Towards Mordell's Theorem: The Finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$

Seminar Paper by Jonathan Weinberger
February 7, 2011 (Talk given on January 13)

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Mathematik
AG Algebra, Geometrie und Funktionalanalysis

Prof. Dr. Nils Scheithauer
Seminar "Elliptic Curves"

Contents

Abstract

In this seminar paper we prove the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$. Here, $E(\mathbb{Q})$ denotes the group of rational points of an elliptic curve E over $\mathbb{Q}$. These statements can be used to prove Mordell's Theorem that $E(\mathbb{Q})$ is finitely generated. Structure and methods are according to [1, Chapter IV, Sections 3, 4 and 9].

Overview

The Case $E(\mathbb{Q})/2E(\mathbb{Q})$ for Rational Roots

Let E be an elliptic curve over $\mathbb{Q}$. By $E(\mathbb{Q})$ we denote the group of rational points of E and by $2E(\mathbb{Q})$ the set of doubled rational points on $E(\mathbb{Q})$. In Section 1 we prove the finiteness of the factor group $E(\mathbb{Q})/2E(\mathbb{Q})$ if the zeros of the polynomial describing E are rational. This will be done by identifying $E(\mathbb{Q})/2E(\mathbb{Q})$ as a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. The homomorphisms to achieve this identification are defined by purely number-theoretic motivation, especially the characterization of the points in $2E(\mathbb{Q})$, [1, cf. Chapter IV.2]. Using unique prime decomposition, the group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ can conviently be represented as an infinite direct sum of $\mathbb{Z}/2\mathbb{Z}$. Then, the embedding of $E(\mathbb{Q})/2E(\mathbb{Q})$ turns out to restrict only to finitely many coordinates with respect to the discriminant of E. Finally, $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

The Case $E(K)/2E(K)$ for General Roots

In Section 2 we prove the more general case that the zeros of the polynomial describing E may have to be adjoined. We thus pass to the splitting field $K/\mathbb{Q}$. Then there is a homomorphism $E(\mathbb{Q})/2E(\mathbb{Q}) \to E(K)/2E(K)$. A combinatorial argument involving the Galois group of $K/\mathbb{Q}$ shows that the kernel is finite. Hence, if $E(K)/2E(K)$ is finite, $E(\mathbb{Q})/2E(\mathbb{Q})$ must be, too.

To establish the finiteness of $E(K)/2E(K)$, we basically imitate the methods used in the first section, but certain obstructions appear. The convenient representation of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ relies on the unique prime decomposition in $\mathbb{Z}$ and the „smallness" of the group of units $\mathbb{Z}^\times = \{\pm 1\}$. In terms of algebraic number theory, $\mathbb{Z}$ is the ring of integers of $\mathbb{Q}$, so we pass to the ring of integers $\mathcal{O}_K$ of K whose structure we would like to control. But in general $\mathcal{O}_K$ fails to be a unique factorization domain.

Thus, we consider a certain ring extension $\mathcal{O}_K \subset R \subset K$ which satisfies our needs. The ring R is constructed using the finiteness of the class number. Then R turns out to be a unique factorization domain. Furthermore, Dirichlet's Theorem tells that the group of units $\mathcal{O}_K^\times$ is finitely generated from which we derive that the same holds for $R^\times$. Still, the quotient field of R is K and using both of the structure results mentioned above, we obtain the desired embedding of $E(K)/2E(K)$ into $K/(K^\times)^2 \times K/(K^\times)^2$.

A further treatment on the techniques from algebraic number theory can be found in [2].

Application to Mordell's Theorem

The result is a key ingredient in the proof of *Mordell's theorem* which states that $E(\mathbb{Q})$ is finitely generated. Our result is used in the following way. One introduces a so-called height function $h\colon E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ satisfying the descent equation $h(P/2) = 1/4 \cdot h(P)$. There is a constant C such that the set $S_C := \{P \in E(\mathbb{Q})\colon h(P) \leq C\}$ contains representatives from all finitely many elements from $E(\mathbb{Q})/2E(\mathbb{Q})$. Then S_C is a generating set of $E(\mathbb{Q})$ as can be proven by the descent equation and some further relations involving the height function.

Generalization to the Mordell-Weil Theorem

In fact, even far more general statements are true. The so-called *Mordell-Weil theorem* says that $E(K)$ is finite for an elliptic curve E over an arbitrary number field K, i.e. a finite extension $K/\mathbb{Q}$. Again, the main parts are a descent method and the *weak Mordell-Weil theorem*: $E(K)/mE(K)$ is finite for any integer $m \geq 2$. Here, the proofs invoke further techniques from algebraic number theory such as valuation theory, Kummer theory or cohomology. For the treatment of these and similar generalizations see [3].

1 The Case $E(\mathbb{Q})/2E(\mathbb{Q})$ for Rational Roots

Let E denote an elliptic curve over $\mathbb{Q}$. By an admissible change of variables we may assume that E is given by

$$E\colon y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

with integer coefficents. As E is a non-singular cubic, the polynomial discriminant $d = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$ must not equal 0, hence the roots α, β, γ have to be pairwisely distinct.

In this section we consider the case where the algebraic integers α, β, γ are rational, therefore already integers.

