EXERCISES FOR MATH 8120: A TOPICS COURSE ON "THE ARITHMETIC OF ELLIPTIC CURVES"

TYLER GENAO

Contents

0. Elliptic Curves: A Planar Approach

Exercise 0.1. This exercise determines when certain plane curves are nonsingular. Let F be a field of characteristic zero.

a) Show that for a polynomial $f(x) \in F[x]$ and for an integer $n \in \mathbb{Z}^+$, the curve
$$C_{/F} : y^n = f(x)$$
in $\mathbb{A}^2$ has a singular point if and only if $f(x)$ has a *repeated root* in $\overline{F}$, i.e., there exists $x_0 \in \overline{F}$ with $f(x_0) = 0$ and $f'(x_0) = 0$.

b) Given a curve
$$C : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$
where $\alpha, \beta, \gamma \in \overline{F}$, the *discriminant* of C is
$$\Delta_C := [(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)]^2.$$
Prove that $\Delta_C = 0$ if and only if C is singular.

In particular, when a cubic polynomial $f(x) \in F[x]$ has no repeated roots, the cubic curve defined by $y^2 = f(x)$ is nonsingular, and in fact is an elliptic curve over F.

Exercise 0.2. **Prerequisite: algebraic number theory.**

This exercise extends Exercise 0.1, by giving a formula for the discriminant of the polynomial x^3+Ax+B associated to the cubic curve $y^2 = x^3+Ax+B$. For a reference, see pp. 37-38 [Mil].

Date: Last updated April 14, 2025.

Let F be a field of characteristic zero, and K/F an extension of degree n. Then by the primitive element theorem, we can write $K = F(\alpha)$ for some $\alpha \in \overline{F}$. Let $m_\alpha(x)$ be its minimal polynomial; suppose its roots are $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n$. Then we have a formula for the discriminant of K/F:

$$\begin{aligned}\Delta_{K/F} &= \Delta(\alpha_1, \ldots, \alpha_n) \\ &= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \cdot \mathrm{Nm}_{K/F}(m'_\alpha(\alpha)).\end{aligned}$$

In general, for a polynomial $f \in F[x]$ of degree $n \ge 1$ whose roots in $\overline{F}$ are $\alpha := \alpha_1, \ldots, \alpha_n$, the *discriminant of* f is

$$\Delta(f) := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \cdot \mathrm{Nm}_{K/F}(f'_\alpha(\alpha)).$$

a. Show that for $n \ge 1$, the discriminant of

$$f(x) := x^n + Ax + B \in F[x]$$

is

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}}(n^n B^{n-1} + (-1)^{n-1}(n-1)^{n-1}A^n).$$

b. Use part a. and Exercise 0.1 to show that a cubic curve

$$E_{/F} : y^2 = x^3 + Ax + B \tag{1}$$

has for its associated polynomial $x^3 + Ax + B$ the discriminant

$$\Delta = -(4A^3 + 27B^2).$$

Remark: This discriminant differs from the usual short Weierstrass form discriminant $\Delta_E := -16(4A^3 + 27B^2)$. The factor of 16 in the latter formula is a useful way to emphasize that over a field of characteristic 2, the curve defined by (1) does *not* define an elliptic curve.

Exercise 0.3. **Prerequisite: algebraic geometry.**

One has in the usual definition of an *affine* elliptic curve that it must be *irreducible,* i.e., it cannot be the union of two nontrivial plane curves. However, this is superfluous for *projective nonsingular* curves: show that for a nonsingular projective plane curve $C_{/k}$, one has that C is irreducible over $\overline{k}$. (Compare this to Exercise 1.5.)

Exercise 0.4. Let $E_{/k}$ be an elliptic curve in general Weierstrass form

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

where $a_1, a_2, a_3, a_4, a_6 \in k$. (Note that this includes short Weierstrass form as a special case.)

a. Show that for two points $P_1 := (x_1, y_1), P_2 := (x_2, y_2) \in E(k)$ which are not collinear to $O := [0 : 1 : 0]$, one has the formula

$$P_1 * P_2 = (x_3, y_3) := (m^2 + a_1m - a_2 - x_1 - x_2, mx_3 + b)$$

where $L : y = mx + b$ is the line through P_1 and P_2.

b. Use part a. to further show that

$$P_1 \oplus P_2 = (x_3, -(m + a_1)x_3 - b - a_3).$$

c. In contrast to part a., show that if P_1, P_2 and O are collinear, then

$$P_1 \oplus P_2 = O.$$

d. Prove that for a point $P = (x, y) \in E(k)$, one has

$$-P = (x, -y - a_1x - a_3).$$

Exercise 0.5. This exercise proves some basic results for elliptic curves in short Weierstrass form,

$$E_{/k} : y^2 = x^3 + Ax + B.$$

a) Using Exercise 0.4, show that for two points $P_1 := (x_1, y_1), P_2 := (x_2, y_2) \in E(k)$ which are not collinear to $O := [0 : 1 : 0]$, one has the formula

$$P_1 \oplus P_2 = (m^2 - x_1 - x_2, -m(m^2 - x_1 - x_2) - b)$$

where $L : y = mx + b$ is the line through P_1 and P_2.

b) Argue that if P_1, P_2 and O are collinear, then $P_2 = -P_1$.

c) Show that for any point $P := (a, b) \in E(k)$, one has the additive inverse

$$-P = (a, -b).$$

Exercise 0.6. For the elliptic curve

$$E_{/\mathbb{Q}} : y^2 = x^3 + 17,$$

given points $P_1 := (-2, 3)$, $P_2 := (-1, 4)$ and $P_3 := (2, 5)$ in $E(\mathbb{Q})$, directly use the chord and tangent method to prove the following.

a. $-2P_1 = (8, 23)$.

b. $P_2 \oplus P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right)$ (which is $\approx (-0.889, -4.037)$).

(You are allowed to use the formula for the inverse of a point.)

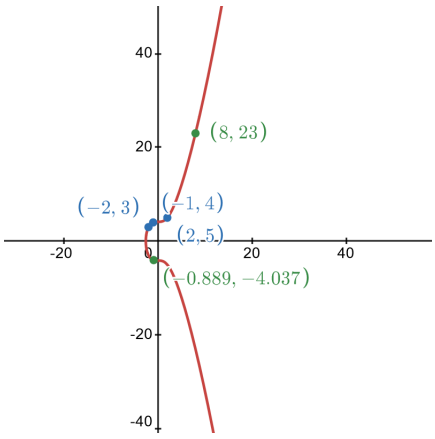

FIGURE 1. The elliptic curve $E : y^2 = x^3 + 17$.

Exercise 0.7. This exercise explores some arithmetic with an elliptic curve not in Weierstrass form.

Consider the cubic curve

$$E_{/\mathbb{Q}} : x^3 + y^3 = 1.$$

a) Write down the projective closure E_H of E. Show that $O := [1 : -1 : 0]$ is the only real point at infinity on E. Also show that E has exactly three points at infinity over $\mathbb{C}$.
b) Show that E_H is nonsingular. Deduce that E_H is a projective elliptic curve.
c) Thus, E is an elliptic curve over $\mathbb{Q}$. Prove that for any point $P = (a, b) \in E(\mathbb{C})$ with $a \neq b$, the inverse of P is

$$-P = (b, a).$$

(You may assume that O is a flex point.)
d) For any point $P = (a, a) \in E(\mathbb{C})$, show that P has order two.
e) (Optional) Explain why E has no positive rational points.

