Chapter VIII

Elliptic Curves over Global Fields

Let K be a number field and let E/K be an elliptic curve. Our primary goal in this chapter is to prove the following result.

Mordell–Weil Theorem. *The group $E(K)$ is finitely generated.*

The proof of this theorem consists of two quite distinct parts, the so-called "weak Mordell–Weil theorem," proven in (VIII §1), and the "infinite descent" using height functions proven in (VIII §§3,5,6). We also give, in (VIII §4), a separate proof of the descent step in the simplest case, where the general theory of height functions may be replaced by explicit polynomial calculations.

The Mordell–Weil theorem tells us that the *Mordell–Weil group* $E(K)$ has the form

$$E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r,$$

where the torsion subgroup $E(K)_{\text{tors}}$ is finite and the *rank* r of $E(K)$ is a nonnegative integer. For a given elliptic curve, it is relatively easy to determine the torsion subgroup; see (VIII §7). The rank is much more difficult to compute, and in general there is no known procedure that is guaranteed to yield an answer. We study the question of computing the rank of $E(K)$ in more detail in Chapter X.

The following notation will be used for the next three chapters:

K	a number field.
M_K	a complete set of inequivalent absolute values on K.
M_K^∞	the archimedean absolute values in M_K.
M_K^0	the nonarchimedean absolute values in M_K.
$v(x)$	$= -\log \lvert x\rvert_v$, for an absolute value $v \in M_K$.
ord_v	normalized valuation for $v \in M_K^0$, i.e., satisfying $\text{ord}_v(K^*) = \mathbb{Z}$.

J.H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, Graduate Texts in Mathematics 106, DOI 10.1007/978-0-387-09494-6_VIII,

R the ring of integers of K, equal to $\{x \in K : v(x) \geq 0 \text{ for all } v \in M_K^0\}$.
R^* the unit group of R, equal to $\{x \in K : v(x) = 0 \text{ for all } v \in M_K^0\}$.
K_v the completion of K at v for $v \in M_K$.
R_v the ring of integers of K_v for $v \in M_K^0$.
$\mathcal{M}_v$ the maximal ideal of R_v for $v \in M_K^0$.
k_v the residue field of R_v for $v \in M_K^0$.

Finally, in those situations in which it is important to have the absolute values in M_K coherently normalized, such as in the theory of height functions, we always adopt the "standard normalization" as described in (VIII §5).

VIII.1 The Weak Mordell–Weil Theorem

Our goal in this section is to prove the following result.

Theorem 1.1. (Weak Mordell–Weil Theorem) *Let K be a number field, let E/K be an elliptic curve, and let $m \geq 2$ be an integer. Then*

$$E(K)/mE(K)$$

is a finite group.

For the rest of this section, E/K and m are as in the statement of (VIII.1.1). We begin with the following reduction lemma.

Lemma 1.1.1. *Let L/K be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is also finite.*

PROOF. The inclusion $E(K) \hookrightarrow E(L)$ induces a natural map

$$E(K)/mE(K) \longrightarrow E(L)/mE(L).$$

Let Φ be the kernel of this map, so

$$\Phi = \frac{E(K) \cap mE(L)}{mE(K)}.$$

Then for each $P \pmod{mE(K)}$ in Φ, we can choose a point $Q_P \in E(L)$ satisfying $[m]Q_P = P$. (The point Q_P need not be unique, of course.) Having done this, we define a map of sets (which is not, in general, a group homomorphism)

$$\lambda_P : G_{L/K} \longrightarrow E[m], \qquad \lambda_P(\sigma) = Q_P^\sigma - Q_P.$$

Note that $Q_P^\sigma - Q_P$ is in $E[m]$, since

$$[m](Q_P^\sigma - Q_P) = \big([m]Q_P\big)^\sigma - [m]Q_P = P^\sigma - P = O.$$

(The map λ_P is an example of a 1-cocycle; see (VIII §2).)

Suppose that $P, P' \in E(K) \cap mE(L)$ satisfy $\lambda_P = \lambda_{P'}$. Then

$$(Q_P - Q_{P'})^\sigma = Q_P - Q_{P'} \qquad \text{for all } \sigma \in G_{L/K},$$

so $Q_P - Q_{P'} \in E(K)$. It follows that

$$P - P' = [m]Q_P - [m]Q_{P'} \in mE(K),$$

and hence that $P \equiv P' \pmod{mE(K)}$. This proves that the association

$$\Phi \longrightarrow \mathrm{Map}\big(G_{L/K}, E[m]\big), \qquad P \longmapsto \lambda_P,$$

is one-to-one. But $G_{L/K}$ and $E[m]$ are finite sets, so there is only a finite number of maps between them. Therefore the set Φ is finite.

Finally, the exact sequence

$$0 \longrightarrow \Phi \longrightarrow E(K)/mE(K) \longrightarrow E(L)/mE(L)$$

nests $E(K)/mE(K)$ between two finite groups, so it, too, is finite. □

Using (VIII.1.1.1), we see that it suffices to prove the weak Mordell–Weil theorem (VIII.1.1) under the additional assumption that

$$E[m] \subset E(K).$$

For this remainder of this section we assume, without further comment, that this inclusion is true.

The next step is to translate the putative finiteness of $E(K)/mE(K)$ into a statement about a certain field extension of K. In order to do this, we use the following tool.

Definition. The *Kummer pairing*

$$\kappa : E(K) \times G_{\bar{K}/K} \longrightarrow E[m]$$

is defined as follows. Let $P \in E(K)$ and choose any point $Q \in E(\bar{K})$ satisfying $[m]Q = P$. Then

$$\kappa(P, \sigma) = Q^\sigma - Q.$$

The next result describes basic properties of the Kummer pairing.

Proposition 1.2. (a) *The Kummer pairing is well-defined.*

(b) *The Kummer pairing is bilinear.*

(c) *The kernel of the Kummer pairing on the left is $mE(K)$.*

(d) *The kernel of the Kummer pairing on the right is $G_{\bar{K}/L}$, where*

$$L = K\big([m]^{-1}E(K)\big)$$

is the compositum of all fields $K(Q)$ as Q ranges over the points in $E(\bar{K})$ satisfying $[m]Q \in E(K)$.

Hence the Kummer pairing induces a perfect bilinear pairing

$$E(K)/mE(K) \times G_{L/K} \longrightarrow E[m],$$

where L is the field given in (d).

Remark 1.2.1. The field L described in (VIII.1.2) is the elliptic analogue of the classical Kummer extension K'/K obtained by adjoining all m^{th} roots to K. More precisely, assuming that $\boldsymbol{\mu}_m \subset K$, there is a perfect bilinear pairing

$$K^*/(K^*)^m \times G_{K'/K} \longrightarrow \boldsymbol{\mu}_m, \qquad (a,\sigma) \longrightarrow \sqrt[m]{a}^{\sigma} \,/\, \sqrt[m]{a},$$

exactly analogous to the pairing $E(K)/mE(K) \times G_{L/K} \to E[m]$ in (VIII.1.2).

PROOF OF (VIII.1.2). Most of this proposition follows immediately from basic properties of group cohomology; see (VIII §2). For the convenience of the reader, we give a direct proof here.
(a) We must show that $\kappa(P,\sigma)$ is in $E[m]$ and that its value does not depend on the choice of Q. For the first statement, we observe that

$$[m]\kappa(P,\sigma) = [m]Q^{\sigma} - [m]Q = P^{\sigma} - P = O,$$

since $P \in E(K)$ and σ fixes K. For the second statement, we note that any other choice has the form $Q+T$ for some $T \in E[m]$. Then

$$(Q+T)^{\sigma} - (Q+T) = Q^{\sigma} + T^{\sigma} - Q - T = Q^{\sigma} - Q,$$

because we have assumed that $E[m] \subset E(K)$, so σ fixes T.
(b) The linearity in P is obvious. For linearity in σ, we let $\sigma, \tau \in G_{\bar{K}/K}$ and compute

$$\kappa(P,\sigma\tau) = Q^{\sigma\tau} - Q = (Q^{\sigma} - Q)^{\tau} + (Q^{\tau} - Q) = \kappa(P,\sigma)^{\tau} + \kappa(P,\tau).$$

But $\kappa(P,\sigma) \in E[m] \subset E(K)$, so $\kappa(P,\sigma)$ is fixed by τ.
(c) Suppose that $P \in mE(K)$, say $P = [m]Q$ with $Q \in E(K)$. Then Q is fixed by every $\sigma \in G_{\bar{K}/K}$, so

$$\kappa(P,\sigma) = Q^{\sigma} - Q = O.$$

Conversely, suppose that $\kappa(P,\sigma) = 0$ for all $\sigma \in G_{\bar{K}/K}$. Then choosing some point $Q \in E(\bar{K})$ with $[m]Q = P$, we have

$$Q^{\sigma} = Q \quad \text{for all } \sigma \in G_{\bar{K}/K}.$$

Therefore $Q \in E(K)$, so $P = [m]Q \in mE(K)$.
(d) If $\sigma \in G_{\bar{K}/L}$, then

$$\kappa(P,\sigma) = Q^{\sigma} - Q = O,$$

since $Q \in E(L)$ from the definition of L. Conversely, suppose that $\sigma \in G_{\bar{K}/K}$ satisfies $\kappa(P,\sigma) = O$ for all $P \in E(K)$. Then for every point $Q \in E(\bar{K})$ satisfying $[m]Q \in E(K)$ we have

$$O = \kappa\big([m]Q, \sigma\big) = Q^\sigma - Q.$$

But L is the compositum of $K(Q)$ over all such Q, so σ fixes L. Hence $\sigma \in G_{\bar{K}/L}$.

Finally, the last statement of (VIII.1.2) is clear from what precedes it, once we note that L/K is Galois because elements of $G_{\bar{K}/K}$ map $[m]^{-1}E(K)$ to itself. Alternatively, it follows from (d) that $G_{\bar{K}/L}$ is the kernel of the homomorphism

$$G_{\bar{K}/K} \longrightarrow \mathrm{Hom}\big(E(K), E[m]\big), \qquad \sigma \longmapsto \kappa(\,\cdot\,, \sigma),$$

so $G_{\bar{K}/L}$ is a normal subgroup of $G_{\bar{K}/K}$. □

It follows from (VIII.1.2) that the finiteness of $E(K)/mE(K)$ is equivalent to the finiteness of the extension L/K. The next step in the proof of the weak Mordell–Weil theorem is to analyze this extension. Our main tool will be (VII.3.1), which we restate after making the appropriate definitions.

Definition. Let K be a number field and let E/K be an elliptic curve. Let $v \in M_K^0$ be a discrete valuation. Then E is said to have *good* (respectively *bad*) *reduction at* v if E has good (respectively bad) reduction when considered over the completion K_v, cf. (VII §5). Taking a minimal Weierstrass equation for E over K_v, we denote the reduced curve over the residue field by $\tilde{E}_v/k_v$. N.B. It is not always possible to choose a single Weierstrass equation for E over K that is simultaneously minimal for all K_v. However, this can be done if $K = \mathbb{Q}$. See (VIII §8) for further details.

Remark 1.3. Take any Weierstrass equation for E/K,

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

say with discriminant Δ. Then for all but finitely $v \in M_K^0$ we have

$$v(a_i) \ge 0 \quad \text{for } i = 1, \dots, 6 \quad \text{and} \quad v(\Delta) = 0.$$

For any v satisfying these conditions, the given equation is already a minimal Weierstrass equation and the reduced curve $\tilde{E}_v/k_v$ is nonsingular. This shows that E *has good reduction at* v *for all but finitely many* $v \in M_K^0$.

Proposition 1.4. (restatement of (VII.3.1b)) *Let $v \in M_K^0$ be a discrete valuation such that $v(m) = 0$ and such that E has good reduction at v. Then the reduction map*

$$E(K)[m] \longrightarrow \tilde{E}_v(k_v)$$

is injective.

We are now ready to analyze the extension L/K appearing in (VIII.1.2).

Proposition 1.5. *Let*

$$L = K\big([m]^{-1}E(K)\big)$$

be the field defined in (VIII.1.2d).

(a) *The extension L/K is abelian and has exponent m, i.e., the Galois group $G_{L/K}$ is abelian and every element of $G_{L/K}$ has order dividing m.*

(b) *Let*

$$S = \bigl\{v \in M_K^0 : E \text{ has bad reduction at } v\bigr\} \cup \bigl\{v \in M_K^0 : v(m) \neq 0\bigr\} \cup M_K^\infty.$$

The L/K is unramified outside S, i.e., if $v \in M_K$ and $v \notin S$, then L/K is unramified at v.

PROOF. (a) This follows immediately from (VIII.1.2), which implies that there is an injection

$$G_{L/K} \longrightarrow \operatorname{Hom}\bigl(E(K), E[m]\bigr), \qquad \sigma \longmapsto \kappa(\,\cdot\,,\sigma).$$

(b) Let $v \in M_K$ with $v \notin S$, let $Q \in E(\bar{K})$ satisfy $[m]Q \in E(K)$, and let $K' = K(Q)$. It suffices to show that K'/K is unramified at v, since L is the compositum of all such K'. Let $v' \in M_{K'}$ be a place of K' lying above v and let $k'_{v'}/k_v$ be the corresponding extension of residue fields. The assumption that $v \notin S$ ensures that E has good reduction at v, so it also has good reduction at v', since we can take the same Weierstrass equation. Thus we have the usual reduction map

$$E(K') \longrightarrow \tilde{E}(k'_{v'}),$$

which we denote as usual by a tilde.

Let $I_{v'/v} \subset G_{K'/K}$ be the inertia group for v'/v, and take any element $\sigma \in I_{v'/v}$. By definition, an element of inertia such as σ acts trivially on $\tilde{E}(k'_{v'})$, so

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = \tilde{O}.$$

On the other hand, the fact that $[m]Q \in E(K)$ tells us that

$$[m](Q^\sigma - Q) = \bigl([m]Q\bigr)^\sigma - [m]Q = O.$$

Thus $Q^\sigma - Q$ is a point of order m that is in the kernel of the reduction-modulo-v' map. It follows from (VIII.1.4) that

$$Q^\sigma - Q = O.$$

This proves that Q is fixed by every element of the inertia group $I_{v'/v}$, and hence that $K' = K(Q)$ is unramified over K at v'. Since this holds for every v' lying over v and for every $v \notin S$, this completes the proof that K'/K is unramified outside of S. □

All that remains to complete the proof of the weak Mordell–Weil theorem is to show that any field extension L/K satisfying the conditions of (VIII.1.5) is necessarily a finite extension. The proof of this fact relies on the two fundamental finiteness theorems of algebraic number theory, namely the finiteness of the ideal class group and the finite generation of the group of S-units.

Proposition 1.6. *Let K be a number field, let $S \subset M_K$ be a finite set of places that contains M_K^∞, and let $m \ge 2$ be an integer. Let L/K be the maximal abelian extension of K having exponent m that is unramified outside of S. Then L/K is a finite extension.*

PROOF. Suppose that we know that the proposition is true for some finite extension K' of K, where S' is the set of places of K' lying over S. Then LK'/K', being abelian of exponent m unramified outside S', would be finite, and hence L/K would also be finite. It thus suffices to prove the proposition under the assumption that K contains the m^{th} roots of unity $\boldsymbol{\mu}_m$.

Similarly, we may increase the size of the set S, since this only has the effect of making L larger. Using the fact that the class number of K is finite, we adjoin a finite number of elements to S so that the *ring of S-integers*

$$R_S = \bigl\{a \in K : v(a) \ge 0 \text{ for all } v \in M_K \text{ with } v \notin S\bigr\}$$

is a principal ideal domain. (Explicitly, choose integral ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ representing the ideal classes of K and adjoin to S the valuations corresponding to the primes dividing $\mathfrak{a}_1 \cdots \mathfrak{a}_h$.) We also enlarge S so as to ensure that $v(m) = 0$ for all $v \notin S$.

We now apply the main theorem of Kummer theory, which says that if a field of characteristic 0 contains $\boldsymbol{\mu}_m$, then its maximal abelian extension of exponent m is obtained by adjoining the m^{th} roots of all of its elements. For a proof of this result, see any basic textbook on field theory, for example [17, §2], [68, §17.3], or [7, Theorem 25], or do Exercise 8.4. Thus L is the largest subfield of

$$K\bigl(\sqrt[m]{a} : a \in K\bigr)$$

that is unramified outside of S.

Let $v \in M_K$ with $v \notin S$. Consider the equation

$$X^m - a = 0$$

over the local field K_v. Since $v(m) = 0$ and since the discriminant of the polynomial $X^m - a$ equals $\pm m^m a^{m-1}$, we see that $K_v\bigl(\sqrt[m]{a}\bigr)/K_v$ is unramified if and only if

$$\operatorname{ord}_v(a) \equiv 0 \pmod{m}.$$

(Recall that ord_v is the normalized valuation associated to v.) We note that when we adjoin m^{th} roots, it is necessary to take only one representative for each class in $K^*/(K^*)^m$, so if we let

$$T_S = \bigl\{a \in K^*/(K^*)^m : \operatorname{ord}_v(a) \equiv 0 \pmod{m} \text{ for all } v \in M_K \text{ with } v \notin S\bigr\},$$

then

$$L = K\bigl(\sqrt[m]{a} : a \in T_S\bigr).$$

To complete the proof of (VIII.1.6), it suffices to show that the set T_S is finite.

Consider the natural map

$$R_S^* \longrightarrow T_S.$$

We claim that this map is surjective. To see this, suppose that $a \in K^*$ represents an element of T_S. Then the ideal aR_S is the m^{th} power of an ideal in R_S, since the prime ideals of R_S correspond to the valuations $v \notin S$. Using the fact that R_S is a principal ideal domain, we can find a $b \in K^*$ such that $aR_S = b^m R_S$. Hence there is a $u \in R_S^*$ satisfying

$$a = ub^m.$$

Then a and u give the same element of T_S, which proves that R_S^* surjects onto T_S. Further, the kernel of the map $R_S^* \to T_S$ clearly contains $(R_S^*)^m$, which proves that there is a surjection

$$R_S^*/(R_S^*)^m \twoheadrightarrow T_S.$$

(This map is actually an isomorphism.) Finally, we apply Dirichlet's S-unit theorem [142, V §1], which says that R_S^* is a finitely generated group. It follows that T_S is finite, which completes the proof of the proposition. □

The preceding three propositions may now be combined to prove the main result of this section.

PROOF OF THE WEAK MORDELL–WEIL THEOREM (VIII.1.1). Let

$$L = K\big([m]^{-1}E(K)\big)$$

be the field defined in (VIII.1.2d). Since $E[m]$ is finite, the perfect pairing given in (VIII.1.2) shows that $E(K)/mE(K)$ is finite if and only if $G_{L/K}$ is finite. Now (VIII.1.5) says that L has certain properties, and (VIII.1.6) says that any extension of K having these properties is a finite extension. This gives the desired result. (Note that (VIII.1.3) ensures that the set S of (VIII.1.5b) is a finite set.) □

Remark 1.7. The heart of the proof of the weak Mordell–Weil theorem lies in the assertion that the field $L = K\big([m]^{-1}E(K)\big)$ is a finite extension of K. We proved this by first showing (VIII.1.5) that it is abelian of exponent m and that it is unramified outside of a certain finite set $S \subset M_K$. The desired result then followed from basic Kummer theory of fields as given in the proof of (VIII.1.6). It is worth noting that rather than using (VIII.1.6), we could have used the more general theorem of Minkowski that asserts that there are only finitely many extensions of K of bounded degree that are unramified outside of S. To apply this in the present instance, note that for any $Q \in [m]^{-1}E(K)$, the field $K(Q)$ has degree at most m^2 over K, since the Galois conjugates of Q all have the form $Q + T$ for some $T \in E[m]$ and we are assuming that $E[m] \subset E(K)$. It follows from Minkowski's theorem that as Q ranges over $[m]^{-1}E(K)$, there are only finitely many possibilities for the fields $K(Q)$. Hence their compositum $K\big([m]^{-1}E(K)\big)$ is a finite extension of K.

