Arithmetic of Hyperelliptic Curves

Summer Semester 2014

University of Bayreuth

Michael Stoll

Contents

Print Version of August 1, 2014, 20:12.

1. Introduction

The main topic of this lecture course will be various methods that (in favorable cases) will allow us to determine the set of *rational points* on a *hyperelliptic curve*. In very down-to-earth terms, what we would like to determine is the set of solutions in rational numbers x and y of an equation of the form

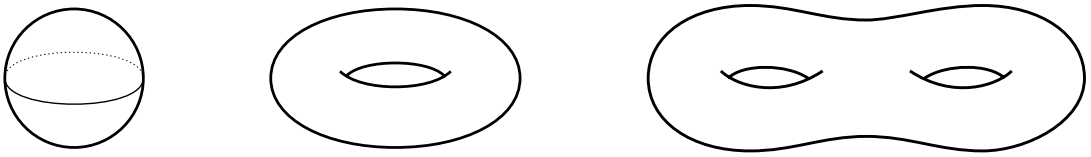
$$y^2 = f(x)\,, \tag{1.1}$$

where $f \in \mathbb{Z}[x]$ is a polynomial with integral coefficients and without multiple roots and such that $\deg f \geq 5$. (If f has multiple roots, then we can write $f = f_1 h^2$ with polynomials $f_1, h \in \mathbb{Z}[x]$ such that h is not constant; then solutions of $y^2 = f(x)$ essentially correspond to solutions of the simpler (in terms of $\deg f$) equation $y^2 = f_1(x)$: we get a solution of the former in the form $(\xi, h(\xi)\eta)$ when (ξ, η) is a solution of the latter, and all solutions (ξ, η) of the former with $h(\xi) \neq 0$ have this form.)

We can think of equation (1.1) as defining an affine plane algebraic curve C_{aff}. Such a curve is said to be *hyperelliptic*. Then the solutions in rational numbers correspond to the rational points (i.e., points with rational coordinates) of this curve C_{aff}. The condition that f has no multiple roots translates into the requirement that the curve C_{aff} be *smooth*: It does not have any singular points, which are points where both partial derivatives of the defining polynomial $y^2 - f(x)$ vanish.

From a geometric point of view, it is more natural to consider projective curves (rather than affine ones). We obtain a smooth projective curve C by adding suitable *points at infinity*. If $\deg f$ is odd, there is just one such point, and it is always a rational point. If $\deg f$ is even, there are two such points, which correspond to the two square roots of the leading coefficient of f. These points are rational if and only if this leading coefficient is a square, so that its square roots are rational numbers. We will give a more symmetric description of C in the next section. The set of rational points on C is denoted $C(\mathbb{Q})$.

The most important invariant associated to a smooth (absolutely irreducible) projective curve is its *genus*, which we will always denote g. The genus is a natural number. For hyperelliptic curves, it turns out to be g if $\deg f = 2g + 1$ or $\deg f = 2g + 2$. Note that our definition above implies that $g \geq 2$ for the curves we consider. In general, one can define the genus by considering the set of complex points of the curve. It forms a compact Riemann surface, which is an orientable surface (2-dimensional manifold) and therefore 'looks like' (meaning: is homeomorphic to) a sphere with a certain number of handles attached. This number of handles is the genus g. For example, the sphere itself has genus 0, since no handle needs to be attached, and a torus has genus 1.



$g = 0$ $g = 1$ $g = 2$

It has been an important insight that this *topological* invariant also governs the nature of the set of rational points, which is an *arithmetic* invariant of the curve:

THM Structure of $C(\mathbb{Q})$

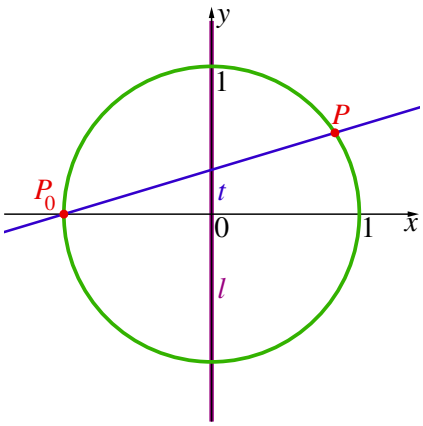
1.1. **Theorem.** *Let C be a smooth projective and absolutely irreducible curve of genus g defined over $\mathbb{Q}$.*

(1) If $g = 0$, then either $C(\mathbb{Q}) = \emptyset$ or C is isomorphic over $\mathbb{Q}$ to the projective line $\mathbb{P}^1$. This isomorphism induces a bijection $\mathbb{Q} \cup \{\infty\} = \mathbb{P}^1(\mathbb{Q}) \to C(\mathbb{Q})$.

(2) If $g = 1$, then either $C(\mathbb{Q}) = \emptyset$ or else, fixing a point $P_0 \in C(\mathbb{Q})$, the set $C(\mathbb{Q})$ has the structure of a finitely generated abelian group with zero P_0. In this case, (C, P_0) is an elliptic curve *over $\mathbb{Q}$.*

(3) If $g \geq 2$, then $C(\mathbb{Q})$ is finite.

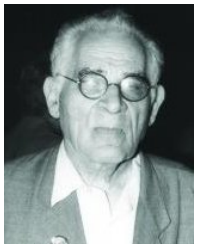
The first part of this is quite classical and can be traced back to Diophantus (who (probably) lived in the third century AD). Here is a sketch: First one can show that any curve of genus 0 is isomorphic to a conic section (a projective plane curve of degree 2). If $C(\mathbb{Q}) = \emptyset$, we have nothing to show. So let $P_0 \in C(\mathbb{Q})$ and let l be a rational line not passing through P_0. Then projecting away from P_0 gives the isomorphism $C \to l \cong \mathbb{P}^1$.



Projecting the unit circle from the point $P_0 = (-1, 0)$ to the line l (the y-axis) leads to the parametrization

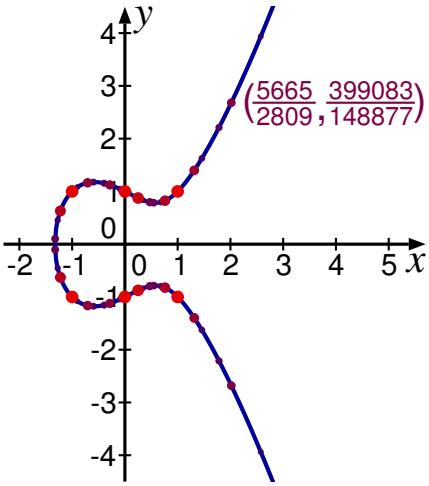
$$t \longmapsto \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$$

of the rational points on the unit circle.



L.J. Mordell
1888–1972

The second part was proved by Mordell in 1922[1] (and later generalized by Weil; we will come back to that).



The group of rational points on this elliptic curve is isomorphic to $\mathbb{Z}$; it is generated by the point $(1, 1)$ (and the zero of the group is the point at infinity).

The curve is given by the equation

$$y^2 = x^3 - x + 1\,.$$

The rational points are marked by dots whose color (from red to blue) and size (from large to small) change with increasing size of the numerator and denominator of the coordinates.

G. Faltings
* 1954

In the same paper that contains his proof, Mordell conjectured the third statement in the theorem above. This was finally proved by Faltings about sixty years later[2],

[1] Louis J. Mordell: *On the rational solutions of the indeterminate equation of the third and fourth degrees*, Proc. Cambridge Philos. Soc. **21**, 179–192 (1922).

[2] Gerd Faltings: *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Mathematicae **73**:3, 349–366 (1983).

who was awarded the Fields Medal for this result in 1986 (and remains the only German to have received this prestigious prize).

Part (3) of the theorem tells us that it is at least possible in principle to give a complete description of $C(\mathbb{Q})$: we simply list the finitely many rational points. This then raises the question whether it is always possible to provably do so. Let us assume that C is a plane curve, with affine part C_{aff}. There are only finitely many points at infinity (i.e., points in $C \setminus C_{\text{aff}}$), and it is easy to check which of them are rational. So we can reduce the problem to that of determining $C_{\text{aff}}(\mathbb{Q})$. Now the set $\mathbb{Q} \times \mathbb{Q}$ of rational points in the affine plane is countable, so we can (in principle, at least) just enumerate all these points one by one and check for each point if it is on the curve. Since there are only finitely many rational points on C, we will eventually find them all. (In practice, this procedure is obviously very inefficient. It is much better to (say) enumerate the x-coordinates and check if the resulting equation for y has rational solutions.) In fact, one should expect these points to be relatively 'small' (in terms of a suitable notion of size, and relative to the size of the coefficients of the equation defining the curve), so that it is usually no problem to *find* all the rational points. The difficult part is to *prove that the list is complete*. We will discuss several approaches that allow us to do this in favorable circumstances. However, so far it is an open question whether this is always possible, i.e., whether there is an algorithm that would construct such a proof whenever the list is indeed complete.


L. Caporaso

Another question that arises is whether there might be a bound for the finite number of rational points. Since it is easy to construct curves of increasing genus with more and more rational points — for example, the curve of genus g given by

$$y^2 = x(x-1)(x-2)\cdots(x-2g)(x-2g-1)$$

has at least the $2g+2$ rational points $(0,0)$, $(1,0)$, $\ldots$, $(2g+1,0)$ — this question only makes sense for curves of fixed genus. In this setting, the question is open. Caporaso, Harris and Mazur[3] have shown that the *Bombieri-Lang Conjecture* on rational points on varieties of general type would imply that such a bound only depending on g exists. The latter conjecture is wide open in general (and not even believed to hold by some people in the field). For curves of genus 2 (which are always hyperelliptic), the current record is held by a curve that has at least 642 rational points. It is given by the following equation:


J. Harris
* 1951

$$\begin{aligned} y^2 = {} & 82342800x^6 - 470135160x^5 + 52485681x^4 \\ & + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600 \end{aligned}$$


B. Mazur
* 1937

[3] Lucia Caporaso, Joe Harris, Barry Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10**:1, 1–35 (1997).

2. Hyperelliptic Curves: Basics

Hyperelliptic curves are special algebraic curves. For reasons of time, we will avoid going into the general theory of algebraic curves to the extent possible, which means that part of what we do here will be somewhat ad hoc.

We will essentially only consider projective curves. We begin by introducing a suitable ambient space.

DEF weighted projective plane

2.1. **Definition.** Fix $g \in \mathbb{Z}_{\geq 0}$. The *weighted projective plane* $\mathbb{P}^2_g = \mathbb{P}^2_{(1,g+1,1)}$ is the geometric object whose points over a field k are the equivalence classes of triples $(\xi, \eta, \zeta) \in k^3 \setminus \{(0,0,0)\}$, where triples (ξ, η, ζ) and (ξ', η', ζ') are equivalent if there is some $\lambda \in k^\times$ such that $(\xi', \eta', \zeta') = (\lambda\xi, \lambda^{g+1}\eta, \lambda\zeta)$. We write $(\xi : \eta : \zeta)$ for the corresponding point. The set of k-rational points of $\mathbb{P}^2_g$ is written $\mathbb{P}^2_g(k)$.

Its *coordinate ring* over k is the ring $k[x, y, z]$ with the grading that assigns to x and z degree 1 and to y degree $g + 1$. A polynomial $f \in k[x, y, z]$ is *homogeneous* of total degree d if all its terms have total degree d, so that it has the form

$$f = \sum_{i_1, i_2, i_3 \colon i_1 + (g+1)i_2 + i_3 = d} a_{i_1,i_2,i_3} x^{i_1} y^{i_2} z^{i_3}$$

with coefficients $a_{i_1,i_2,i_3} \in k$. ♢

For $g = 0$ we obtain the standard projective plane and the standard notion of 'homogeneous' for polynomials.

'$\mathbb{P}^2_g$' is ad hoc notation used in these notes; the general notation $\mathbb{P}^2_{(d_1,d_2,d_3)}$ denotes a weighted projective plane with coordinates of weights d_1, d_2 and d_3. For our purposes, the special case $(d_1, d_2, d_3) = (1, g + 1, 1)$ is sufficient.

In a similar way as for the standard projective plane, we see that there is a natural bijection between the points $(\xi : \eta : \zeta) \in \mathbb{P}^2_g(k)$ with $\zeta \neq 0$ (this is a well-defined condition, since it does not depend on the scaling) and the points of the affine plane $\mathbb{A}^2(k)$ (which are just pairs of elements of k). This bijection is given by

$$(\xi : \eta : \zeta) \longmapsto \left(\frac{\xi}{\zeta}, \frac{\eta}{\zeta^{g+1}}\right) \qquad \text{and} \qquad (\xi, \eta) \longmapsto (\xi : \eta : 1)\,.$$

DEF affine patches of $\mathbb{P}^2_g$

In the same way, we obtain a bijection between the points with $\xi \neq 0$ and $\mathbb{A}^2(k)$. We will call these two subsets of $\mathbb{P}^2_g$ the two *standard affine patches* of $\mathbb{P}^2_g$. Their union covers all of $\mathbb{P}^2_g$ except for the point $(0 : 1 : 0)$, which we will never need to consider. (In fact, for $g \geq 1$, this point is a singular point on $\mathbb{P}^2_g$ and is therefore better avoided in any case.)

DEF hyperelliptic curve

2.2. **Definition.** Fix $g \geq 2$. A *hyperelliptic curve of genus* g over a field k not of characteristic 2 is the subvariety of $\mathbb{P}^2_g$ defined by an equation of the form $y^2 = F(x, z)$, where $F \in k[x, z]$ is homogeneous (in the usual sense) of degree $2g+2$ and is squarefree (i.e., not divisible by the square of a homogeneous polynomial of positive degree).

If C is the curve, then its set of *k-rational points* is

$$C(k) = \{(\xi : \eta : \zeta) \in \mathbb{P}^2_g(k) \mid \eta^2 = F(\xi, \zeta)\}\,.$$ ♢

When $k = \mathbb{Q}$, we simply say 'rational point' instead of '$\mathbb{Q}$-rational point'.

One can also consider hyperelliptic curves over fields of characteristic 2, but then one has to use more general equations of the form

$$y^2 + H(x,z)y = F(x,z)\,,$$

where H and F are homogeneous of degrees $g+1$ and $2g+2$, respectively, and satisfy a suitable condition corresponding to the squarefreeness of F above.

If the characteristic is not 2, then such an equation can be transformed into the standard form $y^2 = 4F(x,z)+H(x,z)^2$ by completing the square, so in this case we do not obtain a richer class of curves.

Note that the definition of $C(k)$ makes sense: if (ξ',η',ζ') is another representative of the point $(\xi:\eta:\zeta)$, then $(\xi',\eta',\zeta') = (\lambda\xi, \lambda^{g+1}\eta, \lambda\zeta)$ for some $\lambda \in k^\times$, and

$$\eta'^2 - F(\xi',\zeta') = (\lambda^{g+1}\eta)^2 - F(\lambda\xi,\lambda\zeta) = \lambda^{2g+2}\eta^2 - \lambda^{2g+2}F(\xi,\zeta) = \lambda^{2g+2}\big(\eta^2 - F(\xi,\zeta)\big)\,,$$

so $\eta^2 = F(\xi,\zeta) \iff \eta'^2 = F(\xi',\zeta')$. In the terminology introduced in Definition 2.1, the defining polynomial $y^2 - F(x,z)$ is homogeneous of degree $2g+2$ in the coordinate ring of $\mathbb{P}^2_g$.

The intersections of C with the affine patches of $\mathbb{P}^2_g$ are the *standard affine patches* of C. They are affine plane curves given by the equations

$$y^2 = F(x,1) \qquad \text{and} \qquad y^2 = F(1,z)\,,$$

respectively. We will use the notation $f(x) = F(x,1)$. To keep notation simple, we will usually just write '$C\colon y^2 = f(x)$', but will always consider C as a projective curve as in Definition 2.2. Note that we must have $\deg f = 2g+1$ or $\deg f = 2g+2$, so that we can reconstruct $F(x,z)$ from $f(x)$.

Let

$$F(x,z) = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1}z + \ldots + f_1 xz^{2g+1} + f_0 z^{2g+2}$$

and let C be the hyperelliptic curve given by $y^2 = F(x,z)$. Then the points $(\xi:\eta:\zeta) \in C(k)$ such that $\zeta \neq 0$ have the form $(\xi:\eta:1)$ where $\eta^2 = f(\xi)$: they correspond to the solutions in k of the equation $y^2 = f(x)$, or equivalently, to the k-rational points on the (first standard) affine patch of C. We will frequently just write (ξ,η) for such an affine point. The remaining points on C are called *points at infinity*. We obtain them by setting $z = 0$ and $x = 1$ in the defining equation, which then reduces to $y^2 = f_{2g+2}$. So if $f_{2g+2} = 0$ (which means that $\deg f = 2g+1$), then there is one such point, namely $(1:0:0)$. We will frequently denote this point simply by ∞. If $f_{2g+2} = s^2$ is a nonzero square in k, then there are two k-rational points at infinity, namely $(1:s:0)$ and $(1:-s:0)$ (denoted ∞_s and ∞_{-s}). Otherwise there are no k-rational points at infinity (but there will be two such points over the larger field $k(\sqrt{f_{2g+2}})$). Note that the 'bad' point $(0:1:0)$ is never a point on a hyperelliptic curve.

DEF points at infinity

2.3. **Example.** Let $k = \mathbb{Q}$ and $C\colon y^2 = x^5+1$. Since the degree of the polynomial on the right is 5, we have $g = 2$ and the projective form of the equation is $y^2 = x^5z + z^6$. We see that there is one point $\infty = (1:0:0)$ at infinity. There are also the affine points $(0,1)$, $(0,-1)$ and $(-1,0)$. One can in fact show that

$$C(\mathbb{Q}) = \{\infty, (0,1), (0,-1), (-1,0)\}\,,$$

i.e., these are all the rational points on this curve! ♣

EXAMPLE

2.4. **Definition.** Every hyperelliptic curve C has a nontrivial automorphism: the *hyperelliptic involution* $\iota = \iota_C$. If C is given by the usual equation $y^2 = F(x,z)$, then ι maps the point $(\xi : \eta : \zeta)$ to $(\xi : -\eta : \zeta)$. The fixed points of ι are the $2g+2$ points $(\xi : 0 : \zeta)$, where $(\xi : \zeta) \in \mathbb{P}^1$ is a root of the homogeneous polynomial F.

DEF hyperelliptic involution

We also have the *hyperelliptic quotient map* $\pi = \pi_C \colon C \to \mathbb{P}^1$, which sends $(\xi : \eta : \zeta)$ to $(\xi : \zeta)$; since $(0 : 1 : 0) \notin C$, this is a well-defined morphism. Then ι is the nontrivial automorphism of the double cover π, and the fixed points of ι are the *ramification points* of π. These points are also frequently called *Weierstrass points*. (There is a notion of 'Weierstrass point' for general curves; in the hyperelliptic case they coincide with the ramification points.) ♢

DEF hyperelliptic quotient map

Restricting the elements of the coordinate ring of $\mathbb{P}^2_g$ to C, we obtain the coordinate ring of C:

2.5. **Definition.** Let $C \colon y^2 = F(x,z)$ be a hyperelliptic curve of genus g over k. The *coordinate ring* of C over k is the quotient ring $k[C] := k[x,y,z]/\langle y^2 - F(x,z)\rangle$. Note that $y^2 - F(x,z)$ is irreducible and homogeneous, so $k[C]$ is an integral domain, which inherits a grading from $k[\mathbb{P}^2_g] = k[x,y,z]$.

