1 The Group Law

Throughout these notes, $\Bbbk$ will be an algebraically closed field and E will be an elliptic curve over $\Bbbk$ in Weierstrass form. Recall that $\infty = [0:1:0]$ is the point at infinity, and the tangent line to ∞ in projective coordinates is given by z, which intersects E at only z, so by Bézout's Theorem, it intersects with multiplicity 3.

1.1 Definition of the group law

If $p, q \in E$, let L be the line connecting p and q, and let t be the third point of the intersection of L with E. Let L' be the line connecting t and ∞. Then $p \oplus q$ is the point such that L' intersecs E at t, ∞, and $p \oplus q$, whose existence is guaranteed by Bézout's Theorem.

1.1 Proposition. *Let E be an elliptic curve. Then:*

(i) *if a line L intersects E at p, q, t, then $(p \oplus q) \oplus t = \infty$;*
(ii) $p \oplus \infty = p$;
(iii) $p \oplus q = q \oplus p$.
(iv) *if $p \in E$, then there exists a $q \in E$ such that $p \oplus q = \infty$.*

PROOF: Only the last statement requires proof. Let L be the line through p and ∞. Then it must intersect E at one more point q, so that by a combination of (i) and (ii),

$$p \oplus q = (p \oplus \infty) \oplus q = \infty. \qquad \square$$

However, we have not yet shown that this group law is actually associative. There are a few ways to do so. The first, which is suggested in Silverman, is to use the explicit formulas given for $p \oplus q$ in terms of the coordinates of p and q to verify that the group law is associative by hand. The second approach, which we will present here, is to use facts about elementary projective plane geometry to derive the associativity. The final approach, which is more in line with the material in the reading course thusfar, is to derive the associativity by first proving that there is an operation-preserving bijection of E with its divisor class group.

1.2 An elementary approach

We will use the following consequence of Bézout's Theorem: if C and D are plane curves of degrees m and n respectively that intersect in more than mn points, then C and D have a common component. This can also be proven for curves over an arbitrary infinite field with a fairly simple direct argument.

1.2 Proposition. *Let E be an elliptic curve. If C and C' are plane cubics such that*

$$E \cap C = \sum_{i=1}^{9} (p_i),$$

and

$$E \cap C' = \sum_{i=1}^{8} (p_i) + (q),$$

then $q = p_9$.

PROOF: Since E and C only intersect in 9 points, they must be distinct. Observe that no four of the points of intersection between E and C can lie on a line, because otherwise by Bézout's Theorem that line would be a common component of E and C, contradicting the fact that E is irreducible and distinct from C. By the same reasoning, no seven of the the points of intersection between E and C can lie on a conic.

If C' is not of the form $\alpha E + \beta C$, then $\alpha E + \beta C + \gamma C'$ is a two-dimensional homogeneous family of cubics, and for any distinct points $p, q \in \mathbb{P}^2$, there exists a point $[\alpha : \beta : \gamma] \in \mathbb{P}^2$ such that $\alpha E + \beta C + \gamma C'$ goes through p and q. We will use this fact to extend the facts mentioned in the previous paragraph to three and six points respectively.

Suppose that p_1, p_2, p_3 lie on a common line L. Let D be the conic through p_4, p_5, p_6, p_7, and p_8. Choose p' on L and p'' off of L and off of D. Then, by Bézout's Theorem, the cubic $\alpha E+\beta C+\gamma C'$ going through p', p'', and $p_1, \ldots, p_8$ has L and D as components. But this contradicts the choice of p'' as being off of D and L. Therefore, our assumption is false, and none of p_1, p_2, and p_3 lie on a common line. By reordering $p_1, \ldots, p_8$, this shows that no three of those points lie on a common line.

Now, suppose that $p_1, \ldots, p_6$ lie on a common conic D. Let L be the line through p_7 and p_8. Choose p' on D and p'' off of D and off of L. Then, by Bézout's Theorem, the cubic $\alpha E+\beta C+\gamma C'$ going through p', p'', and $p_1, \ldots, p_8$ has D and L as components. This contradicts the choice of p'' off of D and L. Therefore, our assumption is false, and none of p_1, p_2, and p_3 lie on a common line. By reordering $p_1, \ldots, p_8$, this shows that no six of those points lie on a common conic.

Finally, let L be the line through p_1 and p_2, and let D be the conic through p_3, p_4, p_5, p_6, and p_7. Choose distinct points p' and p'' on L but not on D. Then, by Bézout's Theorem, the cubic $\alpha E + \beta C + \gamma C'$ going through p', p'', and $p_1, \ldots, p_8$ has L and D as components. This contradicts the fact that p_8 is not on L or C by the previous two paragraphs. Therefore, we must have $C' = \alpha E + \beta C$ for some $[\alpha : \beta] \in \mathbb{P}^2$, which implies that $q = p_9$. □

1.3 Corollary. *Let E be an elliptic curve. The binary operation $\oplus$ on E is associative.*

PROOF: Suppose $p, q, r \in E$. Let L_1, M_1, and L_2 be lines such that

$$\begin{aligned} E \cap L_1 &= (p) + (q) + (s') \\ E \cap M_1 &= (\infty) + (s') + (s), \\ E \cap L_2 &= (s) + (r) + (t'). \end{aligned}$$

Similarly, let M_2, L_3, and M_3 be lines such that

$$\begin{aligned} E \cap M_2 &= (q) + (r) + (u'), \\ E \cap L_3 &= (\infty) + (u') + (u), \\ E \cap M_3 &= (p) + (u) + (t''). \end{aligned}$$

By the definition of the group law, we know that $(p \oplus q) \oplus r$ is the third point on the line joining ∞ and t', and that $p \oplus (q \oplus r)$ is the third point on the line joining ∞ and t''. Thus, it suffices to show that $t' = t''$. To do this, let

$$C = L_1 L_2 L_3 \qquad \text{and} \qquad C' = M_1 M_2 M_3,$$

and apply Proposition 1.2. □

1.3 An approach using divisors

One can show that the group law is associative by using the theory of divisors on curves. The key ingredient is the following proposition, which we will prove by using the Riemann-Roch Theorem, but there is a more elementary proof.