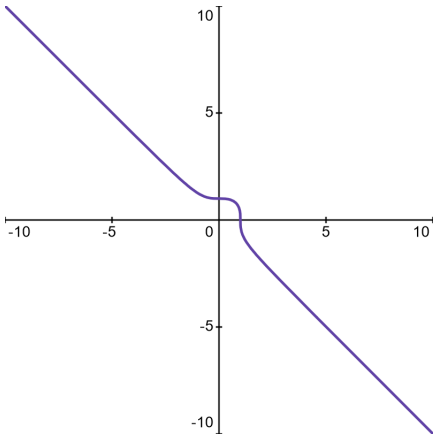

FIGURE 2. The elliptic curve $E : x^3 + y^3 = 1$.

Exercise 0.8. Consider the elliptic curve

$$E : y^2 + y = x^3.$$

a. Using the picture below, guess the real flex points of E.
b. With proof, determine the real flex points of E.

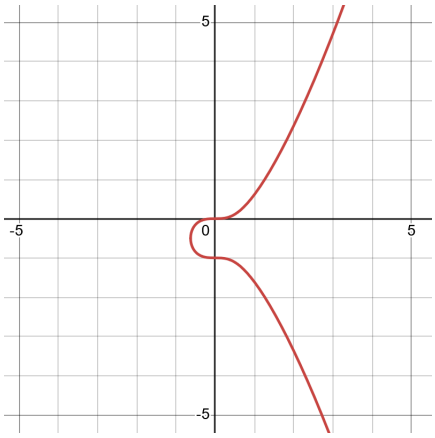

FIGURE 3. The elliptic curve $E : y^2 + y = x^3$.

Exercise 0.9. Let k be a field and $E_{/k}$ an elliptic curve in general Weierstrass form. This exercise will describe the points on E of order 2 and 3, under suitable assumptions.

a. Prove that the points on E of order dividing 2 are precisely the points with vertical tangent lines.
b. Further assume that $\mathrm{char}(k) \neq 2$, and that E is given in short Weierstrass form,

$$E : y^2 = x^3 + Ax + B.$$

Show that the points of order 2 on E have the form $(\alpha, 0)$ where α is a root of $x^3 + Ax + B$.
c. Back to general Weierstrass form: prove that the points on E of order dividing 3 are precisely the flex points of E.

Exercise 0.10.

a. Given a planar elliptic curve $E_{/k}$ and a point $O \in E(k)$ *that is not necessarily flex,* show that the chord and tangent method makes $(E(k), O)$ an abelian group. (You can skip showing associativity.)
b. Consider the elliptic curve $E : y^2 = x^3 - 7x + 10$ from an example in class, pictured below. We showed that for $P_1 := (1, 2)$ and $P_2 := (3, 4)$, one has $P_1 \oplus P_2 = (-3, 2)$ and $2P_1 = (-1, -4)$. Compute $P_1 \oplus P_2$ and $2P_1$ in the group $(E(k), P_2)$ instead.

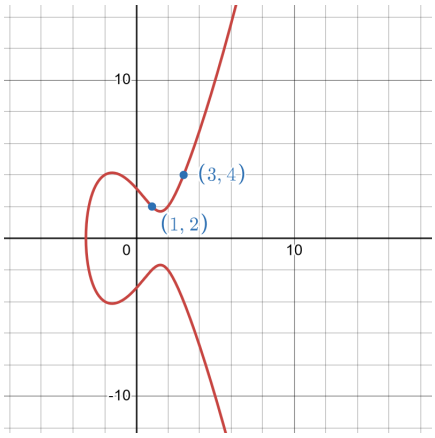

FIGURE 4. The elliptic curve $E : y^2 = x^3 - 7x + 10$.

Exercise 0.11. Show that for a planar elliptic curve $E_{/k}$ and two fixed points $O_1, O_2 \in E(k)$, the groups $(E(k), O_1)$ and $(E(k), O_2)$ are isomorphic.

1. Algebraic Varieties

Exercise 1.1. **Prerequisite: algebraic geometry.**
Show that an algebraic set $V_I \subseteq \mathbb{A}^n$ is irreducible with respect to the Zariski topology iff I is a prime ideal in $\overline{k}[x_1, \ldots, x_n]$. (See also Exercises 0.3 and 1.5.)

Exercise 1.2. Show that for a projective n-variety $V_{/k} \subseteq \mathbb{P}^n$ defined by a single non-constant homogeneous polynomial

$$V : F(X_0, X_1, \ldots, X_n) = 0,$$

one has $\dim(V) = n-1$. Such varieties are called *hypersurfaces.* (For more on projective hypersurfaces, see [Sil09, Exercise 1.11].)

Exercise 1.3. [Sil09, Exercise 1.3] Show that for an affine hypersurface

$$V_{/k} : f(x_1, x_2, \ldots, x_n) = 0,$$

our two definitions of nonsingularity at a point are equivalent. More precisely, for a point $P \in V$, the $1 \times n$ matrix

$$\left(\frac{\partial f}{\partial x_i}\right)_{1 \leq j \leq n}$$

has rank $n-1$ iff $\dim_{\overline{k}}(M_P/M_P^2) = n-1$.

(*Hint:* define the *tangent plane of* V *at* P as

$$T := \left\{(y_1, y_2, \ldots, y_n) \in \mathbb{A}^n : \sum_{i=1}^{n} \left(\left.\frac{\partial f}{\partial x_i}\right|_P\right) \cdot y_i = 0\right\}.$$

Show that the map

$$M_P/M_P^2 \times T \to \overline{k}, \ (g, y) \mapsto \sum_{i=1}^{n} \left(\left.\frac{\partial g}{\partial x_i}\right|_P\right) \cdot y_i$$

is a well-defined perfect pairing of $\overline{k}$-vector spaces.

Exercise 1.4. Prove that for a projective variety $V_{/k} \subseteq \mathbb{P}^n$:

a. $k(V)$ is well-defined;
b. $\dim(V)$ is well-defined;
c. for at least one $0 \leq i \leq n$, one can have $V_i = \emptyset$.

Exercise 1.5. **Prerequisite: algebraic geometry.** Using the Zariski topology, show that an affine algebraic set $C \subseteq \mathbb{A}^n$ is irreducible iff its projective closure $C_H \subseteq \mathbb{P}^n$ is irreducible; thus, C is an affine variety iff C_H is a projective variety. (See also Exercises 0.3 and 1.1.)

Exercise 1.6. [Sil09, Exercise 1.4] Let $V_{/\mathbb{Q}}$ be the projective variety

$$V : 5X^2 + 6XY + 2Y^2 = 2YZ + Z^2.$$

Prove that $V(\mathbb{Q}) = \emptyset$.

Exercise 1.7. [Sil09, Exercise 1.6] Let $V \subseteq \mathbb{P}^2$ be the variety

$$V : Y^2Z = X^3 + Z^3.$$

Show that the map

$$\phi\colon V \dashrightarrow \mathbb{P}^2,\ \phi = [X^2 : XY : Z^2]$$

is a morphism. (Notice that ϕ does not extend to a morphism $\phi\colon \mathbb{P}^2 \to \mathbb{P}^2$.)

