Lectures On Elliptic Curves

Tamás Szamuely (notes by Antonio Di Nunzio feat. Davide Pierrat)

1 Basic notions

Let k be an algebraically closed field. Recall that the projective plane over k is the quotient

$$\mathbf{P}^2_k = \left(k^3 \setminus \{(0,0,0)\}\right) / \sim$$

where $(x,y,z) \sim (x',y',z')$ if and only if there exists a non-zero element λ in k such that $(x',y',z') = (\lambda x, \lambda y, \lambda z)$.

Definition 1.1. A *projective plane curve* over k is

$$X = \{P \in \mathbf{P}^2_k \colon F(P) = 0\},$$

where F is a homogeneous polynomial in $k[X,Y,Z]$. We say that such a curve is

- *irreducible* if F is irreducible;
- *smooth* if for every P in X, one of $\partial_X F(P), \partial_Y F(P), \partial_Z F(P)$ is non-zero.

In particular, a projective plane curve X is smooth if for every P in X there exists a unique tangent line to X at P, given by the equation

$$\partial_X F(P)\, X + \partial_Y F(P)\, Y + \partial_Z F(Z)\, Z = 0.$$

Remark 1.2. Recall that $\mathbf{P}^2_k$ can be covered by three copies of the affine plane $\mathbf{A}^2_k$:

$$\begin{aligned}
\mathbf{A}^2_k &\xrightarrow{\sim} \mathbf{P}^2_k \setminus \{Z=0\}, \quad (x,y) \mapsto (x,y,1);\\
\mathbf{A}^2_k &\xrightarrow{\sim} \mathbf{P}^2_k \setminus \{Y=0\}, \quad (x,z) \mapsto (x,1,z);\\
\mathbf{A}^2_k &\xrightarrow{\sim} \mathbf{P}^2_k \setminus \{X=0\}, \quad (y,z) \mapsto (1,y,z).
\end{aligned}$$

Intersecting X with these three subsets gives three affine plane curves, defined by the equations

$$\begin{aligned}
f_z(x,y) = 0, \quad f_z(x,y) = F(x,y,1);\\
f_y(x,z) = 0, \quad f_y(x,z) = F(x,1,z);\\
f_x(y,z) = 0, \quad f_x(y,z) = F(1,y,z).
\end{aligned}$$

Conversely, one can recover X from $f_z(x,y)$ by setting

$$F \coloneqq Z^d f_z\left(\frac{X}{Z}, \frac{Y}{Z}\right), \qquad d = \deg(f_z)$$

and similarly for f_x and f_y.

Definition 1.3. An *elliptic curve* over k is a smooth irreducible projective plane curve defined by a polynomial of the form

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

with coefficients a_1, a_2, a_3, a_4, a_6 in k. The equation $F = 0$ is called a *Weierstrass equation* for the elliptic curve.

In this case, the affine curve $f_z(x, y) = 0$ is defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

Moreover, there exists a unique point of the elliptic curve on the projective line $\{Z = 0\}$: this is $(0, 1, 0)$ and is called the *point at infinity* of the elliptic curve.

Now we show that, if $\mathrm{char}(k) \neq 2, 3$, after an invertible linear change of variables (with coefficients in k), we can transform the equation (1.1) into the standard form

$$y^2 = x^3 + Ax + B. \tag{1.2}$$

Indeed, starting from equation (1.1) and substituting

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

we get

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

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$. Substituting

$$x \mapsto \frac{x - 3b_2}{36}, \quad y \mapsto \frac{1}{108}y$$

yields

$$y^2 = x^3 + Ax + B,$$

where $A = 648\, b_4 - 27\, b_2^2$ and $B = 54\, b_2^3 - 1944\, b_2b_4 + 11664\, b_6$. The homogeneous equation is given by

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Note. From now on, we assume $\mathrm{char}(k) \neq 2, 3$.

Now let $F = Y^2Z - X^3 - AXZ^2 - BZ^3$. What is the condition on A, B for the curve $\{F = 0\}$ to be smooth?

Note first that $(0, 1, 0)$ is a smooth point, indeed

$$\partial_Z F(0, 1, 0) = (Y^2 - 2AXZ - 3BZ^2)(0, 1, 0) = 1.$$

For the other points, we check in the (x, y)-plane:

$$\partial_x f_z = -3x^2 - A$$
$$\partial_y f_z = 2y$$

and these are both zero if and only if $y = 0$ and x is a multiple root of $x^3 + Ax + B$. Note that the latter holds if and only if the discriminant of $x^3 + Ax + B$

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

is zero. In particular, if $\Delta \neq 0$, the projective curve defined by $F = 0$ is smooth. In fact this condition is also necessary, because if $\partial_X F(P) = \partial_Y F(P) = 0$, then $\partial_Z F(P) = 0$ because of *Euler's formula:*

$$X\partial_X F + Y\partial_Y F + Z\partial_Z F = \deg(F)F.$$

Exercise 1.4. Verify Euler's formula for an elliptic curve (or in general, if you prefer).

Next, note that several Weierstrass equations can define the same curve: starting from

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

and substituting $X \mapsto u^2X$, $Y \mapsto u^3Y$, $Z \mapsto Z$ for some non-zero u in k, we get

$$u^6Y^2Z = u^6X^3 + u^2AXZ^2 + BZ^3.$$

Dividing by u^6 we obtain

$$Y^2Z = X^3 + A'XZ^2 + B'Z^3, \qquad A' = u^{-4}AX,\ B' = u^{-6}B.$$

Definition 1.5. The *j-invariant* of the elliptic curve $E\colon Y^2Z = X^3 + AXZ^2 + BZ^3$ is

$$j(E) \coloneqq 4 \cdot 27 \cdot \frac{(4A)^3}{4A^3 + 27B^2} \in k.$$

Proposition 1.6. If $E : y^2 = x^3 + Ax + B$ and $E' : y^2 = x^3 + A'x + B'$ are two elliptic curves with $j(E) = j(E')$, then there exists a non-zero u in k such that E' is obtained from E by the substitutions $x \mapsto u^2x$ and $y \mapsto u^3y$.

Proof. By hypothesis, we have

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4(A')^3 + 27(B')^2}.$$

Note that $A = 0$ if and only if $A' = 0$ (and, equivalently, $j(E) = j(E') = 0$). This in particular implies $B, B' \neq 0$ and so we get the claim by setting $u = (B/B')^{1/6}$.

Note also that $B = 0$ if and only if $j(E) = 1728$ (and, equivalently, $B' = 0$). In this case $A, A' \neq 0$ and we get the claim by setting $u = (A/A')^{1/4}$.

Finally, if $A, B \neq 0$, the same computations hold and we can check that

$$\left(\frac{B}{B'}\right)^2 = \left(\frac{A}{A'}\right)^3.$$

In this case, setting $u = (B/B')^{1/6} = (A/A')^{1/4}$ we conclude. □

We shall verify later (Remark 3.4) that two elliptic curves are isomorphic if and only if they are related by a substitution of the above type.
So isomorphism classes of elliptic curves correspond bijectively to values of the j-invariant.

Lemma 1.7. For every j in k, there exists an elliptic curve E over k with $j(E) = j$.

Proof. If $j \neq 0, 1728$, then the elliptic curve

$$E\colon \quad y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}, \tag{1.3}$$

whose standard form is given by

$$y^2 = x^3 + \frac{27j}{1728 - j}x - \frac{54j}{1728 - j},$$

is such that $j(E) = j$. (Note that if $j = 0$, the curve defined by the equation (1.3) is not smooth.

As seen in the proof of Proposition 1.6, for an elliptic curve $E\colon y^2 = x^3 + Ax + B$, we have $j(E) = 0$ if and only if $A = 0$ (and $B \neq 0$) and $j(E) = 1728$ if and only if $B = 0$ (and $A \neq 0$). So these cases also arise. □

In the language of algebraic geometry, the above discussion shows that $\mathbf{A}^1_k$ is the moduli space of elliptic curves over k, each curve corresponding to the point on the line defined by its j-invariant.

Definition 1.8. Let K be a subfield of k. We say that E is defined over K if there exists a Weierstrass equation for E with coefficients in K. We define $E(K)$ to be the set of points of E with coordinates in K.

Typical examples of K will be $\mathbf{Q}$ (when $\mathrm{char}(k) = 0$) or $\mathbf{F}_p$ (when $\mathrm{char}(k) = p$).

From the above discussion, we obtain:

Corollary 1.9. An elliptic curve E is defined over K if and only if $j(E)$ belongs to K.

2 The group law on an elliptic curve

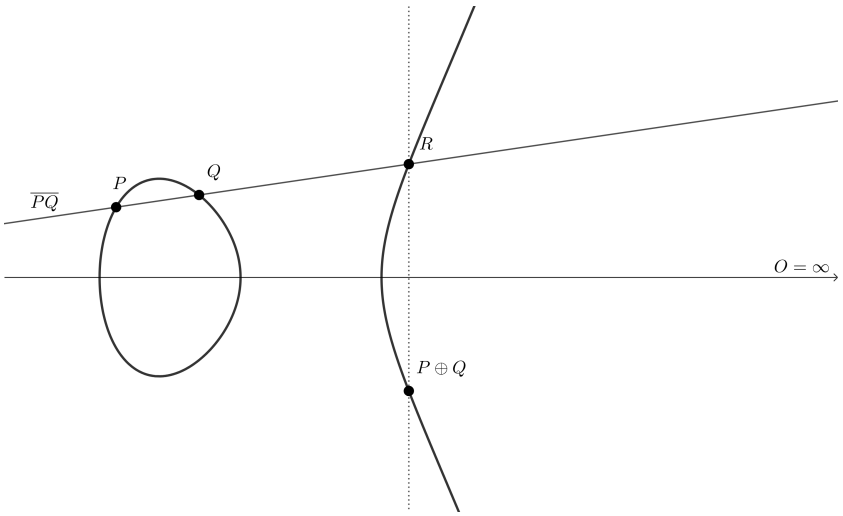
We start with the following observation, allegedly known to Diophantus.

Remark 2.1. If E is an elliptic curve over k and P, Q are two distinct points in $E(k)$, then the line $\overline{PQ}$ has a unique third point of intersection with E. Moreover, if E is defined over a subfield K of k and P, Q belong to $E(K)$, then the third point is in $E(K)$ too.

Proof. After a linear coordinate change, we may assume $\overline{PQ}$ does not go through $(0,1,0)$. So we may argue using the affine equation $y^2 = x^3 + Ax + B$. In this case, the line $\overline{PQ}$ has equation $y = Cx + D$. Intersection points correspond to roots of $(Cx+D)^2 = X^3 + AX + B$. We know that if two roots are in K, then there exists a unique third root in K. □

There is a complement, attributed to Newton: if $P = Q$, the same holds by the tangent line at P to E.

Construction 2.2. Fix a point O in $E(k)$. If P, Q belong to $E(k)$, let R be the third point of intersection of $\overline{PQ}$ with E. We define $P \oplus Q$ to be the third point of intersection of $\overline{RO}$ with E.



Note. If P, Q are in $E(K)$, so is $P \oplus Q$ when E is defined over K and O lies in $E(K)$.

Theorem 2.3. The above construction gives $E(K)$ the structure of an abelian group.

Note that by construction $E(K)$ is clearly commutative with zero element given by the point O. For every point P in $E(K)$ we construct its inverse (denoted by $-P$ or sometimes by $\ominus P$) as follows: let T be the third point of intersection of the tangent line at O (to E) with E (it may happen that $T = O$). We define $-P$ as the third point of intersection of $\overline{PT}$ with E. The most difficult part of the proof of Theorem 2.3 is to show that the composition law is associative. We will prove this after introducing more sophisticated tools.

Remark 2.4. Suppose that O is a *flex* on E (that is, O is a triple intersection point of E with the tangent line at O). It is known that there are nine such points. In this case $-P$ is just the third point of intersection of $\overline{PO}$ with E; moreover, one checks easily that $P \oplus Q \oplus R = O$ if and only if P, Q, R are collinear (this is not true with every O!).

Key example: $O = (0,1,0)$. The tangent line at O to E is $\{Z = 0\}$ and $\{Z = 0\} \cap E = \{X = Z = 0\} = \{(0,1,0)\}$. In what follows we shall make this choice for O.

With an eye for the proof of associativity, we now recall some basic notions from the geometry of plane curves.

Let F be an irreducible polynomial in $k[x,y]$. Then F defines an affine plane curve

$$X = \{P = (a,b) \in \mathbf{A}_k^2 \colon F(P) = 0\}.$$

Since F is irreducible, the ideal (F) is a prime ideal of $k[x,y]$. In particular, the quotient ring $k[x,y]/(F)$ is an integral domain.

Definition 2.5. The *coordinate ring* of the affine plane curve X is the quotient ring

$$\mathcal{A}_X = \frac{k[x,y]}{(F)}.$$

The *function field* of X is the fraction field

$$k(X) \coloneqq \mathrm{Frac}(\mathcal{A}_X)$$

of the coordinate ring of X.

The elements of $k(X)$ can be viewed as functions f/g on X, with f/g and f_1/g_1 identified if F divides $fg_1 - f_1 g$.

Recall that if P is a point in $\mathbf{A}_k^2$, the kernel of the map $k[x,y] \to k$, $f \mapsto f(P)$

$$M_P \coloneqq \{f \in k[x,y] \colon f(P) = 0\}$$

is a maximal ideal of $k[x,y]$. Indeed, setting $P = (a,b)$, the ideal M_P contains the maximal ideal $(x-a, y-b)$. Thus we get $M_P = (x-a, y-b)$.
With a slight abuse of notation, we still denote by M_P the image of M_P in $\mathcal{A}_X$.

Definition 2.6. The *local ring of X at P* is the localization $\mathcal{O}_{X,P}$ of $\mathcal{A}_X$ by M_P.

The ring $\mathcal{O}_{X,P}$ is a subring of the function field $k(X)$ and is represented by elements of the form f/g, with $g(P) \neq 0$, again with f/g and f_1/g_1 identified if F divides $fg_1 - f_1 g$.

Example 2.7. If $F = y^3 - x - 1$ and $P = (-1, 0)$, using the above equivalence relation we have

$$\frac{x+1}{y} = \frac{y^3}{y} = y^2 \in \mathcal{O}_{X,P}.$$

Thus a function in $k(X)$ which at first glance does not look like an element of $\mathcal{O}_{X,P}$ may well be there.

Fact 2.8. Let h be an element in $k(X)$. Then h lies in $\mathcal{O}_{X,P}$ for all but finitely many points P.

Proof. Represent $h = f/g$. Then $\{g = 0\}$ defines an affine plane curve in $\mathbf{A}_k^2$. The plane curves $\{F = 0\}$ and $\{g = 0\}$ do not contain each other (as F is an irreducible polynomial that does not divide g), hence they meet at finitely many points. This can be proved rigorously by an elementary argument on polynomials. A more highbrow argument is: the ring $\mathcal{A}_X$ is an

integral domain whose transcendence degree over k is 1 (as the equation $F = 0$ provides an algebraic dependence relation between the variables x and y). By adding the equation $g = 0$, the transcendence degree of the correspondent coordinate ring drops to zero. Hence the plane curves $\{F = 0\}$ and $\{g = 0\}$ cut out a zero-dimensional variety, that is, a finite set of points. For further details, see [7]. □

Lemma 2.9. Let X be an affine plane curve. Then

$$\mathcal{A}_X = \bigcap_{P \in X} \mathcal{O}_{X,P}.$$

Proof. Clearly $\mathcal{A}_X$ is contained in the intersection. On the other hand, let h be an element in $\bigcap_{P \in X} \mathcal{O}_{X,P}$. Then for each P in X there exist f_P, g_P in $\mathcal{A}_X$ with $g_P(P) \neq 0$ such that $h = f_P/g_P$. Since $\mathcal{A}_X$ is Noetherian, the ideal $(g_P \colon P \in X)$ is finitely generated, say by $g_1, \ldots, g_r$. Then in $k(X)$ we can write

$$h = \frac{f_1}{g_1} = \frac{f_2}{g_2} = \ldots = \frac{f_r}{g_r}$$

so that for each P in X there exists an index $1 \leq i \leq r$ such that $g_i(P) \neq 0$. Observe that $(g_1, \ldots, g_r) = \mathcal{A}_X$. Indeed, if not, the ideal $(g_1, \ldots, g_r)$ would be contained in a maximal ideal of $\mathcal{A}_X$, that is, by Nullstellensatz, the image of some $(x - a, y - b)$ in $\mathcal{A}_X$. But then for $P = (a, b)$ we would have $g_i(P) = 0$ for all indexes i.

Therefore there exist $h_1, \ldots, h_r$ in $\mathcal{A}_X$ such that $\sum_{i=1}^{r} h_i g_i = 1$. Hence

$$h = \sum_{i=1}^{r} h_i h g_i = \sum_{i=1}^{r} h_i \frac{f_i}{g_i} g_i = \sum_{i=1}^{r} h_i f_i \in \mathcal{A}_X.$$

□

Lemma 2.10. If P is a smooth point of an affine plane curve X (i.e. $\partial_x F(P)$ and $\partial_y F(P)$ are not both zero), then the maximal ideal of $\mathcal{O}_{X,P}$ is principal.

Proof. Up to translation, we may assume $P = (0, 0)$. Without loss of generality, we may assume $\partial_y F(0, 0) \neq 0$. We show that the maximal ideal $M_P = (x, y)$ is generated by x, i.e. there exists f in $\mathcal{O}_{X,P}$ such that $y = x \cdot f$. Note that

$$0 = F(x, y) = x\, g(x) + \partial_y F(0, 0)\, y + h(x, y)\, y$$

for some g in $k[x]$ and h in $k[x, y]$ such that $h(0, 0) = 0$. Therefore, setting

$$f \coloneqq -\frac{g}{\partial_y F(0, 0) + h}$$

yields $y = x \cdot f$. Since $h(0, 0) = 0$ and $\partial_y F(0, 0) \neq 0$, we conclude that f belongs to $\mathcal{O}_{X,P}$. □

Corollary 2.11. If P is a smooth point of X, then $\mathcal{O}_{P,X}$ is a discrete valuation ring.

In particular, if P is a smooth point of X, every element f in $k(X)^\times$ can be written as $f = ux^n$, where u is a unit in $\mathcal{O}_{X,P}$ and n is an integer independent of the generator x of M_P.

Notation. If P is a smooth point of X, we denote by v_P the discrete valuation associated to $\mathcal{O}_{X,P}$. In particular, if $f = ux^n$ as before, we have $n \coloneqq v_P(f)$. If $n > 0$, we say that f has a *zero* of order n at P. If $n < 0$, we say that f has a *pole* of order $-n$ at P.

