Introduction to Algebra & Elliptic Curves

Lecture notes

Nagoya University (Fall 2026)

Henrik Bachmann (Math. Building Room 457, henrik.bachmann@math.nagoya-u.ac.jp)
Teaching assistant: Samyak Parashar
Lecture notes and exercises are available at: https://www.henrikbachmann.com

---

These notes contain the definitions, examples and results from the lectures, together with their proofs. We use results marked as "statement only" without proof and give references for them. The notes will be updated regularly (this is Version 5 from November 2, 2026).

If you find any typos in these notes, please let me know!

Contents

1 Overview **1**

2 Groups, rings and fields **10**

3 Elliptic curves **23**

1 Overview

▷ Lecture 1 (October 5, 2026)

We start with the questions and introduce the structures as we need them.

1.1 Goals and topics of the course

For a refresher on the assumed background, see the **Linear Algebra lecture notes** [LA].
In Linear Algebra I and II we worked with vectors and matrices whose entries were real (and sometimes complex) numbers. We added vectors, multiplied them by scalars, solved linear systems by Gaussian elimination, computed determinants and eigenvalues. Building on this background, the course has two goals:

1) **Algebraic structures.** Understand groups, rings and fields, building on familiar examples from linear algebra, and briefly meet modules.

2) **Elliptic curves.** Learn their geometry and group law, and study their points over the rational numbers, finite fields and other fields.

We use examples from arithmetic, geometry and linear algebra to make both topics concrete. An optional outlook later in the course is the Birch and Swinnerton-Dyer conjecture, which relates the rank of the group of rational points to the order of vanishing of an associated L-function at $s = 1$. The course is organized in five parts:

I	L1–2	From linear algebra to algebra, adding points on elliptic curves
II	L3–6	Groups: order, subgroups, homomorphisms, $\mathbb{Z}/n\mathbb{Z}$, cryptography
III	L7–10	Fields: polynomials, field extensions, multiplication as a matrix, finite fields
IV	L11–12	Rational points: elliptic curves over $\mathbb{F}_p$ and Mordell's theorem
V	L13–15	Symmetries: complex points and tori, Galois theory and elliptic curves

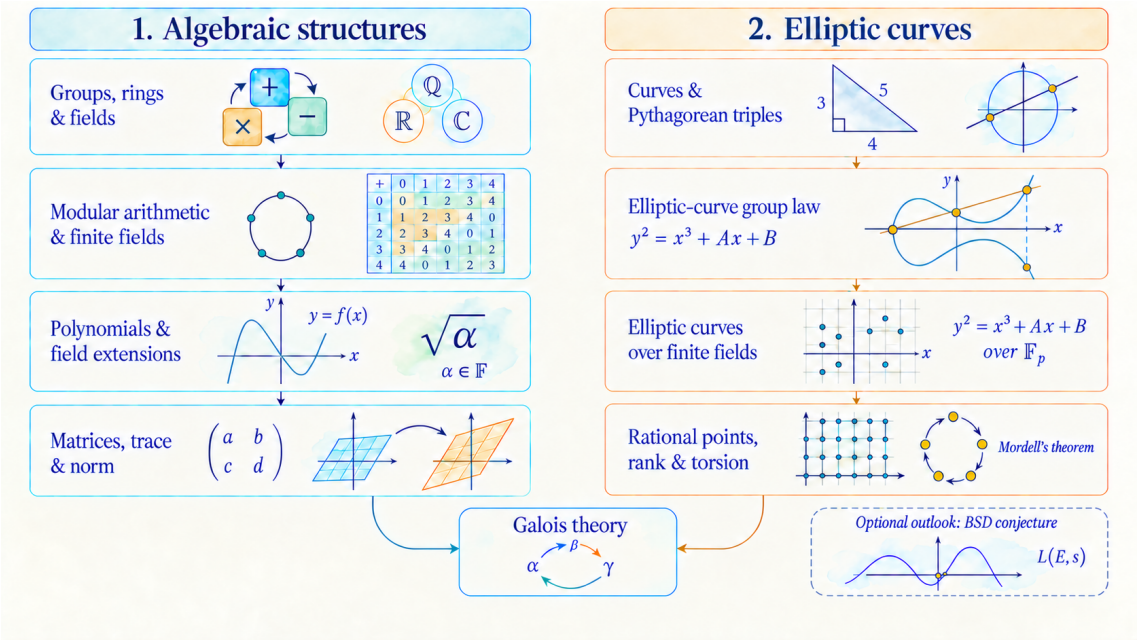


Figure 1: An illustrated map of the two course goals. The pictures are sketches. The BSD conjecture is an optional outlook.

Some questions that will guide us:

(1) Which rules did we use in linear algebra, and where else do they hold?

(2) Can a few elements **generate** everything (as a basis does in a vector space)?

(3) If an equation has no solution in our number system, can we **enlarge** the number system? For example, $t^2 + 1 = 0$ has no solution in $\mathbb{R}$, but the two solutions $\pm i$ in $\mathbb{C}$.

(4) Can numbers have **symmetries**? For example, complex conjugation $a + bi \mapsto a - bi$ respects addition and multiplication, and it exchanges the two solutions i and $-i$ of $t^2 + 1 = 0$.

1.2 A question to start with: congruent numbers

The following question is very easy to state, but very hard to answer. It was already studied by Arab mathematicians around the year 1000.

Definition 1.1. *A natural number n is called a* **congruent number** *if there exists a right triangle with* **rational** *side lengths $a, b, c \in \mathbb{Q}_{>0}$ and area n, i.e.*

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \frac{ab}{2} = n.$$

Example. *(i) $n = 6$ is congruent: take the triangle with sides $3, 4, 5$.*

(ii) $n = 5$ *is congruent:* $\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \frac{9}{4} + \frac{400}{9} = \frac{1681}{36} = \left(\frac{41}{6}\right)^2$ *and* $\frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3} = 5$.

(iii) $n = 7$ *is congruent:* $\left(\frac{24}{5}\right)^2 + \left(\frac{35}{12}\right)^2 = \left(\frac{337}{60}\right)^2$ *and* $\frac{1}{2} \cdot \frac{24}{5} \cdot \frac{35}{12} = 7$.

(iv) $n = 1, 2, 3$ *are not congruent. (For* $n = 1$ *this goes back to Fermat, around 1640.)*

(v) $n = 157$ *is congruent, but the simplest such triangle has a hypotenuse* c *whose numerator and denominator have* 48 *and* 46 *digits (found by Zagier).*

Trying out triangles is hopeless for numbers like 157. To approach this question differently, we first introduce a family of equations and their solutions.

A first look at elliptic curves

In this course, we describe an **elliptic curve over** $\mathbb{Q}$ by an equation in **short Weierstrass form**

$$E: \quad y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Q},$$

with non-zero **discriminant**

$$\Delta(E) = -16(4A^3 + 27B^2) \neq 0.$$

This condition says that the cubic $x^3 + Ax + B$ has no repeated root. Geometrically, the curve is **nonsingular**: its real picture has no cusp or crossing. A proof of the equivalence comes in Section 3.2.

An ordinary **point** on the curve is simply a solution (x, y) of its equation. We usually ask for solutions in a chosen number system R, such as $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, and write

$$E(R) = \{(x, y) \in R^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

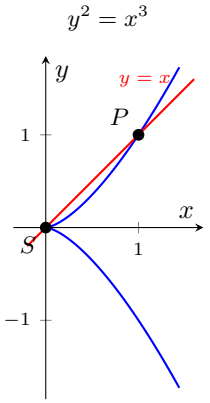
Here $\mathcal{O}$ is one distinguished extra point, called the **point at infinity**. It will be the identity for the addition in Definition 2.12. We explain its geometry in Section 3. Apart from $\mathcal{O}$, the points of $E(\mathbb{R})$ form the real-plane picture, while the points of $E(\mathbb{Q})$ have rational coordinates. The point $\mathcal{O}$ does not enter the triangle correspondence below.

Why require $\Delta(E) \neq 0$? We want the usual addition of points to make **all** points, including $\mathcal{O}$, into a group. At a singular point, this can fail.

For example,

$$C: \; y^2 = x^3 \qquad (A = B = 0, \; \Delta = 0)$$

has a cusp at $S = (0,0)$, so it is excluded from the definition of an elliptic curve.



Take $P = (1,1)$. The red line through S and P is $y = x$. Substituting gives

$$x^2 = x^3 \quad \Longleftrightarrow \quad x^2(x-1) = 0.$$

The root $x = 0$ occurs twice.

The line meets the curve twice at S and once at P, counting repeated intersections. So the third intersection is S again. Reflecting S still gives S, and the usual chord rule would give $S + P = S$. This cannot hold in a group with identity $\mathcal{O}$, since cancelling S would give $P = \mathcal{O}$. The condition $\Delta \neq 0$ avoids this problem. We will state the theorem that the addition formulas then give an abelian group. For a singular curve, the **nonsingular** points can still form a group, but here we want to include all points.

For each positive integer n, the equation

$$E_n: \quad y^2 = x^3 - n^2 x$$

is an elliptic curve: here $A = -n^2$, $B = 0$ and $\Delta(E_n) = 64n^6 \neq 0$. The congruent number problem asks about rational right triangles and their areas, with no mention of curves. The surprising connection is that it can be translated into a question about rational solutions of this equation.

Proposition 1.2. *Let $n \in \mathbb{N}$ and consider the equation $E_n : y^2 = x^3 - n^2 x$ introduced above.*

(i) If $a, b, c \in \mathbb{Q}_{>0}$ with $a^2 + b^2 = c^2$ and $\frac{ab}{2} = n$, then

$$x = \frac{n(a+c)}{b}, \qquad y = \frac{2n^2(a+c)}{b^2}$$

is a point $(x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$.

(ii) Conversely, if $(x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$, then

$$a = \left|\frac{x^2 - n^2}{y}\right|, \qquad b = \left|\frac{2nx}{y}\right|, \qquad c = \left|\frac{x^2 + n^2}{y}\right|$$

are the sides of a right triangle with area n.

In particular: n is congruent $\Longleftrightarrow$ there is a point $(x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$.

Proof. (i) Clearly $y > 0$. We compute

$$x^3 - n^2 x = x\,(x^2 - n^2) = \frac{n(a+c)}{b} \cdot n^2\, \frac{(a+c)^2 - b^2}{b^2}.$$

Using $b^2 = c^2 - a^2$ we get $(a+c)^2 - b^2 = a^2 + 2ac + c^2 - c^2 + a^2 = 2a(a+c)$. Hence, with $a = \frac{2n}{b}$,

$$x^3 - n^2 x = \frac{n^3(a+c)^2 \cdot 2a}{b^3} = \frac{n^3(a+c)^2 \cdot 4n}{b^4} = \left(\frac{2n^2(a+c)}{b^2}\right)^2 = y^2.$$

(ii) Since $y^2 = x(x-n)(x+n) \neq 0$, we have $x \neq 0$ and $x \neq \pm n$, so a, b, c are positive rational numbers. Now

$$\left(\frac{x^2-n^2}{y}\right)^2 + \left(\frac{2nx}{y}\right)^2 = \frac{x^4 - 2n^2x^2 + n^4 + 4n^2x^2}{y^2} = \left(\frac{x^2+n^2}{y}\right)^2,$$

so $a^2 + b^2 = c^2$, and

$$\frac{(x^2-n^2)\cdot 2nx}{2y^2} = \frac{n\,(x^3 - n^2x)}{y^2} = \frac{n\,y^2}{y^2} = n.$$

Taking absolute values does not change this, so $\frac{ab}{2} = n$. □

Example. *For $n = 6$ the triangle $(3, 4, 5)$ gives the point $(x, y) = \left(\frac{6\cdot 8}{4}, \frac{72\cdot 8}{16}\right) = (12, 36)$ on $E_6 : y^2 = x^3 - 36x$. Indeed $12^3 - 36 \cdot 12 = 1728 - 432 = 1296 = 36^2$. Conversely, this point gives side lengths*

$$\frac{12^2 - 6^2}{36} = 3, \qquad \frac{2 \cdot 6 \cdot 12}{36} = 4, \qquad \frac{12^2 + 6^2}{36} = 5.$$

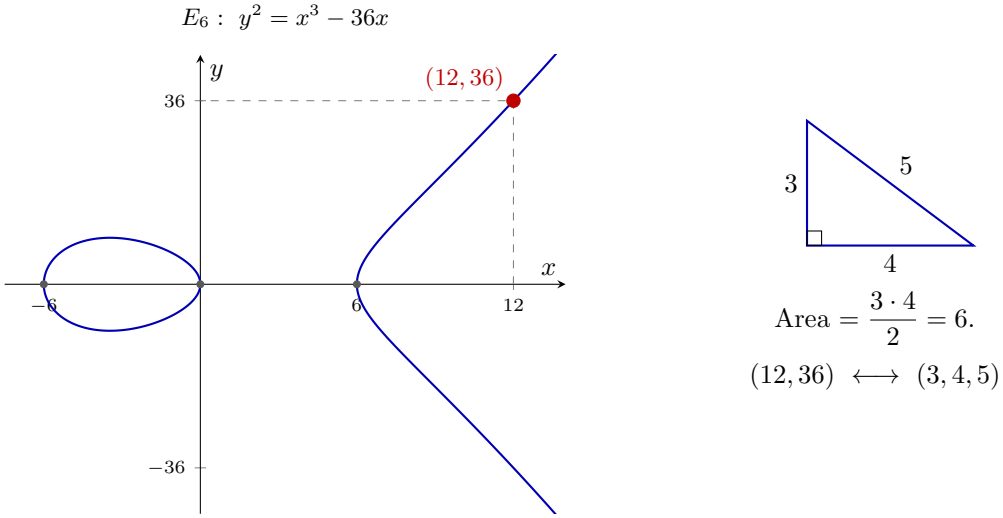


Figure 2: The real solutions of $y^2 = x^3 - 36x$ form two components. The marked point $(12, 36)$ is a rational solution and corresponds to a rational right triangle of area 6. The point at infinity is not shown.

A preview: obtaining another triangle

The addition formulas in Definition 2.12 come from drawing a line and reflecting its third intersection point across the x-axis. We can already try this on E_6. We explain the geometry in Section 3.

