KAPITEL 6

Algebra

6.1. Gruppen

Bekannt sind die Kongruenzklassen, bijektive Abbildungen, Permutationen. Wir hatten in diesen Fällen eine Verknüpfung auf einer Menge. (Addition bzw. Multiplikation bei den Kongruenzklassen, Komposition von Abbildungen bei den bijektiven Abbildungen) Die Gemeinsamkeit dieser Beispiel soll nun formalisiert werden.

6.1.1. Grundlagen, Definitionen, Beispiele.

DEFINITION 6.1.1. Gruppe

Eine *Gruppe* ist eine Menge G mit einer (zweistelligen) Verknüpfung $\star : G \times G \to G$, die folgende Eigenschaften hat:

(1) Für alle $x, y, z \in G$ gilt: $x \star (y \star z) = (x \star y) \star z$ (assoziativ)
(2) Es existiert ein *Eins* $1_G \in G$ mit: $1_G \star x = x \star 1_G$ für alle $x \in G$
(3) Für alle $x \in G$ existiert ein *inverses* Element x^{-1} für das gilt:$x\star x^{-1} = x^{-1}\star x = 1_G$
hat die Gruppe als weitere Eigenschaft:
(4) $x \star y = y \star x$ für alle $x, y \in G$ (kommutativ)

dann heisst sie *Abelsch* (nach Niels Henrik Abel).

EXAMPLE 6.1.2. Beispiel für Gruppen

Die ganzen Zahlen $\mathbb{Z}$ mit der Addition $+$ bilden eine Gruppe $(\mathbb{Z}, +)$. Diese Gruppe ist Abelsch. Die Eins in dieser Gruppe ist die 0. Das inverse Element von x ist $-x$. Betrachtet man statt der positiven Zahlen die natürlichen Zahlen so gibt es kein inverses Element bezüglich der Addition, $(\mathbb{N}, +)$ ist keine Gruppe. Bezüglich der Multiplikation ist keine der beiden Mengen eine Gruppe, da z.B. für 3 kein multiplikativ inverses Element innerhalb der Menge existiert.

Dieses Beispiel ist der Grund warum man gerne Abelsche Gruppen additiv statt multiplikativ schreibt. Das bedeutet auch dass man nx statt x^n für die $n-$fache Verknüpfung verwendet. Das inverse Element wird mit $-x$ bezeichnet und die 0 wird für das Einselement verwendet.

Die Sprechweise 'das inverse Element' und 'das Einselement' (vergleiche auch 0 und 1 in der Booleschen Algebra) ist durch folgendes Lemma gerechtfertigt:

LEMMA 6.1.3. *Eindeutigkeit von 1_G und x^{-1}.*

Sei G eine Gruppe, dann existiert genau ein Einselement und ein inverses Element.

BEWEIS. Seien e und f zwei Einselemente, dann gilt

$$e = fe = f.$$

Die erste Gleichheit ist die Einseigenschaft von f und die zweite Gleichheit die Einseigenschaft von e. Seien nun h und k zwei Inverse von g. Dann gilt

$$h = h1_G = h(gk) = (hg)k = 1_Gk = k.$$

□

EXAMPLE 6.1.4. Beispiel für Gruppen

Ein weiteres Beispiel welches wir schon kennengelernt haben sind die Kongruenzklassen von $\mathbb{Z}$ bei der Divsion durch eine Zahl n. Wir haben die Menge der Kongruenzklassen (man sagt auch Restklassen) in Abschnitt 2.4.2 mit $\mathbb{Z}_n$ bezeichnet. Auch $(\mathbb{Z}_n, +)$ ist eine Gruppe und auch in diesem Fall ist $(\mathbb{Z}_n, *)$ keine Gruppe, da $[0]_n$ kein multiplikativ inverses Element hat. Schränkt man sich aber auf die invertierbaren Elemente ein, wir haben diese Menge mit $\mathbb{Z}^*{}_n$ bezeichnet, dann erhalten wir eine multiplikative Abelsche Gruppe $(\mathbb{Z}^*{}_n, *)$.

