der Elemente von $\mathbb{K}_i$ wegen

$$\mathbb{K}_i = \{a + b\sqrt{r_i} \mid a, b \in \mathbb{K}_{i-1}\}.$$

$a + b\sqrt{r_i}$ ist konstruierbar, wenn a, b und r_i konstruierbar sind, denn $\sqrt{r_i}$ ist konstruierbar.

□

8.3.5 Folgerung

- *Ist $r \in \mathbb{R}$ konstruierbar, so liegt r in einem Zwischenkörper $\mathbb{K}$ von $\mathbb{R} : \mathbb{Q}$ mit $[\mathbb{K} : \mathbb{Q}] = 2^n$, für ein geeignetes $n \in \mathbb{N}$.*
- *Transzendente Zahlen (z.B. π) sind nicht konstruierbar (also ist insbesondere die "Quadratur des Kreises" nicht möglich: Die Strecke $\sqrt{\pi}$ ist* nicht konstruierbar*).*
- *Ist $r \in \mathbb{R}$ algebraisch und über $\mathbb{Q}$ von ungeradem Grad (wie z.B. $\sqrt[3]{2}$ mit dem Minimalpolynom $x^3 - 2$), dann ist r nicht konstruierbar und damit weder die Verdoppelung des Würfels ("Delisches Problem": konstruiere aus r die Strecke $r \cdot \sqrt[3]{2}$, deren dritte Potenz $2 \cdot r^3$ ist) noch die "Dreiteilung des Winkels" mit Zirkel und Lineal zu bewerkstelligen.*

Beweis: Die ersten beiden Behauptungen, und damit auch die Unlösbarkeit der Quadratur des Kreises, sind nach dem Vorangegangenen klar.
Die dritte Behauptung folgt aus der Tatsache, daß kein Zwischenkörper einer Erweiterung vom Grad 2^n einen ungeraden Grad haben kann. Das ergibt die Unlösbarkeit des Delischen Problems. Zur Dreiteilung des Winkels bemerken wir, daß $\cos 20^o$ nicht konstruierbar ist: Wegen $\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha$ gilt, für $a := \cos 20^o$:

$$4a^3 - 3a = \frac{1}{2},$$

a ist also Wurzel von $f := 8x^3 - 6x - 1$, einem irreduziblen Polynom, denn

$$f((x+1)/2) = x^3 + 3x^2 - 3$$

ist irreduzibel nach Eisenstein. Somit gilt $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. □

8.4 Zerfällungskörper, mehrfache Wurzeln

Wir haben bereits gesehen, daß es zu jedem $f \in \mathbb{K}[x]$ Erweiterungen $\mathbb{L} : \mathbb{K}$ gibt, in denen Wurzeln von f existieren. Es geht jetzt um Erweiterungen, in denen *alle* Wurzeln liegen:

8.4.1 Definition (Zerfällungskörper) Ist $f \in \mathbb{K}[x]$ vom Grad $n > 0$, dann heißt ein Erweiterungskörper $\mathbb{L}$ von $\mathbb{K}$ *Zerfällungskörper* von f über $\mathbb{K}$, wenn f dort in *Linearfaktoren* zerfällt, d. h. wenn es $\kappa \in \mathbb{K}$ und $\lambda_i \in \mathbb{L}$ gibt mit

$$f = \kappa \prod_{i=0}^{n-1} (x - \lambda_i),$$

und $\mathbb{L}$ minimal ist mit dieser Eigenschaft, also

$$\mathbb{L} = \mathbb{K}(\lambda_0, \ldots, \lambda_{n-1}).$$

•

Aus dem Satz über die Existenz von Erweiterungskörpern, die Wurzeln enthalten, ergibt sich induktiv:

8.4.2 Folgerung *Zu jedem $f \in \mathbb{K}[x]$ mit $n := Grad(f)$ gibt es Zerfällungskörper $\mathbb{L}$ mit $[\mathbb{L} : \mathbb{K}] \leq n!$.*

□

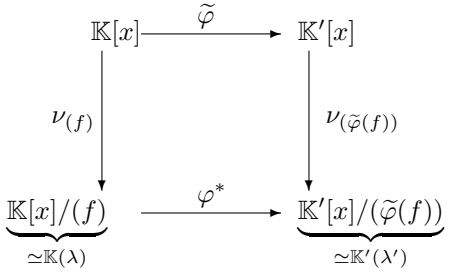
Jetzt soll bewiesen werden, daß Zerfällungskörper eines Polynoms im wesentlichen eindeutig bestimmt sind. Dazu zeigen wir vorbereitend:

8.4.3 Satz *Sind $\mathbb{K}, \mathbb{K}'$ Körper, $\varphi: \mathbb{K} \simeq \mathbb{K}'$ ein Isomorphismus, $\widetilde{\varphi}$ seine Erweiterung auf $\mathbb{K}[x]$, $f \in \mathbb{K}[x]$ irreduzibel, λ eine Wurzel von f in $\mathbb{L} : \mathbb{K}$, λ' eine Wurzel von $\widetilde{\varphi}(f)$ in $\mathbb{L}' : \mathbb{K}'$, dann gibt es eine Fortsetzung*

$$\varphi^*: \mathbb{K}(\lambda) \simeq \mathbb{K}'(\lambda')$$

mit $\varphi^*(\lambda) = \lambda'$.

Beweis: Wegen der Bijektivität von $\widetilde{\varphi}$ gibt es eine eindeutig bestimmte kommutative Ergänzung φ^* des folgenden Diagramms:



□

8.4.4 Folgerung *Ist $f \in \mathbb{K}[x]$ irreduzibel mit Wurzeln $\lambda_0, \lambda_1 \in \mathbb{L} : \mathbb{K}$, dann gibt es einen Isomorphismus $\varphi^*: \mathbb{K}(\lambda_0) \simeq \mathbb{K}(\lambda_1)$ mit $\varphi(\lambda_0) = \varphi(\lambda_1)$, der $\mathbb{K}$ elementweise fest läßt: $\varphi^*(\kappa) = \kappa$, für alle $\kappa \in \mathbb{K}$.*

□

Der nächste Schritt ist die Verallgemeinerung auf beliebige Polynome:

8.4.5 Satz *Ist $f \in \mathbb{K}[x]$ von positivem Grad, $\mathbb{L} : \mathbb{K}$ ein Zerfällungskörper von f, $\varphi: \mathbb{K} \simeq \mathbb{K}'$ und $\mathbb{L}' : \mathbb{K}'$ ein Zerfällungskörper von $\widetilde{\varphi}(f)$, dann gibt es eine Fortsetzung $\Phi: \mathbb{L} \simeq \mathbb{L}'$ von φ.*

Beweis: Induktion nach $[\mathbb{L} : \mathbb{K}]$.

i) $n = 1$: Wegen $\mathbb{L} = \mathbb{K}$ gibt es $\kappa, \kappa_i \in \mathbb{K}$ mit $f = \kappa \prod_i (x - \kappa_i)$, denn $\mathbb{L} : \mathbb{K}$ ist ja als Zerfällungskörper vorausgesetzt. Daraus ergibt sich

$$\widetilde{\varphi}(f) = \varphi(\kappa) \prod_i (x - \varphi(\kappa_i))$$

und damit $\mathbb{L}' = \mathbb{K}'$, so daß $\Phi := \varphi$ die Behauptung erfüllt.

ii) $n > 1$: Ist f_0 irreduzibler Teiler von f und λ_0 eine Wurzel von f_0, dann ist $\widetilde{\varphi}(f_0)$ ein irreduzibler Teiler von $\widetilde{\varphi}(f)$. Ist λ_0' eine Wurzel von $\widetilde{\varphi}(f_0)$, dann gibt es nach 8.4.3 eine Fortsetzung $\varphi^*: \mathbb{K}(\lambda_0) \simeq \mathbb{K}'(\lambda_0')$ von φ mit $\varphi^*(\lambda_0) = \lambda_0'$. Nun ist $\mathbb{L}$ Zerfällungskörper von f über $\mathbb{K}(\lambda_0)$ und $\mathbb{L}'$ Zerfällungskörper von $\widetilde{\varphi}(f)$ über $\mathbb{K}'(\lambda_0')$. Da $[\mathbb{L} : \mathbb{K}(\lambda_0)] < [\mathbb{L} : \mathbb{K}]$ gilt, können wir die Induktionsannahme zum Beweis der Existenz einer Fortsetzung $\Phi: \mathbb{L} \simeq \mathbb{L}'$ von φ^* verwenden. Wegen $\Phi(\kappa) = \varphi^*(\kappa) = \varphi(\kappa)$, für alle $\kappa \in \mathbb{K}$, ist sie auch Fortsetzung von φ.

□

8.4.6 Folgerung *Zu je zwei Zerfällungskörpern von $f \in \mathbb{K}[x]$ über $\mathbb{K}$ gibt es einen Isomorphismus, der $\mathbb{K}$ elementweise fest läßt. Zerfällungskörper sind also im wesentlichen eindeutig bestimmt. Man spricht deshalb auch oft von* dem *Zerfällungskörper von f über $\mathbb{K}$.*

□

Ein Polynom $f \in \mathbb{K}[x]^*$ hat im Zerfällungskörper $\mathbb{L} : \mathbb{K}$ genau $Grad(f)$ (nicht notwendig verschiedene) Wurzeln. Die Zerlegung

$$f = \kappa \prod_{i=0}^{Grad(f)-1} (x - \lambda_i)$$

ist, bis auf die Numerierung der λ_i eindeutig bestimmt. Sind $\lambda_0, \ldots, \lambda_{r-1}$ die *verschiedenen* Wurzeln, dann gilt

$$f = \kappa \prod_{0}^{r-1} (x - \lambda_i)^{n_i}.$$

Die eindeutig bestimmten n_i heißen die *Vielfachheiten* der λ_i. Sie sind unabhängig von der Wahl des Zerfällungskörpers $\mathbb{L}$.
Ist $f = \sum_0^n a_i x^i$, dann heißt das Polynom

$$f' := \sum_1^n (i \cdot a_i) x^{i-1}$$

die (*algebraische* oder auch *formale*) *Ableitung* von f.

8.4.7 Satz *Ein Polynom $f \in \mathbb{K}[x]$ von positivem Grad hat genau dann mehrfache Wurzeln, wenn f und f' einen nicht konstanten Teiler in $\mathbb{K}[x]$ gemeinsam haben.*

Beweis: Wir betrachten f vom Zerfällungskörper $\mathbb{L} : \mathbb{K}$ aus, $\lambda \in \mathbb{L}$ sei eine mehrfache Wurzel.
i) Ist $(x-\lambda)^m,\ m > 1$, ein Teiler von f, dann ist, nach der Produktregel der Differentiation, $(x-\lambda)^{m-1}$ ein Teiler von f', das Polynom $x-\lambda$ also ein gemeinsamer Teiler von f und f', in $\mathbb{L}[x]$. Wären diese beiden Polynome teilerfremd in $\mathbb{K}[x]$, so gäbe es (da $\mathbb{K}[x]$ euklidisch ist!) $p, q \in \mathbb{K}[x]$ mit $fp + f'q = 1$. Letztere Gleichung gilt aber auch in $\mathbb{L}$, im Widerspruch zur Existenz des bereits gefundenen gemeinsamen Teilers.

ii) Sei $p \in \mathbb{K}[x]$ ein gemeinsamer Teiler von f und f', $\lambda \in \mathbb{L}$ eine Wurzel von p. Dann gilt in $\mathbb{L}[x]$ die Gleichung $f = (x-\lambda)q$, mit einem geeigneten $q \in \mathbb{L}[x]$. Die Produktregel liefert jetzt $f' = q + (x-\lambda)q'$. Da $x-\lambda$ das Polynom f' teilt, ist also $x-\lambda$ ein Teiler von q und damit $f = (x-\lambda)^2 g$, es gibt also tatsächlich mehrfache Wurzeln.

□

8.4.8 Hilfssatz *Für irreduzible Polynome $f \in \mathbb{K}[x]$ gilt:*

- *f hat genau dann mehrfache Wurzeln, wenn $f' = 0$.*
- *Ist $char(\mathbb{K}) = 0$, dann hat f nur einfache Wurzeln.*
- *Ist $char(\mathbb{K}) = p > 0$, und hat f mehrfache Wurzeln, dann gibt es $g \in \mathbb{K}[x]$ mit $f = g(x^p)$.*

Beweis:
i) Die Existenz mehrfacher Wurzeln ist äquivalent zur Existenz gemeinsamer nicht konstanter Teiler von f und f'. Ein solcher Teiler von f ist aber, wegen der Irreduzibilität, zu f assoziiert. Wegen $Grad(f') \leq Grad(f) - 1$ ist die Existenz mehrfacher Wurzeln also äquivalent zu $f' = 0$.

ii) Da f nicht konstant ist, folgt, mit $char(\mathbb{K}) = 0$, daß $f' \neq 0$, nach i) gibt es also keine mehrfachen Wurzeln.

iii) Da nach i) $f' = \sum (i a_i) x^{i-1} = 0$, kann wegen $char(\mathbb{K}) = p$ ein Koeffizient a_i höchstens für durch p teilbare Indizes i von 0 verschieden sein, es gilt also

$$f = \sum_{i=0}^{m} a_{i \cdot p} x^{i \cdot p} = \sum_j b_j (x^p)^j = g(x^p).$$

□

Nach 8.4.7 kann man das Vorhandensein mehrfacher Wurzeln unter anderem anhand der Existenz gemeinsamer Teiler von f und f' feststellen. Es soll deshalb an den *Euklidischen Algorithmus* erinnert werden, der der Ermittlung von größten gemeinsamen Teilern in euklidischen Bereichen dient (vgl. 3.8.5): Schrittweise Division mit Rest (solange bis die Division aufgeht) ergibt ein Element $r_m \in \mathrm{ggT}\,(f, f')$:

$$\begin{aligned} f &= f' \cdot q_1 + r_1 \\ f' &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ &\vdots \\ r_{m-2} &= r_{m-1} \cdot q_m + r_m \\ r_{m-1} &= r_m \cdot q_{m+1} \end{aligned}$$

8.5 Symmetrische Polynome, Diskriminate und Resultante

Ein weiteres Verfahren zur Feststellung, ob mehrfache Wurzeln vorliegen, ist die Betrachtung der Diskriminante, deren Einführung jetzt vorbereitet werden soll. Dazu sei $0 \neq R$ ein kommutativer Ring mit 1.

8.5.1 Definition (symmetrische Polynome) Die symmetrische Gruppe S_n operiert kanonisch auf dem Polynomring $R[x_0, \ldots, x_{n-1}]$:

$$S_n \times R[x_0, \ldots, x_{n-1}] \to R[x_0, \ldots, x_{n-1}]\,,\ (\pi, f) \mapsto f(x_{\pi 0}, \ldots, x_{\pi(n-1)}).$$

Die *Invarianten* dieser Operation, also die Polynome f mit

$$\forall\ \pi \in S_n :\ \pi f = f$$

heißen *symmetrische Polynome*. •

8.5.2 Beispiele

- Die *elementarsymmetrischen* Polynome: Diese sind die Bahnensummen der Polynome $x_0 \cdots x_i, i \in n$:

$$\begin{aligned}
\sigma_1^{(n)} &:= x_0 + \ldots + x_{n-1},\\
\sigma_2^{(n)} &:= x_0x_1 + \ldots + x_0x_{n-1} + x_1x_2 + \ldots + x_{n-2}x_{n-1},\\
&\vdots\\
\sigma_n^{(n)} &:= x_0x_1 \cdots x_{n-1}.
\end{aligned}$$

  Schließlich setzen wir noch $\sigma_0^{(n)} := 1$. Für diese Polynome schreiben wir auch kurz $\sigma_0, \sigma_1, \ldots, \sigma_n$, falls n feststeht.

- Die *symmetrischen Potenzsummen*: Das sind die Bahnensummen der Polynome x_0^i:

$$\begin{aligned}
s_1^{(n)} &:= x_0 + \ldots + x_{n-1},\\
s_2^{(n)} &:= x_0^2 + \ldots + x_{n-1}^2,\\
&\vdots\\
s_i^{(n)} &:= x_0^i + \ldots + x_{n-1}^i,\\
&\vdots
\end{aligned}$$

  Diese Polynome kürzen wir auch mit $s_1, s_2, \ldots, s_i$ ab.

◇

Es gibt weitere Serien symmetrischer Polynome, die von Interesse sind (vgl. Übungsblatt).

8.5.3 Hilfssatz *Sei* $f = \sum_0^n a_i x^i \in R[x]$ *und* R *ein Teilring von* $\widetilde{R}$ *mit* $f = \prod_0^{n-1}(x-\rho_i)$, $\rho_i \in \widetilde{R}$. *Dann gilt, wenn* Σ_i *die Polynomfunktion zu* σ_i *bezeichnet und* $\Sigma_0^{(n)} := 1$*:*

$$f = \sum_{i=0}^{n} (-1)^i x^{n-i} \Sigma_i^{(n)}(\rho_0, \ldots, \rho_{n-1}),$$

d.h. die Koeffizienten von f *"sind symmetrische Funktionen in den Wurzeln".*

Zum Beweis braucht man $\prod(x - \rho_i)$ nur auszumultiplizieren. □

8.5.4 Folgerung *Sind* $\lambda_0, \ldots, \lambda_{n-1}$ *die Wurzeln von* $f = \sum_{i=0}^n a_i x^i$ *in einem Zerfällungskörper* $\mathbb{L} : \mathbb{K}$*, dann gilt für die Werte der* elementarsymmetrischen Funktionen $\Sigma_i^{(n)}$ *auf den Wurzeln von* f*:*

$$\Sigma_i^{(n)}(\lambda_0, \ldots, \lambda_{n-1}) \in \mathbb{K}.$$

8.5.5 Der Hauptsatz über symmetrische Polynome *Zu jedem symmetrischen Polynom* $f \in R[x_0, \ldots, x_{n-1}]$ *gibt es genau ein* $g \in R[x_0, \ldots, x_{n-1}]$ *mit*

$$f = g(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)}).$$

Der Beweis verläuft *konstruktiv*:

i) Wir betrachten die *Gewichte* $\alpha := (\alpha_0, \ldots, \alpha_{n-1})$ der monomialen Summanden $ax^\alpha := ax_0^{\alpha_0} \cdots x_{n-1}^{\alpha_{n-1}}$ von $f = \ldots + ax^\alpha + \ldots$. Sie können lexikographisch angeordnet werden:

$\alpha \geq \beta :\Longleftrightarrow$ die erste nicht verschwindende Differenz $\alpha_i - \beta_i$ ist größer als 0.

ii) Ist α das lexikographisch maximale, in f auftretende Gewicht, und damit $f = ax^\alpha + \ldots$, mit $a \neq 0$, dann gilt wegen der Symmetrie von f, daß $\alpha_0 \geq \alpha_1 \geq \ldots \geq \alpha_{n-1}$. Wir können demnach die folgende Differenz bilden:

$$f_1 := f - a \cdot \sigma_1^{\alpha_0 - \alpha_1} \sigma_2^{\alpha_1 - \alpha_2} \cdots \sigma_n^{\alpha_{n-1}} = bx^\beta + cx^\gamma + \ldots.$$

Hierbei gilt $\beta, \gamma, \ldots < \alpha$.
Ist β jetzt das lexikographisch maximale, in f_1 auftretende Gewicht, dann bilden wir analog die Differenz

$$f_2 := f_1 - b \cdot \sigma_1^{\beta_0 - \beta_1} \sigma_2^{\beta_1 - \beta_2} \cdots \sigma_n^{\beta_{n-1}} = dx^\delta + ex^\epsilon + \ldots.$$

Hierbei gilt entsprechend $\delta, \epsilon, \ldots < \beta$.

iii) Nach endlich vielen Schritten erhalten wir als Differenz das Nullpolynom, was die behauptete Existenz eines Polynoms g mit $f = g(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})$ beweist, die Eindeutigkeit erhalten wir aus 8.5.8.

□

8.5.6 Beispiel

$$2(x_0^3 + x_1^3 + x_2^3) - 3(x_0^2x_1 + x_0^2x_2 + x_0x_1^2 + x_0x_2^2 + x_1^2x_2 + x_1x_2^2)$$
$$= 2\sigma_1^3 + 15\sigma_3 - 9\sigma_1\sigma_2.$$

◇

8.5.7 Definition (algebraisch unabhängig) Ist $R \leq \widetilde{R}$, dann heißen Elemente $\rho_0, \ldots, \rho_{n-1} \in \widetilde{R}$ *algebraisch unabhängig über* R, wenn für alle $f \in R[x_0, \ldots, x_{n-1}]^*$ und für die entsprechenden Polynomfunktionen gilt:

$$F(\rho_0, \ldots, \rho_{n-1}) \neq 0.$$

•

8.5.8 Satz *Die elementarsymmetrischen Polynome σ_i sind algebraisch unabhängig.*

Beweis: Sei $f \in R[x_0, \ldots, x_{n-1}]^*$. Wir betrachten dazu die lexikographisch größte Exponentenfolge α, für die f einen monomialen Summanden

$$rx_0^{\alpha_0-\alpha_1}x_1^{\alpha_1-\alpha_2}\cdots x_{n-1}^{\alpha_{n-1}}$$

enthält. Diesem entspricht in $F(\sigma_1, \ldots, \sigma_n)$ der Summand rx^α, also gerade das Monom mit der lexikographisch größten Exponentenfolge. Es kann sich also nicht wegheben, so daß $F(\sigma_1, \ldots, \sigma_n) \neq 0$ folgt.

□

Mit 8.5.4 ergibt sich

8.5.9 Folgerung *Ist $g \in \mathbb{K}[x_0, \ldots, x_{n-1}]$ symmetrisch und hat $f \in \mathbb{K}[x]$ vom Grad n die Wurzeln $\lambda_0, \ldots, \lambda_{n-1}$ in einem Zerfällungskörper $\mathbb{L} : \mathbb{K}$, dann gilt*

$$G(\lambda_0, \ldots, \lambda_{n-1}) \in \mathbb{K}.$$

8.5.10 Definition (Diskriminante) Sei $f \in \mathbb{K}[x]$ vom Grad $n \geq 2$, und im Zerfällungskörper $\mathbb{L} : \mathbb{K}$ gelte $f = \kappa \prod(x - \lambda_i)$. Dann heißt

$$D(f) := \kappa^{2n-2} \prod_{0 \leq i < j \leq n-1} (\lambda_i - \lambda_j)^2$$

die *Diskriminante* von f. •

Die Diskriminante ist also ein Vielfaches des Quadrats der Vandermondeschen Determinante der Wurzeln des Polynoms und damit symmetrisch. Hiermit und nach 8.5.9 gilt

8.5.11 Folgerung *Für die Diskriminante von $f \in \mathbb{K}[x]$ gilt $D(f) \in \mathbb{K}$, und f hat genau dann mehrfache Wurzeln, wenn seine Diskriminante verschwindet: $D(f) = 0$.*

Es bleibt deshalb nur noch eine Berechnungsmethode für $D(f)$ anzugeben.

8.5.12 Definition (Sylvester-Matrix) Zu zwei Polynomen $f = \sum_0^n a_i x^i$ und $g = \sum_0^m b_j x^j$ in $\mathbb{K}[x]$, vom Grand n bzw. m, bezeichnet man folgendes Matrix aus deren Koeffizienten auch als die *Sylvester-Matrix,Resultante* dieser beiden Polynome:

$$S(f,g) := \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & \dots & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \dots & \dots & \dots & a_0 \\ b_m & b_{m-1} & \dots & \dots & \dots & \dots & 0 \\ 0 & b_m & \dots & \dots & \dots & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \dots & \dots & \dots & b_0 \end{pmatrix}$$

(m erste Zeilen aus den a_i wie angegeben, danach n Zeilen aus den b_j).
Ihre Determinante heißt die *Resultante* von f und g,

$$\mathrm{Res}(f,g) := \det(S(f,g)).$$

•

8.5.13 Satz *Die Resultante Res(f,g) von $f,g \in \mathbb{K}[x]^*$ ist genau dann gleich Null, wenn f und g in $\mathbb{K}[x]$ einen nicht konstanten Faktor gemeinsam haben.*

Beweis:
i) Nehmen wir an, die beiden Polynome besitzen einen nicht konstanten gemeinsamen Faktor h: $f = f_1 h, g = g_1 h$, mit

$$f_1 = \sum_{i=0}^{n-1} (-c_i) x^i,\ g_1 = \sum_{i=0}^{m-1} d_i x^i.$$

Wir betrachten die Differenz $fg_1 - gf_1 = f_1 h g_1 - g_1 h f_1 = 0$. Sie ergibt ein lineares Gleichungssystem für die Koeffizienten d_i und c_j mit der Transponierten der Sylvestermatrix $S(f,g)$ als Koeffizientenmatrix. Da es nichttriviale Lösungen gibt, muß die Determinante der Koeffizientenmatrix, also auch die Resultante, verschwinden.
ii) Ist umgekehrt $\mathrm{Res}(f,g) = 0$, dann gibt es nicht triviale Lösungen obigen Gleichungssystems, also Polynome f_1, g_1 mit $fg_1 = gf_1$. Wegen $fg_1 = gf_1$ und $\mathrm{Grad}(f_1) \leq \mathrm{Grad}(f)$ muß also mindestens ein unzerlegbarer Faktor von f in g aufgehen.

□

8.5.14 Folgerung *Haben $f,g \in \mathbb{K}[x]$ in $\mathbb{L} : \mathbb{K}$ eine gemeinsame Wurzel λ, dann gilt Res$(f,g) = 0$. Umgekehrt impliziert Res$(f,g) = 0$, daß f und g in einer geeigneten Erweiterung $\mathbb{L} : \mathbb{K}$ eine Wurzel gemeinsam haben.*

Darüberhinaus läßt sich beweisen (Übungsblatt), daß die Resultante sich auch in den Wurzeln λ_i von f und μ_j von g angeben läßt:

8.5.15 $$\mathrm{Res}(f,g) = a_n^m b_m^n \prod_{i,j=1}^{n,m} (\lambda_i - \mu_j).$$

Der Zusammenhang zwischen Diskriminante und Resultante wird von der folgenden Gleichung beschrieben:

8.5.16 $$a_n D(f) = \pm \mathrm{Res}(f, f').$$

Kapitel 9

Spezielle Klassen von Körpern

Es geht insbesondere um endliche Körper, um Kreisteilungskörper und um den algebraischen Abschluß eines Körpers.

9.1 Endliche Körper

Es soll jetzt nachgewiesen werden, daß es für jede Primzahl p und jedes $n \in \mathbb{N}^*$ bis auf Isomorphie genau einen Körper der Ordnung p^n gibt.

9.1.1 Hilfssatz *In jeder endlichen (multiplikativ geschriebenen) abelschen Gruppe G gibt es Elemente einer Ordnung m mit folgender Eigenschaft:*

$$\forall\ g \in G\colon g^m = 1.$$

Beweis: Der Hauptsatz über abelsche Gruppen besagt, daß G direktes Produkt zyklischer Gruppen von Primzahlpotenzordnung ist. Die dabei auftretenden Primzahlen sind die Primfaktoren p_i von $|G|$. Hält man eine solche Darstellung fest, etwa

$$G = (\underbrace{G_{11} \times G_{12} \times \ldots}_{p_1-Gruppen}) \times (\underbrace{G_{21} \times G_{22} \times \ldots}_{p_2-Gruppen}) \times \ldots \times (\underbrace{G_{r1} \times G_{r2} \times \ldots}_{p_r-Gruppen}),$$

mit $|G_{i1}| \geq |G_{ij}|$, und wählt zu jedem p_i aus dem Faktor *maximaler* p_i-Potenzordnung G_{i1} ein erzeugendes Element g_i, dann ist

$$m := |\langle g_1 \ldots g_r \rangle| = kgV\{|G_{i1}| \mid 1 \leq i \leq r\}$$

die Ordnung von $g_1 \cdots g_r$ und für $g \in G,\ g = g_{11}g_{12}\cdots g_{21}\cdots$ ergibt sich:

$$g^m = g_{11}^m g_{12}^m \cdots g_{21}^m \cdots = \prod (g_{ij})^m = 1,$$

denn $|G_{ij}|$ teilt die Ordnung von G_{i1}. □

9.1.2 Satz *Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch, insbesondere also auch die multiplikative Gruppe $\mathbb{K}^*$ eines endlichen Körpers.*

Beweis: Sei $\mathbb{K}$ ein Körper, G eine endliche Untergruppe von $\mathbb{K}^*$. Nach 9.1.1 gibt es ein Element κ' in G, für dessen Ordnung m folgendes gilt:

$$\forall\ \kappa \in G : \kappa^m = 1.$$

Alle Elemente von G sind deshalb Wurzeln des Polynoms $x^m - 1$, davon gibt es aber höchstens m verschiedene, es gilt demnach $|G| \leq m$. Da die m Potenzen von $\kappa' \in G$ nach der Definition von m alle verschieden sind, muß auch $|G| \geq m$ gelten. G besteht demnach aus den Potenzen dieses Elements κ', ist also zyklisch. □

Eine sehr wichtige und unmittelbare Konsequenz dieses Satzes ist die folgende Zusammenfassung der herausragenden Eigenschaften endlicher Körper:

9.1.3 Folgerung *Für endliche Körper $\mathbb{K}$ gilt:*

- *Es gibt eine Primzahl p mit $p = \mathrm{Char}(\mathbb{K})$ und ein $n \in \mathbb{N}^*$ mit*

$$|\mathbb{K}| = p^n.$$

- *Zu jeder Primzahl p und jedem $n \in \mathbb{N}^*$ gibt es einen Körper der Ordnung p^n.*
- *Die multiplikative Gruppe $\mathbb{K}^*$ ist zyklisch:*

$$\exists\, \lambda \in \mathbb{K}^* : \langle \lambda \rangle = \mathbb{K}^*.$$

- $\mathbb{K}$ *ist einfache algebraische Erweiterungen des Primkörpers*

$$\mathbb{P}(\lambda) = \mathbb{K}.$$

- *Für die Elemente $\kappa \in \mathbb{K}$ gilt*

$$\kappa^{(p^n)} = \kappa,$$

- $\mathbb{K}$ *ist also Zerfällungskörper von*

$$x^{(p^n)} - x \in \mathbb{K}[x].$$

- $\mathbb{K}$ *ist also bis auf Isomorphie eindeutig bestimmt.*

□

Der Zerfällungskörper von $x^q - x$ über $\mathbb{Z}_p$ ($q = p^n, n \in \mathbb{N}^*$) heißt das *Galoisfeld* der Ordnung q, es wird mit

$$GF(q)$$

oder auch mit $\mathbb{F}_q$ bezeichnet.

9.1.4 Beispiel Das Galoisfeld $GF(4)$ der Ordnung 4 ist also der Zerfällungskörper von $x^4 - x$ über $\mathbb{Z}_2$. Für dieses Polynom gilt

$$x^4 - x = x(x^3 - 1) = x(x+1)(x^2 + x + 1).$$

Der Faktor $x^2 + x + 1$ ist irreduzibel über $\mathbb{Z}_2$, also das Minimalpolynom seiner Wurzeln. Ist λ eine dieser Wurzeln, dann gilt also

$$GF(4) = \mathbb{Z}_2(\lambda) = \mathbb{Z}_2[\lambda] \simeq \mathbb{Z}_2[x]/(1 + x + x^2).$$

Daraus erhält man die Verknüpfungstafeln für diesen Körper. ◇

9.1.5 Satz *In $GF(p^n)$ gibt es zu jedem Teiler t von n genau einen Körper der Ordnung p^t. Umgekehrt ist jeder Teilkörper von $GF(p^n)$ von dieser Form. Der Verband der Teilkörper von $GF(p^n)$ ist also isomorph zum Verband*

$$(\{t \mid t \text{ teilt } n\}, \wedge, \vee)$$

der Teiler von n. ($s \wedge t$ ist der natürliche $ggT(s,t)$, $s \vee t$ das natürliche $kgV(s,t)$.)

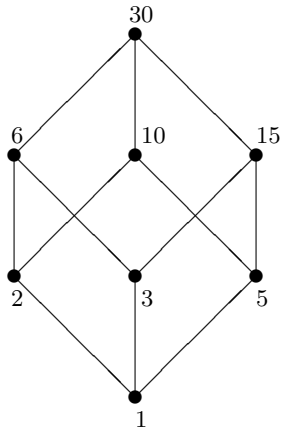
Beweis:
Alle Zwischenkörper $\mathbb{M}$ von $GF(p^n) : \mathbb{Z}_p$ sind Vektorräume über $\mathbb{Z}_p$, sie haben als Ordnung deshalb eine p-Potenz p^t. Da $GF(p^n)$ ein $\mathbb{M}$-Vektorraum ist, folgt $p^n = (p^t)^r$, mit geeignetem r. t ist deshalb ein Teiler von n.
Sei umgekehrt t ein Teiler von n. Wir zeigen, daß in diesem Fall $GF(p^n)$ einen Zerfällungskörper von $x^{(p^t)} - x$ enthält, also einen Teilkörper der Ordnung p^t. Sei dazu λ eine Wurzel von $x^{(p^t)} - x$, also $\lambda^{p^t-1} = 1$. Weil $p^t - 1$ ein Teiler von $p^n - 1$ ist, folgt daraus $\lambda^{p^n-1} = 1$, λ liegt demnach in $GF(p^n)$.
Daß es zu p^t nur *einen* Zwischenkörper $\mathbb{M}$ mit dieser Ordnung gibt folgt aus der Tatsache, daß jede zyklische Gruppe zu jedem Teiler ihrer Ordnung nur *eine* Untergruppe dieser Ordnung enthält.

□

Beispielsweise ist der Verband der Teilkörper von $GF(2^{30})$ isomorph zum Verband

$$(\{1, 2, 3, 5, 6, 10, 15, 30\}, \wedge, \vee)$$

der Teiler von 30. Das *Hassediagramm* hierzu ist



Es zeigt die Elemente des Verbandes, und die Kanten verbinden die unmittelbaren Nachbarn. Gelesen wird von unten nach oben.

9.2 Kreisteilungskörper

Hier geht es um eine weitere wichtige Klasse von Körpern, die sogenannten Kreisteilungskörper. Mit ihrer Hilfe kann man in vielen Fällen *exakt rechnen*, d. h. Rundungsfehler beim Rechnen mit reellen Zahlen vermeiden. So lassen sich beispielsweise alle Rechnungen im Rahmen von Anwendungen der Darstellungstheorie endlicher Gruppen in solchen Körpern führen. Des weiteren dienen sie der Untersuchung der Frage, welche regelmäßigen n-Ecke mit Zirkel und Lineal konstruiert werden können.

9.2.1 Definition Sei $\mathbb{P}$ ein Primkörper, $n \in \mathbb{N}^*$.

- Der Zerfällungskörper $\mathbb{P}^{(n)}$ von $x^n - 1$ über $\mathbb{P}$ heißt der *n-te Kreisteilungskörper* über $\mathbb{P}$.
- Die Wurzeln von $x^n - 1$ heißen *n-te Einheitswurzeln.*
- Die Gruppe der Einheitswurzeln in $\mathbb{P}^{(n)}$ bezeichnen wir mit

$$\mathbb{E}_{\mathbb{P}}^{(n)} := \{\kappa \in \mathbb{P}^{(n)} \mid \kappa^n = 1\} =: \mathbb{E}^{(n)}.$$

- Die Erzeugenden ζ von $\mathbb{E}_{\mathbb{P}}^{(n)}$ heißen *primitive* Einheitswurzeln. Für jede von ihnen gilt also

$$\mathbb{E}_{\mathbb{P}}^{(n)} = \langle\zeta\rangle,$$

und die Menge all dieser Erzeugenden bezeichnen wir mit:

$$\mathbb{F}_{\mathbb{P}}^{(n)} := \{\zeta \mid \langle\zeta\rangle = \mathbb{E}_{\mathbb{P}}^{(n)}\}.$$

•

Beispielsweise ist

$$\mathbb{Z}_p^{(q-1)} = GF(q).$$

9.2.2 Folgerung *Für die Kreisteilungskörper gilt:*

- $\mathbb{P}^{(n)} = \mathbb{P}(\mathbb{E}^{(n)})$.
- $t \mid n \Rightarrow \mathbb{E}^{(t)} \subseteq \mathbb{E}^{(n)} \Rightarrow \mathbb{P}^{(t)} \subseteq \mathbb{P}^{(n)}$.

□

9.2.3 Satz

- $\mathbb{E}_{\mathbb{P}}^{(n)}$ *ist zyklische Untergruppe von* ${\mathbb{P}^{(n)}}^*$.
- $\mathbb{P} = \mathbb{Z}_p \Rightarrow \mathbb{E}_{\mathbb{P}}^{(n)} = \mathbb{E}_{\mathbb{P}}^{(np)}$.
- $Char(\mathbb{P}) \nmid n \Rightarrow |\mathbb{E}_{\mathbb{P}}^{(n)}| = n$.

Beweis:

i) $\mathbb{E}_{\mathbb{P}}^{(n)}$ ist, als endliche Untergruppe der multiplikativen Gruppe eines Körpers, zyklisch nach 9.1.2.

ii) Ist p die Charakteristik, dann gilt $x^{pn} - 1 = (x^n - 1)^p$.

iii) Wegen $(x^n - 1)' = n \cdot x^{n-1} \neq 0$ hat $x^n - 1$ keine mehrfachen Wurzeln.