Start with $P = (12, 36)$ and $T = (-6, 0)$. The line through them is $y = 2x + 12$. Substituting it into $y^2 = x^3 - 36x$ gives

$$(x - 12)(x + 6)(x + 2) = 0.$$

Besides P and T, the line therefore meets the curve at $(-2, 8)$. Reflecting this point gives

$$P + T = (-2, -8) \in E_6(\mathbb{Q}).$$

Proposition 1.2 turns this point into the triangle with sides

$$\left|\frac{4-36}{-8}\right| = 4, \qquad \left|\frac{12\cdot(-2)}{-8}\right| = 3, \qquad \left|\frac{4+36}{-8}\right| = 5.$$

This is the same $3,4,5$ triangle with its legs exchanged: a different point need not give a different triangle.
To obtain a new triangle, add P to itself, using the tangent line at P. Implicit differentiation gives the slope

$$\left.\frac{3x^2-36}{2y}\right|_{(12,36)} = \frac{11}{2},$$

so the tangent line is $y = \frac{11}{2}x - 30$. Its third intersection point is $\left(\frac{25}{4}, \frac{35}{8}\right)$. Reflecting gives

$$2P = P + P = \left(\frac{25}{4}, -\frac{35}{8}\right) \in E_6(\mathbb{Q}).$$

The triangle formulas now give the new side lengths

$$a = \frac{7}{10}, \qquad b = \frac{120}{7}, \qquad c = \frac{1201}{70}.$$

Indeed $a^2 + b^2 = c^2$ and $\frac{ab}{2} = \frac{1}{2} \cdot \frac{7}{10} \cdot \frac{120}{7} = 6$. Thus drawing a tangent has produced a different rational right triangle with the same area.

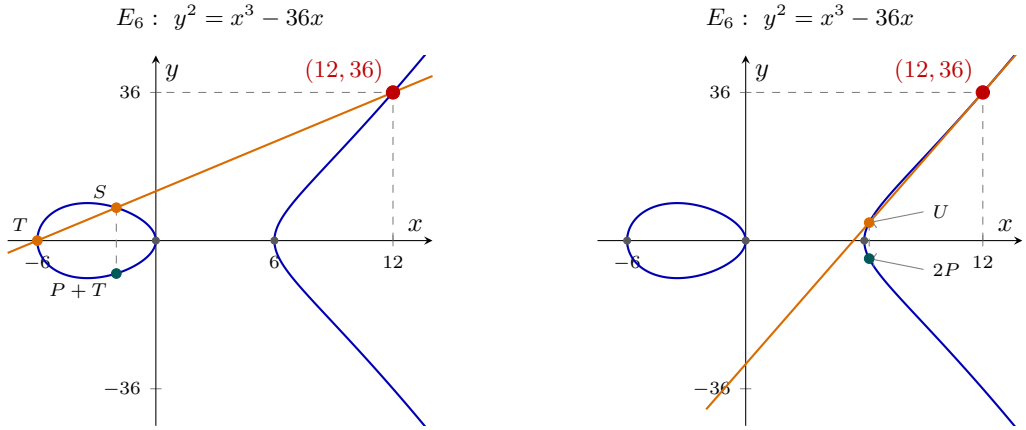


Figure 3: Chord and tangent constructions on E_6. Left: the chord through P and T meets the curve at $S = (-2, 8)$, whose reflection is $P + T = (-2, -8)$. Right: the tangent at P meets the curve again at $U = (25/4, 35/8)$, whose reflection is $2P = (25/4, -35/8)$.

Remark 1.3. The points of E_n with $y = 0$ are $(0, 0)$ and $(\pm n, 0)$. We will see that "adding" a point with $y \neq 0$ to itself again and again produces infinitely many different rational points. Hence: if there is **one** triangle with area n, there are infinitely many. Homework 1, Exercise 5(iv*), uses the same doubling construction for area 30.

Theorem 1.4 (Tunnell, 1983, statement only)**.** *Let n be an odd squarefree natural number and define*

$$A(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid 2x^2+y^2+8z^2 = n\}, \qquad B(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid 2x^2+y^2+32z^2 = n\}.$$

If n is congruent, then $A(n) = 2B(n)$. If the Birch and Swinnerton-Dyer conjecture is true, then the converse also holds.

Example. *For $n = 1$ the only solutions are $(0, \pm 1, 0)$ in both cases, so $A(1) = B(1) = 2$. Since $2 \neq 4$, the number 1 is not congruent. For $n = 11$ one finds $A(11) = 12$ and $B(11) = 4$, so 11 is not congruent. For $n = 5$ and $n = 7$ we get $A(n) = B(n) = 0$.*

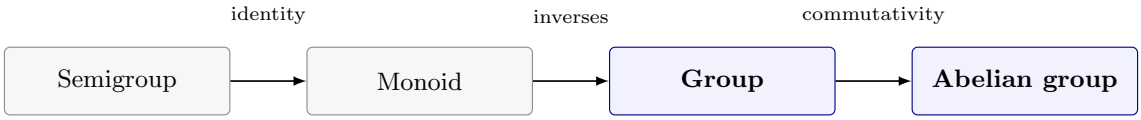
Remark 1.5. The Birch and Swinnerton-Dyer conjecture is one of the seven Millennium Prize Problems ($1 000 000). So the congruent number problem, which a school student can understand, leads directly to one of the most important open problems in mathematics. (For even n there is a similar criterion with $\frac{n}{2} = 4x^2 + y^2 + 8z^2$ and $\frac{n}{2} = 4x^2 + y^2 + 32z^2$.)

Optional outlook. Recent advances in AI-assisted mathematics[1] invite an optimistic speculation: perhaps the Birch and Swinnerton-Dyer conjecture could be solved during this semester, with help from AI. Whether or not that happens, this is a good time to learn its statement.

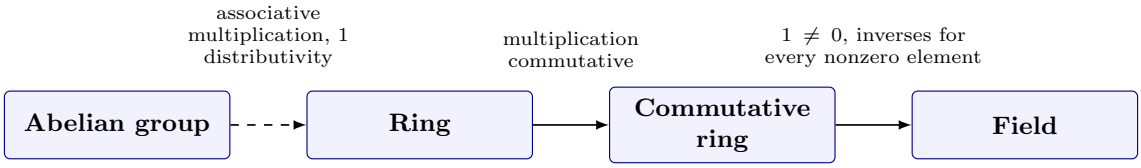
1.3 A map of algebraic structures

A set with one associative operation is called a **semigroup**. If it also has an identity, it is a **monoid**. If every element also has an inverse, it is a **group**. For example, $(\mathbb{N}, +)$ is a semigroup, $(\mathbb{Z}_{\geq 0}, +)$ is a monoid, and $(\mathbb{Z}, +)$ is an abelian group. These names locate the structures in the following map. Our main objects are groups, rings, fields, modules and vector spaces.

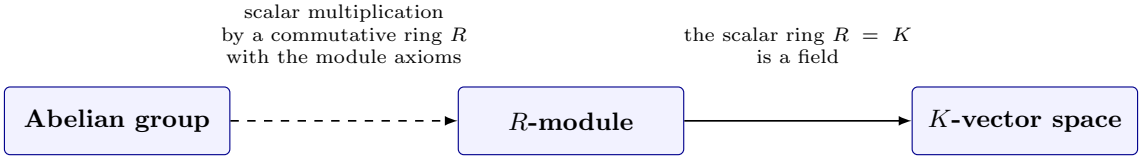
One operation: a semigroup has an associative operation



Addition and multiplication



Addition and scalar multiplication



Solid arrows add conditions. Dashed arrows add compatible operations. Blue boxes mark the structures studied in this course. A vector space is exactly a module over a field.

Until here in Lecture 1 (5 October 2026)

[1] For example, see T. Feng et al., **Towards Autonomous Mathematics Research** (March 2026), available online.

1.4 Arithmetic with remainders

Can a number system have only finitely many elements? We already know a simple example: arithmetic with **even** and **odd**. The sum of two odd integers is even, and their product is odd. To know whether a sum or product is even or odd, we only need to know whether each number is even or odd. Write 0 for even and 1 for odd. We then have two elements with $1 + 1 = 0$ and $1 \cdot 1 = 1$.

Parity keeps only the remainder after division by 2. We can do the same with division by 5: keep only the five possible remainders $0, 1, 2, 3, 4$. For example, $2, 7, 12$ and -3 all have remainder 2, so they are represented by the same element. Add and multiply as usual, then take the remainder:

$$3 + 4 = 7 \longmapsto 2, \qquad 3 \cdot 4 = 12 \longmapsto 2, \qquad 4 + 1 = 5 \longmapsto 0.$$

This works because replacing an integer by another with the same remainder changes sums and products only by multiples of 5. Thus their remainders depend only on the input remainders.

The resulting number system is denoted by $\mathbb{Z}/5\mathbb{Z}$, read "the integers modulo 5". In $\mathbb{Z}/5\mathbb{Z}$ we write $3 + 4 = 2$, $3 \cdot 4 = 2$ and $4 + 1 = 0$. These are equalities of remainders. More generally, for $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is represented by $0, 1, \ldots, n-1$, with addition and multiplication followed by taking the remainder after division by n. Our even/odd arithmetic is $\mathbb{Z}/2\mathbb{Z}$. The precise construction by congruence classes is given in Definition 2.6.

Subtraction works too: in $\mathbb{Z}/5\mathbb{Z}$, $1 - 3 = 3$, since -2 has remainder 3. Division is more interesting. In $\mathbb{Z}/5\mathbb{Z}$, $2 \cdot 3 = 1$, so 3 is an inverse of 2. In $\mathbb{Z}/6\mathbb{Z}$, no multiple of 2 equals 1: the possible remainders are only $0, 2, 4$. The rules depend on the number system. We will see that $\mathbb{Z}/5\mathbb{Z}$ is a **field**, also denoted by $\mathbb{F}_5$.

Algebra is the study of sets together with operations (such as "+" and "·") satisfying certain rules (axioms). The three most important structures are **groups**, **rings**, and **fields**. The advantage of this point of view is that a few axioms cover a huge number of examples, and everything we prove from the axioms holds for all of them at once.

We assume that you know the number systems $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. The table shows which operations always give a result in the same set.

	$a+b$	$a-b$	$a \cdot b$	a/b $(b \neq 0)$	structure
$\mathbb{N} = \{1, 2, 3, \ldots\}$	✓	–	✓	–	–
$\mathbb{Z}$	✓	✓	✓	–	ring
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	✓	✓	✓	✓	field
$\mathrm{M}_2(\mathbb{R})$ (2×2 matrices)	✓	✓	✓	–	ring (not commutative)
$\mathbb{Z}/n\mathbb{Z}$	✓	✓	✓	only if n is prime	ring (field if n prime)

Roughly speaking, a **group** is a set with one operation that can be "undone" (e.g. + and −), a **ring** is a set in which we can add, subtract and multiply, and a **field** is a ring in which we can also divide by every non-zero element.

1.5 An elliptic-curve example

After the congruent-number curves E_n in Section 1.2, we now consider a different elliptic curve

$$E: \quad y^2 = x^3 - x + 1.$$

Here $A = -1$, $B = 1$ and $\Delta(E) = -16(-4 + 27) = -368 \neq 0$. This example lets us compare solutions of the same equation in different number systems. As before, $E(R)$ includes the point at infinity $\mathcal{O}$ as well as the solutions (x, y) with coordinates in R.

- Over $\mathbb{R}$: the solutions form a curve in the plane (Figure 4, left).

- Over $\mathbb{Q}$: which points on this curve have rational coordinates? For example $(0, \pm 1)$, $(\pm 1, \pm 1)$, $(3, \pm 5)$, $(5, \pm 11)$, $(56, \pm 419)$ and $(\frac{1}{4}, \pm\frac{7}{8})$. Check: $3^3 - 3 + 1 = 25 = 5^2$. These are only examples: 12 points with integer coordinates and 2 with fractional coordinates. For example, $(-\frac{11}{9}, -\frac{17}{27})$ is another one. Later we will use addition to produce more rational points.
- Over $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ (arithmetic modulo 5, see Section 1.4): the squares modulo 5 are $0^2 = 0$, $1^2 = 4^2 = 1$, $2^2 = 3^2 = 4$, and

x	0	1	2	3	4
$x^3 - x + 1 \bmod 5$	1	1	2	0	1
y	$1, 4$	$1, 4$	–	0	$1, 4$

  So there are 7 solutions (x, y) (Figure 4, right). Including the point at infinity from our definition gives $|E(\mathbb{F}_5)| = 8$.

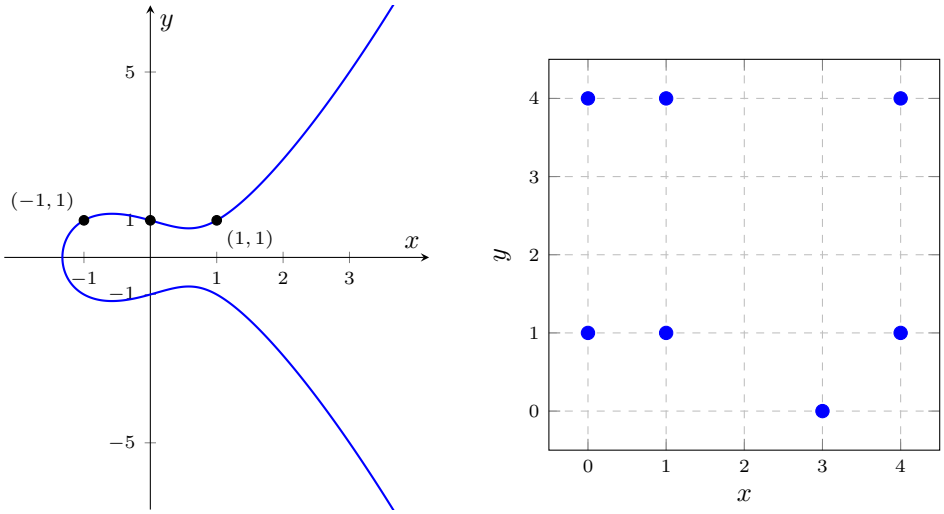


Figure 4: The equation $y^2 = x^3 - x + 1$ over $\mathbb{R}$ (left) and its seven affine points over $\mathbb{F}_5$ (right). The point at infinity $\mathcal{O}$ is not shown. The grid on the right displays coordinates in $\mathbb{F}_5$.

