Definitions and Theorems from Elliptic Curves

Isaac Martin

Last compiled February 22, 2022

Contents

1 Fermat's Method of Infinite Descent

Definition 1.1 (Rational Triangle)**.** Let a, b, c be the side lengths of a right triangle Δ.

1. Δ is *rational* if $a, b, c \in \mathbb{Q}$.
2. Δ is *primitive* if $a, b, c \in \mathbb{Z}$ and are pairwise coprime.

Lemma 1.2 (Lemma 1.1)**.** Every primitive triangle has side lengths of the form $u^2 + v^2$, $2uv$, and $u^2 - v^2$ for some integers $u > v > 0$.

Definition 1.3. $D \in \mathbb{Q}_{>0}$ is a *congruent number* if there exists a rational triangle Δ with $\text{area}(\Delta) = 0$.

N.B. it suffices to to consider D a positive integer which is squarefree, e.g. $D = 5, 6$ are congruent.

Lemma 1.4 (Lemma 1.2)**.** $D \in \mathbb{Q}_{>0}$ is congruent if and only if $Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}$ with $y \neq 0$.

Theorem 1.5. *There is no solution to*

$$w^2 = uv(u+v)(u-v)$$

for $u, v, w \in \mathbb{Z}$ and $w \neq 0$.

Lemma 1.6. Let $u, v \in K[t]$ be coprime polynomials. If $\alpha u + \beta v$ is a square for four distinct choices of $(\alpha : \beta) \in \mathbb{P}^1_K$ then $u, v \in K$.

Corollary 1.7 (1.6 in Lecture)**.** Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.

Proof. Without loss of generality may assume $K = \overline{K}$. By a change of coordinates we may assume $E: y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in K \setminus \{0, 1\}$ Suppose $(x, y) \in E(K(t))$. Write $x = \frac{u}{v}$ for coprime polynomials $u, v \in K[t]$. Then

$$w^2 = uv(u-v)(u-\lambda v)$$

for some $w \in K[t]$. Because $K[t]$ is a UFD, we get that $u, v, u - v$, and $u - \lambda v$ are all squares in $K[t]$ and then Lemma $\square$

2 Remarks on Algebraic Curves

An algebraic curve is a projective variety of dimension 1. All affine curves are algebraic curves, simply take the equation cutting the variety out, homogenize it with a variable Z, and you've got a projective curve. The subset of the curve on which $Z = 1$ recovers the original affine curve.

Throughout these notes, K is a field, $\overline{K}$ is a fixed algebraic closure of K, and $G_{\overline{K}/K}$ is the Galois group $\text{Gal}(\overline{K}/K)$.

2.1 Preliminaries

When we say *curve* in these notes, we always mean a projective variety of dimension one, and almost always we deal with curves that are smooth.

Proposition 2.1. Let C be a curve and $P \in C$ be a smooth point. Then $\mathcal{O}_{C,P} = \overline{K}[C]_P$ is a DVR.

Definition 2.2. Let C be a curve and $P \in C$ be a smooth point. Then the *normalized valuation on* $\overline{K}[C]_P$ is given by

$$\begin{aligned} \mathrm{ord}_P : \overline{K}[C]_P &\longrightarrow \{0,1,2,3,...\} \cup \{\infty\}, \\ \mathrm{ord}_P(f) &= \sup\{d \in \mathbb{Z} \mid f \in \mathfrak{m}_P^d\}. \end{aligned}$$

Here, $\mathfrak{m}_P$ is the unique maximal ideal of $\overline{K}[C]_P$. We extend this function to $\overline{K}(C) \to \mathbb{Z} \cup \{\infty\}$ by declaring $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$.

An alternative definition, or at least a slightly more explicit version of the same definition, involves fixing a uniformizer π_P of $\overline{K}[C]_P$ (note that the any element $f \in K[C]_P$ for which $\mathrm{ord}_P(f) = 1$ is a valid uniformizer) and declaring $\mathrm{ord}_P(f) = d$ where d is the unique integer such that $f = u \cdot \pi^d$ for some unit $u \in \overline{K}[C]_P^\times$. This is necessarily a nonnegative integer when $f \in K[C]_P$.