Remark on Effectivity 1.8. Let E/K be an elliptic curve with $E[m] \subset E(K)$, let $S \subset M_K$ be the usual set of bad places for E/K as described in (VIII.1.5b), and let L/K be the maximal abelian extension of K having exponent m such that L/K

is unramified outside of S. Then (VIII.1.2) and (VIII.1.5) tell us that the Kummer pairing induces an injection

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}\bigl(G_{L/K}, E[m]\bigr).$$

It is possible to make the proof of (VIII.1.6) completely explicit, and hence to exactly determine the group $G_{L/K}$; see Exercise 8.1. Thus we can describe all of the elements of the group $\mathrm{Hom}\bigl(G_{L/K}, E[m]\bigr)$, so the crucial question is that of determining which of these elements come from points of $E(K)/mE(K)$. It is this last question for which there is, at present, no known effective solution. In Chapter X we examine this problem in more detail. There we will exhibit a smaller group into which $E(K)/mE(K)$ injects and discuss what can be said about the cokernel. We want to stress that this is the only stage at which the Mordell–Weil theorem is ineffective; if we know generators for $E(K)/mE(K)$, then we can effectively find generators for $E(K)$; see (VIII.3.1) and Exercise 8.18.

We also remark that there is a conditional algorithm due to Manin [156], [114, § F.4.1] that effectively computes generators for $E(K)$ if one accepts the validity of a number of standard (but very deep) conjectures, including in particular the conjecture of Birch and Swinnerton-Dyer (C.16.5).

VIII.2 The Kummer Pairing via Cohomology

In this section we reinterpret the Kummer pairing from (VIII §1) in terms of group cohomology. The methods used here will not be used again until Chapter X and may be omitted by the reader wishing to proceed directly to the proof of the Mordell–Weil theorem. For a summary of the basic facts on group cohomology that are used in this section, see Appendix B and/or the references listed there.

We start with the short exact sequence of $G_{\bar{K}/K}$-modules

$$0 \longrightarrow E[m] \longrightarrow E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \longrightarrow 0,$$

where $m \ge 2$ is a fixed integer. Taking $G_{\bar{K}/K}$-cohomology yields a long exact sequence that starts

$$\begin{aligned} 0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} \\ H^1\bigl(G_{\bar{K}/K}, E[m]\bigr) \longrightarrow H^1\bigl(G_{\bar{K}/K}, E(\bar{K})\bigr) \xrightarrow{[m]} H^1\bigl(G_{\bar{K}/K}, E(\bar{K})\bigr). \end{aligned}$$

From the middle of this exact sequence we extract the following short exact sequence, which is called the *Kummer sequence for* E/K:

$$0 \longrightarrow \frac{E(K)}{mE(K)} \xrightarrow{\delta} H^1\bigl(G_{\bar{K}/K}, E[m]\bigr) \longrightarrow H^1\bigl(G_{\bar{K}/K}, E(\bar{K})\bigr)[m] \longrightarrow 0.$$

(As usual, for any abelian group A, we write $A[m]$ to denote the m-torsion subgroup of A.)

From general principles, the connecting homomorphism δ is computed as follows. Let $P \in E(K)$ and choose some $Q \in E(\bar{K})$ satisfying $[m]Q = P$. Then a 1-cocycle representing $\delta(P)$ is given by

$$c : G_{\bar{K}/K} \longrightarrow E[m], \qquad c_\sigma = Q^\sigma - Q.$$

But this is exactly the Kummer pairing defined in (VIII §1),

$$c_\sigma = \kappa(P, \sigma).$$

(This assumes that we use the same Q on both sides, of course.)

Now suppose that $E[m]$ is contained in $E(K)$. Then

$$H^1\big(G_{\bar{K}/K}, E[m]\big) = \mathrm{Hom}\big(G_{\bar{K}/K}, E[m]\big),$$

so under this assumption we obtain an injective homomorphism

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}\big(G_{\bar{K}/K}, E[m]\big), \qquad P \longmapsto \kappa(P, \,\cdot\,).$$

This provides an alternative proof of (VIII.1.2abc).

Similarly, we can use the inflation–restriction sequence (B.2.4) to give a quick proof of the reduction lemma described in (VIII.1.1.1). Thus if L/K is a finite Galois extension, say satisfying $E[m] \subset E(L)$, then we have a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \Phi & \longrightarrow & E(K)/mE(K) & \longrightarrow & E(L)/mE(L) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1\big(G_{L/K}, E[m]\big) & \xrightarrow{\text{inf}} & H^1\big(G_{\bar{K}/K}, E[m]\big) & \xrightarrow{\text{res}} & H^1\big(G_{\bar{L}/L}, E[m]\big),
\end{array}$$

where the vertical arrows are injections. Since $G_{L/K}$ and $E[m]$ are finite groups, the cohomology group $H^1\big(G_{L/K}, E[m]\big)$ is finite, so Φ is also finite. We observe that the map $\lambda_P : G_{L/K} \to E[m]$ defined in the proof of (VIII.1.1.1) is a cocycle whose cohomology class is precisely the image of $P \in \Phi$ in $H^1\big(G_{L/K}, E[m]\big)$.

Returning now to the general case, we reinterpret (VIII.1.5b) in terms of cohomology.

Definition. Let M be a $G_{\bar{K}/K}$-module, let $v \in M_K^0$ be a discrete valuation, and let $I_v \subset G_{\bar{K}/K}$ be an inertia group for v. A cohomology class $\xi \in H^r(G_{\bar{K}/K}, M)$ is said to be *unramified at* v if it is trivial when restricted to $H^r(I_v, M)$. (The inertia group I_v depends on choosing an extension of v to $\bar{K}$, but one can show that the definition of unramified cohomology class is independent of this choice; cf. (X.4.1.1) and Exercise B.6.)

Proposition 2.1. *Let*

$$S = \big\{v \in M_K^0 : E \textit{ has bad reduction at } v\big\} \cup \big\{v \in M_K^0 : v(m) \neq 0\big\} \cup M_K^\infty.$$

Then the image of $E(K)$ in $H^1\bigl(G_{\bar K/K}, E[m]\bigr)$ under the connecting homomorphism δ consists of cohomology classes that are unramified at every $v \in M_K$ with $v \notin S$.

PROOF. Let $P \in E(K)$ and, as above, let

$$c_\sigma = Q^\sigma - Q$$

be the cocycle representing $\delta(P)$ for some point Q satisfying $[m]Q = P$. Then (VIII.1.5b) says that the field $K(Q)$ is unramified at v. (N.B. The proof of (VIII.1.5b) did not use the assumption that $E[m]$ is contained in $E(K)$.) Hence I_v acts trivially on Q, so $c_\sigma = 0$ for all $\sigma \in I_v$. □

The Kummer Sequence for Fields

The exact sequences that we have derived for elliptic curves are analogous to the classical exact sequences that arise in Kummer theory for fields. To make the analogy clear, we briefly recall the relevant material. The multiplication-by-m sequence for an elliptic curve E corresponds to the following exact sequence of $G_{\bar K/K}$-modules:

$$1 \longrightarrow \boldsymbol{\mu}_m \longrightarrow \bar K^* \xrightarrow{z \to z^m} \bar K^* \longrightarrow 1.$$

Taking $G_{\bar K/K}$-cohomology yields a long exact sequence from which we extract the short exact sequence

$$1 \longrightarrow K^*/(K^*)^m \xrightarrow{\delta} H^1(G_{\bar K/K}, \boldsymbol{\mu}_m) \longrightarrow H^1(G_{\bar K/K}, \bar K^*)[m] \longrightarrow 0.$$

Hilbert's famous "Theorem 90" (B.2.5) asserts that

$$H^1(G_{\bar K/K}, \bar K^*) = 0,$$

so the connecting homomorphism is an isomorphism. This is in marked contrast to the situation for elliptic curves, where the nontriviality of $H^1\bigl(G_{\bar K/K}, E(\bar K)\bigr)$ provides much added complication. (See Chapter X.) Collecting this material and using an explicit computation of the connecting homomorphism gives the following result.

Proposition 2.2. *There is an isomorphism*

$$\delta : K^*/(K^*)^m \xrightarrow{\sim} H^1(G_{\bar K/K}, \boldsymbol{\mu}_m)$$

given by the formula

$$\delta(a) = \textit{cohomology class of the map } \sigma \mapsto \alpha^\sigma/\alpha,$$

where $\alpha \in \bar K^*$ is any element satisfying $\alpha^m = a$.

VIII.3 The Descent Procedure

Our primary goal in this chapter is to prove that $E(K)$, the group of rational points on an elliptic curve, is finitely generated. So far, we know from (VIII.1.1) that the quotient group $E(K)/mE(K)$ is finite. It is easy to see that this is not enough. For example, $\mathbb{R}/m\mathbb{R} = 0$ for every integer $m \geq 1$, yet $\mathbb{R}$ is certainly not a finitely generated group. Similarly, if $E/\mathbb{Q}_p$ is an elliptic curve, then (VII.6.3) says that $E(\mathbb{Q}_p)$ has a subgroup of finite index that is isomorphic to $\mathbb{Z}_p$. Hence $E(\mathbb{Q}_p)/mE(\mathbb{Q}_p)$ is finite, while $E(\mathbb{Q}_p)$ is not finitely generated.

An examination of these two examples shows that the problem occurs because of the large number of elements in the group that are divisible by m. The idea used to complete the proof of the Mordell–Weil theorem is to show that on an elliptic curve over a number field, the multiplication-by-m map tends to increase the "size" of a point, where there are only finitely many points whose "size" is bounded. This will bound how high a power of m may divide a point, and thus eliminate problems such as in the above examples. Of course, all of this is very vague until we explain what is meant by the "size" of a point.

In this section we axiomatize the situation and describe the type of size (or height) function needed to prove that an abelian group is finitely generated. Then, in the next section, we define such a function on an elliptic curve in the simplest case and use explicit formulas to prove that it has the desired properties. This will suffice to prove a special case of the Mordell–Weil theorem. We then turn to the general case and develop the theory of height functions in sufficient generality both to prove the Mordell–Weil theorem and to be useful for later applications.

Theorem 3.1. (Descent Theorem) *Let A be an abelian group. Suppose that there exists a* (height) function

$$h : A \longrightarrow \mathbb{R}$$

with the following three properties:

(i) *Let $Q \in A$. There is a constant C_1, depending on A and Q, such that*

$$h(P+Q) \leq 2h(P) + C_1 \qquad \text{for all } P \in A.$$

(ii) *There are an integer $m \geq 2$ and a constant C_2, depending on A, such that*

$$h(mP) \geq m^2 h(P) - C_2 \qquad \text{for all } P \in A.$$

(iii) *For every constant C_3, the set*

$$\big\{P \in A : h(P) \leq C_3\big\}$$

is finite.

Suppose further that for the integer m in (ii)*, the quotient group A/mA is finite. Then A is finitely generated.*

PROOF. Choose elements $Q_1, \ldots, Q_r \in A$ to represent the finitely many cosets in A/mA, and let $P \in A$ be an arbitrary element. The idea is to show that the

difference between P and an appropriate linear combination of $Q_1, \dots, Q_r$ is a multiple of a point whose height is smaller than a constant that is *independent of* P. Then $Q_1, \dots, Q_r$ and the finitely many points with height less than this constant are generators for A.

We begin by writing

$$P = mP_1 + Q_{i_1} \qquad \text{for some } 1 \le i_1 \le r.$$

Next we do the same thing with P_1, then with P_2, etc., which gives us a list of points

$$\begin{aligned} P &= mP_1 + Q_{i_1}, \\ P_1 &= mP_2 + Q_{i_2}, \\ &\vdots \\ P_{n-1} &= mP_n + Q_{i_n}. \end{aligned}$$

For any index j, we have

$$\begin{aligned} h(P_j) &\le \frac{1}{m^2}\big(h(mP_j) + C_2\big) && \text{from (ii)}, \\ &= \frac{1}{m^2}\big(h(P_{j-1} - Q_{i_j}) + C_2\big) \\ &\le \frac{1}{m^2}\big(2h(P_{j-1}) + C_1' + C_2\big) && \text{from (i)}, \end{aligned}$$

where C_1' is the maximum of the constants from (i) for $Q \in \{-Q_1, \dots, -Q_r\}$. Note that C_1' and C_2 do not depend on P.

We use this inequality repeatedly, starting from P_n and working back to P. This yields

$$\begin{aligned} h(P_n) &\le \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^8} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2) \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2} \\ &\le \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2) \qquad \text{since } m \ge 2. \end{aligned}$$

It follows that if n is sufficiently large, then

$$h(P_n) \le 1 + \frac{1}{2}(C_1' + C_2).$$

Since P is a linear combination of P_n and $Q_1, \dots, Q_r$,

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j},$$

it follows that every P in A is a linear combination of points in the set

$$\{Q_1,\dots,Q_r\} \cup \left\{ Q \in A : h(Q) \le 1 + \frac{1}{2}(C_1' + C_2) \right\}.$$

Property (iii) of the height function h tells us that this is a finite set, which completes the proof that A is finitely generated. □

Remark 3.2. What is needed to make the descent theorem effective, i.e., to allow us to find generators for the group A? First, we must be able to calculate the constants $C_1 = C_1(Q_i)$ for each of the elements $Q_1,\dots,Q_r \in A$ representing the cosets of A/mA. Second, we must be able to calculate the constant C_2. Third, for any constant C_3, we must be able to determine the elements in the finite set $\{P \in A : h(P) \le C_3\}$. The reader may check (Exercise 8.18) that for the height functions used on elliptic curves (VIII §§4, 5, 6), all of these constants are effectively computable, *provided* that we can find elements of $E(K)$ that generate the finite group $E(K)/mE(K)$. Unfortunately, at present there is no known procedure that is guaranteed to give generators for $E(K)/mE(K)$. We return to this question in Chapter X.

VIII.4 The Mordell–Weil Theorem over $\mathbb{Q}$

In this section we prove the following special case of the Mordell–Weil theorem.

Theorem 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated.*

We will, of course, soon be ready to prove the general case; see (VIII.6.7). However, it seems worthwhile to first prove (VIII.4.1), since in this case the necessary height computations using explicit formulas are not too cumbersome.

Fix a Weierstrass equation for $E/\mathbb{Q}$ of the form

$$E : y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Z}.$$

We know from (VIII.1.1) that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, so in order to apply the descent result (VIII.3.1), we need to define a height function on $E(\mathbb{Q})$ and show that it has the requisite properties.

Definition. Let $t \in \mathbb{Q}$, and write $t = p/q$ as a fraction in lowest terms. The *height of* t, denoted by $H(t)$, is defined by

$$H(t) = \max\{|p|, |q|\}.$$

Definition. The (*logarithmic*) *height on* $E(\mathbb{Q})$, relative to the given Weierstrass equation, is the function

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}, \qquad h_x(P) = \begin{cases} \log H\big(x(P)\big) & \text{if } P \ne O, \\ 0 & \text{if } P = O. \end{cases}$$

We note that $h_x(P)$ is always nonnegative.

The next lemma gives us the information that we need in order to apply (VIII.3.1) with the height function h_x.

Lemma 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation*

$$E : y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Z}.$$

(a) *Let $P_0 \in E(\mathbb{Q})$. There is a constant C_1 that depends on P_0, A, and B such that*

$$h_x(P + P_0) \le 2h_x(P) + C_1 \qquad \text{for all } P \in E(\mathbb{Q}).$$

(b) *There is a constant C_2 that depends on A and B such that*

$$h_x\big([2]P\big) \ge 4h_x(P) - C_2 \qquad \text{for all } P \in E(\mathbb{Q}).$$

(c) *For every constant C_3, the set*

$$\big\{P \in E(\mathbb{Q}) : h_x(P) \le C_3\big\}$$

is finite.

PROOF. We may assume that $C_1 > \max\big\{h_x(P_0), h_x([2]P_0)\big\}$, which ensures that (a) is true if $P_0 = O$ or if $P \in \{O, \pm P_0\}$. In all other cases we write

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \qquad \text{and} \qquad P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right),$$

where all fractions are in lowest terms. The addition formula (III.2.3d) says that

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0.$$

Expanding this expression and using the fact that P and P_0 satisfy the given Weierstrass equation yields

$$\begin{aligned} x(P + P_0) &= \frac{(xx_0 + A)(x + x_0) + 2B - 2yy_0}{(x - x_0)^2} \\ &= \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}. \end{aligned}$$

In computing the height of a rational number, cancellation between numerator and denominator can only decrease the height, so we find by an easy estimation that

$$H\big(x(P + P_0)\big) \le C_1' \max\big\{|a|^2, |d|^4, |bd|\big\},$$

where C_1' has a simple expression in terms of A, B, a_0, b_0, d_0. Since $H\big(x(P)\big) = \max\big\{|a|, |d|^2\big\}$, this is almost what we want, the only possible difficulty being the presence of $|bd|$ in the maximum. To deal with this problem, we use the fact that the point P lies on the curve E, so its coordinates satisfy

$$b^2 = a^3 + Aad^4 + Bd^6.$$

Thus

$$|b| \le C_1'' \max\{|a|^{3/2}, |d|^3\},$$

which combined with the above estimate for $H\big(x(P+P_0)\big)$ yields

$$H\big(x(P+P_0)\big) \le C_1 \max\{|a|^2, |d|^4\} = C_1 H\big(x(P)\big)^2.$$

Taking logarithms gives the desired result.
(b) Choosing C_2 to satisfy

$$C_2 \ge 4 \max\{h_x(T) : T \in E(\mathbb{Q})[2]\},$$

we may assume that $[2]P \ne O$. Then, writing $P = (x, y)$, the duplication formula (III.2.3d) reads

$$x\big([2]P\big) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

It is convenient to define homogeneous polynomials

$$\begin{aligned} F(X,Z) &= X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4, \\ G(X,Z) &= 4X^3Z + 4AXZ^3 + 4BZ^4. \end{aligned}$$

If we write $x = x(P) = a/b$ as a fraction in lowest terms, then $x\big([2]P\big)$ may be written as a quotient of integers,

$$x\big([2]P\big) = \frac{F(a,b)}{G(a,b)}.$$

However, in contrast to the proof of (a), we are now looking for a lower bound for $H\big(x([2]P)\big)$, so it is necessary to bound how much cancellation may occur between numerator and denominator.

To do this, we use the fact that $F(X,1)$ and $G(X,1)$ are relatively prime polynomials, so they generate the unit ideal in $\mathbb{Q}[X]$. This implies that identities of the following sort exist.

