The following are my personal notes for a course done with Professor Isaacs at the University of Wisconsin Madison in the spring of 2010. The notes closely parallel his book, *Finite Group Theory*.

1 01-19-10

We begin with a review of a few important concepts from 741, or basic group theory. We begin with a review of group actions.

1.1 Group Actions

Group actions serve two main purposes. One, they can help in finding subgroups, and second, they can help count things. To see examples of these two principles, we begin with something a little more formal.

Definition 1.1. Given a group G and a set Ω such that $\alpha \cdot g \in \Omega$ for all $\alpha \in \Omega$ and $g \in G$, we say that G *acts* on Ω if for all $\alpha \in \Omega$ and $x, y \in G$ we have $\alpha \cdot 1 = \alpha$ and $(\alpha \cdot x) \cdot y = \alpha \cdot xy$.

Equivalently, we have a homomorphism $\theta : G \to \mathrm{Sym}(\Omega)$, where $\alpha \cdot g = \alpha\theta(g)$. We say that θ is the *permutation representation*.

Definition 1.2. Given $\alpha \in \Omega$, we write $G_\alpha := \{g \in G | \alpha \cdot g = \alpha\}$. This is called the *stabilizer* of α.

It is a fact, although we do not pause to prove it, that the stabilizer of α is a subgroup of G for all $\alpha \in \Omega$.

Definition 1.3. $\bigcap_{\alpha \in \Omega} G_\alpha$ is called the *kernel of the action*.

Note that the kernel of the action is exactly the kernel of the homomorphism θ as described above, and as such, the kernel of the action is a *normal* subgroup of G.

As a brief aside, we make a few comments. Whenever we write G, we operate under the hypothesis that G is a finite group unless otherwise noted. Likewise, when we write $H \subseteq G$, it is automatically implied that H is a subgroup of G. If we do not mean for this to be the assumption, we will also make a comment about this, and hopefully we we call the subset X in order to avoid any possible confusion.

We now continue with a basic fact. By the first homomorphism theorem, we know that $G/\ker(\theta) \cong \mathrm{Im}(\theta)$. Thus $\theta(G)$ is isomorphically embedded in $\mathrm{Sym}(\Omega)$, which has size $|\mathrm{Sym}(\Omega)| = |\Omega|!$.

We now apply this theory with a very important example.

Example 1.1. Let $H \subseteq G$ and let $\Omega = \{Hx | x \in G\}$. Let G act on Ω by right multiplication, where $(Hx) \cdot g = Hxg$. We wish to determine both the stabilizer and kernel of this action. First, we consider G_{Hx}. Now G_{Hx} is the set of $g \in G$

such that $Hxg = Hx$, which we know from our knowledge of cosets holds if and only if $xg \in Hx$. Multiplying on the left by x^{-1}, we see that $xg \in Hx$ if and only if $g \in x^{-1}Hx = H^x$. Therefore $G_{Hx} = H^x$.

Now what is the kernel of the action? By definition, it is $\bigcap_{x \in G} H^x$, which is defined to be the *core of H in G*, written $\text{core}_G(H)$.

Suppose that $|G : H| = n$ in the previous example. Then $|\Omega| = n$ and $G/\text{core}G(H) \subseteq S_n$. [Here, we mean that the quotient is isomorphic to a subset of S_n, but I can't find this symbol in LaTeX]. In particular, LaGrange's theorem implies then that $|G : \text{core}_G(H)| \Big| n!$.

We now prove our first theorem, although it follows fairly directly from this observation.

Theorem 1.1. Let $H \subseteq G$ with $|G : H| = n$. Assume that $n > 1$. If $|G|$ does not divide $n!$, then G is not simple.

Proof. Let $K = \text{core}_G(H)$. We know that $K \lhd G$. It suffices to show that K is not G and K is not trivial. Since $K \subseteq H < G$, we know that $K \neq G$. Therefore we must show that $K \neq 1$. Yet if $K = 1$, then by our previous observation, we must have $|G : K| = |G|$ dividing $n!$, which contradicts our assumption. Thus $K \neq 1$, and G is not simple. □

The above theorem is what we sometimes refer to casually as a good theorem, as it not only helps us to find subgroups of a group, but it helps us find *normal* subgroups of a given group and therefore determine that the group cannot possibly be simple. This shows us how we use group actions to find subgroups. We now change topics and see how we can use group actions to count within groups.

Definition 1.4. Suppose G acts on Ω and that $\alpha \in \Omega$. We write $\mathcal{O}_\alpha := \{\alpha \cdot g | g \in G\}$ for the *orbit* of α.

Since $\alpha \in \mathcal{O}_\alpha$ by our first property of actions, we know that $\Omega = \bigcup_{\alpha \in \Omega} \mathcal{O}_\alpha$. It is an easy exercise (I leave space in the notes) to show that if $\beta \in \mathcal{O}_\alpha$, then in fact $\mathcal{O}_\alpha = \mathcal{O}_\beta$. That is, distinct orbits are disjoint. Thus Ω is actually a *disjoint* union of orbits.

The final theorem which enables us to count, and we will see applications of it later on, is the Fundamental Counting Principle, sometimes shortened to the FCP.

Theorem 1.2 (FCP)**.** Let $\mathcal{O}$ be an orbit and let $\alpha \in \mathcal{O}$. Then $|\mathcal{O}| = |G : G_\alpha|$. In fact, there exists a bijection from $\mathcal{O} \to \{G_\alpha x | x \in G\}$ via the map $\beta \mapsto \{g \in G | \alpha \cdot g = \beta\}$.

Proof. In proving that the above map is a bijection, one proves the theorem. See Isaacs' *Algebra: A Graduate Course* for full details. □

1.2 Sylow Theory

We now begin a brief review of Sylow theory.

Definition 1.5. Given a prime p and a group G, write $|G| = p^a m$, where $a \geq 0$ and p does not divide m. A subgroup $P \subseteq G$ is a *Sylow p-subgroup* if $|P| = p^a$.

We begin proving the three Sylow theorems with the first- that Sylow subgroups always exist.

Theorem 1.3 (Sylow-E)**.** $\mathrm{Syl}_p(G) \neq \emptyset$, where $\mathrm{Syl}_p(G)$ is the set of all Sylow p-subgroups of G.

We note that if $P \subseteq G$ is a subgroup, then $P \in \mathrm{Syl}_p(G)$ if and only if $|P| = p^a$ for some $a \in \mathbb{Z}$ and $|G : P|$ is p'. The notation of a number being p' means that it is coprime to p.