Die Kongruenzklassen sind das erste Beispiel einer *endlichen* Gruppe. Weitere Beispiele für unendliche Gruppen sind $\mathbb{R}$,$\mathbb{Q}$,$\mathbb{C}$ diese sind bezüglich der Addition eine Gruppe, bezüglich der Multiplikation sind sie nach Streichen der Null eine Gruppe. Wenn man die Darstellung der komplexen Zahlen als

$$\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$$

mit der Nebenbedingung $i^2 = -1$, betrachtet kommt man natürlich zur Frage geht das auch noch in allgemeineren Fällen. Auf der Suche nach Verallgemeinerungen entdeckte der Ire Rowan Hamilton die *Quaternionen*.

$$H = \{a + ib + jc + kd : a, b, c, d \in \mathbb{R}\}$$

mit den Nebenbedingungen $i^2 = j^2 = k^2 = -1$ und $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$. Man sieht, dass die Multiplikation nicht mehr kommutativ ist, und man bekommt da $i, j, k, 1, -1, -k, -j, -i$ unter Multiplikation abgeschlossen sind folgende nicht Abelsche multiplikativ geschriebene Gruppe mit 8 Elementen, die sog. *Quaternionengruppe* Q_8. Dargestellt mit der Multiplikationstabelle, wie sie schon bei den Kongruenzklassen verwendet wurde.

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Die Gruppe ist nicht Abelsch, was man daran erkennt, dass die Multiplikationstabelle nicht symmetrisch an der Diagonale ist.

Der Test ob $(G, *)$ eine Gruppe ist kann allein an der Multiplikationstabelle entschieden werden. Die Existenz der 1 ist die Suche nach einer Spalte und einer Zeile in der die Einträge identisch sind zu den Elementen die die Zeilen und Spalten beschreiben. Die Existenz des inversen Elements ist die Frage ob in jeder Zeile und Spalte eine 1 vorkommt. Nur die Überprüfung der Assoziativität ist mühsam, man muss die für alle möglichen $3-$tupel überprüfen, d.h. bei Q_8 sind dies $2 \times 8^3 = 1024$ Produkte, die ausgerechnet werden müssen.

LEMMA 6.1.5. *wichtige Eigenschaft einer Gruppen Multiplikationstafel*

Jede Zeile und Spalte enthält jedes Element von G genau einmal.

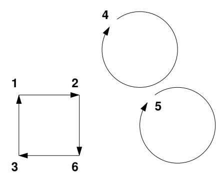
BEWEIS. mit Widerspruchsbeweis. Sei $xg = xh$ mit g, h verschieden. D.h. wir haben den Eintrag xg in der Zeile x in der Spalte für g und auch in der Spalte für h. Nun multipliziert man diese Gleichung von links mit dem inversen Element x^{-1} und erhält $g = h$. □

6.1.2. Permutationen. Bereits in 1.5.2 haben wir gesehen, dass die Permutationen vom Grad n eine Gruppe bilden. Dies ist die symmetrische Gruppe und wird mit S_n bezeichnet. Die Assoziativität folgt aus der entsprechenden Eigenschaft bijektiver Abbildungen. Dies ist nach der Quaternionen Gruppe ein weiteres Beispiel einer nicht kommutativen (=Abelschen) Gruppe. Wir hatten auch schon gesehen, dass die symmetrische Gruppe S_n genau $n!$ Elemente hat.

