THE SCHUR–ZASSENHAUS THEOREM

KEITH CONRAD

When N is a normal subgroup of G, can we reconstruct G from N and G/N? In general, no. For instance, the groups $\mathbf{Z}/(p^2)$ and $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ (for prime p) are nonisomorphic, but each has a cyclic subgroup of order p and the quotient by it also has order p. As another example, the nonisomorphic groups $\mathbf{Z}/(2p)$ and D_p (for odd prime p) have a normal subgroup that is cyclic of order p, whose quotient is cyclic of order 2.

If we impose the condition that N and G/N have relatively prime order, then something nice can be said: G is a semidirect product of N and G/N. This is the Schur-Zassenhaus theorem, which we will discuss below. It doesn't uniquely determine G, as there could be several non-isomorphic semi-direct products of the abstract groups N and G/N, but each one is a group with normal subgroup N and quotient by it isomorphic to G/N. For instance, if $N \cong \mathbf{Z}/(p)$ for odd prime p and $G/N \cong \mathbf{Z}/(2)$ then G must be a semi-direct product $\mathbf{Z}/(p) \rtimes \mathbf{Z}/(2)$. The only two semidirect products are the direct product (which is isomorphic to $\mathbf{Z}/(2p)$) and the nontrivial semidirect product (which is isomorphic to D_p).

Theorem 1 (Schur-Zassenhaus)**.** *Let G be a finite group and write $\#G = ab$ where $(a, b) = 1$. If G has a normal subgroup of order a then it has a subgroup of order b.*

Let's see why this theorem tells us G is a semidirect product. Letting N be the normal subgroup of order a and H be a subgroup of order b, $N \cap H$ is trivial since $(a, b) = 1$, so $G = NH \cong N \rtimes H$ is a semidirect product with N as the normal factor. Conversely, if any group having a normal subgroup and quotient group of relatively prime orders

We will present two proofs of this theorem. Both proofs will be incomplete at the end. Each proof will reduce to the case when N is abelian, at which point the machinery of group cohomology can be applied. While group cohomology provides a general tool to describe the groups having a particular normal subgroup with a particular quotient group (up to isomorphism), it requires the normal subgroup be abelian, and we are making no such assumption. So the proof of the Schur-Zassenhaus theorem amounts to a reduction process to the case when N is abelian.

The first proof of the theorem will use the following lemma.

Lemma 2. *If $N \lhd G$ and $P \in \mathrm{Syl}_p(N)$ then $G = N \cdot \mathrm{N}_G(P)$. In particular, if $P \lhd N$ then $P \lhd G$.*

Proof. Pick $g \in G$. Since $P \subset N$ and $N \lhd G$, $gPg^{-1} \subset N$. Then by Sylow II for the group N, there is an $n \in N$ such that $gPg^{-1} = nPn^{-1}$, so $n^{-1}gPg^{-1}n = P$. That means $n^{-1}g \in \mathrm{N}_G(P)$, so $g \in n\,\mathrm{N}_G(P)$. Thus $G = N \cdot \mathrm{N}_G(P)$.

If $P \lhd N$ then $N \subset \mathrm{N}_G(P)$, so $N \cdot \mathrm{N}_G(P) = \mathrm{N}_G(P)$. Thus $G = \mathrm{N}_G(P)$, so $P \lhd G$. □

Here is the first proof of the Schur–Zassenhaus theorem.

Proof. Assume the theorem is false and let G be a counterexample of minimal order. So any group with order less than $\#G$ satisfies the theorem. Easily $a > 1$ and $b > 1$.

Let $N \lhd G$ with $\#N = a$. We aim to get a contradiction.

Step 1: Show N is a minimal normal subgroup of G: there are no normal subgroups of G lying strictly between $\{e\}$ and N.

Suppose $N' \lhd G$ with $\{e\} \subset N' \subset N$ and $N' \neq \{e\}$ or N. We look at the group G/N' with order $< \#G$. Since $N/N' \lhd G/N'$ and $\#(G/N') = \#(N/N')b$ with the two factors being relatively prime, by minimality of G there is a subgroup of G/N' with order b. It has the form K/N', so $\#K = \#N'b < ab$. Since $\#N'$ and b are relatively prime, by minimality of G there is a subgroup of order b in K and hence in G. This is a contradiction, so N' doesn't exist.