Proof. Before we prove the Sylow-E theorem, we need a number theoretic lemma.

Lemma 1.1. $\binom{p^a m}{p} \equiv m \pmod{p^a}$ where p is a prime.

Proof. From the binomial theorem, we know that $\binom{p^a m}{p^a}$ is the coefficient of the x^{p^a} term in the expansion of $(1+x)^{p^a m}$. Next, observe that $(1+x)^p \equiv 1 + x^p \pmod{p}$, as all of the middle terms have coefficients which are divisible by p. Thus $(1+x)^{p^2} \equiv (1+x^p)^p \equiv 1 + x^{p^2} \pmod{p}$, and continuing in this way we conclude that $(1+x)^{p^a} \equiv 1 + x^{p^a} \pmod{p}$; so $(1+x)^{p^a m} \equiv (1+x^{p^a})^m \pmod{p}$. But the coefficient of x^{p^a} on the right is exactly m[expand it out] and by our first remark we know the coefficient of x^{p^a} on the left to be exactly $\binom{p^a m}{p^a}$. As these two polynomials are congruent when read modulo p, we conclude that $\binom{p^a m}{p^a} \equiv m \pmod{p}$. □

We now continue with the proof of the Sylow-E theorem. The proof that follows is due to the German mathematician Wielandt, who has been called "the great trivializer".

Let Ω be the set of all *subsets* $X \subseteq G$ such that $|X| = p^a$, where $|G| = p^a m$ and p does not divide m. Let G act on Ω by right multiplication, so $X \cdot g = Xg$. [It is easy to check that this is indeed an action]. Note that $Xg \in \Omega$, since right multiplication is clearly injective. Note further that $|\Omega| = \binom{p^a m}{p^a}$ since we have $p^a m$ elements and we may choose any p^a of them to form a subset. By the lemma, $|\Omega| \equiv m \not\equiv 0 \pmod{p}$ since p does not divide m; hence p does not divide $|\Omega|$. Let $\mathcal{O}$ be an orbit with $|\mathcal{O}|$ not divisible by p. Orbits are nonempty,

so let $X \in \mathcal{O}$. By the FCP, we know that $|\mathcal{O}| = |G : G_X| = |G|/|G_X|$. As $|\mathcal{O}|$ is not divisible by p, we conclude that $p^a \Big| |G_X|$ and therefore $p^a \leq |G_X|$. As G_X is a subgroup of G, if we can now show that $p^a \geq |G_X|$, we will have found a Sylow p-subgroup of G, which is what we want.

To see that $p^a \geq |G_X|$,we take $x \in X$ and let $g \in G_X$. Now $xg \in Xg = X$ as g is in the stabilizer of X. So $xG_X \subseteq X$. Hence $|G_X| = |xG_X| \leq |X| = p^a$ as multiplication by x in injective. Therefore $|G_X| = p^a$ by our above comments and G_X is a Sylow p-subgroup.

□

Our next theorem allows us to derive the Sylow-D theorem as a corollary. As an interesting historical aside, we know that the D stands for "development", since every p-subgroup of a group G can be *developed* into a Sylow subgroup.

Theorem 1.4 (Sylow-D)**.** Let $P \in \mathrm{Syl}_p(G)$ and let $Q \subseteq G$ be a p-group. Then $Q \subseteq P^g$ for some $g \in G$.

Proof. Let $\Omega = \{Px | x \in G\}$. By the definition of index, $|\Omega| = |G : P|$, and this quantity is p'. Now Q acts on Ω by right multiplication. As Q partitions Ω into orbits, the FCP tells us that all of these orbit sizes must divide $|Q|$, which is a p-power. On the other hand, the sum of the orbit sizes is equal to $|\Omega|$, which is not divisible by p, and therefore there exists an orbit $\mathcal{O}$ such that $|\mathcal{O}|$ is not divisible by p; hence $|\mathcal{O}| = 1$. Hence $\mathcal{O}$ is of the form $\{Pg\}$ for some $g \in G$. So Q must stabilize Pg and thus $Q \subseteq G_{Pg} = P^g$. □

2 01-21-10

2.1 Sylow Theory, Continued

This section contains a few odds and ends which somewhat relate to Sylow theory. We begin with a generalization of a Sylow subgroup.

Definition 2.1. Let π be a set of primes. A subgroup $H \subseteq G$ is a *Hall π-subgroup* of G if $|H|$ is a π-number and $|G : H|$ is a π'-number.

In the previous definition, we have been a little vague. A number n is said to be a π-number if the only primes in the prime factorization of n lie in the set π. A number n is a π'-number if none of the primes in the prime factorization of n lie in π.

It is an interesting fact that unlike Sylow p-subgroups, Hall π-subgroups do NOT always exist, although it is a fact that we will prove later that Hall π-subgroups exist when the group G is solvable. To see that Hall π-subgroups do not always exist, we provide an example.

Example 2.1. Say $G = A^5$, the alternating group on 5 letters. Then $|G| = 60 = 2^2 \cdot 3 \cdot 5$. Let $\pi = \{3, 5\}$. If $H \subseteq G$ is a Hall π-subgroup, then we must have $|H| = 15$ and $|G : H| = 4$. As $|G|$ does not divide 4!, the existence of such

a subgroup H would violate the $n!$-theorem; hence H cannot exist and Hall π-subgroups need not always exist.

Last time, we showed that if $P \in \mathrm{Syl}_p(G)$ and $Q \subseteq G$ was a p-group, then there exists $g \in G$ for which $Q \subseteq P^g$. We derived the Sylow-D theorem from this theorem. We note here that we may also derive the Sylow-C theorem as a corollary of this fact. The C, of course, stands for conjugacy.

Corollary 2.1 (Sylow-C)**.** If $P, Q \in \mathrm{Syl}_p(G)$ then $Q = p^g$ for some $g \in G$.

Proof. As Q is a p-group, we know that $Q \subseteq P^g$ for some $g \in G$. Yet $|Q| = |P^g|$ and as G is finite, we have equality. □

We now sate a very important theorem and a useful qual fact: the Frattini argument.

Theorem 2.1 (Frattini Argument)**.** Let $N \lhd G$ and let $P \in \mathrm{Syl}_p(G)$. Then $G = \mathbf{N}_G(P)N$.

