Abelian varieties over finite fields

Lassina Dembélé
lassina.dembele@kcl.ac.uk
King's College London
Preliminary Arizona Winter School 2024

Version: September 29, 2023

Contents

1 Definition and properties of abelian varieties **3**
1.1 Definition . . . 3
1.2 Commutativity . . . 4
1.3 Theorem of the cube . . . 4
1.4 Theorem of the square . . . 5
1.5 Isogenies . . . 5
1.6 Structure of torsion . . . 5

2 The dual variety **7**
2.1 Definition of the dual . . . 7
2.2 Construction of the dual . . . 7
2.3 Polarisations . . . 7

3 Structure of the isogeny category **8**
3.1 Poincaré reducibility . . . 8
3.2 The isogeny category . . . 8

4 Basic example: elliptic curves **8**
4.1 Definition of an elliptic curve . . . 8
4.2 Definition of the group law . . . 10
4.3 Computing with the group law . . . 12

1 Definition and properties of abelian varieties

We fix a field k, and let $\overline{k}$ be an algebraic closure of k. We recall the definition and basic properties of abelian varieties. We give some indications as to how the theory is developed, but omit most of the arguments....

1.1 Definition

Definition 1.1. *A* algebraic variety *X over k is a separated k-scheme X of finite type, which is geometrically integral (i.e. $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\overline{k})$ is integral). We say that X is* complete *if it is proper.*

Definition 1.2. *A* group variety *over a field k is a k-variety G together with k-morphisms $m : G \times G \to G$ (the group law) and $i : G \to G$ (the inverse) and a k-rational point $e \in G(k)$ (the identity element) such that we have the following commutative diagrams:*

(i) Associativity of the group law:

$$\begin{tikzcd} G \times G \times G \arrow[r, "id_{G\times G\times G}"] \arrow[d, "id_{G\times G\times G}"'] & (G \times G) \times G \arrow[r, "m \times id_G"] & G \times G \arrow[d, "m"] \\ G \times (G \times G) \arrow[r, "id_G \times m"] & G \times G \arrow[r, "m"] & G \end{tikzcd}$$

(ii) Identity element:

$$\begin{tikzcd} G \times \mathrm{Spec}(k) \arrow[r, "id_G \times e"] \arrow[dr, "j_1"'] & G \times G \arrow[d, "m"] & \mathrm{Spec}(k) \times G \arrow[l, "e \times id_G"'] \arrow[dl, "j_2"] \\ & G & \end{tikzcd}$$

where $j_1 : \mathrm{Spec}(k) \times G \to G$ and $j_2 : G \times \mathrm{Spec}(k) \to G$ are the projection maps on G.

(iii) Existence of inverse element:

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[d, "(id_G, i)"'] & \mathrm{Spec}(k) \arrow[d, "e"] & G \arrow[l, "\pi"'] \arrow[d, "(i, id_G)"] \\ G \times G \arrow[r, "m"'] & G & G \times G \arrow[l, "m"] \end{tikzcd}$$

where $\pi : G \to \mathrm{Spec}(k)$ is the structure morphism.

Definition 1.3. *An* abelian variety *A defined over k is a k-group variety which is complete as a k-variety.*

1.2 Commutativity

We begin by explaining the most basic fact, which is commutativity. The main ingredient in proving this is the following general fact:

Lemma 1.4 (Rigidity Lemma)**.** *Let X be a complete variety over k, and Y and Z be arbitrary varieties. Let $f : X \times Y \to Z$ be a map of varieties. Suppose there exists $x_0 \in X$ and $y_0 \in Y$ such that the restrictions of f to $X \times \{y_0\}$ and $\{x_0\} \times Y$ are constant. Then f is constant.*

Corollary 1.5. *Let X and Y be abelian varieties and let $f : X \to Y$ be any map of varieties such that $f(0) = 0$. Then f is a morphism of abelian varieties, i.e., f respects the group structure.*

Proof. Consider the map

$$\begin{aligned} h : X \times X &\to Y \\ (x, y) &\mapsto f(x + y) - f(x) - f(y). \end{aligned}$$

Then $h(x, 0) = h(0, x) = 0$ for all $x \in X$. So, by the Rigidity Lemma $h = 0$, meaning that f is a homomorphism. □

Corollary 1.6. *An abelian variety is commutative.*

Proof. The map $x \mapsto -x$ takes 0 to 0 and is therefore a homomorphism, which implies commutativity. □