1.4 Proposition. *Let E be an elliptic curve. If $p, q \in E$, then $(p) \sim (q)$ if and only if $p = q$.*

PROOF: The backwards direction is trivial, so we need only prove the forwards direction. Suppose that $(p) \sim (q)$, and $f \in \Bbbk(C)$ is such that $\operatorname{div}(f) = (p) - (q)$. Then $f \in \mathcal{L}((q))$, and by the Riemann-Roch Theorem, $\dim \mathcal{L}(q) = 1$. But $\mathcal{L}((q))$ already contains the constant functions, so f is constant and $p = q$. □

Recall that $\mathrm{Cl}^0(E)$, the (degree zero) divisor class group of E, is the quotient of $\mathrm{Div}^0(E)$, the degree zero divisors on E, by the principal divisors. The above proposition implies that $(p) - \infty$ and $(q) - (\infty)$ give distinct classes in $\mathrm{Cl}^0(E)$ whenever $p \neq q$. Since ∞ is the identity for the group law,

1.5 Proposition. *Let E be an elliptic curve. Then:*

(i) *if $(p) - (\infty) \in \mathrm{Div}^0(E)$, $-((p) - (\infty)) \sim (t) - (\infty)$ for some $t \in E$;*
(ii) *if $(p) - (\infty), (q) - (\infty) \in \mathrm{Div}^0(E)$,*

$$((p) - (\infty)) + ((q) - (\infty)) \equiv (t) - (\infty)$$

for some $t \in E$.

(iii) *if* $D \in \mathrm{Div}^0(E)$*, then there exists a* $p \in E$ *such that* $D \sim (p) - (\infty)$.

PROOF:

(i) Fix $(p) - (\infty) \in \mathrm{Div}^0(E)$. Let L be the line in $\mathbb{P}^2$ through p and ∞. Then, by Bézout's Theorem, $L \cap E = (\infty) + (p) + (t)$ for some $t \in E$. If L is given by the 1-form h, then

$$\begin{aligned}\mathrm{div}(h/z) &= \mathrm{div}(h) - \mathrm{div}(z) \\ &= ((\infty) + (p) + (t)) - 3(\infty) \\ &= p + t - 3(\infty) \\ &= (p - \infty) + (t - \infty)],\end{aligned}$$

so $-((p) - (\infty)) \sim (t) - (\infty)$.

(ii) Fix $(p) - (\infty), (q) - (\infty) \in \mathrm{Div}^0(E)$. Let L be the line through p and q. Then $L \cap E = p + q + r$ for some $r \in E$. If L is given by the 1-form h, then

$$\begin{aligned}\mathrm{div}(h/z) &= \mathrm{div}(h) - \mathrm{div}(z) \\ &= ((p) + (q) + (r)) - 3(\infty) \\ &= ((p) - (\infty)) + ((q) - (\infty)) + ((r) - (\infty)),\end{aligned}$$

so $((p) - (\infty)) + ((q) - (\infty)) \sim -((r) - (\infty))$. By (i), there exists a $t \in E$ such that $-((r) - (\infty)) \sim (t) - (\infty)$. Therefore, $((p) - (\infty)) + ((q) - (\infty)) \sim (t) - (\infty)$.

(iii) Fix $D \in \mathrm{Div}^0(E)$. For some $r_1, \ldots, r_m, s_1, \ldots, s_m \in E$, we have that

$$\begin{aligned}D &= \sum_{i=1}^{m} (r_i) - \sum_{i=1}^{m} (s_i) \\ &= \sum_{i=1}^{m} ((r_i) - (\infty)) - \sum_{i=1}^{m} ((s_i) - (\infty)) \\ &= \sum_{i=1}^{m} ((r_i) - (\infty)) + \sum_{i=1}^{m} -((s_i) - (\infty)).\end{aligned}$$

By part (i), $-((s_i) - (\infty)) \sim ((t_i) - (\infty))$ for some $t_i \in E$, so that

$$D \sim \sum_{i=1}^{m} ((r_i) - (\infty)) + \sum_{i=1}^{m} ((t_i) - (\infty)).$$

By applying part (ii) repeatedly, we have that $D \sim (q) - (\infty)$ for some $q \in E$, □

Define $\Phi_E : E \to \mathrm{Cl}^0(E)$ by $\Phi_E(p) = [(p) - (\infty)]$. It is injective by Proposition 1.4, and surjective by part (iii) of Proposition 1.5. By the proof of part (i) of Proposition 1.5, it is clear that $\Phi_E(p \oplus q) = \Phi_E(p) + \Phi_E(q)$. Therefore, the operation $\oplus$ on E is associative, and Φ_E is a group isomorphism.