There are two things to note about this definition. First, though $\overline{K}(C) = \mathrm{Frac}(\overline{K}[C]_P) = \mathrm{Frac}(\overline{K}[C])$ regardless of which $P \in C$ we choose, ord_P does depend on the choice of P, quite clearly. Second, when we extend ord_P to $K(C)$, it is not necessary to additionally add the point $-\infty$ to the codomain. The only point in $K[C]_P$ which evaluates to ∞ under ord_P is 0, which has no inverse in $K(C)$.

Definition 2.3. Let C be a curve and P a smooth point. The *order of f at P* is $\mathrm{ord}_P(f)$.

- If $\mathrm{ord}_P(f) > 0$ then f has a *zero* at P.
- If $\mathrm{ord}_P(f) < 0$ then f has a *pole* at P.
- If $\mathrm{ord}(f) \geq 0$ then f is *regular* at P or alternatively is *defined* at P. We can evaluate $f(P)$ in this case.
- If $\mathrm{ord}_P(f) < 0$, i.e. if f has a pole at P, then we write $f(P) = \infty$.

All of this should be reminiscent of complex analysis, and indeed, all this is identical to that terminology in the case that $K = \mathbb{C}$.

Proposition 2.4. Let C be a smooth curve and $f \in \overline{K}(C)$ with $f \neq 0$. Then there are only finitely many points $P \in C$ at which f has a zero or pole. Furthermore, f has no poles if and only if $f \in \overline{K}$.

Example 2.5. Let C/K be a smooth curve and let $f \in K(C)$ be a function. Then f defines a rational map, which we also denote by f, given by

$$f : C \longrightarrow \mathbb{P}^1, \qquad P \mapsto [f(P), 1].$$

This map is actually a morphism (i.e. is a rational map which is regular at every point in the domain). It is given by

$$f(P) = \begin{cases} [f(P),1] & \text{if } f \text{ is regular at } P \\ [1,0] & \text{if } f \text{ has a pole at } P \end{cases}.$$

Conversely, if we have some rational map $\phi : C \to \mathbb{P}^1$ defined $\phi = [f,g]$ with $f,g \in K(C)$, then either $g = 0$ in which case $\phi = [1,0]$ and ϕ is constant, or ϕ is the map corresponding to the function $f/g \in K(C)$. Writing it this way also means we can cancel out places where f and g are simultaneously zero. Denoting the case where g is identically zero by $\phi = \infty$ (motivated by the idea that $1/0 = \infty$) we have a one-to-one correspondence

$$K(C) \cup \{\infty\} \leftrightarrow \{\text{maps } C \longrightarrow \mathbb{P}^1 \text{ defined over } K\}.$$

We often identify these sets in practice.

The author of these notes is stupid and incessantly ignorant about matters regarding Galois, so we say a few things more about the Galois action. The Galois group $G_{\overline{K}/K}$ acts on $\mathbb{A}^n_{\overline{K}}$ by

$$P^\sigma = (x_1^\sigma, ..., x_n^\sigma),$$

meaning that $\mathbb{A}^n_K$ can be characterized by

$$\mathbb{A}^n_K = \mathbb{A}^n(K) = \{P \in \mathbb{A}^n_{\overline{K}} \mid P^\sigma = P \text{ for all } \sigma \in G_{\overline{K}/K}\}.$$

When we write $\mathbb{A}^n$ without specifying the base field, it is implied that we mean $\mathbb{A}^n_{\overline{K}}$. Similarly, when we write $\mathbb{P}^n$ we mean $\left(\mathbb{A}^{n+1}_{\overline{K}} \setminus \{0\}\right)/\overline{K}^*$, and we define the *set of K-rational points in* $\mathbb{P}^n$ to be

$$\mathbb{P}^n(K) = \{[x_0, ..., x_n] \in \mathbb{P}^n \mid x_i \in K \text{ for all } 0 \le i \le n\}. \tag{1}$$