1.3 Theorem of the cube

Theorem 1.7 (Theorem of the cube)**.** *Let X, Y and Z be varieties such that X and Y complete. Let $x_0 \in X, y_0 \in Y$ and $z_0 \in Z$ be points. Let $\mathscr{L}$ be a line bundle on $X \times Y \times Z$ such that the restrictions of $\mathscr{L}$ to $X \times Y \times \{z_0\}, X \times \{y_0\} \times Z$ and $\{x_0\} \times Y \times Z$ are trivial. Then $\mathscr{L}$ is trivial.*

Corollary 1.8. *Let A be an abelian variety. Let $\pi_i : A \times A \times A \to A$ denote the projection map on the i-th factor, and set $\pi_{ij} := \pi_i + \pi_j$ and $\pi_{123} := \pi_1 + \pi_2 + \pi_3$. Let $\mathscr{L}$ be a line bundle on A. Then the line bundle*

$$\mathscr{L}' := \pi_{123}^* \mathscr{L} \otimes \pi_{12}^* \mathscr{L}^{-1} \otimes \pi_{13}^* \mathscr{L}^{-1} \otimes \pi_{23}^* \mathscr{L}^{-1} \otimes \pi_1^* \mathscr{L} \otimes \pi_2^* \mathscr{L} \otimes \pi_3^* \mathscr{L}$$

on $A \times A \times A$ is trivial.

Proof. This follows immediately from the theorem of the cube. For example, if we restrict to $A \times A \times \{0\}$ then $\pi_{123}^* \mathscr{L} = \pi_{12}^* \mathscr{L}$, $\pi_{13}^* \mathscr{L} = \pi_1^* \mathscr{L}$, and $\pi_3^* \mathscr{L} = 1$, so all factors cancel. □

Corollary 1.9. *Let A be an abelian variety, and X an arbitrary variety. Let $f, g, h : X \to A$ be maps of varieties, and $\mathscr{L}$ a line bundle on A. Then the line bundle*

$$\mathscr{L}' := (f + g + h)^* \mathscr{L} \otimes (f + g)^* \mathscr{L}^{-1} \otimes (f + h)^* \mathscr{L}^{-1} \otimes (g + h)^* \mathscr{L}^{-1} \otimes f^* \mathscr{L} \otimes g^* \mathscr{L} \otimes h^* \mathscr{L}$$

on X is trivial.

Proof. This follows from Corollary 1.8 by considering the map $X \to A \times A \times A$ given by (f, g, h). □

1.4 Theorem of the square

Theorem 1.10 (Theorem of the square). *Let A be an abelian variety and $\mathscr{L}$ a line bundle on A, and $x, y \in A(\bar{k})$. Then $t_{x+y}^*\mathscr{L} \otimes \mathscr{L} = t_x^*\mathscr{L} \otimes t_y^*\mathscr{L}$. (Here t_x denotes translation by x.)*

Proof. Apply Corollary 1.9 with $f = t_x$ (constant map), $g = t_y$, and $h = id_A$. □

Define $\mathrm{Pic}(A)$ to be the set of isomorphism classes of line bundles on A. For a line bundle $\mathscr{L}$, let $\phi_{\mathscr{L}} : A(\bar{k}) \to \mathrm{Pic}(A)$ be the map $\phi_{\mathscr{L}}(x) = t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. The theorem of the square states exactly that $\phi_{\mathscr{L}}$ is a group homomorphism.

1.5 Isogenies

Proposition 1.11. *Let $f : A \to B$ be a homomorphism of abelian varieties. Then the following conditions are equivalent:*

(a) f is surjective and $\dim(A) = \dim(B)$;

(b) $\ker(f)$ is a finite group scheme and $\dim(A) = \dim(B)$;

(c) f is a finite, flat and surjective morphism.

Definition 1.12. *Let $f : A \to B$ be a homomorphism of abelian varieties. We say that f is an* isogeny *if it satisfies the three equivalent conditions (a), (b) and (c) in Proposition 1.11. The* degree *of an isogeny f is $[k(A) : k(B)]$, the degree of the function field extension $k(A)/k(B)$. (Note that we have a homomorphism $k(B) \to k(A)$, since an isogeny is surjective.)*

Definition 1.13. *Let $f : A \to B$ be an isogeny. Then, we say that*

(i) f is separable *if $k(A)/k(B)$ is a separable extension.*

*(ii) f is (*purely*)* inseparable *if $k(A)/k(B)$ is a (purely) inseparable extension.*

Proposition 1.14. *Let $f : A \to C$ be an isogeny. Then, there exist*

(i) an abelian variety B;

(ii) an inseparable isogeny $g : A \to B$; and

(iii) a separable isogeny $h : B \to C$

such that $f = h \circ g$. This factorisation is unique up to isomorphism. In other words, if $f = h' \circ g' : A \to B' \to C$ is a second such factorisation then there is an isomorphism $\alpha : B \to B'$ such that $g' = \alpha \circ g$ and $h = h' \circ \alpha$.