By $E(\mathbb{Q})$ we denote the set of rational points on E and define

$$2E(\mathbb{Q}) := \{P + P\colon P \in E(\mathbb{Q})\}.$$

We are going to identitfy $E(\mathbb{Q})/2E(\mathbb{Q})$ with a subgroup of the factor group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ where

$$(\mathbb{Q}^\times)^2 := \{r^2\colon r \in \mathbb{Q}^\times\}.$$

Therefore we need a standard picture for the latter group.

We have identifications

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \cong \left\{(\sigma, 2^a, 3^b, 5^c, 7^d, \ldots)\colon \sigma \in \{\pm 1\}, a, b, c, d, \ldots \in \{0,1\}\right\} \cong \bigoplus_{\pm,\, p \text{ prime}} \mathbb{Z}/2\mathbb{Z},$$

i.e. the elements of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ can be represented by the square-free integers. This can be seen as follows. Given a rational number a/b with coprime a and b, we can multiply it by $\operatorname{sgn}(a/b)r^{-1}$ where r is the product of primes occuring in a or b with odd exponent. The factor $\operatorname{sgn}(a/b)r$ is a square-free integer and the product $a/b \cdot \operatorname{sgn}(a/b)r^{-1} = |a/b| \cdot r^{-1}$ is a positive quotient of squares, hence $(a/b)(\mathbb{Q}^\times)^2 = \operatorname{sgn}(a/b)r(\mathbb{Q}^\times)^2$.

Note that by definition of the direct sum of groups, for each element only finitely many coordinates can be different from 1, hence indeed our representatives are given by finite products of prime powers.

We now establish the main idea of how to embed $E(\mathbb{Q})/2E(\mathbb{Q})$ into $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by defining a homomorphism $E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Theorem 1.1 (Embedding of $E(\mathbb{Q})$)**.** *The map*

$$\psi_\alpha\colon E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$
$$P \mapsto \begin{cases} (x-\alpha)(\mathbb{Q}^\times)^2 & \text{if } P = (x,y) \text{ with } P \neq \infty \text{ and } x \neq \alpha \\ (\alpha-\beta)(\alpha-\gamma)(\mathbb{Q}^\times)^2 & \text{if } P = (\alpha, 0) \\ (\mathbb{Q}^\times)^2 & \text{if } P = \infty \end{cases}$$

is a group homomorphism.

Proof. At first we remark that indeed ψ_α is defined on all of $E(\mathbb{Q})$. In particular, if $\alpha = 0$, then by the defining equation for E, $y = 0$.

Let $P_1, P_2 \in E(\mathbb{Q})$. For $P_3 := P_1 + P_2$ we are to show that $\psi_\alpha(P_3) = \psi_\alpha(P_1) \cdot \psi_\alpha(P_2)$, i.e. $\psi_\alpha(P_1)\psi_\alpha(P_2)\psi_\alpha(P_3)^{-1} = (\mathbb{Q}^\times)^2$. As squares become trivial in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, we conclude $\psi_\alpha(P_i) = \psi_\alpha(P_i)^{-1}$. Furthermore, because E is given in the form $y^2 = f(x)$ with a normed cubic polynomial f, we can apply [1, Chapter 4/(3)] which means taking the inverse of a point only changes its second coordinate. From the definition of ψ_α we infer $\psi_\alpha(P_i) = \psi_\alpha(-P_i)$.

Thus, it suffices to show $P_1 + P_2 + P_3 = \infty$ implies $\psi_\alpha(P_1)\psi_\alpha(P_2)\psi_\alpha(P_3) = (\mathbb{Q}^\times)^2$.

If $P_i = \infty$ for any $i \in \{1,2,3\}$ this is obvious, so for all i we assume $P_i = (x_i, y_i)$. Here, we distinguish two cases. At first, let $(x_i, y_i) \neq (\alpha, 0)$ for all i. By the group law, all P_i lie on a line, say $y = mx + b$. Then each $P_i = (x_i, y_i)$ satisfies

$$(x_i - \alpha)(x_i - \beta)(x_i - \gamma) = y_i^2 = (mx_i + b)^2.$$

Counting multiplicities, the polynomial

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2$$

has the roots $x = x_1, x_2, x_3$, therefore by the Fundamental Theorem of Algebra

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-x_1)(x-x_2)(x-x_3).$$

For $x = \alpha$ we obtain

$$(x_1 - \alpha)(x_2 - \alpha)(x_3 - \alpha) = (m\alpha + b)^2 \in (\mathbb{Q}^\times)^2,$$

so $\psi_\alpha(P_1)\psi_\alpha(P_2)\psi_\alpha(P_3)$ is trivial in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Now, w.l.o.g. we suppose $(x_1, y_1) = (\alpha, 0)$. Then neither point $P_i = (x_i, y_i)$ for $i = 2, 3$ can be $(\alpha, 0)$, too, as then the respective remaining point would be ∞. Again, let $y = mx + b$ the common line of the P_i for $i = 1, 2, 3$. Arguing analogously as above, the polynomial

$$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2$$

has the zeros $x = \alpha, x_2, x_3$ with multiplicities, hence

$$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - \alpha)(x - x_2)(x - x_3).$$

This implies $x - \alpha$ divides $(mx + b)^2$, and as $x - \alpha$ is prime, it already divides $mx + b$. This means $mx + b = m(x - \alpha)$, so

$$(x - \alpha)(x - \beta)(x - \gamma) - m^2(x - \alpha)^2 = (x - \alpha)(x - x_2)(x - x_3)$$

or

$$(x - \beta)(x - \gamma) - m^2(x - \alpha) = (x - x_2)(x - x_3).$$

For $x = \alpha$ this yields

$$(\alpha - \beta)(\alpha - \gamma) = (\alpha - x_2)(\alpha - x_3),$$

i.e.