Sublemma 4.3. *Let* $\Delta = 4A^3 + 27B^2$*, and define polynomials*

$$\begin{aligned} F(X,Z) &= X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4, \\ G(X,Z) &= 4X^3Z + 4AXZ^3 + 4BZ^4, \\ f_1(X,Z) &= 12X^2Z + 16AZ^3, \\ g_1(X,Z) &= 3X^3 - 5AXZ^2 - 27BZ^3, \\ f_2(X,Z) &= 4(4A^3 + 27B^2)X^3 - 4A^2BX^2Z \\ &\qquad + 4A(3A^3 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3, \\ g_2(X,Z) &= -A^2BX^3 - A(5A^3 + 32B^2)X^2Z \\ &\qquad - 2B(13A^3 + 96B^2)XZ^2 + 3A^2(A^3 + 8B^2)Z^3. \end{aligned}$$

Then the following identities hold in $\mathbb{Z}[A,B,X,Z]$:

$$f_1(X,Z)F(X,Z) - g_1(X,Z)G(X,Z) = 4\Delta Z^7,$$
$$f_2(X,Z)F(X,Z) - g_2(X,Z)G(X,Z) = 4\Delta X^7.$$

PROOF. One can check that if $\Delta \neq 0$, then $F(X,Z)$ and $G(X,Z)$ are relatively prime homogeneous polynomials, so identities of this sort must exist. Checking the validity of the two identities is, at worst, a tedious calculation, which we leave for the reader. To actually find the polynomials f_1, g_1, f_2, g_2, one can use the Euclidean algorithm or the theory of resultants. □

We return to the proof of (VIII.4.2b). Let

$$\delta = \gcd\bigl(F(a,b), G(a,b)\bigr)$$

denote the cancellation in our fraction for $x\bigl([2]P\bigr)$. From the equations

$$f_1(a,b)F(a,b) - g_1(a,b)G(a,b) = 4\Delta b^7,$$
$$f_2(a,b)F(a,b) - g_2(a,b)G(a,b) = 4\Delta a^7,$$

we see that δ divides 4Δ. This gives the bound

$$|\delta| \le |4\Delta|,$$

and hence

$$H\bigl(x([2]P)\bigr) \ge \frac{\max\bigl\{\bigl|F(a,b)\bigr|, \bigl|G(a,b)\bigr|\bigr\}}{|4\Delta|}.$$

On the other hand, the same identities give the estimates

$$|4\Delta b^7| \le 2\max\bigl\{\bigl|f_1(a,b)\bigr|, \bigl|g_1(a,b)\bigr|\bigr\}\max\bigl\{\bigl|F(a,b)\bigr|, \bigl|G(a,b)\bigr|\bigr\},$$
$$|4\Delta a^7| \le 2\max\bigl\{\bigl|f_2(a,b)\bigr|, \bigl|g_2(a,b)\bigr|\bigr\}\max\bigl\{\bigl|F(a,b)\bigr|, \bigl|G(a,b)\bigr|\bigr\}.$$

Looking at the expressions for f_1, f_2, g_1, g_2 in (VIII.4.3), we have

$$\max\bigl\{\bigl|f_1(a,b)\bigr|, \bigl|g_1(a,b)\bigr|, \bigl|f_2(a,b)\bigr|, \bigl|g_2(a,b)\bigr|\bigr\} \le C\max\bigl\{|a|^3, |b|^3\bigr\},$$

where C is a constant depending on A and B. Combining the last three inequalities yields

$$\max\bigl\{|4\Delta a^7|, |4\Delta b^7|\bigr\} \le 2C\max\bigl\{|a|^3, |b|^3\bigr\}\max\bigl\{\bigl|F(a,b)\bigr|, \bigl|G(a,b)\bigr|\bigr\}.$$

Canceling $\max\bigl\{|a|^3, |b|^3\bigr\}$ from both sides, we obtain the estimate

$$\frac{\max\bigl\{\bigl|F(a,b)\bigr|, \bigl|G(a,b)\bigr|\bigr\}}{|4\Delta|} \ge (2C)^{-1}\max\bigl\{|a|^4, |b|^4\bigr\},$$

and then using the fact that $\max\bigl\{|a|, |b|\bigr\} = H\bigl(x(P)\bigr)$ gives the desired result,

$$H\big(x([2]P)\big) \ge (2C)^{-1} H\big(x(P)\big)^4.$$

(c) For any constant C, the set

$$\big\{t \in \mathbb{Q} : H(t) \le C\big\}$$

is clearly finite. Indeed, it has at most $(2C+1)^2$ elements, since the numerator and denominator of t are integers restricted to lie between $-C$ and C. Further, given any value for x, there are at most two values of y for which (x,y) is a point of E. Therefore

$$\big\{P \in E(\mathbb{Q}) : h_x(P) \le C_3\big\}$$

is also a finite set. □

The proof of (VIII.4.1) is now simply a matter of fitting together what we have already done.

PROOF OF (VIII.4.1). We know from (VIII.1.1) that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. It follows from (VIII.4.2) that the height function

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

satisfies the conditions needed to apply the descent procedure (VIII.3.1) with $m = 2$. The conclusion of (VIII.3.1) is that $E(\mathbb{Q})$ is finitely generated. □

VIII.5 Heights on Projective Space

In order to use the descent theorem (VIII.3.1) to prove the Mordell–Weil theorem in general, we need to define a height function on the K-rational points of an elliptic curve. It is possible to proceed in an ad hoc manner using explicit equations, as was done in the last section, but we instead develop a general theory of height functions. From this general theory will follow all of the necessary properties, plus considerably more. Elliptic curves are given as subsets of projective space, so in this section we study a height function defined on all of projective space, and then in the next section we examine its properties when restricted to the points of an elliptic curve.

Example 5.1. Let $P \in \mathbb{P}^N(\mathbb{Q})$ be a point with rational coordinates. Since $\mathbb{Z}$ is a principal ideal domain, we can find homogeneous coordinates

$$P = [x_0, \ldots, x_N]$$

satisfying

$$x_0, \ldots, x_N \in \mathbb{Z} \qquad \text{and} \qquad \gcd(x_0, \ldots, x_N) = 1.$$

Then a natural measure of the *height of* P is

$$H(P) = \max\big\{|x_0|, \ldots, |x_N|\big\}.$$

With this definition, it is clear that for any constant C, the set

$$\bigl\{P \in \mathbb{P}^N(\mathbb{Q}) : H(P) \le C\bigr\}$$

is a finite set. Indeed, it has at most $(2C+1)^N$ elements. This is the sort of finiteness property that is needed for the descent procedure described in (VIII.3.1).

If we try to generalize (VIII.5.1) to arbitrary number fields, we run into the difficulty that the ring of integers need not be a principal ideal domain. We thus take a somewhat different approach, for which purpose we now specify more precisely how the absolute values in M_K are normalized.

Definition. The *set of standard absolute values on* $\mathbb{Q}$, which we denote by $M_{\mathbb{Q}}$, consists of the following:

(i) $M_{\mathbb{Q}}$ contains one archimedean absolute value, defined by

$$|x|_\infty = \text{usual absolute value} = \max\{x, -x\}.$$

(ii) For each prime $p \in \mathbb{Z}$, the set $M_{\mathbb{Q}}$ contains one nonarchimedean (p-adic) absolute value defined by

$$\left|p^n \frac{a}{b}\right|_p = p^{-n} \qquad \text{for } a, b \in \mathbb{Z} \text{ satisfying } p \nmid ab.$$

The *set of standard absolute values* on a number field K, denoted by M_K, is the set of all absolute values on K whose restriction to $\mathbb{Q}$ is one of the absolute values in $M_{\mathbb{Q}}$.

Definition. Let $v \in M_K$. The *local degree at* v, denoted by n_v, is

$$n_v = [K_v : \mathbb{Q}_v],$$

where K_v and $\mathbb{Q}_v$ denote the completions of K and $\mathbb{Q}$ with respect to the absolute value v.

With the preceding definitions, we state two basic facts from algebraic number theory that will be needed later.

Extension Formula 5.2. *Let $L/K/\mathbb{Q}$ be a tower of number fields, and let $v \in M_K$. Then*

$$\sum_{\substack{w \in M_L \\ w \mid v}} n_w = [L : K] n_v.$$

(*Here $w \mid v$ means that w restricted to K is equal to v.*)

Product Formula 5.3. *Let $x \in K^*$. Then*

$$\prod_{v \in M_K} |x|_v^{n_v} = 1.$$

For proofs of (VIII.5.2) and (VIII.5.3), see any standard text on algebraic number theory, for example [142, II §1 and V §1].

We are now ready to define the height of a point in projective space.

Definition. Let $P \in \mathbb{P}^N(K)$ be a point with homogeneous coordinates

$$P = [x_0, \ldots, x_N], \qquad x_0, \ldots, x_N \in K.$$

The *height of* P (*relative to* K) is

$$H_K(P) = \prod_{v \in M_K} \max\bigl\{|x_0|_v, \ldots, |x_N|_v\bigr\}^{n_v}.$$

Proposition 5.4. *Let* $P \in \mathbb{P}^N(K)$.

(a) *The height* $H_K(P)$ *does not depend on the choice of homogeneous coordinates for* P.

(b) *The height satisfies*

$$H_K(P) \ge 1.$$

(c) *Let* L/K *be a finite extension. Then*

$$H_L(P) = H_K(P)^{[L:K]}.$$

PROOF. (a) Any other choice of homogeneous coordinates for P has the form $[\lambda x_0, \ldots, \lambda x_N]$ for some $\lambda \in K^*$. Using the product formula (VIII.5.3), we have

$$\begin{aligned}\prod_{v \in M_K} \max\bigl\{|\lambda x_0|_v, \ldots, |\lambda x_N|_v\bigr\}^{n_v} &= \prod_{v \in M_K} |\lambda|^{n_v} \max\bigl\{|x_0|_v, \ldots, |x_N|_v\bigr\}^{n_v} \\ &= \prod_{v \in M_K} \max\bigl\{|x_0|_v, \ldots, |x_N|_v\bigr\}^{n_v}.\end{aligned}$$

(b) Given any point P in projective space, we can always find homogeneous coordinates for P such that one of the coordinates is 1. Then every factor in the product defining $H_K(P)$ is at least 1.

(c) We compute

$$\begin{aligned}H_L(P) &= \prod_{w \in M_L} \max\bigl\{|x_i|_w\bigr\}^{n_w} \\ &= \prod_{v \in M_K} \prod_{\substack{w \in M_L \\ w|v}} \max\bigl\{|x_i|_v\bigr\}^{n_w} && \text{since } x_i \in K, \\ &= \prod_{v \in M_K} \max\bigl\{|x_i|_v\bigr\}^{[L:K]n_v} && \text{from (VIII.5.2)}, \\ &= H_K(P)^{[L:K]}.\end{aligned}$$

□

Remark 5.5. If $K = \mathbb{Q}$, then $H_{\mathbb{Q}}$ agrees with the more intuitive height function given in (VIII.5.1). To see this, let $P \in \mathbb{P}^N(\mathbb{Q})$ and choose homogeneous coordinates $[x_0, \dots, x_N]$ for P with $x_i \in \mathbb{Z}$ and $\gcd(x_0, \dots, x_N) = 1$. Then, for any nonarchimedean absolute value $v \in M_{\mathbb{Q}}$, we have $|x_i|_v \le 1$ for all i and $|x_i|_v = 1$ for at least one i. Hence in the product defining $H_{\mathbb{Q}}(P)$, only the factor for the archimedean absolute value contributes, so

$$H_{\mathbb{Q}}(P) = \max\bigl\{|x_0|_\infty, \dots, |x_N|_\infty\bigr\}.$$

In particular, it follows that for any constant C, the set

$$\bigl\{P \in \mathbb{P}^N(\mathbb{Q}) : H_{\mathbb{Q}}(P) \le C\bigr\}$$

is finite. One of our goals is to extend this statement to H_K. We will actually prove something stronger; see (VIII.5.11).

Sometimes it is easier to work with a height function that is not relative to a particular number field. We use (VIII.5.4c) to create such a function.

Definition. Let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. The (*absolute*) *height of* P, denoted by $H(P)$, is defined as follows. Choose a number field K such that $P \in \mathbb{P}^N(K)$. Then

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]},$$

where we take the positive root. We see from (VIII.5.4c) that $H(P)$ is well-defined, independent of the choice of K, and (VIII.5.4b) implies that $H(P) \ge 1$.

We next investigate how the height changes under mappings between projective spaces. We recall the following definition; cf. (I.3.3).

Definition. A *morphism of degree* d between projective spaces is a map

$$F : \mathbb{P}^N \longrightarrow \mathbb{P}^M, \qquad F(P) = \bigl[f_0(P), \dots, f_M(P)\bigr],$$

where $f_0, \dots, f_M \in \bar{\mathbb{Q}}[X_0, \dots, X_N]$ are homogeneous polynomials of degree d having no common zero in $\bar{\mathbb{Q}}^{N+1}$ other than $X_0 = \cdots = X_N = 0$. If F can be written using polynomials f_i having coefficients in K, then F is said to be *defined over* K.

Theorem 5.6. *Let*

$$F : \mathbb{P}^N \longrightarrow \mathbb{P}^M$$

be a morphism of degree d*. Then there are positive constants* C_1 *and* C_2*, depending on* F*, such that*

$$C_1 H(P)^d \le H\bigl(F(P)\bigr) \le C_2 H(P)^d \qquad \textit{for all } P \in \mathbb{P}^N(\bar{\mathbb{Q}}).$$

PROOF. Write $F = [f_0, \dots, f_M]$ using homogeneous polynomials f_i having no common zeros, and let $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\bar{\mathbb{Q}})$ be a point with algebraic coordinates. Choose some number field K that contains $x_0, \dots, x_N$ and also contains all of the coefficients of all of the f_i. For each absolute value $v \in M_K$, we let

$$|P|_v = \max_{0\le i\le N} |x_i|_v \qquad \text{and} \qquad \bigl|F(P)\bigr|_v = \max_{0\le j\le M} \bigl|f_j(P)\bigr|_v,$$

and we also define

$$|F|_v = \max\bigl\{|a|_v : a \text{ is a coefficient of some } f_i\bigr\}.$$

Then, from the definition of height, we have

$$H_K(P) = \prod_{v\in M_K} |P|_v^{n_v} \qquad \text{and} \qquad H_K\bigl(F(P)\bigr) = \prod_{v\in M_K} \bigl|F(P)\bigr|_v^{n_v},$$

so it makes sense to define

$$H_K(F) = \prod_{v\in M_K} |F|_v^{n_v}.$$

In other words, $H_K(F) = H\bigl([a_0, a_1, \ldots]\bigr)$, where the a_j are the coefficients of the f_i. Finally, we let $C_1, C_2, \ldots$ denote constants that depend only on M, N, and d, and we set

$$\epsilon(v) = \begin{cases} 1 & \text{if } v \in M_K^\infty, \\ 0 & \text{if } v \in M_K^0. \end{cases}$$

To illustrate the utility of the function ϵ, we observe that the triangle inequality may be concisely written as

$$|t_1 + \cdots + t_n|_v \le n^{\epsilon(v)} \max\bigl\{|t_1|_v, \ldots, |t_n|_v\bigr\}$$

for all $v \in M_K$, both archimedean and nonarchimedean.

Having set notation, we turn to the proof of (VIII.5.6). The upper bound is relatively easy. Let $v \in M_K$. The triangle inequality yields

$$\bigl|f_i(P)\bigr|_v \le C_1^{\epsilon(v)} |F|_v |P|_v^d,$$

since f_i is homogeneous of degree d. Here C_1 could equal the number of terms in f_i, which is at most $\binom{N+d}{N}$, i.e., the number of monomials of degree d in $N+1$ variables. Since this estimate holds for every i, we find that

$$\bigl|F(P)\bigr|_v \le C_1^{\epsilon(v)} |F|_v |P|_v^d.$$

Now raise to the n_v power, multiply over all $v \in M_K$, and take the $[K:\mathbb{Q}]^{\text{th}}$ root. This yields the desired upper bound

$$H\bigl(F(P)\bigr) \le C_1 H(F) H(P)^d,$$

where we have used the formula (VIII.5.2),

$$\sum_{v\in M_K} \epsilon(v) n_v = \sum_{v\in M_K^\infty} n_v = [K:\mathbb{Q}].$$

It is worth mentioning that in proving this upper bound, we did not use the fact that the f_i have no common nontrivial zeros. However, we will certainly need to use this property to prove the lower bound, since without it there are easy counterexamples; see Exercise 8.10.

Thus we now assume that the set

$$\bigl\{Q \in \mathbb{A}^{N+1}(\bar{\mathbb{Q}}) : f_0(Q) = \cdots = f_M(Q) = 0\bigr\}$$

consists of the single point $(0,\ldots,0)$. It follows from the Nullstellensatz ([111, I.1.3A], [73, Theorem 1.6]) that the ideal generated by $f_0,\ldots,f_M$ in $\bar{\mathbb{Q}}[X_0,\ldots,X_N]$ contains some power of each of $X_0,\ldots,X_N$, since each X_i also vanishes at the point $(0,\ldots,0)$. Thus there are polynomials $g_{ij} \in \bar{\mathbb{Q}}[X_0,\ldots,X_N]$ and an integer $e \ge 1$ such that

$$X_i^e = \sum_{j=0}^{M} g_{ij} f_j \qquad \text{for each } 0 \le i \le N.$$

Replacing K by a finite extension if necessary, we may assume that each $g_{ij} \in K[X_0,\ldots,X_N]$, and discarding all terms on the right-hand side except those that are homogeneous of degree e, we may assume that each g_{ij} is homogeneous of degree $e-d$. We further set the following reasonable notation:

$$\begin{aligned} |G|_v &= \max\bigl\{|b|_v : b \text{ is a coefficient of some } g_{ij}\bigr\},\\ H_K(G) &= \prod_{v\in M_K} |G|_v^{n_v}. \end{aligned}$$

We observe that e and $H_K(G)$ may be bounded in terms of M, N, d, and $H_K(F)$, although finding a good bound is not an easy task. See (VIII.5.7) for a discussion. For our purposes it is enough to know that e and $H_K(G)$ do not depend on the point P.

Recalling that $P = [x_0,\ldots,x_N]$, we see that the formula for X_i^e implies that

$$\begin{aligned} |x_i|_v^e = \left|\sum_{j=0}^{M} g_{ij}(P) f_j(P)\right|_v &\le C_2^{\epsilon(v)} \max_{0\le j\le M} \bigl|g_{ij}(P)f_j(P)\bigr|_v\\ &\le C_2^{\epsilon(v)} \max_{0\le j\le M} \bigl|g_{ij}(P)\bigr|\,\bigl|F(P)\bigr|_v. \end{aligned}$$

We now take the maximum over i to obtain

$$|P|_v^e \le C_2^{\epsilon(v)} \max_{\substack{0\le j\le M\\ 0\le i\le N}} \bigl|g_{ij}(P)\bigr|_v \bigl|F(P)\bigr|_v.$$

Each g_{ij} is homogeneous of degree $e-d$, so the usual application of the triangle inequality yields

$$\bigl|g_{ij}(P)\bigr|_v \le C_3^{\epsilon(v)} |G|_v |P|_v^{e-d}.$$

Here C_3 may depend on e, but as noted earlier, we can bound e in terms of M, N, and d. Substituting this estimate into the earlier one and multiplying by $|P|_v^{d-e}$ gives

$$|P|_v^d \le C_4^{\epsilon(v)} |G|_v \big|F(P)\big|_v,$$

and now the usual raising to the n_v power, multiplying over $v \in M_K$, and taking the $[K:\mathbb{Q}]^{\text{th}}$ root yields the desired lower bound. □

Remark 5.7. As indicated during the proof of (VIII.5.6), the dependence of C_1 on F in the inequality

$$C_1 H(P)^d \le H\big(F(P)\big)$$

is not at all straightforward. It is possible to express C_1 in terms of the coefficients of certain polynomials whose existence is guaranteed by the Nullstellensatz, and the Nullstellensatz can be made completely explicit by the use of elimination theory, but this method leads to a very poor estimate. For an explicit version of the Nullstellensatz in which an effort has been made to give good estimates for the coefficients, see [162].

We also record the special case of (VIII.5.6) for an automorphism of $\mathbb{P}^N$.

Corollary 5.8. *Let $A \in \mathrm{GL}_{N+1}(\bar{\mathbb{Q}})$, so multiplication by the matrix A induces an automorphism $A : \mathbb{P}^N \to \mathbb{P}^N$. There are positive constants C_1 and C_2, depending on the entries of the matrix A, such that*

$$C_1 H(P) \le H(AP) \le C_2 H(P) \qquad \textit{for all } P \in \mathbb{P}^N(\bar{\mathbb{Q}}).$$

PROOF. This is (VIII.5.6) for morphisms of degree one. □

We next investigate the relationship between the coefficients of a polynomial and the height of its roots.

Notation. For $x \in \bar{\mathbb{Q}}$, let

$$H(x) = H\big([x,1]\big),$$

and similarly for $x \in K$, let

$$H_K(x) = H_K\big([x,1]\big).$$

Theorem 5.9. *Let*

$$f(T) = a_0 T^d + a_1 T^{d-1} + \cdots + a_d = a_0 (T-\alpha_1)\cdots(T-\alpha_d) \in \bar{\mathbb{Q}}[T]$$

be a polynomial of degree d. Then

$$2^{-d} \prod_{j=1}^{d} H(\alpha_j) \le H\big([a_0,\ldots,a_d]\big) \le 2^{d-1} \prod_{j=1}^{d} H(\alpha_j).$$

PROOF. First note that the inequality to be proven remains unchanged if $f(T)$ is multiplied by a nonzero constant. It thus suffices to prove the result for monic polynomials, so we may assume that $a_0 = 1$.

Let $K = \mathbb{Q}(\alpha_1,\ldots,\alpha_d)$, and for $v \in M_K$, set

$$\epsilon(v) = \begin{cases} 2 & \text{if } v \in M_K^\infty, \\ 1 & \text{if } v \in M_K^0. \end{cases}$$

Note that this notation differs from the notation used in the proof of (VIII.5.6). In the present instance, the triangle inequality reads

$$|x+y|_v \le \epsilon(v)\max\bigl\{|x|_v, |y|_v\bigr\} \qquad \text{for } v \in M_K \text{ and } x, y \in K.$$

Of course, if $v \in M_K^0$ and $|x|_v \ne |y|_v$, then the triangle inequality becomes an equality.