Exercise 1.8. [Sil09, Exercise 1.7] Let $V \subseteq \mathbb{P}^2$ be the variety

$$V : Y^2Z = X^3,$$

and let ϕ be the rational map

$$\phi\colon \mathbb{P}^1 \dashrightarrow V,\ \phi = [S^2T, S^3, T^3].$$

a. Show that ϕ is a morphism.
b. Find a rational map $\psi\colon V \dashrightarrow \mathbb{P}^1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity wherever they are defined.
c. Is ϕ an isomorphism?

Exercise 1.9. [Sil09, Exercise 1.10] For each prime $p \geq 3$, let $V_p \subseteq \mathbb{P}^2$ be the variety given by the equation

$$V_p : X^2 + Y^2 = pZ^2.$$

a. Prove that V_p is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ if and only if $p \equiv 1 \pmod 4$.
b. Prove that for $p \equiv 3 \pmod 4$, no two of the V_p's are isomorphic over $\mathbb{Q}$.

2. Algebraic Curves

Exercise 2.1. [Sil09, Exercise 2.1] Let R be a Noetherian local domain that is not a field, let $M \subseteq R$ be its maximal ideal and set $k := R/M$ its residue field. Show that the following are equivalent:

a. R is a discrete valuation ring;
b. M is principal;
c. $\dim_k M/M^2 = 1$.

(For us, this exercise is applied to the local ring $\overline{k}[C]_P$ at a smooth point P on a curve C.)

Exercise 2.2. Consider the elliptic curve

$$E_{/\mathbb{Q}} : Y^2Z = X^3 + Z^3.$$

We have a $\mathbb{Q}$-morphism $\phi\colon E \to \mathbb{P}^1$ given by projection,

$$\phi := [X : Z].$$

a. Prove that $[\mathbb{Q}(E) : \phi^*(\mathbb{Q}(\mathbb{P}^1))] = 2$.
b. Prove that ϕ is ramified at $P := [-1 : 0 : 1]$.
c. Argue that P is the only ramified point of ϕ above $\phi(P)$.
d. (Optional) Using visuals, explain what ϕ being ramified at P means in this example.

(*Hint for all parts:* do things locally!)

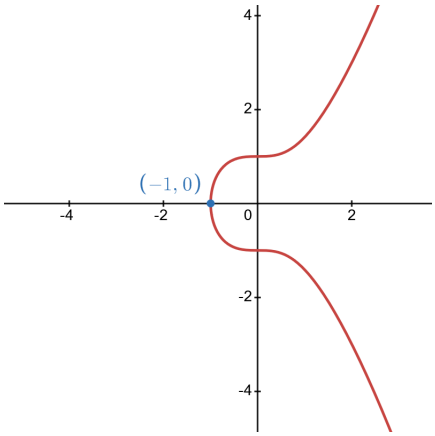

FIGURE 5. The elliptic curve $E : y^2 = x^3 + 1$.

Exercise 2.3. [Sil09, Exercise 2.2] Let $\phi\colon C_1 \to C_2$ be a morphism of smooth curves. Let $g \in \overline{k}(C_2)^\times$, and let $P \in C_1$. Prove that

$$v_P(\phi^*(g)) = e_\phi(P) \cdot v_{\phi(P)}(g).$$

Exercise 2.4. This exercise proves some properties about the Frobenius morphism, see [Sil09, Proposition II.2.11]. It also serves as a review of inseparable extensions.

Recall that an algebraic field extension K/F is **separable** if for any element $\alpha \in K$, the minimal polynomial $m(x) \in F[x]$ of α over F has no repeated roots; this is equivalent to $\gcd(m(x), m'(x)) = 1$. If all elements $\alpha \in K$ have minimal polynomials over F with repeated roots, then K/F is said to be **purely inseparable.**

a. Show that if K/F is not separable, then $\mathrm{char}(K)$=$\mathrm{char}(F) > 0$.
b. Show that the following are equivalent:
   1. K is purely inseparable over F;
   2. for all $\alpha \in K$, there exists $n \geq 0$ with $\alpha^{p^n} \in F$;

3. each $\alpha \in K$ has a minimal polynomial over F of the form $x^{p^n} - a$ for some $n \in \mathbb{Z}_{\geq 0}$ and some $a \in F$.

Let k be a field with $p :=\text{char}(k) > 0$. Fix a power $q := p^r$, as well as a curve $C_{/k}$. Prove the following:

c. $F_q^*(k(C^{(q)})) = k(C)^q := \{f^q : f \in k(C)\}$.
d. F_q is purely inseparable.
e. $\deg(F_q) = q$.

For more on separable and inseparable extensions, see these notes from Keith Conrad: `https://kconrad.math.uconn.edu/blurbs/galoistheory/separable1.pdf`.

Exercise 2.5. [Sil09, Exercise 2.4] Let C be a smooth curve and $D \in \text{Div}(C)$. Without using Riemann-Roch, prove the following:

a. $\mathcal{L}(D)$ is a $\overline{k}$-vector space.
b. If $\deg(D) \geq 0$, then
$$\ell(D) \leq \deg(D) + 1.$$

Exercise 2.6. [Sil09, Exercise 2.5] Let C be a smooth curve. Prove that the following are equivalent (over $\overline{k}$):

a. C is isomorphic to $\mathbb{P}^1$.
b. C has genus 0.
c. There exist distinct points $P, Q \in C$ with $(P) \sim (Q)$.

Exercise 2.7. [Sil09, Exercise 2.6] Let C be a smooth curve of genus one, and fix a base point $P_0 \in C$.

a. Prove that for all $P, Q \in C$ there exists a unique $R \in C$ such that
$$(P) + (Q) \sim (R) + (P_0).$$
Denote this point R by $\sigma(P, Q)$.
b. Prove that the map $\sigma\colon C \times C \to C$ makes C into an abelian group with identity element P_0.
c. Define a map
$$\kappa\colon C \to \text{Pic}^0(C)$$
via
$$P \mapsto [(P) - (P_0)].$$
Prove that κ is a bijection, and thus κ can be used to make C into a group via the rule
$$P + Q := \kappa^{-1}(\kappa(P) + \kappa(Q)).$$
d. Prove that the group operations on C defined in parts b. and c. are the same.

Exercise 2.8. [Sil09, Exercise 2.7] Let $F(X, Y, Z) \in k[X, Y, Z]$ be a homogeneous polynomial of degree $d \geq 1$, and assume that the curve $C \subseteq \mathbb{P}^2$ defined by
$$C : F(X, Y, Z) = 0$$
is nonsingular. Prove that
$$g(C) = \frac{(d-1)(d-2)}{2}.$$

(*Hint:* one way to do this is to define a map $C \to \mathbb{P}^1$ and use Riemann-Hurwitz. Another way is to cleverly construct a nonzero differential ω on C, and then use the fact that $\deg(\mathrm{div}(\omega)) = 2g(C) - 2$.)

Exercise 2.9. [Sil09, Exercise 2.8] Let $\phi\colon C_1 \to C_2$ be a separable morphism of smooth curves.

a. Prove that $g(C_1) \geq g(C_2)$.
b. Prove that if C_1 and C_2 have the same genus g, then one of the following is true:
   i. $g = 0$.
   ii. $g = 1$ and ϕ is unramified.
   iii. $g \geq 2$ and ϕ is an isomorphism.

Exercise 2.10. [Sil09, Exercise 2.13] Let $C_{/k}$ be a smooth curve.

a. Prove that the following sequence is exact:
$$1 \to k^\times \to k(C)^\times \to \mathrm{Div}_k^0(C) \to \mathrm{Pic}_k^0(C).$$
b. Suppose that C has genus one and $C(k) \neq \emptyset$. Prove that the map
$$\mathrm{Div}_k^0(C) \to \mathrm{Pic}_k^0(C)$$
is surjective.