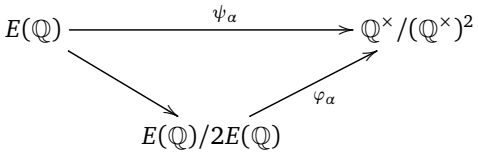
$$\psi_\alpha(P_1) = \psi_\alpha(-P_2)\psi_\alpha(-P_3).$$

According to the introductory remark, $\psi_\alpha(-P_i) = \psi_\alpha(P_i)$ and $\psi_\alpha(P_i)^{-1} = \psi_\alpha(P_i)$, so all in all

$$\psi_\alpha(P_1)\psi_\alpha(P_2)\psi_\alpha(P_3) = (\psi_\alpha(P_2)\psi_\alpha(P_3))^2 \in (\mathbb{Q}^\times)^2.$$

□

We now pass on to the quotient $E(\mathbb{Q})/2E(\mathbb{Q})$. As $\psi_\alpha(2P) = \psi_\alpha(P)^2$ for every $P \in E(\mathbb{Q})$ and squares vanish in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, we see $2E(\mathbb{Q}) \subset \ker\psi_\alpha$. By the homomorphism theorem, there exists a unique induced group homomorphism $\varphi_\alpha\colon E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ such that the following diagram commutes:



Swapping α and β in the definition of ψ_α, we obtain the map ψ_β which induces φ_β as just described. By forming pairs in the codomain, we now obtain the desired injective homomorphism $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Theorem 1.2 (Embedding of $E(\mathbb{Q})/2E(\mathbb{Q})$)**.** *The homomorphism*

$$\begin{aligned}(\varphi_\alpha, \varphi_\beta)\colon E(\mathbb{Q})/2E(\mathbb{Q}) &\to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ P + 2E(\mathbb{Q}) = [P] &\mapsto (\varphi_\alpha([P]), \varphi_\beta([P]))\end{aligned}$$

is injective.

Proof. Let $(x,y) \in E(\mathbb{Q})$ with $(\varphi_\alpha, \varphi_\beta)([x,y]) = ((\mathbb{Q}^\times)^2, (\mathbb{Q}^\times)^2)$, i.e. $[x,y] \in \ker(\varphi_\alpha, \varphi_\beta)$. We distinguish three cases.

At first, let $(x,y) \notin \{\infty, (\alpha,0), (\beta,0)\}$. Then

$$(\varphi_\alpha, \varphi_\beta)([(x,y)]) = \left((x-\alpha)(\mathbb{Q}^\times)^2, (x-\beta)(\mathbb{Q}^\times)^2\right) \overset{!}{=} \left((\mathbb{Q}^\times)^2, (\mathbb{Q}^\times)^2\right).$$

This means, $(x-\alpha)$ and $(x-\beta)$ are squares. Also the product $(x-\alpha)(x-\beta)(x-\gamma) = y^2$ is a square and it follows that $(x-\gamma)$ is a square, too. Hence, we can apply [1, Theorem 4.2] and find $(x',y') \in E(\mathbb{Q})$ such that $(x,y) = 2(x',y')$, hence $(x,y) \in 2E(\mathbb{Q})$ which means $[(x,y)] = 2E(\mathbb{Q}) \in E(\mathbb{Q})/2E(\mathbb{Q})$.

We now assume $(x,y) = (\alpha,0)$. Then

$$(\varphi_\alpha, \varphi_\beta)([(x,y)]) = \left((\alpha-\beta)(\alpha-\gamma)(\mathbb{Q}^\times)^2, (\alpha-\beta)(\mathbb{Q}^\times)^2\right) \overset{!}{=} \left((\mathbb{Q}^\times)^2, (\mathbb{Q}^\times)^2\right),$$

which implies $\alpha-\beta$ and $(\alpha-\beta)(\alpha-\gamma)$ are squares, hence also $\alpha-\gamma$. As 0 is a square, too, again [1, Theorem 4.2] implies that, $(\alpha,0) = 2(x',y')$ for some (x',y'), so $(\alpha,0) \in 2E(\mathbb{Q})$.

The remaining case $P = (\beta,0)$ follows analogously.

So in either of the considered cases, the kernel of $(\varphi_\alpha, \varphi_\beta)$ is trivial.

The remaining case $P = \infty$ is clear as $\infty \in 2E(\mathbb{Q})$. □

It is left to show that the image of the injection defined in the preceding theorem is indeed a finite group, i.e. the image elements under $(\varphi_\alpha, \varphi_\beta)$ are zero in almost all coordinates of

$$\bigoplus_{\pm,\ p \text{ prime}} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

To be precise, this image essentially restricts to coordinates of primes dividing the polynomial discriminant d, hence also the discriminant $\Delta = -16d$ of E.

After introducing a helpful number-theoretic relation we will be able to prove this.

