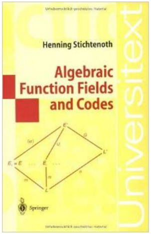
An Introduction to Function Fields

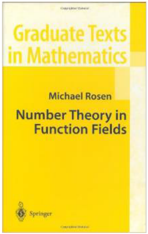
Renate Scheidler

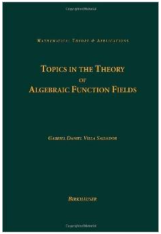
PIMS Summer School *Inclusive Paths to Number Theory*
August 23-27, 2021
University of Calgary

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 $a = 0$
- $|ab| = |a||b|$
- $|a+b| \leq |a| + |b|$ (archimedean) or
  $|a+b| \leq \max\{|a|, |b|\}$ (non-archimedean)

Examples

- The well-known absolute value on $\mathbb{Q}$ (or on $\mathbb{R}$ or on $\mathbb{C}$) is an archimedean 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-archimedean absolute value.

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

Let p be a 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 $\mathbb{Q}$.

Rational Function Fields

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-archimedean 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-archimedean 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-archimedean (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 $c = e = 2.71828\ldots$.

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-archimedean 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 $K(x)$.

UNIVERSITY OF CALGARY

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 $\mathbb{Q}$:

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

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

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

Example: Infinite Valuation on $K(x)$

UNIVERSITY OF CALGARY

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

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

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

Example

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

UNIVERSITY OF CALGARY

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

UNIVERSITY OF CALGARY

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. F/K is global if K is finite.

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 $[F : K(y)] = \deg(f)$.

UNIVERSITY OF CALGARY

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 $F/K(x)$.

More on Function Fields and Curves

General form of a function field F/K:

$$F = K(x, y) \quad \text{with} \quad \Phi(x, y) = 0 \ ,$$

where $\Phi(x, Y)$ is a polynomial in Y with coefficients in $K(x)$ that is irreducible over $K(x)$ and has a root $y \in F$.

Note that a function field has many defining curves!

Example: Let $A, B \in K$ and consider the two curves

$$C_1 : y^2 = x^3 + Ax + B \ ,$$
$$C_2 : v^2 = Bu^4 + Au^3 + u \ .$$

Then $K(x, y) = K(u, v)$.
Dividing C_1 by x^4 and putting $u = x^{-1}$, $v = yx^{-2}$ yields C_2.

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 (otherwise $\tilde{K} = K(y)$ and $F = \tilde{K}(x)$).
- Suppose -1 is not a square in K (e.g. $K = \mathbb{R}$ or $K = \mathbb{F}_q$ with $q \equiv 3 \pmod 4$).

  Let $F = K(x, y)$ where $x^2 + y^4 = 0$. Then $[F : K(x)] = 4$.

  Let $i \notin K$ be a square root of -1. Then $i^2 + 1 = 0$, so i is algebraic over K. Thus $i \in \tilde{K} \setminus K$. In fact, $\tilde{K} = K(i)$, so F/K is not geometric.

  Over $\tilde{K}$, we have $x \pm iy^2 = 0$.

  Note that $[\tilde{K} : K] = [\tilde{K}(x) : K(x)] = 2$ and $[F : \tilde{K}(x)] = 2$.

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 $K(x)$

UNIVERSITY OF CALGARY

- 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.

Divisors and Class Groups

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.

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 surjective group homomorphism $v_P : \text{Div}(F) \to \mathbb{Z} \cup \{\infty\}$.
  - The degree map defined on places of F extends to a group homomorphism $\deg : \text{Div}(F) \to \mathbb{Z} \cup \{\infty\}$ whose kernel is the subgroup $\text{Div}^0(F)$ of $\text{Div}(F)$ 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 $\text{Div}(F)$ is surjective.

Principal Divisors

UNIVERSITY OF CALGARY

Definition

A divisor $D \in \text{Div}(F)$ 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 $D = \text{div}(z)$.

Definition

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

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

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

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

More on Principal Divisors

UNIVERSITY OF CALGARY

Theorem

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

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

Definition

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

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

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 the latter is referred to as just the class group of F/K.)

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 class number of F/K.
- h_F is always finite for a function field F/K over a *finite* field K.

Theorem

Let F/K be a non-rational function field that has a rational place, denoted P_∞. Then the map

$$\Phi : \mathbb{P}_1(F) \to \mathrm{Cl}^0(F) \quad \textit{via} \quad P \mapsto [P - P_\infty]$$

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_∞).

The class group and class number are important invariants of any function field. Unfortunately, they are not easy to compute ... ☹

UNIVERSITY OF CALGARY

Definition

Define a partial order $\geq$ on $\text{Div}(F)$ 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 $D \in \text{Div}(F)$ 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 $\text{Div}(F)$.

Decomposition of Places

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

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

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

Function Field Extensions

Notation and Assumption

- K is perfect, i.e. every irreducible polynomial in $K[x]$ has distinct roots.
- F/K is a geometric function field.
- Fix any $x \in F \setminus K$ and put $n = [F : K(x)]$ (extension degree).

Remarks

- Finite fields, algebraically closed fields, and characteristic 0 fields are all perfect.
- $K = \mathbb{F}_p(x)$ is *not* perfect:

  E.g. let α be a root of $\phi(T) = T^p - x$, so $\alpha^p = x$.

  Then $\phi(T) = (T^p - \alpha^p) = (T - \alpha)^p$, so α has multiplicity p.

Recap: the Places of $K(x)$

Finite places of $K(x)$:

- $P_{p(x)}$, where $p(x) \in K[x]$ is monic and irreducible;
- Uniformizer is $p(x)$;
- Residue field is $F_{P_{p(x)}} = K[x]/(p(x))$;
- Degree of $P_{p(x)}$ is $\deg(P_{p(x)}) = \deg(p(x))$.

Infinite place of $K(x)$:

- P_∞, corresponding to the infinite valuation (denominator degree minus numerator degree);
- Uniformizer is x^{-1};
- Residue field is $F_{P_\infty} = K$;
- Degree of P_∞ is $\deg(P_\infty) = 1$.

Places in $K(x)$ and F

For a place P' of F, the intersection $P = P' \cap K(x)$ is a place of $K(x)$.

We write $P'|P$ and say that P' lies above P and P lies below P'.

Theorem

- *Every place P' of F lies above a unique place P of $K(x)$.*
- *Every place P of $K(x)$ lies below finitely many places P' of F.*
- *$P'|P$ if and only if $P = P' \cap K(x)$ and $O_P = O_{P'} \cap K(x)$; In this case $O_{P'}$ is an O_P-module of rank $n = [F : K(x)]$.*

The "lift" $P\,O_{P'}$ of P to F is no longer a place. Rather, it is a divisor of F called the *co-norm* of P.

