Algorithmic Number Theory in Function Fields

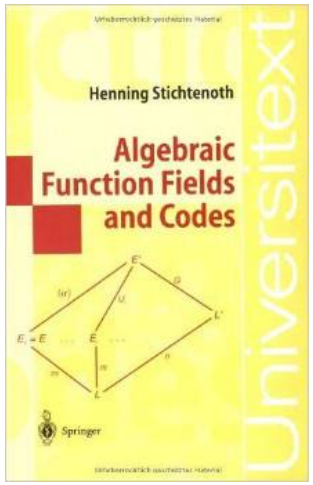
Renate Scheidler

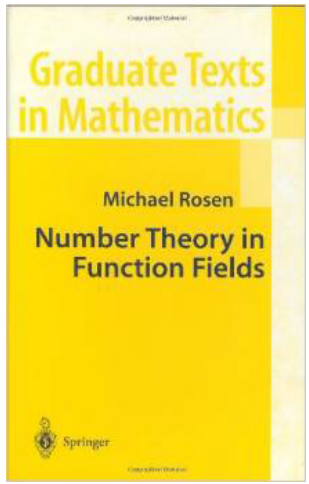
UNIVERSITY OF CALGARY

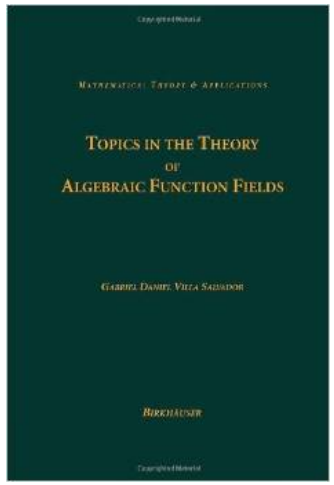
UNCG Summer School in Computational Number Theory 2016: Function Fields
May 30 – June 3, 2016

References

- Henning Stichtenoth, *Algebraic Function Fields and Codes*, second ed., GTM vol. 54, Springer 2009
- Michael Rosen, *Number Theory in Function Fields*, GTM vol. 210, Springer 2002
- Gabriel Daniel Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Birkhäuser 2006







Valuation Theory

Absolute Values

Throughout, let F be a field.

Definition

An absolute value on F is a map $|\cdot| : F \to \mathbb{R}$ such that for all $a, b \in F$:

- $|a| \geq 0$, with equality if and only if $a = 0$
- $|ab| = |a||b|$
- $|a + b| \leq |a| + |b|$ (archimedian) or
  $|a + b| \leq \max\{|a|, |b|\}$ (non-archimedian)

Examples

- The well-known absolute value on $\mathbb{Q}$ (or on $\mathbb{R}$ or on $\mathbb{C}$) is an archimedian absolute value in the sense of the above definition.
- The trivial absolute value on any field F, defined via $|a| = 0$ when $a = 0$ and $|a| = 1$ otherwise, is a non-archimedian absolute value.

p-Adic Absolute Values on $\mathbb{Q}$

Let p be ay prime number, and define a map $|\cdot|_p$ on $\mathbb{Q}$ as follows:

For $r \in \mathbb{Q}^*$, write $r = p^n \frac{a}{b}$ with $n \in \mathbb{Z}$ and $p \nmid ab$ and set

$$|r|_p = p^{-n}.$$

Then $|\cdot|_p$ is a non-archimedian absolute value on $\mathbb{Q}$, called the p-adic absolute value on $\mathbb{Q}$.

Theorem (Ostrowski)

The p-adic absolute values, along with the trivial and the ordinary absolute value, are the only valuations on $\mathbb{Q}$.

UNIVERSITY OF CALGARY

Notation

For any field K:

$K[x]$ denotes the ring of polynomials in x with coefficients in K.

$K(x)$ denotes the field of rational functions in x with coefficients in K:

$$K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ with } g(x) \neq 0 \right\}.$$

Note that $F = K(x)$ is our first example of an algebraic function field.
More formally:

Definition

A rational function field F/K is a field F of the form $F = K(x)$ where $x \in F$ is transcendental over K.

Absolute Values on $K(x)$

Fix a constant $c \in \mathbb{R}$, $c > 1$, and let $r(x) \in K(x)$ be nonzero.

p-adic absolute values on $K(x)$:
Let $p(x)$ be any monic irreducible polynomial in $K[x]$, and write $r(x) = p(x)^n a(x)/b(x)$ with $n \in \mathbb{Z}$ and $p(x) \nmid a(x)b(x)$. Define

$$|r(x)|_{p(x)} = c^{-n}.$$

Then $|\cdot|_{p(x)}$ is a non-archimedian absolute value on $K(x)$.

Infinite absolute value on $K(x)$:
Write $r(x) = f(x)/g(x)$ and define

$$|r(x)|_\infty = c^{\deg(f)-\deg(g)}.$$

Then $|\cdot|_\infty$ is a non-archimedian absolute value on $K(x)$.

Remarks on Absolute Values on $K(x)$

- These, plus the trivial absolute value, are essentially all the absolute values on $K(x)$, up to trivial modifications such as
  - using a different constant c,
  - using a different normalization on the irreducible polynomials $p(x)$.
- All absolute values on $K(x)$ are non-archimedian (different from $\mathbb{Q}$!)
- When $K = \mathbb{F}_q$ is a finite field of order q, one usually chooses $c = q$.
- When K is a field of characteristic 0, one usually chooses $c = e = 2.71828\ldots$.

Valuations

Definition

A valuation on F is a map $v : F \to \mathbb{R} \cup \{\infty\}$ such that for all $a, b \in F$:

- $v(a) = \infty$ if and only if $a = 0$
- $v(ab) = v(a) + v(b)$
- $v(a + b) \geq \min\{v(a), v(b)\}$

The pair (F, v) is called a valued field.

(Here, $\infty \geq \infty \geq n$ and $\infty + \infty = \infty + n = \infty$ for all $n \in \mathbb{Z}$.)

Remark

Let $c > 1$ be any constant. Then v is a valuation on F if and only if $|\cdot| := c^{-v(\cdot)}$ is a non-archimedian absolute value on F (with $c^{-\infty} := 0$).

Examples

- **Trivial valuation**: for any $a \in F$, define $v(a) = \infty$ when $a = 0$ and $v(a) = 0$ otherwise. Then v is a valuation on F.

- **p-adic valuations on $\mathbb{Q}$**: for any prime p and $r = p^n a/b \in \mathbb{Q}^*$, define $v_p(r) = n$. Then v_p is a valuation on $\mathbb{Q}$.

- **p-adic valuations on $K(x)$**: for any monic irreducible polynomial $p(x) \in K[x]$ and $r(x) = p(x)^n a(x)/b(x) \in K(x)^*$, define $v_{p(x)}(r(x)) = n$. Then $v_{p(x)}$ is a valuation on $K(x)$.

- **Infinite valuation on $K(x)$**: for $r(x) = f(x)/g(x) \in K(x)^*$, define $v_\infty(r(x)) = \deg(g) - \deg(f)$. Then v_∞ is a valuation on $K(x)$.

More on Valuations

Definition

A valuation v is discrete if it takes on values in $\mathbb{Z} \cup \{\infty\}$ and normalized if there exists an element $u \in F$ with $v(u) = 1$. Such an element u is a uniformizer (or prime element) for v.

Remarks

- All four valuations from the previous slide are discrete.
- Every p-adic valuation on $\mathbb{Q}$ is normalized with uniformizer p.
- Every p-adic valuation on $K(x)$ is normalized with uniformizer $p(x)$.
- The infinite valuation on $K(x)$ is normalized with uniformizer $1/x$.
- The p-adic and infinite valuations on $K(x)$ all satisfy $v(a) = 0$ for all $a \in K^*$. They constitute all the valuations on $K(x)$ with that property.

Remark

A discrete valuation is normalized if and only if it is surjective.

Valuation Rings

For a discretely valued field (F, v), define the following subsets of F:

$$O_v = \{a \in F \mid v(a) \geq 0\},$$
$$O_v^* = \{a \in F \mid v(a) = 0\},$$
$$P_v = \{a \in F \mid v(a) > 0\} = O_v \setminus O_v^*.$$
$$F_v = O_v/P_v.$$

Properties:

- O_v is an integral domain and a discrete valuation ring, i.e. $O_v \subsetneq F$ and for $a \in F^*$, we have $a \in O_v$ or $a^{-1} \in O_v$.
- O_v^* is the unit group of O_v.
- P_v is the unique maximal ideal of O_v; in particular, F_v is a field called the residue field of v.
- Every $a \in F^*$ has a unique representation $a = \epsilon u^n$ with $\epsilon \in O_v^*$ and $n = v(a) \in \mathbb{Z}$.
- O_v is principal ideal domain whose ideals are generated by the non-negative powers of u; in particular, u is a generator of P_v.

Example: p-Adic Valuations

For any p-adic valuation v_p on $\mathbb{Q}$:

$$O_{v_p} = \{r \in \mathbb{Q} \mid r = a/b \text{ with } \gcd(a,b) = 1 \text{ and } p \nmid b\}$$
$$O_{v_p}^* = \{r \in \mathbb{Q} \mid r = a/b \text{ with } \gcd(a,b) = 1 \text{ and } p \nmid ab\}$$
$$P_{v_p} = \{r \in \mathbb{Q} \mid r = a/b \text{ with } \gcd(a,b) = 1,\ p \mid a,\ p \nmid b\}$$
$$F_{v_p} = \mathbb{F}_p.$$

Similarly, for any p-adic valuation $v_{p(x)}$ on $K(x)$:

$$O_{v_{p(x)}} = \{r(x) \in K(x) \mid r(x) = a(x)/b(x) \text{ with } \gcd(a,b) = 1,\ p(x) \nmid b(x)\}$$
$$O_{v_{p(x)}}^* = \{r(x) \in K(x) \mid r(x) = a(x)/b(x) \text{ with } \gcd(a,b) = 1,\ p(x) \nmid a(x)b(x)\}$$
$$P_{v_{p(x)}} = \{r(x) \in K(x) \mid (x) = a(x)/b(x) \text{ with } \gcd(a,b) = 1,\ p(x) \mid a(x),\ p(x) \nmid b(x)\}$$
$$F_{v_{p(x)}} = K[x]/(p(x)) \text{ where } (p(x)) \text{ is the } K[x]\text{-ideal generated by } p(x)$$

Example: Infinite Valuation on $K(x)$

For the infinite valuation v_∞ on $K(x)$:

$$O_{v_\infty} = \{r(x) \in K(x) \mid r(x) = f(x)/g(x) \text{ with } \deg(f) \leq \deg(g)\}$$
$$O^*_{v_\infty} = \{r(x) \in K(x) \mid r(x) = f(x)/g(x) \text{ with } \deg(f) = \deg(g)\}$$
$$P_{v_\infty} = \{r(x) \in K(x) \mid (x) = f(x)/g(x) \text{ with } \deg(f) < \deg(g)\}$$
$$F_{v_\infty} = K$$

We will henceforth write O_∞, P_∞, F_∞ for brevity.

Example

$$v_\infty\left(\frac{x-7}{2x^3+3x}\right) = 2 \quad \text{and} \quad \frac{x-7}{2x^3+3x} = \left(\frac{1}{x}\right)^2 \cdot \underbrace{\frac{x^3-7x^2}{2x^3+3}}_{\in O^*_\infty}.$$

Places

Definition

A place of F is the unique maximal ideal of a discrete valuation ring in F. The set of places of F is denoted $\mathbb{P}(F)$.

Theorem

There is a one-to-one correspondence between the set of normalized discrete valuations on F and the set $\mathbb{P}(F)$ of places of F as follows:

- *If v is a normalized discrete valuation on F, then $P_v \in \mathbb{P}(F)$ is the unique maximal ideal in the discrete valuation ring O_v.*
- *If P is a place of F, then the discrete valuation ring $O \subset F$ containing P as its unique maximal ideal is determined, and P defines a discrete normalized valuation on F as follows: if u is any generator of P, then every element $a \in F^*$ has a unique representation $a = \epsilon u^n$ with $n \in \mathbb{Z}$ and ϵ a unit in O, and we define $v(a) = n$ and $v(0) = \infty$. Note that u is a uniformizer for v.*

Examples of Places

For any prime number p, the set

$$P = \{r \in \mathbb{Q} \mid r = a/b \text{ with } \gcd(a,b) = 1,\ p \mid a,\ p \nmid b\} = P_{v_p}$$

is a place of $\mathbb{Q}$ with corresponding valuation v_p.

The set $\mathbb{P}(K(x))$ consists of the finite places of $K(x)$ of the form $P_{p(x)} = P_{v_{p(x)}}$ where $p(x)$ is a monic irreducible polynomial in $K[x]$ and the infinite place of $K(x)$ of the form $P_\infty = P_{v_\infty}$.

Let $F/\mathbb{Q}$ be a number field with ring of integers $\mathcal{O}_F$ (the integral closure of $\mathbb{Z}$ in F). Then every prime ideal in $\mathcal{O}_F$ is a place of F.