Definition 1.3. If p is a prime number and r rational, we define

$$p^a \| r$$

iff there exists $q \in \mathbb{Q}$ such that $r = p^a q$ and q has no factor of p neither in its enumerator nor its denominator. Put differently, a is the maximal exponent such that r factors into a product $p^a q$ with $q \in \mathbb{Q}$.

Theorem 1.4 (Coordinates of $E(\mathbb{Q})/2E(\mathbb{Q})$)**.** *The image elements of $(\varphi_\alpha, \varphi_\beta)$ can be non-zero only in the coordinates indicating the sign and the ones where the associated prime p divides the discriminant d. Thus, the homomorphism*

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to \bigoplus_{\pm,\ p|d \text{ prime}} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

is injective.

Proof. Let $(x,y) \in E(\mathbb{Q}) \setminus \{\infty\}$.

For the time being, we assume $x \notin \{\alpha, \beta, \gamma\}$. We fix a prime p and consider $a,b,c \in \mathbb{Z}$ satisfying

$$p^a \| (x-\alpha),\ p^b \| (x-\beta) \quad \text{and} \quad p^c \| (x-\gamma).$$

Hence, there exist $q, q', q'' \in \mathbb{Q}$ with

$$x-\alpha = p^a \cdot q, \quad x-\beta = p^b \cdot q' \quad \text{and} \quad x-\gamma = p^c \cdot q'' \tag{1.1}$$

such that neither element from q, q', q'' them has p in its numerator or denominator. By definition of the elliptic curve E, we have

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = p^{a+b+c} \cdot qq'q''$$

which is a square. As none of the factors p can be cancelled, it holds that

$$a+b+c \equiv 0 \pmod 2. \tag{1.2}$$

We proceed by distinguishing two cases. Let at least one of a, b, c be negative, without loss of generality $a < 0$. Then $p^a = p^{-|a|}$. Writing $x = \frac{r}{s}$ we obtain $p^{|a|}\left(\frac{r}{s} - \alpha\right) = q$. But as q does not contain p in its denominator nor in its enumerator and $\alpha \in \mathbb{Z}$, $p^{|a|}$ must get cancelled by multiplication with $\frac{r}{s}$ when expanding the left-hand side. Thus, $p^{|a|} \| s$. Consequently, there exists $r' \in \mathbb{Z}$ with $s = p^{|a|} r'$ such that $p \nmid r'$. This implies

$$x - \beta = \frac{r}{p^{|a|} r'} - \beta = p^a \left(\frac{r}{r'} - p^{|a|}\beta\right)$$

where no p from p^a can be cancelled, so $p^a \| x - \beta$ and analogously $p^a \| x - \gamma$. Invoking the equations (1.1), this yields $a = b$ and analogously $a = c$. As $a + b + c = 3a$ has turned out to be even, so is $a = b = c$. This means

$$(\varphi_\alpha, \varphi_\beta)([x, y]) = ((x - \alpha)(\mathbb{Q}^\times)^2, (x - \beta)(\mathbb{Q}^\times)^2) = (q(\mathbb{Q}^\times)^2, q'(\mathbb{Q}^\times)^2).$$

As q and q' do not contain p neither in their enumerators nor in their denominators, identification in $\bigoplus_{\pm,\ p \text{ prime}} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ yields 0 in the p-coordinate.

We assume, all elements a, b, c are nonnegative. If p does not divide the discriminant

$$d = (\alpha - \beta)^2 (\alpha - \gamma)^2 (\beta - \gamma)^2$$

then p does not divide $\alpha - \beta$ either. As $\alpha - \beta$ is an integer, p does not occur in the enumerator of

$$(x - \alpha) + (\alpha - \beta) = x - \beta.$$

Now $p^b \| x - \beta$ implies $b = 0$. Analogously we conclude that $p \nmid d$ implies $p \nmid (x - \gamma)$, hence $c = 0$. By equation (1.2), a is even. Similarly to the conclusion of the previous case, the image of (x, y) in the p-coordinate is 0.

We remain to treat the case when $x \in \{\alpha, \beta, \gamma\}$. Then, modulo equivalence, $(x, y) = (x, 0)$ is being mapped into $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ as follows:

$$\begin{cases} (\alpha, 0) \mapsto ((\alpha - \beta)(\alpha - \gamma)(\mathbb{Q}^\times)^2, (\alpha - \beta)(\mathbb{Q}^\times)^2) \\ (\beta, 0) \mapsto ((\beta - \alpha)(\beta - \gamma)(\mathbb{Q}^\times)^2, (\beta - \alpha)(\mathbb{Q}^\times)^2) \\ (\gamma, 0) \mapsto ((\gamma - \alpha)(\mathbb{Q}^\times)^2, (\gamma - \beta)(\mathbb{Q}^\times)^2) \end{cases}$$

So in each case the image of (x, y) is given by a pair of products of $(\alpha - \beta)$, $(\alpha - \gamma)$ or $(\beta - \gamma)$. As p does not divide $d = (\alpha - \beta)^2 (\alpha - \gamma)^2 (\beta - \gamma)^2$, p is prime to either of these factors, hence (x, y) becomes trivial at the p-coordinate in $\bigoplus_{\pm,\ p \text{ prime}} (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