Step 2: Show N is an abelian p-group.

Let P be a nontrivial Sylow subgroup of N, so by Theorem 2 we have $G = N\,\mathrm{N}_G(P)$. Then $G/N \cong \mathrm{N}_G(P)/(N \cap \mathrm{N}_G(P))$ and the order of $\mathrm{N}_G(P)$ is $\#(N \cap \mathrm{N}_G(P))b$ with $\#(N \cap \mathrm{N}_G(P))$ a factor of a (hence relatively prime to b). Since $N \cap \mathrm{N}_G(P)$ is a normal subgroup of $\mathrm{N}_G(P)$, if $N_G(P)$ is a proper subgroup of G then by minimality of G there is a subgroup of order b in $\mathrm{N}_G(P)$, and hence in G. This isn't possible, so $N_G(P) = G$, which means $P \lhd G$. Therefore, by the Sylow theorems, P is a normal subgroup of N, so $P = N$ by Step 1. Then $Z(P)$ is a nontrivial normal subgroup of P, so $Z(P) = P$ by Step 1 again, which means N is an abelian p-group.

Step 3: Show $N \cong (\mathbf{Z}/(p))^k$.

Considering the structure of finite abelian p-groups, this step is equivalent to showing $N^p = \{x^p : x \in N\}$ is trivial. Assume N^p is nontrivial. It is preserved as a set by all group automorphisms of N, so in particular $gN^pg^{-1} = N^p$ for any $g \in G$. Thus $N^p \lhd G$, so $N/N^p \lhd G/N^p$. Since N/N^p is a p-group while the index $[G/N^p : N/N^p] = [G : N]$ is relatively prime to p, by induction G/N^p has a subgroup of order $[G : N]$. The subgroup is H/N^p for some $H \subset G$, so $[H : N^p] = [G : N]$ is not divisible by p. Since $N^p \lhd H$, N^p is a p-group with index prime to p in H, and $\#H < \#G$, by induction again there is a subgroup K of H with order $[H : N^p] = [G : N]$. This K is also in G, so G has a subgroup of order $[G : N]$. This is a contradiction, so N^p is trivial.

Step 4: Get a final contradiction.

Let G act on N by conjugation. Since $N \cong (\mathbf{Z}/(p))^k$, automorphisms of N can be interpreted as elements of $\mathrm{GL}_k(\mathbf{Z}/(p))$. Therefore the conjugation action of G on N is a group homomorphism $G \to \mathrm{GL}_k(\mathbf{Z}/(p))$. Since N is abelian, it acts trivially on itself, so our action descends to a homomorphism $G/N \to \mathrm{GL}_k(\mathbf{Z}/(p))$. At this point the reader is referred to the literature for the rest of the proof. Two possible approaches are representation theory [2, p. 146] or group cohomology (the vanishing of $\mathrm{H}^2(G/N, N)$; a cohomological neophyte can find this done without any reference to cohomology in [3, pp. 246–247], but it is not very illuminating). □

Here is a second proof. Again we will reduce to the case of an abelian normal subgroup.

Proof. Let $N \lhd G$ with $\#N$ and $[G : N]$ relatively prime. We want to prove G has a subgroup of order $[G : N]$. Of course we can assume N is a nontrivial proper subgroup of G.

We induct on $\#G$. Assume $\#G > 1$ and the theorem is verified for subgroups with smaller order. Let p be a prime factor of $\#N$ and P be a p-Sylow subgroup of N, so P is nontrivial. Because $[G : N]$ is prime to $\#N$, p does not divide $[G : N]$ so P is also a p-Sylow subgroup of G. Since $P \subset N$ and $N \lhd G$, all G-conjugates of P are in N. Therefore all the