After defining groups, we will define addition on $E(K)$ in Definition 2.12 and study how these points behave under addition.

2 Groups, rings and fields

2.1 Groups

Recall from Linear Algebra that a real vector space V comes with an addition $V \times V \to V$, $(v, w) \mapsto v + w$, satisfying for all $u, v, w \in V$:

$$(u + v) + w = u + (v + w), \qquad v + w = w + v, \qquad v + 0 = v, \qquad v + (-v) = 0.$$

The scalar multiplication plays no role here. We forget the vectors and keep the rules.

Definition 2.1. *(i) A* **group** $(G, *)$ *is a set G together with an operation $* : G \times G \to G$, $(a, b) \mapsto a * b$, such that*

1) (associativity) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$,

2) (identity element) there exists $e \in G$ with $e * a = a * e = a$ for all $a \in G$,

3) (inverse elements) for every $a \in G$ there exists $b \in G$ with $a * b = b * a = e$.

(ii) A group is called **abelian** *(or* **commutative***) if in addition $a * b = b * a$ for all $a, b \in G$.*

(iii) The number of elements $|G|$ is called the **order** *of G. If $|G| < \infty$ we call G a* **finite group***.*

Lemma 2.2. *Let $(G, *)$ be a group.*

(i) The identity element is unique.

(ii) The inverse of an element $a \in G$ is unique. We denote it by a^{-1}.

(iii) For all $a, b \in G$ we have $(a * b)^{-1} = b^{-1} * a^{-1}$ and $(a^{-1})^{-1} = a$.

(iv) (Cancellation) If $a * b = a * c$, then $b = c$. If $b * a = c * a$, then $b = c$.

(v) For $a, b \in G$ the equation $a * x = b$ has exactly one solution $x \in G$, namely $x = a^{-1} * b$.

Proof. (i) If e and e' are identity elements, then $e = e * e' = e'$ (the first equality since e' is an identity, the second since e is an identity).
(ii) Let b and b' be inverses of a. Then, using associativity,

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'.$$

(iii) We have $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*a^{-1} = e$, and similarly $(b^{-1}*a^{-1})*(a*b) = e$. By (ii), $b^{-1} * a^{-1}$ is the inverse of $a * b$. Since $a^{-1} * a = a * a^{-1} = e$, the element a is the inverse of a^{-1}.
(iv) Multiply $a * b = a * c$ from the left by a^{-1}: $b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * (a * c) = c$. The second statement is similar.
(v) $x = a^{-1} * b$ is a solution, since $a * (a^{-1} * b) = b$. If x' is another solution, then $a * x = a * x'$, so $x = x'$ by (iv). □

Notation: For abelian groups one often writes the operation as $+$, the identity element as 0 and the inverse of a as $-a$ (**additive notation**). Otherwise one often writes $a \cdot b$ or ab, the identity as 1 and the inverse as a^{-1} (**multiplicative notation**). Because of associativity we can omit brackets and write abc for $(ab)c = a(bc)$.

Remark 2.3. Lemma 2.2 (v) says: in the **multiplication table** of a finite group, every element appears exactly once in every row (and similarly in every column). This is a quick test whether a given table can belong to a group.

Example 2.4 (Groups)**.** *(i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups with identity 0.*

(ii) *Every vector space $(V,+)$ is an abelian group, e.g. $(\mathbb{R}^n,+)$ or $(\mathrm{M}_{m\times n}(\mathbb{R}),+)$.*

(iii) *$(\mathbb{Q}^\times,\cdot)$, $(\mathbb{R}^\times,\cdot)$, $(\mathbb{C}^\times,\cdot)$ are abelian groups, where $\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}$ etc. The identity is 1 and the inverse of a is $\frac{1}{a}$.*

(iv) *The set of n-**th roots of unity***

$$\mu_n=\{z\in\mathbb{C}\mid z^n=1\}=\{1,\zeta_n,\zeta_n^2,\dots,\zeta_n^{n-1}\},\qquad \zeta_n=e^{2\pi i/n},$$

is an abelian group with respect to multiplication of order n. Geometrically, the elements are the corners of a regular n-gon on the unit circle.

(v) *The **general linear group** $\mathrm{GL}_n(\mathbb{R})=\{A\in\mathrm{M}_n(\mathbb{R})\mid\det(A)\neq 0\}$ is a group with respect to matrix multiplication, with identity I_n and inverse A^{-1}. For $n\geq 2$ it is **not** abelian, e.g.*

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}=\begin{pmatrix}2&1\\1&1\end{pmatrix}\neq\begin{pmatrix}1&1\\1&2\end{pmatrix}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

(vi) *The rotation matrices $R_\theta=\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}$, $\theta\in\mathbb{R}$, form an abelian group with respect to matrix multiplication.*

Proof of (iv)–(vi). In each case we have to check that the result stays in the set ("closure"). Associativity follows from associativity in $\mathbb{C}$ or of matrix multiplication.
(iv) If $z^n=w^n=1$, then $(zw)^n=z^nw^n=1$ (here we use that $\mathbb{C}^\times$ is commutative), so $zw\in\mu_n$. Further $1\in\mu_n$, and $z\in\mu_n$ has the inverse z^{-1} with $(z^{-1})^n=(z^n)^{-1}=1$. Writing $z=re^{i\varphi}$ with $r>0$, the equation $z^n=r^ne^{in\varphi}=1$ means $r=1$ and $n\varphi\in 2\pi\mathbb{Z}$, which gives exactly the n elements $\zeta_n^k=e^{2\pi ik/n}$, $k=0,\dots,n-1$.
(v) If $\det A\neq 0$ and $\det B\neq 0$, then $\det(AB)=\det(A)\det(B)\neq 0$. Further $\det I_n=1$, and for $A\in\mathrm{GL}_n(\mathbb{R})$ the inverse matrix exists and $\det(A^{-1})=\det(A)^{-1}\neq 0$.
(vi) By the addition theorems of sin and cos we have $R_\theta R_\varphi=R_{\theta+\varphi}=R_\varphi R_\theta$. Hence the set is closed and commutative, $R_0=I_2$ is the identity and $R_\theta^{-1}=R_{-\theta}$. □

Example 2.5 (Non-examples)**.** *(i) $(\mathbb{N},+)$: there is no identity element in $\mathbb{N}=\{1,2,\dots\}$, and even in $\mathbb{Z}_{\geq 0}$ the element 1 has no inverse.*

(ii) $(\mathbb{Z},\cdot)$: the identity is 1, but 2 has no inverse in $\mathbb{Z}$ since $\frac{1}{2}\notin\mathbb{Z}$.

(iii) $(\mathbb{R},\cdot)$: the element 0 has no inverse. (This is why we remove 0 in $\mathbb{R}^\times$.)

(iv) $(\mathrm{M}_n(\mathbb{R}),\cdot)$: matrices with $\det(A)=0$, e.g. $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, have no inverse.

(v) $(\mathbb{Z},-)$: subtraction is not associative, $(1-1)-1=-1\neq 1=1-(1-1)$.

Arithmetic modulo n. We now make the arithmetic with remainders from Section 1.4 precise. The idea is to replace the remainder of a by the set of **all** integers with the same remainder as a.

Definition 2.6. *Let $n\in\mathbb{N}$.*

(i) *Two integers a,b are **congruent modulo** n, written $a\equiv b\pmod n$, if $n\mid a-b$.*

(ii) *The **congruence class** of $a\in\mathbb{Z}$ modulo n is*

$$[a]=\{b\in\mathbb{Z}\mid b\equiv a\pmod n\}=\{\dots,a-2n,\ a-n,\ a,\ a+n,\ a+2n,\dots\}.$$

*Every $b\in[a]$ is called a **representative** of $[a]$.*

(iii) *$\mathbb{Z}/n\mathbb{Z}=\{[a]\mid a\in\mathbb{Z}\}$ is the set of all congruence classes modulo n, with the operations*

$$[a]+[b]=[a+b],\qquad [a]\cdot[b]=[ab].$$

For example, modulo 5 we have $[2]=\{\dots,-8,-3,2,7,12,\dots\}=[7]=[-3]$, and $[3]+[4]=[7]=[2]$.

Lemma 2.7. *Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$.*

(i) Congruence modulo n is an **equivalence relation**. *We have $a \equiv a$, and $a \equiv b$ implies $b \equiv a$. If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.*

(ii) $[a] = [b]$ if and only if $a \equiv b \pmod{n}$.

(iii) $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$, and these n classes are distinct. In particular $|\mathbb{Z}/n\mathbb{Z}| = n$.

(iv) The operations are **well-defined**: *if $[a] = [a']$ and $[b] = [b']$, then $[a+b] = [a'+b']$ and $[ab] = [a'b']$.*

Proof. (i) We have $n \mid 0 = a - a$. If $n \mid a - b$, then $n \mid b - a$. If $n \mid a - b$ and $n \mid b - c$, then $n \mid (a-b) + (b-c) = a - c$.
(ii) If $[a] = [b]$, then $a \in [a] = [b]$, so $a \equiv b$. Conversely, let $a \equiv b$. If $c \in [a]$, then $c \equiv a$ and $a \equiv b$, so $c \equiv b$ by (i), i.e. $c \in [b]$. Hence $[a] \subseteq [b]$, and $[b] \subseteq [a]$ follows in the same way.
(iii) Division with remainder gives $a = qn + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$. Then $n \mid a - r$, so $[a] = [r]$ by (ii). If $0 \le r < s \le n-1$, then $0 < s - r < n$, so $n \nmid s - r$ and $[r] \neq [s]$.
(iv) By (ii) we can write $a' = a + kn$ and $b' = b + ln$ with $k, l \in \mathbb{Z}$. Then

$$a' + b' = a + b + (k+l)n, \qquad a'b' = ab + (al + bk + kln)n,$$

so $a' + b' \equiv a + b$ and $a'b' \equiv ab$. Now apply (ii). □

Part (iv) is the important point. The definition of $[a] + [b]$ uses the representatives a and b, but the result does not depend on which representatives we choose. The rules of calculation then carry over from $\mathbb{Z}$, for example

$$([a] + [b]) \cdot [c] = [(a+b)c] = [ac + bc] = [a] \cdot [c] + [b] \cdot [c].$$

In practice we write a instead of $[a]$ and compute with the representatives $0, 1, \ldots, n-1$ from (iii). This is exactly the arithmetic with remainders from Section 1.4. For example, in $\mathbb{Z}/12\mathbb{Z}$ we have $9 + 5 = 14 = 2$, $5 \cdot 5 = 25 = 1$ and $7 \cdot 7 = 49 = 1$. In Lecture 5 we will see that $[a] = a + n\mathbb{Z}$ is a **coset** of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, and that $\mathbb{Z}/n\mathbb{Z}$ is a special case of a general construction, the **quotient group**.

Example 2.8. *$(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group of order n. The axioms carry over from $(\mathbb{Z}, +)$, the identity is 0, and the inverse of a is $-a = n - a$. Compare the addition table of $\mathbb{Z}/4\mathbb{Z}$ with the multiplication table of $\mu_4 = \{1, i, -1, -i\}$:*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

The two tables have exactly the same pattern ($a \leftrightarrow i^a$). We call such groups **isomorphic**. *We make this precise in Definition 2.16 below.*

Products of groups. Two groups can be combined into a new one by computing in both at the same time, as for vectors in $\mathbb{R}^2$.

Definition 2.9. *Let $(G, *)$ and $(H, \star)$ be groups. The* **(direct) product** *of G and H is the set of pairs*

$$G \times H = \{(g, h) \mid g \in G,\ h \in H\}$$

with the componentwise operation $(g, h) \cdot (g', h') = (g * g',\ h \star h')$.

Lemma 2.10. *$G \times H$ is a group of order $|G| \cdot |H|$. Its identity is (e_G, e_H), and the inverse of (g, h) is (g^{-1}, h^{-1}). If G and H are abelian, then so is $G \times H$.*

Proof. Every axiom holds in each component separately. Writing both operations as multiplication, associativity in G and in H gives

$$\big((g,h)(g',h')\big)(g'',h'') = \big((gg')g'',\ (hh')h''\big) = \big(g(g'g''),\ h(h'h'')\big) = (g,h)\big((g',h')(g'',h'')\big).$$

In the same way, (e_G, e_H) is an identity element, and $(g,h)(g^{-1},h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$ and similarly $(g^{-1},h^{-1})(g,h) = (e_G, e_H)$. Commutativity also holds componentwise. □

Products of more than two groups are defined in the same way. We write $G^n = G \times \cdots \times G$ (n factors). For example, $(\mathbb{R}^n, +) = (\mathbb{R}, +)^n$ and $(\mathbb{Z}^2, +) = (\mathbb{Z}, +) \times (\mathbb{Z}, +)$.

Example 2.11 (Bit strings)**.** *In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(0,1),(1,0),(1,1)\}$ we add componentwise modulo 2, e.g. $(1,1)+(1,0) = (0,1)$. If we write the pair (a,b) as the bit string ab, this is* **bitwise addition modulo** 2 *("XOR", i.e. $1+1=0$ in each bit):*

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

So the bit strings $\{00, 01, 10, 11\}$ with XOR are the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the same way, bit strings of length n with XOR form the group $(\mathbb{Z}/2\mathbb{Z})^n$.
Like $\mathbb{Z}/4\mathbb{Z}$, this is an abelian group with 4 elements, but it does **not** *have the same pattern as $\mathbb{Z}/4\mathbb{Z}$. For every bit string v we have $v + v = 00$, while in $\mathbb{Z}/4\mathbb{Z}$ adding 1 repeatedly runs through all four elements $1, 2, 3, 0$. So the number of elements alone does not determine a group.*

Elliptic curves as groups. We return to the curve from Section 1.5. We give the addition formulas now so that you can use them in Homework 1. We explain their geometry in Section 3.