Exercise 2.11. [Sil09, Exercise 2.14] For this exercise, we assume that $\mathrm{char}(k) \neq 2$. Let $f(x) \in k[x]$ be a polynomial of degree $d \geq 1$ with nonzero discriminant (see Exercise 0.2), let C_0/k be the affine curve given by the equation
$$C_0 : y^2 = f(x) := a_0x^d + a_1x^{d-1} + \ldots + a_{d-1}x + a_d,$$
and let g be the unique integer satisfying $d - 3 < 2g \leq d - 1$.

a. Let C be the closure of the image of C_0 via the map
$$[1 : x : x^2 : \ldots : x^{g+1} : y]\colon C_0 \to \mathbb{P}^{g+2}.$$
Prove that C is smooth, and that the affine piece C_{X_0} is isomorphic to C_0. The curve C is called a *hyperelliptic curve.*
b. Let
$$f^*(v) := v^{2g+2}f\left(\frac{1}{v}\right) := \begin{cases} a_0 + a_1v + \ldots + a_{d-1}v^{d-1} + a_dv^d & \text{if } d \text{ is even,} \\ a_0v + a_1v^2 + \ldots + a_{d-1}v^d + a_dv^{d+1} & \text{if } d \text{ is odd.} \end{cases}$$
Show that C consists of two affine pieces
$$C_0 : y^2 = f(x)$$
and
$$C_1 : w^2 = f^*(v),$$
"glued together" via the maps
$$C_0 \to C_1$$
where
$$(x, y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right),$$

and

$$C_1 \to C_0$$

where

$$(v, w) \mapsto \left(\frac{1}{v}, \frac{w}{v^{g+1}}\right).$$

c. Calculate the divisor of the differential $\frac{dx}{y}$ on C and use the result to show that C has genus g. Check your answer by applying Riemann-Hurwitz to the map $[1 : x] \colon C \to \mathbb{P}^1$. (Note that Exercise 2.8 does not apply, since $C \not\subseteq \mathbb{P}^2$.)

d. Find a basis for the holomorphic differentials on C. (*Hint:* consider the set of differential forms $\{x^i \frac{dx}{y} : i = 0, 1, 2, \ldots\}$. How many elements in this set are holomorphic?)

3. The Geometry of Elliptic Curves

Exercise 3.1. [Sil09, Exercise 3.3] Assume that $\mathrm{char}(k) \neq 3$, and let $A \in k^\times$. Then Exercise 2.8 ([Sil09, Exercise 2.7]) shows that the curve

$$E : X^3 + Y^3 = AZ^3$$

is a curve of genus one, so together with the point $O = [1 : -1 : 0]$, it is an elliptic curve. (See also Exercise 0.7.)

a. Prove that three points on E add to O if and only if they are collinear.

b. Let $P := [X : Y : Z]$. Prove the formulas

$$-P = [Y : X : Z]$$

and

$$[2]P = [-Y(X^3 + AZ^3) : X(Y^3 + AZ^3) : X^3Z - Y^3Z].$$

c. Develop an analogous formula for the sum of two distinct points.

d. Prove that E has j-invariant 0.

Exercise 3.2. [Sil09, Exercise 3.6] Let C be a smooth curve of genus g, let $P_0 \in C$, and let $n \geq 2g + 1$ be an integer. Choose a basis $\{f_0, \ldots, f_m\}$ for $\mathcal{L}(n(P_0))$, and define a map

$$\phi \colon C \to \mathbb{P}^m$$

via

$$\phi := [f_0 : \ldots : f_m].$$

a. Prove that the image $C' := \phi(C)$ is a curve in $\mathbb{P}^m$.

b. Prove that the map $\phi \colon C \to C'$ has degree one.

c. *Prove that C' is smooth and that $\phi \colon C \to C'$ is an isomorphism.

Exercise 3.3. **Towards local fields.** Let K be a field.

a. Show that if $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ is a non-Archimedean absolute value, then $|\cdot|$ induces a valuation $v_{|\cdot|} \colon K \to \mathbb{R}_{\geq 0}$ via

$$v_{|\cdot|}(x) := \begin{cases} -\ln|x| & \text{if } x \neq 0, \\ \infty & \text{if } x = 0. \end{cases}$$

b. Show that if $v\colon K \to \mathbb{R} \cup \{\infty\}$ is a valuation, then we have an induced absolute value $|\cdot|_v\colon K \to \mathbb{Z} \cup \{\infty\}$ via

$$|x|_v := \begin{cases} 2^{-v(x)} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

c. Prove that an absolute value $|\cdot|\colon K \to \mathbb{R}$ is non-Archimedean if and only if $|\mathbb{Z} \cdot 1_K|$ is bounded.

d. Deduce that if $v\colon K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation, then $|\cdot|_v$ is non-Archimedean.

Exercise 3.4. **Towards local fields.**

a. Prove directly that $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation.

b. More generally, show that every nonzero prime ideal $\mathfrak{P} \subseteq K$ induces a discrete valuation $v_{\mathfrak{P}}\colon K \to \mathbb{Z} \cup \{\infty\}$.

c. Show that $\mathbb{Q}_p \neq \mathbb{Q}$.

Exercise 3.5. **Towards local fields.**

a. Show that for any real number $c > 1$, the p-adic norm $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ satisfies

$$|x|_p \sim c^{-v_p(x)}.$$

b. Let K be a field. Show that two nontrivial absolute values $|\cdot|_1, |\cdot|_2$ on K are equivalent if and only if they induce the same topology on K.

Exercise 3.6. **Towards local fields.** Prove **Hensel's Lemma** on lifting roots:

Theorem (Hensel's Lemma)**.** *Let K be a complete non-Archimedean field with valuation ring R, maximal ideal M and residue field $k := R/M$. Let $f \in R[t]$ be a polynomial, and let $\overline{f} \in k[t]$ be its reduction modulo M. If $a \in k$ is a simple root of $\overline{f}$ (i.e., $\overline{f}(a) = 0$ and $\overline{f}'(a) \neq 0$), then there exists $\alpha \in R$ with $\alpha \equiv a \pmod{M}$ and $f(\alpha) = 0$.*

Exercise 3.7. [Sil09, Exercise 3.30] Let G be a finite abelian group of order n^r. Suppose that for each $d \mid n$ we have $\#G[d] = d^r$, where $G[d]$ is the subgroup of G of elements whose orders divide d. Prove that

$$G \cong (\mathbb{Z}/n\mathbb{Z})^r.$$

Exercise 3.8. In this exercise, we assume that $\mathrm{char}(k) = 0$.

a. Suppose that C_1 and C_2 are curves defined over k, and that $\phi\colon C_1 \to C_2$ is a morphism. Let us write

$$\phi = [f_0 : f_1 : \ldots : f_n]$$

where each $f_i \in \overline{k}(C_1)$. Prove that for each $\sigma \in G_k$, the map $\phi^\sigma\colon C_1 \to C_2$ defined by

$$\phi^\sigma := [f_0^\sigma : f_1^\sigma : \ldots : f_n^\sigma]$$

is a morphism to C_2 with $\deg(\phi^\sigma) = \deg(\phi)$. (*Hint:* show that $\phi^*(\overline{k}(C_2)) \cong (\phi^\sigma)^*(\overline{k}(C_2))$.)

