

Introduction

The purpose of this note is to give a few proofs of

HUPPERT'S THEOREM: *If G is a finite group such that every maximal subgroup has prime index, then G is supersolvable.*

Recall a group is called **supersolvable** if the factors of its chief series are made up of cyclic groups of prime order. Equivalently, it has a normal series where the factors are cyclic. It's relatively easy to give a proof that the converse of Huppert's Theorem holds as well, by induction on $|G|$ and quotienting by a minimal normal subgroup.

Below we will give three different proofs of Huppert's Theorem. All the proofs follow the same pattern: assume the existence of a minimal counterexample, and reach a contradiction. We capture some common facts about such a minimal counterexample (MCE) in the next section, before turning to the three proofs. They all share some similarities and overlaps: the **local proof** uses linear techniques for relating a local version of supersolvability to a fact about group quotients; the **linear proof** has several cohomological ideas underpinning the approach; and the **cohomological proof** uses some local flavor to find a subgroup to apply the cohomology to.

Throughout this note, all groups are finite. We write $GF(p^n)$ for the field with p^n elements, and $GL(p^n)$ for the automorphism group of that field's underlying Abelian group.

A few facts

Obviously, for a group to be supersolvable, it seems likely it needs to be solvable first. In fact, proving that is significantly easier than proving [Huppert's Theorem](#).

THEOREM 1 (P. Hall): *Let G be a group with every maximal subgroup of prime index. Then G has a normal Sylow subgroup and is solvable.*

Proof. Let p be the largest prime dividing $|G|$, and P a Sylow p -subgroup. If $N_G(P)$ is a proper subgroup, then let M with $N_G(P) \leq M \leq G$ be a maximal subgroup of G . Since $[G : N_G(P)] \equiv 1 \pmod{p}$, then $[G : M] \equiv 1 \pmod{p}$ as well (since $N_G(P) = N_M(P)$). But since $[G : M]$ is a prime dividing $|G|$, we would have a prime q dividing $|G|$ and $q > p$, contradicting our choice of p . Hence $N_G(P) = G$ and P is a normal subgroup.

To see that G is solvable, we can induct on $|G|$. Since $P \trianglelefteq G$ is a non-trivial normal subgroup, and the maximal subgroups of G/P are exactly the images of maximal subgroups of G containing P , we see that by our induction hypothesis G/P is solvable. But P is also solvable (being a p -group), and hence G is solvable too. $\square$

Now we lay out some facts about what a minimal counterexample (MCE) to [Huppert's Theorem](#) would look like. This would be a group G such that every maximal subgroup of G has prime index, but G is **not** supersolvable, and $|G|$ is minimum amongst all such counterexamples. We can use P. Hall's Theorem to conclude G is solvable, and in particular has a minimal normal subgroup N that is an elementary Abelian p -group for some prime p .

MCE FACTS: Let G be a minimal counterexample to [Huppert's Theorem](#), and N a minimal normal subgroup of G .

- (I) If $1 \leq K \trianglelefteq G$ is a nontrivial normal subgroup of G , then G/K is supersolvable.
- (II) G has no normal subgroups of prime order.
- (III) $|N| = p^a$ for $a > 1$.
- (IV) If K and L are normal subgroups of G with $1 < K < L$, then there exists a normal subgroup H of G with $K \leq H \leq L$ and $[H : K]$ prime.
- (V) N is the unique normal subgroup of G .
- (VI) If H is a subgroup of G with $G = HN$, then $H = G$.
- (VII) $N \leq \Phi(G)$.

Proof.

- (I) The maximal subgroups of G/K are precisely the images of maximal subgroups in G that contain K , and hence all still have prime index. Since $|G/K| < |G|$ and G is a minimal counterexample, G/K is supersolvable.
- (II) If K was a normal subgroup of prime order, then by the previous fact G/K would be supersolvable. But then a chief series for G can be built from the one for G/K and K , all having prime order factor groups; this contradicts the fact that G is a counterexample.
- (III) N is an elementary Abelian p -group since G is solvable, so is of order p^a for some prime p and positive integer a . By the preceding fact, we cannot have $a = 1$.
- (IV) By (I) G/K is supersolvable, and hence any minimal normal subgroup contained in L/K will look like H/K with $|H/K|$ prime.
- (V) Let K be another minimal normal subgroup of G . Since then $1 < K < NK$, the preceding fact gives a normal subgroup $L \leq NK$ with $[L : K] = p$. We have $K(N \cap L) = KN \cap L = L$ and hence $N \cap L$ is a normal subgroup of order $[L : K] = p$ in G , contradicting (II). Thus K does not exist.