EXAMPLE 6.1.6. Multiplikationstabelle S_3

	$[1,2,3]$	$[1,3,2]$	$[2,1,3]$	$[2,3,1]$	$[3,1,2]$	$[3,2,1]$
$[1,2,3]$	$[1,2,3]$	$[1,3,2]$	$[2,1,3]$	$[2,3,1]$	$[3,1,2]$	$[3,2,1]$
$[1,3,2]$	$[1,3,2]$	$[1,2,3]$	$[3,1,2]$	$[3,2,1]$	$[2,1,3]$	$[2,3,1]$
$[2,1,3]$	$[2,1,3]$	$[2,3,1]$	$[1,2,3]$	$[1,3,2]$	$[3,2,1]$	$[3,1,2]$
$[2,3,1]$	$[2,3,1]$	$[2,1,3]$	$[3,2,1]$	$[3,1,2]$	$[1,2,3]$	$[1,3,2]$
$[3,1,2]$	$[3,1,2]$	$[3,2,1]$	$[1,3,2]$	$[1,2,3]$	$[2,3,1]$	$[2,1,3]$
$[3,2,1]$	$[3,2,1]$	$[3,1,2]$	$[2,3,1]$	$[2,1,3]$	$[1,3,2]$	$[1,2,3]$

Die Menge aller Bijektionen auf einer Menge bilden auch im Falle einer unendlichen Grundmenge eine Gruppe. Dies ist dann eine unendliche Gruppe. Wichtig ist die folgende Visualisierung einer Permutation π vom Grad n mittels eines gerichteten Graphen mit n Knoten. Man verbindet dazu den Knoten i mit dem Knoten $\pi(i)$ mit einem Pfeil von i nach $\pi(i)$.



gehört zur Permutation $[2,6,1,4,5,3]$. Man kann davon direkt die sog. Zyklen von π ablesen, dies sind die Kreise in der Visualisierung. Man schreibt dann

$$[2,6,1,4,5,3] = (1,2,6,3)(4)(5) = (1,2,6,3).$$

Zykel der Länge 1 sind sog. *Fixpunkte*. Die *Zykelschreibweise* ist eine weitere Notation für Permutationen. Man lässt im allgemeinen die Fixpunkte weg. Eine Zykel der Länge 2 heisst *Transposition*. Es werden nur zwei Zahlen aus den n Zahlen vertauscht. Eine Permutation heisst Zykel, wenn sie in der Zykeldarstellung nur einen Zykel der Länge > 1 hat. Zwei Zykel heissen *disjunkt*, wenn sie keine gemeinsamen Bestandteile (=bewegte Elemente) haben. Ein Zykel der Länge n wird auch als $n-$Zykel bezeichnet.

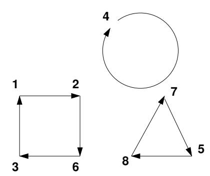
LEMMA 6.1.7. *Zykelschreibweise*

Jede Permutation lässt sich (bis auf Reihenfolge) eindeutig als Produkt von disjunkten Zykeln schreiben.

BEWEIS. Das ist das Ergebnis obiger Visualisierung. □

EXAMPLE 6.1.8. Zykelschreibweise

Die Permutation $[2,6,1,4,8,3,5,7]$ hat folgende Visualisierung:



was die Zykelschreibweise $(1, 2, 6, 3)(7, 5, 8)$ (oder aber auch z.B. $(3, 1, 2, 6)(8, 7, 5)(4)$) liefert und die eindeutige Produktzerlegung ist $[2, 6, 1, 4, 8, 3, 5, 7] = [2, 6, 1, 4, 5, 3, 7, 8]$ $[1, 2, 3, 4, 8, 6, 5, 7]$. In diesem Sinne kann die Zykelzerlegung auch als Produkt von Zykeln gelesen werden.

Der Vorteil der Zykelschreibweise ist die leichte Berechnung der inversen Permutation:

$$[2, 6, 1, 4, 8, 3, 5, 7]^{-1} = (1, 2, 6, 3)^{-1}(7, 5, 8)^{-1} = (3, 6, 2, 1)(8, 5, 7).$$

Man muss nur die einzelnen Zyklen umdrehen um die inverse Permutation zu bekommen. Eine wichtige Beobachtung ist, dass bereits Teilmengen von Permutationen der S_n eine Gruppe bilden können. Im Prinzip muss man nur ein paar Permutationen nehmen, alle Produkte und inversen Elemente dazunehmen und man erhält eine Gruppe. Dies ist eine sog. Untergruppe der S_n. Untergruppen der symmetrischen Gruppe werden auch Permutationsgruppe genannt.