Proof. Let $g \in G$. Since $P \subseteq N$, we know $P^g \subseteq N^g = N$ since $N \lhd G$, so $P^g \subseteq N$. As $|P| = |P^g|$, we know that $P^g \in \mathrm{Syl}_p(N)$. By the Sylow-C theorem, we know that there exists $n \in N$ such that $(P^g)^n = P$, or equivalently, we have $P^{gn} = P$. By definition, this places $gn \in \mathbf{N}_G(P)$. Multiplying both sides on the right by n^{-1}, we have $g \in \mathbf{N_G(P)}n^{-1} \subseteq \mathbf{N}_G(P)N$. As $g \in G$ was arbitrary, we have $G \subseteq \mathbf{N}_G(P)N$, which implies equality. □

In order to see an example of the Frattini argument at work, we make one more quick (but useful) definition.

Definition 2.2. $\Phi(G)$, the *Frattini subgroup* of G, is the intersection of all of the maximal subgroups of G.

Theorem 2.2. Let $F = \Phi(G)$ and let $P \in \mathrm{Syl}_p(F)$. Then $P \lhd G$.

As a quick remark before beginning the proof, we note that it would be enough to show that a Sylow p-subgroup of F is normal in F; if P is normal in F, then it is THE Sylow p-subgroup of F and is hence characteristic in F. as $F \lhd G$, it would follow that $P \lhd G$. We will not proceed in this way, but it is a good fact to note. Additionally, note that another way to state this theorem is that the Frattini subgroup of any G is nilpotent, as an equivalent definition for a group to be nilpotent is to have all of its Sylow p-subgroups normal.

Proof. Let $G = \mathbf{N}_G(P)F$. by the Frattini argument since $F \lhd G$. To show that $P \lhd G$, we wish to show that $\mathbf{N}_G(P) = G$. If $\mathbf{N}_G(P) < G$, then $\mathbf{N}_G(P) \subseteq M$ for some M maximal in G. So $G = \mathbf{N}_G(P)F \subseteq MF$. Yet $F \subseteq M$ for all maximal subgroups M, so $MF = M$ and we have $G = M$. But this is a contradiction since $M < G$ by definition. □

We now introduce a bit of notation. Fix a prime p and write $|G| = p^a m$, where p does not divide m. We write $n_p(G) = |\mathrm{Syl}_p(G)|$. Using the FCP and the Sylow-C theorem, we can conclude that $n_p(G) = |G : \mathbf{N}_G(P)|$ for $P \in \mathrm{Syl}_p(G)$[Let G act on $\Omega = \mathrm{Syl}_p(G)$ by conjugation. Consider orbits and stabilizers]. As $P \subseteq \mathbf{N}_G(P)$ and $|G : \mathbf{N}_G(P)|$ divides $|G : P|$, we can conclude that $|G : \mathbf{N}_G(P)|$ divides m and is therefore coprime to p.

From here, we next state a theorem called the Sylow counting theorem, which is very useful theorem for proving non-simplicity. To prove the Sylow counting theorem, we will prove a more general form of the Sylow counting theorem which is sometimes more useful when proving non-simplicity. We will also give an example of how to use this most general form, to motivate its use.

Theorem 2.3 (Sylow Counting)**.** $n_p(G) \equiv 1 \pmod{p}$.

Theorem 2.4. Suppose $n_p(G) \not\equiv 1 \pmod{p^e}$. Then there exist $P, Q \in \mathrm{Syl}_p(G)$ with $P \neq Q$ and $|P : P \cap Q| < p^e$.

This more general form of the Sylow counting theorem is slightly bothersome for two obvious reasons. The first, that there is somehow an asymmetry with indices, can be resolved easily. We note that $|P : P \cap Q| = |Q : P \cap Q|$ since $|P : P \cap Q| = |P|/|P \cap Q| = |Q|/|P \cap Q|$ since $|P| = |Q|$, so the theorem IS actually symmetric. The second reason, that the theorem is stated negatively, is also avoidable, but the statement of the theorem then becomes more convoluted. In practice, we will often use the contrapositive of this theorem.

We first assume the validity of the more general form of this theorem and prove the Sylow counting theorem as a corollary.

Proof. Suppose for contradiction that $n_p(G) \not\equiv 1 \pmod{p}$. Then apply this more general theorem with $e = 1$. We then know that there exists $P, Q \in \mathrm{Syl}_p(G)$ with $P \neq Q$ and $|P : P \cap Q| < p$. Since $|P : P \cap Q|$ must be a p-power as P is a p-group, we conclude that $|P : P \cap Q| = 1$, which is a contradiction as this implies that $P \cap Q = P$ and thus $P \subseteq Q$ and $P = Q$. □

We now give an example of how to use this more general form of the Sylow counting theorem. This type of argument is very typically seen on qualifying exams.

Example 2.2. If $|G| = 2^6 \cdot 7^3$ then G is not simple.

Proof. we know that $n_7(G)$ divides 2^6 and therefore $n_7 \in \{1, 2, 4, 8, 16, 32, 64\}$. Using the Sylow-counting theorem, we know that $n_7 \equiv 1 \pmod{7}$, so actually we must have $n_7 \in \{1, 8, 64\}$. If $n_7 = 1$, then G has a normal Sylow 7-subgroup and G is not simple. We may therefore assume that n_7 is either 8 or 64, neither of which is congruent to 1 modulo $49 = 7^2$. Using the more general version of this theorem, we can conclude that there exist $P, Q \in \mathrm{Syl}_7(G)$ with $P \neq Q$ such that $|P : P \cap Q| < 7^2$ and $|P : P \cap Q| > 1$ since P and Q are distinct Sylow 7-subgroups. Thus $|P : P \cap Q| = 7$. Let $D = P \cap Q$. hen $|P : D| = |Q : D| = 7$. Now $D \lhd P$ and $D \lhd Q$ since 7 is the smallest prime divisor of $|P|$(or alternatively,

because normalizers grow in p-groups). Let $N = \mathbf{N}_G(D)$. We know that both $P, Q \subseteq N$ and therefore $7^3 \Big| |N|$. More importantly, we know that $n_7(N) > 1$ as both $P, Q \subseteq N$ and P and Q are both Sylow 7-subgroups of N. If we again apply the Sylow counting theorem, we know that $n_7(N)$ must be either 8 or 64. Hence $8 \Big| |N|$, making $|N| \geq 7^3 \cdot 2^3$ and $|G : N| \leq 8$. If $|G : N| = 1$, then $D \lhd G$ and G is not simple, so we assume that $1 < |G : N| \leq 8$ and apply the $n!$-theorem. $|G|$ does not divide $|G : N|$ since $|G|$ is divisible by 7^3 and 8! (or any smaller factorial, for that matter) is not divisible by 7^3. In any case, G is seen not to be simple. □

We now state an easy lemma that we will need for the proof of the general version of the Sylow counting theorem.