Definition 2.12 (Addition on an elliptic curve)**.** *Let*

$$E:\ y^2 = x^3 + Ax + B, \qquad 4A^3 + 27B^2 \neq 0,$$

over $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *or* $\mathbb{F}_p$ *with* $p \geq 5$*. Put*

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ *is one additional point. Define addition as follows:*

(i) $P + \mathcal{O} = \mathcal{O} + P = P$ *for every* $P \in E(K)$*.*

(ii) For $P = (x_1, y_1)$ *and* $Q = (x_2, y_2)$*, if* $x_1 = x_2$ *and* $y_1 = -y_2$*, put* $P + Q = \mathcal{O}$*. In particular,* $2(x_1, 0) = \mathcal{O}$*.*

(iii) In all other cases, put

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P = Q \text{ and } y_1 \neq 0, \end{cases}$$

and define $P + Q = (x_3, y_3)$ *by*

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

All arithmetic is in K*. In* $\mathbb{F}_p$*, divide by a non-zero element by multiplying by its inverse. Write* $2P = P + P$ *and* $P - Q = P + (-Q)$*, where* $-(x, y) = (x, -y)$ *and* $-\mathcal{O} = \mathcal{O}$*.*

Proposition 2.13. *With the addition in Definition 2.12,* $(E(K), +)$ *is an abelian group. Its identity is* $\mathcal{O}$*. The inverse of* (x, y) *is* $(x, -y)$*, and* $-\mathcal{O} = \mathcal{O}$*.*

Proof later. We return to the proof in Section 3.4. You may use this proposition without proof in Homework 1. In particular, you do not need to prove associativity.

Remark 2.14 (Why $p \geq 5$?). The condition $p \geq 5$ means that $2 \neq 0$ and $3 \neq 0$ in $\mathbb{F}_p$.

(i) $p = 2$: The doubling formula divides by $2y_1$, but $2y_1 = 0$ in $\mathbb{F}_2$. Worse, over $\mathbb{F}_2$ every curve $y^2 = x^3 + Ax + B$ is singular: the point $S = (A, B)$ lies on it, and every line through S meets the curve twice at S. For example, on $y^2 = x^3 + x + 1$ the line $y = 1$ through $S = (1, 1)$ and $P = (0, 1)$ gives $x^3 + x = x(x + 1)^2 = 0$. As for the cusp in Section 1.2, the chord rule would give $S + P = -S = S$, so $P = \mathcal{O}$, a contradiction. Notice that $\Delta(E) = -16(4A^3 + 27B^2) = 0$ in $\mathbb{F}_2$ for all A, B, since $16 = 0$. The shorter condition $4A^3 + 27B^2 \neq 0$ does not detect this: here $4 + 27 = 31 = 1$ in $\mathbb{F}_2$.

(ii) $p = 3$: The formulas contain no division by 3, and they still give a group. The problem is that the short form $y^2 = x^3 + Ax + B$ misses curves. To remove the x^2-term from $x^3 + ax^2 + bx + c$, we substitute $x - \frac{a}{3}$ for x, which requires $3 \neq 0$. For example, $y^2 = x^3 + x^2 + 1$ over $\mathbb{F}_3$ cannot be brought into short form.

Over $\mathbb{F}_2$ and $\mathbb{F}_3$ one uses the general equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with longer addition formulas. We will not need these two primes for elliptic curves.

More rational points by doubling. Return to $E : y^2 = x^3 - x + 1$ over $\mathbb{Q}$ and start with $Q = (1, 1)$. The doubling formula gives $2Q = (-1, 1)$. Now double this new point. At $(-1, 1)$ the slope is again $\lambda = 1$, so $4Q = 2Q + 2Q = (3, -5)$. Doubling once more uses $\lambda = \frac{3 \cdot 3^2 - 1}{2 \cdot (-5)} = -\frac{13}{5}$ and gives

n	1	2	4	8
nQ	$(1, 1)$	$(-1, 1)$	$(3, -5)$	$\left(\frac{19}{25}, -\frac{103}{125}\right)$

We can keep doubling. These calculations suggest that there are many rational points. In fact, one can show much more.

Fact (without proof). Every point of $E(\mathbb{Q})$ is nQ for exactly one integer n.

Here nQ means adding Q to itself n times when $n > 0$. We set $0Q = \mathcal{O}$ and $(-n)Q = -(nQ)$. Doubling alone gives the labels $1, 2, 4, 8, \ldots$. To obtain all points, we allow every integer label. For example, adding Q to $2Q$ gives $3Q = (0, -1)$, which the doubling sequence misses. Thus repeated addition of Q, together with taking negatives, gives all rational points.

The labels add just like integers:

$$(mQ) + (nQ) = (m + n)Q.$$

So $E(\mathbb{Q})$ has the addition pattern of $\mathbb{Z}$. In particular, the doubling sequence gives infinitely many distinct points. Proving that Q gives all rational points requires a separate computation.[2] Mordell's theorem later in the course says that finitely many points generate $E(\mathbb{Q})$. It does not by itself prove that this point generates $E(\mathbb{Q})$.

The geometric idea. We can add points on E by drawing a line and reflecting the third intersection point, just as for E_6 in Section 1.2. For example, the line $y = 1$ meets E where $x^3 - x + 1 = 1$, i.e. $x(x - 1)(x + 1) = 0$. Starting with $(-1, 1)$ and $(0, 1)$, the third intersection point is $(1, 1)$, so reflection gives

$$(-1, 1) + (0, 1) = (1, -1).$$

Since $\mathcal{O}$ is the identity, we also have $(-1, 1) + (0, 1) + (1, 1) = \mathcal{O}$. In general, three distinct points on the curve that lie on one line add to $\mathcal{O}$. We will explain the geometry behind the formulas in Section 3.

Remark 2.15. This addition is **not** the coordinate-wise addition of vectors. For example $(1, 1) + (1, 1) = (2, 2)$ coordinate-wise, but $(2, 2)$ is not on E, since $2^2 = 4 \neq 7 = 2^3 - 2 + 1$. The addition defined above gives $2 \cdot (1, 1) = (-1, 1)$ over $\mathbb{Q}$.

Do lines still make sense over $\mathbb{F}_5$? Yes: a line is given by a linear equation, with all arithmetic done modulo 5. For example,

$$y = 1 : \qquad \{(0, 1), (1, 1), (2, 1), (3, 1), (4, 1)\}.$$

Its intersections with E satisfy the same equation $x(x - 1)(x + 1) = 0$, now with roots $0, 1, 4$. Starting with $(0, 1)$ and $(1, 1)$, the third intersection is $(4, 1)$. Replacing y by $-y$ gives

$$(0, 1) + (1, 1) = (4, 4) \qquad \text{in } E(\mathbb{F}_5).$$

The line and its intersections are defined by equations. The grid in Figure 4 displays the coordinates, but we cannot read off addition by drawing ordinary lines in that grid. Negating y also uses arithmetic modulo 5. For example, $(4, 1)$ becomes $(4, 4)$, since $-1 = 4$ in $\mathbb{F}_5$. This is not reflection across the horizontal axis in the drawing. The formulas above also cover tangents and $\mathcal{O}$. We explain their geometric meaning in Section 3.

Until here in Lecture 2 (12 October 2026)

[2] Cremona's elliptic-curve tables, curve `92b1`, give rank 1, trivial torsion and generator $(1, 1)$. See the database documentation and its generator table.

The curve over $\mathbb{F}_5$. Recall

$$E:\ y^2 = x^3 - x + 1, \qquad E(\mathbb{F}_5) = \{(x,y) \in \mathbb{F}_5^2 \mid y^2 = x^3 - x + 1\} \cup \{\mathcal{O}\}.$$

Here $4(-1)^3 + 27 = 23 = 3 \neq 0$ in $\mathbb{F}_5$. Definition 2.12 gives the addition, and Proposition 2.13 says that it makes $E(\mathbb{F}_5)$ an abelian group. The formulas come from the geometric picture over $\mathbb{R}$, but they also make sense over $\mathbb{F}_5$: all coordinate calculations, including division, are now modulo 5. Before computing, we make precise what it means for two groups to have the same addition pattern.

Definition 2.16 (Group isomorphism)**.** *Let $(G, *)$ and $(H, \star)$ be groups. A* **group isomorphism** *is a bijection $\varphi : G \to H$ such that*

$$\varphi(g * h) = \varphi(g) \star \varphi(h) \qquad \text{for all } g, h \in G.$$

If such a map exists, we call the groups **isomorphic** *and write $G \cong H$.*

An isomorphism renames the elements while preserving the operation. For example, the tables in Example 2.8 show that $\mathbb{Z}/4\mathbb{Z} \to \mu_4$, $[a] \mapsto i^a$, is an isomorphism: $i^{a+b} = i^a i^b$.

Over $\mathbb{F}_5$: a cycle of eight points. For $x = 0, 1, 2, 3, 4$, the values of $x^3 - x + 1$ modulo 5 are $1, 1, 2, 0, 1$. Since the squares are $0, 1, 4$, we obtain seven affine points and $\mathcal{O}$.
Start with $Q = (1, 1)$. Definition 2.12 gives

$$2Q = (4,1) \quad (\lambda = 1), \qquad 3Q = (4,1) + (1,1) = (0,4) \quad (\lambda = 0).$$

Doubling $2Q = (4, 1)$ gives $4Q = (3, 0)$, so $8Q = 2(3, 0) = \mathcal{O}$. Thus $5Q = -3Q$, $6Q = -2Q$ and $7Q = -Q$. Writing out all the points gives

n	0	1	2	3	4	5	6	7
nQ	$\mathcal{O}$	$(1,1)$	$(4,1)$	$(0,4)$	$(3,0)$	$(0,1)$	$(4,4)$	$(1,4)$

These are all eight points, with no repetitions. The map

$$\varphi : \mathbb{Z}/8\mathbb{Z} \longrightarrow E(\mathbb{F}_5), \qquad [n] \longmapsto nQ,$$

is well-defined because $8Q = \mathcal{O}$, and the table shows it is bijective. By the group laws,

$$\varphi([m] + [n]) = (m + n)Q = mQ + nQ = \varphi([m]) + \varphi([n]).$$

Hence $E(\mathbb{F}_5) \cong \mathbb{Z}/8\mathbb{Z}$. To add points, add their labels modulo 8. For example,

$$(0,4) + (4,4) = (1,1) \qquad \text{corresponds to} \qquad [3] + [6] = [1].$$

We compute **coordinates** modulo 5 and add **point labels** modulo 8. Likewise, the fact about rational points above says that $\mathbb{Z} \to E(\mathbb{Q})$, $n \mapsto nQ$, is an isomorphism.

A small example whose group axioms we can check by hand. Consider a different curve

$$E_0 : \ y^2 = x^3 + x \quad \text{over } \mathbb{F}_5.$$

Here $A = 1$ and $B = 0$, so $4A^3 + 27B^2 = 4 \neq 0$. The squares in $\mathbb{F}_5$ are $0, 1, 4$. For $x = 0, 1, 2, 3, 4$, the values of $x^3 + x$ are $0, 2, 0, 0, 3$, respectively. Hence

$$E_0(\mathbb{F}_5) = \{\mathcal{O}, P_1, P_2, P_3\}, \qquad P_1 = (0, 0), \quad P_2 = (2, 0), \quad P_3 = (3, 0).$$

Every affine point has $y = 0$, so $P_1 + P_1 = P_2 + P_2 = P_3 + P_3 = \mathcal{O}$. For two distinct affine points the slope is 0. For example, $P_1 + P_2 = (-0 - 2, 0) = (3, 0) = P_3$. The formulas give the complete table:

$+$	$\mathcal{O}$	P_1	P_2	P_3
$\mathcal{O}$	$\mathcal{O}$	P_1	P_2	P_3
P_1	P_1	$\mathcal{O}$	P_3	P_2
P_2	P_2	P_3	$\mathcal{O}$	P_1
P_3	P_3	P_2	P_1	$\mathcal{O}$

point	two-bit label
$\mathcal{O}$	$(0, 0)$
P_1	$(1, 0)$
P_2	$(0, 1)$
P_3	$(1, 1)$

Closure, the identity, inverses and commutativity are visible in the table. For **associativity**, use the labels: every entry agrees with component-wise addition modulo 2, i.e. with the addition in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (Example 2.11). That addition is associative by Lemma 2.10, so the point addition is associative too. This checks the group axioms for this particular curve without using the general elliptic-curve group theorem. With the definition of isomorphism above,

$$E_0(\mathbb{F}_5) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

A group with four elements need not have the same addition as $\mathbb{Z}/4\mathbb{Z}$. Here every point added to itself gives $\mathcal{O}$. In $\mathbb{Z}/4\mathbb{Z}$, we have $1 + 1 \neq 0$.

2.2 Questions we ask about a group

The following questions about a group will come back throughout the course. For each of them, there are groups where the answer is easy, groups where the answer is surprising or hard, and groups where it is unknown.

Question	easy	surprising / hard	for the curve E
Size: how many elements?	$\lvert\mu_n\rvert = \lvert\mathbb{Z}/n\mathbb{Z}\rvert = n$	Rubik's cube group: 43 252 003 274 489 856 000 elements	$\lvert E(\mathbb{F}_5)\rvert = 8$. Is $E(\mathbb{Q})$ infinite?
Repetition: does $g, g^2, g^3, \ldots$ return to e?	$i^4 = 1$ in μ_4	8 perfect shuffles restore a deck of 52 cards	is $nP = \mathcal{O}$ possible?
Generators: do a few elements give everything?	$(\mathbb{Z}^2, +)$: $(1, 0)$, $(0, 1)$	$(\mathbb{Q}, +)$: no finite set suffices (Prop. 3.14)	yes for $E(\mathbb{Q})$ (Mordell)
Relations: when do different expressions give the same element?	$n \cdot 1 = 0$ in $\mathbb{Z}/n\mathbb{Z}$	$2, 3$ generate $\mathbb{Z}$, but $3 \cdot 2 - 2 \cdot 3 = 0$	$(-1, 1) + (0, 1) + (1, 1) = \mathcal{O}$
Same group?	$\mathbb{Z}/4\mathbb{Z}$ and μ_4	$\mathbb{Z}/4\mathbb{Z}$ and bit strings: no	$E(\mathbb{F}_5) \cong \mathbb{Z}/8\mathbb{Z}$

Some of these questions are open even for very simple groups. The powers of 2 modulo 5 are $2, 4, 3, 1$, i.e. all non-zero remainders, while modulo 7 they are only $2, 4, 1$.

Conjecture 2.17 (Artin, 1927)**.** *There are infinitely many primes p such that the powers of* 2 *modulo p give all non-zero remainders* $1, \ldots, p - 1$.