EXAMPLE 6.1.9. Untergruppe in Zykelschreibweise

	id	(1342)	$(14)(23)$	(1243)	(23)	(14)	$(12)(34)$	$(13)(24)$
id	id	(1342)	$(14)(23)$	(1243)	(23)	(14)	$(12)(34)$	$(13)(24)$
(1342)	(1342)							
$(14)(23)$	$(14)(23)$							
(1243)	(1243)							
(23)	(23)							
(14)	(14)							
$(12)(34)$	$(12)(34)$							
$(13)(24)$	$(13)(24)$	(23)						

Dies ist eine nicht Abelsche Untergruppe der Ordnung 8 in der symmetrischen Gruppe S_4, die die Ordnung 24 hat. Es gibt aber auch Abelsche Untergruppen der symmetrischen Gruppe.

	id	(124)	(142)
id	id	(124)	(142)
(124)	(124)	(142)	id
(142)	(142)	id	(124)

Dies ist eine sog. zyklische Untergruppe, erzeugt von einem einzigen Element. Die Frage nach der Ordnung eines Elements g (siehe 2.4.19) ist die Frage nach der Anzahl der Elemente in der Gruppe $\{g, g^2, \ldots, g^k = id\}$. Dies ist immer eine kommutative Gruppe.

LEMMA 6.1.10. *Ordnung einer Permutation*

Die Ordnung einer Permutation π ist das kgV der Zykellängen in der Zykelschreibweise.

BEWEIS. klar wenn man die Potenzen in der Zykelschreibweise betrachtet. □

COROLLARY 6.1.11. *Ordnung von Zykeln*

Die Ordnung einer Transposition ist 2.

Die Ordnung eines $n-$Zykels ist n.

Ein weiteres wichtiges Konzept kann auch am Beispiel der Permutationen klar gemacht werden. Eine Teilmenge H einer Gruppe G heisst *Erzeuger* von G, wenn sich jedes Gruppenelement als endliches Produkt von Elementen aus H schreiben lässt.

LEMMA 6.1.12. *Erzeuger der S_n*

Die Menge der Transpositionen ist ein Erzeuger von S_n.

BEWEIS. Wir haben gesehen, dass die Zykel Erzeuger sind, das war gerade die Zykelschreibweise. Ein einzelner $k-$Zykel $(...,l,m,n)$ lässt sich als Produkt eines $(k-1)$ Zykels und einer Transposition schreiben:

$$(...,l,m,n) = (....,l,n)(l,m),$$

also kann ich jeden $k-$Zykel als Produkt von $k-1$ Transpositionen schreiben. □

Dies geht noch besser, betrachtet man nur *Elementartranspositionen*, dies sind Transpositionen $(i,i+1)$ benachbarter Zahlen, so kann man auch damit die symmetrische Gruppe erzeugen.

LEMMA 6.1.13. *Erzeuger der S_n*
Die Elementartranspositionen erzeugen die S_n.

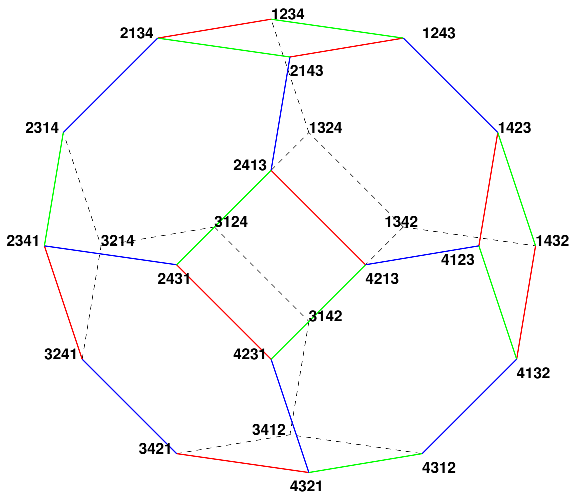
BEWEIS. Man hat folgende Gleichung für $i < j-1$:

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

□

Ein wichtiges Hilsmittel bei der Untersuchung von Fragen mit Gruppen und Erzeugern von Gruppen ist der *Cayleygraph*, Knoten sind die Gruppenelemente und für jeden Erzeuger x gibt es eine Kante markiert mit diesen Erzeuger (z.B. unterschiedliche Farben). Zwei Knoten g, h sind durch eine Kante mit Farbe x verbunden wenn $g = xh$.

EXAMPLE 6.1.14. S_4 erzeugt durch die 3 Elementartranspositionen. ungerichtet da die Transpositionen selbstinvers.



Warum man sich im Zusammenhang mit der Gruppentheorie soviel mit Permutationen beschäftigt wird klarer wenn man das folgende wichtige Ergebnis aus den Anfängen der Gruppentheorie von Cayley (1854) betrachtet.

THEOREM 6.1.15. *Satz von Cayley*
Jede endliche Gruppe ist als Permutationsgruppe darstellbar.

BEWEIS. Wir führen die Vorgehensweise zuerst anhand des Beispiels der Quaternionengruppe vor. Da jedes Gruppenelement aus G in einer Zeile zum Element g der Multiplikationstafel von G genau einmal vorkommt, definiert die Multiplikation mit g eine Permutation auf G. Wir bezeichnen diese Abbildung mit ϕ. Betrachtet man nochmal die Quaternionenmultiplikationstafel so erhält man z.B.

	1	-1	i	$-i$	j	$-j$	k	$-k$
1								
-1								
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$								
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$								
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$								

Damit wir die Multiplikation mit j zur Permutation $[5,6,8,7,2,1,3,4]$. Was jetzt noch zu prüfen ist, dass die Multiplikation bei den Permutationen im Prinzip die gleiche ist wie in der ursprünglichen Gruppe, d.h. $\phi(gh) = \phi(g)\phi(h)$. Wir müssen überprüfen, dass z.B.

$$ij = k$$

ist. In der Permutationsdarstellung erhält man:

$$[3,4,2,1,7,8,6,5][5,6,8,7,2,1,3,4] = [7,8,5,6,4,3,2,1]$$

wobei die rechte Seite wie gewünscht $\phi(k)$ ist. Auf diesen Rest des Beweises wird hier verzichtet. $\square$

Diese Eigenschaft, einer verträglichen Abbildung findet sich an vielen Stellen wieder. Mit einer solchen Abbildung kann man ein Problem in ein eventuell leichter zu untersuchendes Objekt transferieren.

Ein Abbildung $\phi : G \to H$ zwischen zwei Gruppen G und H heisst *(Gruppen-) Homomorphismus* wenn für alle g, h aus G gilt:

$$\phi(gh) = \phi(g)\phi(h).$$

Ist der Homomorphismus bijektiv spricht man von einem *Isomorphismus*. Obiger Satz von Cayley wird dann:

THEOREM 6.1.16. *Cayley*

Jede endliche Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe.

6.1.3. Matrix Gruppen. Man versucht gern Gruppen durch eine isomorphes Bild zu ersetzen, welches man gut im Griff hat. Im obigen Abschnitt waren dies Permutationen. Ein anderes Objekt welches man gut kennt sind die Matrizen. Dies ist sogar allgemeiner als die Permutatioen, denn die Permutationen sind bei den Matrizen durch die *Permutationsmatrizen* mit enthalten.