□

Corollary 1.5. *If E is an elliptic curve over $\mathbb{Q}$ with rational roots then the Abelian group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. By the preceding theorem, the elements in the image of $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ are zero in all coordinates but the one for the sign and the ones associated to primes dividing the discriminant d of E. As there exist only finitely many such divisors, the claim follows. □

2 The Case $E(K)/2E(K)$ for General Roots

2.1 Order estimation for the kernel of the embedding

In the previous section, α, β, γ from the Weierstrass equation

$$E\colon y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

are assumed to be rational. If the right-hand side polynomial possesses non-rational roots, we have to consider the splitting field K of $(x - \alpha)(x - \beta)(x - \gamma)$ over $\mathbb{Q}$ and inspect the group $E(K)/2E(K)$. We are about to show that from the finiteness of $E(K)/2E(K)$ also the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$ follows.

Theorem 2.1. *Let*

$$\kappa\colon E(\mathbb{Q})/2E(\mathbb{Q}) \to E(K)/2E(K)$$

be the homomorphism induced by the inclusion $E(\mathbb{Q}) \hookrightarrow E(K)$. Then the order of the kernel is bounded by

$$\ker \kappa \leq 2^{2[K:\mathbb{Q}]}.$$

Proof. We have $\kappa(P+2E(\mathbb{Q}))=0$ iff $P\in E(\mathbb{Q})\cap 2E(K)$. For each such P we can choose a point Q_P in $E(K)$ such that $P=2Q_P$.

By definition, $K/\mathbb{Q}$ is a normal. Also, this extension is finite and separable as an extension in characteristic 0, hence a Galois extension. Setting

$$E[2]:=\{Q\in E(K)\colon 2Q=0\},$$

for each such P and with respect to the choices Q_P we define a function

$$\lambda_P\colon \mathrm{Gal}(K/\mathbb{Q})\to E[2],\ \sigma\mapsto Q_P^\sigma-Q_P=(\sigma(x),\sigma(y))-(x,y).$$

Indeed, the image of λ_P lies in $E[2]$ as

$$2(Q_P^\sigma-Q_P)=(2Q_P)^\sigma-2Q_P=P^\sigma-P\overset{\sigma|_{\mathbb{Q}}=\mathrm{id}_{\mathbb{Q}}}{=}0.$$

We now show that non-equivalent points induce different such maps. Let $\lambda_P=\lambda_{P'}$. Then for all $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ we compute $Q_P^\sigma-Q_P=\lambda_P=\lambda_{P'}=Q_{P'}^\sigma-Q_{P'}$, i.e. $(Q_P-Q_{P'})^\sigma=Q_P-Q_{P'}$. The fixed field under the action of the Galois group is $K^{\mathrm{Gal}(K/\mathbb{Q})}=\mathbb{Q}$, so $Q_P-Q_{P'}\in E(\mathbb{Q})$. Then

$$P-P'=2(Q_P-Q_{P'})\in 2E(\mathbb{Q}),$$

i.e. $P+2E(\mathbb{Q})=P'+2E(\mathbb{Q})$.

Now, for each element in $\ker\kappa$ we can choose a point $P\in E(\mathbb{Q})\cap 2E(K)$ and associate λ_P. As shown above, choosing different elements $P+2E(\mathbb{Q})$ leads to different maps λ_P. Thus, the kernel of κ contains at most as many elements as there are maps $\mathrm{Gal}(K/\mathbb{Q})\to E[2]$.

Let P be a point of order 2. In our special case, taking inverses of points of E means inverting the second coordinate (again, cf. [1, Chapter 4/(3)]). Thus, because $P=-P$ and α,β,γ are pairwisely distinct as remarked at the beginning, the rational points of order 2 are exactly given by $(\alpha,0)$, $(\beta,0)$ and $(\gamma,0)$. Hence there is a group isomorphism $E[2]\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. With $[K:\mathbb{Q}]=|\mathrm{Gal}(K/\mathbb{Q})|$ we obtain

$$|\ker\kappa|\le\left|\{\mathrm{Gal}(K/\mathbb{Q})\to E[2]\}\right|=4^{|\mathrm{Gal}(K/\mathbb{Q})|}=2^{2[K:\mathbb{Q}]}.$$

□

Corollary 2.2. *If $E(K)/2E(K)$ is finite, then so is $E(\mathbb{Q})/2E(\mathbb{Q})$.*

Proof. Given the preceding theorem, the claim follows from general principles of elementary group theory.

We define $G:=E(\mathbb{Q})/2E(\mathbb{Q})$ and $H:=E(K)/2E(K)$. Let H be finite. As shown above, $|\ker\kappa|<\infty$. Then Lagrange's Theorem and the Homomorphism Theorem imply

$$|G|=|G/\ker\kappa|\cdot|\ker\kappa|=|\mathrm{im}\kappa|\cdot|\ker\kappa|\le|H|\cdot|\ker\kappa|<\infty.$$

□

2.2 An extension of the ring of integers

We want to prove the finiteness of $E(K)/2E(K)$ similar to the case $E(\mathbb{Q})/2E(\mathbb{Q})$ in the first section. The latter relies on the two important features of the integers, namely the unique prime factorization of elements and the fact that the group of units is finite. In the current situation we have to consider a suitable generalization of $\mathbb{Z}$, the ring of integers $\mathcal{O}_K:=\mathcal{O}\cap K$ (*ger. Ganzheitsring*). The elements of $\mathcal{O}_K$ are given by elements of $\overline{\mathbb{Q}}\cap K$ which satisfy a normed polynomial equation with integer coefficients. The following examples list some rings of integers and show which difficulties can arise for our method. The calculations will be stated without proof.