1.6 Structure of torsion

For an integer n, let $[n]_A$ (or simply $[n]$) be the morphism

$$\begin{aligned} A(\bar{k}) &\to A(\bar{k}) \\ x &\mapsto nx. \end{aligned}$$

Proposition 1.15. *Let A be abelian variety, $\mathscr{L}$ a line bundle on A, and $n \in \mathbb{Z}$. Then, we have*

$$[n]^*\mathscr{L} = \mathscr{L}^{(n^2+n)/2} \otimes [-1]^*\mathscr{L}^{(n^2-n)/2}.$$

In particular,

(i) if $\mathscr{L}$ is symmetric (i.e. $[-1]^*\mathscr{L} = \mathscr{L}$) then $[n]^*\mathscr{L} = \mathscr{L}^{n^2}$;

(ii) if $\mathscr{L}$ is anti-symmetric (i.e. $[-1]^*\mathscr{L} = \mathscr{L}^{-1}$) then $[n]^*\mathscr{L} = \mathscr{L}^n$.

Proof. Applying Corollary 1.9 to the maps $[n]$, $[1]$, and $[-1]$, we see that

$$\mathscr{L}' := [n]^*\mathscr{L} \otimes [n+1]^*\mathscr{L}^{-1} \otimes [n-1]^*\mathscr{L}^{-1} \otimes [n]^*\mathscr{L} \otimes \mathscr{L} \otimes [-1]^*\mathscr{L}$$

is trivial. In other words, we have

$$[n+1]^*\mathscr{L} = [n]^*\mathscr{L}^2 \otimes [n-1]^*\mathscr{L}^{-1} \otimes \mathscr{L} \otimes [-1]^*\mathscr{L}.$$

The result now follows by induction. □

Theorem 1.16. *Let A be an abelian variety of dimension g, and $n > 0$ an integer. Then $[n]_A : A \to A$ is an isogeny; it is étale if and only if $(\mathrm{char}(k), n) = 1$.*

Proof. One can show that abelian varieties are projective. Let $\mathscr{L}$ be an ample line bundle on A. Replacing $\mathscr{L}$ by $\mathscr{L} \otimes [-1]^*\mathscr{L}$, we can assume $\mathscr{L}$ is symmetric. Since $[n]^*\mathscr{L} = \mathscr{L}^{n^2}$, it is ample. However, the restriction of this to the n-torsion is obviously trivial. Since the n-torsion is a complete variety on which the trivial bundle is ample, it must be finite. This implies that $[n]$ is surjective, by reasoning with dimension. □

Proposition 1.17. *The degree of $[n]_A$ is n^{2g}.*

Proof. Let $f : X \to Y$ be a finite map of complete varieties of degree d. If $D_1, \dots, D_n$ are divisors on Y, where $n = \dim(X) = \dim(Y)$, then there is an equality of intersection numbers:

$$(f^*D_1 \cdots f^*D_n) = d(D_1 \cdots D_n).$$

Now, let D be an ample divisor such that $[-1]^*D$ is linearly equivalent to D (e.g., the divisor associated to the line bundle used above). Then $[n]^*D$ is linearly equivalent to n^2D. We thus find

$$\deg([n])(D \cdots D) = ((n^2D) \cdots (n^2D)) = n^{2g}(D \cdots D).$$

Since D is ample, $(D \cdots D) \neq 0$, and thus $\deg([n]) = n^{2g}$. □

One can show that $[n] : A \to A$ induces multiplication by n on the tangent space. This shows that $[n]$ is separable if and only if n is prime to the characteristic. Combined with the above (and the usual induction argument), we see that:

Corollary 1.18. *If $(\mathrm{char}(k), n) = 1$, then $A[n](\bar{k})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$.*

Since $[p]$ is not separable, $A[p](\bar{k})$ must have fewer than p^{2g} points. We will see later, when studying group schemes, that it can have at most p^g points.

Corollary 1.19. *Let $f : A \to B$ be an isogeny of degree n. Then there exists an isogeny $g : B \to A$ such that $g \circ f = [n]_A$ and $f \circ g = [n]_B$.*

2 The dual variety

2.1 Definition of the dual

Let k be an arbitrary field, and A an abelian variety defined over k. We define $\mathrm{Pic}(A)$ to be the set of isomorphism classes of line bundles on A. Then, we let $\mathrm{Pic}^0(A)$ be the subgroup consisting of those line bundles $\mathscr{L}$ which are translation invariant, i.e., which satisfy $t_x^*(\mathscr{L}) \simeq \mathscr{L}$ for all $x \in A$. We define the following functor. For each variety T over k, let $F(T)$ be the of isomorphism classes of line bundles $\mathscr{L}$ on $A \times T$ satisfying the following two conditions:

(a) for all $t \in T$, the restriction of $\mathscr{L}$ to $A \times \{t\}$ belongs to $\mathrm{Pic}^0(A)$; and

(b) the restriction of $\mathscr{L}$ to $\{0\} \times T$ is trivial.