- (VI) We can assume H is maximal in G , and reach a contradiction. If $N \leq H$, then $H = HN = G$, as desired. Otherwise, $N \cap H$ is normal in H , and also in N since it's Abelian. Thus $N \cap H$ is normal in $HN = G$, and by the minimality of N that means $N \cap H = \{1\}$. Thus $[G : H] = [N : N \cap H] = |N|$, but $|N|$ is not prime by (III), contradicting that $[G : H]$ should be prime. Thus $H = G$.
- (VII) If M was a maximal subgroup of G not containing N , then $G = MN$ contradicts the preceding fact. Thus every maximal subgroup of G contains N , so $N \leq \Phi(G)$.

□

Local proof

The proof in this section will rely on local versions of nilpotency and supersolvability, which we will define and prove a few facts about first. The primary reason for using the "localized" versions is that they have criteria that can be verified in group quotients, allowing us to leverage some facts about a minimal counterexample to reach a contradiction. Everything here is largely based on [Hup83, VI.9.5].

All of the localized definitions rely on a normal series for a group G . Recall that a normal series looks like

$$G_0 = 1 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

with each G_k normal in G . This normal series is a chief series when G_{k+1}/G_k is a minimal normal subgroup of G/G_k for all k . Essentially this says there are no more normal subgroups that can be "squeezed" in between successive elements in a chief series. There are two key facts about normal series that we need, whose proofs are omitted since they are trivial:

LEMMA 2: *Let K be a subgroup of G . Then*

1. *If K is normal, there is a normal (chief) series of G containing K .*
2. *For a normal series of G , defining $K_i = G_i \cap K$ gives a normal series for K .*

First we define **p -nilpotency** for a group G . In terms of a chief series G is p -nilpotent when every factor group G_{k+1}/G_k is either central in G/G_k or has order coprime to p . Note that being central here is equivalent to saying $[G, G_{k+1}] \leq G_k$. Since it's impossible for $|G_{k+1}/G_k|$ to be coprime to all prime numbers, being p -nilpotent for all primes p is equivalent to all factor groups of the chief series being central. Thus

$$G \text{ is nilpotent} \iff G \text{ is } p\text{-nilpotent for all primes } p$$

Lemma 2 makes it obvious that quotients of p -nilpotent groups are p -nilpotent. Lemma 2 together with the following also makes it clear that subgroups of p -nilpotent groups are p -nilpotent (see the first paragraph of the proof of Proposition 5 for more details).

LEMMA 3 (Index Trick): If $H \leq G$ and $A \leq B \leq G$ are subgroups of G , such that AH and BH are subgroups, then $[B \cap H : A \cap H]$ divides $[B : A]$.

Proof.

$$\begin{aligned} [BH : AH] &= \frac{\frac{|B||H|}{|B \cap H|}}{\frac{|A||H|}{|A \cap H|}} \\ &= \frac{[B : A]}{[B \cap H : A \cap H]} \quad \square \end{aligned}$$

One final fact about p -nilpotent groups, which is a localized version of what holds for nilpotent groups.

LEMMA 4: If $N \trianglelefteq G$ is a minimal normal subgroup, with G p -nilpotent and p divides $|N|$, then $N \leq Z(G)$.

Proof. By Lemma 2 we can build a chief series for G containing N , and since N is a minimal normal subgroup, it will be G_1 . Since p divides $|G_1/G_0| = |N|$, it follows from the definition of p -nilpotency that N is central in G . $\square$

Of course, nilpotency is not our final goal. But we will be making heavy use of p -nilpotent subgroups, so let's see how to construct them. G acts on each factor of a normal series by conjugation. For a chief series of G , let

$$\mathcal{F}_p = \{G_{k+1}/G_k \mid p \text{ divides } |G_{k+1}/G_k|\}$$

be the chief factors that are not coprime to p . By the Jordan–Hölder theorem, $\mathcal{F}_p$ does not depend on the chief series chosen. If G is a p -nilpotent group, then the conjugation action on every factor in $\mathcal{F}_p$ is trivial. This motivates the following

PROPOSITION 5: Let $\mathbf{F}_p(G)$ be the set of elements in G that centralize every factor in $\mathcal{F}_p$. Then $\mathbf{F}_p(G)$ is the largest normal p -nilpotent subgroup of G .