We are going to prove that

$$\epsilon(v)^{-d}\prod_{j=1}^{d}\max\bigl\{|\alpha_j|_v, 1\bigr\} \le \max_{0\le i\le d}\bigl\{|a_i|_v\bigr\} \le \epsilon(v)^{d-1}\prod_{j=1}^{d}\max\bigl\{|\alpha_j|_v, 1\bigr\}.$$

Once we have done this, raising to the n_v power, multiplying over all $v \in M_K$, and taking the $[K:\mathbb{Q}]^{\text{th}}$ root gives the desired result.

The proof is by induction on $d = \deg(f)$. For $d = 1$ we have $f(T) = T - \alpha_1$, so the inequalities are clear. Assume now that we know the result for all polynomials (with roots in K) of degree $d-1$. Choose an index k such that

$$|\alpha_k|_v \ge |\alpha_j|_v \qquad \text{for all } 0 \le j \le d,$$

and define a polynomial

$$\begin{aligned} g(T) &= (T-\alpha_1)\cdots(T-\alpha_{k-1})(T-\alpha_{k+1})\cdots(T-\alpha_d) \\ &= b_0T^{d-1} + b_1T^{d-2} + \cdots + b_{d-1}. \end{aligned}$$

Thus $f(T) = (T-\alpha_k)g(T)$, so comparing coefficients yields

$$a_i = b_i - \alpha_k b_{i-1}.$$

(This holds for all $0 \le i \le d$ if we set $b_{-1} = b_d = 0$.)

We begin with the upper bound:

$$\begin{aligned} \max_{0\le i\le d}\bigl\{|a_i|_v\bigr\} &= \max_{0\le i\le d}\bigl\{|b_i - \alpha_k b_{i-1}|_v\bigr\} \\ &\le \epsilon(v)\max_{0\le i\le d}\bigl\{|b_i|_v, |\alpha_k b_{i-1}|_v\bigr\} && \text{triangle inequality,} \\ &\le \epsilon(v)\max_{0\le i\le d}\bigl\{|b_i|_v\bigr\}\max\bigl\{|\alpha_k|_v, 1\bigr\} \\ &\le \epsilon(v)^{d-1}\prod_{j=1}^{d}\max\bigl\{|\alpha_j|_v, 1\bigr\} && \text{induction hypothesis} \\ & && \text{applied to } g. \end{aligned}$$

Next, to prove the lower bound, we consider two cases. First, if $|\alpha_k|_v \le \epsilon(v)$, then by the choice of the index k we have

$$\prod_{j=1}^{d} \max\bigl\{|\alpha_j|_v, 1\bigr\} \le \max\bigl\{|\alpha_k|_v, 1\bigr\}^d \le \epsilon(v)^d,$$

so the result is clear. (Remember that $a_0 = 1$.) Next, suppose that $|\alpha_k|_v > \epsilon(v)$. Then

$$\max_{0\le i\le d}\bigl\{|a_i|_v\bigr\} = \max_{0\le i\le d}\bigl\{|b_i - \alpha_k b_{i-1}|_v\bigr\} \ge \epsilon(v)^{-1} \max_{0\le i\le d-1}\bigl\{|b_i|_v\bigr\}\bigl\{|\alpha_k|_v, 1\bigr\}.$$

Here the last line is an equality for $v \in M_K^0$, while for $v \in M_K^\infty$ we are using the calculation

$$\begin{aligned}\max_{0\le i\le d}\bigl\{|b_i - \alpha_k b_{i-1}|_v\bigr\} &\ge \bigl(|\alpha_k|_v - 1\bigr) \max_{0\le i\le d-1}\bigl\{|b_i|_v\bigr\} \\ &> \epsilon(v)^{-1}|\alpha_k|_v \max_{0\le i\le d-1}\bigl\{|b_i|_v\bigr\} \quad \text{since } |\alpha_k|_v > \epsilon(v) = 2.\end{aligned}$$

Applying the induction hypothesis to g gives the desired lower bound, which completes the proof of (VIII.5.9). □

Our first application of (VIII.5.9) is to show that there are only finitely many points of bounded height in projective space. To do this, we first need to show that the action of the Galois group does not affect the height of a point.

Theorem 5.10. *Let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$ and let $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$. Then*

$$H(P^\sigma) = H(P).$$

PROOF. Let $K/\mathbb{Q}$ be a field such that $P \in \mathbb{P}^N(K)$. The field K may not be Galois over $\mathbb{Q}$, but in any case σ gives an isomorphism $\sigma : K \xrightarrow{\sim} K^\sigma$, and σ likewise identifies the sets of absolute values of K and K^σ,

$$\sigma : M_K \xrightarrow{\sim} M_{K^\sigma}, \qquad v \longmapsto v^\sigma.$$

Here, if $x \in K$ and $v \in M_K$, then the associated absolute value v^σ satisfies $|x^\sigma|_{v^\sigma} = |x|_v$. It is clear that σ also induces an isomorphism $K_v \xrightarrow{\sim} K_{v^\sigma}^\sigma$, so the local degrees satisfy $n_v = n_{v^\sigma}$. We now compute

$$\begin{aligned}H_{K^\sigma}(P^\sigma) &= \prod_{w\in M_{K^\sigma}} \max\bigl\{|x_i^\sigma|_w\bigr\}^{n_w} \\ &= \prod_{v\in M_K} \max\bigl\{|x_i^\sigma|_{v^\sigma}\bigr\}^{n_{v^\sigma}} \\ &= \prod_{v\in M_K} \max\bigl\{|x_i|_v\bigr\}^{n_v} \\ &= H_K(P).\end{aligned}$$

Since $[K : \mathbb{Q}] = [K^\sigma : \mathbb{Q}]$, this is the desired result. □

Theorem 5.11. *Let C and d be constants. Then the set*

$$\bigl\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \le C \text{ and } \bigl[\mathbb{Q}(P) : \mathbb{Q}\bigr] \le d\bigr\}$$

is a finite set of points, where we recall from (I §2) *that $\mathbb{Q}(P)$ is the minimal field of definition of P. In particular, for any number field K,*

$$\bigl\{P \in \mathbb{P}^N(K) : H_K(P) \le C\bigr\}$$

is a finite set.

PROOF. Let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. We choose homogeneous coordinates for P, say

$$P = [x_0, \ldots, x_N],$$

with some $x_j = 1$. Then $\mathbb{Q}(P) = \mathbb{Q}(x_0, \ldots, x_N)$, and we have the easy estimate

$$\begin{aligned} H_{\mathbb{Q}(P)}(P) &= \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \le i \le N} \bigl\{|x_i|_v\bigr\}^{n_v} \\ &\ge \max_{0 \le i \le N} \left(\prod_{v \in M_{\mathbb{Q}(P)}} \max\bigl\{|x_i|_v, 1\bigr\}^{n_v} \right) \\ &= \max_{0 \le i \le N} H_{\mathbb{Q}(P)}(x_i). \end{aligned}$$

Thus if $H(P) \le C$ and $\bigl[\mathbb{Q}(P) : \mathbb{Q}\bigr] \le d$, then

$$\max_{0 \le i \le N} H_{\mathbb{Q}(P)}(x_i) \le C^d \qquad \text{and} \qquad \max_{0 \le i \le N} \bigl[\mathbb{Q}(x_i) : \mathbb{Q}\bigr] \le d.$$

Replacing C^d by C, it thus suffices to prove that the set

$$\bigl\{x \in \bar{\mathbb{Q}} : H(x) \le C \text{ and } \bigl[\mathbb{Q}(x) : \mathbb{Q}\bigr] \le d\bigr\}$$

is finite. In other words, we have reduced to the case that $N = 1$.

Suppose that $x \in \bar{\mathbb{Q}}$ is in this set, and let $e = \bigl[\mathbb{Q}(x) : \mathbb{Q}\bigr]$, so $e \le d$. Further, let $x_1, \ldots, x_e \in \bar{\mathbb{Q}}$ be the conjugates of x, where we take $x_1 = x$. The minimal polynomial of x over $\mathbb{Q}$ is

$$f_x(T) = (T - x_1) \cdots (T - x_e) = T^e + a_1 T^{e-1} + \cdots + a_e \in \mathbb{Q}[T].$$

We estimate

$$\begin{aligned} H\bigl([1, a_1, \ldots, a_e]\bigr) &\le 2^{e-1} \prod_{j=1}^{e} H(x_j) && \text{from (VIII.5.9),} \\ &= 2^{e-1} H(x)^e && \text{from (VIII.5.10),} \\ &\le (2C)^d && \text{since } H(x) \le C \text{ and } e \le d. \end{aligned}$$

Since the a_i are in $\mathbb{Q}$, it follows that for a given C and d, there are only finitely many possibilities for the polynomial $f_x(T)$. (We are using the easy-to-prove case of (VIII.5.11) with $K = \mathbb{Q}$; see (VIII.5.1) and (VIII.5.3).) Since each polynomial $f_x(T)$ has at most d roots in K, and thus contributes at most d elements to our set, this completes the proof that the set is finite. □

Remark 5.12. Tracing through the proof of (VIII.5.11), it is easy to give an upper bound, in terms of C and d, for the number of points in the set

$$\bigl\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \le C \text{ and } \bigl[\mathbb{Q}(P) : \mathbb{Q}\bigr] \le d\bigr\}.$$

(See Exercise 8.7a.) A formula due to Schanuel gives a precise asymptotic formula for

$$\#\bigl\{P \in \mathbb{P}^N(K) : H_K(P) \le C\bigr\}$$

as a function of C as $C \to \infty$. See [139, Chapter 3, Section 5] or [220] for details.

VIII.6 Heights on Elliptic Curves

In this section we use the general theory of heights as developed in the previous section to define height functions on elliptic curves. The main theorems that we prove, (VIII.6.2) and (VIII.6.4), highlight the interplay between the height function and the addition law on the elliptic curve. As an immediate corollary, we deduce the remaining results needed to prove the Mordell–Weil theorem for arbitrary number fields (VIII.6.7).

It is convenient to use "big-O" notation.

Notation. Let f and g be real-valued functions on a set $\mathcal{S}$. We write

$$f = g + O(1)$$

if there are constants C_1 and C_2 such that

$$C_1 \le f(P) - g(P) \le C_2 \qquad \text{for all } P \in \mathcal{S}.$$

If only the lower inequality is satisfied, then we write $f \ge g + O(1)$, and similarly if only the upper inequality is true, then we write $f \le g + O(1)$.

Let E/K be an elliptic curve. Recall from (II.2.2) that any nonconstant function $f \in \bar{K}(E)$ determines a surjective morphism, which we also denote by f,

$$f : E \longrightarrow \mathbb{P}^1, \qquad P \longmapsto \begin{cases} [1,0] & \text{if } P \text{ is a pole of } f, \\ [f(P),1] & \text{otherwise.} \end{cases}$$

It would be reasonable to use f to define a height function on $E(\bar{K})$ by setting $H_f(P) = H\bigl(f(P)\bigr)$. However, the height function H tends to behave multiplicatively, as for example in (VIII.5.6), while for our purposes it is more convenient to have a height function that behaves additively. This prompts the following definitions.

Definition. The (*absolute logarithmic*) *height* on projective space is the function

$$h : \mathbb{P}^N(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}, \qquad h(P) = \log H(P).$$

Note that (VIII.5.4b) tells us that $h(P) \ge 0$ for all P.

Definition. Let E/K be an elliptic curve, and let $f \in \bar{K}(E)$ be a function. The *height on E (relative to f)* is the function

$$h_f : E(\bar{K}) \longrightarrow \mathbb{R}, \qquad h_f(P) = h\big(f(P)\big).$$

We start by transcribing the finiteness result from (VIII §5) into the current setting.

Proposition 6.1. *Let E/K be an elliptic curve, and let $f \in K(E)$ be a nonconstant function. Then for any constant C, the set*

$$\big\{P \in E(K) : h_f(P) \le C\big\}$$

is a finite set of points.

PROOF. The function $f \in K(E)$ is defined over K, so it maps points $P \in E(K)$ to points $f(P) \in \mathbb{P}^1(K)$. Hence f gives a finite-to-one map from the set in question to the set

$$\big\{Q \in \mathbb{P}^1(K) : H(Q) \le e^C\big\}.$$

Finally, we know from (VIII.5.11) that this last set is finite. □

The next theorem gives a fundamental relationship between height functions and the addition law on an elliptic curve.

Theorem 6.2. *Let E/K be an elliptic curve, and let $f \in K(E)$ be an even function, i.e., a function satisfying $f \circ [-1] = f$. Then for all $P, Q \in E(\bar{K})$ we have*

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1).$$

The constants inherent in the $O(1)$ depend on the elliptic curve E and the function f, but are independent of the points P and Q.

PROOF. Choose a Weierstrass equation for E/K of the form

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

We start by proving the theorem for the particular function $f = x$. The general case is then an easy corollary.

Since $h_x(O) = 0$ and $h_x(-P) = h_x(P)$, the desired result is clear if $P = O$ or if $Q = O$. We now assume that $P \ne O$ and $Q \ne O$, and we write

$$\begin{aligned} x(P) &= [x_1, 1], & x(Q) &= [x_2, 1], \\ x(P+Q) &= [x_3, 1], & x(P-Q) &= [x_4, 1]. \end{aligned}$$

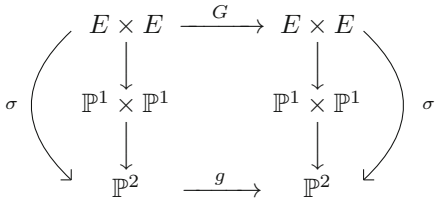
Here x_3 or x_4 may equal ∞ if $P = \pm Q$. The addition formula (III.2.3d) and a little bit of algebra yield the relations

$$x_3 + x_4 = \frac{2(x_1+x_2)(A+x_1x_2)+4B}{(x_1+x_2)^2-4x_1x_2},$$
$$x_3x_4 = \frac{(x_1x_2-A)^2-4B(x_1+x_2)}{(x_1+x_2)^2-4x_1x_2}.$$

Define a map $g : \mathbb{P}^2 \to \mathbb{P}^2$ by

$$g\big([t,u,v]\big) = \big[u^2-4tv,\, 2u(At+v)+4Bt^2,\, (v-At)^2-4Btu\big].$$

Then the formulas for x_3 and x_4 show that there is a commutative diagram



where

$$G(P,Q) = (P+Q, P-Q),$$

and where the vertical map σ is the composition of the two maps

$$E \times E \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1, \qquad (P,Q) \longmapsto \big(x(P), x(Q)\big),$$

and

$$\mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^2, \qquad \big([\alpha_1,\beta_1],[\alpha_2,\beta_2]\big) \longmapsto [\beta_1\beta_2, \alpha_1\beta_2+\alpha_2\beta_1, \alpha_1\alpha_2].$$

The idea here is that we are viewing t, u, and v as representing 1, x_1+x_2, andx_1x_2, so $g\big([t,u,v]\big)$ becomes $[1, x_3+x_4, x_3x_4]$.

The next step is to show that g is a morphism, which will allow us to apply (VIII.5.6). By definition (cf. (I.3.3)), we must show that the three homogeneous polynomials defining g have no common zeros other than $t=u=v=0$. Suppose that $g\big([t,u,v]\big)=0$. If $t=0$, then from

$$u^2-4tv=0 \qquad \text{and} \qquad (v-At)^2-4Btu=0$$

we see that $u=v=0$. Thus we may assume that $t\neq 0$, so we may define a new quantity $x=u/2t$. [*Intuition*: If we identify

$$t=1, \qquad u=x_1+x_2, \qquad v=x_1x_2,$$

then the equation $u^2-4tv=0$ becomes $(x_1-x_2)^2=0$, so $x_1=x_2=u/2t$. In other words, we are now dealing with the case that $P=\pm Q$.]

Using the new quantity x, the equation $u^2-4tv=0$ can be written as $x^2=v/t$. Now dividing the equalities

$$2u(At+v)+4Bt^2=0 \qquad \text{and} \qquad (v-At)^2-4Btu=0$$

by t^2 and rewriting them in terms of x yields the two equations

$$\psi(x) = 4x(A + x^2) + 4B = 4x^3 + 4Ax + 4B = 0,$$
$$\phi(x) = (x^2 - A)^2 - 8Bx = x^4 - 2Ax^2 - 8Bx + A^2 = 0.$$

These polynomials should be familiar, since their ratio is the rational function that appears in the duplication formula (III.2.3d). In order to show that $\psi(X)$ and $\phi(X)$ have no common root, it suffices to verify the following formal identity that we already used in the proof of (VIII.4.3),

$$(12X^2 + 16A)\phi(X) - (3X^3 - 5AX - 27B)\psi(X) = 4(4A^3 + 27B^2) \neq 0.$$

Note how the nonsingularity of the Weierstrass equation plays a crucial role here. This completes the proof that g is a morphism.

We return to our commutative diagram and compute

$$\begin{aligned} h\big(\sigma(P+Q, P-Q)\big) &= h\big(\sigma \circ G(P,Q)\big) \\ &= h\big(g \circ \sigma(P,Q)\big) \\ &= 2h\big(\sigma(P,Q)\big) + O(1) \qquad \text{from (VIII.5.6),} \end{aligned}$$

since g is a morphism of degree 2. To complete the proof of (VIII.6.2) for $f = x$, we will show that

$$h\big(\sigma(R_1, R_2)\big) = h_x(R_1) + h_x(R_2) + O(1) \qquad \text{for all } R_1, R_2, \in E(\bar{K}).$$

Then, applying this relation to each side of the equation

$$h\big(\sigma(P+Q, P-Q)\big) = 2h\big(\sigma(P,Q)\big) + O(1)$$

gives the desired result.

It is clear that if either $R_1 = O$ or $R_2 = O$, then $h\big(\sigma(R_1, R_2)\big)$ is equal to $h_x(R_1) + h_x(R_2)$. Otherwise we write

$$x(R_1) = [\alpha_1, 1] \qquad \text{and} \qquad x(R_2) = [\alpha_2, 1],$$

and then

$$h\big(\sigma(R_1, R_2)\big) = h\big([1, \alpha_1{+}\alpha_2, \alpha_1\alpha_2]\big) \quad \text{and} \quad h_x(R_1){+}h_x(R_2) = h(\alpha_1){+}h(\alpha_2).$$

We apply (VIII.5.9) to the polynomial $(T{+}\alpha_1)(T{+}\alpha_2)$ to obtain the desired estimate

$$h(\alpha_1) + h(\alpha_2) - \log 4 \le h\big([1, \alpha_1 + \alpha_2, \alpha_1\alpha_2]\big) \le h(\alpha_1) + h(\alpha_2) + \log 2.$$

Finally, in order to deal with an arbitrary even function $f \in K(E)$, we prove in the next lemma (VIII.6.3) that

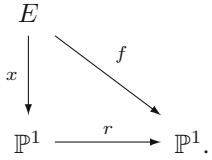
$$h_f = \frac{1}{2}(\deg f)h_x + O(1).$$

Then (VIII.6.2) follows immediately on multiplying the proven relation for h_x by $\frac{1}{2}\deg f$. □

Lemma 6.3. *Let $f, g \in K(E)$ be even functions. Then*

$$(\deg g)h_f = (\deg f)h_g + O(1).$$

PROOF. Let $x, y \in K(E)$ be Weierstrass coordinates for E/K. We know from (III.2.3.1) that the subfield of $K(E)$ consisting of even functions is exactly $K(x)$, so we can find a rational function $r(X) \in K(X)$ such that there is a commutative diagram



Hence, using (VIII.5.6) and the fact (II.2.1) that r is a morphism, we deduce that

$$h_f = h_x \circ r = (\deg r)h_x + O(1).$$

The diagram tells us that

$$\deg f = (\deg x)(\deg r) = 2\deg r,$$

so we find that

$$2h_f = (\deg f)h_x + O(1).$$

The same reasoning applied to g yields

$$2h_g = (\deg g)h_x + O(1),$$

and combining these last two equalities gives the desired result. □

Corollary 6.4. *Let E/K be an elliptic curve, and let $f \in K(E)$ be an even function.*
(a) *Let $Q \in E(\bar{K})$. Then*

$$h_f(P+Q) \le 2h_f(P) + O(1) \qquad \textit{for all } P \in E(\bar{K}),$$

where the $O(1)$ depends on E, f, and Q.
(b) *Let $m \in \mathbb{Z}$. Then*

$$h_f\big([m]P\big) = m^2 h_f(P) + O(1) \qquad \textit{for all } P \in E(\bar{K}),$$

where the $O(1)$ depends on E, f, and m.

