Instructor: Henrik Bachmann
Teaching Assistant: Samyak Parashar

# Homework 1: Groups, Fields & Elliptic Curves

Deadline: 9th November 2026 (23:55 JST) in TACT.
Total points: 20.

*Exercises marked with $\star$ are bonus exercises. Those marked with $\star\star$ are very hard bonus problems. Bonus points are added to your score. The regular total stays at 20 points.*

**Exercise 1.** $(1+1+1+1=4$ Points) Decide whether the following are groups. If yes, give the identity element and the inverse of an element. If not, name an axiom that fails.

(i) $\mathbb{Z}$ with the operation $a * b = a + b - 1$.

(ii) $\mathbb{Q}_{>0}$ with the operation $a * b = \frac{a}{b}$.

(iii) The set of odd integers with $+$.

(iv) The set of matrices $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, $t \in \mathbb{R}$, with matrix multiplication.

**Exercise 2.** $(1+1+1+1+(2^\star)=4$ Points) Rings and fields.

(i) Write down the multiplication table of $\mathbb{Z}/6\mathbb{Z}$ and determine the units $(\mathbb{Z}/6\mathbb{Z})^\times$.

(ii) Let $K$ be a field and $a, b \in K$ with $ab = 0$. Show that $a = 0$ or $b = 0$. Use this to give a second proof that $\mathbb{Z}/6\mathbb{Z}$ is not a field.

(iii) Solve $3x + 5 = 2$ in $\mathbb{F}_7$.

(iv) Find all solutions of $x^2 = -1$ in $\mathbb{F}_5$, $\mathbb{F}_7$ and $\mathbb{F}_{13}$.

(v$^\star$) Find all primes $p < 30$ for which $x^2 = -1$ has a solution in $\mathbb{F}_p$. State a conjecture for all primes $p$.

**Exercise 3.** $(2+2+(2^\star)=4$ Points) Linear algebra over finite fields.

(i) Solve the following system over $\mathbb{F}_3$ with Gaussian elimination:

$$x + y + z = 1, \qquad x + 2y + z = 2, \qquad 2x + y = 0.$$

(ii) Recall $\mathrm{GL}_2(\mathbb{F}_2) = \{A \in \mathrm{M}_2(\mathbb{F}_2) \mid \det(A) \neq 0\}$. Write down all elements of $\mathrm{GL}_2(\mathbb{F}_2)$. How many are there? Show that $\mathrm{GL}_2(\mathbb{F}_2)$ is not abelian.

(iii$^\star$) Let $p$ be a prime. Show that $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$.
(*Hint: A matrix is invertible if and only if its columns are linearly independent.*)

**Exercise 4.** $(1+1+2=4$ Points) Order of elements and generators.

(i) Determine the order of every element of $(\mathbb{Z}/12\mathbb{Z}, +)$ and list all the cyclic subgroups $\langle a \rangle$, $a \in \mathbb{Z}/12\mathbb{Z}$.

(ii) Compute the powers $2, 2^2, \ldots, 2^{12}$ in $\mathbb{F}_{13}^\times$ and show that 2 generates $\mathbb{F}_{13}^\times$. Which other elements of $\mathbb{F}_{13}^\times$ generate $\mathbb{F}_{13}^\times$?

(iii) Let $G$ be a group with $g * g = e$ for all $g \in G$. Show that $G$ is abelian. Give an example of such a group with 8 elements.

**Addition of points on an elliptic curve (for Exercise 5).** Let $K$ be a field with $2, 3 \neq 0$. Let $E : y^2 = x^3 + Ax + B$, where $A, B \in K$ and $4A^3 + 27B^2 \neq 0$. This is the condition $\Delta(E) \neq 0$ from the lecture. Set

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

where $\mathcal{O}$ is an extra point, called the point at infinity. Define $P + \mathcal{O} = \mathcal{O} + P = P$, $-\mathcal{O} = \mathcal{O}$ and $-(x, y) = (x, -y)$. For points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, define their sum as follows:

- If $x_1 = x_2$ and $y_1 = -y_2$, set $P + Q = \mathcal{O}$. This includes $P = Q$ with $y_1 = 0$.
- Otherwise, put

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2, \\ \dfrac{3x_1^2 + A}{2y_1}, & P = Q \text{ and } y_1 \neq 0, \end{cases} \qquad \begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$

  and set $P + Q = (x_3, y_3)$.

You may assume that these rules make $E(K)$ an abelian group, with identity $\mathcal{O}$ and inverses as above. You do not need to prove associativity. We write $2P = P + P$ and $P - Q = P + (-Q)$. All calculations are in $K$. Over $\mathbb{F}_p$, divide by a non-zero element by multiplying by its inverse.

**Exercise 5.** $(1 + 1 + 2 + (3^\star) + (1000^{\star\star}) = 4$ Points) Elliptic curves.

(i) Consider the elliptic curve $E : y^2 = x^3 + 17$ over $\mathbb{Q}$ and the points $P = (-2, 3)$, $Q = (-1, 4)$. Compute $P + Q$ and $P - Q$.

(ii) For the same curve compute $2P$ and $2Q$. What do you notice?

(iii) Consider our guiding curve $E : y^2 = x^3 - x + 1$ over $\mathbb{F}_{11}$. List all points of $E(\mathbb{F}_{11})$, including $\mathcal{O}$. Determine the order of the points $(1, 1)$ and $(3, 5)$.

(iv$^\star$) Recall from Lecture 1 that a right triangle with rational sides $a, b, c$ and area $n$ gives the point $(x, y) = \left(\frac{n(a+c)}{b}, \frac{2n^2(a+c)}{b^2}\right)$ on $E_n : y^2 = x^3 - n^2x$. Conversely, a point $(x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$ gives a triangle with sides

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

Find the point $R \in E_{30}(\mathbb{Q})$ for the triangle $(5, 12, 13)$. Compute $2R$ and use it to find a **new** right triangle with rational sides and area 30.

(v$^{\star\star}$) Show that every positive integer $n \equiv 5, 6, 7 \pmod 8$ is the area of a right triangle with rational sides. Equivalently, show that $E_n : y^2 = x^3 - n^2x$ has a rational point $(x, y)$ with $y \neq 0$.

**Exercise 6.** ($3^\star$ Points) Abelian groups are $\mathbb{Z}$-modules.
Let $(G, +)$ be an abelian group. For $n > 0$ and $g \in G$ define $ng = g + \cdots + g$ ($n$ terms), $0g = 0$ and $(-n)g = -(ng)$.

(i) Show that this makes $G$ a $\mathbb{Z}$-module.

(ii) Show that this is the **only** $\mathbb{Z}$-module structure on $G$ (with the given addition).

(iii) Show that a map $\varphi : G \to H$ between abelian groups satisfies $\varphi(g + h) = \varphi(g) + \varphi(h)$ for all $g, h$ if and only if it is $\mathbb{Z}$-linear. Thus you need to show that an additive map also satisfies $\varphi(ng) = n\varphi(g)$ for all $n \in \mathbb{Z}$.