Lemma 2.1. Let $P \in \mathrm{Syl}_p(G)$ and let $Q \subseteq \mathbf{N}_G(P)$ be a p-group. Then $Q \subseteq P$.

Proof. Let $N = \mathbf{N}_G(P)$. Since $P \in \mathrm{Syl}_p(N)$ and $Q \subseteq N$, we know that there exists $n \in N$ such that $Q \subseteq P^n$. Yet $P^n = P$ as $P \lhd N$, hence $Q \subseteq P$. □

We proceed to prove the theorem next time.

3 01-26-10

We prove the generalized Sylow theorem.

Theorem 3.1. Assume that $n_p(G) \not\equiv 1 \pmod{p^e}$. Then there exists $P, Q \in \mathrm{Syl}_p(G)$ with $P \neq Q$ and $|P : P \cap Q| < p^e$.

Proof. Let $Q \in \mathrm{Syl}_p(G)$, and let Q act by conjugation on $\Omega = \mathrm{Syl}_p(G)$. One orbit is $\{Q\}$ as Q normalizes itself. So $|\mathrm{Syl}_p(G)| = 1 + \sum_i |\mathcal{O}_i|$, where the $\mathcal{O}_i$ are the orbits other than $\{Q\}$. By hypothesis, p^e does not divide $\sum_i |\mathcal{O}_i|$. In particular, this means that p^e cannot divide $|\mathcal{O}_i|$ for all of the $\mathcal{O}_i$; that is, there exists an orbit $\mathcal{O}$ such that p^e does not divide $|\mathcal{O}|$. Let $P \in \mathcal{O}$. We know that $P \in \mathrm{Syl}_p(G)$ and that $P \neq Q$ as orbits are disjoint and $\{Q\}$ is not one of the $\mathcal{O}_i$. Additionally, we know that the orbit sizes divide the order of the group acting by the FCP ($|\mathcal{O}| = |Q : Q_P|$) and since Q is a p-group, we conclude that $|\mathcal{O}|$ is a power of p. As $|\mathcal{O}|$ is a p-power and yet p^e does not divide $|\mathcal{O}|$, we conclude that $|\mathcal{O}| < p^e$ and therefore that $|Q : Q_P| < p^e$. Now Q_P, the stabilizer of P in Q, is just $Q \cap \mathbf{N}_G(P)$, so we have $|Q : Q \cap \mathbf{N}_G(P)| < p^e$. By the lemma we proved last time in class, $Q \cap \mathbf{N}_G(P) \subseteq P$ as $Q \cap \mathbf{N}_G(P)$ is a p-group contained in $\mathbf{N}_G(P)$. Yet $Q \cap \mathbf{N}_G(P)$ is also contained in Q, so $Q \cap \mathbf{N}_G(P) \subseteq Q \cap P$. Since $|Q : Q \cap P|$ divides $|Q : Q \cap \mathbf{N}_G(P)| < p^e$, we have our result. □

Now consider $\bigcap \mathrm{Syl}_p(G) = \bigcap_{x \in G} P^x$ for $P \in \mathrm{Syl}_p(G)$. We know that this intersection is $\mathrm{core}_G(P)$, and say $D = \bigcap \mathrm{Syl}_p(G)$ temporarily. We know that

$D \lhd G$, $D \subseteq P$ and therefore D is a normal p-subgroup of G. Often, D is the identity. Suppose that $N \lhd P$ is a p-subgroup. We know that $N \subseteq P^g$ for some $g \in G$. If we conjugate both sides by g^{-1}, we get that $N^{g^{-1}} = N \subseteq P$ as $N \lhd G$. Since P was arbitrary, this shows that $N \subseteq P$ for all $P \in \mathrm{Syl}_p(G)$; hence $N \subseteq \bigcap \mathrm{Syl}_p(G) = D$. Thus D is *the* largest normal p-subgroup of G, and we write $\mathbf{O}_p(G)$.

More generally, we can write $\mathbf{O}_\pi(G)$ to represent the unique largest normal π-subgroup of G whenever π is a collection of primes. Note that there are two possible definitions of largest here, and that, in this case, they coincide. But a good question arises: Why should $\mathbf{O}_\pi(G)$ exist at all, when we have seen that it needn't always be the case that Hall π-subgroups exist? We certainly cannot obtain it the way we did for $\mathbf{O}_p(G)$.

Let M be a normal π-subgroup of G of largest possible order; this exist as 1 certainly works for M. Let N be any normal π-subgroup. We wish to show that $N \subseteq M$. Now $|NM|$ is certainly a π-number and NM is a normal subgroup of G since both N and M are normal in G. So NM is a π-group containing M. By the maximality of M, we must have $|M| = |NM|$, implying that $M = MN$. Yet $N \subseteq MN = M$, so we see that in this case, M is maximal in both interpretations of the word.

As a final definition, we mention a different but related subgroup, $\mathbf{O}^\pi(G)$, which is the (unique) smallest normal subgroup of G with $|G : \mathbf{O}^\pi(G)|$ a π-number.

We now prove a useful non-simplicity theorem.

Theorem 3.2. Let $|G| = p^a q$ where p and q are primes and $a > 0$. Then G is not simple.

Proof. If $p = q$, then G is a p-group or order at least p^2 since $a > 0$. Then G has a normal subgroup of index p, say N. Then $1 < N < G$ since $|G : N| = p$ and $N \lhd G$ so G is not simple. We can now assume that $p \neq q$. We know that $n_p(G) \in \{1, q\}$. if $n_p(G) = 1$ then G is again not simple, so we may assume that $n_p(G) = q$. Let $D = P \cap S$ be the intersection of two different Sylow p-subgroups with $|D|$ as large as possible.