□

9.2.4 Folgerung *Ist $Char(\mathbb{P}) \nmid n$ und ζ eine primitive n-te Einheitswurzel über $\mathbb{P}$, dann gilt:*

- $\mathbb{E}_{\mathbb{P}}^{(n)} = \langle\zeta\rangle = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$,
- $\mathbb{P}^{(n)} = \mathbb{P}(\mathbb{E}_{\mathbb{P}}^{(n)}) = \mathbb{P}(\zeta) = \mathbb{P}[\zeta]$.
- $|\mathbb{F}_{\mathbb{P}}^{(n)}| = \varphi(n) = \{i \mid 0 \leq i < n, 1 \in ggT(i, n)\}$.
- $Char(\mathbb{P}) \nmid m \neq n \Rightarrow \mathbb{F}_{\mathbb{P}}{}^{(m)} \cap \mathbb{F}_{\mathbb{P}}^{(n)} = \emptyset$.
- $\mathbb{E}_{\mathbb{P}}^{(n)} = \bigcup_{t|n} \mathbb{F}_{\mathbb{P}}{}^{(t)}$.
- $\sum_{t|n} \varphi(t) = n$.

□

9.2.5 Beispiele

i) Hier sind zunächst einige Anzahlen primitiver n-ter Einheitswurzeln bzw. von Werten $\varphi(n)$ der *Eulerfunktion* φ, für die der letzte Punkt der Folgerung eine Rekursionsformel angibt:

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

.

ii) Für den Primkörper $\mathbb{Q}$ gilt:

$$\mathbb{E}_{\mathbb{Q}}^{(n)} = \left\{ \zeta^k = \exp\frac{2\pi i k}{n} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \;\middle|\; k \in n \right\},$$

sowie

$$\mathbb{F}_{\mathbb{Q}}^{(n)} = \{\zeta^k \in \mathbb{E}_{\mathbb{Q}}^{(n)} \mid 1 \in \mathrm{ggT}\,(k, n)\}.$$

◇

Mit Hilfe der Mengen primitiver Einheitswurzeln definieren wir nun

9.2.6 Definition (Kreisteilungspolynome) Das n-te *Kreisteilungspolynom* über $\mathbb{P}$, mit $\mathrm{Char}(\mathbb{P}) \nmid n$, ist das Polynom

$$\Phi_n := \prod_{\zeta \in \mathbb{F}_{\mathbb{P}}^{(n)}} (x - \zeta) = \prod_{k \in n : 1 \in ggT(k,n)} (x - \zeta^k),$$

wobei ganz rechts irgendeine der primitiven n-ten Einheitswurzeln genommen werden kann. •

9.2.7 Folgerung *Die Kreisteilungspolynome über Primkörpern $\mathbb{P}$ haben, wenn* $\mathrm{Char}(\mathbb{P}) \nmid n$, *die folgenden Eigenschaften:*

- $x^n - 1 = \prod_{t|n} \Phi_t = \prod_{\zeta \in \mathbb{F}_{\mathbb{P}}^{(n)}} (x - \zeta)$,
- *Ist $n = p$ eine Primzahl, dann gilt*

$$\Phi_p = x^{p-1} + \ldots x + 1 = \frac{x^p - 1}{x - 1},$$

- *Es gilt die Rekursionsformel*

$$\Phi_n = \frac{x^n - 1}{\prod_{n > t \mid n} \Phi_t}.$$

9.2.8 Beispiele Hier sind einige Beispiel von Kreisteilungspolynomen:

n	Φ_n
1	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$

◇

9.2.9 Satz *Jedes Kreisteilungspolynom ist ein Polynom mit Koeffizienten im Primkörper $\mathbb{P}$, und für $\mathbb{P} = \mathbb{Q}$ gilt sogar:*

$$\Phi_n \in \mathbb{Z}[x].$$

Beweis: Durch Induktion nach n.

i) Wegen $\Phi_1 = x - 1$ gilt die Behauptung für $n = 1$.

ii) Für $n > 1$ gilt $\Phi_n = (x^n - 1)/f$, mit

$$f := \prod_{n > t | n} \Phi_t.$$

Nach der Induktionsannahme ist f ein Polynom über dem Primkörper, bei Charakteristik 0 sogar über $\mathbb{Z}$. Division mit Rest im euklidischen Bereich $\mathbb{P}[x]$ ergibt

$$x^n - 1 = f \cdot q + r, \text{ mit } r = 0 \text{ oder } Grad(r) < Grad(f).$$

Das ist aber auch eine Zerlegung über $\mathbb{P}^{(n)}$, und dort gilt: $x^n - 1 = f \cdot \Phi_n$, also ist $r = 0$. Das impliziert aber $q = \Phi_n \in \mathbb{P}[x]$ bzw. $\in \mathbb{Z}[x]$.

□

9.2.10 Satz *Die Kreisteilungspolynome über $\mathbb{Q}$ sind irreduzibel. Für die Kreisteilungspolynome über $\mathbb{Z}_p$ gilt dies jedoch im allgemeinen nicht.*

Beweis: Sei (vgl. Unzerlegbarkeitskriterien) $\Phi_n = f \cdot g$, mit normierten $f, g \in \mathbb{Z}[x]$ und irreduziblem f, λ sei eine Wurzel von f. Dann ist $\lambda \in \mathbb{F}_{\mathbb{Q}}^{(n)}$, also $f = f_{\mathbb{Q},\lambda}$.

i) Wir zeigen, daß $F(\lambda^p) = 0$ gilt, falls p prim ist und n nicht teilt. Der Beweis verläuft indirekt.

$$F(\lambda^p) \neq 0 \Rightarrow G(\lambda^p) = 0 \Rightarrow f_{\mathbb{Q},\lambda} \mid g(x^p) \text{ in } \mathbb{Q}[x] \Rightarrow f_{\mathbb{Q},\lambda} \mid g(x^p) \text{ in } \mathbb{Z}[x],$$

etwa $g(x^p) = f_{\mathbb{Q},\lambda} \cdot h$, in $\mathbb{Z}[x]$. Wir rechnen jetzt modular weiter, die Restklassen der Zahlen bzw. die Polynome, die durch Reduktion modulo p entstehen, kennzeichnen wir durch Querstriche. Die Gleichung

$$\underbrace{\bar{g}(x^p)}_{=(\bar{g}(x))^p} = \bar{f}_{\mathbb{Q},\lambda} \cdot \bar{h}$$

ergibt die Existenz eines gemeinsamen Faktors $\bar{f}_0$ von $\bar{f}_{\mathbb{Q},\lambda}$ und $\bar{h}$, so daß folgendes herauskommt:

$$\overline{x^n - 1} = \bar{\Phi}_n \cdot \bar{q} = \bar{f} \cdot \bar{g} \cdot \bar{q} = \bar{f}_0^2 \cdot \bar{r}.$$

Demnach hat $\overline{x^n - 1}$ mehrfache Wurzeln, im Widerspruch zu $p \nmid n$.

ii) Jetzt zeigen wir noch die Gleichheit $\Phi_n = f$. Wir zeigen dazu, daß $Grad(\Phi_n) = Grad(f)$, wozu wir verifizieren, daß jede primitive n-te Einheitswurzel λ Wurzel von f ist. Sei dazu $\zeta \in \mathbb{F}_{\mathbb{Q}}^{(n)}$, etwa $\zeta = \lambda^k, \text{ggT}\,(k, n) \ni 1$. Ist jetzt $k = p_1 \cdots p_r$ die Primfaktorzerlegung, dann gilt:

$$0 = F(\lambda) =_{i)} F(\lambda^{p_1}) =_{i)} F(\lambda^{p_1 p_2}) =_{i)} \ldots =_{i)} F(\lambda^k) = F(\zeta).$$

iii) Über $\mathbb{Z}_5$ dagegen gilt beispielsweise

$$\Phi_{12} = x^4 - x^2 + 1 = (x^2 - 2x - 1)(x^2 + 2x - 1),$$

hier sind also *nicht alle* Kreisteilungspolynome irreduzibel.

□

9.2.11 Folgerung *Ist $\zeta \in \mathbb{F}_{\mathbb{Q}}^{(n)}$, dann gilt*

- $\Phi_n = f_{\mathbb{Q},\zeta}$,
- $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

9.2.12 Satz *Ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar, dann gilt*

$$n = 2^k \cdot p_1 \cdots p_r,$$

mit verschiedenen Fermatschen Primzahlen *(das sind Primzahlen der Form* $p_i = 2^{m_i} + 1$*)* $p_1, \ldots, p_r$.

Beweis:

i) Das regelmäßige n-Eck ist genau dann konstruierbar, wenn eine primitive n-te Einheitswurzel konstruierbar ist.

ii) Nach 9.2.11 und 8.3.5 folgt demnach aus der Konstruierbarkeit, daß $\varphi(n)$ eine Potenz von 2 ist.

iii) Ist $n = 2^k \cdot p_1^{k_1} \cdots p_r^{k_r}$ die Primfaktorzerlegung von n, dann gilt (mit dem Hilfssatz 9.2.13):

$$\varphi(n) = \varphi(2^k)\varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r}) = 2^{k-1} \prod_i p_i^{k_i - 1}(p_i - 1),$$

denn für Primzahlen p gilt offensichtlich $\varphi(p^k) = p^k - p^{k-1}$. Es muß also jeder Faktor $p_i^{k_i-1}(p_i - 1)$ eine Zweierpotenz sein, was $k_i = 1, p_i - 1 = 2^{l_i}$ impliziert. □

9.2.13 Hilfssatz *Für teilerfremde positive natürliche Zahlen* a, b *gilt:*

$$\varphi(a \cdot b) = \varphi(a)\varphi(b).$$

Beweis: Induktion nach $a \cdot b$.

i) Ist $ab = 1$, dann gilt die Behauptung: $\varphi(1) = 1$.

ii) Ist $ab > 1$, dann haben wir

$$ab = \sum_{t|ab} \varphi(t) = \varphi(ab) - \varphi(a)\varphi(b) + \sum_{(r,s):r|a,s|b} \varphi(r)\varphi(s) = \varphi(ab) - \varphi(a)\varphi(b) + ab.$$

□

Hiervon gilt auch die Umkehrung, was wir allerdings mit den vorhandenen Mitteln noch nicht beweisen können! Damit ist auch 9.2.12 vollständig bewiesen. Man kann übrigens leicht zeigen, daß der Exponent m einer Fermatschen Primzahl $p = 2^m + 1$ eine Potenz von 2 sein muß (Übungsblatt).

9.2.14 Folgerung *Für* $n \in \{7, 9, 11, 13, 14, 18, 19\}$ *ist das regelmäßige n-Eck* nicht *mit Zirkel und Lineal konstruierbar.*

Vermutlich ist $\{3, 5, 17, 257, 65537\}$ die Menge *aller* Fermatschen Primzahlen, das ist aber noch nicht bewiesen. Zum Abschluß noch eine besonders elegante Konstruktion des regelmäßigen Fünfecks (vgl. H. S. M. Coxeter: Unvergängliche Geometrie):

9.2.15 Eine Konstruktion des Fünfecks *Ausgangspunkt ist der Kreis vom Radius 1 um den Nullpunkt* $O := (0, 0)$ *mit den Punkten* $A := (1, 0)$ *und* $B := (0, 1)$ *auf der Peripherie. Man führt die folgenden Schritte aus:*

- *Konstruiere den Punkt* $C := (0, 1/2)$ *und verbinde ihn mit dem Punkt* $P_0 = (1, 0)$.
- *Halbiere den Winkel* $\sphericalangle(O, C, A)$*, sein Schenkel schneidet den Durchmesser durch den Nullpunkt* O *und den Punkt* A *im Punkt* D.

Die Parallele durch D *zur Geraden durch* O *und* C *schneidet den Kreis in 2 Punkten, die zusammen mit* A *drei Eckpunkte des Fünfecks bilden, die beiden anderen Punkte lassen sich dazu leicht ergänzen. (Vgl. H. S. M. Coxeter:* Unvergängliche Geometrie.*)*

9.3 Normale und separable Erweiterungen

Wir betrachten jetzt noch algebraische Erweiterungen der folgenden Form:

9.3.1 Definition (normale Erweiterung) Algebraische Erweiterungen $\mathbb{L} : \mathbb{K}$, in denen jedes irreduzible $f \in \mathbb{K}[x]$, das eine Wurzel in $\mathbb{L}$ hat, in Linearfaktoren zerfällt, nennen wir *normale* Erweiterungen. •

9.3.2 Satz *Eine endliche Körpererweiterung $\mathbb{L} : \mathbb{K}$ ist genau dann normal, wenn $\mathbb{L}$ Zerfällungskörper eines Polynoms $f \in \mathbb{K}[x]$ ist.*

Beweis:

i) "⇒": Ist $\mathbb{L} : \mathbb{K}$ eine endliche normale Erweiterung, $\{\lambda_0, \ldots, \lambda_{n-1}\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$, dann zerfällt — weil $\mathbb{L} : \mathbb{K}$ als normal angenommen wird — jedes $f_i := f_{\mathbb{K},\lambda_i}$ in Linearfaktoren, also auch deren Produkt $f := \prod_i f_i$. $\mathbb{L}$ ist demnach Zerfällungskörper von f, denn $\mathbb{L}$ ist ja durch Adjunktion der Wurzeln von f entstanden und die minimale Erweiterung von $\mathbb{K}$, über der f zerfällt.

ii) "⇐": Sei jetzt umgekehrt $\mathbb{L}$ ein Zerfällungskörper von $f \in \mathbb{K}[x]$ und $g \in \mathbb{K}[x]$ irreduzibel, $\lambda \in \mathbb{L}$ eine Wurzel von $g : G(\lambda) = 0$. Ist jetzt μ eine weitere Wurzel von g, dann gibt es nach 8.4.4 einen Isomorphismus $\varphi\colon \mathbb{K}(\lambda) \simeq \mathbb{K}(\mu)$, mit $\varphi \downarrow \mathbb{K} = \mathrm{id}$ und $\varphi(\lambda) = \mu$. $\mathbb{L} = \mathbb{L}(\lambda)$ ist Zerfällungskörper von f über $\mathbb{K}$, also auch über $\mathbb{K}(\lambda)$, und $\mathbb{L}(\mu)$ ist Zerfällungskörper von f über $\mathbb{K}(\mu)$. Nach 8.4.5 gibt es eine Fortsetzung $\Phi\colon \mathbb{L} = \mathbb{L}(\lambda) \simeq \mathbb{L}(\mu)$ von φ mit $\Phi \downarrow \mathbb{K} = \mathrm{id}$. Diese Fortsetzung ist ein $\mathbb{K}$-Isomorphismus von $\mathbb{L}$ auf $\mathbb{L}(\mu)$. Zum Nachweis der Gleichheit von $\mathbb{L}$ und $\mathbb{L}(\mu)$ genügt deshalb ein Vergleich der Dimensionen, denn diese sind ja endlich:

$$[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L}) = \dim_{\mathbb{K}}(\mathbb{L}(\mu)) = [\mathbb{L}(\mu) : \mathbb{K}].$$

Dabei folgt die mittlere Gleichung aus der Tatsache, daß Φ ein $\mathbb{K}$-Isomorphismus ist. $\mathbb{L}$ enthält also nicht nur λ sondern auch μ und (Induktion) damit *alle* Wurzeln von g.

□

9.3.3 Folgerung *Sei $\mathbb{L} : \mathbb{K}$ eine endliche Körpererweiterung, dann gilt*

- *$\mathbb{L}$ läßt sich zu normalem $\mathbb{M} : \mathbb{K}$ erweitern.*
- *Ist $\mathbb{L} : \mathbb{K}$ normal, dann auch $\mathbb{L} : \mathbb{M}$, für jeden Zwischenkörper $\mathbb{M}$.*

□

9.3.4 Definition (separable Polynome) Wir nennen $f \in \mathbb{K}[x]$ *separabel,* wenn jeder irreduzible Faktor von f nur einfache Wurzeln hat. •

Nach 8.4.8 gilt also

9.3.5 Folgerung

- *Ein irreduzibles f ist genau dann separabel, wenn $f' \neq 0$.*

- *Bei* $char(\mathbb{K}) = 0$ *ist jedes* $f \in \mathbb{K}[x]$ *separabel.*

□

9.3.6 Definition (vollkommene Körper) Körper, über denen jedes Polynom separabel ist, heißen *vollkommen.* •

9.3.7 Satz *Körper der Charakteristik 0 sind vollkommen. Ist dagegen* $char(\mathbb{K}) = p \neq 0$, *dann ist* $\mathbb{K}$ *genau dann vollkommen, wenn der* Frobeniushomomorphismus $\kappa \mapsto \kappa^p$ *surjektiv ist.*

Beweis: Die Aussage über die Separabilität von Körpern der Charakteristik 0 steht bereits oben. Sei deshalb $\text{char}(\mathbb{K}) = p \neq 0$.

a) Es sei zunächst der Frobeniushomomorphismus surjektiv und f ein irreduzibles Polynom mit mehrfachen Wurzeln. Nach 8.4.8 gibt es $g = \sum_i b_i x^i$ mit $f = g(x^p) = \sum_i b_i x^{ip}$. Wegen der Surjektivität des Frobeniushomomorphismus gibt es a_i mit $a_i^p = b_i$. Das ergibt

$$f(x) = g(x^p) = \sum_i b_i x^{ip} = \sum_i a_i^p x^{ip} = (\sum_i a_i x^i)^p,$$

im Widerspruch zur Irreduzibilität von f.

b) Ist dagegen $\kappa \mapsto \kappa^p$ *nicht* surjektiv, dann gibt es $a \in \mathbb{K}$, so daß $f = x^p - a$ *keine* Wurzel in $\mathbb{K}$ hat. Sei g jetzt ein normierter irreduzibler Teilerr von $f = gh$, $\lambda \in \mathbb{L}$ eine Wurzel von f. Es gilt

$$f = gh = x^p - a = (x - \lambda)^p.$$

Weil $\mathbb{L}[x]$ ein Gaußbereich ist, folgt $g = (x - \lambda)^l$, und weil $\lambda \notin \mathbb{K}$ gilt $l \geq 2$, g hat also mehrfache Wurzeln. □

9.3.8 Satz *Endliche Körper sind vollkommen.*

Beweis: Der Frobeniushomomorphismus ist von der Nullabbildung verschieden, und Körper besitzen keine nicht trivialen Ideale, der Frobeniushomomorphismus ist demnach auf jedem Körper injektiv. Eine injektive Abbildung einer endlichen Menge auf sich selbst ist aber auch surjektiv.

□

9.3.9 Beispiel Der Körper $\mathbb{K}(x)$ der rationalen Funktionen über einem Körper $\mathbb{K}$ der Charakteristik $p > 0$ ist *nicht* vollkommen, denn der Frobeniushomomorphismus ist dort nicht surjektiv:

$$x = \left(\frac{f(x)}{g(x)}\right)^p$$

ergäbe $xg(x)^p = f(x)^p$. Mit $f = \sum a_i x^i$ und $g = \sum_i b_i x^i$ erhielten wir daraus

$$\sum_i b_i^p x^{ip+1} = \sum a_i^p x^{ip},$$

anhand eines Koeffizientenvergleichs also den Widerspruch $a_i = b_i = 0$. ◇

□

9.3.10 Definition (separable Elemente und Erweiterungen) Ein Element $\lambda \in \mathbb{L} : \mathbb{K}$ heißt *separabel* über $\mathbb{K}$, wenn λ Wurzel eines separablen Polynoms $f \in \mathbb{K}[x]$ ist. $\mathbb{L} : \mathbb{K}$ heißt *separable Erweiterung,* wenn jedes $\lambda \in \mathbb{L}$ über $\mathbb{K}$ separabel ist. •

9.3.11 Beispiele
i) $i \in \mathbb{C}$ ist separabel über $\mathbb{R}$:

$$f = x^2 + 1 = (x - i)(x + i).$$

ii) Ist $\text{char}(\mathbb{K}) = p > 0$, κ keine p-te Wurzel, dann ist $x^p - \kappa$ kein separables Polynom. ◇

9.3.12 Folgerung

- *Jede separable Erweiterung ist algebraisch.*
- *Jede algebraische Erweiterung eines vollkommenen Körpers ist separabel.*
- *Algebraische Erweiterungen von Körpern der Charakteristik 0 und von endlichen Körpern sind separabel.*

9.3.13 Satz *Ist $\mathbb{L} : \mathbb{K}$ eine algebraische Erweiterung, dann sind die folgenden Bedingungen für $\lambda \in \mathbb{L}$ äquivalent:*

i) λ *ist separabel,*

ii) $f_{\mathbb{K},\lambda}$ *ist separabel,*

iii) λ *ist einfache Wurzel von* $f_{\mathbb{K},\lambda}$,

iv) $f'_{\mathbb{K},\lambda} \neq 0$.

Beweis:

i)⇒ii): Ist $\lambda \in \mathbb{L}$ separabel, dann gibt es separable $g \in \mathbb{K}[x]$, die λ als Wurzel haben. Dafür gilt $G(\lambda) = 0$, $f_{\mathbb{K},\lambda}$ ist also ein Teiler von g und damit ebenfalls separabel.

ii)⇒iii): Separable Polynome haben ausschließlich einfache Wurzeln.

iii)⇒iv): In einer geeigneten Erweiterung $\mathbb{M}$ von $\mathbb{L}$ gilt $f_{\mathbb{K},\lambda} = (x - \lambda)g$, mit einem geeigneten Polynom $g \neq 0$. In diesem Erweiterungskörper gilt für die formale Ableitung

$$f'_{\mathbb{K},\lambda} = (x - \lambda)g' + g,$$

und damit $F'_{\mathbb{K},\lambda}(\lambda) = G(\lambda) \neq 0$ (letzteres, weil λ *einfache* Wurzel des Minimalpolynoms ist).

iv)⇒i): folgt aus 9.3.5. □

9.3.14 Satz *Jede endliche, normale und separable Erweiterung* $\mathbb{L} : \mathbb{K}$ *ist Zerfällungskörper eines separablen* $f \in \mathbb{K}[x]$.

Beweis: Weil $\mathbb{L} : \mathbb{K}$ normal vorausgesetzt wird, ist $\mathbb{L}$ Zerfällungskörper eines $f \in \mathbb{K}[x]$, das, wegen der Separabilität von $\mathbb{L} : \mathbb{K}$, über $\mathbb{L}$ in Linearfaktoren zerfällt. Sei g ein normierter irreduzibler Faktor von f. $\mathbb{L}$ enthält alle Wurzeln von g, dieses Polynom ist also das Minimalpolynom seiner Wurzeln und separabel, also ist auch f separabel. □

9.3.15 Der Satz vom primitiven Element $\mathbb{L} : \mathbb{K}$ *sei eine Körpererweiterung,* λ *ein separables Element,* μ *ein algebraisches Element von* $\mathbb{L}$. *Es gibt dann Elemente* $\nu \in \mathbb{L}$ *mit*

$$\mathbb{K}(\lambda, \mu) = \mathbb{K}(\nu).$$

Solche $\nu \in \mathbb{L}$ *heißen* primitive Elemente.

Beweis: Wir unterscheiden zwei Fälle, je nachdem ob $\mathbb{K}$ endlich ist oder nicht. Der Beweis ist konstruktiv.

i) Ist $\mathbb{K}$ endlich, dann ist die multiplikative Gruppe $\mathbb{K}(\lambda, \mu)^*$ zyklisch, jedes erzeugende Element ν dieser multiplikativen Gruppe erfüllt natürlich die Behauptung.

ii) Sei jetzt $\mathbb{K}$ unendlich. $\lambda = \lambda_1, \ldots, \lambda_r$ seien die Wurzeln des Minimalpolynoms von λ, $\mu = \mu_1, \ldots, \mu_s$ die Wurzeln des Minimalpolynoms von μ.
Ist $\lambda \in \mathbb{K}$, dann ist natürlich $\mathbb{K}(\lambda, \mu) = \mathbb{K}(\mu)$, die Behauptung gilt also.
Ist dagegen $\lambda \notin \mathbb{K}$, dann ist $r \geq 2$. Wir können deshalb zu jedem $\kappa \in \mathbb{K}$ die folgende Menge betrachten:

$$W(\kappa) := \{\lambda_i \kappa + \mu_j \mid 2 \leq i \leq r, 1 \leq j \leq s\}.$$

Weil $\mathbb{K}$ als unendlich vorausgesetzt ist, gibt es $y \in \mathbb{K}$ mit

$$y \notin \left\{ \frac{\mu_j - \mu}{\lambda - \lambda_i} \;\middle|\; 2 \leq i \leq r, 1 \leq j \leq s \right\}.$$

Zu einem solchen y sei

$$\nu := \lambda y + \mu.$$

Wir wollen zeigen, daß $\mathbb{K}(\nu) = \mathbb{K}(\lambda, \mu)$ gilt. Dazu bemerken wir zunächst, daß $\nu \notin W(y)$, denn andernfalls wäre $y(\lambda - \lambda_i) = \mu_j - \mu$, für geeignete i und j. Die Inklusion $\mathbb{K}(\nu) \subseteq \mathbb{K}(\lambda, \mu)$ ist trivial, es bleibt die Umkehrung zu zeigen.
Sei $h \in \mathrm{ggT}\,(f_{\mathbb{K},\lambda}, f_{\mathbb{K},\mu}(\nu - yx)) \in \mathbb{K}(\nu)[x]$. Das Polynom $x - \lambda$ teilt sowohl $f_{\mathbb{K},\lambda}$ als auch $f_{\mathbb{K},\mu}(\nu - yx)$, denn

$$F_{\mathbb{K},\mu}(\nu - y\lambda) = F_{\mathbb{K},\mu}(\mu) = 0.$$

Dagegen sind die $\lambda_i, i \geq 2$, keine Wurzeln von $f_{\mathbb{K},\mu}(\nu - yx)$, denn $\nu - y\lambda_i = \mu_j$ ergäbe $\nu \in W(y)$.
λ ist also die einzige Wurzel von h, weshalb $h = (x - \lambda)^m$ gelten muß, wegen der Separabilität von $f_{\mathbb{K},\lambda}$, einem Vielfachen von h, sogar $h = x - \lambda$. Da diese Polynom in $\mathbb{K}(\nu)[x]$ liegt, folgt $\lambda \in \mathbb{K}(\nu)$ und daraus auch $\mu = \nu - \lambda y \in \mathbb{K}(\nu)$, was $\mathbb{K}(\lambda, \mu) \subseteq \mathbb{K}(\nu)$ impliziert und den Beweis vervollständigt. □

9.3.16 Folgerungen

- *Sind $\lambda_1, \ldots, \lambda_r$ separabel und ist μ algebraisch, dann ist $\mathbb{K}(\lambda_1, \ldots, \lambda_r, \mu)$ eine einfache Erweiterung.*
- *Jede endliche Erweiterung eines vollkommenen Körpers ist einfach.*
- *Jede endliche Erweiterung eines Körpers der Charakteristik 0 ist einfach.*
- *Jede endliche Erweiterung eines endlichen Körpers ist einfach.*

Endliche Erweiterungen von $\mathbb{Q}$ heißen *algebraische Zahlkörper.*

9.3.17 Folgerung *Algebraische Zahlkörper sind genau die einfachen Erweiterungen von $\mathbb{Q}$.*

9.3.18 Beispiel Betrachten wir $\mathbb{Q}(\lambda, \mu) := \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$. Wir haben

$$f_{\mathbb{Q},\lambda} = x^3 - 2, \ f_{\mathbb{Q},\mu} = x^2 - 2.$$

Ist ζ eine primitive dritte Einheitswurzel, dann gilt

$$\lambda = \lambda_1 = \sqrt[3]{2}, \ \lambda_2 = \zeta\sqrt[3]{2}, \ \lambda_3 = \zeta^2\sqrt[3]{2},$$

und

$$\mu = \mu_1 = \sqrt{2}, \ \mu_2 = -\sqrt{2}.$$

Weiterhin gilt

$$\left\{ \frac{\mu_j - \mu}{\lambda - \lambda_i} \;\middle|\; 2 \leq i \leq 3, 1 \leq j \leq 2 \right\} = \left\{ 0, 2\sqrt{2}\sqrt[3]{2}(\zeta - 1), 2\sqrt{2}\sqrt[3]{2}(\zeta^2 - 1) \right\} \not\ni 1.$$

Entsprechend obigem Beweis erhalten wir daraus als primitives Element

$$\nu = \lambda + \mu = \sqrt[3]{2} + \sqrt{2}.$$

$\diamond$

9.4 Algebraisch abgeschlossene Körper

9.4.1 Definition (algebraisch abgeschlossen) Ein Körper $\mathbb{K}$ heißt *algebraisch abgeschlossen,* wenn jedes $f \in \mathbb{K}[x] \setminus \mathbb{K}$ eine — und damit alle — Wurzeln in $\mathbb{K}$ hat. •

9.4.2 Folgerungen *Äquivalent sind:*

- $\mathbb{K}$ *ist algebraisch abgeschlossen,*
- $\mathbb{K}$ *ist Zerfällungskörper für jedes* $f \in \mathbb{K}[x]$,
- *Jedes irreduzible* $f \in \mathbb{K}[x]$ *ist vom Grad 1,*
- $\mathbb{K}$ *selbst ist die einzige algebraische Erweiterung von* $\mathbb{K}$.

9.4.3 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *algebraisch abgeschlossen, dann ist*

$$\mathcal{A}(\mathbb{L} : \mathbb{K}) = \{\lambda \in \mathbb{L} \mid \ \lambda \text{ algebraisch über } \mathbb{K}\},$$

der Körper der algebraischen Elemente von $\mathbb{L}$, *ein algebraisch abgeschlossener Körper.*

Beweis: Wir wollen Punkt iv) in 9.4.2 benutzen und zeigen, daß $\mathcal{A}(\mathbb{L} : \mathbb{K})$ seine einzige algebraische Erweiterung ist.
Sei deshalb $\mathbb{M} : \mathcal{A}(\mathbb{L} : \mathbb{K})$ eine algebraische Erweiterung, $\mu \in \mathbb{M}$. Weil $\mathcal{A}(\mathbb{L} : \mathbb{K}) : \mathbb{K}$ algebraisch ist, ist μ auch algebraisch über $\mathbb{K}$, liegt also in $\mathbb{L}$ und damit auch in $\mathcal{A}(\mathbb{L} : \mathbb{K})$.

□

Unter einem *algebraischen Abschluß von* $\mathbb{K}$ verstehen wir eine algebraische Erweiterung $\mathbb{L} : \mathbb{K}$ von $\mathbb{K}$, die algebraisch abgeschlossen ist.

9.4.4 Folgerung *Besitzt* $\mathbb{K}$ *algebraisch abgeschlossene Erweiterungen, dann besitzt* $\mathbb{K}$ *auch einen algebraischen Abschluß.*

Ist $A \subseteq \mathbb{K}[x]$, also eine Menge von Polynomen über $\mathbb{K}$, dann heißt $\mathbb{L} : \mathbb{K}$ ein *Zerfällungkörper von* A, wenn jedes $f \in A$ in $\mathbb{L}$ in Linearfaktoren zerfällt und $\mathbb{L}$ durch Adjunktion der Wurzeln der $f \in A$ aus $\mathbb{K}$ entsteht.

9.4.5 Satz

- *Zu jedem* $A \subseteq \mathbb{K}[x]$ *gibt es Zerfällungskörper.*
- *Zu je zwei Zerfällungskörpern* $\mathbb{L}, \mathbb{L}'$ *von* A *gibt es Isomorphismen* $\Phi\colon \mathbb{L} \simeq \mathbb{L}'$ *mit* $\Phi \downarrow \mathbb{K} = \mathrm{id}_{\mathbb{K}}$.

Beweis: Wir betrachten die Klasse

$$\mathcal{M} := \{(\mathbb{L}, B) \mid B \subseteq A, \mathbb{L} \text{ ist Zerfällungskörper von } B\}.$$

$\mathcal{M} \neq \emptyset$ ist induktiv geordnet vermöge

$$(\mathbb{L}, B) \leq (\mathbb{L}', B') :\Longleftrightarrow \mathbb{L} \subseteq \mathbb{L}' \wedge B \subseteq B'.$$

Nach Zorns Lemma besitzt $\mathcal{M}$ also maximale Elemente, etwa $(\mathbb{L}, S)$. Hierfür gilt offensichtlich $S = A$.
iii) $\mathcal{F}$ bezeichne jetzt die Klasse der Zwischenkörperisomorphismen $f\colon \mathbb{M} \simeq \mathbb{M}'$, die $\mathrm{id}_{\mathbb{K}}$ fortsetzen, für $\mathbb{K} \leq \mathbb{M} \leq \mathbb{L}$, und $\mathbb{K} \leq \mathbb{M}' \leq \mathbb{L}'$. Auch diese Klasse ist induktiv geordnet:

$$(\sigma\colon \mathbb{M} \to \mathbb{M}') \leq (\tau\colon \mathbb{N} \to \mathbb{N}') :\Longleftrightarrow \mathbb{M} \subseteq \mathbb{N} \wedge \tau \downarrow \mathbb{M} = \sigma.$$

Nach Zorns Lemma gibt es also maximale Elemente in $\mathcal{F}$, etwa $f\colon \mathbb{M} \simeq \mathbb{M}'$. Hierfür gilt (vgl. 8.4.5) $\mathbb{M} = \mathbb{L}, \mathbb{M}' = \mathbb{L}'$, wegen **??**. □

9.4.6 Folgerung *Jeder Körper $\mathbb{K}$ besitzt algebraische Abschlüsse, und zu je zwei algebraischen Abschlüssen $\mathbb{L}$ und $\mathbb{L}'$ von $\mathbb{K}$ gibt es einen Isomorphismus $\Phi\colon \mathbb{L} \simeq \mathbb{L}'$ mit $\Phi \downarrow \mathbb{K} = \mathrm{id}_{\mathbb{K}}$.*

Beweis: $\mathbb{L} : \mathbb{K}$ ist genau dann algebraischer Abschluß von $\mathbb{K}$, wenn $\mathbb{L}$ Zerfällungskörper von $\mathbb{K}[x] \setminus \mathbb{K}$ ist. Nach 9.4.5 gibt es Zerfällungskörper $\bar{\mathbb{K}}$ von $\mathbb{K}[x] \setminus \mathbb{K}$, wir wollen die algebraische Abgeschlossenheit von $\bar{\mathbb{K}}$ beweisen.
Sei dazu $\mathbb{L} : \bar{\mathbb{K}}$ eine algebraische Erweiterung, $\lambda \in \mathbb{L}$. Das Minimalpolynom $f_{\mathbb{K},\lambda}$ von λ zerfällt über $\bar{\mathbb{K}}$ in Linearfaktoren, also liegt λ in $\bar{\mathbb{K}}$, also ist $\mathbb{L} = \bar{\mathbb{K}}$, und $\bar{\mathbb{K}}$ ist demnach algebraisch abgeschlossen.
Ist umgekehrt $\bar{\mathbb{K}} : \mathbb{K}$ algebraischer Abschluß von $\mathbb{K}$, $f \in \mathbb{K}[x] \setminus \mathbb{K}$, dann zerfällt f in Linearfaktoren. $\bar{\mathbb{K}}$ enthält demnach einen Zerfällungskörper $\mathbb{L}$ von $\mathbb{K}[x] \setminus \mathbb{K}$, dieser ist algebraisch abgeschlossen. Weil $\bar{\mathbb{K}} : \mathbb{K}$ algebraisch ist, gilt das auch für $\bar{\mathbb{K}} : \mathbb{L}$, was $\bar{\mathbb{K}} = \mathbb{L}$ impliziert. □

9.4.7 Beispiele
i) $\mathbb{C}$ ist algebraischer Abschluß von $\mathbb{R}$.
ii) Der Körper $\bar{\mathbb{Q}}$ der algebraischen Zahlen ist algebraischer Abschluß von $\mathbb{Q}$:

$$\bar{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ algebraisch über } \mathbb{Q}\}.$$

iii) Kein endlicher Körper $\mathbb{K}$ ist algebraisch abgeschlossen, denn für jedes $\kappa \in \mathbb{K}^*$ hat das Polynom

$$f := \kappa + x \prod_{\lambda \in \mathbb{K}^*} (x - \lambda)$$

Wurzeln, die nicht in $\mathbb{K}$ liegen.
iv) Der algebraische Abschluß $\mathcal{K}$ eines endlichen Körpers $\mathbb{K}$ besteht aus lauter Einheitswurzeln:

$$\bar{\kappa} \in \mathcal{K} \Rightarrow \bar{\kappa} \text{ algebraisch} \Rightarrow [\mathbb{K}(\bar{\kappa}) : \mathbb{K}] \in \mathbb{N} \Rightarrow \mathbb{K}(\bar{\kappa})^* \text{ endlich} \Rightarrow \bar{\kappa}^{|\mathbb{K}(\bar{\kappa})|-1} = 1.$$

◇

9.5 Endliche Schiefkörper

In diesem Paragraphen sollen Schiefkörper diskutiert und insbesondere der Satz von Wedderburn bewiesen werden, daß *endliche* Schiefkörper kommutativ und damit *Körper* sind. Zunächst soll aber das prominenteste Beispiel für (nicht kommutative) Schiefkörper eingeführt werden.