Let F be a finite algebraic extension of $\mathbb{F}_q(x)$ and let $\mathcal{O}_F$ be the integral closure of the polynomial ring $\mathbb{F}_q[x]$ in F. Then every prime ideal in $\mathcal{O}_F$ is a place of K. Note that there are other places of F that do not arise in this way (more on this later).

Function Fields

Function Fields

Definition

Let K be a field. An algebraic function field F/K in one variable over K is a field extension $F \supseteq K$ such that F is finite algebraic extension of $K(x)$ for some $x \in F$ that is transcendental over K.

We will shorten this terminology to just "function field".

In other words, a function field is of the form $F = K(x, y)$ where

- $x \in F$ is transcendental over K,
- $y \in F$ is algebraic over $K(x)$, so there exists a monic irreducible polynomial $\phi(Y) \in K(x)[Y]$ of degree $n = [F : K(x)]$ with $\phi(y) = 0$.

Remark

It is important to note that there are many choices for x, and the degree $[F : K(x)]$ may change with the choice of x. This is different from number fields where the degree over $\mathbb{Q}$ is fixed.

Examples of Function Fields

A function field is rational if $F = K(x)$ for some element $x \in F$ that is transcendental over K.

The meromorphic functions on a compact Riemann surface form a function field over $\mathbb{C}$ (the complex numbers).

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over a field K of characteristic different from 2 and 3. Then $F = K(x, y)$ is a function field over K. Note that $[F : K(x)] = 2$ and $[F : K(y)] = 3$.

More generally, consider the curve $y^2 = f(x)$ where $f(x) \in K[x]$ is a square-free polynomial and K has characteristic different from 2. Then $F = K(x, y)$ is a function field over K whose elements are of the form

$$F = \{ a(x) + b(x)y \mid a(x), b(x) \in K(x) \}.$$

Note that $[F : K(x)] = 2$ and $[F : K(y)] = \deg(f)$.

Function Fields of Curves

Definition

A plane affine irreducible algebraic curve over a field K is the zero locus of an irreducible polynomial $\Phi(x, Y)$ in two variables with coefficients in K.

We will shorten this terminology to just "curve".

Definition

The coordinate ring of a curve $C : \Phi(x, y) = 0$ over a field K is the ring $K[x, Y]/(\Phi(x, Y))$ where $(\Phi(x, y))$ is the principal $K[x, y]$-ideal generated by $\Phi(x, y)$.
The function field of C is the field of fractions of its coordinate ring.

Remark: The function field of a curve is a function field as defined previously. Conversely, every function field F/K is the function field of the curve given by a minimal polynomial of $F/K(x)$.

Note that a function field has many defining curves.

Constant Fields

Definition

The constant field of a function field F/K is the algebraic closure of K in F, i.e. the field

$$\tilde{K} = \{z \in F \mid z \text{ is algebraic over } K\}.$$

F/K is a geometric function field if $\tilde{K} = K$.

Sometimes $\tilde{K}$ is called the "full" or the "exact" field of constants of F/K.

Remark

$K \subseteq \tilde{K} \subsetneq F$, and every element in $F \setminus \tilde{K}$ is transcendental over K.

Remark

Write $F = K(x, y)$. Then F/K is a geometric function field if and only if the minimal polynomial of y over $K(x)$ is absolutely irreducible, i.e. irreducible over $\overline{K}(x)$ where $\overline{K}$ is the algebraic closure of K.

Examples

$K(x)/K$ is always geometric.

If K is algebraically closed (e.g. $K = \mathbb{C}$), then any F/K is geometric.

Let $F = K(x, y)$ where $y^2 = f(x)$ with $f(x) \in K[x]$ square-free. Then $F/K(x)$ is geometric if and only if $f(x)$ is non-constant.

Suppose -1 is not a square in K (e.g. $K = \mathbb{R}$ or $K = \mathbb{F}_q$ with $q \equiv 3 \pmod 4$), and let $F = K(x, y)$ where $x^2 + y^4 = 0$. Then $\tilde{K} = K(i)$ where $i \notin K$ is a square root of -1. So $[\tilde{K} : K] = 2$, and F/K is not geometric. Note that $[F : K(x)] = 4$ and $[F : \tilde{K}(x)] = [\tilde{K}(x) : K(x)] = 2$.

Residue Fields and Degrees

Recall that a place P of a field F is the unique maximal ideal of some discrete valuation ring O_P of F, and its residue field is $F_P = O_P/P$.

Remark: $\tilde{K} \subset O_P$ for all $P \in \mathbb{P}(F)$.

Definition

Let F/K be a geometric function field and P a place of F. Then the degree of P is the field extension degree $\deg(P) := [F_P : K]$. Places of degree one are called rational. The set of rational places of F is denoted $\mathbb{P}_1(F)$.

Remark

$\deg(P) \leq [F : K(x)]$ for any $x \in P$, so $\deg(P)$ is always finite.

Example: Residue Fields of Places of $K(x)$

- For any finite place $P_{p(x)}$ of $K(x)$, a K–basis of F_P is $\{1, x, \ldots, x^{\deg(p)-1}\}$, so $\deg(P_{p(x)}) = \deg(p)$.

- For the infinite place P_∞ of $K(x)$, we have $F_P = K$ and hence $\deg(P_\infty) = 1$.

- K is algebraically closed if and only if the finite places of $K(x)$ correspond exactly the linear polynomials $x + \alpha$ with $\alpha \in K$, i.e. if and only if all the places of $K(x)$ are rational, so $\mathbb{P}(K(x)) = \mathbb{P}_1(K(x))$.

  In this case, there is a one-to-one correspondence between $\mathbb{P}_1(K(x))$ and the *points on the projective line* $\mathbb{P}^1(K) := K \cup \{\infty\}$ via

  $$\mathbb{P}_1(K(x)) \longleftrightarrow \mathbb{P}^1(K) \quad \text{via} \quad x + \alpha \longleftrightarrow \alpha\,, \quad 1/x \longleftrightarrow \infty\,.$$

  Hence the name 'infinite place" — think of this as "substituting $x = 0$" into the uniformizer.

Values of Functions

Recall that $h(x) = q(x)(x-\alpha) + h(\alpha)$ for all $h(x) \in K[x]$ and $\alpha \in K$.

One can think of $h(a) = h(x) (\mathrm{mod}\ x-\alpha)$ as the "value of $h(x)$ at the place $x-\alpha$". For $h(x) \in K$, this value is the same for any α, i.e. constant.

More generally, for any place P of a function field F/K, one can interpret cosets $z+P$ as "values" $z(P)$ which are "constant" for elements $z \in K$. Hence the terms "function field" and "constant field".

Let $r(x) = f(x)/g(x) \in K(x)$ with $\gcd(f,g) = 1$. Consider a finite place $P_{x-\alpha}$ ($\alpha \in K$). Then

$$v_{x-\alpha}(r(x)) > 0 \implies f(\alpha) = 0,\ g(\alpha) \neq 0 \implies \alpha \text{ is a zero of } r(x).$$
$$v_{x-\alpha}(r(x)) < 0 \implies g(\alpha) = 0,\ f(\alpha) \neq 0 \implies \alpha \text{ is a pole of } r(x).$$

Zeros and Poles

Definition

Let P be a place of a function field F/K and $z \in F$. Then P is a zero of z if $v_P(z) > 0$ and a pole of z if $v_P(z) < 0$. More generally, for any positive integer m, P is a zero of z of order (or multiplicity) m if $v_p(z) = m$ and a pole of z of order m if $v_P(z) = -m$.

Properties:

- Every transcendental element in F/K has at least one zero and at least one pole. In particular, if F/K is geometric, then every element in $F \setminus K$ has at least one zero and at least one pole.
- Every non-zero element in F has only finitely many zeros and poles.
- When counted with multiplicities, every non-zero element in F has the same number of zeros and poles.

Divisors and Genus

Recollection: Ideals in Number Fields

Recall that in a number field:

- Every ideal in the ring of integers has a unique factorization into prime ideals.
- By allowing negative exponents, this extends to fractional ideals. So the prime ideals generate the group of fractional ideals.
- Two non-zero fractional ideals are equivalent if they differ by a factor that is a principal ideal.
- The ideal class group is the group of non-zero fractional ideals modulo (principal) equivalence whose order is class number of the field. It is a finite abelian group that is an important invariant of the field.

We now consider analogous notions in function fields, with prime ideals replaced by places, and multiplication (products) replaced by addition (sums).

Assume henceforth that F/K is a geometric function field.

UNIVERSITY OF CALGARY

Definition

The Divisor group of F/K, denoted $\mathrm{Div}(F)$, is the free group generated by the places of F/K. Its elements, called divisors of F, are formal finite sums of places.

Let

$$D = \sum_{P \in \mathbb{P}(F)} n_P P \text{ with } n_P \in \mathbb{Z} \text{ and } n_P = 0 \text{ for almost all } P \in \mathbb{P}(F).$$

Then

- the value of D at P is $v_P(D) := n_P$ for any $P \in \mathbb{P}(F)$.
- the support of D is $\mathrm{supp}(D) := \{P \in \mathbb{P}(F) \mid v_P(D) \neq 0\}$.
- the degree of D is $\deg(D) := \sum_{P \in \mathbb{P}(F)} n_P \deg(P)$.
- D is a prime divisor if it is of the form $D = P$ for some $P \in \mathbb{P}(F)$.

More on Divisors

Remarks

- Every divisor is a unique sum of finitely many prime divisors (note that some prime divisors in the support may have negative coefficients).
- The notions of value and degree are compatible with their previous definitions. In particular:
  - For any place P of F, the normalized discrete valuation on F associated to P extends to a group homomorphism $v_P : \mathrm{Div}(F) \to \mathbb{Z} \cup \{\infty\}$.
  - The degree map defined on places of F extends to a group homomorphism $\deg : \mathrm{Div}(F) \to \mathbb{Z} \cup \{\infty\}$ whose kernel is the subgroup $\mathrm{Div}^0(F)$ of $\mathrm{Div}(F)$ consisting of all degree zero divisors.
- **F. K. Schmidt** proved that every function field F over a *finite* field $K = \mathbb{F}_q$ has a divisor of degree one, so in this case, the degree homomorphism on $\mathrm{Div}(F)$ is surjective.

Principal Divisors

Definition

A divisor $D \in \mathrm{Div}(F)$ is principal if it is of the form

$$D = \sum_{P \in \mathbb{P}(F)} v_P(z) P$$

for some $z \in F^*$. Write $D = \mathrm{div}(z)$.

Definition

The zero divisor and pole divisor of a principal divisor $\mathrm{div}(z)$ are the respective divisors

$$\mathrm{div}(z)_0 = \sum_{v_P(z)>0} v_P(z) P\,, \qquad \mathrm{div}(z)_\infty = -\sum_{v_P(z)<0} v_P(z) P\,.$$

So $\mathrm{div}(z) = \mathrm{div}(z)_0 - \mathrm{div}(z)_\infty$.

Example: In $F = K(x)$, we have $\mathrm{div}(x)_0 = P_x$ and $\mathrm{div}(x)_\infty = P_\infty$.

More on Principal Divisors

UNIVERSITY OF CALGARY

Theorem

Let $x \in F \setminus K$. *Then* $\deg(\operatorname{div}(x)_0) = \deg(\operatorname{div}(x)_\infty) = [F : K(x)]$.

It follows that $\deg(\operatorname{div}(z)) = 0$, *so the principal divisors form a subgroup of* $\operatorname{Div}^0(F)$, *denoted* $\operatorname{Prin}(F)$.

Definition

Two divisors $D_1, D_2 \in \operatorname{Div}(F)$ are (linearly) equivalent, denoted $D_1 \sim D_2$, if $D_1 - D_2 \in \operatorname{Prin}(F)$.

Remark and Notation

Linear equivalence is an equivalence relation. The class of a divisor D under linear equivalence is denoted $[D]$.

Class Group and Zero Class Group

UNIVERSITY OF CALGARY

Definition

The factor groups

$$\mathrm{Cl}(F) = \mathrm{Div}(F)/\mathrm{Prin}(F) \quad \text{and} \quad \mathrm{Cl}^0(F) = \mathrm{Div}^0(F)/\mathrm{Prin}(F)$$

are the divisor class group and the degree zero divisor class group of F/K, respectively. (Usually abbreviated to just class group and zero class group.)

Remarks and Definition

- Both $\mathrm{Cl}(F)$ and $\mathrm{Cl}^0(F)$ are abelian groups.
- $\mathrm{Cl}(F)$ is always infinite, but $\mathrm{Cl}^0(F)$ may or may not be infinite. It it is finite, then the order h_F is called the degree zero divisor class number (or just class number) of F/K. We will see later on that h_F is always finite for a function field over a *finite* field.
- Sometimes the zero class group is also called the Jacobian of F/K.

More on Class Groups

UNIVERSITY OF CALGARY

Theorem

Every rational function field has class number one.

Remark

There are 8 non-rational function fields $F/\mathbb{F}_q$ of class number one. All have $q \leq 4$, and defining curves for all of them are known.

Theorem

Let F/K be a non-rational function field that has a rational place, denoted P_∞. Then the map $\Phi : \mathbb{P}_1(F) \to \mathrm{Cl}^0(F)$ via $P \mapsto [P - P_\infty]$ is injective.