For example, this is the case for $p = 3, 5, 11, 13, 19, 29, 37, \ldots$, but not for $p = 7, 17, 23, 31, 41, 43, \ldots$. The conjecture would follow from the generalised Riemann hypothesis (Hooley, 1967).

2.3 Rings and fields

In a vector space we can also multiply by scalars from $\mathbb{R}$ or $\mathbb{C}$. For this, we used that scalars can be added, subtracted, multiplied and divided. This leads to the following definitions.

Definition 2.18. *(i) A* **ring** $(R, +, \cdot)$ *is a set R together with two operations "+" and "·" such that*

1) $(R, +)$ is an abelian group (with identity element 0),

2) the multiplication is associative, $(ab)c = a(bc)$, and there is an element $1 \in R$ with $1 \cdot a = a \cdot 1 = a$ for all $a \in R$,

3) the distributive laws hold: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$.

(ii) A ring R is called **commutative** *if $ab = ba$ for all $a, b \in R$.*

(iii) The set of **units** *(invertible elements) of a ring R is*

$$R^\times = \{a \in R \mid \text{there exists } b \in R \text{ with } ab = ba = 1\}.$$

(iv) A commutative ring K with $1 \neq 0$ is called a **field** *if $K^\times = K \setminus \{0\}$, i.e. every non-zero element has a multiplicative inverse.*

Lemma 2.19. *Let R be a ring and $a, b \in R$.*

(i) $0 \cdot a = a \cdot 0 = 0$.

(ii) $(-a)b = a(-b) = -(ab)$. *In particular* $(-1)a = -a$ *and* $(-a)(-b) = ab$.

(iii) If $1 \neq 0$, then $0 \notin R^\times$: one can never divide by 0.

Proof. (i) By the distributive law $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Adding $-(0 \cdot a)$ on both sides gives $0 = 0 \cdot a$. Similarly $a \cdot 0 = 0$.
(ii) $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$ by (i), so $(-a)b$ is the additive inverse of ab. Similarly for $a(-b)$. Then $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.
(iii) By (i), $0 \cdot b = 0 \neq 1$ for every $b \in R$. □

Lemma 2.20. *For every ring R, the units $(R^\times, \cdot)$ form a group.*

Proof. If $a, b \in R^\times$, then $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$ and similarly $(b^{-1}a^{-1})(ab) = 1$, so $ab \in R^\times$. Associativity holds in R. We have $1 \in R^\times$, and if $a \in R^\times$ with $ab = ba = 1$, then also $b \in R^\times$, so b is the inverse of a in $R^\times$. □

Example 2.21 (Rings and fields)**.** *(i) $\mathbb{Z}$ is a commutative ring, but not a field. We have $\mathbb{Z}^\times = \{1, -1\}$.*

(ii) $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

(iii) For a field K, the polynomials $K[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \geq 0,\ a_i \in K\}$ form a commutative ring. It is not a field, since $x \cdot f(x)$ has degree at least 1 for every $f \neq 0$, so $x \cdot f(x) \neq 1$.

(iv) $\mathrm{M}_n(\mathbb{R})$ is a ring, which is not commutative for $n \geq 2$. Its units are $\mathrm{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$.

(v) $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring, since all axioms carry over from $\mathbb{Z}$ (see after Lemma 2.7). Compare the multiplication tables of $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	①	2	3
2	0	2	0	2
3	0	3	2	①

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	①	2	3	4
2	0	2	4	①	3
3	0	3	①	4	2
4	0	4	3	2	①

In $\mathbb{Z}/4\mathbb{Z}$ we have $2 \cdot 2 = 0$, and the row of 2 contains no 1. So $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$ and $\mathbb{Z}/4\mathbb{Z}$ is not a field. In $\mathbb{Z}/5\mathbb{Z}$ we have $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$, so $\mathbb{Z}/5\mathbb{Z}$ is a field.

Proposition 2.22. *Let $n \geq 2$. Then $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.*

Proof. "⇒": Suppose n is not prime, i.e. $n = ab$ with $1 < a, b < n$. Then $a \cdot b = n = 0$ in $\mathbb{Z}/n\mathbb{Z}$. If a had an inverse c (i.e. $ca = 1$), then

$$b = 1 \cdot b = (ca)b = c(ab) = c \cdot 0 = 0,$$

but $b \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$ since $0 < b < n$. This is a contradiction, so $a \notin (\mathbb{Z}/n\mathbb{Z})^\times$ and $\mathbb{Z}/n\mathbb{Z}$ is not a field.
"⇐": Let $n = p$ be prime and $a \in \{1, \ldots, p-1\}$. Consider the map

$$m_a : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}, \qquad x \longmapsto a \cdot x.$$

This map is injective: if $ax = ay$ in $\mathbb{Z}/p\mathbb{Z}$ with $x, y \in \{0, \ldots, p-1\}$, then p divides $ax - ay = a(x-y)$. Since p is prime and $p \nmid a$, we get $p \mid x - y$ (Euclid's lemma: if a prime divides a product, it divides one of the factors). As $|x - y| < p$, this means $x = y$. An injective map from a finite set to itself is also surjective. Hence there is an x with $ax = 1$, i.e. $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. □

Remark 2.23. The proof of "⇒" shows a general principle: if $ab = 0$ with $a, b \neq 0$ ("zero divisors"), then a and b cannot have inverses. The proof of "⇐" is not constructive. In Lecture 5 we will compute inverses in $\mathbb{Z}/p\mathbb{Z}$ efficiently with the Euclidean algorithm.

Definition 2.24. *For a prime p we write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and call it the* **finite field with p elements**.

Example. *The smallest field is $\mathbb{F}_2 = \{0, 1\}$ with $1 + 1 = 0$. If we think of 0 as "even" and 1 as "odd", the tables of $\mathbb{F}_2$ are the rules "odd + odd = even", "odd · odd = odd", etc. In $\mathbb{F}_2$ we have $-1 = 1$.*

Remark 2.25 (A field with 4 elements). Proposition 2.22 does **not** say that every field with finitely many elements has a prime number of elements. It only says that $\mathbb{Z}/n\mathbb{Z}$ is not a field when n is composite. In fact, there is a field with 4 elements,

$$\mathbb{F}_4 = \{0,\ 1,\ \alpha,\ \alpha + 1\}.$$

We compute with the expressions $a + b\alpha$ with $a, b \in \mathbb{F}_2$ as with polynomials in α, taking coefficients modulo 2, and replace α^2 by $\alpha + 1$. For example, $\alpha(\alpha + 1) = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1$, since $2 = 0$ in $\mathbb{F}_2$. So α and $\alpha + 1$ are inverse to each other. In $\mathbb{F}_4$ we have $1 + 1 = 0$, while $1 + 1 = 2 \neq 0$ in $\mathbb{Z}/4\mathbb{Z}$. So $\mathbb{F}_4$ is **not** $\mathbb{Z}/4\mathbb{Z}$. We construct $\mathbb{F}_4$ properly, and check the field axioms, in Lecture 10.
In general, a finite field always has p^n elements for a prime p (Corollary 2.29 below). Conversely, for every prime power p^n there is exactly one field with p^n elements, up to renaming the elements. This field is denoted $\mathbb{F}_{p^n}$ (Lecture 10). So there are fields with 4, 8 and 9 elements, but none with 6, 10 or 12 elements.

Proposition 2.26. *$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field (with the operations of $\mathbb{R}$).*

Proof. $\mathbb{Q}(\sqrt{2})$ contains 0 and 1 and is closed under $+$, $-$ and $\cdot$, since

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}.$$

All rules of a commutative ring are inherited from $\mathbb{R}$. Let $a+b\sqrt{2} \neq 0$. Then $a^2-2b^2 \neq 0$: otherwise $b \neq 0$ (as $b=0$ would give $a=0$) and $\left(\frac{a}{b}\right)^2 = 2$, which is impossible since $\sqrt{2}$ is irrational. Hence

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}). \qquad \square$$

For example $\frac{1}{1+\sqrt{2}} = -1+\sqrt{2}$. Such **field extensions** of $\mathbb{Q}$ are a main topic of Lectures 7–10.

Until here in Lecture 3 (19 October 2026)

2.4 Linear algebra over an arbitrary field

In the definition of a vector space we can replace $\mathbb{R}$ by any field K.

Definition 2.27. *Let K be a field. A* **vector space over** K *(or* K**-vector space**$)$ *is an abelian group $(V,+)$ together with a scalar multiplication $K \times V \to V$, $(\lambda, v) \mapsto \lambda v$, such that for all $\lambda, \mu \in K$ and $v, w \in V$*

$$\lambda(v+w) = \lambda v + \lambda w, \qquad (\lambda+\mu)v = \lambda v + \mu v, \qquad (\lambda\mu)v = \lambda(\mu v), \qquad 1v = v.$$

Principle: Everything from Linear Algebra I/II whose proof only uses $+, -, \cdot$ and division by non-zero scalars works over any field K, with the same proofs. This includes: Gaussian elimination, linear independence, bases and dimension, rank, linear maps and their matrices, determinants, invertibility (A invertible $\iff \det(A) \neq 0$), and eigenvectors.
What does **not** carry over directly are notions that use sizes or order, such as lengths, angles, inner products and orthogonality. Also, eigenvalues need not exist in K (Example 2.31).

Proposition 2.28. *Let K be a finite field with q elements and V a K-vector space of dimension n. Then $|V| = q^n$.*

Proof. Let $v_1, \ldots, v_n$ be a basis of V. The map $K^n \to V$, $(\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1 v_1 + \cdots + \lambda_n v_n$ is surjective since the v_i span V, and injective since they are linearly independent. Hence $|V| = |K^n| = q^n$. $\square$

Corollary 2.29. *Every finite field K has p^n elements for some prime p and some $n \geq 1$. In particular, there is no field with 6 elements.*

Idea of proof. Since K is finite, the elements $1,\ 1+1,\ 1+1+1, \ldots$ cannot all be different. Hence $m \cdot 1 = 1+\cdots+1 = 0$ for some $m \geq 1$. Let p be the smallest such m. This integer is called the **characteristic** of K, written $\mathrm{char}(K) = p$. Then $p \geq 2$, since $1 \neq 0$. If $p = ab$ with $1 < a, b < p$, then $(a \cdot 1)(b \cdot 1) = p \cdot 1 = 0$ with both factors non-zero. This is impossible in a field (Remark 2.23), so p is prime. The elements $0,\ 1,\ 2 \cdot 1, \ldots, (p-1) \cdot 1$ of K add and multiply exactly like $\mathbb{F}_p$. So we can multiply elements of K by scalars from $\mathbb{F}_p$, and K becomes an $\mathbb{F}_p$-vector space. Since K is finite, its dimension n is finite, and $|K| = p^n$ by Proposition 2.28. $\square$

For example, $\mathbb{F}_4$ from Remark 2.25 is an $\mathbb{F}_2$-vector space with basis $1, \alpha$, so $|\mathbb{F}_4| = 2^2$. Its addition is componentwise in the coordinates (a, b) of $a + b\alpha$. Hence $(\mathbb{F}_4, +)$ is the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of bit strings (Example 2.11), not $\mathbb{Z}/4\mathbb{Z}$.

Example 2.30 (Vector spaces)**.** *(i) $K^n = \{(x_1, \ldots, x_n) \mid x_i \in K\}$ with componentwise operations is a K-vector space of dimension n.*

(ii) $\mathbb{F}_2^n$ *is the set of all "bit strings" of length* n*. It has* 2^n *elements. Its addition is the XOR of Example 2.11, so* $(\mathbb{F}_2^n, +) = (\mathbb{Z}/2\mathbb{Z})^n$*.*

(iii) The dimension depends on the field of scalars: $\mathbb{C}$ *is a* $\mathbb{C}$*-vector space of dimension* 1*, but an* $\mathbb{R}$*-vector space of dimension* 2 *with basis* $\{1, i\}$*.*

(iv) $\mathbb{Q}(\sqrt{2})$ *is a* $\mathbb{Q}$*-vector space of dimension* 2 *with basis* $\{1, \sqrt{2}\}$*. (The elements* $1, \sqrt{2}$ *are linearly independent over* $\mathbb{Q}$ *since* $\sqrt{2} \notin \mathbb{Q}$*.)*

(v) $\mathbb{R}$ *is a* $\mathbb{Q}$*-vector space of infinite dimension. (Otherwise* $\mathbb{R}$ *would be countable, like* $\mathbb{Q}^n$*.)*

Example 2.31 (Eigenvalues depend on the field)**.** *The rotation* $A = R_{\pi/2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *has the characteristic polynomial* $\det(tI - A) = t^2 + 1$*.*

- *Over* $\mathbb{R}$*,* A *has no eigenvalues (a rotation by* $90°$ *fixes no line).*
- *Over* $\mathbb{C}$*,* A *has the eigenvalues* i *and* $-i$*.*
- *Over* $\mathbb{F}_5$*,* A *has the eigenvalues* 2 *and* 3*, since* $2^2 + 1 = 3^2 + 1 = 0$ *in* $\mathbb{F}_5$*. For example*

$$A\begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} -3 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2\begin{pmatrix} 1 \\ 3 \end{pmatrix} \qquad \text{in } \mathbb{F}_5^2.$$

Remark 2.32. We will see that $E(\mathbb{F}_5)$ is a group with 8 elements. By Proposition 2.28, an $\mathbb{F}_5$-vector space has 5^n elements, so $E(\mathbb{F}_5)$ cannot be an $\mathbb{F}_5$-vector space. This is one reason why we need more general structures than vector spaces.