Now let X be an irreducible projective plane curve defined by a homogeneous polynomial F in $k[X, Y, Z]$ of degree d. Recall that

$$\begin{aligned}
&\text{if } Z \neq 0, \text{ then } f_Z = F(x, y, 1) \text{ defines } X_Z \subset \mathbf{A}^2_k \text{ with coordinates } x, y;\\
&\text{if } Y \neq 0, \text{ then } f_Y = F(x, 1, z) \text{ defines } X_Y \subset \mathbf{A}^2_k \text{ with coordinates } x, z;\\
&\text{if } X \neq 0, \text{ then } f_X = F(1, y, z) \text{ defines } X_X \subset \mathbf{A}^2_k \text{ with coordinates } y, z.
\end{aligned}$$

Recall that f_Z and f_Y are linked by

$$f_Y(x, z) = z^d f_Z\left(\frac{x}{z}, \frac{1}{z}\right).$$

Now if P lies in $X(k) \cap \{Z \neq 0\} \cap \{Y \neq 0\}$, then P defines a point of both X_Z and X_Y (that we still denote by P). We have a canonical isomorphism $\mathcal{O}_{X_Z,P} \xrightarrow{\sim} \mathcal{O}_{X_Y,P}$ by

$$\frac{g(x, y)}{h(x, y)} \longmapsto \frac{g\left(x/z, 1/z\right)}{h\left(x/z, 1/z\right)}. \tag{2.1}$$

This is an isomorphism because the procedure can be reversed. Obviously we can argue in a similar way when P lies in $X(k) \cap \{Z \neq 0\} \cap \{X \neq 0\}$ or in $X(k) \cap \{X \neq 0\} \cap \{Y \neq 0\}$, so we can define

$$\mathcal{O}_{X,P} \coloneqq \begin{cases} \mathcal{O}_{X_Z,P} & \text{if } P \in \{Z \neq 0\} \\ \mathcal{O}_{X_Y,P} & \text{if } P \in \{Y \neq 0\} \\ \mathcal{O}_{X_X,P} & \text{if } P \in \{X \neq 0\} \end{cases}$$

and this is well-defined by the above. We can also define $k(X)$ as the common fraction field of the $\mathcal{O}_{X,P}$:

$$k(X) \coloneqq k(X_Z) = k(X_Y) = k(X_X).$$

So there exists a notion of zero and pole of an element f in $k(X)$ at a point P in X.

Example 2.12. Let X be the elliptic curve with equation

$$Y^2Z = X^3 + AXZ + BZ^3.$$

For $Z \neq 0$, the affine curve X_Z has equation $y^2 = x^3 + Ax + B$ and x, y lie in $\mathcal{A}_{X_Z}$ (thus in $k(X_Z) = k(X)$). What about $P = (0, 1, 0)$? It is contained in X_Y.

General recipe:

$$x \in k(X_Z) \Longrightarrow \frac{x}{z} \in k(X_Y).$$

The affine curve X_Y has equation $z = x^3 + Axz^2 + Bz^3$. The maximal ideal of $\mathcal{O}_{X_Y,P}$ is the ideal generated by x (because, as in the proof of Lemma 2.10, ∂_Z does not vanish at P). In this case, we have

$$z = \underbrace{\frac{1}{1 - Axz - Bz^2}}_{\text{unit}} x^3$$

Hence z has a zero of order 3 at P and x/z has a pole of order $2 = 3 - 1$ at P. Also, the element y in $k(X_Z)$ (which corresponds to $1/z$ in $k(X_Y)$ by the isomorphism in (2.1)) has a pole of order 3 at P.

Remark 2.13. We have another description of $k(X)$. Consider the quotient set

$$\widetilde{k(X)} \coloneqq \left\{ \frac{P}{Q} \colon P, Q \in k[X, Y, Z] \text{ homogeneous, } F \nmid Q, \ \deg(P) = \deg(Q) \right\} \Big/ \sim$$

where the equivalence relation is given by

$$\frac{P}{Q} \sim \frac{P'}{Q'} \iff F \mid PQ' - P'Q.$$

Here the condition on degrees is needed to get a well-defined function at points of the projective curve. Recall that

$$k(X) = k(X_Z) = \operatorname{Frac}(\mathcal{A}_{X_Z}) = \left\{ \frac{f}{g} \colon f, g \in k[x, y], \ f_Z \nmid g \right\} \Big/ \sim$$

where

$$\frac{f}{g} \sim \frac{f'}{g'} \iff f_Z \mid fg' - f'g.$$

Define a map $k(X_Z) \to \widetilde{k(X)}$ by

$$\frac{f}{g} \longmapsto \frac{f(X/Z, Y/Z)}{g(X/Z, Y/Z)} = \frac{f(X/Z, Y/Z)Z^d}{g(X/Z, Y/Z)Z^e} Z^{e-d},$$

where $d = \deg(f)$ and $e = \deg(g)$. This map has an inverse, given by

$$\frac{P}{Q} \longmapsto \frac{P(x, y, 1)}{Q(x, y, 1)}.$$

Thus $\widetilde{k(X)}$ provides another description of the function field of X.

Definition 2.14. Let X be a smooth projective plane curve. The *group of divisors* on X is the free abelian group

$$\operatorname{Div}(X) \coloneqq \bigoplus_{P \in X} \mathbf{Z} \cdot P.$$

If f is an element of $k(X)^\times$, the *divisor* of f is the element

$$\operatorname{div}(f) \coloneqq \sum_{P \in X} v_P(f) \cdot P \ \in \operatorname{Div}(X).$$

Note that $\operatorname{div}(f) \in \operatorname{Div}(X)$ because f has only finitely many zeros and poles on X (apply Fact 2.8 to f and $1/f$). Also, the map $\operatorname{div}\colon k(X)^\times \to \operatorname{Div}(X)$ defined by $f \mapsto \operatorname{div}(f)$ is a group homomorphism.

Definition 2.15. Let X be a smooth projective plane curve. The *Picard group* of X is the quotient group

$$\operatorname{Pic}(X) \coloneqq \operatorname{coker}(\operatorname{div}).$$

We denote by $[D]$ the class in $\operatorname{Pic}(X)$ of an element D in $\operatorname{Div}(X)$.

So we have an exact sequence

$$1 \to k^\times \to k(X)^\times \xrightarrow{\operatorname{div}} \operatorname{Div}(X) \to \operatorname{Pic}(X) \to 0.$$

Definition 2.16. The *degree* of an element $D = \sum_{P \in X} n_P \cdot P$ in $\operatorname{Div}(X)$ is the integer

$$\deg(D) \coloneqq \sum_{P \in X} n_P.$$

Note that the map $\deg\colon \operatorname{Div}(X) \to \mathbf{Z}$ defined by $D \mapsto \deg(D)$ is a group homomorphism.

Proposition 2.17. If f is a non-zero element in $k(X)$, then $\deg(\operatorname{div}(f)) = 0$.

Proof. We shall only prove the cases $X = \mathbf{P}^1_k$ or X an elliptic curve. We start with the case $X = \mathbf{P}^1_k$. We identify points of $\mathbf{P}^1_k$ with elements of $k \cup \{\infty\}$. We may assume that f lies in $k[x]$ (this is sufficient, as $\deg \circ \operatorname{div}$ is a group homomorphism). In particular, we can write

$$f = \prod_{i=1}^{r} (x - a_i)^{n_i},$$

whit $n_i = v_{a_i}(f)$. Note that

$$v_\infty(f) = -\deg(f) = -\sum_{i=1}^{r} n_i$$

because x^{-1} generates the maximal ideal of $\mathcal{O}_{\mathbf{P}^1_k,\infty}$. Hence we get

$$\deg(\operatorname{div}(f)) = \sum_{P \in X} v_P(f) = v_\infty(f) + \sum_{i=1}^{r} v_{a_i}(f) = 0.$$

Now we consider an elliptic curve E of equation $y^2 = x^3 + Ax + B$. Write

$$x^3 + Ax + B = \prod_{i=1}^{3} (x - e_i).$$

Then the projection $(x, y) \mapsto x$ is a $2:1$ correspondence except at $(e_i, 0)$ and O. Note that $k(E)|k(\mathbf{P}^1_k)$, where $k(\mathbf{P}^1_k) = k(x)$, is a degree 2 field extension, hence a Galois extension with Galois group isomorphic to $\mathbf{Z}/2\mathbf{Z}$. The non-trivial element sends $f(x, y)$ to $\bar{f}(x, y) \coloneqq f(x, -y)$. For every f in $k(E)$, the element $f\bar{f}$ is fixed by the Galois group, thus is in $k(x)$. Then by the previous case, we have $\deg(\mathrm{div}_{\mathbf{P}^1_k}(f\bar{f})) = 0$. Now we show that

$$\deg(\mathrm{div}_{\mathbf{P}^1_k}(f\bar{f})) = 2\deg(\mathrm{div}_E(f\bar{f})). \tag{2.2}$$

This will be enough because $\deg(\mathrm{div}_E(f)) = \deg(\mathrm{div}_E(\bar{f}))$ since $v_P(f) = v_{-P}(\bar{f})$.

For a in $k \setminus \{e_1, e_2, e_3\}$, the element $x - a$ generates the maximal ideal of $\mathcal{O}_{\mathbf{P}^1_k, a}$, but also that of $\mathcal{O}_{E,\pm P}$, where $\pm P$ are the two points above $a \in \mathbf{P}^1_k$ (because $\partial_y F(\pm P)$ does not vanish). Since the projection is $2:1$, this gives the contribution of $\pm P$.

If $a = e_i$, then $x - e_i$ generates the maximal ideal of $\mathcal{O}_{\mathbf{P}^1_k, e_i}$, but not of $\mathcal{O}_{E,(e_i,0)}$ (there y is a generator). We have

$$y^2 = (x - e_i)\prod_{j \neq i}(x - e_j)$$

and the second factor is a unit in $\mathcal{O}_{E,(e_i,0)}$. Hence $(x - e_i)$ has a zero of order 2 at the point $(e_i, 0)$ of $E(k)$. Finally, the case of O is similar and is left as exercise. □

The above argument also make it possible to prove the following basic fact for elliptic curves.

Proposition 2.18. If X is a projective plane curve, then

$$\bigcap_{P \in X} \mathcal{O}_{X,P} = k.$$

Proof in the case of elliptic curves. Let $X = E$ be an elliptic curve, and let f be an element in $\bigcap_{P \in E} \mathcal{O}_{E,P}$. Then f is contained in $\bigcap_{P \in E \setminus \{O\}} \mathcal{O}_{E,P}$ and thus in $\mathcal{A}_{E \setminus \{O\}}$ by Lemma 2.9. By the previous argument, the element $f\bar{f}$ lies in $\mathcal{A}_{\mathbf{P}^1_k \setminus \{\infty\}} = \mathcal{A}_{\mathbf{A}^1_k} = k[x]$, thus either it is constant or has a pole at ∞. In the latter case, using formula (2.2), we see that f then has a pole at O which contradicts our assumption. So f is constant. □

Definition 2.19. If X is a projective plane curve, we set

$$\mathrm{Div}^0(X) \coloneqq \ker(\deg\colon \mathrm{Div}(X) \to \mathbf{Z}).$$

We define $\mathrm{Pic}^0(X)$ as the image of $\mathrm{Div}^0(X)$ in $\mathrm{Pic}(X)$.

By Proposition 2.17, we have an exact sequence:

$$1 \to k^\times \to k(X)^\times \to \mathrm{Div}^0(X) \to \mathrm{Pic}^0(X) \to 0.$$

Now assume that $X = E$ is an elliptic curve with $O \in E$. Define the map

$$\begin{array}{ccccc} \Phi & : & E(k) & \longrightarrow & \mathrm{Pic}^0(E) \\ & & P & \longmapsto & [P - O] \end{array}.$$

Lemma 2.20. For every P, Q in E, we have

$$\Phi(P \oplus Q) = \Phi(P) + \Phi(Q).$$

Proof. Let R be the third point of intersection of the line $\overline{PQ}$ with E. Let $L_1 = 0$ and $L_2 = 0$ be the equations of the lines $\overline{PQ}$ and $\overline{RO}$ respectively. Then L_1, L_2 are homogeneous polynomials of degree 1, thus the element L_1/L_2 belongs to $k(E)$. We have

$$\operatorname{div}\left(\frac{L_1}{L_2}\right) = P + Q + R - R - O - P \oplus Q = (P - O) + (Q - O) - (P \oplus Q - O).$$

Taking the equivalence classes in $\mathrm{Pic}^0(E)$, we conclude. □

Notation. Let E be an elliptic curve, let P be a point of E and let m be a positive integer. We set

$$P^{\oplus m} \coloneqq \underbrace{P \oplus \ldots \oplus P}_{m \text{ times}} \quad \text{and} \quad P^{\oplus(-m)} \coloneqq \underbrace{(\ominus P) \oplus \ldots \oplus (\ominus P)}_{m \text{ times}}.$$

We also set $P^{\oplus 0} = O$. Finally, if $P_1, \ldots, P_r$ are points in E, we set

$$\sum_{1 \le i \le r}^{\oplus} P_i = P_1 \oplus \ldots \oplus P_r.$$

Corollary 2.21. Let $D = \sum_{P \in E} m_p \cdot P$ be a divisor on an elliptic curve E. Set

$$\sum(D) \coloneqq \sum_{P \in E}^{\oplus} P^{\oplus m_P} \in E(k).$$

Then in $\mathrm{Pic}(E)$ we have

$$[D] = \left[\sum(D)\right] + [(\deg(D) - 1)O].$$

Proof. By Lemma 2.20, for every point Q in E we have $\Phi(\ominus Q) + \Phi(Q) = \Phi(O) = 0$, hence, for every P, Q in E, we get

$$\Phi(P \ominus Q) = \Phi(P) + \Phi(\ominus Q) = \Phi(P) - \Phi(Q).$$

The case $D = P$ is clear. By the above argument, if the formula holds for D, then it holds for $D + P$ and $D - P$. □

Corollary 2.22. The map Φ is surjective.

While we are at it, we mention that a special case of Corollary 2.21 is the following classical theorem, proven by Abel over $\mathbf{C}$.

Theorem 2.23 (Abel)**.** If E is an elliptic curve and $D = \sum_{P \in E} m_p P$ is a divisor on E such that $\deg(D) = 0$, $\sum(D) = O \in E$, then $D = \operatorname{div}(f)$ for some f in $k(E)$.

To conclude the proof of Theorem 2.3, it remains to show that $\ker \Phi$ is trivial. Once we prove this, we will get that $\Phi\colon E(K) \to \operatorname{Pic}^0(E)$ is an additive bijection and therefore $E(k)$ is an abelian group isomorphic to $\operatorname{Pic}^0(E)$.

Remark 2.24. In general, if X is a smooth projective curve, it is possible to give $\operatorname{Pic}^0(E)$ the structure of a projective variety (called the *Jacobian variety*) such that the addition is geometrically defined (like the case of elliptic curves) and $P \mapsto [P - O]$ induces a map $X \to \operatorname{Pic}^0(X)$ which is an embedding if $X \ncong \mathbf{P}^1_k$.

We need the following 'obvious' lemma that has many different proofs.

Lemma 2.25. If E is an elliptic curve, then $k(E)$ is not isomorphic to $k(\mathbf{P}^1_k)$.

Proof. Suppose that X is a plane curve defined by the equation $F = 0$ and let $\rho\colon k(X) \to k(X)$ be a field automorphism, then there exists an induced map (not everywhere defined) $\widetilde{\rho}\colon X \to X$, because $k(X) = \operatorname{Frac}(k[x,y]/(F))$: let $\overline{x}, \overline{y}$ be the image modulo F of x, y respectively, and set $f \coloneqq \rho(\overline{x})$, $g \coloneqq \rho(\overline{y})$ in $k(X)$. So if $P = (a,b)$, then $\widetilde{\rho}(P) = (f(a), g(b))$. If $X = \mathbf{P}^1_k = \{y = 0\}$, we have $k(X) = k(\overline{x})$. Since $\rho^{-1} \circ \rho = \mathrm{id}_{k(\mathbf{P}^1_k)}$, the induced map $\widetilde{\rho}$ must be $1:1$ (everywhere where defined), so if $f = p/q$ for p, q in $k[x]$, for every α in k the equation $p(x)/q(x) = \alpha$ has at most one solution. Thus $p(x) - \alpha q(x) = 0$ has at most one solution, hence $\deg(p) \leq 1$ and $\deg(q) \leq 1$. Therefore we can write

$$f = \frac{ax + b}{cx + d},$$

which has at most two fixed points. But for an elliptic curve E the map $E \to E$ defined by $(x, y) \mapsto (x, -y)$ has four fixed points, so $k(\mathbf{P}^1_k)$ cannot be isomorphic to $k(E)$. □

Definition 2.26. Let X be a smooth projective plane curve and let $D = \sum_{P \in X} m_P P$ be a divisor on X. We set $D \geq 0$ if and only if $m_P \geq 0$ for all P in X. We set $D_1 \geq D_2$ if and only if $D_1 - D_2 \geq 0$.

The previous definition provides a partial order on the group of divisors.

Definition 2.27. Let D be a divisor on X. The *Mittag-Leffler space* of D is the space

$$\mathscr{L}(D) \coloneqq \{f \in k(X)^\times \colon \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

Note that $\mathscr{L}$ is a k-vector subspace of $k(X)$.

Lemma 2.28. Let D, D' be divisors on X.

(*a*) If $D \geq D'$, then $\mathscr{L}(D) \supseteq \mathscr{L}(D')$.

(*b*) If $[D] = [D']$ in $\mathrm{Pic}(X)$, then $\mathscr{L}(D) \cong \mathscr{L}(D')$.

Proof. The first statement is immediate. For the second, if $D' = D + \mathrm{div}(g)$ for some g in $k(X)^\times$, then the k-linear map $\mathscr{L}(D) \to \mathscr{L}(D')$ defined by $f \mapsto fg$ has inverse $f \mapsto fg^{-1}$. □

Lemma 2.29. For every D in $\mathrm{Div}(X)$, we have $\dim_k \mathscr{L}(D) < \infty$. If $D \geq 0$, then $\dim_k \mathscr{L}(D) \leq \deg(D) + 1$.

Proof. By Lemma 2.28, part (*a*), it is enough to prove the second statement because for each D there exists $D' \geq 0$ such that $D' \geq D$. If $D = 0$, then $\mathscr{L}(D) = \mathscr{L}(0) = \bigcap_{P \in X} \mathcal{O}_{X,P} = k$ (Proposition 2.18) and so the lemma is true. By induction, it is enough to prove

$$\forall P \in X, \quad D \geq 0, \quad \dim_k \mathscr{L}(D + P) - \dim_k \mathscr{L}(D) \leq 1.$$

If t generates the maximal ideal of $\mathcal{O}_{X,P}$ and P has coefficient m_P in D, then the k-linear map $\varphi_P \colon \mathscr{L}(D + P) \to k$ defined by $f \mapsto t^{m_P+1} f(P)$ has kernel $\mathscr{L}(D)$. So φ_P induces

$$\mathscr{L}(D + P)/\mathscr{L}(D) \hookrightarrow k.$$

Since k is one-dimensional, we conclude. □

Notation. For f in $k(X)^\times$ with $\mathrm{div}(f) = \sum_{P \in X} m_P P$, we set

$$\mathrm{div}_0(f) \coloneqq \sum_{m_P > 0} m_P P$$
$$\mathrm{div}_\infty(f) \coloneqq \sum_{m_P < 0} (-m_P) P$$

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

Proposition 2.30. If $k(X) \ncong k(\mathbf{P}^1_k)$, then there is no $f \in k(X)^\times$ such that $\mathrm{div}_\infty(f) = P$.

Corollary 2.31. If X is an elliptic curve with origin O and $P \neq O$ is a point of X, then is no $f \in k(X)^\times$ such that $\mathrm{div}(f) = P - O$. In particular, $\ker \Phi = 0$.