b. Let E_1/k and E_2/k be non-CM elliptic curves, and fix an isogeny $\phi\colon E_1 \to E_2$. Show that for each $\sigma \in G_k$, there exists $a_\sigma \in \{\pm 1\}$ with $\phi^\sigma = a_\sigma \cdot \phi$.

c. Continuing part b., show that the map $\chi\colon G_k \to \{\pm 1\}$ defined by $\sigma \mapsto a_\sigma$ is a homomorphism. Conclude that there exists $d \in \overline{k}^\times$ such that for all $\sigma \in G_k$, one has

$$\sigma(\sqrt{d}) = \chi(\sigma) \cdot \sqrt{d}.$$

This exercise can be used to show that there exists a *twist*[1] of E_2 by χ, denoted E_2^χ/k, and a k**-rational** isogeny $\psi\colon E_1 \to E_2^\chi$. Thus, in the non-CM case, we can assume an isogeny between k-rational elliptic curves is also k-rational (up to $\overline{k}$-isomorphism of the target elliptic curve). More on twists in Chapter 10.

Exercise 3.9. Let E and E' be elliptic curves, and let $\phi\colon E \to E'$ be an isogeny.

a. Show that if E, E' and ϕ are k-rational, then so is the dual $\widehat{\phi}$.
b. Show that if ϕ is *cyclic,*[2] then so is its dual $\widehat{\phi}$ if one of the following holds:
   i. $\mathrm{char}(k) = 0$.
   ii. $\mathrm{char}(k) > 0$ is coprime to $\deg(\phi)$.

Exercise 3.10. [Sil09, Exercise 3.24] Let $E_{/k}$ be an elliptic curve with complex multiplication over k, i.e., such that $\mathrm{End}_k(E) \neq \mathbb{Z}$. Prove that for all primes $p \neq \mathrm{char}(k)$, the action of G_k on $T_p(E)$ is abelian. (*Hint:* use the fact that all endomorphisms in $\mathrm{End}_k(E)$ commute with the action of G_k on $T_p(E)$.)

Exercise 3.11. [Sil09, Exercise 3.26] Let $E_{/k}$ be the elliptic curve $y^2 = x^3 + x$ having complex multiplication by $\mathbb{Z}[i]$, let $p \geq 3$ be a prime, and let $T \in E[p]$ be a point of order p. In each of the following situations, prove that $\{T, [i]T\}$ is a basis for $E[p]$, and thus $e_p(T, [i]T)$ is a primitive p'th root of unity.

a. $p \equiv 3 \pmod 4$.
b. $i \notin k$ and $T \in E(k)$.

The map $[i]$ is an example of a *distortion map.*

Exercise 3.12. **Prerequisite: algebraic number theory.** This exercise proves some properties that the mod-n Galois representation of an elliptic curve can satisfy.

Fix an integer $n \in \mathbb{Z}^+$ and an algebraic extension $F/\mathbb{Q}$. Let

$$\chi_n\colon G_F \to (\mathbb{Z}/n\mathbb{Z})^\times$$

denote the *mod-n cyclotomic character on* G_F, which describes the action of G_F on the group $\mu_n \subseteq \overline{\mathbb{Q}}$ of n'th roots of unity.

a. Prove that if each prime $p \mid n$ is unramified in F, then χ_n is surjective. Deduce that χ_n is always surjective when $F = \mathbb{Q}$.
b. Prove that for any elliptic curve $E_{/\mathbb{Q}}$ and for any integer $n \in \mathbb{Z}^+$, one has $\det(\rho_{E,n}(G_\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^\times$.
c. Suppose that $F/\mathbb{Q}$ is a real algebraic extension. Prove that for any elliptic curve $E_{/F}$, there exists an order two element $m \in \rho_{E,n}(G_F)$ with trace 0 and determinant -1.

[1] A *twist* of an elliptic curve E is an elliptic curve E' which is isomorphic to E over $\overline{k}$.
[2] Say that an isogeny is *cyclic* if its kernel is cyclic.

5. Elliptic Curves Over Finite Fields

Exercise 5.1. This exercise gives a formula for point counts of elliptic curves base-changed over finite fields. If $q \in \mathbb{Z}^+$ is a prime power and $E_{/\mathbb{F}_q}$ is an elliptic curve, then writing

$$x^2 - a_q(E)x + q = (x - \alpha)(x - \beta)$$

where $\alpha, \beta \in \overline{\mathbb{Q}}$, this exercise shows that for all $n \in \mathbb{Z}^+$, one has

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

a. Writing $F_q \colon E \to E$ for q-power Frobenius, prove that

$$F_q^2 - a_q(E)F_q + q = [0].$$

b. For the polynomial

$$f_n(x) := (x^n - \alpha^n)(x^n - \beta^n),$$

show that $f_n(x) = x^{2n} - (\alpha^n + \beta^n)x^n + q$. Then prove that $x^2 - a_q(E)x + q$ divides $f_n(x)$ in $\mathbb{Z}[x]$.

c. Deduce that we can write

$$f_n(x) = g_n(x) \cdot (x^2 - a_q(E)x + q)$$

for some $g_n(x) \in \mathbb{Z}[x]$. Use this and part a. to prove that

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

Exercise 5.2. Let $p > 2$ be a prime, and let $E_{/\mathbb{F}_p}$ be the elliptic curve

$$E : y^2 = x^3 + x.$$

a. Prove that if $p \equiv 1 \pmod 4$, then

$$4 \mid \#E(\mathbb{F}_p).$$

b. Prove that if $p \equiv 3 \pmod 4$, then

$$\#E(\mathbb{F}_p) = p + 1,$$

i.e., $a_p(E) = 0$.

Thus, in both cases we have $4 \mid \#E(\mathbb{F}_p)$.

c. Create a computer program that does the following: given a prime $p \in \mathbb{Z}^+$ and an elliptic curve $E_{/\mathbb{F}_p} : y^2 = x^3 + Ax + B$, it returns the set $E(\mathbb{F}_p)$, as well as the size $\#E(\mathbb{F}_p)$. What patterns do you notice for $E : y^2 = x^3 + x$ when $p \equiv 1 \pmod 4$, beyond part a.? Based on your calculations, make a reasonable conjecture – and prove it if you can!

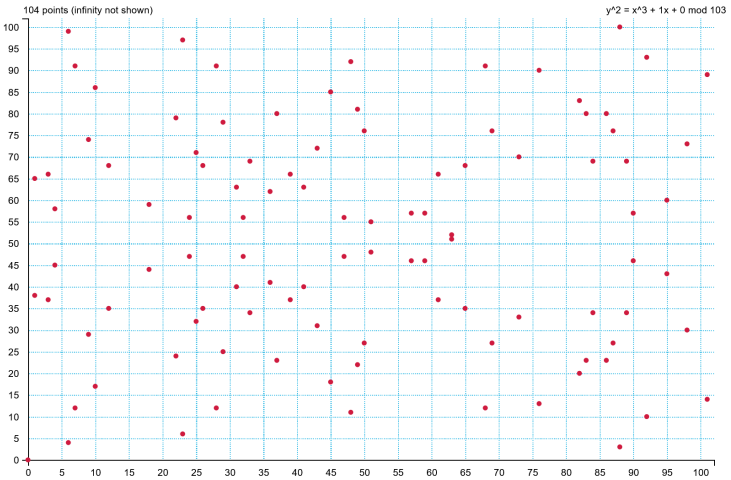

FIGURE 6. The elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{F}_{103}$.

