Group law

David Kurniadi Angdinata

Winter 2019

1 Statement

Let K be an algebraically closed field and let E be an *elliptic curve* over K defined by the *Weierstrass equation*

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in K,$$

in *dehomogenised* form. Then the following theorem holds.

Theorem 1 (Group law)**.** *$(E, \mathcal{O}, +)$ is an abelian group.*

Rather than providing the conventional geometric proof using *Bézout's theorem* and *the Cayley-Bacharach theorem*, this algebraic proof using the theory of *divisors* establishes Theorem 1 more naturally.

2 Restatement

Let the *coordinate ring* R of E be

$$R = \frac{K[x, y]}{I},$$

where I is the ideal generated by the Weierstrass equation of E,

$$I = \left\langle y^2 - x^3 - Ax - B \right\rangle.$$

Let $\mathcal{A}(R)$ be the *ideal class group* of R, defined as the quotient

$$\mathcal{A}(R) = \frac{\mathcal{I}(R)}{\mathcal{P}(R)},$$

where $\mathcal{I}(R)$ is the group of *fractional ideals* of R and $\mathcal{P}(R)$ is the subgroup of *principal fractional ideals* of R.

Definition 2. The **Picard group** of E is

$$Pic^0(E) = \mathcal{A}(R).$$

Remark 3. Strictly speaking, Definition 2 is that of the *degree zero* subgroup of the actual *Picard group*, but this terminology will be used for the sake of brevity.

It is then sufficient to prove the following theorem, which implies Theorem 1.

Theorem 4. *There is a set bijection*

$$Pic^0(E) \leftrightarrow E.$$

In fact, the following stronger theorem will be proven as well, assuming the geometric group law.

Theorem 5. *There is a group isomorphism*

$$Pic^0(E) \cong E.$$

The proof involves defining $Pic^0(E)$ in detail, which requires the notion of a *divisor* of E.

3 Divisors

A *divisor* is defined as follows.

Definition 6. A **divisor** of E is a free abelian group generated by a finite basis $C \subseteq E$ of formal symbols of the form $[P]$ for some point $P \in E$, denoted

$$D = \sum_{P \in C} n_P \left[P\right],$$

for some $n_P \in \mathbb{Z}$.

It can be easily shown that the set of divisors forms an additive group $Div\left(E\right)$, called the **divisor group** of E. Let $D, D' \in Div\left(E\right)$ be divisors as in Definition 6 throughout.

Definition 7. The **degree** of D is

$$\deg\left(D\right) = \sum_{P \in C} n_P \in \mathbb{Z}.$$

It follows easily that the set of divisors of E of degree zero forms a subgroup $Div^0\left(E\right)$ of $Div\left(E\right)$, which is precisely the group of fractional ideals $\mathcal{I}\left(R\right)$. Now divisors can also be defined for *functions* $f \in K\left(E\right)^*$. Let $P \in E$ be a point throughout. With some commutative algebra, it can be shown that there is a function $u_P \in K\left(E\right)^*$ that is zero at P, called the **uniformiser** at P, such that any other function $f \in K\left(E\right)^*$ can be written in the form $f \equiv u_P^{d_P} g$, for some $d_P \in \mathbb{Z}$, and some function $g \in K\left(E\right)^*$ such that $g\left(P\right) \notin \{0, \infty\}$. In fact, it can be shown that simply choosing

$$u_P = \begin{cases} x - a & P = (a, b) \\ y & P = (a, 0) \\ \frac{x}{y} & P = \mathcal{O} \end{cases}$$

works as a uniformiser at P.

Remark 8. The functions $f, g, u_P \in K\left(E\right)^*$ must take values in $K \cup \{\infty\}$.

The **valuation** of f at P is

$$ord_P\left(f\right) = d_P \in \mathbb{Z}.$$

Then f has a **zero** at P if $ord\left(P\right) > 0$, which corresponds to the multiplicity of $f\left(P\right) = 0$. Similarly, f has a **pole** at P if $ord\left(P\right) < 0$, which corresponds to the multiplicity of $f\left(P\right) = \infty$. With some algebraic geometry, the following proposition can be shown.

Proposition 9.

- *f has only finitely many zeroes and poles, that is $ord_P\left(f\right) \neq 0$ for only finitely many points $P \in E$.*
- *f has an equal number of zeroes and poles counted with multiplicity, that is $\deg\left(div\left(f\right)\right) = 0$.*
- *if f has no zeroes or poles, that is $div\left(f\right) = 0$, then f is constant.*

The following definition is then well-defined.

Definition 10. D is **principal** if

$$D = div\left(f\right) = \sum_{P \in E} ord_P\left(f\right)\left[P\right],$$

for some function $f \in K\left(E\right)^*$.