DEF coordinate ring of C

The subfield $k(C)$ of the field of fractions of $k[C]$ consisting of elements of degree zero is the *function field* of C over k. Its elements are the *rational functions* on C over k. If $P = (\xi : \eta : \zeta) \in C(k)$ and $\phi \in k(C)$ such that ϕ is represented by a quotient h_1/h_2 (of elements of $k[C]$ of the same degree) such that $h_2(\xi,\eta,\zeta) \neq 0$, then we can define the *value* of ϕ at P by $\phi(P) = h_1(\xi,\eta,\zeta)/h_2(\xi,\eta,\zeta)$; ϕ is then said to be *regular* at P. ♢

DEF function field of C

DEF rational function

One checks easily that $\phi(P)$ does not depend on the coordinates chosen for P or on the choice of representative of ϕ (as long as the denominator does not vanish at P).

The subring of $k(C)$ consisting of functions that are everywhere (i.e., at all points in $C(\bar{k})$, where $\bar{k}$ is an algebraic closure of k) regular except possibly at the points at infinity is isomorphic to the ring $k[C_{\mathrm{aff}}] := k[x,y]/\langle y^2 - f(x)\rangle$ (Exercise). It follows that the function field $k(C)$ is isomorphic to the field of fractions of $k[C_{\mathrm{aff}}]$, so that we will usually write down functions in this affine form. Simple examples of functions on C are then given by $1, x, x^2, \ldots, y, xy, \ldots$; they are all regular outside the points at infinity.

2.6. **Definition.** Let C be a curve over k and let $P \in C(k)$. Then the ring

$$\mathcal{O}_{C,P} = \{\phi \in k(C) : \phi \text{ is regular at } P\}$$

DEF local ring at a point

is called the *local ring* of C at the point P. We write

$$\mathfrak{m}_P = \{\phi \in \mathcal{O}_{C,P} : \phi(P) = 0\}$$

for its unique maximal ideal. ♢

Recall that a ring R is said to be *local* if it has a unique maximal ideal. This is equivalent to the statement that the complement of the unit group $R^\times$ is an ideal M (which is then the unique maximal ideal): any proper ideal I of R must satisfy $I \cap R^\times = \emptyset$, so $I \subset R \setminus R^\times = M$. On the other hand, assume that M is the unique maximal ideal. Take any $r \in R \setminus R^\times$. Then r is contained in a maximal ideal, so $r \in M$, showing that $R \setminus R^\times \subset M$. The reverse inclusion is obvious.

In our case, we see that every $\phi \in \mathcal{O}_{C,P} \setminus \mathfrak{m}_P$ is regular at P with $\phi(P) \neq 0$, which implies that ϕ^{-1} is also regular at P, so $\phi^{-1} \in \mathcal{O}_{C,P}$, whence $\phi \in \mathcal{O}^\times_{C,P}$.

2.7. **Definition.** Let R be a domain (i.e., a commutative ring without zero divisors). A *discrete valuation* on R is a surjective map $v\colon R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ with the following properties, which hold for all $r, r' \in R$:

DEF DVR

(1) $v(r) = \infty \iff r = 0$.
(2) $v(rr') = v(r) + v(r')$.
(3) $v(r + r') \geq \min\{v(r), v(r')\}$.

A domain R together with a discrete valuation v on it such that every $r \in R$ with $v(r) = 0$ is in $R^\times$ and such that the ideal $\{r \in R : v(r) > 0\}$ is principal is a *discrete valuation ring* or short *DVR*. ♢

2.8. **Lemma.** *Let R be a DVR with discrete valuation v; we can assume without loss of generality that $v(R \setminus \{0\}) = \mathbb{Z}_{\geq 0}$. Then R is a local ring with unique maximal ideal $M = \{r \in R : v(r) > 0\}$ and unit group $R^\times = \{r \in R : v(r) = 0\}$. Also, R is a principal ideal domain (PID) with only one prime (up to associates): let $t \in R$ be an element such that $v(t) = 1$ (such a t is called a* uniformizer *of R); then every $r \in R \setminus \{0\}$ can be written uniquely in the form $r = ut^n$ with a unit $u \in R^\times$ and $n \in \mathbb{Z}_{\geq 0}$.*

LEMMA Properties of DVRs

DEF uniformizer

Conversely, every PID with only one prime ideal is a DVR.

Proof. Exercise. ❑

If R is a DVR with field of fractions K, then v extends to a valuation on K in a unique way by setting $v(r/s) = v(r) - v(s)$. Then the extended v is a map $v\colon K \to \mathbb{Z} \cup \{\infty\}$ satisfying the conditions in Definition 2.7. We call (K, v) a *discretely valued field*.

DEF discretely valued field

2.9. **Example.** Let p be a prime number and let

EXAMPLE DVR $\mathbb{Z}_{(p)}$

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}.$$

Then $\mathbb{Z}_{(p)}$ is a DVR with the discrete valuation given by the p-adic valuation v_p ($v_p(a/b) = v_p(a) = \max\{n : p^n \mid a\}$). Its field of fraction is $\mathbb{Q}$, which becomes a discretely valued field with the valuation v_p. ♣

2.10. **Example.** Let k be any field; we denote by $k[\![t]\!]$ the *ring of formal power series* over k. Its elements are power series $\sum_{n\geq 0} a_n t^n$ with $a_n \in k$. This ring is a DVR with valuation

EXAMPLE DVR $k[\![t]\!]$

$$v\Big(\sum_{n\geq 0} a_n t^n\Big) = \min\{n \geq 0 : a_n \neq 0\}. \qquad ♣$$

2.11. **Lemma.** *Let $C\colon y^2 = F(x,z)$ be a hyperelliptic curve over k and let $P = (\xi:\eta:\zeta) \in C(k)$. Then the local ring $\mathcal{O}_{C,P}$ is a DVR with field of fractions $k(C)$.*

LEMMA local ring at P is DVR

Proof. We can assume that $\zeta = 1$, so that $P = (\xi,\eta)$ is a point on C_{aff}. (The case $\xi = 1$ can be dealt with analogously using the other affine chart.)

First assume that $\eta \neq 0$. I claim that there is a k-linear ring homomorphism $k[C_{\text{aff}}] \to k[\![t]\!]$ that sends x to $\xi + t$ and y to a power series with constant term η. For this we only have to check that $f(\xi+t) \in k[\![t]\!]$ has a square root in $k[\![t]\!]$ of the form $\tilde{y} = \eta + a_1 t + a_2 t^2 + \ldots$. This follows from $f(\xi+t) = \eta^2 + b_1 t + b_2 t^2 + \ldots$ and $\eta \neq 0$ (writing

$$(\eta + a_1 t + a_2 t^2 + \ldots)^2 = \eta^2 + b_1 t + b_2 t^2 + \ldots ,$$

expanding the left hand side and comparing coefficients, we obtain successive linear equations of the form $2\eta a_n = \ldots$ for the coefficients of $\tilde{y}$). It follows that the homomorphism $k[x,y] \to k[\![t]\!]$ given by $x \mapsto \xi + t$ and $y \mapsto \tilde{y}$ has kernel containing $y^2 - f(x)$, so it induces a k-linear ring homomorphism $\alpha\colon k[C_{\text{aff}}] \to k[\![t]\!]$. It has the property that the constant term of $\alpha(\phi)$ is $\phi(P)$. Since the units of $k[\![t]\!]$ are exactly the power series with non-vanishing constant term, this implies that α extends to a k-linear ring homomorphism $\alpha\colon \mathcal{O}_{C,P} \to k[\![t]\!]$. We define the valuation v_P on $\mathcal{O}_{C,P}$ by $v_P = v \circ \alpha$, where v is the valuation on $k[\![t]\!]$. Then if $\phi \in \mathcal{O}_{C,P}$ has $v_P(\phi) = 0$, we have $\phi(P) \neq 0$, so $\phi^{-1} \in \mathcal{O}_{C,P}$. We still have to verify that the maximal ideal $\mathfrak{m}_P$ is principal. We show that $\mathfrak{m}_P$ is generated by $x - \xi$. Note that the equation $y^2 = f(x)$ can be written

$$(y-\eta)(y+\eta) = f(x) - \eta^2 = (x-\xi) f_1(x)$$

with a polynomial f_1 and that $(y+\eta)(P) = 2\eta \neq 0$, so that $y + \eta \in \mathcal{O}_{C,P}^\times$. This shows that $y - \eta \in \mathcal{O}_{C,P} \cdot (x-\xi)$. More generally, we can use this to show that if $h \in k[x,y]$ with $h(P) = 0$, then $h(x,y) \in \mathcal{O}_{C,P} \cdot (x-\xi)$. This in turn implies that every rational function ϕ has a representative $h_1(x,y)/h_2(x,y)$ such that $h_1(P) \neq 0$ or $h_2(P) \neq 0$ (or both). If $\phi \in \mathfrak{m}_P$, then we must have $h_1(P) = 0$ and $h_2(P) \neq 0$, and we can deduce that $\phi \in \mathcal{O}_{C,P} \cdot (x-\xi)$ as desired. This finally shows that $\mathcal{O}_{C,P}$ is a DVR.

When $\eta = 0$, we have $f(\xi + a) = f'(\xi)a + \ldots$ with $f'(\xi) \neq 0$. We can then in a similar way as above solve

$$t^2 = f(\xi + a_2 t^2 + a_4 t^4 + \ldots)$$

to obtain a power series $\tilde{x} = \xi + a_2 t^2 + a_4 t^4 + \ldots \in k[\![t]\!]$ such that $t^2 = f(\tilde{x})$. We then obtain a k-linear ring homomorphism $\alpha\colon \mathcal{O}_{C,P} \to k[\![t]\!]$ that sends x to $\tilde{x}$ and y to t and conclude in a similar way as before (this time showing that $\mathfrak{m}_P$ is generated by y, using that $(x-\xi)f_1(x) = y^2$ with $f_1(x) \in \mathcal{O}_{C,P}^\times$).

It is clear that the field of fractions of $\mathcal{O}_{C,P}$ is contained in $k(C)$. The reverse inclusion follows, since $\mathcal{O}_{C,P}$ contains field generators (x and y if $\zeta = 1$) of $k(C)$ over k. ❑

2.12. **Definition.** The valuation v_P and its extension to $k(C)$ (again denoted v_P) is the *P-adic valuation* of $k(C)$. Any element $t \in k(C)$ such that $v_P(t) = 1$ is called a *uniformizer* at P. ♢

DEF P-adic valuation

uniformizer at P

The standard choice of uniformizer at $P = (\xi,\eta)$ is that made in the proof above: if $\eta \neq 0$, we take $t = x - \xi$, and if $\eta = 0$, we take $t = y$. In terms of the affine

coordinate functions x and y, a uniformizer at a point $(1 : s : 0)$ at infinity is given by $t = 1/x$ if $s \neq 0$ and $t = y/x^{g+1}$ when $s = 0$.

2.13. **Remark.** The results above generalize to arbitrary curves C: if $P \in C(k)$ is a smooth point, then the local ring $\mathcal{O}_{C,P}$ is a DVR. ♠ **REMARK**

3. Digression: p-adic numbers

Before we continue to introduce notions related to hyperelliptic curves, I would like to introduce the ring of p-adic integers and the field of p-adic numbers. Let p be a prime number. We had seen in Example 2.9 that $\mathbb{Q}$ is a discretely valued field with respect to the p-adic valuation v_p. Now any valuation induces an absolute value, a notion we define next.

DEF absolute value

3.1. **Definition.** Let k be a field. An *absolute value* on k is a map $k \to \mathbb{R}_{\geq 0}$, usually written $x \mapsto |x|$ or similar, with the following properties (for all $a, b \in k$):

(1) $|a| = 0 \iff a = 0$.

(2) $|ab| = |a| \cdot |b|$.

(3) $|a + b| \leq |a| + |b|$.

The absolute value is said to be *non-archimedean* if we have the stronger property that

(3′) $|a + b| \leq \max\{|a|, |b|\}$.

Otherwise it is *archimedean*.

Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on k are said to be *equivalent*, if there is some $\alpha \in \mathbb{R}_{>0}$ such that $|a|_1 = |a|_2^\alpha$ for all $a \in k$. ♢

EXAMPLES absolute values

3.2. **Examples.** The standard absolute value is an archimedean absolute value on $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

If $v\colon k \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation, then we obtain a non-archimedean absolute value $|\cdot|_v$ by setting

$$|a|_v = \begin{cases} 0 & \text{if } a = 0, \\ \alpha^{v(a)} & \text{if } a \neq 0 \end{cases}$$

for some $0 < \alpha < 1$. The equivalence class of $|\cdot|_v$ does not depend on the choice of α. ♣

DEF p-adic absolute value

3.3. **Definition.** The *p-adic absolute value* $|\cdot|_p$ on $\mathbb{Q}$ is defined by

$$|a|_p = \begin{cases} 0 & \text{if } a = 0, \\ p^{-v_p(a)} & \text{if } a \neq 0. \end{cases}$$

We also write $|a|_\infty$ for the standard absolute value $|a|$. ♢

Taking $\alpha = 1/p$ is the usual choice here. It has the convenient property that the following holds.

3.4. **Lemma.** *Let $a \in \mathbb{Q}^\times$. Then*

$$|a|_\infty \cdot \prod_p |a|_p = 1\,,$$

where the product runs over all prime numbers.

LEMMA
Product formula

Proof. The left hand side is multiplicative, so it suffices to check this for $a = -1$ and $a = q$ a prime number. But any absolute value of -1 is 1, and for $a = q$ we have $|a|_\infty = q$, $|a|_q = 1/q$ and all other $|a|_p = 1$. (In particular, all but finitely many factors in the product are 1, so that the formally infinite product makes sense.) ❑

One possible way of constructing the field $\mathbb{R}$ of real numbers starting from the rational numbers is to define $\mathbb{R}$ to be the quotient of the ring of Cauchy sequences over $\mathbb{Q}$ modulo the (maximal) ideal of sequences with limit zero. This construction works with *any* absolute value on any field k and produces the *completion* of k with respect to the absolute value: the new field is a complete metric space (with respect to the metric $d(a, b) = |a-b|$) that contains k as a dense subset. We apply this to $\mathbb{Q}$ and the p-adic absolute value.

3.5. **Definition.** The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is the *field $\mathbb{Q}_p$ of p-adic numbers*. The closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ is the *ring $\mathbb{Z}_p$ of p-adic integers*. ♢

DEF
field of p-adic numbers
ring of p-adic integers

The p-adic valuation v_p and absolute value $|\cdot|_p$ extend to $\mathbb{Q}_p$; the absolute value defines the metric and therefore the topology on $\mathbb{Q}_p$.

In these terms, $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\} = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$ is the 'closed unit ball' in $\mathbb{Q}_p$.

3.6. **Lemma.** *$\mathbb{Z}_p$ is compact in the p-adic topology. In particular, $\mathbb{Q}_p$ is a locally compact field.*

LEMMA
$\mathbb{Z}_p$ is compact

Local compactness is a property that $\mathbb{Q}_p$ shares with $\mathbb{R}$ and $\mathbb{C}$.

Proof. $\mathbb{Z}_p$ is a closed subset of a complete metric space with the property that it can be covered by finitely many open ε-balls for every $\varepsilon > 0$. This implies compactness. We check the second condition: if $\varepsilon > p^{-n}$, then $\mathbb{Z}_p$ is the union of the open balls with radius ε centered at the points $0, 1, 2, \ldots, p^n - 1$.

Now note that $\mathbb{Z}_p$ is also an open subset of $\mathbb{Q}_p$ (it is the open ball of radius $1 + \varepsilon$ for any $0 < \varepsilon < p - 1$), so it is a neighborhood of 0. It follows that $a + \mathbb{Z}_p$ is a compact neighborhood of a in $\mathbb{Q}_p$, for any $a \in \mathbb{Q}_p$. ❑

$\mathbb{Z}_p$ is a DVR: v_p is a discrete valuation on $\mathbb{Z}_p$, every element of valuation 0 is a unit, and its maximal ideal is $p\mathbb{Z}_p$, hence principal. The residue field is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. We usually write $a \mapsto \bar{a}$ for the reduction homomorphism $\mathbb{Z}_p \to \mathbb{F}_p$. Every element of $\mathbb{Z}_p$ can be written uniquely as a 'power series' in p with coefficients taken out of a complete set of representatives of the residue classes mod p (Exercise). More generally, every power series with coefficients in $\mathbb{Z}_p$ converges on the 'open unit ball' $p\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p < 1\}$. This follows from the following simple convergence criterion for series.

3.7. **Lemma.** *Let $(a_n)_{n\geq 0}$ be a sequence of elements of $\mathbb{Q}_p$. Then the series $\sum_{n=0}^{\infty} a_n$ converges in $\mathbb{Q}_p$ if and only if $a_n \to 0$ as $n \to \infty$.*

LEMMA Convergence of series

This property makes p-adic analysis much nicer than the usual variety over $\mathbb{R}$!

Proof. The terms of any convergent series have to tend to zero. The interesting direction is the other one. So assume that $a_n \to 0$ and write s_n for the partial sum $\sum_{m=0}^{n} a_m$. For any $\varepsilon > 0$, there is some $N \geq 0$ such that $|a_n|_p < \varepsilon$ for all $n \geq N$. By the 'ultrametric' triangle inequality, this implies that

$$|s_{n+m} - s_n|_p = \left| \sum_{k=n+1}^{n+m} a_k \right|_p \leq \max\bigl\{ |a_k|_p : n+1 \leq k \leq n+m \bigr\} < \varepsilon \,,$$

so the sequence (s_n) of partial sums is a Cauchy sequence and therefore convergent in the complete metric space $\mathbb{Q}_p$. ❑

If we consider a power series $\sum_{n=0}^{\infty} a_n x^n$ with $a_n \in \mathbb{Z}_p$, then $|a_n x^n|_p \to 0$ as soon as $|x|_p < 1$ (use that $|a_n|_p \leq 1$). In particular, $\sum_{n=0}^{\infty} a_n p^n$ converges (and the value is in $\mathbb{Z}_p$).

The following result is important, because it allows us to reduce many questions about p-adic numbers to questions about the field $\mathbb{F}_p$.

3.8. **Theorem.** *Let $h \in \mathbb{Z}_p[x]$ be a polynomial and let $a \in \mathbb{F}_p$ such that a is a simple root of $\bar{h} \in \mathbb{F}_p[x]$, where $\bar{h}$ is obtained from h by reducing the coefficients mod p. Then h has a unique root $\alpha \in \mathbb{Z}_p$ such that $\bar{\alpha} = a$.*

THM Hensel's Lemma

More generally, suppose that $\bar{h} = u_1 u_2$ with $u_1, u_2 \in \mathbb{F}_p[x]$ monic and without common factors. Then there are unique monic polynomials $h_1, h_2 \in \mathbb{Z}_p[x]$ such that $\bar{h}_1 = u_1$, $\bar{h}_2 = u_2$ and $h = h_1 h_2$.

Proof. We prove the first statement and leave the second as an exercise.