Proof. It's easy to see $\mathbf{F}_p(G)$ is a normal subgroup of G ; we call it F throughout the rest of this proof for ease of notation. Let's first show F is p -nilpotent. By Lemma 2 we have a normal series

$$F_0 = 1 \trianglelefteq F_1 = G_1 \cap F \trianglelefteq \cdots \trianglelefteq F_n = F$$

coming from a chief series of G . Now if p divides $[F_{k+1} : F_k]$, then it must also divide $[G_{k+1} : G_k]$ by the Index Trick. By the definition of F then, it centralizes G_{k+1}/G_k and hence

$$[F, F_{k+1}] \leq F \cap [F, G_{k+1}] \leq F \cap G_k = F_k$$

Thus F_{k+1}/F_k is central in F/F_k , and this implies F is p -nilpotent. To see this, note that refining this normal series to a chief series can only add factors whose orders are divisible by p as subgroups of the already central factors F_{k+1}/F_k .

Now let K be any normal p -nilpotent subgroup of G , and let $G_{k+1}/G_k \in \mathcal{F}_p$. Since G_{k+1} is a minimal normal subgroup of G/G_k , either $K \cap G_{k+1} \leq G_k$ or $G_{k+1} \leq K$. In the first case, since $[K, G_{k+1}] \leq K \cap G_{k+1}$, we have K centralizing the factor. In the second case, we can work in G/G_k with the images $N = G_{k+1}/G_k$ and $K = K/G_k$ by abuse of notation. K is p -nilpotent, and thus $N \leq K$ is too. $|N|$ is divisible by p , and N is p -nilpotent; since N is minimal normal, and thus a direct product of simple groups, it must be an elementary Abelian p -group. Let $M \leq N$ be a minimal normal subgroup of K . Then p divides M and hence by Lemma 4 $M \leq Z(K)$. Since N is minimal normal and $1 < M \leq N \cap Z(K)$, it must be $N \leq Z(K)$. Thus in all cases K centralized the arbitrary factor of $\mathcal{F}_p$. This implies $K \leq \mathbf{F}_p(G)$.

So every normal p -nilpotent subgroup is contained in $\mathbf{F}_p(G)$, and hence it is the unique largest normal p -nilpotent subgroup in G . $\square$

Note that the preceding proposition shows the non-trivial fact that the product of two normal p -nilpotent subgroups is also p -nilpotent: this is because if K, L are two such subgroups, then both are in $\mathbf{F}_p(G)$, and hence so is their product KL , which must also then be p -nilpotent.

Since $\Phi(G)$ is nilpotent, clearly $\Phi(G) \leq \mathbf{F}_p(G)$. Quotients of p -nilpotent groups are p -nilpotent, and that implies

$$\mathbf{F}_p(G)/\Phi(G) \leq \mathbf{F}_p(G/\Phi(G))$$

The next lemma shows this containment is actually an equality.

LEMMA 6: *If K is a normal subgroup of G and $K/\Phi(G)$ is p -nilpotent, then K is p -nilpotent.*

For the proof we first need to establish a slightly different criteria for being p -nilpotent, based on a particular quotient of G . Recall that $\mathbf{O}_{p'}(G)$ is the largest normal subgroup of G with order coprime to p . Its existence is much simpler than for $\mathbf{F}_p(G)$: the product of normal subgroups with order coprime to p is clearly a normal subgroup with order coprime to p .

PROPOSITION 7: *G is p -nilpotent if and only if $G/\mathbf{O}_{p'}(G)$ is a p -group.*

Note that to show $G/\mathbf{O}_{p'}(G)$ is a p -group, it's enough to show the existence of $K \trianglelefteq G$ with $|K|$ coprime to p and $[G : K]$ a power of p . Such a subgroup is called a normal p -complement.

Proof. Let G be p -nilpotent, and let L be the largest normal subgroup of G such that G/L does not have a normal p -complement, and note that $L \neq G$ since the trivial group has a p -complement. Let M/L be a minimal normal subgroup of G/L . If $[M : L]$ is coprime to p , then the maximality of L shows G/M has a normal p -complement C/M , and $[C : L] = [C : M][M : L]$ is coprime to p , while $[G : C]$ is a power of p . This contradicts the choice of L . So we can assume p divides $[M : L]$, and thus by p -nilpotency M/L is central. Let C/M be the normal p -complement in G/M ; then M/L is a Sylow p -subgroup of C/L . Since it is central, the Burnside transfer theorem shows there is a normal p -complement $D/L \leq C/L$. Then D/L is characteristic in C/L and hence normal in G/L . Since it is also a p -complement in G/L , this contradicts the existence of L . Thus G (and all its quotients) have normal p -complements.