We note that $|D| < p^a$ as P and Q are chosen to be different. We suppose first that $|D| = 1$ and count elements. We have $q(p^a - 1)$ non-identity p-elements, and only q other elements in G. Let X be the set of these; $|X| = q$. Let $Q \in \mathrm{Syl}_q(G)$. Then $Q \subseteq X$ and $|Q| = q = |X|$ and we must therefore have $Q = X$. This makes $n_q(G) = 1$ and in this case G is not simple. We therefore assume that $|D| > 1$ Let $N = \mathbf{N}_G(D)$.

We claim that N is not a p-group. Now $N \cap S = \mathbf{N}_S(D)$. Now $D < S$, so $\mathbf{N}_S(D) > D$ as normalizers grow in p-groups. If N is a p-group, then we have that $N \subseteq T$ for some $T \in \mathrm{Syl}_p(G)$ by the Sylow-D theorem. If we then consider $T \cap P$, we know that $T \cap P$ contains $N \cap P = \mathbf{N}_P(D) > D$. By the maximality of $|D|$, we conclude that $T = P$. The same logic allows us to conclude that $T \cap S > D$ and that we also have $T = S$. Yet this implies that $P = T = S$ and thus $P = S$, which is a contradiction. So N is not a p-group, as claimed, and we can therefore conclude (since $N \neq 1$ either) that q divides the order of N.

Choose $Q \in \mathrm{Syl}_q(N)$. Now $|Q| = q$ of course, and we know that $PQ = G$. This follows as $P \cap Q = 1$ as P is a p-group and Q is a q-group and thus $|PQ| = |P||Q| = |G|$. So let $g \in G$. As $G = PQ$, we can write $g = xy$ for $x \in P$ and $y \in Q$. Now $P^g = P^{xy} = P^y$ as $x \in P$ and P certainly normalizes itself. Now $D^y \subseteq P^y$ as $D \subseteq P$, yet $D^y = D$ as $y \in Q \subseteq N$ and $N = \mathbf{N}_G(D)$, and we can now conclude that $D \subseteq P^y$. So $D^y \subseteq P^g$ for all $g \in G$, so $D \subseteq \bigcap_{g \in G} P^g = \mathbf{O}_p(G)$. As $D \subseteq \mathbf{O}_p(G)$ we see that $\mathbf{O}_p(G)$ is nontrivial, not all of G, and normal, proving the non-simplicity of G. □

We now state Brodkey's theorem, which tells us a sufficient condition to have $\mathbf{O}_p(G) = P \cap Q$ for two distinct Sylow p-subgroups of G. As was the case with the Sylow counting theorem, we will also state a stronger theorem of Brodkey's theorem and prove this instead of Brodkey's theorem.

Theorem 3.3 (Brodkey)**.** Assume $P \in \mathrm{Syl}_p(G)$ with P abelian. Then there exists $Q \in \mathrm{Syl}_p(G)$ such that $P \cap Q = \mathbf{O}_p(G)$.

Here is the more general version of Brodkey's theorem.

Theorem 3.4. Let $P, Q \in \mathrm{Syl}_p(G)$ with $P \neq Q$ and such that $P \cap Q$ is minimal in the set of intersections of pairs of distinct Sylow p-subgroups. Let $R \subseteq P \cap Q$ such that $R \lhd G$, $R \lhd Q$. Then $R \subseteq \mathbf{O}_p(G)$.

We end today by noting why this theorem implies Bodkey's. Note that if we are in the situation of Brodkey's theorem, then $P \in \mathrm{Syl}_p(G)$ abelian implies that ALL Sylow p-subgroups of G are abelian, and hence all subgroups of P and Q are normal in both P and Q. If in this case we set $R = P \cap Q$, then we have that $P \cap Q \subseteq \mathbf{O}_p(G)$. As $\mathbf{O}_p(G) = \cap \mathrm{Syl}_p(G) \subseteq P \cap Q$, we have the equality of $P \cap Q$ and $\mathbf{O}_p(G)$, as desired.

4 Problem Set 1

Problem 1. Let $H \subseteq G$. Show that $|\mathrm{Syl}_p(H)| \leq |\mathrm{Syl}_p(G)|$ for each prime p.

Problem 2. Let $Q \in \mathrm{Syl}_p(H)$ where $H \subseteq G$, and assume that $\mathbf{N}_G(Q) \subseteq H$. Show that $Q \in \mathrm{Syl}_p(G)$.

Problem 3. A p-complement in a group G is a Hall p'-subgroup. In other words, its index is a power of the prime p and its order is not divisible by p.

(a) Show that if K is a normal p-complement in G, then K is exactly the set of p'-elements of G, and hence K is characteristic in G.

(b) Let $T \in \mathrm{Syl}_2(G)$ and suppose that T is cyclic. Show that G has a normal 2-complement.

HINT: For (b), show that G has a subgroup of index 2 and apply induction on $|G|$. Do this by showing that G is isomorphic to a subgroup of the symmetric group $\mathrm{Sym}(n)$ not contained in $\mathrm{Alt}(n)$, where $n = |G|$.

NOTE: Corollary: If $|G| = 2m$ where m is odd, then G has a normal subgroup of order m.

Problem 4. Fix a prime number p and suppose that $H \subseteq G$ has the property that $\mathbf{C}_G(x) \subseteq H$ for all elements $x \in H$ of order p. Show that either $|H|$ or $|G : H|$ is not divisible by p.

Problem 5. A subgroup $U \subseteq G$ is called a trivial intersection or T.I. subgroup if $U \cap U^g = 1$ whenever $g \in G$ and $U^g \neq U$. Suppose $P \in \mathrm{Syl}_p(G)$ is a T.I. subgroup of G. Show that if $Q \in \mathrm{Syl}_p(H)$ and $H \subseteq G$ then Q is T.I. in H.

Problem 6. Let $|G| = pqr$ where $p < q < r$ are primes. Show that $|\mathrm{Syl}_r(G)| = 1$.

HINT: First prove the (easy) two prime version of this result as a lemma. Then show that if the result fails, a Sylow q-subgroup is normal and use your lemma.

NOTE: The general result concerning the case where $|G|$ is the product of any number of distinct primes is valid. I am not aware of any elementary proof, however, even for four primes.

5 01-28-10

We restate the generalized Brodkey theorem, and then give a proof.

Theorem 5.1. Let $P \in \mathrm{Syl}_p(G)$. Choose $Q \in \mathrm{Syl}_p(G)$ such that $P \cap Q$ is minimal. Let $R \subseteq P \cap Q$ with $R \lhd P$, $R \lhd Q$. Then $R \subseteq \mathbf{O}_p(G)$.