Example 2.3. (i) Let $E\colon y^2=x^3+x$. Then the splitting field is $K=\mathbb{Q}(\sqrt{-1})$. The ring of integers is given by $\mathcal{O}_K=\mathbb{Z}[\sqrt{-1}]$, the so-called *ring of Gaussian integers*. This is a unique factorization domain with $\mathcal{O}_K^\times=\{(\sqrt{-1})^k\colon k=0,\dots,3\}\cong\mathbb{Z}/4\mathbb{Z}$.

(ii) Let $E\colon y^2=x^3-2x$. The splitting field is $K=\mathbb{Q}(\sqrt{2})$ and again the ring of integers $\mathcal{O}_K=\mathbb{Z}[\sqrt{2}]$ is a unique factorization domain. Its group of units is infinite but finitely generated, namely $\mathcal{O}_K^\times=\{\pm(1\pm\sqrt{2})^k\colon k\in\mathbb{Z}\}\cong\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

(iii) Let $E\colon y^2 = x^3 + 5x$. The splitting field is $K = \mathbb{Q}(\sqrt{-5})$ and the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. But this is not a unique factorization domain since

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

exhibits two decompositions into products of pairwisely non-associated prime elements. The group of units is $\mathcal{O}_K^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

The following theorem gives a ring extension of $\mathcal{O}_K$ to establish a setting in which our desired method works.

Theorem 2.4. *Let $K/\mathbb{Q}$ be a finite field extension with the ring of integers $\mathcal{O}_K$. Then there exists a principal ideal domain R with*

$$\mathcal{O}_K \subset R \subset K$$

and the group of units $R^\times$ is finitely generated. As a principal ideal domain, R is a unique factorization domain.

Let $(\mathfrak{a}_j)_j$ be the finitely many ideals of $\mathcal{O}_K$ modulo principal ideals. Choosing $u_j \in \mathfrak{a}_j$ for every j we define $u := \prod_j u_j$. In the proof, we construct the ring R as the localization of $\mathcal{O}_K$ by the element u. This means, denoting by S as the multiplicative set generated by u, we have $R := S^{-1}\mathcal{O}_K$. The ring $\mathcal{O}_K$ does not need to be a unique factorization domain in general, but it has a unique prime factorization property for ideals. We will use this fact and Dirichlet's Unit Theorem to show that $R^\times = (S^{-1}\mathcal{O}_K)^\times$ is finitely generated.

Proof. Let $h := h_K = |\mathrm{Cl}(K)|$ be the class number of K. By [1, Theorem 4.31], h is finite. Thus, the ideal class group can be written in terms of finitely many representatives, say $\mathfrak{a}_1, \dots, \mathfrak{a}_h$. Setting $\mathfrak{a}_1 := (1)$ and choosing non-zero elements $u_j \in \mathfrak{a}_j$ for all $j \in \{1, \dots, h\}$, we define $u := \prod_{j=1}^h u_j$. Then $u \in \bigcap_{j=1}^h \mathfrak{a}_j$ as $u = u_j \cdot \underbrace{\prod_{k \in \{1,\dots,h\}\setminus\{j\}} u_k}_{\in \mathcal{O}_K} \in \mathfrak{a}_j$ for all j by definition of an ideal. Obviously the set

$$S := \{u^k \colon k = 0, 1, \dots\}$$

is closed under multiplication, does not contain 0 but does contain 1. We define $R := S^{-1}\mathcal{O}_K = \{s^{-1}\alpha \colon s \in S,\ \alpha \in \mathcal{O}_K\}$.

By construction $\mathcal{O}_K \subset R \subset K$. It is left to show that R is a principal ideal domain and $R^\times$ is finitely generated.

If $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ is an ideal, then $\tilde{\mathfrak{a}} := S^{-1}\mathfrak{a}$ is easily to be seen an ideal in $S^{-1}\mathcal{O}_K$.

Now, let $\mathfrak{a}_S \trianglelefteq S^{-1}\mathcal{O}_K$ and $\tilde{\mathfrak{a}} := S^{-1}(\mathfrak{a}_S \cap \mathcal{O}_K)$. We are about to establish the equality

$$\mathfrak{a}_S = S^{-1}(\mathfrak{a}_S \cap \mathcal{O}_K). \tag{2.1}$$

The inclusion $S^{-1}(\mathfrak{a}_s \cap \mathcal{O}_K) \subset \mathfrak{a}_S$ is clear since $\mathfrak{a}_S$ is closed under multiplication by S^{-1}. For the reverse inclusion, we remark that every $a \in \mathfrak{a}_S$ can be written as $a = s^{-1}\alpha$ for suitable $s \in S$ and $\alpha \in \mathcal{O}_K$. Then $\alpha = sa \in \mathfrak{a}_S$, in particular $\alpha \in \mathfrak{a}_S \cap \mathcal{O}_K$. Thus, $a = s^{-1}\alpha \in S^{-1}(\mathfrak{a}_S \cap \mathcal{O}_K) = \tilde{\mathfrak{a}}$.