Example 2.33 (Gaussian elimination over $\mathbb{F}_5$)**.** *We solve the following system in* $\mathbb{F}_5$*:*

$$x + 2y + z = 3, \qquad 2x + y + 3z = 1, \qquad x + y + z = 4.$$

All calculations are in $\mathbb{F}_5$*. We use the circled multipliers and arrows from the Linear Algebra notes: a circled factor on an arrow means that we add that multiple of the source row to the target row. A circled factor without an arrow scales that row.*

$$\begin{pmatrix} 1 & 2 & 1 & 3 \\ 2 & 1 & 3 & 1 \\ 1 & 1 & 1 & 4 \end{pmatrix} \overset{\substack{\textcircled{-1}\ \textcircled{-2}}}{\sim} \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 2 & 1 & 0 \\ 0 & 4 & 0 & 1 \end{pmatrix} \overset{\textcircled{4}}{\sim} \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 4 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{pmatrix}$$

$$\overset{\textcircled{-2}\ \textcircled{-2}}{\sim} \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & 0 & 4 \\ 0 & 2 & 1 & 0 \end{pmatrix} \overset{\textcircled{-1}}{\sim} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

For example, $1 - 2 \cdot 2 = -3 = 2$ *in the first step. To make the second pivot* 1*, we multiply by* 4*, since* $4^{-1} = 4$ *in* $\mathbb{F}_5$*. The final matrix is in* **reduced row echelon form***, so the unique solution is*

$$(x, y, z) = (3, 4, 2).$$

Check in the original equations: $3 + 8 + 2 = 13 = 3$*,* $6 + 4 + 6 = 16 = 1$*, and* $3 + 4 + 2 = 9 = 4$ *in* $\mathbb{F}_5$*.*

Example 2.34 (A line with two points)**.** *The system $x+y=1$, $y+z=1$, $x+z=0$ over $\mathbb{F}_2$ has rank 2 (the third equation is the sum of the first two, since $2y=0$ in $\mathbb{F}_2$). The solution set is the affine line $v_0+\operatorname{span}\{v_1\}$, here*

$$\begin{pmatrix}0\\1\\0\end{pmatrix}+\operatorname{span}\left\{\begin{pmatrix}1\\1\\1\end{pmatrix}\right\}=\left\{\begin{pmatrix}0\\1\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\end{pmatrix}\right\}.$$

Over $\mathbb{F}_2$ a "line" consists of just 2 points!

Remark 2.35. Over $\mathbb{F}_2$ the vector $v=(1,1)$ satisfies $v\cdot v=1^2+1^2=0$, although $v\neq 0$. This is why lengths and angles do not make sense over finite fields.

2.5 Modules: linear algebra over a ring

A natural question is: what happens if the scalars only form a ring, such as $\mathbb{Z}$, instead of a field? Many arguments in linear algebra use division by non-zero scalars, and we will see that some familiar statements are no longer true.

Definition 2.36. *Let R be a commutative ring.*

*(i) An R-**module** is an abelian group $(M,+)$ together with a scalar multiplication $R\times M\to M$, $(r,v)\mapsto rv$, such that for all $r,s\in R$ and $v,w\in M$*

$$r(v+w)=rv+rw,\qquad (r+s)v=rv+sv,\qquad (rs)v=r(sv),\qquad 1v=v.$$

*(ii) As in linear algebra, a subset $S\subseteq M$ **generates** M if every $v\in M$ is a linear combination $r_1v_1+\cdots+r_kv_k$ with $r_i\in R$, $v_i\in S$. The set S is **linearly independent** if $r_1v_1+\cdots+r_kv_k=0$ with distinct $v_i\in S$ implies $r_1=\cdots=r_k=0$. A **basis** is a linearly independent generating set. M is **finitely generated** if it has a finite generating set.*

If $R=K$ is a field, a K-module is exactly a K-vector space. Further examples are R^n (with the standard basis $e_1,\dots,e_n$) and $\mathbb{Z}/6\mathbb{Z}$ with the scalars $\mathbb{Z}$ (multiply, then take the remainder).
For a matrix $A\in \mathrm{M}_n(R)$ the determinant $\det(A)\in R$ is defined by the same formula as in linear algebra, and it is still multiplicative: $\det(AB)=\det(A)\det(B)$.

Proposition 2.37. *Let R be a commutative ring and $A\in \mathrm{M}_n(R)$. Then there exists $B\in \mathrm{M}_n(R)$ with $AB=BA=I_n$ if and only if $\det(A)\in R^\times$. In particular, a matrix $A\in \mathrm{M}_n(\mathbb{Z})$ has an inverse with integer entries if and only if $\det(A)=\pm 1$.*

Proof. "⇒": From $AB=I_n$ we get $\det(A)\det(B)=\det(I_n)=1$, so $\det(A)\in R^\times$.
"⇐": We give the proof for $n=2$. For $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ let $A^{\#}=\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\in \mathrm{M}_2(R)$. Then

$$AA^{\#}=A^{\#}A=\begin{pmatrix}ad-bc&0\\0&ad-bc\end{pmatrix}=\det(A)\,I_2.$$

If $\det(A)\in R^\times$, then $B=\det(A)^{-1}A^{\#}$ has entries in R and satisfies $AB=BA=I_2$. For general n the same argument works with the adjugate matrix $\operatorname{adj}(A)$ (the transposed matrix of cofactors), which has entries in R and satisfies $A\operatorname{adj}(A)=\operatorname{adj}(A)A=\det(A)I_n$ (Laplace expansion). □

Example 2.38 (Linear algebra over $\mathbb{Z}$ behaves differently)**.**

(i) **An injective linear map need not be surjective.** *The matrix*

$$A=\begin{pmatrix}2&0\\0&1\end{pmatrix}$$

defines a $\mathbb{Z}$-linear map $\mathbb{Z}^2 \to \mathbb{Z}^2$. It is injective, since $Ax = (2x_1, x_2)^T = 0$ implies $x = 0$. But $\begin{pmatrix}1\\0\end{pmatrix}$ is not in the image, since $2x_1 = 1$ has no solution in $\mathbb{Z}$. Although $\det(A) = 2 \neq 0$, the inverse $\begin{pmatrix}1/2 & 0\\0 & 1\end{pmatrix}$ has non-integer entries. Thus A is not invertible over $\mathbb{Z}$ (Proposition 2.37). Over $\mathbb{Q}$, A is invertible.

(ii) **A minimal generating set need not be a basis.** *The elements $2, 3$ generate the $\mathbb{Z}$-module $\mathbb{Z}$, since $n = n \cdot 3 + (-n) \cdot 2$ for every $n \in \mathbb{Z}$. They are linearly dependent, since $3 \cdot 2 + (-2) \cdot 3 = 0$. But neither of them can be removed: 2 alone generates only the even numbers $2\mathbb{Z}$, and 3 alone only $3\mathbb{Z}$. (Over a field, every generating set contains a basis.)*

(iii) **A finitely generated module need not have a basis.** *The $\mathbb{Z}$-module $\mathbb{Z}/6\mathbb{Z}$ is generated by 1. But for every $v \in \mathbb{Z}/6\mathbb{Z}$ we have $6 \cdot v = 0$ with $6 \neq 0$ in $\mathbb{Z}$, so no non-empty subset is linearly independent. Hence $\mathbb{Z}/6\mathbb{Z}$ has no basis over $\mathbb{Z}$. (Over the ring $\mathbb{Z}/6\mathbb{Z}$ itself, $\{1\}$ is a basis. The ring of scalars matters!)*

Proposition 2.39. *Let $(G, +)$ be an abelian group. Then there is exactly one way to make G a $\mathbb{Z}$-module, namely*

$$ng = \underbrace{g + \cdots + g}_{n \text{ terms}}, \qquad 0g = 0, \qquad (-n)g = -(ng) \qquad (n \in \mathbb{N},\ g \in G).$$

Proof. See Homework 1, Exercise 6. (The uniqueness follows from $1g = g$ and the distributive law: $ng = (1 + \cdots + 1)g = g + \cdots + g$.) □

So "abelian group" and "$\mathbb{Z}$-module" mean the same thing. In this language, Mordell's theorem (Section 3.6) says that $E(\mathbb{Q})$ is a **finitely generated** $\mathbb{Z}$-module. We will see that this implies $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$ with a finite group T. The **rank** r and the **torsion** T take over the role that dimension and basis play for vector spaces.

Until here in Lecture 4 (26 October 2026)

3 Elliptic curves

3.1 Curves and their rational points

Before studying elliptic curves, we begin with polynomial equations defining plane curves. Lines and conics provide familiar examples, and Pythagorean triples connect integer solutions with rational points on the unit circle. This introduction follows the approach of [ST, Chapter 1].
Let K be a field and let $f(x, y)$ be a non-constant polynomial with coefficients in K. The set

$$C(K) = \{(x, y) \in K^2 \mid f(x, y) = 0\}$$

is the set of **K-rational points** of the curve $C : f(x, y) = 0$. For $K = \mathbb{R}$, these are the real points we can draw in the plane.

Dimension. Informally, an **algebraic variety** is a geometric object described by polynomial equations. We now want to make its dimension precise in the **affine** case, where the equations use coordinates $x_1, \ldots, x_n$.
Let V be a nonempty affine algebraic set over K and let $\overline{K}$ be an **algebraic closure** of K, i.e. an algebraic extension in which every nonconstant polynomial splits into linear factors. We call coordinate functions $x_{i_1}, \ldots, x_{i_d}$ **algebraically independent on** V if there is no nonzero polynomial $P \in \overline{K}[T_1, \ldots, T_d]$ such that

$$P(x_{i_1}, \ldots, x_{i_d}) = 0 \qquad \text{at every point of } V(\overline{K}).$$

The **dimension** $\dim V$ is the largest possible number d of such coordinate functions. This number is independent of the chosen affine embedding (see [Mi, Section 2m]). For a general variety, one computes dimension in affine coordinate charts and takes the largest value.

- A point has dimension 0: each coordinate is constant, so it satisfies a relation $x_i - a_i = 0$. Affine n-space has dimension n: its coordinates satisfy no nonzero polynomial relation.
- The circle $x^2 + y^2 = 1$ has dimension 1. Every $x \in \overline{K}$ occurs, since $y^2 = 1 - x^2$ has a solution in $\overline{K}$, so no nonzero polynomial in x alone vanishes everywhere. But x and y satisfy the relation $x^2 + y^2 - 1 = 0$. The same reasoning gives dimension 1 for $y^2 = x^3 + Ax + B$, even when the curve is singular.
- The sphere $x^2 + y^2 + z^2 = 1$ has dimension 2: any pair $(x, y) \in \overline{K}^2$ extends to a solution by choosing z, while all three coordinates satisfy the displayed relation. A variety of dimension 1 is called a **curve**, and a variety of dimension 2 is called a **surface**.

Over $\mathbb{R}$ or $\mathbb{C}$, near a nonsingular point on a component of dimension d, this agrees with having d independent local real or complex parameters. Thus a smooth complex curve has two real dimensions. This local description does not imply a global rational parametrisation.
Notice that over $\mathbb{F}_q$ every coordinate on $V(\mathbb{F}_q)$ satisfies $x_i^q - x_i = 0$. Testing polynomial relations only on $V(\mathbb{F}_q)$ would therefore give dimension 0, which is why we consider all points in $V(\overline{K})$. A curve over a finite field still has dimension 1, even though it has only finitely many rational points. Dimension is not the number of points or the vector-space dimension of the point set, which is generally not a vector space.
For the following examples, we take coefficients in $\mathbb{Q}$ and ask for $C(\mathbb{Q})$. The answer depends very much on the degree of f.
Degree 1. A line $ax + by + c = 0$ with $a, b, c \in \mathbb{Q}$ and $b \neq 0$ has the rational points $\left(x, -\frac{ax+c}{b}\right)$, $x \in \mathbb{Q}$.
Degree 2. We consider the unit circle $C : x^2 + y^2 = 1$ with the known rational point $(-1, 0)$.

Proposition 3.1. *The rational points on the unit circle are*

$$C(\mathbb{Q}) = \{(-1, 0)\} \cup \left\{ \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) \;\middle|\; t \in \mathbb{Q} \right\}.$$

Proof. Let $t \in \mathbb{Q}$ and consider the line $y = t(x + 1)$ through $(-1, 0)$ with slope t. Its intersection points with C satisfy $x^2 + t^2(x + 1)^2 = 1$, i.e.

$$(1 + t^2)\, x^2 + 2t^2\, x + (t^2 - 1) = 0.$$

This quadratic equation has the root $x_1 = -1$. If x_2 is the other root, then $x_1 x_2 = \frac{t^2-1}{1+t^2}$ (product of the roots), so

$$x_2 = \frac{1 - t^2}{1 + t^2} \in \mathbb{Q}, \qquad y_2 = t(x_2 + 1) = \frac{2t}{1 + t^2} \in \mathbb{Q}.$$

So all the points in the claim are rational points on C. Conversely, let $(x, y) \in C(\mathbb{Q})$ with $(x, y) \neq (-1, 0)$. Then $x \neq -1$ (since $x = -1$ forces $y = 0$), so the line through $(-1, 0)$ and (x, y) has the rational slope $t = \frac{y}{x+1}$. By the computation above, its second intersection point with C is $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$, which therefore equals (x, y). □

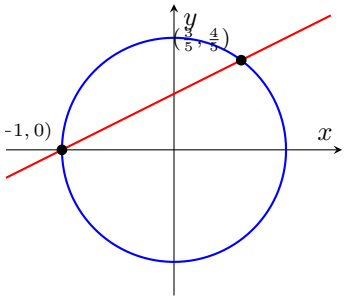


Figure 5: The line through $(-1,0)$ with slope $t = \frac{1}{2}$ meets the unit circle in $\left(\frac{3}{5}, \frac{4}{5}\right)$.

Pythagorean triples

A **Pythagorean triple** is a triple of positive integers (a,b,c) with $a^2+b^2=c^2$. Dividing by c^2 gives a rational point $\left(\frac{a}{c}, \frac{b}{c}\right)$ on $x^2+y^2=1$. Conversely, clearing denominators of a rational point with positive coordinates gives a Pythagorean triple. Thus the parametrisation of the circle describes all such triples.

Example. $t = \frac{1}{2}$ *gives* $\left(\frac{3}{5}, \frac{4}{5}\right)$, *i.e.* $3^2+4^2=5^2$, *and* $t = \frac{2}{3}$ *gives* $\left(\frac{5}{13}, \frac{12}{13}\right)$, *i.e.* $5^2+12^2=13^2$.

Corollary 3.2. *Every Pythagorean triple* $(a,b,c) \in \mathbb{N}^3$, $a^2+b^2=c^2$, *is proportional to* $(n^2-m^2,\ 2mn,\ n^2+m^2)$ *for some* $m,n \in \mathbb{Z}$.