One approach for showing existence is to use Newton's method. Let $\alpha_0 \in \mathbb{Z}_p$ be arbitrary such that $\bar{\alpha}_0 = a$ and define

$$\alpha_{n+1} = \alpha_n - \frac{h(\alpha_n)}{h'(\alpha_n)} \,.$$

Then one shows by induction that $h(\alpha_n) \in p\mathbb{Z}_p$, $h'(\alpha_n) \in \mathbb{Z}_p^\times$ and (in a similar way as for the standard Newton's method) $|\alpha_{n+1} - \alpha_n|_p \leq |\alpha_n - \alpha_{n-1}|_p^2$; this uses the relation $h(x+y) = h(x) + yh'(x) + y^2 h_2(x,y)$ with $h_2 \in \mathbb{Z}_p[x,y]$. Since we have $|\alpha_1 - \alpha_0| < 1$, the sequence $(\alpha_n)_n$ is a Cauchy sequence in the complete metric space $\mathbb{Z}_p$, hence converges to a limit $\alpha \in \mathbb{Z}_p$. Since everything is continuous, it follows that $h(\alpha) = 0$. To show uniqueness, observe that for $\beta \in \mathbb{Z}_p$ with $h(\beta) = 0$,

$$0 = h(\beta) - h(\alpha) = (\beta - \alpha)\bigl(h'(\alpha) + (\beta - \alpha) h_2(\alpha, \beta - \alpha)\bigr) \,;$$

if $|\beta - \alpha|_p < 1$, then the right hand factor is a unit, and it follows that $\beta = \alpha$. ❑

As a sample application, we have the following.

3.9. **Corollary.** *Let p be an odd prime and let $\alpha = p^n u \in \mathbb{Q}_p$ with $u \in \mathbb{Z}_p^\times$. Then α is a square in $\mathbb{Q}_p$ if and only if n is even and $\bar{u}$ is a square in $\mathbb{F}_p$.* **COR** squares in $\mathbb{Q}_p$

Proof. That the condition is necessary is obvious. For the sufficiency, we can reduce to the case $n = 0$. Consider the polynomial $x^2 - u$. By assumption, its reduction has a root; this root is simple (since $\bar{u} \neq 0$ and the derivative $2x$ only vanishes at 0; here we use that p is odd), so by Hensel's Lemma, $x^2 - u$ has a root in $\mathbb{Z}_p$; this means that u is a square. ❑

If $p = 2$, the condition is that n is even and $u \equiv 1 \bmod 8$ (Exercise).

Now consider a hyperelliptic curve $C\colon y^2 = F(x, z)$ over $\mathbb{Q}_p$ such that F has coefficients in $\mathbb{Z}_p$. Then we can reduce the coefficients mod p and obtain a homogeneous polynomial $\bar{F} \in \mathbb{F}_p[x, z]$ of degree $2g + 2$. If $\bar{F}$ is squarefree, then we say that C has *good reduction*. If C is defined over $\mathbb{Q}$, with $F \in \mathbb{Z}[x, z]$, then we say that C has *good reduction at p* if C has good reduction as a curve over $\mathbb{Q}_p$. Otherwise, we say that C has *bad reduction (at p)*. **DEF** good/bad reduction

In both cases, good reduction is equivalent to $p \nmid \operatorname{disc}(F)$ and $p \neq 2$ (in characteristic 2 our equations always define singular curves), where $\operatorname{disc}(F)$ is the discriminant of the binary form F (which is a polynomial in the coefficients of F and vanishes if and only if F is not squarefree). If C is a curve over $\mathbb{Q}$ with $F \in \mathbb{Z}[x, z]$, then $\operatorname{disc}(F) \in \mathbb{Z} \setminus \{0\}$ according to our definition of 'hyperelliptic curve', so we see that C can have bad reduction at only finitely many primes p.

Even if C has bad reduction, we can write $\bar{C}$ for the curve over $\mathbb{F}_p$ defined by $y^2 = \bar{F}(x, z)$. (This is again a hyperelliptic curve of genus g when C has good reduction). Given a point $P = (\xi : \eta : \zeta) \in C(\mathbb{Q}_p)$, we can scale the coordinates so that $\xi, \zeta \in \mathbb{Z}_p$ and so that ξ and ζ are not both divisible by p. Then $\eta \in \mathbb{Z}_p$ as well (since $\eta^2 = F(\xi, \zeta) \in \mathbb{Z}_p$). Then $\bar{P} = (\bar{\xi} : \bar{\eta} : \bar{\zeta})$ is a point in $\mathbb{P}^2_g(\mathbb{F}_p)$, which lies on $\bar{C}$ (note that at least one of $\bar{\xi}$ and $\bar{\zeta}$ is nonzero). We therefore obtain a *reduction map*

$$\rho_p\colon C(\mathbb{Q}_p) \longrightarrow \bar{C}(\mathbb{F}_p)\,, \quad P \longmapsto \bar{P}\,.$$

Now Hensel's Lemma implies the following useful result.

3.10. **Corollary.** *Let $C\colon y^2 = F(x, z)$ be a hyperelliptic curve over $\mathbb{Q}_p$ such that $F \in \mathbb{Z}_p[x, z]$. Consider the curve $\bar{C}\colon y^2 = \bar{F}(x, z)$ over $\mathbb{F}_p$. If $Q \in \bar{C}(\mathbb{F}_p)$ is a smooth point, then there are points $P \in C(\mathbb{Q}_p)$ such that $\bar{P} = Q$.* **COR** lifting smooth points

Proof. We prove this more generally for affine plane curves (in the setting of the statement, we first restrict to an affine patch whose reduction contains Q). By shifting coordinates, we can assume that $Q = (0, 0) \in \mathbb{F}_p^2$, and by switching coordinates if necessary, we can assume that C is given by $f(x, y) = 0$ with $f \in \mathbb{Z}_p[x, y]$ such that $p \nmid \frac{\partial f}{\partial y}(0, 0)$ (this comes from the condition that Q is smooth on $\bar{C}$). Scaling f by a p-adic unit, we can even assume that the partial derivative is 1. Then

$$f(0, y) = pa_0 + y + a_2 y^2 + \ldots + a_n y^n$$

with $a_0, a_2, a_3, \ldots, a_n \in \mathbb{Z}_p$. This is a polynomial in y whose reduction mod p has the simple root 0, so by Hensel's Lemma, $f(0, y)$ has a root $\eta \in p\mathbb{Z}_p$. Then $P = (0, \eta) \in C(\mathbb{Q}_p)$ is a point reducing to Q. ❑

The proof shows more generally that

$$\{P \in C(\mathbb{Q}_p) : \bar{P} = Q\} \longrightarrow p\mathbb{Z}_p\,, \quad (\xi, \eta) \longmapsto \xi$$

is a bijection (in the situation of the proof: $Q = (0,0)$ and $\partial f/\partial y(Q) \neq 0$). The inverse map is given by $\xi \mapsto (\xi, \tilde{y}(\xi))$ where $\tilde{y} \in \mathbb{Z}_p[\![t]\!]$ is a power series, which converges on $p\mathbb{Z}_p$ (since its coefficients are p-adic integers). Compare the proof of Lemma 2.11, where similar power series were constructed.

Regarding curves over finite fields, there is the following important result.

3.11. **Theorem.** *Let C be a smooth and absolutely irreducible projective curve of genus g over a finite field F with q elements. Then*

THM Hasse-Weil Theorem

$$|\#C(F) - (q+1)| \leq 2g\sqrt{q}\,.$$

Helmut Hasse proved this for elliptic curves, André Weil generalized it to curves of arbitrary genus.

3.12. **Corollary.** *Let $C\colon y^2 = F(x,z)$ be a hyperelliptic curve of genus g such that $F \in \mathbb{Z}[x,z]$ and let $p > 4g^2 - 2$ be a prime such that C has good reduction at p. Then $C(\mathbb{Q}_p) \neq \emptyset$.*

COR $C(\mathbb{Q}_p) \neq \emptyset$

Proof. Let $\bar{C}$ be the reduction mod p of C. Since C has good reduction at p, $\bar{C}$ is a hyperelliptic curve of genus g, so it is in particular smooth, projective and absolutely irreducible. By the Hasse-Weil Theorem, we have

$$\#\bar{C}(\mathbb{F}_p) \geq p + 1 - 2g\sqrt{p} > 0\,,$$

since $p > 4g^2 - 2$ implies $p^2 + 1 > p^2 > (4g^2 - 2)p$, so $(p+1)^2 = p^2 + 2p + 1 > 4g^2p = (2g\sqrt{p})^2$. So $\bar{C}(\mathbb{F}_p) \neq \emptyset$. Since $\bar{C}$ is smooth, any point $Q \in \bar{C}(\mathbb{F}_p)$ is smooth, so by Corollary 3.10 there are points $P \in C(\mathbb{Q}_p)$ reducing to Q; in particular, $C(\mathbb{Q}_p) \neq \emptyset$. ❑

The condition that C has good reduction is necessary. To see this, take a monic polynomial $f \in \mathbb{Z}[x]$ of degree $2g+2$ whose reduction mod p is irreducible and consider the curve $C\colon y^2 = pf(x)$. Then for any $\xi \in \mathbb{Z}_p$, we have $p \nmid f(\xi)$, so $v_p(pf(\xi)) = 1$, and $f(\xi)$ cannot be a square. If $\xi \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, then we have $v_p(f(\xi)) = -2g - 2$ (the term x^{2g+2} dominates), and $v_p(pf(\xi))$ is odd, so $f(\xi)$ cannot be a square again. So $C(\mathbb{Q}_p) = \emptyset$.

Another type of example is given by polynomials F whose reduction has the form $\bar{F}(x,z) = cH(x,z)^2$ with $c \in \mathbb{F}_p^\times$ a non-square and $H \in \mathbb{F}_p[x,z]$ such that H has no roots in $\mathbb{P}^1(\mathbb{F}_p)$. Then $F(\xi,\zeta) \in \mathbb{Z}_p^\times$ for all coprime (i.e., not both divisible by p) pairs $(\xi,\zeta) \in \mathbb{Z}_p^2$, and the reduction is a non-square, so $F(\xi,\zeta)$ is never a square.

If F is not divisible by p and the reduction of F does not have the form cH^2 as above, then it is still true that for p large enough, $C(\mathbb{Q}_p) \neq \emptyset$ (Exercise).

Why is this interesting? Well, obviously, if $C(\mathbb{Q}_p) = \emptyset$ for some p (or $C(\mathbb{R}) = \emptyset$), then this implies that $C(\mathbb{Q}) = \emptyset$ as well. So checking for 'local points' (this means points over $\mathbb{Q}_p$ or $\mathbb{R}$) might give us a proof that our curve has no rational points. The Corollary above now shows that we have to consider only a finite number of primes p, since for all sufficiently large primes of good reduction, we always have $\mathbb{Q}_p$-points.

For a prime p that is not covered by the Corollary, we can still check explicitly whether $C(\mathbb{Q}_p)$ is empty or not. We compute $\bar{C}(\mathbb{F}_p)$ as a first step.

- If $\bar{C}(\mathbb{F}_p)$ is empty, then $C(\mathbb{Q}_p)$ must be empty (since any point in $C(\mathbb{Q}_p)$ would have to reduce to a point in $\bar{C}(\mathbb{F}_p)$).
- If $\bar{C}(\mathbb{F}_p)$ contains smooth points, then $C(\mathbb{Q}_p)$ is non-empty by Corollary 3.10.
- Otherwise, we consider each point $Q \in \bar{C}(\mathbb{F}_p)$ in turn. After a coordinate change, we can assume that $Q = (0, \bar{\eta})$ on the standard affine patch. We assume $p \neq 2$ for simplicity; the case $p = 2$ is similar, but more involved. If C is given by $y^2 = f(x)$, then $\bar{f}$ must have a multiple root at zero (otherwise Q would be smooth), so $\bar{\eta} = 0$, and we can write

  $$f(x) = pa_0 + pa_1x + a_2x^2 + a_3x^3 + \ldots + a_{2g+2}x^{2g+2}$$

  with $a_j \in \mathbb{Z}_p$. If $p \nmid a_0$, then $v_p(f(\xi)) = 1$ for all $\xi \in p\mathbb{Z}_p$, so Q does not lift to a point in $C(\mathbb{Q}_p)$. Otherwise, replace f by

  $$f_1(x) = p^{-2}f(px) = p^{-1}a_0 + a_1x + a_2x^2 + pa_3x^3 + \ldots + p^{2g}a_{2g+2}x^{2g+2}\,.$$

  Now we are looking for $\xi \in \mathbb{Z}_p$ such that $f_1(\xi)$ is a square in $\mathbb{Z}_p$. In effect, we look for points in $C_1(\mathbb{Q}_p)$ with x-coordinate in $\mathbb{Z}_p$, where $C_1\colon y^2 = f_1(x)$; this curve is isomorphic to C. So we apply the method recursively to the new equation. This recursion has to stop eventually, since otherwise f would have to have a multiple root (as one can show), and either shows that Q does not lift or that it does. If one of the points $Q \in \bar{C}(\mathbb{F}_p)$ lifts, then $C(\mathbb{Q}_p) \neq \emptyset$; otherwise $C(\mathbb{Q}_p)$ is empty.

3.13. **Definition.** We say that a (hyperelliptic) curve C over $\mathbb{Q}$ *has points everywhere locally*, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p. ♢

DEF points everywhere locally

As noted earlier, a curve that has rational points must also have points everywhere locally.

3.14. **Theorem.** *Let C be a hyperelliptic curve of genus g over $\mathbb{Q}$, given by an equation $y^2 = F(x, z)$ with $F \in \mathbb{Z}[x, z]$. Then we can check by a finite procedure whether C has points everywhere locally or not.*

THM checking for local points

Proof. First $C(\mathbb{R}) = \emptyset$ is equivalent to F having no roots in $\mathbb{P}^1(\mathbb{R})$ and negative leading coefficient; both conditions can be checked.

Now let p be a prime. There are only finitely many p such that C has bad reduction at p or $p \leq 4g^2 - 2$; for all other p we know that $C(\mathbb{Q}_p) \neq \emptyset$ by Corollary 3.12. For the finitely many remaining primes we can use the procedure sketched above. ❑

One can show that for every genus $g \geq 2$, there is a certain positive 'density' of hyperelliptic curves of genus g over $\mathbb{Q}$ that fail to have points everywhere locally, in the following sense. Let $\mathcal{F}_g(X)$ be the set of binary forms $F(x, z) \in \mathbb{Z}[x, z]$ of degree $2g + 2$ and without multiple factors, with coefficients of absolute value bounded by X. Then

$$\rho_g = \lim_{X\to\infty} \frac{\#\{F \in \mathcal{F}_g(X) : y^2 = F(x, z) \text{ fails to have points everywhere locally}\}}{\#\mathcal{F}_g(X)}$$

exists and is positive. For example, ρ_2 is about 0.15 to 0.16 (and the limit is approached rather quickly).

3.15. **Example.** The curve **EXAMPLE**

$$C\colon y^2 = 2x^6 - 4$$

has no rational points. This is because there are no $\mathbb{Q}_2$-points: If $\xi \in 2\mathbb{Z}_2$, then $2\xi^6 - 4 \equiv -4 \bmod 2^7$, and so $f(\xi) = 4u$ with $u \equiv -1 \bmod 8$, so $f(\xi)$ is not a square. If $\xi \in \mathbb{Z}_2^\times$, then $v_2(f(\xi)) = 1$, so $f(\xi)$ is not a square. If $\xi \in \mathbb{Q}_2 \setminus \mathbb{Z}_2$, then $v_2(f(\xi)) = 1 + 6v_2(\xi)$ is odd, so $f(\xi)$ is not a square. And since 2 is not a square in $\mathbb{Q}_2$, the two points at infinity are not defined over $\mathbb{Q}_2$ either.

On the other hand, $C(\mathbb{R}) \neq \emptyset$ (the points at infinity are real) and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes $p \neq 2$: 2 and 3 are the only primes of bad reduction (the discriminant of F is $2^{21} \cdot 3^6$), there is a $\mathbb{Q}_3$-point with $\xi = 1$ (-2 is a square in $\mathbb{Q}_3$), there are $\mathbb{Q}_p$-points with $\xi = 0$ for $p = 5$ and 13, with $\xi = 1$ for $p = 11$ and with $\xi = \infty$ for $p = 7$. For all $p > 13$, we have $C(\mathbb{Q}_p) \neq \emptyset$ by Corollary 3.12. ♣

4. Divisors and the Picard group

If k is a field, we write k^{sep} for its *separable closure*; this is the subfield of the algebraic closure $\bar{k}$ consisting of all elements that are separable over k. The group of k-automorphisms of k^{sep} is the *absolute Galois group* of k, written $\mathrm{Gal}(k)$.

Now consider a (hyperelliptic) curve C over k. Then $\mathrm{Gal}(k)$ acts on the set $C(k^{\mathrm{sep}})$ of k^{sep}-points on C via the natural action of $\mathrm{Gal}(k)$ on the coordinates.

DEF divisor group; divisor; degree; effective; support

4.1. **Definition.** Let C be a smooth, projective and absolutely irreducible curve over a field k. The free abelian group with basis the set of k^{sep}-points on C is called the *divisor group* of C, written Div_C. Its elements, which are formal integral linear combinations of points in $C(k^{\mathrm{sep}})$, are *divisors* on C. We will usually write a divisor D as

$$D = \sum_{P \in C(k^{\mathrm{sep}})} n_P \cdot P\,,$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many points P. We also denote n_P by $v_P(D)$. The *degree* of such a divisor is $\deg(D) = \sum_P n_P$; this defines a homomorphism $\deg\colon \mathrm{Div}_C \to \mathbb{Z}$. The set of divisors of degree zero forms a subgroup Div_C^0 of Div_C. We write $D \geq D'$ if $v_P(D) \geq v_P(D')$ for all points P. A divisor D such that $D \geq 0$ is said to be *effective*. The *support* of D is the set $\mathrm{supp}(D) = \{P \in C(k^{\mathrm{sep}}) : v_P(D) \neq 0\}$ of points occurring in D with a nonzero coefficient. ♢

The action of $\mathrm{Gal}(k)$ on $C(k^{\mathrm{sep}})$ induces an action on Div_C by group automorphisms.

DEF rational divisor

4.2. **Definition.** A divisor $D \in \mathrm{Div}_C$ is *k-rational* if it is fixed by the action of $\mathrm{Gal}(k)$. We write $\mathrm{Div}_C(k)$ ($\mathrm{Div}_C^0(k)$) for the subgroup of k-rational divisors (of degree zero) on C. ♢

EXAMPLE rational divisor

4.3. **Example.** Let $C\colon y^2 = f(x)$ be hyperelliptic over k. Then for every $\xi \in k$ the divisor $D_\xi = (\xi, \eta) + (\xi, -\eta)$ is k-rational, where $\eta \in k^{\mathrm{sep}}$ is a square root of $f(\xi)$: either $\eta \in k$, then both points in the support are fixed by the Galois action, or else $k(\eta)$ is a quadratic extension of k and an element $\sigma \in \mathrm{Gal}(k)$ either fixes both points or interchanges them, leaving D_ξ invariant in both cases. ♣

Now if $\phi \in k^{\mathrm{sep}}(C)^\times$ is a nonzero rational function on C, then it is easy to see (considering a representative quotient of polynomials) that ϕ has only finitely many zeros and poles on C. The following definition therefore makes sense.