9.5.1 Beispiel Wir betrachten einen kommutativen Ring R und definieren

$$H(R) = \{r + is + jt + ku \mid r, s, t, u \in R\}.$$

Die Koeffzienten 1 (von r), i, j und k dienen uns zur Einführung einer Multiplikation, die $H(R)$ zu einer Algebra über R und damit zu einem Ring macht. Diese Multiplikation wird als distributive Fortsetzung der durch folgende Tafel definierten Multiplikation dieser "Basiselemente" definiert:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Die addition sei komponentenweise definiert. $H(R)$ heißt die *Quaternionenalgebra* über R. Das H steht für Hurwitz. Zu einem Element

$$\rho := r + is + jt + ku \in H(R),$$

heißt

$$\bar{\rho} := r - is - jt - ku$$

das *konjugierte Element,* und

$$N(\rho) := \rho \cdot \bar{\rho} = r^2 + s^2 + t^2 + u^2$$

wird als die *Norm* von ρ bezeichnet. Es zeigt sich, daß ρ genau dann invertierbar ist, wenn $N(\rho)$ eine Einheit ist. Hieran sieht man sofort, daß die Algebren $H(\mathbb{Q})$ und $H(\mathbb{R})$ *Schiefkörper* sind, denn jedes ihrer von Null verschiedenen Elemente ist ja invertierbar. $H(\mathbb{Q})$ ist am bekanntesten und heißt deshalb auch *der* Quaterionenschiefkörper oder *die* Quaternionenalgebra.
Dagegen ist $H(\mathbb{Z})$ *kein* Schiefkörper. Die Einheitengruppe von $H(\mathbb{Z})$ ist nämlich

$$E(H(\mathbb{Z})) = \{\pm 1, \pm i, \pm j \pm k\},$$

die *Quaternionengruppe.* ◇

9.5.2 Der Satz von Wedderburn *Endliche Schiefkörper sind Körper.*

Beweis: Sei $\mathbb{K}$ ein endlicher Schiefkörper.

i) Das Zentrum

$$Z(\mathbb{K}) := \{\kappa \in \mathbb{K} \mid \forall\, \lambda \in \mathbb{K} \colon \kappa\lambda = \lambda\kappa\}$$

von $\mathbb{K}$ ist Teilkörper von $\mathbb{K}$, und wir haben die Identität $Z(\mathbb{K}) = \mathbb{K}$ zu beweisen.

ii) Als Körper ist $Z(\mathbb{K})$ isomorph $GF(q)$, q geeignet. $\mathbb{K}$ ist Vektorraum über diesem Teilkörper, hat also eine Potenz von q als Ordnung, etwa $|\mathbb{K}| = q^n$. Wir haben also $n = 1$ zu verifizieren.

iii) Die Gruppe $G := \mathbb{K}^*$ ist disjunkte Vereinigung ihrer Konjugiertenklassen. Die Konjugiertenklassen der Ordnung 1 bilden $Z(\mathbb{K})^*$. Außerdem ist die Ordnung einer Konjugiertenklasse, d.h. einer Bahn unter der Konjugation, gleich dem Index des Zentralisators $C_{\mathbb{K}^*}(\kappa)$ (in $\mathbb{K}^*$) jedes ihrer Elemente κ. Daraus ergibt sich als *Klassengleichung*

$$q^n - 1 = q - 1 + \sum_{\kappa \in \mathcal{C}} \frac{q^n - 1}{q^{n(\kappa)} - 1},$$

$\mathcal{C}$ ein Repräsentantensystem der Konjugiertenklassen außerhalb $Z(\mathbb{K})$, denn der Zentralisator $C_{\mathbb{K}}(\kappa) = C_{\mathbb{K}^*}(\kappa) \cup \{0\}$ enthält das Zentrum $Z(\mathbb{K})$ und ist demnach ein Vektorraum über $GF(q)$. Der Zentralisator in $\mathbb{K}^*$ hat also die Ordnung $q^{n(\kappa)} - 1$, mit geeignetem $n(\kappa)$.

iv) Die Ordnung jeden Zentralisators teilt die Gruppenordnung also ist $q^{n(\kappa)} - 1$ ein Teiler von $q^n - 1$, also $n(\kappa)$ ein Teiler von n. Hieraus ergibt sich mit Hilfe der zyklotomischen Polynome (über $\mathbb{Q}$, also in $\mathbb{Z}[x]$) und deren Werten an der Stelle q :

$$\frac{q^n - 1}{q^{n(\kappa)} - 1} = \frac{\prod_{t|n} \Phi_t(q)}{\prod_{t|n(\kappa)} \Phi_t(q)} = \Phi_n(q) F(q),$$

für ein Polynom $f \in \mathbb{Z}[x]$.

v) Nach iv) teilt $\Phi_n(q)$ sowohl die linke Seite als auch den dritten Summanden auf der rechten Seite der Klassengleichung, diese Zahl ist demnach auch ein Teiler von $q - 1 > 0$, und damit ist $|\Phi_n(q)| \leq q - 1$.

vi) Unser Ziel ist der Beweis von $\mathbb{K} = Z(\mathbb{K})$, also von $n = 1$. Betrachten wir die Gleichung

$$\Phi_n(q) = \prod_{\zeta \in \mathbb{F}^{(n)}} (q - \zeta).$$

Für $n > 1$ gibt es eine von 1 verschiedene primitive $n-$te Einheitswurzel $\zeta \in \mathbb{C}$, hierfür ist der Abstand von q aber größer als der von 1, $|q - \zeta| > q - 1$,

$$\forall\, n > 1 \colon |\Phi_n(q)| > (q-1)^{\varphi(n)} \geq q - 1,$$

im Widerspruch zu v). □

Kapitel 10

Galoistheorie

Wir wollen die Körpertheorie jetzt zur Untersuchung von Gleichungen höheren Grades auf ihre Lösbarkeit durch Wurzelziehen verwenden. Bekanntlich kann man quadratische Gleichungen durch Wurzelziehen lösen: die beiden Lösungen von $x^2+px+q=0$ sind $x_{1,2}=-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}$. Gleichungen dritten und vierten Grades können ebenfalls durch Ziehen von Wurzeln (Quadratwurzeln, kubische Wurzeln etc.) von Ausdrücken in den Koeffizienten gelöst werden. Lösungen von quadratischen Gleichungen sind schon vor der Zeitenwende diskutiert worden, bei den Gleichungen dritten Grades sind die Lösungen seit der Mitte des 16. Jahrhunderts bekannt, für die Gleichungen vierten Grades seit dem Ende des 18. Jahrhunderts. Der Beweis dafür, daß demgegenüber Gleichungen fünften Grades *nicht immer* lösbar sind, gelang zu Beginn des 19. Jahrhunderts, zu einer Zeit als E. Galois den Zugang zur Klassifizierung der lösbaren Gleichungen fand, einen Zusammenhang zwischen dem Untergruppenverband der sogenannten *Galoisgruppe* der Gleichung und dem Verband der Zwischenkörper des Zerfällungskörpers. Nach ihm heißt die betreffende Theorie *Galoistheorie.*

10.1 Galoisgruppen

Unser Ziel ist der Beweis des Hauptsatzes der Galoistheorie, der einen Ordnungsisomorphismus zwischen dem Untergruppenverband der sogenannten Galoisgruppe beschreibt und dem Verband der Zwischenkörper des Zerfällungskörpers. Definieren wir deshalb zunächst *die Galoisgruppe, die aus den Körperautomorphismen von* $\mathbb{L}$ *besteht, die Wurzeln von Polynomen* $f \in \mathbb{K}[x]$ *wieder in Wurzeln überführen*:

10.1.1 Definition (Galoisgruppe) Als *Galoisgruppe* $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ der Körpererweiterung $\mathbb{L}:\mathbb{K}$ bezeichnet man den punktweisen Stabilisator von $\mathbb{K}$ in der Automorphismengruppe von $\mathbb{L}$:

$$\mathrm{Gal}(\mathbb{L}:\mathbb{K}) := \{\sigma \in \mathrm{Aut}(\mathbb{L}) \mid \forall\, \kappa \in \mathbb{K}\colon \sigma(\kappa) = \kappa\} = \mathrm{Aut}(\mathbb{L})_{\mathbb{K}}.$$

•

Man kan dies auch noch anders formulieren, denn wir wissen ja, daß $\mathbb{L}$ ein $\mathbb{K}-$Vektorraum ist:

10.1.2 Hilfssatz $\sigma \in \mathrm{Aut}(\mathbb{L})$ *liegt genau dann in* $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$, *wenn* σ *eine lineare Abbildung auf dem* $\mathbb{K}-$*Vektorraum* $\mathbb{L}$ *induziert.*

Beweis: Ist σ $\mathbb{K}$-linear, dann gilt

$$\sigma(\kappa) = \sigma(\kappa \cdot 1_{\mathbb{L}}) = \kappa\sigma(1_{\mathbb{L}}) = \kappa.$$

Ist umgekehrt $\sigma \in \mathrm{Gal}(\mathbb{L}:\mathbb{K})$, dann haben wir, für jedes $x \in \mathbb{L}$,

$$\sigma(\kappa x) = \sigma(\kappa)\sigma(x) = \kappa\sigma(x),$$

σ ist also $\mathbb{K}$-linear. □

10.1.3 Folgerung

$$\mathrm{Gal}(\mathbb{L}:\mathbb{K}) = \mathrm{Aut}(\mathbb{L})_{\mathbb{K}} = \mathrm{End}_{\mathbb{K}}(\mathbb{L}) \cap \mathrm{Aut}(\mathbb{L}).$$

Wir können ein Element σ der Galoisgruppe also auch als *lineare Abbildung* — und nicht nur als *Körperautomorphismus* — betrachten. Eine dritte Interpretationsmöglichkeit kommt hinzu: $\sigma \in \mathbb{L}^{\mathbb{L}}$ zeigt, daß σ auch als *Vektor* verstanden werden kann, denn $\mathbb{L}^{\mathbb{L}}$ ist ja ein $\mathbb{L}-$Vektorraum! Tatsächlich werden wir gleich sehen, daß $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ sich als linear unabhängige Menge erweist, so daß an wichtigen Stellen dieser Theorie *Dimensionsargumente* benutzt werden können. Dies wird mit dem folgenden ganz allgemeinen Satz fundiert:

10.1.4 Der Satz von Dedekind *Sei* $\mathbb{L}$ *ein Körper,* H *eine nicht leere, multiplikativ geschriebene Halbgruppe. Dann ist die Menge* $\mathrm{Hom}(H,\mathbb{L})^*$ *der Homomorphismen* $\neq 0$ *von* H *in* $\mathbb{L}$ *als Teilmenge des* $\mathbb{L}$*-Vektorraums* $\mathbb{L}^H$ *linear unabhängig.*

Beweis: Sei $\{\sigma_0, \ldots, \sigma_{n-1}\}_{\neq} \subseteq \mathrm{Hom}(H, \mathbb{L})^*$. Wir zeigen, per Induktion nach n, daß jede Linearkombination der Nullabbildung aus diesen σ_i trivial sein muß.

i) $n = 1$: Wegen $\sigma_0 \neq 0$ erzwingt $\lambda \cdot \sigma_0 = 0$, daß $\lambda = 0$.

ii) $n > 1$: Wegen $\sigma_0 \neq \sigma_{n-1}$ gibt es $h' \in H$ mit $\sigma_0(h') \neq \sigma_{n-1}(h')$. Der Ansatz $\sum_i \lambda_i \sigma_i = 0$ ergibt, für jedes $h \in H$, die beiden Gleichungen

$$\sum_{i=0}^{n-1} \lambda_i \sigma_i(h'h) = 0 = \sigma_{n-1}(h') \sum_{i=0}^{n-1} \lambda_i \sigma_i(h).$$

Subtraktion der rechten von der linken Seite liefert — unter Verwendung der Homomorphieeigenschaft von σ_i — die Identität

$$\sum_{i=0}^{n-2} \lambda_i (\sigma_i(h') - \sigma_{n-1}(h'))\sigma_i(h) = 0.$$

Die Induktionsannahme impliziert die lineare Unabhängigkeit von $\{\sigma_0, \ldots, \sigma_{n-2}\}$, und damit

$$\lambda_i(\sigma_i(h') - \sigma_{n-1}(h')) = 0, 0 \leq i \leq n-2,$$

woraus, wegen $\sigma_0(h') \neq \sigma_{n-1}(h')$, die Identität $\lambda_0 = 0$ folgt.
Aus $\lambda_0 = 0$ folgt aber $\sum_{i=1}^{n-1} \lambda_i \sigma_i = 0$, so daß sich mit der Induktionsannahme auch $\lambda_1 = \ldots = \lambda_{n-1} = 0$, und damit die lineare Unabhängigkeit der σ_i, insgesamt also die Behauptung ergibt. □

10.1.5 Folgerung $\mathrm{Aut}(\mathbb{L})$ *ist, als Teilmenge des* $\mathbb{L}$*-Vektorraums* $\mathbb{L}^{\mathbb{L}}$*, linear unabhängig, ebenso natürlich auch die Teilmenge* $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$*. Beide Mengen sind auch* $\mathbb{K}-$*linear unabhängig, als Teilmengen von* $\mathbb{L}^{\mathbb{L}}$*, als* $\mathbb{K}-$*Vektorraum.*

Dies ermöglicht den Beweis von

10.1.6 Satz *Ist* $[\mathbb{L} : \mathbb{K}]$ *endlich, dann gilt*

$$dim_{\mathbb{L}}(\mathrm{End}_{\mathbb{K}}(\mathbb{L})) = [\mathbb{L} : \mathbb{K}] \geq |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|.$$

Ist $[\mathbb{L} : \mathbb{K}]$ *endlich und* $\mathbb{L} : \mathbb{K}$ *normal und separabel, dann gilt sogar*

$$|\mathrm{Gal}(\mathbb{L} : \mathbb{K})| = [\mathbb{L} : \mathbb{K}].$$

Beweis:

i) Ist $\{\beta_0, \ldots, \beta_{n-1}\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$, dann bilden die $f_i \in \mathrm{End}_{\mathbb{K}}(\mathbb{L}), i \in n$, definiert durch $f_i(\beta_k) := \delta_{ik}$ eine $\mathbb{K}$-Basis von $\mathrm{End}_{\mathbb{K}}(\mathbb{L})$. Daraus folgt die Behauptung, denn die Galoisgruppe liegt in $\mathrm{End}_{\mathbb{K}}(\mathbb{L})$, und sie besteht aus linear unabhängigen Elementen.

ii) Ist $\mathbb{L} : \mathbb{K}$ darüberhinaus normal und separabel, dann gibt es β_i mit

$$\mathbb{L} = \mathbb{K}(\beta_0, \ldots, \beta_{n-1}).$$

Wegen der Separabilität sind die β_i separabel, also auch algebraisch. Nach dem Satz vom primitiven Element folgt die Existenz eines $\lambda \in \mathbb{L}$ mit

$$\mathbb{L} = \mathbb{K}(\lambda).$$

Das Minimalpolynom $f_{\mathbb{K},\lambda}$ von λ ist separabel, die Wurzeln $\lambda = \lambda_1, \ldots, \lambda_n$ also alle verschieden, und sie liegen in $\mathbb{L}$, wegen der Normalität. Für die Erweiterungen gibt es also $\sigma_i \in \mathrm{Aut}(\mathbb{L})$ mit $\sigma_i(\lambda) = \lambda_i$, die $\mathbb{K}$ elementweise fest lassen. Die σ_i liegen also in der Galoisgruppe, und es folgt $n \leq |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|$. Zusammen mit der Abschätzung der Ordnung der Galoisgruppe nach oben in i) folgt damit die Behauptung. □

10.1.7 Beispiele Wir fassen zunächst die *allgemeine Methode zur Bestimmung von Galoisgruppen endlicher normaler und separabler Erweiterungen* zusammen, die sich aus obigen Beweisen ergibt:

i) Ist $\mathbb{L} : \mathbb{K}$ endlich, normal und separabel, dann kann man wie folgt vorgehen:

a) Man ermittelt zunächst ein primitives Element λ, wie im Beweis vom Satz vom primitiven Element vorgeschlagen.

b) Danach bestimmt man das Minimalpolynom von λ, indem man das minimale s ermittelt, für welches $\{1, \lambda, \ldots, \lambda^s\}$ linear abhängig ist (vgl. 8.2.6). Gilt hierfür
$$\lambda^s = \kappa_{s-1}\lambda^{s-1} + \ldots + \kappa_0,$$
dann ist
$$f_{\mathbb{K},\lambda} = x^s - \kappa_{s-1}x^{s-1} - \ldots - \kappa_0.$$

c) Dann folgt die Berechnung der Wurzeln dieses Minimalpolynoms, hierfür sind allerdings nur wenige Methoden bekannt und sie ist nur in günstigen Fällen durchführbar.

d) Die abschließende Beschreibung der Elemente $\sigma_i\colon \lambda \mapsto \lambda_i$ der Galoisgruppe ist einfach, denn ganz offensichtlich gilt
$$\sigma_i\colon (x = \sum_{j=0}^{s-1} \kappa_j \lambda^j) \mapsto \sum_{j=0}^{s-1} \kappa_j \lambda_i^j.$$

e) Zusammenfassend ist also
$$\mathrm{Gal}(\mathbb{L} : \mathbb{K}) = \{\sigma_1 = \mathrm{id}_{\mathbb{K}}, \sigma_2, \ldots, \sigma_n\}.$$

ii) Ein konkretes und ganz einfaches Beispiel illustriert die gerade beschriebene Methode:

a) Wegen $\mathbb{C} = \{r + is \mid r, s \in \mathbb{R}\}$ ist $\mathbb{C} : \mathbb{R}$ endlich, $[\mathbb{C} : \mathbb{R}] = 2$.

b) $\mathbb{C} : \mathbb{R}$ ist auch normal, denn $\mathbb{C}$ ist algebraisch und Zerfällungskörper von $1 + x^2$.

c) Als Körper der Charakteristik 0 ist $\mathbb{C} : \mathbb{R}$ zudem separabel.

d) Ein primitives Element ist i, $\mathbb{C} = \mathbb{R}(i)$.

e) Die Menge $\{1, i, i^2\}$ ist linear abhängig, und es gilt

$$i^2 = -1 + 0 \cdot i \in \mathbb{C},$$

also

$$f_{\mathbb{R},i} = x^2 + 1$$

das Minimalpolynom von i.

f) Dieses Minimalpolynom zerfällt wie folgt in Linearfaktoren:

$$x^2 + 1 = (x - i)(x + i).$$

Die Galoisgruppe besteht demnach aus den beiden Elementen

$$\sigma_1 : i \mapsto i \text{und } \sigma_2 : i \mapsto -i.$$

Offensichtlich ist $\sigma_1 = \mathrm{id}_{\mathbb{C}}$ und σ_2 die Konjugation $r + is \mapsto r - is$.

iii) Die Kreisteilungskörper $\mathbb{Q}(\zeta)$: Hier ist ζ eine primitive n-te Einheitswurzel. Wir wissen bereits, daß folgendes gilt:

a) $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, der Kreisteilungskörper ist also eine endliche Erweiterung. Er ist algebraisch, also normal, denn er ist Zerfällungskörper von Φ_n. Als Erweiterung von $\mathbb{Q}$ ist er separabel.

b) Das Minimalpolynom von ζ zerfällt wie folgt:

$$f_{\mathbb{Q},\zeta} = \Phi_n = \prod_{k \in n : \mathrm{ggT}\,(k,n) \ni 1} (x - \zeta^k).$$

c) Für die Galoisgruppe über $\mathbb{Q}$ gilt also

$$G(\mathbb{Q}(\zeta) : \mathbb{Q}) = \{\sigma_k \mid \zeta \mapsto \zeta^k \mid \mathrm{ggT}\,(k, n) \ni 1\}.$$

Diese Galoisgruppe ist also isomorph zur Einheitengruppe des Rings $\mathbb{Z}_n$, also zur *primen Restklassengruppe* modulo n.

$\diamond$

Neben dieser systematischen Vorgehensweise gibt es in vielen Fällen erfolgreiche *ad hoc* Methoden.

10.1.8 Beispiele

i) $\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}$ ist *keine* normale Erweiterung, da $\sqrt[3]{2}$ die einzige Wurzel von $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2}\,)$ ist. Liegt σ in der Galoisgruppe, dann ist $\sigma(\sqrt[3]{2}\,)$ eine Wurzel des Minimalpolynoms von $\sqrt[3]{2}$, die in $\mathbb{Q}(\sqrt[3]{2}\,)$ liegt. Dort liegt aber nur diese eine Wurzel, so daß sich $\sigma = \mathrm{id}$ ergibt und damit

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}\,) : \mathbb{Q}) = \{1\}.$$

ii) Die Körpererweiterung $\mathbb{R} : \mathbb{Q}$ ist nicht algebraisch, also nicht normal.

a) Jedes $\sigma \in \mathrm{Aut}(\mathbb{R})$ läßt jedes Element von $\mathbb{Q}$ fest: Ist $z \in \mathbb{Z}^*$, so gilt, weil $\sigma(z) = z\sigma(1) = z$,

$$1 = \sigma\left(\frac{z}{z}\right) = z \cdot \sigma\left(\frac{1}{z}\right),$$

also

$$\sigma\left(\frac{1}{z}\right) = \frac{1}{z}.$$

Das ergibt natürlich auch, für $z' \in \mathbb{Z}$,

$$\sigma\left(\frac{z'}{z}\right) = \frac{z'}{z}.$$

b) Ist σ eine Automorphismus von $\mathbb{R}$, $x \in \mathbb{R}_{>0}$, dan gibt es $y \in \mathbb{R}$ mit $y^2 = x$, also

$$\sigma(x) = \sigma(y^2) = \sigma(y)^2 \geq 0,$$

d.h. $0 \leq x$ ergibt $\sigma(0) \leq \sigma(x)$. Daraus folgt, wegen der Homomorphie bzgl. Addition, daß $x \leq y$ die Ungleichung $\sigma(x) \leq \sigma(y)$ impliziert, σ respektiert demnach die Anordnung auf $\mathbb{R}$.

c) Jede reelle Zahl ist rational approximierbar. Sei $(x_n)_{n\in\mathbb{N}}$ eine gegen $x \in \mathbb{R}$ strebende Folge rationaler Zahlen. Für alle $n \in \mathbb{N}$ gibt es dann $N_n \in \mathbb{N}$ mit

$$\forall\ k \geq N_n\colon\ x - \frac{1}{n} \leq x_k \leq x + \frac{1}{n}.$$

Dies impliziert

$$\sigma(x) - \frac{1}{n} \leq x_k \leq \sigma(x) + \frac{1}{n}.$$

Hieraus folgt die Konvergenz von $(x_k)_{k\in\mathbb{N}}$ gegen $\sigma(x)$ und daraus $\sigma(x) = x$. σ läßt also auch die reellen Zahlen fest, es gilt

$$\mathrm{Gal}(\mathbb{R} : \mathbb{Q}) = \{1\}.$$

iii) Wichtig ist die Galoisgruppe eines Galoisfelds über einem endlichen Primkörper. Hierzu wissen wir folgendes:

a) Der Körpergrad ist $[GF(p^n) : GF(p)] = n$.

b) Der Erweiterungskörper $GF(p^n)$ ist Zerfällungskörper von $x^{(p^n)} - x$.

c) Die Erweiterung ist normal und separabel, die Ordnung der Galoisgruppe also gleich dem Körpergrad n.

d) Wir wissen bereits, daß der Frobeniusautomorphismus $\sigma\colon \kappa \mapsto \kappa^p$ in der Galoisgruppe liegt, denn er läßt den Primkörper elementweise fest.

e) Dieser Automorphismus hat die Ordnung n. Setzen wir nämlich $m := |\langle\sigma\rangle|$, so gilt

$$\forall\ \kappa \in GF(p^n)\colon \kappa^{(p^m)} = \kappa,$$

was $GF(p^n) \subseteq GF(p^m)$ und damit $n \leq m$ ergibt. Andererseits gilt aber $m \leq |\mathrm{Gal}(GF(p^n) : GF(p)| = n$, insgesamt also $m = n$. σ erzeugt demnach die Galoisgruppe:

$$\mathrm{Gal}(GF(p^n) : GF(p)) = \langle\sigma\rangle \simeq C_n.$$

$\diamond$

10.2 Galoisverbindungen

Es sei eine Körpererweiterung $\mathbb{L} : \mathbb{K}$ gegeben. Zu $A \subseteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ sei

$$\mathbb{L}_A := \{\lambda \in \mathbb{L} \mid \forall\, \sigma \in A \colon \sigma(\lambda) = \lambda\},$$

die Menge der Fixpunkte von A. Man sieht leicht ein, daß diese Menge ein *Zwischenkörpe* ist, $\mathbb{K} \leq \mathbb{L}_A \leq \mathbb{L}$, der *Fixkörper* von A in $\mathbb{L}$. Weil A in der Galoisgruppe $\mathrm{Gal}(\mathbb{L} : \mathbb{L}_A)$ liegt, gilt die Abschätzung

10.2.1 $$|A| \leq [\mathbb{L} : \mathbb{L}_A].$$

Wir wollen jetzt den *Untergruppenverband der Galoisgruppe,*

$$\mathrm{U}(\mathrm{Gal}(\mathbb{L} : \mathbb{K})) := \{U \mid U \leq \mathrm{Gal}(\mathbb{L} : \mathbb{K})\},$$

mit dem *Verband der Zwischenkörper,*

$$\mathrm{ZwK}(\mathbb{L} : \mathbb{K}) := \{\mathbb{M} \mid \mathbb{K} \leq \mathbb{M} \leq \mathbb{L}\},$$

in Verbindung bringen. Dazu verwenden wir die Abbildungen

$$\Phi \colon \mathrm{U}(\mathrm{Gal}(\mathbb{L} : \mathbb{K})) \to \mathrm{ZwK}(\mathbb{L} : \mathbb{K})\,,\ U \mapsto \mathbb{L}_U$$

und

$$\Gamma \colon \mathrm{ZwK}(\mathbb{L} : \mathbb{K}) \to \mathrm{U}(\mathrm{Gal}(\mathbb{L} : \mathbb{K}))\,,\ \mathbb{M} \mapsto \mathrm{Gal}(\mathbb{L} : \mathbb{M}).$$

Es wird sich zeigen, daß die im folgenden Hilfssatz aufgelisteten und leicht nachvollziehbaren Eigenschaften dieser Abbildungen entscheidend sind:

10.2.2 Hilfssatz

i) Φ *und* Γ *sind antiton,*

$$U_0 \leq U_1 \Longrightarrow \mathbb{L}_{U_0} \geq \mathbb{L}_{U_1},\ \mathbb{M}_0 \leq \mathbb{M}_1 \Longrightarrow \mathrm{Gal}(\mathbb{L} : \mathbb{M}_0) \geq \mathrm{Gal}(\mathbb{L} : \mathbb{M}_1).$$

ii) $\Gamma \circ \Phi$ *und* $\Phi \circ \Gamma$ *sind extensiv:*

$$\mathbb{M} \subseteq \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{M})},\ U \subseteq \mathrm{Gal}(\mathbb{L} : \mathbb{L}_U).$$

Das Paar (Φ, Γ) dieser Abbildungen ist also eine *Galoisverbindung* zwischen dem Untergruppenverband der Galoisgruppe und dem Zwischenkörperverband, im Sinne der folgenden Definition:

10.2.3 Definition (Galoisverbindung) Sind $(M, \leq)$ und $(N, \leq)$ nicht leere Halbordnungen, dann bilden $\sigma \in N^M$ und $\tau \in M^N$ genau dann eine *Galoisverbindung* (σ, τ), wenn die beiden Abbildungen σ und τ antiton und ihre Kompositionen $\sigma\tau$ und $\tau\sigma$ extensiv sind:

$$m \leq m' \Longrightarrow \sigma(m) \geq \sigma(m'),\ n \leq n' \Longrightarrow \tau(n) \geq \tau(n'),$$

und

$$m \leq \tau(\sigma(m)),\ n \leq \sigma(\tau(n)).$$

•

Man prüft leicht nach, daß folgendes gilt:

10.2.4 Hilfssatz *Für Galoisverbindungen (σ, τ) gilt stets:*

i) $\sigma\tau\sigma = \sigma,\ \tau\sigma\tau = \tau$.

ii) Sind beide Elemente der Galoisverbindung surjektiv oder sind beide Elemente der Galoisverbindung injektiv, dann sind diese beiden Abbildungen auch bijektiv.

Beweis: Die erste Behauptung folgt leicht mit der Extensivität und der Antitonie, während man die zweite schnell aus der ersten herleiten kann, denn Abbildungen sind genau dann surjektiv (injektiv), wenn sie rechts (links) kürzbar sind. □

10.2.5 Beispiele weiterer Galoisverbindungen:

i) $M := N := \mathbb{Q}_{>0}$ ist, zusammen mit $\leq$, eine Halbordnung. Setzen wir $\sigma := \tau\colon x \mapsto x^{-1}$, dann ist (σ, τ) eine Galoisverbindung.

ii) Die Teilbarkeit definiert eine Halbordnung $(N, \leq) := (\mathbb{N}^*, |\,)$ auf $\mathbb{N}$. Eine weitere Halbordnung besteht aus den *Teilermengen*

$$T(n) := \{t \mid t \in \mathbb{N}^*, t \text{ teilt } n\}.$$

zusammen mit der Inklusion:

$$(M, \leq) := (\{T(n) \mid n \in \mathbb{N}^*\}, \subseteq).$$

Setzen wir

$$\sigma\colon \{T(n) \mid n \in \mathbb{N}^*\} \to \mathbb{N}^*\,,\ T(n) \mapsto n$$

und

$$\tau\colon \mathbb{N}^* \to \{T(n) \mid n \in \mathbb{N}^*\}\,,\ n \mapsto T(n),$$

dann ist (σ, τ) eine Galoisverbindung.

iii) Ein interessanteres Beispiel findet sich auf dem Übungsblatt. Ist ${}_GX$ eine Gruppenoperation, dann gibt es eine natürliche Galoisverbindung zwichen dem Untergruppenverband $U(G)$ von G und der Halbordnung (via Verfeinerung) der Partitionen von X. Man erhält sozusagen eine *Galoistheorie der Gruppenoperation.*

iv) Eine weitere wichtige Anwendung einer Galoisverbindung findet man in der *Begriffsanalyse.* Dort werden u.a. Kontexte mit Hilfe des zugehörigen *Begriffsverbands* visualisiert, und den Begriffsverband bekommt man mit Hilfe einer Galoisverbindung.
Unter einem *(einwertigen) Kontext* versteht man in der Begriffsanalyse ein Tripel

$$\mathcal{K} := (G, M, I),$$

bestehend aus einer Menge G von Gegenständen, einer Menge M von Merkmalen und einer Relation I zwischen diesen beiden, also $I \subseteq G \times M$. $(g, m) \in I$ bedeute, *der Gegenstand g habe oder besitze das Merkmal m*, oder *m komme g zu.*
Einen endlichen Kontext $\mathcal{K} = (G, M, I)$ können wir, wie bei binären Relationen allgemein üblich, nach Numerierung der Elemente von G und M, etwa $G = \{g_1, g_2, \ldots\}$ und $M = \{m_1, m_2, \ldots\}$, als eine $|G| \times |M|-$Matrix $\Gamma(\mathcal{K})$ mit Einträgen 0 oder 1 notieren, oder auch als sogenannte *Kreuzchentabelle,* wobei anstelle der Einsen ein Kreuzchen $\times$, an allen anderen Stellen nichts eingefügt wird:

$$\Gamma(\mathcal{K}) = (\gamma_{ik}),\ \textit{mit}\ \gamma_{ik} := \begin{cases} 1, & \text{falls } g_i I m_k \\ 0, & \text{sonst.} \end{cases}$$

Der mathematische Kontext mit der folgenden Gegenstandsmenge $G := \{2, \sqrt{2}, \pi\}$ aus reellen Zahlen und der Merkmalsmenge

$$M := \{\underline{r}ational, \underline{i}rrational, \underline{a}lgebraisch, \underline{t}ranszendent\},$$

also ein Kontext, der Wissen aus der Algebra-Vorlesung beschreiben kann, ergibt dabei die 0, 1-Matrix bzw. die Kreuzchentabelle

10.2.6

$g_i \backslash m_k$	r	i	a	t
2	1	0	1	0
$\sqrt{2}$	0	1	1	0
π	0	1	0	1

bzw.

$g_i \backslash m_k$	r	i	a	t
2	$\times$		$\times$	
$\sqrt{2}$		$\times$	$\times$	
π		$\times$		$\times$

Ein Begriff β zum Kontext (G, M, I) ist ein Paar (A, B) aus einer Gegenstandsmenge A, dem *Umfang* von β, d. h. der Menge aller Gegenstände, die unter den Begriff β fallen, und aus einer Merkmalsmenge B, dem *Inhalt* von β, d. h. der Menge aller Merkmale, die dem Begriff β zukommen. Dabei muß jeder Gegenstand aus A jedes Merkmal aus B besitzen und umgekehrt, es muß also gIm gelten für alle $g \in A$ und alle $m \in B$.
Dieser Zusammenhang zwischen Umfang und Inhalt eines Begriffs legt es nun nahe, allgemeiner für *beliebige* Gegenstandsmengen A und Merkmalsmengen B die *Ableitungen* A' und B' einzuführen:

$$A' := \{m \in M \mid \forall\ g \in A\colon\ gIm\},\ B' := \{g \in G \mid \forall\ m \in B\colon\ gIm\}.$$

Ein *Begriff* zum Kontext (G, M, I) ist ein Paar $\beta := (A, B)$ mit $A \subseteq G, B \subseteq M$ und $A' = B, B' = A$. Dabei heiße A der *Umfang,* auch die *Extension,* und B der *Inhalt* oder die *Bedeutung,* auch *Intension,* des Begriffs β. Ein Beispiel für einen Begriff im Rahmen des Kontextes 10.2.6 ist

$$(A, B) := (\{\pi\}, \{i, t\}).$$

Mit $\mathrm{BV}(\mathcal{K})$ wollen wir *die Menge aller Begriffe zum Kontext $\mathcal{K} = (G, M, I)$* bezeichnen, also

$$\mathrm{BV}(\mathcal{K}) := \{(A, B) \mid A \subseteq G, B \subseteq M, A' = B, B' = A\}.$$

Diese Menge können wir hierarchisch anordnen, was der üblichen Einteilung in *Ober- und Unterbegriffe* entspricht. Dazu bemerken wir, daß die Ableitungen antiton sind:

$$A_1 \subseteq A_2 \Longrightarrow A_1' \supseteq A_2',\ B_1 \subseteq B_2 \Longrightarrow B_1' \supseteq B_2'$$

und extensiv:

$$A \subseteq A'',\ B \subseteq B''.$$

Das Paar $(-', -')$ ist also eine Galoisverbindung!

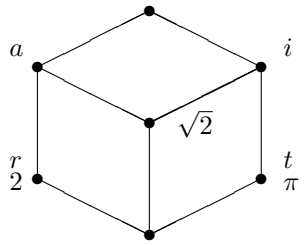
Da man in den natürlichen Sprachen als Unterbegriff eines Begriffes β einen spezielleren Begriff als β bezeichnet, also einen, der meist weniger Gegenstände als β umfaßt, dafür aber in der Regel mehr Merkmale als β aufweist, ordnen wir $\mathrm{BV}(\mathcal{K})$ entsprechend an: Für Begriffe $(A_i, B_i) \in \mathrm{BV}(\mathcal{K})$, mit $i = 1, 2$, sei

$$(A_1, B_1) \leq (A_2, B_2) :\Longleftrightarrow A_1 \subseteq A_2\ (\Longleftrightarrow B_2 \subseteq B_1).$$

(A_1, B_1) heißt dabei *Unterbegriff* von (A_2, B_2), und entsprechend (A_2, B_2) *Oberbegriff* von (A_1, B_1). Wir erhalten so die geordnete Menge

$$(\mathrm{BV}(\mathcal{K}), \leq),$$

den Begriffsverband zum Kontext $\mathcal{K}$. Er veranschaulicht — mit Hilfe geeigneter Beschriftung — die Information, die in dem Kontext steckt. Für unser Beispiel erhält man das Hasse Diagramm



◇

Die Kompositionen $\sigma\tau$ und $\tau\sigma$ der Elemente einer Galoisverbindung (σ, τ) haben eine weitere interessante Eigenschaft, sie sind *Hüllenoperatoren* im folgenden Sinn:

10.2.7 Definition (Hüllenoperatoren) $(X, \leq)$ eine (partiell) geordnete Menge, dann heißt eine Abbildung

$$X \to X\,,\ x \mapsto \overline{x}$$

von X in sich *Hüllenoperator* (auf X), wenn sie die folgenden Eigenschaften hat:

- $x \leq \overline{x}$ *(Extensivität)*

- $x \leq y \Rightarrow \overline{x} \leq \overline{y}$ *(Monotonie)*
- $\overline{\overline{x}} = \overline{x}$ *(Idempotenz)*

für alle $x, y \in X$; dabei heißt $\overline{x}$ auch *Abschluß von* x oder *abgeschlossen* (bez. des Hüllenoperators) oder *von* x *erzeugt.* •

Hüllenoperatoren kommen häufig vor:

10.2.8 Beispiele von Hüllenoperatoren:

i) Ein Hüllenoperator ist zum Beispiel die Abbildung, die jedem reellen x die kleinste ganze Zahl $\geq x$ zuordnet:

$$\lceil\text{-}\rceil\colon \mathbb{R} \to \mathbb{R}\,,\ x \mapsto \lceil x \rceil := \mathrm{Min}\{z \in \mathbb{Z} \mid x \leq z\}$$

ist Hüllenoperator auf $\mathbb{R}$.

ii) Noch einfacher sind die identischen Abbildungen $x \mapsto x$, die natürlich ebenfalls Hüllenoperatoren sind. Bei den folgenden grundlegenden Beispielen ist die Halbordnung jeweils die Mengeninklusion $\subseteq$ auf der Potenzmenge einer Menge M :

- Die Bildung der *konvexen Hülle* von Teilmengen x des Raums $M = \mathbb{R}^n$.
- Die Bildung der *transitiven Hülle* von Relationen x, also von Teilmengen $x \subseteq M = N \times N$.
- Die Zuordnung der *abgeschlossenen Hülle* zu einer Teilmenge x eines topologischen Raums M.
- Das Erzeugnis $\overline{x}$ einer Teilmenge x einer algebraischen Struktur M, also beispielsweise die *lineare Hülle* von x in einem Vektorraum M.