PROOF. (a) This follows immediately from (VIII.6.2), since $h_f(P-Q) \ge 0$.
(b) Since f is even, it suffices to consider $m \ge 0$. Further, the result is trivial for $m = 0$ and $m = 1$. We use induction to complete the proof. Suppose that the desired result is known for $m-1$ and for m. Replacing P and Q in (VIII.6.2) by $[m]P$ and P, respectively, we find that

$$\begin{aligned} h_f\big([m+1]P\big) &= -h_f\big([m-1]P\big) + 2h_f\big([m]P\big) + 2h_f(P) + O(1) \\ &= \big(-(m-1)^2 + 2m^2 + 2\big)h_f(P) + O(1) \qquad \text{by the induction hypothesis,} \\ &= (m+1)^2 h_f(P) + O(1). \end{aligned}$$

This completes the induction proof. □

Remark 6.5. It is clear that (VIII.6.2), (VIII.6.3), and (VIII.6.4) are also true for odd functions f, since then f^2 is even, and it is easy to check that $h_{f^2} = 2h_f$. More generally, although we do not give the proof, our results are true for arbitrary $f \in K(E)$ to "within ϵ." Precisely, say for (VIII.6.4b), for every $\epsilon > 0$ it is true that

$$(1-\epsilon)m^2 h_f + O(1) \le h_f \circ [m] \le (1+\epsilon)m^2 h_f + O(1),$$

where now the $O(1)$ depends on E, f, m, and ϵ. See Exercise 9.14c or, for a general result, see [139, Chapter 4, Corollary 3.5].

Remark 6.6. We can interpret (VIII.6.2) as saying that the height function h_f is more or less a quadratic form. We will see later (VIII §9) that there is an actual quadratic form, called the *canonical height*, that differs from h_f by a bounded amount.

We now have all of the tools needed to complete the proof of the Mordell–Weil theorem.

Theorem 6.7. (Mordell–Weil theorem) *Let K be a number field, and let E/K be an elliptic curve. Then the group $E(K)$ is finitely generated.*

PROOF. Choose any even nonconstant function $f \in K(E)$, for example, f could be the x-coordinate on a Weierstrass equation. The Mordell–Weil theorem follows immediately from the weak Mordell–Weil theorem (VIII.1.1) with $m = 2$ and the descent theorem (VIII.3.1) as soon as we show that the height function

$$h_f : E(K) \longrightarrow \mathbb{R}$$

has the following three properties:

(i) Let $Q \in E(K)$. There is a constant C_1, depending on E, f,and Q, such that

$$h_f(P+Q) \le 2h_f(P) + C_1 \qquad \text{for all } P \in E(K).$$

(ii) There is a constant C_2, depending on E and f, such that

$$h_f\big([2]P\big) \ge 4h_f(P) - C_2 \qquad \text{for all } P \in E(K).$$

(iii) For every constant C_3, the set

$$\big\{P \in E(K) : h_f(P) \le C_3\big\}$$

is a finite set of points.

Here (i) is a restatement of (VIII.6.4a), while (ii) is immediate from the $m = 2$ case of (VIII.6.4b), and (iii) is (VIII.6.1). This completes the proof of the Mordell–Weil theorem. □

VIII.7 Torsion Points

The Mordell–Weil theorem implies that the group of rational torsion points on an elliptic curve is finite. Of course, this also follows from the corresponding result for local fields. Since we may view an elliptic curve defined over a number field K as being defined over the completion K_v for each $v \in M_K$, the local integrality conditions for torsion points (VII.3.4) can be pieced together to give the following global statement.

Theorem 7.1. *Let E/K be an elliptic curve with Weierstrass equation*

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

and assume that $a_1, \dots, a_6$ are all in the ring of integers R of K. Let $P \in E(K)$ be a torsion point of exact order $m \ge 2$.
(a) *If m is not a prime power, then*

$$x(P), y(P) \in R.$$

(b) *If $m = p^n$ is a prime power, then for each $v \in M_K^0$ we let*

$$r_v = \left[\frac{\operatorname{ord}_v(p)}{p^n - p^{n-1}} \right],$$

where $[\,\cdot\,]$ denotes the greatest integer. Then

$$\operatorname{ord}_v\big(x(P)\big) \ge -2r_v \qquad \text{and} \qquad \operatorname{ord}_v\big(y(P)\big) \ge -3r_v.$$

In particular, if $\operatorname{ord}_v(p) = 0$, then $x(P)$ and $y(P)$ are v-integral.

The next corollary was proven independently by Lutz and Nagell, who had discovered divisibility conditions somewhat weaker than those given in (VIII.7.1).

Corollary 7.2. ([152], [190]) *Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation*

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}.$$

Suppose that $P \in E(\mathbb{Q})$ is a nonzero torsion point.
(a) *$x(P), y(P) \in \mathbb{Z}$.*
(b) *Either $[2]P = O$ or else $y(P)^2$ divides $4A^3 + 27B^2$.*

PROOF. (a) Let P have exact order m. If $m = 2$, then $y(P) = 0$, so $x(P) \in \mathbb{Z}$, since it is the root of a monic polynomial with integer coefficients. If $m > 2$, the desired result follows immediately from (VIII.7.1), since the quantity r_v in (VIII.7.1b) is necessarily 0.
(b) We assume that $[2]P \ne O$, so $y(P) \ne 0$. Then applying (a) to both P and $[2]P$, we deduce that $x(P), y(P), x\big([2]P\big) \in \mathbb{Z}$. Let

$$\phi(X) = X^4 - 2AX^2 - 8BX + A^2 \qquad \text{and} \qquad \psi(X) = X^3 + AX + B.$$

Then the duplication formula (III.2.3d) reads

$$x\bigl([2]P\bigr) = \frac{\phi\bigl(x(P)\bigr)}{4\psi\bigl(x(P)\bigr)}.$$

On the other hand, we have the usual polynomial identity (VIII.4.3)

$$f(X)\phi(X) - g(X)\psi(X) = 4A^3 + 27B^2,$$

where $f(X) = 3X^2 + 4A$ and $g(X) = 3X^3 - 5AX - 27B$. Setting $X = x(P)$ and using the duplication formula and the fact that $y(P)^2 = \psi\bigl(x(P)\bigr)$ yields

$$y(P)^2\Bigl(4f\bigl(x(P)\bigr)x\bigl([2]P\bigr) - g\bigl(x(P)\bigr)\Bigr) = 4A^3 + 27B^2.$$

Since all of the quantities in this equation are integers, the desired result follows. □

Remark 7.3.1. A glance at the proof of (VIII.7.2b) shows that we have proved that any point $P \in E(\mathbb{Q})$ such that $x(P)$ and $x\bigl([2]P\bigr)$ are both integers has the property that $y(P)^2$ divides $4A^3 + 27B^2$. The same argument works for number fields. Further, even if $x(P)$ or $x\bigl([2]P\bigr)$ is not integral, any bound on their denominators, for example as in (VIII.7.1b), gives a corresponding bound for $y(P)$; see Exercise 8.11.

Remark 7.3.2. Recall from (VII.3.2) that in practice, one of the fastest methods to bound the torsion in $E(K)$ is to choose various finite places v for which E has good reduction and use the injection (VII.3.1)

$$E(K_v)[m] \hookrightarrow \tilde{E}(k_v),$$

which is valid for integers m that are prime to $\mathrm{char}(k_v)$.

Example 7.4. The Weierstrass equation

$$E : y^2 = x^3 - 43x + 166$$

has

$$4A^3 + 27B^2 = 425984 = 2^{15} \cdot 13.$$

Hence any torsion point in $E(\mathbb{Q})$ has its y-coordinate in the set

$$\{0, \pm1, \pm2, \pm4, \pm8, \pm16, \pm32, \pm64, \pm128\}.$$

A little bit of work with a calculator reveals the points

$$\bigl\{(3, \pm8),\ (-5, \pm16),\ (11, \pm32)\bigr\}.$$

On the other hand, since E has good reduction modulo 3, we know that $E_{\mathrm{tors}}(\mathbb{Q})$ injects into $\tilde{E}(\mathbb{F}_3)$ (cf. VII.3.5), and it is easy to check that $\#\tilde{E}(\mathbb{F}_3) = 7$. This still does not prove anything, since the divisibility condition in (VIII.7.2b) is only necessary, not sufficient. However, using the doubling formula for $P = (3, 8)$ yields

$$x(P) = 3, \qquad x\big([2]P\big) = -5, \qquad x\big([4]P\big) = 11, \qquad x\big([8]P\big) = 3.$$

Hence $[8]P = \pm P$, so P is a torsion point of exact order 7 or 9. (Note that it doesn't have order 3, since $x(P) \neq x\big([2]P\big)$.) From above, the only possibility is order 7, so we conclude that $E_{\text{tors}}(\mathbb{Q})$ is a cyclic group of order 7 consisting of the six listed points, together with O.

Our discussion thus far has focused on characterizing the torsion subgroup of a given elliptic curve. Another type of question that one might ask is the following: given a prime p, does there exist an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q})$ contains a point of order p? The answer for most primes is no. For example, $E(\mathbb{Q})$ can never contain a point of order 11, a fact that is by no means obvious. Such a statement, which deals uniformly with the set of all elliptic curves, naturally tends to be more difficult to prove than does a result such as (VIII.7.2) in which the bound changes as the elliptic curve is varied. The definitive characterization of torsion subgroups over $\mathbb{Q}$ is given by the following theorem due to Mazur; the proof is unfortunately far beyond the scope of this book.

Theorem 7.5. (Mazur [165], [166]) *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups*:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && \text{with } 1 \le N \le 10 \text{ or } N = 12, \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} && \text{with } 1 \le N \le 4. \end{aligned}$$

Further, each of these groups occurs as $E_{\text{tors}}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$. (*See Exercise 8.12 for an example of each possible group.*)

Mazur's theorem was generalized to number fields of degree up to 14 by Kamienny and others [2, 121, 122], and then the general case was settled by Merel.

Theorem 7.5.1. (Merel [170]) *For every integer $d \ge 1$ there is a constant $N(d)$ such that for all number fields $K/\mathbb{Q}$ of degree at most d and all elliptic curves E/K,*

$$\big|E_{\text{tors}}(K)\big| \le N(d).$$

Remark 7.6. Prior to the proof of Merel's theorem (VIII.7.5.1), Manin [155] used a completely different method to show that for any fixed prime p, the p-primary component of $E_{\text{tors}}(K)$ may be bounded in terms of K and p.

Remark 7.8. For those torsion subgroups that are allowed by Mazur's theorem (VIII.7.5), it is a classical result that the elliptic curves having the specified torsion subgroup lie in a one-parameter family. For example, the curves E/K with a point $P \in E(K)$ of order 7 all have Weierstrass equations of the form

$$y^2 + (1 + d - d^2)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2, \qquad P = (0, 0),$$

with

$$d \in K \quad \text{and} \quad \Delta = d^7(d-1)^7(d^3 - 8d^2 + 5d + 1) \neq 0.$$

See Exercise 8.13a,b for a derivation and [132] for a complete list of such formulas. In general, the elliptic curves E/K with a point $P \in E(K)$ of order $m \ge 4$ are parametrized by the K-rational points of another curve, called a *modular curve*; see Exercise 8.13c and (C §13).

VIII.8 The Minimal Discriminant

Let E/K be an elliptic curve. For each nonarchimedean absolute value $v \in M_K^0$ we choose a Weierstrass equation for E,

$$y_v^2 + a_{1,v}x_vy_v + a_{3,v}y_v = x_v^3 + a_{2,v}x_v^2 + a_{4,v}x_v + a_{6,v},$$

that is a minimal equation for E at v. In other words, all of the $a_{i,v}$ satisfy

$$\operatorname{ord}_v(a_{i,v}) \ge 0,$$

and subject to this condition, the discriminant Δ_v of the equation has valuation $\operatorname{ord}_v(\Delta_v)$ that is as small as possible.

Definition. The *minimal discriminant of* E/K, denoted by $\mathcal{D}_{E/K}$, is the (integral) ideal of K given by

$$\mathcal{D}_{E/K} = \prod_{v \in M_K^0} \mathfrak{p}_v^{\operatorname{ord}_v(\Delta_v)}.$$

Here $\mathfrak{p}_v$ is the prime ideal of R associated to v. Thus $\mathcal{D}_{E/K}$ catalogs the valuation of the minimal discriminant of E at every place $v \in M_K^0$. It measures, in some sense, the arithmetic complexity of the elliptic curve E.

We now ask whether it is possible to find a single Weierstrass equation that is simultaneously minimal for every $v \in M_K^0$. Let

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

be any Weierstrass equation for E/K, say with discriminant Δ. For each $v \in M_K^0$ we can find a change of coordinates

$$x = u_v^2x_v + r_v, \qquad y = u_v^3y_v + s_vu_v^2x_v + t_v,$$

that transforms the initial equation into an equation that is minimal at v. As usual, the discriminants of the two equations are related by

$$\Delta = u_v^{12}\Delta_v.$$

Hence if we define an ideal

$$\mathfrak{a}_\Delta = \prod_{v \in M_K^0} \mathfrak{p}_v^{-\operatorname{ord}_v(u_v)},$$

then the minimal discriminant is related to Δ via the formula

$$\mathcal{D}_{E/K} = (\Delta)\mathfrak{a}_\Delta^{12}.$$

Lemma 8.1. *With notation as above, the ideal class in K of the ideal $\mathfrak{a}_\Delta$ is independent of Δ.*

PROOF. Suppose that we take a different Weierstrass equation for E over K, say with discriminant Δ'. Then $\Delta = u^{12}\Delta'$ for some $u \in K^*$, so directly from the definitions we see that

$$(\Delta')\mathfrak{a}_{\Delta'}^{12} = \mathcal{D}_{E/K} = (\Delta)\mathfrak{a}_{\Delta}^{12} = (\Delta')\big((u)\mathfrak{a}_{\Delta}\big)^{12}.$$

Hence $\mathfrak{a}_{\Delta'} = (u)\mathfrak{a}_{\Delta}$, so $\mathfrak{a}_{\Delta'}$ and $\mathfrak{a}_{\Delta}$ are in the same ideal class. □

Definition. The *Weierstrass class of* E/K, denoted by $\bar{\mathfrak{a}}_{E/K}$, is the ideal class in K corresponding to any ideal $\mathfrak{a}_{\Delta}$ as above.

Definition. A *global minimal Weierstrass equation for* E/K is a Weierstrass equation

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

for E/K such that $a_1, a_2, a_3, a_4, a_6 \in R$ and such that the discriminant Δ of the equation satisfies $\mathcal{D}_{E/K} = (\Delta)$.

Proposition 8.2. *There exists a global minimal Weierstrass equation for* E/K *if and only if* $\bar{\mathfrak{a}}_{E/K} = (1)$.

PROOF. Suppose that E/K has a global minimal Weierstrass equation, say with discriminant Δ. Then $\mathcal{D}_{E/K} = (\Delta)$, so with notation as above, for any $v \in M_K^0$ we have

$$12\,\mathrm{ord}_v(\mathfrak{a}_{\Delta}) = \mathrm{ord}_v(\mathcal{D}_{E/K}) - \mathrm{ord}_v(\Delta) = 0.$$

Hence $\mathfrak{a}_{\Delta} = (1)$, so $\bar{\mathfrak{a}}_{E/K} = (\text{class of } \mathfrak{a}_{\Delta}) = (1)$.

Conversely, suppose that $\bar{\mathfrak{a}}_{E/K} = (1)$. Choose any Weierstrass equation for E/K having $a_1, \ldots, a_6 \in R$, and let Δ be the discriminant of this chosen equation. For each $v \in M_K^0$, let

$$x = u_v^2x_v + r_v, \qquad y = u_v^3y_v + s_vu_v^2x_v + t_v,$$

be a change of variables that produces a minimal equation at v, say with coefficients $a_{1,v}, \ldots, a_{6,v}$ and discriminant Δ_v. Letting

$$S = \big\{v \in M_K^0 : \mathrm{ord}_v(\Delta) \neq 0\big\},$$

the chosen equation is already minimal for all $v \notin S$, so we may take $u_v = 1$ and $r_v = s_v = t_v = 0$ for $v \notin S$. Note that S is a finite set. Further, from (VII.1.3d), we see that u_v, r_v, s_v, t_v are v-integral for all $v \in M_K^0$.

The assumption that $\bar{\mathfrak{a}}_{E/K} = (1)$ means that the ideal

$$\prod_{v \in M_K^0} \mathfrak{p}_v^{\mathrm{ord}_v(u_v)}$$

is principal, say generated by $u \in K^*$. This means that

$$\mathrm{ord}_v(u) = \mathrm{ord}_v(u_v) \qquad \text{for all } v \in M_K^0.$$

We use the Chinese remainder theorem [142, Chapter I, Section 4] to find elements $r, s, t \in R$ such that for all $v \in S$ we have

$$\operatorname{ord}_v(r - r_v),\ \operatorname{ord}_v(s - s_v),\ \operatorname{ord}_v(t - t_v) > \max_{i=1,2,3,4,6} \operatorname{ord}_v(u_v^i a_{i,v}).$$

Now consider the new Weierstrass equation for E/K given by the change of coordinates

$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t,$$

having coefficients $a'_1, \dots, a'_6$ and discriminant Δ'. Then $\Delta = u^{12}\Delta'$, so

$$\operatorname{ord}_v(\Delta') = \operatorname{ord}_v(u^{-12}\Delta) = \operatorname{ord}_v\big((u_v/u)^{12}\Delta_v\big) = \operatorname{ord}_v(\Delta_v).$$

Thus the discriminant of the new equation is minimal at all $v \in M_K^0$, so in order to verify that it is a global minimal equation, we must show that all of its coefficients are integral. This is easily checked using the coefficient transformation formulas Table 3.1. If $v \notin S$, then $\operatorname{ord}_v(u) = 0$, so each a'_i is v-integral since it is a polynomial in $r, s, t, a_1, \dots, a_6$. For $v \in S$ we illustrate the argument for a'_2, the other coefficients being done similarly. Thus

$$\begin{aligned}\operatorname{ord}_v(u^2a'_2) &= \operatorname{ord}_v(a_2 - sa_1 + 3r - s^2)\\ &= \operatorname{ord}_v\big(u_v^2a_{2,v} - (s - s_v)(a_1 + s + s_v) + 3(r - r_v)\big)\\ &= \operatorname{ord}_v(u_v^2a_{2,v}),\end{aligned}$$

where the last line follows from the previous one by our choice of r and s and the nonarchimedean nature of v. Since

$$\operatorname{ord}_v(u) = \operatorname{ord}_v(u_v) \qquad \text{and} \qquad \operatorname{ord}_v(a_{2,v}) \ge 0,$$

this gives the desired result. □

Corollary 8.3. *If K has class number one, then every elliptic curve E/K has a global minimal Weierstrass equation. In particular, this is true for $K = \mathbb{Q}$.*

The converse to (VIII.8.3) is also true; see Exercise 8.14.