Proof. $\left(\frac{a}{c}, \frac{b}{c}\right)$ is a rational point on C different from $(-1,0)$, so by Proposition 3.1 it equals $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ for some $t = \frac{m}{n} \in \mathbb{Q}$. Multiplying numerator and denominator by n^2 gives $\frac{a}{c} = \frac{n^2-m^2}{n^2+m^2}$ and $\frac{b}{c} = \frac{2mn}{n^2+m^2}$. □

The key observation in the proof is: **a quadratic equation with rational coefficients and one rational root has its other root rational too.** Of course, a curve of degree 2 need not have a rational point to start with:

Proposition 3.3. *The circle* $x^2+y^2=3$ *has no rational points.*

Proof. Suppose $x = \frac{a}{c}$, $y = \frac{b}{c}$ with $a,b \in \mathbb{Z}$, $c \in \mathbb{N}$ and $\gcd(a,b,c) = 1$ (common denominator, then cancel common factors). Then $a^2+b^2 = 3c^2$. The squares modulo 3 are $0^2 = 0$ and $1^2 = 2^2 = 1$. Since $a^2+b^2 \equiv 0 \bmod 3$, both a^2 and b^2 must be $\equiv 0$, i.e. $3 \mid a$ and $3 \mid b$. Then $9 \mid a^2+b^2 = 3c^2$, so $3 \mid c^2$ and $3 \mid c$. This contradicts $\gcd(a,b,c) = 1$. □

Degree 3. For a cubic curve, a line through **one** rational point leads to a cubic equation with one known root, and the other two roots are in general not rational. But a line through **two** rational points leads to a cubic equation with two known rational roots, and then the third root is rational as well (Proposition 3.7). This is the key to everything that follows.

3.2 Elliptic curves

We now return to the equations introduced in Section 1.2, allow coefficients in other fields, and explain the non-zero discriminant condition.

Definition 3.4. *Let* K *be a field with* $2 \neq 0$ *and* $3 \neq 0$ *in* K *(e.g.* $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *or* $\mathbb{F}_p$ *with* $p \geq 5$, *see Remark 2.14).*

(i) An **elliptic curve** *over* K *is given by an equation*

$$E:\ y^2 = x^3 + Ax + B, \qquad A,B \in K, \qquad 4A^3 + 27B^2 \neq 0.$$

(ii) The set of K**-rational points** *of* E *is*

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ *is an extra point, the "point at infinity".*

Over an arbitrary field. Over any field K, an elliptic curve can be given by a **general Weierstrass equation**

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in K,$$

together with the chosen point at infinity $\mathcal{O} = [0 : 1 : 0]$, which is the group identity. We require the resulting projective curve to be nonsingular, even after extending the field. When $\mathrm{char}(K) \neq 2, 3$, changes of variables remove the extra terms and give the short equation above. In characteristics 2 and 3, those terms may be necessary (see Remark 2.14).

Example (Changing to a short Weierstrass equation)**.** *Over* $\mathbb{Q}$*, consider*

$$y^2 + 2xy + 2y = x^3 + 2x^2.$$

Putting $Y = y + x + 1$ *gives*

$$Y^2 = y^2 + 2xy + 2y + (x + 1)^2 = x^3 + 3x^2 + 2x + 1.$$

With $X = x + 1$ *we then get*

$$x^3 + 3x^2 + 2x + 1 = (x + 1)^3 - (x + 1) + 1 = X^3 - X + 1.$$

Thus the equation becomes $Y^2 = X^3 - X + 1$*. The inverse substitution is given by* $x = X - 1$ *and* $y = Y - X$*. In general, completing the square uses division by* 2*, and removing the quadratic term of the cubic uses division by* 3*. This explains the assumption that* $2, 3 \neq 0$ *in* K*.*

For the following computations we return to the short equation with $2, 3 \neq 0$ in K. Its discriminant is $\Delta(E) = -16(4A^3 + 27B^2)$, so $\Delta(E) \neq 0$ is equivalent to $4A^3 + 27B^2 \neq 0$. This condition means that the curve is **non-singular**: over $\mathbb{R}$, its plane picture has no cusps or self-intersections. Algebraically, it says that the cubic has no repeated roots, as the following lemma explains. Here we use the **formal derivative** $f'(x) = 3x^2 + A$ of $f(x) = x^3 + Ax + B$, which makes sense over every field.

Lemma 3.5. *Let* $f(x) = x^3 + Ax + B$ *with* $A, B \in K$*. Then* f *has a repeated root* r *(i.e.* $(x - r)^2$ *divides* f*) if and only if* $4A^3 + 27B^2 = 0$*. More precisely,* r *is a repeated root of* f *if and only if* $f(r) = f'(r) = 0$*.*

Proof. If $f(r) = 0$, then $f(x) = (x - r)g(x)$ with a polynomial g, and $f'(x) = g(x) + (x - r)g'(x)$ (product rule), so $f'(r) = g(r)$. Hence r is a repeated root $\iff g(r) = 0 \iff f(r) = f'(r) = 0$. Now suppose $f(r) = f'(r) = 0$, i.e. $r^3 + Ar + B = 0$ and $3r^2 = -A$. Then $0 = r(r^2 + A) + B = r \cdot \frac{2A}{3} + B$. If $A = 0$, this gives $B = 0$, so $4A^3 + 27B^2 = 0$. If $A \neq 0$, then $r = -\frac{3B}{2A}$, and $3r^2 = -A$ gives $\frac{27B^2}{4A^2} = -A$, i.e. $4A^3 + 27B^2 = 0$.
Conversely, suppose $4A^3 + 27B^2 = 0$. If $A = 0$, then $B = 0$ and $f = x^3$ has the repeated root 0. If $A \neq 0$, let $r = -\frac{3B}{2A}$. Then $3r^2 + A = \frac{27B^2 + 4A^3}{4A^2} = 0$, so $f'(r) = 0$ and $r^2 = -\frac{A}{3}$, and hence $f(r) = r(r^2 + A) + B = r \cdot \frac{2A}{3} + B = -B + B = 0$. □

Example.

curve	$4A^3 + 27B^2$	
$y^2 = x^3 - x + 1$	$-4 + 27 = 23$	*elliptic curve*
$y^2 = x^3 - x = (x + 1)x(x - 1)$	-4	*elliptic curve*
$y^2 = x^3 - 2$	$27 \cdot 4 = 108$	*elliptic curve*
$y^2 = x^3$	0	*singular (cusp at* $(0, 0)$*)*
$y^2 = x^3 - 3x + 2 = (x - 1)^2(x + 2)$	$-108 + 108 = 0$	*singular (node at* $(1, 0)$*)*

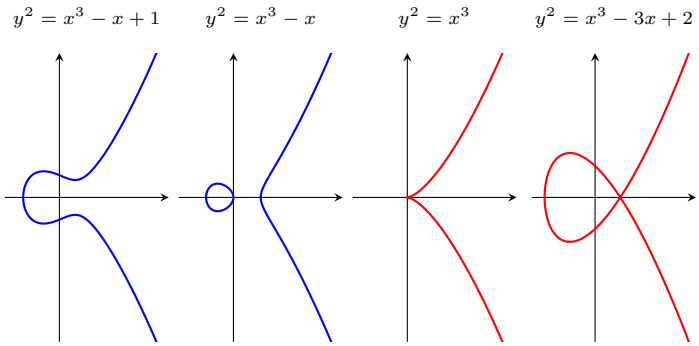


Figure 6: Two elliptic curves over $\mathbb{R}$ (with one and two components) and two singular cubics (cusp and node).

Remark 3.6. (i) $E(\mathbb{R})$ has one component if $x^3 + Ax + B$ has one real root, and two components if it has three real roots, see Figure 6.

(ii) **Symmetry:** if $(x, y) \in E(K)$, then also $(x, -y) \in E(K)$, since only y^2 appears in the equation.

(iii) **The point $\mathcal{O}$:** think of $\mathcal{O}$ as a point "infinitely far up and down", where all vertical lines meet. So the vertical line $x = c$ meets E in (c, y), $(c, -y)$ and $\mathcal{O}$. This can be made precise using the projective plane: E is given by $Y^2Z = X^3 + AXZ^2 + BZ^3$ and $\mathcal{O} = [0 : 1 : 0]$ (see [ST, Appendix A]). We will not need this.

(iv) **An algebraic group:** Including $\mathcal{O}$, the smooth projective curve E is a **one-dimensional abelian variety**. Its abelian group structure is compatible with its algebraic geometry: addition $(P, Q) \mapsto P + Q$ and inversion $P \mapsto -P$ are **regular maps**. In suitable local coordinates, these maps are described by quotients of polynomials whose denominators are nonzero throughout the neighbourhood where the formulas are used. Different coordinate charts may require different formulas, including near $\mathcal{O}$.

(v) **Why a torus?** An elliptic curve over $\mathbb{C}$, including $\mathcal{O}$, has one complex dimension, hence two real dimensions. A theorem (without proof here) identifies

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda, \qquad \Lambda = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\},$$

for suitable $\omega_1, \omega_2 \in \mathbb{C}$ linearly independent over $\mathbb{R}$. The lattice Λ is a repeating grid in the complex plane. In $\mathbb{C}/\Lambda$, complex numbers differing by a lattice vector represent the same point. Every point has a representative in the parallelogram spanned by ω_1, ω_2, with opposite edges identified. Glue one pair of opposite edges to form a cylinder, then join its two circular ends: the resulting surface is **topologically a torus**, the surface of a doughnut.

This identification preserves the complex structure and group law: $\mathcal{O}$ corresponds to $[0]$, and $[z] + [w] = [z + w]$. To add, add complex numbers and subtract a lattice vector to return to the parallelogram. For real coefficients, $E(\mathbb{R})$, including $\mathcal{O}$, consists topologically of one or two circles. The drawing in the real plane omits $\mathcal{O}$, whereas the torus describes all of $E(\mathbb{C})$.

(vi) **The isomorphism more explicitly.** Keep $E : y^2 = x^3 + Ax + B$ over $\mathbb{C}$. The parameter $z \in \mathbb{C}$ represents a class $[z] \in \mathbb{C}/\Lambda$ and is not the x-coordinate of a point on E.

To obtain the lattice from the curve, use the differential $\eta = \frac{dx}{2y}$, which we integrate along smooth paths on $E(\mathbb{C})$. It extends without poles over the whole curve, including $\mathcal{O}$. The apparent division by zero at $y = 0$ disappears in another coordinate chart. Integrals around closed paths are called **periods**. Part of the theorem is that all these periods form a lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, with ω_1, ω_2 linearly independent over $\mathbb{R}$. The map from the curve to the torus is

$$\alpha : E(\mathbb{C}) \longrightarrow \mathbb{C}/\Lambda, \qquad P \longmapsto \left[\int_{\mathcal{O}}^{P} \frac{dx}{2y}\right].$$

Choose any path from $\mathcal{O}$ to P. Two choices differ by going around a closed path, so their integrals differ by a period. Thus the class modulo Λ is independent of the path, and $\alpha(\mathcal{O}) = [0]$.

Conversely, the **Weierstrass $\wp$-function** associated with this lattice is

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right), \qquad z \notin \Lambda.$$

The series converges away from the lattice. This function has the periods in Λ: $\wp_\Lambda(z + \lambda) = \wp_\Lambda(z)$ for $\lambda \in \Lambda$. Writing $\wp'_\Lambda$ for its complex derivative, the inverse map is

$$\beta : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}), \qquad [z] \longmapsto \begin{cases} \left(\wp_\Lambda(z), \frac{1}{2}\wp'_\Lambda(z)\right), & z \notin \Lambda, \\ \mathcal{O}, & z \in \Lambda. \end{cases}$$

Periodicity makes this independent of the representative z. The poles at lattice points correspond to the point at infinity. For the lattice obtained from E above, the function satisfies

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 + 4A\wp_\Lambda(z) + 4B.$$

Dividing this identity by 4 shows that the coordinates in $\beta([z])$ satisfy $y^2 = x^3 + Ax + B$.

The **uniformization theorem** asserts that α and β are inverse maps, are holomorphic (complex-differentiable in local coordinates), and preserve addition: $\alpha(P+Q) = \alpha(P)+\alpha(Q)$. Thus two complex parameters give the same point exactly when their difference lies in Λ. We state this theorem without proof.

3.3 Lines meet elliptic curves in three points

Proposition 3.7. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over K and $L : y = \lambda x + \nu$ a non-vertical line with $\lambda, \nu \in K$. If $x_1, x_2, x_3 \in K$ are the roots of*

$$x^3 + Ax + B - (\lambda x + \nu)^2 = x^3 - \lambda^2 x^2 + (A - 2\lambda\nu)\, x + (B - \nu^2), \tag{3.1}$$

i.e. the x-coordinates of the intersection points of L and E (counted with multiplicity), then

$$x_1 + x_2 + x_3 = \lambda^2.$$

In particular: if L meets E in two points of $E(K)$ with x-coordinates x_1, x_2 (where $x_1 = x_2$ is allowed if L is tangent there, i.e. x_1 is a double root), then the third intersection point has the x-coordinate $x_3 = \lambda^2 - x_1 - x_2 \in K$ and lies in $E(K)$.

Proof. A point (x, y) lies on L and E if and only if $y = \lambda x + \nu$ and $(\lambda x + \nu)^2 = x^3 + Ax + B$, i.e. x is a root of (3.1). If x_1 and x_2 are roots in K (with x_1 a double root if $x_1 = x_2$), then the

monic cubic polynomial (3.1) is divisible by $(x - x_1)(x - x_2)$, and the quotient is a monic linear polynomial $x - x_3$ with $x_3 \in K$. Expanding

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)\, x^2 + \dots$$

and comparing the coefficients of x^2 with (3.1) gives $x_1 + x_2 + x_3 = \lambda^2$. The third intersection point is $(x_3, \lambda x_3 + \nu) \in E(K)$. □

So every line meets E in exactly three points, if we count correctly: a tangent point counts twice, and a vertical line meets E in two points $(c, \pm y)$ (or in one point counted twice, if $y = 0$) and in $\mathcal{O}$.

3.4 The group law

Definition 3.8 (Chord-and-tangent rule)**.** *Let $P, Q \in E(K)$.*

(i) Draw the line through P and Q (the tangent line at P if $P = Q$), and let R be its third intersection point with E.

(ii) Define $P + Q$ to be the reflection of R at the x-axis, i.e. $P + Q = (x_R, -y_R)$.

Further, $P + \mathcal{O} = \mathcal{O} + P = P$ for all P, and we write $-(x, y) = (x, -y)$ and $-\mathcal{O} = \mathcal{O}$.