Decomposition Data

UNIVERSITY OF CALGARY

Theorem and Definition

- The co-norm of $P \in \mathbb{P}(K(x))$ is the divisor
$$coN(P) = \sum_{P'|P} e(P'|P)P'$$
of F, where $e(P'|P)$ is the ramification index of $P'|P$, defined via $v_{P'}(r) = e(P'|P)v_P(r)$ for all $r(x) \in K(x)$.
- For all $P'|P$, the norm of P' is the divisor
$$N(P') = f(P'|P)P$$
of F, where $f(P'|P)$ is called the residue (or relative degree) of $P'|P$, defined as the residue field extension degree $f(P'|P) = [F_{P'} : K(x)_P]$.
- $\deg(P') = f(P'|P)\deg(P)$ for all $P'|P$.
- Fundamental identity: $\sum_{P'|P} e(P'|P)f(P'|P) = n$ for all $P \in \mathbb{P}(K(x))$.

Decomposition Terminology

Definition

Let $P \in \mathbb{P}(K(x))$.

- P is unramified in F if $e(P'|P) = 1$ for all $P'|P$ and ramified otherwise.
- P is wildly ramified in F if char(K) divides $e(P'|P)$ for some $P'|P$, and tamely ramified otherwise.
- P is totally ramified in F if there is a unique $P'|P$ with $e(P'|P) = n$.
- P is inert in F in F if there is a unique $P'|P$ with $f(P'|P) = n$.
- 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:

- char$(K) = 0$.
- $n <$ char(K) when char(K) is positive.

Computing Ramification Data

UNIVERSITY OF CALGARY

Theorem (Kummer's Theorem in function fields)

Let $F = K(x, y)$, $P \in \mathbb{P}(K(x))$, and let $\Phi(Y) \in O_P[Y]$ be the minimal polynomial of y over O_P. Let

$$\Phi(Y) \equiv \phi_1(Y)^{\epsilon_1}\, \phi_2(Y)^{\epsilon_2}\, \cdots\, \phi_r(Y)^{\epsilon_r} \pmod{P}$$

be the factorization of $\Phi(Y) \pmod{P}$ into powers of distinct monic irreducible polynomials in $O_P(Y)$. Then the following hold:

1. *The number of places of F lying above P is at least r.*
2. *For the i-th place $P_i'|P$, we have $f(P_i'|P) \geq \deg(\phi_i)$.*
3. *Under certain conditions, equality holds in items 1 and 2, and $e(P_i'|P) = \epsilon_i$.*

Two sufficient conditions for item 3 are:

- *All $\epsilon_i = 1$ (so $\Phi(Y)$ is squarefree modulo P) or*
- *$\{1, y, \ldots, y^{n-1}\}$ is an O_P-basis of $\bigcap_{i=1}^{r} O_{P_i'}$.*

Example: Quadratic Fields, Part I

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

For a finite place $P = P_{p(x)}$ of $K(x)$:

$$\Phi(Y) = Y^2 - f(x) \pmod{p(x)} .$$

1. Case $p(x) \nmid f(x)$ and $f(x)$ is a square modulo $p(x)$:

   $$f(x) \equiv h(x)^2 \pmod{p(x)}$$

   with $h(x) \in K[x]/(p(x))$ non-zero. Then

   $$\Phi(Y) \equiv (Y - h(x))(Y + h(x)) \pmod{p(x)} .$$

   So there are two places $P_1', P_2' \in \mathbb{P}(F)$ with

   $$e(P_1'|P) = e(P_2'|P) = f(P_1'|P) = f(P_2'|P) = 1 .$$

   Hence P splits completely in F.

Example: Quadratic Fields, Part II

2. Case $p(x) \nmid f(x)$ and $f(x)$ is not a square modulo $p(x)$:

$$\Phi(Y) \equiv Y^2 - f(x) \pmod{p(x)} \text{ irreducible over } K[x]/(p(x)) .$$

So there is one place $P' \in \mathbb{P}(F)$ with

$$e(P'|P) = 1 , \quad f(P'|P) = 2 .$$

Hence P is inert in F.

3. Case $p(x) \mid f(x)$:

$$\Phi(Y) \equiv Y^2 - f(x) \equiv Y^2 \pmod{p(x)} .$$

Kummer's Theorem is inconclusive. However, for any place $P'|P$:

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

So there is one place $P' \in \mathbb{P}(F)$ with

$$e(P'|P) = 2 , \quad f(P'|P) = 1 .$$

Hence P is totally ramified in F.

Example: Quadratic Fields, Part III

For the infinite place $P = P_\infty$, recall that

- x^{-1} is a uniformizer of P_∞,
- $O_\infty = \{f(x)/g(x) \in K(x) \mid \deg(f(x)) \leq \deg(g(x))\}$,
- $F_\infty = O_\infty / P_\infty = K$.

Write $f(x) = ax^{2m-\delta} +$ terms of lower degree in x, with $0 \neq a \in K$ and $\delta \in \{0, 1\}$, and put $z = yx^{-m}$. Then

$$z^2 = \frac{y^2}{x^{2m}} = \frac{f(x)}{x^{2m}} = \frac{a}{x^\delta} + \text{multiples of } \frac{1}{x} .$$

Note that $F = K(x, z)$ and the minimal polynomial of z over O_∞ is

$$\Phi(Z) = Z^2 - \left(\frac{a}{x^\delta} + \text{multiples of } \frac{1}{x} \right) \equiv Z^2 - \frac{a}{x^\delta} \pmod{\frac{1}{x}} .$$

Example: Quadratic Fields, Part IV

UNIVERSITY OF CALGARY

1. Case $\deg(f(x))$ even and a is a square in K, say $a = b^2$ with $b \in K^*$:
$$\Phi(Z) \equiv Z^2 - a \equiv Z^2 - b^2 \equiv (Z-b)(Z+b) \left(\bmod \frac{1}{x}\right) .$$
Then P_∞ splits completely in F.

2. Case $\deg(f(x))$ even and a is not a square in K:
$$\Phi(Z) \equiv Z^2 - a \left(\bmod \frac{1}{x}\right) \text{ irreducible over } K .$$
Then P_∞ is inert in F.