Conversely, if $G/\mathbf{O}_{p'}(G)$ is a p -group, then [Lemma 2](#) shows we can build a chief series of G containing $\mathbf{O}_{p'}(G)$. All the factors under $\mathbf{O}_{p'}(G)$ have order coprime to p , so saying G is p -nilpotent is the same as saying that about $G/\mathbf{O}_{p'}(G)$. But that's a p -group, so clearly is p -nilpotent. $\square$

Proof of Lemma 6. Let $P \leq \Phi(G)$ be the Sylow p -subgroup of $\Phi(G)$, normal in G . Since $K/\Phi(G)$ is p -nilpotent, [Proposition 7](#) shows the existence of N normal in K with $[N : \Phi(G)]$ coprime to p and $[K : N]$ a power of p . Thus P is a normal Sylow subgroup of N , and by the Schur-Zassenhaus theorem there exists C in N with $N = CP$ and $C \cap P = \{1\}$. Also by the Schur-Zassenhaus theorem, all complements of P in N are conjugate in N . Since N is normal in G , a Frattini-like argument shows

$$\begin{aligned} G &= N_G(C)N \\ &= N_G(C)CP \\ &= N_G(C)P \\ &= N_G(C) \end{aligned}$$

Here the last equality follows because $P \leq \Phi(G)$. Thus C is normal in G (and so in K), with $|C|$ coprime to p and $[K : C] = |P|[K : N]$ a power of p . Hence by [Proposition 7](#) K is p -nilpotent. $\square$

Now let us define the localized version of supersolvability: a group G is **p -supersolvable** if in the chief series of G , every factor group is either of order p or order coprime to p . Since no factor group can have an order coprime to all primes, and since supersolvable groups are those where each chief factor is prime order, we have

$$G \text{ is supersolvable} \iff G \text{ is } p\text{-supersolvable for all primes } p$$

Just as in [Proposition 7](#) we can detect p -supersolvability by looking at a quotient. In the following, we call a group an A_p group if it is Abelian and if $x^{p-1} = 1$ for all elements x . Clearly subgroups, quotients, and direct products of A_p groups are A_p groups.

PROPOSITION 8: If G is solvable, then it is p -supersolvable if and only if $G/\mathbf{F}_p(G)$ is an A_p group.

Proof. If G is p -supersolvable, then let $F_1, \dots, F_m$ be the factors in $\mathcal{F}_p$. Note that each F_i has order p . The action of G on F_i gives a homomorphism

$$G/C_G(F_i) \hookrightarrow \text{Aut}(F_i) = GL(p)$$

where the group on the right is an A_p group. Thus since $\mathbf{F}_p(G) = \cap C_G(F_i)$ by Proposition 5 we have

$$G/\mathbf{F}_p(G) \hookrightarrow \prod_{i=1}^m GL(p)$$

and so it is an A_p group.

Conversely, assume $G/\mathbf{F}_p(G)$ is an A_p group, and let $N \trianglelefteq G$ be a minimal normal subgroup of G . We induct on $|G|$. If $|N|$ is coprime to p , then by induction G/N is p -supersolvable, since $(G/N)/\mathbf{F}_p(G/N)$ is a quotient of $G/\mathbf{F}_p(G)$, and hence an A_p group. But then Lemma 2 gives a chief series of G built from that of G/N and N , and this shows G is p -supersolvable.

So now assume N is an elementary Abelian p -group of order p^n . Then $G/C_G(N)$, which is a quotient of $G/\mathbf{F}_p(G)$, acts as a subgroup of $GL(p^n)$. Let us rename this subgroup as A since it is an A_p group. Our goal is to show $|N| = p$, since then Lemma 2 gives a chief series for G built from G/N and N ; induction shows G/N is p -supersolvable, and thus $|N| = p$ implies G is too.