Proof. Let $S \in Syl_p(G)$. We want to show that $R \subseteq S$. Let $N - \mathbf{N}_G(R)$. We know that both P and Q are contained in N and both $P, Q \in \mathrm{Syl}_p(N)$. Now $N \cap S$ is a p-subgroup of N, so we can find a $n \in N$ with $N \cap S \subseteq Q^n$ by the Sylow-C theorem. Conjugating both sides of this on the left by n^{-1}, we see that $(N \cap S)^{n^{-1}} \subseteq Q$. Distributing the n^{-1} and using the fact that $n^{-1} \in N$, we see that $N \cap S^{n^{-1}} \subseteq Q$. Taking intersections with P, we see that $P \cap (N \cap S^{n^{-1}}) \subseteq P \cap Q$. As $P \subseteq N$, we know that $P \cap N = P$, and so the above simplifies to yield $P \cap S^{n^{-1}} \subseteq P \cap Q$. As $S^{n^{-1}} \in \mathrm{Syl}_p(G)$, we see by the minimality of the intersection $P \cap Q$ we see that we must actually have equality here; hence $P \cap S^{n^{-1}} = P \cap Q$. As $R \subseteq P \cap Q$, this gives that $R \subseteq P \cap S^{n^{-1}}$. Yet $P \cap S^{n^{-1}} \subseteq S^{n^{-1}}$ so we have that $R \subseteq S^{n^{-1}}$. Finally, we again conjugate both sides of this containment by n, yielding $R^n \subseteq S$. However, n was an element of $N = \mathbf{N}_G(R)$ so $R^n = R$, and we have $R \subseteq S$, as desired. This puts R into ALL Sylow p-subgroups of G, and therefore into the intersection of all Sylow p-subgroups of G; hence $R \subseteq \mathbf{O}_p(G)$. □

We now deduce a few quick corollaries.

Corollary 5.1. Let $P \in \mathrm{Syl}_p(G)$. Assume that P is abelian. If $|P| > \sqrt{|G|}$ then $\mathbf{O}_p(G) > 1$.

Proof. Suppose that $\mathbf{O}_p(G) = 1$. By Brodkey's theorem, there exists $Q \in \mathrm{Syl}_p(G)$ with $P \cap Q = \mathbf{O}_p(G) = 1$. Now $|PQ| \leq |G|$ since $PQ \subseteq G$. However, we see that $|PQ| = |P||Q|/|P \cap Q| = |P||Q|$ since $P \cap Q = 1$. However, this is a contradiction since $|P||Q| = |P|^2 \geq |G|$. □

Corollary 5.2. If $|G| = 2^2 \cdot 3^3 \cdot 13^2$ then G is not simple.

Proof. Let $P \in \mathrm{Syl}_{13}(G)$. Any group of order p^2 is abelian, and $|P| = 13^2 \geq 2^2 3^3$, so we are finished by the previous corollary. □

We now begin a new topic.

5.1 Subnormality

We begin with a definition.

Definition 5.1. We say that H is *subnormal* in G and write $H \lhd\lhd G$ if there exist subgroups H_i such that $H = H_0 \lhd H_1 \lhd \ldots \lhd H_r = G$.

The notion of subnormality was introduced by Wielandt, the great trivializer. We now give a few examples of groups which are subnormal but NOT normal.

Example 5.1.

- A_4 has a normal subgroup of order 4, which is abelian. If we consider a subgroup of order two, it is normal inside this subgroup of order four which is normal in A_4. However, A_4 has no normal subgroup of order 2.

- Nilpotent groups; one equivalent definition for a nilpotent group is that all of its subgroups are subnormal. As a short "proof" of this, let $H \subseteq G$ where G is nilpotent. Then $H \lhd \mathbf{N}_G(H)$ and $\mathbf{N}_G(H) > H$ since normalizers grow in nilpotent groups. If we continue in this way, we will eventually get to G, making H subnormal. If every subgroup is subnormal, then in particular we have that maximal subgroups are subnormal. Yet this means that they must be normal in the whole group as there cannot be any in between groups. Therefore G has all maximal subgroups normal and G is nilpotent.

- In the previous example, we took a subgroup of G, say H, and kept taking normalizers until we reached the whole group. In a way, this is a sort of greedy algorithm, as at each state we are looking for the largest possible normal subgroup to contain a given group. This is NOT always the way to obtain a subnormal series. If we look at S_4, we can take the element $(12)(34) \in A_4$ and consider its normalizer in S_4, which is a full Sylow 2-subgroup of order 8. Now the Sylow subgroup is not normal in S_4; in fact, it is its own normalizer; so this will not work as a subnormal series. However, $(12)(34) \lhd A_4 \lhd S_4$, so $(12)(34)$ (the subgroup of order two that

it generates) is subnormal in S_4, but we would not have known this from the greedy algorithm.

We now mention a few basic facts about subnormal series. It is helpful to keep in mind the analogous facts that we know about normal subgroups.

1. If $H \lhd \lhd G$ and $K \subseteq G$ then $(H \cap K) \lhd \lhd K$; this is like the diamond lemma for subnormal series. If $H = H_0 \lhd H_1 \lhd \ldots \lhd H_r = G$ then $H_0 \cap K \lhd H_1 \cap K \lhd \ldots H_r \cap \lhd K$. To see why $H_i \cap K \lhd H_{i+1} \cap K$, conjugate $H_i \cap K$ by an element of $H_{i+1} \cap K$. On the one hand, the elements of $H_i \cap K$ are contained in K, so when you conjugate by an element of K you stay in K. On the other hand, $H_i \cap K \subseteq H_i$ so if you conjugate an element of $H_i \cap K$ by an element of H_{i+1} you stay in H_i since $H_i \lhd H_{i+1}$.

2. If $H \lhd \lhd K$ and $K \lhd \lhd G$ then $H \lhd \lhd G$. Note that the analogous fact here does NOT hold in general for normal subgroups.

3. If $H \lhd \lhd G$ and $K \lhd \lhd G$ then $(H \cap K) \lhd \lhd G$. To see this, simply combine facts (1) and (2). By (1), we have $H \cap K \lhd \lhd K$ and $K \lhd \lhd G$ so fact two tells us that $(H \cap K) \lhd \lhd G$.

4. If $H \lhd \lhd G$ then $\overline{H} \lhd \lhd \overline{G}$ Where $\overline{G} = G/N$ for some $N \lhd G$. That is, homomorphic images of subnormal series form subnormal series.