DEF principal divisor; Picard group; linear equivalence

4.4. **Definition.** Let $\phi \in k^{\mathrm{sep}}(C)^\times$. We set

$$\mathrm{div}(\phi) = \sum_P n_P(\phi) \cdot P$$

and call this the *divisor of ϕ*. A divisor of this form is said to be *principal*. We write Princ_C for the subgroup of principal divisors. The quotient group

$$\mathrm{Pic}_C = \mathrm{Div}_C \,/\, \mathrm{Princ}_C$$

is the *Picard group* of C. Two divisors D, D' are said to be *linearly equivalent* if $D - D'$ is principal; we write $D \sim D'$. We usually write $[D]$ for the linear equivalence class of a divisor $D \in \mathrm{Div}_C$, i.e., for the image of D in Pic_C. ♢

4.5. **Example.** All divisors D_ξ in Example 4.3 are linearly equivalent, since

$$\operatorname{div}\Big(\frac{x-\xi}{x-\xi'}\Big) = D_\xi - D_{\xi'}\,. \qquad \clubsuit$$

EXAMPLE linearly equivalent divisors

Note that by the properties of valuations, the map

$$\operatorname{div}\colon k^{\mathrm{sep}}(C)^\times \longrightarrow \mathrm{Div}_C$$

is a group homomorphism, so its image Princ_C is a subgroup.

The absolute Galois group $\mathrm{Gal}(k)$ acts on $k^{\mathrm{sep}}(C)$ (via the action on the coefficients of the representing quotients of polynomials); the map div is equivariant (i.e., compatible) with the actions of $\mathrm{Gal}(k)$ on both sides. This implies that $\operatorname{div}(\phi) \in \mathrm{Div}_C(k)$ if $\phi \in k(C)^\times$. We also obtain an action of $\mathrm{Gal}(k)$ on the Picard group; as usual, we write $\mathrm{Pic}_C(k)$ for the subgroup of elements fixed by the action and say that they are *k-rational*.

4.6. **Example.** Let $C\colon y^2 = f(x)$ as usual. The divisor of the function x is

EXAMPLE divisors of functions

$$\operatorname{div}(x) = (0, \sqrt{f(0)}) + (0, -\sqrt{f(0)}) - \infty_s - \infty_{-s}$$

where s is a square root of the coefficient of x^{2g+2} in f. The divisor of y is

$$\operatorname{div}(y) = \sum_{\alpha\colon f(\alpha)=0} (\alpha, 0) - (g+1)(\infty_s + \infty_{-s})$$

if $\deg(f) = 2g+2$ and

$$\operatorname{div}(y) = \sum_{\alpha\colon f(\alpha)=0} (\alpha, 0) - (2g+1)\cdot\infty$$

if $\deg(f) = 2g+1$.

Note that any polynomial in x and y is regular on C_{aff}, so the only points occurring with negative coefficients in the divisor of such a function are the points at infinity. $\clubsuit$

These examples already hint at the following fact.

4.7. **Lemma.** *Let $\phi \in k^{\mathrm{sep}}(C)^\times$. Then* $\deg\operatorname{div}(\phi) = 0$.

LEMMA $\mathrm{Princ}_C \subset \mathrm{Div}_C^0$

Proof. We prove this for hyperelliptic curves. One can prove it in a similar way for arbitrary curves, using some morphism $C \to \mathbb{P}^1$.

The hyperelliptic involution acts on $k^{\mathrm{sep}}(C)^\times$ and on Div_C (by sending (x,y) to $(x,-y)$ and by its action on the points, respectively). Let $\iota^*\phi$ be the image of ϕ under this action. Then $\deg\operatorname{div}(\iota^*\phi) = \deg\operatorname{div}(\phi)$, so $\deg\operatorname{div}(\phi\cdot\iota^*\phi) = 2\deg\operatorname{div}(\phi)$. ϕ is represented by a function on $\mathbb{P}^2_g$ of the form $h_1(x) + h_2(x)y$ (this is because $y^2 = f(x)$); then $\iota^*\phi = h_1(x) - h_2(x)y$ and

$$\phi\cdot\iota^*\phi = h_1(x)^2 - h_2(x)^2y^2 = h_1(x)^2 - h_2(x)^2 f(x) \in k^{\mathrm{sep}}(x)$$

is a function of x alone. Writing this projectively as a quotient of homogeneous polynomials in x and z of the same degree, one sees that this has the same number of zeros and poles (counted with multiplicity), so the degree above is zero. ❑

This means that Princ_C is contained in Div_C^0, so that deg descends to a homomorphism $\mathrm{Pic}_C \to \mathbb{Z}$. We denote its kernel by Pic_C^0.

We now state an important fact, whose proof is beyond the scope of this course.

4.8. **Theorem.** *Let C be a smooth, projective and absolutely irreducible curve of genus g over some field k. Then there exists an abelian variety J of dimension g over k such that for each field $k \subset L \subset k^{\mathrm{sep}}$, we have $J(L) = \mathrm{Pic}^0_C(L)$.*

THM Existence of the Jacobian

4.9. **Definition.** The abelian variety J is called the *Jacobian variety* (or just *Jacobian*) of the curve C. ♢

DEF Jacobian variety

An *abelian variety* A is a smooth projective group variety, i.e., a variety that carries a group structure that is compatible with the geometry: the group law $A \times A \to A$ and the formation of inverses $A \to A$ are morphisms of algebraic varieties. It can be shown that on a *projective* group variety, the group structure is necessarily abelian. Therefore one usually writes the group additively (which fits well with the notation we have introduced for the Picard group). One-dimensional abelian varieties are exactly elliptic curves.

Since J is a projective variety, it can be embedded in some projective space $\mathbb{P}^N$ over k. One can show that $N = 4^g - 1$ always works for hyperelliptic curves (in a natural way). Already for $g = 2$, this is (mostly) too large for practical purposes. The advantage of the identification of the Jacobian with the group Pic^0 is that we can represent points on J by divisors on C. We can also use this representation to do computations in the group $J(k)$ (say).

Note that if $P_0 \in C(k)$, then we obtain a natural map $i\colon C \to J$, given by sending a point $P \in C$ to the class of the divisor $P - P_0$. This map turns out to be a morphism of algebraic varieties, which is injective when $g > 0$. (If $i(P) = i(Q)$, then $[P - P_0] = [Q - P_0]$, hence $[Q - P] = 0$. So there is a rational function ϕ on C such that ϕ has a simple zero at Q and a simple pole at P. ϕ extends to a morphism $C \to \mathbb{P}^1$, which is bijective on points — the divisor of $\phi - c$ must be of the form $[Q_c - P]$ for some $Q_c \in C$ — and since C is smooth, ϕ is an isomorphism, so the genus of C is that of $\mathbb{P}^1$, which is zero.) The problem of finding the set $C(k)$ of k-rational points on C can now be stated equivalently in the form 'find the set $J(k) \cap i(C)$'. The advantage of this point of view is that we can use the additional (group) structure we have on J to obtain information on $C(k)$. A very trivial instance of this is that $J(k) = \{0\}$ implies $C(k) = \{P_0\}$. That $J(k)$ is not 'very large' in the cases of interest is reflected by the following result that we also state without proof.

4.10. **Theorem.** *Let k be a number field and let J be the Jacobian of a curve over k. Then the group $J(k)$ is a finitely generated abelian group.*

THM Mordell-Weil Theorem

This was proved by Mordell[4] in 1922 for elliptic curves over $\mathbb{Q}$ and generalized by Weil[5] a few years later.

By the structure theorem for finitely generated abelian groups, as a group $J(k)$ is isomorphic to $\mathbb{Z}^r \times T$, where $T = J(k)_{\mathrm{tors}}$ is the finite torsion subgroup of $J(k)$ and $r \in \mathbb{Z}_{\geq 0}$ is the *rank* of $J(k)$. So at least in principle, there is a finite explicit description of $J(k)$, given by divisors representing the generators of the free abelian part $\mathbb{Z}^r$, together with divisors representing generators of the torsion subgroup.

To know how we can represent points on J by divisors, we need another result.

4.11. **Definition.** Let C be a smooth, projective, absolutely irreducible curve over a field k and let $D \in \mathrm{Div}_C(k)$ be a divisor. The *Riemann-Roch space* of D is the k-vector space

DEF Riemann-Roch space

$$L(D) = \{\phi \in k(C)^\times : \mathrm{div}(\phi) + D \geq 0\} \cup \{0\}\,. \qquad \diamondsuit$$

If D is effective, say $D = n_1P_1 + \ldots + n_mP_m$ with $n_j > 0$, then the condition $\mathrm{div}(\phi) + D \geq 0$, or equivalently, $\mathrm{div}(\phi) \geq -D$, says that ϕ must be regular outside the support of D, with poles of orders at most $n_1, \ldots, n_m$ at the points $P_1, \ldots, P_m$. If D is not effective, then we also have conditions that require ϕ to have a zero of at least a certain order at each point occurring with a negative coefficient in D.

Since $\deg \mathrm{div}(\phi) = 0$, we see immediately that $L(D) = \{0\}$ if $\deg D < 0$. If $\deg D = 0$, then $L(D) \neq \{0\}$ means that there is some $\phi \in k(C)^\times$ with divisor $\mathrm{div}(\phi) = -D$, so that $D = -\mathrm{div}(\phi) = \mathrm{div}(\phi^{-1})$ is principal. More generally, if D and D' are linearly equivalent, so that there is some $\phi \in k(C)^\times$ with $D - D' = \mathrm{div}(\phi)$, then multiplication by ϕ induces an isomorphism $L(D) \to L(D')$. The space $L(0)$ consists of the functions that are regular everywhere, which are just the constants, so $L(0) = k$. Another simple property is that $D \geq D'$ implies $L(D) \supset L(D')$.

4.12. **Theorem.** *Let C be a smooth, projective, absolutely irreducible curve of genus g over a field k. There is a divisor $W \in \mathrm{Div}_C(k)$ such that for every $D \in \mathrm{Div}_C(k)$ we have that $\dim_k L(D)$ is finite and*

THM Riemann-Roch Theorem

$$\dim_k L(D) = \deg D - g + 1 + \dim_k L(W - D)\,.$$

In particular, $\dim_k L(W) = g$, $\deg W = 2g-2$, the class of W in Pic_C is uniquely determined, and we get the equality

$$\dim_k L(D) = \deg D - g + 1$$

for $\deg D \geq 2g - 1$.

Proof. The proof is again beyond the scope of this course. The divisor W can be constructed using differentials (see later). The idea of the proof is to first show the equality for $D = 0$ and then check that it remains true if one adds or subtracts a point to or from D.

For $D = 0$, we obtain

$$1 = \dim_k k = \dim_k L(0) = 0 - g + 1 + \dim_k L(W)\,,$$

so $\dim_k L(W) = g$. Then for $D = W$, we find

$$g = \dim_k L(W) = \deg W - g + 1 + \dim_k L(0) = \deg W - g + 2\,,$$

so $\deg W = 2g - 2$. If W' is another divisor with the properties of W, then taking $D = W'$, we find that $\dim_k L(W - W') = 1$, which, since $\deg(W - W') = 0$, implies that W and W' are linearly equivalent. Finally, if $\deg D \geq 2g - 1 > \deg W$, then $\deg(W - D) < 0$, so $\dim_k L(W - D) = 0$ and the relation simplifies. ❑

EXAMPLE RR spaces on hyp. curves

4.13. **Example.** Consider an hyperelliptic curve $C\colon y^2 = f(x)$ of odd degree and genus g. Then the set of rational functions on C that are regular away from ∞ is the coordinate ring $k[x,y]$ of C_{aff}. Using the curve equation, we can eliminate all powers of y strictly larger than the first, and we see that $k[x,y]$ has the k-basis $1, x, x^2, \ldots, y, xy, x^2y, \ldots$. From Example 4.6 we know that $v_\infty(x) = -2$ and $v_\infty(y) = -(2g+1)$. This implies $v_\infty(x^n) = -2n$ and $v_\infty(x^n y) = -(2n+2g+1)$, so that the basis elements have pairwise distinct valuations at ∞. This in turn means that the valuation of a linear combination of the basis elements is the minimal valuation occurring among the basis elements with nonzero coefficient. We therefore obtain

$$\begin{aligned}
L(0) &= \langle 1\rangle \\
L(\infty) &= \langle 1\rangle \\
L(2\cdot\infty) &= \langle 1, x\rangle \\
L(3\cdot\infty) &= \langle 1, x\rangle \\
&\vdots \qquad\qquad \vdots \\
L(2n\cdot\infty) &= \langle 1, x, x^2, \ldots, x^n\rangle && \text{if } n \le g \\
L((2n+1)\cdot\infty) &= \langle 1, x, x^2, \ldots, x^n\rangle && \text{if } n < g \\
&\vdots \qquad\qquad \vdots \\
L(2g\cdot\infty) &= \langle 1, x, x^2, \ldots, x^g\rangle \\
L((2g+1)\cdot\infty) &= \langle 1, x, x^2, \ldots, x^g, y\rangle \\
L((2g+2)\cdot\infty) &= \langle 1, x, x^2, \ldots, x^g, y, x^{g+1}\rangle \\
&\vdots \qquad\qquad \vdots \\
L(2n\cdot\infty) &= \langle 1, x, x^2, \ldots, x^g, y, x^{g+1}, xy, \ldots, x^{n-g-1}y, x^n\rangle && \text{if } n \ge g+1 \\
L((2n+1)\cdot\infty) &= \langle 1, x, x^2, \ldots, x^g, y, x^{g+1}, xy, \ldots, x^n, x^{n-g}y\rangle && \text{if } n \ge g \\
&\vdots \qquad\qquad \vdots
\end{aligned}$$

For the dimensions, we have

$$\dim L(n\cdot\infty) = \begin{cases} 0, & \text{if } n < 0; \\ \lfloor n/2\rfloor + 1, & \text{if } 0 \le n \le 2g; \\ n - g + 1, & \text{if } 2g+1 \le n. \end{cases}$$

Note that $\lfloor n/2\rfloor + 1 = n - g + 1$ for $n = 2g-1$ and $n = 2g$, so this confirms the last statement in Theorem 4.12. ♣

COR Representation of points on J

4.14. **Corollary.** *Let C be as above and fix a k-rational point $P_0 \in C(k)$. Then for each $Q \in J(k)$, there is a unique effective divisor $D_Q \in \mathrm{Div}_C(k)$ of minimal degree such that $Q = [D_Q - (\deg D_Q)\cdot P_0]$. We have $\deg D_Q \le g$.*

Proof. Let $D \in \mathrm{Div}^0_C$ be any divisor such that $Q = [D]$. We first work over k^{sep}. Consider the spaces $L_n = L(D + n\cdot P_0)$ for $n = -1, 0, 1, 2, \ldots$. We have $\{0\} = L_{-1} \subset L_0 \subset L_1 \subset \ldots$ with $\dim L_{n+1} - \dim L_n \in \{0, 1\}$ (from the Riemann-Roch

[4] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Cambr. Phil. Soc. Proc. **21**, 179–192 (1922).

[5] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52**, 281–315 (1929).

formula; the degree increases by 1, and the dimension of $L(W - D - n \cdot P_0)$ cannot increase). This implies that there is a unique smallest $n \in \mathbb{Z}_{\geq 0}$ such that $\dim L_n = 1$. Let ϕ be a nontrivial element of L_n. Then $\operatorname{div}(\phi) = D_Q - D - n \cdot P_0$ (with $D_Q \geq 0$) does not depend on the choice of ϕ, and

$$Q = [D] = [D + \operatorname{div}(\phi)] = [D_Q - n \cdot P_0]\,.$$

It is clear that D_Q is unique with these properties and that there is no such divisor of smaller degree. It remains to show that D_Q is k-rational. Let $\sigma \in \operatorname{Gal}(k)$. Then (since $Q \in J(k)$ and $P_0 \in C(k)$) we have

$$[\sigma(D_Q) - n \cdot P_0] = [\sigma(D_Q - n \cdot P_0)] = \sigma([D_Q - n \cdot P_0]) = \sigma(Q) = Q = [D_Q - n \cdot P_0]\,.$$

Since D_Q is the unique effective divisor of degree n satisfying $Q = [D_Q - n \cdot P_0]$, it follows that $\sigma(D_Q) = D_Q$. So D_Q is fixed by the action of the Galois group, hence it is k-rational.

We have $\dim L_g = g - g + 1 + \dim L(W - D - g \cdot P_0) \geq 1$, so $n \leq g$. ❑

We will make this more concrete for hyperelliptic curves of odd degree. In this case, there is always the point $\infty \in C(k)$, so it is natural to use this as our basepoint P_0.

4.15. **Definition.** Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of odd degree and genus g over k. A divisor $D \in \operatorname{Div}_C$ is said to be *in general position* if D is effective, $\infty \notin \operatorname{supp}(D)$, and there is no point $P \in C$ such that $D \geq P + \iota(P)$. ♢

DEF divisor in general position

The latter condition means that D contains each ramification point $(\xi, 0)$ with coefficient 0 or 1 and that $\operatorname{supp}(D)$ cannot contain a point (ξ, η) with $\eta \neq 0$ together with its 'opposite' $(\xi, -\eta)$.

4.16. **Lemma.** *Let C be as above and let D be a divisor in general position on C. Then there are unique polynomials $a, b \in k[x]$ such that*

LEMMA Mumford representation

(1) a is monic of degree $d = \deg(D)$;

(2) $\deg(b) < d$;

(3) $f \equiv b^2 \bmod a$;

(4) if $P = (\xi, \eta) \in C_{\text{aff}}$, then $P \in \operatorname{supp}(D) \iff a(\xi) = 0, b(\xi) = \eta$, and in this case, $v_P(D)$ is the multiplicity of ξ as a root of a.

Conversely, such a pair (a, b) determines a divisor D in general position.

This representation of D by a pair of polynomials is the *Mumford representation* of D.

DEF Mumford representation

Proof. Write $\pi(D) = \sum_P v_P(D) \cdot \pi(P) \in \operatorname{Div}_{\mathbb{P}^1}$, where $\pi\colon C \to \mathbb{P}^1$ is the hyperelliptic quotient map. Since D is in general position, we have

$$v_Q(\pi(D)) = \max\{v_P(D) : \pi(P) = Q\} \qquad \text{for } Q \in \mathbb{P}^1.$$

Properties (1) and (4) then imply that $a = \prod_{\xi\colon v_\xi(\pi(D)) \neq 0} (x - \xi)^{v_\xi(\pi(D))}$; this shows that a is uniquely determined; also $a \in k[x]$ since $\pi(D)$ is defined over k. We obtain b essentially as the polynomial interpolating the points in the support of D. More precisely, let $(\xi, \eta) \in \operatorname{supp}(D)$. Then $f \equiv \eta^2 \bmod (x - \xi)$. If $\eta \neq 0$, by a variant of Hensel's Lemma, we can construct a ($\bmod (x - \xi)^n$ unique) $b_\xi \in k[x]$ such that $f \equiv b_\xi^2 \bmod (x - \xi)^n$ and $b(\xi) = \eta$, where $n = v_\xi(\pi(D)) = v_{(\xi,\eta)}(D)$. If $\eta = 0$,

we just set $b_\xi = 0$ (note that $n = 1$ in this case). We then obtain b from the b_ξ via the Chinese Remainder Theorem, which also implies that b is unique (and has therefore coefficients in k) if we require $\deg(b) < \deg(a) = d$.

