LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Laurenz Wiesenberger

Tutorial sheet 3
Algebra
Suggested Solutions

Winter term 25/26
November 10, 2025

Exercise 1. (a) Let $C := \{z \in \mathbb{C}^\times \mid |z| = 1\}$. Consider the map

$$\phi\colon \mathbb{R} \to \mathbb{C}^\times, \quad \phi(x) := e^{2\pi i x}.$$

Prove that $\mathbb{R}/\mathbb{Z} \cong C$.

Suggested solution. Consider the map

$$\varphi\colon \mathbb{R} \longrightarrow \mathbb{C}^\times, \qquad x \longmapsto e^{2\pi i x}.$$

Since

$$\varphi(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x}\, e^{2\pi i y} = \varphi(x)\varphi(y),$$

the map φ is a group homomorphism. It is a basic fact (see, for instance, Analysis I) that φ maps $\mathbb{R}$ surjectively onto the unit circle C. Furthermore,

$$\varphi(x) = 1 \quad \Longleftrightarrow \quad e^{2\pi i x} = 1 \quad \Longleftrightarrow \quad x \in \mathbb{Z}.$$

Hence $\ker(\varphi) = \mathbb{Z}$. By the fundamental theorem of homomorphisms, we obtain

$$\mathbb{R}/\mathbb{Z} \;\cong\; C.$$

□

(b) We denote, as usual, by $\zeta_p := \exp(2\pi i/p)$ a primitive p-th root of unity. Consider the map

$$\psi\colon \mathbb{Z} \longrightarrow \mathbb{C}^\times, \qquad \psi(k) := \zeta_p^k.$$

Show that $\mathbb{Z}/p\mathbb{Z} \;\cong\; \{\,1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\,\}$.

Suggested solution. Consider the map

$$\psi\colon \mathbb{Z} \longrightarrow \mathbb{C}^\times, \qquad k \longmapsto \zeta_p^k.$$

Then ψ is a group homomorphism, since

$$\psi(k+k') = \zeta_p^{k+k'} = \zeta_p^k \zeta_p^{k'} = \psi(k)\psi(k').$$

Now let $k \in \mathbb{Z}$ be arbitrary. By the division algorithm, there exist unique integers $m, r \in \mathbb{Z}$ such that $x = mp + r$ with $0 \le r < p$. Then

$$\psi(k) = \zeta_p^{mp+r} = (\zeta_p^p)^m \zeta_p^r = \zeta_p^r.$$

Hence ψ maps $\mathbb{Z}$ surjectively onto the subgroup

$$\langle \zeta_p \rangle = \{\, \zeta_p^r \mid 0 \leq r < p \,\} \subseteq \mathbb{C}^\times.$$

Furthermore,

$$\psi(k) = 1 \quad \Longleftrightarrow \quad \zeta_p^k = 1 \quad \Longleftrightarrow \quad p \mid k.$$

Thus $\ker(\psi) = p\mathbb{Z}$.

By the fundamental theorem of homomorphisms, we obtain an isomorphism

$$\mathbb{Z}/p\mathbb{Z} \;\cong\; \langle \zeta_p \rangle.$$

Alternative argument. $\langle \zeta_p \rangle$ is a cyclic group of order p. By Exercise sheet 1, Exercise 1, $\mathbb{Z}/p\mathbb{Z} \cong \langle \zeta_p \rangle$.

□

(c) Let k be a field. Consider the map

$$\det\colon \mathrm{GL}_n(k) \to k^\times.$$

Show that $\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \cong k^\times$.

Suggested solution. Consider the map

$$\det\colon\ \mathrm{GL}_n(k) \longrightarrow k^\times, \qquad A \longmapsto \det(A).$$

Since the determinant is multiplicative, this is a group homomorphism.

To see that det is surjective, note that for any $x \in k^\times$, the matrix

$$A = (a_{ij}) \quad \text{with} \quad a_{11} = x,\ a_{ii} = 1 \text{ for } i \geq 2, \text{ and } a_{ij} = 0 \text{ for } i \neq j,$$

belongs to $\mathrm{GL}_n(k)$ and satisfies $\det(A) = x$.

By definition,

$$A \in \ker(\det) \quad \Longleftrightarrow \quad \det(A) = 1,$$

so the kernel of the determinant map is precisely

$$\mathrm{SL}_n(k) = \{\, A \in \mathrm{GL}_n(k) \mid \det(A) = 1 \,\}.$$

Hence, by the fundamental theorem of homomorphisms, we obtain

$$\mathrm{GL}_n(k)/\,\mathrm{SL}_n(k) \;\cong\; k^\times.$$

□

Exercise 2. (a) Let $f\colon G \to H$ be a homomorphism of finite groups such that $|G|$ and $|H|$ are coprime. Show that f is trivial, i.e. $\mathrm{im}(f) = \{e_H\}$.