◇

Die abgeschlossenen Mengen spielen eine wichtige Rolle, wir erwähnen deshalb die folgenden wichtigen Konsequenzen aus dem Bisherigen:

10.2.9 Satz *Ist* (σ, τ) *Galoisverbindung zwischen* $(M, \leq)$ *und* $(N, \leq)$*, dann sind* $\sigma\tau$ *und* $\tau\sigma$ *Hüllenoperatoren, und die Mengen der abgeschlossenen Elemente in* N *bzw.* M *sind*

$$\overline{N} := \sigma(M) = \{\sigma(m) \mid m \in M\},\ \overline{M} := \tau(N) = \{\tau(n) \mid n \in N\}.$$

Diese beiden Mengen sind ordnungsantiisomorph vermöge der entsprechenden und zueinander inversen Einschränkungen von σ *und* τ*.*

Beweis: Die Eigenschaft von $\sigma\tau$ und $\tau\sigma$ Hüllenoperator zu sein, ist sehr leicht nachzurechnen, ebenso die Tatsache, daß $\overline{N}$ bzw. $\overline{M}$ gerade aus den abgeschlossenen Elementen von N bzw. M bestehen.

Die Ordnungsantiisomorphie bedeutet, daß

$$\tau\colon \overline{N} \to \overline{M}\,,\ \overline{n} := \sigma(m) \mapsto \tau(\sigma(m)) = \tau(\overline{n})$$

bijektiv ist und Ordnungsantiisomorphismus, d.h.

$$\overline{n}_1 \leq \overline{n}_2 \iff \tau(\overline{n}_1) \geq \tau(\overline{n}_2),$$

bzw. daß analog für

$$\sigma\colon \overline{M} \to \overline{N}\,,\ \overline{m} := \tau(n) \mapsto \sigma(\tau(n)) = \sigma(\overline{m})$$

gilt

$$\overline{m}_1 \leq \overline{m}_2 \iff \sigma(\overline{m}_1) \geq \sigma(\overline{m}_2).$$

□

Ähnlich wie mit antitonen Abbildungen kann man natürlich auch mit monotonen verfahren:

10.2.10 Definition (Galoisfunktionen) Sind $(M, \leq)$ und $(N, \leq)$ Halbordnungen, dann heißt $\alpha\colon M \to N$ *Galoisfunktion*, wenn eine Abbildung $\beta\colon N \to M$ existiert, so daß gilt

- α und β sind monoton,
- $\beta\alpha$ ist exteniv: $m \leq \beta\alpha(m)$,
- $\alpha\beta$ ist intensiv: $n \geq \alpha\beta(n)$.

•

(Vgl. Übungsblatt)

10.3 Galoiserweiterungen, der Hauptsatz

Kehren wir wieder zu der oben beschriebenen Galoisverbindung (Φ, Γ) zurück. Wir bemerken zunächst, daß gilt:

10.3.1 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Körpererweiterung, dann gilt:*

- *Für jedes* $U \leq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *ist*

$$U = \mathrm{Gal}(\mathbb{L} : \mathbb{L}_U),\ |U| = [\mathbb{L} : \mathbb{L}_U].$$

- $\Gamma \circ \Phi = \mathrm{id}_{\mathrm{U}(\mathrm{Gal}(\mathbb{L}:\mathbb{K}))}$, Γ *ist also surjektiv, und* Φ *ist injektiv.*

Beweis:

i) Trivialerweise ist $U \leq \mathrm{Gal}(\mathbb{L} : \mathbb{L}_U)$, 10.1.6 liefert $|\mathrm{Gal}(\mathbb{L} : \mathbb{L}_U)| \leq [\mathbb{L} : \mathbb{L}_U]$, es gilt also $|U| \leq [\mathbb{L} : \mathbb{L}_U]$. Zum Beweis des ersten Punkts genügt demnach der Beweis von

$$|U| \geq [\mathbb{L} : \mathbb{L}_U],$$

bzw. der Nachweis, daß beliebige $|U| + 1$ Elemente

$$\lambda_0, \ldots, \lambda_{|U|} \in \mathbb{L}$$

über $\mathbb{L}_U$ linear abhängig sind. Zu diesem Zweck betrachten wir eine Gleichung $\sum_i \lambda_i x_i = 0$, mit Koeffizienten $x_i \in \mathbb{L}_U$. Wenden wir auf beiden Seiten $\sigma \in U$ an, so erhalten wir, weil σ jedes $x_i \in \mathbb{L}_U$ fest läßt, das lineare Gleichungssystem

$$\sum_{i=0}^{|U|} \sigma^{-1}(\lambda_i) x_i = 0,\ \sigma \in U.$$

Die Anzahl $|U|$ der Gleichungen ist dabei kleiner als die der Unbestimmten, es gibt also nichttriviale Lösungen

$$(x_0, \ldots, x_{|U|}) \neq 0.$$

Ohne Einschränkung können wir $x_0 \neq 0$ annehmen, denn andernfalls können wir die λ_i ja umnumerieren. Weil es sich bei dieser nichttrivialen Lösung um eine Lösung eines homogenen Gleichungssystems handelt, können wir dieses x_0 sogar beliebig vorgeben.
Das Gleichungssystem ist äquivalent zu dem Gleichungssystem

$$\sum_i \lambda_i \sigma(x_i) = 0,\ \sigma \in U,$$

aus dem wir jetzt, durch Aufsummieren der Gleichungen, die Identität

$$\sum_i \left(\sum_{\sigma \in U} \sigma \right) (x_i) \lambda_i = 0$$

bekommen. Nach dem Satz von Dedekind ist $\sum\sigma \neq 0$, es gibt also geeignete $x_0 \in \mathbb{L}_U$, für die $(\sum\sigma)(x_0) \neq 0$ gilt. Die λ_i sind also tatsächlich linear abhängig über $\mathbb{L}_U$. Das beweist den ersten Punkt.

ii) Zum Nachweis der zweiten Behauptung bemerken wir, daß

$$(\Gamma \circ \Phi)(U) = \Gamma(\Phi(U)) = \Gamma(\mathbb{L}_U) = \mathrm{Gal}(\mathbb{L} : \mathbb{L}_U) = U,$$

letzere Gleichung nach i).

□

Wir kommen damit zur Formulierung einer Bedingung, die gewährleistet, daß Φ und Γ (zueinander inverse) Bijektionen sind:

10.3.2 Definition (Galoiserweiterung) Eine Körpererweiterung $\mathbb{L} : \mathbb{K}$ heißt *Galoiserweiterung,* wenn

$$\mathbb{K} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}$$

gilt, d.h. wenn $\mathbb{K}$ der Fixkörper der Galoisgruppe ist. •

Beispielsweise ist $\mathbb{R} : \mathbb{Q}$ *keine* Galoiserweiterung, denn $\mathrm{Aut}(\mathbb{R}) = \{1\}$, wie bereits erwähnt. Dagegen ist $\mathbb{C} : \mathbb{R}$ eine Galoiserweiterung.

Für endliche Erweiterungen $\mathbb{L} : \mathbb{K}$ läßt sich die Bedingung Galoiserweiterung zu sein auch anders formulieren bzw. nachweisen:

10.3.3 Satz *Ist* $[\mathbb{L} : \mathbb{K}] \in \mathbb{N}$, *dann sind äquivalent:*

i) $\mathbb{L} : \mathbb{K}$ *ist Galoiserweiterung,*

ii) $[\mathbb{L} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|$,

iii) $\mathbb{L} : \mathbb{K}$ *ist normal und separabel,*

iv) $\mathbb{L}$ *ist Zerfällungskörper eines über* $\mathbb{K}$ *separablen Polynoms.*

Beweis:

i)$\Rightarrow$ ii):

$$[\mathbb{L} : \mathbb{K}] \in \mathbb{N} \Rightarrow_{10.3.1} |\mathrm{Gal}(\mathbb{L} : \mathbb{K})| = [\mathbb{L} : \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}] =_{i)} [\mathbb{L} : \mathbb{K}].$$

ii)$\Rightarrow$ i):

$$[\mathbb{L} : \mathbb{K}] =_{ii)} |\mathrm{Gal}(\mathbb{L} : \mathbb{K})| =_{10.3.1} [\mathbb{L} : \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}] \Rightarrow_{\mathbb{K}\subseteq\mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}} \mathbb{K} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}.$$

i)$\Rightarrow$ iii): Sei $\lambda \in \mathbb{L}$. Wir betrachten die Bahn dieses Elements unter der Galoisgruppe:

$$\mathrm{Gal}(\mathbb{L} : \mathbb{K})(\lambda) = \{\lambda = \lambda_0, \ldots, \lambda_{n-1}\},$$

und das normierte Polynom mit diesen Wurzeln:

$$f_\lambda := \prod_{i\in n}(x - \lambda_i) = \sum_{j\in n}\mu_j x^j,\ \mu_j \in \mathbb{L}.$$

Für die Fortsetzung $\tilde{\sigma}$ von σ auf $\mathbb{L}[x]$ gilt

$$\tilde{\sigma}(f_\lambda) = \sum \sigma(\mu_j)x^j = \prod(x - \sigma(\lambda_i)) = f_\lambda,$$

es gilt also $\mu_j = \sigma(\mu_j)$, für alle $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$, also, wegen i), $\mu_j \in \mathbb{K}$ und damit $f_\lambda \in \mathbb{K}[x]$. Weil f_λ separabel ist, gilt das auch für λ, die Erweiterung $\mathbb{L} : \mathbb{K}$ ist demnach separabel. Sie ist auch normal: Ist $\{b_0, \ldots, b_{[\mathbb{L}:\mathbb{K}]-1}\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$, dann können wir — analog zu f_λ — die Polynome f_{b_i} betrachten, $\mathbb{L}$ ist Zerfällungskörper von deren Produkt $f = \prod_i f_{b_i}$, die Erweiterung also normal.

iii)$\Rightarrow$ iv) ist klar.

iv)$\Rightarrow$ i): Sei $\mathbb{L}$ Zerfällungskörper von $f \in \mathbb{K}[x]$, f separabel. Die Implikation $\mathbb{K} \subseteq \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}$ ist klar, es gilt, die Umkehrung zu beweisen. Wir induzieren nach der Anzahl r der nicht in $\mathbb{K}$ liegenden Wurzeln von f.

I $r = 0$: $\mathbb{K} = \mathbb{L}$ ergibt die Behauptung.

II $r > 0$: Sei $\lambda \notin \mathbb{K}$, aber Wurzel von f. Dann ist $f = f_{\mathbb{K},\lambda} \cdot h$. Wir betrachten $\mathbb{M} := \mathbb{K}(\lambda)$. $\mathbb{L}$ ist Zerfällungskörper von f über $\mathbb{K}$, also auch über $\mathbb{M}$. Die Induktionsannahme liefert, daß $\mathbb{L} : \mathbb{M}$ eine Galoiserweiterung ist, es gilt demnach $\mathbb{M} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{M})}$ und damit

$$\mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})} \subseteq \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{M})} = \mathbb{M} = \mathbb{K}(\lambda).$$

Ist $s := [\mathbb{K}(\lambda) : \mathbb{K}] = \mathrm{Grad}(f_{\mathbb{K},\lambda})$, dann gibt es, zu jedem $x \in \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}$, Elemente κ_i von $\mathbb{K}$ mit

$$x = \kappa_0 + \kappa_1\lambda^1 + \ldots + \kappa_{s-1}\lambda^{s-1}.$$

Wir wollen zeigen, daß $x = \kappa_0 \in \mathbb{K}$.
f ist separabel, also auch $f_{\mathbb{K},\lambda}$, die (verschiedenen) Wurzeln dieses Minimalpolynoms seien $\lambda = \lambda_0, \ldots, \lambda_{s-1}$. Wir wissen, daß es Isomorphismen $\varphi_i\colon \mathbb{K}(\lambda) \simeq \mathbb{K}(\lambda_i)$ gibt mit $\varphi_i(\lambda) = \lambda_i$, und die auf $\mathbb{K}$ die identische Abbildung induzieren. ϕ_i sei die Fortsetzung von φ_i auf $\mathbb{L}$. Wegen $\phi_i \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ und $\phi_i(\lambda) = \lambda_i$ gilt

$$\forall\, x \in \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})}\colon\ x = \phi_i(x) = \kappa_0 + \kappa_1\lambda_i^1 + \ldots + \kappa_{s-1}\lambda_i^{s-1}.$$

Das Polynom

$$g := (\kappa_0 - x) + \kappa_1\mu^1 + \ldots + \kappa_{s-1}\mu^{s-1}$$

hat dann die $\lambda_i, i \in s$, als Wurzeln, obwohl es nur den Grad $s - 1$ hat, es muß also das Nullpolynom sein, d.h. es gilt $x = \kappa_0 \in \mathbb{K}$ und damit $\mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{K})} \subseteq \mathbb{K}$, was noch zu zeigen war. □

Endliche Galoiserweiterungen $\mathbb{L} : \mathbb{K}$ sind also genau die endlichen Körpererweiterungen $\mathbb{L} : \mathbb{K}$, die normal und separabel sind. Hieraus folgt, daß endliche Galoiserweiterungen auch Galoiserweiterungen ihrer Zwischenkörper sind, denn endliche, normale und separable Erweiterungen sind natürlich auch endliche, normale und separable Erweiterungen ihrer Zwischenkörper $\mathbb{M}$. Es gilt demnach

$$\mathbb{M} = \mathbb{L}_{\mathrm{Gal}(\mathbb{L}:\mathbb{M})} = (\Phi\Gamma)(\mathbb{M}),$$

und wir erhalten die

10.3.4 Folgerung *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung und* $\mathbb{M}$ *ein Zwischenkörper, dann ist* $\mathbb{L} : \mathbb{M}$ *ebenfalls Galoiserweiterung. Die Komposition* $\Phi \circ \Gamma$ *induziert die Identität auf ZwK*$(\mathbb{L} : \mathbb{K})$, $\Phi: U \mapsto \mathbb{L}_U$ *ist also ebenfalls surjektiv. Die Abbildungen* Φ *und* Γ *sind zueinander inverse Ordnungsantiisomorphismen zwischen* $\mathrm{U}(\mathrm{Gal}(\mathbb{L} : \mathbb{K}))$ *und ZwK*$(\mathbb{L} : \mathbb{K})$.

Es bleibt zu untersuchen, wann $\mathbb{M} : \mathbb{K}$ Galoiserweiterung ist.

10.3.5 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung,* $\mathbb{M}$ *ein Zwischenkörper, dann sind äquivalent:*

- $\mathbb{M} : \mathbb{K}$ *ist normal,*
- $\sigma(\mathbb{M}) = \mathbb{M}$, *für alle* $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$,
- $\mathrm{Gal}(\mathbb{L} : \mathbb{M}) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$.

Beweis: $\mathbb{M}$ ist einfache Erweiterung, etwa $\mathbb{M} = \mathbb{K}(\lambda)$.

i)$\Rightarrow$ ii): Ist $\mathbb{M} = \mathbb{K}(\lambda)$ normal, dann liegen alle Wurzeln von $f_{\mathbb{K},\lambda}$ in $\mathbb{M}$. Das Bild $\sigma(\lambda)$ von λ unter der Operation eines Elements σ der Galoisgruppe ist Wurzel, liegt demnach für alle $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ in $\mathbb{M}$ und damit auch $\sigma(m = \sum_i \kappa_i \lambda^i)$. Es folgt $\sigma(\mathbb{M}) = \mathbb{M}$.

ii) $\Rightarrow$ i): Ist $\sigma(\mathbb{M}) = \mathbb{M}$, dann gilt $\sigma(\lambda) \in \mathbb{M}$. Das Polynom

$$f := \prod_{\sigma \in \mathrm{Gal}(\mathbb{L}:\mathbb{K})} (x - \sigma(\lambda)) = \sum_j \mu_j x^j$$

hat λ als Wurzel und zerfällt in Linearfaktoren. Ist jetzt $\tau \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$, dann gilt für die Fortsetzung $\tilde{\tau}$:

$$\tilde{\tau} f = \prod_{\sigma} (x - \tau\sigma(\lambda)) = f,$$

also $\tau\mu_j = \mu_j \in \mathbb{K}$. Der Zwischenkörper $\mathbb{M} = \mathbb{K}(\lambda)$ ist demnach Zerfällungskörper von f über $\mathbb{K}$, $\mathbb{M} : \mathbb{K}$ ist also normale Erweiterung.

iii) $\Leftrightarrow$ ii): Die Normalteilereigenschaft

$$\Gamma(\mathbb{M}) = \mathrm{Gal}(\mathbb{L} : \mathbb{M}) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$$

ist äquivalent zu $\sigma\Gamma(\mathbb{M})\sigma^{-1} = \Gamma(\mathbb{M})$, für alle $\sigma \in \mathrm{Gal}(\mathbb{L} : \mathbb{K})$, und das wiederum ist, wegen

$$\sigma\Gamma(\mathbb{M})\sigma^{-1} = \sigma\mathrm{Gal}(\mathbb{L} : \mathbb{M})\sigma^{-1} = \sigma\mathrm{Aut}(\mathbb{L})_{\mathbb{M}}\sigma^{-1} = \mathrm{Aut}(\mathbb{L})_{\sigma(\mathbb{M})} = \Gamma(\sigma(\mathbb{M}))$$

äquivalent zu $\Gamma(\sigma(\mathbb{M})) = \Gamma(\mathbb{M})$, für alle σ. Wegen der Injektivität von Γ ist das äquivalent zu $\sigma(\mathbb{M}) = \mathbb{M}$, für alle σ aus der Galoisgruppe.

□

Fassen wir zusammen, so ergibt sich der

10.3.6 Hauptsatz der Galoistheorie *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung, dann gilt*

- *Die Abbildungen* $\Phi: U \mapsto \mathbb{L}_U$ *und* $\Gamma: \mathbb{M} \mapsto \mathrm{Gal}(\mathbb{L} : \mathbb{M})$ *sind zueinander inverse Ordnungsantiisomorphismen zwischen dem Untergruppenverband* $\mathrm{U}(\mathrm{Gal}(\mathbb{L} : \mathbb{K}))$ *und dem Zwischenkörperverband ZwK*$(\mathbb{L} : \mathbb{K})$.
- *Für alle Zwischenkörper* $\mathbb{M}$ *ist* $\mathbb{L} : \mathbb{M}$ *ebenfalls Galoiserweiterung.*
- *Für jede Untergruppe* U *der Galoisgruppe und für jeden Zwischenkörper* $\mathbb{M}$ *von* $\mathbb{L} : \mathbb{K}$ *gilt*

$$[\mathbb{M} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{L} : \mathbb{K})/\mathrm{Gal}(\mathbb{L} : \mathbb{M})|, \ |U| = [\mathbb{L} : \mathbb{L}_U].$$

- $\mathbb{M} : \mathbb{K}$ *ist genau dann eine Galoiserweiterung, wenn* $\mathrm{Gal}(\mathbb{L} : \mathbb{M}) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *ist, in welchem Fall gilt*

$$\mathrm{Gal}(\mathbb{M} : \mathbb{K}) \simeq \mathrm{Gal}(\mathbb{L} : \mathbb{K})/\mathrm{Gal}(\mathbb{L} : \mathbb{M}).$$

□

(Die letzte Behauptung ergibt sich durch den Nachweis, daß die Einschränkung der σ auf $\mathbb{M}$ einen Epimorphismus von $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ auf $\mathrm{Gal}(\mathbb{M} : \mathbb{K})$ ergibt mit $\mathrm{Gal}(\mathbb{L} : \mathbb{M})$ als Kern!)

Als Anwendung können wir jetzt beispielsweise die noch fehlende Hälfte des Satzes über die Konstruierbarkeit regelmäßiger $n-$Ecke beweisen:

10.3.7 Satz *Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn*

$$n = 2^k p_1 \cdots p_r,$$

mit verschiedenen Fermatschen Primfaktoren $p_1, \ldots, p_r$.

Beweis:

i) Wir wissen bereits, daß diese Form von n notwendig ist (vgl. 9.2.12) für die Konstruierbarkei.

ii) Zum Beweis der Umkehrung betrachten wir den Kreisteilungskörper $\mathbb{Q}(\zeta)$, mit einer primitiven n-ten Einheitswurzel ζ.

a) Wegen
$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = 2^m,$$
m geeignet, ist $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ eine 2-Gruppe der Ordnung 2^m.

b) Da, nach dem Satz von Sylow, jede Gruppe der Ordnung 2^r eine Untergruppe der Ordnung 2^{r-1} besitzt, also einen Normalteiler vom Index 2, gibt es eine Kette
$$\{1\} = U_0 \triangleleft U_1 \triangleleft \ldots \triangleleft U_m = \mathrm{Gal}\mathbb{Q}(\zeta) : \mathbb{Q}),$$
bei der $|U_i/U_{i-1}| = 2$ gilt.

c) Nach dem Hauptsatz gibt es deshalb eine Kette von Zwischenkörpern

$$\mathbb{Q}(\zeta) = \mathbb{M}_0 \supset \mathbb{M}_1 \supset \ldots \supset \mathbb{M}_m = \mathbb{Q},$$

mit $[\mathbb{M}_i : \mathbb{M}_{i+1}] = 2$. Damit ist jedes Element von $\mathbb{Q}(\zeta)$ konstruierbar, insbesondere also ζ und damit das regelmäßige n-Eck.

□

10.4 Galoisgruppen von Polynomen

Weil der Zerfällungskörper $\mathbb{L}$ von $f \in \mathbb{K}[x] \setminus \mathbb{K}$ bis auf Isomorphie eindeutig bestimmt ist, können wir

$$\mathrm{Gal}(f, \mathbb{K}) := \mathrm{Gal}(\mathbb{L} : \mathbb{K})$$

als die *Galoisgruppe von f über $\mathbb{K}$* (oder auch *der Gleichung $F(x) = 0$*) bezeichnen.

10.4.1 Beispiele Mit Hilfe der bereits berechneten Galoisgruppen erhalten wir die folgenden Resultate:

i) $GF(p^n)$ ist Zerfällungskörper von $x^{(p^n)} - x$ über $GF(p)$, es folgt

$$\mathrm{Gal}(x^{(p^n)} - x, GF(p)) = \mathrm{Gal}(GF(p^n) : GF(p)) \simeq C_n.$$

ii) Für Kreisteilungspolynome erhalten wir

$$GF(\Phi_n, \mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \simeq E(\mathbb{Z}_n).$$

iii)

$$\mathrm{Gal}(1 + x^2, \mathbb{R}) \simeq C_2.$$

iv)

$$\mathrm{Gal}(x^4 - 2, \mathbb{Q}) \simeq D_4.$$

◇

10.4.2 Folgerung *Ist $f \in \mathbb{K}[x]$, und hat f nur einfache Wurzeln λ_i, dann ist*

$$\delta\colon \mathrm{Gal}(f, \mathbb{K}) \to S_{W(f)}\,,\ \sigma \mapsto \begin{pmatrix} \lambda_i \\ \sigma(\lambda_i) \end{pmatrix}$$

ein Monomorphismus von $\mathrm{Gal}(f, \mathbb{K})$ *in die symmetrische Gruppe $S_{W(f)}$ auf der Menge $W(f)$ der Wurzeln von f. Die Galoisgruppe eines Polynoms mit n verschiedenen Wurzeln ist also isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.* Man bezeichnet dann einfachheitshalber auch diese Gruppe als Galoisgruppe von f. □

10.4.3 Beispiele

i) $\mathrm{Gal}(1 + x^2, \mathbb{R}) = \{1, \tau\} \simeq S_2$, wobei $\tau\colon i \mapsto -i$.

ii) $\Phi_{12} = x^4 - x^2 + 1 = (x - \zeta)(x - \zeta^5)(x - \zeta^7)(x - \zeta^{11})$, wobei $\zeta = \exp(2\pi i/12)$ eine primitive 12-te Einheitswurzel ist. Es gilt also

$$\mathrm{Gal}(\Phi_{12}, \mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = \{\sigma_1, \sigma_5, \sigma_7, \sigma_{11}\},$$

wenn $\sigma_i\colon \zeta \mapsto \zeta^i$. Wir erhalten also, wenn $\lambda_0 := \zeta, \lambda_1 := \zeta^5, \lambda_2 := \zeta^7, \lambda_3 := \zeta^{11}$,

$$\delta(\sigma_1) = 1, \delta(\sigma_5) = (01)(23), \delta(\sigma_7) = (02)(13), \delta(\sigma_{11}) = (03)(12).$$

Hieraus folgt

$$\mathrm{Gal}(\Phi_{12}, \mathbb{Q}) \simeq V_4,$$

die Kleinsche Vierergruppe. ◇

Da *irreduzible* Polynome in ihrem Zerfällungskörper lauter einfache Wurzeln haben, ergibt sich unmittelbar die

10.4.4 Folgerung *Die Menge*

$$\mathrm{Gal}(f,\mathbb{K})\,\backslash\backslash W(f)$$

der Bahnen der Galoisgruppe von f auf $W(f)$ beteht aus den Wurzelmengen der irreduziblen Faktoren von f. Ist f selbst irreduzibel, dann operiert die Galoisgruppe transitiv *auf der Wurzelmenge, es gilt dann*

$$\mathrm{Gal}(f,\mathbb{K})\,\backslash\backslash W(f) = \{W(f)\}.$$

10.4.5 Anwendung Beispielsweise sind also die Bahnen von

$$\mathrm{Gal}(x^{(p^n)} - x, GF(p)) = \mathrm{Gal}(GF(p^n) : GF(p)) \simeq C_n$$

auf $GF(p^n)$ die Wurzelmengen der irreduziblen Faktoren von $x^{(p^n)} - x$. Das sind aber gerade die *sämtlichen* normierten irreduziblen Polnome $f \in GF(p)[x]$ vom Grad $\leq n$, deren Wurzeln in $GF(p^n)$ liegen.

Man kann die Anzahl dieser Polynome also als Bahnenanzahl ermitteln. Hierzu kann man mit Gewinn die Existenz einer sogenannten *Normalbasis* verwenden, das ist eine $GF(p)-$Basis der Form

$$\mathcal{B} = \{\sigma(\lambda) \mid \sigma \in \mathrm{Gal}(GF(p^n) : GF(p))\},$$

$\lambda \in GF(p^n)$ geeignet. (Die Existenz einer solchen Basis kann man für jede endliche Galoiserweiterung beweisen!)

Bei geeigneter Numerierung der Basiselemente operiert die zyklische Gruppe auf $GF(p^n)$ durch zyklische Vertauschung der Basiselemente. Das ist gerade die Art von Operation

$$_G\left(Y^X\right),$$

die wir bei der Definition der Symmetrieklassen von Abbildungen gesehen haben. Die gesuchte Gesamtanzahl irreduzibler Polynome ist also

$$|\,\mathrm{Gal}(GF(p^n) : GF(p))\,\backslash\backslash GF(p^n)\,| = |\,C_n\,\backslash\backslash p^n\,| = \frac{1}{n}\sum_{t|n}\varphi(t)p^{n/t}.$$

Und die Anzahl solcher irreduziblen Polynome vom Grad n ist die Anzahl der Bahnen von *maximaler* Länge n, also gerade gleich

$$|\,C_n\,\backslash\backslash_{\bar{1}}\,p^n\,| = \frac{1}{n}\sum_{t|n}\mu(t)p^{n/t}.$$

$\diamond$

Weil die symmetrische Gruppe S_p, für Primzahlen p, mit irgendeinem Zyklus voller Länge, zusammen mit irgendeiner Transposition erzeugt werden kann (Übungsblatt), gilt auch:

10.4.6 Folgerung *Ist f irreduzibel, von primem Grad p, und enthält* $\mathrm{Gal}(f,\mathbb{K})$ *ein Element σ der Ordnung p sowie eine Transposition τ, dann ist*

$$\mathrm{Gal}(f,\mathbb{K}) \simeq S_p.$$

Mit Hilfe dieses Resultats werden wir folgendes beweisen können:

10.4.7 Satz *Ist $f \in \mathbb{Q}[x]$ irreduzibel, vom primen Grad p, dann gilt*

$$\mathrm{Gal}(f,\mathbb{Q}) \simeq S_p,$$

wenn f genau zwei verschiedene nicht reelle Wurzeln hat.

Beweis: Sind $\lambda, \mu \in W(f) \setminus \mathbb{R}$ verschieden, dann führt das Element $z \mapsto \overline{z}$ der Galoisgruppe diese beiden Wurzeln ineinander über, ist also eine Transposition auf $W(f)$. Bezeichnet $\mathbb{L}$ den Zerfällungskörper von f, und ist ν eine Wurzel von f, dann gilt

$$[\mathbb{L}:\mathbb{Q}] = [\mathbb{L}:\mathbb{Q}(\nu)][\mathbb{Q}(\nu):\mathbb{Q}] = [\mathbb{L}:\mathbb{Q}(\nu)]\cdot p,$$

denn f ist — evtl. bis auf einen Zahlenfaktor — das Minimalpolynom von ν. Nach dem Satz von Sylow enthält die Galoisgruppe Elemente der Ordnung p, woraus mit 10.4.6 die Behauptung folgt. □

Jetzt sei an die *elementarsymmetrischen Polynome* erinnert:

$$\sigma_i^{(n)} := \sum_{0\le\nu_0<\ldots<\nu_{i-1}\le n-1} x_{\nu_0}\cdots x_{\nu_{i-1}} \in \mathbb{K}[x_0,\ldots,x_{n-1}],\ 1\le i\le n,\ \sigma_0^{(n)} := 1,$$

und an die Tatsache, daß diese wie folgt die Koeffizienten gewisser Polynome mit Hilfe der Wurzeln auszudrücken erlauben:

$$f := \prod_{i\in n}(x-x_i) = \sum_{i=0}^{n}(-1)^i\sigma_i^{(n)}x^{n-i}.$$

Die symmetrische Gruppe S_n operiert auf $\mathbb{K}[x_0,\ldots,x_{n-1}]$, also auch auf dessen Quotientenkörper $\mathbb{K}(x_0,\ldots,x_{n-1})$, dem Körper der rationalen Funktionen in den Unbestimmten $x_0,\ldots,x_{n-1}$. Die Menge der Fixpunkte von S_n, der Fixring von S_n auf $\mathbb{K}[x_0,\ldots,x_{n-1}]$, ist der Ring der symmetrischen Polynome, der Fixkörper

$$\mathbb{K}(x_0,\ldots,x_{n-1})_{S_n},$$

heißt entsprechend der Körper der *symmetrischen Funktionen.*

10.4.8 Satz *Es gilt:*

- *Der Körper der symmetrischen Funktionen ist der Quotientenkörper des Rings der symmetrischen Polynome:*

$$\mathbb{K}(x_0,\ldots,x_{n-1})_{S_n} = \mathbb{K}(\sigma_1^{(n)},\ldots,\sigma_n^{(n)}).$$

- *Dieser Körper ist Zerfällungskörper von*

$$f = \prod_{i \in n}(x - x_i) = \sum_{i=0}^{n}(-1)^i \sigma_i^{(n)} x^{n-i} \in \mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})[x].$$

- *Die Körpererweiterung*

$$\mathbb{K}(x_0, \ldots, x_{n-1}) : \mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})$$

  ist endliche Galoiserweiterung.

- *Für die zugehörige Galoisgruppe gilt:*

$$\mathrm{Gal}(f, \mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})) \simeq S_n.$$

Beweis:

i) Zunächst gilt ganz offensichtlich die Inklusion

$$\mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)}) \leq \mathbb{K}(x_0, \ldots, x_{n-1})_{S_n}.$$

ii) $\mathbb{K}(x_0, \ldots, x_{n-1})$ ist natürlich Zerfällungskörper des separablen Polynoms

$$f \in \mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})[x],$$

$\mathbb{K}(x_0, \ldots, x_{n-1}) : \mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})$ also eine Galoiserweiterung.

iii) Weil dieser Körper Zerfällungskörper eines Polynoms vom Grad n ist, gilt für den Körpergrad:

$$[\mathbb{K}(x_0, \ldots, x_{n-1}) : \mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})] \leq n!.$$

Die Galoiserweiterung ist also endliche Galoiserweiterung.

iv) Wegen

$$S_n \leq \mathrm{Gal}(\mathbb{K}(x_0, \ldots, x_{n-1}) : \mathbb{K}(x_0, \ldots, x_{n-1})_{S_n})$$

folgt schließlich auch

$$n! \leq |\mathrm{Gal}(\mathbb{K}(x_0, \ldots, x_{n-1}) : \mathbb{K}(x_0, \ldots, x_{n-1})_{S_n})|,$$

mit i) also

$$n! \leq |\mathrm{Gal}(\mathbb{K}(x_0, \ldots, x_{n-1}) : \mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)}))|,$$

was beweist, daß die Galoisgruppe von f über $\mathbb{K}(x_0, \ldots, x_{n-1})$ isomorph zur symmetrischen Gruppe S_n ist.

v) Obige Ungleichungen sind also aus Dimensionsgründen Gleichungen, und wir erhalten somit auch

$$\mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)}) = \mathbb{K}(x_0, \ldots, x_{n-1})_{S_n},$$

was den Beweis vervollständigt.

□

Das Polynom

$$h := x^n + x_0 x^{n-1} + \ldots + x_{n-2}x + x_{n-1} \in \mathbb{K}(x_0, \ldots, x_{n-1})[x]$$

heißt *allgemeines Polynome n-ten Grades.* Weil die Substitution

$$x_i \mapsto (-1)^{i+1}\sigma_{i+1}^{(n)}$$

einen Isomorphismus φ von $\mathbb{K}(x_0, \ldots, x_{n-1})$ auf $\mathbb{K}(\sigma_1^{(n)}, \ldots, \sigma_n^{(n)})$ definiert, bei dem h auf $f = \prod(x - x_i)$ abgebildet wird, ergibt sich auch die

10.4.9 Folgerung *Das allgemeine Polynom hat die symmetrische Gruppe als Galoisgruppe:*

$$\mathrm{Gal}(h, \mathbb{K}(x_0, \ldots, x_{n-1})) \simeq S_n.$$

□

Damit haben wir ein Polynom mit *symmetrischer* Galoisgruppe. Für die Anwendungen der Galoistheorie auf das Problem der Lösbarkeit algebraischer Gleichungen benötigen wir noch Aussagen über Polynome mit *zyklischen* Galoisgruppen. Wir betrachten deshalb als nächste die *reinen Polynome,* das sind die Polynome der Form $x^n - \kappa \in \mathbb{K}[x]$, und zu den entsprechenden *reinen Gleichungen* $x^n = \kappa$. Wegen der schon angesprochenen Anwendungen machen wir die Voraussetzung

Char($\mathbb{K}$) teilt n nicht und $\mathbb{K}$ enthält alle n-ten Einheitswurzeln.

Wir stellen zunächst folgendes fest: Ist λ eine Wurzel des reinen Polynoms $x^n - \kappa$, ζ eine primitive n-te Einheitswurzel, dann gilt:

i) $\lambda, \lambda\zeta, \ldots, \lambda\zeta^{n-1}$ sind die Wurzeln von $x^n - \kappa$.

ii) Diese Wurzeln sind paarweise verschieden.

iii) $\mathbb{K}(\lambda)$ ist Zerfällungskörper von $x^n - \kappa$. Dieses Polynom ist separabel, $\mathbb{K}(\lambda) : \mathbb{K}$ also eine Galoiserweiterung.

10.4.10 Satz *Die Galoisgruppe* $\mathrm{Gal}(x^n - \kappa, \mathbb{K}) = \mathrm{Gal}(\mathbb{K}(\lambda) : \mathbb{K})$ *der reinen Gleichung ist isomorph zu einer Untergruppe von C_n, insbesondere also eine zyklische Gruppe. Ist $x^n - \kappa$ irreduzibel, dann ist die Galoisgruppe isomorph C_n.*

Beweis: Ist $\sigma \in \mathrm{Gal}(x^n - \kappa, \mathbb{K})$, dann gilt $\sigma(\lambda) = \lambda\zeta^k$, mit einem geeigneten k. Die Abbildung

$$\varphi\colon \mathrm{Gal}(x^n - \kappa, \mathbb{K}) \to \mathbb{Z}_n\,,\ \sigma \mapsto \overline{k} := k + (n)$$

ist ein Gruppenhomomorphismus von der Galoisgruppe in die additive Gruppe $(\mathbb{Z}_n, +) \simeq C_n$.

Ist $x^n - \kappa$ irreduzibel, dann ist $x^n - \kappa = f_{\mathbb{K},\lambda}$, also $[\mathbb{K}(\lambda) : \mathbb{K}] = n$. Die Körpererweiterung $\mathbb{K}(\lambda) : \mathbb{K}$ ist Galoiserweiterung, es gilt also

$$|\mathrm{Gal}(x^n - \kappa, \mathbb{K})| = [\mathbb{K}(\lambda) : \mathbb{K}] = n = |C_n|,$$

was die Behauptung ergibt.

□

Hiervon gilt auch die Umkehrung:

10.4.11 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine Galoiserweiterung,* $\mathrm{Gal}(\mathbb{L} : \mathbb{K}) \simeq C_n$, $\mathrm{Char}(\mathbb{K})$ *kein Teiler von* n*, und enthält* $\mathbb{K}$ *alle* n*-ten Einheitswurzeln, dann ist* $\mathbb{L}$ *Zerfällungskörper eines irreduziblen reinen Polynoms über* $\mathbb{K}$*.*

Beweis: Sei $\mathrm{Gal}(\mathbb{L} : \mathbb{K}) = \langle\sigma\rangle$. Die Menge $\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\} \subseteq \mathbb{K}^{\mathbb{K}}$ ist nach dem Satz von Dedekind linear unabhängig über $\mathbb{K}$. Ist ζ eine primitive n-te Einheitswurzel, dann liegt diese nach Voraussetzung in $\mathbb{K}$. Wegen der linearen Unabhängigkeit der σ^i ist die sogenannte *Lagrangesche Resolvente*

$$\mu := \sum_{i=0}^{n-1} \zeta^i \sigma^i \neq 0.$$

Es gibt also $\lambda \in \mathbb{L}$ mit

$$\mu(\lambda) = \sum_{i=0}^{n-1} \zeta^i \sigma^i(\lambda) \neq 0.$$

Hierfür ist

$$\sigma(\mu(\lambda)) = \sum_i \zeta^i \sigma^{i+1}(\lambda) = \zeta^{-1}\mu(\lambda) \neq 0.$$

Es folgt

$$\sigma(\mu(\lambda)^n) = (\sigma(\mu(\lambda))^n = (\zeta^{-1}\mu(\lambda))^n = \zeta^{-n}\mu(\lambda)^n = \mu(\lambda)^n.$$

Wir erhalten also, daß für alle k gilt: $\sigma^k(\mu(\lambda)^n) = \mu(\lambda)^n$, also $\mu(\lambda)^n \in \mathbb{K}$. Das Element $\mu(\lambda)$ ist demnach Wurzel eines reinen Polynoms $x^n - \kappa$ über $\mathbb{K}$.