For the converse, we set $D = \sum_{\xi\colon a(\xi)=0} v_{(x-\xi)}(a) \cdot (\xi, b(\xi))$. Then D is effective and of degree $d = \deg(a)$, and the support of D does not contain both a non-ramification point and its opposite. For a ramification point $P = (\xi, 0)$, we note that $f \equiv b^2 \bmod a$ and $b(\xi) = 0$, $f(\xi) = 0$ together imply that ξ is a simple root of a, since it is a simple root of f. ❑

LEMMA representation of points in $J(k)$

4.17. **Lemma.** *Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of odd degree and of genus g over k. Denote its Jacobian as usual by J. Then for every point $P \in J(k)$ there is a unique divisor $D \in \mathrm{Div}_C(k)$ in general position and of degree $d = \deg(D) \leq g$ such that $P = [D - d \cdot \infty]$.*

Proof. By Corollary 4.14 there is a unique effective divisor D of minimal degree d such that $P = [D - d \cdot \infty]$. We must show that D is in general position and that any D' in general position, of degree $d' \leq g$ and such that $P = [D' - d' \cdot \infty]$ equals D.

If D were not in general position, then $D \geq D_\xi$ for some ξ or $D \geq \infty$. But D_ξ is linearly equivalent to $2 \cdot \infty = D_\infty$, so

$$P = [D - d \cdot \infty] = [(D - D_\xi) - (d-2) \cdot \infty]\,,$$

contradicting the minimality of d. If $D \geq \infty$, then

$$P = [D - d \cdot \infty] = [(D - \infty) - (d-1) \cdot \infty]\,,$$

again contradicting the minimality of d.

If D' is in general position, of degree $d' \leq g$ and such that $[D' - d' \cdot \infty] = [D - d \cdot \infty]$, then $D' - D \sim (d' - d) \cdot \infty$, which implies that $D' + \iota(D) \sim (d' + d) \cdot \infty$. So there is a function $\phi \in L((d' + d) \cdot \infty)$ such that $D' + \iota(D)$ is its divisor of zeros. But $d' + d \leq 2g$, so this Riemann-Roch space is contained in $\langle 1, x, x^2, \ldots, x^g \rangle$, which implies that ϕ is a polynomial in x. But then $\mathrm{div}(\phi)$ is a linear combination of divisors of the form D_ξ, which (since both D' and $\iota(D)$ are in general position) is only possible when $D' = \iota(\iota(D)) = D$. ❑

The upshot of these considerations is that we can represent every $P \in J(k)$ uniquely by a pair of polynomials in $k[x]$ as in Lemma 4.16. We will now discuss how we can perform addition in $J(k)$ using this representation.

THM Addition on J

4.18. **Theorem.** *Let $C\colon y^2 = f(x)$ a hyperelliptic curve of odd degree and genus g over k; denote its Jacobian by J. Let the points $P_1, P_2 \in J(k)$ be given by the Mumford representations (a_1, b_1) and (a_2, b_2), respectively. Then we can compute the Mumford representation of $P_1 + P_2$ as follows:*

1. *(Composition — add the divisors and subtract D_ξ whenever possible)*
   (i) *Let $d = \gcd(a_1, a_2, b_1 + b_2)$.*
   (ii) *Set $a = a_1 a_2 / d^2$.*
   (iii) *Let b be the unique polynomial of degree $< \deg(a)$ such that $b \equiv b_1 \bmod a_1/d$, $b \equiv b_2 \bmod a_2/d$ and $f \equiv b^2 \bmod a$.*
   Then (a, b) represents a divisor D such that $P_1 + P_2 = [D - (\deg D) \cdot \infty]$.
2. *(Reduction — replace D by a divisor of degree $\leq g$)*
   While $\deg(a) > g$, do the following:

(i) *Write* $f - b^2 = \lambda ac$ *with* $\lambda \in k^\times$ *and* $c \in k[x]$ *monic.*
(ii) *Replace* a *by* c. *Note that* $\deg(c) < \deg(a)$.
(iii) *Replace* b *by the remainder of* $-b$ *mod (the new)* a.
Now (a, b) *represents a divisor* D *such that* $P_1 + P_2 = [D - (\deg D) \cdot \infty]$ *and* $\deg(D) \le g$.

Proof. Let (a_j, b_j) represent the divisor D_j, so that $P_j = [D_j - (\deg D_j) \cdot \infty]$. Let D' be the largest effective divisor that is a sum of divisors of the form D_ξ and such that $D' \le D_1 + D_2$. Then the divisor D obtained after part (1) of the procedure is $D = D_1 + D_2 - D'$. To see this, write $D' = D_{\xi_1} + \ldots + D_{\xi_n}$. Since D_1 and D_2 are in general position, for every $1 \le j \le n$, there must be η_j such that $(\xi_j, \eta_j) \in \operatorname{supp}(D_1)$ and $(\xi_j, -\eta_j) \in \operatorname{supp}(D_2)$. We deduce that $d = \prod_{j=1}^n (x - \xi_j)$ (if $d(\xi) = 0$, then $a_1(\xi) = a_2(\xi) = 0$ and $b_2(\xi) = -b_1(\xi)$, so $D_\xi \le D_1 + D_2$, and conversely; the claim follows by induction on n), so that a describes the projection of D to $\mathbb{P}^1$. The claim then follows, if we can show that b exists. We have $b_1^2 \equiv f \equiv b_2^2 \bmod \gcd(a_1, a_2)$, so $\gcd(a_1, a_2)$ divides $(b_1 + b_2)(b_1 - b_2)$. Since $\gcd(a_1, a_2, b_1 + b_2) = d$, it follows that $\gcd(a_1, a_2)/d = \gcd(a_1/d, a_2/d)$ divides $b_1 - b_2$. So by the Chinese Remainder Theorem, there is b' such that

$$b' \equiv b_1 \bmod a_1/d \qquad \text{and} \qquad b' \equiv b_2 \bmod a_2/d\,,$$

so $f \equiv b'^2 \bmod a_1 a_2/(d \gcd(a_1, a_2))$. A variant of Hensel's Lemma lets us lift b' uniquely (mod a) to a b satisfying $f \equiv b^2 \bmod a$.

The relation $f - b^2 = \lambda ac$ implies that $(c, -b)$ represents some divisor D' in general position, with (c, b) corresponding to $\iota(D')$. Then

$$D + \iota(D') - \deg(ac) \cdot \infty = \operatorname{div}(y - b(x))$$

is principal, implying that $[D - \deg(a) \cdot \infty] = [D' - \deg(c) \cdot \infty]$. We obtain the Mumford representation of D' by reducing $-b$ mod c as prescribed in the algorithm. We have $\deg(b) \le \deg(a) - 1$, hence

$$\deg(f - b^2) \le \max\{2g + 1, 2\deg(a) - 2\}\,,$$

which is $< 2\deg(a)$ if $\deg(a) > g$. Since $\deg(c) = \deg(f - b^2) - \deg(a)$, this implies $\deg(c) < \deg(a)$ as claimed. In particular, this part of the algorithm terminates, and upon termination we must have $\deg(a) \le g$. ❑

This algorithm is described in a paper by D.G. Cantor[6]

EXAMPLE
Multiples of a point

4.19. **Example.** Let us compute the multiples of $P = [(0, 1) - \infty] \in J(\mathbb{Q})$, where J is the Jacobian of $C\colon y^2 = x^5 + 1$, which has genus 2.

P is represented by $(a_1, b_1) = (x, 1)$. In the computation of $2P$, we first obtain $d = \gcd(x, x, 2) = 1$, and we have to find b such that

$$b \equiv 1 \bmod x \qquad \text{and} \qquad x^5 + 1 \equiv b^2 \bmod x^2\,.$$

The first condition (plus $\deg(b) < 2$) says that $b = 1 + \beta x$; the second then implies $\beta = 0$. So $2P$ is given by $(a_2, b_2) = (x^2, 1)$.

To get $3P$, we add P and $2P$. This gives $d = \gcd(x, x^2, 2) = 1$ and (in a similar way as for $2P$) $(a, b) = (x^3, 1)$. Now $\deg(a) > 2$, so we need a reduction step. We have $f - b^2 = x^5 = x^3 \cdot x^2$, so $c = x^2$ and we obtain $(a_3, b_3) = (x^2, -1)$ as the representation of $3P$.

[6] David G. Cantor: *Computing the Jacobian of a hyperelliptic curve*, Math. Comput. **48**, 95–101 (1987).

Now we add P and $3P$. This time, $d = \gcd(x, x^2, 0) = x$ is nontrivial. We have $a = x$, and b must satisfy $b \equiv 1 \bmod 1$, $b \equiv -1 \bmod x$ and $x^5 + 1 \equiv b^2 \bmod x$, which means that $b = -1$. So $4P$ is represented by $(a_4, b_4) = (x, -1)$.

For the addition of P and $4P$, we obtain $d = \gcd(x, x, 0) = x$, so $a = 1$ and $b = 0$, so that $5P$ is represented by $(1, 0)$, which corresponds to the zero element of J. This shows that P has exact order 5 in $J(\mathbb{Q})$. ♣

An important consequence of the fact that Pic^0_C can be represented by an abelian variety J is the following.

4.20. **Lemma.** *Let C be a hyperelliptic curve over $\mathbb{Q}$, with Jacobian J, and let p be a prime of good reduction for C. Denote the Jacobian of $\bar{C}$ by $\bar{J}$. Then there is a reduction map $J(\mathbb{Q}) \to \bar{J}(\mathbb{F}_p)$ that is actually a group homomorphism.*

LEMMA Reduction of J

If we fix a basepoint $P_0 \in C(\mathbb{Q})$ and denote the induced embedding of C into J by $i\colon P \mapsto [P - P_0]$, then there is also the embedding $\bar{i}\colon \bar{C} \to \bar{J}$ that sends P to $[P - \bar{P}_0]$, and the following diagram commutes:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\ i\ } & J(\mathbb{Q}) \\ {\scriptstyle \rho_{p,C}}\downarrow & & \downarrow{\scriptstyle \rho_{p,J}} \\ \bar{C}(\mathbb{F}_p) & \xrightarrow{\ \bar{i}\ } & \bar{J}(\mathbb{F}_p) \end{array}$$

Proof. This is a consequence of the fact that the construction of the Jacobian is 'functorial'. In fairly down-to-earth terms, the reduction map on J is given by 'reducing mod p' the points in the support of a divisor representing a given point in $J(\mathbb{Q})$; one checks that the reduction of divisors respects principal divisors, which shows that one gets a well-defined group homomorphism. That the final diagram commutes is then clear. (This works in fact for any smooth, projective and absolutely irreducible curve over $\mathbb{Q}$.) ❑

The statement above also works with $\mathbb{Q}_p$ instead of $\mathbb{Q}$, so that the reduction mod p map can be defined on $J(\mathbb{Q}_p)$. Its kernel is called the *kernel of reduction* $J(\mathbb{Q}_p)_1$. If $p > 2$ (which follows from the 'good reduction' assumption when C is hyperelliptic), then one can show that $J(\mathbb{Q}_p)_1 \cong \mathbb{Z}_p^g$ as groups, which implies that $J(\mathbb{Q}_p)_1$ is torsion-free. (Behind this is the theory of 'formal groups'. One obtains a homomorphism $\log_{p,J}\colon J(\mathbb{Q}_p) \to \mathbb{Q}_p^g$ with kernel the (finite) torsion subgroup $J(\mathbb{Q}_p)_{\mathrm{tors}}$. One can arrange that the image of $J(\mathbb{Q}_p)_1$ is $(p\mathbb{Z}_p)^g$. There is an inverse map $\exp_{p,J}\colon (p\mathbb{Z}_p)^g \to J(\mathbb{Q}_p)_1$ when $p > 2$. In general, $\exp_{p,J}$ is given by power series that converge on g-tuples whose entries have $v_p > 1/(p-1)$; we need convergence as soon as $v_p \geq 1$, so we need $p > 2$.) As a consequence we have the following result. Recall the notation $J(\mathbb{Q})_{\mathrm{tors}}$ for the torsion subgroup of $J(\mathbb{Q})$.

DEF kernel of reduction

4.21. **Theorem.** *Let C be a hyperelliptic curve over $\mathbb{Q}$, with Jacobian J, and let p be a prime of good reduction for C. Then the reduction map $J(\mathbb{Q}) \to \bar{J}(\mathbb{F}_p)$ restricts to an injective group homomorphism on $J(\mathbb{Q})_{\mathrm{tors}}$.*

THM Reduction of torsion

Proof. Let $P \in \ker\bigl(J(\mathbb{Q})_{\mathrm{tors}} \to \bar{J}(\mathbb{F}_p)\bigr)$. Then P is also in $J(\mathbb{Q}_p)_1$. Since this group has no nontrivial elements of finite order, it follows that $P = 0$. ❑

The theorem and proof extend to $J(\mathbb{Q}_p)_{\text{tors}} \to \bar{J}(\mathbb{F}_p)$ (showing in particular that $J(\mathbb{Q}_p)_{\text{tors}}$ is finite). This map actually restricts to an isomorphism on the subgroups of elements of order not divisible by p (this is essentially an application of Hensel's Lemma again).

EXAMPLE Order of $J(\mathbb{Q})_{\text{tors}}$

4.22. **Example.** Consider $C\colon y^2 = x^5+1$ again. We have the points $[(-1,0)-\infty]$ of order 2 and $[(0,1)-\infty]$ of order 5 in $J(\mathbb{Q})$, so $\#J(\mathbb{Q})_{\text{tors}} \geq 10$. On the other hand, $p = 3$ is a prime of good reduction and $\#\bar{J}(\mathbb{F}_3) = 10$ (exercise), so Theorem 4.21 implies $\#J(\mathbb{Q})_{\text{tors}} \leq 10$. We conclude that $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/10\mathbb{Z}$. ♣

EXAMPLE $J(\mathbb{Q})_{\text{tors}}$ trivial

4.23. **Example.** Now consider $C\colon y^2 = x^5-x+1$. 3 and 5 are both good primes, and $\#\bar{J}(\mathbb{F}_3) = 29$, $\#\bar{J}(\mathbb{F}_5) = 71$. Since $J(\mathbb{Q})_{\text{tors}}$ can be embedded in a group of order 29 and in a group of order 71 by Theorem 4.21, it follows that $J(\mathbb{Q})_{\text{tors}} = \{0\}$ ($\gcd(29,71) = 1$). ♣

The preceding two examples show how one can use Theorem 4.21 to determine the torsion subgroup of $J(\mathbb{Q})$: Take the first few primes p of good reduction and compute $n(p) = \#\bar{J}(\mathbb{F}_p)$. Then $\#J(\mathbb{Q})_{\text{tors}}$ must divide the greatest common divisor of the numbers $n(p)$. Usually this gcd is 1, which shows that $J(\mathbb{Q})$ is torsion-free. In any case, we obtain an upper bound for the size of the torsion subgroup. To get lower bounds, we have to find suitable torsion points in $J(\mathbb{Q})$. In some cases, we can get a sharper bound by looking at the actual structure of the groups $\bar{J}(\mathbb{F}_p)$ instead of just at their size. For example, if we find that $\bar{J}(\mathbb{F}_3) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} = G_3$ and $\bar{J}(\mathbb{F}_5) \cong \mathbb{Z}/20\mathbb{Z} = G_5$, then we can conclude that $J(\mathbb{Q})_{\text{tors}}$ has order at most 2 (since $\mathbb{Z}/2\mathbb{Z}$ is the only nontrivial group that can be embedded into both G_3 and G_5), whereas $\gcd(\#G_3, \#G_5) = 4$.

EXAMPLE point of infinite order

4.24. **Example.** We continue working with $C\colon y^2 = x^5 - x + 1$. The point $P = [(0,1) - \infty] \in J(\mathbb{Q})$ is nontrivial, hence must be of infinite order. Another possibility for showing this (which does not require the torsion group to be trivial) is to find the orders of the images of P in $\bar{J}(\mathbb{F}_3)$ and $\bar{J}(\mathbb{F}_5)$. They turn out to be 29 and 71 (not very surprisingly). If P were a torsion point, then Theorem 4.21 would imply that $\bar{P} \in \bar{J}(\mathbb{F}_p)$ has the same order as P for every good prime $p > 2$. So P cannot have finite order. ♣

5. The 2-Selmer group

We have seen that it is usually possible to find the rational torsion subgroup of the group $J(\mathbb{Q})$, where J is the Jacobian of a hyperelliptic curve. It is much more difficult to determine the rank of the free abelian part of this group. We can obtain lower bounds by exhibiting points in $J(\mathbb{Q})$ (in the form of rational divisors representing them, say) and checking that they are independent. The hard part is to get a good upper bound on the rank. The standard way of doing this is to compute the so-called *2-Selmer group*.

Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of genus g over $\mathbb{Q}$, as usual. We will assume that $\deg(f)$ is odd and f is monic, since this leads to somewhat simpler statements. Let $A = \mathbb{Q}[x]/\langle f\rangle$ be the quotient ring; we write θ for the image of x in A, then $A = \mathbb{Q}[\theta]$. If f is irreducible, then A is an algebraic number field (i.e., a field extension of $\mathbb{Q}$ of finite degree). In general, if $f = f_1 f_2 \cdots f_m$ is the factorization of f into monic irreducible factors (which are all distinct, since f is squarefree), then by the Chinese Remainder Theorem, A is isomorphic to the direct product of the number fields $\mathbb{Q}[x]/\langle f_j\rangle$.

Now consider a divisor D in general position, with Mumford representation (a, b). Assume for now that $\gcd(a, f) = 1$. Then we can define $\delta(D) = (-1)^{\deg(a)}a(\theta) \in A^\times$. For a divisor D_ξ (with $f(\xi) \neq 0$), we set $\delta(D_\xi) = (\theta - \xi)^2$. If we set $\bar{A} = \bar{\mathbb{Q}}[x]/\langle f\rangle = \bar{\mathbb{Q}}[\theta]$ and $D = \sum_P n_P \cdot P$, then we have $\delta(D) = \prod_P (x(P) - \theta)^{n_P}$ (recall that $a(x) = \prod_P (x - x(P))^{n_P}$) in $\bar{A}^\times$, but the result is in $A^\times$, of course. We also set $\delta(\infty) = 1$. In this way, we obtain a group homomorphism $\mathrm{Div}_C^\perp(\mathbb{Q}) \to A^\times$, where $\mathrm{Div}_C^\perp(\mathbb{Q})$ denotes rational divisors whose support does not contain one of the ramification points of C other than ∞.