EXAMPLE 6.1.17. Quaternionengruppe

$ij = k$ wird zu den Permutationen

$$[3,4,2,1,7,8,6,5][5,6,8,7,2,1,3,4] = [7,8,5,6,4,3,2,1]$$

und als Matrizen

$$\begin{pmatrix} &&&1&&&& \\ &&1&&&&& \\ 1&&&&&&& \\ &1&&&&&& \\ &&&&&&&1 \\ &&&&&&1& \\ &&&&1&&& \\ &&&&&1&& \end{pmatrix} \begin{pmatrix} &&&&&1&& \\ &&&&1&&& \\ &&&&&&1& \\ &&&&&&&1 \\ 1&&&&&&& \\ &1&&&&&& \\ &&&1&&&& \\ &&1&&&&& \end{pmatrix} = \begin{pmatrix} &&&&&&&1 \\ &&&&&&1& \\ &&&&&1&& \\ &&&&1&&& \\ &&1&&&&& \\ &&&1&&&& \\ 1&&&&&&& \\ &1&&&&&& \end{pmatrix}.$$

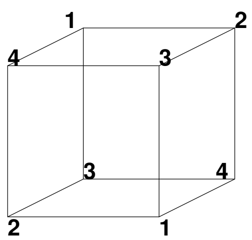
Nicht nur die Permutationsmatrizen bilden vers. Matrixgruppen. Die Menge aller invertierbaren Matrizen mit Einträgen aus $\mathbb{R}$ und Dimension n bildet eine Gruppe. Dies ist die volle *lineare Gruppe* und wird mit $GL(n, \mathbb{R})$ bezeichnet. Diese Gruppe ist nicht Abelsch. Es gibt weitere Untergruppen, so z.B. die *Diagonalmatrizen*, d.h. die Einträge auf der Diagonale sind nicht 0 alle nicht-Diagonalelemente sind 0.Eine weitere Untergruppe sind die oberen *Dreicksmatrizen* mit Einträgen ungleich 0 auf der Diagonale.

EXAMPLE 6.1.18. Quaternionengruppe
Betrachtet man die beiden 2×2 Matrizen über den komplexen Zahlen

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

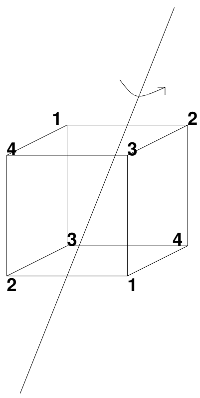
bekommt man einen Homomorphismus $Q_8 \to GL(2, \mathbb{C})$. Und schränkt man sich dann auf das Erzeugnis von X, Y ein bekommt man ein isomorphes Bild der Quaternionengruppe Q_8.

6.1.4. Symmetrie Gruppen. Ein weiteres typisches Auftreten von Gruppen ist als Symmetriegruppen von Objekten. Ein erstes Beispiel ist der Würfel als ein festes Objekt im dreidimensionalen Raum und man ist interessiert an Drehungen, die den Würfel wieder in sich selbst überführen. Dies ist eine Gruppe (assoziativ da Hintereinanderausführung von Abbildungen, inverse Drehung, Identität) Wir wollen die entsprechenden Drehungen als Permutationen bekommen. Drehungen führen Diagonalen in Diagonalen über, daher markieren wir die beiden Ecken zu einer Diagonalen mit der gleichen Nummer.



Nun bekommt man jede Permutation vom Grad vier, was zeigt dass die Rotationsgruppe die symmetrische Gruppe S_4 ist. Um dies zu zeigen genügt es die 3 bekannten Erzeuger wieder zu finden:

z.B. $(1, 2)$ ist die Drehung um 180 Grad um eine Achse durch die gegenüberliegenden Kanten zwischen 1 und 2.



Insgesamt sind es 24 Rotationen

- 3 Rotationen $(90°, 180°, 270°)$ an der Achse durch gegenüberliegende Flächen (3 Paar) = 9 Rotationen
- 2 Rotationen $(120°, 240°)$ an der Achse durch gegenüberliegende Ecken (4 Paar) = 8 Rotationen
- 1 Rotation $(180°)$ entlang der Achse durch die Mitte gegenüberliegender Kanten (6 Paar) = 6 Rotationen
- Identität