The above embedding imposes an abelian group structure on $\mathbb{P}_1(F)$. Note that this group structure is non-canonical (depends on the choice of P_∞).

Effective Divisors

Definition

Define a partial order $\geq$ on $\mathrm{Div}(F)$ via

$$D_1 \geq D_2 \quad \Leftrightarrow \quad v_P(D_1) \geq v_P(D_2) \text{ for all } P \in \mathbb{P}(F).$$

A divisor $D \in \mathrm{Div}(F)$ is effective (or integral or positive) if $D \geq 0$.

Examples

- The trivial divisor $D = 0$ is effective.
- Every prime divisor is effective.
- The zero and pole divisors of a principal divisor are effective.
- The sum of two effective divisors is effective. So the effective divisors form a sub-monoid of $\mathrm{Div}(F)$.

Riemann-Roch Spaces

Definition

The Riemann-Roch space of a divisor $D \in \mathrm{Div}(F)$ is the set

$$L(D) = \{x \in F \mid \mathrm{div}(x) + D \geq 0\} \cup \{0\}.$$

Interpretation

$L(D)$ consists of all $x \in F$ such that

- If D has a pole of order m at P, then x has a zero of order at least m at P.
- If D has a zero of order m at P, then x may have a pole at P, but its order cannot exceed m.

Examples

Let $F = K(x)$.

- $L(nP_\infty) = \{f(x) \in K[x] \mid \deg(f) \leq n\}$ for $n \geq 0$.
- If $D = -3P_{x-1} + 2P_{x-2} + 4P_{x-7}$, then

$$L(D) = \left\{ \frac{(x-1)^3}{(x-2)^2(x-7)^4} r(x) \mid r(x) \in K(x), \deg(r) \leq 3 \right\}.$$

For any function field F/K, if $P \in \mathbb{P}(F)$ and $n \in \mathbb{Z}$ with $n > 0$, then

$$L(nP) \setminus L((n-1)P) = \{x \in F \mid \operatorname{div}(x)_\infty = nP\}.$$

Properties of Riemann-Roch Spaces

- $x \in L(D)$ if and only if $v_P(x) \geq -v_P(D)$ for all $P \in \mathbb{P}(F)$.
- $L(D)$ is a K-vector space.
- If $D_1 \sim D_2$, then $L(D_1) \cong L(D_2)$ (isomorphic as K-vector spaces).
- $L(0) = K$.
- If $\deg(D) < 0$ or $D \in \mathrm{Div}^0(F) \setminus \mathrm{Prin}(F)$, then $L(D) = \{0\}$.
- $L(D) \neq \{0\}$ if and only if the class $[D]$ contains an effective divisor.

Notation

The K-vector space dimension of $L(D)$ is denoted $\ell(D) = \dim_K(L(D))$.

Remark

Both $\deg(D)$ and $\ell(D)$ depend only on the divisor class $[D]$.

Genus

Definition

The genus of F/K is $g = \max\{\deg(D) - \ell(D) + 1 \mid D \in \mathrm{Div}(F)\}$.

Remark

$g \geq 0$. (Because $\deg(0) - \ell(0) + 1 = 0$.)

Theorem (Hasse-Weil)

Let $F/\mathbb{F}_q$ be a function field of genus g over a finite field of order q.

$$q+1-2g\sqrt{q} \;\leq\; |\mathbb{P}_1(F)| \;\leq\; q+1+2g\sqrt{q} \quad (\text{so } |\mathbb{P}_1(F)| \approx q \text{ for } q \text{ large}).$$

$$(\sqrt{q}-1)^{2g} \;\leq\; |\mathrm{Cl}^0(F)| \;\leq\; (\sqrt{q}+1)^{2g} \quad (\text{so } |\mathrm{Cl}^0(F)| \approx q^g \text{ for } q \text{ large}).$$

The class group and genus are important invariants of any function field!

Unfortunately, they are not easy to compute ... ☹

Riemann-Roch Theorem

Theorem (**Riemann-Roch**)

There exist a divisor class $\mathcal{W} \in \mathrm{Cl}(D)$ *such that for all* $D \in \mathrm{Div}(F)$ *and all* $W \in \mathcal{W}$, *we have* $\ell(W - D) = g - 1 + \ell(D) - \deg(D)$.

Remarks and Definition

- $\mathcal{W}$ is unique with this property.
- $\mathcal{W}$ is called the canonical divisor class and its elements are called canonical divisors.
- $\mathcal{W}$ can be explicitly described as the class of Weil differentials of F.

Corollary

- $\deg(W) = 2g - 2$ and $\ell(W) = g$ for any canonical divisor W.
- If $\deg(D) \geq 2g - 1$, then $\ell(D) = \deg(D) - g + 1$.

Function Field Extensions

Recollection: Prime Ideals in Number Fields

Recall that in a number field extension $F'/F/\mathbb{Q}$:

- A prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ need not remain prime when extended to $\mathcal{O}_{F'}$.
  Rather, it has a prime ideal factorization $\mathfrak{p}\mathcal{O}_{F'} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$ in $\mathcal{O}_{F'}$.
- Each $\mathfrak{P}_i$ is said to lie above $\mathfrak{p}$, written $\mathfrak{P}_i|\mathfrak{p}$.
  Finitely many prime ideals of $\mathcal{O}_{F'}$ lie above any prime ideal of $\mathcal{O}_F$.
- $\mathfrak{p}$ is said to lie below each $\mathfrak{P}_i$.
  A unique prime ideal of $\mathcal{O}_F$ lies below every prime ideal of $\mathcal{O}_{F'}$.
- e_i is called the ramification index of $\mathfrak{P}_i|\mathfrak{p}$.
- The field extension degree $f_i = [\mathcal{O}_{F'}/\mathfrak{P} : \mathcal{O}_F/\mathfrak{p}]$ is called the residue degree of $\mathfrak{P}_i|\mathfrak{p}$.
- The norm of $\mathfrak{P}_i$ is the $\mathcal{O}_F$-ideal $N_{F'/F}(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$.
  The norm extends multiplicatively to all ideals of $\mathcal{O}_{F'}$.
- The fundamental identity $\sum_{i=1}^{r} e_i f_i = [F' : F]$ holds.

Once again, we consider analogous notions in function field extensions, with prime ideals replaced by places, and products replaced by sums.

UNIVERSITY OF CALGARY

Notation and Assumption

- F/K and F'/K' are geometric function fields with $F \subseteq F'$ and $K \subseteq K'$.
- F' is a finite algebraic extension of F.
- K is perfect, i.e. every irreducible polynomial in $K[x]$ has distinct roots.

Remark: Finite fields, algebraically closed fields, and characteristic 0 fields are all perfect. $K = \mathbb{F}_q(x)$ is *not* perfect (consider $\phi(T) = T^q - x$).

Theorem and Definition

- Every place P' of F' contains a unique place P of F, namely $P = P' \cap F$. Write $P'|P$.
- For every place P of F, $P'|P$ for only finitely many places P' of F'.
- $P'|P$ if and only if $O_P = O_{P'} \cap F$. In this case $O_{P'}$ is an O_P-module of rank $[F' : F]$.

Ramification, Residue Degree, Norm and Co-Norm

Theorem and Definition

Let $P \in \mathbb{P}(F)$, $P' \in \mathbb{P}(F')$ with respective discrete normalized valuations v_P, $v_{P'}$ and residue fields $F_P = O_P/P$, $F'_{P'} = O_{P'}/P'$. Assume $P'|P$.

- There is a unique positive integer $e = e(P'|P)$ such that $v_{P'}(x) = e v_P(x)$ for all $x \in F$, called the ramification index of $P'|P$.
- There is a natural embedding $F_P \hookrightarrow F'_{P'}$ via $x + P \mapsto x + P'$. The extension degree $f(P'|P) = [F'_{P'} : F_P]$ is called the residue degree (or relative degree) of $P'|P$.
- The norm of P' is the divisor $N_{F'/F}(P') = f(P'|P)P$ of F.
- The co-norm of P is the divisor $con_{F'/F}(P) = \sum_{P'|P} e(P'|P)P'$ of F'.
- The norm and co-norm extend additively to homomorphisms on divisors and respect principal divisors, so they also extend to homomorphisms on divisor classes.
- $\sum_{P'|P} e(P'|P) f(P'|P) = [F' : F]$ (fundamental identity).

Example — Quadratic Extensions

Let $\mathrm{char}(K) \neq 2$, $F = K(x, y)$ where $x \in F$ is transcendental over K and $y^2 = f(x)$ with $f(x) \in K[x] \setminus K^2$ square-free.

For any place P' of F, with $P = P' \cap K(x)$:

$$2v_{P'}(y) = v_{P'}(y^2) = v_{P'}(f) = e(P'|P)v_P(f) \ .$$

Case P is finite. Write $P = P_{p(x)}$ with $p(x) \in K[x]$ monic and irreducible.

- If $p(x) \nmid f(x)$ then $v_{P'}(y) = 0$.
- If $p(x) \mid f(x)$, then $v_P(f) = 1$ (since f is square-free), so $e(P'|P) = 2$. Then $v_{P'}(y) = 1$ and $\mathrm{Con}_{F/K(x)}(P) = 2P'$.

Case $P = P_\infty$. Then $v_P(f) = v_\infty(f) = -\deg(f)$.

- If $\deg(f)$ is odd, then $e(P'|P) = 2$. Then $v_{P'}(y) = -\deg(f)$ and $\mathrm{Con}_{F/K(x)}(P) = 2P'$.
- If $\deg(f)$ is even, then we will later see that $e(P'|P) = 1$. Then $v_{P'}(y) = -\deg(f)/2$.

Extension Terminology

UNIVERSITY OF CALGARY

Definition

Let $P \in \mathbb{P}(F)$.

- If $P' \in \mathbb{P}(F')$ with $P'|P$, then P' lies above P and P lies below P'.
- P is unramified if $e(P'|P) = 1$ for all $P'|P$ and ramified otherwise.
- P is wildly ramified if $\mathrm{char}(K)$ divides $e(P'|P)$ for some $P'P$, and tamely ramified otherwise.
- P is totally ramified if $\mathrm{Con}_{F'/F}(P) = [F : F']P'$.
- P is inert in F' if $\mathrm{Con}_{F'/F}(P) = P'$ with $f(P'|P) = [F : F']$.
- P splits completely in F' if $e(P'|P) = f(P'|P) = 1$ for all $P'|P$.

Sufficient (but not necessary) conditions for a function field to be tamely ramified are:

- $\mathrm{char}(K) = 0$.
- $[F' : F] < \mathrm{char}(K)$ when $\mathrm{char}(K)$ is positive.)

UNIVERSITY OF CALGARY

Properties relating "Upstairs" to "Downstairs":

- $\deg(P') = \dfrac{f(P'|P)}{[K' : K]} \deg(P)$ for all $P \in \mathbb{P}(F)$, $P' \in \mathbb{P}(F')$ with $P'|P$.
- $\deg(\mathrm{Con}_{F'/F}(D)) = \dfrac{[F' : F]}{[K' : K]} \deg(D)$ for all $D \in \mathrm{Div}(F)$.
- $N_{F'/F}(\mathrm{Con}_{F'/F}(D)) = [F' : F]\, D$ for all $D \in \mathrm{Div}(F)$.

Transitivity Theorem

Consider F/K, F'/K' and F''/K'' with $F \subseteq F' \subseteq F''$ and $K \subseteq K' \subseteq K''$.

- Let $P \in \mathbb{P}(F)$, $P' \in \mathbb{P}(F')$, $P'' \in \mathbb{P}(F'')$ with $P''|P'|P$. Then $e(P''|P) = e(P''|P')e(P'|P)$ and $f(P''|P) = f(P''|P')f(P'|P)$.
- $N_{F''/F}(D'') = N_{F'/F}(N_{F''/F'}(D''))$ for all $D'' \in \mathrm{Div}(F'')$.
- $\mathrm{Con}_{F''/F}(D) = \mathrm{Con}_{F''/F'}(\mathrm{Con}_{F'/F}(D))$ for all $D \in \mathrm{Div}(F)$.

Recollection: Prime Splitting in Number Fields

In number fields, prime decomposition can almost always be obtained from

Kummer's Theorem (Number Fields)

Let $F/\mathbb{Q}$ be a number field and p a prime. Let $F = \mathbb{Q}(\alpha)$ such that $\alpha \in \mathcal{O}_F$ and p does not divide the index $[\mathcal{O}_F : \mathbb{Z}[\alpha]]$. Let $\phi_\alpha(T) \in \mathbb{Z}[T]$ be the minimal polynomial of α and consider $\overline{\phi}_\alpha(T) \in \mathbb{F}_p[T]$, the reduction of $\phi_\alpha(T)$ modulo p. Let

$$\overline{\phi}_\alpha(T) \equiv \overline{\phi}_1(T)^{e_1}\,\overline{\phi}_2(T)^{e_2} \cdots \overline{\phi}_r(T)^{e_r} \pmod{p}$$

be the factorization of $\overline{\phi}_\alpha(T)$ over $\mathbb{F}_p$ into distinct irreducible polynomials. Then the prime ideal factorization of p in $\mathcal{O}_F$ is

$$p\mathcal{O}_F = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i = p\mathcal{O}_F + \phi_i(\alpha)\mathcal{O}_F$, and $\mathfrak{p}_i$ has residue degree $f_i = \deg(\phi_i)$, for $1 \le i \le r$.