Proof of Proposition 2.30. By hypothesis, for f in $k(X)$, the field $k(f)$ is strictly contained in $k(X)$ (indeed the first is purely transcendental over k and so is isomorphic to $k(\mathbf{P}^1_k)$). Since $k(X)$ has transcendence degree 1 over k, there exists a $k(f)$-basis $y_1, \ldots, y_n$ of $k(X)$, with $n \geq 2$. Now assume $\mathrm{div}_\infty(f) = P$. Fix $m > 0$ and fix a divisor $D \geq 0$ such that $y_1, \ldots, y_n$ lie in $\mathscr{L}(D)$,

set $D_m \coloneqq m \cdot \mathrm{div}_\infty(f) + D$. Observe that the elements $f^j y_i$ are in $\mathscr{L}(D_m)$ for $1 \leq j \leq m$ and $1 \leq i \leq n$. Moreover, they are linearly independent over k, thus $\dim_k \mathscr{L}(D_m) \geq m \cdot n$. On the other hand, by Lemma 2.29 we get

$$\dim_k \mathscr{L}(D_m) \leq 1 + \deg(D_m) = 1 + m + \deg(D).$$

For m large, this gives a contradiction. □

3 The Riemann-Roch theorem for elliptic curves

The aim of this section is to prove the following result.

Theorem 3.1 (Riemann-Roch for elliptic curves)**.** Let E be an elliptic curve and let D be a divisor on E such that $\deg(D) > 0$. Then

$$\dim_k \mathscr{L}(D) = \deg(D).$$

We start with some remarks.

Remark 3.2. Let X be a projective plane curve and let D be a divisor on X.

1. If $\deg(D) < 0$, then $\mathscr{L}(D) = 0$.

   > Indeed, if $\mathscr{L}(D) \neq 0$, there exists a f in $k(X)^\times$ such that $\mathrm{div}(f) + D \geq 0$. But then
   >
   > $$0 \leq \deg(\mathrm{div}(f) + D) = \deg(\mathrm{div}(f)) + \deg(D) = \deg(D).$$

2. In general, if X is a smooth projective plane curve defined by the polynomial F of degree d, the *genus* of X is
   $$g \coloneqq \frac{(d-1)(d-2)}{2}.$$
   A form of the Riemann-Roch theorem is the following: if D is a divisor of X such that $\deg(D) \geq 2g - 2$, then
   $$\dim_k \mathscr{L}(D) = \deg(D) - g + 1.$$
   For arbitrary D the inequality $\geq$ always holds (this is Riemann's part) and the difference is equal to the dimension of a certain first cohomology group associated with D.

Exercise 3.3. Show that if $\deg(D) = 0$, then $\dim_k \mathscr{L}(D)$ can be either 0 or 1.

Proof of Theorem 3.1. We start with the case $D = mO$, for $m \geq 1$. If $m = 1$, we have already seen in the proof of Lemma 2.29 that $\mathscr{L}(O) = k$. It is sufficient to prove by induction that

$$\dim_k \mathscr{L}(mO) - \dim_k \mathscr{L}((m-1)O) \geq 1,$$

because we know that the left hand side must be less then or equal to 1.

It is enough to find for $m \geq 2$ an element of $k(E)$ with a pole of order m at O and no poles elsewhere. We have seen that

$$\mathrm{div}_\infty\left(\frac{X}{Z}\right) = 2O, \quad \text{and} \quad \mathrm{div}_\infty\left(\frac{Y}{Z}\right) = 3O.$$

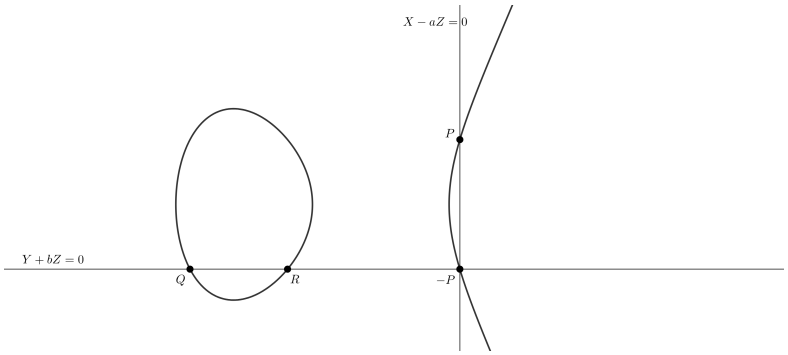
So if $m = 2k \geq 2$, we have $(X/Z)^k \in \mathscr{L}(mO) \setminus \mathscr{L}((m-1)O)$. If $m = 2k+1$, we have

$$\left(\frac{X}{Z}\right)^{k-1}\left(\frac{Y}{Z}\right) \in \mathscr{L}(mO) \setminus \mathscr{L}((m-1)O).$$

Now we consider the case $D = P + mO$, for $m \geq 0$ and P different from O. If $m = 0$, we have again $\mathscr{L}_k(P) = k$. If $m \geq 1$, again it is enough to find an element f in $\mathscr{L}(mO) \setminus \mathscr{L}((m-1)O)$. Suppose $P = (a, b)$ and consider the projective lines $\{X - aZ = 0\}$ and $\{Y + bZ = 0\}$. Then

$$\{X - aZ = 0\} \cap E = \{P, -P, O\},$$
$$\{Y + bZ = 0\} \cap E = \{-P, Q, R\},$$

for some Q, R different from P.



Then

$$\operatorname{div}\left(\frac{Y+bZ}{X-aZ}\right) = Q + R + (-P) - (P + O + (-P)) = Q + R - P - O \geq -P - mO$$

and this is strictly less than $-mO$ because P is different from Q, R. This means

$$\frac{Y+bZ}{X-aZ} \in \mathscr{L}(P + mO) \setminus \mathscr{L}(mO).$$

For the general case, recall that if $[D] = [D']$ in $\operatorname{Pic}(E)$, then $\mathscr{L}(D) \cong \mathscr{L}(D')$. From Corollary 2.21, we know that in $\operatorname{Pic}(E)$

$$[D] = \left[\sum(D) + (\deg(D) - 1)O\right].$$

Thus we reduce to the previous cases. □

Remark 3.4. If $y^2 = x^3 + Ax + B$ and $(y')^2 = (x')^3 + A'x' + B'$ define the same elliptic curve E, then there exists a unit u such that $x = u^2x'$ and $y = u^3y'$.

> Indeed $\{1, x\}$, $\{1, x'\}$ are k-basis of $\mathscr{L}(2O)$ and $\{1, x, y\}$,$\{1, x', y'\}$ are k-basis of $\mathscr{L}(3O)$. Then $x = u_1x' + r$ and $y = u_2y' + sx' + t$ for some u_1, u_2, s, t, r in k. Substituting yields
>
> $$(u_2y' + sx' + t)^2 = (u_1x' + r)^3 + A(u_1x' + r) + B.$$
>
> Checking the equality, we get $s = t = r = 0$ and $u_2^2 = u_1^3$.

Assume now X a smooth projective plane curve defined over a *perfect* field $K \subset k$ such that $k = \overline{K}$, set $G \coloneqq \mathrm{Gal}(k|K)$. Then G acts on $\mathrm{Div}(X)$ by

$$\sigma\left(\sum_{P\in X} m_P P\right) = \sum_{P\in X} m_P\, \sigma(P).$$

Definition 3.5. The *group of K-rational divisors* on X is

$$\mathrm{Div}_K(X) \coloneqq \{D \in \mathrm{Div}(X) \colon \sigma(D) = D \text{ for all } \sigma \in G\}.$$

Also, set $K(X) \coloneqq k(X)^G$. One can show that if X is defined by $\{F = 0\}$ for some F in $K[x, y]$, then

$$K(X) = \mathrm{Frac}\left(\frac{K[x,y]}{(F)}\right).$$

Definition 3.6. Let D be an element in $\mathrm{Div}_K(X)$. We define

$$\mathscr{L}_K(D) = \{f \in K(X)^\times \colon \mathrm{div}(f) + D \geq 0\}.$$

Note that $\mathscr{L}_K(D)$ is a K-vector space and that G acts on $\mathscr{L}(D)$.

Proposition 3.7. The following equalities hold.

$$\dim_K \mathscr{L}_K(D) = \dim_k \mathscr{L}(D)$$
$$\mathscr{L}(D)^G = \mathscr{L}_K(D).$$

This follows from an algebraic result of Spesier, for the proof of which we refer to [9, Lemma 3.7]

Proposition 3.8 (Galois descent)**.** Let V be a finite-dimensional k-vector space with a semi-linear G-action (i.e. $\sigma(v + w) = \sigma(v) + \sigma(w)$ and $\sigma(\lambda v) = \sigma(\lambda)\sigma(v)$).
Then V has a basis consisting of G-invariant vectors (or, in other words, $V^G \otimes_K k \xrightarrow{\sim} V$).

4 Elliptic curves over C

We only include a brief sketch of the theory, referring to the books of Milne [2] or Silverman [5] for details.

Let w_1, w_2 be non-zero complex numbers which are $\mathbf{R}$-linearly independent.

Definition 4.1. A *lattice* in $\mathbf{C}$ is an additive subgroup of $\mathbf{C}$ of the form

$$\Lambda = \{mw_1 + mw_2 \colon (m,n) \in \mathbf{Z}^2\}.$$

Note that Λ is a discrete subset for the topology of $\mathbf{C}$. On $\mathbf{C}/\Lambda$ there is an induced topology, and topologically $\mathbf{C}/\Lambda$ is a torus. It also has a complex analytic structure: together with the group structure it becomes a complex commutative Lie group.

Definition 4.2. An *elliptic function* is a meromorphic function f on $\mathbf{C}$ such that $f(z+w) = f(z)$ for all z and for all w in some lattice Λ in $\mathbf{C}$.
We denote by $\mathcal{E}$ the field of elliptic functions.

Elliptic functions also be viewed as meromorphic functions on $\mathbf{C}/\Lambda$. A basic example is:

Example 4.3 (Weierstrass $\wp$ function)**.**

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-w)^2} - \frac{1}{w^2} \right].$$

Fact 4.4. If $\wp'$ denotes the complex derivative of $\wp$, then

1. $\mathcal{E} = \mathbf{C}(\wp, \wp')$.
2. There is a functional equation
$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$
with $g_2^3 - 27g_3^2 \neq 0$. In fact, g_2 and g_3 are given by the Eisenstein series $g_2 = 60\sum_{w\neq 0} \frac{1}{w^4}$ and $g_3 = 140\sum_{w\neq 0} \frac{1}{w^6}$.

Corollary 4.5. The map

$$\begin{array}{rccc} \Psi & : & \mathbf{C}/\Lambda & \longrightarrow & \mathbf{P}^2_{\mathbf{C}} \\ & & z & \longmapsto & (\wp(z), \wp'(z), 1) \end{array}$$

has an elliptic curve as its image.

Fact 4.6. The map Ψ is a $1:1$ correspondence onto its image and induces an isomorphism of complex Lie groups (where the elliptic curve is considered with its group law). Moreover, every elliptic curve over $\mathbf{C}$ arises from a lattice Λ in this way.

We give a proof sketch of the additivity of Ψ. We first start with the following lemma.

Lemma 4.7. Let $n_1, \ldots, n_r$ be integers and let $z_1, \ldots, z_r$ be complex numbers such that $\sum_{i=1}^r n_i = 0$ and $\sum_{i=1}^r n_i z_i = 0$. Then there exists f in $\mathcal{E}$ such that (as a formal sum) $\operatorname{div}(f) = \sum_{i=1}^r n_i z_i$.

Here we convene that $\mathrm{div}(f)$ counts zeros and poles modulo Λ.

Proof. We consider the Weierstrass σ-function:

$$\sigma(z,\Lambda) \coloneqq z \prod_{w\in\Lambda\setminus\{0\}} \left(1-\frac{z}{w}\right)\exp\left(\frac{z}{w}+\frac{1}{2}\left(\frac{z}{w}\right)^2\right).$$

This is holomorphic on $\mathbf{C}$ and has simple zeros at the points in Λ. One checks $(\log\sigma)'' = -\wp$, hence there exist a, b in $\mathbf{C}$ such that $\sigma(z+w) = \exp(az+b)\sigma(z)$ for all w in Λ. Now consider

$$f(z) = \prod_{i=1}^{r} \sigma(z-z_i)^{n_i}.$$

Then f satisfies $\mathrm{div}(f) = \sum_i n_i z_i$ and

$$\frac{f(z+w)}{f(z)} = \prod_{i=1}^{r} \exp\left(a(z-z_i)+b\right)^{n_i} = \exp\left((az+b)\sum_{i=1}^{r} n_i - a\sum_{i=1}^{r} n_i z_i\right) = 1.$$

□

Proof of the additivity of Ψ. For each z_1, z_2 in $\mathbf{C}$, Lemma 4.7 gives a function f in $\mathcal{E}$ such that

$$\mathrm{div}(f) = (z_1)+(z_2)-(z_1+z_2)-(0).$$

By Fact 4.4 (1), there exists F in $\mathbf{C}(X,Y)$ such that $f = F(\wp,\wp')$. So Ψ sends $\mathcal{E}$ to the function field of E. Hence we get a rational function over E with divisor $\Psi(z_1)+\Psi(z_2)-\Psi(z_1+z_2)-\Psi(0)$. Now use $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$. □

Corollary 4.8. If $E|\mathbf{C}$ is an elliptic curve, then

$$E[m] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z},$$

where $E[m]$ is the set of points of E of order dividing m.

5 Elliptic curves over finite fields

We shall define a zeta function associated with a smooth projective plane curve over a finite field. To motivate the definition, we first discuss the classical Riemann ζ.

Definition 5.1. The *Riemann zeta function* is defined by the formula

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}.$$

It is absolutely convergent for $\Re(s) > 1$ and has the following representation as an Euler product

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

Facts 5.2. The following properties hold.

1. The function $\zeta(s)$ extends to a holomorphic function on $\mathbf{C}\setminus\{1\}$ with a simple pole at $s=1$.
2. The function
$$\xi(s) \coloneqq \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$
where $\Gamma(s) \coloneqq \int_0^\infty t^{s-1}\exp(-t)\,\mathrm{d}t$ is the Gamma function (defined for $\Re(s)>1$ and extended holomorphically to $\mathbf{C}$), satisfies the functional equation
$$\xi(s) = \xi(1-s).$$

Conjecture 5.3 (Riemann hypothesis)**.** If $0 \le \Re(s) \le 1$ and $\zeta(s)=0$, then $\Re(s)=\frac{1}{2}$.

Now we consider a smooth projective plane curve C over the finite field $\mathbf{F}_q$ with q elements. We denote
$$N_m \coloneqq \#C(\mathbf{F}_{q^m})$$
the number of points of C over $\mathbf{F}_{q^m}$.

Definition 5.4. The *zeta function* of C is the exponential generating function
$$Z_C(T) \coloneqq \exp\left(\sum_{m\ge 1} N_m \frac{T^m}{m}\right).$$

Why is this a zeta function? Notice that if $P=(a_0,a_1,a_2)$ is a point in $C(\mathbf{F}_{q^m})$, then $\sigma(P)=(\sigma(a_0),\sigma(a_1),\sigma(a_2))$ is in $C(\mathbf{F}_{q^m})$ for all σ in the Galois group $\mathrm{Gal}(\overline{\mathbf{F}_q}|\mathbf{F}_q)$, indeed $C=\{F=0\}$ for some homogeneous polynomial F in $\mathbf{F}_q[X,Y,Z]$.

Definition 5.5. Given a point P in $C(\overline{F_q})$, we set
$$\deg(P) \coloneqq \min\{m\ge 1 \colon P \in C(\mathbf{F}_{q^m})\}.$$
This is the same as the size of the orbit of P under $\mathrm{Gal}(\overline{\mathbf{F}_q}|\mathbf{F}_q)$.

By definition of the logarithmic series, we have
$$\log\left(\frac{1}{1-T^{\deg(P)}}\right) = \sum_{N=1}^{\infty}\frac{T^{N\deg(P)}}{N} = \sum_{N=1}^{\infty}\deg(P)\frac{T^{N\deg(P)}}{N\deg(P)}.$$

Taking the sum over the P-orbits and substituting $m = N\deg(P)$, we get

$$\begin{aligned}\sum_{P\text{-orbits}} \log\left(\frac{1}{1-T^{\deg(P)}}\right) &= \sum_{P\text{-orbits}} \sum_{N=1}^{\infty} \deg(P)\frac{T^{N\deg(P)}}{N\deg(P)} \\ &= \sum_{m=1}^{\infty} \frac{T^m}{m} \sum_{\substack{P\text{-orbits} \\ \deg(P)|m}} \deg(P) \\ &= \sum_{m\geq 1} \frac{T^m}{m} N_m = \log(Z_C(T)).\end{aligned}$$

So

$$Z_C(T) = \prod_{P\text{-orbits}} \frac{1}{1-T^{\deg(P)}}.$$

Substitute $T = q^{-s}$: then $Z_C(q^{-s})$ looks like the Riemann zeta function.

Recall that the genus of C is the number

$$g = \frac{(d-1)(d-2)}{2}.$$

Theorem 5.6 (Hasse for elliptic curve, Weil in general)**.** The following properties hold.

1. $Z_C(T)$ lies in $\mathbf{Q}(T)$. More precisely
$$Z_C(T) = \frac{p(T)}{(1-T)(1-qT)}, \quad P \in \mathbf{Z}[T],\ P(0) = 1,\ \deg(P) = 2g.$$
2. (Functional equation)
$$Z_C(T) = q^{g-1}\,T^{2g-2}\,Z_C\left(\frac{1}{qT}\right).$$
3. ("Riemann Hypothesis") If $p(T) = \prod_{j=1}^{2g}(1-\alpha_j T)$, then $|\alpha_j| = q^{1/2}$.

Note that, setting $\zeta_C(s) \coloneqq Z_C(q^{-s})$, the third condition of Theorem 5.6 means

$$\zeta_C(s) = 0 \implies \Re(s) = 1/2.$$

- The α_j are algebraic integers which have absolute value $q^{1/2}$ in *every complex embedding* (e.g. for $g = 1$ are conjugate complex numbers but can't be distinct real numbers).
- Let F be the homogeneous polynomial in $\mathbf{F}_q[X,Y,Z]$ defining C. If F lifts to $\widetilde{F}$ in $\mathcal{O}_K[X,Y,Z]$, with K a number field and $\mathcal{O}_K$ its ring of integers, then it defines a curve over $\mathbf{C}$. The first Betti number of this curve (that is, the rank of the first homology/cohomology group) is $2g$.

Theorem 5.6 has the following generalization.

Theorem 5.7 (Weil Conjectures)**.** Let $X|\mathbf{F}_q$ be a smooth projective variety of dimension d. Define

$$Z_X(T) \coloneqq \exp\left(\sum_{m=1}^{\infty} \#X(\mathbf{F}_{q^m})\frac{T^m}{m}\right).$$

The following properties hold.

(1) $Z_X(T)$ lies in $\mathbf{Q}(T)$ and in fact

$$Z_X(T) = \frac{P_1(T)\cdot P_3(T)\dots P_{2d-1}(T)}{P_0(T)\cdot P_2(T)\dots P_{2d}(T)}$$

where $P_i \in \mathbf{Q}[T]$, $P_i(0) = 1$, $P_0(T) = 1 - T$, $P_{2d}(T) = 1 - q^dT$.

(2) $Z_X(T)$ satisfies the following functional equation

$$Z_X(T) = \pm q^{-\frac{\chi\cdot d}{2}} T^{-\chi} Z\left(\frac{1}{q^dT}\right)$$

where χ is a certain Euler characteristic (which in dimension 1 is $2-2g$).

(3) ("Riemann Hypothesis") If $P_i(T) = \prod_j (1-\alpha_{i,j}T)$, then $|\alpha_{i,j}| = q^{i/2}$ in every complex embedding.

