LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Laurenz Wiesenberger

REPETITION WEEK 5
ALGEBRA

Winter term 25/26

Before we start with the actual content, let me mention two preliminary notational remarks. In last week's repetition sheet I used the notation X^G for the set of all fixed points. Since we are consistently working with left actions, I should have written ${}^G X$, as you did in the lecture.

Similarly, for the quotient I wrote X/G, but in the context of left actions the correct notation would have been $G\backslash X$.

Sorry for the inconsistency.

More about Group Action on a Set

Lemma. Let X be a G-set and let $(x, y) \in X^2$ be two elements in the same orbit of the action. Then $I_x, I_y \leq G$ are conjugate groups.

You will prove this in exercise sheet 4, exercise 1.

For a G-set X, we have the following decomposition:

$$X = {}^G X \sqcup \left(\bigsqcup_{\substack{\alpha \in G\backslash X \\ |\alpha| \geq 2}} \alpha \right).$$

To see this, note that

$$|G \cdot x| = 1 \iff g \cdot x = x \text{ for all } g \in G \iff x \in {}^G X.$$

Let $n \geq 1$ and $\sigma \in S_n$. Consider the cyclic group $\langle \sigma \rangle \leq S_n$ generated by σ. As S_n acts on $\{1, \ldots, n\}$ (see last repetition sheet), $\langle \sigma \rangle$ acts as well on $\{1, \ldots, n\}$:

$$\langle \sigma \rangle \times \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}, \qquad (\sigma^s, i) \longmapsto \sigma^s(i),$$

where $s \in \{1, \ldots, r\}$ and $r = \operatorname{ord}(\sigma)$.

We analyse the decomposition into orbits:

$$\{1, \ldots, n\} = \bigsqcup_{\alpha \in \langle \sigma \rangle \backslash \{1, \ldots, n\}} \alpha = {}^{\langle \sigma \rangle}\{1, \ldots, n\} \sqcup \left(\bigsqcup_{\substack{\alpha \in \langle \sigma \rangle \backslash \{1, \ldots, n\} \\ |\alpha| \geq 2}} \alpha \right).$$

Note that

$$^{\langle\sigma\rangle}\{1,\dots,n\} = \{\, i \in \{1,\dots,n\} \mid \sigma(i) = i \,\}.$$

In this case we have

$$^{\langle\sigma\rangle}\{1,\dots,n\} = {}^{\sigma}\{1,\dots,n\}.$$

We set

$$\operatorname{supp}(\sigma) := \{1,\dots,n\} \setminus {}^{\sigma}\{1,\dots,n\}$$

and call it the support of σ.

We now want to characterize the orbits of σ with cardinality ≥ 2. So let $\alpha \in \langle\sigma\rangle\backslash\{1,\dots,n\}$ be an orbit with $|\alpha| \geq 2$. Let $i \in \alpha$. Then

$$\alpha = \{\, i, \sigma(i), \sigma^2(i), \dots, \sigma^{l_\alpha - 1}(i) \,\}, \quad l_\alpha := |\alpha|.$$

Indeed, we know $\langle\sigma\rangle \cong \mathbb{Z}/r\mathbb{Z}$ (cyclic group of order r), and by the orbit–stabilizer theorem We have an isomorphism

$$\langle\sigma\rangle / I_i \xrightarrow{\sim} \alpha, \qquad \overline{\sigma}^s \longmapsto \sigma^s(i),$$

Now let $\alpha_1,\dots,\alpha_s$ be the distinct orbits of $\langle\sigma\rangle$ on $\{1,\dots,n\}$ that have at least two elements. We set $l_j := l_{\alpha_j}$. For each $j \in \{1,\dots,s\}$ let $i_j \in \alpha_j$ and consider the corresponding cycle

$$\gamma_j := (i_j, \sigma(i_j), \dots, \sigma^{l_j - 1}(i_j)).$$

Note that $\operatorname{supp}(\gamma_j) = \alpha_j$.

Lemma. (i) For all $(j_1, j_2) \in \{1,\dots,s\}^2$ we have

$$\gamma_{j_1} \circ \gamma_{j_2} = \gamma_{j_2} \circ \gamma_{j_1}.$$

(ii)

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s.$$

This is called the decomposition of σ into a product of cycles with pairwise disjoint supports.

You will apply the next corollary in the exercises.

Corollary.

$$r = \operatorname{ord}(\sigma) = \operatorname{lcm}(l_1,\dots,l_s).$$

Before we start with the next subsection, we give a characterization for normal subgroups.

Let G act on itself by conjugation. This induces a left action of G on the set $\mathcal{U}(G)$ of subgroups of G (see last repetition sheet). Let $H \in \mathcal{U}(G)$. Then, by definition, the isotropy subgroup is given by

$$I_H = \{\, g \in G \mid gHg^{-1} = H \,\} \subseteq G.$$

We also call I_H the normalizer of H in G and denote it by $N_G(H)$.

