Definitions and Theorems from Elliptic Curves

Isaac Martin

Last compiled February 15, 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 □

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

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

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

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 $\operatorname{ord}_P(f) = 1$ is a valid uniformizer) and declaring $\operatorname{ord}_P(f) = d$ 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 $\overline{K}(C) = \operatorname{Frac}(\overline{K}[C]_P) = \operatorname{Frac}(\overline{K}[C])$ 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 $\operatorname{ord}_P(f)$.

- If $\operatorname{ord}_P(f) > 0$ then f has a *zero* at P.
- If $\operatorname{ord}_P(f) < 0$ then f has a *pole* at P.
- If $\operatorname{ord}(f) \geq 0$ then f is *regular* at P or alternatively is *defined* at P. We can evaluate $f(P)$ in this case.
- If $\operatorname{ord}_P(f) < 0$, 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 $f \in \overline{K}$.

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

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

Definition 2.5. 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 2.6. 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.

Definition 2.7. The **divisor class 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.

Definition 2.8 (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 K-vector space of rational functions on C with "poles no worse than specified by D."

Here, the space $K(C)$ is $\mathrm{Frac}\left(K[x_1, \ldots, x_n]/(F)\right)$.

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 $a_1, \ldots, a_6 \in \overline{K}$, 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 $a_1, \ldots, a_6 \in K$ 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 is useful quantities:

$$
\begin{aligned}
b_8 &= a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2, \\
c_4 &= b_2^2-24b_4, \\
c_6 &= -b_2^3+36b_2b_4-216b_6, \\
\Delta &= -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6, && \text{the } \textbf{discriminant} \text{ of } E \\
j &= c_4^3/\Delta, && \text{the } \textbf{j-invariant} \text{ of } E \\
\omega &= \frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y} && \text{the } \textbf{invariant differential}.
\end{aligned}
$$

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

$$E:\ y^2 = x^3-27c_4x-54c_6$$

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.