Since N is minimal normal, A acts on N irreducibly. Let $R \subset \text{Hom}(N, N)$ be the subring generated by A . $\text{Hom}_R(N, N)$ is a division ring by Schur's Lemma, and since R is commutative, $R \subset \text{Hom}_R(N, N)$. Now the nonzero elements R^* form a multiplicatively closed subset of the group $\text{Hom}(N, N)^*$, and since $\text{Hom}(N, N)^*$ is finite, this implies R^* is an Abelian subgroup; that is, R is a field. (Note this also follows from Wedderburn's theorem.) For $1 \neq n \in N$, Rn is an invariant R -module of N , so by irreducibility $Rn = N$ and since there are no nonzero ideals of R we have $|R| = |N|$, so that $R \cong GF(p^n)$.

Thus A , as a finite subgroup of R^* , is cyclic. Since A is an A_p group, this implies $|A|$ divides $p - 1$, and hence is actually a subgroup of $GF(p)^* \leq R^*$. But then A acts by scalar multiplication of $GF(p)$, and thus leaves every vector subspace (subgroup) of N fixed. Since N is minimal normal, this implies N is a one-dimensional vector space, so that $|N| = p$ as desired. $\square$

We can now finally prove Huppert's Theorem:

Proof of Huppert's Theorem. Let G be a minimal counterexample (MCE) to Huppert's Theorem. By MCE Fact VII $\Phi(G)$ is non-trivial, and so by MCE Fact I $G/\Phi(G)$ is supersolvable; in particular, it is p -supersolvable for all primes p . Since G (and thus $G/\Phi(G)$) is solvable

by [Theorem 1](#), we can use [Proposition 8](#) to conclude that $G/\Phi(G)/\mathbf{F}_p(G/\Phi(G))$ is an A_p group for all primes p . But by the discussion following [Lemma 6](#), we have

$$G/\Phi(G)/\mathbf{F}_p(G/\Phi(G)) = (G/\Phi(G))/(\mathbf{F}_p(G)/\Phi(G)) \cong G/\mathbf{F}_p(G)$$

Thus $G/\mathbf{F}_p(G)$ is an A_p group for all primes p as well. Then again by [Proposition 8](#) G is p -supersolvable for all primes p , and hence G is supersolvable. This shows the MCE G cannot exist. $\square$

Cohomological proof

For this proof, we will find a splitting of a minimal counterexample over a minimal normal subgroup. Note that instead of relying on group cohomology as a black box, we develop the "low-tech" version of $H^1(G)$ and $H^2(G)$ here via crossed morphisms and transversal products. This proof is heavily inspired by [\[Sco87, 9.3.8\]](#) and [\[Isao8, 3.5\]](#).

The main crux of the proof is showing how a splitting of a subgroup leads to a splitting in the main group. We spend the majority of our time here building the theory for this, which as mentioned above is a low-tech retreading of some group cohomology fundamentals.

First, we define a **crossed morphism**. For a group G acting on an abelian group A , a crossed morphism is a map $\phi : G \rightarrow A$ such that

$$\phi(gh) = \phi(g)^h \phi(h)$$

Here we write a^g for the action of g on the element a . The crossed morphisms form the foundation of the first cohomology group $H^1(G, A)$, after quotienting out the **principal** crossed morphisms, which look like $\phi_a(g) = a^{-1}a^g$ and mimic what commutators do. We won't need these later on however; instead, we only need a few facts about crossed morphisms:

LEMMA 9: *Let $\phi : G \rightarrow A$ be a crossed morphism. Then*

1. $\ker(\phi)$ is a subgroup of G .
2. $[G : \ker(\phi)] = |\phi(G)|$.

Proof.

1. Since $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$, it follows that $\phi(1) = 1$. Now suppose $k \in \ker(\phi)$. We have

$$\begin{aligned} 1 &= \phi(k^{-1}k) \\ &= \phi(k^{-1})^k \phi(k) \\ &= \phi(k^{-1})^k \end{aligned}$$

and so conjugating both sides by k^{-1} gives $1 = \phi(k^{-1})$. If x also belongs to $\ker(\phi)$, then $\phi(xk) = 1^k 1 = 1$, so we have shown $\ker(\phi)$ is a subgroup.

2. It will be enough to show that ϕ is constant on cosets of $K = \ker(\phi)$, but takes different values on different cosets. If $x = ky$ for some $k \in K$, then

$$\phi(x) = \phi(k)^y \phi(y) = \phi(y)$$

Conversely, if $\phi(x) = \phi(y)$, then

$$\begin{aligned} \phi(xy^{-1}) &= \phi(x)^{y^{-1}} \phi(y^{-1}) \\ &= \phi(y)^{y^{-1}} \phi(y^{-1}) \\ &= \phi(yy^{-1}) \\ &= 1 \end{aligned}$$

so that $xy^{-1} \in K$.