We see that $F(k) = \mathrm{Pic}^0(A)$. We define the *dual abelian variety* $A^\vee$ to be the variety that represents F, if it exists. We will always assume that the dual variety $A^\vee$ exists. Then, it automatically comes with a universal bundle $\mathscr{P}$ on $A \times A^\vee$, which is called the *Poincaré bundle*.

2.2 Construction of the dual

Let $\mathscr{L}$ be an ample bundle on A. We then have the map

$$\begin{aligned} \phi_{\mathscr{L}} : A &\to \mathrm{Pic}^0(A) \\ x &\mapsto [t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}]. \end{aligned}$$

By the theorem of the square, the image is in $\mathrm{Pic}^0(A)$. One can prove the map $\phi_{\mathscr{L}}$ it is surjective, and has finite kernel $K(\mathscr{L})$. In fact, $K(\mathscr{L})$ has a natural structure of a group scheme. This suggests that $A^\vee$ should be the quotient $A/K(\mathscr{L})$, and one can show that this is indeed the case.

Proposition 2.1. *Let $f : A \to B$ be a homomorphism of abelian varieties over k, and $\mathscr{P}_A$ and $\mathscr{P}_B$ be the Poincaré line bundles on A and B, respectively. Then, there exists an induced homomorphism $f^\vee : B^\vee \to A^\vee$, called the* dual *or* transpose *of f. Thus, $f^\vee$ is the unique homomorphism such that*

$$(id_A \times f^\vee)^* \mathscr{P}_A \simeq (f \times id_B)^* \mathscr{P}_B$$

as line bundles on $A \times B^\vee$ with rigidification along $\{0\} \times B^\vee$.

2.3 Polarisations

Definition 2.2. *Let A be an abelian variety. A* polarisation *on A is an isogeny $\lambda : A \to A^\vee$ such that $\lambda_{\overline{k}} : A(\overline{k}) \to \mathrm{Pic}^0(A)$ is given by $\lambda_{\overline{k}} = \phi_{\mathscr{L}}$ for some ample line bundle $\mathscr{L}$ on A over $\overline{k}$. The* degree *of the polarisation λ is its degree as an isogeny. An abelian variety together with a polarisation is called a* polarised abelian variety.

There is an obvious notion of morphisms of polarised abelian varieties. If λ has degree 1, then we say that (A, λ) is a *principally polarised* abelian variety.

3 Structure of the isogeny category

3.1 Poincaré reducibility

Theorem 3.1 (Poincaré reducibility)**.** *Let A be an abelian variety, and let B be an abelian subvariety. Then there exists an abelian subvariety C such that $B \cap C$ is finite and $B \times C \to A$ is an isogeny.*

Proof. Choosing polarisations on A and A/B to identify them with their duals, the dual to the quotient map $A \to A/B$ is a map $A/B \to A$. We let C be its image. The properties are easy to verify. □

We say that an abelian variety A is *simple* if the only abelian subvarieties of A are 0 and A.

Proof. Every abelian variety is isogenous to a product of simple varieties. □

3.2 The isogeny category

Define a category **Isog** as follows. The objects are abelian varieties. For two abelian varieties A and B, we put

$$\mathrm{Hom}_{\mathbf{Isog}}(A, B) = \mathrm{Hom}(A, B) \otimes \mathbb{Q}.$$

One can show that if $f : A \to B$ is an isogeny then there exists an isogeny $g : B \to A$ such that $gf = [n]$, for some n; it follows that $\frac{1}{n}g$ is the inverse to f in **Isog**. Thus isogenies become isomorphisms in **Isog**.

It is not difficult to see that **Isog** is in fact an abelian category. The simple objects of this category are exactly the simple abelian varieties. Poincaré's theorem shows that **Isog** is semi-simple as an abelian category. From this formalism, and general facts about abelian varieties, we deduce two results:

1. The decomposition (up to isogeny) into a product of simple abelian varieties is unique (up to isogeny). (Reason: in any semi-simple abelian category, the decomposition into simples is unique up to isomorphism.)
2. If A is a simple abelian variety then $\mathrm{End}(A) \otimes \mathbb{Q}$ is a division algebra over $\mathbb{Q}$. (Reason: if A is a simple object in an abelian category and $\mathrm{End}(A)$ contains a field k, then it is a division algebra over k.)