Exercise 5.3. Let $E_{/k}$ be an elliptic curve. This exercise explores the structure of $E(k)[\text{tors}]$ over various fields.

a. Prove there exist $m, n \in \mathbb{Z}^+$ with $m \mid n$, such that
$$E(k)[\text{tors}] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

b. Show that if $k = F$ is a real number field, then there exists $n \in \mathbb{Z}^+$ such that
$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}. \end{cases}$$

c. Show that if $k = \mathbb{F}_q$ is a finite field, then there exist $m, n \in \mathbb{Z}^+$ with $m \mid n$ and $q \equiv 1 \pmod{m}$, such that
$$E(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

d. Show that if $k = \overline{\mathbb{Q}}$, then
$$E(\overline{\mathbb{Q}})[\text{tors}] \cong (\mathbb{Q}/\mathbb{Z}) \times (\mathbb{Q}/\mathbb{Z}).$$

Exercise 5.4.

a. Suppose that $E_{/k}$ and $E'_{/k}$ are k-rationally isogenous elliptic curves. Prove that their k-endomorphism algebras are isomorphic, i.e., $\text{End}_k(E) \otimes \mathbb{Q} \cong \text{End}_k(E') \otimes \mathbb{Q}$.

b. Let $E_{/\mathbb{F}_q}$ and $E'_{/\mathbb{F}_q}$ be elliptic curves, and suppose there exists an $\mathbb{F}_q$-rational isogeny $\phi\colon E \to E'$. Prove that $\#E(\mathbb{F}_{q^r}) = \#E'(\mathbb{F}_{q^r})$ for all $r \geq 1$. (The converse is also true, see [Sil09, Exercise 5.4] or [Tat66].)

7. Elliptic Curves Over Local Fields

Exercise 7.1. Towards local fields. This exercise proves the following result on unramified extensions of local fields.

Theorem. *Given a perfect non-Archimedean local field (K, v) with discrete valuation ring R, uniformizer π and perfect residue field $k := R/\pi$, there is a correspondence between the category of unramified extensions of K and the category of algebraic extensions of k.*

Let L/K be a finite extension; then L is also a non-Archimedean local field, say with discrete valuation w extending v, a discrete valuation ring S for w, a uniformizer Π and residue field $\ell := S/\Pi$.

a. Use Hensel's Lemma to prove there exists an unramified subextension $K \subseteq L' \subseteq L$ with residue field $\ell' = \ell$. Deduce that a finite unramified extension of K is completely determined by its residue field.
b. Show that for each $n \in \mathbb{Z}^+$, there is a unique unramified extension of K with degree n.
c. Conclude that the theorem holds.
d. (Optional) Prove that an unramified extension L/K is always Galois. Then give an explicit isomorphism
$$\mathrm{Gal}(K^{\mathrm{nr}}/K) \xrightarrow{\sim} G_k.$$

Exercise 7.2. [Sil09, Exercise 3.5] Let k be a perfect field, and let $E_{/k}$ be a singular curve in Weierstrass form.

a. Suppose that E has a node, and let the tangent lines at the node be
$$y = m_1 x + b_1 \qquad \text{and} \qquad y = m_2 x + b_2.$$
   i. If $m_1 \in k$, prove that $m_2 \in k$ and
   $$E_{\mathrm{ns}}(k) \cong k^\times.$$
   (This is the *split* case, see Section 7.5.)
   ii. If $m_1 \notin k$, prove that $\ell := k(m_1, m_2)$ is a quadratic extension of k. Note that i. tells us that $E_{\mathrm{ns}}(k) \subseteq E_{\mathrm{ns}}(\ell) \cong \ell^\times$. Prove that
   $$E_{\mathrm{ns}}(k) \cong \{a \in \ell^\times : N_{\ell/k}(a) = 1\}.$$
   (This is the *nonsplit* case, see Section 7.5.)
b. Suppose that E has a cusp. Prove that
$$E_{\mathrm{ns}}(k) \cong (k, +).$$

Exercise 7.3. [Sil09, Exercise 7.1] Assume that $\mathrm{char}(k) \neq 2, 3$.

a. Let $E_{/K}$ be an elliptic curve given by a Weierstrass equation with coefficients $a_i \in R$. Prove that the equation is minimal if and only if either $v(\Delta) < 12$ or $v(c_4) < 4$.
b. Let $E_{/K}$ be given by a minimal Weierstrass equation of the form
$$E : y^2 = x^3 + Ax + B.$$
Prove that E has
   i. *good reduction,* i.e., $\tilde{E}$ is nonsingular, $\iff 4A^3 + 27B^2 \in R^\times$,
   ii. *multiplicative reduction,* i.e., $\tilde{E}$ has a node, $\iff 4A^3 + 27B^2 \in M$ and $AB \in R^\times$,

iii. *additive reduction,* i.e., $\tilde{E}$ has a cusp, $\iff A \in M$ and $B \in M$.

Exercise 7.4. [Sil09, Exercise 7.3] Describe all Weierstrass equations

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

with $a_i \in \mathbb{Z}$ and $\Delta \neq 0$ such that $E(\mathbb{Q})$ contains a torsion point P with $x(P) \notin \mathbb{Z}$. (*Hint:* see the Application in §7.3.)

Exercise 7.5. a. Prove that the elliptic curve

$$E : y^2 + y = x^3 - x$$

has trivial torsion subgroup, but positive rank over $\mathbb{Q}$. (This is the first elliptic curve of minimal *conductor*[3] and positive rank. See its LMFDB page: 37.a1. See also [Sil09, Exercise 9.13].)

b. Prove that the elliptic curve

$$E : y^2 - y = x^3 - x^2$$

has $E(\mathbb{Q})[\text{tors}] \cong \mathbb{Z}/5\mathbb{Z}$. (This is "the first elliptic curve in nature" (minimal conductor), and is a model for the *modular curve* $X_1(11)$. See its LMFDB page: 11.a3.)

c. Prove that the elliptic curve

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 5$$

has $E(\mathbb{Q})[\text{tors}] \cong \mathbb{Z}/3\mathbb{Z}$. (This curve corresponds to a *sporadic* point of degree 3 on the modular curve $X_1(21)$. Up to $\overline{\mathbb{Q}}$-isomorphism, it is the only elliptic curve which has the torsion group $\mathbb{Z}/21\mathbb{Z}$ over a cubic number field. See its LMFDB page: 162.c3.)

Exercise 7.6. Let F be a number field and $E_{/F}$ an elliptic curve. For a nonzero prime ideal $\mathfrak{P} \subseteq \mathcal{O}_F$, say that E has *good reduction at* $\mathfrak{P}$ if $E_{/F_\mathfrak{P}}$ has good reduction, where $F_\mathfrak{P}$ is the completion of F at the discrete valuation $v_\mathfrak{P}$ associated to $\mathfrak{P}$. We also use $\mathcal{O}_{F,\mathfrak{P}}$ to denote the discrete valuation ring in $F_\mathfrak{P}$ associated to $v_\mathfrak{P}$.

a. Assume that E is given by a Weierstrass equation over $\mathcal{O}_F$ that is minimal over $F_\mathfrak{P}$. Prove that E has good reduction at $\mathfrak{P}$ if and only if $\mathfrak{P} \nmid \Delta_{E,F}$.

b. Prove that no elliptic curve $E_{/\mathbb{Q}}$ has good reduction at every prime $p \in \mathbb{Z}^+$. (*Hint:* see [Sil09, Exercise 8.15].)