Definition 2.6. Let $P = [x_0, ..., x_n] \in \mathbb{P}^n(\overline{K})$. The **minimal field of definition for** P is the field

$$K(P) = K(x_0/x_i, ..., x_n/x_i)$$

where x_i is (one of) the nonzero coordinate(s) of P. Note that different valid choices of x_i yield isomorphic fields when we adjoin elements.

The Galois group acts on $\mathbb{P}^n$ in the way one would hope. Given $\sigma \in G_{\overline{K}/K}$,

$$[x_0, ..., x_n]^\sigma = [x_0^\sigma, ..., x_n^\sigma].$$

This action is well defined since

$$[\lambda x_0, ..., \lambda x_n]^\sigma = \lambda^\sigma [x_0^\sigma, ..., x_n^\sigma] = [x_0, ..., x_n]^\sigma.$$

We have a notion of the rationalization of a curve and a rational curve.

Definition 2.7. A plane curve $\{f(x,y) = 0 \mid (x,y) \in K = \overline{K}\} \subseteq \mathbb{A}^2$ (with f irreducible over $\overline{K}$) is said to be **rational** if it has a rational parameterization, i.e. $\exists \phi, \psi \in K(t)$ such that

(i) $\mathbb{A}^1 \to \mathbb{A}^2$ defined $t \mapsto (\phi(t), \psi(t))$ is an injection on $\mathbb{A}^1 \setminus \{\text{finite set}\}$

(ii) $f(\phi(t), \psi(t)) = 0$

2.2 Divisors

The only codimension subschemes of a curve are the points on the curve. This makes the divisor class group of an algebraic curve C particularly nice. We go through the construction here and note that we care divisors in this context because they give us a much more algebraic way to study the group law on an elliptic curve. We'll see that an elliptic curve is actually isomorphic to a subgroup of its Picard group.

Definition 2.8. The **divisor group** of a curve C is the free abelian group generated by the points of C. More explicitly, a divisor $D \in \mathrm{Div}(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

where only finitely many of the n_P are nonzero. The **degree** of a divisor is defined by

$$\deg(D) = \sum_{P \in C} n_P.$$

The **divisors of degree 0** form a subgroup of $\mathrm{Div}(C)$ which we denote by $\mathrm{Div}^0(C)$.

The Galois action on divisors is exactly what you'd expect: given $\sigma \in G_{\overline{K}/K}$ we define

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma).$$

We say that D is *defined over* K if $D^\sigma = D$ for each $\sigma \in G_{\overline{K}/K}$. This does *not* mean that D is defined over K if and only if $P \in K$ for each $n_P \neq 0$ is the formal sum defining D, instead, the Galois action could simply permute the nonzero P's in some way.

We, of course, have a notion of principal divisors on a curve C. If C is a smooth curve and $f \in \overline{K}(C)$, then we define

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)P$$

to be the divisor associated to f. Note that this is indeed a divisor since $\mathrm{ord}_P(f) \neq 0$ for only finitely many $P \in C$. If $\sigma \in G_{\overline{K}/K}$ then

$$\mathrm{div}(f^\sigma) = (\mathrm{div}(f))^\sigma,$$

noting that the Galois action on elements of $\overline{K}(C)$ is simply the action of $G_{\overline{K}/K}$ on the coefficients. The map $\mathrm{ord}_P : \overline{K}(C) \to \mathbb{Z} \cup \{\infty\}$ is a valuation, so the map

$$\mathrm{div} : \overline{K}(C) \longrightarrow \mathrm{Div}(C)$$

is a map homomorphism of Abelian groups. It is analogous to the map that sends elements of a number field to the fractional ideal they define. We can now define the Picard group, which is what we're really after.