□

The next concept we introduce is the **difference** for two right transversals of an Abelian normal subgroup A in G . Let S and T be the transversals, and call $s \in S$ equivalent to $t \in T$, written $s \equiv t$, when $As = At$. Then we define

$$d(S, T) = \prod_{s \equiv t} s^{-1}t$$

Clearly each term of the product is in A , and the product is well-defined since A is Abelian. We will need a slightly more general version of this difference for our purposes below. Let H be a subgroup with $A \leq H \leq G$, and suppose now that H **splits** over A . This means that there exists a subgroup $K \leq H$ with $H = AK$ and $A \cap K = \{1\}$. For $h \in H$, write k_h for the unique element of K such that $h^{-1}k_h \in A$. Finally let S and T be two right transversals for H in G . Then we write

$$d_K(S, T) = \prod_{s \equiv t} s^{-1}k_{st^{-1}}t$$

Again, each term of the product is in A and hence it is well-defined. To see each term is in A we have

$$s^{-1}k_{st^{-1}}t = t^{-1}(ts^{-1}k_{st^{-1}})t$$

which is the conjugate of an element in the normal subgroup A . Note that taking $H = A$ gives the previous version of this definition.

LEMMA 10: *The difference defined above satisfies:*

1. $d_K(S, T)d_K(T, U) = d_K(S, U)$.
2. $d_K(Sg, Tg) = d_K(S, T)^g$ for $g \in G$.
3. $d_K(S, Sa) = a^{[G:H]}$ for $a \in A$.

Proof.

1. First note that since K is a subgroup, $k_x k_y = k_{xy}$, because

$$y^{-1} x^{-1} k_x k_y = y^{-1} (x^{-1} k_x) k_y = (x^{-1} k_x) (y^{-1} k_y) \pmod{A}$$

We can thus compute

$$\begin{aligned} d_K(S, T) d_K(T, U) &= \prod_{s \equiv t} s^{-1} k_{st^{-1}t} \prod_{t \equiv u} t^{-1} k_{tu^{-1}u} \\ &= \prod_{\substack{s \equiv t \\ t \equiv u}} s^{-1} k_{st^{-1}t} t t^{-1} k_{tu^{-1}u} \\ &= \prod_{s \equiv u} s^{-1} k_{su^{-1}u} \\ &= d_K(S, U) \end{aligned}$$

2. Note that $s \equiv t$ precisely when $sg \equiv tg$. Direct computation shows

$$\begin{aligned} d_K(Sg, Tg) &= \prod_{sg \equiv tg} g^{-1} s^{-1} k_{sgg^{-1}t^{-1}tg} \\ &= \prod_{s \equiv t} g^{-1} s^{-1} k_{st^{-1}tg} \\ &= g^{-1} \left(\prod_{s \equiv t} s^{-1} k_{st^{-1}t} \right) g \\ &= d_K(S, T)^g \end{aligned}$$

3. If $a \in A$, then $s \equiv sa$ because $a^s \in A \leq H$, and once more direct computation shows

$$\begin{aligned} d_K(S, Sa) &= \prod_{s \in S} s^{-1} k_{sa^{-1}s^{-1}sa} \\ &= \prod_{s \in S} s^{-1} sa \\ &= a^{[G:H]} \end{aligned}$$

where the second equality follows because $k_x = 1$ for any $x \in A$.

□

We can now prove the main cohomological theorem we need.

THEOREM 11 (Gaschütz): *Let A be an abelian normal subgroup of G , with a subgroup H containing A , and $|A|$ coprime to $[G : H]$. Then if H splits over A , G does too.*

In the case $H = A$, this is a special case of the Schur-Zassenhaus theorem.

Proof. Pick a transversal S for H in G and a complement K for A in H , and define the map $\phi : G \rightarrow A$ by

$$\phi(g) = d_K(S, Sg)$$

The key fact is that ϕ is a crossed morphism. To see this we use [Lemma 10](#) to find

$$d_K(S, Sgh) = d_K(S, Sh)d_K(Sh, Sgh) = d_K(S, Sh)d_K(S, Sg)^h$$

and thus $\phi(gh) = \phi(g)^h\phi(h)$ (here we're relying on A being Abelian to reorder that product). Let $L = \ker(\phi)$. Now by the same lemma $\phi(a) = a^{[G:H]}$ for all $a \in A$, and since this is coprime to $|A|$ we see that $A \cap L = \{1\}$ and ϕ is surjective. But [Lemma 9](#) then implies that $[G : L] = |A|$ and so $AL = G$ and L is a complement for A in G . $\square$

In terms of group cohomology, this theorem is a statement about the map $H^2(G, A) \rightarrow H^2(H, A)$ and the fact extensions of Abelian groups are classified by second cohomology, the split ones having the zero class.

