Prof. Dr. Fabien Morel
Laurenz Wiesenberger

Tutorial sheet 4
Algebra
Suggested Solutions

Winter term 25/26
November 17, 2025

Exercise 1. Let X be a G-set and $Y \subseteq X$ be a subset. Then

$$Y \text{ is } G\text{-invariant} \iff Y \text{ is a disjoint union of orbits.}$$

Suggested solution. "$\Rightarrow$" Let Y be G-invariant. For any $y \in Y$, consider the orbit $G \cdot y$. Since Y is G-invariant, we have $G \cdot y \subseteq Y$. In particular,

$$\bigcup_{y \in Y} G \cdot y = Y.$$

Now consider the distinct orbits; then

$$\bigsqcup G \cdot y = Y,$$

and hence Y is a disjoint union of orbits.

Alternative argument. As Y is G-invariant, it follows from the lecture that Y is a G-set, and hence a disjoint union of orbits.

"$\Leftarrow$" For the converse, let Y be a disjoint union of orbits. We know from the lecture that orbits are G-invariant, and by the definition of G-invariance, it is straightforward to check that arbitrary unions of G-invariant sets are again G-invariant. Thus Y is G-invariant.

$\square$

Exercise 2. Let G be a finite group acting on itself by conjugation, i.e.

$$G \times G \longrightarrow G, \quad (g, x) \longmapsto gxg^{-1}.$$

(a) The corresponding orbit decomposition yields the *class equation*:

$$|G| = |Z(G)| + \sum_{|G \cdot x| > 1} |G \cdot x|,$$

where $Z(G)$ denotes the center of G, and the sum runs over the disjoint, non-trivial orbits $G \cdot x$.

Suggested solution. From the lecture, we know that

$$G = \bigsqcup G \cdot x$$

for the distinct orbits, and hence

$$|G| = \sum |G \cdot x|,$$

where the sum runs over all disjoint orbits.

Now consider the orbits of cardinality 1. Then we have

$$|G \cdot x| = 1 \iff G \cdot x = \{x\} \iff gxg^{-1} = x \text{ for all } g \in G \iff x \in Z(G).$$

Therefore,

$$Z(G) = \bigsqcup_{|G\cdot x|=1} G \cdot x,$$

that is, the union of all disjoint orbits of cardinality 1. Hence,

$$|G| = |Z(G)| + \sum_{|G\cdot x|>1} |G \cdot x|.$$

$\square$

(b) Let G be a group such that $|G| = p^r$ for some prime number p and $r \geq 1$. Show that $Z(G)$ is non-trivial.

Suggested solution. Let $|G| = p^r$ for some prime number p and integer $r \geq 1$. We may assume, without loss of generality, that $Z(G) \subsetneq G$. So let $x \in G \setminus Z(G)$. Then, by part (a), we have $|G \cdot x| > 1$, and by the Orbit–Stabilizer Theorem,

$$|G \cdot x| = [G : I_x].$$

Hence, by Lagrange's Theorem, $|G \cdot x|$ divides $|G|$, and therefore

$$|G \cdot x| = p^{r_x} \quad \text{for some } 1 \leq r_x \leq r.$$

In particular, p divides $|G \cdot x|$ for all $x \in G \setminus Z(G)$. Since p divides $|G|$, the class equation yields

$$p \mid \Big(|Z(G)| + \sum_{|G\cdot x|>1} |G \cdot x|\Big).$$

As p divides each $|G \cdot x|$ in the sum and $p \mid |G|$, it follows that

$$p \mid |Z(G)|.$$

Consequently, $|Z(G)| \neq 1$.

$\square$

(c) Let G be a group such that $|G| = p^2$. Show that G is abelian.

Note: You already proved this result in Exercise Sheet 3.

Suggested solution. It is well known from the lecture that $Z(G) \leq G$ is a subgroup. By Lagrange's Theorem and part (b), we have $|Z(G)| = p^2$ or $|Z(G)| = p$.

In the first case, $Z(G) = G$, and hence G is abelian. Now consider the second case and let $x \in G \setminus Z(G)$. Then, by definition, $Z(G) \subsetneq I_x$ (since $Z(G) \subseteq I_x$, $x \in I_x$, but $x \notin Z(G)$). As $I_x \leq G$ is a subgroup, Lagrange's Theorem gives

$$|I_x| = p \quad \text{or} \quad |I_x| = p^2.$$

Since $Z(G) \subsetneq I_x \leq G$, it follows that $|I_x| = p^2$, and therefore $I_x = G$. This, however, means that x commutes with every element of G, i.e. $x \in Z(G)$, which is a contradiction. Hence, we conclude that $|Z(G)| = p^2$, that is, $Z(G) = G$.