Betrachten wir jetzt das Minimalpolynom $f_{\mathbb{K},\mu(\lambda)}$. $\sigma^k(\mu(\lambda)) = \zeta^{-k}\mu(\lambda)$ ist Wurzel dieses Polynoms, $0 \leq k \leq n-1$, es hat also einen Grad $\geq n$. Da es ein Teiler von $x^n - \kappa$ ist, gleicht es diesem:

$$f_{\mathbb{K},\mu(\lambda)} = x^n - \kappa.$$

$\mathbb{L}$ ist also tatsächlich Zerfällungskörper eines irreduziblen reinen Polynoms über $\mathbb{K}$, wie behauptet. □

10.5 Die Auflösbarkeit algebraischer Gleichungen

Gleichungen der Form $x^2 + ax + b = 0$, $a, b \in \mathbb{R}$, also algebraische Gleichungen zweiten Grades, besitzen bekanntlich die Wurzeln

$$x_{1,2} = \frac{-a}{2} \pm \sqrt[2]{\frac{a^2}{4} - b},$$

sie sind also durch Wurzelziehen bei arithmetischen Ausdrücken in den Koeffizienten lösbar. Das gilt auch für die Gleichungen $x^3 + a_1x^2 + a_2x + a_3 = 0$, $a_i \in \mathbb{R}$. Setzt man

$$p := a_2 - \frac{a_1^2}{2},\ q := \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + a_3,\ r := \frac{p^3}{27} + \frac{q^2}{4},$$

sowie

$$P := \sqrt[3]{\frac{-q}{2} + r},\ Q := \sqrt[3]{\frac{-q}{2} - r},\ \zeta := \exp(\frac{2\pi i}{3}),$$

dann ergeben sich die Wurzeln zu

$$x_1 = P + Q - \frac{a_1}{3}, x_2 = \zeta P + \zeta^2 Q - \frac{a_1}{3}, x_3 = \zeta^2 P + \zeta Q - \frac{a_1}{3},\ \text{(Cardano)}$$

Ähnliches gilt für Gleichungen vierten Grades, wie man schon im 16. Jahrhundert festgestellt hat. 1826 hat dann N. H. Abel bewiesen, daß Gleichungen fünften Grades nicht immer auf diese Weise durch Wurzelziehen lösbar sind, und E. Galois fand dann eine notwendige und hinreichende Bedingung für die Existenz solcher Lösungen. Diese Bedingung soll jetzt hergeleitet werden.

10.5.1 Definition (Radikalerweiterung) $\mathbb{L} : \mathbb{K}$ heißt *Radikalerweiterung,* wenn $\mathbb{L}$ von $\mathbb{K}$ aus in endlich vielen Schritten durch sukzessives Adjungieren von Wurzeln reiner Polynome erzeugbar ist, d.h. es gilt $\mathbb{L} = \mathbb{K}$ oder es gibt eine endliche Kette

$$\mathbb{K} = \mathbb{K}_0 < \cdots < \mathbb{K}_m = \mathbb{L}$$

von Zwischenkörpern $\mathbb{K}_i$ mit $\mathbb{K}_{i+1} = \mathbb{K}_i(\lambda_i)$, und $\lambda_i^{n_i} \in \mathbb{K}_i$, n_i geeignet. •

10.5.2 Hilfssatz *Ist* $\mathbb{L} : \mathbb{K}$ *eine Radikalerweiterung und* $\mathrm{Char}(\mathbb{K}) = 0$, *dann gibt es Erweiterungen* $\mathbb{M} : \mathbb{L}$, *so daß* $\mathbb{M} : \mathbb{K}$ *Galoiserweiterung und Radikalerweiterung von* $\mathbb{K}$ *ist.*

Beweis: Durch Induktion nach $[\mathbb{L} : \mathbb{K}]$.

I $[\mathbb{L} : \mathbb{K}] = 1 : \mathbb{K} = \mathbb{L}$, hier gilt also die Behauptung.

II $[\mathbb{L} : \mathbb{K}] > 1$: Sei $\mathbb{K} = \mathbb{K}_0 < \cdots < \mathbb{K}_m = \mathbb{L}$. Wir unterscheiden zwei Fälle:

a) $m = 1$: Sei $\mathbb{L} = \mathbb{K}(\lambda)$ und $\lambda^n \in \mathbb{K}$. Wir adjungieren, falls notwendig, noch eine primitive n-te Einheitswurzel ζ und setzen $\mathbb{M} := \mathbb{L}(\zeta)$. $\mathbb{M}$ enthält mit λ und ζ alle Wurzeln von $x^n - \kappa$, wenn $\kappa := \lambda^n$. $\mathbb{M}$ ist also Zerfällungskörper dieses reinen Polynoms. Demnach ist $\mathbb{M} : \mathbb{K}$ eine Radikalerweiterung mit der Kette von Zwischenkörpern

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 = \mathbb{L} \subseteq \mathbb{K}_2 = \mathbb{M}.$$

Außerdem ist $\mathbb{M} : \mathbb{K}$ eine Galoiserweiterung, denn $\mathbb{M}$ ist ja Zerfällungskörper eines über $\mathbb{K}$ separablen Polynoms.

b) $m > 1$: Ohne Einschränkung können wir $\mathbb{K}_{m-1} \subset \mathbb{L}$ und damit, wegen der Endlichkeit von $[\mathbb{L} : \mathbb{K}]$, die Ungleichung $[\mathbb{K}_{m-1} : \mathbb{K}] < [\mathbb{L} : \mathbb{K}]$ voraussetzen, so daß die Induktionsannahme die Existenz eines Erweiterungskörpers $\mathbb{M}'$ (oberhalb von $\mathbb{K}_{m-1}$) liefert, der Galoiserweiterung und Radikalerweiterung von $\mathbb{K}$ ist.

Mit Hilfe von dessen Galoisgruppe definieren wir das Polynom

$$f := \prod_{\sigma \in \mathrm{Gal}(\mathbb{M}':\mathbb{K})} (x^n - \sigma(\kappa^n)),$$

wobei κ und n durch $\mathbb{L} = \mathbb{K}_{m-1}(\kappa)$ und $\kappa^n \in \mathbb{K}_{m-1}$ definiert seien (für irgendein κ, das durch Adjunktion $\mathbb{L}$ ergibt). Wegen $\tau f = f$, für alle $\tau \in \mathrm{Gal}(\mathbb{M}' : \mathbb{K})$ folgt $f \in \mathbb{K}[x]$.

Jetzt sei $\mathbb{M}$ definiert als Zerfällungskörper von f über $\mathbb{M}'$. Er entsteht durch Adjunktion der n-ten Wurzeln der $\sigma(\kappa^n)$ an $\mathbb{M}'$, also ist $\mathbb{M} : \mathbb{M}'$ eine Radikalerweiterung. Da auch $\mathbb{M}' : \mathbb{K}$ Radikalerweiterung ist, erweist sich insgesamt auch $\mathbb{M} : \mathbb{K}$ als Radikalerweiterung.

Es bleibt zu zeigen, daß $\mathbb{M} : \mathbb{K}$ Galoiserweiterung ist. $\mathbb{M}'$ ist Zerfällungskörper eines $g \in \mathbb{K}[x]$, $\mathbb{M}$ ist Zerfällungskörper von f über $\mathbb{M}'$. Insgesamt ist also $\mathbb{M}$ Zerfällungskörper von gf über $\mathbb{K}$, also eine Galoiserweiterung von $\mathbb{K}$, denn gf ist, wegen $\mathrm{Char}(\mathbb{K}) = 0$, separabel.

□

10.5.3 Satz *Ist* $\mathrm{Char}(\mathbb{K}) = 0$ *und* $\mathbb{L} : \mathbb{K}$ *sowohl Galoiserweiterung als auch Radikalerweiterung, dann besitzt die Galoisgruppe* $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *eine Normalreihe mit zyklischen Faktoren.*

Beweis: Der Fall $\mathbb{L} = \mathbb{K}$ ist trivial. Sei deshalb

$$\mathbb{K} = \mathbb{K}_0 < \cdots < \mathbb{K}_m = \mathbb{L}$$

mit $\mathbb{K}_{i+1} = \mathbb{K}_i(\lambda_i)$ und $\lambda_i^{n_i} \in \mathbb{K}_i$. Wir setzen

$$n := n_0 \cdots n_{m-1},$$

bezeichnen mit ζ eine primitive n-te Einheitswurzel und betrachten die Erweiterungen $\mathbb{K}'_i := \mathbb{K}_i(\zeta)$. Sie bilden die Kette

$$\mathbb{K} \leq \mathbb{K}'_0 \leq \mathbb{K}'_1 \leq \cdots \leq \mathbb{K}'_m = \mathbb{L}' = \mathbb{L}(\zeta).$$

In dieser Kette bilden benachbarte Zwischenkörper Galoiserweiterungen $\mathbb{K}'_{i+1} : \mathbb{K}'_i$, denn $\mathbb{K}'_i$ enthält ja die primitive n_i-te Einheitswurzel ζ^{n/n_i}, das Polynom $x^{n/n_i} - \lambda_i^{n_i}$ ist also separabel über $\mathbb{K}'_i$. Außerdem ist die Galoisgruppe dieser Erweiterung, $G_i := \mathrm{Gal}(\mathbb{K}'_{i+1} : \mathbb{K}'_i)$, zyklisch, nach 10.4.10.
Die Erweiterung $\mathbb{L} : \mathbb{K}$ ist Galoiserweiterung, also Zerfällungskörper, etwa von $g \in \mathbb{K}[x]$. $\mathbb{L}(\zeta)$ ist dann Zerfällungskörper von $g(x^n - 1)$, $\mathbb{L}(\zeta) : \mathbb{K}$ ist also Galoiserweiterung, und auch $\mathbb{L}(\zeta) : \mathbb{K}(\zeta)$.
Der Kette

$$\mathbb{K} \leq \mathbb{K}'_0 \leq \mathbb{K}'_1 \leq \ldots \leq \mathbb{K}'_m = \mathbb{L}' = \mathbb{L}(\zeta).$$

entspricht deshalb, nach dem Hauptsatz der Galoistheorie, die Normalkette der entsprechenden Galoisgruppen (durch Anwendung von Γ):

$$\mathrm{Gal}(\mathbb{L}' : \mathbb{K}) \trianglerighteq \mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_0) \trianglerighteq \ldots \trianglerighteq \mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_m) = \{1\}.$$

Weiter gilt nach dem Hauptsatz, daß deren Faktoren

$$\mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_i)/\mathrm{Gal}(\mathbb{L}' : \mathbb{K}'_{i+1}) \simeq \mathrm{Gal}(\mathbb{K}'_{i+1} : \mathbb{K}'_i)$$

zyklisch sind. Daraus folgt, weil mit $\mathbb{L}' : \mathbb{K}$ auch $\mathbb{L} : \mathbb{K}$ Galoiserweiterung ist, nach dem Hauptsatz:

$$\mathrm{Gal}(\mathbb{L} : \mathbb{K}) \simeq \mathrm{Gal}(\mathbb{L}' : \mathbb{K})/\mathrm{Gal}(\mathbb{L}' : \mathbb{L}).$$

Demnach besitzt auch $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ eine Normalreihe mit zyklischen Faktoren.
□

10.5.4 Satz *Ist* $\mathbb{L} : \mathbb{K}$ *eine endliche Galoiserweiterung,* $\mathrm{Char}(\mathbb{K}) = 0$ *und besitzt* $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ *eine Kompositionsreihe mit zyklischen Faktoren, dann gibt es eine Einheitswurzel* ζ*, so daß* $\mathbb{L}(\zeta) : \mathbb{K}$ *eine Radikalerweiterung ist.*

Beweis: Eine aus dieser Normalreihe durch Verfeinerung hervorgegangene Kompositionsreihe sei

$$\mathrm{Gal}(\mathbb{L} : \mathbb{K}) = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\},$$

mit den (zyklischen!) Faktoren G_i/G_{i+1}. Die Abbildung Φ aus der Galoisverbindung ergibt die entsprechende Kette von Fixkörpern

$$\mathbb{K} = \mathbb{L}_{G_0} < \mathbb{L}_{G_1} < \cdots < \mathbb{L}_{G_m} = \mathbb{L}.$$

Hierfür gilt nach dem Hauptsatz, wenn $\mathbb{K}_i := \mathbb{L}_{G_i}$,

a) $G_i = \mathrm{Gal}(\mathbb{L} : \mathbb{K}_i) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K})$,

b) $\mathbb{K}_{i+1} : \mathbb{K}_i$ ist endliche Galoiserweiterung,

c) $\mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i) \simeq \mathrm{Gal}(\mathbb{L} : \mathbb{K}_i)/\mathrm{Gal}(\mathbb{L} : \mathbb{K}_{i+1})$,

und aus der letzten Isomorphie folgt noch, daß $\mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i)$ zyklisch ist.

Sei jetzt $n := |\mathrm{Gal}(\mathbb{L} : \mathbb{K})|$, ζ eine primitive $n-$te Einheitswurzel. Wir wollen zeigen, daß $\mathbb{L}(\zeta) : \mathbb{K}$ die Behauptung erfüllt.

$\mathbb{K}_{i+1} : \mathbb{K}_i$ ist Galoiserweiterung, also auch $\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i$ und $\mathbb{K}_{i+1} : \mathbb{K}_i(\zeta)$. Die Einschränkung ψ der Automorphismen auf $\mathbb{K}_{i+1}$ ist ein Homomorphismus

$$\psi\colon \mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i) \to \mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i), \sigma \mapsto \sigma \downarrow \mathbb{K}_{i+1}.$$

Dessen Einschränkung auf die Untergruppe $\mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta))$ ist dann ein Homomorphismus

$$\psi \downarrow \mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta))\colon \mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta)) \to \mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i), \sigma \mapsto \sigma \downarrow \mathbb{K}_{i+1}.$$

Dieser erweist sich als injektiv: Liegt σ im Kern, dann ist $\sigma(\kappa) = \kappa$, für alle $\kappa \in \mathbb{K}_{i+1} \cup \mathbb{K}_i(\zeta) = \mathbb{K}_{i+1}(\zeta)$, und damit die identische Abbildung.
Wir können also darauf schließen, daß $\mathrm{Gal}(\mathbb{K}_{i+1}(\zeta) : \mathbb{K}_i(\zeta))$ isomorph zu einer Untergruppe von $\mathrm{Gal}(\mathbb{K}_{i+1} : \mathbb{K}_i)$ und damit ebenfalls zyklisch ist, ihre Ordnung n_i teilt n. Also enthält $\mathbb{K}_i(\zeta)$ eine primitive n_i-te Einheitswurzel: ζ^{n/n_i}. $\mathbb{K}_{i+1}(\zeta)$ entsteht demnach aus $\mathbb{K}_i(\zeta)$ durch Adjunktion einer n_i-ten Wurzel. Demnach ist $\mathbb{L}(\zeta) : \mathbb{K}$ eine Radikalerweiterung, wie behauptet.

□

10.6 Auflösbare Gruppen

Unser Ziel ist es jetzt, die Auflösbarkeit algebraischer Gleichungen durch die Auflösbarkeit der Galoisgruppe zu charakterisieren. Deshalb geht es zunächst um die Einführung des Begriffs der Auflösbarkeit von Gruppen. Wir erinnern uns dazu an den Begriff der Kommutatorgruppe: G sei eine Gruppe,

- Eine Untergruppe $U \leq G$ heißt *charakteristische* Untergruppe, wenn für alle Elemente α der Automorphismengruppe $Aut(G)$ von G gilt

$$\alpha(U) = U.$$

- Zu zwei Elementen $g, h \in G$ heißt

$$[g, h] := g^{-1}h^{-1}gh$$

  ihr *Kommutator*.

- Die von allen Kommutatoren erzeugte Untergruppe

$$G^{(1)} := [G, G] := \langle g^{-1}h^{-1}gh \mid g, h \in G\rangle$$

  heißt die *Kommutatorgruppe* von G.

- Die *höheren Kommutatorgruppen* $G^{(i)}$ werden rekursiv so definiert:

$$\forall\ i > 1 : G^{(i)} := [G^{(i-1)}, G^{(i-1)}],$$

  dabei sei $G^{(0)} := G$.

- Die Kommutatorgruppe ist die kleinste Untergruppe mit abelscher Faktorgruppe in G. Sie ist charakteristische Untergruppe.

- Ein Beispiel ist die Kommutatorgruppe der symmetrischen Gruppe: $S_n^{(1)} = A_n$. Tatsächlich ist sogar jedes Element der alternierenden Gruppe ein Kommutator.

- Eine Gruppe heißt *auflösbar*, wenn G Kompositionsreihen besitzt und diese nur Faktoren von Primzahlordnung haben. Wegen

$$S_3 \rhd A_3 \rhd 1$$

  ist also beispielsweise S_3 auflösbar, und nach

$$S_4 \rhd A_4 \rhd V_4 \rhd C_2 \rhd 1$$

  gilt das auch für S_4 (für S_5 dagegen nicht, s.u.).

– Äquivalent dazu ist offenbar, eine Gruppe als auflösbar zu bezeichnen, wenn die Faktoren ihrer Kompositionsreihen abelsch sind (denn eine abelsche Gruppe $G \neq 1$ ist genau dann einfach, wenn sie zyklisch von Primzahlordnung ist, und Gruppen von Primzahlordnung sind zyklisch, insbesondere also abelsch).

$\diamond$

Wir wollen noch zeigen, daß die Auflösbarkeit auch mit Hilfe höherer Kommutatorgruppen charakterisiert werden kann, denn G wird sich als auflösbar herausstellen, wenn es n gibt mit

$$G^{(n)} = \{1\}.$$

Zunächst deshalb einige ergänzende Überlegungen zu höheren Kommutatorgruppen:

10.6.1 Hilfssatz *Für höhere Kommutatorgruppen ist folgendes richtig:*

- $U \leq G \Longrightarrow U^{(n)} \subseteq G^{(n)}$,
- $N \trianglelefteq G \Longrightarrow (G/N)^{(n)} = (G^{(n)} \cdot N)/N \simeq G^{(n)}/(G^{(n)} \cap N)$,
- $(G \times H)^{(n)} = G^{(n)} \times H^{(n)}$.

Beweis:

i) ist trivial.

ii) Induktion nach n :

I $n = 0$: dieser Fall ist klar wegen $G^{(0)} = G$.

II $n > 0$:

$$\begin{array}{rcl} (G/N)^{(n)} & = & [\,(G/N)^{(n-1)}, (G/N)^{(n-1)}\,] \\ & =_{IA} & [\,(G^{(n-1)}N)/N, (G^{(n-1)}N)/N\,] \\ & = & [\,\{gN \mid g \in G^{(n-1)}\}, \{gN \mid g \in G^{(n-1)}\}\,] \\ & = & \langle\,[\,g_0N, g_1N\,] \mid g_i \in G^{(n-1)}\,\rangle \\ & = & \langle\,[\,g_0, g_1\,]N \mid g_i \in G^{(n-1)}\,\rangle \\ & = & (G^{(n)} \cdot N)/N. \end{array}$$

iii) ist klar.

$\square$

10.6.2 Folgerung *Für endliche Gruppen gilt:*

- *Gibt es $n \in \mathbb{N}$ mit $G^{(n)} = \{1\}$, dann gilt auch für jede ihrer Untergruppen $U^{(n)} = \{1\}$, und auch für jede Faktorgruppe ist $(G/N)^{(n)} = \{1\}$.*

- *Sind* $G_0, \ldots, G_{m-1}$ *Gruppen mit* $G_i^{(n_i)} = \{1\}$, $n := kgV\{n_i \mid i \in m\}$, *dann ist*
$$(G_0 \times \cdots \times G_{m-1})^{(n)} = \{1\}.$$
- *Ist* $N \trianglelefteq G$ *und* $N^{(r)} = (G/N)^{(n)} = 1$, *dann ist* $G^{(n+r)} = 1$.

□

10.6.3 Satz *Eine endliche Gruppe* G *ist genau dann auflösbar, wenn es ein* $k \in \mathbb{N}$ *gibt mit* $G^{(k)} = 1$.

Beweis:

i) Sei zunächst G auflösbar. Es gibt also eine Kompositionsreihe

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = \{1\},\ G_i/G_{i+1} \text{ von primer Ordnung.}$$

Wir verwenden Induktion nach n.

I $n = 0, 1$: trivial, denn G ist hier abelsch.

I $n > 1$: Nach Induktionsannahme gibt es $n_1 \in \mathbb{N}$ mit $G_1^{(n_1)} = \{1\}$. Weil die Faktorgruppe G_0/G_1 abelsch ist, haben wir auch $(G_0/G_1)^{(1)} = \{1\}$, so daß wir auf
$$G^{(n_1+1)} = G_0^{(n_1+1)} = \{1\}$$
schließen können.

ii) Ist umgekehrt $G^{(n)} = \{1\}$, dann bilden die höheren Kommutatorgruppen die Normalreihe
$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^{(n)} = \{1\}$$
mit abelschen Faktoren. Aus dieser Kette kann man durch Verfeinerung eine Kompositionsreihe gewinnen, ihre Faktoren sind ebenfalls abelsch und natürlich von primer Ordnung, nach dem Hauptsatz über abelsche Gruppen.

□

10.6.4 Definition (auflösbare Gleichungen) Eine algebraische Gleichung $F(x) = 0$, zu einem $f \in \mathbb{K}[x]\backslash\mathbb{K}$, heißt über $\mathbb{K}$ (durch Radikale) *auflösbar*, bzw. f heißt auflösbar, wenn ihre sämtlichen Lösungen, d.h. alle Wurzeln von f, aus den Koeffizienten des Polynoms mit Hilfe der Grundrechnungsarten und Wurzelziehen gewonnen werden können, mit anderen Worten: wenn der Zerfällungskörper in einer Radikalerweiterung von $\mathbb{K}$ liegt. •

10.6.5 Satz *Ist* $\mathrm{Char}(\mathbb{K}) = 0$, *dann ist* $F(x) = 0$, *zu* $f \in \mathbb{K}[x] \setminus \mathbb{K}$, *genau dann über* $\mathbb{K}$ *durch Radikale lösbar, wenn* $G(f, \mathbb{K})$ *auflösbar ist.*

Beweis:

i) Ist f durch Radikale auflösbar, dann gibt es eine Körpererweiterung $\mathbb{L} : \mathbb{K}$, die den Zerfällungskörper $\mathbb{M}$ umfaßt, Galoiserweiterung und Radikalerweiterung ist. Die Galoisgruppe $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ hat abelsche Normalreihen und ist damit auflösbar. Weil mit $\mathbb{L} : \mathbb{K}$ auch $\mathbb{M} : \mathbb{K}$ eine Galoiserweiterung ist, gilt nach dem Hauptsatz der Galoistheorie

$$\mathrm{Gal}(\mathbb{L} : \mathbb{M}) \trianglelefteq \mathrm{Gal}(\mathbb{L} : \mathbb{K}) \text{ und } \mathrm{Gal}(\mathbb{M} : \mathbb{K}) \simeq \mathrm{Gal}(\mathbb{L} : \mathbb{K})/\mathrm{Gal}(\mathbb{L} : \mathbb{M}).$$

Aus der Auflösbarkeit von $\mathrm{Gal}(\mathbb{L} : \mathbb{K})$ ergibt sich also auch die von $\mathrm{Gal}(\mathbb{M} : \mathbb{K})$ und damit die Auflösbarkeit der Galoisgruppe des Polynoms.

ii) Ist umgekehrt $G(f, \mathbb{K}) = \mathrm{Gal}(\mathbb{M} : \mathbb{K})$ auflösbar, dann gibt es eine Erweiterung $\mathbb{L} : \mathbb{K}$, mit $\mathbb{K} \leq \mathbb{M} \leq \mathbb{L}$, die Radikalerweiterung ist, das Polynom ist also auflösbar.

□

10.6.6 Folgerungen

i) Das allgemeine Polynom vom Grad n ist für $n \geq 5$ nicht durch Radikale auflösbar.

ii) Das allgemeine Polynom vom Grad n ist für $n \leq 4$ durch Radikale auflösbar.

iii) Polynome mit abelschen Galoisgruppen sind durch Radikale auflösbar, beispielsweise also die Kreisteilungspolynome.

Kapitel 11

Kategorien und Funktoren

In den Vorlesungen Lineare Algebra I,II und Algebra I,II sind mehrere Klassen mathematischer Strukturen im Detail betrachtet worden: Mengen, Gruppen, Ringe, Körper, Vektorräume usw. Wir wollen deshalb diese Betrachtung von Klassen von Strukturen systematisieren und vereinheitlichen unter Verwendung der — seit etwa 1945 vorhandenen — Begriffsbildung der *Kategorie*.

11.1 Kategorien

11.1.1 Definition (Kategorie) Eine *Kategorie* $\mathcal{C}$ besteht aus einer Klasse $\mathrm{Ob}(\mathcal{C})$ von *Objekten* $A, B, C, \ldots$ und einer Klasse $\mathrm{Mor}(\mathcal{C})$ von Mengen $\hom_{\mathcal{C}}(A, B)$ von *Morphismen* $f, g, h, \ldots$, zu jedem Paar (A, B) von Objekten, also

$$\mathcal{C} = (\mathrm{Ob}(\mathcal{C}), \mathrm{Mor}(\mathcal{C})).$$

Dabei heißt A der *Bereich* der Morphismen in $\hom_{\mathcal{C}}(A, B)$, B ihr *Cobereich*. Darüberhinaus wird die Existenz einer *Multiplikation* von Morphismen verlangt:

$$\hom_{\mathcal{C}}(A, B) \times \hom_{\mathcal{C}}(B, C) \to \hom_{\mathcal{C}}(A, C), (f, g) \mapsto gf.$$

Hierfür müssen die folgenden Bedingungen erfüllt sein:

- $(A, B) \neq (C, D) \Longrightarrow \hom_{\mathcal{C}}(A, B) \cap \hom_{\mathcal{C}}(C, D) = \emptyset$, mit anderen Worten: Morphismen $f \in \hom_{\mathcal{C}}(A, B)$ sind genau genommen Tripel

  $$(A, \mathrm{Graph}(f), B).$$

- $(hg)f = h(gf)$, d.h. die Multiplikation der Morphismen ist assoziativ (meist ist sie sowieso einfach gleich der Komposition der Abbildungen).

- Zu jedem Objekt A gibt es in $\hom_{\mathcal{C}}(A, A)$ einen Morphismus 1_A mit $f1_A = f$, für alle $f \in \hom_{\mathcal{C}}(A, B)$ sowie $1_A g = g$, für alle $g \in \hom_{\mathcal{C}}(B, A)$. Diese Morphismen sind in der Regel natürlich die Identitäten.

•

11.1.2 Beispiele Bekannte Beispiele sind

- Die Kategorie $\mathcal{S}$ der *Mengen* (sets), mit den Mengen als Objekten, den Morphismenmengen $\hom_{\mathcal{S}}(A, B) := B^A$, der Komposition von Abbildungen als Multiplikation: $gf = g \circ f$, sowie den Identitäten $\mathrm{id}_A = 1_A$.

- Die Kategorie $\mathcal{G}$ der *Gruppen*, mit den Gruppen als Objekten, den Morphismenmengen $\hom_{\mathcal{G}}(A, B) := \mathrm{Hom}(A, B)$, der Komposition von Abbildungen als Multiplikation, sowie den Identitäten $1_A := \mathrm{id}_A$. Die Kategorie $\mathcal{A}$ der *abelschen Gruppen* ist analog zu $\mathcal{G}$ definiert, ebenso die Kategorie $\mathcal{M}$ der *Monoide* wie auch $\mathcal{H}$, die Kategorie der Halbgruppen.

- Die Kategorie $\mathcal{R}$ der Ringe mit Einselement, hier sind die Morphismen natürlich die Ringhomomorphismen, die Einselement auf Einselement abbilden. Entsprechendes gilt für die Kategorie $\mathcal{K}$ der Körper.

- Ist R ein Ring, dann bezeichne ${}_R\mathcal{M}$ die Kategorie der $R-$Linksmoduln, $\mathcal{M}_R$ die der $R-$Rechtsmoduln, mit den $R-$linearen Abbildungen als Morphismen. Für Körper $\mathbb{K}$ sei ${}_{\mathbb{K}}\mathcal{V}$ die Kategorie der $\mathbb{K}-$Linksvektorräume, analog ist $\mathcal{V}_{\mathbb{K}}$ zu verstehen.

◇

Als *Teilkategorie* von $\mathcal{C}$ (kurz $\mathcal{D} \leq \mathcal{C}$) bezeichnen wir jede Kategorie $\mathcal{D}$, deren Objekteklasse $\mathrm{Ob}(\mathcal{D})$ eine Teilklasse von $\mathrm{Ob}(\mathcal{C})$ ist, und für die gilt $\hom_{\mathcal{D}}(A,B) \subseteq \hom_{\mathcal{C}}(A,B)$, falls $A, B \in \mathrm{Ob}(\mathcal{D})$. Darüberhinaus wird natürlich noch verlangt, daß die Multiplikation zweier Morphismen in $\mathrm{Mor}(\mathcal{D})$ dieselbe ist wie in $\mathrm{Mor}(\mathcal{C})$, und daß die Einsen 1_A übereinstimmen.

Sind die Morphismenmengen sogar gleich, $\hom_{\mathcal{D}}(A,B) = \hom_{\mathcal{C}}(A,B)$, dann spricht man von einer *vollen* Teilkategorie. Beispiele voller Teilkategorien sind $\mathcal{G}$ und $\mathcal{A}$ in $\mathcal{M}$.

11.1.3 Definition (Iso-, Mono-, Epimorphismen) Morphismen mit links- und rechtsinversen Morphismen, d.h. die $f \in \hom_{\mathcal{C}}(A,B)$, für die es $g, h \in \hom_{\mathcal{C}}(B,A)$ gibt mit $fg = 1_B$ und $hf = 1_A$ (woraus natürlich $g = h$ folgt, so daß wir $f^{-1} := g = h$ setzen dürfen) heißen auch hier *Isomorphismen*. Es sind bijektive Abbildungen.

Mono- bzw. *Epimorphismen* sind die in $\mathrm{Mor}(\mathcal{C})$ links- bzw rechts kürzbaren Morphismen, also diejenigen Morphismen f, für die zu Morphismen g, h mit $fg = fh$ folgt $g = h$ bzw. für die zu Morphismen g, h mit $gf = hf$ folgt $g = h$.

•

Hier ist jedoch Vorsicht geboten, denn wir fordern die Kürzbarkeit nur bei Produkten mit Morphismen (und nicht stets!): Beispielsweise ist

$$f\colon \mathbb{Z} \to \mathbb{Q}\,,\ z \mapsto z$$

ein Morphismus in der Kategorie $\mathcal{R}$. Sind jetzt $g, h \in \hom_{\mathcal{R}}(\mathbb{Q}, R)$ Morphismen mit $gf = hf$, dann gilt $g \downarrow \mathbb{Z} = h \downarrow \mathbb{Z}$. Weil jeder Homomorphismus auf $\mathbb{Q}$ durch seine Wirkung auf $\mathbb{Z}$ vollständig bestimmt ist, ergibt das $g = h$, f ist also rechts kürzbar, allerdings keineswegs surjektiv!

11.1.4 Folgerung *Für Monomorphismen und Epimorphismen in Kategorien gilt:*

- *Injektive Morphismen sind Monomorphismen, surjektive Morphismen sind Epimorphismen,*
- *Produkte von Monomorphismen sind Monomorphismen, Produkte von Epimorphismen sind Epimorphismen,*
- *Monomorphismen sind aber nicht notwendig injektiv sein, Epimorphismen nicht notwendig surjektiv.*

□

Andererseits git es natürlich Kategorien, in denen Morphismen genau dann Monomorphismen (Epimorphismen), wenn sie injektiv (surjektiv) sind:

11.1.5 Beispiele In den Kategorien

$$\mathcal{S},\ {}_R\mathcal{M},\ \mathcal{M}_R,\ {}_{\mathbb{K}}\mathcal{V},\ \mathcal{V}_{\mathbb{K}},\ \mathcal{A},\ \mathcal{G}$$

sind genau die injektiven Morphismen Monomorphismen und genau die surjektiven Morphismen Epimorphismen. In der Kategorie

$$\mathcal{R}$$

dagegen sind die Monomorphismen genau die injektiven Morphismen, die Epimorphismen jedoch nicht notwendig surjektiv. ◇

Vgl. Übungsblatt.

Interessant ist auch die Klassifizierung von Unter- und Faktorstrukturen: Um die Unterstrukturen von $A \in \mathrm{Ob}(\mathcal{C})$ zu klassifizieren, kann man nämlich auf der Klasse der Morphismen f, g mit Cobereich A die folgende transitive Relation einführen: Ist $f \in \hom_{\mathcal{C}}(B, A), g \in \hom_{\mathcal{C}}(C, A)$, dann sei

$$f \preceq g :\Longleftrightarrow\ \exists\ h \in \hom_{\mathcal{C}}(B, C) :\ f = gh.$$

Dann ist nämlich

$$f \equiv g \iff f \preceq g \wedge g \preceq f$$

Eine Äquivalenzrelation auf der Klasse der Monomorphismen mit Cobereich A. Die Äquivalenzklassen heißen *Subobjekte* von A.

Entsprechend kann man die Epimorphismen mit Bereich A in Äquivalenzklassen zusammenfassen, die man *Faktorobjekte* nennt (vgl. Übungsblatt).

Abschließend sei noch bemerkt, daß man einen Morphismus $f \in \hom_{\mathcal{C}}(A, B)$ als *Sektion* (*Retraktion*) bezeichnet, wenn es $g \in \hom_{\mathcal{C}}(B, A)$ gibt mit $fg = 1_B$ ($gf = 1_A$).

11.2 Funktoren

Von großer Bedeutung sind Abbildungen der folgenden Form *zwischen* Kategorien:

11.2.1 Definition (Funktoren) Sind $\mathcal{C}$ und $\mathcal{D}$ Kategorien, dann besteht ein (*kovarianter*) *Funktor* $F\colon \mathcal{C} \to \mathcal{D}$ aus zwei Abbildungen, die wir einfachheitshalber ebenfalls mit F bezeichnen:

- $F\colon A \mapsto F(A)$, auf den Objekten von $\mathcal{C}$, mit $F(A) \in \mathrm{Ob}(\mathcal{D})$,
- und einer Abbildung $F\colon f \mapsto F(f)$ auf den Morphismen von $\mathcal{C}$, wobei $F(f) \in \hom_{\mathcal{D}}(F(A), F(B))$, falls $f \in \hom_C(A, B)$.

Für diese wir verlangt, daß $F(gf) = F(g)F(f)$, sowie $F(1_A) = 1_{F(A)}$.

Ein (*kontravarianter*) *Funktor* $F\colon \mathcal{C} \to \mathcal{D}$ besteht ebenfalls aus zwei Abbildungen,

- $F\colon A \mapsto F(A)$,
- $F\colon f \mapsto F(f)$, wobei diesmal $F(f) \in \hom_{\mathcal{D}}(F(B), F(A))$, falls $f \in \hom_{\mathcal{C}}(A, B)$,

mit $F(fg) = F(g)F(f)$, sowie $F(1_A) = 1_{F(A)}$. •

11.2.2 Beispiele

- Ein triviales Beispiel ist die Identität $1_{\mathcal{C}}$, die jedes Objekt von auf sich selbst und jeden Morphismus auf sich selbst abbildet.
- Typische Beispiele von Funktoren sind *Vergißfunktoren*, die sozusagen die (oder Teile der) Struktur vergessen, z.B.

  $$F\colon \mathcal{G} \to \mathcal{S},\ A \mapsto A,\ f \mapsto f,$$

  bei dem die Gruppe $A \in \mathrm{Ob}(\mathcal{G})$ auf ihre Grundmenge $A \in \mathrm{Ob}(\mathcal{S})$ abgebildet wird etc., oder auch

  $$F\colon \mathcal{R} \to \mathcal{A},\ A \mapsto A,\ f \mapsto f.$$

  Hier wird der Ring A auf seine additive Gruppe abgebildet. Entsprechend kann ein Ring mit Einselement natürlich auch auf seine multiplikative Halbgruppe, ein Monoid, abgebildet werden, wobei sich ein Funktor $F\colon \mathcal{R} \to \mathcal{M}$ ergibt.
- Ist $n \in \mathbb{N}^*$, dann ist

  $$F\colon \mathcal{R} \to \mathcal{R},\ R \mapsto R^{n\times n},\ f \mapsto \tilde{f}$$

  ein kovarianter Funktor, der den Ring R auf den Ring der $n-$reihigen Matrizen über R abbildet und dem Ringhomomorphismus $f \in \hom_{\mathcal{R}}(R, S)$ den Ringhomomorphismus

  $$\tilde{f}\colon R^{n\times n} \to S^{n\times n},\ (a_{ik}) \mapsto (f(a_{ik}))$$

  zuordnet.

- Ein kovarianter Funktor ist auch

$$F\colon \mathcal{G} \to \mathcal{A},\ G \mapsto G/[G,G],\ f \mapsto \bar{f}.$$

  Er bildet die Gruppe G auf die (abelsche!) Faktorgruppe nach der Kommutatorgruppe ab, und dem Homomorphismus f auf G wird der davon induzierte Homomorphismus auf dieser Faktorgruppe zugeordnet.