(4) If X comes via "reduction modulo p" from a smooth projective variety $\widetilde{X}$ defined over some $\mathcal{O}_K$, then $\deg(P_i)$ is the i-th Betti number of $\widetilde{X}$ considered as a variety over $\mathbf{C}$.

Properties (1), (2) and (4) was proved by Grothendieck; property (3) by Deligne (and the fact that $Z_X(T)$ lies in $\mathbf{Q}(T)$ by Dwork). For the proof of Theorem 5.7 we refer to [6].

Now we prove (1) and (2) in the case of elliptic curves. Let E be an elliptic curve. Write

$$Z_E(T) = \prod_{P\text{-orbits}} \frac{1}{1-T^{\deg(P)}} = \prod_{P\text{-orbits}} (1 + T^{\deg(P)} + T^{2\deg(P)} + \dots) = \sum_{\substack{D\in \mathrm{Div}_{\mathbf{F}_q}(E)\\ D\geq 0}} T^{\deg(D)}.$$

We use the following lemma.

Lemma 5.8. Let E be an elliptic curve over $\mathbf{F}_q$.

(a) The number A of classes of degree $d \geq 0$ in $\mathrm{Pic}(E)$ represented by divisors D in $\mathrm{Div}_{\mathbf{F}_q}(E)$ is finite and does not depend on d.

(b) Given $D \geq 0$ in $\mathrm{Div}_{\mathbf{F}_q}(E)$, we have

$$\#\{D' \in \mathrm{Div}_{\mathbf{F}_q}(E)\colon D' \geq 0,\ [D] = [D'] \text{ in } \mathrm{Pic}(E)\} = \frac{q^d-1}{q-1},$$

where $d = \deg(D)$.

Proof. We start by proving (a). From Corollary 2.21, we know that

$$[D] = \left[\sum(D) - (\deg(D) - 1)O\right].$$

Since D is $\mathbf{F}_q$-rational, the element $\sum(D)$ lies in $E(\mathbf{F}_q)$, but $E(\mathbf{F}_q)$ is finite, hence for fixed d there are finitely many of these. Also, the map $D \mapsto D - (\deg(D))O$ induces a bijection

$$\{D \in \mathrm{Div}_{\mathbf{F}_q}(E)\colon\ \deg(D) = d\} \longleftrightarrow \{D \in \mathrm{Div}_{\mathbf{F}_q}(E)\colon\ \deg(D) = 0\}.$$

This bijection preserves classes in $\mathrm{Pic}(E)$.

Now we prove (b). If $[D] = [D']$, then $D' = D + \deg(f)$ for some non-zero function f. Recall that there is an exact sequence

$$\overline{\mathbf{F}_q}^{\times} \to \overline{\mathbf{F}_q}(E)^{\times} \xrightarrow{\mathrm{div}} \mathrm{Div}(E)$$

so there is an injection

$$\frac{\overline{\mathbf{F}_q}(E)^{\times}}{\overline{\mathbf{F}_q}^{\times}} \hookrightarrow \mathrm{Div}(E)$$

equivariant for $G = \mathrm{Gal}(\overline{\mathbf{F}_q}|\mathbf{F}_q)$. So there is an injection

$$\left(\frac{\overline{\mathbf{F}_q}(E)^{\times}}{\overline{\mathbf{F}_q}^{\times}}\right)^G \hookrightarrow \mathrm{Div}(E)^G = \mathrm{Div}_{\mathbf{F}_q}(E).$$

We will see later (Remark 8.19 below) that the map

$$\mathbf{F}_q(E)^{\times} = \left(\overline{\mathbf{F}_q}(E)^{\times}\right)^G \longrightarrow \left(\frac{\overline{\mathbf{F}_q}(E)^{\times}}{\overline{\mathbf{F}_q}^{\times}}\right)^G$$

is surjective: this will be a consequence of Hilbert's Theorem 90.
So we may assume that the above f lies in $\mathbf{F}_q(E)^{\times}$. Note that $D' = D + \deg(f) \geq 0$ is equivalent to f lying in $\mathscr{L}(D)^G = \mathscr{L}_{\mathbf{F}_q}(D)$, and by Riemann-Roch theorem $\mathscr{L}_{\mathbf{F}_q}(D)$ is an $\mathbf{F}_q$-vector space of dimension $\deg(D) = d$. So the number of these functions is $q^d - 1$. Also, we have

$$\deg(f) = \deg(f') \iff \deg\left(\frac{f}{f'}\right) = 0 \iff \frac{f}{f'} \in \mathbf{F}_q^{\times},$$

so exactly $q - 1$ functions have the same divisor. □

Proof of (1) *for elliptic curves.* By Lemma 5.8, we get

$$\begin{aligned}
\sum_{\substack{D \in \mathrm{Div}_{\mathbf{F}_q}(E)\\ D \geq 0}} T^{\deg(D)} &= 1 + \sum_{d \geq 1} T^d \sum_{\substack{\deg(D) = d\\ D \geq 0}} 1 = 1 + A \sum_{d \geq 1} \frac{q^d - 1}{q - 1} T^d \\
&= 1 + \frac{A}{q-1} \sum_{d \geq 1} \left((qT)^d - T^d\right) \\
&= 1 + \frac{A}{q-1}\left(\frac{qT}{1-qT} - \frac{T}{1-T}\right) \\
&= 1 + \frac{AT}{(1-T)(1-qT)} = \frac{1 + aT + qT^2}{(1-T)(1-qT)},
\end{aligned}$$

with $a = A - 1 - q$. □

Proof of (2) *for elliptic curves.* Using (1), a straightforward calculation shows

$$Z_E\left(\frac{1}{qT}\right) = \frac{1+\frac{a}{qT}+\frac{1}{qT^2}}{\left(1-\frac{1}{qT}\right)\left(1-\frac{1}{T}\right)} = \frac{qT^2+aT+1}{(qT-1)(T-1)} = Z_E(T).$$

□

Remark 5.9. Write $1+aT+qT^2 = (1-\alpha T)(1-\beta T)$. Then

$$\log Z_E(T) = \sum_{m\geq 1} N_m \frac{T^m}{m} = \log\left(\frac{1}{1-T}\right) + \log\left(\frac{1}{1-qT}\right) - \log\left(\frac{1}{1-\alpha T}\right) - \log\left(\frac{1}{1-\beta T}\right).$$

Comparing coefficients, we get

$$N_m = 1 + q^m - \alpha^m - \beta^m.$$

So if (3) is true, then $|\alpha| = |\beta| = q^{1/2}$, and we get the *Hasse-Weil bound*

$$|N_m - (1+q^m)| \leq 2 \cdot \sqrt{q^m}.$$

Conversely, if we know that $|N_m - (1+q^m)| \leq C \cdot \sqrt{q^m}$ for some positive C, then (3) follows.

Indeed, recall from complex analysis that if f is a meromorphic function in $\mathbf{C}$, then the logarithmic derivative f'/f has simple poles at the zeros and poles of f. So the function

$$\varphi_E(T) \coloneqq \frac{Z_E'(T)}{Z_E(T)} - \frac{1}{1-T} - \frac{q}{1-qT}$$

has poles only where $Z_E(T)$ has zeros. By comparing coefficients, we can write

$$\varphi_E(T) = \sum_{m\geq 0} a_m T^m, \quad a_m = N_{m+1} - q^{m+1} - 1$$

So if $|a_m| \leq Cq^{(m+1)/2}$, then the convergence radius of $\varphi_E(T)$ is

$$\liminf_{m\to\infty} \frac{1}{\sqrt[m]{|a_m|}} \geq q^{-1/2}.$$

So $\varphi_E(T)$ is holomorphic for $|T| < q^{-1/2}$. Therefore, all *reciprocal* roots of $Z_E(T)$ have absolute value less then or equal to $q^{1/2}$. But then they have absolute value equal to $q^{1/2}$, because by (2) we have $Z_E(T) = Z_E(1/qT)$.

Thus it remains to prove:

Theorem 5.10. Let $E|\mathbf{F}_q$ be an elliptic curve and let m be a positive integer. Then

$$|\#E(\mathbf{F}_{q^m}) - (q^m+1)| \leq C\sqrt{q^m}$$

for some $C > 0$

As noted in the above remark, the theorem implies the Riemann hypothesis for E and hence also that we may choose $C = 2$.

Proof (Bombieri-Stepanov). Up to changing the power of the prime p, we may assume $m = 1$. We construct a non-zero function Φ in $\mathbf{F}_q(E)$ that has a pole only at O and zeros at every point in $E(\mathbf{F}_q)\setminus\{O\}$. Since $\deg(\mathrm{div}(\Phi)) = 0$, a bound on the order of pole at O gives a bound on $\#E(\mathbf{F}_q)$.

We shall fix constants $n, m \geq 0$ that will be chosen later. We have seen that $\mathscr{L}_{\mathbf{F}_q}(mO)$ has a basis $f_1, \ldots, f_m$ such that each f_i is in $\mathscr{L}_{\mathbf{F}_q}(iO) \setminus \mathscr{L}_{\mathbf{F}_q}((i-1)O)$. We also fix $s_1, \ldots, s_m$ in $\mathscr{L}_{\mathbf{F}_q}(nO)$.

Notation. For each $i = 1, \ldots, m$, we set $f_i^{(q)}(x, y) = f_i(x^q, y^q)$.

Now there are two lemmas:

Lemma 5.11. If b, q are such that $q > np^b$ and there exists i such that $s_i \neq 0$, then the function

$$\Phi \coloneqq \sum_{i=1}^{m} s_i^{p^b} f_i^{(q)}$$

is non-zero.

Lemma 5.12. If $mn > p^b n + m$, then there exist $s_1, \ldots, s_m$ in $\mathscr{L}(nO)$ not all zero, such that

$$\sum_{i=1}^{m} s_i^{p^b} f_i^{(q)} = 0.$$

If we make choices as in Lemma 5.11 and in Lemma 5.12, then Φ is non-zero, has a pole only at O (as s_i and f_i have only poles at O), and $\Phi(P) = 0$ for all P in $E(\mathbf{F}_q)\setminus\{O\}$. Indeed, a point $P = (a, b)$ lies in $E(\mathbf{F}_q)$ if and only if $(a, b) = (a^q, b^q)$, that is, if and only if $f_i(P) = f_i^{(q)}(P)$ for each index i, so

$$\Phi(P) = \sum_{i=1}^{m} s_i^{p^b}(P) f_i^{(q)}(P) = \sum_{i=1}^{m} s_i^{p^b}(P) f_i(P) = 0.$$

Proof of Lemma 5.11. Suppose by contradiction that $\Phi = 0$. Let h be the index where $s_h \neq 0$ but $s_i = 0$ for all $i > h$. Then

$$s_h^{p^b} f_h^{(q)} = -\sum_{i=1}^{h-1} s_i^{p^b} f_i^{(q)}.$$

Applying v_O (which computes the order of pole at O), we find

$$p^b\, v_O(s_h) + q\, v_O(f_h) \geq \min_{i<h} \left\{p^b\, v_O(s_i) + q\, v_O(f_i)\right\} \geq -p^b n - q(h-1).$$

Hence we get

$$p^b\, v_O(s_h) \geq -p^b n - q(h - 1 + v_O(f_h)) \geq -p^b n + q > 0.$$

Therefore $s_h(O) = 0$, but s_h has no poles outside O, hence $s_h = 0$. □

Proof of Lemma 5.12. All functions of the form $\sum_{i=1}^{r} s_i^{p^b} f_i$ are in $\mathscr{L}_{\mathbf{F}_q}((p^b n + m)O)$ and this is an $\mathbf{F}_q$-vector space of dimension $p^b n + m$ by the (easy) special case of the Riemann–Roch theorem for $D = (p^b n + m)O$. Similarly, $\dim \mathscr{L}_{\mathbf{F}_q}(nO) = n$, hence the $s_1, \ldots, s_m$ can be chosen in nm ways, but $nm > p^b n + m$, so two of the $\sum_{i=1}^{r} s_i^{p^b} f_i$ are equal. Their difference is of the same form and is equal to 0. □

Notice that Φ is in $\mathbf{F}_q(E)^{\times p^b}$ because $q > p^b$. Thus for every P in $E(\mathbf{F}_q) \setminus \{O\}$ we have $v_P(\Phi) \geq p^b$. On the other hand, Φ lies in $\mathscr{L}((p^b n + mq)O)$, so since $\deg(\operatorname{div}(\Phi)) = 0$, we have

$$p^b(\#E(\mathbf{F}_q) - 1) \leq p^b n + mq.$$

Now choose $q = p^{2b}$, $n = p^b - 1$ and $m = p^b + 2$. Then

$$q > np^b$$
$$nm > p^b n + m$$

and so

$$p^b(\#E(\mathbf{F}_q) - 1) \leq p^b(p^b - 1) + (p^b + 2)p^{2b} = p^{3b} + 3p^{2b} - p^b.$$

So we get

$$\#E(\mathbf{F}_q) - q - 1 = \#E(\mathbf{F}_q) - p^{2b} - 1 \leq 3p^b - 1 \leq 3\sqrt{p^{2b}} \leq 3\sqrt{q}.$$

The lower bound comes from a trick: suppose $P = (x, y)$ is such that x lies in $\mathbf{F}_q$. Then $x^q = x$ and $y^2 = x^3 + Ax + B$, so $y^q = \pm y$. But $(x, -y) = -P$. Denote by F_q the map $(x, y) \mapsto (x^q, y^q)$. We have just seen that

$$\#\{P \in E(\overline{\mathbf{F}_q}) \colon F_q(P) = P\} - (q + 1) \leq 3\sqrt{q}. \tag{5.1}$$

Similarly, we get

$$\#\{P \in E(\overline{\mathbf{F}_q}) \colon F_q(P) = -P\} - (q + 1) \leq 3\sqrt{q} \tag{5.2}$$

by the same argument, except we apply Lemma 5.12 with the substitution $f_i \to f_i^{(-)}$, where $f_i^{(-)}(x, y) = f_i(x, -y)$. Moreover, we have

$$\#\{P \in E(\overline{\mathbf{F}_q}) \colon F_q(P) = P\} + \#\{P \in E(\overline{\mathbf{F}_q}) \colon F_q(P) = -P\} = 2(q - 1) - C \tag{5.3}$$

for $1 \leq C \leq 4$ (here C is the number of 2-torsion points of E defined over $\mathbf{F}_q$). But for q large, (5.1), (5.2) and (5.3) can only hold together if

$$\#\{P \in E(\overline{\mathbf{F}_q}) \colon F_q(P) = P\} - (q + 1) \geq -C' - 3\sqrt{q},$$

where $C' = C + 4$. Choosing $C'' > 3 + C'/\sqrt{q}$, this proves $|\#E(\mathbf{F}_q) - (q + 1)| < C''\sqrt{q}$. □

6 Introduction to p-adic numbers

The notes for this section were taken by Davide Pierrat.

Let us give some motivation for the need of p-adic numbers.

Consider a polynomial f in $\mathbf{Z}[x_1, \ldots, x_m]$. We are interested in studying its roots in $\mathbf{Z}$ (that is, points in $\mathbf{Z}^m$ where f vanishes). Does a solution exist?

A necessary condition is: $f \equiv 0 \pmod{n}$ has solution for all n. Equivalently (by Chinese Remainder Theorem), $f \equiv 0 \pmod{p^r}$ for all choices of p prime, $r \geq 1$.

A solution modulo p^r reduces to a solution modulo p^s for all $s \leq r$. We want some way to go the other way around, and investigate higher and higher powers of p. The p-adic integers will allow us to "talk about modulo p^r" for all r-s at once.

Definition 6.1. An *inverse system* of sets indexed by $\mathbf{N}$ is given by

- for all n in $\mathbf{N}$, a set X_n;
- for all n in $\mathbf{N}^+$, a map $\varphi_n : X_n \to X_{n-1}$.

The *inverse limit* of the system is

$$\varprojlim X_n := \left\{ (x_n) \in \prod_{n \geq 0} X_n : \varphi_n(x_n) = x_{n-1} \text{ for all } n > 0 \right\}.$$

In other words, it is the set of coherent sequences with elements in X_n.

Note that if the sets X_n are groups (or rings, topological spaces) and the maps φ_n are group homomorphisms (resp., ring homomorphisms, continuous maps), then the inverse limit is also equipped with that additional structure.

Example 6.2. Let k be a field. Let $X_n = k[t]/(t^n)$ and let $\varphi_n : X_n \to X_{n-1}$ be the map defined by $p(t) \mod t^n \mapsto p(t) \mod t^{n-1}$. This is an inverse system of rings whose limit is

$$\varprojlim k[t]/(t^n) = k[\![t]\!],$$

the ring of formal power series in one variable.

So we are developing polynomials in power series. Applying a similar construction to the rings $\mathbf{Z}/(p^n)$ for a fixed prime p, we get:

Definition 6.3. Let $X_n = \mathbf{Z}/(p^n)$ and let $\varphi_n : \mathbf{Z}/(p^n) \to \mathbf{Z}/(p^{n-1})$ be the map defined by $x \mod p^n \mapsto x \mod p^{n-1}$.
The inverse limit $\mathbf{Z}_p$ of this inverse system is called the *ring of p-adic integers*.

This definition is due to Kurt Hensel, as is the following proposition.

Proposition 6.4. For a prime p and a polynomial f in $\mathbf{Z}[x_1, \ldots, x_m]$, we have

$$f \equiv 0 \pmod{p^r} \text{ is solvable for all } r \iff f = 0 \text{ is solvable in } \mathbf{Z}_p.$$

Before proving this, we need a lemma.

Lemma 6.5. Let (X_n) be an inverse system of nonempty finite sets. Then the inverse limit $\varprojlim X_n$ is non empty.

Note: this holds more generally if the X_n are compact Hausdorff spaces and the maps φ_n are continuous, but not in general. Counterexample: the inverse limit of the intervals $(0, 1/n)$ in $\mathbf{R}$ with respect to the natural inclusions is their intersection, which is empty.

Proof. The claim is clear if every transition map φ_n is surjective, as we can recursively choose lifts to higher and higher values of n. Let us reduce the problem to this particular case.

First note we can compose the maps φ_i to get $\varphi_{nm} = \varphi_m \circ \cdots \circ \varphi_{n+1} : X_m \to X_n$ whenever $m > n$.

Now define

$$Y_n = \{x \in X_n \colon x \in \mathrm{im}(\varphi_{mn}) \text{ for all } m > n\}.$$

It is easily checked (by crucially using the fact that X_n is finite) that the Y_n are non empty. The transition maps restricted to the sets Y_n are surjective, so we have reduced to the case of surjective transition maps and we are done. □

Proof of Proposition 6.4. For the non-trivial implication, let X_r be the set of solution of the equation $f \equiv 0 \mod p^r$. Then the above lemma shows $\varprojlim X_r$ is non empty, and an element of this inverse limit is exactly a solution in $\mathbf{Z}_p^m$. □

Proposition 6.6. An element $b = (b_n)$ in $\mathbf{Z}_p$ is a unit if and only if $b_1 \neq 0$.

Proof. If (b_n) is invertible, then every b_n is invertible, so that $b_1 \neq 0$.

Conversely, if $b_1 \neq 0$, then the equation $b_n x \equiv 1 \mod p^n$ is solvable by the Euler-Fermat theorem and gives a unique solution x_n in $\mathbf{Z}/(p^n)$. By uniqueness, the mod p^{n-1} image of x_n must be x_{n-1}, so the (x_n) assemble to a solution of $bx = 1$ in $\mathbf{Z}_p$. □

Corollary 6.7. The ring $\mathbf{Z}_p$ is a local ring with maximal ideal $p\mathbf{Z}_p$. The residue field is $\mathbf{Z}_p/p\mathbf{Z}_p = \mathbf{F}_p$.

