Lecture 09

Jose Capco (jcapco@risc.jku.at)

We try to, without too much words, illustrate what happened in Step 5 of the proof of theorem in the last lecture. We used a birational map between $\mathbb{P}^2$ and where it is defined it is given by $\phi(x:y:z) = (xz : xy : z^2)$ this bijective at all but some *measure* 0 region of $\mathbb{P}^2$ (say $\mathbb{P}^2$ without $z = 0$ and $x = 0$ line). The inverse of the map is (where defined, say at $\mathbb{P}^2$ without $u = 0$ and $w = 0$) $\phi^{-1}(u, v, w) = (u^2 : vw : uw)$. This birational map of $\mathbb{P}^2$ is also called a *quadratic birational map* or a *Cremona transformation*. Notice (see figure) the $x = 0$ line, except at $(0:1:0)$, collapses to $(0:0:1)$, the line is called an *exceptional line of* ϕ_5. Similarly for the inverse, ϕ_5^{-1}, the $z = 1$, except at $(0:1:0)$, collapses to $(1:0:0)$.

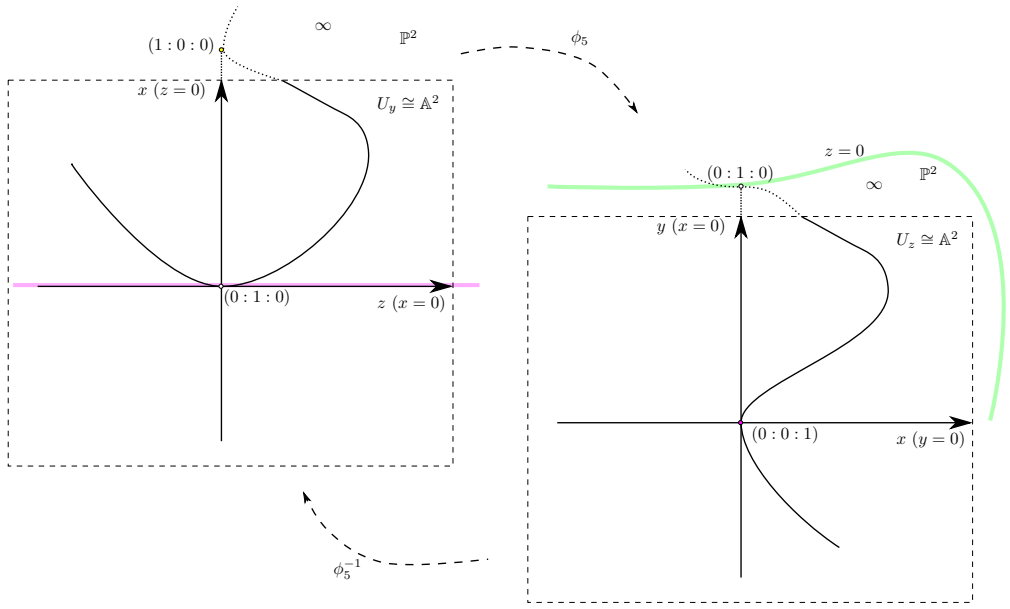


Figure 1: Cremona transformation used in the proof of theorem in the last lecture

Group Law. Let E be an elliptic curve, then we define the following addition rule: Let $P, Q \in E$ (not necessarily distinct) then there is a third point (counted by multiplicity, so not necessarily different from P or Q) $R = P * P$ that the line $\overline{PQ}$ meets. The line $\overline{RO}$ then meets E at a third point $P + Q$, if $R = O$ then this third point is O. We follow this rule counting multiplicity, i.e. if $P = Q$ or $R = O$ then we take the tangent line to P as $\overline{PQ}$ resp. tangent line to O as $\overline{RO}$.