4 Basic example: elliptic curves

We will assume throughout this section, that k is a field of characteristic different from 2.

4.1 Definition of an elliptic curve

Definition 4.1. *Let $E : y^2 = f(x)$ be a cubic curve, where $f(x) = x^3 + ax^2 + bx + c$. Then, the* discriminant *Δ_E of E is the discriminant Δ_f of the polynomial f:*

$$\Delta_E := \Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Example 4.2. For a cubic curve $E : y^2 = x^3 + ax + b$, $a, b \in k$, the discriminant $\Delta_E = -4a^3 - 27b^2$.

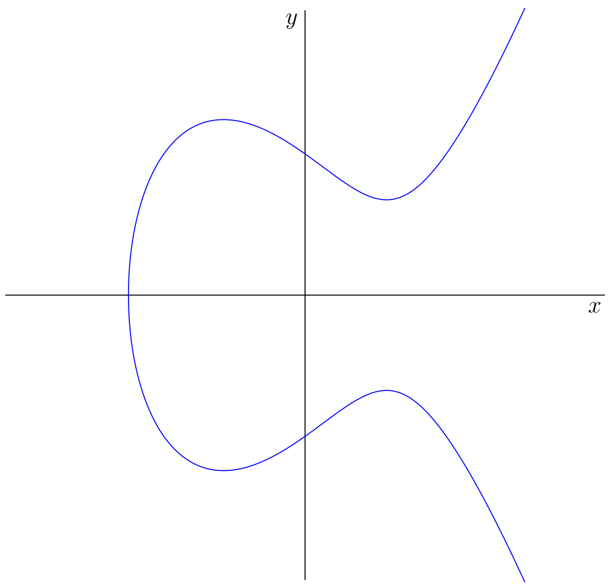

Figure 1: Real points of the elliptic curve $y^2 = x^3 - 8$

We can now give the definition of an elliptic curve.

Definition 4.3. *Let k be a field with characteristic different from 2. An* elliptic curve *over k is a cubic curve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$, with $a, b, c \in k$, such that $\Delta_E \neq 0$.*

The following lemma expresses the discriminant of a cubic polynomial in terms of its roots.

Lemma 4.4. *Let $f(x) = x^3 + ax^2 + bx + c$, with $a, b, c \in k$, and e_1, e_2, e_3 the roots of f in $\overline{k}$. Then the discriminant of f is given by*

$$\Delta_f = [(e_1 - e_2)(e_2 - e_3)(e_1 - e_3)]^2.$$

A useful criteria to check whether a cubic is an elliptic curve.

Proposition 4.5. *Let $E : y^2 = f(x)$ be a cubic curve, with $f(x) = x^3 + ax^2 + bx + c$ and $a, b, c \in k$. Then, we have E is an elliptic curve $\iff$ f has* **no** *repeated roots $\iff$ $\Delta_E \neq 0$.*

Example 4.6. (a) The cubic $E : y^2 = x^3 - 2x + 1$ is an elliptic curve over $\mathbb{Q}$ since $\Delta_E = -4(-2)^3 - 27(1) = 5 \neq 0$.

(b) For $c \in \mathbb{Z}$ non-zero, the curve $E : y^2 = x^3 + c$ is an elliptic curve over $\mathbb{Q}$ since $\Delta_E = -27c^2 \neq 0$. (See Figure 1 for the real locus of this curve.)

(c) The curve $E : y^2 = x^3 + x^2 + 1$ is an elliptic curve over $\mathbb{F}_3$. Definition 4.1 shows that $\Delta_E = -1 \neq 0 \in \mathbb{F}_3$. Alternatively, letting $f(x) = x^3 + x^2 + 1$, we see that $f'(x) = 3x^2 + 2x = 2x$ $(\mathrm{char}(\mathbb{F}_3) = 3)$. So $\gcd(f, f') = 1$, which implies that f has distinct roots.

4.2 Definition of the group law

The homogenisation of the curve E in Definition 4.3 is given by

$$E : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3. \tag{1}$$

The *only* point at infinity on E is $[0:1:0]$, which we denote by ∞ from now on. We will see that this point is the *neutral* element in the group structure on E.