Proof. By Corollary 6.6, the complement of $p\mathbf{Z}_p$ is exactly the set of units of $\mathbf{Z}_p$.

The map $\mathbf{Z}_p \to \mathbf{F}_p$ defined by $(a_n) \mapsto a_1$ induces $\mathbf{Z}_p/p\mathbf{Z}_p = \mathbf{F}_p$. □

From the definitions it follows that $\bigcap_{n\geq 1} p^n \mathbf{Z}_p = 0$. We thus obtain the following statement.

Corollary 6.8. Every nonzero element of $\mathbf{Z}_p$ can be written as up^n, where u is a unit in $\mathbf{Z}_p$ and n is a non-negative integer.

Corollary 6.9. The ring of p-adic integers $\mathbf{Z}_p$ is an integral domain (and thus a discrete valuation ring by Corollary 6.8).

Proof. Let x, y be non-zero elements in $\mathbf{Z}_p$. Then $x = up^n$ and $y = vp^m$. Then the product $xy = uvp^{m+n}$ is non-zero (we are using the fact that powers of p don't vanish; this is because $\mathbf{Z} \to \mathbf{Z}_p$ is injective). □

Let $\mathbf{Q}_p$ be the fraction field of $\mathbf{Z}_p$. It follows easily from Corollary 6.8 that every non-zero element of $\mathbf{Q}_p$ can be uniquely written as up^k, where u is a unit in $\mathbf{Z}_p$ and k is an integer.

We define the *p-adic valuation* on $\mathbf{Q}_p$ by the formula

$$\begin{array}{rccc} v_p & : & \mathbf{Q}_p & \longrightarrow & \mathbf{Z} \cup \{+\infty\} \\ & & 0 & \longmapsto & +\infty \\ & & up^k & \longmapsto & k. \end{array}$$

This is indeed a discrete valuation. Namely, it satisfies

$$\begin{aligned} v_p(xy) &= v_p(x) + v_p(y) \\ v_p(x+y) &\geq \min\{v_p(x), v_p(y)\}. \end{aligned}$$

The embedding $\mathbf{Z} \to \mathbf{Z}_p$ sending a to the sequence of its mod p^n reductions induces an embedding $\mathbf{Q} \to \mathbf{Q}_p$ of fraction fields. We easily see that

$$\mathbf{Z}_p \cap \mathbf{Q} = \mathbf{Z}_{(p)} \coloneqq \left\{ \frac{a}{b} \in \mathbf{Q} \colon p \nmid b \right\}.$$

The p-adic valuation can be translated into a norm function on $\mathbf{Q}_p$ as follows. Let

$$\|x\|_p \coloneqq \mathrm{e}^{-v_p(x)},$$

where we agree that $\mathrm{e}^{-\infty} = 0$. The properties of the valuation translate to

$$\begin{aligned} \|xy\|_p &= \|x\|_p \|y\|_p \\ \|x+y\|_p &\leq \max\{\|x\|_p, \|y\|_p\}. \end{aligned}$$

We used the number e as our base, but any choice of real number $\alpha > 1$ was fine. Often $\alpha = p$ is chosen.

Note the triangle inequality is stronger than the usual one. It is sometimes called the "strong triangle inequality", and metric spaces satisfying this are called *ultrametric spaces*.

A consequence of the strong triangle inequality is that a sequence (x_n) in $\mathbf{Q}_p$ is Cauchy if and only if $\|x_n - x_{n+1}\|$ tends to 0 as n goes to ∞. This is false for general metric spaces and is a feature of ultrametric spaces.

Notice $\mathbf{Q}_p$ is then a complete (ultra)metric space: to see this, it suffices to prove the same statement for $\mathbf{Z}_p$. Cauchy sequences stabilize modulo p^k, and hence converge to an element of $\mathbf{Z}_p$.

The following lemma is of crucial importance and is one of the countless forms of Hensel's lemma.

Lemma 6.10 (Hensel's lemma)**.** Let f in $\mathbf{Z}_p[x]$. Suppose a_1 in $\mathbf{Z}_p$ is such that $f(a_1) \equiv 0 \pmod{p}$ and $f'(a_1) \not\equiv 0 \pmod{p}$. Then there exists a in $\mathbf{Z}_p$ such that $f(a) = 0$ and $a \equiv a_1 \pmod{p}$.

Proof. We will construct inductively a sequence (a_n) in $\mathbf{Z}_p$ such that

$$\begin{aligned} f(a_n) &\equiv 0 \pmod{p^n} \\ f'(a_n) &\not\equiv 0 \pmod{p} \\ a_n &\equiv a_{n-1} \pmod{p^{n-1}}. \end{aligned}$$

By the last property they will converge to an element a in $\mathbf{Z}_p$.

The first term a_1 is already given. Suppose a_n has been defined, and inductively satisfies the stated conditions. Let $a_{n+1} = a_n + p^n b$, for some b in $\mathbf{Z}_p$ yet to be chosen.

By the Taylor formula (no analysis is going on, Taylor expansion for polynomials is purely formal) we can write

$$f(a_{n+1}) = f(a_n) + f'(a_n)p^n b + p^{2n}h$$

for some h in $\mathbf{Z}_p$. Since $f(a_n) \equiv 0 \pmod{p^n}$, we have $f(a_n) = p^n c$ for some c in $\mathbf{Z}_p$. As $f'(a_n) \not\equiv 0 \pmod{p}$, we can find b in $\mathbf{Z}_p$ such that $c + bf'(a_n) \equiv 0 \pmod{p}$, so that $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$ as required.

Also, since $a_{n+1} \equiv a_n \pmod{p}$, we have $f'(a_{n+1}) \equiv f'(a_n) \not\equiv 0 \pmod{p}$. □

Two corollaries follow.

Corollary 6.11 (Smooth points of hypersurfaces over $\mathbf{F}_p$ lift to $\mathbf{Z}_p$)**.** Let f be in $\mathbf{Z}_p[x_1, \ldots, x_m]$. Suppose $P = (a_1, \ldots, a_m)$ in $\mathbf{Z}_p^m$ is such that $f(P) \equiv 0 \pmod{p}$ and there exists an index i such that $\partial_i f(P) \not\equiv 0 \pmod{p}$. Then there exists $P' = (\widetilde{a}_1, \ldots, \widetilde{a}_m)$ in $\mathbf{Z}_p^m$ such that $f(P) = 0$ and $\widetilde{a}_j \equiv a_j \pmod{p}$ for all $j = 1, \ldots, m$.

Proof. Let $\widetilde{a}_j = a_j$ for all $j \neq i$. Then $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_m)$ is a polynomial in a single variable. The claim follows from the one-variable Hensel lemma. □

Corollary 6.12 (Roots of unity in $\mathbf{Z}_p$)**.** The ring $\mathbf{Z}_p$ contains all roots of $x^{p-1} - 1$.

Proof. The polynomial $x^{p-1} - 1$ has a full set of $p - 1$ *distinct* roots modulo p. The claim then follows from Hensel's lemma. □

Recall every element in a in $\mathbf{Q}_p^\times$ can be written uniquely in the form $a = up^k$ where u is in $\mathbf{Z}_p^\times$ and k in $\mathbf{Z}$. Thus sending $a \mapsto (u, k)$ defines an isomorphism

$$\mathbf{Q}_p^\times \cong \mathbf{Z}_p^\times \times \mathbf{Z}.$$

Let us define the principal unit groups (*Einseinheitengruppen* in German) by

$$U^{(i)} = \left\{ u \in \mathbf{Z}_p^\times : u \equiv 1 \pmod{p^i} \right\}, \quad i \geq 1.$$

These help us study $\mathbf{Q}_p^\times$ through the filtration

$$\mathbf{Q}_p^\times \supseteq \mathbf{Z}_p^\times \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \ldots$$

Note that $\bigcap_{i \geq 1} U^{(i)} = \{1\}$. Let's investigate the quotients.

- $\mathbf{Q}_p^\times/\mathbf{Z}_p^\times \cong \mathbf{Z}$. We argued this already, and we have seen this quotient splits.
- $\mathbf{Z}_p^\times/U^{(1)} \cong \mathbf{F}_p^\times$. This isomorphism is induced by the map $u \mapsto u \mod p$. This is also a split sequence: a section exists by sending an element of $\mathbf{F}_p^\times$ to the unique $(p-1)$-th root of unity in $\mathbf{Z}_p^\times$ which is congruent to it.
- $U^{(n)}/U^{(n+1)} \cong \mathbf{F}_p$ (*additive* group) for all $n \geq 1$. Indeed there is a map (which is *not* a homomorphism) $U^{(i)} \to p^i\mathbf{Z}_p$ given by $u \mapsto u - 1$. This induces a map $U^{(i)}/U^{(i+1)} \to p^i\mathbf{Z}_p/p^{i+1}\mathbf{Z}_p \cong \mathbf{F}_p$, which *is* a homomorphism (this can be easily checked).

In summary, we get $\mathbf{Q}_p^\times = \mathbf{Z} \times \mathbf{F}_p^\times \times U^{(1)}$, and $U^{(1)}$ has a filtration with successive quotients isomorphic to $\mathbf{F}_p$. We will later see (Proposition 7.15) that

$$U^{(1)} \cong \begin{cases} \mathbf{Z}_p, & \text{if } p > 2 \\ \mathbf{Z}_2 \times \mathbf{Z}/(2), & \text{if } p = 2. \end{cases}$$

Definition 6.13. An abelian group A is *uniquely m-divisible* if multiplication by m is a bijective function from A to itself.

Corollary 6.14. $U^{(1)}$ is uniquely m-divisible for every integer m such that $(m, p) = 1$.

Proof. Let u be in $U^{(1)}$. Consider the polynomial $f(x) = x^m - u$. The element 1 of $\mathbf{F}_p$ is a simple root of the reduction of f modulo p. By Hensel's lemma it lifts to a root of $f(x)$.

We are left with proving uniqueness of m-th roots in $U^{(1)}$.

- We first prove that 1 is the only m-th root of 1 in $U^{(1)}$. If $u \neq 1$ is an element in $U^{(1)}$ such that $u^m = 1$, there is some n such that u lies in $U^{(n)} \setminus U^{(n+1)}$. If we set $\overline{u}$ to be the image of u in $\mathbf{F}_p \cong U^{(n)}/U^{(n+1)}$, we have $\overline{u} \neq 0$ and thus $m\overline{u} \neq 0$ because $(m, p) = 1$. Under the isomorphism, $m\overline{u}$ corresponds to u^m, so we are done.
- If a, b are elements in $U^{(1)}$ such that $a^m = b^m = u$, then a/b is an m-th root of 1 which belongs to $U^{(1)}$. By the above, $a/b = 1$ so that $a = b$.

□

7 Elliptic curves over $\mathbf{Q}_p$

Consider the filtration of $\mathbf{Z}_p^\times$ by the principal unit groups. We prove that there is an analoguous filtration for $E(\mathbf{Q}_p)$, where E is an elliptic curve over $\mathbf{Q}_p$.

Recall that a point P of the projective space $\mathbf{P}^2_{\mathbf{Q}_p}$ is represented by (x, y, z), where x, y, z are in $\mathbf{Q}_p$ and not all zero. In fact, we can assume

$$\min\{v_p(x), v_p(y), v_p(z)\} = 0.$$

We get a reduction map

$$\begin{array}{rccc} r & : & \mathbf{P}^2_{\mathbf{Q}_p} & \longrightarrow & \mathbf{P}^2_{\mathbf{F}_p} \\ & & (x, y, z) & \longmapsto & (\overline{x}, \overline{y}, \overline{z}) \end{array}$$

where, for each a in $\mathbf{Q}_p$, we set $\overline{a} = a \mod p$.

Now we want to define the reduction of an elliptic curve modulo p. But several equations can define the same elliptic curve: if

$$y^2 = x^3 + Ax + B \tag{7.1}$$

is the affine Weierstrass equation of E, the substitution $x \mapsto u^2 x$, $y \mapsto u^3 y$ gives the equation

$$y^2 = x^3 + (A/u^4)x + (B/u^6) \tag{7.2}$$

which defines the same curve. If here A, B are in $\mathbf{Z}_p$ and $v_p(u) < 0$, then equation (7.2) modulo p becomes $y^2 = x^3$ whereas equation (7.1) modulo p may be $y^2 = x^3 + \overline{A}x + \overline{B}$, with $\overline{A}, \overline{B} \neq 0$.

Recall that the discriminant of the elliptic curve defined by the Weierstrass equation $Y^2Z = X^3 + AXZ^2 + BZ^3$ is given by

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

Definition 7.1. Let $Y^2Z = X^3 + AXZ^2 + BZ^3$ be an equation for an elliptic curve E for which $v_p(\Delta)$ is minimal and A, B lie in $\mathbf{Z}_p$. We define $\overline{E}$ as the elliptic curve over $\mathbf{F}_p$ defined by the equation

$$Y^2Z = X^3 + \overline{A}XZ^2 + \overline{B}Z^3,$$

where $\overline{A} = A \mod p$ and $\overline{B} = B \mod p$.

We say that E has

- *good reduction* if $\overline{E}$ is smooth (that is, if $v_p(\Delta) = 0$);
- *bad reduction* otherwise.

Note that bad reduction may happen, e.g. for $A = B = p$.

In the case of bad reduction, how does $\overline{E}$ look like?
For this we consider a cubic projective plane curve $\overline{E}$ over an algebraically closed field k, with equation $Y^2Z = X^3 + AXZ^2 + BZ^3$ and $\Delta = 0$.

Lemma 7.2. The curve $\overline{E}$ has exactly one singular point.

Proof. Recall that $(0, 1, 0)$ is a smooth point. So we may consider the affine curve given by the equation $y^2 = x^3 + Ax + B$ and we know that a point $P = (a, b)$ is not smooth if and only if $b = 0$ and a is a multiple root of $x^3 + Ax + B$. But this polynomial has at most one multiple root (so it has exactly one multiple root), hence $\overline{E}$ has exactly one singular point. □

So suppose $P = (a, 0)$ is the singular point of $\overline{E}$. Transform it to $(0, 0)$ by the substitution $x \mapsto x - a$, $y \mapsto y$. The equation becomes

$$y^2 = (x + a)^3 + A(x + a) + B = x^3 + 3ax^2 + (3a^2 + A)x + a^2 + aA + B.$$

But $(0,0)$ is on the curve and ∂_X vanishes at $(0,0)$. Therefore $\begin{cases} a^3 + aA + B = 0 \\ 3a^2 + A = 0 \end{cases}$

Hence $y^2 = x^3 + 3ax^2$. Now there are two cases

(a) $a = 0$ (that is, $A = 0$), so we get $y^2 = x^3$ and $\overline{E}$ has a cusp.

(b) $a \neq 0$ (that is, $A \neq 0$), so $y^2 = x^3 + 3ax^2$ and $\overline{E}$ has a node (double point) with two half-tangents $y \pm \sqrt{-3a}\, x = 0$.

Note that if $y = cx$ is a line through the point $(0,0)$ of $\overline{E}$, it meets $\overline{E}$ in at most one other point. Indeed,it does not pass through $(0,1,0)$ and

$$(cx)^2 = x^3 + 3ax^2 \iff x = 0 \text{ or } x = -3a + c^2.$$

So if P, Q are points of $\overline{E}$ different from $(0,0,1)$, the projective line $\overline{PQ}$ does not pass through $(0,0,1)$, so we can define $P \oplus Q$ as in the case of elliptic curves.

Proposition 7.3. The map $(P,Q) \mapsto P \oplus Q$ gives $\overline{E} \setminus \{(0,0,1)\}$ the structure of an abelian group isomorphic to k^+ in case (a) and to $k^\times$ in case (b).

(Here we assume the singular point has been transformed to the origin as above.)

Proof. We shall prove in both cases that there exists a bijection $\overline{E} \setminus \{(0,0,1)\} \leftrightarrow k^+$ (respectively $\overline{E} \setminus \{(0,0,1)\} \leftrightarrow k^\times$) which sends $\oplus$ to $+$ (respectively to $\cdot$). This will prove that $\overline{E} \setminus \{(0,0,1)\}$ is an abelian group.
Recall that since $O = (0,1,0)$, the operation $\oplus$ is characterized by

$$P \oplus Q \oplus R = O \iff P, Q, R \text{ are collinear.}$$

(a) The equation is $Y^2Z = X^3$. Here $Y = 0$ implies $X = 0$, so $\overline{E} \cap \{Y \neq 0\} = \overline{E} \setminus \{(0,0,1)\}$. On the (x,z)-plane, the equation becomes $z = x^3$. The map $(x,z) \mapsto x$ defines a bijection with k, indeed if $(x_1,z_1),(x_2,z_2),(x_3,z_3)$ are on the line $z = mx + b$, then x_1, x_2, x_3 are roots of $x^3 - mx - b = 0$, so $x_1 + x_2 + x_3 = 0$. Thus the bijection is additive.

(b) The equation is $Y^2Z = X^3 + 3aX^2Z$. The substitution $X \mapsto X$, $Y \mapsto Y + \sqrt{3a}X$, $Z \mapsto Z$ yields

$$(Y + \sqrt{3a}X)^2 Z = X^3 + aX^2Z,$$

so

$$Y^2 + 2\sqrt{3a}XYZ = X^3,$$

The substitution $X \mapsto (2\sqrt{3a})^2(X - Y)$, $Y \mapsto (2\sqrt{3a})^3 Y$, $Z \mapsto Z$ yields

$$(2\sqrt{3a})^6 Y^2 Z + (2\sqrt{3a})^6 (X - Y)YZ = (2\sqrt{3a})^6 (X - Y)^3,$$

that is,

$$XYZ = (X - Y)^3.$$

Thus if $Y = 0$, then $X = 0$ and we may again work in the (x,z)-plane, where we have the equation $xz = (x-1)^3$. Here if three points $(x_1,z_1),(x_2,z_2),(x_3,z_3)$ are on the line $z = mx + b$, then x_1, x_2, x_3 are roots of $x(mx + b) = (x-1)^3$, so $x_1x_2x_3 = 1$.

□

Remark 7.4. If $\overline{E}$ is defined over a subfield K of k, then $O = (0,1,0)$ lies in $\overline{E}(K)$ and if P, Q are points in $\overline{E}(K)$, so is $P \oplus Q$ (using the same argument as for elliptic curves). So $\overline{E}(K)$ is a subgroup of $\overline{E}(k)$.

In case (a), the above proof shows that $\overline{E}(K)$ is isomorphic to K^+. In case (b) it is isomorphic to $K^\times$ when $\sqrt{3a}$ lies in K; otherwise, one can show that $\overline{E}(K)$ as a group is isomorphic to

$$\{z \in K(\sqrt{3a})\colon N_{K(\sqrt{3a})|K}(z) = 1\},$$

where $N_{K(\sqrt{3a})|K}$ is the norm of the extension $K(\sqrt{3a})|K$: if x, y are in K, then

$$N_{K(\sqrt{3a})|K}(x + \sqrt{3a}y) = x^2 - 3ay^2.$$

Definition 7.5. Let E be an elliptic curve over $\mathbf{Q}_p$. If E has bad reduction, we say that E has

- *additive reduction* in case (a);
- *multiplicative reduction* in case (b).

