Group Theory

Thomas Browning

November 2016

Let G be a group and let H be a subgroup of G. For each $g \in N_G(H)$, we have the conjugation automorphism of H given by $h \mapsto g^{-1}hg$. This gives a homomorphism $N_G(H) \to \mathrm{Aut}(H)$ with kernel $C_G(H)$. By the first isomorphism theorem for groups, $N_G(H)/C_G(H)$ embeds as a subgroup of $\mathrm{Aut}(H)$. In the case that $H = G$, this states that $G/Z(G)$ embeds as a subgroup of $\mathrm{Aut}(G)$.

Theorem 1. *Let G be a finite group. If $\mathrm{Aut}(G)$ is cyclic then G is cyclic.*

Proof. This proof will repeatedly use the fact that a subgroup of a cyclic group is cyclic. First note that $G/Z(G)$ is cyclic. If $x \in G$ is a representative for a coset of $Z(G)$ that generates $G/Z(G)$ then every element of G is of the form $x^k z$ for some integer k and some $z \in Z(G)$. However, all elements of this form commute. This shows that G is abelian. If $p \geq 3$ is a prime dividing G and if the direct product decomposition of G contains a factor isomorphic to $C_{p^a} \times C_{p^b}$ then $\mathrm{Aut}(G)$ contains $\mathrm{Aut}(C_{p^a}) \times \mathrm{Aut}(C_{p^b})$ which contains $C_{p-1} \times C_{p-1}$ which is not cyclic. If the direct product decomposition of G contains a factor isomorphic to C_{2^k} then $\mathrm{Aut}(G)$ contains $\mathrm{Aut}(C_{2^k})$ which is not cyclic for $k \geq 3$. If the direct product decomposition of G contains a factor isomorphic to $C_2 \times C_2$ or to $C_2 \times C_4$ or to $C_4 \times C_4$ then $\mathrm{Aut}(G)$ contains $\mathrm{Aut}(C_2 \times C_2)$ or $\mathrm{Aut}(C_2 \times C_4)$ or $\mathrm{Aut}(C_4 \times C_4)$, none of which are cyclic. We have shown that for each prime p, the direct product decomposition of G contains at most one factor isomorphic to C_{p^k} for some k. Then the classification of finite abelian groups gives that G is cyclic. ☐

Burnside's normal p-complement states that if G is a finite group and if P is a Sylow p-subgroup of G and if $C_G(P) = N_G(P)$ then G contains a normal p-complement (a normal subgroup of order $|G|/|P|$).

Theorem 2. *Let G be a finite group, let p be the smallest prime divisor of the order of G, and suppose that Sylow p-subgroups of G are cyclic. Then G contains a normal p-complement.*

Proof. Let P be a Sylow p-subgroup of G. Note that the order of $\mathrm{Aut}(P)$ is given by $p-1$ times a power of p. In particular, $|N_G(P)/C_G(P)|$ divides $p-1$ times a power of p. However, the minimality of p gives that $|N_G(P)/C_G(P)|$ is coprime to $p-1$. Also, the fact that P is abelian gives that $|N_G(P)/C_G(P)|$ is coprime to p. Then $|N_G(P)/C_G(P)| = 1$ and Burnside's normal p-complement theorem applies. ☐

A slight refinement of the proof of theorem 1 gives the following result.

Theorem 3. *Let G be a finite group, let p be the smallest prime divisor of the order of G, suppose that p^3 does not divide the order of G, and suppose that G does not have a normal p-complement. Then 12 divides the order of G and all involutions of G are conjugate.*

Proof. Let P be a Sylow p-subgroup of G. By theorem 1, P is not cyclic so we must have that $P \cong C_p \times C_p$. Then $\mathrm{Aut}(P) \cong \mathrm{GL}_2(\mathbb{F}_p)$ so $|\mathrm{Aut}(P)| = p(p-1)^2(p+1)$. The same argument as in the proof of theorem 1 gives that $|N_G(P)/C_G(P)|$ is coprime to $p-1$ and to p. Also, if $p \neq 2$ then $p+1$ is composite and factors as a product of primes less than p in which case $|N_G(P)/C_G(P)|$ would also be coprime to $p+1$. By Burnside's normal p-complement theorem, we must have that $p = 2$ and that $|N_G(P)/C_G(P)| = 3$. Note that $\mathrm{Aut}(P) \cong S_3$ is the permutation group on the three involutions of P. The image of $N_G(P)/C_G(P)$ in $\mathrm{Aut}(P)$ has order 3 so $N_G(P)$ acts transitively on the three involutions of P. Then Sylow's theorems give that G acts transitively on the involutions of G. ☐

If G is a finite simple group then theorem 3 states that either the smallest prime divisor of the order of G divides the order of G to the third power or that 12 divides the order of G. When combined with Burnside's $p^a q^b$ theorem, this implies that 60 and 84 are the only potential orders less than 120 for a finite simple group. However, Sylow's theorems show that a group of order 84 has a normal Sylow 7-subgroup.

There are other results that involve the smallest prime dividing the order of a finite group.

Theorem 4. *Let G be a finite group and let p be the smallest prime divisor of the order of G. Every normal subgroup of G of order p is central and every subgroup of G of index p is normal.*

Proof. Let H be a normal subgroup of G of order p. For each $h \in H$, the order of the conjugacy class of h is strictly smaller than p but is a divisor of G. Then for each $h \in H$, the conjugacy class of h has order 1 so $h \in Z(G)$. Now let H be a subgroup of G of index p. Letting G act on the left cosets of H by left-multiplication gives a homomorphism $G \to S_p$ with kernel K contained in H. The first isomorphism theorem for groups gives that G/K embeds as a subgroup of S_p. In particular $[G : K]$ divides both $p!$ and G. By the minimality of p, $[G : K]$ divides p. However, $[G : K] = [G : H][H : K]$ so $[H : K] = 1$. Then $H = K$ which shows that H is a normal subgroup of G. □

Similar results hold even when G is not finite.

Theorem 5. *Let G be a group. Every subgroup of G of index 2 is normal. If G contains no subgroup of index 2 then every subgroup of index 3 is normal. If G contains a subgroup of index 4 then G contains a subgroup of index 2 or of index 3.*

Proof. Let H be a subgroup of G of index 2. Then $gH = H = Hg$ if $g \in H$ and $gH = (G \setminus H) = Hg$ if $g \notin H$. This shows that H is a normal subgroup of G. Now let H be a subgroup of G of index 3 and suppose that G contains no subgroup of index 2. As in the proof of theorem 4, we obtain a homomorphism $G \to S_3$ with kernel K contained in H. The composition $G \to S_3 \to \{\pm 1\}$ must be trivial so we obtain a homomorphism $G \to A_3$ with kernel K contained in H. Then $[G : K]$ divides 3 so the same argument as in the proof of theorem 4 gives that H is a normal subgroup of G. Now let H be a subgroup of G of index 4 and suppose that G contains no subgroup of index 2 or of index 3. As in the proof of theorem 4, we obtain a homomorphism $G \to S_4$ with kernel K contained in H. The composition $G \to S_4 \to \{\pm 1\}$ must be trivial so we obtain a homomorphism $G \to A_4$ with kernel K contained in H. The composition $G \to A_4 \to C_3$ must also be trivial so we obtain a homomorphism $G \to C_2 \times C_2$ with kernel K contained in H. Then $[G : K]$ divides 4 so the same argument as in the proof of theorem 4 gives that H is a normal subgroup of G. However, then the correspondence theorem gives that G contains a subgroup of index 2. □