Prof. Dr. Fabien Morel
Laurenz Wiesenberger

Exercise sheet 2
Algebra
Suggested Solutions

Winter term 25/26

Exercise 1. Let $n \geq 3$ be an integer. Show that the center $Z(S_n)$ of the n-th symmetric group is trivial.

Suggested solution. Recall that $Z(S_n) = \{ \sigma \in S_n \mid \forall \tau \in S_n : \tau\sigma = \sigma\tau \}$. Let $\sigma \in S_n$ be a nontrivial element. Then there exists $i \in \{1, \ldots, n\}$ such that $\sigma(i) \neq i$. Since $n \geq 3$, we can choose another element $j \in \{1, \ldots, n\}$ with $j \neq i$ and $j \neq \sigma(i)$.

Now consider the transposition $\tau = (\sigma(i)\, j) \in S_n$. We compute:

$$(\tau\sigma)(i) = \tau(\sigma(i)) = j,$$

whereas

$$(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i).$$

Since $j \neq \sigma(i)$, we have $\tau\sigma \neq \sigma\tau$. Hence, the only element commuting with all others is the identity, and therefore the center of S_n is trivial, i.e. $Z(S_n) = \{\mathrm{id}\}$.

□

Exercise 2. Let $n \geq 1$ be an integer, and let $\mathbb{F}$ be a finite field with $q = |\mathbb{F}|$ elements. Prove that $\mathrm{GL}_n(\mathbb{F})$ is a finite group of order

$$(q^n - 1) \times (q^n - q) \times \cdots \times (q^n - q^{n-1}) \;=\; \prod_{i=0}^{n-1} \big(q^n - q^i\big).$$

Compute the index of $\mathrm{SL}_n(\mathbb{F})$ in $\mathrm{GL}_n(\mathbb{F})$ and conclude that the order of $\mathrm{SL}_n(\mathbb{F})$ is

$$\frac{1}{q-1} \prod_{i=0}^{n-1} \big(q^n - q^i\big) \;=\; \big(q^{n-1} + q^{n-2} + \cdots + q + 1\big) \prod_{i=1}^{n-1} \big(q^n - q^i\big).$$

Suggested solution. This argument is based on a basic fact from linear algebra: Since there is a one-to-one correspondence between automorphisms $\mathbb{F}^n \to \mathbb{F}^n$ and invertible matrices $A \in \mathrm{GL}_n(\mathbb{F})$, it suffices to determine the number of different bases of $\mathbb{F}^n$.

Let us now compute the number of possible bases. For the first basis vector v_1, we may choose any nonzero vector in $\mathbb{F}^n$; thus, there are $q^n - 1$ possibilities. For the second basis vector v_2, we may choose any vector $v_2 \in \mathbb{F}^n \setminus \langle v_1 \rangle$, so there are $q^n - q$ options. Similarly, for the third basis vector v_3, we may choose $v_3 \in \mathbb{F}^n \setminus \langle v_1, v_2 \rangle$, which gives $q^n - q^2$ possibilities. Continuing in the same way, for the final vector v_n we must have $v_n \in \mathbb{F}^n \setminus \langle v_1, \ldots, v_{n-1} \rangle$, and hence there are $q^n - q^{n-1}$ possible choices. Therefore, we obtain exactly the formula given in the exercise.

From Tutorial Sheet 3, Exercise 1(c), we know that $\mathrm{GL}_n(\mathbb{F})/\mathrm{SL}_n(\mathbb{F}) \cong \mathbb{F}^\times$, and hence

$$|\mathrm{GL}_n(\mathbb{F}) : \mathrm{SL}_n(\mathbb{F})| = |\mathbb{F}^\times| = q - 1.$$

By Lagrange's theorem, we therefore conclude that

$$|\mathrm{SL}_n(\mathbb{F})| = \frac{|\mathrm{GL}_n(\mathbb{F})|}{q-1}.$$

This is precisely the formula stated in the exercise.

□

Exercise 3. Let $n \geq 5$ be an integer. Show that in A_n, a 3-cycle is a commutateur. Conclude that for $n \geq 5$,

$$[A_n, A_n] = A_n.$$

Deduce that for $n \geq 5$ the group A_n is not solvable, and consequently S_n is not solvable either.

Suggested solution. Recall (for instance from linear algebra) that A_n consists precisely of finite products of 3-cycles. So it suffices to show that every 3-cycle is a commutator in A_n.
Let (x_1, x_2, x_3) be a 3-cycle. Since $n \geq 5$, there are distinct x_4, x_5. Hence we can write

$$\begin{aligned}(x_1, x_2, x_3) &= (x_1, x_2, x_4)(x_1, x_3, x_5)(x_1, x_4, x_2)(x_1, x_5, x_3)\\ &= (x_1, x_2, x_4)(x_1, x_3, x_5)(x_1, x_2, x_4)^{-1}(x_1, x_3, x_5)^{-1}\\ &= \big[(x_1, x_2, x_4),\ (x_1, x_3, x_5)\big].\end{aligned}$$

Thus $(x_1, x_2, x_3) \in [A_n, A_n]$ and therefore $A_n = [A_n, A_n]$.
We can now easily deduce that A_n is not solvable for $n \geq 5$. Indeed, by definition A_n is solvable if there exists $k \in \mathbb{N}$ such that $D^{(k)}(A_n) = *$. But since $D^{(k)}(A_n) = A_n$, no such k can exist. Hence A_n is not solvable for $n \geq 5$.
In Tutorial Sheet 2, Exercise 3, we showed that $[S_n, S_n] = A_n$ (already true for $n \geq 2$). Therefore, for $n \geq 5$ we have $D^{(k)}(S_n) = A_n \neq *$, and thus S_n is not solvable.