3. Case $\deg(f(x))$ is odd.
$$\Phi(Z) \equiv Z^2 - \frac{a}{x} \equiv Z^2 \left(\bmod \frac{1}{x}\right) .$$
Kummer's Theorem is inconclusive. However, for any place $P'|P$:
$$-e(P'|P)\deg(f(x)) = e(P'|P)v_\infty(f(x)) = v_{P'}(f(x)) = 2v_{P'}(y) .$$
Hence, 2 divides $e(P'|P)$, so P is totally ramified in F.

Let $F = \mathbb{F}_5(x, y)$ with $y^2 = x^3 + x = x(x+2)(x+3) \in \mathbb{F}_5[x]$.

- The ramified places of $\mathbb{F}_5(x)$ are P_x, P_{x+2}, P_{x+3} and P_∞.
- The place $P_{x^3+x^2x+3}$ of $\mathbb{F}_5(x)$ splits completely in F because
  $x^3 + x = (x^2+2)^2 + (x+2)(x^3+x^2+x+3) \equiv (x^2+2)^2 \quad (\text{mod } x^3$

Remark: When $K = \mathbb{F}_q$, determining whether or not $f(x)$ is a square modulo $p(x)$ can be done with the quadratic residue symbol

$$\left(\frac{f(x)}{p(x)}\right) = \begin{cases} 1 & \text{if } f(x) \text{ is a non-zero square} \quad (\text{mod } p(x)), \\ -1 & \text{if } f(x) \text{ is a non-square} \quad (\text{mod } p(x)), \\ 0 & \text{if } p(x) \text{ divides } f(x) \end{cases}.$$

This function field version of the Legendre symbol can be computed via

$$\left(\frac{f(x)}{p(x)}\right) \equiv f(x)^{\frac{|p(x)|-1}{2}} \equiv f(x)^{\frac{q^{\deg(p(x))}-1}{2}} \quad (\text{mod } p(x)) .$$

The Different

Assume that all places of $K(x)$ are tamely ramified in F.

Definition

The different (or ramification divisor) of $F/K(x)$ is

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

Example

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

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

- $P'_{p_i(x)}$ 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).

Definition

The genus of F/K is the integer

$$g = \frac{1}{2}\deg(\mathrm{Diff}(F)) - n + 1$$

for any $x \in F \setminus K$, where $n = [F : K(x)]$.

Examples:

- Every rational function field $K(x)$ has genus 0.
- Let $F = K(x, y)$ with $\mathrm{char}(K) \neq 2$; $y^2 = f(x)$ with $f(x) \in K[x]$ square-free. Then
  - $g = \lfloor(\deg(f) - 1)/2\rfloor$ (so $\deg(f) = 2g + 1$ or $2g + 2$).
  - $\deg(\mathrm{Diff}(F/K(x)) = 2g + 2$.

Bounds on $\mathbb{P}_1(F)$ and $\mathrm{Cl}^0(F)$ for K finite

UNIVERSITY OF CALGARY

Theorem (Hasse-Weil)

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

- $q + 1 - 2g\sqrt{q} \;\le\; |\mathbb{P}_1(F)| \;\le\; q + 1 + 2g\sqrt{q}$,
- $(\sqrt{q} - 1)^{2g} \;\le\; |\,\mathrm{Cl}^0(F)| \;\le\; (\sqrt{q} + 1)^{2g}$.

Corollary

$|\mathbb{P}_1(F)| \approx q$ *and* $|\,\mathrm{Cl}^0(F)| \approx q^g$ *for q large and g fixed.*

Corollary

Every rational function field $K(x)$ has class number one.

Remark

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

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.

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 $x^4 + y^2 = -1$ 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. Note that $[F : K(x)] = 2$ and $[F : K(y)] = 3$.

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

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

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

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 $(K\text{-})$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:

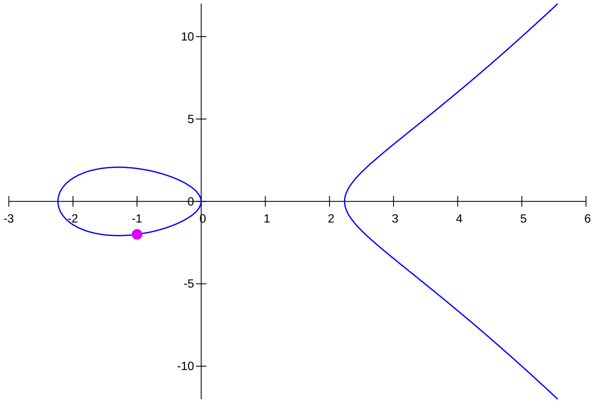
$$E_H : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

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 $z \neq 0$
∞	$\longleftarrow$	$[0 : 1 : 0]$

An Elliptic Curve and a Point

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



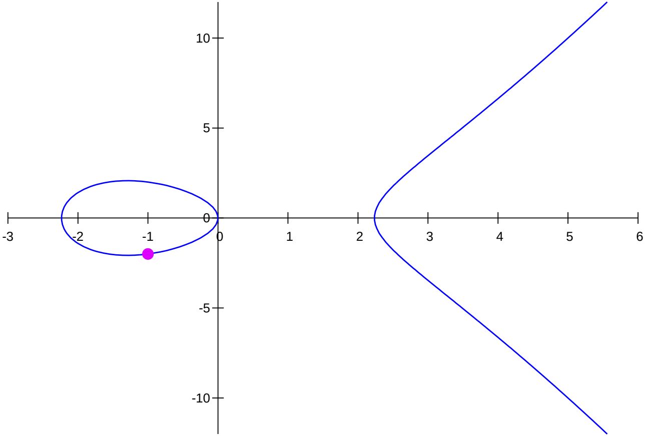
Any line intersects E in three points.

- Need to count multiplicities;
- One of the points may be ∞.

Group Law on $E(K)$:

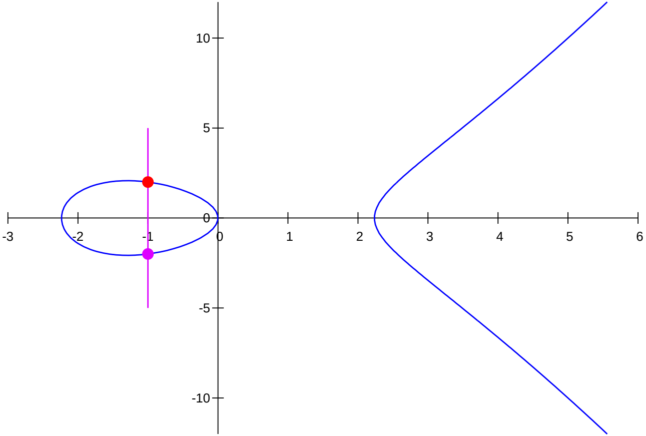
- Identity: ∞.
- Inverses: $-p$ is defined as the third point of intersection of the line through p and ∞ with E.
  For short Weierstraß models, this line is "vertical", so if $p = (x_0, y_0)$, then $-p = (x_0, -y_0)$.
- Addition:"Any three collinear points on E sum to zero (i.e. ∞)."
  - If $p \neq q$, 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.