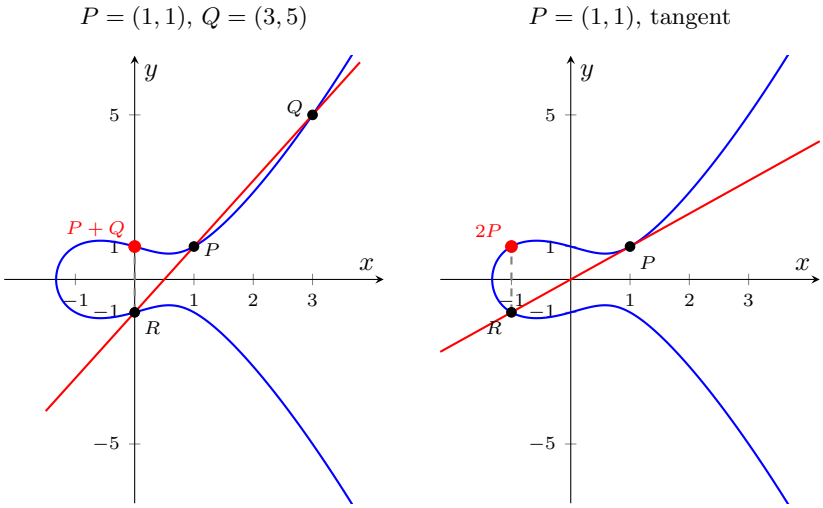


Figure 7: The chord-and-tangent rule on $E : y^2 = x^3 - x + 1$: $(1, 1) + (3, 5) = (0, 1)$ and $2 \cdot (1, 1) = (-1, 1)$.

Remark 3.9. Why do we reflect? If we simply defined $P + Q = R$, there would be no identity element. With the reflection, $\mathcal{O}$ is the identity (Proposition 2.13).

Over $\mathbb{R}$ the tangent line at $P = (x_1, y_1)$ with $y_1 \neq 0$ has the slope $\frac{3x_1^2 + A}{2y_1}$, by implicit differentiation of $y^2 = x^3 + Ax + B$: $2yy' = 3x^2 + A$. Formal differentiation of polynomials works over a general field too. The algebraic tangent at P is the line $2y_1(y - y_1) = (3x_1^2 + A)(x - x_1)$, which has the same slope. No limits are needed. The following proposition shows that it has the property we want: it meets E at P with multiplicity 2.

Proposition 3.10 (Addition formulas)**.** *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over K and $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(K)$.*

(i) If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \mathcal{O}$.

(ii) Otherwise let

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2, \end{cases} \qquad \begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1. \end{aligned}$$

Then $P_1 + P_2 = (x_3, y_3) \in E(K)$.

Proof. (i) If $x_1 = x_2$ and $y_1 = -y_2$, then P_1 and P_2 lie on the vertical line $x = x_1$, whose third intersection point is $\mathcal{O}$. The reflection of $\mathcal{O}$ is $\mathcal{O}$. (This includes the case $P_1 = P_2$ with $y_1 = 0$, where the tangent line is vertical.)
(ii) If $x_1 \neq x_2$, then $L : y = \lambda(x - x_1) + y_1$ with $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ is the line through P_1 and P_2. If $P_1 = P_2$ and $y_1 \neq 0$, let $L : y = \lambda(x - x_1) + y_1$ with $\lambda = \frac{3x_1^2 + A}{2y_1}$. We show that x_1 is a double root of $g(x) = x^3 + Ax + B - (\lambda(x - x_1) + y_1)^2$. We have $g(x_1) = x_1^3 + Ax_1 + B - y_1^2 = 0$ and

$$g'(x) = 3x^2 + A - 2\lambda\big(\lambda(x - x_1) + y_1\big), \qquad g'(x_1) = 3x_1^2 + A - 2\lambda y_1 = 0,$$

so x_1 is a double root by Lemma 3.5 (its first part holds for every polynomial). In both cases, Proposition 3.7 shows that the third intersection point of L and E is

$$R = (x_3,\ \lambda(x_3 - x_1) + y_1) \qquad \text{with} \qquad x_3 = \lambda^2 - x_1 - x_2 \in K.$$

Reflecting at the x-axis gives $P_1 + P_2 = (x_3, \lambda(x_1 - x_3) - y_1) = (x_3, y_3)$. □

Remark 3.11. The formulas only use $+, -, \cdot$ and division by non-zero elements. Hence they make sense over **every** field K (with $2, 3 \neq 0$), for example over $\mathbb{F}_p$. Lines and tangents are defined by their equations. Over $\mathbb{F}_p$, their pictures are finite sets of points.

We now return to Proposition 2.13. We prove the group axioms below, apart from associativity, which we quote.

Proof apart from associativity. By Proposition 3.10, $P + Q \in E(K)$ for all $P, Q \in E(K)$.

- **Identity:** $P + \mathcal{O} = \mathcal{O} + P = P$ by definition. (Geometrically: the line through P and $\mathcal{O}$ is the vertical line through P, its third intersection point is $-P$, and the reflection of $-P$ is P.)
- **Inverse:** $P = (x, y)$ and $-P = (x, -y)$ lie on a vertical line, so $P + (-P) = \mathcal{O}$ by Proposition 3.10 (i).
- **Commutativity:** the line through P and Q is the line through Q and P. (In the formulas: λ and x_3 are symmetric in P_1, P_2, and $y_3 = \lambda(x_1 - x_3) - y_1 = \lambda(x_2 - x_3) - y_2$ since $y_2 - y_1 = \lambda(x_2 - x_1)$.)
- **Associativity:** $(P + Q) + R = P + (Q + R)$ is much harder and we do not prove it. It can be verified by a long computation with the addition formulas (a computer algebra system can do this), or with more geometry. See [ST, Ch. 1.2]. □

Corollary 3.12. *(i) Three points $P, Q, R \in E(K)$ lie on a line if and only if $P + Q + R = \mathcal{O}$.*

(ii) $E(\mathbb{Q})$ is a subgroup of $E(\mathbb{R})$, i.e. sums and inverses of rational points are rational points.

Proof. (i) If P, Q, R lie on a line, then by definition $P + Q = -R$, so $P + Q + R = \mathcal{O}$. Conversely, if $P + Q + R = \mathcal{O}$, then $R = -(P + Q)$, which is the third intersection point of the line through P and Q. (ii) If P, Q have rational coordinates, then λ, x_3, y_3 in Proposition 3.10 are rational, and so are the coordinates of $-P$. □

Example. *For our guiding curve $E : y^2 = x^3 - x + 1$, the points $(-1, 1)$, $(0, 1)$, $(1, 1)$ lie on the line $y = 1$, so $(-1, 1) + (0, 1) + (1, 1) = \mathcal{O}$, and therefore $(-1, 1) + (0, 1) = -(1, 1) = (1, -1)$.*

3.5 Examples

For these calculations, we use the example $E : y^2 = x^3 - x + 1$, i.e. $A = -1$, $B = 1$.

(i) $P = (1,1)$, $Q = (3,5)$: $\lambda = \frac{5-1}{3-1} = 2$, $x_3 = 4-1-3 = 0$, $y_3 = 2(1-0)-1 = 1$, so $P+Q = (0,1)$ (Figure 7, left).

(ii) $2P$ for $P = (1,1)$: $\lambda = \frac{3\cdot 1-1}{2\cdot 1} = 1$, $x_3 = 1-1-1 = -1$, $y_3 = 1\cdot(1-(-1))-1 = 1$, so $2P = (-1,1)$. Check: the tangent $y = x$ meets E where $x^3-x+1 = x^2$, i.e. $(x-1)^2(x+1) = 0$.

(iii) $2P$ for $P = (0,1)$: $\lambda = -\frac{1}{2}$, $x_3 = \frac{1}{4}$, $y_3 = -\frac{1}{2}\left(0-\frac{1}{4}\right)-1 = -\frac{7}{8}$, so $2P = \left(\frac{1}{4}, -\frac{7}{8}\right)$. Check: $\left(\frac{1}{4}\right)^3 - \frac{1}{4} + 1 = \frac{49}{64} = \left(\frac{7}{8}\right)^2$. So from points with integer coordinates we obtain points with fractions.

For $Q = (1,1)$ the multiples $nQ = Q + \cdots + Q$ are:

n	nQ	n	nQ
1	$(1,1)$	6	$(\frac{1}{4}, \frac{7}{8})$
2	$(-1,1)$	7	$(-\frac{11}{9}, -\frac{17}{27})$
3	$(0,-1)$	8	$(\frac{19}{25}, -\frac{103}{125})$
4	$(3,-5)$	9	$(56,-419)$
5	$(5,11)$	10	$(\frac{159}{121}, \frac{1861}{1331})$

All the points from Section 1.5 appear (up to sign). The denominators of x are squares and those of y are cubes of the same number, e.g. $\frac{159}{11^2}$ and $\frac{1861}{11^3}$, and the numbers grow very fast.
The same curve over $\mathbb{F}_5$. Here $E(\mathbb{F}_5) = \{\mathcal{O},\ (0,1),\ (0,4),\ (1,1),\ (1,4),\ (3,0),\ (4,1),\ (4,4)\}$ has 8 elements. The same formulas apply, where division by 2 means multiplication by $2^{-1} = 3$:

(i) $(0,1)+(1,1)$: $\lambda = 0$, $x_3 = -1 = 4$, $y_3 = -1 = 4$, so $(0,1)+(1,1) = (4,4)$.

(ii) $2\cdot(0,1)$: $\lambda = \frac{-1}{2} = -3 = 2$, $x_3 = 4$, $y_3 = 2(0-4)-1 = -9 = 1$, so $2\cdot(0,1) = (4,1)$.

(iii) $2\cdot(3,0) = \mathcal{O}$, since the tangent at a point with $y = 0$ is vertical.

Compare (ii) with $2\cdot(0,1) = \left(\frac{1}{4}, -\frac{7}{8}\right)$ over $\mathbb{Q}$: in $\mathbb{F}_5$ we have $\frac{1}{4} = 4^{-1} = 4$ and $-\frac{7}{8} = -7\cdot 8^{-1} = -2\cdot 2 = 1$. So we get the same answer $(4,1)$: reducing modulo 5 is compatible with the group law. (This will be an important tool in Lecture 11.)

3.6 Outlook: generators and Mordell's theorem

Starting from finitely many rational points and adding again and again, do we get **all** rational points?
In linear algebra, $(x,y) = x(1,0)+y(0,1)$ with $x, y \in \mathbb{R}$ gives the whole plane $\mathbb{R}^2$. If we are only allowed to add and subtract, we get $m(1,0)+n(0,1)$ with $m, n \in \mathbb{Z}$, i.e. only the lattice $\mathbb{Z}^2$. In an abelian group, the elements "generated" by $P_1, \ldots, P_s$ are the **integer** combinations $n_1P_1 + \cdots + n_sP_s$, $n_i \in \mathbb{Z}$ (in the language of modules: the $\mathbb{Z}$-linear combinations).

Definition 3.13. *An abelian group G is* **finitely generated** *if there are $g_1, \ldots, g_s \in G$ with*

$$G = \{n_1g_1 + \cdots + n_sg_s \mid n_1, \ldots, n_s \in \mathbb{Z}\}.$$

Proposition 3.14. *The group $(\mathbb{Q}, +)$ is not finitely generated.*

Proof. Let $g_1, \ldots, g_s \in \mathbb{Q}$ and let $D \in \mathbb{N}$ be a common denominator, i.e. $g_i = \frac{a_i}{D}$ with $a_i \in \mathbb{Z}$. Then every integer combination $n_1g_1 + \cdots + n_sg_s = \frac{n_1a_1+\cdots+n_sa_s}{D}$ lies in $\frac{1}{D}\mathbb{Z}$. But $\frac{1}{2D} \notin \frac{1}{D}\mathbb{Z}$. So $g_1, \ldots, g_s$ do not generate $\mathbb{Q}$. □

Since the points of $E(\mathbb{Q})$ have rational coordinates, one might expect $E(\mathbb{Q})$ to behave like $\mathbb{Q}$. The following deep theorem says that this is not the case.

Theorem 3.15 (Mordell, 1922)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated: there are $P_1, \dots, P_s \in E(\mathbb{Q})$ with*

$$E(\mathbb{Q}) = \{n_1 P_1 + \cdots + n_s P_s \mid n_1, \dots, n_s \in \mathbb{Z}\}.$$

We will discuss the proof in Lecture 12. The theorem does not say how to find the generators or how many are needed. For the example $E : y^2 = x^3 - x + 1$, one generator suffices: $E(\mathbb{Q}) = \{n \cdot (1,1) \mid n \in \mathbb{Z}\}$ (this needs an additional computation, done by computer). For the congruent number problem (Section 1.2): n is congruent if and only if $E_n(\mathbb{Q})$ is infinite, i.e. at least one generator of infinite order is needed.

Theorem 3.16 (Hasse, 1933, statement only)**.** *Let E be an elliptic curve over $\mathbb{F}_p$. Then $\big|\,|E(\mathbb{F}_p)| - (p+1)\,\big| \le 2\sqrt{p}$.*

For our curve and $p = 5$: $|8 - 6| = 2 \le 2\sqrt{5} \approx 4.47$.

Remark 3.17 (Cryptography). For an elliptic curve over $\mathbb{F}_p$ with $p \approx 2^{256}$, computing nP from n and P is fast, but recovering n from P and nP is believed to be very hard. This is the basis of elliptic curve cryptography, which is used for example by Bitcoin with the curve $y^2 = x^3 + 7$ (Lecture 6).

References

[Hu] T. W. Hungerford: **Abstract Algebra: An Introduction**, Saunders College Publishing, Philadelphia (1990). ISBN 978-0-03-030558-0.

[LA] H. Bachmann: **Linear Algebra lecture notes**, `https://www.henrikbachmann.com/uploads/7/7/6/3/77634444/linearalgebra_v24.pdf`. Reference for the assumed linear algebra background.

[Mi] J. S. Milne: **Algebraic Geometry**, version 6.10 (2024), `https://www.jmilne.org/math/CourseNotes/AG.pdf`. Section 2m discusses dimension.

[ST] J. H. Silverman, J. Tate: **Rational Points on Elliptic Curves**, 2nd ed., Undergraduate Texts in Mathematics, Springer (2015).