UNIVERSITY OF CALGARY

Kummer's Theorem (Function Fields)

Let F'/F be a finite algebraic extension of function fields of degree $n = [F' : F]$ and $P \in \mathbb{P}(F)$. Let $F' = F(y)$ such that y is integral over O_P. Let $\phi_y(T) \in O_P[T]$ be the minimal polynomial of y over F, and consider $\overline{\phi}_y(T) \in F_P[T]$, the image of $\phi_y(T)$ modulo P under the residue map $O_P \to F_P$. Let

$$\overline{\phi}_y(T) \equiv \overline{\phi}_1(T)^{\epsilon_1}\,\overline{\phi}_2(T)^{\epsilon_2} \cdots \overline{\phi}_r(T)^{\epsilon_r} \pmod{P}$$

be the factorization of $\overline{\phi}_y(T)$ over F_P into distinct irreducible polynomials. Then there are at least r distinct places $P'_1, P'_2, \ldots, P'_r \in \mathbb{P}(F')$ lying above P. Furthermore, $\phi_i(y) \in P'_i$ and $f(P'_i|P) \geq \deg(\phi_i)$ for $1 \leq i \leq r$.

If in addition, $\{1, y, \ldots, y^{n-1}\}$ is an O_P-basis of the integral closure $\overline{O}_P = \bigcap_{i=1}^{r} O_{P'_i}$ in F' or $\epsilon_i = 1$ for $1 \leq i \leq r$, then

$$\mathrm{Con}_{F'/F}(P) = \epsilon_1 P'_1 + \epsilon_2 P'_2 + \cdots + \epsilon_r P'_r,$$

so $e(P'_i|P) = \epsilon_i$ and $f(P'_i|P) = \deg(\phi_i)$ for $1 \leq i \leq r$.

Example — Quadratic Extensions

Let $\mathrm{char}(K) \neq 2$, $F = K(x, y)$ where $x \in F$ is transcendental over K and $y^2 = f(x)$ with $f(x) \in K[x] \setminus K^2$ square-free.

A finite place $P = P_{p(x)}$ of $K(x)$

- ramifies in F if $p(x)$ divides $f(x)$;
- splits in F if $f(x)$ is a square modulo $p(x)$;
- is inert in F if $f(x)$ is a non-square modulo $p(x)$.

The infinite place of $K(x)$

- ramifies in F if $\deg(f)$ is odd;
- splits in F if $\deg(f)$ is even and $\mathrm{sgn}(f)$ is a square in K^*;
- is inert in F if $\deg(f)$ is even and $\mathrm{sgn}(f)$ is a non-square in K^*.

E.g. if $K = \mathbb{F}_5$ and $f(x) = x^3 + 3x + 2 = (x+1)(x+2) \in \mathbb{F}_5[x]$, then the ramified places of $\mathbb{F}_5(x)$ are P_{x+1}, P_{x+2} and P_∞.

The place P_{x^2+2x+4} of $\mathbb{F}_5(x)$ splits in F because

$$x^2 + 2x + 4 = (2x^2 + 2)^2 + x(x^3 + 3x + 2) \equiv (2x^2 + 2)^2 \pmod{f(x)} .$$

The Different

Assume that F'/F is a tamely ramified function field extension.

Definition

The different (or ramification divisor) of F'/F is

$$\mathrm{Diff}(F'/F) = \sum_{P \in \mathbb{P}(F)} \sum_{P'|P} (e(P'|P) - 1)P' \in \mathrm{Div}(F').$$

Example

$F = K(x, y)$ with $y^2 = f(x) = p_1(x) \cdots p_r(x)$ (prime factorization of $f(x)$).

$$\mathrm{Diff}(F/K(x)) = P'_{p_1(x)} + \cdots + P'_{p_r(x)} + \delta P'_\infty \quad \text{where}$$

- $P'_{p_i(x)}$ is the unique place lying above $P_{p_i(x)}$;
- P'_∞ is the unique place lying above P_∞ when P_∞ is ramified;
- $\delta \in \{0, 1\}$ is the parity of $\deg(f)$.

It follows that $\deg(\mathrm{Diff}(F/K(x))) = \deg(f) + \delta$ (an even integer).

UNIVERSITY OF CALGARY

Theorem (**Hurwitz Genus Formula**)

Let F'/K' be a finite algebraic function field extension of F/K, and denote by $g_{F'}$ and g_F the genera of F' and F, respectively. Then

$$2g_{F'} - 2 = \frac{[F' : F]}{[K' : K]}(2g_F - 2) + \deg(\mathrm{Diff}(F'/F)).$$

Corollary

- *The different has even degree.*
- *If $x \in F \setminus K$, then $g_F = \frac{1}{2}\deg(\mathrm{Diff}(F/K(x)) - [F : K(x)] + 1$.*

Example (elliptic and hyperelliptic function fields):
$F = K(x, y)$ with $\mathrm{char}(K) \neq 2$; $y^2 = f(x)$ with $f(x) \in K[x]$ square-free.

- $g = \lfloor (\deg(f) - 1)/2 \rfloor$ (so $\deg(f) = 2g + 1$ or $2g + 2$).
- $\deg(\mathrm{Diff}(F/K(x)) = 2g + 2$.

Constant Field Extensions

Recall our assumptions that K is perfect and K'/K is algebraic.

Definition

An extension F'/K' of F/K is a constant field extension if $F' = FK'$.

Theorem

Let F/K be a constant field extension of F/K. Then the following hold:

- *K' is the full constant field of F'.*
- *$[F : K(x)] = [F' : K'(x)]$ for all $x \in F \setminus K$.*
- *F'/F is unramified, i.e. no place of F ramifies in F'.*
- *$g_{F'} = g_F$.*
- *The conorm map $\mathrm{Con}_{F/F'} : \mathrm{Cl}(F) \hookrightarrow \mathrm{Cl}(F')$ is injective.*

Corollary

If F/K has finite class group, then h_F divides $h_{F'}$.

Genus 0 and 1 Function Fields

Genus 0 Function Fields

We continue to assume that K is perfect.

Theorem

Let F/K be a function field of genus 0. Then the following hold:

- *F/K is rational if and only if it has a rational (i.e. degree 1) place.*
- *If F/K is not rational, then F has a place of degree 2, and there exists $x \in F$ with $[F : K(x)] = 2$.*

Corollary

For K algebraically closed, F/K is rational if and only if F has genus 0.

Example

$F = \mathbb{R}(x, y)$ where $x^2 + y^2 = -1$ has genus 0 but is not rational.

Remark

Every genus 0 function field has class number 1.

Genus 1 Function Fields

UNIVERSITY OF CALGARY

Definition

A function field F/K is elliptic if it has genus 1 and a rational place.

Corollary

For K algebraically closed, F/K is elliptic if and only if F has genus 1.

Example

$F = \mathbb{R}(x, y)$ where $x^2 + y^4 = -1$ has genus 1 but is not elliptic.

Theorem

If F/K is elliptic, then there exist $x, y \in F$ such that $F = K(x, y)$ and

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

for some $a_1, a_2, a_3, a_4, a_6 \in K$. This equation defines an elliptic curve in Weierstrass form.

Remark

Short Weierstrass Form

Consider $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

- If $\mathrm{char}(K) \neq 2$, then "completing the square for y", i.e. substituting y by $y - (a_1x + a_3)/2$ leaves F/K unchanged and produces an equation of the form

$$y^2 = x^3 + b_2x^2 + b_4x + b_6 \quad (b_2, b_4, b_6 \in K).$$

- If in addition $\mathrm{char}(K) \neq 3$, then "completing the cube for x", i.e. substituting x by $x - b_2/3$ leaves F/K unchanged and produces an equation of the form

$$y^2 = x^3 + Ax + B \quad (A, B \in K).$$

  This is an elliptic curve in short Weierstrass form.

- Similarly, if $\mathrm{char}(K) = 2$, one can always convert a (long) Weierstrass form to an equation of the form

$$y^2 + y = \text{cubic polynomial in } x \quad \text{or} \quad y^2 + xy = \text{cubic polynomial in } x.$$

Interlude – Why "Genus"?

Brief excursion into the topology and geometry of function fields. ☺

In topology, the genus g of a connected, orientable surface is the number of "handles" on it (or "holes" in it). It is the maximum number of (closed non-intersecting) cuts that are possible without disconnecting the surface.

For example:

- A sphere has genus 0
- A "doughnut" (torus) has genus 1, as does a coffee mug with a handle
- A "pretzel" (3-dimensional figure 8) has genus 2

Geometrically, over an algebraically closed field K, places of a function field F/K correspond one-to-one to the points on the unique non-singular plane curve defining F/K.

- A rational (i.e. genus 0) function field over $\mathbb{C}$ corresponds to the projective line $\mathbb{P}^1(\mathbb{C})$, which is a sphere and thus a genus 0 object.
- An elliptic (i.e. genus 1) curve over $\mathbb{C}$ corresponds to the plane $\mathbb{C}^2$ modulo its period lattice which is a torus and thus a genus 1 object.

$\mathbb{P}_1(F)$ as an Abelian Group

UNIVERSITY OF CALGARY

Theorem

Let F/K be an elliptic function field, and fix a rational place $P_\infty \in \mathbb{P}_1(F)$. Then the injection $\Phi : \mathbb{P}_1(F) \to \mathrm{Cl}^0(F)$ via $P \mapsto [P - P_\infty]$ is a bijection.

Corollary

- Every degree zero divisor class of F/K has a unique representative of the form $[P - P_\infty]$ with $P \in \mathbb{P}_1(F)$.
- The set $\mathbb{P}_1(F)$ becomes an abelian group (and Φ a group isomorphism) under the addition law

$$P \oplus Q =: R \quad \Longleftrightarrow \quad [P - P_\infty] + [Q - P_\infty] = [R - P_\infty].$$

Points on an Elliptic Curve

Consider $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Definition

The set of (K-)rational points on E is

$$E(K) = \{ (x_0, y_0) \in K \times K \mid y_0^2 + a_1x_0y_0 + a_3y_0 = x_0^3 + a_2x_0^2 + a_4x_0 + a_6 \} \cup \{\infty\} .$$

The "point" ∞ arises from the homogenization of E:

$$E_H : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Points on E_H: $[x : y : z] \neq [0 : 0 : 0]$ normalized to last non-zero entry $= 1$.

Points on E	$\longleftrightarrow$	Points on E_H
(x, y)	$\longrightarrow$	$[x : y : 1]$
$(x/z, y/z)$	$\longleftarrow$	$[x : y : z]$ when $z \neq 0$
∞	$\longleftarrow$	$[0 : 1 : 0]$

Point Arithmetic

Theorem (Bezout)

Two curves of respective degrees m and n intersect in exactly mn points (counting point multiplicities).

Corollary

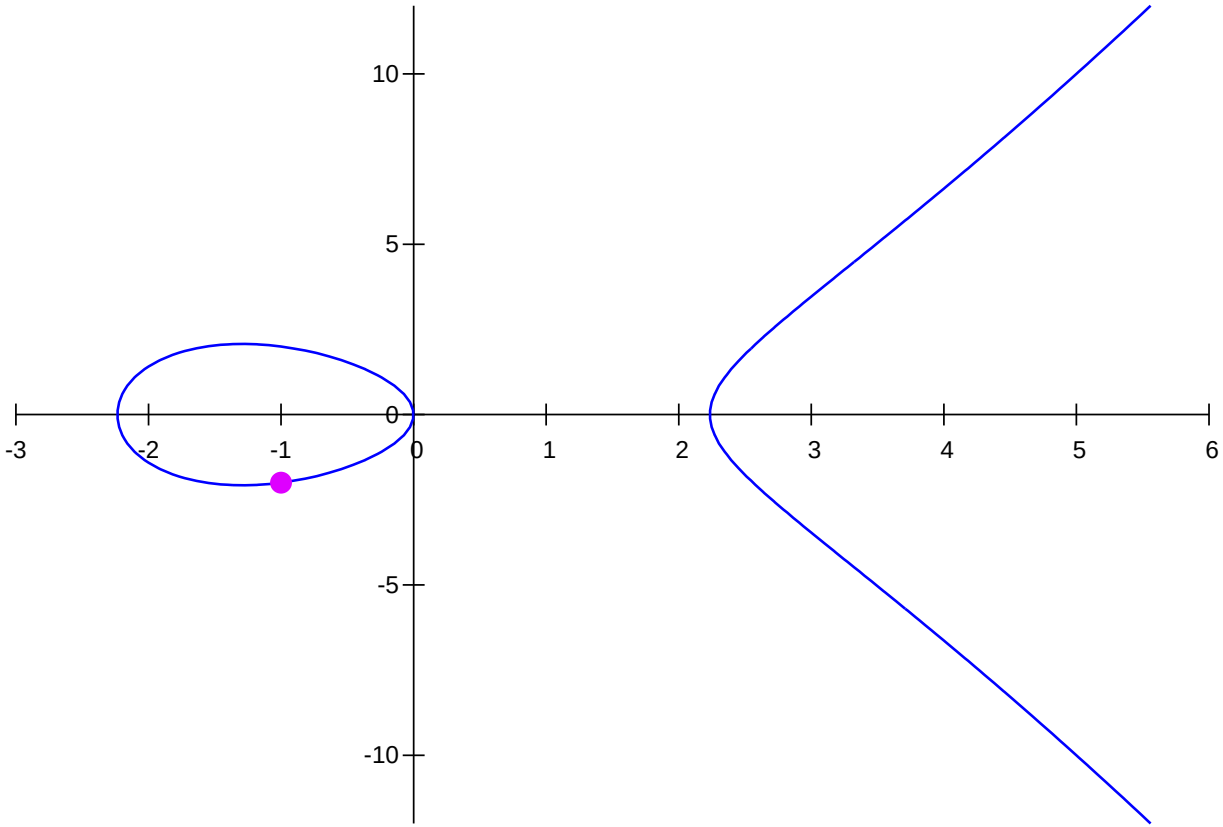
A line intersects an elliptic curve in exactly 3 points.