□

Exercise 3 (Burnside's Lemma)**.** (a) Let G be a finite group acting on a finite set X. For each $g \in G$, let

$$X^g := \{ x \in X \mid g \cdot x = x \}$$

denote the set of elements fixed by g. Show that the number of orbits of G on X is given by

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Suggested solution. This exercise requires a few additional ideas, which is why we discussed it together in the tutorial. First, one should notice that there is a certain similarity between the sets X^g and the subgroups I_x. The set X^g consists of all $x \in X$ that are fixed under the group element g, while I_x denotes the set of all $g \in G$ such that x is fixed under the action of g. This observation suggests considering the disjoint union (the coproduct in the category of sets) to express their similarity. We obtain a bijection

$$\coprod_{g \in G} X^g \;\cong\; \coprod_{x \in X} I_x.$$

This allows us to conclude that

$$\sum_{g \in G} |X^g| \;=\; \sum_{x \in X} |I_x|.$$

We can proceed with the next step. By the Orbit–Stabilizer Theorem, we know that

$$|G \cdot x| \;=\; \frac{|G|}{|I_x|},$$

and hence

$$|I_x| \;=\; \frac{|G|}{|G \cdot x|}.$$

Therefore,

$$\sum_{x \in X} |I_x| \;=\; |G| \sum_{x \in X} \frac{1}{|G \cdot x|}.$$

The next step is to split the sum into separate parts corresponding to the distinct orbits. We can write

$$\sum_{x\in X} \frac{1}{|G\cdot x|} \;=\; \sum_{S\in G/X} \sum_{x\in S} \frac{1}{|S|} \;=\; \sum_{S\in G/X} 1 \;=\; |X/G|.$$

Hence,

$$\sum_{g\in G} |X^g| \;=\; |G|\,|X/G|.$$

□

(b) In this exercise, we determine the number of distinct colorings of the vertices of a square using two colors (e.g. blue and green), up to rotation.

Let r denote the rotation of the square by 90° counterclockwise. Label the vertices in counterclockwise order by $1, 2, 3, 4$. This rotation can be represented by the 4-cycle

$$r = (1\ 2\ 3\ 4) \in S_4.$$

Hence, the cyclic group

$$G = \langle r \rangle = \{e, r, r^2, r^3\}$$

acts on the set

$$X = \{0, 1\}^4,$$

which represents all possible colorings of the four vertices of the square with two colors (encoded by 0 and 1). The action is defined by

$$r \cdot (x_1, x_2, x_3, x_4) = (x_4, x_1, x_2, x_3),$$

and extended to all of $G = \{e, r, r^2, r^3\}$ by iteration. Use Burnside's Lemma to compute the number of distinct colorings up to rotation.

Suggested solution. First, observe that $|X/G|$ is precisely the number of distinct colorings of the vertices of a square using two colors, counted up to rotation. By Burnside's Lemma,

$$|X/G| = \frac{1}{|G|} \sum_{g\in G} |X^g|.$$

Hence, it suffices to determine $|X^g|$ for each $g \in G$.

To determine X^g, it may be helpful to draw some pictures (that is what the exercise is about, drawing pictures).

If $g = e = r^0$, every vertex remains fixed, and there are 2^4 possible colorings: for each of the four vertices, one can independently choose between blue or green. Thus, $|X^e| = 16$.

If we act with r on X, this corresponds to a rotation of 90° counterclockwise. For (x_1, x_2, x_3, x_4) to satisfy $r \cdot (x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4)$, we must have

$$x_1 = x_2 = x_3 = x_4.$$

Hence, there are only two possible colorings: all blue or all green. Therefore, $|X^r| = 2$.

If we act with r^2, this corresponds to a rotation by 180° counterclockwise. In this case,

$$r^2 \cdot (x_1, x_2, x_3, x_4) = (x_3, x_4, x_1, x_2),$$

and the equality $r^2 \cdot (x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4)$ implies

$$x_1 = x_3, \quad x_2 = x_4.$$

Thus, there are four possible colorings, and we obtain $|X^{r^2}| = 4$.

If we act with r^3, we rotate the square by 270° counterclockwise. Here,

$$r^3 \cdot (x_1, x_2, x_3, x_4) = (x_2, x_3, x_4, x_1),$$

and the condition $r^3 \cdot (x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4)$ again forces

$$x_1 = x_2 = x_3 = x_4,$$

so there are two possible colorings. Hence, $|X^{r^3}| = 2$.

Finally, by Burnside's Lemma, we conclude:

$$|X/G| = \frac{1}{4}(16 + 2 + 4 + 2) = 6.$$

$\square$