□

Exercise 4. Let G be a group, and $\mathbb{Z}[G]$ be the group ring of G: it is the free abelian group with basis $([g])_{g \in G}$, where $[g] \in \mathbb{Z}[G]$, and the product is induced by the bilinear map

$$\mathbb{Z}[G] \times \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G], \quad ([g], [h]) \longmapsto [g \cdot h].$$

We denote by $[e]$ the element $1 \in \mathbb{Z}[G]$, with $e \in G$ the neutral element; observe indeed that $[e]$ is the neutral element for the product in $\mathbb{Z}[G]$. The canonical homomorphism

$$\varepsilon \colon \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \quad [g] \longmapsto 1,$$

is a ring homomorphism called the *augmentation*. The kernel $I(G)$ is a two-sided ideal in $\mathbb{Z}[G]$. We denote by $I(G)^2$ the two-sided ideal product of $I(G)$ with itself. Clearly $I(G)^2 \subseteq I(G)$.

1) Show that $I(G)$, as an abelian group, is the free abelian group with basis $([g] - [e])_{g \in G \setminus \{e\}}$, with $e \in G$ the neutral element. Conclude that $I(G)^2$, as an abelian group, is generated by the family

$$([g \cdot h] - [g] - [h] + 1)_{(g,h) \in (G \setminus \{e\})^2}.$$

Suggested solution. Consider the augmentation map

$$\varepsilon \colon \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \qquad \sum_{g \in G} a_g[g] \longmapsto \sum_{g \in G} a_g.$$

From Tutorial Sheet 3 we know that $I(G) = \ker(\varepsilon)$ is a two-sided ideal in $\mathbb{Z}[G]$. Explicitly,

$$I(G) = \left\{ \sum_{g \in G} a_g[g] \;\middle|\; \sum_{g \in G} a_g = 0 \right\}.$$

We show that $I(G)$ is a free abelian group with $\mathbb{Z}$-basis $[g] - [e]$ for all $g \in G \setminus \{e\}$.

First, these elements lie indeed in the kernel:

$$\varepsilon([g] - [e]) = 1 - 1 = 0.$$

Hence $[g] - [e] \in I(G)$ for all $g \in G$. Thus, the ideal generated by these elements is contained in $I(G)$:

$$\langle [g] - [e] \mid g \in G \setminus \{e\} \rangle \subseteq I(G).$$

In particular, $\langle [g] - [e] \mid g \in G \setminus \{e\} \rangle_{\mathbb{Z}} \subseteq I(G)$. For the converse, let $\sum_{g \in G} a_g[g] \in I(G)$, so that $\sum_{g \in G} a_g = 0$. Then we have

$$\sum_{g \in G} a_g[g] = \sum_{g \in G \setminus \{e\}} a_g[g] + a_e[e].$$

Since $\sum_{g \in G} a_g = 0$, it follows that

$$a_e = - \sum_{g \in G \setminus \{e\}} a_g,$$

and therefore

$$\sum_{g \in G} a_g[g] = \sum_{g \in G \setminus \{e\}} a_g([g] - [e]).$$

Hence we deduce

$$I(G) = \langle [g] - [e] \mid g \in G \setminus \{e\} \rangle_{\mathbb{Z}}.$$

So it remains to show that $\big([g] - [e]\big)_{g \in G \setminus \{e\}}$ is linearly independent over $\mathbb{Z}$. Let

$$0 = \sum_{g \in G \setminus \{e\}} a_g\big([g] - [e]\big).$$

Then

$$\sum_{g \in G \setminus \{e\}} a_g[g] \;-\; \Big(\sum_{g \in G \setminus \{e\}} a_g \Big)[e] \;=\; 0.$$

Since $\big([g]\big)_{g\in G}$ is a basis of the free abelian group $\mathbb{Z}[G]$, all coefficients must vanish. Hence all $a_g = 0$, and $\big([g]-[e]\big)_{g\in G\setminus\{e\}}$ is a $\mathbb{Z}$-basis of $I(G)$. This means that $I(G)$ is a free $\mathbb{Z}$-module, a notion we will learn about later in the lecture.