Definition 2.9. A divisor $D \in \mathrm{Div}(C)$ is said to be *principal* if there is some $f \in \overline{K}(C)$ such that $D = \mathrm{div}(f)$. We say that two divisors D_1 and D_2 are *linearly equivalent* if $D_1 - D_2$ is principal, and we write $D_1 \sim D_2$ in this case because linear equivalence is an equivalence relation. The *divisor class group* or the *Picard group* of C is denoted $\mathrm{Pic}(C)$ and is defined $\mathrm{Pic}(C) = \mathrm{Div} / \sim$. We let $\mathrm{Pic}_K(C)$ denote the subgroup of $\mathrm{Pic}(C)$ fixed by the action of $G_{\overline{K}/K}$, and we note that $\mathrm{Pic}_K(C)$ is not, in general, isomorphic to a quotient of $\mathrm{Div}_K(C)$.

There are some scenarios when $\mathrm{Pic}_K(C)$ can be realized as a quotient of $\mathrm{Div}_K(C)$:

Example 2.10. Let C/K be a curve. Then

$$1 \longrightarrow K^\times \longrightarrow K(C)^\times \longrightarrow \mathrm{Div}_K^0(C) \longrightarrow \mathrm{Pic}_K^0(C)$$

is an exact sequence, where the maps are given by the trivial map, inclusion, $\mathrm{div}(-)$, and projection going from left to right. In the case that C is genus one and $C(K) \neq \emptyset$ (*cough* an elliptic curve *cough*) then

$$1 \longrightarrow K^\times \longrightarrow K(C)^\times \longrightarrow \mathrm{Div}_K^0(C) \longrightarrow \mathrm{Pic}_K^0(C) \longrightarrow 0$$

is exact, i.e. $\mathrm{Div}_K^0(C) \longrightarrow \mathrm{Pic}_K^0(C)$ is surjective.

We haven't actually defined $\mathrm{Div}_K^0(C)$ or $\mathrm{Pic}_K^0(C)$ yet, so we do that now. First a proposition, then the definition.

Proposition 2.11. Let C be a smooth curve and let $f \in \overline{K}(C)^\times$.

(a) $\mathrm{div}(f) = 0$ if and only if $f \in \overline{K}^\times$.

(b) $\deg(\mathrm{div}(f)) = 0$.

Proof.

(a) If $\mathrm{div}(f) = 0$ then f has no poles by definition, and hence the associated map $f : C \longrightarrow \mathbb{P}^1$ given in example (2.5) is not surjective (it misses the point $[1,0]$). Silverman Theorem (II.2.3) tells us that a morphism $\phi : C_1 \longrightarrow C_2$ of curves is either constant or surjective, hence f is constant. The reverse implication is clear.

(b) Proof for this not included, see Silverman Proposition (II.3.1 b).

□

Definition 2.12. The principal divisors form a subgroup of $\mathrm{Div}^0(C)$ by Proposition (2.11 b). We define the *degree 0 part of the divisor class group of C* to be the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors. We denote this group by $\mathrm{Pic}^0(C)$. Similarly, we write $\mathrm{Pic}_K^0(C)$ for the subgroup of $\mathrm{Pic}^0(C)$ which is fixed by $G_{\overline{K}/K}$.

This discussion can be summed up by saying that the following sequence is exact:

$$1 \longrightarrow \overline{K}^\times \xrightarrow{\text{inclusion}} \overline{K}(C)^\times \xrightarrow{\text{div}} \mathrm{Div}^0(C) \xrightarrow{projection} \mathrm{Pic}^0(C) \longrightarrow 0.$$

The divisor group has a partial ordering which is useful. We say that a divisor $D = n_1P_1 + ...n_\ell P_\ell$ if $n_i \geq 0$ for each $1 \leq i \leq \ell$, and we say that D is *effective*. We say that D is *anti-effective* if $-D$ is effective.