Inverses on Elliptic Curves



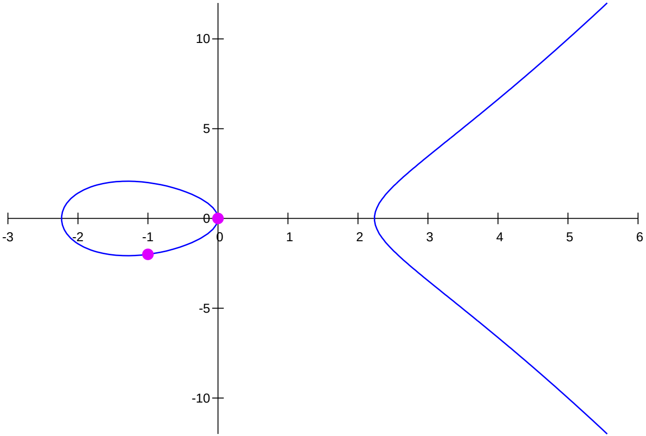
$-(\bullet) = ?$

Inverses on Elliptic Curves



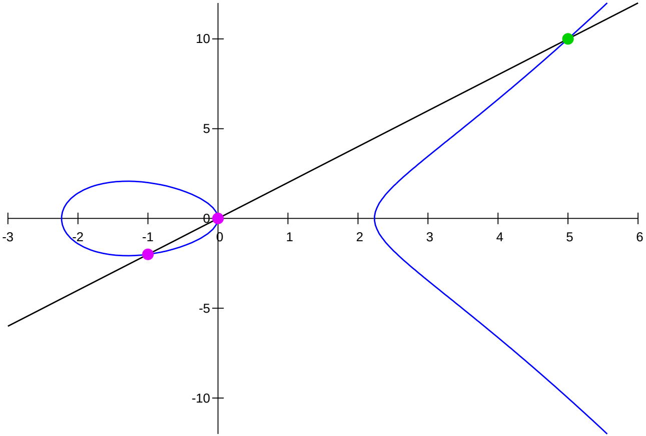
$$\bullet + \bullet + \infty = 0 \qquad \Rightarrow \qquad -(\bullet) = \bullet$$

Addition on Elliptic Curves



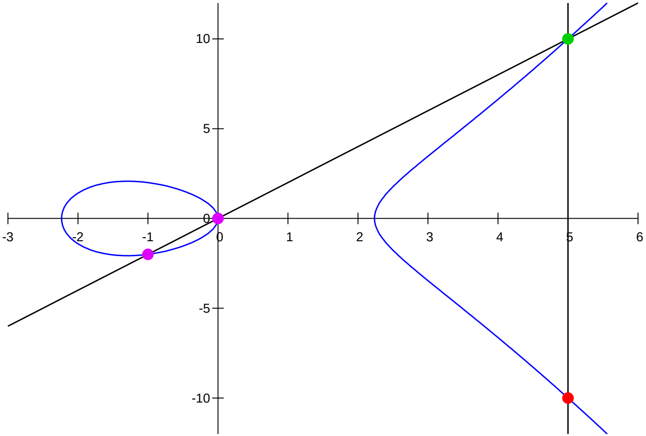
$\bullet + \bullet = ?$

Addition on Elliptic Curves



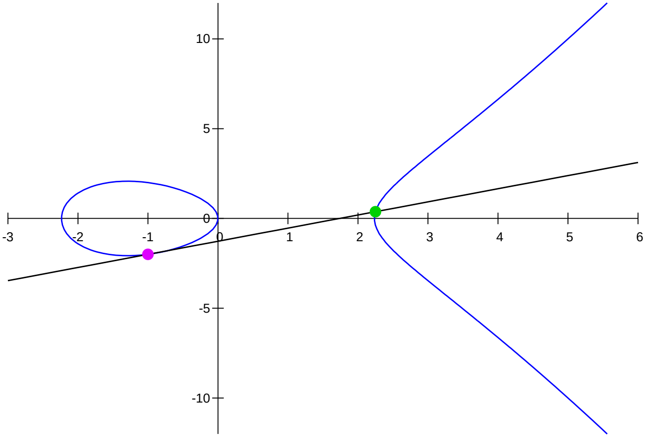
● + ● + ● = 0

Addition on Elliptic Curves

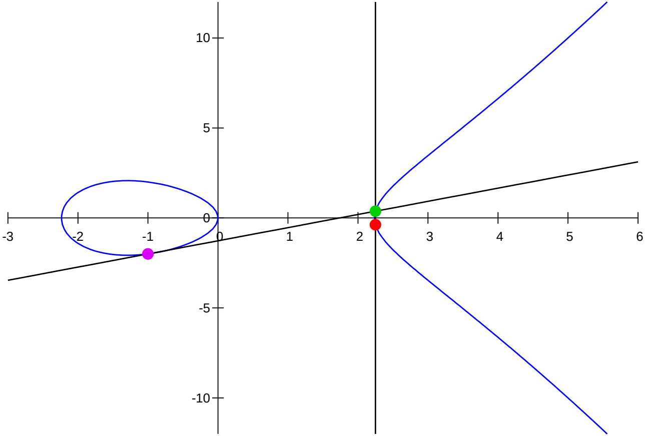


$\bullet + \bullet + \bullet = 0 \quad \Rightarrow \quad \bullet + \bullet = \bullet$

Doubling on Elliptic Curves



$2 \times$ ● $= ?$



$$2 \times \bullet + \bullet = 0 \qquad \Rightarrow \qquad 2 \times \bullet = \bullet$$

Arithmetic on Short Weierstraß Form

Let

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \qquad (P_1 \neq \infty,\ P_2 \neq \infty,\ P_1 + P_2 \neq \infty)\ .$$

Then

$$\begin{aligned} -P_1 &= (x_1, -y_1) \\ P_1 + P_2 &= (\lambda^2 - x_1 - x_2,\ -\lambda^3 + \lambda(x_1 + x_2) - \mu) \end{aligned}$$

where

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases} \qquad \mu = \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\[2ex] \dfrac{-x_1^3 + Ax_1 + 2B}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

Rational Points and Rational Places

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

$$P \oplus Q = R \quad \Leftrightarrow \quad [P - P_\infty] + [Q - P_\infty] = [R - P_\infty]$$
$$\Leftrightarrow \quad [P] + [Q] - [R] = [P_\infty]$$

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* $\mathrm{supp}(\mathrm{div}(x - x_0)) \cap \mathrm{supp}(\mathrm{div}(y - y_0)) = \{P_{(x_0,y_0)}, P_\infty\}$.
- *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 $[F : K(x)] = 2$.

