What is the Schur-Zassenhaus Theorem?

Linus Ge

July 21, 2025

Presentation Overview

Short Exact Sequences

Definition

Given groups A, B, C and homomorphisms $\phi : A \to B$, $\psi : B \to C$, we say these form a short exact sequence if ϕ is injective, ψ is surjective, and $Im(\phi) = Ker(\psi)$.

Usually, when we have a short exact sequence, it is denoted by

$$0 \to A \to B \to C \to 0.$$

Typically, the maps are omitted when understood.

Short Exact Sequences

A canonical example of a short exact sequence is

$$0 \to N \to G \to G/N \to 0,$$

where G is a group, $N \lhd G$ is a normal subgroup, and G/N is the quotient group. The maps $\phi : N \to G$ and $\psi : G \to G/N$ would be the inclusion and quotient maps respectively.

From this example it is clear that if one knows G and one of N or G/N, it is possible to deduce the third using exactness of the sequence. But what can be said if one only knows N and G/N?

Short Exact Sequences

Suppose $N = G/N = \mathbb{Z}/2\mathbb{Z}$. Then we have the following short exact sequence,

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

One can check that both $G = \mathbb{Z}/4\mathbb{Z}$ and $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are both valid choices for G in this short exact sequence. So it is not always possible to determine G from knowledge of $N \lhd G$ and G/N.

Short Exact Sequences

Definition

Given groups A, B, C, we say B is an extension of A and C if there exists a short exact sequence

$$0 \to A \to B \to C \to 0.$$

The theory of group extensions is quite deep, and as illustrated by the previous example extensions are not always unique. But certain properties of groups may or may not be preserved by extensions.

For the purpose of this talk, all groups mentioned are finite unless otherwise stated.

The Schur-Zassenhaus Theorem

Theorem (Schur)

Let G be a group and $N \lhd G$ be a normal subgroup. If $\gcd(|N|, |G/N|) = 1$, then there exists $H \leq G$ such that $H \cong G/N$.

Corollary

Let G be a group and $N \lhd G$ be a normal subgroup. If $\gcd(|N|, |G/N|) = 1$, then there exists $H \leq G$ such that $G = N \rtimes H$.

In general, such a subgroup H is called a complement of N in G.

Statement of the Theorem

Alternatively, one can state the theorem as follows.

Theorem (Schur)

Given a short exact sequence

$$0 \to A \to B \to C \to 0,$$

with homomorphisms $\phi : A \to B$ and $\psi : B \to C$, if $\gcd(|A|, |B|) = 1$, then the short exact sequence splits. This means there exists a homomorphism $\rho : C \to B$ such that $\psi \circ \rho$ is the identity map on C.

Statement of the Theorem

As is typical in mathematics, this theorem is attributed to Schur by Zassenhaus, but it is not fully clear where Schur proved this in his work. Schur's work on Schur multipliers, however, does imply this theorem in the case that $N \leq Z(G)$, i.e. the normal subgroup is in the center.

Zassenhaus himself provided a complete proof of this theorem, along with an additional stronger statement.

Statement of the Theorem

Theorem (Zassenhaus)

Let G be a group and $N \lhd G$ be a normal subgroup. If $\gcd(|N|, |G/N|) = 1$, then there exists $H \leq G$ such that $H \cong G/N$.

Additionally, for any $K \leq G$ with $K \cong G/N$ there exists $g \in G$ such that $K = gHg^{-1}$.

So not only does N have a complement, but all its complements are conjugate. Zassenhaus at the time was only able to prove the second part of the statement under the assumption that one of N or G/N was solvable, but that assumption can be dropped.

Reduction to Abelian N

To prove the Schur-Zassenhaus theorem, we now proceed by strong induction on the order of G. It is clear that we can further assume N is a proper nontrivial normal subgroup. Let p be a prime dividing $|N|$, and P be a Sylow p subgroup of N. As $(|N|, |G/N|) = 1$, P is also a Sylow p subgroup of G. As N is normal and $P \leq N$, all conjugates of P in G are contained in N. This means we have

$$\frac{|G|}{|N_G(P)|} = [G : N_G(P)] = [N : N_N(P)] = [N : N_G(P) \cap N] = \frac{|N|}{|N_G(P) \cap N|}.$$

Here, we are using that the index of the normalizer is the number of conjugates.

Reduction to Abelian N

Suppose that P is not a normal subgroup of G. Then $N_G(P)$ is a proper subgroup of G and thus has strictly smaller order. We also have $N_G(P) \cap N \lhd N_G(P)$ as $N \lhd G$. However,

$$\frac{|G|}{|N_G(P)|} = \frac{|N|}{|N_G(P) \cap N|} \implies \frac{|N_G(P)|}{|N_G(P) \cap N|} = \frac{|G|}{|N|}.$$

So our strong induction hypothesis applies to $N_G(P)$ and $N_G(P) \cap N$. Thus, there exists $H \leq N_G(P) \leq G$ with

$$|H| = \frac{|N_G(P)|}{|N_G(P) \cap N|} = \frac{|G|}{|N|} = |G/N|.$$

This completes the proof in this specific case.