2.3 Differentials

Differentials are useful because they perform the linearization that we have learned to appreciate from Calculus and because they provide a useful condition for the separability of a map of curves. Recall that a map of curves $\phi : C_1 \longrightarrow C_2$ is said to be separable if the induced field extension $\phi^* : K(C_2) \longrightarrow K(C_1)$ is separable.

Definition 2.13. Let C be a curve. The *space of (meromorphic) differential forms* on C, denoted by Ω_C, is the $\overline{K}$-vector space generated by symbols of the form dx for $x \in \overline{K}(C)$, subject to the usual relations:

(i) $d(x+y) = dx + dy$ for all $x, y \in \overline{K}(C)$.

(ii) $d(xy) = x\,dy + y\,dx$ for all $x, y \in \overline{K}(C)$.

(iii) $da = 0$ for all $a \in \overline{K}$.

A map of curves induces a map on function fields which in turn induces a map on differential forms.

Remark 2.14. Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. The associated map on function fields $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ induces a map on differentials:

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}, \qquad \phi^*\left(\sum f_i\, dx_i\right) = \sum (\phi^* f_i) d(\phi^* x_i).$$

Here are some nice facts about Ω_C.

Proposition 2.15. Let C be a curve.

(a) Ω_C is a one-dimensional $\overline{K}(C)$-vector space.

(b) An element $x \in \overline{K}(C)$ is a $\overline{K}(C)$-basis for Ω_C if and only if $\overline{K}(C)/\overline{K}(x)$ is a finite separable extension.

(c) A nonconstant map of curves $\phi : C_1 \to C_2$ is separable if and only if the induced map $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is injective, or equivalently, nonzero.

Note that one implication of (a) in the above proposition is that $\overline{K}(C) \cong \Omega_C$ as $\overline{K}(C)$-vector spaces. There is, in fact, a useful way to identify these spaces and thus to think of differential forms as functions on C:

Proposition 2.16 (Silverman Proposition II.4.3)**.** Let C be a curve, let $P \in C$, and let $t \in \overline{K}(C)$ be a uniformizer at P.

(a) For every $\omega \in \Omega_C$ there exists a unique function $g \in \overline{K}(C)$, depending on ω and t, satisfying

$$\omega = g\,dt.$$

we then denote g by ω/dt.

(b) Let $f \in \overline{K}(C)$ be regular at P. Then df/dt is also regular at P.

(c) Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity

$$\mathrm{ord}_P(\omega/dt)$$

depends only on ω and P; it is independent of the choice of uniformizer t. We call this value the **order** of *omega* at P and denote it by $\mathrm{ord}_P(\omega)$.

(d) Let $x, f \in \overline{K}(C)$ with $x(P) = 0$, and let $p = \mathrm{char}(K)$. Then

$$\begin{aligned} &\mathrm{ord}_P(f\,dx) = \mathrm{ord}_P(f) + \mathrm{ord}_P(x) - 1 && \text{if } p = 0 \text{ or } p \not\mid \mathrm{ord}_P(x) \\ &\mathrm{ord}_P(f\,dx) \geq \mathrm{ord}_P(f) + \mathrm{ord}_P(x), && \text{if } p > 0 \text{ and } p \mid \mathrm{ord}_P(x) \end{aligned}$$

(e) Let $\omega \in \Omega_C$ with $\omega \neq 0$. Then

$$\mathrm{ord}_P(\omega) = 0 \qquad \text{for all but finitely many } P \in C.$$

We don't include the proof of this theorem here. We do comment, however, that if $t \in \overline{K}(C)$ is a uniformizer of $\overline{K}[C]_P$ then dt ought to be a basis for Ω_C as a $\overline{K}(C)$-vector space. This follows from Proposition (2.15 (b)), I think. We additionally wish to point out that (d) in Proposition (2.16) resembles the idea that taking derivatives ought to cut down the order of vanishing of a meromorphic function at a point P by 1, at least in characteristic 0.