Remark

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 $\neq 2$.

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:

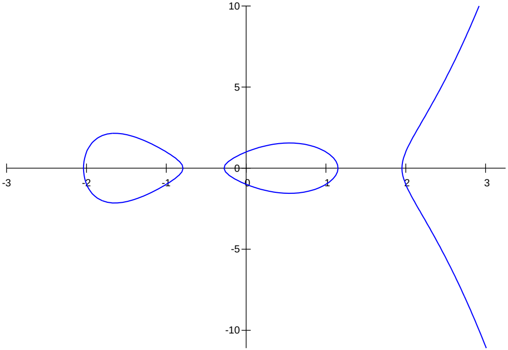
- $f(x), h(x) \in K[x]$;
- C is irreducible over $K(x)$;
- C is non-singular (or smooth), i.e. there are no simultaneous solutions to C and its partial derivatives with respect to x and y.
- $\deg(f) = 2g + 1$ or $2g + 2$;
- If K has characteristic $\neq 2$, then $h(x) = 0$;
- If K has characteristic 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 $f(x) \in K[x]$ squarefree.
- $y^2 = x^5 - 5x^3 + 4x - 1$ over $\mathbb{Q}$, genus $g = 2$:



Note that the cord & tangent law no longer works when $g \geq 2$. In fact, any injection $\Phi : \mathbb{P}_1(F) \to Cl^0(F)$ is no longer surjective.

Classification by to Splitting at Infinity

Let $\mathrm{sgn}(f)$ denote the leading coefficient of $f(x)$.

Case 1: $\deg(f) = 2g + 1$ (odd). Then the infinite place of $K(x)$ ramifies in F.

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

$\mathrm{sgn}(f)$ is a square in K^* when $\mathrm{char}(K) \neq 2$;

$\mathrm{sgn}(f)$ is of the form $s^2 + s$ for some $s \in K$ when $\mathrm{char}(K) = 2$.

Then the infinite place of $K(x)$ splits in F.

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

$\mathrm{sgn}(f)$ is a non-square in K^* when $\mathrm{char}(K) \neq 2$;

$\mathrm{sgn}(f)$ is not of the form $s^2 + s$ with $s \in K$ when $\mathrm{char}(K) = 2$.

Then the infinite place of $K(x)$ 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. We will not discuss them here.

Theorem

- *Suppose $F/K(x)$ is ramified, with infinite place $P_\infty \in \mathbb{P}(F)$. Then every degree divisor class in $Cl^0(F)$ contains a unique divisor of the form*
$$D = D_0 - \deg(D_0)P_\infty \ ,$$
where D_0 is effective, $\deg(D_0) \leq g$ and $P'_\infty \notin supp(D_0)$.
- *Suppose $F/K(x)$ is split, with infinite places $P_{\infty,1}, P_{\infty,2} \in \mathbb{P}(F)$. Then every degree divisor class in $Cl^0(F)$ contains a unique divisor of the form*
$$D = D_0 - \deg(D_0)P_{\infty,2} + n(P_{\infty,1} - P_{\infty,2}) \ ,$$
where D_0 is effective, $\deg(D_0) \leq g$, $P_{\infty,1}, P_{\infty,2} \notin supp(D_0)$ and $-\lceil g/2 \rceil \leq n \leq \lfloor g/2 \rfloor - \deg(D_0)$.

The divisor D is said to be reduced.

Remarks:

- D is uniquely determined by D_0 when $F/K(x)$ is ramified and by the pair (D_0, n) when $F/K(x)$ is split.
- "Generically" (i.e. for almost all classes in $\mathrm{Cl}(F)$), unless K is small, we have $\deg(D_0) = g$ and hence

  $D = D_0 - gP_\infty$ when $F/K(x)$ is ramified;

  $D = D_0 - \lceil g/2 \rceil P_{\infty,1} - \lfloor g/2 \rfloor P_{\infty,2}$ when $F/K(x)$ is split.

Arithmetic in $Cl^0(F)$ is conducted on reduced divisors:

$$[D_1] + [D_2] = [\text{Reduced divisor in the class of } D_1 + D_2] ,$$

where D_1 and D_2 are reduced.

Question: How to efficiently compute the reduced divisor in $[D_1 + D_2]$?

Rational Points and Rational Places

Let $(x_0, y_0) \in K \times K$ be a rational point on C, i.e.

$$y_0^2 + h(x_0)y_0 = g(x_0) \ .$$

Then $\mathrm{supp}(\mathrm{div}(x - x_0)) \cap \mathrm{supp}(\mathrm{div}(y - y_0))$ contains a unique finite rational place $P_{(x_0,y_0)}$.

As before, we identity $(x_0, y_0) \leftrightarrow P_{(x_0,y_0)}$, but this is no longer a group isomorphism.

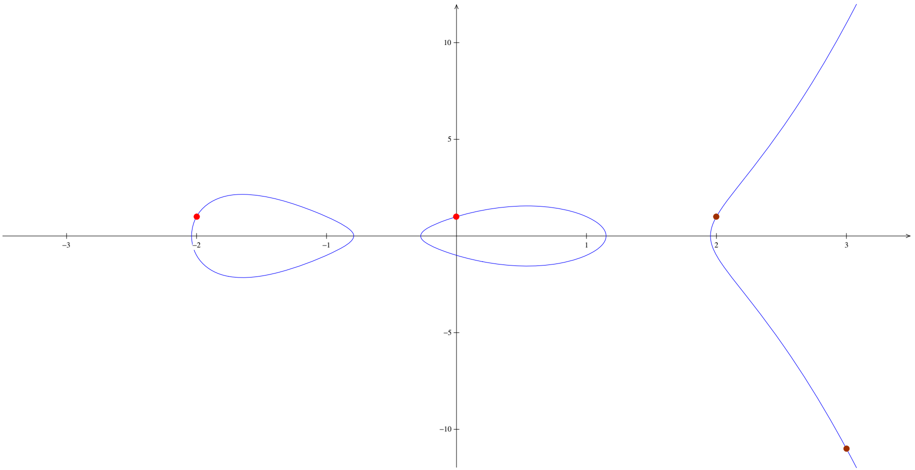
A divisor of the form

$$D = \sum_{i=1}^{r} P_i \in \mathrm{Div}(F) \quad \text{with} \quad P_i \in \mathbb{P}_1(F) \quad \text{for all } i$$

can thus be identified with a multiset of r rational points on C.