Group Law on $E(K)$ (additive, abelian):

- Identity: ∞.
- Inverses: $-p$ is defined as the third point of intersection of the "vertical" line through p and ∞ with E.
- Addition:
  - If $p \neq q$, then $-r$ is defined as the third point of intersection of the secant line through p and q with r.
  - If $p = q$, then $-r$ is defined as the third point of intersection of the tangent line at p to E.
  - Must then invert $-r$ to obtain r.

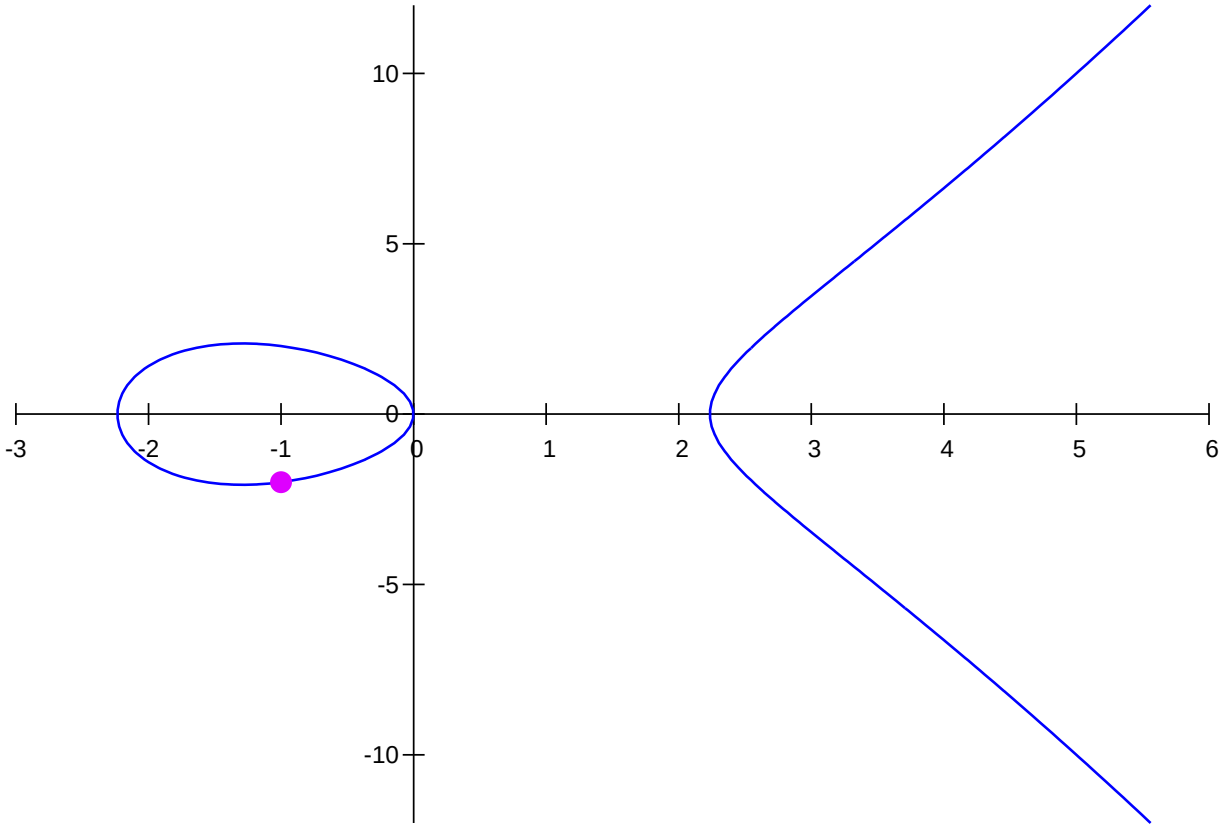
An Elliptic Curve and a Point

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $\quad p = (-1, -2) \in E(\mathbb{Q})$



Inversion on E

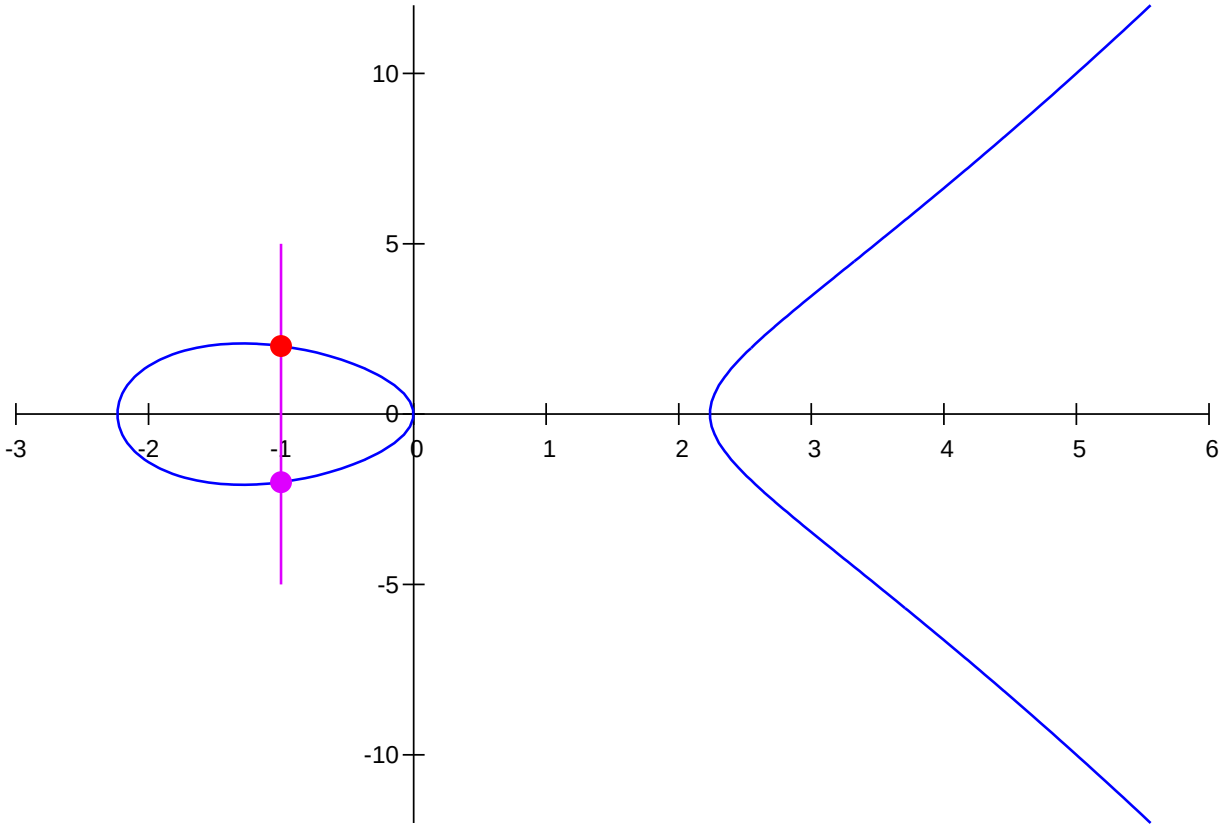
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $\quad p = (-1, -2)$



The vertical line through p and ∞ is $\boxed{x = -1}$

Inversion on E

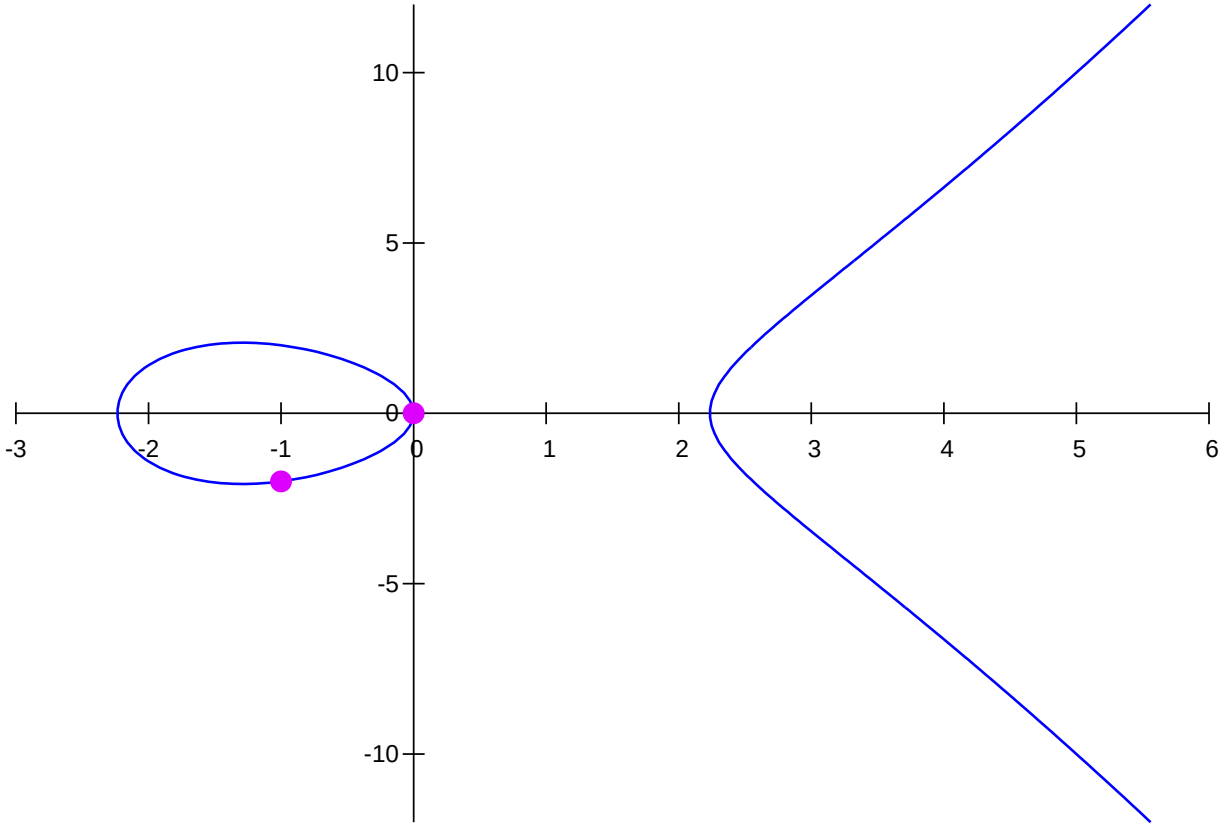
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $p = (-1, -2)$