If $D - \deg(D)\cdot\infty = \mathrm{div}(\phi)$ is a principal divisor, where ϕ is some polynomial in x and y, say (without loss of generality) $\phi = h_1(x) + h_2(x)y$, then $a = \lambda(h_1^2 - h_2^2 f)$ with some $\lambda \in \mathbb{Q}^\times$, hence $\delta(D) = (-1)^{\deg(a)}a(\theta) = (-1)^{\deg(a)}\lambda h_1(\theta)^2$, since $f(\theta) = 0$. Since f has odd degree, there is no cancellation in the leading term in $h_1^2 - h_2^2 f$, and since a and f are monic, we have that λ is a square when $\deg(a)$ is even and $-\lambda$ is a square when $\deg(a)$ is odd. So $\delta(D)$ is a square in A in both cases. The homomorphism theorem for groups then gives us an induced homomorphism

$$\delta\colon \frac{\mathrm{Div}_C^\perp(\mathbb{Q})}{\mathrm{Div}_C^\perp(\mathbb{Q}) \cap \mathrm{Princ}_C(\mathbb{Q})} \longrightarrow \frac{A^\times}{(A^\times)^2}\,,$$

where $(A^\times)^2$ denotes the subgroup of squares in $A^\times$. Now one can show that it is always possible to represent a point in $J(\mathbb{Q})$ by a divisor in $\mathrm{Div}_C^\perp(\mathbb{Q})$, which finally gives us

$$\delta\colon J(\mathbb{Q}) \longrightarrow A^\times/(A^\times)^2\,.$$

We can write a divisor in general position as a sum of divisors D_j with Mumford representations (a_j, b_j) such that a_j is irreducible. If a_j does not divide f, then we compute $\delta([D_j - \deg(D_j)\cdot\infty])$ as above as the coset of $(-1)^{\deg(a_j)}a_j(\theta)$ modulo squares. If a_j does divide f, then we write $f = a_j a_j'$, and it turns out that

$$\delta([D_j - \deg(D_j)\cdot\infty]) = (-1)^{\deg(a_j)}a_j(\theta) + (-1)^{\deg(a_j')}a_j'(\theta)\,,$$

so we can evaluate δ easily at any point in $J(\mathbb{Q})$ given in Mumford representation.

5.1. **Lemma.** *The homomorphism $\delta\colon J(\mathbb{Q}) \longrightarrow A^\times/(A^\times)^2$ has kernel $2J(\mathbb{Q})$.* **LEMMA** kernel of δ

Proof. It is clear that $2J(\mathbb{Q}) \subset \ker(\delta)$, since $\delta(2P) = \delta(P)^2$ becomes trivial modulo squares. We have to show that the kernel is not larger. Let P be in the kernel and let (a, b) be the Mumford representation of P with $\deg(a) \le g$. For simplicity, we assume that $\gcd(a, f) = 1$ (the general case is similar, but more involved). Then $(-1)^{\deg(a)}a(\theta)$ is a square, which we can write as $s(\theta)^2$ with a polynomial $s \in \mathbb{Q}[x]$ of degree at most $2g$. For polynomials q, u and v, consider the following system of congruences:

$$v \equiv qs \bmod f\,, \quad v \equiv ub \bmod a\,.$$

We claim that this system has a nontrivial solution (q, u, v) such that $\deg(q) \le g$, $\deg(u) < \deg(a)/2$, $\deg(v) \le g + \deg(a)/2$ and q is monic. To see that there is a solution as claimed, write the congruences as a system of linear equations for the coefficients $q_0, \dots, q_g$, $u_0, \dots, u_{\lceil \deg(a)/2 \rceil - 1}$, $v_0, \dots, v_{g+\lfloor \deg(a)/2 \rfloor}$ of q, u and v. There are

$$(g+1) + \lceil \deg(a)/2 \rceil + (g + \lfloor \deg(a)/2 \rfloor + 1) = 2g + 2 + \deg(a)$$

such coefficients in total and $\deg(f) + \deg(a) = 2g + 1 + \deg(a)$ homogeneous equations, so nontrivial solutions must exist. If q were zero, then it would follow that $v = 0$ (since $\deg(v) < \deg(f)$) and then also $u = 0$ (since under our assumption on a, we have $\gcd(a, b) = 1$ and $\deg(u) < \deg(a)$), which is not possible. We can then scale all three polynomials so that q is monic. Now we have (recall that $f \equiv b^2 \bmod a$)

$$u^2 f \equiv u^2 b^2 \equiv v^2 \bmod a$$

and (recall that $\pm a(\theta) = s(\theta)^2$, which means that $\pm a \equiv s^2 \bmod f$)

$$v^2 \equiv q^2 s^2 \equiv (-1)^{\deg(a)} a q^2 \bmod f\,.$$

Together (and using $\gcd(a, f) = 1$ again) these two imply

$$u^2 f \equiv v^2 - (-1)^{\deg(a)} a q^2 \bmod af\,,$$

and since the degrees of all terms are less than $\deg(af) = \deg(a) + 2g + 1$, we find the relation

$$u^2 f = v^2 - (-1)^{\deg(a)} a q^2\,. \tag{5.1}$$

We see that we can assume that q and u are coprime; otherwise we can divide q, u and v by $\gcd(q, u)$ (which has to divide v). If $u = 0$, then a must be a square; indeed, $q = 1$, so $a = v^2$, and $P = 2Q$ with $Q = (v, b)$. Otherwise let $r \in \mathbb{Q}[x]$ be such that $ru \equiv -v \bmod q$; then $Q = (q, r)$ satisfies $P = 2Q$: (5.1) implies

$$u^2 f \equiv v^2 \equiv u^2 r^2 \bmod q\,,$$

and since u and q are coprime, we have $f \equiv r^2 \bmod q$, so that $Q = (q, r)$ really defines a point in $J(\mathbb{Q})$. The divisor of the function $u(x)y - v(x) \in \mathbb{Q}(C)^\times$ is $(a, b) + 2 \cdot (q, -r) - n \cdot \infty$ (with $n = \deg(a) + 2\deg(q)$): its norm is $u^2 f - v^2 = \pm a q^2$, and $ub \equiv v \bmod a$, $-ur \equiv v \bmod q$. This implies $P = 2Q$. We see that in both cases, $P \in 2J(\mathbb{Q})$. ❑

This tells us that $\delta(J(\mathbb{Q})) \cong J(\mathbb{Q})/2J(\mathbb{Q}) \cong J(\mathbb{Q})_{\mathrm{tors}}/2J(\mathbb{Q})_{\mathrm{tors}} \times (\mathbb{Z}/2\mathbb{Z})^r$ when r is the rank of $J(\mathbb{Q})$. Writing the finite abelian group $J(\mathbb{Q})_{\mathrm{tors}}$ as a product of cyclic groups of prime power order, we see that $J(\mathbb{Q})_{\mathrm{tors}}/2J(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^m$, where m is the number of factors of 2-power order. This is the same as the dimension of $J(\mathbb{Q})[2]$ as a vector space over $\mathbb{F}_2$, where for an abelian group G and $n \in \mathbb{Z}_{>0}$, $G[n]$ denotes the subgroup $\{g \in G : ng = 0\}$ of elements of order dividing n. The next lemma tells us how to find m.

LEMMA dimension of $J(k)[2]$

5.2. **Lemma.** *Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of odd degree over the field k. Let $f = cf_1f_2\cdots f_n$ be the factorization of f into irreducible factors with f_j monic and $c \in k^\times$. Then the points P_j with Mumford representation $(f_j, 0)$ generate the 2-torsion subgroup $J(k)[2]$, with the only relation $P_1 + \ldots + P_n = 0$. In particular,* $\dim_{\mathbb{F}_2} J(k)[2] = n - 1$.

Proof. If $P \in J[2]$, then $P = -P$ and conversely. If (a, b) is the Mumford representation of $P \in J(k)[2]$, then $(a, -b)$ is that of $-P$; since the representation is unique, we have $P = -P$ if and only if $b = 0$. This implies that a divides f, so (since $a \in k[x]$), a is a product of some subset of the f_j, of degree $\leq g$, the genus of C. This shows that the P_j generate $J(k)[2]$ (P is the sum of the P_j corresponding to the factors occurring in a) and that the order of $J(k)[2]$ is 2^{n-1} (which is the number of subsets $S \subset \{1, 2, \ldots, n\}$ such that $\sum_{j\in S} \deg(f_j) \leq g$ — note that exactly one of S and its complement has this property). So $\dim_{\mathbb{F}_2} J(k)[2] = n - 1$ and there must be exactly one relation among the n generators P_j. Since $\operatorname{div}(y)$ is the sum of the divisors $(f_j, 0)$ minus $(2g + 1)\cdot\infty$, there is a relation as stated, which must then be the unique such relation. ❑

So if we can get an upper bound s on $\dim_{\mathbb{F}_2} \delta(J(\mathbb{Q}))$ (or equivalently, a bound 2^s on the size of the image), we can conclude that $r \leq s - m$. We first show that the image of δ is contained in a certain subgroup H of $A^\times/(A^\times)^2$.

DEF norm $A \to k$

5.3. **Definition.** Let k be a field and let A be a finite-dimensional commutative k-algebra (a commutative ring A together with a ring homomorphism $k \to A$, which can be used to define a scalar multiplication with elements of k, thus turning A into a k-vector space, whose dimension we assume to be finite). Then for every $a \in A$, the map $m_a\colon A \to A$, $x \mapsto ax$, is k-linear, and we set $N_{A/k}(a) = \det(m_a)$ and call it the *norm* of a. ♢

Since determinants are multiplicative, we see that the map $N_{A/k}\colon A \to k$ satisfies $N_{A/k}(aa') = N_{A/k}(a)N_{A/k}(a')$. In particular, we obtain a group homomorphism $N_{A/k}\colon A^\times \to k^\times$.

EXAMPLE norm $k(C) \to k(x)$

5.4. **Example.** Let k be a field and consider a *quadratic k-algebra* A, so that $A = k[y]/\langle y^2 - a\rangle$ (if k has characteristic 2, this is not the most general quadratic algebra). Let $\alpha \in A$ be the image of y, so that $\alpha^2 = a$. Then $(1, \alpha)$ is a k-basis of A. Let $z = z_1 + z_2\alpha \in A$ with $z_1, z_2 \in k$. Then the matrix of the multiplication-by-z map m_z with respect to the basis $(1, \alpha)$ is

$$M = \begin{pmatrix} z_1 & az_2 \\ z_2 & z_1 \end{pmatrix},$$

so $N_{A/k}(z) = \det(M) = z_1^2 - az_2^2$.

A special case of this is $k(C)$ as a quadratic algebra over $k(x)$, when $C\colon y^2 = f(x)$ is a hyperelliptic curve. For a function $\phi = h_1(x) + h_2(x)y \in k(C)$, we get that $N_{k(C)/k(x)}(\phi) = h_1(x)^2 - h_2(x)^2 f(x)$. ♣

5.5. **Example.** Let k be a field and let $f \in k[x]$ be a monic polynomial of degree n; consider $A = k[x]/\langle f\rangle$ and let θ be the image of x in A, then $(1, \theta, \theta^2, \dots, \theta^{n-1})$ is a k-basis of A. We have $N_{A/k}(a - \theta) = f(a)$ for all $a \in k$. One way of seeing this is to realize that the matrix of m_θ with respect to the basis above is the companion matrix of f, whose characteristic polynomial is just f. Now let $s(\theta) \in A$ be arbitrary, where $s \in k[x]$. Working over $\bar{k}$, we can write $s = c\prod_{j=1}^m (x - \sigma_j)$ and $f = \prod_{i=1}^n (x - \theta_i)$. Then

EXAMPLE norm

$$\begin{aligned} N_{A/k}(s(\theta)) &= c^n \prod_{j=1}^m N_{\bar{A}/\bar{k}}(\theta - \sigma_j) \\ &= (-1)^{mn} c^n \prod_{j=1}^m f(\sigma_j) = c^n \prod_{j=1}^m \prod_{i=1}^n (\theta_i - \sigma_j) = \prod_{i=1}^n s(\theta_i) \end{aligned}$$

is the *resultant* $\operatorname{Res}(s, f)$ of s and f. ♣

For the following, note that the homomorphism $\delta\colon J(\mathbb{Q}) \to A^\times/(A^\times)^2$ can be constructed in the same way for any other field k (not of characteristic 2) in place of $\mathbb{Q}$.

Also note that since the norm is multiplicative, we get an induced homomorphism $A^\times/(A^\times)^2 \to k^\times/(k^\times)^2$, which we again denote by $N_{A/k}$.

5.6. **Lemma.** *Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of odd degree over a field k, with Jacobian J, and define $A = k[x]/\langle f\rangle$ and $\delta\colon J(k) \to A^\times/(A^\times)^2$ as above. Then the image of δ is contained in the kernel of the homomorphism $N_{A/k}\colon A^\times/(A^\times)^2 \to k^\times/(k^\times)^2$.*

LEMMA im of δ in kernel of norm

Proof. We can represent any point $P \in J(k)$ in the form $[D - \deg(D)\cdot\infty]$, where D is a divisor in general position avoiding the ramification points in its support (we do not assume that $\deg(D) \le g$ here). Let (a, b) be the Mumford representation of D. Then, with $a = \prod_{j=1}^d (x - \xi_j)$ and using Example 5.5 above,

$$N_{A/k}(\delta(D)) = N_{A/k}((-1)^d a(\theta)) = \prod_{j=1}^d f(\xi_j) = \prod_{j=1}^d b(\xi_j)^2 = \operatorname{Res}(b, a)^2$$

is a (non-zero) square in k, which is equivalent to saying that $N_{A/k}(P)$ is trivial. ❑

We now consider a hyperelliptic curve C of odd degree over $\mathbb{Q}$ again. Write H for the kernel of $N_{A/k}\colon A^\times/(A^\times)^2 \to k^\times/(k^\times)^2$. For a prime p, we set $A_p = \mathbb{Q}_p[x]/\langle f\rangle$ and H_p for the corresponding kernel. We extend this to $p = \infty$, where $\mathbb{Q}_\infty = \mathbb{R}$. The inclusion $\mathbb{Q} \to \mathbb{Q}_p$ induces a homomorphism $\rho_p\colon H \to H_p$. We write δ_p for the map $J(\mathbb{Q}_p) \to H_p$ (which is the δ map for C considered as a curve over $\mathbb{Q}_p$).

5.7. **Definition.** Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of odd degree over $\mathbb{Q}$, with Jacobian J. With the notations just introduced, we define the *2-Selmer group of J* to be

DEF 2-Selmer group

$$\operatorname{Sel}^{(2)}(J) = \{\alpha \in H \mid \forall p\colon \rho_p(\alpha) \in \operatorname{im}(\delta_p)\}\,. \qquad \diamondsuit$$

The 2-Selmer group gives us an upper bound on the rank r as the following result shows.

5.8. **Theorem.** *Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of odd degree over $\mathbb{Q}$, with Jacobian J. Then $\delta(J(\mathbb{Q})) \subset \mathrm{Sel}^{(2)}(J)$, and the 2-Selmer group is finite and computable.*

THM 2-Selmer group is finite

Proof. For every p (a prime or ∞), we have the following commutative diagram:

$$\begin{array}{ccc} J(\mathbb{Q}) & \xrightarrow{\delta} & H \\ \downarrow & & \downarrow{\scriptstyle \rho_p} \\ J(\mathbb{Q}_p) & \xrightarrow{\delta_p} & H_p \end{array}$$

This shows that for all $P \in J(\mathbb{Q})$ and all p, $\rho_p(\delta(P)) = \delta_p(P)$, so $\delta(P) \in \mathrm{Sel}^{(2)}(J)$.

We give the proof of the finiteness of the Selmer group in the special case that f splits into linear factors over $\mathbb{Q}$. The general case is essentially similar; it uses finiteness results for algebraic number fields (the group of units of the ring of integers is finitely generated, the ideal class group is finite) that are trivial for $\mathbb{Q}$. So assume that f splits completely over $\mathbb{Q}$. By scaling the variables, we can assume that f is monic and all its roots are integers; let $t_1, \dots, t_{2g+1}$ be the roots. Then $A \cong \mathbb{Q}^{2g+1}$, and the canonical map $\mathbb{Q}[x] \to A$ is simply $s \mapsto (s(t_1), \dots, s(t_{2g+1}))$, the norm map is $(a_1, \dots, a_{2g+1}) \mapsto a_1 \cdots a_{2g+1}$, so

$$H = \{(\alpha_1, \dots, \alpha_{2g+1}) : \alpha_1, \dots, \alpha_{2g+1} \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \alpha_1 \cdots \alpha_{2g+1} = 1\}\,.$$

An element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ can be uniquely represented by a squarefree integer. Let H' be the subgroup of H such that the squarefree integers representing the components of its elements are only divisible by primes dividing $t_j - t_i$ for some $1 \le i < j \le 2g+1$ (note: this includes the prime 2, since there must be two of the t_j that have the same parity). Then H' is clearly finite. So to prove that the Selmer group is finite, it suffices to show that it is contained in H'. This follows from the following statement: If p does not divide any of the differences $t_i - t_j$, then the image of δ_p is contained in the subgroup of H_p whose elements can be represented by tuples of p-adic units. (Note that $\rho_p(\alpha)$ is in that subgroup if and only if α can be represented using squarefree integers not divisible by p.) So let $P \in J(\mathbb{Q}_p)$, represented by $D - \deg(D)\cdot\infty$ with D in general position and avoiding the ramification points and with Mumford representation (a, b). Then $\delta_p(D) = \pm(a(t_1), \dots, a(t_{2g+1}))$. We can assume that a is irreducible (otherwise factor a and write D as a sum of divisors (a_j, b)). If a has coefficients in $\mathbb{Z}_p$, then $a(t_j)$ can be divisible by p for at most one j (otherwise a factors by the factorization version of Hensel's Lemma). So for all but at most one j, $v_p(a(t_j)) = 0$, and since the sum of the valuations must be even (this comes from the 'kernel of the norm' condition), all of them are even, so the $a(t_j)$ are units up to square factors. If a has non-integral coefficients, then one can show that all roots of a in $\bar{\mathbb{Q}}_p$ have the same negative valuation (one can extend v_p uniquely to $v_p\colon \bar{\mathbb{Q}}_p^\times \to \mathbb{Q}$), which implies that all $a(t_j)$ have the same (negative) valuation. Since there is an odd number of roots of f and the sum of the valuations must be even, each individual valuation is even, which is what we need.

For the computability, one shows that for the p discussed above, the image $\delta_p(J(\mathbb{Q}_p))$ is indeed exactly the subgroup represented by units, which means that the conditions from these primes amount exactly to the condition $\alpha \in H'$. It remains to find the conditions coming from the remaining primes (including ∞). The key to

this is the formula

$$\dim_{\mathbb{F}_2} \delta_p(J(\mathbb{Q}_p)) = \dim_{\mathbb{F}_2} J(\mathbb{Q}_p)[2] + \begin{cases} 0 & \text{if } p \neq 2, \infty, \\ g & \text{if } p = 2, \\ -g & \text{if } p = \infty. \end{cases}$$

(This formula also implies the statement about the image of δ_p at the 'good' primes, since it shows that the image has the same dimension as the subgroup coming from the units.) For $p \neq 2, \infty$, this follows from the fact that $J(\mathbb{Q}_p)$ has a finite-index subgroup isomorphic to $\mathbb{Z}_p^g$ (which can be taken to be the kernel of reduction $J(\mathbb{Q}_p)_1$ if p is a good prime): Let Q be the quotient group. Since 2 is invertible in $\mathbb{Z}_p$, we get that

$$\delta_p(J(\mathbb{Q}_p)) \cong J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \cong Q/2Q \cong Q[2] \cong J(\mathbb{Q}_p)[2]\,,$$

where the isomorphism $Q/2Q \cong Q[2]$ is not canonical and uses that Q is finite. For $p = 2$, one gets an adjustment of g coming from the fact that $\mathbb{Z}_2/2\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z}$. For $p = \infty$, one can check the formula fairly directly. In any case, knowing the dimension of the image (recall that $\dim_{\mathbb{F}_2} J(k)[2]$ can be computed from the factorization of f; if f splits completely, then this is $2g$), it suffices to compute δ_p of randomly chosen points in $J(\mathbb{Q}_p)$ until the images generate a subspace of the correct dimension. This gives us the image of δ_p in H_p; then the computation of the Selmer group as a subgroup of H' is a matter of linear algebra. ❑

EXAMPLE 2-Selmer group

5.9. **Example.** Consider $C\colon y^2 = x(x-1)(x-2)(x-5)(x-6)$. The primes dividing differences of the roots are $p = 2, 3, 5$. The image of $J(\mathbb{Q})[2]$ in H' is generated by

$$(15, -1, -2, -5, -6),\ (1, -5, -1, -1, -5),\ (2, 1, 6, -3, -1),\ (5, 1, 3, -15, -1)$$

(we can evaluate $-a = t_j - x$ at all other t_j; then we use that the product of the entries must be a square). The image of δ_∞ has dimension 2; it is generated by

$$(1, -1, -1, -1, -1) \qquad \text{and} \qquad (1, 1, 1, -1, -1)\,;$$

this tells us which combinations of signs are possible for elements of the Selmer group.