Example 8.4. The Weierstrass equation

$$E : y^2 = x^3 + 16$$

has discriminant $\Delta = -2^{12}3^3$ and it is not minimal at 2. The substitution

$$x = 4x', \qquad y = 8y' + 4,$$

gives the global minimal equation

$$(y')^2 + y' = (x')^3.$$

Example 8.5. Let $K = \mathbb{Q}(\sqrt{-10}\,)$, so K has class number 2, the class group being generated by the prime ideal $\mathfrak{p} = (5, \sqrt{-10}\,)$. Let E/K be the elliptic curve given by the equation

$$E : y^2 = x^3 + 125.$$

This equation has discriminant $\Delta = -2^4 3^3 5^6$, so (VII.1.1) tells us that it is already minimal at every prime of K except possibly at the prime $\mathfrak{p}$ lying over (5). For $\mathfrak{p}$, the change of coordinates

$$x = (\sqrt{-10}\,)^2 x', \qquad y = (\sqrt{-10}\,)^3 y'$$

gives an equation

$$(y')^2 = (x')^3 - \frac{1}{8}$$

that has good reduction at $\mathfrak{p}$. Hence

$$\mathcal{D}_{E/K} = (2^4 3^3) \qquad \text{and} \qquad \bar{\mathfrak{a}}_{E/K} = (\text{ideal class of } \mathfrak{p}).$$

Since $\bar{\mathfrak{a}}_{E/K}$ is not principal, (VIII.8.2) tells us that E/K does not have a global minimal Weierstrass equation.

Remark 8.6. If K has class number one and E/K is an elliptic curve, then we can construct a global minimal Weierstrass equation for E/K by finding local minimal equations, e.g., by using Tate's algorithm [266, IV §9], [283], and then following the proof of (VIII.8.2). There is also an algorithm, due to Laska [146], that is fast and easy to implement on a computer.

Even if R has class number greater than one, it is often useful to know that an elliptic curve E/K has a global Weierstrass equation that is, in some sense, "almost minimal." The following proposition gives one possibility; see Exercise 8.14c for another.

Proposition 8.7. *Let $S \subset M_K$ be a finite set of absolute values containing M_K^∞ and all finite places dividing 2 and 3. Assume further that the ring of S-integers R_S is a principal ideal domain. Then every elliptic curve E/K has a Weierstrass equation of the form*

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

with $A, B \in R_S$ and discriminant $\Delta = -16(4A^3 + 27B^2)$ satisfying

$$\mathcal{D}_{E/K} R_S = \Delta R_S.$$

(*Such a Weierstrass equation might be called* S-minimal.)

PROOF. Choose any Weierstrass equation for E/K of the form

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

and let $\Delta = -16(4A^3 + 27B^2)$. For each $v \in M_K$ with $v \notin S$, choose $u_v \in K^*$ such that the substitution

$$x = u_v^2 x', \qquad y = u_v^3 y',$$

gives a minimal equation at v. Then

$$v(\mathcal{D}_{E/K}) = v(\Delta) - 12v(u_v) \qquad \text{for all } v \in M_K \text{ with } v \notin S.$$

Since R_S is a principal ideal domain, we can find an element $u \in K^*$ satisfying

$$v(u) = v(u_v) \qquad \text{for all } v \in M_K \text{ with } v \notin S.$$

Then the equation

$$E : y^2 = x^3 + u^{-4}Ax + u^{-6}B$$

has the desired property. □

VIII.9 The Canonical Height

Let E/K be an elliptic curve, and let $f \in K(E)$ be an even function. We saw in (VIII.6.1) and (VIII.6.4) that the height function h_f is more or less a quadratic form, at least "up to $O(1)$." André Néron asked whether one could find an actual quadratic form that differs from h_f by a bounded amount. He constructed such a function by writing it as a sum of "quasi-quadratic" local functions [194]. At the same time, John Tate gave a simpler global definition. In this section we describe Tate's construction. (For a discussion of local height functions, see (C §18) or [266, Chapter VI].)

Proposition 9.1. (Tate) *Let E/K be an elliptic curve, let $f \in K(E)$ be a nonconstant even function, and let $P \in E(\bar{K})$. Then the limit*

$$\frac{1}{\deg(f)} \lim_{N\to\infty} 4^{-N} h_f\big([2^N]P\big)$$

exists and is independent of f.

PROOF. We prove that the limit exists by showing that the sequence is Cauchy. Applying (VIII.6.4b) with $m = 2$, there is a constant C such that for all $Q \in E(\bar{K})$,

$$\big|h_f\big([2]Q\big) - 4h_f(Q)\big| \le C.$$

For integers $N \ge M \ge 0$ we use a telescoping sum argument to estimate

$$\begin{aligned}
&\Big|4^{-N}h_f\big([2^N]P\big) - 4^{-M}h_f\big([2^M]P\big)\Big| \\
&\qquad = \left|\sum_{n=M}^{N-1} 4^{-n-1}h_f\big([2^{n+1}]P\big) - 4^{-n}h_f\big([2^n]P\big)\right| \\
&\qquad \le \sum_{n=M}^{N-1} 4^{-n-1}\Big|h_f\big([2^{n+1}]P\big) - 4h_f\big([2^n]P\big)\Big| \\
&\qquad \le \sum_{n=M}^{N-1} 4^{-n-1}C \qquad \text{taking } Q = [2^n]P \text{ above,} \\
&\qquad \le 4^{-M}C.
\end{aligned}$$

This shows that the sequence $4^{-N}h_f\big([2^N]P\big)$ is Cauchy, hence it converges.

Next let $g \in K(E)$ be another nonconstant even function. Then from (VIII.6.3) we have

$$(\deg g)h_f = (\deg f)h_g + O(1),$$

so

$$\frac{4^{-N}h_f\big([2^N]P\big)}{\deg(f)} - \frac{4^{-N}h_g\big([2^N]P\big)}{\deg(g)} = O(4^{-N}) \xrightarrow[N\to\infty]{} 0.$$

Hence the limit does not depend on the choice of the function f. □

Definition. The *canonical* (or *Néron–Tate*) *height on* E/K, denoted by $\hat{h}$ or $\hat{h}_E$, is the function

$$\hat{h} : E(\bar{K}) \longrightarrow \mathbb{R}$$

defined by

$$\hat{h}(P) = \frac{1}{\deg(f)} \lim_{N\to\infty} 4^{-N}h_f\big([2^N]P\big),$$

where $f \in K(E)$ is any nonconstant even function.

Remark 9.2. From (VIII.9.1), the canonical height is well-defined and independent of the choice of f. We remark that some authors use a canonical height that is equal to $2\hat{h}$. This is more natural in some contexts, for example it eliminates a power of 2 in the statement of the conjecture of Birch and Swinnerton-Dyer (C.16.5).

Theorem 9.3. (Néron, Tate) *Let E/K be an elliptic curve, and let $\hat{h}$ be the canonical height on E.*

(a) *For all $P, Q \in E(\bar{K})$ we have*

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \qquad \textit{(parallelogram law)}.$$

(b) *For all $P \in E(\bar{K})$ and all $m \in \mathbb{Z}$,*

$$\hat{h}\big([m]P\big) = m^2\hat{h}(P).$$

(c) *The canonical height $\hat{h}$ is a quadratic form on E, i.e., $\hat{h}$ is an even function, and the pairing*

$$\langle\, \cdot\,,\, \cdot\,\rangle : E(\bar{K}) \times E(\bar{K}) \longrightarrow \mathbb{R},$$
$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q),$$

is bilinear.

(d) *Let $P \in E(\bar{K})$. Then $\hat{h}(P) \ge 0$, and*

$$\hat{h}(P) = 0 \quad \textit{if and only if} \quad P \textit{ is a torsion point.}$$

(*See also Exercise 8.6.*)

(e) *Let $f \in K(E)$ be an even function. Then*

$$(\deg f)\hat{h} = h_f + O(1),$$

where the $O(1)$ depends on E and f.

Further, if $\hat{h}' : E(\bar{K}) \to \mathbb{R}$ is any other function satisfying (e) *for some nonconstant even function f and satisfying* (b) *for some integer $m \ge 2$, then $\hat{h}' = \hat{h}$.*

PROOF. We start with (e) and then return to (a)–(d).

(e) In the course of proving (VIII.9.1) we found a constant C, depending on f, such that for all integers $N \ge M \ge 0$ and all points $P \in E(\bar{K})$,

$$\left|4^{-N}h_f\big([2^N]P\big) - 4^{-M}h_f\big([2^M]P\big)\right| \le 4^{-M}C.$$

Taking $M = 0$ and letting $N \to \infty$ gives the desired estimate

$$\big|(\deg f)\hat{h}(P) - h_f(P)\big| \le C.$$

(a) From (VIII.6.2) we have

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1).$$

We replace P and Q by $[2^N]P$ and $[2^N Q]$, respectively, divide by $(\deg f)4^N$, and let $N \to \infty$. The $O(1)$ term disappears and we obtain

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

(b) From (VIII.6.4b) we have

$$h_f\big([m]P\big) = m^2 h_f(P) + O(1).$$

As usual, we replace P by $[2^N]P$, divide by 4^N, and let $N \to \infty$. (Alternative proof: Use (a) and induction on m.)

(c) It is a standard fact from linear algebra that a function satisfying the parallelogram law is quadratic. For completeness, we include a proof.

Putting $P = O$ in the parallelogram law (a) shows that $\hat{h}(-Q) = \hat{h}(Q)$, so $\hat{h}$ is even. By symmetry, it suffices to prove that

$$\langle P+R, Q\rangle = \langle P, Q\rangle + \langle R, Q\rangle,$$

which in terms of $\hat{h}$ is

$$\hat{h}(P+Q+R) - \hat{h}(P+R) - \hat{h}(P+Q) - \hat{h}(R+Q) + \hat{h}(P) + \hat{h}(Q) + \hat{h}(R) = 0.$$

Four applications of the parallelogram law and the evenness of $\hat{h}$ yield

$$\begin{aligned}
\hat{h}(P+R+Q) + \hat{h}(P+R-Q) - 2\hat{h}(P+R) - 2\hat{h}(Q) &= 0,\\
\hat{h}(P-R+Q) + \hat{h}(P+R-Q) - 2\hat{h}(P) - 2\hat{h}(R-Q) &= 0,\\
\hat{h}(P-R+Q) + \hat{h}(P+R+Q) - 2\hat{h}(P+Q) - 2\hat{h}(R) &= 0,\\
2\hat{h}(R+Q) + 2\hat{h}(R-Q) - 4\hat{h}(R) - 4\hat{h}(Q) &= 0.
\end{aligned}$$

The alternating sum of these four equations is the desired result.

(d) The first conclusion is clear, since $h_f(P) \ge 0$ for all functions f and all points P, so $\hat{h}(P)$ is a limit of nonnegative values. For the second, we observe that one implication is immediate, since if P is a torsion point, then $[2^N]P$ takes on only finitely many values as N varies, so $4^{-N}h_f\big([2^N]P\big) \to 0$ as $N \to \infty$.

Conversely, let $P \in E(K')$ for some finite extension K'/K, and suppose that $\hat{h}(P) = 0$. Then

$$\hat{h}\big([m]P\big) = m^2\hat{h}(P) = 0 \qquad \text{for every integer } m,$$

so from (e) there is a constant C such that for all $m \in \mathbb{Z}$,

$$h_f\big([m]P\big) = \Big|(\deg f)\hat{h}\big([m]P\big) - h_f\big([m]P\big)\Big| \le C.$$

Thus the set $\big\{P, [2]P, [3]P, \ldots\big\}$ is contained in

$$\big\{Q \in E(K') : h_f(Q) \le C\big\}.$$

Now (VIII.6.1) tells us that this set of bounded height is a finite set, so P must have finite order.

This completes the proof of (a)–(e). Finally, to prove uniqueness, suppose that there are an integer $m \ge 2$ and a nonconstant even function f such that $\hat{h}'$ satisfies

$$\hat{h}' \circ [m] = m^2\hat{h}' \qquad \text{and} \qquad (\deg f)\hat{h}' = h_f + O(1).$$

Repeated application of the first equality yields

$$\hat{h}' \circ [m^N] = m^{2N}\hat{h}' \quad \text{for } N = 1, 2, 3, \ldots.$$

Further, since $\hat{h}$ satisfies (e), we have

$$\hat{h}' - \hat{h} = O(1).$$

Hence for any point $P \in E(\bar{K})$ we have

$$\begin{aligned}\hat{h}'(P) &= m^{-2N}\hat{h}'\big([m^N]P\big)\\ &= m^{-2N}\Big(\hat{h}\big([m^N]P\big) + O(1)\Big)\\ &= \hat{h}(P) + O(m^{-2N}) \qquad \text{since } \hat{h} \text{ satisfies (b).}\end{aligned}$$

Letting $N \to \infty$ yields $\hat{h}'(P) = \hat{h}(P)$. □

Remark 9.4. The Mordell–Weil theorem implies that $E(K) \otimes \mathbb{R}$ is a finite-dimensional real vector space, and (VIII.9.3cd) implies that $\hat{h}$ is a positive definite quadratic form on the quotient space $E(K)/E_{\text{tors}}(K)$, where $E_{\text{tors}}(K)$ denotes the torsion subgroup of $E(K)$. The quotient $E(K)/E_{\text{tors}}(K)$ sits as a lattice in the vector space $E(K) \otimes \mathbb{R}$, so it would appear to be clear that the extension of $\hat{h}$ to $E(K) \otimes \mathbb{R}$ is also positive definite. This is true, but as was pointed out by Cassels, one must use more than just (VIII.9.3cd).

Lemma 9.5. *Let V be a finite-dimensional real vector space and let $L \subset V$ be a lattice, i.e., L is a discrete subgroup of V containing a basis for V. Let $q : V \to \mathbb{R}$ be a quadratic form, and suppose that q has the following properties*:

(i) *For $P \in L$, we have $q(P) = 0$ if and only if $P = 0$.*

(ii) *For every constant C, the set*

$$\{P \in L : q(P) \le C\}$$

is finite.

Then q is positive definite on V.

PROOF. Choose a basis for V such that for a vector $\mathbf{x} = (x_1, \dots, x_r) \in V$, the quadratic form q has the form

$$q(\mathbf{x}) = \sum_{i=1}^{s} x_i^2 - \sum_{i=1}^{t} x_{s+i}^2,$$

where $s + t \le r = \dim(V)$. For the existence of such a basis, see for example [143, Chapter XV, §§3,7] or [296, §12.7]. Using this basis to identify $V \cong \mathbb{R}^n$ as $\mathbb{R}$-vector spaces, we let μ be the measure on V corresponding to the usual measure on $\mathbb{R}^n$. We apply the following basic result due to Minkowski:

> Let $B \subset V$ be a convex set that is symmetric about the origin. If $\mu(B)$ is sufficiently large, then B contains a nonzero lattice point.

For a proof of Minkowski's result, see for example [108, Theorem 447] or [142, Chapter 5, Section 3]. Now consider the set

$$B(\epsilon,\delta)=\left\{\mathbf{x}=(x_1,\dots,x_r)\in V:\sum_{i=1}^{s}x_i^2\le\epsilon\quad\text{and}\quad\sum_{i=1}^{t}x_{s+i}^2\le\delta\right\}.$$

The set $B(\epsilon,\delta)$ is convex and symmetric about the origin. Further, let

$$\lambda=\inf\bigl\{q(P):P\in L,\ P\ne0\bigr\}.$$

From (i) and (ii) we have $\lambda>0$.

Now suppose that q is not positive definite on V, so $s<r$. Then Minkowski's theorem tells us that if δ is sufficiently large, then $B\left(\frac{1}{2}\lambda,\delta\right)$ contains a nonzero lattice point P. (The volume of $B\left(\frac{1}{2}\lambda,\delta\right)$ is infinite if $s+t<r$, and it grows like $\delta^{t/2}$ as $\delta\to\infty$ if $s+t=r$.) But the point P satisfies

$$q(P)=\sum_{i=1}^{s}x_i^2-\sum_{i=1}^{t}x_{i+s}^2\le\frac{1}{2}\lambda,$$

contradicting the definition of λ. Therefore q is positive definite on V. □

Proposition 9.6. *The canonical height extends to a positive definite quadratic form on the real vector space $E(K)\otimes\mathbb{R}$.*

PROOF. We consider the lattice $E(K)/E_{\text{tors}}(K)$ inside the vector space $E(K)\otimes\mathbb{R}$ and apply (VIII.9.5) to get the desired result. Condition (i) of (VIII.9.5) is exactly (VIII.9.3cd). Condition (ii) of (VIII.9.5) follows from (VIII.9.3e), which says that bounding $\hat{h}$ is the same as bounding h_f, and then applying (VIII.6.1). □

We now have the following quantities associated to E/K:

$E(K)\otimes\mathbb{R}$	a finite-dimensional vector space.
$\hat{h}$	a positive definite quadratic form on $E(K)\otimes\mathbb{R}$.
$E(K)/E_{\text{tors}}(K)$	a lattice in $E(K)\otimes\mathbb{R}$.

In such a situation, an extremely important invariant is the volume of a fundamental domain for the lattice, computed with respect to the metric induced by the quadratic form. For example, the discriminant of a number field K is the volume of its ring of integers with respect to the quadratic form $x\mapsto\operatorname{Trace}_{K/\mathbb{Q}}(x^2)$. Similarly, the regulator of K is the volume of its unit group via the logarithm mapping and the usual metric on Euclidean space.

Definition. The *canonical height* (or *Néron–Tate*) *pairing on* E/K is the bilinear form

$$\langle\,\cdot\,,\,\cdot\,\rangle:E(\bar{K})\times E(\bar{K})\longrightarrow\mathbb{R},$$

defined by

$$\langle P,Q\rangle=\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q).$$

Definition. The *elliptic regulator of* E/K, denoted by $R_{E/K}$, is the volume of a fundamental domain for $E(K)/E_{\text{tors}}(K)$ computed using the quadratic form $\hat{h}$. In other words, choose points $P_1, \dots, P_r \in E(K)$ that generate $E(K)/E_{\text{tors}}(K)$, and then

$$R_{E/K} = \det\bigl(\langle P_i, P_j\rangle\bigr)_{\substack{1\le i\le r\\ 1\le j\le r}}.$$

(If $r = 0$, we set $R_{E/K} = 1$ by convention.)

An immediate corollary of (VIII.9.6) is the following result.

Corollary 9.7. *The elliptic regulator satisfies* $R_{E/K} > 0$.

Remark 9.8. We have defined the elliptic regulator using the absolute height, but there are situations in which it is more convenient to define the height relative to a given number field K. The regulator relative to K differs from $R_{E/K}$ by a factor of $[K : \mathbb{Q}]^r$.

Since $\hat{h}(P) > 0$ for all nontorsion points $P \in E(K)$, it is natural to ask how small $\hat{h}(P)$ can be if it is not zero. One might guess that $\hat{h}(P)$ must be large if the elliptic curve is "complicated" in some sense. The following precise conjecture is a strengthened version of a conjecture of Lang [135, page 92].

Conjecture 9.9. *Let* E/K *be an elliptic curve with* j*-invariant* j_E *and minimal discriminant* $\mathcal{D}_{E/K}$. *There is a constant* $C > 0$, *depending only on* $[K : \mathbb{Q}]$, *such that for all nontorsion points* $P \in E(K)$ *we have*

$$\hat{h}(P) > C \max\bigl\{h(j_E), \log \mathrm{N}_{K/\mathbb{Q}}\,\mathcal{D}_{E/K}, 1\bigr\}.$$

Note that the strength of the conjecture lies in the fact that the constant c is independent of both the elliptic curve E and the point P. Such estimates have applications to counting integral points on elliptic curves; see (IX.3.6). We briefly summarize what is currently known about (VIII.9.9).

Theorem 9.10. *Let* E/K, j_E, *and* $\mathcal{D}_{E/K}$ *be as in* (VIII.9.9). *Then the height inequality*

$$\hat{h}(P) > C \max\bigl\{h(j_E), \log \mathrm{N}_{K/\mathbb{Q}}\,\mathcal{D}_{E/K}, 1\bigr\}$$

is valid for the following choices of C:

(a) (Silverman [254], [260]) *Let* $\nu(E)$ *be the number of places* $v \in M_K^0$ *such that* $\mathrm{ord}_v(j_E) < 0$, *i.e., the number of primes dividing the denominator of* j_E. *Then* $C > 0$ *may be chosen to depend only on* $[K : \mathbb{Q}]$ *and* $\nu(E)$.

(b) (Hindry–Silverman [113]) *Assume that the* ABC *conjecture*[1] *is true for the field* K. *Then* $C > 0$ *may be chosen to depend only on* $[K : \mathbb{Q}]$ *and on the exponent and constant appearing in the* ABC *conjecture.*

The proof of (VIII.9.10) is beyond the scope of this book, but see Exercise 8.17 for a special case.