Furthermore, we obtain

$$H \in {}^G\mathcal{U}(G) \iff H \text{ is normal in } G \iff I_H = G$$

and set $N(G) := {}^G\mathcal{U}(G)$, the set of normal subgroups of G.

Finite Groups and Sylow Theorems

We begin by recalling some results from the last repetition sheet.
Let G be a finite group acting on a finite set X. Then $G\backslash X$ is finite, and for all $x \in X$ we have

$$G/I_x \cong G \cdot x.$$

In particular, recall that they are not only bijective, but in fact isomorphic as G-sets. By Lagrange's theorem we obtain

$$|G \cdot x| = |G|/|I_x|,$$

which yields

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

where the sum runs over the disjoint orbits.

Corollary. Let G be a group such that $|G| = p^r$ for some $r \geq 1$, and let X be a finite G-set. Then

$$|X| \equiv |{}^G X| \pmod{p}.$$

Definition. Let p be a prime number. A (finite) p-group G is a group whose order is p^r for some $r \geq 0$.

Example.

$$\mathbb{Z}/p\mathbb{Z}, \qquad \mathbb{Z}/p^r\mathbb{Z}, \qquad D_4 = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}, \ldots$$

Using the corollary, we can now easily prove the following theorem.

Theorem. Let G be a non-trivial finite p-group. Then $Z(G) \neq 1$.

To prove this theorem using the above corollary, observe that

$${}^G G = Z(G),$$

where G acts on itself by conjugation. This then already suffices, since in every group we always have $|Z(G)| \geq 1$. Note that this proof is shorter and easier than the proof using the class equation from the tutorials.

As an immediate corollary, and using the fact that subgroups of a p-group are again p-groups (by Lagrange's theorem), we obtain:

Corollary. A finite p-group is nilpotent (and hence solvable).

Recall that for a group G we define inductively

$$G^{[0]} := G, \qquad G^{[i+1]} := G^{[i]}/Z(G^{[i]}).$$

A group is called *nilpotent* if there exists $r \geq 1$ such that $G^{[r]} = 1$.

Theorem (Cauchy)**.** Let G be a finite group and p a prime number dividing $|G|$. Then there exists an element $g \in G$ of order p.

Definition. Let G be a group and let p be a prime number such that

$$|G| = p^r m, \qquad p \nmid m.$$

A *Sylow p-subgroup* of G is a subgroup $U \leq G$ such that

$$|U| = p^r.$$

Example. 1) Consider S_3. Since $|S_3| = 3! = 6 = 2 \cdot 3$, we have

$$1 \longrightarrow A_3 \longrightarrow S_3 \xrightarrow{\text{sgn}} \{\pm 1\} \longrightarrow 1,$$

and therefore

$$S_3/A_3 \cong \{\pm 1\}.$$

(We already proved this in the tutorials, using the fundamental theorem of homomorphisms.) Hence A_3 is the Sylow 3-subgroup of S_3. For any transposition $\tau \in S_3$, $\langle \tau \rangle$ is a Sylow 2-subgroup of S_3.

2) Consider S_4. Since $|S_4| = 4! = 24 = 3 \cdot 2^3$, we have that

$$\langle (1\,2\,3) \rangle \leq S_4$$

is a Sylow 3-subgroup. Moreover,

$$D_4 \leq S_4$$

has order $8 = 2^3$, hence D_4 is a Sylow 2-subgroup of S_4.

We now turn to the important Sylow theorems.

Theorem (Sylow I)**.** Let G be a group of order $|G| = p^r m$ with $p \nmid m$. Then, for all $1 \leq s \leq r$, there exists a subgroup $U \leq G$ such that

$$|U| = p^s.$$

In particular, there exists a Sylow p-subgroup of G (namely of order p^r).

Note that, as a special case, we obtain Cauchy's theorem.

Theorem (Sylow II)**.** Let G be a group such that $|G| = p^r m$ with $p \nmid m$. Let P be a Sylow p-subgroup of G and let $U \leq G$ be a subgroup such that $|U| = p^s$ for some $1 \leq s \leq r$. Then there exists $g \in G$ such that

$$gUg^{-1} \leq P.$$

Remark. (i) If $s = r$, then U is itself a Sylow p-subgroup, and Sylow II yields that Sylow p-subgroups are unique up to conjugation.

(ii) A Sylow p-subgroup P is the only Sylow p-subgroup of G if and only if $P \trianglelefteq G$. Indeed, if $P \trianglelefteq G$, then $gPg^{-1} = P$ for all $g \in G$ (as we have already proved in the lecture), so no other conjugate Sylow p-subgroups can appear.

Theorem (Sylow III)**.** Let G be a group with $|G| = p^r m$ and $p \nmid m$, and let n_p be the number of Sylow p-subgroups of G. Then

$$n_p \mid m \quad \text{and} \quad n_p \equiv 1 \pmod{p}.$$