Example, Genus 2, Ramified Model

$D_1 = P_{(-2,1)} + P_{(0,1)}$, $D_2 = P_{(2,1)} + P_{(3,-11)}$



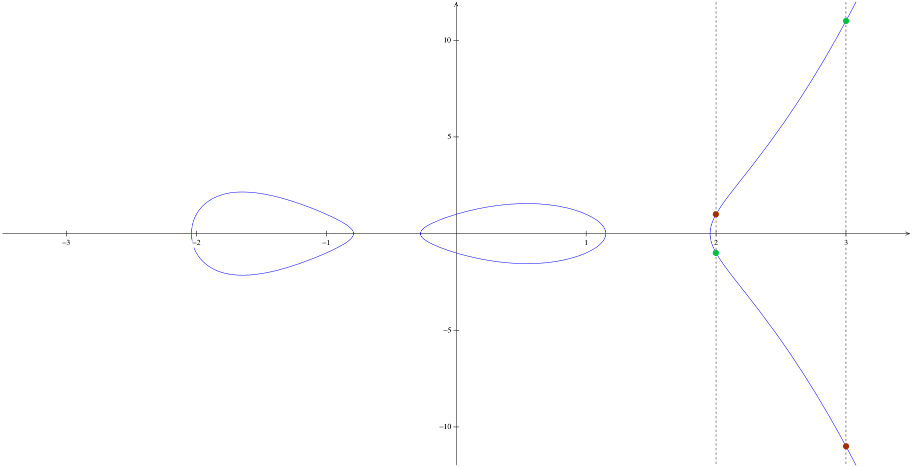
Group Law, Genus 2, Ramified Models

- Generic reduced divisors are determined by two finite points on C.
- The sum of two generic divisors consists of 4 finite points.
- Any 4 points on C determine a *cubic* $y = v(x)$ with $\deg(v(x)) = 3$. This cubic intersects C in two more points (again need to account for multiplicities)

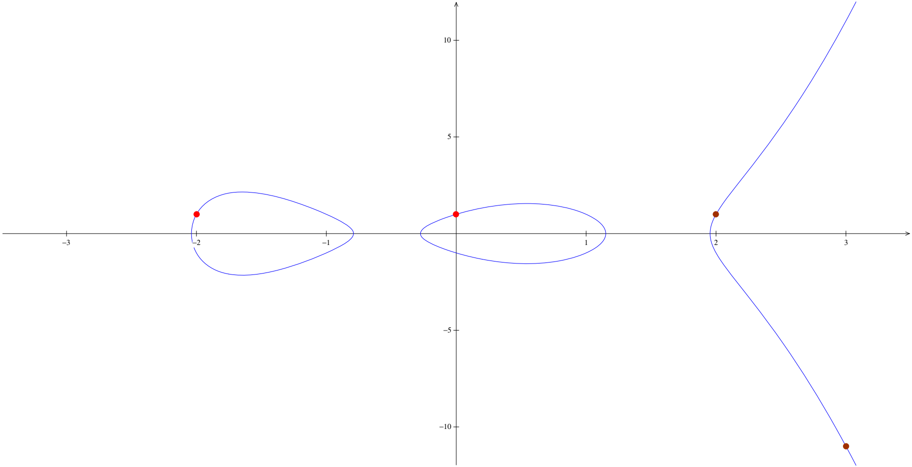
Degree 2 divisor class addition:

- Identity: $[0]$ ($D_0) = 0$).
- Inverses: invert points as before; the inverse of a divisor D consists of the inverses of the points in $\text{supp}(D)$.
- Addition: "Any three degree 2 divisors on C lying on a cubic sum to zero."

Inverses in Genus 2, Ramified Models

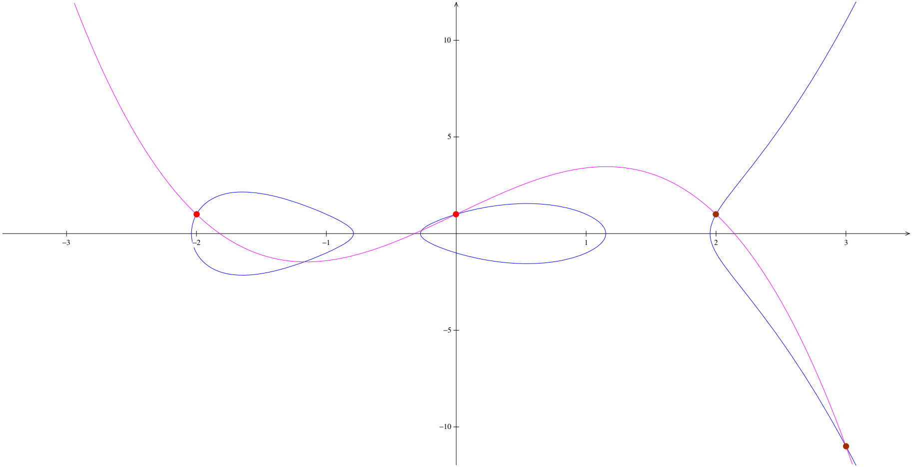


$-(\bullet + \bullet) = \bullet + \bullet$



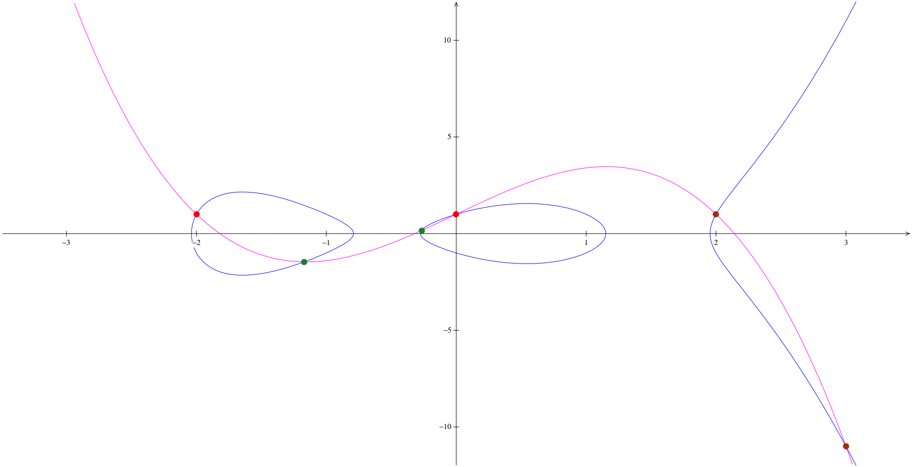
10
5
−5
−10
−3
−2
−1
1
2
3

(● + ●) + (● + ●) = ?