If moreover $(\overline{E} \setminus \{(0,0,1)\})(\mathbf{F}_p)$ is isomorphic to $\mathbf{F}_p^\times$, we say that $\overline{E}$ has *split* multiplicative reduction.

Let E be an elliptic curve over $\mathbf{Q}_p$. We denote

$$E(\mathbf{Q}_p)^{(0)} \coloneqq \left\{P \in E(\mathbf{Q}_p)\colon r(P) \text{ is a smooth point in } \overline{E}(\mathbf{F}_p)\right\}.$$

If E has good reduction, then $E(\mathbf{Q}_p)^{(0)} = E(\mathbf{Q}_p)$. We also denote

$$E(\mathbf{Q}_p)^{(1)} \coloneqq \{P \in E(\mathbf{Q}_p)\colon r(P) = (0,1,0)\}.$$

Lemma 7.6. The sets $E(\mathbf{Q}_p)^{(0)}$ and $E(\mathbf{Q}_p)^{(1)}$ are subgroups of $E(\mathbf{Q}_p)$.

Proof. For $E(\mathbf{Q}_p)^{(0)}$, we only have to consider the case of E having bad reduction. Note that if P, Q, R are points of $E(\mathbf{Q}_p)^{(0)}$ on a line L, then $r(P), r(Q), r(R)$ are on the reduction $\overline{L}$ of L. If $r(P) = r(Q)$, then $\overline{L}$ is a tangent line to $\overline{E}$ at $r(P) = r(Q)$. [Idea: if $P, Q, R \neq (0,1,0)$ and L has (affine) equation $y = mx+b$, then the x-coordinates of P, Q, R are roots of $(mx+b)^2 = x^3+Ax+B$, so $(\overline{m}x + \overline{b})^2 = x^3 + \overline{A}x + \overline{B}$ will have a multiple root.]

So if P, Q are in $E(\mathbf{Q}_p)^{(0)}$, then the line through P and Q cannot reduce to a line passing through $(0,0,1)$, so $P \oplus Q \in E(\mathbf{Q}_p)^{(0)}$ as well. Then r induces a homomorphism from $E(\mathbf{Q}_p)^{(0)}$ to the smooth part of $\overline{E}(\mathbf{F}_p)$ whose kernel is exactly $E(\mathbf{Q}_p)^{(1)}$. □

Lemma 7.7. A point $P = (x, y, z)$ lies in $E(\mathbf{Q}_p)^{(1)}$ if and only if there exists a positive integer N such that

$$v_p\left(\frac{x}{y}\right) = N \quad \text{and} \quad v_p\left(\frac{z}{y}\right) = 3N.$$

Proof. Note that by definition of $E(\mathbf{Q}_p)^{(1)}$, sufficiency is immediate. For necessity, assume $\min\{v_p(x), v_p(y), v_p(z)\} = 0$. Then $r(P) = (0, 1, 0)$ if and only if $v_p(x)$ and $v_p(z)$ are both positive and $v_p(y) = 0$. Hence $v_p(y/z) < 0$ and if we choose an equation $Y^2Z = X^3 + AXZ^2 + BZ^3$ with $A, B \in \mathbf{Z}_p$, we get $v_p(x/z) < 0$, as

$$\left(\frac{y}{z}\right)^2 = \left(\frac{x}{z}\right)^3 + A\left(\frac{x}{z}\right) + B.$$

The equation also gives $3v_p(x/z) = 2v_p(y/z)$. So we may set $v_p(x/z) = -2N$ and $v_p(y/z) = -3N$ with $N > 0$. Then $v_p(z/y) = 3N$ and $v_p(x/y) = v_p(x/z) - v_p(y/z) = N$. □

Definition 7.8. For each $N \geq 1$, we set

$$E(\mathbf{Q}_p)^{(N)} \coloneqq \left\{(x, y, z) \in E(\mathbf{Q}_p)^{(1)} \colon v_p\left(\frac{x}{y}\right) \geq N\right\}.$$

Proposition 7.9. The sets $E(\mathbf{Q}_p)^{(N)}$ are subgroups of $E(\mathbf{Q}_p)$ such that

$$\bigcap_{N \geq 2} E(\mathbf{Q}_p)^{(N)} = \{(0, 1, 0)\}$$

and there is a group isomorphism

$$\frac{E(\mathbf{Q}_p)^{(N)}}{E(\mathbf{Q}_p)^{(N+1)}} \xrightarrow{\sim} \mathbf{F}_p^+.$$

Proof of Proposition 7.9. The statement on the intersection of the $E(\mathbf{Q}_p)^{(N)}$ is obvious. For the other two, let $P = (x, y, z)$ be a point in $E(\mathbf{Q}_p)^{(N)}$. By Lemma 7.7 we may assume that $v_p(x) \geq N$, $v_p(y) = 0$ and $v_p(z) = 3v_p(x)$. Consider $\widetilde{P} = (p^{-N}x, y, p^{-3N}z)$. Recall that the equation of E is $y^2z = x^3 + Axz^2 + Bz^3$, where A, B lie in $\mathbf{Z}_p$. Plugging in coordinates of $\widetilde{P}$ and correcting coefficients we get

$$p^{3N}(y^2p^{-3N}z) = p^{3N}(p^{-N}x)^3 + p^{7N}A(p^{-N}x)(p^{-3N}z)^2 + p^{9N}B(p^{-3N}z)^3.$$

Thus $\widetilde{P}$ is a point on the curve $E^{(N)}$ of equation

$$y^2z = x^3 + p^{4N}Axz^2 + p^{6N}Bz^3.$$

Therefore $r(\widetilde{P})$ lies in $\overline{E^{(N)}}(\mathbf{F}_p)$, where $\overline{E^{(N)}}$ has equation $y^2z = x^3$. Also, $r(\widetilde{P}) \neq (0, 0, 1)$ as $v_p(y) = 0$ and $r(\widetilde{P}) = (0, 1, 0)$ if and only if P lies in $E(\mathbf{Q}_p)^{(N+1)}$.

Note that the reduction $P \mapsto r(\widetilde{P})$ preserves collinearity, thus gives a map with the property $P \oplus Q \mapsto r(\widetilde{P}) \oplus r(\widetilde{Q})$. By induction on $N \geq 1$, we obtain that $\overline{E^{(N)}}(\mathbf{F}_p)$ is a subgroup and the map $P \mapsto r(\widetilde{P})$ induces a group homomorphism

$$E(\mathbf{Q}_p)^{(N)} \longrightarrow \overline{E^{(N)}}(\mathbf{F}_p) \setminus \{(0,0,1)\}$$

with kernel $E(\mathbf{Q}_p)^{(N+1)}$. Moreover, this map is surjective by Hensel's lemma (Corollary 6.11). Since $\overline{E^{(N)}}(\mathbf{F}_p) \setminus \{(0,0,1)\}$ is isomorphic to $\mathbf{F}_p^+$, we conclude. □

Corollary 7.10. The group $E(\mathbf{Q}_p)$ has a filtration

$$E(\mathbf{Q}_p) \supseteq E(\mathbf{Q}_p)^{(0)} \supseteq E(\mathbf{Q}_p)^{(1)} \supseteq E(\mathbf{Q}_p)^{(2)} \supseteq \dots$$

whose successive quotients are isomorphic to $\mathbf{F}_p^+$ from $E(\mathbf{Q}_p)^{(1)}/E(\mathbf{Q}_p)^{(2)}$ on and $E(\mathbf{Q}_p)^{(0)}/E(\mathbf{Q}_p)^{(1)}$ is isomorphic to the group of smooth $\mathbf{F}_p$-points on $\overline{E}$, hence is finite.

Remark 7.11. The quotient $E(\mathbf{Q}_p)/E(\mathbf{Q}_p)^{(1)}$ is also finite (and trivial in case of good reduction). Indeed, the projective space $\mathbf{P}^2_{\mathbf{Q}_p}$ has the quotient topology from $\mathbf{Q}_p^3 \setminus \{(0,0,0)\}$, which is compact because it can be covered by the compact sets $\mathbf{Z}_p^\times \times \mathbf{Z}_p \times \mathbf{Z}_p$, $\mathbf{Z}_p \times \mathbf{Z}_p^\times \times \mathbf{Z}_p$ and $\mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_p^\times$. Hence $E(\mathbf{Q}_p)$ is compact because it is closed in $\mathbf{P}^2_{\mathbf{Q}_p}$. Moreover, $E(\mathbf{Q}_p)^{(0)}$ is open in $E(\mathbf{Q}_p)$ because if P is in $E(\mathbf{Q}_p)^{(0)}$ with $r(P) = \overline{P}$ and Q is close to P in the p-adic topology, then $r(Q) = \overline{P}$ and so Q lies in $E(\mathbf{Q}_p)^{(0)}$. The conclusion follows from the fact that in a compact topological group every open subgroup is of finite index.

Corollary 7.12. If $(m,p) = 1$, then $E(\mathbf{Q}_p)^{(1)}$ is uniquely m-divisible.

Proof. For injectivity, suppose there exists P in $E(\mathbf{Q}_p)^{(1)} \setminus \{O\}$ such that $mP = O$. Let N be the integer (given by Proposition 7.9) such that P belongs to $E(\mathbf{Q}_p)^{(N)} \setminus E(\mathbf{Q}_p)^{(N+1)}$. If $\overline{P} \coloneqq P \mod E(\mathbf{Q}_p)^{(N+1)}$, then $\overline{P} \neq O$ and $m\overline{P} \neq O$ because the quotient $E(\mathbf{Q}_p)^{(N)}/E(\mathbf{Q}_p)^{(N+1)}$ is isomorphic to $\mathbf{F}_p^+$. Contradiction.

For surjectivity, if P is a point in $E(\mathbf{Q}_p)^{(1)}$, then there exists Q_1 in $E(\mathbf{Q}_p)^{(1)}$ such that $P = mQ_1 \mod E(\mathbf{Q}_p)^{(2)}$, because the quotient $E(\mathbf{Q}_p)^{(N)}/E(\mathbf{Q}_p)^{(N+1)}$ is isomorphic to $\mathbf{F}_p^+$, which is m-divisible. Repeating the argument, we get Q_2 in $E(\mathbf{Q}_p)^{(2)}$ such that $P - mQ_1 = mQ_2 \mod E(\mathbf{Q}_p)^{(3)}$ and, for each $i \geq 1$, we get inductively Q_i in $E(\mathbf{Q}_p)^{(i)}$ such that $P - m\sum_{j=1}^{i} Q_j$ lies in $E(\mathbf{Q}_p)^{(i+1)}$. The following lemma implies that $\sum_{j=1}^{i} Q_j$ converges to a point Q of $E(\mathbf{Q}_p)^{(1)}$, which then satisfies $P = mQ$. □

Lemma 7.13. Let G be a compact topological group and let $\{U^i\}_{i\geq 1}$ be a family of open normal subgroups of G such that $\bigcap_{i\geq 1} U^i = \{1\}$. If $(g_i)_{i\geq 1}$ is a sequence in G such that $g_i g_{i+1}^{-1}$ belongs to U^{i+1} for all i, then there exists an element g in G such that g_i converges to g (i.e. $g g_i^{-1}$ belongs to U^{i+1} for all i).

Proof. Set $\overline{g_i} \coloneqq g_i \mod U^{i+1}$. Then $g \coloneqq (\overline{g_i})_{i\geq 1}$ belongs to $\widehat{G} \coloneqq \varprojlim G/U^{i+1}$. Let $\rho\colon G \to \widehat{G}$ be the natural map. Since $\bigcap_{i\geq 1} U^i$ is trivial, this map is injective and its image $\rho(G)$ is a closed subgroup of $\widehat{G}$ because G is compact. But in $\widehat{G}$ the sequence $(\rho(g_i))_{i\geq 1} \subset \rho(G)$ converges to g, thus g lies in $\rho(G)$. □

Remark 7.14. If $K|\mathbf{Q}_p$ is a finite extension, then v_p extends uniquely to a discrete valuation v_K on K. The ring $\mathcal{O}_K \coloneqq \{a \in K\colon v_K(a) \geq 0\}$ is a discrete valuation ring with maximal ideal generated by an element π and the quotient $\mathcal{O}_K/(\pi)$ is isomorphic to $\mathbf{F}_{p^r}$ for some positive integer r. All the above statements hold more generally for K in place of $\mathbf{Q}_p$ with the same proofs if one substitutes v_p with v_K, p with π and $\mathbf{F}_p$ with $\mathbf{F}_{p^r}$.

To motivate the next considerations, we return to the case of the multiplicative group of $\mathbf{Q}_p$.

Proposition 7.15. In $\mathbf{Q}_p^\times$, we have

$$U^{(1)} \cong \begin{cases} \mathbf{Z}_p & \text{if } p > 2 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}_2 & \text{if } p = 2 \end{cases}$$

Before showing this, we define the power series

$$\log(1+x) = \sum_{i\geq 1} (-1)^{i-1} \frac{x^i}{i}$$

and we prove the following lemma.

Lemma 7.16. The power series $\log(1+x)$ converges for x in $U^{(1)}$. Moreover, if $n > 1/(p-1)$, then $1 + x \in U^{(n)}$ if and only if $\log(1+x) \in p^n\mathbf{Z}_p$.

Recall that, if $(a_i)_{i\geq 1}$ is a sequence in $\mathbf{Q}_p$, then the series $\sum_{i\geq 1} a_i$ converges in $\mathbf{Q}_p$ if and only if $v_p(a_i) \to \infty$ as $i \to \infty$.

Proof of Lemma 7.16. Let x be an element in $U^{(1)}$ and set $C \coloneqq p^{v_p(x)} > 1$. Since $p^{v_p(m)} \leq m$ for all positive integers m, we get

$$v_p\left(\frac{x^m}{m}\right) = m\, v_p(x) - v_p(m) = m\frac{\log C}{\log p} - v_p(m) \geq m\frac{\log C}{\log p} - \frac{\log m}{\log p} = \frac{1}{\log p}\log\left(\frac{C^m}{m}\right) \to \infty$$

as $m \to \infty$. So $\log(1+x)$ is a well-defined element of $\mathbf{Q}_p$.

For the second part, we show that if x lies in $p^n\mathbf{Z}_p$ for $n > 1/(p-1)$ (so $v_p(x) \geq n > 1/(p-1)$), then $v_p(\log(1+x)) = v_p(x)$. In particular, for $n > 1/(p-1)$ this means that $1+x$ lies in $U^{(n)}$ if and only if $\log(1+x)$ lies in $p^n\mathbf{Z}_p$. Notice that

$$v_p\left(\frac{x^m}{m}\right) - v_p(x) = (m-1)v_p(x) - v_p(m) > (m-1)\left(\frac{1}{p-1} - \frac{v_p(m)}{m-1}\right)$$

for all $m \geq 1$, so if we prove that

$$\frac{v_p(m)}{m-1} \leq \frac{1}{p-1}$$

we conclude, because $v_p(x) = \min_{m\geq 1}\{v_p(x^m/m)\}$ and so $v_p(\log(1+x)) = v_p(x)$. Write $m = p^{v_p(m)}m_0$ for some m_0 prime to p. Then

$$\frac{v_p(m)}{m-1} \leq \frac{v_p(m)}{p^{v_p(m)}-1} = \frac{1}{p-1}\frac{v_p(m)}{p^{v_p(m)-1}+\ldots+p+1} \leq \frac{1}{p-1}$$

as $p^{v_p(m)-1}+\ldots+p+1 \geq v_p(m)$. □

Proof of Proposition 7.15. If $p > 2$, then Lemma 7.16 implies that the map

$$\log\colon U^{(1)} \longrightarrow p\mathbf{Z}_p \cong \mathbf{Z}_p$$

is well-defined. We show that in fact it is an isomorphism. We can see this by two different arguments:

1. The inverse of log is given by $\exp(x) = \sum_{i\geq 0}\frac{x^i}{i!}$ (but then one has to prove similar convergence results for exp).
2. Alternatively, by the second statement of Lemma 7.16, $\log(U^{(n)})$ is contained in $p^n\mathbf{Z}_p$, and moreover log induces an injective group homomorphism

   $$U^{(1)}/U^{(n)} \hookrightarrow p\mathbf{Z}_p/p^{n+1}\mathbf{Z}_p.$$

   Since by the results preceding Definition 6.13 these groups have the same order p^n, the induced map is an isomorphism for all $n \geq 1$ and by passing to the inverse limit we get

   $$U^{(1)} \cong \varprojlim U^{(1)}/U^{(n)} \xrightarrow{\sim} \varprojlim p\mathbf{Z}_p/p^{n+1}\mathbf{Z}_p \cong p\mathbf{Z}_p.$$

If $p = 2$, by Lemma 7.16 and by repeating the previous argument, we get $U^{(2)} \cong 2^2\mathbf{Z}_2 \cong \mathbf{Z}_2$. Therefore we conclude by observing that $U^{(1)} \cong \langle -1\rangle \times U^{(2)} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}_2$. □

We now sketch without proof an an analogue of the above result for elliptic curves.

Note first that $E(\mathbf{Q}_p)$ is a commutative p-adic Lie group (i.e. $E(\mathbf{Q}_p)$ is a p-adic analytic manifold over $\mathbf{Q}_p$, and the addition and the inverse maps are defined by polynomial, hence also p-adic analytic functions). In general, if G is an arbitrary p-adic Lie group with identity e, one defines its Lie algebra $\mathrm{Lie}(G)$ as the tangent space T_eG at e. It is a $\mathbf{Q}_p$-vector space of dimension $d = \dim G$ equipped with a Lie bracket $[\cdot,\cdot]$. When G is abelian, the Lie bracket reduces to 0. Using $[\cdot,\cdot]$ one can define on $\mathbf{Q}_p^d$ a Lie group structure $\underline{\mathrm{Lie}}(G)$ with the property $\mathrm{Lie}(\underline{\mathrm{Lie}}(G)) = \mathrm{Lie}(G)$. In case $[\cdot,\cdot] = 0$, this will just be $(\mathbf{Q}_p^+)^d$ (in general the group law will be non-commutative).

Fact 7.17. Let G be a p-adic Lie group. There exists a unique homomorphism of Lie groups

$$\log\colon G \to \underline{\mathrm{Lie}}(G)$$

inducing the identity $\mathrm{Lie}(G) \to \mathrm{Lie}(\underline{\mathrm{Lie}}(G))$ on tangents spaces at e. This map induces an isomorphism on suitable open subgroups (like in the classical case over $\mathbf{R}$ or $\mathbf{C}$).

For the proof (and further details) we refer to [1] or [4]. Note that [5] gives a detailed account of the theory in the special case of elliptic curves without using the language of Lie theory.

Example 7.18. If $G = \mathbf{Q}_p^\times$, then $\mathrm{Lie}(G) = \mathbf{Q}_p^+$ and the map log is the p-adic logarithm discussed above.
If $G = E(\mathbf{Q}_p)$, then $\mathrm{Lie}(G) \cong \mathbf{Q}_p^+$ and the map log induces isomorphisms

$$E(\mathbf{Q}_p)^{(1)} \cong \mathbf{Z}_p^+ \quad \text{if } p > 2,$$
$$E(\mathbf{Q}_p)^{(2)} \cong \mathbf{Z}_p^+ \quad \text{if } p = 2.$$

It is possible to write down an explicit power series defining log, but the formula is not as simple as in the case $G = \mathbf{Q}_p^\times$.