- Ein kontravarianter Funktor zwischen ${}_R\mathcal{M}$ und $\mathcal{M}_R$ ist

$$^*\colon M \mapsto M^* = \hom_R(M,R),$$

  wobei vermöge $(\varphi \cdot r)(m) := \varphi(m) \cdot r$ die Menge $M^* = \hom_R(M,R)$ zu einem $R-$Rechtsmodul gemacht wurde. Dieser Modul M^* heißt der zu M *duale* Modul. Einem $f \in \hom_{{}_{\mathcal{R}}\mathcal{M}}(M,N)$ wird dabei $f^* \in \hom_{\mathcal{M}_{\mathcal{R}}}(N^*,M^*)$ zugeordnet, mit

$$\forall\ \psi \in N^*\colon\ f^*(\psi) := \psi \circ f.$$

  Dieser Funktor heißt die *Dualisierung*.

◇

Bilder von Isomorphismen unter Funktoren sind wieder Isomorphismen, entsprechendes gilt aber weder für Monomorphismen noch für Epimorphismen.

11.2.3 Definition (natürliche Transformation) Sind F und G zwei Funktoren von $\mathcal{C}$ nach $\mathcal{D}$, dann heißt η eine *natürliche Transformation* von F nach G, wenn η jedem $A \in \mathrm{Ob}(\mathcal{C})$ einen Morphismus $\eta_A \in \hom_{\mathcal{D}}(F(A),G(A))$ zuordnet, so daß für alle $f \in \hom_{\mathcal{C}}(A,B)$ und alle $A,B \in \mathrm{Ob}(\mathcal{C})$ folgendes Diagramm kommutativ ist:

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & \circlearrowright & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\eta_B]{} & G(B) \end{array}$$

Ist dabei jedes η_A ein Isomorphismus, dann heißt η ein *natürlicher Isomorphismus*. •

11.2.4 Beispiele

Ein Beispiel ist die Abbildung auf die Faktorgruppe nach der Kommutatorgruppe, denn

$$\begin{array}{ccc} G & \xrightarrow{\nu_{[G,G]}} & G/[G,G] \\ {\scriptstyle f}\downarrow & \circlearrowright & \downarrow{\scriptstyle \bar{f}} \\ H & \xrightarrow[\nu_{[H,H]}]{} & H/[H,H] \end{array}$$

ist kommutativ, also ist die Abbildung

$$G \mapsto \nu_{[G,G]}$$

eine natürliche Transformation von $1_{\mathcal{G}}$ auf die *Abelisierung.*

Ein weiteres Beispiel ist die Diagonale: Ist

$$\oplus^n\colon {}_{\mathcal{R}}\mathcal{M} \to {}_{\mathcal{R}}\mathcal{M}$$

der Funktor mit

$$\oplus^n\colon M \mapsto \oplus^n M$$

und

$$(\oplus^n f)(m_0, \ldots, m_{n-1}) := (f(m_0), \ldots, f(m_{n-1})),$$

dann ist, mit der Diagonale Δ und

$$\Delta_M : m \mapsto (m, \ldots, m),$$

offensichtlich folgendes Diagramm

$$\begin{array}{ccc} M & \xrightarrow{\Delta_M} & \oplus^n M \\ {\scriptstyle f}\downarrow & \circlearrowright & \downarrow{\scriptstyle \oplus^n f} \\ N & \xrightarrow[\Delta_N]{} & \oplus^n N \end{array}$$

kommutativ. ◇

Abschließend sei noch bemerkt, daß die Komposition

$$G \circ F\colon \mathcal{C} \to \mathcal{E}$$

zweier (kovarianter) Funktoren $F\colon \mathcal{C} \to \mathcal{D}$ und $G\colon \mathcal{D} \to \mathcal{E}$ wieder ein (kovarianter) Funktor ist. Analoges gilt für Funktoren, von denen einer oder zwei kontravariant sind. Wir werden das gleich anwenden können.

11.3 Spezies

In einem gewissen Gegensatz zu den Vergißfunktoren, die vorhandene Struktur *vergessen*, stehen Funktoren F, die Struktur *hineinbringen*. Die Intention dabei ist, F als Konstruktionsverfahren, als Algorithmus zu interpretieren, der einer endlichen Menge alle Strukturen einer durch F vorgegebenen Form zuordnet, die "auf der Menge A leben", z.B. die Graphen mit A als Knotenmenge etc.

11.3.1 Definition (Spezies) Eine *Spezies* ist ein kovarianter Funktor auf der Kategorie $\mathcal{S}_b^e$ der endlichen Mengen mit den bijektiven Abbildungen als Morphismen. Ist F ein solcher Funktor, dann heißt $F(A)$, die Menge aller $F-$Strukturen σ auf A, die durch die Elemente $a \in A$ eindeutig beschreibbar sind, *$F-$Struktur* auf A, und $F(f)$, $f\colon A \rightarrowtail\!\!\!\!\!\rightarrow B$, heißt *Transport von $F-$Struktur mittels f*. Gemeint ist damit, daß man die $\tau \in F(B)$ aus den $\sigma \in F(A)$ durch die Umbenennung $a \mapsto f(a)$ erhält. •

Zunächst ein paar ganz einfache *mengentheoretische* Beispiele:

11.3.2 Beispiele

- Die Spezies P *Potenzmenge* bildet M auf die Potenzmengen ab:

  $$P(M) := \{N \mid N \subseteq M\}.$$

  $P(M)$ kann bekanntlich mit der Abbildungenmenge 2^M identifiziert werden.

- $P^{[k]}$, die Spezies *k-Teilmengen*, entsteht durch Abbildung von M auf die Menge

  $$P^{[k]}(M) := \binom{M}{k} := \{N \mid N \subseteq M, |N| = k\}$$

  aller $k-$Teilmengen.

- Par bezeichne die Spezies *Mengenpartitionen,* sie ordnet M die Menge $Par(M)$ zu, definiert als

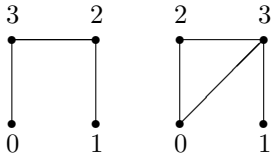
  $$\{\{N_0, \ldots, N_{n-1}\} \mid n \in \mathbb{N}^*, N_i \neq \emptyset, N_i \cap N_j = \emptyset, \text{ falls } i \neq j, \cup_i N_i = M\}\,.$$

◇

Mit Hilfe dieser mengentheoretischen Spezies können wir jetzt einige *graphentheoretische* Spezies definieren:

11.3.3 Graphische Spezies

- Die Spezies *(schlichte) Graphen* ordnet M die Menge $Graph(M)$ aller schlichten Graphen mit der Knotenmenge M zu. Hier sind zwei Elemente von $Graph(\{0,1,2,3\})$,



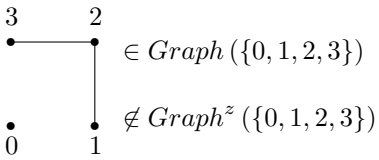
Es ist klar, daß ein Graph auf M mit der Menge der Paare verbundener Knoten identifiziert werden kann, so daß wir $Graph(M)$ mit der Potenzmenge

$$2^{\binom{M}{2}}$$

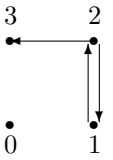
identifizieren dürfen. Es gilt demnach

$$Graph(M) = P(P^{[2]}(M)).$$

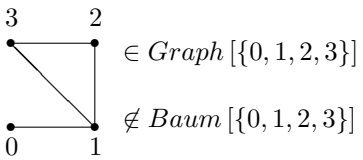
- Die Spezies *zusammenhängende* Graphen $Graph^z$ ordnet M die zusammenhängenden schlichten Graphen auf M zu. Hier ist ein *nicht* zusammenhängender Graph:



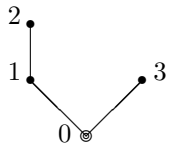
- Die Spezies der *gerichteten* Graphen, also der Graphen mit gerichteten Kanten, aber ohne Schleifen und ohne Parallelkanten. Hier ein Beispiel aus $Graph^g(\{0,1,2,3\})$:



- Die Spezies der *Bäume* liefert zu M die Menge aller zusamenhängenden Graphen ohne Zyklen. Hier zur Veranschaulichung ein Graph, der *kein* Baum ist:



- Wurzelbäume sind Bäume mit einem ausgezeichneten Punkt, hier ist ein Beispiel, ein Element aus $Wbaum(\{0,1,2,3\})$:

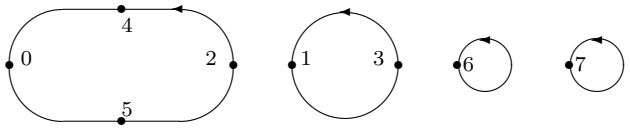


◇

Weitere interessante Spezies ordnen M Mengen spezieller Abbildungen zu:

11.3.4 Spezies aus Abbildungen

- Die Spezies *Permutationen* ordnet M die Menge aller Permutationen von M zu,
$$Per(M) := S_M := \{\pi \mid \pi\colon M \rightarrowtail\!\!\!\!\!\twoheadrightarrow M\}.$$
Hier ist eine Permutation π der Menge $M := \{0,1,2,3,4,5,6,7\}$:



Diese Skizze entspricht der Zyklenschreibweise

$$\pi = (0425)(13)(6)(7) = (0, \pi(0), \pi^2(0), \pi^3(0))(1, \pi(1))(6)(7).$$

Die Listenschreibweise hierfür ist

$$\pi = [43512067].$$

- Die Spezies *orientierte Zyklen* liefert $Zyk^o(M)$.

  Beispielsweise ist jede Permutation eine Vereinigung eindeutig bestimmter orientierter Zyklen, das zeigt voranstehendes Beispiel aus 4 orientierten Zyklen.

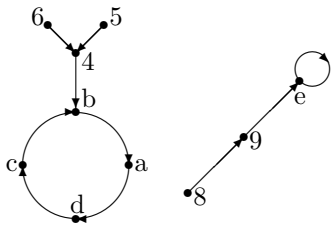
- Die Spezies *lineare (oder auch: totale) Ordnungen.* Hier ist ein Element von $Lin(\{0,1,2,3,4,5,6,7\})$:

$$2 < 4 < 3 < 6 < 7 < 5 < 1 < 0.$$

- Die Spezies *Endo* der *Endofunktionen* ergibt

$$Endo(M) := M^M.$$

Man sieht leicht ein, daß eine Endofunktion $\varepsilon \in Endo(M)$ die Elemente von M in zwei Teilmengen einteilt, nämlich in solche m, die durch eine geeignete Potenz von ε auf sich selbst abgebildet werden: $m = \varepsilon^n(m)$, für ein geeignetes n in $\mathbb{N}^*$. Diese liegen in orientierten Zyklen. Hier ist ein Beispiel aus $Endo(\{4,5,6,8,9,a,b,c,d,e\})$:



Demnach ist eine Endofunktion auf einer endlichen Menge eine Permutation einer Menge von Wurzelbäumen. Unser Beispiel ist eine Permutation $(adcb)(e)$ der Bäume mit den Wurzeln a, b, c, d, e. Wir werden diese Überlegung weiter unten aufgreifen.

$\diamond$

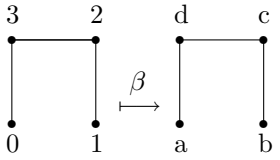
Betrachten wir jetzt den *Transport von Struktur* und seine Bedeutung für Spezies. Ist $\beta\colon M \rightarrowtail\!\!\!\!\!\rightarrow N$ ein Morphismus in $\mathcal{S}_b^e$ und $\sigma \in F(M)$ eine $F-$Struktur auf M. Die Struktur $\tau := F(\beta)(\sigma) \in F(N)$ ergibt sich durch Ersetzen des Labels $m \in M$ durch das Label $n := \beta(m) \in N$. Hier ist ein Beispiel zu $F = Graph$.

11.3.5 Beispiele

i) Ein Graph auf der Menge $M = \{0, 1, 2, 3\}$ wird mit Hilfe der Bijektion

$$\beta : 0 \mapsto a, 1 \mapsto b, 2 \mapsto c, 3 \mapsto d,$$

genauer: Mit Hilfe der Bijektion $Graph(\beta)$ zu einem Graphen auf $N := \{a, b, c, d\}$: Beispielsweise



Formaler liest sich das so: Identifiziert man den Graphen γ auf M mit seiner Kantenmenge,

$$\gamma \doteq \{\{m, m'\} \mid m, m' \in M, m \neq m', \{m, m'\} \in \gamma\},$$

dann wird hieraus mit Hilfe des Graphenmorphismus $Graph(\beta)$ der Graph

$$Graph(\beta)(\gamma) \doteq \{\{\beta(m), \beta(m')\} \mid m, m' \in M, m \neq m', \{m, m'\} \in \gamma\}.$$

ii) Bei Endofunktionen sieht es etwas anders aus: Identifizieren wir $\varepsilon \in M^M$ mit dem Graphen der Funktion, also

$$\varepsilon \doteq \{(m, \varepsilon(m)) \mid m \in M\},$$

$\beta\colon M \rightarrowtail\!\!\!\!\!\rightarrow N$, dann ist

$$Endo(\beta)(\varepsilon) \quad \doteq \quad \big\{(\beta(m), \beta(\varepsilon(m))) \mid m \in M\big\}$$

$$\begin{aligned} &= \big\{(\beta(m), \beta\varepsilon\beta^{-1}(\beta(m))) \mid m \in M\big\} \\ &= \big\{(n, \beta\varepsilon\beta^{-1}(n)) \mid n \in N\big\}. \end{aligned}$$

Es hat sich also folgendes ergeben:

$$Endo(\beta)(\varepsilon) = \beta\varepsilon\beta^{-1}.$$

◇

Um später weitere Spezies als Kompositionen schreiben zu können, brauchen wir noch weitere Beispiele, die auf den ersten Blick vielleicht etwas merkwürdig anmuten:

11.3.6 Weitere Beispiele von Spezies

- Die Spezies *Menge* ordnet M die einelementige Menge $\{M\}$ zu:

$$Menge(M) := \{M\}.$$

- Die Spezies *Elemente* liefert die Menge der Elemente,

$$Elemente(M) := M.$$

- Die Spezies *Singleton* ist so definiert:

$$Single(M) := \begin{cases} \{M\}, & \text{falls } |M| = 1, \\ \emptyset, & \text{sonst.} \end{cases}$$

- Die *leere* Spezies wird definiert durch

$$Leer(M) := \emptyset.$$

- Im Gegensatz zur leeren Spezies sei die Spezies *leere Menge* so eingeführt:

$$LM(M) := \begin{cases} \{M\}, & \text{falls } M = \emptyset, \\ \emptyset, & \text{sonst.} \end{cases}$$

- Schließlich sei noch

$$k - Menge(M) := \begin{cases} \{M\}, & \text{falls } |M| = k, \\ \emptyset, & \text{sonst,} \end{cases}$$

  die Spezies *k-Menge.*

◇

11.4 Kardinalitäten

Da jede Bijektion $\beta\colon M \to N$ eine Bijektion $F(\beta)$ zwischen $F(M)$ und $F(N)$ induziert, spielt die "Natur" der Elemente von M keine wesentliche Rolle,denn $F(\beta)$ entspricht einer *Umbenennung*, einer *Umnumerierung* der Elemente m von M in $\beta(m)$. Was dagegen eine wesentliche Rolle spielt, ist die Ordnung $|M|$ der Menge M. Insbesondere hängt die Ordnung $|F(M)|$ nur von der Kardinalzahl $|M|$ ab. Weil sämtliche Umbenennungen β auch tatsächlich auftreten, können wir uns deshalb auf die $F-$Strukturen auf den *Standardmengen* der Ordnungen $n \in \mathbb{N}$ konzentrieren, auf

$$n := \{0, \ldots, n-1\}.$$

Hierzu setzen wir noch

$$f_n := |F(n)|.$$

Die erzeugenden Funktion dieser Kardinalzahlen f_n schreiben wir in *Exponentialform,* d.h. als formale Potenzreihe

11.4.1
$$F(x) := \sum_{n\geq 0} f_n \frac{x^n}{n!} \ \in \ \mathbb{Q}[\![x]\!].$$

Sie heißt*Kardinalität* von F. Hier sind eine paar einfache Fälle:

11.4.2 Beispiele

$$\begin{aligned}
Lin(x) &= 1 + x + x^2 + x^3 + \ldots = \frac{1}{1-x} = Per(x),\\
Menge(x) &= \sum_{n\geq 0} \frac{x^n}{n!} = e^x,\\
Elemente(x) &= \sum_{n>0} n \cdot \frac{x^n}{n!} = x \cdot e^x,\\
P(x) &= \sum_{n\geq 0} 2^n \cdot \frac{x^n}{n!} = e^{2x},\\
Single(x) &= x,\\
Leer(x) &= 1,\\
LM(x) &= 0,\\
Graph(x) &= \sum_{n>0} 2^{\binom{n}{2}} \cdot \frac{x^n}{n!},\\
Endo(x) &= \sum_{n\geq 0} n^n \cdot \frac{x^n}{n!}.
\end{aligned}$$

$\diamond$

Wir bemerken noch, daß — in Übereinstimmung mit den gerade angegebenen Kardinalitäten — die folgenden Strukturen auf der leeren Menge *nicht* leer sind:

$$Lin(\emptyset) = Menge(\emptyset) = P(\emptyset) = LM(\emptyset) = Endo(\emptyset) = \{\emptyset\} \neq \emptyset,$$

während

$$Elemente(\emptyset) = Single(\emptyset) = Leere(\emptyset) = Graph(\emptyset) = \emptyset.$$

Da wir weiter unten Kardinalitäten ineinander einsetzen wollen, und weil man $f(g(x))$, für $f, g \in \mathbb{Q}[\![x]\!]$ nur bilden kann, wenn das konstante Glied $g_0 = 0$ ist, ordnen wir jeder Spezies G eine Spezies G_+ zu, deren Kardinalität diese Eigenschaft hat:

11.4.3
$$G_+(M) := \begin{cases} G(M), & \text{falls } M \neq \emptyset, \\ \emptyset, & \text{sonst.} \end{cases}$$

Zwei Spezies F und G mit derselben Kardinalität heißen *äquipotent.* Ist dies der Fall, dann schreiben wir

$$F \equiv G,$$

als Abkürzung für $F(x) = G(x)$. Ein offensichtliches Beispiel ist

11.4.4
$$Per \equiv Lin.$$

Eine kanonische Bijektion zwischen $Per(M)$ und $Lin(M)$ benutzt die sogenannte *Listenschreibweise*, zum Beispiel entspricht der die Permutation (038)(124)(57)(6) die folgende Liste

$$[324817650],$$

die Folge der Bilder der Punkte $0, 1, \ldots$. Ihr wiederum entspricht die lineare Ordnung

$$3 < 2 < 4 < 8 < 1 < 7 < 6 < 5 < 0.$$

Eine restriktivere Bedingung als Äquipotenz ist die Forderung nach folgender Eigenschaft:

11.4.5 Definition (Isomorphie von Spezies) Zwei Spezies F und G heißen *isomorph*,

$$F \simeq G,$$

wenn es zu allen endlichen Mengen M, N Bijektionen $\Theta_M \colon F(M) \to G(M)$ und $\Theta_N \colon F(N) \to G(N)$ gibt derart, daß die folgenden Diagramme kommutativ sind, für alle Bijektionen $\beta \colon M \to N$:

$$\begin{array}{ccc} F(M) & \xrightarrow{\Theta_M} & G(M) \\ \Big\downarrow{\scriptstyle F(\beta)} & & \Big\downarrow{\scriptstyle G(\beta)} \\ F(N) & \xrightarrow{\Theta_N} & G(N) \end{array}$$

•

Äquipotenz impliziert natürlich keineswegs Isomorphie, ein Standardbeispiel hierfür ist folgendes:

11.4.6 Beispiel Wir wissen bereits, daß $Per \equiv Lin$, und wir wollen zeigen, daß diese beiden Spezies *nicht* isomorph sind:

$$Per \not\simeq Lin.$$

Um dies indirekt zu beweisen bemerken wir, daß Isomorphie $Per \simeq Lin$ die Existenz einer Bijektion $\Theta_M \colon Per(M) \to Lin(M)$ (wir können ja $N := M$ wählen!) mit

$$Lin(\beta) \circ \Theta_M = \Theta_M \circ Per(\beta),$$

für jede Bijektion $\beta \colon M \to M$ impliziert. Wenden wir dies auf ein M mit $|M| > 1$, eine Bijektion $\beta \neq \mathrm{id}_M$, und die Permutation $\pi := \mathrm{id}_M \in Per(M)$ an. Betrachten wir die lineare Ordnung

$$(m_0 < \ldots < m_{|M|-1}) := \Theta_M(\pi).$$

Anwendung der linken Seite obiger Identität auf π gibt

$$\begin{array}{rcl} (Lin(\beta) \circ \Theta_M)(\pi) & = & Lin(\beta)(m_0 < \ldots < m_{|M|-1}) \\ & = & \big(\beta(m_0) < \ldots < \beta(m_{|M|-1})\big)\,, \end{array}$$

während eine Anwendung der rechten Seite folgendes liefert:

$$\begin{array}{rcl} (\Theta_M \circ Per(\beta))(\pi) & = & \Theta_M(\beta \circ \pi \circ \beta^{-1}) \\ & = & \Theta_M(1) \\ & = & (m_0 < \ldots < m_{|M|-1}) \\ & \neq & \big(\beta(m_0) < \ldots < \beta(m_{|M|-1})\big)\,, \end{array}$$

weil wir $\beta \neq \mathrm{id}_M$ vorausgesetzt haben. ◇

Aus Äquipotenz kann man also nicht auf Isomorphie schließen:

11.4.7 $$F \equiv G \not\Rightarrow F \simeq G.$$

Anstelle von $F \simeq G$ schreibt man oft auch einfach

$$F = G,$$

d.h. man betrachtet eigentlich Isomorphieklassen von Spezies.

11.5 Summe und Produkt von Spezies

Es gibt diverse Verknüpfungen von Spezies, mit denen man aus bereits vorhandenen neue Spezies erhalten kann, z.B. Graphen aus zusammenhängenden Graphen, Permutationen aus orientierten Zyklen usw.
Die einfachste Verknüpfung ist die *Summe* $F + G$ der Spezies F und G mittels disjunkter Vereinigung:

$$F(M) + G(M) := F(M) \dot\cup G(M),$$

falls $F(M) \cap G(M) = \emptyset$, andernfalls hat man zu erzwingen, daß diese Mengen disjunkt sind, durch Umbenennung, etwa durch Ersetzung von $F(M)$ durch $F(M) \times \{0\}$ und von $G(M)$ durch $G(M) \times \{1\}$. Die Kardinalität dieser Summe genügt der Gleichung

11.5.1 $$(F + G)(x) = F(x) + G(x).$$

Triviale Beispiele bilden die Strukturen für die der Begriff zusammenhängend existiert. Ein Beispiel bilden die Graphen, die entweder zusammenhängend oder nicht zusammenhängend sind:

$$Graph = Graph^z + Graph^{nz}.$$

Diese Summation kann man auf Familien von Strukturen ausdehnen: Die Familie $(F_i)_{i\in I}$ von Spezies heißt *summierbar,* wenn es für jede endliche Menge M nur endlich viele $F_i(M)$ nicht leer sind. In diesem Fall definieren wir die Summe dieser Familie durch

$$\left(\sum_{i\in I} F_i\right)(M) := \sum_{i\in I} F_i(M) := \bigcup_{i\in I} F_i(M) \times \{i\}.$$

Dies verträgt sich mit dem folgenden Begriff: Die *kanonische Zerlegung* von F gleicht per definitionem der folgenden summierbaren Familie $(F_n)_{n\geq 0}$, mit

$$F_n(M) := \begin{cases} F(M), & \text{falls } |M| = n, \\ \emptyset, & \text{sonst.} \end{cases}$$

Wir kürzen dies wie folgt ab:

$$F = F_0 + F_1 + F_2 + \ldots.$$

Falls $F_n = \emptyset$, für $n \neq k$, sagen F *konzentriere sich auf* k. Ein triviales Beispiel ist die Zerlegung von $Menge$ in k-Mengen:

$$Menge = \sum_k k - Menge.$$

Im Gegensatz zu dieser Zerlegung von $Menge$ sind die folgenden Zerlegungen von Per (nach Permutationen mit gegebener Anzahl zyklischer Faktoren) und

die Zerlegung von Par (nach Partitionen mit gegebener Anzahl von Blöcken) *nicht kanonisch:*

$$Per = \sum_k Per^{[k]},\ Par = \sum_k Par^{[k]}.$$

Das *Produkt* $F \cdot G$ ist wie folgt definiert:

11.5.2 $$(F \cdot G)(M) := \sum_{(M_0,M_1):\ M=M_0 \dot\cup M_1} F(M_0) \times G(M_1).$$

11.5.3 Beispiele

- Ein Beispiel ist die (eindeutige) Zerlegung von Permutationen in die Menge ihrer Fixpunkte plus eine fixpunktfreie Permutation, ein sogenanntes *Derangement:*
$$Per = Menge \cdot Der.$$
- Ein weiteres Beispiel ist die Darstellung der Potenzmenge als Menge von Paaren, bestehend aus einer Teilmenge und deren Komplement:
$$P = Menge \cdot Menge.$$
- Entsprechendes gilt für k-Teilmengen:
$$P^{[k]} = (k - Menge) \cdot Menge.$$
- Schließlich haben wir auch noch — per Iterierung — die *Potenzen* von Spezies:
$$Par^{[k]} = (Menge_+)^k.$$

◇

Zusammen mit

11.5.4 $$(F \cdot G)(x) = F(x) \cdot G(x)$$

(Übungsaufgabe) ergeben sich Anwendungsmöglichkeiten,

11.5.5 Beispiel Wenden wir die letzte Gleichung für die Kardinalität des Produkts auf die Identität

$$Per = Menge \cdot Der$$

an so erhalten wir, daß

$$\frac{1}{1-x} = e^x \cdot Der(x),$$

woraus sich die folgende Gleichung für die Kardinalität der Spezies der Derangements ergibt:

$$Der(x) = \frac{e^{-x}}{1-x} = e^{-x} \cdot (1 + x + x^2 + x^3 + \ldots).$$

Der Koeffizient von $x^n/n!$ in dieser formalen Potenzreihe ist die gesuchte Anzahl der Derangements auf n Elementen, also der Anzahl der fixpunktfreien Permutationen in S_n :

11.5.6
$$der_n = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Hier ist eine Tabelle mit den kleinsten Anzahlen von Derangements:

n	0	1	2	3	4	5	6	...
der_n	1	0	1	2	9	44	265	...

$\diamond$

11.6 Substitution, Verwurzelung, Komposition

Eine etwas kompliziertere Zusammensetzung von Spezies ergibt sich bei der Suche nach einer Spezies, deren Kardinalität die Substitution $F(G(x))$ von $G(x)$ für x in $F(x)$ ist. Sie ist sehr anwendungsrelevant, ermöglicht sie doch die Beschreibung von Permutationen als Mengen von Zyklen, oder auch die von Graphen als Mengen zusammenhängender Graphen. In beiden Fällen müssen wir deshalb die Punktemenge M partitionieren und dann auf jedem Block der entstandenen Partition alle Zyklen bzw. alle zusammenhängenden Graphen bilden. Die Definition der Substitution $F(G)$ der Spezies G in die Spezies F ist also wie folgt zu formulieren:

11.6.1 Definition (Substitution von Spezies) Sind F und G Spezies mit $G(\emptyset) = \emptyset$, dann setzen wir

$$F(G)(M) := \bigcup_{p=\{p_0,\ldots,p_{r-1}\}\in Par(M)} F(p) \times (\times_{i\in r} G(p_i))\,.$$

•

11.6.2 Beispiel Sei $M := 3 = \{0,1,2\}$. Die Menge $Par(3)$ ist

$$\big\{\{0,1,2\}\big\}, \big\{\{0,1\},\{2\}\big\}, \big\{\{0,2\},\{1\}\big\}, \big\{\{1,2\},\{0\}\big\}, \big\{\{0\},\{1\},\{2\}\big\}.$$

Die Partition $\big\{\{0,1,2\}\big\}$ trägt zur Substitution

$$Menge(Zyk^o)$$

folgendes bei:

$$Menge\big(\big\{\{0,1,2\}\big\}\big) \times Zyk^o\big(\{0,1,2\}\big) = \Big\{\big\{\{0,1,2\}\big\}\Big\} \times \{(012),(021)\}$$

$$= \big\{\big(\big\{\{0,1,2\}\big\},(012)\big), \big(\big\{\{0,1,2\}\big\},(021)\big)\big\}.$$

Der nächste Summand der gesuchten Menge gehört zur Partition $\big\{\{0,1\},\{2\}\big\}$, es ist die Menge

$$\Big\{\big\{\{0,1\},\{2\}\big\}\Big\} \times \Big\{\big((01),(2)\big)\Big\}.$$

Die weiteren Summanden sind

$$\Big\{\big\{\{0,2\},\{1\}\big\}\Big\} \times \Big\{\big((02),(1)\big)\Big\},$$

$$\Big\{\big\{\{1,2\},\{0\}\big\}\Big\} \times \Big\{\big((12),(0)\big)\Big\},$$

und schließlich noch der Summand zur Partition $\big\{\{0\},\{1\},\{2\}\big\}$, es ist

$$\Big\{\big\{\{0\},\{1\},\{2\}\big\}\Big\} \times \Big\{\big((0),(1),(2)\big)\Big\}.$$

Bilden wir die Vereinigung dieser fünf Mengen, so erhalten wir eine Menge der Ordnung 6, die offensichtlich mit der symmetrischen Gruppe S_3 identifiziert werden kann.
Ganz allgemein haben wir die Isomorphie $Menge(Zyk^o) \simeq Per$. Wir können das auch als Identität schreiben:

11.6.3 $$Per = Menge(Zyk^o).$$

◇

Auch anhand des Beispiels sieht man, daß

11.6.4 $$(F(G))(x) = F(G(x)).$$

Für obiges Beispiel ergibt sich

$$\frac{1}{1-x} = Per(x) = Menge(Zyk^o(x)) = e^{Zyk^o(x)},$$

woraus sich für die Kardinalität der Spezies der orientierten Zyklen ergibt:

11.6.5 $$Zyk^o(x) = \log(1-x)^{-1} = \sum_{n>0} \frac{x^n}{n}.$$

Die Anzahl orientierter Zyklen auf einer Menge der Ordnung n ist demnach gleich

$$c_n = (n-1)!,$$

ein Resultat, das man natürlich auch aus der Formel für die Ordnungen der Konjugiertenklassen von Elementen in der symmetrischen Gruppe gewinnen kann!
Analog folgt die Identitäten

11.6.6 $$Graph = Menge(Graph^z),\ Par = Menge(Menge_+),$$

aus denen man die folgenden Kardinalitäten gewinnt:

$$Graph^z(x) = \log(Graph(x)),\ Par(x) = e^{e^x - 1}.$$

Als nützlich erweist sich auch die Bemerkung, daß aus F eine Spezies, deren Kardinalität sich aus $F(x)$ durch Multiplikation mit x ergibt, durch Auszeichnung eines Punktes, durch *Verwurzelung* entsteht, wir bezeichnen diese Spezies wie folgt:

11.6.7 $$F^\bullet(M) := F(M) \times M.$$

Offenbar gilt

11.6.8 $$F^\bullet(x) = x \cdot \frac{d}{dx} F(x).$$

Ein Beispiel ist natürlich

11.6.9 $$Baum^{\bullet} = Wbaum.$$

Eine brilliante Anwendung ist der Beweis von A. Joyal des folgenden berühmten Resultats:

11.6.10 Satz (Cayley) *Die Anzahl der Bäume mit n Knoten ist*

$$|Baum(n)| = n^{n-2}.$$

Beweis: Aus

$$Endo_+ = Per_+(Wbaum) \equiv Lin_+(Wbaum) = Baum^{\bullet\bullet}.$$

Daraus erhalten wir durch Koeffizientenvergleich:

$$n^n = n^2 \cdot |Baum(n)|.$$

□

Selbstverständlich existiert auch das *cartesische Produkt* $F \times G$ zweier Spezies, definiert durch

11.6.11 $$(F \times G)(M) := F(M) \times G(M).$$

Seine Kardinalität ist das *Hadamardprodukt* der Kardinalitäten der Faktoren:

11.6.12 $$(F \times G)(x) = \sum_n f_n g_n \frac{x^n}{n!}.$$

Schließlich ist da noch die bereits erwähnte *(funktorielle) Komposition* $F \circ G$,

11.6.13 $$(F \circ G)(M) := F(G(M)).$$

Ein Beispiel bilden die Graphen, denn ein Graph auf n Punkten kann ja als Teilmenge der Menge aller Zweiermengen der Punktemenge angesehen werden, so daß, wie gesagt

11.6.14 $$Graph = P \circ P^{[2]}.$$

Man kann dies noch weiter zerlegen unter Verwendung des Produkts:

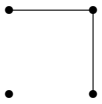
$$Graph = (Menge \cdot Menge) \circ (2 - Menge \cdot Menge).$$

Die Kardinalität der Komposition ist

11.6.15 $$(F \circ G)(x) = \sum_n (f \circ g)_n \frac{x^n}{n!} = \sum_n f_{g_n} \frac{x^n}{n!}.$$

11.7 Typen von Spezies

Ist F eine Spezies, dann besteht $F(M)$ aus den $F-$Strukturen σ auf M, und diese σ sind *numerierte Strukturen*, denn die "Punkte" tragen ja die *Namen*, *Nummern* oder *labels* m der elemente von M.
Spielen diese Namen, Nummern oder labels m keine Rolle, beispielsweise, wenn ein Graph als Wechselwirkungsmodell aufgefaßt wird, d.h. wenn es uns nur darauf ankommt zu zeigen, wieviele Knoten es sind und wieviele Paare von ihnen auf welche Weise verbunden sind, d.h. wechselwirken, dann geht es uns um *unnumerierte* Graphen. Hier ist ein Beispiel:



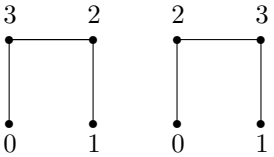
Solche unnumerierten Strukturen erhält man durch Zusammenfassung numerierter Strukturen zu Äquivalenzklassen, die aus denjenigen Strukturen bestehen, die *bis auf Umnumerierung gleich* sind. Dazu genügt es natürlich, die $F-$Strukturen nur auf den Standardmengen n zu betrachten und diejenigen zusammenzufassen, die bis auf eine Umnumerierung $\pi: n \rightarrowtail n$, also bis auf eine Permutation $\pi \in S_n$, gleich sind. Mit anderen Worten: Diese Äquivalenzklassen sind die Bahnen der symmetrischen Gruppen S_n auf den Mengen von $F-$Strukturen $F(n)$ unter der Operation

$$S_n \times F(n) \to F(n)\,,\ (\pi, \sigma) \mapsto F(\pi)(\sigma).$$

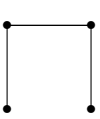
Die Mengen

$$S_n \setminus\!\setminus F(n),\ n \in \mathbb{N},$$

dieser Bahnen heißen die *Typen* von $F-$Strukturen vom *Rang* n. Hier sind zwei Graphen auf der Menge $4 = \{0, 1, 2, 3\}$, die offenbar vom selben Typ sind:



Und ihr Typ wird durch den unnumerierten Graphen beschrieben, den wir durch Entfernen der labels erhalten:



Die erzeugende Funktion für die Anzahlen

$$\tilde{f}_n := |\, S_n \wr\!\wr F(n)\,|$$

bezeichnen wir mit

$$\tilde{F}(x) := \sum_n \tilde{f}_n x^n$$

und nennen sie die *Typreihe* von F. Hierbei ist zu beachten, daß die Typreihe *nicht* in Exponentialform geschrieben wird! Hier sind ein paar einfache Fälle:

11.7.1 Beispiele

- $\widetilde{Lin}(x) = \widetilde{Menge}(x) = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots,$
- $\widetilde{Zyk^o}(x) = \widetilde{Elemente}(x) = \frac{x}{1-x} = x + x^2 + x^3 + \ldots,$
- $\widetilde{P}(x) = \left(\frac{1}{1-x}\right)^2 = 1 + x + 2x^2 + 3x^3 + \ldots,$
- $\widetilde{Single}(x) = x, \widetilde{LM}(x) = 1, \widetilde{Leere}(x) = 0.$

$\diamond$

Wir bemerken noch, daß für die Typenreihen von Summe und Produkt gilt

11.7.2 $$(\widetilde{F+G})(x) = \widetilde{F}(x) + \widetilde{G}(x),\ (\widetilde{F \cdot G})(x) = \widetilde{F}(x) \cdot \widetilde{G}(x).$$

Äquipotenz impliziert natürlich keineswegs die Gleichheit der Typreihen:

11.7.3 $$F(x) = G(x) \not\Rightarrow \widetilde{F}(x) = \widetilde{G}(x).$$

Eine gemeinsame Verallgemeinerung von Kardinalität und Typenreihe ist die folgende Potenzreihe in mehreren Unbestimmten:

11.7.4 Definition (Zykelindexreihe) Sei F eine Spezies, und, zu $n \in \mathbb{N}$ und $\beta \in S_n$, sei

$$F(n)_{F(\beta)} := \{\sigma \in F(n) \mid F(\beta)(\sigma) = \sigma\}$$

die Menge der Fixpunkte von $F(\beta)$ auf der Menge $F(n)$ der $F-$Strukturen auf n. Die Ordnung dieser Menge ist also die Anzahl der Einerzyklen von $F(\beta)$:

$$a_1(F(\beta)) = |F(n)_{F(\beta)}|.$$

Die folgende formale Potenzreihe über $\mathbb{Q}$ in den (kommutativen) Unbestimmten $x_i, i \in \mathbb{N}^*$

$$Z_F(x_1, x_2, \ldots) := \sum_{n\in\mathbb{N}} \frac{1}{n!} \sum_{\beta\in S_n} a_1(F(\beta)) x_1^{a_1(\beta)} x_2^{a_2(\beta)} \cdots x_n^{a_n(\beta)} \in \mathbb{Q}[\![x_1, x_2, \ldots]\!]$$

heißt die *Zykelindexreihe* von F. •

11.7.5 Beispiele Einfach nachzuprüfende Beispiele sind

- $Z_{Leere} = 0$,
- $Z_{LM} = 1$,
- $Z_{Single} = x_1$,
- $Z_{Lin} = \frac{1}{1-x_1}$,
- $Z_{Per} = \frac{1}{(1-x_1)(1-x_2)\cdots}$.