At this point in the lecture, Isaacs went on a particularly memorable digression where he used the Isaacsism "Subnormality is like normality with a stutter", which I thought was pretty awesome.

We now present a good example of how one uses the assumption that a subgroup H is subnormal in G.

Theorem 5.2. Let $H \lhd \lhd G$ and suppose that H is a π-subgroup for some set of primes π. Then $H \subseteq \mathbf{O}_\pi(G)$.

Proof. We induct on $|G : H|$. If $|G : H| = 1$ then $G = H$ is a Hall π-subgroup and $G \lhd G$ so $G = \mathbf{O}_\pi(G)$. We may therefore assume that $H < G$. As $H \lhd \lhd G$, we know that there exists a subgroup $M \lhd G$ with $M \neq G$ and $H \lhd \lhd M$, with $|M : H| < |G : H|$. The induction hypothesis may therefore be applied to M, and we see that $H \subseteq \mathbf{O}_\pi(M)$. Yet $\mathbf{O}_\pi(M)$ is characteristic in M which is normal in G, so $\mathbf{O}_\pi(M) \lhd G$ and is a π-subgroup; as such, $\mathbf{O}_\pi(M) \subseteq \mathbf{O}_\pi(G)$. So $H \subseteq \mathbf{O}_\pi(M) \subseteq \mathbf{O}_\pi(G)$. □

Theorem 5.3. Let H be a nilpotent subgroup of G. Then $H \lhd \lhd G$ if and only if $H \subseteq \mathbf{F}(G)$.

Proof. If $H \subseteq \mathbf{F}(G)$ then $H \lhd \lhd G$ as $H \lhd \lhd \mathbf{F}(G)$ by one of our first facts about subnormal seres ($X \subseteq G$ for G nilpotent implies that X is subnormal in G) and $\mathbf{F}(G) \lhd G$. For the other direction, we again induct on $|G : H|$. If $|G : H| = 1$, then G is nilpotent and $\mathbf{F}(G) = G$, and we are again finished. So assume that $H < G$, and take $M < G$, with $M \lhd G$ and $H \lhd \lhd M$. H is

nilpotent and subnormal in M, so $H \subseteq \mathbf{F}(M)$ and $\mathbf{F}(M)$ is characteristic in M which is normal in G, so we have $\mathbf{F}(M) \lhd G$ and nilpotent, placing $\mathbf{F}(M)$, and therefore H, as a subgroup of $\mathbf{F}(G)$. □

6 Problem Set 2

Problem 7. Let $N \lhd G$. Show that $\Phi(N) \subseteq \Phi(G)$.

HINT: Otherwise, choose a maximal subgroup M of G not containing $\Phi(N)$ and deduce that $N = \Phi(N)(N \cap M)$.

Problem 8. Let $N \lhd G$ and both N and G/N' are nilpotent. Show that G is nilpotent.

HINT: Show that $N' \subseteq \Phi(G)$.
NOTE: If $N \lhd G$ and both N and G/N are nilpotent, it does not follow that G is nilpotent.

Problem 9. Suppose that G acts transitively on a set Ω with $|\Omega| > 1$. In the notes on group actions we saw that there is at least one element of G that fixes no element of Ω. If $H = G_\alpha$ is the stabilizer of a point $\alpha \in \Omega$, show that in fact there are at least $|H|$ elements in G that fix no element of Ω.

HINT: Let χ be the permutation character associated with the action and note that $\sum_{x \in G} \chi(x) = |G|$, but that $\sum_{x \in H} \chi(x) \geq 2|H|$.

Problem 10. Let $H < G$. Then H is a *Frobenius complement* in G if $H \cap H^x = 1$ whenever $x \in G - H$. Prove that H is a Frobenius complement in G if and only if $\mathbf{N}_G(X) \subseteq H$ for all nonidentity subgroups $X \subseteq H$.

HINT: For "if", suppose P is a nontrivial Sylow subgroup of $H \cap H^x$ with $x \notin H$. Consider $\mathbf{N}_G(P)$ and show that both P and $P^{x^{-1}}$ are Sylow in H.
NOTE: We will give a different, but equivalent, definition of a Frobenius complement later.

Problem 11. A group G is *dihedral* if it has a cyclic subgroup C if index 2 such that every element of $G - C$ is an involution.

(a) Let $A \subseteq G$ be abelian of index 2. Show that all elements of $G - A$ are involutions if and only if there exists an involution $t \in G - A$ such that $x^t = x^{-1}$ for all elements $x \in A$.

(b) Show that a group G is dihedral if and only if it is generated by two involutions, s and t, and that in this case, $|G|$ is twice the order of the element st.

NOTE: For each integer n, there is a unique group (up to isomorphism) that is dihedral of order $2n$. Group theorists call this group D_{2n}, and so shall we, although others call it D_n. Usually the case $n = 1$ is excluded.

7 02-02-10

We recall our theorem from last time that if H is a nilpotent subgroup of G and $H \lhd \lhd G$, then $H \subseteq \mathbf{F}(G)$.

Lemma 7.1. Let N be minimal normal in G. Then $N \subseteq \mathbf{N}_G(H)$ for all subnormal $H \subseteq G$.

Before we prove this lemma, we make a definition that we will need in order to continue with the proof.

Definition 7.1. The *socle* of G, denoted $\mathrm{soc}(G)$, is the subgroup generated by all minimal normal subgroups of G.

We note that if $N \lhd G$ and $N > 1$ then $N \cap \mathrm{soc}(G) > 1$. Also, we note that the word socle is a typical english word which means foundation or base (it is often used in architecture).

With this definition in mind, we now proceed with the proof of our lemma.