It follows that the subset of principal divisors of E forms a subgroup $Prin\left(E\right)$ of $Div^0\left(E\right)$, which is precisely the subgroup of principal fractional ideals $\mathcal{P}\left(R\right)$. Definition 2 can now be restated as

$$Pic^0\left(E\right) = \frac{Div^0\left(E\right)}{Prin\left(E\right)}.$$

Alternatively, $Pic^0\left(E\right)$ can also be thought of as $Div^0\left(E\right)$ modulo an equivalence relation $\sim$, where

$$D \sim D' \qquad \iff \qquad D - D' \text{ is principal.}$$

4 The Riemann-Roch theorem

Before proceeding to the proof in the next section, a fundamental result in algebraic geometry concerning divisors will be stated in this section in its full generality. Although it is possible to complete the proof without this theorem, its statement allows for a simpler argument. Let C be an algebraic curve throughout. The notion of a *divisor* $D \in Div(C)$ and the results that follow can be defined analogously. Now let $\leq$ be a partial order on $Div(C)$ defined by

$$\sum_{P \in C} n_P [P] \leq \sum_{P' \in C'} n'_{P'} [P'] \qquad \Longleftrightarrow \qquad \forall P \in C \cup C',\ n_P \leq n'_{P'}.$$

For any divisor $D \in Div(C)$, define a finite-dimensional K-vector space of functions by

$$\mathcal{L}(D) = \left\{ f \in K(C)^* \mid div(f) \geq -D \right\} \cup \{0\},$$

denoting its dimension as

$$l(D) = \dim_K (\mathcal{L}(D)).$$

The theorem can then be stated as follows.

Theorem 11 (Riemann-Roch)**.** *Let $D \in Div(C)$ be a divisor. There is a divisor $K_C \in Div(C)$ such that*

$$l(D) - l(K_C - D) = \deg(D) - g_C + 1,$$

where g_C is the genus of C.

Remark 12. The divisor K_C in Theorem 11 is called a *canonical divisor*. It is the divisor $div(\omega)$ of some *meromorphic differential* ω in the $K(C)$*-vector space of meromorphic differential forms* Ω_C. In turn, it is a divisor of the *canonical divisor class* subgroup $div(\Omega_C)$ of $Pic(C)$.

The proof of Theorem 11 can be found in basic algebraic geometry books. Fortunately, the argument in the next section does not require formally defining K_C, leaving the following corollary sufficient for purposes of the proof.

Corollary 13 (Roch)**.** *Let $D \in Div(C)$ be a divisor such that* $\deg(D) > 2g_C - 2$*. Then*

$$l(D) = \deg(D) - g_C + 1.$$

Furthermore, if $C = E$ and $\deg(D) > 0$*, then*

$$l(D) = \deg(D).$$

Proof. Let $f \in \mathcal{L}(0)^*$ be a function, so

$$div(f) = \sum_{P \in C} n_P [P],$$

for some finite basis $C \subseteq E$, and some $n_P \in \mathbb{Z}$. Then $div(f) \geq 0$, so $n_P \geq 0$ for all $P \in C$. Since $\deg(div(f)) = 0$, it holds that $n_P = 0$ for all $P \in C$, so $div(f) = 0$. Proposition 9 gives that f is constant, so $\mathcal{L}(0) = K$. Hence $l(0) = 1$, so letting $D = 0$ in Theorem 11 gives

$$l(0) - l(K_C - 0) = \deg(0) - g_C + 1 \qquad \Longrightarrow \qquad l(K_C) = g_C.$$

Similarly, letting $D = K_C$ in Theorem 11 gives

$$l(K_C) - l(K_C - K_C) = \deg(K_C) - g_C + 1 \qquad \Longrightarrow \qquad \deg(K_C) = 2g_C - 2.$$

Now let D be the given divisor. If $l(K_C - D) \neq 0$, then let $f \in \mathcal{L}(K_C - D)^*$ be a function, so $div(f) \geq K_C - D$. Then

$$0 = \deg(div(f)) \geq \deg(K_C - D) = \deg(K_C) - \deg(D) < (2g_C - 2) - (2g_C - 2) = 0,$$

which is a contradiction. Hence $l(K_C - D) = 0$. Thus Theorem 11 gives

$$l(D) = \deg(D) - g_C + 1.$$

The final part follows by virtue of the genus $g_E = 1$ of elliptic curves. $\square$

5 Summation

The required bijection is defined as follows.

Definition 14. Let $D \in Div(E)$ be a divisor as in Definition 6. Then the **sum** of D is

$$sum(D) = \sum_{P \in C} n_P P \in E.$$

Define the **summation** map as the restriction of sum onto the subgroup $Div^0(E)$,

$$\begin{array}{rrcl} \sigma: & Div^0(E) & \to & E \\ & \sum_{P \in C} n_P [P] & \mapsto & \sum_{P \in C} n_P P \end{array},$$

and denote its inverse by

$$\begin{array}{rrcl} \kappa: & E & \to & Div^0(E) \\ & P & \mapsto & [P] - [\mathcal{O}] \end{array}.$$

With the first isomorphism theorem, Theorem 4 is equivalent to the following two propositions and an application of forgetful functors.

Proposition 15. $Im(\sigma) = E$.

Proposition 15 is practically trivial, considering κ.