Reduction to Abelian N

Now suppose that $P \triangleleft G$. Then $P \triangleleft N$ and $N/P \triangleleft G/P$ as $N \triangleleft G$. We also know $[G/P : N/P] = [G : N] = |G/N|$ and $\gcd(|N/P|, |G/N|) = 1$, so our strong induction hypothesis applies to $N/P \triangleleft G/P$. This means there exists $K \leq G/P$ with $|K| = |G/N|$. Lift K to $H \leq G$, so that $K = H/P$.

As P is a nontrivial p-group, it has nontrivial center $Z(P) = Z$. The center of a normal subgroup is normal, so $Z \triangleleft H$ and $P/Z \triangleleft H/Z$. We once again apply our strong induction hypothesis and lift the resulting subgroup to get $L \leq H$, with $L/Z \leq H/Z$ and $|L/Z| = |G/N|$.

Reduction to Abelian N

After applying our strong induction hypothesis and lifting twice, we now have subgroups, $L \leq H \leq G$ and $Z = Z(P) \lhd L$ a normal p-group with $\gcd(|Z|, |L/Z|) = 1$. If $|L| < |G|$, we can apply our strong induction hypothesis again and get $M \leq L \leq G$ with $|M| = |L/Z| = |G/N|$. This would complete the proof.

If $|L| = |G|$, then $L = H = G$. In other words, $[G : N] = [H : P] = [G : P]$ and $N = P$ is a normal Sylow p-group. In fact, N must be an abelian Sylow p-subgroup since $[G : N] = [L : Z] = [G : Z]$, which implies $N = P = Z(P) = Z$. This completes the reduction to N being abelian.

Proof for Abelian N

After a reduction to abelian N, most proofs use either representation theory or group cohomology to complete the proof. The idea of this approach is the second cohomology group $H^2(G/N, N)$ is trivial since $\gcd(|N|, |G/N|) = 1$, and using a bijection between H^2 and equivalence classes of group extensions. But one should always try and find an elementary argument when possible.

We will now outline a constructive proof that avoids heavy machinery.

Proof for Abelian N

Given $N \triangleleft G$ is abelian and $\gcd(|N|, |G/N|) = 1$, fix two sets of coset representatives for N, denoted A and B. Notice for every $a, b \in G$ with $aN = bN$, $a^{-1}b \in N$ since $a^{-1}bN = a^{-1}(aN) = N$. Define

$$T(A, B) = \prod_{(a,b) \in A \times B,\ aN = bN} a^{-1}b.$$

$T(A, B)$ is well defined since $a^{-1}b \in N$ and N is abelian, meaning the order of multiplication in the product does not matter.

Define an equivalence relation on sets of coset representatives of N, where A and B are equivalent if $T(A, B) = e$. One can check this is a genuine equivalence relation.

Proof for Abelian N

With this equivalence relation, G acts by left multiplication on equivalence classes of sets of coset representatives. This is because

$$T(gA, gB) = \prod_{(ga,gb)\in A\times B,\, gaN=gbN} (ga)^{-1}gb = \prod_{(a,b)\in A\times B,\, aN=bN} a^{-1}b = T(A, B)$$

With more work, one can check there are exactly $|N|$ equivalence classes of sets of coset representatives. Hence, a stabilizer subgroup will be a complement. Furthermore, this group action is transitive, proving the second part as that implies all stabilizer subgroups are conjugate.

Conjugacy of Complements

Zassenhaus himself in 1937 only managed to prove all complements H of N are conjugate in the case that one of N or G/N is solvable. He did, however, note that the theorem in full generality would follow if groups of odd order were solvable.

And it turns out this did indeed turn out to be true. Feit and Thompson proves solvability of groups of odd order in 1963. Unfortunately, this talk is not long enough to cover all the details of this proof.

There are, however, more elementary proofs of conjugacy which do not go through solvability of groups of odd order.

A Corollary

Corollary

Let p be a prime. For a finite group G with order divisible by p, the following are equivalent:

1. $|Aut(G)|$ *is not divisible by* p.
2. $G \cong \mathbb{Z}/p\mathbb{Z} \times H$ *where* $|H|$ *and* $|Aut(H)|$ *are not divisible by* p.

In particular, if $|G|$ *is divisible by* p^2 *then* $|Aut(G)|$ *is divisible by* p.

References


https://kconrad.math.uconn.edu/blurbs/grouptheory/schurzass.pdf


The theory of finite groups by Kurzweil and Stellmacher


Zassenhaus, Hans J. (1958) [1949], *The theory of groups*. (2nd ed.), New York: Chelsea Publishing Company, MR 0091275

The End

Questions? Comments?