Proof of Huppert's Theorem. Let G be an MCE for [Huppert's Theorem](#). By [Theorem 1](#) G has a normal Sylow subgroup P . Suppose first that P is non-Abelian. Then $Z(P) \neq P$ and both are normal subgroups of G , hence by [MCE Fact IV](#) we can find $K \leq P$ normal in G with $[K : Z(P)] = p$. Note this since $K/Z(P)$ is a minimal normal subgroup of the p -group $P/Z(P)$, we must have $[P, K] \leq Z(P)$. Similarly, $C_P(K) \neq P$ and so we again can get $L \leq P$ normal in G , with $[L : C_P(K)] = p$. Let $k \in K \setminus Z(P)$ and $l \in L \setminus C_P(K)$. Then for any $z \in Z(P)$ and $c \in C_P(K)$ we have (with r, s integers)

$$\begin{aligned} [l^r c, k^s z] &= [l^r, k^s z]^c [c, k^s z] \\ &= [l^r, k^s z]^c & c \in C_P(K) \\ &= [l^r, z]^c [l^r, k^s]^{cz} \\ &= [l^r, k^s]^{cz} & z \in Z(P) \\ &= [l^r, k^s] & [P, K] \leq Z(P) \end{aligned}$$

And using $[P, K] \leq Z(P)$ repeatedly, that last commutator is equal to $[l, k]^{rs}$. This implies $[L, K]$ is cyclic, generated by $[l, k]$; it is non-trivial since $L \neq C_P(K)$. The unique subgroup of order p in $[L, K]$ is thus normal in G , contradicting [MCE Fact II](#).

Thus we assume P is Abelian. Let K be the subgroup of P of elements of order dividing p . If $P \neq K$ then again by [MCE Fact IV](#) we have an $L \leq P$ normal in G with $[L : K] = p$. But then the p th powers of elements in L is a characteristic subgroup of L of order p . This subgroup is normal in G and that contradicts [MCE Fact II](#). So $P = K$ is elementary Abelian.

Let N be a minimal normal subgroup of G contained in P . Then since P is elementary Abelian, there is a subgroup K of P such that $P = KN$ and $K \cap N = \{1\}$. Since N is a p -group and $[G : P]$ is coprime to p , [Theorem 11](#) shows that there exists a subgroup $M \leq G$ that complements N , so that $G = MN$ and $M \cap N = \{1\}$. This contradicts [MCE Fact VI](#) and shows G does not exist. $\square$

Linear proof

The linear proof of [Huppert's Theorem](#) is in some sense easier than the other two, since it doesn't require much preamble. The main idea is to treat G as acting on a vector space. The clever part is to not use a minimal normal subgroup, but instead a slightly larger group; this allows an application of Maschke's theorem to reach the final contradiction. This proof is slightly modified from [\[Hal99, 10.5.8\]](#).

Proof of Huppert's Theorem. Let G be a minimal counterexample, and N a minimal normal subgroup of G with order p^a for some $a > 1$ by [MCE Fact III](#). Applying [MCE Fact IV](#) we get a normal subgroup $V \trianglelefteq G$ with $[V : N]$ prime. If $[V : N] = q \neq p$, then let Q be the Sylow q -subgroup of V , which has order q . By the Frattini argument $G = N_G(Q)V = N_G(Q)N$, and so by [MCE Fact VI](#) $G = N_G(Q)$ and Q is normal in G . But this contradicts [MCE Fact II](#).

So we have $[V : N] = p$ and V is a p -group. Since $[V : V'] \geq p^2$, this would imply $V' \trianglelefteq G$ is a proper normal subgroup of N ; thus $V' = 1$ and V is Abelian. Now N is of course elementary Abelian; if V were not then the subgroup of p th powers in V would of order $[V : N] = p$ and would be normal in G , contradicting [MCE Fact II](#). So V is elementary Abelian.