It intersects E in the third point $-p = (-1, 2)$

Addition of Distinct Points on E

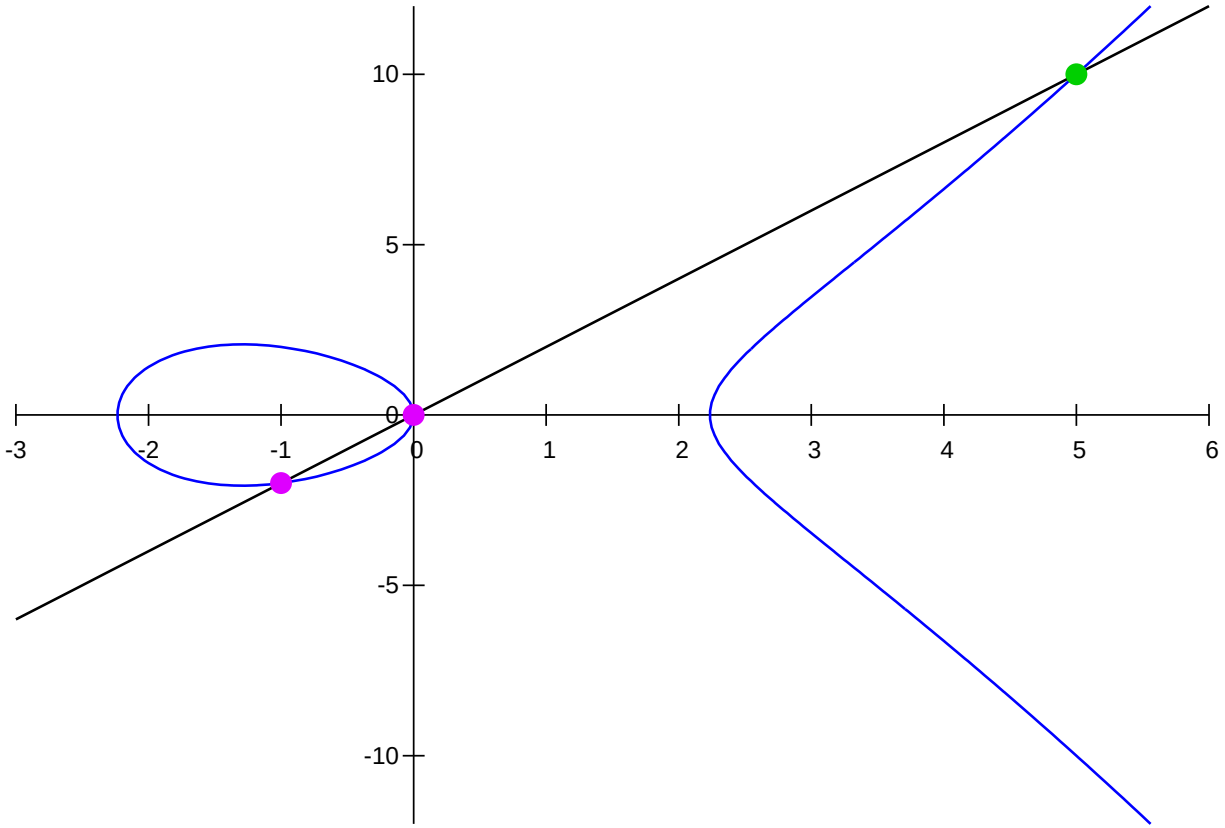
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $p = (-1, -2)$, $q = (0, 0)$



The line through p and q is $\boxed{y = 2x}$

Addition of Distinct Points on E

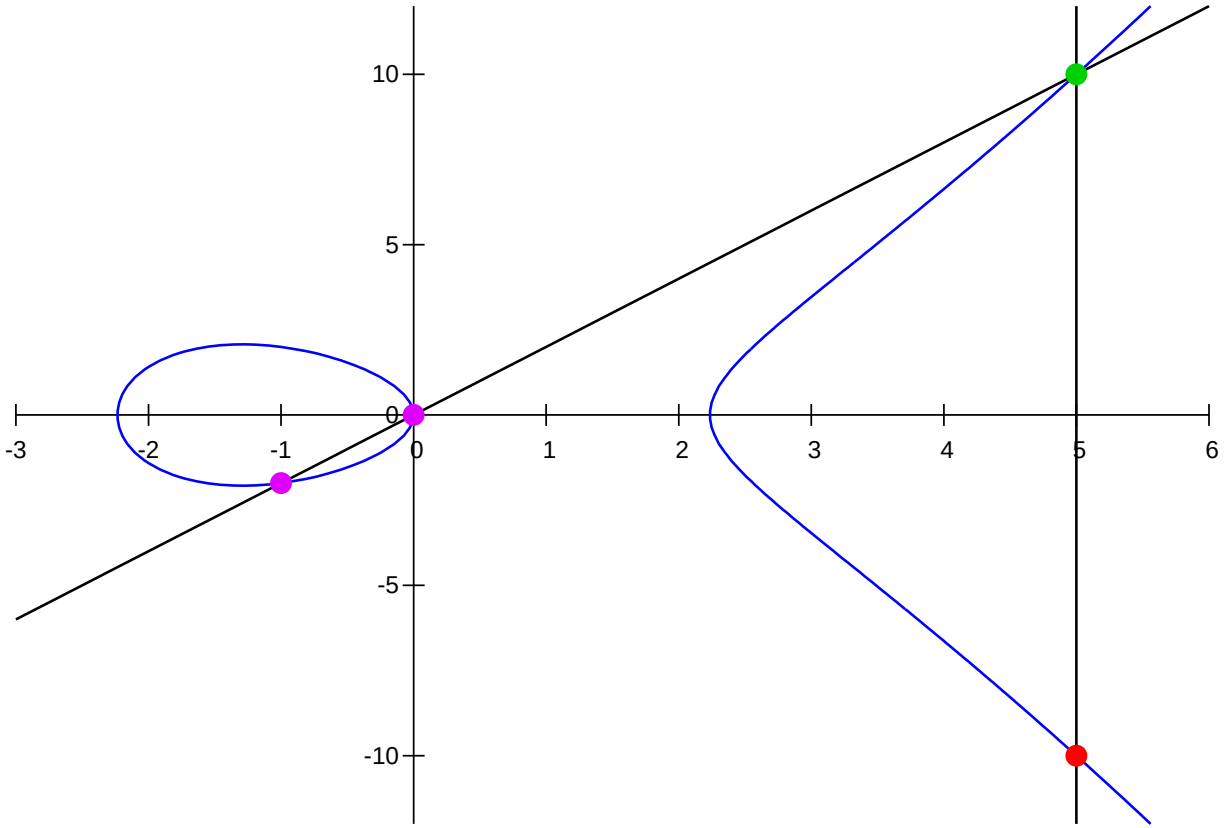
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $p = (-1, -2)$, $q = (0, 0)$



It intersects E in the third point $-r = (5, 10)$

Addition of Distinct Points on E

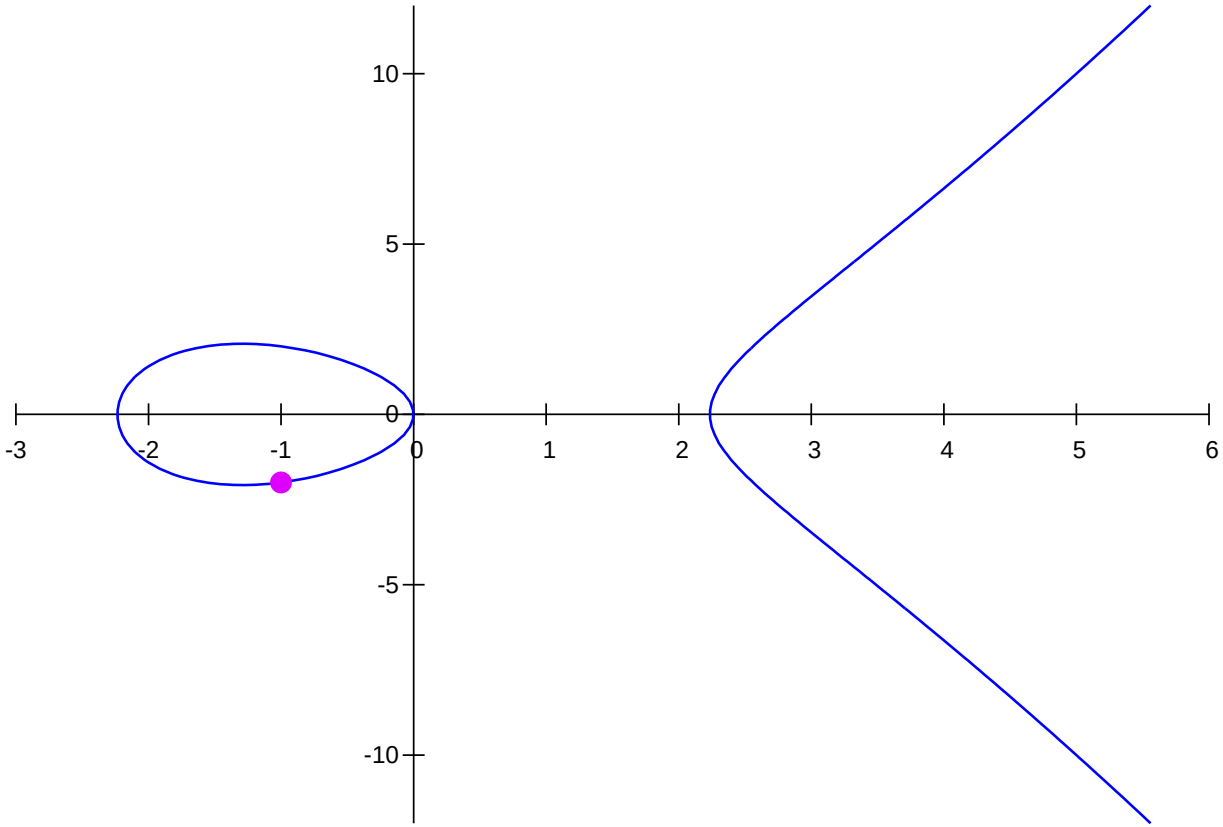
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $p = (-1, -2)$, $q = (0, 0)$



The sum $r = p + q$ is the inverse of $-r$, i.e. $r = (5, -10)$

Doubling on E

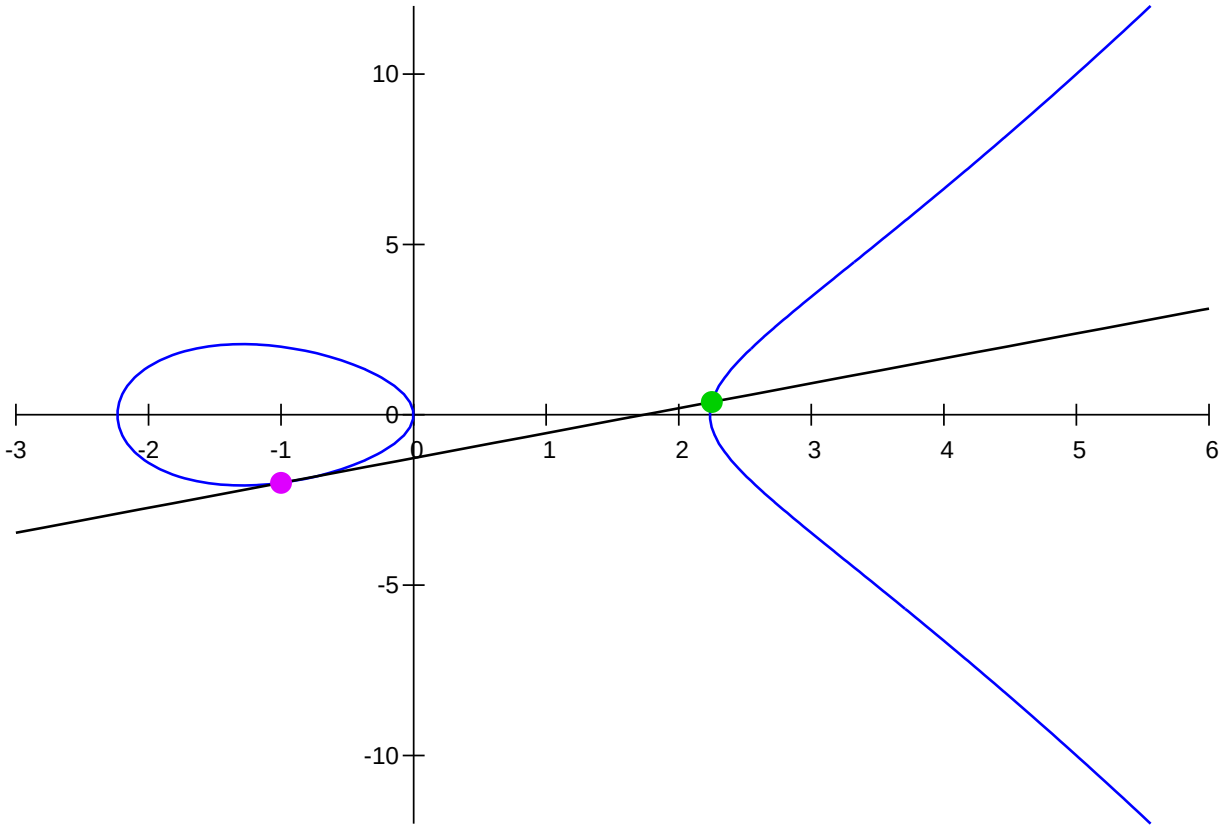
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $p = (-1, -2)$