Let us now recall the definition of the product of ideals. Let R be a ring and $\mathfrak{a}, \mathfrak{b}$ be two (two-sided) ideals in R. Then the product $\mathfrak{ab}$ is again a (two-sided) ideal, defined by

$$\mathfrak{ab} := \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n \in \mathbb{N},\, a_i \in \mathfrak{a},\, b_i \in \mathfrak{b} \right\}.$$

By this definition, the square of the augmentation ideal is given by

$$I(G)^2 = \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i, b_i \in I(G),\, n \in \mathbb{N} \right\}.$$

Now choose $n = 1$, $a_1 = [g]-[e]$, and $b_1 = [h]-[e]$ for $g, h \in G\setminus\{e\}$. Then

$$a_1 b_1 = ([g]-[e])([h]-[e]) = [gh]-[g]-[h]+[e] \in I(G)^2.$$

Hence the ideal generated by the elements $[gh]-[g]-[h]+[e] \mid g,h \in G\setminus\{e\}$ is contained in $I(G)^2$; in particular, the $\mathbb{Z}$-submodule generated by these elements is contained in $I(G)^2$.

The converse inclusion follows immediately since $I(G)$ is generated over $\mathbb{Z}$ by the elements $[g]-[e]$ for $g \in G\setminus\{e\}$. More precisely, it suffices to show that for any $a, b \in I(G)$, the product ab is a linear combination of such elements. So let

$$a = \sum_{i=1}^{n} a_i([g_i]-[e]), \quad b = \sum_{j=1}^{m} b_j([h_j]-[e]), \quad a_i, b_j \in \mathbb{Z}.$$

Then

$$ab = \sum_{i=1}^{n} a_i([g_i]-[e]) \sum_{j=1}^{m} b_j([h_j]-[e]) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j([g_i h_j]-[g_i]-[h_j]+[e]),$$

which shows that

$$ab \in \langle [gh]-[g]-[h]+[e] \mid g,h \in G\setminus\{e\}\rangle_{\mathbb{Z}}.$$

Hence we conclude that

$$I(G)^2 = \langle [gh]-[g]-[h]+[e] \mid g,h \in G\setminus\{e\}\rangle_{\mathbb{Z}}.$$

□

2) (*) Let G_{ab} be the abelianisation of G. Show that the morphism of abelian groups

$$I(G) \longrightarrow G_{\mathrm{ab}}, \quad [g]-1 \longmapsto \overline{g},$$

where $\overline{g}$ is the class of g in $G_{\mathrm{ab}} = G/[G,G]$, is trivial on $I(G)^2$ and induces an isomorphism of abelian groups

$$I(G)/I(G)^2 \cong G_{\mathrm{ab}}.$$

[Hint: define a group homomorphism $G_{\mathrm{ab}} \to I(G)/I(G)^2$ *which is inverse...]*

Suggested solution. Recall that every abelian group is a $\mathbb{Z}$-module. By Exercise 4, 1), the elements $\{[g]-[e] \mid g \in G \setminus \{e\}\}$ form a $\mathbb{Z}$-basis of $I(G)$, and hence the map

$$\varphi\colon I(G) \longrightarrow G_{\mathrm{ab}}, \qquad [g]-[e] \longmapsto \overline{g}$$

is a well-defined $\mathbb{Z}$-linear map. In particular, φ is a morphism of abelian groups. First we show that $I(G)^2 \subseteq \ker(\varphi)$. Then, by the fundamental theorem of homomorphisms, we obtain a morphism

$$\overline{\varphi}\colon I(G)/I(G)^2 \longrightarrow G_{\mathrm{ab}}, \qquad \overline{[g]-[e]} \longmapsto \overline{g}.$$

Since $\ker(\varphi)$ is a submodule, it suffices to show that the generators of $I(G)^2$ lie in $\ker(\varphi)$. So let $g,h \in G \setminus \{e\}$ be given. Then

$$\varphi([gh]-[g]-[h]+[e]) = \overline{ghg^{-1}h^{-1}} = 0.$$

Thus $[gh]-[g]-[h]+[e] \in \ker(\varphi)$, and therefore $I(G)^2 \subseteq \ker(\varphi)$.

Now consider the morphism

$$\psi\colon G \longrightarrow I(G)/I(G)^2, \qquad g \longmapsto \overline{[g]-[e]}.$$

First note that this is indeed a group homomorphism:

$$\psi(gh) = \overline{[gh]-[e]} = \overline{[g]-[e]+[h]-[e]} = \psi(g)+\psi(h).$$

Since $[G,G]$ is the smallest normal subgroup, such that the quotient is abelian, we immediately obtain $[G,G] \subseteq \ker(\psi)$. Again the fundamental theorem of homomorphism, yields an induced map

$$\overline{\psi}\colon G_{\mathrm{ab}} \longrightarrow I(G)/I(G)^2, \qquad \overline{g} \longmapsto \overline{[g]-[e]}.$$

Obviously, $\overline{\psi}$ and $\overline{\varphi}$ are inverse to each other, and hence we obtain an isomorphism

$$I(G)/I(G)^2 \;\cong\; G_{\mathrm{ab}}.$$

□