Since Ω_C can be identified with $\overline{K}(C)$, it makes sense that we can associate divisors to differential forms.

Definition 2.17. Let $\omega \in \Omega_C$. The *divisor associated to* ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C).$$

The differential ω is said to be *regular* or *holomorphic* if

$$\mathrm{ord}_P(\omega) \geq 0 \qquad \text{for all } P \in C$$

and nonvanishing if

$$\mathrm{ord}_P(\omega) \leq 0 \qquad \text{for all } P \in C.$$

If $\omega, \omega' \in \Omega_C$ are nonzero differentials, then Proposition (2.16 (a)) implies that there is some function $f \in \overline{K}(C)^\times$ such that $\omega = f\omega'$. Thus

$$\mathrm{div}(\omega) = \mathrm{div}(f) + \mathrm{div}(\omega'),$$

so this definition makes sense. It also means that all differentials are linearly equivalent.

Definition 2.18. The *canonical divisor class on C* is the image in $\mathrm{Pic}(C)$ of $\mathrm{div}(\omega)$ for any nonzero differential $\omega \in \Omega_C$. Any divisor in this divisor class is called a canonical divisor, and this divisor class includes $\mathrm{div}(\omega)$ for every $\omega \in \Omega_C$ by the above discussion.

We now introduce this thing.

Definition 2.19 (Riemann-Roch Space)**.** Let C be a smooth projective curve. The Riemann-Roch space of a $D \in \mathrm{Div}(C)$ is

$$\mathcal{L}(D) = \left\{ f \in K(C)^* \;\middle|\; \mathrm{div}(f) + D \geq 0 \right\} \cup \{0\}$$

i.e. the set of rational functions on C with "poles no worse than specified by D." The set $\mathcal{L}(D)$ is a finite dimensional $\overline{K}$-vector space and we denote its dimension by

$$\ell(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

It is called the Reimann-Roch space, in part, because of its connection with the Riemann-Roch theorem.

2.4 Review of Morphisms

This section summarizes basic facts about maps of curves and the maps they induce on function fields, divisor groups, and differentials.

2.4.1 Morphisms of Varieties

Let V_1 and V_2 be projective varieties and let $\phi : V_1 \to V_2$ be a function.

- ϕ is a *rational map of varieties* if $\phi = [f_0, ..., f_n]$ where $f_0, ..., f_n \in \overline{K}(V_1)$ have the property that for every point $P \in V_1$ at which all the f_i are defined, $\phi(P) = [f_0(P), ..., f_n(P)]$.
- If ϕ is a rational map of varieties as above and if additionally there is some $\lambda \in \overline{K}^\times$ such that $\lambda f_0, ..., \lambda f_n \in K(V_1)$, then ϕ is said to be *defined over K*. Note that $[f_0, ..., f_n]$ and $[\lambda f_0, ..., \lambda f_n]$ give the same map on points, so this condition really means that ϕ is defined over K if the functions $f_0, ..., f_n$ can be taken to be in $K(V_1)$. It's true that ϕ is defined over K if and only if $\phi = \phi^\sigma$ for all $\sigma \in G_{\overline{K}/K}$.
- If V_1 and V_2 are defined over K then $G_{\overline{K}/K}$ acts on ϕ by

$$\phi^\sigma(P) = [f_0^\sigma(P), ..., f_n^\sigma(P)].$$

- ϕ is *regular at a point* $P \in V_1$, if for each $P \in V_1$ there is a function $g \in \overline{K}(V_1)$ such that $g \circ f_i$ is regular at P (i.e. $g \circ f_i \in \overline{K}[V_1]_P$ i.e. $g \circ f_i$ is defined at P) for each $0 \leq i \leq n$ and there is at least one such i where $(g \circ f_i)(P) \neq 0$. It is *regular* if it is regular at every point $P \in V_1$. We say that ϕ is a morphism of varieties if it is regular.
- With P and g as above, we have

$$\phi(P) = [gf_0(P), ..., gf_n(P)].$$

  Note that it may be necessary to vary g as we vary g; this presentation of ϕ is local.
- We say that ϕ is an isomorphism if there is a morphism $\psi : V_2 \to V_1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps on V_2 and V_1 respectively.