Definition 4.7. *Let E be an elliptic curve over k, and k' a field containing k. The set of* k'-rational points *of E is the set of k'-rational points on the homogenisation of E, namely*

$$E(k') := \left\{[x:y:z] \in \mathbf{P}^2(k') : zy^2 = x^3 + ax^2z + bxz^2 + cz^3\right\}.$$

Since $\mathbf{P}^2(k') = \mathbf{A}^2(k') \sqcup \{Z=0\}$, and $\infty = [0:1:0]$ is the unique point at infinity, we can write

$$E(k') := \left\{(x,y) \in K'^2 : y^2 = x^3 + ax^2 + bx + c\right\} \sqcup \{\infty\}.$$

Example 4.8. Let $k = \mathbb{Q}$, and $E : y^2 = x^3 + 1$. The set of $\mathbb{Q}$-rational points $E(\mathbb{Q})$ is given by

$$E(\mathbb{Q}) = \{(-1,0),(0,\pm1),(2,\pm3)\} \cup \{\infty\}.$$

We have the natural inclusions $E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$. (See Figure 3 for the sets $E(\mathbb{Q}) \subset E(\mathbb{R})$.)

Example 4.9. Let $E : y^2 = x^3 + 2x + 5$ be the curve over $\mathbb{F}_{11}$. Then, we have

$$E(\mathbb{F}_{11}) = \{(0,\pm4),(3,\pm4),(4,0),(-3,\pm4),(-2,\pm2)\} \cup \{\infty\}.$$

Let $h \in k[x]$ be a polynomial of degree n. The number of roots of h counted with multiplicity in $\overline{k}$ is n. The following theorem can be see as a generalisation of that statement to elliptic curves.

Theorem 4.10 (Bézout)**.** *Let k be a field, $E : y^2 = x^3 + ax^2 + bx + c$ an elliptic curve over k, and $L \subset \mathbf{P}^1(\overline{k})$ a line. The set $L \cap E$ contains* three *points counted with multiplicity.*

Let $L : \alpha x + \beta y + \gamma = 0$ be a line, with $\alpha, \beta, \gamma \in k$. We want to find $L \cap E \subset \mathbf{P}^1(\overline{k})$, so we first homogenise $L : \alpha X + \beta Y + \gamma Z = 0$. Then we have two cases:

Case 1: The *unique* point infinity $\infty = [0:1:0] \in L \cap E$.
In that case, we see that $\alpha x + \beta y + \gamma z = 0$ implies that $\beta = 0$. This means that either:

(a) L is the line at infinity $Z = 0$. In that case $P = \infty$ is the *only* point of intersection, hence has multiplicity *three.*

(b) L is vertical line $\alpha X + \gamma Z = 0$ ($\alpha \neq 0$). The other points of intersection are $(x_0, \pm y_0)$, where $x_0 = -\frac{\gamma}{\alpha}$ and $y_0 = \sqrt{f(x_0)}$. If $y_0 = 0$, then we get a unique point $P = (x_0, 0)$ with multiplicity *two*; otherwise, we get two distinct points $P = (x_0, y_0)$ and $Q = (x_0, -y_0)$, with multiplicity *one* each. In either case, the point ∞ has multiplicity *one.*

Case 2: $L \cap E$ consists of three *affine* points counted with multiplicity.

(a) $L \cap E$ has *two distinct* points P and Q: In this case, L is a tangent to E at P or Q. The tangent point has multiplicity *two*, and the other point has multiplicity *one.*

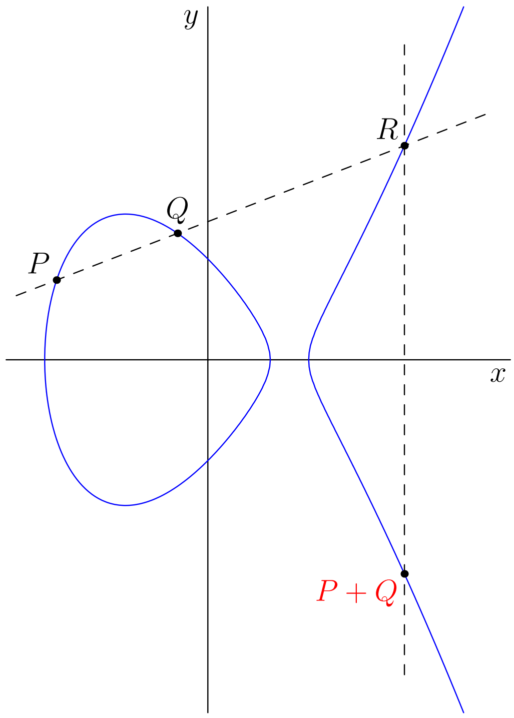

Figure 2: Group addition law

(b) $L \cap E$ has *three disctint* points P, Q and R. In that case, each point has multiplicity *one*.

We are now ready to define the group structure on $E(\overline{k})$.