Let $\mathfrak{a}_S$ be an ideal in $S^{-1}\mathcal{O}_K$. To see that $\mathfrak{a}_S$ is a principal ideal, we at first define $\mathfrak{a} := \mathfrak{a}_S \cap \mathcal{O}_K$. Then $\mathfrak{a}$ is equivalent to some $\mathfrak{a}_j$ for some index $1 \le j \le h$, i.e. there exist $\alpha, \beta \in \mathcal{O}_K$ such that

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{a}_j. \tag{2.2}$$

The element u defined above lies in $\mathfrak{a}_j \cap S$, hence $u^{-1} \cdot u = 1 \in S^{-1}\mathfrak{a}_j$, so

$$S^{-1}\mathfrak{a}_j = S^{-1}\mathcal{O}_K. \tag{2.3}$$

Denoting the principal ideals in $S^{-1}\mathcal{O}_K$ by $(\alpha)_S$ and $(\beta)_S$, we obtain

$$(\alpha)_S \cdot \mathfrak{a}_S \overset{(2.1)}{=} S^{-1}(\alpha) \cdot S^{-1}\mathfrak{a} = S^{-1}(\alpha)\mathfrak{a} \overset{(2.2)}{=} S^{-1}(\beta)\mathfrak{a}_j \overset{(2.3)}{=} S^{-1}\mathcal{O}_K(\beta) = (\beta)_S. \tag{2.4}$$

This implies $\frac{\beta}{\alpha} \in S^{-1}\mathcal{O}_K$ and $\mathfrak{a}_S = \left(\frac{\beta}{\alpha}\right)_S$ as we shall see. First of all $\beta \in \alpha\mathfrak{a}_S$, i.e., there exists $a_0 \in \mathfrak{a}_S$ such that $\beta = \alpha a_0$. Thus, $\frac{\beta}{\alpha} = a_0 \in \mathfrak{a}_S \subset S^{-1}\mathcal{O}_K$ and consequently $\left(\frac{\alpha}{\beta}\right)_S \subset \mathfrak{a}_S$. Conversely, let $a \in \mathfrak{a}_S$ be given. Then, by (2.4), there exists an $x \in S^{-1}\mathcal{O}_K$ so $\alpha a = \beta x$, so $a = \frac{\beta}{\alpha}x \in \left(\frac{\beta}{\alpha}\right)_S$.

We have shown now that an arbitrary ideal $\mathfrak{a}_S \trianglelefteq S^{-1}\mathcal{O}_K$ is generated by a single element, hence $S^{-1}\mathcal{O}_K$ is a principal ideal domain, in particular a unique factorization domain. It remains to prove that the group of units $(S^{-1}\mathcal{O}_K)^\times$ is finitely generated.

Let $u^{-s}\alpha \in (S^{-1}\mathcal{O}_K)^\times$ with $(u^{-s}\alpha)^{-1} =: u^{-t}\beta$. Then $\alpha\beta = u^{s+t}$, so α divides a non-negative power of u. It suffices to construct a finite set of generators for the group of divisors of non-negative powers of u.

In order to do this, let $\alpha, \beta \in \mathcal{O}_K$ with $\alpha\beta := u^r$. By the theorem of unique factorization of ideals in $\mathcal{O}_K$ into powers of prime ideals [1, Theorem 4.33] we can write

$$(u) = \prod_{j=1}^{N} \mathfrak{p}_j^{k_j}$$

for proper prime ideals $\mathfrak{p}_j \trianglelefteq \mathcal{O}_K$ and integers $k_i > 0$. We compute

$$(\alpha)(\beta) = (u^r) = (u)^r = \prod_{j=1}^{N} \mathfrak{p}_j^{k_j \cdot r}.$$

The uniqueness in [1, Theorem 4.33] implies the factorization

$$(\alpha) = \prod_{j=1}^{N} \mathfrak{p}^{l_j} \tag{2.5}$$

with exponents $0 \leq l_j \leq k_j \cdot r$ for $1 \leq j \leq N$. Now, for each j, the equivalence class of $\mathfrak{p}_j^h = \mathfrak{p}_j^{|\mathrm{Cl}(K)|}$ is the trivial element in the ideal class group $\mathrm{Cl}(K)$. Hence, $\mathfrak{p}_j^h$ is a principal ideal, say $\mathfrak{p}_j^h = (\gamma_j)$. For each j we write $l_j = q_j h + r_j$ with $0 \leq r_j < h$, so

$$(\alpha) = \prod_{j=1}^{N} (\gamma_j)^{q_j} \cdot \prod_{j=1}^{N} \mathfrak{p}_j^{r_j}. \tag{2.6}$$

We conclude

$$\alpha = \prod_{j=1}^{N} \gamma_j^{q_j} \cdot p$$

for some $p \in \prod_{j=1}^{N} \mathfrak{p}_j^{r_j}$, i.e.

$$\frac{\alpha}{\prod_{j=1}^{N} \gamma_j^{q_j}} = p \in \mathcal{O}_K. \tag{2.7}$$