See page 11 of Silverman for a more detailed discussion of morphisms of algebraic variates and for methods by which we gain useful additional properties in the case that C_1 and C_2 are projective varieties, which they are when C_1 and C_2 are curves.

2.4.2 Morphisms of curves

Let $\phi : C_1 \to C_2$ be a map of curves. This is simply a morphism of varieties, both of which happen to be curves.

- Assume for a moment that $C_2 \subseteq \mathbb{P}^n$ is only a variety and not necessarily a curve. Then if ϕ is a rational map and $P \in C_1$ is a smooth point, then ϕ is regular at P. In particular, if C_1 is smooth and ϕ is rational then ϕ is regular. [Silverman Proposition II.2.1]
- The morphism ϕ is either surjective or constant. [Silverman Theorem II.2.3]

2.4.3 Induced map on function fields

Let C_1/K and C_2/K be curves and let $\phi : C_1 \to C_2$ be a rational non-constant map defined over K.

- Composition with ϕ induces an injection of function fields which fixes K:

$$\phi^* : K(C_2) \longrightarrow K(C_1), \qquad \phi^*(f) = f \circ \phi.$$

- If ϕ is defined over K then $K(C_1)$ is a finite extension of $\phi^*(K(C_2))$, which is isomorphic to $K(C_1)$ remember.

- If $\iota : K(C_2) \to K(C_1)$ is an injection of function fields fixing K, then there is a unique nonconstant map $\phi : C_1 \to C_2$ defined over K such that $\phi^* = \iota$.

- If $L \subseteq K(C_1)$ is a subfield of finite index which contains K, then there is a smooth curve C'/K, unique up to K-isomorphism, and a nonconstant map $\phi : C_1 \to C'$ defined over K such that $\phi^*(K(C')) = L$.

- Let ϕ be a map of curves defined over K. If ϕ is constant then we set the degree of ϕ to be 0; otherwise, we define

$$\deg \phi = [K(C_1) \ : \ \phi^* K(C_2)].$$

  we say that ϕ is *separable*, *inseparable,* or *purely inseparable* if the field extension $K(C_1)/\phi^*K(C_2)$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $\deg_s \phi$ and $\deg_i \phi$ respectively.

- We use the norm map relative to ϕ^* to define a map ϕ_* in the other direction:

$$\phi_* : K(C_1) \longrightarrow K(C_2), \qquad \phi_* = (\phi^*)^{-1} N_{K(C_1)/\phi^* K(C_2)}.$$

  Recall that for a finite field extension $K \subseteq L$, each element $\alpha \in L$ defines a K-linear map $m_\alpha : L \to L$ given by left multiplication by α. The norm of α, relative to K, is defined to be the determinant of m_α.

- If C_1 and C_2 are smooth and ϕ_1 is degree 1 then ϕ is an isomorphism.

- The map ϕ^* is the map induced on the stalk of the generic point (I think).

2.4.4 Induced map on divisors

Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves.

- Suppose $P \in C_1$, $Q \in C_2$ such that $\phi(P) = Q$, and let $t \in K(C_2)$ be a uniformizer at Q (i.e. a generator for the maximal ideal of $K[C_2]_Q$). We then define $e_\phi(Q) = \mathrm{ord}_P(\phi^* t)$. Note that this is the ramification index of t in $K(C_1)$, considering t to be a prime ideal.