Thus we have G acting on the vector space V over $GF(p)$, and this gives a homomorphism $G/C_G(V) \hookrightarrow GL(p^{a+1})$. To ease notation, we will write $\bar{H}$ for the image of subgroups containing $C_G(V)$ in $GL(p^{a+1})$. Note that $V \leq C_G(V) \neq G$ since otherwise any subgroup of order p would be normal in G , contradicting [MCE Fact II](#). Let $\bar{K} \trianglelefteq \bar{G}$ be the subgroup of scalar matrices, which is central in $\bar{G}$, and note that $|\bar{K}|$ is coprime to p . If $K = G$, then every vector subspace of V would be normal, again contradicting [MCE Fact II](#). Thus by [MCE Fact IV](#) there is a normal subgroup $\bar{M} \leq \bar{G}$ with $[\bar{M} : \bar{K}]$ prime.

If $[\bar{M} : \bar{K}] = p$, then $\bar{M} = \bar{K}\bar{P}$ for $\bar{P}$ a subgroup of order p in $\bar{M}$. Since $\bar{K}$ is central of order coprime to p , $\bar{P}$ is a normal Sylow p -subgroup of $\bar{M}$, and hence P is normal in G . Now the number of elements of N fixed by $\bar{P}$ is divisible by p by the orbit-stabilizer theorem, and hence $N \cap Z(P)$ is a non-trivial normal subgroup of G ; the minimality of N forces $N \leq Z(P)$ and so $\bar{P}$ fixes N pointwise. Let X be a matrix representing the action of a generator $\bar{x}$ of $\bar{P}$ on V . Since X has order p , its determinant is 1 (mod p). Let B be a basis for N and $v \in V$ an element that extends this basis to V . Then X fixes B by the above and in the basis $B \cup \{v\}$ it looks like

$$X = \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & r \end{pmatrix}$$

where X sends h to $h^r n$ for an integer r and $n \in N$. Since $\det(X) = 1$ we must have $r = 1$ and thus X sends h to hn ; $n \neq 1$ because $x \notin C_G(V)$. But then back in G we have $[x, h] = n^{-1}$ and so we see that $[P, V] = \langle n \rangle$ is a normal subgroup of order p in G , contradicting [MCE Fact II](#).

Bibliography

So finally we are in the last case, where $[\overline{M} : \overline{K}] \neq p$. But then $|\overline{M}|$ is coprime to p . Since N is a vector subspace fixed by $\overline{M}$, Maschke's theorem implies the existence of a complement $C \leq V$ also fixed by $\overline{M}$, with $|C| = p$ and $C \cap N = \{1\}$. Let H be the subgroup of G generated by all the conjugates of C . H is normal in G , and $H \neq C$ by [MCE Fact II](#). Thus $|H| > p$ and $H \leq V$, so $H \cap N > 1$ and thus $N \leq H$. Since $C \leq H$ is not contained in N the only possibility is $H = V$. Since all the conjugates of C intersect trivially and are normal in V , we can thus write

$$V = C_1 \oplus C_2 \oplus \cdots \oplus C_{a+1}$$

for some conjugates $\{C_i\}$ of C . In the basis that comes from this decomposition, every element $x \in \overline{M}$ acts as a diagonal matrix X since it fixes each C_i . But for $i \neq j$, $C_i C_j \cap N > 1$, and this one-dimensional subspace is also fixed by x ; this is only possible if the diagonal entries in X for C_i and C_j are equal. Thus X is a scalar matrix, and $x \in K$. Since x was arbitrary, this shows $M = K$ which contradicts that $[M : K] > 1$, and thus G does not exist. $\square$

Bibliography

- Hall, M. *The Theory of Groups*. AMS Chelsea Publishing Series. AMS Chelsea Pub., 1999. ISBN: 9780821819678. URL: <https://books.google.com/books?id=oyxnWF9ssI8C>.
- Huppert, B. *Endliche Gruppen*. Finite groups / B. Huppert, N. Blackburn. Springer, 1983. URL: <https://books.google.com/books?id=wBDVzAEACAAJ>.
- Isaacs, I.M. *Finite Group Theory*. Graduate studies in mathematics. American Mathematical Society, 2008. ISBN: 9780821843444. URL: <https://books.google.com/books?id=E9kOCgAAQBAJ>.
- Scott, W.R. *Group Theory*. Dover Books on Mathematics. Dover Publications, 1987. ISBN: 9780486653778. URL: <https://books.google.com/books?id=kt4o5ZTwH4wC>.