Note that a Weierstrass equation of an elliptic curve $E_{/F}$ with coefficients in $\mathcal{O}_F$ need not be a minimal equation over each completion $F_\mathfrak{P}$; in fact, such a "global minimal equation" for E is not guaranteed to exist unless F has class number 1 – see §8.8 of [Sil09]. It is worth noting that a global minimal equation always exists when $F = \mathbb{Q}$.

Exercise 7.7. [Sil09, Exercise 7.3] Show that the following elliptic curves have good reduction over a field of the indicated form by writing down a minimal equation for E over that field.

a. $E : y^2 = x^3 + x$, $\mathbb{Q}_2(\eta, i), \eta^8 = 2, i^2 = -1$.

[3]The **conductor** of an elliptic curve $E_{/\mathbb{Q}}$ is a specific integer divisible precisely by the primes of *bad reduction* for E, i.e., the primes p for which $\tilde{E}_{/\mathbb{F}_p}$ is singular.

b. $E : y^2 + y = x^3$, $\mathbb{Q}_3(\pi, \eta), \pi^2 = \sqrt{-3}, \eta^3 = 2.$
c. $E : y^2 = x^3 + x^2 - 3x - 2$, $\mathbb{Q}_5(\pi), \pi^4 = 5.$

Exercise 7.8. [Sil09, Exercise 7.9] Let $E_{/K}$ be an elliptic curve with potential good reduction. Let $n \in \mathbb{Z}^+$ be an integer coprime to $p := \mathrm{char}(k)$, and let $K(E[n])$ be the n-division field of E, obtained by adjoining to K the coordinates of points in $E[n]$.

a. Prove that the inertia group of $K(E[n])/K$ is independent of n. (*Hint:* for each prime $\ell \neq p$, let $\ell' := \ell$ if $\ell \geq 3$ and let $\ell' := 4$ if $\ell = 2$. Show that $\rho_{E,\ell^\infty} \colon I_v \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ has trivial intersection with the kernel of the map
$$\mathrm{Aut}(T_\ell(E)) \to \mathrm{Aut}(T_\ell(E)/\ell' T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}/\ell'\mathbb{Z}).$$
Characterize the inertia group of $K(E[n])/K$ in terms of the kernels of the various ρ_{E,ℓ^∞}.)
b. Prove that $K(E[n])/K$ is unramified if and only if E has good reduction at v.
c. If $p \geq 5$, prove that $K(E[n])/K$ is *tamely ramified,* i.e., the ramification index is coprime to p.

8. Elliptic Curves Over Global Fields

Exercise 8.1. [Sil09, Exercise 8.1] Let $E_{/F}$ be an elliptic curve, let $n \geq 2$ be an integer, let $\mathrm{Cl}(\mathcal{O}_F)$ be the ideal class group of F, and let
$$S := \{v_{\mathfrak{P}} \in \Sigma_F^{\mathrm{NA}} : E \text{ has bad reduction at } \mathfrak{P}\} \cup \{v_{\mathfrak{P}} \in \Sigma_F^{\mathrm{NA}} : \mathfrak{P} \mid n\} \cup \Sigma_F^{\mathrm{Arch}}.$$
Assume that $E[n] \subseteq E(F)$. Prove the following quantitative version of the weak Mordell-Weil theorem:
$$\mathrm{rank}_{\mathbb{Z}/n\mathbb{Z}} E(F)/nE(F) \leq 2 \cdot \#S + 2 \cdot \mathrm{rank}_{\mathbb{Z}/n\mathbb{Z}}(\mathrm{Cl}(\mathcal{O}_F))[n].$$

Exercise 8.2. [Sil09, Exercise 8.2] For each integer $d \geq 1$, let $E_d/\mathbb{Q}$ be the elliptic curve
$$E_d : y^2 = x^3 - d^2 x.$$
Prove that
$$E_d(\mathbb{Q}) \cong \mathbb{Z}^r \times T,$$
where T is a finite group and $r \geq 0$ is an integer satisfying
$$r \leq 2\nu(2d),$$
where $\nu(N)$ denotes the number of distinct primes dividing N. (*Hint:* use Exercise 8.1 ([Sil09, Exercise 8.1])).

Exercise 8.3. [Sil09, Exercise 8.3] Let $E_{/F}$ be an elliptic curve and let L/F be an (infinite) algebraic extension. Suppose that the rank of $E(M)$ is bounded as M ranges over all finite subextensions of L/F, i.e., assume that
$$\sup_{\substack{F \subseteq M \subseteq L: \\ [M:F] < \infty}} \mathrm{rank}(E(M)) < \infty.$$

a. Prove that $E(L) \otimes \mathbb{Q}$ is a finite-dimensional $\mathbb{Q}$-vector space.
b. Assume further that L/F is Galois and that $E(L)[\mathrm{tors}]$ is finite. Prove that $E(L)$ is finitely generated.

Exercise 8.4. [Sil09, Exercise 8.4] Assume that $\mu_n \subseteq F$. Prove that the maximal abelian extension of F of exponent n is the field

$$F(\{a^{1/n} : a \in F\}).$$

(*Hint:* use [Sil09, Proposition VIII.2.2], which says that every homomorphism $\chi\colon G_F \to \mu_n$ has the form $\chi(\sigma) = \frac{\alpha^\sigma}{\alpha}$ for some $\alpha \in \overline{\mathbb{Q}}^\times$ satisfying $\alpha^n \in F^\times$.)

Appendix A. A Review of Local Fields

Several exercises above deal with basic results on *local fields*. They will serve as necessary background for Chapter 7. For a more comprehensive set of notes, see e.g. [ClaANT2].

For a field K, a *valuation on* K is a map $v\colon K \to \mathbb{R} \cup \{\infty\}$ with the following properties:

1. $v(xy) = v(x) + v(y)$ for all $x, y \in K$;
2. $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$;
3. $v(x) = \infty$ if and only if $x = 0$.

For a valuation $v\colon K \to \mathbb{R} \cup \{\infty\}$, the subset

$$R_v := \{x \in K : v(x) \geq 0\}$$

is a local ring in K, with maximal ideal

$$M_v := \{x \in K : v(x) > 0\}.$$

Say v is a *discrete valuation* if its image is $\mathbb{Z} \cup \{\infty\}$. In this case, R_v is a discrete valuation ring.

Given a field K, an *absolute value,* or *norm,* on K, is a map $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ with the following properties:

1. $|xy| = |x| \cdot |y|$ for all $x, y \in K$;
2. $|x+y| \leq |x| + |y|$ for all $x, y \in K$ (triangle inequality);
3. $|x| = 0$ if and only if $x = 0$.