- We have maps

$$\phi^* : \overline{K}(C_2) \longrightarrow \overline{K}(C_1) \qquad \text{and} \qquad \phi_* : \overline{K}(C_1) \longrightarrow \overline{K}(C_2)$$

induced by ϕ. We similarly define maps of divisor groups as follows:

$$\begin{array}{ll} \phi^* : \mathrm{Div}(C_2) \longrightarrow \mathrm{Div}(C_1) & \text{and} \qquad \phi_* : \mathrm{Div}(C_1) \longrightarrow \mathrm{Div}(C_2), \\ (Q) \mapsto \displaystyle\sum_{P \in \phi^{-1}(Q)} e_\phi(P) P & \qquad\qquad\quad (P) \mapsto (\phi P) \end{array}$$

and extend $\mathbb{Z}$-linearly.

2.4.5 Induced map on differential forms

Let $\phi : C_1 \longrightarrow C_2$ be a nonconstant map of curves.

- The associated function field map $\phi^* : \overline{K}(C_2) \longrightarrow \overline{K}(C_1)$ the induces a map on differentials:

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}, \qquad \phi^* \left(\sum f_i \, dx_i \right) = \sum (\phi^* f_i) d(\phi^* x_i).$$

- The map ϕ is separable if and only if the induced map $\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}$ is injective, or equivalently, nonzero.

3 Geometry of Elliptic Curves

3.1 Weierstrass Equations

An elliptic curve is a genus one curve in $\mathbb{P}^2$ with a single specified base point on the line at infinity (remember that the line at infinity in $\mathbb{P}^2$ is the set of points $[X : Y : 0]$). After scaling X and Y appropriately an elliptic curve has an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{2}$$

Here, $O = [0 : 1 : 0]$ is the base point and $a_1, ..., a_6 \in \overline{K}$, and equation (2). We generally write an elliptic curve in non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$:

$$E : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3}$$

and remember that we always have a single extra point at infinity given by $O = [0 : 1 : 0]$. If $a_1, ..., a_6 \in K$ then we say that E is **defined over** K.

We can make some simplifications in the cases that $\mathrm{char}(\overline{K}) \neq 2, 3$. If $\mathrm{char}(\overline{K}) \neq 2$ then we can complete the square:

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

to get an equation

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_4, \qquad b^4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6.$$

The following are useful quantities:

$$
\begin{aligned}
b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24 b_4, \\
c_6 &= -b_2^3 + 36 b_2 b_4 - 216 b_6, \\
\Delta &= -b_2^2 b_8 - 8 b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, && \text{the } \textbf{discriminant} \text{ of } E \\
j &= c_4^3 / \Delta, && \text{the } \textbf{j-invariant} \text{ of } E \\
\omega &= \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y} && \text{the } \textbf{invariant differential}.
\end{aligned}
$$

In the case that $\operatorname{char} \overline{K} \neq 2, 3$ we can make an additional substitution

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

to eliminate the x^2 term and obtain the simpler equation

$$E: \; y^2 = x^3 - 27 c_4 x - 54 c_6$$

for the elliptic curve.

The last three terms in the above table of quantities are of particular interest in classifying elliptic curves up to isomorphism. We also note that the "invariant differential" will turn out to be an invariant differential of the formal group law on an elliptic curve.

3.2 Isogenies

Definition 3.1. Let A be an abelian group. A function $q : A \longrightarrow \mathbb{Z}$ (or sometimes $q : A \longrightarrow \mathbb{R}$) is a *quadratic form* if

(i) For all $n \in \mathbb{Z}$ we have $q(nx) = n^2 q(x)$

(ii) The pairing $\langle x, y \rangle \mapsto q(x+y) - q(x) - q(y)$ is $\mathbb{Z}$-bilinear for any $x, y \in A$.

If we instead take $q : A \longrightarrow \mathbb{R}$, then a quadratic form instead must satisfy

(i) For all $x \in A$, $q(x) = q(-x)$

(ii) The pairing $\langle x, y \rangle \mapsto q(x+y) - q(x) - q(y)$ is $\mathbb{R}$-bilinear for any $x, y \in A$.