p-Sylow subgroups of G are in N, hence by counting p-Sylows in G and in N we get

$$[G : \mathrm{N}_G(P)] = [N : \mathrm{N}_G(P) \cap N].$$

Writing these indices as ratios and rearranging terms,

$$[G : N] = [\mathrm{N}_G(P) : \mathrm{N}_G(P) \cap N]. \tag{1}$$

Case 1: P is not normal in G. Then $\mathrm{N}_G(P)$ is a proper subgroup of G. The group $\mathrm{N}_G(P) \cap N$ is normal in $\mathrm{N}_G(P)$ since $N \lhd G$, the order of $\mathrm{N}_G(P) \cap N$ divides $\#N$, and the index of $\mathrm{N}_G(P) \cap N$ in $\mathrm{N}_G(P)$ is $[G : N]$ by (1), so $\mathrm{N}_G(P)$ and its normal subgroup $\mathrm{N}_G(P) \cap N$ satisfy the hypotheses of the theorem. Since $\# \mathrm{N}_G(P) < \#G$, by induction $\mathrm{N}_G(P)$ has a subgroup of order $[\mathrm{N}_G(P) : \mathrm{N}_G(P) \cap N] = [G : N]$. This is a subgroup of G too, so we're done.

Case 2: $P \lhd G$. Then $P \lhd N$ and $N/P \lhd G/P$ with $\#(N/P)$ dividing $\#N$ and $[G/P : N/P] = [G : N]$. This order and index are relatively prime, and $\#(G/P) < \#G$, so by induction the theorem holds for G/P and its subgroup N/P: there is a subgroup in G/P of order $[G/P : N/P] = [G : N]$. Write the subgroup as H/P, so H is a subgroup of G and

$$[H : P] = \#(H/P) = [G : N] \tag{2}$$

is not divisible by p. (If $P = N$ then $H = G$.)

Since P is a nontrivial p-group, its center $Z := Z(P)$ is nontrivial. Also $Z \lhd H$ (the center of a normal subgroup is also a normal subgroup), so $P/Z \lhd H/Z$. The group P/Z is a p-group (possibly trivial, if P is abelian) while $[H/Z : P/Z] = [H : P] = [G : N]$ is prime to p, so (since $\#(H/Z) < \#H \leq \#G$) by induction H/Z contains a subgroup K/Z of order $[H : P]$. (If P is abelian then $K = H$.)

Now we have $Z \lhd K$ with Z a p-group and

$$[K : Z] = \#(K/Z) = [H : P] = [G : N]$$

being prime to p, so K and its normal subgroup Z satisfy the hypotheses of the theorem. Now *if* $\#K < \#G$ then we can apply induction to conclude K has a subgroup of order $[K : Z] = [G : N]$, and this is also a subgroup of G, so we're done. What if $K = G$? Since $K \subset H \subset G$, if $K = G$ then $H = G$ so $[G : P] = [G : N]$ by (2). Therefore $N = P$ since $P \subset N$, so N is a normal Sylow subgroup of G.

If N is a normal p-Sylow in G and it is not abelian, we can use induction yet again to finish the proof. Run through the argument two paragraphs up (with $P = N$, $H = G$, and $Z = Z(P) = Z(N)$ the center of N). We get a subgroup K/Z of G/Z with order $[G : N]$. Now $\#K = \#Z[G : N]$. If $Z \neq N$ (*i.e.*, N is non-abelian) then $\#Z < \#N$ so $\#K < \#N[G : N] = \#G$ and we are done as before.

What if N is normal in G and N is abelian? In this case we can, as in the previous proof, consider $N^p = \{x \in N : x^p = 1\}$. This is a normal subgroup of N and in fact it is normal in G too. Running through the previous paragraph with N^p in place of Z we are done by another induction unless $N^p = N$, which means all the elements of N have order p. So we are left to contemplate the same case as at the end of the first proof: N is a normal p-Sylow subgroup of G and is isomorphic to $(\mathbf{Z}/(p))^k$ for some k. The end of the proof is now the same as in the first proof: use either representation theory or group cohomology. □

Remark 3. The Schur–Zassenhaus theorem actually has an important second part, which we omitted: any two subgroups of order b in G are conjugate to each other. See [3, p. 248] for the proof of that.

Let's put the Schur–Zassenhaus theorem to work. We ask, out of idle curiosity, whether $p|\#G$ implies $p|\#\operatorname{Aut}(G)$. The answer, of course, is no: try $G = \mathbf{Z}/(p)$. As we now show, this counterexample essentially explains all the others.

Corollary 4. *Fix a prime p. For a finite group G with order divisible by p, the following are equivalent:*

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

In particular, if $p^2|\#G$ then $p|\#\operatorname{Aut}(G)$.