Say $|\cdot|$ is *non-Archimedean* if for all $x, y \in K$ one has $|x+y| \leq \max\{|x|, |y|\}$. Otherwise, say it is *Archimedean.* In general, we call $(K, |\cdot|)$ a *normed field.*

Given a normed field $(K, |\cdot|)$, the subset

$$R_{|\cdot|} := \{x \in K : |x| \leq 1\}$$

is a local ring in K, with maximal ideal

$$M_{|\cdot|} := \{x \in K : |x| < 1\}.$$

Observe that a normed field $(K, |\cdot|)$ inherits a metric space topology from $|\cdot|$. The completion of K with respect to $|\cdot|$ is denoted by $\widehat{K}$. Let us recall the construction of the completion of a metric space (X, d). A sequence $\{x_n\}_{i=1}^\infty \subseteq X$ is called *Cauchy* if for all $\epsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that for any $m, n \geq N$, one has $d(x_m, x_n) < \epsilon$. Two Cauchy sequences $\{x_n\}_{i=1}^\infty, \{y_n\}_{i=1}^\infty \subseteq X$ are said to be *equivalent* if

$$\lim_{n\to\infty} d(x_n, y_n) = 0.$$

Then the *completion of X with respect to d*, written as $\widehat{X}$, is the quotient space of Cauchy sequences of X under this equivalence. The completion $\widehat{X}$ admits the following metric: for all $A, B \in \widehat{X}$, writing $x = [\{x_n\}_{i=1}^{\infty}]$ and $y = [\{y_n\}_{i=1}^{\infty}]$ one has

$$\widehat{d}(x, y) := \lim_{n\to\infty} d(x_n, y_n).$$

We have a natural embedding $\iota\colon X \hookrightarrow \widehat{X}$, and $\iota(X)$ is dense in $\widehat{X}$ under the metric of the completion; furthermore, $\widehat{d} = d$ on $\iota(X)$. If $(X, d) = (K, |\cdot|)$ is a normed field, then the norm extension of $|\cdot|$ to $\widehat{K}$ can be defined as $|x| := \lim_{n\to\infty} |x_n|$.

For each prime $p \in \mathbb{Z}^+$, we let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to the *p-adic norm* $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$. Recall that the *$p$-adic valuation* $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is defined on integers $n \in \mathbb{Z}$ by the relation $p^{v_p(n)} \parallel n$; this extends to a map on $\mathbb{Q}$ in a natural way. In turn, this induces a norm map $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ via

$$|x|_p := |x|_{v_p} := p^{-v_p(x)}.$$

Since $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation which extends to $\mathbb{Q}_p$, there exists a discrete valuation ring $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ for v_p, called the *p-adic integers.* More generally, for a number field F and a nonzero prime ideal $\mathfrak{P} \subseteq F$, we let $F_{\mathfrak{P}}$ denote the $\mathfrak{P}$-adic completion of F with respect to the $\mathfrak{P}$-adic norm $|\cdot|_{\mathfrak{P}}$, and $\mathcal{O}_{F,\mathfrak{P}}$ its discrete valuation ring. The field $\mathbb{Q}_p$, and more generally $F_{\mathfrak{P}}$, is an example of a non-Archimedean local field.

Given a field K and two absolute values $|\cdot|_1, |\cdot|_2$ on K, we say that $|\cdot|_1$ and $|\cdot|_2$ are *equivalent* if there exists $r \in \mathbb{R}_{>0}$ with $|\cdot|_2 = |\cdot|_1^r$. We then write $|\cdot|_1 \sim |\cdot|_2$. There is a classification of absolute values on a number field, due to Ostrowski.

Theorem (Ostrowski's Theorem)**.** *Up to equivalence, the only nontrivial absolute values on $\mathbb{Q}$ are:*

1. *the p-adic norms $|\cdot|_p$ (non-Archimedean);*
2. *the restriction of the usual absolute value $|\cdot|\colon \mathbb{C} \to \mathbb{R}_{\geq 0}$ (Archimedean).*

More generally, for a number field F, up to equivalence any nontrivial absolute absolute value on F is either:

1. *a $\mathfrak{P}$-adic norm $|\cdot|_{\mathfrak{P}}$ for some nonzero prime ideal $\mathfrak{P} \subseteq F$ (non-Archimedean);*
2. *the restriction of the usual absolute value $|\cdot|\colon \mathbb{C} \to \mathbb{R}_{\geq 0}$* to an embedding of F into $\mathbb{C}$. *Such a norm has the form $|\sigma(\cdot)|$ where $\sigma\colon F \hookrightarrow \mathbb{C}$ (Archimedean).*

From here on out, any local field (K, v) we consider will be perfect, as well as its residue field $k := R/\pi$. If L/K is a finite extension, then L is also a complete local field, by a unique discrete valuation w extending v via

$$w(x) := \frac{1}{n} \cdot v(N_{L/K}(x)),$$

where $n := [L : K]$. In terms of norms, this is equivalent to

$$|x|_w := |N_{L/K}(x)|_v^{1/n};$$

see also [ClaANT2, Theorems 1.43, 1.46]. Note, however, that the valuation w above is *not* necessarily normalized, i.e., we might not have $w(L) = \mathbb{Z} \cup \{\infty\}$.

Let $(L, w)/(K, v)$ be a finite extension of complete local fields, with normalized discrete valuations. Let S be the associated discrete valuation ring of L, with uniformizer Π, and let $\ell := S/\Pi$ be the residue field of L. Then the *ramification index* of L/K is the ramification index of π in S; this is well-defined since S has only one prime up to associates, namely Π. One can show that $e(L/K) = [w(L) : w(K)] = w(\pi)$. From $R \subseteq S$ and $\Pi \mid \pi$, we also have an extension of residue fields ℓ/k; the *inertial degree* of L/K is then $f(L/K) := [\ell : k]$. We see that an extension L/K is unramified if and only if $[L : K] = [\ell : k]$.

To make things more concrete: if F is a number field, then for each nonzero prime ideal $\mathfrak{P} \subseteq F$, we have a complete local field $F_{\mathfrak{P}}$ with a discrete valuation $v_{\mathfrak{P}} \colon F \to \mathbb{Z} \cup \{\infty\}$ given by ideal divisibility by $\mathfrak{P}$. If $L/F_{\mathfrak{P}}$ is a finite extension, then $L = M_{\mathfrak{Q}}$ where M/F is some finite extension with $[M_{\mathfrak{Q}} : F_{\mathfrak{Q}}] = [M : F]$, and $\mathfrak{Q} \subseteq M$ is some prime ideal which divides $\mathfrak{P}$ in M. One also has $e(M_{\mathfrak{Q}}|F_{\mathfrak{P}}) = e(\mathfrak{Q}|\mathfrak{P})$ and $f(M_{\mathfrak{Q}}|F_{\mathfrak{P}}) = f(\mathfrak{Q}|\mathfrak{P})$.

Finally, we use K^{nr} to denote the *maximal unramified extension of K,* which is the compositum of all unramified extensions of K. By Exercise 7.1, we have an isomorphism $\mathrm{Gal}(K^{\mathrm{nr}}/K) \cong G_k$ via reduction of automorphisms $\sigma \colon L \xrightarrow{\sim} L$ to $\tilde{\sigma} \colon \ell \xrightarrow{\sim} \ell$, where L/K is unramified (and hence Galois). This fits into a short exact sequence

$$1 \to \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}}) \to G_K \xrightarrow{\mathrm{red}} G_k \to 1.$$

The Galois group $I_v := \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})$ is called the *inertia group* of K.

References

[ClaANT2] P.L. Clark, *Algebraic Number Theory II: Valuations, Local Fields and Adeles*, course notes, `http://alpha.math.uga.edu/~pete/8410FULL.pdf`.

[Mil] J.S. Milne, *Algebraic Number Theory*, v3.08, course notes, `https://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, 2nd Ed., Graduate Texts in Mathematics, vol. 106, Springer (2009).

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134–144.