The image of $J(\mathbb{Q})[2]$ under δ_3 is generated by (using $1, -1, 3, -3$ as representatives of $\mathbb{Q}_3^\times/(\mathbb{Q}_3^\times)^2$)

$$(-3, -1, 1, 1, 3),\quad (1, 1, -1, -1, 1),\quad (-1, 1, -3, -3, -1),\quad (-1, 1, 3, 3, -1)\,;$$

these elements generate a subspace of dimension 3, so we need another generator. Since $f(3) = 3 \cdot 2 \cdot 1 \cdot (-2) \cdot (-3) = 36$, there is a point $(3, 6) \in C(\mathbb{Q})$ giving $P = [(3, 6) - \infty] \in J(\mathbb{Q})$; the image of P under δ_3 is $(3, -1, 1, 1, -3)$, which is independent of the known subspace. We can deduce that the image of δ surjects onto the image of δ_3 (since our generators of this image all come from points in $J(\mathbb{Q})$). Any element in $\mathrm{Sel}^{(2)}(J)$ must therefore have the form $\alpha\beta$ with α in the subgroup generated by the images of the known rational points under δ and $\beta \in \ker(\rho_3)$; the condition for being in $\mathrm{Sel}^{(2)}(J)$ is that $\rho_p(\beta) \in \mathrm{im}(\delta_p)$ for $p = \infty, 2, 5$.

The image of the known points in $J(\mathbb{Q})$ under δ_5 is generated by (we use $1, 2, 5, 10$ as representatives; note that $\delta(P) = (3, 2, 1, -2, -3)$)

$$(10, 1, 2, 5, 1),\ (1, 5, 1, 1, 5),\ (2, 1, 1, 2, 1),\ (5, 1, 2, 10, 1),\ (2, 2, 1, 2, 2)\,;$$

this already gives a 4-dimensional space. Now one checks that $\mathrm{Sel}^{(2)}(J) \cap \ker(\rho_3)$ is trivial (the conditions at $p = \infty$ and $p = 5$ are satisfied only for $\beta = 1$), which implies that $\mathrm{Sel}^{(2)}(J) = \mathrm{im}(\delta)$ is generated by $\delta(J(\mathbb{Q})[2])$ and $\delta(P)$. We conclude that $J(\mathbb{Q})$ has rank 1. Since $\#\bar{J}(\mathbb{F}_7) = 3 \cdot 16$ and $\#\bar{J}(\mathbb{F}_{11}) = 11 \cdot 16$, we see that $J(\mathbb{Q})_{\mathrm{tors}} = J(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$, so

$$J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}\,,$$

and P is a point of infinite order that is not in $2J(\mathbb{Q}) + J(\mathbb{Q})[2]$.

One nice feature of this example is that it was not necessary to find the image of δ_2, which is usually more involved, but also usually gives most of the information. ♣

EXAMPLE 2-Selmer group

5.10. **Example.** Consider $C\colon y^2 = x^5 + 1 = (x+1)(x^4 - x^3 + x^2 - x + 1)$. Here $A \cong \mathbb{Q} \times \mathbb{Q}(\zeta)$ where ζ is a primitive fifth root of unity. The 'ring of integers' of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$; this is a principal ideal domain. The bad primes are 2 and 5. The group H can be identified with $\mathbb{Q}(\zeta)^\times/(\mathbb{Q}(\zeta)^\times)^2$ (the component in $\mathbb{Q}$ is uniquely determined by the requirement that the element is in the kernel of the norm). H' can be taken to be $\langle -1, 2, 1+\zeta, 1-\zeta\rangle$ ($1+\zeta$ generates the free part of the unit group of $\mathbb{Z}[\zeta]$, 2 stays prime and $1-\zeta$ generates the unique prime ideal dividing 5 in $\mathbb{Z}[\zeta]$). Computing the images of δ_2 and δ_5 (δ_∞ is trivial), we find that $\mathrm{Sel}^{(2)}(J) = \delta(J(\mathbb{Q})[2])$ (note that $J(\mathbb{Q})[2]$ has order 2 and is generated by $[(-1,0) - \infty]$) and therefore that $J(\mathbb{Q})$ has rank zero. We know from Example 4.22 that $J(\mathbb{Q})_{\mathrm{tors}}$ has order 10, so we deduce that $J(\mathbb{Q}) \cong \mathbb{Z}/10\mathbb{Z}$. Enumerating these ten points and checking which of them can be written as $[P - \infty]$ with $P \in C$ then shows that $C(\mathbb{Q}) = \{\infty, (-1,0), (0,1), (0,-1)\}$, as announced earlier in Example 2.3. More precisely, the ten points in $J(\mathbb{Q})$ have Mumford representation (these are the multiples $n \cdot P$ for $n = 0, 1, \ldots, 9$ where $P = (x^2 + x, x + 1)$ is one of the points of order 10)

$$(1,0), \quad (x^2+x, x+1), \quad (x^2, 1), \quad (x^2 - 2x + 2, -2x + 3), \quad (x, -1),$$
$$(x+1, 0), \quad (x, 1), \quad (x^2 - 2x + 2, 2x - 3), \quad (x^2, -1), \quad (x^2 + x, -x - 1).$$

The relevant ones are those with $\deg(a) \le 1$:

$$(1,0) \leftrightarrow \infty, \quad (x,-1) \leftrightarrow (0,-1), \quad (x+1,0) \leftrightarrow (-1,0), \quad (x,1) \leftrightarrow (0,1). \quad ♣$$

6. Differentials and Chabauty's Method

Differentials on curves are the algebraic analogue of smooth 1-forms in differential geometry. We list the most important facts and properties.

DEF differential

6.1. **Definition.** Let C be a smooth and irreducible curve over a field k. The *space of differentials* on C (over k) is a one-dimensional $k(C)$-vector space $\Omega_C(k)$. There is a nontrivial k-linear derivation $d\colon k(C) \to \Omega_C(k)$ (meaning that d is k-linear and satisfies $d(fg) = f\,dg + g\,df$ for all $f, g \in k(C)$ and that there is some $f \in k(C)$ such that $df \neq 0$). The elements of $\Omega_C(k)$ are called *differentials* on C. ♢

A general differential can therefore be written in the form $\omega = f\,dg$ where $g \in k(C)$ with $dg \neq 0$; fixing g, this representation is unique. If $\omega, \omega' \in \Omega_C(k)$ with $\omega' \neq 0$, then there is a unique $f \in k(C)$ such that $\omega = f\omega'$; we write $\omega/\omega' = f$.

In a similar way as for functions, we can associate to a nonzero differential a divisor.

DEF divisor of a differential

6.2. **Definition.** Let $0 \neq \omega \in \Omega_C(k)$ and let $P \in C(k)$; pick a uniformizer $t \in k(C)$ at P. Then $v_P(\omega) = v_P(\omega/dt)$ is the *valuation* of ω at P. This valuation is nonzero for only finitely many points $P \in C(\bar{k})$; the divisor

$$\operatorname{div}(\omega) = \sum_{P \in C(\bar{k})} v_P(\omega) \cdot P \in \operatorname{Div}_C(k)$$

is the *divisor of* ω. If $v_P(\omega) \geq 0$ (or $\omega = 0$), then ω is said to be *regular* at P, and ω is *regular*, if it is regular at all points $P \in C(\bar{k})$. ♢

DEF canonical class/ divisor

Since the quotient of any two nonzero differentials is a function, the difference of any two divisors of differentials is a principal divisor. This implies that the divisors of differentials form one linear equivalence class of divisors, the *canonical class*. Each such divisor is a canonical divisor. One can show that this class is exactly the class of the divisors W in the Riemann-Roch Theorem. In particular, $\deg \operatorname{div}(\omega) = 2g - 2$ for $\omega \neq 0$, and the k-vector space of regular differentials has dimension $\dim L(W) = g$. We write $\Omega_C^{\mathrm{reg}}(k)$ for this space.

LEMMA regular differentials on hyp. curves

6.3. **Lemma.** *Let $C\colon y^2 = f(x)$ be a hyperelliptic curve of genus g over k. Then the space of regular differentials on C has k-basis*

$$\frac{dx}{2y}, \quad \frac{x\,dx}{2y}, \quad \frac{x^2\,dx}{2y}, \quad \dots, \quad \frac{x^{g-1}\,dx}{2y},$$

so every regular differential can be written uniquely as $p(x)\,dx/2y$ with a polynomial p of degree $\leq g - 1$.

Proof. Consider $\omega_0 = dx/(2y)$. We show that $\operatorname{div}(\omega_0) = (g-1)D_\infty$, where D_∞ is the divisor of poles of x. ($D_\infty = 2 \cdot \infty$ if $\deg(f)$ is odd, and is the sum of the two points at infinity otherwise.) So let $P = (\xi, \eta) \in C_{\mathrm{aff}}(\bar{k})$. If $\eta \neq 0$, then $t = x - \xi$ is a uniformizer at P, and $dt = dx$, so $v_P(\omega_0) = v_P(1/(2y)) = 0$, since y does not vanish at P. If $\eta = 0$, then $t = y$ is a uniformizer at P. The relation $y^2 = f(x)$ implies $2y\,dy = f'(x)\,dx$, so

$$\frac{\omega_0}{dt} = \frac{dx}{2y\,dy} = \frac{1}{f'(x)},$$

and $v_P(\omega_0) = v_P(1/f'(x)) = 0$, since $f'(\xi) \neq 0$ (otherwise f would have a multiple zero at ξ). It remains to deal with the point(s) at infinity. First assume that $\deg(f)$ is even; then $t = 1/x$ is a uniformizer at both points at infinity. We find (using $dt = -x^{-2}\,dx$)

$$v_P(\omega_0) = v_P\Big(\frac{dx}{2y\,dt}\Big) = -v_P(y) + v_P(x^2) = (g+1) - 2 = g - 1$$

as claimed. Finally, if $\deg(f)$ is odd, then $t = y/x^{g+1}$ is a uniformizer at $P = \infty$. We have

$$dt = -(g+1)\frac{y}{x^{g+2}}\,dx + \frac{1}{x^{g+1}}\,dy = \frac{-2(g+1)f(x) + xf'(x)}{2x^{g+2}y}\,dx\,,$$

so

$$\frac{\omega_0}{dt} = \frac{x^{g+2}}{-2(g+1)f(x) + xf'(x)}\,.$$

The polynomial in the denominator has degree $2g+1$ (the leading coefficient is not canceled), so $v_P(\omega_0) = -v_P(x^{1-g}) = 2g - 2$ as claimed.

Writing a general differential as $\omega = \phi\omega_0$ with $\phi \in k(C)$, this implies that ω is regular if and only if $\phi \in L((g-1)D_\infty)$. This space is generated by $1, x, x^2, \dots, x^{g-1}$ (compare Example 4.13 for the odd degree case): these functions are clearly contained in it, and we know that its dimension must be g. ❑

Differentials want to be integrated. You know from complex analysis or from differential geometry that regular 1-forms can be integrated along paths and that in favorable circumstances the integral depends only on the endpoints and not on the path. This is not true in general, however, if we integrate our differentials over paths in $C(\mathbb{R})$ or $C(\mathbb{C})$ — integrating around a loop that cannot be contracted may result in a nonzero value. Over the p-adic numbers, however, there is a nice integration theory available.

6.4. **Theorem.** *Let C be a smooth, projective, absolutely irreducible curve over $\mathbb{Q}_p$, of good reduction. Then there is an integral $\int_P^Q \omega \in \bar{\mathbb{Q}}_p$ defined for each pair of points $P, Q \in C(\bar{\mathbb{Q}}_p)$ and each regular differential $\omega \in \Omega^{\mathrm{reg}}_C(\bar{\mathbb{Q}}_p)$ that satisfies the following properties.* **THM** Coleman integration

(1) The integral is $\bar{\mathbb{Q}}_p$-linear in ω.

(2) If P and Q both reduce to the same point $\bar{P} \in \bar{C}(\bar{\mathbb{F}}_p)$, the the integral can be evaluated by writing $\omega = w(t)\,dt$ with t a uniformizer at P reducing to a uniformizer at $\bar{P}$ and w a power series, then integrating w formally, obtaining a power series ℓ such that $d\ell(t) = w(t)\,dt$ and $\ell(0) = 0$, and finally evaluating $\ell(t(Q))$ (which converges). This implies that $\int_P^P \omega = 0$.

(3) $$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega.$$

It then makes sense to define $\int^D \omega$ for a divisor $D = \sum_{j=1}^n (Q_j - P_j) \in \mathrm{Div}^0_C(\bar{\mathbb{Q}}_p)$ as

$$\int^D \omega = \sum_{j=1}^n \int_{P_j}^{Q_j} \omega\,.$$

(4) If D is a principal divisor, then $\int^D \omega = 0$.

(5) *The integral is compatible with the action of the absolute Galois group of* $\mathbb{Q}_p$.

(6) *Fix* $P_0 \in C(\bar{\mathbb{Q}}_p)$. *If* $0 \neq \omega \in \Omega^{\mathrm{reg}}_C(\bar{\mathbb{Q}}_p)$, *then the set of points* $P \in C(\bar{\mathbb{Q}}_p)$ *reducing to a fixed point on* $\bar{C}(\bar{\mathbb{F}}_p)$ *as* P_0 *and such that* $\int_{P_0}^{P} \omega = 0$ *is finite.*

Proof. We do not prove this here. This integration theory was introduced[7] by Robert Coleman, who died recently in March 2014. ❑

We remark that the assumption that the curve has good reduction is not really necessary, but it simplifies the statement of property (2) above.

6.5. **Corollary.** *In the situation of Theorem 6.4, let* $P_0 \in C(\mathbb{Q}_p)$, *let* J *be the Jacobian of* C *and* $i\colon C \to J$ *the embedding given by* P_0. *There is a map*

$$J(\mathbb{Q}_p) \times \Omega^{\mathrm{reg}}_C(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p\,, \qquad (P, \omega) \longmapsto \langle P, \omega \rangle$$

that is additive in P *and* $\mathbb{Q}_p$*-linear in* ω, *which is given by* $\langle [D], \omega \rangle = \int^D \omega$. *In particular, we have*

$$\langle i(P), \omega \rangle = \int_{P_0}^{P} \omega\,.$$

COR integration pairing

Proof. By Theorem 6.4, we obtain a map

$$\mathrm{Div}^0_C(\bar{\mathbb{Q}}_p) \times \Omega^{\mathrm{reg}}_C(\bar{\mathbb{Q}}_p) \longrightarrow \bar{\mathbb{Q}}_p\,, \qquad (D, \omega) \longmapsto \int^{D} \omega$$

that is additive on the left and $\bar{\mathbb{Q}}_p$-linear on the right. Since $\int^D \omega = 0$ for every ω when D is a principal divisor, this induces a map $J(\bar{\mathbb{Q}}_p) \times \Omega^{\mathrm{reg}}_C(\bar{\mathbb{Q}}_p) \longrightarrow \bar{\mathbb{Q}}_p$. The compatibility of integration with the Galois action then implies that this map descends to the map whose existence is claimed in the statement. ❑

Note that if $P \in J(\mathbb{Q}_p)$ has finite order, then $\langle P, \omega \rangle = 0$ for all ω (if $nP = 0$, then $\langle P, \omega \rangle = \frac{1}{n}\langle nP, \omega \rangle = 0$). One can in fact show that the torsion points are the only points with that property. On the other hand, the last property in Theorem 6.4 implies that if ω has the property that $\langle P, \omega \rangle = 0$ for all $P \in J(\mathbb{Q}_p)$, then $\omega = 0$.

6.6. **Corollary.** *Let* C *be a smooth, projective and absolutely irreducible curve of genus* g *over* $\mathbb{Q}$, *with Jacobian* J. *Assume that the rank* r *of the Mordell-Weil group* $J(\mathbb{Q})$ *is strictly less than* g. *Then* $C(\mathbb{Q})$ *is finite.*

COR finiteness of $C(\mathbb{Q})$

This special case of Faltings' Theorem (formerly Mordell's Conjecture) was proved by Chabauty in 1941[8] by related methods. (Note that one does not require $g \geq 2$ here: the statement is true for $g = 1$ when $r = 0$, and $g = 0$ is ruled out by the assumption $r < g$.)

[7] Robert F. Coleman: *Torsion points on curves and p-adic abelian integrals,* Ann. Math. (2) **121**, 111–168 (1985).

[8] Claude Chabauty: *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité,* C. R. Acad. Sci., Paris **212**, 882–885 (1941).

Proof. Pick a prime p of good reduction for C and let

$$V = \{\omega \in \Omega^{\mathrm{reg}}_C(\bar{\mathbb{Q}}_p) \mid \forall P \in J(\mathbb{Q})\colon \langle P, \omega\rangle = 0\}\,.$$

Since the condition is equivalent to requiring $\langle P_j, \omega\rangle = 0$ for a basis $P_1, \dots, P_r$ of the free part of $J(\mathbb{Q})$ (this comes from the additivity of the integration pairing in the first argument), it leads to at most r linear constraints, so $\dim V \geq g - r > 0$. So there is some $0 \neq \omega \in V$. Pick $P_0 \in C(\mathbb{Q})$ (if $C(\mathbb{Q})$ is empty, the claim is trivially true) to define $i\colon C \to J$. Since $i(P) \in J(\mathbb{Q})$ for all $P \in C(\mathbb{Q})$, it follows that $\int_{P_0}^{P} \omega = 0$ for all $P \in C(\mathbb{Q})$. By Theorem 6.4, the number of such P is finite in each 'residue class' of $C(\mathbb{Q}_p)$ (meaning a set of points in $C(\mathbb{Q}_p)$ reducing to the same point in $C(\mathbb{F}_p)$). Since the number of residue classes is $\#\bar{C}(\mathbb{F}_p) < \infty$, the total number of rational points on C must be finite as well. ❑

We now want to give a more precise statement. For this, we need a bound on the number of zeros in $\mathbb{Z}_p$ of a power series with coefficients in $\mathbb{Q}_p$. We first prove a statement on p-adic power series.

