LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Prof. Dr. Fabien Morel
Laurenz Wiesenberger

More about quotients

In the last repetition sheet we saw that if G is a group and $N \trianglelefteq G$ is a normal subgroup, then G/N is, in a canonical way, again a group, where the group structure is induced by G. Furthermore, the canonical projection

$$\pi\colon G \longrightarrow G/N, \quad g \longmapsto gN,$$

is an epimorphism with kernel N.

We have the following universal property. Let $N \trianglelefteq G$ be a normal subgroup. Then for all groups M we have an injective map

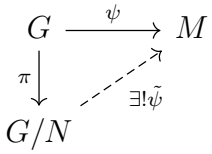
$$\mathrm{Hom}_{\mathrm{grp}}(G/N, M) \xrightarrow{\pi^*} \mathrm{Hom}_{\mathrm{grp}}(G, M), \quad \phi \mapsto \phi \circ \pi,$$

whose image consists precisely of those homomorphisms $\psi\colon G \to M$ satisfying $\psi|_N = *$, where $*$ denotes the trivial group homomorphism.

In other words, we obtain the following: For all groups M and group homomorphisms $\psi\colon G \to M$, there exists a unique group homomorphism

$$\tilde{\psi}\colon G/N \longrightarrow M$$

such that the following diagram commutes:



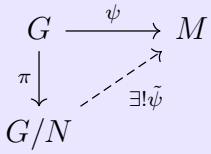
if and only $\psi|_N = *$.

Let us rephrase this again, as the following corollary:

Corollary (Fundamental theorem of homomorphisms)**.** Let M be an arbitrary group, $\psi\colon G \to M$ a group homomorphism, and $N \trianglelefteq G$ a normal subgroup such that $N \subseteq \ker(\psi)$. Then there exists a unique group homomorphism

$$\tilde{\psi}\colon G/N \longrightarrow M$$

such that the following diagram commutes:



Furthermore, one can show that $\tilde{\psi}$ is surjective if and only if ψ is surjective, and $\tilde{\psi}$ is injective if and only if $N = \ker(\psi)$. Hence, we always have

$$G/\ker(\psi) \cong \mathrm{im}(\psi).$$

In the tutorials we will see plenty of examples illustrating how to use this result.

Conjugation

Let $g \in G$ be an arbitrary element. Then the map

$$c_g \colon G \to G, \quad h \mapsto ghg^{-1},$$

is an automorphism of G. Now consider the homomorphism

$$c \colon G \to \mathrm{Aut}(G), \quad g \mapsto c_g.$$

The image of this map, denoted by

$$\mathrm{Inn}(G) := \mathrm{im}(c),$$

is called the *group of inner automorphisms* of G, and its kernel,

$$Z(G) := \ker(c),$$

is called the *center* of G.
In particular, $Z(G) \trianglelefteq G$ and $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Explicitly,

$$\mathrm{Inn}(G) = \{\, c_g \mid c_g(h) = ghg^{-1},\ g, h \in G \,\}, \quad Z(G) = \{\, g \in G \mid gh = hg \text{ for all } h \in G \,\}.$$

How can we think of $\mathrm{Inn}(G)$? These are the automorphisms that we can directly "see", they arise from elements of G itself. In general, however, we do not know what the other automorphisms look like.
Hence, it makes sense to introduce the notion of the *group of outer automorphisms*, which is defined as

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G).$$

Please note that, since $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, this is indeed a group. The cardinality of the quotient $|\mathrm{Out}(G)|$ measures the number of distinct equivalence classes of automorphisms of G modulo inner automorphisms, and can therefore be viewed as indicating how many "essentially different" (non-inner) automorphisms G admits.

Solvable Groups

Recall that for a group G, the *commutator subgroup* $[G, G]$ is defined as the subgroup generated by all commutators in G, i.e.

$$[G, G] := \langle [a, b] \mid a, b \in G \rangle, \quad \text{where } [a, b] := a^{-1}b^{-1}ab.$$

In the tutorials, we showed that the inverse of a commutator of two elements in G is again a commutator. Hence we concluded that

$$[G, G] = \{[a_1, b_1] \cdots [a_n, b_n] \mid n \in \mathbb{N}_0,\ a_i, b_i \in G\}.$$

We then showed that $[G, G] \trianglelefteq G$, i.e. that the commutator subgroup is a normal subgroup of G. In one of the exercises (Exercise 4, not discussed in detail but with solutions available on the website), we saw that the quotient $G/[G, G]$ is abelian and the smallest normal subgroup of G with this property. We call this quotient the *abelianization* of G and denote it by

$$G^{\text{ab}} := G/[G, G].$$

In the following, we use the notion of commutators to define the so-called *solvable groups*. At this point, we do not yet know why this definition is useful or interesting, but we will later learn in the lecture that this concept is fundamental, as it provides the precise link between the solvability of finite groups and the solvability of algebraic equations by radicals.

We define the *i-th derived (or iterated commutator) subgroup* of G inductively by

$$D^0(G) := G, \quad D^{i+1}(G) := [D^i(G), D^i(G)].$$

The subgroup $D(G) := [G, G]$ is also called the *derived subgroup* of G.

Definition. A group G is called *solvable* if there exists an $n \geq 1$ such that $D^n(G) = *$, where $*$ denotes the trivial subgroup of G.

Equivalently, this means that there exists a descending chain of subgroups

$$G \trianglerighteq D^1(G) \trianglerighteq D^2(G) \trianglerighteq \cdots \trianglerighteq D^n(G) = \{e\}.$$

Lemma. Let G be a group. Then the following are equivalent:

(i) G is solvable.