The line tangent to E at p is $\boxed{y = \frac{19}{26}x - \frac{33}{26}}$

Doubling on E

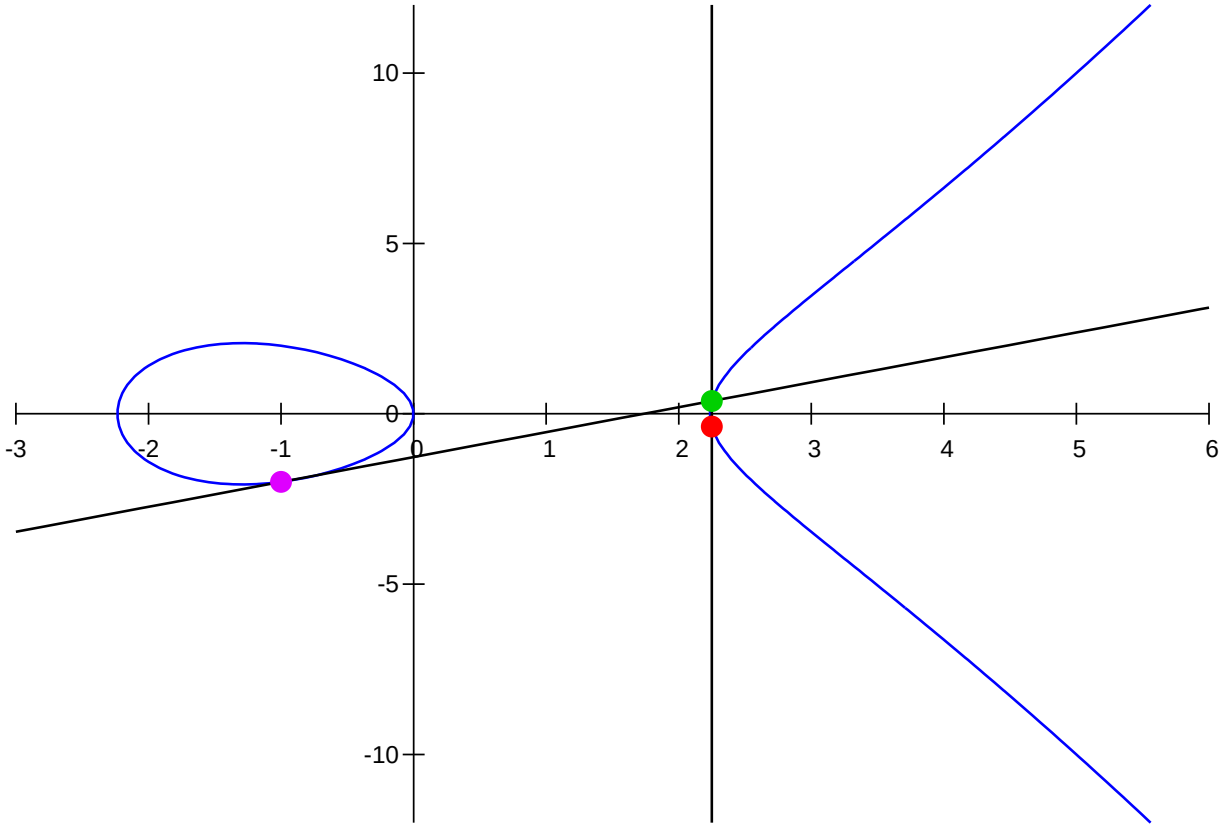
$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $p = (-1, -2)$



It intersects E in the third point $-r = \left(\frac{9}{4}, \frac{3}{8}\right)$

Doubling on E

$E : y^2 = x^3 - 5x$ over $\mathbb{Q}$, $p = (-1, -2)$



The sum $r = p + p$ is the inverse of $-r$, i.e. $r = \left(\frac{9}{4}, -\frac{3}{8}\right)$

Rational Points and Rational Places

Recall the addition law on $\mathbb{P}_1(F)$:

$$\begin{aligned} P \oplus Q = R \quad &\Leftrightarrow \quad [P - P_\infty] + [Q - P_\infty] = [R - P_\infty] \\ &\Leftrightarrow \quad [P] + [Q] - [R] = [P_\infty] \end{aligned}$$

Recall the addition law on $E(K)$: $p + q - r = \infty$.

Theorem

- *Let $(x_0, y_0) \in E(K) \setminus \{\infty\}$. Then exists a unique $P_{(x_0,y_0)} \in \mathbb{P}_1(F)$ such that $\operatorname{supp}(\operatorname{div}(x - x_0)) \cap \operatorname{supp}(\operatorname{div}(y - y_0)) = \{P_{(x_0,y_0)}, P_\infty\}$.*
- *The map $\Psi : E(K) \to \mathbb{P}_1(K)$ via $(x_0, y_0) \mapsto P_{(x_0,y_0)}$ and $\infty \mapsto P_\infty$ is a group isomorphism.*

So we have group isomorphisms

$$(E(K), \text{ point addition}) \overset{\Psi}{\longleftrightarrow} (\mathbb{P}_1(F), \oplus) \overset{\Phi}{\longleftrightarrow} (\mathrm{Cl}^0(F), \text{ divisor addition})$$

Hyperelliptic Function Fields

Hyperelliptic Function Fields

Definition

A function field F/K is hyperelliptic if it has genus at least 2 and there exists $x \in F$ such that $[F : K(x)] = 2$.

Properties:

- F/K is hyperelliptic if and only if there exists $D \in \mathrm{Div}(F)$ with $\deg(D) = 2$ and $\ell(D) \geq 2$.
- Every genus 2 function field is hyperelliptic.

Description: Write $F = K(x, y)$ with $[F : K(x)] = 2$.
Then $F/K(x)$ has a minimal polynomial of the form

$$y^2 + h(x)y = f(x)$$

where $h(x)$ and $f(x)$ are polynomials (after we make everything integral) and $h(x) = 0$ if K has characteristic $\neq 2$.

Hyperelliptic Curves

A hyperelliptic function field of genus g is of the form $F = K(x, y)$ where

$$C : y^2 + h(x)y = f(x)$$

with the following properties:

- $f(x), h(x) \in K[x]$;
- C is irreducible over $K(x)$;
- C is non-singular (or smooth), i.e. there are no simultaneous solutions to C and its partial derivatives with respect to x and y.
- $\deg(f) = 2g + 1$ or $2g + 2$;
- If K has characteristic $\neq 2$, then $h(x) = 0$;
- If K has characteristic 2, then $\deg(h) \leq g$ when $\deg(f) = 2g + 1$, and $h(x)$ is monic of degree $g + 1$ when $\deg(f) = 2g + 2$;

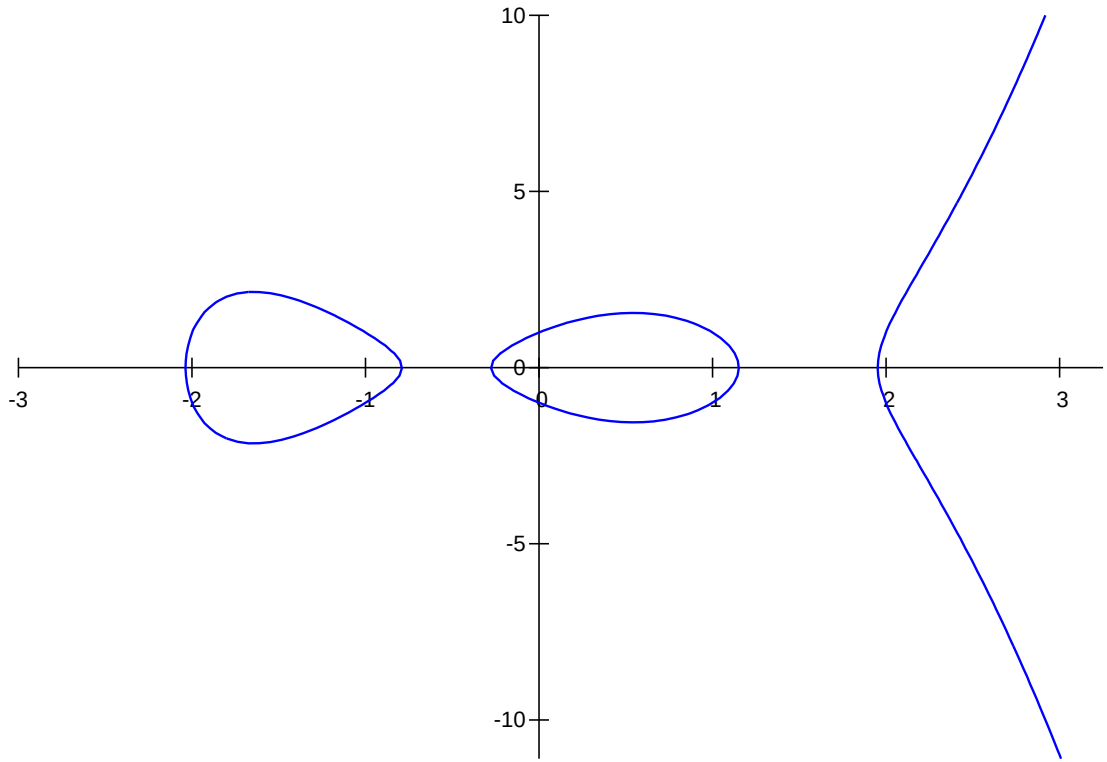
C is a hyperelliptic curve of genus g over K.

Remark: The case $g = 1$ and $\deg(f)$ odd also covers elliptic curves.

Examples

- Every hyperelliptic curve over a field K of characteristic $\neq 2$ has the form $y^2 = f(x)$ with $f(x) \in K[x]$ square-free.

- $y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$, genus $g = 2$



Classification by to Splitting at Infinity

Case 1: $\deg(f) = 2g + 1$ (odd). Then P_∞ ramifies in F.

Case 2: $\deg(f) = 2g + 2$ (even) and

$\operatorname{sgn}(f)$ is a square in K^* when q is odd;
$\operatorname{sgn}(f)$ is of the form $s^2 + s$ for some $s \in K$ when q is even.

Then P_∞ splits in F.

Case 3: $\deg(f) = 2g + 2$ (even) and

$\operatorname{sgn}(f)$ is a non-square in K^* when q is odd;
$\operatorname{sgn}(f)$ is not of the form $s^2 + s$ with $s \in K$ when q is even.

Then P_∞ is inert in F.

The representation of $F/K(x)$ by C is referred to as ramified, split, and inert according to these three cases, or alternatively as imaginary, real, and unusual.

Model Properties

- Ramified representations are the function field analogue of imaginary quadratic number fields. Split representations are the function field analogue of real quadratic number fields. Inert representations have no number field analogue.

- The variable transformation $x \mapsto 1/(x-a)$ and $y \mapsto y/(x-a)^{g+1}$, with $f(a) \neq 0$, converts a ramified representation of $F/K(x)$ into a split or inert representation of $F/K(x)$ without changing the underlying rational function field $K(x)$.

- The same variable transformation, with $f(a) = 0$, converts an inert or split representation of $F/K(x)$ into a ramified representation of $F(a)/K(a)(x)$; note that this may require an extension of the constant field.

- Inert models $F/K(x)$ become split when considered over a quadratic extension over K. They don't exist over algebraically closed fields.

Degree Zero Divisors

Let $D \in \mathrm{Div}^0(F)$.

Ramified model: $\mathrm{Con}_{F/K(x)}(P_\infty) = 2\infty$ with $\deg(\infty) = 1$.

$$D = D_0 - \deg(D_0)\infty \text{ with } \infty \notin \mathrm{supp}(D_0) \ .$$

This gives rise to a group isomorphism from $\mathrm{Div}^0(F)$ onto the group of *finite* divisors $\{D \in \mathrm{Div}(F) \mid \infty \notin \mathrm{supp}(D)\}$.

Split model: $\mathrm{Con}_{F/K(x)}(P_\infty) = \infty_+ + \infty_-$ with $\deg(\infty_+) = \deg(\infty_-) = 1$.

$$D = D_0 - \deg(D_0)\infty_- - n(\infty_+ - \infty_-) \text{ with } \infty_+, \infty_- \notin \mathrm{supp}(D_0) \text{ and } n \in \mathbb{Z} \ .$$

This gives rise to a surjective group homomorphism from $\mathrm{Div}^0(F)$ onto the group of finite divisors $\{D \in \mathrm{Div}(F) \mid \infty_+, \infty_- \notin \mathrm{supp}(D)\}$ with kernel $\langle \infty_+ - \infty_- \rangle$.

Henceforth concentrate on finite divisors.

Semi-Reduced and Reduced Divisors

UNIVERSITY OF CALGARY

Definition

A finite divisor D of F is semi-reduced if it is

- *effective*, i.e. $v_P(D) \geq 0$ for all $P \in \mathbb{P}(F)$, and
- *co-norm-free*, i.e. can't be written as $D = E + A$ where A is the con-norm of some divisor of $K(x)$.

D is reduced if it is semi-reduced and $\deg(D) \leq g$.

Proposition

A finite divisor is semi-reduced if and only if D is effective and for all finite $P \in \mathbb{P}(F)$, the following hold:

- If $P \cap K$ is inert in F, then $v_P(D) = 0$.
- If $P \cap K$ is ramified in F, then $v_P(D) \in \{0, 1\}$.
- If $P \cap K$ splits in F, say as $P + Q$, then either $v_P(D) = 0$ or $v_Q(D) = 0$.

More on Semi-Reduced Divisors

UNIVERSITY OF CALGARY

Lemma

Every class in $\mathrm{Cl}^0(F)$ contains a divisor whose finite part is semi-reduced.

Theorem

- *Every class in $\mathrm{Cl}^0(F)$ contains a divisor D whose finite part D_0 is reduced.*
- *If $F/K(x)$ is ramified, then D is unique.*
- *If $F/K(x)$ is split, then there is a unique such divisor D with $0 \leq n \leq g - \deg(D_0)$. All but at most g classes have $n = 0$, i.e. $D = D_0 - \deg(D_0)\infty_+$.*

Remark

If $[F : K(x)]$ is split, then the divisors $D = D_0 - \deg(D_0)\infty_+$ form the infrastructure of $F/K(x)$ (more on that later).

