LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Laurenz Wiesenberger

REPETITION WEEK 2
ALGEBRA

Winter term 25/26

1) Cayley's Theorem

Let G be a group and $S(G)$ the group of bijective maps from G to G. Then every element $a \in G$ induces a bijection

$$\tau_a : G \to G, \quad g \mapsto ag.$$

Hence $\tau_a \in S(G)$, and the assignment

$$G \to S(G), \quad a \mapsto \tau_a,$$

defines a monomorphism. Therefore G can be identified with a subgroup of $S(G)$. This result is called *Cayley's Theorem.*

Consequence: Any finite group G of order n is isomorphic to (and can therefore be viewed as) a subgroup of S_n.

2) Subgroups generated by a family of elements

Let G be a group and $(g_i)_{i\in I}$ a family of elements in G. There exists a unique smallest subgroup of G that contains all elements g_i. It can be described as the intersection of all subgroups $H \leq G$ such that $g_i \in H$ for all $i \in I$.

We denote this subgroup by

$$\langle (g_i)_{i\in I} \rangle,$$

and call it the *subgroup generated by* $(g_i)_{i\in I}$.

The subgroup $\langle (g_i)_{i\in I} \rangle$ can also be explicitly described as

$$\langle (g_i)_{i\in I} \rangle = \{ g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \cdots g_{i_n}^{\varepsilon_n} \mid n \in \mathbb{N}_0,\ i_k \in I,\ \varepsilon_k \in \{\pm 1\} \}.$$

Example (Commutator subgroup). Let G be a group. For $g, h \in G$, we define

$$[g, h] := ghg^{-1}h^{-1}$$

and call this element the *commutator* of g and h. The subgroup of G generated by all elements of the form $[g, h]$ is called the *commutator subgroup* of G and is denoted by $[G, G]$.

Definition. (a) A group G is called *finitely generated* if there exist finitely many elements $g_1, \ldots, g_n \in G$ such that $\langle g_1, \ldots, g_n \rangle = G$.

(b) A group is called *cyclic* if it is generated by a single element, i.e. $\langle g \rangle = G$ for some $g \in G$.

Lemma. Let G be a cyclic group generated by g. Then the map

$$\varphi : \mathbb{Z} \to G, \quad n \mapsto g^n,$$

induces an isomorphism

$$G \cong \begin{cases} \mathbb{Z}, & \text{if } |G| = \infty, \\ \mathbb{Z}/m\mathbb{Z}, & \text{if } |G| = m. \end{cases}$$

Let G be a group and $g \in G$. Then $\langle g \rangle \leq G$ is a subgroup, and the cardinality of $\langle g \rangle$ is called the *order* of g. In particular (see *Lagrange's theorem* below), if G is finite, then

$$\operatorname{ord}(g) \mid |G|.$$

Furthermore, the lemma stated above provides an equivalent definition of the order of an element: if G is finite, then the order of an element g is the smallest $n \in \mathbb{N}$ such that

$$g^n = e_G.$$

3) Quotient of a Group by a Subgroup

Let $H \leq G$ be a subgroup of a group G. We define the equivalence relation

$$a \sim b \quad \iff \quad a^{-1}b \in H.$$

The set of equivalence classes is denoted by G/H, and we have

$$[a] = aH.$$

Since $\sim$ is an equivalence relation, we further have

$$G = \coprod_{aH \in G/H} aH.$$

The map $H \to aH$, $h \mapsto ah$, is a bijection, so each equivalence class has the same cardinality, i.e.

$$|aH| = |bH| \quad \text{for all } a, b \in G.$$

Definition. If G/H is finite, $|G/H|$ is called the *index* of H in G, and we denote it by

$$[G : H] = |G/H|.$$

As an immediate consequence we obtain:

Theorem (Lagrange's Theorem)**.** Let G be a finite group and $H \leq G$ a subgroup. Then

$$|G| = [G : H] \cdot |H|.$$

In particular, for a finite group G, a necessary condition for a subset $H \subseteq G$ to be a subgroup is that the cardinality of H divides the cardinality of G.

We want to define a group structure on G/H. The obvious operation is given by

$$\cdot : G/H \times G/H \longrightarrow G/H, \quad aH \cdot bH \longmapsto (a \cdot_G b)H.$$

Problem: The operation on G/H is, in general, not well-defined.
Let $aH = a'H$ and $bH = b'H$. Then there exist $h_1, h_2 \in H$ such that $a' = ah_1, b' = bh_2$. For the operation to be well-defined, we require

$$(ab)H = (a'b')H \quad \Longleftrightarrow \quad ab(b^{-1}h_1b)h_2 \in H.$$

That is, we need $b^{-1}h_1b \in H$ for all $b \in G$ and $h_1 \in H$.
(*The part after Lagrange's Theorem has not been covered in the lecture so far, but it will probably be treated at the beginning of week 3.*)
This leads us to the following definition.

Definition. A subgroup $H \leq G$ is called a *normal subgroup* of G if

$$gHg^{-1} = H \quad \text{for all } g \in G.$$

In this case we write $H \trianglelefteq G$.

By the above observation, we see that for a normal subgroup $N \leq G$, the operation

$$(aN) \cdot (bN) = (ab)N$$

is well defined. Hence, $(G/N, \cdot)$ is a group with identity element e_GN.