Suggested solution. Let $f\colon G \to H$ be a group homomorphism between finite groups and assume $\gcd(|G|, |H|) = 1$. By the fundamental theorem of homomorphisms we have

$$G/\ker(f) \;\cong\; \operatorname{im}(f),$$

hence

$$|\operatorname{im}(f)| \;=\; [G : \ker(f)]$$

By Lagrange's theorem the subgroup $\operatorname{im}(\varphi) \leq H$ satisfies $|\operatorname{im}(\varphi)| \mid |H|$, and the index $[G : \ker(f)] \mid |G|$. Therefore

$$|\operatorname{im}(f)| \mid \gcd(|G|, |H|) = 1.$$

Consequently $|\operatorname{im}(f)| = 1$, i.e. $\operatorname{im}(f) = \{e_H\}$ is trivial.

Note: This generalizes the statement of Tutorial Sheet 1, Exercise 2(c).

□

(b) Let G be a finite group and let $N \trianglelefteq G$ be a normal subgroup. Show that if $n := |N|$ and $|G/N|$ are coprime, then N is the only subgroup of G of order n.

Suggested solution. Let $U \trianglelefteq G$ be a normal subgroup of order n and consider the composition

$$U \hookrightarrow G \xrightarrow{\pi} G/N.$$

By part (a), this homomorphism is trivial. Hence $U \subseteq N$ and as $|U| = |N|$ we have equality.

□

Please don't worry about Exercise 3. In the tutorial, we will mainly focus on Exercises 1 and 2. If time permits, I will also explain Exercise 3 to help you to gain a better understanding of Exercise 4 from Exercise Sheet 2.

Exercise 3. In this exercise, we become familiar with *(integral) group rings*.
Let $\mathbb{Z}$ be the ring of integers and G a group. The *(integral) group ring* $\mathbb{Z}[G]$ is the set of all finite formal linear combinations

$$\sum_{g \in G} a_g g, \quad a_g \in \mathbb{Z},$$

i.e. $a_g = 0$ for all but finitely many $g \in G$ (*note that this is the same definition as given in Exercise Sheet 2*).
The set $\mathbb{Z}[G]$ becomes a ring with the operations

$$+_{\mathbb{Z}[G]}\colon \mathbb{Z}[G] \times \mathbb{Z}[G] \to \mathbb{Z}[G], \quad \sum_{g \in G} a_g g \;+_{\mathbb{Z}[G]}\; \sum_{g \in G} b_g g := \sum_{g \in G} (a_g +_{\mathbb{Z}} b_g) g,$$

$$\cdot_{\mathbb{Z}[G]}\colon \mathbb{Z}[G] \times \mathbb{Z}[G] \to \mathbb{Z}[G], \quad \sum_{g \in G} a_g g \;\cdot_{\mathbb{Z}[G]}\; \sum_{g \in G} b_g g := \sum_{g \in G} c_g g,$$

where

$$c_g := \sum_{\substack{g_1,g_2\in G\\ g_1\cdot_G g_2=g}} a_{g_1}\cdot_{\mathbb{Z}} b_{g_2}.$$

The additive identity in $\mathbb{Z}[G]$ is the formal linear combination in which all coefficients a_g are zero, and the multiplicative identity is given by $1_{\mathbb{Z}[G]} = 1_{\mathbb{Z}} \cdot e_G$.
Note that there is no need to restrict ourselves to $\mathbb{Z}$; we can define the group ring $R[G]$ in an analogous way for any commutative ring R.

(a) Let G be the cyclic group of order 3, say $G = \{e_G, g, g^2\}$. Write down some elements in the ring $\mathbb{Z}[G]$ and compute:

$$(5 + 2g + 7g^2) +_{\mathbb{Z}[G]} (3 + 4g - 479g^2),$$
$$(4 + 3g) \cdot_{\mathbb{Z}[G]} (11 + 4g + 15g^2).$$

Suggested solution.

$$\begin{aligned}(5 + 2g + 7g^2) + (3 + 4g - 479g^2) &= (5 + 3) + (2 + 4)g + (7 - 479)g^2\\ &= 8 + 6g - 472g^2.\end{aligned}$$

Next, we compute:

$$\begin{aligned}(4 + 3g)(11 + 4g + 15g^2) &= (44 + 45) + (16 + 33)g + (60 + 12)g^2\\ &= 89 + 49g + 72g^2.\end{aligned}$$

□

(b) Show that $\mathbb{Z}[G]$ is a commutative ring if and only if G is abelian. It suffices to prove that multiplication in $\mathbb{Z}[G]$ is commutative if and only if G is abelian.