6.7. **Theorem.** *Let $0 \neq \ell(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbb{Q}_p[\![t]\!]$ such that $a_n \to 0$ as $n \to \infty$ in the p-adic topology. Let*

$$v_0 = \min\{v_p(a_n) : n \geq 0\} \quad \textit{and} \quad N = \max\{n \geq 0 : v_p(a_n) = v_0\}\,.$$

Then there is a constant $c \in \mathbb{Q}_p^{\times}$, a monic polynomial $q \in \mathbb{Z}_p[t]$ of degree N and a power series $h(t) = \sum_{n=0}^{\infty} b_n t^n \in 1 + pt\mathbb{Z}_p[\![t]\!]$ with $b_n \to 0$ as $n \to \infty$ such that

$$\ell(t) = cq(t)h(t)\,.$$

THM factorization of power series

Proof. After scaling by a_N^{-1}; we can assume that $v_0 = 0$ and $a_N = 1$, so that in particular $\ell(t) \in \mathbb{Z}_p[\![t]\!]$. The condition $a_n \to 0$ means that the image $\ell_m(t)$ of $\ell(t)$ in $(\mathbb{Z}/p^m\mathbb{Z})[\![t]\!]$ is actually a polynomial, for every $m \geq 1$. We construct inductively constants $c_m \in (\mathbb{Z}/p^m\mathbb{Z})^{\times}$, monic polynomials $q_m(t) \in (\mathbb{Z}/p^m\mathbb{Z})[t]$ of degree N and polynomials $h_m(t) \in (\mathbb{Z}/p^m\mathbb{Z})[t]$ with $h_m(t) \equiv 1 \bmod pt$ satisfying $\ell_m(t) = c_m q_m(t) h_m(t)$ and such that $(c_{m+1}, q_{m+1}(t), h_{m+1}(t))$ reduce mod p^m to $(c_m, q_m(t), h_m(t))$. There are then unique $c \in \mathbb{Z}_p^{\times}$, $q(t) \in \mathbb{Z}_p[t]$ monic of degree N and $h(t) \in 1 + pt\mathbb{Z}_p[\![t]\!]$ such that $(c, q(t), h(t))$ reduces mod p^m to $(c_m, q_m(t), h_m(t))$ for all m; the claim then follows.

To start the induction, we set $c_1 = 1$, $q_1(t) = \ell_1(t)$ and $h_1(t) = 1$. This is possible, since $\ell_1(t)$ is a monic polynomial of degree N. Now assume we have already constructed c_m, $q_m(t)$ and $h_m(t)$. Let $\tilde{c}_{m+1}$, $\tilde{q}_{m+1}(t)$ and $\tilde{h}_{m+1}$ be arbitrary lifts of c_m, $q_m(t)$ and $h_m(t)$ to objects over $\mathbb{Z}/p^{m+1}\mathbb{Z}$ (with q_{m+1} monic of degree N and $\tilde{h}_{m+1}(t) \equiv 1 \bmod pt$). Then

$$\ell_{m+1}(t) - \tilde{c}_{m+1}\tilde{q}_{m+1}(t)\tilde{h}_{m+1}(t) = p^m d(t)$$

with some $d(t) \in (\mathbb{Z}/p\mathbb{Z})[t]$. We must have

$$c_{m+1} = \tilde{c}_{m+1} + p^m\gamma,\ q_{m+1}(t) = \tilde{q}_{m+1}(t) + p^m\kappa(t) \text{ and } h_{m+1}(t) = \tilde{h}_{m+1}(t) + p^m\eta(t),$$

with $\gamma \in \mathbb{Z}/p\mathbb{Z}$, $\kappa(t) \in (\mathbb{Z}/p\mathbb{Z})[t]$ of degree $< N$ and $\eta(t) \in (\mathbb{Z}/p\mathbb{Z})[t]$ with $\eta(0) = 0$. The desired relation $\ell_{m+1}(t) = c_{m+1}q_{m+1}(t)h_{m+1}(t)$ is then equivalent to

$$d(t) = (\gamma + \eta(t))\ell_1(t) + \kappa(t)\,.$$

We obtain γ, $\kappa(t)$ and $\eta(t)$ (uniquely) from a division with remainder of the polynomial $d(t)$ by $\ell_1(t)$. This concludes the inductive step and finishes the proof. ❑

The statement can be considered as a variant of the factorization version of Hensel's Lemma.

6.8. **Corollary.** *Let $\ell(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbb{Q}_p[\![t]\!]$ such that $a_n \to 0$ as $n \to \infty$ in the p-adic topology. (Then ℓ converges on $\mathbb{Z}_p$.) Let $v_0 = \min\{v_p(a_n) : n \geq 0\}$ and $N = \max\{n \geq 0 : v_p(a_n) = v_0\}$. Then*

COR roots of a power series

$$\#\{\tau \in \mathbb{Z}_p : \ell(\tau) = 0\} \leq N\,.$$

Proof. By Theorem 6.7, we can write $\ell(t) = cq(t)h(t)$ with a constant $c \in \mathbb{Q}_p^\times$, a monic polynomial $q \in \mathbb{Z}_p[t]$ of degree N and a power series $h(t) \in 1 + pt\mathbb{Z}_p[\![t]\!]$. Since h never vanishes on $\mathbb{Z}_p$, the roots of ℓ are exactly the roots of q, of which there are at most N. ❑

More precisely, the number of roots $\alpha \in \bar{\mathbb{Q}}_p$ of ℓ such that $v_p(\alpha) \geq 0$, counted with multiplicity, is exactly N: For $\tau \in \bar{\mathbb{Q}}_p$ with $v_p(\tau) \geq 0$ we have $h(\tau) \neq 0$, so the roots are exactly the roots α of q, which all have the property that $v_p(\alpha) \geq 0$ (by the ultrametric triangle inequality).

Note that the p-adic valuation on $\mathbb{Q}_p^\times$ can be uniquely extended to a homomorphism $v_p\colon \bar{\mathbb{Q}}_p^\times \to \mathbb{Q}$. (If $\alpha \in \bar{\mathbb{Q}}_p^\times$ with minimal polynomial $x^d + \ldots + a \in \mathbb{Q}_p[x]$, then set $v_p(\alpha) = v_p(a)/d$. Up to a sign, a is the norm of α with respect to the extension $\mathbb{Q}_p \subset \mathbb{Q}_p(\alpha)$.)

6.9. **Lemma.** *Let $\ell(t) \in \mathbb{Q}_p[\![t]\!]$, with formal derivative $w(t) \in \mathbb{Z}_p[\![t]\!]$ such that the image $\bar{w}(t) \in \mathbb{F}_p[\![t]\!]$ has the form $ut^\nu + \ldots$ with $u \in \mathbb{F}_p^\times$. Then ℓ converges on $p\mathbb{Z}_p$. If $p > \nu + 2$, then*

LEMMA roots of integrals

$$\#\{\tau \in p\mathbb{Z}_p : \ell(\tau) = 0\} \leq \nu + 1\,.$$

Proof. Write $w(t) = w_0 + w_1 t + w_2 t^2 + \ldots$ and $\ell(t) = \ell_0 + \ell_1 t + \ell_2 t^2 + \ldots$. Then $\ell_{n+1} = w_n/(n+1) \in \mathbb{Z}_p/(n+1)$. Since $v_p(n+1) \ll \log n$, the assumption $w_n \in \mathbb{Z}_p$ implies $v_p(\ell_n) \geq -c \log n$ with a constant c. If $\tau \in p\mathbb{Z}_p$ (so $v_p(\tau) \geq 1$), then $v_p(\ell_n \tau^n) \geq n - c \log n \to \infty$ as $n \to \infty$, hence $\ell(\tau)$ converges.

Now we consider $\ell(pt) = \ell_0 + p\ell_1 t + p^2 \ell_2 t^2 + \ldots$. We claim that in terms of the notation of Theorem 6.7, we have $N \leq \nu + 1$. Indeed, we have

$$v_p(p^{\nu+1}\ell_{\nu+1}) = \nu + 1 + v_p(w_\nu) - v_p(\nu+1) \leq \nu + 1\,,$$

and for $n > \nu$, we have

$$v_p(p^{n+1}\ell_{n+1}) = n + 1 + v_p(w_n) - v_p(n+1) \geq n + 1 - v_p(n+1)$$

(note that $v_p(w_\nu) = 0$ and $v_p(w_n) \geq 0$ for $n > \nu$), so that it suffices to show that $n - v_p(n+1) > \nu$. This is clear for $v_p(n+1) = 0$. Otherwise let $e = v_p(n+1)$, then $p^e \mid n+1$, so $n+1 \geq p^e > \nu + e + 1$, where the second estimate can be shown be induction: for $e = 1$, this is the assumption $p > \nu + 2$; then use $p^{e+1} \geq p^e + 1$.

Now Corollary 6.8 gives the desired result. ❑

We can use this to show the following.

6.10. **Theorem.** *Let C be a smooth, projective and absolutely irreducible curve of genus g over $\mathbb{Q}$, with Jacobian J. Assume that the rank r of the Mordell-Weil group $J(\mathbb{Q})$ is strictly less than g. Let p be a prime of good reduction for C such that $p > 2g$. Then*

$$\#C(\mathbb{Q}) \le \#\bar{C}(\mathbb{F}_p) + 2g - 2\,.$$

THM bound for $\#C(\mathbb{Q})$

This result is due to Coleman.[9]

Proof. We can assume that there is some point $P_0 \in C(\mathbb{Q})$. Arguing as in the proof of Corollary 6.6, there is a nonzero differential $\omega \in \Omega^{\mathrm{reg}}_C(\mathbb{Q}_p)$ such that $\int_{P_0}^{P} \omega = 0$ for all $P \in C(\mathbb{Q})$. Now consider a point $\bar{Q} \in \bar{C}(\mathbb{F}_p)$ and lift it to $Q \in C(\mathbb{Q}_p)$. We can pick a uniformizer $t \in \mathbb{Q}_p(C)^\times$ at Q such that t reduces to a uniformizer $\bar{t} \in \mathbb{F}_p(\bar{C})^\times$ at $\bar{Q}$. (For example, if C is hyperelliptic and $\bar{Q} = (\bar{\xi}, \bar{\eta})$, then we can take $Q = (\xi, \eta)$ and $t = x - \xi$ if $\bar{\eta} \ne 0$, and $Q = (\xi, 0)$ and $t = y$ if $\bar{\eta} = 0$.) We can scale ω such that its reduction $\bar{\omega}$ is defined and nonzero; then $\bar{\omega} \in \Omega^{\mathrm{reg}}_{\bar{C}}(\mathbb{F}_p)$. Recall that $\mathrm{div}(\bar{\omega})$ is effective and has degree $2g-2$. We write $\nu(\bar{Q})$ for $v_{\bar{Q}}(\bar{\omega})$. We can write $\omega = w(t)\,dt$ with a power series $w(t) \in \mathbb{Z}_p[\![t]\!]$ (the coefficients are in $\mathbb{Z}_p$, since $\bar{\omega}$ is defined); then $\bar{\omega} = \bar{w}(\bar{t})\,d\bar{t}$, where $\bar{w}(\bar{t}) = \bar{t}^{\nu(\bar{Q})}(u_0 + u_1\bar{t} + \ldots)$ with $u_0 \in \mathbb{F}_p^\times$. We also have $\int_{P_0}^{P} \omega = \ell(t(P))$ for $P \in C(\mathbb{Q}_p)$ such that $\bar{P} = \bar{Q}$, where $\ell(t) \in \mathbb{Q}_p[\![t]\!]$ is a power series such that $\ell'(t) = w(t)$. Now we apply Lemma 6.9 to ℓ and w; we find that the number of zeros of $\ell(t)$ (which is the number of points $P \in C(\mathbb{Q}_p)$ reducing to $\bar{Q}$ satisfying $\int_{P_0}^{P} \omega = 0$) is at most $\nu(\bar{Q}) + 1$. Adding up, we get

$$\begin{aligned}
\#C(\mathbb{Q}) &\le \#\Big\{P \in C(\mathbb{Q}_p) : \int_{P_0}^{P} \omega = 0\Big\} \\
&\le \sum_{\bar{Q} \in \bar{C}(\mathbb{F}_p)} (\nu(\bar{Q}) + 1) \le \deg \mathrm{div}(\bar{\omega}) + \#\bar{C}(\mathbb{F}_p) \\
&= 2g - 2 + \#\bar{C}(\mathbb{F}_p)\,.
\end{aligned}$$

❑

We make a few remarks.[10]

(1) By choosing the 'best' ω for each residue class, one can improve this: if $r < g$ and $p > 2r + 2$ is a prime of good reduction for C, then

$$\#C(\mathbb{Q}) \le \#\bar{C}(\mathbb{F}_p) + 2r\,.$$

(2) One can weaken the assumption that $p > 2r + 2$. If $p > 2$, then

$$\#C(\mathbb{Q}) \le \#\bar{C}(\mathbb{F}_p) + 2r + \left\lfloor \frac{2r}{p-2} \right\rfloor\,.$$

This refinement follows from a corresponding refinement of Lemma 6.9. For $p > 2r + 2$, we obtain the previous statement.

6.11. **Example.** We continue Example 5.9. Let

$$C\colon y^2 = x(x-1)(x-2)(x-5)(x-6)\,.$$

EXAMPLE

[9] R.F. Coleman: *Effective Chabauty*, Duke Math. J. **52**, 765–770 (1985).

[10] M. Stoll: *Independence of rational points on twists of a given curve,* Compositio Math. **142**, 1201–1214 (2006)

In Example 5.9, we had shown that $J(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}$. One finds the ten rational points

$$(0,0),\ (1,0),\ (2,0),\ (5,0),\ (6,0),\ (3,\pm 6) \quad \text{and} \quad (10,\pm 120)$$

on C. The prime $p = 7$ is a prime of good reduction for C, and

$$\bar{C}(\mathbb{F}_7) = \{\infty, (0,0), (1,0), (2,0), (-2,0), (-1,0), (3,\pm 1)\}$$

(note that $f(4) = -24$ is a non-square mod 7), so $\#\bar{C}(\mathbb{F}_7) = 8$. Theorem 6.10 tells us that (note that $g = 2$)

$$10 \le \#C(\mathbb{Q}) \le \#\bar{C}(\mathbb{F}_7) + 2 = 10\,.$$

Therefore

$$C(\mathbb{Q}) = \{(0,0), (1,0), (2,0), (5,0), (6,0), (3,6), (3,-6), (10,120), (10,-120)\}\,.$$

The fact that there are two rational points each in the residue classes coming from $(3,\pm 1) \in \bar{C}(\mathbb{F}_7)$ tells us that $\bar{\omega} = (x-3)\,dx/(2y)$, up to a constant factor. ♣

Usually, however, the bound in Theorem 6.10 (even in its improved versions) is not sharp. For large p, $\#\bar{C}(\mathbb{F}_p)$ grows roughly like p by the Weil bounds, so $\#\bar{C}(\mathbb{F}_p) + 2r$ will be larger than $\#C(\mathbb{Q})$ if p is sufficiently large. On the other hand, it is possible to rule out certain residue classes mod p by using information coming from other primes. To explain this, assume for simplicity that $J(\mathbb{Q}) \cong \mathbb{Z}^r$ has no torsion. Let q be a prime of good reduction. Fix $P_0 \in C(\mathbb{Q})$ to define an embedding $i\colon C \to J$. Then we have the following commutative diagram:

$$\begin{array}{ccccc} C(\mathbb{Q}) & \xrightarrow{i} & J(\mathbb{Q}) & \xrightarrow{\cong} & \mathbb{Z}^r \\ \downarrow{\scriptstyle \rho_q} & & \downarrow{\scriptstyle \rho_q} & \swarrow{\scriptstyle \phi_q} & \\ \bar{C}(\mathbb{F}_q) & \xrightarrow{i} & \bar{J}(\mathbb{F}_q) & & \end{array}$$

The image of $C(\mathbb{Q})$ in $\mathbb{Z}^r$ must then be contained in a union V_q of $\#\bar{C}(\mathbb{F}_q)$ cosets of $U_q = \ker(\phi_q)$ (since the image under ϕ_q of an element in $\mathbb{Z}^r$ that comes from a point in $C(\mathbb{Q})$ must map into $i\big(\bar{C}(\mathbb{F}_q)\big)$). If we have explicit generators of $J(\mathbb{Q})$, then we can compute U_q. If the indices $(\mathbb{Z}^r : U_q)$ and $(\mathbb{Z}^r : U_p)$ are not coprime, then the image of $V_q \cap V_p$ in $\mathbb{Z}^r/U_p \hookrightarrow \bar{J}(\mathbb{F}_p)$ can be smaller than that of V_p, which comes down to excluding certain points in $\bar{C}(\mathbb{F}_p)$ as possible images of rational points under ρ_p. One can as well use several primes q together and combine the information obtained from them. This approach is known as the 'Mordell-Weil Sieve'[11] and can be used independently of Chabauty's method, for example to show that $C(\mathbb{Q})$ is empty. In conjunction with Chabauty's method, it gives a quite powerful and (in the case $g = 2$, $r = 1$, say) efficient approach to determine $C(\mathbb{Q})$ explicitly.

Coming back to Theorem 6.10 and its variants, it is also possible to remove the condition that p be a prime of good reduction. Then one has to replace $\bar{C}(\mathbb{F}_p)$ by the number of smooth $\mathbb{F}_p$-points on 'the special fiber of a (minimal) proper regular model of C over $\mathbb{Z}_p$'. (If p is a good prime, then such a model is simply given by interpreting the equation defining C as an equation over $\mathbb{Z}_p$. Otherwise, the special fiber (which is the reduced curve over $\mathbb{F}_p$) has singularities, which one has to resolve to a certain extent to obtain a 'regular scheme' over $\mathbb{Z}_p$, which will then be a proper regular model.) This is of relevance when one tries to prove *uniform*

[11] N. Bruin, M. Stoll: *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math. **13**, 272–306 (2010).

bounds for the number of rational points on curves (when the rank of $J(\mathbb{Q})$ is strictly smaller than g): Since C could have bad reduction at all primes $p < X$ for X arbitrarily large, one would have to use arbitrarily large primes p if p must be a good prime. As discussed above, the bound grows with p, so that would not be useful. But even when fixing a prime p, there is the problem that the number of residue classes (i.e., the number of smooth $\mathbb{F}_p$-points on the special fiber of a minimal proper regular model of the curve over $\mathbb{Z}_p$) is unbounded. Still, there is the following recent result[12].

6.12. **Theorem.** *Let C be a hyperelliptic curve over $\mathbb{Q}$ of genus g and with Jacobian J. Assume that the rank r of $J(\mathbb{Q})$ satisfies $r \le g-3$. Then*

$$\#C(\mathbb{Q}) \le 8(r+4)(g-1) + \max\{1, 4r\} \cdot g\,.$$

THM uniform bound for $\#C(\mathbb{Q})$

The key idea for the proof is that one can partition $C(\mathbb{Q}_p)$ into a union of residue disks and 'residue annuli', whose number is bounded in terms of g only. We obtain a bound for the rational points lying in residue disks in the same way as above. For each residue annulus A, there is a codimension ≤ 2 subspace V_A of $\Omega^{\mathrm{reg}}_C(\mathbb{Q}_p)$ such that for $0 \ne \omega \in V_A$, one can bound the number of zeros of $P \mapsto \int_{P_0}^{P} \omega$ on A in terms of r and g. If $r \le g-3$, then each such space V_A contains a nonzero differential that kills $J(\mathbb{Q})$ under the integration pairing, and we get a bound for the number of rational points in A. Adding all the bounds (and working with $p = 3$) then leads to the result.

[12] M. Stoll: *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*, arXiv:1307.1773 [math.NT].