Definition 4.11. *Let E be an elliptic curve over k, and*

$$E(\overline{k}) = \{(x,y) \in \overline{k}^2 : y^2 = x^3 + ax^2 + bx + c\} \sqcup \{\infty\}.$$

The addition law + on $E(\overline{k})$ is defined as follows:

(i) The neutral *element is ∞;*

(ii) If $P, Q, R \in E(\overline{k})$ are collinear, then $P + Q + R = \infty$ ($\Leftrightarrow P + Q = -R$).

In words, to obtain the sum $P+Q$, we first draw the line L through P and Q (if $P \neq Q$) or the tangent line (if $P = Q$), and let R be its third intersection point with $E(\overline{k})$. If $R = (x_R, y_R)$ is affine, then $P + Q = -R = (x_R, -y_R)$; otherwise, $P + Q = \infty$. (See Figure 2.)

Remark 4.12. By Definition 4.11 and the discussion preceding it, if $P = (x,y)$ is affine, then the *negative* of P is $-P = (x, -y)$ since (x,y) and $(x,-y)$ are on a vertical line, which intersects E at ∞.

Example 4.13. Let $E : y^2 = x^3 + 1$ over $\mathbb{Q}$ be the curve in Example 4.8. Let $P = (-1, 0)$ and $Q = (0, 1)$. Th equation of the line through P and Q is $y = x + 1$. So, we see that the point $R = (2, 3)$. The line through R and ∞ is the vertical line $x = 2$. It intersects E at $(2, -3)$, so $P + Q = (2, -3)$ (see Figure 3). Similarly, one can compute the sum of any two points in $E(\mathbb{Q})$.

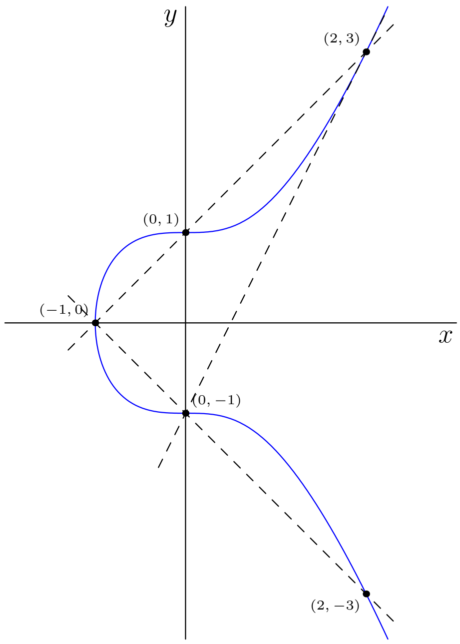

Figure 3: Euler cubic: $y^2 = x^3 + 1$

The theorem below says that Definition 4.11 makes $E(\overline{k})$ into an abelian group.

Theorem 4.14. *Let E be an elliptic curve defined over a field K. Then, $E(\overline{k})$ is an abelian group under the operation $+$, with identity element $\infty (= [0:1:0])$. In other words, we have*

(i) $P + Q = Q + P \ \ \forall P, Q \in E(\overline{k})$ *(commutativity).*

(ii) $P + \infty = P \ \ \forall P \in E(\overline{k})$ *(identity element).*

(iii) If $P = (x, y)$*, then* $-P = (x, -y)$ *(opposite element).*

(iv) $P + (Q + R) = (P + Q) + R, \ \ \forall P, Q, R \in E(\overline{k})$ *(associativity).*

Proof. Properties (i)-(iii) follow easily from Definition 4.11 and the discussion preceding it. However, the last statement (iv) is very hard to prove, and beyond the scope of this course. □

4.3 Computing with the group law

We now give a more explicit description of the group law on $E(\overline{k})$.

Proposition 4.15. *Let E be as above, and $P_1, P_2 \in E(\overline{k})$. Then $P_1 + P_2$ is given by*

(1) If $P_1 = \infty$ *then* $P_1 + P_2 = P_2$*; if* $P_2 = \infty$*, then* $P_1 + P_2 = P_1$.

Assume that $P_1, P_2 \neq \infty$, so that $P_i = (x_i, y_i)$, $i = 1, 2$; then

(2) If $x_1 = x_2$ *and* $y_1 = -y_2$ *then* $P_1 + P_2 = \infty$.

(3) If $x_1 = x_2$ *and* $y_1 = y_2 \neq 0$ *then set* $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$*; otherwise, set* $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$*. Let* $x_3 = \lambda^2 - a - x_1 - x_2$, $y_3 = y_1 + \lambda(x_3 - x_1)$ *and* $P_3 = (x_3, -y_3)$*, then* $P_1 + P_2 = P_3$.