Proof. Assume (1) holds and let P be a p-Sylow subgroup of G. We expect to show $G \cong P \times H$ and $P \cong \mathbf{Z}/(p)$.

For any $x \in P$ there is the automorphism $\gamma_x \in \operatorname{Aut}(G)$ which is conjugation by x. Since x has p-power order, so does γ_x (recall $\gamma_x^n = \gamma_{x^n}$ for all n). By hypothesis $\#\operatorname{Aut}(G)$ is not divisible by p, so the only element of p-power order in $\operatorname{Aut}(G)$ is the identity. Thus $\gamma_x = \mathrm{id}_G$ for all $x \in P$, which means $P \subset Z(G)$. In particular, $P \lhd G$ by Sylow II and P is abelian. Therefore the Schur-Zassenhaus theorem tells us $G \cong PH$ for some subgroup H with order not divisible by p. Since $P \subset Z(G)$, $G \cong P \times H$. Because the groups P and H have relatively prime order and commute in G, $\operatorname{Aut}(G) \cong \operatorname{Aut}(P) \times \operatorname{Aut}(H)$ in the natural way. Therefore p doesn't divide $\#\operatorname{Aut}(P)$ or $\#\operatorname{Aut}(H)$.

Which finite abelian p-groups P have $\#\operatorname{Aut}(P)$ not divisible by p? Write P as a direct product of cyclic groups, say

$$P = \mathbf{Z}/(p^{r_1}) \times \cdots \times \mathbf{Z}/(p^{r_k}).$$

Since $\operatorname{Aut}(\mathbf{Z}/(p^r)) \cong (\mathbf{Z}/(p^r))^\times$ has order $p^{r-1}(p-1)$, we see that if some $r_i > 1$ then that $\mathbf{Z}/(p^{r_i})$ has an automorphism of order p, so P does as well (act by the chosen automorphism on the i-th factor and fix elements in the other factors). Thus, if $\#\operatorname{Aut}(P)$ is not divisible by p we must have $r_i = 1$ for all i, so $P \cong (\mathbf{Z}/(p))^k$ is a direct sum of copies of $\mathbf{Z}/(p)$. That means $\operatorname{Aut}(P) \cong \mathrm{GL}_k(\mathbf{Z}/(p))$, whose order is divisible by $p^{k(k-1)/2}$, and thus is divisible by p unless $k = 1$. So we must have $P \cong \mathbf{Z}/(p)$, which concludes the proof that (1) implies (2).

To show (2) implies (1), $\operatorname{Aut}(\mathbf{Z}/(p) \times H) \cong \operatorname{Aut}(\mathbf{Z}/(p)) \times \operatorname{Aut}(H) \cong (\mathbf{Z}/(p))^\times \times \operatorname{Aut}(H)$, and this has order not divisible by p since $\#\operatorname{Aut}(H)$ is not divisible by p. □

Example 5. If $\#G$ is even and $\#\operatorname{Aut}(G)$ is odd then $G \cong \mathbf{Z}/(2) \times H$ where H is a group of odd order with $\operatorname{Aut}(H)$ of odd order too. The smallest such nontrivial H has order $729 = 3^6$ with automorphism group $19683 = 3^9$.

When $p|\#\operatorname{Aut}(G)$, one way to search for elements of order p in $\operatorname{Aut}(G)$ is by looking for an inner automorphism: if $g \in G$ has order p and g is not in the center of G then conjugation by G is an (inner) automorphism of G with order p. Since inner automorphisms are a cheap construction, we ask: when are there non-inner automorphisms of order p, assuming that we know $p|\#\operatorname{Aut}(G)$ (and $p|\#G$)? For p-groups there is a complete answer. When G is a finite abelian p-group, it has an automorphism of order p as long as $G \not\cong \mathbf{Z}/(p)$, and that automorphism is not inner since G is abelian. When G is a finite non-abelian p-group, Gatschütz [1] showed that there is an automorphism of order p which is not inner, using cohomology.

References

[1] W. Gatschütz, Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen, *J. Algebra* **4** (1966), 1–2.

[2] M. I. Kargapolov and Y. I. Merzlyakov, "Fundamentals of the theory of groups," Springer–Verlag, New York, 1979.

[3] D. J. S. Robinson, "A Course in the Theory of Groups," Springer-Verlag, New York, 1982.