(ii) There exists a descending chain of subgroups

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = *$$

such that $G_i \trianglelefteq G_{i-1}$ for all i, and each quotient G_{i-1}/G_i is abelian.

Corollary. If G is finite, then the following are equivalent:

(i) G is solvable.

(ii) There exists a descending chain

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = *$$

of subgroups such that $G_i \trianglelefteq G_{i-1}$ and each quotient $G_{i-1}/G_i \cong \mathbb{Z}/p_i\mathbb{Z}$ is cyclic of prime order.

Group Extensions

Before we define group extensions, we first introduce the concept of *exact sequences*.

Definition. A sequence of group homomorphisms

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_i} G_i \xrightarrow{f_{i+1}} G_{i+1} \longrightarrow \cdots$$

is said to be *exact at* G_i if

$$\operatorname{im}(f_i) = \ker(f_{i+1}).$$

The sequence is called *exact* if it is exact at every G_i.

A *short exact sequence* is an exact sequence of the form

$$* \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow *. \tag{1}$$

Remark. Sequence (1) is short exact if and only if f is a monomorphism, g is an epimorphism and $\operatorname{im}(f) = \ker(g)$.

Definition. Let G, K, H be groups. Then G is called an *extension* of H by K if there exists a short exact sequence

$$* \longrightarrow K \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow *.$$

Since ι is injective, we can regard K as a subgroup of G. As $\operatorname{im}(\iota) = \ker(\pi)$, $K \trianglelefteq G$ is a normal subgroup and we always have

$$G/K \cong H.$$

The question of what groups G are extensions of H by N is called the extension problem. As to its motivation, recall that the *composition series* of a finite group is a finite sequence of subgroups

$$* = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_n = G,$$

where each A_{i+1} is an extension of A_i by some simple group A_{i+1}/A_i. (A simple group is one that has no nontrivial normal subgroups.)

The classification of finite simple groups provides a complete list of all finite simple groups. Thus, solving the *extension problem* — that is, determining all possible extensions of one group by another — would in principle give enough information to construct and classify all finite groups in general. In practice, however, the extension problem is very hard.
Now let

$$* \longrightarrow K \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow * \tag{2}$$

be a group extension of H by K. We say that (2) is *split* if there exists a group homomorphism $\sigma\colon H \longrightarrow G$ such that

$$\pi \circ \sigma = \mathrm{id}_H\,.$$

Such a homomorphism is called a *section* (or *splitting map*).
Split extensions are particularly easy to classify, since, as we will see, an extension is split if and only if

$$G \cong K \rtimes H,$$

where $K \rtimes H$ denotes a *semidirect product* of K and H. Semidirect products themselves are easier to study, since they are in one-to-one correspondence with group homomorphisms $H \longrightarrow \mathrm{Aut}(K)$.

Example. Consider the following short exact sequence:

$$* \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow *,$$

where $\iota(1) = 2 \in \mathbb{Z}/4\mathbb{Z}$ and $\pi(x) = x \bmod 2$.
This is an *extension* of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$. However, this extension is *not split*: there exists no homomorphism

$$\sigma\colon \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$$

such that $\pi \circ \sigma = \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}}$. Indeed, if such a section existed, $\sigma(1)$ would have to be an element of order 2 in $\mathbb{Z}/4\mathbb{Z}$, but the only element of order 2 is 2, and $\pi(2) = 0$. Hence no such section can exist.
In contrast, consider the direct product

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Then we have another short exact sequence

$$* \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota} G \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow *,$$

where $\iota(a) = (a, 0)$ and $\pi(a, b) = b$. This extension *is split*, since the map

$$\sigma\colon \mathbb{Z}/2\mathbb{Z} \longrightarrow G, \quad \sigma(b) = (0, b),$$

satisfies $\pi \circ \sigma = \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}}$.
In summary:

- $\mathbb{Z}/4\mathbb{Z}$ is a *non-split extension* of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$.
- $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is a *split extension*.

Now let us turn to semidirect products. Let $\sigma\colon H \to G$ be a section of π. Then the map

$$K \times H \longrightarrow G, \quad (k,h) \longmapsto k\,\sigma(h),$$

is a bijection. Let

$$* \longrightarrow K \longrightarrow G \xrightarrow{\pi} H \longrightarrow *$$

be a split extension. Then for all $h \in H$ and $k \in K$, we have

$$\sigma(h)\,k\,\sigma(h)^{-1} \in K.$$

This defines an action

$$\varphi\colon H \longrightarrow \mathrm{Aut}(K),$$

given by $\varphi(h)(k) = \sigma(h)k\sigma(h)^{-1}$.

Lemma. Let H, K be groups and let $\varphi\colon H \to \mathrm{Aut}(K)$ be a homomorphism. Then

$$(K \times H) \times (K \times H) \longrightarrow K \times H, \quad ((k_1,h_1),(k_2,h_2)) \longmapsto (k_1\,\varphi(h_1)(k_2),\, h_1h_2),$$

defines a group structure on $K \times H$, denoted by

$$K \rtimes_\varphi H = K \rtimes H,$$

and called the *semidirect product* of K and H.

Lemma (Characterization of Split Extensions)**.** Every split extension

$$* \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow *$$

is isomorphic to a semidirect product $K \rtimes_\varphi H$.
Equivalently: Split extensions are precisely semidirect products.