Suggested solution. "⇒" Let $\mathbb{Z}[G]$ be a commutative ring and let $g, h \in G$ be arbitrary elements. Then we have

$$gh = g \cdot_{\mathbb{Z}[G]} h = h \cdot_{\mathbb{Z}[G]} g = hg.$$

Thus G is an abelian group.

"⇐" For the converse, let G be an abelian group. Then for

$$a = \sum_{g\in G} a_g g \quad \text{and} \quad b = \sum_{g\in G} b_g g,$$

we have

$$ab = \sum_{g\in G} c_g g, \qquad c_g = \sum_{\substack{g_1,g_2\in G\\ g_1 g_2=g}} a_{g_1} b_{g_2}.$$

Since G is abelian, the condition $g_1 g_2 = g$ is equivalent to $g_2 g_1 = g$, and hence

$$c_g = \sum_{\substack{g_1, g_2 \in G \\ g_2 g_1 = g}} b_{g_2} a_{g_1}.$$

Therefore,

$$ab = ba.$$

Thus $\mathbb{Z}[G]$ is commutative. □

From now on, we will use some basic concepts from ring theory, such as ideals or the fundamental theorem on homomorphisms. If you are already familiar with these notions, the following exercises are a good opportunity to practise working with group rings. If not, there is no need to worry, these concepts will be covered in detail later in the lecture, and we can return to these exercises once they have been discussed. You may also view them as optional "fun exercises" for those who already know this material.

(c) Let G be the cyclic group of order m. Show that

$$\mathbb{C}[G] \cong \mathbb{C}[X]/(X^m - 1).$$

Hint: Consider the homomorphism $\mathbb{C}[X] \to \mathbb{C}[G]$, $\quad \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} a_i g^i$.

Suggested solution. Let g be a generator of G, i.e. $\langle g \rangle = G$. Consider the map

$$\psi \colon \mathbb{C}[X] \longrightarrow \mathbb{C}[G], \qquad \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} a_i g^i.$$

By the definition of addition and multiplication in $\mathbb{C}[G]$, the map ψ is a ring homomorphism. Furthermore, ψ is surjective by the definition of $\mathbb{C}[G]$.

Hence it suffices to determine $\ker(\psi)$. Since $\mathbb{C}[X]$ is a principal ideal domain (PID), the kernel $\ker(\psi)$ is generated by a single polynomial f of minimal (non-negative) degree such that $\psi(f) = 0$. Because $\operatorname{ord}(g) = m$, where m is the smallest natural number satisfying $g^m = e_G$, we obtain $f = X^m - 1$. Therefore, the kernel of ψ is

$$\ker(\psi) = (X^m - 1).$$

By the homomorphism theorem (for rings), we obtain $\mathbb{C}[G] \cong \mathbb{C}[X]/(X^m - 1)$.

□

(d) Let G be the cyclic group of order 2. Show that

$$\mathbb{C}[G] \cong \mathbb{C} \times \mathbb{C}.$$

Hint: You may use the Chinese Remainder Theorem.

Suggested solution. By part (c), we have

$$\mathbb{C}[G] \cong \mathbb{C}[X]/(X^2-1) = \mathbb{C}[X]/(X+1)(X-1).$$

Applying the *Chinese Remainder Theorem*, we obtain

$$\mathbb{C}[X]/(X^2-1) \;\cong\; \mathbb{C}[X]/(X+1) \times \mathbb{C}[X]/(X-1) \;\cong\; \mathbb{C} \times \mathbb{C}.$$

Here we use that

$$\mathbb{C}[X]/(X+1) \cong \mathbb{C} \quad \text{and} \quad \mathbb{C}[X]/(X-1) \cong \mathbb{C}.$$

□

(e) Let R be a (not necessarily commutative) ring and $f\colon R \to S$ a ring homomorphism. Show that $\ker(f) \subseteq R$ is a two-sided ideal.

Hence, we can conclude that the kernel of the *augmentation map*

$$\varepsilon\colon \mathbb{Z}[G] \to \mathbb{Z}, \quad \sum_{g\in G} a_g g \longmapsto \sum_{g\in G} a_g,$$

which we denote by $I(G)$, is a two-sided ideal. We call $I(G)$ the *augmentation ideal*.

Suggested solution. Let $r_1, r_2 \in R$ be arbitrary elements and $x \in \ker(\varphi)$. Then we have

$$\varphi(r_1 x r_2) = \varphi(r_1)\,\varphi(x)\,\varphi(r_2) = \varphi(r_1)\,0\,\varphi(r_2) = 0.$$

Thus $r_1 x r_2 \in \ker(\varphi)$, and therefore $\ker(\varphi)$ is a two-sided ideal of R.

□