◇

Die Verbindung zwischen Kardinalität und Typreihe via Zykelindexreihe stellt folgendes Resultat her:

11.7.6 Satz *Für jede Spezies F ergeben sich Kardinalität und Typreihe aus der Zykelindexreihe wie folgt durch Einsetzung:*

$$F(x) = Z_F(x, 0, 0, \ldots)$$

und

$$\widetilde{F}(x) = Z_F(x, x^2, x^3, \ldots).$$

Beweis: Zum Beweis der ersten Identität bemerken wir, daß

$$Z_F(x, 0, 0, \ldots) = \sum_{n\in\mathbb{N}} \frac{1}{n!} \sum_{\beta\in S_n} a_1(F(\beta)) x^{a_1(\beta)} 0^{a_2(\beta)} \cdots 0^{a_n(\beta)}.$$

Zur inneren Summe trägt demnach allein das Eiselement $1 \in S_n$ (mit $a_1(F(1)) = f_n$) bei, so daß

$$Z_F(x, 0, 0, \ldots) = \sum_n \frac{1}{n!} \cdot f_n \cdot x^n = F(x),$$

wie behauptet.

Für die zweite Substitution ergibt sich

$$Z_F(x, x^2, x^3, \ldots) = \sum_{n\in\mathbb{N}} \frac{1}{n!} \underbrace{\sum_{\beta\in S_n} a_1(F(\beta))}_{=n!\widetilde{f}_n} x^{\sum_i i\cdot a_i(\beta)} = \sum_n \widetilde{f}_n \cdot x^n = \widetilde{F}(x).$$

□

Als Beispiel ergibt sich aus der oben angegebenen Zykelindexreihe von Per :

$$\widetilde{Per}(x) = Z_{Per}(x, x^2, x^3, \ldots) = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots}.$$

Wir halten noch fest, daß Äquipotenz keineswegs die Gleichheit der Zykelindexreihen impliziert, Isomorphie dagegen sehr wohl. Interessant sind natürlich auch die Identitäten

11.7.7 $$Z_{F+G} = Z_F + Z_G,\ Z_{F\cdot G} = Z_F \cdot Z_G.$$

Aus dem Satz ergibt sich eine Anwendung auf die Bestimmung der Kardinalität, der Typenreihe und der Zykelindexreihe der *Ableitung* F' von F, die wie folgt definiert wird. Zunächst einmal definieren wir zu jeder endlichen Menge M die um ein Element $*_M$, das nicht in M liegen darf, vergrößerte Menge

$$M^+ := M \cup \{*_M\}.$$

Damit setzen wir

$$F'(M) := F(M^+).$$

Die Umnumerierung $F'(\beta)$ wird dementsprechend gleich $F(\beta^+)$ gesetzt, wobei

$$\beta^+ \colon M \cup \{*_M\} \to N \cup \{*_N\}\,,\ x \mapsto \begin{cases} \beta(x), & \text{if } x \in M, \\ *_N, & x = *_M. \end{cases}$$

Beispielsweise ist

$$(Zyk^o)' = Lin,$$

und für die Kardinalität dieser Spezies haben wir

$$F'(x) = \frac{d}{dx} F(x).$$

Aus obigem Satz erhalten wir dazu

$$\widetilde{F'}(x) = \left(\frac{\partial}{\partial x_1} Z_F\right)(x, x^2, x^3, \ldots)$$

sowie

$$Z_{F'} = \left(\frac{\partial}{\partial x_1} Z_F\right).$$

11.8 Der Ring der Isomorphieklassen von Spezies

Wir können die Isomorphieklassen von Spezies addieren und multiplizieren, verstehen dabei natürlich unter der Summe von Isomorphieklassen die Isomorphieklasse der Summe, entsprechend beim Produkt. Beide Verknüpfungen, die Summen- und die Produktbildung, sind kommutativ und assoziativ, und es gibt neutrale Elemente, denn

$$(F + Leere)(n) = F(n) \cup \emptyset = F(n),$$

sowie

$$(F \cdot LM)(n) = F(n) \times \{\emptyset\}.$$

Die Distributivgesetze sind ebenfalls erfüllt. Soche Strukturen nennt man *Halbringe*. Es gilt also die

11.8.1 Folgerung *Die Isomorphieklassen der Spezies bilden einen Halbring bzgl. Summen- und Produktbildung. Das neutrale Element bzgl. Addition ist die leere Spezies, neutrales Element bzgl. Multiplikation ist die Spezies leere Menge.*

Mit Hilfe dieses Halbrings können wir einen kommutativen Ring mit den Isomorphieklassen als $\mathbb{Z}$-Basis konstruieren. Dazu benutzen wir ein Verfahren analog zur Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$, d.h. wir bilden das cartesische Quadrat der Klasse

$$\mathtt{S}$$

der Isomorphieklassen der Spezies und definieren darauf — mit Hilfe der Addition — die folgende Äquivalenzrelation auf der Klasse $\mathtt{S}^2$ der Paare (F, G) von Isomorphieklassen von Spezies:

$$(F_0, G_0) \sim (F_1, G_1) \ :\Longleftrightarrow \ F_0 + G_1 = F_1 + G_0.$$

Zur Vereinfachung der Notation ersetzen wir die Bezeichnung (F, G) als Paar durch den Ausdruck

$$F - G.$$

Ein einfaches Beispiel ergibt sich aus der Tatsache, daß die Menge der Permutationen von n die disjunkte Vereinigung aus der Menge $Der(n)$ der fixpunktfreien Permutationen und der Menge der Permutationen mit Fixpunkten ist, letztere wollen wir mit $\mathcal{F}$ bezeichnen, also

$$Per = \mathcal{F} + Der,$$

und damit

$$\mathcal{F} = Per - Der.$$

Die Menge der Äquivalenzklassen bezeichnen wir mit:

$$\mathrm{S} := (\mathtt{S} \times \mathtt{S})/\sim .$$

Dies ist ein kommutativer Ring. Elemente der Form $(F, Leere)$ bezeichnen wir kurz mit F und die der Form $(Leere, F)$ als $-F$. $-F$ heißt auch *virtuelle* Spezies.

11.8.2 Anwendung Daß man Wurzelbäume mit Hilfe von Bäumen beschreiben kann, hatten wir bereits gesehen:

$$Wbaum = Baum^\bullet.$$

Daß man umgekehrt aber auch Bäume mit Wurzelbäumen beschreiben kann, ist viel weniger trivial.

Beginnen wir dazu mit der Einführung des Begriffs der *Exzentrizität* eines Knotens v in einem Baum τ. Man versteht darunter die maximale Distanz zwischen v einem anderen Knoten des Baumes:

$$e(v) := \max\{d(u,v) \mid u \text{ ein Knoten des Baumes } \tau\}.$$

Ein Knoten heißt *zentral,* wenn seine Exzentrizität minimal ist, d.h. wenn

$$e(v) = \min\{e(u) \mid u \in \tau\}.$$

Es ist nicht schwierig einzusehen, daß in einem Baum entweder ein oder zwei zentrale Knoten existieren (Übungsblatt), kurz: *Das Zentrum eines Baumes besteht entweder aus einem Punkt oder einer Kante.* Man kann also jeden Baum *kanonisch markieren*, durch Markieren dieses Zentrums, sei es ein Knoten oder eine Kante!

Betrachten wir jetzt die Substitution $2 - Menge(Wbaum)(M)$, also die Menge

$$\bigcup_{(M_0,M_1):\ M=M_0\dot\cup M_1} 2 - Menge(\{M_0,M_1\}) \times Wbaum(M_0) \times Wbaum(M_1).$$

Diese Menge von Strukturen kann mit den Bäumen auf M identifiziert werden, bei denen eine Kante ausgezeichnet ist, denn jedes ihrer Elemente ist ja von der Form (ρ,σ), mit $\rho \in Wbaum(M_0)$ und $\sigma \in Wbaum(M_1)$. Die ausgezeichnete Kante ergibt sich als Verbindung der Wurzeln von ρ und σ durch eine Kante.

Zudem benutzen wir, daß $Wbaum^2(M)$ und die Menge der *nicht kanonisch* markierten Bäume auf M bijektiv zueinander sind (Übungsblatt).

Zusammen ergibt das die Gleichung

$$Wbaum + 2 - Menge(Wbaum) = Baum + Wbaum^2,$$

bzw. mit Hilfe der gerade eingeführten virtuellen Spezies die folgende Beschreibung von Bäumen durch Wurzelbäume:

11.8.3 $$Baum = Wbaum + 2 - Menge(Wbaum) - (Wbaum)^2.$$

Dieses Resultat heißt auch das *Dissymmetrietheorem für Bäume.* Eine unmittelbare Folgerung ist die nächste Gleichung für die entsprechenden Kardinalitäten:

$$Baum(x) = Wbaum(x) - \frac{1}{2}Wbaum(x)^2.$$

11.9 Molekulare und atomare Spezies

Es geht jetzt um eine Verfeinerung der Zerlegung $F = \sum_n F_n$.

11.9.1 Definition (molekulare Spezies) Eine Spezies F heißt *molekular*, wenn es genau einen Typ von $F-$Strukturen gibt. •

Dies bedeutet, daß

- F nicht die leere Spezies ist:
$$F \neq Leere,$$
- daß F sich auf ein n konzentriert:
$$\exists_1\ n \in \mathbb{N}\colon\ F(n) \neq \emptyset,$$
- und daß es genau einen Typ von $F-$Struktur auf diesem n gibt, d.h. daß die Operation der symmetrischen Gruppe S_n via Transport von $F-$Struktur
$$S_n \times F(n) \to F(n)\,,\ (\pi, \sigma) \mapsto F(\pi)(\sigma)$$
dort transitiv ist:
$$S_n \backslash\backslash F(n) = \{F(n)\}.$$

Beispiele sind bereits vorhanden: $Single$, LM, $k - Menge$, natürlich auch die Spezies Zyk_n^o der orientierten Zyklen der Längen$n$, die Spezies Lin_n der linearen Ordnungen auf n Elementen usw.. Nicht molekular sind dagegen die Spezies $Wbaum_n$, $Graph_n$, Per_n der Wurzelbäume, der Graphen oder der Permutationen auf $n \geq 2$ Elementen.

Mit anderen Worten: Die Zerlegung von F in die F_n, also in die Spezies $F-$Strukturen auf n Elementen kann durch Zerlegung von F_n in die molekularen Subspezies verfeinert werden:

11.9.2
$$F = \sum_n F_n = \sum_n \sum_{G \subseteq F_n, G\ mol.} G.$$

Beispiele solcher Zerlegungen sind, wie bereits erwähnt,

$$Zyk^o = \sum_n Zyk_n^o,\ Lin = \sum_n Lin_n.$$

Der interessanteste Aspekt dabei ist, daß die molekularen Subspezies mit sehr einfachen Spezies formuliert werden können, z.B. ist die Zerlegung von $Wbaum$ die folgende:

$$Single + Single^2 + (Single^3 + Single \cdot (2 - Menge))$$
$$+(2 \cdot Single^4 + Single^2 \cdot (2 - Menge) + Single \cdot (3 - Menge)) + \ldots$$

Dabei ist zu beachten, daß hier Vielfachheiten auftreten, beispielsweise kommt der Typ von $Single^4$ unter den molekularen Spezies der Wurzelbäume mit 4 Knoten *zweimal* vor, entsprechend den zwei wesentlich verschiedenen Möglichkeiten, im Graphen

einen Punkt als Wurzel zu markieren:

oder so:

Interessante Konsequenzen ergeben sich aus dem, was wir bereits über Bahnen von Gruppen wissen:

11.9.3 Folgerung

- *Die molekularen Spezies auf $F(n)$ entsprechen Bahnen*

$$S_n(\sigma) \in S_n \setminus\setminus F(n),\ \sigma \in F(n),$$

  der symmetrischen Gruppen S_n.

- *Bahnen von S_n sind bijektiv zu Mengen von Linksnebenklassen:*

$$S_n(\sigma) \rightarrowtail S_n / (S_n)_\sigma ,$$

  mit dem Stabilisator $(S_n)_\sigma$ der $F-$Struktur $\sigma \in F(n)$.

- *Die Operation von S_n auf der Bahn $S_n(\sigma)$ entspricht also der Operation von S_n auf der Menge $S_n/(S_n)_\sigma$ von Linksnebenklassen, und diese Operation ist genau dann zu der auf $S_n/(S_n)_\tau$ isomorph, wenn die Stabilisatoren $(S_n)_\sigma$ und $(S_n)_\tau$ zueinander konjugierte Untergruppen von S_n sind.*

- *Die molekularen Spezies entsprechen also den Konjugiertenklassen von Untergruppen der symmetrischen Gruppen!*

Für $n = 0, 1, 2, 3, \ldots$ sind die Anzahlen der Konjugiertenklassen von Untergruppen in S_n gleich

$$1, 1, 2, 4, 11, 19, 56, 96, 296, 554, 1593, 3093, \ldots .$$

Und mit Hilfe der oben eingeführten Spezies kann man nachprüfen, daß die Mengen

$$\mathtt{M}_i$$

der molekularen Spezies auf den kleinsten $i \in \mathbb{N}$ die folgenden sind:

$\mathtt{M}_0 = \{LM\}$,

$\mathtt{M}_1 = \{Single\}$,

$\mathtt{M}_2 = \{Single^2, 2 - Menge\}$,

$\mathtt{M}_3 = \{Single^3, Single \cdot (2 - Menge), 3 - Menge, Zyk_3^0\}$,

$\vdots$

Ist G eine modulare Spezies, und ist $U \leq S_n$ der entsprechende Stabilisator, dann schreiben wir auch kurz

$$\frac{G}{U}$$

für den Typ von G. Diese Schreibweise bewährt sich, wenn man Verknüpfungen bildet, z.B. ist

$$\frac{Single^m}{U} \cdot \frac{Single^n}{V} = \frac{Single^{m+n}}{U \oplus V}.$$

etc.

11.9.4 Definition (atomare Spezies) Moleculare Spezies $G \neq LM$ heißen *atomar*, wenn sie nur trivial multiplikativ zerlegbar sind:

$$G = H \cdot K \Longrightarrow H = LM \vee K = LM.$$

•

Man kann zeigen, daß jede molekulare Spezies als Monom aus atomaren geschrieben werden kann.

11.10 Äquivalenz von Kategorien

Kehren wir wieder zu allgemeinen Kategorien zurück. Man nennt zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$ *isomorph* und schreibt

$$\mathcal{C} \simeq \mathcal{D},$$

wenn es Funktoren $F\colon \mathcal{C} \to \mathcal{D}$ und $G\colon \mathcal{D} \to \mathcal{C}$ gibt mit $FG = 1_{\mathcal{D}}$ sowie $GF = 1_{\mathcal{C}}$. Ein Beispiel bilden die Kategorie $\mathcal{C} = \mathcal{A}$ der abelschen Gruppen und die Kategorie $\mathcal{D} = {}_{\mathbb{Z}}\mathcal{M}$ der $\mathbb{Z}-$Linksmoduln,

$$\mathcal{A} \simeq {}_{\mathbb{Z}}\mathcal{M}.$$

Das Konzept der Isomorphie ist jedoch zu restriktiv, denn solche Kategorien wird man als im wesentlichen gleich ansehen. Ein geeigneter aber weniger einschränkender Begriff ist folgende:

11.10.1 Definition (Äquivalenz von Kategorien) Zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$ heißen *äquivalent,*

$$\mathcal{C} \equiv \mathcal{D},$$

wenn es Funktoren $F\colon \mathcal{C} \to \mathcal{D}$ und $G\colon \mathcal{D} \to \mathcal{C}$ gibt mit natürlichen Isomorphismen von FG auf $1_{\mathcal{D}}$ und von GF auf $1_{\mathcal{C}}$, kurz:

$$FG \simeq 1_{\mathcal{D}},\ GF \simeq 1_{\mathcal{C}}.$$

•

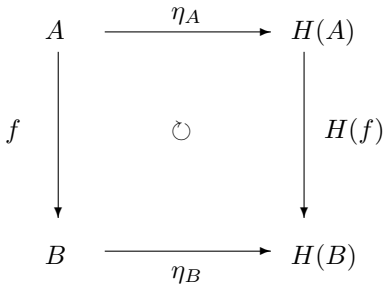
Zur Vorbereitung der Demonstration eines Beispiels — und zur genaueren Analyse dieses Begriffs Äquivalenz — bemerken wir zunächst folgendes:

11.10.2 Hilfssatz *Ist $H\colon \mathcal{C} \to \mathcal{D}$ ein Funktor mit $H \simeq 1_{\mathcal{C}}$, dann ist die Abbildung*

$$\hom_{\mathcal{C}}(A, B) \to \hom_{\mathcal{D}}(H(A), H(B)),\ f \mapsto H(f)$$

bijektiv.

Beweis: Die Kommutativität von



ergibt $H(f) = \eta_B f \eta_A^{-1}$. Aus der Bijektivität von η_A und η_B folgt also die Behauptung.

□

Tatsächlich genügt es im Fall der Äquivalenz, von den beiden Funktoren F und G nur einen zu kennen, weil der andere daraus folgt. Deshalb die

11.10.3 Definition (Äquivalenzabbildung) Ein Funktor $F\colon \mathcal{C} \to \mathcal{D}$ heißt *Äquivalenzabbildung*, wenn es einen Funktor $G\colon \mathcal{D} \to \mathcal{C}$ gibt, so daß $FG \simeq 1_{\mathcal{D}}$ und von $GF \simeq 1_{\mathcal{C}}$. •

11.10.4 Hilfssatz *$F\colon \mathcal{C} \to \mathcal{D}$ ist genau dann eine Äquivalenzabbildung, wenn*

- *$F\colon \hom_{\mathcal{C}}(A,B) \to \hom_{\mathcal{D}}(F(A),F(B))\,,\ f \mapsto F(f)$ bijektiv ist, für alle $A, B \in \mathrm{Ob}(\mathcal{C})$, und*
- *für jedes $A' \in \mathrm{Ob}(\mathcal{D})$ ein Objekt $A \in \mathrm{Ob}(\mathcal{C})$ existiert, so daß $F(A)$ und A' isomorph sind.*

Beweis: Übungsaufgabe.

Ein Beispiel äquivalenter Kategorien ist

11.10.5 $$\mathcal{M}_R \ \equiv\ \mathcal{M}_{R^{n\times n}}.$$

Beweis: Zu $R-$Rechtsmoduln M sei

$$M^{(n)} := \oplus^n M = \{(m_0,\dots,m_{n-1}) \mid m_i \in M\}$$

und zu $f \in \hom_R(M,N)$ entsprechend

$$f^{(n)} := \oplus^n f\colon M^{(n)} \to N^{(n)}\,,\ (m_0,\dots,m_{n-1}) \mapsto (f(m_0),\dots,f(m_{n-1})).$$

Wir wollen zeigen, daß

$$F\colon M \mapsto M^{(n)},\ f \mapsto f^{(n)}$$

eine Äquivalenzabbildung ist.

a) Die Injektivität ist klar.

b) Zum Nachweis der Surjektivität betrachten wir ein $g \in \hom_{R^{n\times n}}(M^{(n)},N^{(n)})$. Ist E_{ik} die Matrix mit einer Eins in $i-$ter Zeile und $k-$ter Spalte und sonst nur Nullen $i,k \in n$, dann ist, weil g mit E_{ik} vertauschbar ist,

$$g\big(M^{(n)}E_{ik}\big) \subseteq N^{(n)}E_{ik}.$$

Also gilt beispielsweise $(i = k := 0)$:

$$g(x,0,\dots,0) = (y,0,\dots,0),$$

mit einem $y \in N$, und man überlegt sich leicht, daß die Abbildung f, die durch $f(x) = y$ definiert wird, in $\hom_R(M,N)$ liegt. Wählt man $i = 1, k := 1$, so erhält man

$$g(0,x,0,\dots,0) = (0,y,0,\dots,0),$$

usw.. Insgesamt ergibt sich desshalb mit dem gerade definierten f, daß $g = f^{(n)}$, und die Surjektivität ist nachgewiesen.

c) Es bleibt zu einem $R^{n\times n}-$Modul M' ein $R-$Modul M zu finden, so daß M' isomorph $F(M)$ ist.

Die Diagonaleinbettung $r \mapsto r' := (r, \ldots, r)$ ist ein Homomorphismus von R in $R^{n\times n}$. Damit kann M' zu einem $R-$Rechtsmodul gemacht werden: $m'r := m'r'$. Die Teilmenge $M := M'E_{00}$ ist dann, wegen $r'E_{00} = E_{00}r'$, ein Untermodul von M'.

Wir wollen zeigen, daß die Abbildung

$$\eta_{M'}\colon M' \to F(M) = M^{(n)}\,,\; m' \mapsto (m'E_{00}, m'E_{10}, \ldots, m'E_{n-1,0})$$

ein Isomorphismus ist.

Zum Nachweis der Injektivität bemerken wir, daß $m'E_{i0} = 0$ für alle i, $m' = 0$ impliziert:

$$m' = m'\left(\sum_i E_{ii}\right) = m'\left(\sum_i E_{i0}E_{0i}\right) = \sum_i \left(m'E_{i0}\right)E_{0i} = 0.$$

Die Surjektivität ergibt sich durch Nachweis eines Urbildes von $(m_0, \ldots, m_{n-1})$. Zu jedem m_i gibt es ja, nach der Definition von M, m_i' mit

$$m_i = m_i'E_{00}.$$

Das Bild von $\sum_i m_i'E_{0i}$ ist

$$\eta_{M'}\left(\sum_i m_i'E_{0i}\right) = \sum_i \left(\eta_{M'}\left(m_i'E_{0i}\right)\right)$$

$$= \sum_i \left(m_i'E_{0i}E_{00}, \ldots, m_i'E_{0i}E_{i0}, \ldots, m_i'E_{0i}E_{n-1,0}\right) = \sum_i (0, \ldots, 0, m_i, 0, \ldots, 0).$$

□

Kapitel 12

Konstruktive Algebra

Die *algebraische Konstruktion anwendungsrelevanter mathematischer Strukturen* soll jetzt noch mit Hilfe von Vertiefungen der Theorie der Gruppenoperationen anhand von exemplarischen Beispielen weiter vorangetrieben werden. Dabei werden auch Methoden und Ergebnisse von Forchungsprojekten am Lehrstuhl II geschildert, die diesem Themenkreis gewidmet sind. Ihre Anwendung auf die Konstruktion kombinatoricher Designs wir detailliert beschrieben.

12.1 Gruppenoperationen auf Halbordnungen

Wir betrachten jetzt Gruppenoperationen auf strukturierten Mengen, die eine Halbordnung oder eine Verknüpfung oder beides respektieren, insbesondere solche, die Halbordnungen und/oder die Verknüpfungen $\wedge$ und $\vee$ auf einem endlichen Verband respektieren. Es geht also jetzt um *endliche Operationen von Gruppen als Gruppen von Automorphismen auf Halbordnungen, Halbgruppen oder Verbänden*, in folgendem Sinne:

12.1.1 Definition (ordnungsgemäße Operation) Ist $(X, \leq)$ eine Halbordnung, ${}_GX$ eine Operation von G auf X, dann operiert G auf X als eine Gruppe von *Automorphismen* genau dann, wenn

$$\forall\ g \in G,\ x, x' \in X\ (x \leq x' \iff gx \leq gx').$$

Wir kürzen dies wie folgt ab:

$${}_G(X, \leq),$$

und nennen die Operation auch *ordnungsgemäß*. •

Ein Beispiel ist die Operation

$${}_G(L(G), \leq).$$

von G auf dem Untergruppenverband via Konjugation.

12.1.2 Hilfssatz *Ist* ${}_G(X, \leq)$ *eine endliche ordnungsgemäße Operation, dann gilt:*

- *Je zwei Elemente in derselben Bahn sind unvergleichbar, d.h Bahnen sind Antiketten.*

- *Man kann die Bahnen* ω_i *von* G *auf* X *so numerieren, daß*

  $$\omega_i \ni x \leq x' \in \omega_k \Longrightarrow i \leq k.$$

- *Für jede Bahn* ω *und für festes* $x \in X$ *sind die Anzahlen*

  $$\left|\, \{x' \in \omega \mid x \leq x'\} \,\right| \text{ und } \left|\, \{x' \in \omega \mid x \geq x'\} \,\right|$$

  nur von der Bahn von x *abhängig und nicht von der Wahl des Repräsentanten* x*.*

- *Für alle* $x, x' \in X$ *haben wir*

  $$|G(x)| \cdot |\{x'' \in X \mid x \leq x'' \in G(x')\}| = |G(x')| \cdot |\{x''' \in X \mid x' \geq x''' \in G(x)\}|.$$

Beweis:

i) Wäre $x \in X$ vergleichbar mit $gx \neq x$, und etwa (oBdA!) $x < gx$, dann ergäbe sich der Widerspruch

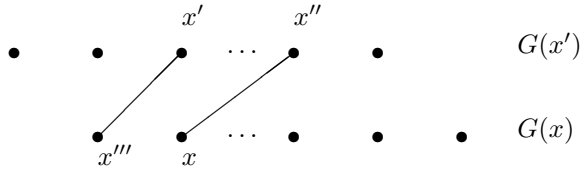
$$x < gx < g^2x < \ldots < g^{-1}x < x.$$

ii) Seien $x_0, x_1 \in \omega_i, x_0', x_1' \in \omega_k, i \neq k$. Angenommen $x_0 < x_0'$ und x_1, x_1' seien vergleichbar. Dann würde $x_1 > x_1'$ ergeben, für geeignete $g, g' \in G$: $gx_0 = x_1 > x_1' = g'x_0'$, also $x_0 > g^{-1}g'x_0'$, was den Widerspruch $x_0' > g^{-1}g'x_0'$ ergibt. Demnach kann die Halbordnung in eine Totalordnung eingebettet werden, welche die Halbordnung respektiert:

$$\underbrace{x_0, x_1, \ldots, x_{|\omega_0|-1}}_{\in\, \omega_0}, \underbrace{x_{|\omega_0|}, \ldots, x_{|\omega_0|+|\omega_1|-1}}_{\in\, \omega_1}, \ldots, \text{wobei } x_i < x_k \text{ impliziert } i < k.$$

iii) ist klar nach 12.1.1.

iv) folgt mit Hilfe einer doppelten Abzählung. Wir betrachten dazu den bipartiten Graphen aus den beiden Bahnen $G(x)$ und $G(x')$, wobei vergleichbare Elemente durch eine Kante verbunden seien:



□

12.1.3 Folgerung *Jede endliche ordnungsgemäße Operation* ${}_G(X, \leq)$ *induziert eine Halbordnung* $(G \setminus\!\setminus X, \leq)$ *auf* $G \setminus\!\setminus X$:

$$\omega \leq \omega' \iff \exists\, x \in \omega, x' \in \omega' \colon\ x \leq x'.$$

□

Hilfssatz 12.1.2 zeigt, daß für jede endliche ordnungsgemäße Operation ${}_G(X, \leq)$ und jede Numerierung ihrer Bahnen ω_i (mit Repräsentanten $x_i \in \omega_i$), die den Bedingungen des Hilfssatzes gehorcht, erhalten wir die beiden Matrizen

$$A^{\leq} := \left(a_{ik}^{\leq}\right) \ \text{ und } \ A^{\geq} := \left(a_{ik}^{\geq}\right),$$

definiert durch

$$a_{ik}^{\leq} := \left|\, \{x'' \in \omega_k \mid x_i \leq x''\} \,\right| \ \text{ und } \ a_{ik}^{\geq} := \left|\, \{x'' \in \omega_k \mid x_i \geq x''\} \,\right|.$$

Ihre Einträge hängen über die folgenden Identitäten eng zusammen, so daß die eine aus der anderen mit Hilfe der Bahnenlängen berechnet werden kann:

12.1.4 $$|\,\omega_i| \cdot a_{ik}^{\leq} = |\,\omega_k| \cdot a_{ki}^{\geq}.$$

Ein Verband $(L, \wedge, \vee)$ definiert eine Halbordnung $(L, \leq)$ und liefert darüberhinaus die beiden *Halbgruppen* $(L, \wedge)$ und $(L, \vee)$, denn beide Verknüpfungen sind ja assoziativ.

12.1.5 Hilfssatz *Sei ${}_GL$ eine endliche Operation auf einem Verband $(L, \wedge, \vee)$. Dann sind die folgenden drei Bedingungen äquivalent:*

- $\forall\ x, x', g:\ x < x' \Longrightarrow gx < gx'$,
- $\forall\ x, x', g:\ g(x \wedge x') = gx \wedge gx'$,
- $\forall\ x, x', g:\ g(x \vee x') = gx \vee gx'$.

Beweis:

i) $\Rightarrow$ ii)$\wedge$iii): Weil $x \wedge x'$ kleiner gleich x und kleiner gleich x' ist, erhalten wir aus i), daß $g(x \wedge x')$ kleiner gleich gx ist und kleiner gleich gx'. Das liefert

$$g(x \wedge x') \leq gx \wedge gx'. \qquad (\star)$$

Wäre $g(x \wedge x')$ strikt kleiner als $gx \wedge gx'$, dann hätten wir, nach i):

$$g^2(x \wedge x') < g(gx \wedge gx') \leq g^2x \wedge g^2x',$$

wobei sich die letzte Ungleichung sich aus $(\star)$ ergibt. Demnach haben wir, für jedes $n \in \mathbb{N}$,

$$g^n(x \wedge x') < g^nx \wedge g^nx',$$

was einen Widerspruch ergibt, wenn wir $n := |\langle g \rangle|$ setzen. Also muß $g(x \wedge x') = gx \wedge gx'$ gelten. Die dritte Identität folgt ganz analog.

ii) $\Rightarrow$ i): Die Annahme $x < x'$ ergibt $x \wedge x' = x$, so daß $g(x \wedge x') = gx$, und damit, wegen ii), $gx \leq gx'$. Dies impliziert $gx < gx'$, weil $x \neq x'$.

iii) $\Rightarrow$ i) ergibt sich ganz entsprechend.

□

12.1.6 Definition (Verbandsoperation) Ist eine dieser Bedingungen erfüllt, dann schreiben wir

$${}_GL(L, \wedge, \vee)$$

und nennen die Opertion eine *Verbandsoperation*. •

Eine direkte Konsequenz von 12.1.2 ist, daß in diesem Fall die folgenden Anzahlen nicht von der Wahl der Repräsentanten sondern nur von deren Bahn abhängen:

12.1.7 $\quad a_{ik}^{\wedge} := \big|\, \{x' \in \omega_k \mid x_i \leq x'\} \,\big|$ and $a_{ik}^{\vee} := \big|\, \{x' \in \omega_k \mid x_i \geq x'\} \,\big|$,

wobei wieder $x_i \in \omega_i$.
Erfüllt die Numerierung die Bedingung von Punkt ii) in 12.1.2, dnn ist $A^{\wedge} := (a_{ik}^{\wedge})$ eine obere, $A^{\vee} := (a_{ik}^{\vee})$ eine untere Dreiecksmatrix. Die Hauptdiagonalen bestehen aus Einsen, beide Matrizen sind also invertierbar über $\mathbb{Z}$. Weiterhin folgt aus 12.1.4, daß die Elemente dieser Matrizen über die folgenden Gleichungen zusammenhängen:

$$|\,\omega_i| \cdot a_{ik}^{\wedge} = |\,\omega_k| \cdot a_{ki}^{\vee}.$$

$(L, \wedge)$ und $(L, \vee)$ sind Halbgruppen. Betrachten wir deshalb jetzt den allgemeineren Fall:

12.1.8 Definition (Halbgruppenoperation) Ist $(X, \cdot)$ eine Halbgruppe, dann heißt ${}_GX$ *Halbgruppenoperation*, wenn

$$\forall\ x, x', g:\ \ g(x \cdot x') = gx \cdot gx'.$$

Wir bezeichnen sie mit

$${}_G(X, \cdot).$$

•

Sind dabei

$$\omega_0, \ldots, \omega_{d-1}$$

die Bahnen, dann bemerken wir zunächst, daß die Anzahlen der Lösungen $(x, x') \in \omega_i \times \omega_j$ von $x \cdot x' = z$, *nicht* von der Auswahl des Repräsentanten z, sondern nur von dessen Bahn abhängen, denn aus Lösungen (x, x') der Gleichung $x \cdot x' = z$ ergeben sich bijektiv die Paare (gx, gx') mit $gx \cdot gx' = gz$. Wir können demnach die folgenden Anzahlen definieren, für $x_k \in \omega_k$,

12.1.9 $$a_{ijk} := \big|\, \{(x, x') \in \omega_i \times \omega_j \mid x \cdot x' = x_k\} \,\big|.$$

Jetzt soll ein Ring definiert werden, der diese Zahlen als Strukturkonstanten hat. Zu diesm Zweck betrachten wir den *Halbgruppenring* von X über $\mathbb{Z}$,

$$\mathbb{Z}^X = \{f \mid f\colon X \to \mathbb{Z}\},$$

mit punktweiser Addition und Faltung als Multiplikation:

$$(f + f')(x) := f(x) + f'(x),\ \ (f \star f')(x) := \sum_{x' \cdot x'' = x} f(x') f'(x'').$$

Wir bezeichnen diesen Ring mit $\mathbb{Z}^{X,\cdot}$. Seine Elemente schreiben wir wie meist üblich als "formale Summen"

$$f = \sum_{x \in X} f_x x,\ \text{ mit } f_x := f(x).$$

Ist jetzt ${}_GX$ eine Halbgruppenoperation, dann gilt:

12.1.10 Folgerung *Für jede endliche Halbgruppenoperation* ${}_G(X, \cdot)$ *gilt:*

- *Die G–Invarianten von $f \in \mathbb{Z}^X$ bilden den Teilring:*

$$\mathbb{Z}_G^{X,\cdot} := \{f : X \to \mathbb{Z} \mid \forall\ g \in G\colon f = f \circ \bar{g}^{-1}\}.$$

- *Dieser Teilring hat als $\mathbb{Z}$–Basis die* Bahnensummen

$$\underline{\omega_i} := \sum_{x \in \omega_i} x\ \ \in\ \ \mathbb{Z}_G^{X,\cdot}.$$

- *Die Strukturkonstanten von $\mathbb{Z}_G^{X,\cdot}$ sind die $a_{ijk}^{\cdot}$ von 12.1.9, d.h. für die Produkte der Basiselemente gilt*

$$\underline{\omega_i} \star \underline{\omega_j} = \sum_k a_{ijk}^{\cdot}\ \underline{\omega_k}.$$

□

Anwendung auf Verbandsoperationen liefert

12.1.11 Folgerung

- *Jede endliche Verbandsoperation ${}_G(L, \wedge, \vee)$ liefert die beiden Halbgruppenringe*

$$\mathbb{Z}^{L,\wedge} \text{ und } \mathbb{Z}^{L,\vee}.$$

- *Sie enthalten als Teilringe die Invariantenringe*

$$\mathbb{Z}_G^{L,\wedge} \text{ bzw. } \mathbb{Z}_G^{L,\vee}.$$

- *$\mathbb{Z}$–Basen dieser Teilringe sind die Bahnensummen, und ihre Strukturkonstanten sind die*

$$a_{ijk}^{\wedge} := \left| \{(x, x') \in \omega_i \times \omega_j \mid x \wedge x' = x_k\} \right|,$$

bzw.

$$a_{ijk}^{\vee} := \left| \{(x, x') \in \omega_i \times \omega_j \mid x \vee x' = x_k\} \right|.$$

□

Ein paradigmatisches Beispiel ist der Untergruppenverband $L := L(G)$ mit der Konjugation als Operation.

12.1.12 Der Satz von Plesken *Sei ${}_G(L, \wedge, \vee)$ eine endliche Verbandsopertion mit den Bahnen $\omega_0, \ldots, \omega_{d-1}$ und deren Summen $\underline{\omega_0}, \ldots, \underline{\omega_{d-1}}$ im Halbgruppenring, numeriert entsprechend 12.1.2.*

- *Die Abbildung*

$$\underline{\omega_k} \mapsto \begin{pmatrix} a_{0,k}^{\wedge} \\ \vdots \\ a_{d-1,k}^{\wedge} \end{pmatrix}$$

definiert einen Ringisomorphismus zwischen $\mathbb{Z}_G^{L,\wedge}$ und $\mathbb{Z}^d$, während

- *die Abbildung*

$$\underline{\omega_k} \mapsto \begin{pmatrix} a_{0,k}^{\vee} \\ \vdots \\ a_{d-1,k}^{\vee} \end{pmatrix}$$

einen Ringisomorphismus zwischen $\mathbb{Z}_G^{L,\vee}$ und $\mathbb{Z}^d$, dabei sei $\mathbb{Z}^d$ der Ring der Abbildungen von d nach $\mathbb{Z}$ mit punktweiser Addition und Multiplikation.