Proof. It is sufficient to verify that κ is well-defined. Let $P \in E$ be a point. Then $\deg([P] - [\mathcal{O}]) = 1 - 1 = 0$, so $[P] - [\mathcal{O}] \in Div^0(E)$. Now $\sigma([P] - [\mathcal{O}]) = P - \mathcal{O} = P$, so $P \in Im(E)$. Hence $E \subseteq Im(E) \subseteq E$. Thus $Im(\sigma) = E$. □

Proposition 16. $Ker(\sigma) = Prin(E)$.

Proposition 16 requires more work, starting with the following lemma that utilises Theorem 13.

Lemma 17. *Let $P, Q \in E$ be points. Then*

$$P = Q \qquad \Longleftrightarrow \qquad [P] \sim [Q].$$

Proof. The forward direction is clear. Conversely, assume that $[P] \sim [Q]$. Then there is some function $f \in K(E)^*$ such that $div(f) = [P] - [Q]$, so $f \in \mathcal{L}([Q])$. Hence Theorem 13 gives

$$l([Q]) = \deg([Q]) = 1,$$

so f is constant. Thus $P - Q = \mathcal{O}$, so $P = Q$. □

The following lemma relates the group law definition with linear equivalence of divisors.

Lemma 18. *Let $P, Q \in E$ be points. Then*

$$[P] + [Q] \sim [P + Q] + [\mathcal{O}].$$

Proof. Let $L : f(x, y) = 0$ be the unique line through P, Q, and $-(P + Q)$. Then f has exactly three zeroes at these points. Since $\deg(div(f)) = 0$ and f has no affine poles, it holds that f has exactly one triple pole at $\mathcal{O}$. Hence

$$div(f) = [P] + [Q] + [-(P + Q)] - 3[\mathcal{O}].$$

Now let $L' : g(x, y) = 0$ be the unique line through $P + Q$, $-(P + Q)$, and $\mathcal{O}$. Similarly,

$$div(g) = [P + Q] + [-(P + Q)] - 2[\mathcal{O}].$$

Hence

$$div\left(\frac{f}{g}\right) = div(f) - div(g) = [P] + [Q] - [P + Q] - [\mathcal{O}].$$

Thus

$$[P] + [Q] \sim [P + Q] + [\mathcal{O}].$$

□

The following lemma consequently hinges on this observation.

Lemma 19. *Let $D \in Div^0(E)$ be a divisor of degree zero. Then*

$$D \sim [P] - [Q], \qquad \sigma(D) = P - Q,$$

for some points $P, Q \in E$.

Proof. Let

$$D = \sum_{P \in C} n_P [P] - \sum_{P' \in C'} n'_{P'} [P'],$$

for some finite subsets $C, C' \subseteq E$ such that $C \cup C' \subseteq E$ is a finite basis, and some $n_P, n'_{P'} \in \mathbb{N}$ such that

$$\sum_{P \in C} n_P - \sum_{P' \in C'} n'_{P'} = \deg(D) = 0.$$

Then for any $P, P' \in C$ or any $P, P' \in C'$,

$$[P] + [P'] = [P + P'] + [\mathcal{O}] + div(f),$$

for some function $f \in K(E)^*$ such that

$$\sigma(div(f)) = \sigma([P] + [P'] - [P + P'] + [\mathcal{O}]) = P + P' - (P + P') + \mathcal{O} = \mathcal{O}.$$

Hence by induction,

$$D = \left([P] + \left(\sum_{P \in C} n_P - 1\right)[\mathcal{O}]\right) - \left([Q] + \left(\sum_{P' \in C'} n'_{P'} - 1\right)[\mathcal{O}]\right) + div(g) = [P] - [Q] + div(g),$$

for some function $g \in K(E)^*$ such that $\sigma(div(g)) = 0$, where

$$P = \sum_{P \in C} n_P P, \qquad Q = \sum_{P' \in C'} n'_{P'} P'.$$

Thus

$$\sigma(D) = \sigma([P] - [Q] + div(g)) = P - Q.$$

□

Proof of Proposition 16. Let $D \in Div^0(E)$ be a divisor of degree zero. Then

$$\begin{aligned} D \in Ker(\sigma) \quad &\iff \quad \sigma(D) = \mathcal{O} \\ &\iff \quad P = Q \qquad \text{for some points } P, Q \in E \\ &\iff \quad [P] \sim [Q] \\ &\iff \quad D \sim 0 \qquad \iff \qquad D \in Prin(E). \end{aligned}$$

Thus $Ker(\sigma) = Prin(E)$. □

Hence Theorem 4 follows. The observation that for any points $P, Q, R \in E$,

$$P + Q = R \qquad \iff \qquad ([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}]) \sim ([R] - [\mathcal{O}]),$$

is clear from the definition of κ. Thus Theorem 5 follows as well.

Remark 20. In fact, the following fundamental *exact sequence* in algebraic number theory, applied to elliptic curves, would provide a succinct summary.

$$1 \to K^* \xrightarrow{\subseteq} K(E)^* \xrightarrow{div} Div^0(E) \xrightarrow{\sigma} E \cong Pic^0(E) \to 1.$$

6 References

[1] J Silverman's 1986 book *The arithmetic of elliptic curves*

[2] L Washington's 2003 book *Elliptic curves: number theory and cryptography*

[3] R Hartshorne's 1977 book *Algebraic geometry*