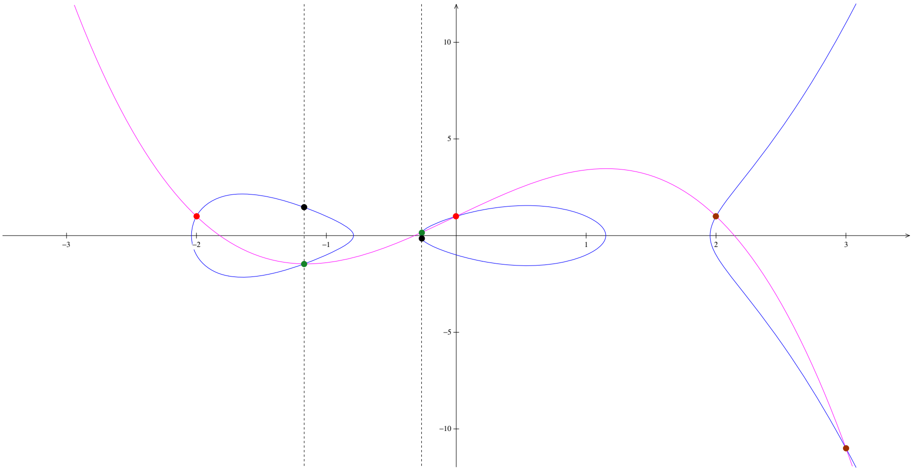


$$(\bullet + \bullet) + (\bullet + \bullet) = \,?$$

Addition in Genus 2, Ramified Models



(● + ●) + (● + ●) + (● + ●) = 0



10
5
−5
−10
−3
−2
−1
1
2
3

(● + ●) + (● + ●) = ● + ●

Addition Procedure

To add two divisors $D = P_1 + P_2$ and $E = Q_1 + Q_2$:

- The four points corresponding to the places P_1, P_2, Q_1, Q_2 lie on a unique cubic $y = v(x)$.
- This cubic intersects C in two more points corresponding to two places $-R_1$ and $-R_2$:
  - The x-coordinates of these points can be obtained by finding the remaining two roots of the sextic $v(x)^2 + h(x)v(x) - f(x)$.
  - The y-coordinates of these points can be obtained by substituting the x-coordinates into $y = v(x)$.
- $[P_1 + P_2 - 2P_\infty] + [Q_1 + Q_2 - 2P_\infty] + [-R_1 - R_2 - 2P_\infty] = [0]$.
- So $[P_1 + P_2 - 2P_\infty] + [Q_1 + Q_2 - 2P_\infty] = [R_1 + R_2 - 2P_\infty]$.

Addition Example

Consider $C : y^2 = f(x)$ with $f(x) = x^5 - 5x^3 + 4x + 1$ over $\mathbb{Q}$.

To add $[P_{(-2,1)} + P_{(0,1)} - 2P_\infty]$ and $[P_{(2,1)} + P_{(3,-11)} - 2P_\infty]$:

- The unique cubic through $(-2, 1)$, $(0, 1)$, $(2, 1)$ and $(3, -11)$ is $y = v(x)$ with $v(x) = -(4/5)x^3 + (16/5)x + 1$.
- The equation $v(x)^2 = f(x)$ becomes
$$(x - (-2))(x - 0)(x - 2)(x - 3)(16x^2 + 23x + 5) = 0 \ .$$
- The roots of $16x^2 + 23x + 5$ are $\dfrac{-23 \pm \sqrt{209}}{32}$.
- The corresponding y-coordinates are $\dfrac{-1333 \pm 115\sqrt{209}}{2048}$.
- $[P_{(-2,1)} + P_{(0,1)} - 2P_\infty] + [P_{(2,1)} + P_{(3,-11)} - 2P_\infty]$
$= [P_{(x_+,y_+)} + P_{(x_-,y_-)} - 2P_\infty]$ where
$$(x_\pm, y_\pm) = \left(\frac{-23 \pm \sqrt{209}}{32}, \frac{1333 \mp 115\sqrt{209}}{2048} \right)$$

Mumford Representation

Note that our final divisor D consisted of points with *irrational* coordinates (though with lots of symmetries), whereas all our polynomials had *rational* coefficients.

Avoid points altogether and work only with polynomials over K:

The **Mumford representation** of a divisor $D = P_{(x_1,y_1)} + P_{(x_2,y_2)}$ on a genus 2 ramified curve is the pair of polynomials $(u(x), v(x))$ where

- $u(x) = (x - x_1)(x - x_2)$.
- $y = v(x)$ is the line through (x_1, y_1) and (x_2, y_2) (the tangent line to C at (x_1, y_1) if $(x_1, y_1) = (x_2, y_2)$).

Write $D = [u, v]$.

Remark: $u(x), v(x)$ have coefficients in K.

Divisor Addition Via Mumford Reps

UNIVERSITY OF CALGARY

To add two disjoint divisors $D_1 = [u_1, v_1]$ and $D_2 = [u_2, v_2]$ on a genus 2 ramified curve

$$C : y^2 + hy = f$$

1. Collect the four x-coordinates of the points in D_1 and D_2:

$$u = u_1 u_2 \ .$$

2. Find the cubic $y = v(x)$ determined by the points in D_1 and D_2:

$$v \equiv \begin{cases} v_1 & \pmod{u_1} \ , \\ v_2 & \pmod{u_2} \ . \end{cases}$$

3. Find the remaining two roots of $v^2 - hv - f$:

$$u \leftarrow (f - vh - v^2)/u \ .$$

4. Replace the intersection divisor of v and C by its opposite:

$$v \leftarrow (-v - h) \pmod{u} \ .$$

5. Output $D_1 + D_2 = [u, v]$.

Mumford Arithmetic — Example

Consider again $C : y^2 = f(x)$ with $f(x) = x^5 - 5x^3 + 4x + 1$ over $\mathbb{Q}$.