More generally, when A is an abelian variety of dimension g, we have

$$\mathrm{Lie}(A(\mathbf{Q}_p)) \cong (\mathbf{Q}_p^+)^g$$

and $\log\colon U \xrightarrow{\sim} \mathbf{Z}_p^g$ for some open subgroup U in $A(\mathbf{Q}_p)$ (a theorem first proved by Mattuck).

Finally, all of the above again holds more generally over finite extensions of $\mathbf{Q}_p$ but for log to converge and induce an isomorphism one needs to take smaller open subgroups.

8 Rudiments of Galois cohomology

In this section we present the basic results on Galois cohomology which will be used later. For our purpose, we only need to consider cohomology groups in degrees 0 and 1, so we shall define them "by hand", but this is part of a more general theory for which we refer to [8].

Definition 8.1. Let G be a group. A *G-module* is an abelian group A endowed with a G-action $G \times A \to A$ such that

1. $\sigma(a_1 + a_2) = \sigma(a_1) + \sigma(a_2)$ for all σ in G and a_1, a_2 in A.
2. $(\sigma\tau)(a) = \sigma(\tau(a))$ for all σ, τ in G and a in A.

Example 8.2. Let $L|K$ be a finite Galois extension with Galois group G. The following are G-modules.

1. The additive group L^+.
2. The multiplicative group $L^\times$.
3. The group $E(L)$, where $E|K$ is an elliptic curve.

Definition 8.3. Let A be a G-module. The 0-*th cohomology group* of A is

$$H^0(G,A) \coloneqq A^G = \{a \in A \colon \sigma(a) = a \text{ for all } \sigma \in G\}.$$

The *group of* 1-*cocycles* is

$$Z^1(G,A) \coloneqq \{\varphi \colon G \to A \colon \ \varphi(\sigma\tau) = \varphi(\sigma) + \sigma(\varphi(\tau)) \text{ for all } \sigma,\tau \in G\}.$$

The *group of* 1-*coboundaries* is the subgroup of $Z^1(G,A)$ defined by

$$B^1(G,A) \coloneqq \{\varphi \colon G \to A \colon \ \varphi(\sigma) = a - \sigma(a) \text{ for some } a \in A\}.$$

The *first cohomology group* of A is

$$H^1(G,A) \coloneqq Z^1(G,A)/B^1(G,A).$$

Remark 8.4. Let A be G-module.

1. If G acts trivially on A (i.e. $\sigma(a) = a$ for all σ in G and for all a in A), then $H^0(G,A) = A$ and $H^1(G,A) = \mathrm{Hom}(G,A)$.
2. $H^0(G,A)$ and $H^1(G,A)$ are *functorial* in A, i.e. every G-homomorphism $A \to B$ induces a map $H^i(G,A) \to H^i(G,B)$ for $i = 0, 1$.

Proposition 8.5 (Long exact sequence)**.** If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, then there exists an exact sequence

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C).$$

Proof. The definition of the maps in the sequence is clear except for δ. We define δ in the following way: suppose c is an element in $H^0(G,C) = C^G$. Since the map $B \to C$ is surjective, there exists a preimage b in B of c. Note that $\sigma(b)$ and b have the same image in C because $\sigma(c) = c$ implies that $b - \sigma(b)$ lies in A. One checks that the map $\sigma \mapsto b - \sigma(b)$ lies in $Z^1(G,A)$ and its class in $H^1(G,A)$ does not depend on b. We define $\delta(c)$ as this class. Checking that the sequence is exact is an easy exercise. □

Let $i \colon H \to G$ be a group homomorphism. Then every G-module becomes an H-module via i, and i induces a homomorphism

$$i^* \colon H^1(G,A) \to H^1(H,A).$$

In the special case when H is a subgroup of G, the inclusion $i \colon H \hookrightarrow G$ induces a map

$$\mathrm{Res} \colon H^1(G,A^H) \to H^1(H,A),$$

called the *restriction map*.

If H is a normal subgroup of G, then G/H acts on A^H, so the projection $G \to G/H$ induces a map

$$\mathrm{Inf} \colon H^1(G/H,A^H) \to H^1(G,A),$$

called the *inflation map*.

Lemma 8.6 (Inflation-restriction sequence)**.** If H is a normal subgroup of G, then

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A)$$

is an exact sequence.

The proof is easy and is left as exercise.

Theorem 8.7 (Hilbert's Theorem 90)**.** If $L|K$ is a finite Galois extension and $G = \text{Gal}(L|K)$, then

$$H^1(G, L^\times) = 0.$$

Before showing this, we need the following lemma.

Lemma 8.8 (Dedekind)**.** If $\sigma_1, \ldots, \sigma_n$ are the elements of G, then they are linearly independent in the L-vector space of functions $L \to L$.

Proof of Lemma 8.8. Suppose that $\sigma_1, \ldots, \sigma_n$ are linearly dependent and consider the shortest non-trivial linear combination that is zero. We may assume this is

$$a_1\sigma_1 + \ldots + a_i\sigma_i = 0 \tag{8.1}$$

for certain non-zero a_i in L. Choose x in L such that $\sigma_1(x) \neq \sigma_2(x)$. Then for every y in L we get

$$a_1\sigma_1(x)\sigma_1(y) + \ldots + a_i\sigma_i(x)\sigma_i(y) = 0. \tag{8.2}$$

Evaluating (8.1) at y and multiplying it by $\sigma_1(x)$, we get

$$a_1\sigma_1(x)\sigma_1(y) + \ldots + a_i\sigma_1(x)\sigma_i(y) = 0. \tag{8.3}$$

Subtracting (8.3) from (8.2) we get

$$a_2(\sigma_2(x) - \sigma_1(x)) \cdot \sigma_2(y) + \ldots + a_i(\sigma_i(x) - \sigma_1(x)) \cdot \sigma_i(y) = 0,$$

which holds for all y in L. This is a contradiction, as the previous sequence is non-trivial and shorter than (8.1). □

Proof of Theorem 8.7. Let φ be an element of $Z^1(G, L^\times)$. Consider the map

$$\Phi := \sum_{\sigma \in G} \varphi(\sigma)\sigma \ : G \to L^\times.$$

By Lemma 8.8 this is not identically zero, so there exist x, y in $L^\times$ such that

$$y = \Phi(x) = \sum_{\sigma \in G} \varphi(\sigma)\sigma(x).$$

Since φ lies in $Z^1(G, L^\times)$, for each τ in G we have

$$\tau(y) = \sum_{\sigma \in G} (\tau\varphi(\sigma))\tau\sigma(x) = \sum_{\sigma \in G} \frac{\varphi(\tau\sigma)}{\varphi(\tau)}\tau\sigma(x) = \frac{1}{\varphi(\tau)} \sum_{\sigma \in G} \varphi(\tau\sigma)\tau\sigma(x) = \frac{y}{\varphi(\tau)}.$$

Therefore $\varphi(\tau) = y \cdot \tau(y)^{-1}$ for all τ in G, so φ belongs to $B^1(G, L^\times)$. □

Our next goal is to extend the above theory to infinite Galois groups. If we keep the above definition of H^1, Hilbert's Theorem 90 will not necessarily hold in the infinite case, so we make a modification.

First we review infinite Galois theory. Let K be a field and let K^s be a separable closure of K. Consider the partial order on finite Galois extensions $L|K$ (which are contained in K^s) defined by

$$L_1 \leq L_2 \iff L_1 \subseteq L_2.$$

Note that if $L_1 \leq L_2$, we get a group homomorphism $\varphi_{L_1 L_2} \colon \mathrm{Gal}(L_2|K) \to \mathrm{Gal}(L_1|K)$ given by restriction of automorphisms. The Galois groups $\mathrm{Gal}(L|K)$ form a *filtered inverse system* in the following sense.

Definition 8.9. A partially ordered set $(I, \leq)$ is *filtered* if

$$\forall\, i, j \in I \;\; \exists\, k \in I \;:\; k \geq i,\, k \geq j.$$

Definition 8.10. An *inverse system* of groups indexed by I is given by

- For each i in I, a group G_i;
- For each $i \leq j$, a homomorphism $\varphi_{ij} \colon G_j \to G_i$.

The *inverse limit* of the system is

$$\varprojlim G_i \coloneqq \left\{ (g_i) \in \prod_{i \in I} G_i \colon \;\; \varphi_{ij}(g_j) = g_i \text{ for all } i \leq j \right\}.$$

The dual notion of inverse limit is that of *direct limit*:

Definition 8.11. Let $(I, \leq)$ be a filtered set. A *direct system* of abelian groups is given by

- For each i in I, an abelian group A_i;
- For each $i \leq j$, a homomorphism $\varphi_{ij} \colon A_i \to A_j$.

The *direct limit* of the system is

$$\varinjlim A_i \coloneqq \left(\bigoplus_{i \in I} A_i \right) \Big/ \left\{ (0, \ldots, 0, a_i, 0, \ldots, 0, a_j, 0, \ldots) \colon \ \varphi_{ij}(a_i) = -a_j \right\}.$$

Proposition 8.12. In the above example, the Galois groups form a filtered inverse system whose inverse limit is $\mathrm{Gal}(K^s|K)$.

Proof. The fact that the Galois groups form a filtered inverse system is immediate. Now consider the map

$$\begin{array}{rccc} \Phi & : & \mathrm{Gal}(K^s|K) & \longrightarrow & \varprojlim_L \mathrm{Gal}(L|K) \\ & & \sigma & \longmapsto & \left(\sigma|_L \right)_L. \end{array}$$

This map is surjective: given $(\sigma_L)_L$ in $\varprojlim_L \mathrm{Gal}(L|K)$, one can glue them together to an element σ in $\mathrm{Gal}(K^s|K)$. More precisely, if x is an element in K^s, then there exists a finite Galois extension $L|K$ such that x lies in L. Define $\sigma(x) = \sigma_L(x)$. This definition is unambiguous because of the compatibility of the σ_L in the inverse system. Then $\Phi(\sigma) = (\sigma_L)_L$.

The map Φ is also injective, as if σ is an element in $\mathrm{Gal}(K^s|K) \setminus \{\mathrm{id}_{K^s}\}$, then there exists an element x in $K^s \setminus K$ such that $\sigma(x) \neq x$. If x lies in an extension L as above, then $\sigma|_L(x) \neq x$ and so $\sigma|_L \neq \mathrm{id}_L$. □

Remark 8.13. If we put the discrete topology on $\mathrm{Gal}(L|K)$ and then the product topology on $\prod_L \mathrm{Gal}(L|K)$, one shows easily that the subgroup $\varprojlim \mathrm{Gal}(L|K)$ of $\prod_L \mathrm{Gal}(L|K)$ – endowed with the induced topology – is closed. Since finite discrete groups are compact and the product of compact spaces is also compact, we get that $\varprojlim \mathrm{Gal}(L|K)$ is compact. It is also totally disconnected, i.e. its only connected subsets are one-point sets. A topological group is called *profinite* if it is an inverse limit of finite discrete groups. It can be shown that every compact totally disconnected group is profinite.

The above considerations extend without change to arbitrary infinite Galois extensions of K in place of K^s but for the definition to follow we only need the case of K_s

Let now $G \coloneqq \mathrm{Gal}(K^s|K)$ and let A be a G-module such that the stabilizer of every a in A is open (hence of finite index by compactness of G). One can show that this is equivalent to saying that the action $G \times A \to A$ is continuous if A carries the discrete topology.

Note that open subgroups H of G are exactly the subgroups fixing a finite extension $L|K$ contained in K^s. Indeed, when H is normal, then G/H must be one of the $\mathrm{Gal}(L|K)$ in the inverse system. In the general case choose an open normal subgroup $H' \subset H$ and apply finite Galois theory.

If $L|K$ is a finite Galois extension, by the above it corresponds to an open subgroup $H \coloneqq \mathrm{Gal}(K^s|L)$ of G. If $L_1 \leq L_2$, then $H_2 \leq H_1$ and we have an inflation map

$$\mathrm{Inf}\colon H^1(G/H_1, A^{H_1}) \to H^1(G/H_2, A^{H_2}).$$

In this way, the groups $H^1(G/H, A^H)$ form a filtered direct system. Thus we can define

$$H^1(G, A) \coloneqq \varinjlim_H H^1(G/H, A^H).$$

We make the convention that whenever G is profinite, the group $H^1(G, A)$ is to be understood in the above sense and not as mere group cohomology.

Also, we define

$$H^0(G, A) \coloneqq A^G.$$

Notation. For $i = 0, 1$, we define the *Galois cohomology groups* of K as

$$H^i(K, A) \coloneqq H^i(\mathrm{Gal}(K^s|K), A).$$

Hilbert's Theorem 90 (Theorem 8.7) then immediately extends to the infinite case as follows.

Corollary 8.14. With the previous notation, we have

$$H^1(K, (K^s)^\times) = 0.$$

To extend exact sequences from group cohomology to Galois cohomology we need the following lemma.

Lemma 8.15. Let $(I, \leq)$ be a filtered set and let $(A_i), (B_i), (C_i)$ be direct systems indexed by I. Suppose that for each i in I there is an exact sequence

$$0 \to A_i \to B_i \to C_i \to 0$$

such that for each $i \leq j$ the following diagram commutes.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_i & \longrightarrow & B_i & \longrightarrow & C_i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_{ij}^A} & & \downarrow{\scriptstyle \varphi_{ij}^B} & & \downarrow{\scriptstyle \varphi_{ij}^C} & & \\ 0 & \longrightarrow & A_j & \longrightarrow & B_j & \longrightarrow & C_j & \longrightarrow & 0 \end{array}$$

Then the sequence

$$0 \to \varinjlim A_i \to \varinjlim B_i \to \varinjlim C_i \to 0$$

is exact.

The proof follows directly from the definitions and is left as an exercise.

Corollary 8.16. The long exact sequence (Proposition 8.5) and the inflation-restriction sequence (Lemma 8.6) hold in Galois cohomology too.

Here in the inflation-restriction sequence one has to assume that the subgroup H of G is closed.

We arrive at the main application of the above constructions.

Proposition 8.17 (Kummer theory)**.** Let K be a field, let n be a positive integer such that $(n, \mathrm{char}(K)) = 1$ and let μ_n be the subgroup of K^s consisting of the n-th roots of unity. There is a group isomorphism

$$K^\times/K^{\times n} \xrightarrow{\sim} H^1(K, \mu_n).$$

Proof. Consider the exact sequence of $\mathrm{Gal}(K^s|K)$-modules

$$1 \to \mu_n \to (K^s)^\times \xrightarrow{\times n} (K^s)^\times \to 1. \tag{8.4}$$

Part of the long exact sequence is

$$\big((K^s)^\times\big)^G \xrightarrow{\wedge n} \big((K^s)^\times\big)^G \to H^1(K, \mu_n) \to H^1\big(K, (K^s)^\times\big),$$

but the last group is trivial by Theorem 8.7 and $\big((K^s)^\times\big)^G = K^\times$, thus we conclude. □

Note that in exact sequence (8.4) the last map is surjective because K^s is separably closed and hence every element has an n-th root. One could not write a similar exact sequence for finite extensions of K.

Remark 8.18. When $\mu_n \subset K$, we have $\mu_n \cong \mathbf{Z}/n\mathbf{Z}$ as $\mathrm{Gal}(K^s|K)$-modules and hence

$$H^1(K, \mu_n) \cong \mathrm{Hom}(\mathrm{Gal}(K^s|K), \mathbf{Z}/n\mathbf{Z}).$$

Following the construction of the map δ in Proposition 8.5 one deduces that under the assumption $\mu_n \subset K$ every Galois extension of K with group $\mathbf{Z}/n\mathbf{Z}$ is of the form $K(\sqrt[n]{a})$ for some $a \in K^\times$. (This is the classical form of Kummer theory.)

Remark 8.19. We can now also fill in a small gap in a previous proof. Assume K is perfect with algebraic closure $\overline{K}$ and $G = \mathrm{Gal}(\overline{K}|K)$. Let C be a plane curve defined over K with function field $\overline{K}(C)$ over $\overline{K}$. The short exact sequence

$$1 \to \overline{K}^\times \to \overline{K}(C)^\times \to \overline{K}(C)^\times/\overline{K}^\times \to 1$$

induces an exact sequence

$$(\overline{K}(C)^\times)^G \to (\overline{K}(C)^\times/\overline{K}^\times)^G \to H^1(K, \overline{K}^\times)$$

where the last term is 0 by Corollary 8.14. Thus the map $(\overline{K}(C)^\times)^G \to (\overline{K}(C)^\times/\overline{K}^\times)^G$ is surjective.

9 The weak Mordell-Weil theorem for elliptic curves

The aim of this section and the next is to prove the following result, which is due to Mordell in the case $K = \mathbf{Q}$ and to Weil in the general case.

Theorem 9.1 (Mordell-Weil Theorem)**.** Let $K|\mathbf{Q}$ be a finite extension an let $E|K$ be an elliptic curve. Then $E(K)$ is a finitely generated abelian group.

Remark 9.2. Theorem 9.1 holds more generally for an abelian variety $A|K$ (as proven by Weil).

The first step towards the proof is:

Theorem 9.3 (Weak Mordell-Weil Theorem)**.** Let $K|\mathbf{Q}$ be a finite extension an let $E|K$ be an elliptic curve. If $m > 1$ is an integer, then the quotient group $E(K)/mE(K)$ is finite.

Remark 9.4.

1. Mordell proved Theorem 9.3 only for $m = 2$, which, as we shall see, is enough for deducing Theorem 9.1.
2. Even in the case $K = \mathbf{Q}$, the proof passes through some finite extension $L|\mathbf{Q}$ (except for $m = 2$ if moreover the torsion points of order 2 are contained in $E(\mathbf{Q})$).

We now start the proof of theorem 9.3.

Recall that, if $E|K$ is an elliptic and $\overline{K}$ is a fixed algebraic closure of K, we denote by $E[m]$ the set of points of $E(\overline{K})$ of order dividing m. For any extension $L|K$ in $\overline{K}$, we set $E[m](L) = E[m] \cap E(L)$.

Lemma 9.5. Let k be an algebraically closed field and let $E|k$ be an elliptic curve. The map $m\colon P \mapsto mP$ is surjective with finite kernel.

Sketch of proof. The map m is defined by polynomial functions, so it is a morphism in the sense of algebraic geometry. Since E is a projective variety, the image mE is Zariski closed in E. Since E is connected, the image mE is either E or a point. But mE cannot be a point: to see this, it is enough to consider the case where m is prime p. If $p \neq 2$, we have seen that there exist three points of order 2 which cannot be killed by p; if $p = 2$, one can for instance check that there exist points of order 3.
Finally, since $m\colon P \mapsto mP$ is a non-constant morphism, its kernel $E[m]$ is a proper closed subset of E, thus it is finite. □

Remark 9.6. When $k = \mathbf{C}$, by Corollary 4.8 we have

$$E[m] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \tag{9.1}$$

as an abelian group. In fact, this also implies the case of algebraically closed fields of characteristic zero (see [2]). Note that we already know this result for $m = 2$ (and this is sufficient for the full Mordell-Weil theorem, as mentioned in Remark 9.4 (1)). Anyway, in case one wants to avoid the use of the above result, it is sufficient to know that

$$E[m] \cong \mathbf{Z}/m_1\mathbf{Z} \times \ldots \times \mathbf{Z}/m_r\mathbf{Z} \tag{9.2}$$

as an abelian group by Lemma 9.5, and then the proof of Theorem 9.3 will go through with minimal modifications.