Mumford Representation of Places

Write $F = K(x, y)]$ with $y^2 + h(x)y = f(x)$.

Lemma

- *Let P be a finite place of F, and write $P \cap K(x) = P_{p(x)}$ with $p(x) \in K[x]$ monic and irreducible. Suppose $P_{p(x)}$ ramifies or splits in F. Then there exists a polynomial $v(x) \in K[x]$, unique modulo $p(x)$, with $v(x)^2 + h(x)v(x) \equiv f(x) \pmod{p(x)}$ and $v_P(v + y) > 0$. .*
- *Conversely, let $p(x), v(x) \in K[x]$ with $p(x)$ be monic and irreducible, and $v(x)^2 + h(x)v(x) \equiv f(x) \pmod{p(x)}$. Then $P_{p(x)}$ ramifies or splits in F and there exists a unique finite place P of F lying above $P_{p(x)}$ with $v_P(v + y) > 0$.*

Corollary

The polynomials $(p(x), v(x) \bmod p(x))$ as above are in one-to-one correspondence with the finite places P of F such that $P \cap K(x)$ ramifies or splits in F.

Mumford Representation of of Divisors

Theorem

- *Let D be a semi-reduced divisor of F. Then there exist $u(x), v(x) \in K[x]$, with $u(x)$ unique and $v(x)$ unique modulo $u(x)$, such that*
  - *$u(x)$ is monic;*
  - *$v(x)^2 + h(x)v(x) \equiv f(x) \pmod{u(x)}$;*
  - *$v_P(u) > 0$ and $v_P(y + v) > 0$ for all $P \in \mathrm{supp}(D)$.*
- *Conversely, let $u(x), v(x) \in K[x]$ with $u(x)$ monic and $v(x)^2 + h(x)v(x) \equiv f(x) \pmod{u(x)}$. Then the divisor $D = \sum n_P P$ where $n_P = \min\{v_P(u), v_P(y + v)\}$ for all finite places P of F is semi-reduced.*

Corollary and Definition

The polynomials $(u(x), v(x) \bmod u(x))$ as above are in one-to-one correspondence with the semi-reduced divisors D of F. They are the Mumford representation of D, and we write $D = (u, v)$.
Note also that $\deg(D) = \deg(u)$.

Examples of Mumford Representations

- The Mumford representation of the trivial divisor is $(1, 0)$.

- Suppose K has characteristic $\neq 2$ and $F = K(x, y)$ with $y^2 = f(x)$ square-free. Let $P \in \mathbb{P}(F)$ be ramified, and write $P \cap K(x) = P_{p(x)}$. Then $f(x) \equiv 0 \pmod{p(x)}$, and P has Mumford representation $(p(x), 0)$.

- Every finite point (x_0, y_0) on a hyperelliptic curve corresponds to a rational place P of the function field of C with Mumford representation $(x - x_0, y_0)$.

Semi-reduced Divisors and $K[x,y]$-ideals

Theorem

Let $u(x), v(x) \in K[x]$. Then the following are equivalent:

- *(u,v) is the Mumford representation of a reduced divisor of F.*
- *The $K[x]$-submodule of $K[x,y]$ of rank 2 generated by $u(x)$ and $v(x)+y$ is an ideal of $K[x,y]$.*
- $v(x)^2 + h(x)v(x) \equiv f(x) \pmod{u(x)}$.

Remark

If $F/K(x)$ is ramified, then the bijection between semi-reduced divisors and $K[x,y]$-ideals of the form above extends to a group isomorphism from $\mathrm{Cl}^0(F)$ onto the ideal class group of $K[x,y]$.

Arithmetic in $\mathrm{Cl}^0(F)$ for Ramified Models

UNIVERSITY OF CALGARY

Goal: efficient arithmetic on $\mathrm{Cl}^0(F)$ via unique reduced divisor class representatives in Mumford representations when $F/K(x)$ is ramified:

$$[D_1] + [D_2] = [D_1 \oplus D_2] \qquad \text{where}$$

- D_1 and D_2 are the unique reduced divisors in their respective classes;
- $D_1 \oplus D_2$ is the unique reduced divsor in the class of $D_1 + D_2$;
- All three divisors are given in Mumford representation.

Road map: Cantor's Algorithm

1. First compute a semi-reduced divisor D equivalent to $D_1 + D_2$ in Mumford representation.
2. Then reduce D, i.e. compute the Mumford representation of the unique reduced divisor $D_1 \oplus D_2$ equivalent to D.

Divisor Addition, Simplest Case

Consider a ramified hyperelliptic function field $F = K(x, y)$ where $y^2 + h(x)y = f(x)$.

Let $D_1 = (u_1, v_1)$ and $D_2 = (u_2, v_2)$.

Proposition

$D_1 + D_2$ is semi-reduced if and only if $\gcd(u_1, u_2, v_1 + v_2 + h) = 1$.

In this case, $D_1 + D_2 = (u, v)$ where

$$u = u_1 u_2 \ , \quad v \equiv \begin{cases} v_1 & (\mathrm{mod}\ u_1)\,, \\ v_2 & (\mathrm{mod}\ u_2)\,. \end{cases}$$

Divisor Addition, General Case

UNIVERSITY OF CALGARY

Theorem

Let $D_1 = (u_1, v_1)$ and $D_2 = (u_2, v_2)$ be semi-reduced divisors. Then $D_1 + D_2 = D + \mathrm{div}(s)$ where $D = (u, v)$ is a semi-reduced divisor, and $s, u, v \in K[x]$ are computed as follows:

1. *Let $s = \gcd(u_1, u_2, v_1 + v_2 + h) = au_1 + bu_2 + c(v_1 + v_2 + h)$ where $a, b, c \in K[x]$ are computed using the extended euclidean algorithm.*
2. *Set $u = \dfrac{u_1 u_2}{s^2}$.*
3. *Set $v \equiv \dfrac{au_1 v_2 + bu_2 v_1 + c(v_1 v_2 + f)}{s} \pmod{u}$.*

Note that even when D_1 and D_2 are reduced, D is generally **not** reduced!

Divisor Reduction

Let $D = (u, v)$ be a semi-reduced divisor with $\deg(u) > g$. Set

$$u' = \frac{f + hv - v^2}{u}, \quad v' \equiv h - v \pmod{u'}.$$

Properties:

- The divisor $D' = (u', v')$ is equivalent to D.
- If $\deg(u) \geq g + 2$, then $\deg(u') \leq \deg(u) - 2$.
- If $\deg(u) = g + 1$, then $\deg(u') \leq g$.

Remarks

- If we repeatedly compute (u', v') and substitute these values for u and v, we will obtain the reduced divisor $D' = (u', v')$ equivalent to D.
- The number of these reduction steps required to obtain D' is $\lceil (\deg(u) - g)/2 \rceil$.
- If D was obtained by addition of two reduced divisors, then $\deg(u) \leq 2g$, and hence the number of reduction steps is $\lceil g/2 \rceil$.

Inert Models

One infinite degree 2 place ∞.

Properties:

- If $F/K(x)$ is inert and L is a quadratic extension of K, then $FL/L(x)$ is split.
- Only the finite divisors of even degree correspond to degree zero divisors $D_0 - (\deg(D_0)/2)\infty$.
- If $K = \mathbb{F}_q$, then very degree zero divisor class contains either a unique reduced representative or $q+1$ almost reduced divisors (semi-reduced and $\deg(D_0) = g+1$, Artin 1924).
- Reduction finds the reduced or an almost reduced representative. For the latter case, Artin provided a procedure for finding the other q almost reduced equivalent divisors.

Split Models

Two infinite places ∞_+, ∞_-, both of degree 1.

Theorem (Paulus & Rück 1999)

Every degree zero divisor class has a unique representative of the form $D_0 - \deg(D_0)\infty_- + n(\infty_+ - \infty_-)$, *where* D *is reduced and* $0 \le n \le g - \deg(D_0)$.

Divisor class addition: Cantor plus adjustment steps (usually $\lceil g/2 \rceil$ of them) to get n to the correct range.
Infrastructure: Divisors with $n = 0$ ("almost" a group)

Theorem (Galbraith, Harrison & Mireles Morales 2008)

Every degree zero divisor class has a unique balanced representative $D_0 + \deg(D_0)\infty_- + n(\infty_+ - \infty_)$, *where* D *is reduced and* $-\lceil g/2 \rceil \le n \le \lfloor g/2 \rfloor - \deg(D_0)$.

Divisor class addition: Cantor with occasionally some balancing steps.

Why Consider Split Representations?

UNIVERSITY OF CALGARY

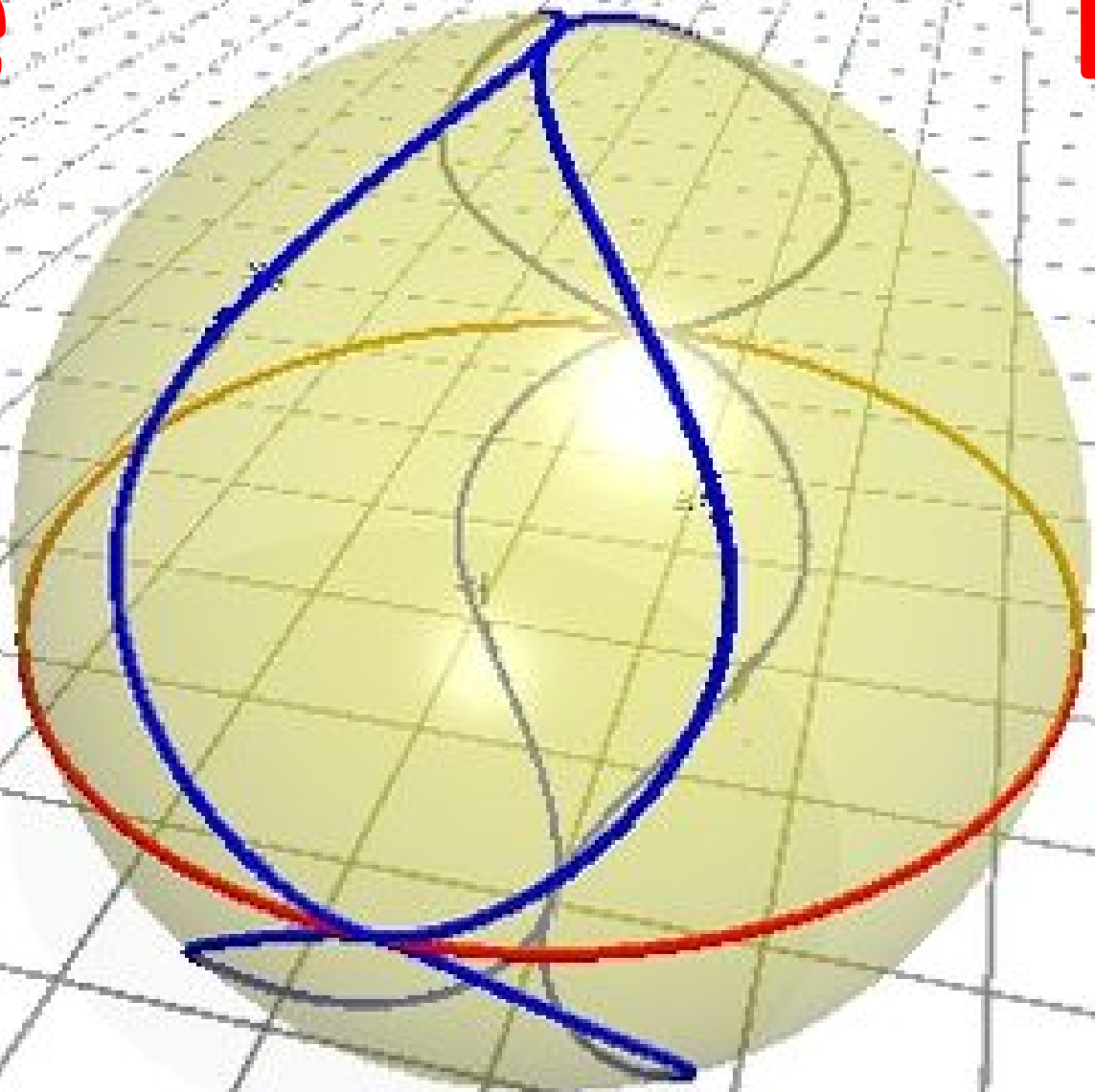
Advantages:

- A ramified representation need not always exist.
- Construction methods (e.g. for cryptography) don't always produce ramified models.
- Ramified $F/K(x)$ models can be converted to split models $F/K(x)$, but the reverse direction is only possible over a base field that contains a rational point.
- Mathematically interesting.
- Less researched than ramified models.

Disadvantages:

- Mathematically more complicated than ramified models.
- Arithmetic is slightly slower.
- Less researched than ramified models.

The End



$y^2=x^6+x^2+x$

http://voltage.typepad.com/superconductor/2011/09/a-projective-imaginary-hyperelliptic-curve.html