The factorization (2.6) then means

$$\left(\prod_{j=1}^{N} \gamma_j^{q_j}\right)\left(\frac{\alpha}{\prod_{j=1}^{N} \gamma_j^{q_j}}\right) = \left(\prod_{j=1}^{N} \gamma_j^{q_j}\right) \prod_{j=1}^{N} \mathfrak{p}_j^{r_j}.$$

The cancellation property [1, Equation (4.89)] for nonzero ideals in the ring of integers yields

$$\prod_{j=1}^{N} \mathfrak{p}_j^{r_j} = \left(\frac{\alpha}{\prod_{j=1}^{N} \gamma_j^{q_j}}\right) \overset{(2.7)}{=} (p).$$

Hence the product $\prod_{j=1}^{N} \mathfrak{p}_j^{r_j}$ is a principal ideal. Choosing a generator $\delta_{r_1,\ldots,r_N}$ with respect to the family $(r_i)_{i=1,\ldots,N}$, we rewrite

$$\prod_{j=1}^{N} \mathfrak{p}_j^{r_j} = (\delta_{r_1,\ldots,r_N}).$$

This leads to

$$\alpha = \prod_{j=1}^{N} \gamma_j^{q_j} \cdot \delta_{r_1,\ldots,r_N} \varepsilon$$

for a unit $\varepsilon \in \mathcal{O}_K^\times$. As for each j the choice of r_j is restricted by $r_j < h$, there exist only finitely many generators of the form $\delta_{r_1,\ldots,r_N}$. Now, the latter equation exhibits $(S^{-1}\mathcal{O}_K)^\times$ as generated by $\gamma_1, \ldots, \gamma_N$, the elements $\delta_{r_1,\ldots,r_N}$ and $\mathcal{O}_K^\times$. By [1, Dirichlet's Unit Theorem 4.29] the group $\mathcal{O}_K^\times$ is finitely generated and so is $(S^{-1}\mathcal{O}_K)^\times$. □

Example 2.5. In the case $K = \mathbb{Q}(\sqrt{-5})$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. It can be shown that the class number equals 2 in this case. Analogous to the proof we define $\mathfrak{a}_1 := (1)$ and $\mathfrak{a}_2 := (2, 1+\sqrt{-5})$. For $u_1 = 1$ and $u_2 := 2$ we have $u := u_1 u_2 = 2$. With $\mathfrak{p}_1 := (2, 1+\sqrt{-5})$, the prime ideal factorization for $(u) \neq (1)$ is

$$(2) = \mathfrak{p}_1^2.$$

This equality follows from the fact that $(2a + (1+\sqrt{-5})b)^2$ is a multiple of 2 for any $a, b \in \mathbb{Z}$. So all in all, $N = 1$ and we consider $\gamma_1 = 2$. The only relevant ideals of the form $\prod_{i=1}^{N} \mathfrak{p}_i^{r_i}$ are $\mathfrak{p}_1^0 = (1)$ and $\mathfrak{p}_1^1 = (2, 1+\sqrt{-5})$. As the latter is not principal, we have $\delta_{r_1,\dots,r_N} = 1$. As $\mathcal{O}_K^\times = \{\pm 1\}$, the group $(S^{-1}\mathcal{O}_K)^\times$ is generated by $\{-1, 1, 2\}$.

Theorem 2.6. *Let $E\colon y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$ with and $K/\mathbb{Q}$ be the splitting field of f. Then the Abelian group $E(K)/2E(K)$ is finite.*

Proof. We give a sketch of the proof indicating the crucial steps. The details are analogous to the methods developed in the first section.

Let us first assume $\mathcal{O}_K$ is not a unique factorization domain. Forming $R := S^{-1}\mathcal{O}_K$ as in the preceding theorem, we obtain a unique factorization domain with a finitely generated group of units. The quotient field of R is still K as $\mathcal{O}_K \subset R \subset K$. Thus, as in the first section, we have an identification $K^\times/(K^\times)^2 \cong R^\times/(R^\times)^2 \times \bigoplus_{p \text{ prime}} \mathbb{Z}/2\mathbb{Z}$ where in the sum we take one representative from each class of associated primes. As $R^\times$ is finitely generated and Abelian, it is isomorphic to a direct sum of cyclic groups decomposing into a free part and a torsion part. Factoring out squares, the free part is becoming a torsion part, hence $R^\times/(R^\times)^2$ is finite.

We analogously obtain homomorphisms $\psi_\alpha, \psi_\beta\colon E(K) \to K^\times/(K^\times)^2$ inducing the injective homomorphism

$$(\varphi_\alpha, \varphi_\beta)\colon E(K)/2E(K) \to K^\times/(K^\times)^2 \times K^\times/(K^\times)^2.$$

Again, the image within $K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$ restricts to the coordinates of primes p dividing the discriminant d which are of finite number by unique prime factorization in K.

If on the other hand $\mathcal{O}_K$ is already a unique factorization domain we can proceed analogously, so in either case $E(K)/2E(K)$ is finite. □

Corollary 2.7. *If E is an elliptic curve over $\mathbb{Q}$ then the Abelian group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. Combining Corollary 2.2 and Theorem 2.6 implies the claim. □

References

[1] Knapp, A. W. *Elliptic Curves*. Princeton University Press, 1992.

[2] Neukirch, J. *Algebraic Number Theory*. Springer-Verlag, 1999.

[3] Silverman, J. H. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.