Now let $K|\mathbf{Q}$ be a finite extension and let $E|K$ be an elliptic curve. Denote by $\overline{K}$ a fixed algebraic closure of K. Lemma 9.5 implies the existence of an exact sequence

$$0 \to E[m](\overline{K}) \to E(\overline{K}) \xrightarrow{m} E(\overline{K}) \to 0.$$

Note that, if $G = \mathrm{Gal}(\overline{K}|K)$, this is an exact sequence of G-modules. Thus it induces a long exact sequence, part of which is given by

$$\begin{array}{ccccccccc} E(\overline{K})^G & \xrightarrow{m} & E(\overline{K})^G & \longrightarrow & H^1(K, E[m](\overline{K})) & \longrightarrow & H^1(K, E(\overline{K})) & \xrightarrow{m} & H^1(K, E(\overline{K})) \\ \| & & \| & & & & & & \\ E(K) & & E(K) & & & & & & \end{array}$$

Therefore there is an exact sequence

$$0 \to E(K)/mE(K) \to H^1(K, E[m](\overline{K})) \to H^1(K, E(\overline{K}))[m] \to 0.$$

Here $H^1(K, E[m](\overline{K}))$ is infinite, but we will prove that it has a finite subgroup containing $E(K)/mE(K)$ (and this will prove Theorem 9.3). To define this subgroup, we use arithmetic considerations.

We start with the case $K = \mathbf{Q}$. For every prime p, fix an algebraic closure $\overline{\mathbf{Q}_p}$ of $\mathbf{Q}_p$ and let $\overline{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{Q}_p$. Then we have a diagram of embeddings

$$\begin{array}{ccc} \mathbf{Q} & \hookrightarrow & \mathbf{Q}_p \\ \downarrow & & \downarrow \\ \overline{\mathbf{Q}} & \hookrightarrow & \overline{\mathbf{Q}_p} \end{array}$$

whence a restriction map

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbf{Q}_p}|\mathbf{Q}_p) & \longrightarrow & \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \\ \sigma & \longmapsto & \sigma|_{\overline{\mathbf{Q}}} \end{array}$$

Therefore, there exists an induced map $H^1(\mathbf{Q}, A) \to H^1(\mathbf{Q}_p, A)$ for any $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-module A. Similarly, the immersion $\mathbf{Q} \hookrightarrow \mathbf{R}$ induces a map $H^1(\mathbf{Q}, A) \to H^1(\mathbf{R}, A)$ for any $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-module A, where this time $\overline{\mathbf{Q}}$ is the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$.

Now we generalize this to the case of a finite extension $K|\mathbf{Q}$. Let $\mathcal{O}_K$ be the integral closure of $\mathbf{Z}$ in K. For each non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, the localization $O_{K,\mathfrak{p}}$ of $\mathcal{O}_K$ at $\mathfrak{p}$ is a discrete

valuation ring with fraction field K. Denote by $v_{\mathfrak{p}}\colon K^\times \to \mathbf{Z}$ the associated discrete valuation. We define

$$\widehat{\mathcal{O}}_{K,\mathfrak{p}} \coloneqq \varprojlim \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^i\mathcal{O}_{K,\mathfrak{p}}$$
$$K_{\mathfrak{p}} \coloneqq \mathrm{Frac}(\widehat{\mathcal{O}}_{K,\mathfrak{p}}).$$

In particular, there exists an embedding $K \hookrightarrow K_{\mathfrak{p}}$ which induces a restriction map

$$\mathrm{Res}\colon H^1(K,A) \to H^1(K_{\mathfrak{p}},A)$$

for all $\mathrm{Gal}(\overline{K}|K)$-modules A after fixing algebraic closures as in the special case above. Also, every embedding $K \hookrightarrow \mathbf{R}$ induces $H^1(K,A) \to H^1(\mathbf{R},A)$ for all $\mathrm{Gal}(\overline{K}|K)$-modules A. (Note that in general there may be no embeddings $K \hookrightarrow \mathbf{R}$, or several of them).

We have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(K,E[m]) & \longrightarrow & H^1(K,E)[m] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \prod_{\mathfrak{p}} \mathrm{Res}} & & \downarrow{\scriptstyle \prod_{\mathfrak{p}} \mathrm{Res}} & & \\
0 & \longrightarrow & \prod_{\mathfrak{p}} E(K_{\mathfrak{p}})/mE(K_{\mathfrak{p}}) & \longrightarrow & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}},E[m]) & \longrightarrow & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}},E)[m] & \longrightarrow & 0
\end{array}$$

where in the products $\mathfrak{p}$ runs over all non-zero prime ideals in $\mathcal{O}_K$ and, with a slight abuse of notation, over all embeddings $K \hookrightarrow \mathbf{R}$ (when they exist).

Definition 9.7. Let $m > 1$ be an integer. The *m-Selmer group* of E is

$$\mathrm{Sel}^{(m)}(E) \coloneqq \ker\left(H^1(K,E[m]) \to \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}},E)\right).$$

The *Tate-Shafarevich group* of E is

$$Ш(E) \coloneqq \ker\left(H^1(K,E) \to \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}},E)\right).$$

We get the following exact sequence:

$$0 \to E(K)/mE(K) \to \mathrm{Sel}^{(m)}(E) \to Ш(E)[m] \to 0. \tag{9.3}$$

Remark 9.8. The exact sequence (9.3) exists more generally for abelian varieties or even commutative algebraic groups.

We shall now prove:

Theorem 9.9. For every integer $m > 1$, the group $\mathrm{Sel}^{(m)}(E)$ is finite.

As a direct consequence, we obtain Theorem 9.3:

Corollary 9.10. For every integer $m > 1$, the groups $E(K)/mE(K)$ and $Ш(E)[m]$ are finite.

In fact, there is the following famous conjecture.

Conjecture 9.11. The Tate-Shafarevich group $Ш(E)$ is finite.

The conjecture is known in some cases but open in general. We shall return to this point when discussing the Birch–Swinnerton-Dyer conjecture.

Idea of proof of Theorem 9.9. Suppose that $E[m]$ is contained in $E(K)$ and that K contains the group μ_m of the m-th roots of unities. Set $G = \mathrm{Gal}(\overline{K}|K)$. Using (9.1) and the fact that, by assumption, G acts trivially on $E[m]$, we get

$$\begin{aligned} H^1(K, E[m]) &\cong H^1\left(K, (\mathbf{Z}/m\mathbf{Z})^2\right) = \mathrm{Hom}(G, (\mathbf{Z}/m\mathbf{Z})^2) \cong \mathrm{Hom}(G, \mathbf{Z}/m\mathbf{Z})^2 \\ &\cong \left(H^1(G, \mathbf{Z}/m\mathbf{Z})\right)^2 \cong \left(H^1(K, \mu_m)\right)^2 \cong \left(K^\times/K^{\times m}\right)^2, \end{aligned}$$

where the last isomorphism follows from Proposition 8.17. In particular, we can identify $\mathrm{Sel}^{(m)}$ with a subgroup of $(K^\times/K^{\times m})^2$, so the main idea is to translate the problem in terms of algebraic number fields, forgetting about elliptic curves. (If one does not want to use (9.1), the previous isomorphism can be modified using (9.2), obtaining that $H^1(K, E[m])$ is isomorphic to $\bigoplus_{i=1}^r K^\times/K^{\times m_i}$.)

To reduce to the case discussed above we use the following lemma.

Lemma 9.12. If $L|K$ is a finite extension, then the map

$$\mathrm{Res}\colon H^1(K, E[m]) \to H^1(L, E[m])$$

has finite kernel.

Proof. Let $H = \mathrm{Gal}(L|K)$. By the inflation-restriction sequence, there is an exact sequence

$$0 \to H^1(H, E[m](L)) \xrightarrow{\mathrm{Inf}} H^1(K, E[m]) \xrightarrow{\mathrm{Res}} H^1(L, E[m]).$$

But $H^1(H, E[m](L))$ is finite because both H and $E[m](L)$ are finite, so there are finitely many maps between them. □

As consequence, denoting by $\mathrm{Sel}^{(m)}(E_L)$ the m-Selmer group of E considered as an elliptic curve defined over L, we get the following result.

Corollary 9.13. The map $\mathrm{Sel}^{(m)}(E) \to \mathrm{Sel}^{(m)}(E_L)$ has finite kernel.

Thus to prove Theorem 9.9, we may replace K by a finite extension. So we can assume that K is so large that $E[m](\overline{K})$ is contained in $E(K)$ and that K contains μ_m. In other words, we are in the situation discussed before Lemma 9.12.

Proposition 9.14. There exists a finite set S consisting of nonzero prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ and all the embeddings $K \hookrightarrow \mathbf{R}$ such that the image of $\mathrm{Sel}^{(m)}(E)$ via the isomorphism $H^1(K, E[m]) \xrightarrow{\sim} (K^\times/K^{\times m})^2$ is contained in

$$\left(\left\{x \in K^\times \colon\ v_\mathfrak{p}(x) \equiv 0 \pmod{m} \text{ for all } \mathfrak{p} \notin S\right\}/K^{\times m}\right)^2.$$

In this way the proof of Theorem 9.9 reduces to a purely number-theoretic problem.

To show Proposition 9.14, we need some preliminaries. First we recall that a finite extension $L_\mathfrak{p}|K_\mathfrak{p}$ is *unramified* if the unique extension $v_{L_\mathfrak{p}}$ of $v_\mathfrak{p}$ to $L_\mathfrak{p}$ has values in $\mathbf{Z}$ (and not $\frac{1}{r}\mathbf{Z}$ for some $r > 1$). In other words, if π is an element of $K_\mathfrak{p}$ such that $v_\mathfrak{p}(\pi) = 1$, then $v_{L_\mathfrak{p}}(\pi) = 1$. Now we recall the following fact from algebraic number theory.

Fact 9.15. For every integer $n \geq 1$, there is a unique unramified extension $L_\mathfrak{p}|K_\mathfrak{p}$ of degree n.

(We briefly recall the construction of $L_\mathfrak{p}$: If $\mathbf{F}_q$ is the residue field of $K_\mathfrak{p}$, let α be in $\overline{\mathbf{F}_q}$ such that $\mathbf{F}_{q^n} = \mathbf{F}_q[\alpha]$. If $f(X)$ is the minimal polynomial of α over $\mathbf{F}_q$, consider a monic lift $\widetilde{f}(X)$ of $f(X)$ in $\mathcal{O}_{K_\mathfrak{p}}[X]$ (where $\mathcal{O}_{K_\mathfrak{p}}$ is the valuation ring of $K_\mathfrak{p}$) and define $L_\mathfrak{p} = K_\mathfrak{p}[X]/(\widetilde{f})$.)

Lemma 9.16. Let $E|K_\mathfrak{p}$ be an elliptic curve having good reduction and let m be an integer prime to p. If Q is a point in $E(K_\mathfrak{p})$, then there exists a finite unramified extension $L_\mathfrak{p}|K_\mathfrak{p}$ and a point P in $E(L_\mathfrak{p})$ such that $mP = Q$.

Proof. With notation as at the beginning of Section 7, set $\overline{Q} \coloneqq r(Q) \in \overline{E}(\mathbf{F}_q)$. By Lemma 9.5 there exists $\widetilde{\overline{Q}}$ in $\overline{E}(\overline{\mathbf{F}_q})$ such that $m\widetilde{\overline{Q}} = \overline{Q}$. Let n be an integer such that $\widetilde{\overline{Q}}$ lies in $\overline{E}(\mathbf{F}_{q^n})$ and let $L_\mathfrak{p}$ be the degree n unramified extension of $K_\mathfrak{p}$. By Hensel's lemma (more precisely, by Corollary 6.11), we can lift $\widetilde{\overline{Q}}$ to $\widetilde{Q}$ in $E(L_\mathfrak{p})$. Note that in $\overline{E}(\mathbf{F}_q)$ we have $r(m\widetilde{Q}) = r(Q)$. Hence

$$Q - m\widetilde{Q} \in \ker\left(r \colon E(K_\mathfrak{p}) \to \overline{E}(\mathbf{F}_q)\right) = E(K_\mathfrak{p})^{(1)}.$$

But by Corollary 7.12 (and Remark 7.14, as $(m, p) = 1$ implies $(m, \mathfrak{p}) = 1$) we know that $E(K_\mathfrak{p})^{(1)}$ is (uniquely) m-divisible, so there exists Q' in $E(K_\mathfrak{p})^{(1)}$ such that $mQ' = Q - m\widetilde{Q}$. Setting $P = Q' + \widetilde{Q} \in E(L_\mathfrak{p})$, we conclude $mP = m(Q' + \widetilde{Q}) = Q$. □

Proof of Proposition 9.14. Let $S = S_1 \cup S_2 \cup S_3$, where S_1 is the set of all non-zero primes ideals $\mathfrak{p}$ of $\mathcal{O}_K$ such that E has bad reduction modulo $\mathfrak{p}$, S_2 is the set of all non-zero primes $\mathfrak{p}$ dividing (m) and S_3 is the set of all embeddings $K \hookrightarrow \mathbf{R}$. Let α be an element in $\mathrm{Sel}^{(m)}(E)$ with image $\alpha_\mathfrak{p}$

in $H^1(K_\mathfrak{p}, E[m])$ for $\mathfrak{p} \notin S$. Since $\alpha_\mathfrak{p}$ maps to zero in $H^1(K, E)$, it comes from an element $\beta_\mathfrak{p}$ in the quotient $E(K_\mathfrak{p})/mE(K_\mathfrak{p})$. Now $\beta_\mathfrak{p}$ is represented by a point Q in $E(K_\mathfrak{p})$. Using that $\mathfrak{p} \notin S$, we may apply Lemma 9.16 to get a finite unramified extension $L_\mathfrak{p}|K_\mathfrak{p}$ such that Q is m-divisible in $E(L_\mathfrak{p})$. Therefore $\beta_\mathfrak{p}$ maps to zero in $E(L_\mathfrak{p})/mE(L_\mathfrak{p})$, thus $\alpha_\mathfrak{p}$ maps to zero in $H^1(L_\mathfrak{p}, E[m])$.

$$\begin{array}{ccccc} \beta_\mathfrak{p} & & E(K_\mathfrak{p})/mE(K_\mathfrak{p}) & \longrightarrow & H^1(K_\mathfrak{p}, E[m]) & & \alpha_\mathfrak{p} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & & E(L_\mathfrak{p})/mE(L_\mathfrak{p}) & \longrightarrow & H^1(L_\mathfrak{p}, E[m]) & & 0 \end{array}$$

Since $L_\mathfrak{p}|K_\mathfrak{p}$ is unramified, we get the following diagram.

$$\begin{array}{ccccccc} \alpha_\mathfrak{p} & & H^1(K_\mathfrak{p}, E[m]) & \xrightarrow{\sim} & (K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times m})^2 & \xrightarrow{v_{K_\mathfrak{p}}} & (\mathbf{Z}/m\mathbf{Z})^2 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \mathrm{id} \\ 0 & & H^1(L_\mathfrak{p}, E[m]) & \xrightarrow{\sim} & (L_\mathfrak{p}^\times/L_\mathfrak{p}^{\times m})^2 & \xrightarrow{v_{L_\mathfrak{p}}} & (\mathbf{Z}/m\mathbf{Z})^2 \end{array}$$

In particular, we deduce that $\alpha_\mathfrak{p}$ corresponds to a pair $(\alpha_1, \alpha_2) \in (K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times m})^2$ such that $v_{K_\mathfrak{p}}(\alpha_1) \equiv v_{K_\mathfrak{p}}(\alpha_2) \equiv 0 \pmod m$. □

To conclude the proof of Theorem 9.3, it is enough to prove the following lemma.

Lemma 9.17. If S is a finite set consisting of non-zero primes of $\mathcal{O}_K$ and all embeddings $K \hookrightarrow \mathbf{R}$, then the group

$$\left\{x \in K^\times : \ v_\mathfrak{p}(x) \equiv 0 \pmod m \text{ for all } \mathfrak{p} \notin S\right\}/K^{\times m}$$

is finite.

To prove Lemma 9.17 we need some tools from algebraic number theory.

Definition 9.18. With the previous notation, define a map

$$\begin{array}{rccc} \mathrm{div} & : & K^\times & \longrightarrow & \bigoplus_{\mathfrak{p} \notin S} \mathbf{Z} \\ & & a & \longmapsto & (v_\mathfrak{p}(a))_{\mathfrak{p} \notin S}. \end{array}$$

The *group of S-units* in K is

$$\mathcal{O}_{K,S}^\times := \ker(\mathrm{div}).$$

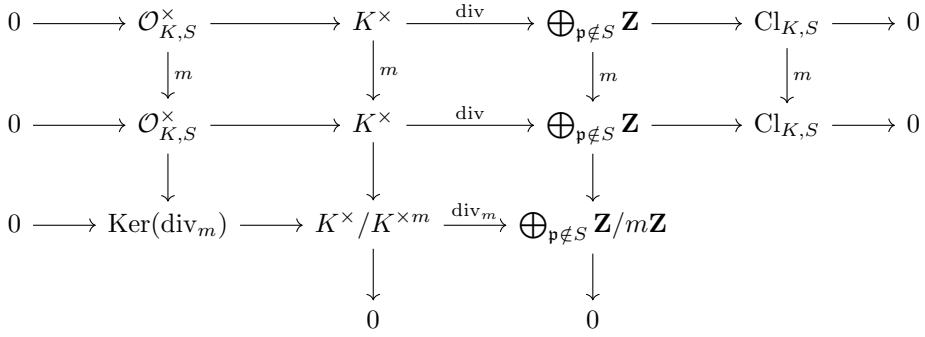
The *S-class group* of K is

$$\mathrm{Cl}_{K,S} := \mathrm{coker}(\mathrm{div}).$$

We need two classical facts, for the proof of which we refer to books on algebraic number theory such as [3].

Facts 9.19. The group $\mathcal{O}_{K,S}^\times$ is finitely generated and the group $\mathrm{Cl}_{K,S}$ is finite.

Proof of Lemma 9.17. We have the following commutative diagram with exact rows:



where $\mathrm{Ker}(\mathrm{div}_m) = \{x \in K^\times \colon v_\mathfrak{p}(x) \equiv 0 \pmod m \text{ for all } \mathfrak{p} \notin S\}/K^{\times m}$ as in the statement. A diagram chase gives an exact sequence

$$\mathcal{O}_{K,S}^\times/m\mathcal{O}_{K,S}^\times \to \mathrm{Ker} \to \mathrm{Cl}_{K,S}[m]$$

and we conclude by Facts 9.19. □

References

[1] N. Bourbaki. *Lie Groups and Lie Algebras: Chapters 1-3*. Bourbaki, Nicolas: Elements of mathematics. Springer, 1989.

[2] J. Milne. *Elliptic Curves*. Kea books. BookSurge Publishers, 2006.

[3] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[4] J.-P. Serre. *Lie Algebras and Lie Groups: 1964 Lectures Given at Harvard University*. Number No. 1500 in Lecture Notes in Mathematics. Springer, 1992.

[5] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[6] T. Szamuely. *A course on the Weil conjectures*. Notes by Davide Lombardo. `https://pagine.dm.unipi.it/tamas/Weil.pdf`.

[7] T. Szamuely. *Notes on commutative algebra*. `https://pagine.dm.unipi.it/tamas/ist-alg.pdf`.

[8] T. Szamuely. *Notes on homological algebra*. `https://pagine.dm.unipi.it/tamas/ist-alg2new.pdf`.

[9] T. Szamuely. *Notes on noncommutative algebra*. `https://pagine.dm.unipi.it/tamas/ist-alg3.pdf`.