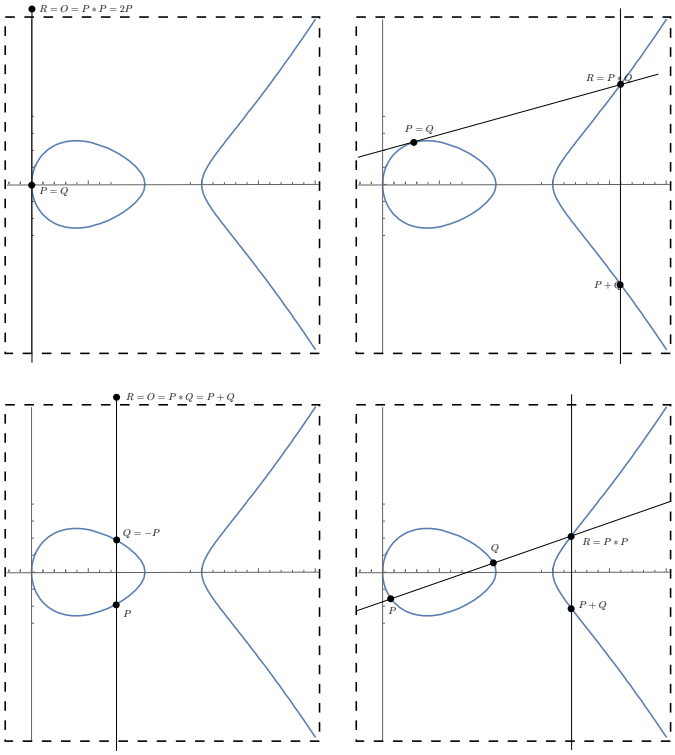
Proposition 1. The above defined addition endows E an abelian group structure, i.e.

- $P + O = P$ for all $P \in E$
- $P + Q = Q + P$ for all $P, Q \in E$
- For any point $P \in E$ there is a $-P \in E$ such that $P + (-P) = O$
- For any $P, Q, R \in E$ we have associativity

$$(P + Q) + R = P + (Q + R)$$

Furthermore if $L \geq K$ as fields then $E(L) \geq E$ as groups.

Proving all of the above is an easy exercise. Only the associativity is rather long (this can be proven elegantly with more algebraic geometry, but we avoid this). Here is a nice geometric exercise that will help you prove associativity

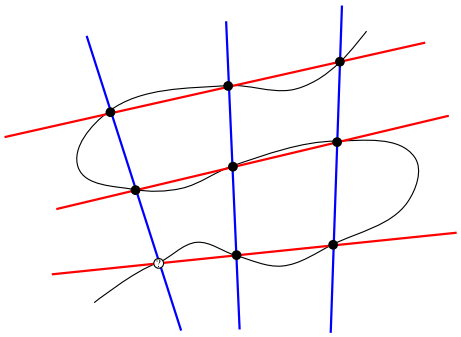


The possible cases for addition of points of an elliptic curve

Exercise 1. The Cayley-Bacharach theorem states that if C_1, C_2 are two cubic curves in the projective plane such that $\#(C_1 \cap C_2) = 9$ and if C_3 is a third cubic curve then

$$\#(C_1 \cap C_2 \cap C_3) \geq 8 \Rightarrow C_1 \cap C_2 \cap C_3 = C_1 \cap C_2$$

i.e. the ninth point will also be in C_3 (see figure below).



Use this result to prove associativity of addition of points in an elliptic curve E.

Below is the group addition algorithm (for points that are not the identity O), given $P, Q \in E\backslash\{O\}$ where $E : y^2 = x^3 + ax + b$ and $\operatorname{char} K \nmid 6$

- If $P \neq Q$ but $x_P = x_Q$ (so $y_P = -y_Q$) then return O
- If $P \neq Q$ and $x_P \neq x_Q$ then compute the slope of the line $\overline{PQ}$ i.e. $\mu = \frac{y_P - y_Q}{x_P - x_Q}$ and return

$$x_{P+Q} = \mu^2 - x_P - x_Q$$
$$y_{P+Q} = y_Q + \mu(x_{P+Q} - x_Q)$$

Note that this will return P if the line $\overline{PQ}$ is tangent to P.

- If $P = Q$ and $y_P = 0$ then return O
- If $P = Q$ then compute the slope of the tangent line at P i.e. $\mu = \frac{3x_P^2+a}{2y_P}$ and return the duplication formula

$$x_{2P} = \mu^2 - 2x_P$$
$$y_{2P} = y_P + \mu(x_{2P} - x_P)$$

Exercise 2. Write the addition formula for points of elliptic curves given by an equation in the Weierstrass long form. Write an algorithm that adds points of an elliptic curve given by this general form.

Let us now discuss a little about maps between elliptic curve

Definition. Let E_1 and E_2 be elliptic curves defined over a field K, assume for brevity that $E_1 : y^2 = x^3 + ax + b$, then a map

$$\phi : E_1(\bar{K}) \to E_2(\bar{K})$$

with the property that

- ϕ is a group homomorphism so $\phi(O_1) = \phi(O_2)$.
- $\phi(x, y) = (R_1(x, y), R_2(x, y))$ for some $R_1, R_2 \in K(E_1)$

(think of $K(E_1)$ as the rational functions $K(x, y)$ where any occurence of y^2 is replaced by $x^3 + ax + b$) is called an *isogeny*. There are some technicalities when the rational functions in $K(x, y)$ are not defined, but it is sufficient to know this rational functions defined on all but possibly finite points of E_1, we will deal with this later. If $E_1 = E_2$ we call the isogeny an *endomorphism*.