[1]The ABC conjecture is described in (VIII.11.4), (VIII.11.6). It suffices to assume that the ABC conjecture is true for some fixed exponent, or equivalently, that Szpiro's conjecture (VIII.11.1) is true for some fixed exponent.

VIII.10 The Rank of an Elliptic Curve

The Mordell–Weil theorem (VIII.6.7) says that the *Mordell–Weil group* $E(K)$ of an elliptic curve can be written in the form

$$E(K) \cong E_{\text{tors}}(K) \times \mathbb{Z}^r.$$

As we have seen in (VIII §7), the torsion subgroup $E_{\text{tors}}(K)$ is relatively easy to compute, both in theory and in practice. The *rank* r is much more mysterious, and an effective procedure for determining it in all cases is still being sought. There are very few general facts known concerning the rank of elliptic curves, but there are a large number of fascinating conjectures. In Chapter X we describe some of the methods that have been developed for actually computing the group $E(K)$.

The rank of a "randomly chosen" elliptic curve over $\mathbb{Q}$ tends to be quite small, and it is difficult to produce curves $E/\mathbb{Q}$ having even moderately high rank. Nonetheless, there is the following folklore conjecture:

Conjecture 10.1. *There exist elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.*

A key piece of evidence for this conjecture comes from work of Shafarevich and Tate [244], who show that the analogous result is true for function fields, i.e., with $\mathbb{Q}$ replaced by the field of rational functions $\mathbb{F}_p(T)$. The Shafarevich–Tate construction leads to curves with constant j-invariant $j_E \in \mathbb{F}_p$, but subsequent constructions by Shioda [251] for $\overline{\mathbb{F}}_p(T)$ and Ulmer [295] for $\mathbb{F}_p(T)$ give examples with nonconstant j-invariant.

Néron constructed an infinite family of elliptic curves over $\mathbb{Q}$ having rank at least 10 [192], and later authors have constructed families of rank up to 19; see for example [76, 85, 188]. Within these families, clever search techniques due to Mestre [171] and others have yielded individual curves of higher rank. For example, Elkies [76] has produced the elliptic curve

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 \\ - 2006776241557552658503320820933854275093023031217895650 2x \\ + 3448161179503055646703298569039072037485594435931918 \\ 0361266008296291939448732243429 \end{aligned}$$

with $\operatorname{rank} E(\mathbb{Q}) \ge 28$.

Attached to an elliptic curve E/K is a certain Dirichlet series $L_{E/K}(s)$ called the *L-series of E/K*; see Exercise 8.19. or (C §16). For the moment, it is enough to know that the definition of $L_{E/K}(s)$ involves only the number of points on the reductions $\tilde{E}(k_v)$ for the finite places $v \in M_K^0$. There is a famous conjecture of Birch and Swinnerton-Dyer that says that the order of vanishing of $L_{E/K}(s)$ at $s = 1$ is exactly equal to the rank of $E(K)$. The conjecture further asserts that the leading coefficient in the Taylor series expansion of $L_{E/K}(s)$ around $s = 1$ should be expressible in terms of various global arithmetic quantities associated to $E(K)$, including the elliptic regulator $R_{E/K}$. Thus in some sense, the conjecture of Birch and Swinnerton-Dyer is a local–global principle for elliptic curves, since it hypothetically shows how

information about the v-adic behavior of E for all places $v \in M_K$ determines global information such as the rank of $E(K)$ and the elliptic regulator $R_{E/K}$. For further discussion of L-series and the conjecture of Birch and Swinnerton-Dyer, including some progress toward proving it, see (C §16).

In addition to wanting an effective method for computing the rank of an elliptic curve, it would be good to have a theoretical bound for the size of a generating set. Based partly on an analogy with the problem of computing generators for the unit group in a number field and partly on a number of deep conjectures in analytic number theory, Serge Lang suggested the following estimate.

Conjecture 10.2. (Lang [138], [141, Conjecture III.6.4]) *Let $\epsilon > 0$ and let $E/\mathbb{Q}$ be an elliptic curve of rank r. Then there is a basis $P_1, \ldots, P_r$ for the free part of $E(\mathbb{Q})$ satisfying*

$$\max_{1\le i\le r} \hat{h}(P_i) \le C_\epsilon^{r^2} |\mathcal{D}_{E/\mathbb{Q}}|^{\frac{1}{12}+\epsilon}.$$

Here $\hat{h}$ is the canonical height on E (VIII §9)*, $\mathcal{D}_{E/\mathbb{Q}}$ is the minimal discriminant of $E/\mathbb{Q}$* (VIII §8)*, and C_ϵ is a constant depending only on ϵ.*

Lang's conjecture is actually more precise than (VIII.10.2); see [138] or [141, Conjecture III.6.4].

Since $\hat{h}$ is a *logarithmic* height, the conjecture says that the x-coordinates of the generators may grow exponentially with the discriminant of the curve. This is similar to the way in which the height $H(u)$ of a generator for the unit group in a real quadratic field often grows exponentially with the discriminant of the field. Of course, it is easy to chose a sequence of fields such that $H(u)$ grows polynomially, but on average, one expects the growth to be exponential. The following example of Bremner and Cassels illustrates this exponential behavior. They show that the curve

$$y^2 = x^3 + 877x$$

has rank 1 and that the x-coordinate of the smallest generator P is

$$x(P) = \left(\frac{612776083187947368101}{78841535860683900210}\right)^2.$$

We compute

$$\frac{\log \hat{h}(P)}{\log |\mathcal{D}_{E/\mathbb{Q}}|} \approx 0.158,$$

so this example is roughly in the range suggested by Lang's conjecture.

VIII.11 Szpiro's Conjecture and ABC

For ease of exposition, we restrict attention in this section to elliptic curves defined over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be such a curve, and let

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

be a global minimal Weierstrass equation (VIII.8.3) for $E/\mathbb{Q}$. The discriminant Δ_E of this equation is then the minimal discriminant of $E/\mathbb{Q}$, or, more properly, the minimal discriminant of $E/\mathbb{Q}$ is the ideal generated by Δ_E.

The primes dividing Δ_E are the primes for which E has bad reduction. There is another quantity associated to E that also encodes the primes of bad reduction. It is called the *conductor of* E and is denoted by N_E. The following definition of N_E is not quite correct, but suffices for our purposes. We write N_E as a product

$$N_E = \prod_{p \text{ prime}} p^{f_p(E)},$$

where

$$f_p(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

(For $p = 2$ or 3, if E has additive reduction, then $f_p(E)$ may be greater than 2, but in any case it always satisfies $f_3(E) \le 5$ and $f_2(E) \le 8$. See [266, IV §10] for further information about the conductor of an elliptic curve.)

Roughly speaking, the conductor N_E is the product of the primes at which E has bad reduction raised to small powers, while the discriminant Δ_E is a product of the same primes, but they may sometimes appear to large powers. A deep conjecture made by Szpiro in 1983 says that although an occasional prime may appear in Δ_E to a high power, most primes do not.

Conjecture 11.1. (Szpiro's conjecture) *For every $\epsilon > 0$ there exists a κ_ϵ such that for all elliptic curves $E/\mathbb{Q}$,*

$$|\Delta_E| \le \kappa_\epsilon N_E^{6+\epsilon}.$$

Although the statement of (VIII.11.1) seems relatively innocuous, the next result gives some indication of its strength.

Proposition 11.2. *Szpiro's conjecture* (*easily*) *implies Fermat's last theorem for all sufficiently large exponents, i.e., if n is sufficiently large, then the Fermat equation $a^n + b^n = c^n$ has no solutions with $a, b, c \in \mathbb{Z}$ and $abc \ne 0$.*

PROOF. Suppose that $a^n + b^n = c^n$ with $a, b, c \in \mathbb{Z}$ and $abc \ne 0$. We consider the elliptic curve (sometimes called a *Frey curve*)

$$E : y^2 = x(x + a^n)(x - b^n).$$

This Weierstrass equation for E has discriminant

$$\Delta_{a,b,c} = 16a^{2n}b^{2n}(a^n + b^n)^2 = 16(abc)^{2n}.$$

The minimal discriminant of $E/\mathbb{Q}$, which for notational clarity we denote by $\Delta_E^{\min}$, may be somewhat smaller than $\Delta_{a,b,c}$, but it cannot be too much smaller. More precisely, we prove below (VIII.11.3a) that the minimal discriminant of $E/\mathbb{Q}$ satisfies

$$|\Delta_E^{\min}| \ge \frac{|abc|^{2n}}{2^8}.$$

Szpiro's conjecture (VIII.11.1) relates the minimal discriminant $\Delta_E^{\min}$ to the conductor N_E, where we observe that the conductor has the trivial upper bound

$$N_E = \prod_{p|2abc} p^{f_p(E)} \le \prod_{p|2abc} p^2 \le |2abc|^2.$$

Szpiro's conjecture with $\epsilon = 1$ gives

$$\frac{|abc|^{2n}}{2^8} \le |\Delta_E^{\min}| \le \kappa N_E^7 \le \kappa |2abc|^{14}$$

for an absolute constant κ. Thus

$$|abc|^{2n-14} \le 2^{22}\kappa,$$

and since we certainly have $|abc| \ge 2$, this inequality yields an absolute upper bound for n. Hence if n is sufficiently large, then the equation $a^n + b^n = c^n$ has no solutions in nonzero integers. □

Lemma 11.3. *Let $A, B, C \in \mathbb{Z}$ be nonzero integers satisfying*

$$A + B = C \qquad \textit{and} \qquad \gcd(A, B, C) = 1,$$

and let $E/\mathbb{Q}$ be the elliptic curve

$$E : y^2 = x(x + A)(x - B).$$

(a) *The minimal discriminant Δ_E of E is given by either*

$$|\Delta_E| = 2^4|ABC|^2 \qquad \textit{or} \qquad |\Delta_E| = 2^{-8}|ABC|^2.$$

In particular,

$$|\Delta_E| \ge 2^{-8}|ABC|^2.$$

(b) *The curve E has multiplicative reduction modulo p for all odd primes dividing ABC.*

PROOF. (a) The given Weierstrass equation for E has discriminant

$$\Delta = 16A^2B^2(A + B)^2 = 16A^2B^2C^2$$

and associated quantities

$$c_4 = 16(A^2 + AB + B^2) \qquad \text{and} \qquad c_6 = -32(2A^3 + 3A^2B + 3AB^2 + 2B^3).$$

Let $x = u^2x' + r$ and $y = u^3y' + u^2sx' + t$ be a change of variables that creates a global minimal Weierstrass equation for E; see (VIII.8.3). Applying (VII.1.3d)

one prime at a time, we deduce that $u, r, s, t \in \mathbb{Z}$. The change of variable formulas in (III §1) then imply that

$$u^4 \mid c_4 \qquad \text{and} \qquad u^6 \mid c_6.$$

A simple resultant or Euclidean algorithm calculation gives the identities

$$\begin{aligned}(22A^2 - 8AB - 8B^2)c_4 + (A + 2B)c_6 &= 288A^2,\\ -(8A^2 + 8AB - 22B^2)c_4 - (2A + B)c_6 &= 288B^2.\end{aligned}$$

Hence, using the assumption that $\gcd(A, B) = 1$, we find that

$$u^4 \mid \gcd(288A^4, 288B^4) = 288 = 2^5 \cdot 3^2,$$

from which it follows that $u = 1$ or 2. Therefore the absolute value of the minimal discriminant Δ_E of $E/\mathbb{Q}$,

$$|\Delta_E| = |u^{-12}\Delta| = |u^{-12}(4ABC)^2|,$$

is equal to either $16|ABC|^2$ or $2^{-8}|ABC|^2$.
(b) We recall from (a) that the c_4 value and the discriminant Δ of the Weierstrass equation $y^2 = x(x + A)(x - B)$ are

$$c_4 = 16(A^2 + AB + B^2) \qquad \text{and} \qquad \Delta = 16A^2B^2C^2.$$

For any prime p, we have from (VII.5.1) that

$$\begin{aligned}&E \text{ has good reduction if } p \nmid \Delta,\\ &E \text{ has multiplicative reduction if } p \mid \Delta \text{ and } p \nmid c_4,\\ &E \text{ has additive reduction if } p \mid \Delta \text{ and } p \mid c_4.\end{aligned}$$

Let p be an odd prime dividing Δ. If $p \mid A$ or $p \mid B$, then the assumption that $\gcd(A, B) = 1$ implies that $p \nmid c_4$, so E has multiplicative reduction at p. Similarly, if $p \mid C$, so $A + B \equiv 0 \pmod{p}$, then $c_4 \equiv 16A^2 \pmod{p}$, and hence again $p \nmid c_4$ and E has multiplicative reduction at p. □

Szpiro's conjecture is closely related to the ABC conjecture that was proposed by Masser and Oesterlé in 1985; see [196, Part I].

The ABC Conjecture 11.4. (Masser–Oesterlé) *For every $\epsilon > 0$ there exists a constant κ_ϵ such that for all nonzero integers $A, B, C \in \mathbb{Z}$ satisfying*

$$A + B = C \qquad \textit{and} \qquad \gcd(A, B, C) = 1,$$

we have

$$\max\bigl\{|A|, |B|, |C|\bigr\} \le \kappa_\epsilon \biggl(\prod_{p \mid ABC} p\biggr)^{1+\epsilon}.$$

(*The product is over all primes dividing ABC.*)

The intuition behind the ABC conjecture is that in any sum of three relatively prime integers, it is not possible for all three terms to be divisible by many high prime powers. It is not hard to show that the ABC conjecture implies Szpiro's conjecture, and the converse is also true if one allows a slightly larger exponent.

Proposition 11.5. (a) *If Szpiro's conjecture* (VIII.11.1) *is true, then the ABC conjecture* (VIII.11.4) *is true with exponent $\frac{3}{2}$.* (*See also Exercise 8.20.*)
(b) *The ABC conjecture implies Szpiro's conjecture.*

PROOF. (a) Let A, B, C be as in the statement of the ABC conjecture. Relabeling if necessary, we may assume that $C > B > A > 0$, so in particular

$$2B > A + B = C.$$

We consider the elliptic curve

$$E : y^2 = x(x + A)(x - B).$$

From (VIII.11.3a) we know that the minimal discriminant of E satisfies

$$|\Delta_E| \ge 2^{-8}(ABC)^2.$$

On the other hand, we know from (VIII.11.3b) that E has multiplicative reduction at all odd primes of bad reduction, so directly from the definition of the conductor,

$$N_E = 2^e \prod_{\substack{p \ge 3 \\ p \mid ABC}} p \qquad \text{for some } e \le 2.$$

Applying Szpiro's conjecture to E, we deduce that for every $\epsilon > 0$ there is a $\kappa_\epsilon > 0$ such that

$$2^{-8}(ABC)^2 \le |\Delta_E| \le \kappa_\epsilon N_E^{6+\epsilon} \le \kappa_\epsilon 2^{12+2\epsilon} \prod_{p \mid ABC} p^{6+\epsilon}.$$

Using the fact that $A \ge 1$ and $B > \frac{1}{2}C$ yields

$$2^{-10}C^4 \le \kappa_\epsilon 2^{12+2\epsilon} \prod_{p \mid ABC} p^{6+\epsilon},$$

and taking fourth roots gives the ABC conjecture with exponent $\frac{3}{2}$.
(b) Let $E/\mathbb{Q}$ be an elliptic curve given by a minimal Weierstrass equation. Then as described in (III §2), the discriminant and associated quantities c_4 and c_6 are related by the formula

$$1728\Delta = c_4^3 - c_6^2.$$

We will prove (b) under the assumption that $\gcd(c_4^3, c_6^2) = 1$ and leave the general case as an exercise for the reader; see Exercise 8.21. This assumption allows us to apply the ABC conjecture with

$$A = c_4^3, \qquad B = -c_6^2, \qquad \text{and} \qquad C = 1728\Delta,$$

which yields

$$\max\bigl\{|c_4^3|, |c_6^2|, |1728\Delta|\bigr\} \le \kappa_\epsilon \prod_{p \mid 6c_4c_6\Delta} p^{1+\epsilon}.$$

The product on the right is clearly smaller than $|6c_4c_6N_E|^{1+\epsilon}$, so we obtain the following three inequalities:

$$\begin{aligned} |c_4|^{2-\epsilon} &\le \kappa_\epsilon |6c_6N_E|^{1+\epsilon}, \\ |c_6|^{1-\epsilon} &\le \kappa_\epsilon |6c_4N_E|^{1+\epsilon}, \\ |1728\Delta| &\le \kappa_\epsilon |6c_4c_6N_E|^{1+\epsilon}. \end{aligned}$$

We are going to take an appropriate (multiplicative) linear combination of these inequalities to eliminate c_4 and c_6. To do this, we raise the first inequality to the $2+2\epsilon$ power, raise the second inequality to the $3+3\epsilon$ power, raise the third inequality to the $1-5\epsilon$ power, and multiply the resulting three inequalities. Canceling $|c_4|^{4+2\epsilon-2\epsilon^2}|c_6|^{3-3\epsilon^2}$ from both sides yields

$$|1728\Delta|^{1-5\epsilon} \le \kappa_\epsilon^6 (6N_E)^{6+6\epsilon}.$$

This is Szpiro's conjecture, up to adjusting the ϵ. □

Remark 11.6. It is not difficult to formulate versions of Szpiro's conjecture and the ABC conjecture over a number fields. For example, if E/K is an elliptic curve defined over a number field K, we define the (naive) conductor of E/K to be the ideal

$$\mathfrak{N}_{E/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(E)},$$

where $f_{\mathfrak{p}}(E)$ is 0, 1, or 2 according to whether E has good, multiplicative, or additive reduction at $\mathfrak{p}$. Then Szpiro's conjecture says that for every $\epsilon > 0$ there is a constant $\kappa = \kappa(\epsilon, K)$, depending only on ϵ and K, such that

$$\mathrm{N}_{K/\mathbb{Q}}\, \mathcal{D}_{E/K} \le \kappa (\mathrm{N}_{K/\mathbb{Q}}\, \mathfrak{N}_{E/K})^{6+\epsilon}.$$

Next suppose that $A, B, C \in R_K$ satisfy $A + B = C$. Then the ABC conjecture says that for every $\epsilon > 0$ there is a constant $\kappa = \kappa(\epsilon, K)$, depending only on ϵ and K, such that

$$H_K\bigl([A,B,C]\bigr) \le \kappa \prod_{\mathfrak{p} \mid ABC} (\mathrm{N}_{K/\mathbb{Q}}\, \mathfrak{p})^{1+\epsilon}.$$

(There is no relative primality condition on A, B, and C, since any common "factors" leave the left-hand side unchanged while increasing the right-hand side.)

It is very interesting to ask how the constants κ appearing in these conjectures depend on the field K.

Remark 11.7. Let k be a field of characteristic 0. There are analogues of Szpiro's conjecture and the ABC conjecture in which $\mathbb{Q}$ is replaced by a rational function field $k(T)$, or more generally, the number field K is replaced by the function field $k(C)$ of an algebraic curve C. Somewhat surprisingly, both conjectures are quite easy to prove in the function field setting, and indeed considerably stronger results are known. For example, the three-term sum in the ABC conjecture may be replaced by a sum having more terms. See [157, 258, 278] for $A + B = C$ and [31, 158, 300] for $A_1 + \cdots + A_n = 0$.

Remark 11.8. Frey has noted that Szpiro's conjecture (VIII.11.1) implies the uniform boundedness of torsion on elliptic curves (VIII.7.5), (VIII.7.5.1). The idea is as follows. Suppose that $P \in E(K)$ is a point of exact order N, and let $\phi : E \to E'$ be the isogeny whose kernel is the subgroup generated by P. Assuming that N is sufficiently large (depending only on the field K), an elementary calculation using Tate curves (see (C §14) or [266, Chapter V]) shows that there are ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that the minimal discriminants of E and E' have the form

$$\mathcal{D}_E = \mathfrak{a}\mathfrak{b}^N \qquad \text{and} \qquad \mathcal{D}_{E'} = \mathfrak{a}^N\mathfrak{b}.$$

Since the primes of bad reduction divide the discriminant, we see that the conductors $\mathfrak{N}_E$ and $\mathfrak{N}_{E'}$ divide $\mathfrak{a}^2\mathfrak{b}^2$. We apply Szpiro's conjecture to E and E' to obtain

$$\mathrm{N}_{K/\mathbb{Q}}(\mathcal{D}_E\mathcal{D}_{E'}) \le \kappa_\epsilon \,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{N}_E\mathfrak{N}_{E'})^{6+\epsilon},$$

and then substituting the discriminants' and conductors' values gives

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{b})^{N+1} \le \kappa_\epsilon \,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{b})^{12+2\epsilon}.$$

Discarding the finitely many elliptic curves defined over K with everywhere good reduction (IX.6.1), we may assume that $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{b}) \ge 2$, and then the last inequality gives a bound for N that is independent of the curve E. See [89, 90, 113] for further details.