Compute $D_1 + D_2$ with $D_1 = P_{(-2,1)} + P_{(0,1)}$ and $D_2 = P_{(2,1)} + P_{(3,-11)}$:

Mumford representation of D_1: $u_1(x) = x^2 + 2x, \qquad v_1(x) = 1.$

Mumford representation of D_2: $u_2(x) = x^2 - 5x + 6,\ v_2(x) = -12x + 25.$

$$u(x) = u_1(x)u_2(x) = x^4 - 3x^3 - 4x^2 + 12x \ ;$$

$$v(x) = -(4/5)x^3 + (16/5)x + 1 \ ;$$

$$u(x) \leftarrow (f(x) - v(x)^2)/u(x) = 16x^2 + 23x + 5 \ ;$$

$$v(x) \leftarrow -v(x) \pmod{u(x)} = (16x - 23)/320 \ ;$$

Mumford rep of $D_1 + D_2 = P_{\left(\frac{-23+\sqrt{209}}{32}, \frac{1333-115\sqrt{209}}{2048}\right)} + P_{\left(\frac{-23-\sqrt{209}}{32}, \frac{1333+115\sqrt{209}}{2048}\right)}$:

$$u(x) = 16x^2 + 23x + 5, \quad v(x) = (16x - 23)/320.$$

Generalization to ramified models of arbitrary genus g:

- Reduced divisors correspond to multisets of up to g points.
- Mumford representations $[u, v]$ uniquely determine a reduced divisor and satisfy
$$\deg(v) < \deg(u) \leq g \ .$$
- Identity and Inverses as before.
- Addition Motto: "Any three divisors on C lying on a function of degree $\leq 2g - 1$ sum to zero."

Addition on Genus g Ramified Models

Let $D_1 = P_1 + \cdots + P_r$ and $D_2 = Q_1 + \cdots + Q_s$ $(r, s \leq g)$ be disjoint.

To add $[D_1 - rP_\infty]$ and $[D_2 - sP_\infty]$:

1. Put $D = P_1 + \cdots + P_r + Q_1 + \cdots + Q_s$ // $(\deg(D) = r + s \leq 2g)$.
2. Repeat until $\deg(D) \leq g$ (up to $\lceil g/2 \rceil$ times):
   1. Compute the unique function $y = v(x)$ with $\deg(v) = \deg(D) - 1$ through the points in $\mathrm{supp}(D)$.
   2. The equation $v^2 + hv - f = 0$ has $2\deg(D) - 2$ roots.*
      $\deg(D)$ of these are the x-coordinates of the points in $\mathrm{supp}(D)$.
      Denote the remaining roots by $x_1, \ldots, x_{\deg(D)-2}$.
   3. Substitute the x_i into $y = v(x)$, i.e. compute $y_i = v(x_i)$ and put $-R_i = P_{(x_i, y_i)}$, for $1 \leq i \leq \deg(D) - 2$.
   4. Put $D = R_1 + R_2 + \cdots + R_{|D|-2}$.
3. Output $[D - \deg(D)P_\infty]$.

*If $\deg(D) = g + 1$ in the last iteration, then the equation has $2g + 1$ roots. In this case, $\deg(D)$ decreases by 1 only, from $g + 1$ to g.

Suppose $\mathrm{supp}(D)$ contains r places $P_i = P_{(x_i,y_i)}$ where where each point (x_i, y_i) occurs m_i times.

Mumford representation: $D = [u, v]$ where

$$u(x) = \prod_{i=1}^{r}(x - x_i)^{m_i}.$$

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{x=x_i} = 0 \qquad (0 \leq j \leq m_i - 1).$$

Note: $\deg(v) < \deg(u) \leq g$.

Example: if $D = P_{(x_0,y_0)}$ (a prime divisor), then $u(x) = x - x_0$, $v(x) = y_0$.

Addition Via Mumford Representations

UNIVERSITY OF CALGARY

Let $D_1 = [u_1, v_1]$, $D_2 = [u_2, v_2]$ be disjoint divisors.

To compute the reduced divisor $D = [u, v]$ in the class $[D_1 + D_2]$:

1. Collect the x-coordinates of the points in D_1 and D_2:
$$u = u_1 u_2 \ .$$
2. Find the function v determined by the points in D_1 and D_2:
$$v \equiv \begin{cases} v_1 \pmod{u_1} \ , \\ v_2 \pmod{u_2} \ . \end{cases}$$
3. while $\deg(u) > g$ do
    1. Find the remaining roots of $v^2 - hv - f$:
    $$u \leftarrow (f - vh - v^2)/u \ .$$
    2. Replace the intersection divisor of v and C by its opposite:
    $$v \leftarrow (-v - h) \pmod{u} \ .$$
4. Output $D = [u, v]$.

Final Remarks

Adding non-disjoint divisors via their Mumford representation is slightly more complicated, but can also be done with a simple polynomial arithmetic and two gcd calculations.

Note that this includes the case of doubling a divisor.

Arithmetic on split models is very similar to that for ramified models, except that one needs to keep track of the extra parameter n

However, unless K is small, we know that $n = -\lceil g/2 \rceil$ almost certainly, so there is no need.

References

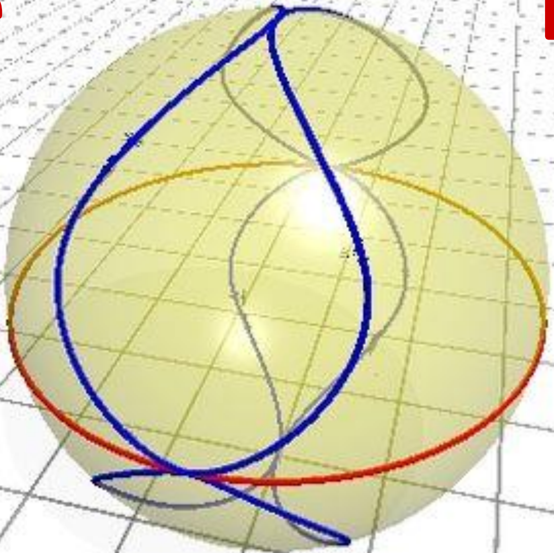
For divisor class arithmetic on ramified models:

- Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato, *An elementary introduction to hyperelliptic curves*, CORR 96-19, University of Waterloo 1996; Also appeared as an appendix in: Neal Koblitz, *Algebraic Aspects of Cryptography*, Algorithms and Computation in Mathematics, vol. 3. Springer, Berlin, 1998.

For divisor class arithmetic on split models:

- Steven D. Galbraith, Michael Harrison and David J. Mireles Morales, Efficient hyperelliptic arithmetic using balanced representation for divisors. In *Algorithmic Number Theory*, Lecture Notes in Computer Science, vol. 5011, Springer, Berlin, 2008, 342–356.

The End



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

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