We sometimes write $\phi : E \to E$ if the isogeny is defined over K.

Example 2. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over K with $\operatorname{char} K \neq 2$

1. The trivial map taking any $P \in E(\bar{K})$ to O is the constant isogeny. Another easy isogeny is the map defined by $\phi(P) = -P$ for all $P \in E(\bar{K})$. This is defined by $\phi(x, y) := (x, -y)$ for points in $E\backslash\{O\}$
2. The duplication of points is an isogeny (endomorpism) $\phi(P) = 2P$. The rational functions can be computed as follows

$$R_1(x, y) = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x$$
$$R_2(x, y) = \frac{3x^2 + a}{2y}\left(3x - \left(\frac{3x^2 + a}{2y}\right)^2\right) - y$$

3. Let $K = \mathbb{F}_p$ for a prime number p and E be defined over K. Then, the *Frobenious endomorphism* is the isogeny defined by $\phi(x, y) = (x^p, y^p)$ one easily checks that for any $P \in E(\bar{K})\backslash\{O\}$ the point $\phi(P) \in E(\bar{K})\backslash\{O\}$.

Notation. The Frobenious map for an elliptic curves E over $\mathbb{F}_p$ is denoted ϕ_p.

In this course, unless otherwise stated, our elliptic curve is given by short Weierstrass form $y^2 = x^3 + ax + b$. Suppose we have an isogeny of elliptic curve given by short Weierstrass forms. Because y^2 can be replaced by polynomial in x we may write the numerators and denominators of R_i as element in $K[x] + yK[x]$. We can further simplify by multiplying the denominators say $p(x)+yq(x)$ with $p(x)-yq(x)$ and replace y^2 with a polynomial in x (this will not vanish identically on C, because they are rational functions in $K(C)$). So in fact we can write R_i in the form

$$\frac{p_i(x) + yq_i(x)}{s_i(x)}$$

for some $p, q, s \in K[x]$. Observe now that since ϕ is a group homomorphism we have

$$\phi(x, -y) = \phi(-(x, y)) = -\phi(x, y)$$

and so

- $R_1(x, y) = R_1(x, -y)$ implying that the numerator of $R_1(x, y)$ is only $p_1(x)$ i.e. $R_1(x, y) = r_1(x) \in K(x)$
- $R_2(x, y) = -R_2(x, -y)$ implying that the numerator of $R_2(x, y)$ is only $yq_2(x)$ i.e. $R_2(x, y) = yr_2(x) \in yK(x)$

So we can write an isogeny as a map between elliptic curves in Weierstrass short form

$$\phi : E_1(\bar{K}) \to E_2(\bar{K})$$

such that $\phi(x, y) = (r_1(x), yr_2(x))$ for rational functions $r_1, r_2 \in K(x)$. We now describe the situation when the rational functions are not defined at a point. For this let us write $r_1(x) = p(x)/q(x)$ for $p, q \in K[x]$ and $\gcd(p, q) = 1$. We will need the following results which we give as an exercise:

Exercise 3. Suppose $E : y^2 = x^3 + ax + b$ be an elliptic curve over K ($\operatorname{char} K > 3$ or $\operatorname{char} K = 0$). Let $\phi : E(\bar{K}) \to E(\bar{K})$ be an isogeny with

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right) \qquad \gcd(p, q) = 1, \gcd(s, t) = 1$$

1. Use the fact that (x, y) and $\phi(x, y)$ lies on E to show that

   $$\frac{(x^3 + ax + b)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}$$

   for some $q, u \in K[x]$ with $\gcd(q, u) = 1$. Hint: Show that a common root u and q is a root of p.

2. Suppose that $t(\alpha) = 0$, then use the fact that $x^3 + ax + b$ has no multiple root and all roots of t^2 are multiple roots to show that $q(\alpha) = 0$. In other words, show that $q(\alpha) \neq 0$ implies that $\phi(\alpha, \beta)$ is defined for any point $(\alpha, \beta) \in E$.

3. Show that $\frac{d}{dx}\frac{p(x)}{q(x)} \equiv 0$ iff $p'(x) \equiv 0$ and $q'(x) \equiv 0$ (so if p is nonconstant in this case $\operatorname{char} K > 0$).

So if $P = (\alpha, \beta)$ and $q(\alpha) = 0$ we assume that $\phi(P) = O$[1], if $q(\alpha) \neq 0$ we know from the above exercise that ϕ is defined at P.

[1] we can also go to the projective plane to check this