Exercises

8.1. Let E/K be an elliptic curve, let $m \ge 2$ be an integer, let $\mathcal{H}_K$ be the ideal class group of K, and let

$$S = \{v \in M_K^0 : E \text{ has bad reduction at } v\} \cup \{v \in M_K^0 : v(m) \ne 0\} \cup M_K^\infty.$$

Assume that $E[m] \subset E(K)$. Prove the following quantitative version of the weak Mordell–Weil theorem:

$$\mathrm{rank}_{\mathbb{Z}/m\mathbb{Z}}\, E(K)/mE(K) \le 2\#S + 2\,\mathrm{rank}_{\mathbb{Z}/m\mathbb{Z}}\, \mathcal{H}_K[m].$$

8.2. For each integer $d \ge 1$, let E_d be the elliptic curve

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

Prove that

$$E_d(\mathbb{Q}) \cong (\text{finite group}) \times \mathbb{Z}^r$$

for an integer r satisfying

$$r \le 2\nu(2d),$$

where $\nu(N)$ denotes the number of distinct primes dividing N. (*Hint*. Use Exercise 8.1.)

8.3. Let E/K be an elliptic curve and let L/K be an (infinite) algebraic extension. Suppose that the rank of $E(M)$ is bounded as M ranges over all finite extensions M/K such that M is contained in L, i.e., assume that

$$\sup_{\substack{K\subset M\subset L\\ [M:K]\ \text{finite}}} \operatorname{rank} E(M)$$

is finite.

(a) Prove that $E(L)\otimes\mathbb{Q}$ is a finite-dimensional $\mathbb{Q}$-vector space.

(b) Assume further that L/K is Galois and that $E_{\text{tors}}(L)$ is finite. Prove that $E(L)$ is finitely generated.

8.4. Assume that $\boldsymbol{\mu}_m \subset K$. Prove that the maximal abelian extension of K of exponent m is the field

$$K(a^{1/m} : a \in K).$$

(*Hint*. Use (VIII.2.2), which in this case says that every homomorphism $\chi : G_{\bar K/K} \to \boldsymbol{\mu}_m$ has the form $\chi(\sigma) = \alpha^\sigma/\alpha$ for some $\alpha \in \bar K^*$ satisfying $\alpha^m \in K$.)

8.5. Let $\xi \in H^1(G_{\bar K/K}, M)$ be unramified at v. Prove that the cohomology class of ξ contains a 1-cocycle $c : G_{\bar K/K} \to M$ satisfying $c_\sigma = 0$ for all $\sigma \in I_v$. (*Hint*. Use the inflation–restriction sequence (B.2.4) for $I_v \subset G_{\bar K/K}$.)

8.6. Prove *Kronecker's theorem*: Let $x \in \bar{\mathbb{Q}}^*$. Then $H(x) = 1$ if and only if x is a root of unity. (This is the multiplicative group version of (VIII.9.3d).)

8.7. (a) Give an explicit upper bound, in terms of N, C, and d, for the number of points in the set

$$\bigl\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \le C \text{ and } \bigl[\mathbb{Q}(P) : \mathbb{Q}\bigr] \le d\bigr\}.$$

(b) Let

$$\nu_K(N, C) = \#\bigl\{P \in \mathbb{P}^N(K) : H_K(P) \le C\bigr\}.$$

Prove that

$$\lim_{C\to\infty} \frac{\nu_{\mathbb{Q}}(N, C)}{C^{N+1}} = \frac{2^N}{\zeta(N+1)},$$

where $\zeta(s)$ is the Riemann zeta function. (For further information about $\nu_K(N, C)$, see (VIII.5.12).)

8.8. Prove the following basic properties of height functions.

(a) $H(x_1x_2\cdots x_N) \le H(x_1)H(x_1)\cdots H(x_N)$.

(b) $H(x_1 + x_2 + \cdots + x_N) \le NH(x_1)H(x_2)\cdots H(x_N)$.

(c) For $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\bar{\mathbb{Q}})$ and $Q = [y_0, \dots, y_M] \in \mathbb{P}^M(\bar{\mathbb{Q}})$, define

$$P \star Q = [x_0y_0, x_0y_1, \dots, x_iy_j, \dots, x_Ny_M] \in \mathbb{P}^{MN+M+N}(\bar{\mathbb{Q}}).$$

Prove that

$$H(P \star Q) = H(P)H(Q).$$

(The map $(P, Q) \mapsto P \star Q$ is the *Segre embedding* of $\mathbb{P}^N \times \mathbb{P}^M$ into $\mathbb{P}^{MN+M+N}$. See [111, exercise I.2.14].)

(d) Let $M = \binom{N+d}{N} - 1$ and let $f_0(X), \dots, f_M(X)$ be the M distinct monomials of degree d in the $N+1$ variables $X_0, \dots, X_N$. For any point $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\bar{\mathbb{Q}})$, let

$$P^{(d)} = \big[f_0(P), \dots, f_M(P)\big] \in \mathbb{P}^M(\bar{\mathbb{Q}}).$$

Prove that

$$H(P^{(d)}) = H(P)^d = H\big([x_0^d, \dots, x_N^d]\big).$$

(The map $P \mapsto P^{(d)}$ is the *d-uple embedding* of $\mathbb{P}^n$ into $\mathbb{P}^M$. See [111, exercise I.2.12].)

8.9. Let $x_0, \dots, x_N \in K$ and let $\mathfrak{b}$ be the fractional ideal of K generated by $x_0, \dots, x_N$. Prove that

$$H_K\big([x_0, \dots, x_N]\big) = \big(\mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{b}\big)^{-1} \prod_{v \in M_K^\infty} \max_{0 \le i \le N} \big\{|x_i|_v\big\}^{n_v}.$$

8.10. Let F be the rational map

$$F : \mathbb{P}^2 \longrightarrow \mathbb{P}^2, \qquad [x, y, z] \longmapsto [x^2, xy, z^2],$$

from (I.3.6). Note that F is a morphism at every point except at $[0, 1, 0]$, where it is not defined. Prove that there are infinitely many points $P \in \mathbb{P}^2(\mathbb{Q})$ such that

$$H\big(F(P)\big) = H(P).$$

In particular, (VIII.5.6) is false if the map F is merely required to be a rational map.

8.11. Prove the following generalization of (VIII.7.2) to arbitrary number fields. Let E/K be an elliptic curve given by an equation

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

with $A, B \in R$, and let $\Delta = 4A^3 + 27B^2$. Let $P \in E(K)$ be a point of exact order $m \ge 3$, and let $v \in M_K^0$.

(a) If $m = p^n$ is a prime power, prove that

$$-6r_v \le \mathrm{ord}_v\big(y(P)^2\big) \le 6r_v + \mathrm{ord}_v(\Delta),$$

where

$$r_v = \left\lfloor \frac{\mathrm{ord}_v(p)}{p^n - p^{n-1}} \right\rfloor.$$

(b) If $m = 2p^n$ is twice a prime power, prove that

$$0 \le \mathrm{ord}_v\big(y(P)^2\big) \le 2r_v + \mathrm{ord}_v(\Delta),$$

where r_v is as in (a).

(c) If m is not of the form p^n or $2p^n$, prove that

$$0 \le \operatorname{ord}_v\bigl(y(P)^2\bigr) \le \operatorname{ord}_v(\Delta).$$

8.12. Calculate $E(\mathbb{Q})_{\text{tors}}$ for each of the following elliptic curves.

(a) $y^2 = x^3 - 2$
(b) $y^2 = x^3 + 8$
(c) $y^2 = x^3 + 4$
(d) $y^2 = x^3 + 4x$
(e) $y^2 - y = x^3 - x^2$
(f) $y^2 = x^3 + 1$
(g) $y^2 = x^3 - 43x + 166$
(h) $y^2 + 7xy = x^3 + 16x$
(i) $y^2 + xy + y = x^3 - x^2 - 14x + 29$
(j) $y^2 + xy = x^3 - 45x + 81$
(k) $y^2 + 43xy - 210y = x^3 - 210x^2$
(l) $y^2 = x^3 - 4x$
(m) $y^2 = x^3 + 2x^2 - 3x$
(n) $y^2 + 5xy - 6y = x^3 - 3x^2$
(o) $y^2 + 17xy - 120y = x^3 - 60x^2$

8.13. (a) Let E/K be an elliptic curve and let $P \in E(K)$ be a point of order at least 4. Prove that there is a change of coordinates such that E has a Weierstrass equation of the form

$$E : y^2 + uxy + vy = x^3 + vx^2$$

with $u, v \in K$ and $P = (0, 0)$.

(b) Prove that there is a one-parameter family of elliptic curves E/K having a K-rational point of order 6. (*Hint*. Set $[3]P = [-3]P$ in (a) and find a relation between u and v.) Same question for points of order 7, order 9, and order 12.

(c) Prove that the elliptic curves E/K having a K-rational point of order 11 are parametrized by the K-rational points of a certain curve of genus one.

8.14. (a) Generalize (VIII.8.2) as follows. Let E/K be an elliptic curve, and let $\mathfrak{a}$ be an *integral* ideal in $\bar{\mathfrak{a}}_{E/K}^{-1}$, i.e., in the inverse of the ideal class $\bar{\mathfrak{a}}_{E/K}$. Prove that there is a Weierstrass equation of E/K having coefficients $a_i \in R$ and discriminant Δ satisfying

$$(\Delta) = \mathcal{D}_{E/K}\mathfrak{a}^{12}.$$

(b) Suppose that E/K has everywhere good reduction and that the class number of K is relatively prime to 6. Prove that E/K has a global minimal Weierstrass equation.

(c) Prove that every elliptic curve E/K has a Weierstrass equation with coefficients $a_i \in R$ and discriminant Δ satisfying

$$|\,\mathrm{N}_{K/\mathbb{Q}}\,\Delta| \le |\,\mathrm{Disc}\,K/\mathbb{Q}|^6\,|\,\mathrm{N}_{K/\mathbb{Q}}\,\mathcal{D}_{E/K}|.$$

Qualitatively, this says that there is a Weierstrass equation for E whose nonminimality is bounded solely in terms of K. Such an equation might be called *quasiminimal*.

(d) Let $\bar{\mathfrak{b}}$ be an ideal class of K. Prove that there is an elliptic curve E/K such that $\bar{\mathfrak{a}}_{E/K} = \bar{\mathfrak{b}}$. In particular, if K does not have class number one, then there exist elliptic curves over K that do not have global minimal Weierstrass equations. This gives a converse to (VIII.8.3). (See also [15] for an estimate of how many E/K have $\bar{\mathfrak{a}}_{E/K}$ equal to $\bar{\mathfrak{b}}$.)

8.15. Prove that there are no elliptic curves $E/\mathbb{Q}$ having everywhere good reduction.
(*Hint*. Suppose that there is a Weierstrass equation with integer coefficients and discriminant $\Delta = \pm 1$. Use congruences modulo 8 to show that a_1 is odd, and hence $c_4 \equiv 1 \pmod 8$. Substitute $c_4 = u \pm 12$ into the formula $c_4^3 - c_6^2 = \pm 1728$. Show that u is either a square or three times a square. Rule out both cases by reducing modulo 8.)

8.16. Show that the conclusion of (VIII.9.5) is false if the quadratic form q is not required to satisfy the finiteness condition (ii).

8.17. Fix nonzero integers A and B with $4A^3+27B^2 \neq 0$. For each integer $d \neq 0$, let $E_d/\mathbb{Q}$ be the elliptic curve

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

Assuming that d is squarefree, prove the following properties of E_d:

(a) j_E is independent of d.

(b) $\log|\mathcal{D}_{E/\mathbb{Q}}| = 6\log|d| + O(1)$.

(c) Every $P \in E_d(\mathbb{Q})$ satisfies either $[2]P = 0$ or $\hat{h}(P) > \frac{1}{8}\log|d| + O(1)$.

(d) For all but finitely many squarefree integers d, the torsion subgroup of $E_d(\mathbb{Q})$ is one of $\{0\}$, $\mathbb{Z}/2\mathbb{Z}$, and $(\mathbb{Z}/2\mathbb{Z})^2$.

Note that the $O(1)$ bounds in (b) and (c) may depend on A and B, but they should be independent of d. In particular, (c) provides a proof of (VIII.9.9) for the family of curves E_d. (*Hint for* (c). If $P = (r,s) \in E_d(\mathbb{Q})$, then $P' = (r/d, s/d^{3/2}) \in E_1(\bar{\mathbb{Q}})$. Prove the following facts: (i) $\hat{h}(P) = \hat{h}(P')$; (ii) either $s = 0$ or $h_y(P')$ is greater than $\frac{3}{8}\log|d|$; and (iii) $|\hat{h} - \frac{1}{3}h_y|$ is bounded.)

8.18. Let E/K be an elliptic curve given by a Weierstrass equation

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

(a) Prove that there are *absolute constants* c_1 and c_2 such that for all points $P \in E(\bar{K})$ we have

$$\bigl|h_x\bigl([2]P\bigr) - 4h_x(P)\bigr| \le c_1 h\bigl([A,B,1]\bigr) + c_2.$$

Find explicit values for c_1 and c_2. (*Hint*. Combine the proofs of (VIII.4.2) and (VIII.5.6), keeping track of the dependence on the constants. In particular, note that the use of the Nullstellensatz in (VIII.5.6) can be replaced by the explicit identities given in (VIII.4.3).)

(b) Find *absolute constants* c_3 and c_4 such that for all points $P \in E(\bar{K})$ we have

$$\left|\frac{1}{2}h_x(P) - \hat{h}(P)\right| \le c_3 h\bigl([A,B,1]\bigr) + c_4.$$

(*Hint*. Use (a) and the proof of (VIII.9.1).)

(c) Prove that for all integers $m \ge 1$ and all points $P, Q \in E(\bar{K})$ we have

$$\bigl|h_x\bigl([m]P\bigr) - m^2h_x(P)\bigr| \le 2(m^2+1)\bigl(c_3h\bigl([A,B,1]\bigr) + c_4\bigr)$$

and

$$h_x(P+Q) \le 2h_x(P) + 2h_x(Q) + 5\bigl(c_3h\bigl([A,B,1]\bigr) + c_4\bigr).$$

(*Hint*. Use (b) and (VIII.9.3).)

(d) Let $Q_1, \ldots, Q_r \in E(K)$ be a set of generators for $E(K)/2E(K)$. Find *absolute constants* c_5, c_6, and c_7 such that the set of points $P \in E(K)$ satisfying

$$h_x(P) \le c_5 \max_{1\le i\le r} h_x(Q_i) + c_6h\bigl([A,B,1]\bigr) + c_7$$

contains a complete set of generators for $E(K)$. (*Hint*. Follow the proof of (VIII.3.1), using (c) to evaluate the constants that appear.)

8.19. *The L-Series Attached to an Elliptic Curve.* Let $E/\mathbb{Q}$ be an elliptic curve and choose a global minimal Weierstrass equation for $E/\mathbb{Q}$,

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

(See (VIII.8.3).) For each prime p, let $\tilde{E}$ denote the reduction of the Weierstrass equation modulo p, and let

$$t_p = p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

The *L-series associated to* $E/\mathbb{Q}$ is defined by the Euler product

$$L_E(s) = \prod_{p|\Delta(E)} (1 - t_p p^{-s})^{-1} \prod_{p\nmid\Delta(E)} (1 - t_p p^{-s} + p^{1-2s})^{-1}.$$

(a) If $L_E(s)$ is expanded as a Dirichlet series $\sum c_n n^{-s}$, show that for all primes p, its p^{th} coefficient satisfies $c_p = t_p$.

(b) If E has bad reduction at p, so $p \mid \Delta(E)$, prove that t_p equals 1, -1, or 0 according to whether the reduced curve $\tilde{E} \pmod p$ has a node with tangents whose slopes are rational over $\mathbb{F}_p$ (split multiplicative reduction), a node with tangents whose slopes are quadratic over $\mathbb{F}_p$ (nonsplit multiplicative reduction), or a cusp (additive reduction). (Cf. Exercise 3.5).

(c) Prove that the Euler product for $L_E(s)$ converges for all $s \in \mathbb{C}$ with $\operatorname{Re}(s) > \frac{3}{2}$. (*Hint.* Use (V.1.1).)

There are many important theorems and conjectures concerning the L-series of elliptic curves; see (C §16).

8.20. We proved in (VIII.11.5a) that Szpiro's conjecture implies a weaker form of the ABC conjecture with exponent $\frac{3}{2}$. This exercise explains how to reduce the exponent to $\frac{6}{5}$.

Relabeling A, B, C if necessary, we may assume that $C > B > A > 0$. Let E be the curve $y^2 = x(x + A)(x - B)$ used in the proof of (VIII.11.5a).

(a) Prove that there is an isogeny of degree 2 from E to the elliptic curve

$$E' : y^2 = x^3 - 2(A - B)x^2 + C^2x.$$

Show that the discriminant of the equation for E' is $\Delta' = -2^8ABC^4$.

(b) Prove a version of (VIII.11.3) for E'. In particular, prove that E' has multiplicative reduction modulo p for all odd primes dividing ABC and that its minimal discriminant satisfies

$$|\Delta_{E'}| \ge 2^{-28}|ABC^4|.$$

(c) Apply Szpiro's conjecture to E' and deduce that

$$C \le \kappa_\epsilon \prod_{p|ABC} p^{\frac{6}{5}+\epsilon},$$

where the constant κ_ϵ depends only on ϵ.

8.21. We proved (VIII.11.5b) that the ABC conjecture (VIII.11.4) implies Szpiro's conjecture (VIII.11.1) under the assumption that $\gcd(c_4, c_6) = 1$. Prove that this implication is still true when $\gcd(c_4, c_6) > 1$. (*Hint.* Let $G = \gcd(c_4^3, c_6^2)$ and apply the ABC conjecture with $A = c_4^3/G$, $B = -c_6^2/G$, and $C = \Delta/G$. Use the minimality of the equation to bound the powers of the primes p dividing G. Also show that if $p \ge 5$ divides G, then E has additive reduction at p, so $p^2 \mid N_E$.)

8.22. Let m, n, ℓ be positive integers and consider the equation

$$x^m + y^n = z^\ell. \tag{$*$}$$

Assuming the ABC conjecture (VIII.11.4), prove the following two statements (see also Exercise 9.17):

(a) If $m^{-1} + n^{-1} + \ell^{-1} < 1$, then ($*$) has only finitely many solutions $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$.

(b) There is a constant κ', depending only on the constant appearing in the ABC conjecture, such that if ($*$) has a solution in relatively prime integers satisfying $|x|, |y|, |z| \ge 2$, then

$$\max\{m, n, \ell\} \le \kappa'.$$

8.23. Let $A, B, C \in \mathbb{Z}$ be as in the statement of the ABC conjecture (VIII.11.4), and let

$$E : y^2 = x(x + A)(x - B)$$

be the elliptic curve used in the proof of (VIII.11.5a). Assume further that

$$A \equiv 0 \pmod{16} \qquad \text{and} \qquad B \equiv 3 \pmod{4}.$$

(a) Prove that the substitutions $x \mapsto 4x$ and $y \mapsto 8y + 4x$ give a global minimal Weierstrass equation for E,

$$y^2 + xy = x^3 + \frac{A - B - 1}{4}x^2 - \frac{AB}{16}x.$$

(b) Verify that the Weierstrass equation in (a) satisfies

$$c_4 = A^2 + AB + B^2, \quad c_6 = \frac{(B - A)(A + C)(B + C)}{2}, \quad \text{and} \quad \Delta = \left(\frac{ABC}{16}\right)^2.$$

(c) Prove that E has multiplicative reduction for every prime p dividing Δ.