Beweis: Um zunächst die Homomorphieeigenschaft zu beweisen, betrachten wir das Hadamardprodukt $a_i^\wedge \cdot a_j^\wedge$ von i–ter und j–ter Spalte von $A^\wedge$. Wir wollen verifizieren, daß

$$a_i^\wedge \cdot a_j^\wedge = \sum_k a_{ijk}^\wedge a_k^\wedge.$$

Aus der Definition von $a_{li}^\wedge$ ergibt sich (für ein festes $x \in \omega_l$):

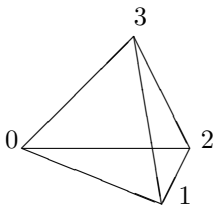
$$a_{li}^\wedge \cdot a_{lj}^\wedge = |\{y \in \omega_i \mid y \geq x\}| \cdot |\{z \in \omega_j \mid z \geq x\}|$$

$$= |\{(y,z) \in \omega_i \times \omega_j \mid x \leq (y \wedge z)\}| = \sum_k a_{ijk}^\wedge a_{lk}^\wedge,$$

was die Homomorphie beweist. Um die Isomorphie zu zeigen, verwenden wir, daß sowohl $A^\wedge := (a_{ik}^\wedge)$ als auch $A^\vee := (a_{ik}^\vee)$ invertierbar sind über $\mathbb{Z}$. Das zeigt Isomorphie und vervollständigt den Beweis des ersten Teils der Behauptung, der zweite Teil ergibt sich ganz analog.

□

Dekorative Verbände, auf denen endliche Gruppen als Gruppen von Automorphismen operieren, bilden die Flächen, Kanten und Ecken der regulären Polyeder: Tetraeder, Würfel, Oktaeder, Dodekaeder, Ikosaeder usw.. Betrachten wir den einfachsten Fall, das *Tetraeder*:



Seine vier Flächen, sechs Kanten und vier Ecken bilden zusammen mit dem Tetraeder T selbst und mit der leeren Menge $\emptyset$ einen Verband L der Ordnung 16, der per Inklusion halbgeordnet ist. Offenbar operiert die alternierende Gruppe A_4 auf L und respektiert Inklusionen, d.h. sie operiert auf L als Gruppe von Automorphismen. Die entsprechenden Matrizen $A^\wedge$ und $A^\vee$ sind:

$$A^\wedge = \begin{pmatrix} 1 & 4 & 6 & 4 & 1 \\ & 1 & 3 & 3 & 1 \\ & & 1 & 2 & 1 \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}, \quad A^\vee = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix}.$$

Als eine Anwendung betrachten wir einmal das Hadamardprodukt zweier Spalten und schreiben dieses als Linearkombination der Spalten, z.B.

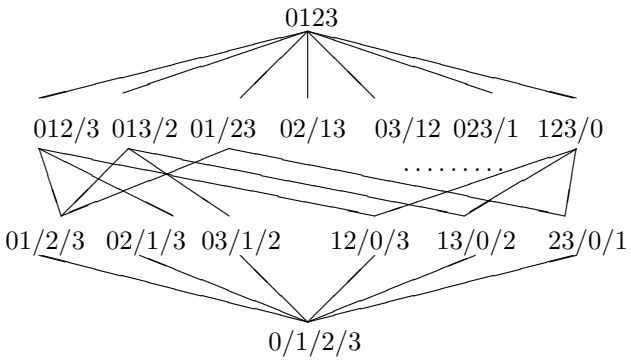
$$a_2^\wedge \cdot a_3^\wedge = \begin{pmatrix} 24 \\ 9 \\ 2 \\ 0 \\ 0 \end{pmatrix} = 2a_2^\wedge + 3a_1^\wedge.$$

Diese Identität zeigt, daß $a^{\wedge}_{232} = 2$ and $a^{\wedge}_{231} = 3$, und dies wiederum bedeutet, daß jede Kante des Tetraeders auf genau zwei Weisen als Infimum einer Fläche und einer Kante beschrieben werden kann, während eine Ecke auf genau drei Weisen als ein solches Infimum dargestellt werden kann.

Ein weiteres Beispiel ist der Verband

$$Par(n),$$

halbgeordnet via Verfeinerung. Hier ist eine Skizze von $Par(4)$:



Ordnen wir die Längen der Blöcke von $p \in Par(n)$ absteigend in eine Folge α, dann erhalten wir eine Zahlpartition

$$\alpha(p) = (\alpha_0, \alpha_1, \ldots) \vdash n,$$

den *Typ* von p.

S_n operiert auf $Par(n)$ als Gruppe von Automorphismen. Die Bahnen sind die Mengen der Partitionen vom selben Typ. Wählen wir für unser Beispiel die Numerierung

$$\omega_0 := S_4(0/1/2/3),\ \omega_1 := S_4(01/2/3),\ \omega_2 := S_4(01/23),$$

$$\omega_3 := S_4(012/3),\ \omega_4 := S_4(0123),$$

dann sehen die Matrizen $A^{\wedge}$ und $A^{\vee}$ von $Par(4)$ so aus:

$$A^{\wedge} = \begin{pmatrix} 1 & 6 & 3 & 4 & 1 \\ & 1 & 1 & 2 & 1 \\ & & 1 & 0 & 1 \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix},\quad A^{\vee} = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 0 & 1 & \\ 1 & 6 & 3 & 4 & 1 \end{pmatrix}.$$

Wieder liefern Spaltenprodukte interessante Abzählresultate, z.B. zeigt

$$a^{\vee}_1 \cdot a^{\vee}_2 = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \\ 18 \end{pmatrix} = 2a^{\vee}_2 + 12a^{\vee}_4,$$

daß es genau zwei Möglichkeiten gibt, eine Mengenpartition vom Typ (2^2) der Menge 4 als Supremum $p \vee p'$ aus einer Partition p vom Typ $(2, 1^2)$ und einer Partition p' vom Typ (2^2). Darüberhinaus zeigt diese Gleichung noch, daß die Partition 0123 vom Typ (4) auf genau 12 Weisen als Supremum $p \vee p'$ geschrieben werden kann, mit $\alpha(p) = (2, 1^2)$ und $\alpha(p') = (2^2)$.

12.2 Kombinatorische Designs

Designs sind kombinatorische Strukturen, die aus der statistischen Versuchsplanung (design of experiments) und aus der Geometrie stammen, auch Systemtips im Lotto gehören dazu. Sie werden mit Hilfe von Parameterquadrupeln $t, v, k, \lambda \in \mathbb{N}^*$ beschrieben, so daß sich u.a. auch die Frage stellt, zu welchen Parameterquadrupeln Designs existieren.

Bei entsprechenden Untersuchungen spielten in jüngster Zeit Verbandsoperationen eine zentrale Rolle, diese werden jetzt bechrieben. Dabei gelang u.a. die weltweit erste Konstruktion eines 7-Designs ($t = 7$) mit kleinen Parametern durch die Verwendung einer Matrix $A^\wedge$, im Zusammenspiel mit einer modernen Implementierung des LLL-Algorithmus zur Lösung diophantischer Gleichungen.

12.2.1 Definition ($t-(v,k,\lambda)$-Design) Ein $t-(v,k,\lambda)$-*Design* ist eine Teilmenge

$$\mathcal{B} \subseteq \binom{v}{k}$$

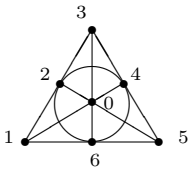
der Menge der k-Teilmengen einer Menge v von *Punkten*. Die Elemente $B \in \mathcal{B}$ heißen *Blöcke*, und die *Parameter* t, v, k und λ müssen den folgenden Bedingungen genügen:

$$\forall\, T \in \binom{v}{t} \colon \; \big|\, \{B \in \mathcal{B} \mid T \subseteq B\} \,\big| = \lambda,$$

d.h. jede t-Teilmenge der Punktemenge liegt in genau λ Blöcken. •

12.2.2 Beispiele aus der Geometrie sind die projektiven Ebenen.

i) Hier zunächst ein gut bekannter Spezialfall, die *Fanoebene,*



Hierbei ist

$$\mathcal{B} = \{\{1,2,3\},\{3,4,5\},\{5,6,1\},\{0,1,4\},\{0,2,5\},\{0,3,6\},\{2,4,6\}\},$$

$v = 7$, $k = 3$. Die Fanoebene ist ein 1-Design mit $\lambda = 3$, und sie ist auch ein 2-Design mit $\lambda = 1$.

ii) Wie die Fanoebene sind sämtliche *projektiven Ebenen* 2-Designs mit $\lambda = 1$ (und der Zusatzbedingung, daß je zwei Blöcke genau einen Punkt gemeinsam haben). Genauer: Die klassischen projektiven Ebenen sind, für Primzahlpotenzen q, $2-(q^2+q+1, q+1, 1)$–Designs. ◇

Die Designs auf der Punktemenge v kann man mit Hilfe der *Inzidenzmatrix* $M^v_{t,k}$ beschreiben, deren Zeilen zu den $T \in \binom{v}{t}$ gehören, die Spalten zu den $K \in \binom{v}{k}$. Die Einträge m^v_{TK} von $M^v_{t,k}$ sind wie folgt definiert:

$$m^v_{TK} := \begin{cases} 1, & \text{falls } T \subseteq K, \\ 0, & \text{sonst.} \end{cases}$$

Ein $t-(v,k,\lambda)$-Design $\mathcal{B}$ ist dann eine Auswahl geeigneter Spalten dieser Matrix:

12.2.3 Folgerung *Die Menge aller $t-(v,k,\lambda)$-Designs auf v ist die Menge der Blöckemengen $\mathcal{B}$, die man aus den 0-1-Lösungen x des linearen Gleichungssystems*

$$M^v_{t,k} \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}$$

wie folgt bekommt:

$$\mathcal{B} := \Big\{ B \in \binom{v}{k} \;\Big|\; x_B = 1 \Big\}.$$

□

$M^v_{t,k}$ ist eine $\binom{v}{t} \times \binom{v}{k}$-Matrix, und die Ermittlung von 0-1-Lösungen ist ein schwieriges Problem. Nach der Konstruktion der ersten 6-Designs versuchte man lange vergeblich, 7-Designs mit moderaten Parametern zu finden (solche mit "astronomischen" Parametern waren aus einem Existenzsatz von Teirlinck seit 1987 bekannt). Es bestand bald die Vermutung, daß es womöglich 7-Designs mit $v = 33$ und $k = 8$ geben könne. In diesem Fall hat die Inzidenzmatrix etwa $6 \cdot 10^{13}$ Einträge, λ war unbekannt, es war (und ist) aber zur Zeit unmöglich, 0-1-Lösungen für derart große Systeme zu finden.

Der "Trick" war (und ist) es, zur Reduktion des Problems weitere Bedingungen an die Designs zu stellen, die wir konstruieren wollen. Als sehr wirksam hat sich die Methode erwiesen, *eine Untergruppe $G \leq S_v$ vorzugeben, die in der Automorphismengruppe enthalten sein soll.* Das ist natürlich riskant, denn oft wird es keine Designs mit dieser Eigenschaft geben. Andererseits reduziert man den Suchraum und die Datenmenge ganz gewaltig. Hinzukommt, daß diese Methode auch bei anderen Strukturen verwendbar ist, z.B. bei der Suche nach linearen Codes mit vorgegebener Minimaldistanz (M. Braun und A.Kohnert haben auf diese Weise mehrere Hundert Codes gefunden mit besseren Parametern als bisher bekannt).

Im Fall der 7-Designs hatte man tatsächlich eine Gruppe "in Verdacht", konnte aber das entsprechende Gleichungssystem nicht lösen, was dann hier in Bayreuth 1995 gelungen ist. Seitdem konnte mit dieser Methode die Existenz von $t-(v,k,\lambda)$-Designs für Tausende neuer Parameterquadrupel (t,v,k,λ) nachgewiesen werden (R. Laue).

Ein Element $\pi \in S_v$ heißt *Automorphismus* des Designs $\mathcal{B}$, wenn gilt

$$\pi\mathcal{B} := \big\{ \pi B := \{\pi b \mid b \in B\} \;\big|\; B \in \mathcal{B} \big\} = \mathcal{B}.$$

Jede Untergruppe $G \leq S_v$, die aus solchen Automorphismen besteht, heißt *eine* Gruppe von Automorphismen des Designs, und die Gruppe aller dieser Automorphismen heißt *die* oder die *volle* Automorphismengruppe:

$$Aut(\mathcal{B}) := \{\pi \in S_v \mid \pi\mathcal{B} = \mathcal{B}\}.$$

Die Aufgabe ist also die Berechnung von mindestens einem $t-(v,k,\lambda)$-Design, das G in seiner vollen Automorphismengruppe enthält und, wenn möglich, alle solchen $t-(v,k,\lambda)$-Designs zu ermitteln und zu klassifizieren. Natürlich hätte man auch gerne all diejenigen Designs bestimmt, die G als *volle* Automorphismengruppe haben.
Um diese Probleme in die Reichweite heutiger PCs zu bringen, betrachten wir, anstelle von $M^v_{t,k}$, eine weit kleinere Matrix, die mit Hilfe von G gewonnen wird. *Diese Matrix ist eine Teilmatrix der Matrix $A^\wedge$ zur Verbandsoperation ${}_G(2^v, \cap, \cup)$, die oben schon erwähnt wurde*:

$$M^G_{t,k} := (m^G_{T,K}), \text{ mit } m^G_{T,K} := |\{K' \in G(K) \mid T \subseteq K'\}|,$$

T durchläuft dabei eine Transversale von $G \setminus\!\setminus \binom{v}{t}$, K eine Transversale von $G \setminus\!\setminus \binom{v}{k}$.

Es sei jetzt daran erinnert, daß die Berechnung solcher Transveralen via Doppelnebenklassentransveralen erfolgen kann: S_v operiert transitiv auf $\binom{v}{k}$ und auf $\binom{v}{t}$, wir erhalten also — über das Fundamentallemma — Bijektionen

$$G \setminus\!\setminus \binom{v}{k} \to G\backslash S_v / S_k \oplus S_{v\backslash k}\,,\; G(\gamma K) \mapsto G\gamma(S_k \oplus S_{v\backslash k}),$$

wobei $K := \{0, 1, \ldots, k-1\} \in \binom{v}{k}$, $S_k \oplus S_{v\backslash k}$ der Stabilisator von K, $\gamma \in S_v$. Ganz entsprechend haben wir auch

$$G \setminus\!\setminus \binom{v}{t} \to G\backslash S_v / S_t \oplus S_{v\backslash t}\,,\; G(\gamma T) \mapsto G\gamma(S_t \oplus S_{v\backslash t}).$$

Man kann also aus Transversalen dieser Mengen von Doppelnebenklassen Transversalen der Bahnen von G auf den k– und auf den t–Teilmengen gewinnen, also die Spaltenindizes K und die Zeilenindizes T der gesuchten Matrix $M^G_{t,k} := (m^G_{T,K})$, samt den entsprechenden Einträgen.

Spielentscheidend sind dabei Methoden, Transversalen von solchen Doppelnebenklassenmengen

$$G\backslash S_v / S_t \oplus S_{v-t}$$

sukzessive nach ansteigendem t zu berechnen (das *Leiterspiel*).

Weil G in der Automorphismengruppe liegen soll, besteht jedes Design $\mathcal{B}$ aus vollen Bahnen von G auf $\binom{v}{k}$, und weil G die Inklusion von t– in k–Teilmengen erhält, gilt

12.2.4 Der Satz von Kramer und Mesner *Die Menge aller $t-(v,k,\lambda)$-Designs mit $G \leq S_v$ als Gruppe von Automorphismen ergibt sich aus der Menge der 0-1-Lösungen x von*

$$M_{t,k}^{G} \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}.$$

□

12.2.5 Beispiel Betrachten wir zunächst ein Beispiel mit den sehr kleinen Parametern $t := \lambda := 1$, $v := 4$ und $k := 2$. Wegen

$$\binom{4}{2} = \big\{\{0,1\},\{0,2\},\{0,3\},\{1,2\},\{1,3\},\{2,3\}\big\}$$

und

$$\binom{4}{1} = \big\{\{0\},\{1\},\{2\},\{3\}\big\}$$

ergibt sich als Inzidenzmatrix

$$M_{t,k}^{v} = M_{1,2}^{4} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Schreibt man jetzt als Zusatzbedingung die folgende Gruppe von Automorphismen vor:

$$G := \langle (0123) \rangle,$$

eine Untergruppe der Ordnung 4 in S_4, dann ergeben sich die Bahnenmengen

$$G \setminus\!\setminus \binom{4}{2} = \Big\{\big\{\{0,1\},\{0,3\},\{1,2\},\{2,3\}\big\},\big\{\{0,2\},\{1,3\}\big\}\Big\},$$

und

$$G \setminus\!\setminus \binom{4}{1} = \big\{\{0\},\{1\},\{2\},\{3\}\big\}.$$

Diese Bahnenmengen entsprechen den Spalten bzw. den Zeilen der Kramer–Mesner–Matrix

$$M_{t,k}^{G} = M_{1,2}^{G} = \begin{pmatrix} 2 & 1 \end{pmatrix}.$$

Aus der Inzidenzmatrix mit 12 Elementen ist also eine Kramer–Mesner–Matrix mit nur noch 2 Einträgen geworden, und man sieht sofort, daß das lineare Gleichungssystem

$$M_{1,2}^{G} \cdot x = \begin{pmatrix} 2 & 1 \end{pmatrix} \cdot x = (\lambda)$$

für $\lambda = 1$ genau eine Lösung hat,

$$x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Das entsprechende Design ist

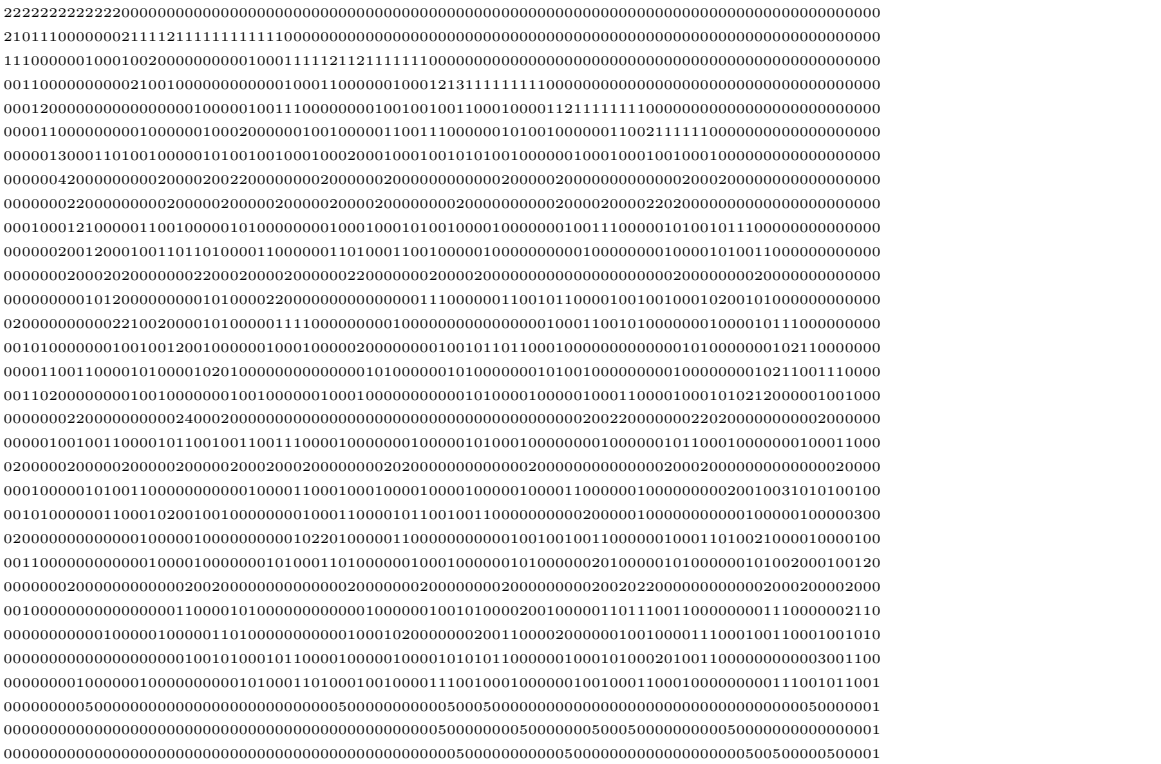
$$\mathcal{B} = \{\{0,2\},\{1,3\}\}.$$

Demnach existiert genau ein $1-(4,2,1)$-Design mit G als einer Gruppe von Automorphismen. (Weil G, als Gruppe der Ordnung 8, maximal in S_4 ist und S_4 offenbar *nicht* in der Automorphismengruppe liegt, ist G sogar die *volle* Automorphismengruppe dieses Designs.) ◇

Das historisch erste 7-Design mit moderaten Parametern, das gefunden wurde, war ein $7-(33,8,10)$-Design mit $G = \mathrm{P\Gamma L}_2(32)$, einer Untergruppe von S_{33} mit den Erzeugenden

$$\begin{aligned}\alpha &= (0)(1\,2\,4\,8\,16)(3\,6\,12\,24\,17)(5\,10\,20\,9\,18)(7\,14\,28\,25\,19)\\ &\quad (11\,22\,13\,26\,21)(15\,30\,29\,27\,23)(31)(32)\\ \beta &= (1\,18\,30)(2\,21\,12)(3\,10\,28)(4\,31\,32)(5\,24\,14)(6\,7\,17)(8\,25\,27)\\ &\quad (9\,19\,20)(11\,15\,13)(16\,23\,29)(22\,0\,26).\end{aligned}$$

Die Kramer–Mesner–Matrix, die bereits Magliveras und Leavitt bekannt war, und die von A. Betten erneut und mit Hilfe von Doppelnebenklassen berechnet wurde, ist



Sie hat um den *Faktor* 10^{10} weniger Einträge als die Inzidenzmatrix, so daß mit der verbesserten Implementierung des LLL-Algorithmus durch A. Wassermann die folgenden beiden Lösungen des Gleichungssystems mit $\lambda = 10$ und $\lambda = 16$ gefunden werden konnten:

00111000101001001100011010000100100000001011011000101111000000010010010100001101110110010101110001100011101011011001110010111011011111110100100111010000111111101101101011110010001001101010001111

Es zeigte sich später, daß es insgesamt 4 996 426 0-1-Vektoren x gibt, die das System für $\lambda = 10$ lösen. In der Zwischenzeit sind auch 8-Designs, 9-Designs ... gefunden worden.

12.3 Leiterspiel und Homomorphieprinzip

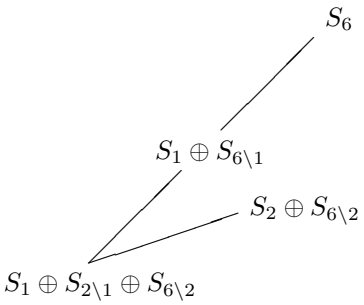
Zur Ermittlung von Kramer–Mesner–Matrizen benötigen wir also zunächst einmal Transversalen der Bahnenmengen $G \setminus\!\setminus \binom{v}{t}$ und $G \setminus\!\setminus \binom{v}{k}$, oder, bijektiv dazu, Transversalen der Doppelnebenklassenmengen

$$G\backslash S_v / S_t \oplus S_{v\backslash t}, \text{ und } G\backslash S_v / S_k \oplus S_{v\backslash k}.$$

Dabei ist $t \leq k$, es wäre also zweckmäßig, einen Algorithmus zu entwickeln, der die sukzessive Berechnung von Transversalen der Doppelnebenklassenmengen

$$G\backslash S_v / S_u \oplus S_{v\backslash u}$$

zu berechnen erlaubt, sukzessive nach an- oder absteigendem u.
Ein solcher Algorithmus existiert, das *Leiterspiel*, und er ist sehr vielseitig verwendbar. B. Schmalz hat ihn erstmals zur systematischen Berechnung von Designs mit gegebener Gruppe von Automorphismen verwendet (1990), hier in Bayreuth. Er verwendet auf- und absteigende Folgen von Untergruppen, wie beim Leiterspiel, daher der Name.
Nehmen wir beispielsweise einmal an, es gehe um die Berechnung von $1-(6,2,\lambda)$–Designs. Zur Ermittlung der Kramer–Mesner–Matrix brauchen wir dann Transversalen von $G\backslash S_6/S_1 \oplus S_{6\backslash 1}$ und von $G\backslash S_6/S_2 \oplus S_{6\backslash 2}$. Das Problem ist, daß die beiden Stabilisatoren $S_1 \oplus S_{6\backslash 1}$ und $S_2 \oplus S_{6\backslash 2}$ unvergleichbar sind bzgl. Inklusion, keine ist in der anderen enthalten. es gibt also keine absteigende oder ansteigende Kette von Untergruppen, in der beide enthalten sind. Es gibt aber eine auf- und absteigende *Leiter* von Untergruppen, die beide enthält:



Es stellt sich also die Frage, wie wir sukzessive Transversalen der Doppelnebenklassenmengen

$$G\backslash S_6 / U$$

berechnen können, für die U aus dieser Leiter. Diese Doppelnebenklassenmengen sind Bahnenmengen $G \backslash\backslash S_6/U$, es geht also um Transversalen der Bahnenmengen von G auf den Nebenklassenmengen S_6/U, sukzessive zu berechnen für die U entlang der Untergruppenleiter.

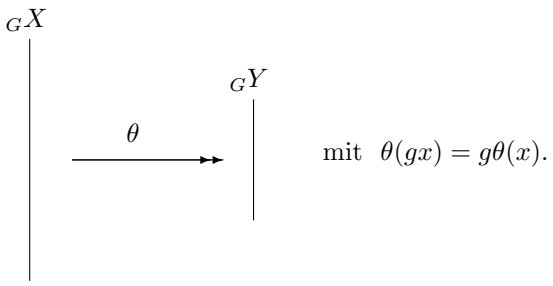
Ein Problem entsteht z.B. wenn wir von U zu einer Untergruppe $V \leq U$ übergehen. Es fragt sich, wie wir aus einer Transversale von $G \backslash\backslash S_6/U$ eine Transversale von $G \backslash\backslash S_6/V$ ermitteln können. Hier hilft die Anwendung des im folgenden beschriebenen Homomorphieprinzips. Dazu bezeichnen wir wei Operationen ${}_GX$ und ${}_GY$ als *epimorph*, kurz

$$ {}_GX \twoheadrightarrow_G {}_GY, $$

wenn es eine surjektive Abbildung $\theta\colon X \twoheadrightarrow Y$ gibt mit

$$ \theta(gx) = g\theta(x). $$

Hier ist eine Skizze dieser Situation:



Die Frage ist, wie man aus einer Transversalen T_Y von $G \backslash\backslash Y$, eine Transversale T_X von $G \backslash\backslash X$ ermitteln kann. Der folgende Satz gibt hierauf eine Antwort:

12.3.1 Das Homomorphieprinzip für Gruppenoperationen *Gegeben seien zwei* epimorphe *Operationen ${}_GX$ und ${}_GY$, d.h. wir haben eine surjektive Abbildung $\theta\colon X \twoheadrightarrow Y$ mit $\theta(gx) = g\theta(x)$, für alle $x \in X$, $g \in G$. Weiterhin sei bereits eine Transversale $T_{G \backslash\backslash Y}$ von $G \backslash\backslash Y$ ermittelt worden. Es gilt dann folgendes:*

- *Jede Bahn $\omega \in G \backslash\backslash X$ schneidet genau eines der Urbilder $\theta^{-1}(y)$ der Elemente $y \in T_{G \backslash\backslash Y}$,*

$$ \forall\ \omega \in G \backslash\backslash X\ \exists_1\ y \in T_{G \backslash\backslash Y}\colon\ \omega \cap \theta^{-1}(y) \neq \emptyset. $$

- *$\theta^{-1}(y)$ zerfällt in Bahnen von G_y, und zwei verschieden G_y-Bahnen auf $\theta^{-1}(y)$ liegen in verschiedenen Bahnen von G auf X.*

- *Es folgt, daß man eine Transversale $T_{G \backslash\backslash X}$ von $G \backslash\backslash X$ als (disjunkte) Vereinigung von Transversalen der Bahnen auf diesen Urbildern bekommt:*

$$ T_{G \backslash\backslash X} := \bigcup_{y \in T_{G \backslash\backslash Y}} T_{G_y \backslash\backslash \theta^{-1}(y)}. $$

Beweis:

i) Daß $\omega \in G \setminus\!\setminus X$ in genau einem Urbild repräsentiert ist folgt so:

a) Wegen der Surjektivität von θ hat jede Bahn $\omega \in G \setminus\!\setminus X$ einen nicht leeren Schnitt mit einem Urbild $\theta^{-1}(y)$, für ein geeignetes $y \in Y$, etwa

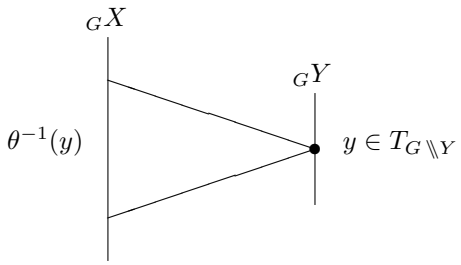
$$x \in \omega \cap \theta^{-1}(y) \neq \emptyset.$$

b) Wird die Bahn dieses y von $y' = gy \in T_{G \setminus\!\setminus Y}$ repräsentiert, dann gilt $\theta(gx) = g\theta(x) = gy = y'$, so daß $gx \in \theta^{-1}(y')$, also

$$gx \in \omega \cap \theta^{-1}(y') \neq \emptyset.$$

c) Umgekehrt ist das Bild $\theta(g'x)$ jedes $g'x \in \omega$ Element der Bahn von y', es gibt also tatsächlich *genau ein* Transversalenelement, dessen Urbild ω schneidet.

ii) Punkt i) hat gezeigt, daß wir nur die Urbilder $\theta^{-1}(y)$ der $y \in T_{G \setminus\!\setminus Y}$ betrachten müssen, um eine Transversale von $G \setminus\!\setminus X$ zu ermitteln:



Tatsächlich brauchen wir dort nicht G zu betrachten (i.a. ist $\theta^{-1}(y)$ auch keine Vereinigung von G-Bahnen), sondern es genügt die Verwendung der oftmals deutlich kleineren Untergruppe G_y. Sind nämlich $x, x' \in \theta^{-1}(y)$, mit $x' = gx$, dann gilt

$$y = \theta(x) = \theta(x') = \theta(gx) = g\theta(x) = gy,$$

was $g \in G_y$ ergibt. Darüberhinaus zerfällt $\theta^{-1}(y)$ ganz in Bahnen von G_y, denn $x \in \omega \cap \theta^{-1}(y)$ und $g \in G_y$ implizieren

$$\theta(gx) = g\theta(x) = gy = y.$$

Hinzukommt schließlich noch, daß verschiedene Bahnen von G_y in verschiedenen Bahnen von G liegen.

Punkt iii) faßt i) und ii) zusammen.

□

Eine direkte Konsequenz des Homomorphieprinzips ist die folgende systematische Methode zur rekursiven Berechnung von Transversalen:

12.3.2 Surjektive Auflösung *G operiere auf den Mengen $X_i, i \in m$, und es seien surjektive Abbildungen*

$$\theta_{i+1} : X_{i+1} \twoheadrightarrow X_i, \text{ zu jedem } i \in m-1$$

gegeben, die mit der jeweiligen Operation kommutieren:

$$\theta_{i+1}(gx_{i+1}) = g\theta_{i+1}(x_{i+1}), \text{ für jedes } i \in m-2, g \in G, x_{i+1} \in X_{i+1}.$$

Wir können dann eine Transversale T_{m-1} von $G \setminus\setminus X_{m-1}$ ermitteln, indem wir sukzessive, und ausgehend von einer Transversalen T_0 von $G \setminus\setminus X_0$ und den Stabilisatoren ihrer Elemente, die Urbilder $\theta_1^{-1}(x)$ der $x \in T_0$ und Transversalen der $G_x \setminus\setminus \theta_1^{-1}(x)$ berechnen. Aus der so berechneten Transversale T_1 von $G \setminus\setminus X_1$ erhält man analog T_2 usw. bis hin zu T_{m-1}, wie in 12.3.1 beschrieben.

□

Wir können diese Methode auf die rekursive Berechnung von Transversalen von Symmetrieklassen von Abbildungen $f \in Y^X$ anwenden, die Rekursion ist eine nach $|Y|$:

12.3.3 Anwendung (Repräsentanten von Symmetrieklaasen) Einfachheitshalber sei

$$Y^X = m^n.$$

G operiere also auf n und damit in kanonischer Weise auf $Y^X = m^n$. Die Methode der Surjektiven Auflösung 12.3.2 kann hier angewandt werden, denn die folgende Abbildung kommutiert mit der Operation von G auf den G–Mengen $X_k := k^n, k \geq 2$,

$$\theta_k \colon k^n \to (k-1)^n \,,\, f \mapsto f',$$

mit f', definiert durch

$$f'(i) := \begin{cases} f(i), & \text{falls } f(i) \in k-1, \\ k-2, & \text{sonst.} \end{cases}$$

Wir können demnach von $X_1 := 1^n$ starten, einer Menge, die au einer einzigen Abbildung besteht, nämlich aus der konstanten Abbildung $i \mapsto 0, i \in n$. Der Stabilisator ist G, das Urbild die Menge $X_2 := 2^n$. Im ersten Schritt haben wir also eine Transversale T_2 von $G \setminus\setminus 2^n$ zu ermitteln. Nehmen wir an, dies sei geschehen, und betrachten wir ein $f_2 \in T_2$, G_{f_2} sei der Stabilisator. Es bleibt, eine Transversale T_3 von

$$G_{f_2} \setminus\setminus \theta_3^{-1}(f_2)$$

zu bestimmen. Dieser Schritt kann wie folgt ausgeführt werden. Zwei Elemente f_3 und f_3' von $\theta_3^{-1}(f_2)$ können sich nur auf dem Urbild $f_2^{-1}(1)$ des Punktes 1 unterscheiden, und dort können nur die Werte 1 oder 2 angenommen werden. Wir brauchen deshalb nur eine Transversale T von

$$G_{f_2} \setminus\setminus \{1,2\}^{f_2^{-1}(1)}.$$

Die gesuchte Transversale T_3 besteht dann aus den Abbildungen $f_3'' \in 3^n$ mit

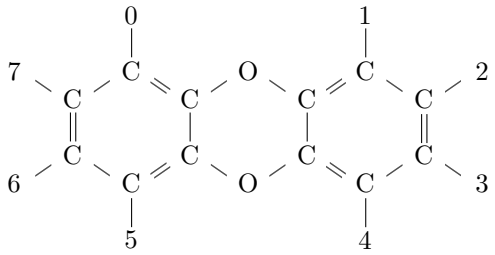
$$f_3'' \downarrow f_2^{-1}(1) \in T, \text{ und } f_3'' \downarrow n \backslash f_2^{-1}(1) = f_2 \downarrow n \backslash f_2^{-1}(1).$$

$\diamond$

Man kann dieses Verfahren beispielsweise zur Berechnung von Katalogen von k-Graphen verwenden, d.h. von Multigraphen mit durch k bechränkten Kantenvielfachheiten. Eine Erweiterung ist Th. Grüners Generator chemicher Strukturformeln, zusammenhängender Multigraphen mit gegebener Eckengradfolge.

Ein konkretes Beispiel aus den Naturwissenschaften soll diesen Paragraphen (und die Vorlesung) abschließen:

12.3.4 Anwendung Wir wollen die 22 Permutationsisomere des *Dioxin* konstruieren. Die chemische Formel ist $C_{12}O_2Cl_4H_4$. Unter den *Permuationsisomeren* des Dioxin versteht man die Moleküle mit dieser Formel und folgendem Molekülgerüst:



Es wird angenommen, daß dieses Gerüst planar und regelmäßig, die Symmetriegruppe also die Kleinsche Vierergruppe V_4 ist, die Symmetriegruppe des Rechtecks. Es geht also um die Bahnen dieser Gruppe auf den Abbildungen

$$f \in \{H, Cl\}^8,$$

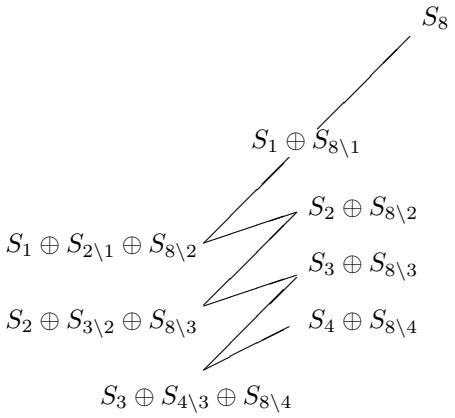
von der Menge 8 der acht freien Plätze des Molekülgerüsts in die Menge $\{H, Cl\}$, denn von diesen acht Plätzen sollen 4 durch ein Wasserstoffatom und 4 durch ein Chloratom besetzt werden. Es geht also genauer um die Bahnen von V_4 die aus Abbildungen vom Inhalt $(4, 4)$ bestehen, also um eine Transversale der Bahnenmenge

$$V_4 \backslash\backslash_{(4,4)} \{H, Cl\}^8.$$

Die symmetrische Gruppe S_8 ist transitiv auf der Menge dieser Abbildungen vom Inhalt $(4, 4)$. Der Stabilisator einer dieser Abbildungen ist $S_4 \oplus S_{8\backslash 4}$, die Bahnenmenge also bijektiv zu

$$V_4 \backslash S_8 / S_4 \oplus S_{8\backslash 4}.$$

Wir können also auch hier Untergruppenleitern und Homomorphieprinzip verwenden. Eine geeignete Leiter ist


S_8
$S_1 \oplus S_{8\setminus 1}$
$S_2 \oplus S_{8\setminus 2}$
$S_1 \oplus S_{2\setminus 1} \oplus S_{8\setminus 2}$
$S_3 \oplus S_{8\setminus 3}$
$S_2 \oplus S_{3\setminus 2} \oplus S_{8\setminus 3}$
$S_4 \oplus S_{8\setminus 4}$
$S_3 \oplus S_{4\setminus 3} \oplus S_{8\setminus 4}$

Index