Proof. We note that (1) and (2) are just a restatement of Theorem 4.14 (ii) and (iii). So we only need to prove (3). In that case, let $L : y = \lambda x + \nu$ be the line through P_1, P_2, and $R = (x_3, y_3)$ its 3rd point of intersection with E. If $P_1 = P_2$, then L is the tangent line at P_1 with $\lambda = \frac{3x_1^2+2ax_1+b}{2y_1}$ and $\nu = y_1 - \lambda x_1$. Otherwise, L is the line with slope $\lambda = \frac{y_2-y_1}{x_2-y_1}$ and x-intercept $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. The x-coordinates x_1, x_2 and x_3 of the points in $L \cap E$ (counted with multiplicity) satisfy the equation

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c.$$

By moving all terms to the same side, expanding and then factorising, we get

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + c - \nu^2 = (x - x_1)(x - x_2)(x - x_3) = 0.$$

By equating the terms of degree 2, we get $x_1 + x_2 + x_3 = -(a - \lambda^2)$. From this, we recover $R = (x_3, y_3)$, which gives $P_1 + P_2 = P_3 = (x_3, -y_3)$. □

Remark 4.16. From proof above, we note that if $x_i \in k$, then $y_i = \lambda x_i + \nu \in k$ and the intersection point (x_i, y_i) is defined over k. We also note that, if two of the roots x_1, x_2, x_3 are defined over k, then so is the third one since $x_1 + x_2 + x_3 = -(a - \lambda^2) \in k$.

Example 4.17. Let $E : y^2 = x^3 + 73$, and $P = (2, 9)$, $Q = (3, 10)$.

(a) The slope of the line through P and Q is $\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{10-9}{3-2} = 1$. Let $R = (x_R, y_R)$ be the 3rd point of intersection of this line with E. Then, we have $x_P + x_Q + x_R = \lambda^2$. So $x_R = (1)^2 - 2 - 3 = -4$, and $y_R = y_P + \lambda(x_R - x_P) = 9 + (-4 - 2) = 3$. Hence $P + Q = -R = (-4, -3)$.

(b) The slope of the tangent line at P is $\lambda = \frac{3x_P^2}{2y_P} = \frac{3(2)^2}{2(9)} = \frac{2}{3}$. For the 3rd point of intersection $R = (x_R, y_R)$, we have $2x_P + x_R = \lambda^2$. So $x_R = (\frac{2}{3})^2 - 2(2) = -\frac{32}{9}$, and $y_R = y_P + \lambda(x_R - x_P) = 9 + \frac{2}{3}(-\frac{32}{9} - 2) = \frac{143}{27}$. Hence $2P = -R = -(x_R, y_R) = (x_R, -y_R) = (-\frac{32}{9}, -\frac{143}{27})$.

Example 4.18. Let $E : y^2 = x^3 + 2x + 5$ be the curve defined $\mathbb{F}_{11}$ in Example 4.9, and $P = (-3, 4)$. We compute $2P$ using Proposition 4.15. We have $\lambda = \frac{3x_P^2+2}{2y_P} = \frac{3(-3)^2+2}{2(4)} = 5 \bmod 11$. So, we have $x_{2P} = \lambda^2 - 2x_P = (5^2) - 2(-3) = 25 + 6 = -2 \bmod 11$. So, we get that $-y_{2P} = y_P + \lambda(x_{2P} - x_P) = 4 + 5(-2 - (-3)) = -2 \bmod 11$. This gives $y_{2P} = 2$ and $2P = (-2, 2)$. If we compute $4P$, we obtain $4P = 2(2P) = 2(-2, 2) = (-3, -4) = -P$.

This means that $5P = (4 + 1)P = \infty$. Since $P \neq \infty$, we see that P is a point of order 5. Now, let us observe that $Q = (4, 0) \in E(\mathbb{F}_{11})$ is a point of order 2 since $y_Q = 0$, hence $Q = -Q$. (Observe that, if $Q = (x, y) \in E(K)$ then $-Q = (x, -y)$.) This means that $P + Q$ is a point of order 10. Since $\#E(\mathbb{F}_{11}) = 10$, we deduce from these computations that $E(\mathbb{F}_{11})$ is a cyclic group of order 10.

Corollary 4.19. *If $k \subseteq k' \subseteq \overline{k}$ is a subfield, then $E(k')$ is a subgroup of $E(\overline{k})$.*

Proof. By definition, the identity element $\infty \in E(k')$; also $P = (x, y) \in E(k')$ implies that $-P = (x, -y) \in E(k')$. So we only need to show that

$$P, Q \in E(k') \Rightarrow P + Q \in E(k').$$

But this follows from Proposition 4.15 and Remark 4.16. □