Proof. We wish to show that $\mathrm{soc}(G) \subseteq \mathbf{N}_G(H)$ for all $H \lhd \lhd G$, as this is equivalent to the above statement of the lemma; if $\mathrm{soc}(G) \subseteq \mathbf{N}_G(H)$ then as $N \subseteq \mathrm{soc}(G)$, we have what we want. We proceed by induction on $|G|$. Let $H \lhd \lhd G$ and N minimal normal in G. If $H = G$ we are done so assume that $H < G$. Then we know that there exists M such that $H \subseteq M \lhd G$ with $M \neq G$ since H is subnormal. Also, $H \lhd \lhd M$ so if $N \nsubseteq M$ then $N \cap M < N$ and $N \cap M \lhd G$ since both N and M are normal in G, so we must have that N and M intersect trivially by the minimality of N. As disjoint normal subgroups commute, we have that $N \subseteq \mathbf{C}_G(M) \subseteq \mathbf{C}_G(H)$, thus putting $N \subseteq \mathbf{N}_G(H)$, and we are finished. We can therefore assume that $N \subseteq M$, although we may NOT assume that N is minimal normal in M. We get around this as follows. Since $1 < N \lhd M$, we know that $N \cap \mathrm{soc}(M) > 1$. But $\mathrm{soc}(M) \lhd G$ since it is characteristic in M which is normal in G. By the minimality of N, this means that $N \cap \mathrm{soc}(M) = N$ and thus $N \subseteq \mathrm{soc}(M)$. By induction, we know that $\mathrm{soc}(M) \subseteq \mathbf{N}_M(H) \subseteq \mathbf{N}_G(H)$. As $N \subseteq \mathrm{soc}(M)$, transitivity gives us the result. □

The next theorem that we prove is quite important and useful, but it certainly NOT obvious. The proof we present is due to Isaacs, of course, and is NOT Wielandt's original proof (In fact, Isaacs says that Wielandt doesn't like this proof). A brute force proof exists also, due to Passman, and can be found in his book on permutation groups.

Theorem 7.1. Let H and K be subnormal in G. Then $\langle H, K \rangle \lhd \lhd G$.

Proof. We first note that we do not say $HK \lhd \lhd G$ since HK need not be a subgroup at all, as H and K are only subnormal in G. We work by induction on $|G|$, not being particularly concerned with a base case as everything is trivial when $|G| = 1$. So assume that $|G| > 1$ and let N be minimal normal in G; write $\overline{G} = G/N$. [We use the bar convention]. It follows that $\overline{H} \lhd \lhd \overline{G}$ and that

$\overline{K} \lhd \lhd \overline{G}$ since homomorphisms preserve subnormality. Since $|\overline{G}| < |G|$, we have that $\langle \overline{H}, \overline{K} \rangle \lhd \lhd \overline{G}$ by the inductive hypothesis. We know that $\langle \overline{H}, \overline{K} \rangle = \overline{\langle H, K \rangle}$ since is a homomorphism [think if this element wise; $\overline{h_1 k_1} \ldots = \bar{h_1} \bar{k_1} \ldots$]. We therefore know that $\overline{\langle H, K \rangle} \lhd \overline{G}$. Yet $\overline{\langle H, K \rangle} = \overline{\langle H, K \rangle N}$ Since $\overline{N}$ is the identity of $\overline{G}$. By the correspondence theorem, we therefore have that $\langle H, K \rangle N \lhd \lhd G$.

We now use the previous lemma to conclude that N, which was taken to be minimal normal in G, is contained in both $\mathbf{N}_G(H)$ and $\mathbf{N}_G(K)$, which implies that $N \subseteq \mathbf{N}_G(\langle H, K \rangle)$. Of course, we also know that $\langle H, K \rangle \subseteq \mathbf{N}_G(\langle H, K \rangle)$, giving us that $\langle H, K \rangle \lhd \langle H, K \rangle N \lhd \lhd G$, which implies that $\langle H, K \rangle \lhd \lhd G$. □

We have established a few useful properties about subnormality and seen some conclusions that can be drawn from knowing that we have a subnormal subgroup. We now wish to develop the machinery for going the other way - we wish to see what conditions could imply that a particular group is subnormal. For this, we will need a very important lemma called the zipper lemma. We first state the zipper lemma, and then give an example of a theorem which can be proved using the zipper lemma. We will then go on to prove the zipper lemma in the next section.

Lemma 7.2. Let $H \subseteq G$ and assume that H is not subnormal in G¡ but that $H \lhd \lhd X$ whenever $H \subseteq X < G$. Then H is contained in a unique maximal subgroup of G.

We note that the zipper lemma is a particular instance of when a sort of "subnormalizer" exists. Unlike the normalizer of a subgroup, there is no guarantee of such a thing when it comes to subnormality. An example mentioned by Isaacs, which I am not too terribly comfortable with, is in a simple group of order 168. This simple group has two different copies of S_4 contained within it which I believe intersect along the Klein 4 group, which is of course normal within both of them. Yet the group generated by the two copies of S_4 is the whole group.

We now give an example where we use the zipper lemma.

Theorem 7.2. Let $H \subseteq G$ and assume that $HH^g = H^g H$ for all $g \in G$. Then $H \lhd \lhd G$.

Proof. To prove this theorem, we need a quick lemma.

Lemma 7.3. If $HH^g = G$ then $H = G$.

Proof. For $g \in G$, write $g = xy$, where $x \in H$ and $y \in H^g$. Since $x \in H$, we have $H = H^x = H^{gy^{-1}} = (H^g)^{y^{-1}} = H^g$ because $y^{-1} \in H^g$. Thus $H = H^g$ and the product $G = HH^g = HH = H$. □

We now continue with the proof of the theorem. We again induct on $|G|$. Assume for contradiction that H is not subnormal in G and consider X with $H \subseteq X < G$. Then H satisfies all hypotheses of the theorem in the group X, and we can therefore conclude by induction that $H \lhd \lhd X$. By the zipper lemma, let $H \subseteq M \subseteq G$ with M the unique maximal subgroup of G containing H. Let

$g \in G$. Now $HH^g \neq G$ since $H \neq G$ and using our lemma. However, we DO know that HH^g is a group since $HH^g = H^gH$, so HH^g is contained in some maximal subgroup of G. As $H \subseteq HH^g$, we conclude that $HH^g \subseteq M$. As g was taken to be arbitrary, we know that $HH^g \subseteq M$ for all $g \in G$. Since $H \subseteq M$, we can sort of multiply HH^G on the left by H^{-1}, implying that we must have $H^g \subseteq M$ as well. Write $H^G = \langle H^g | g \in G \rangle$. Since $H^g \subseteq M$ for all $g \in G$, we see that $H^G \subseteq M$. However, $H \lhd \lhd H^G \lhd G$ because $H^G < G$ as $H^G \subseteq M < G$, and this gives us that $H \lhd \lhd G$, which is a contradiction.

□

We end with a few comments. We note that the last proof is a bit tricky, since it requires both proof by induction and proof by contradiction, and we must contradict what we want (that $H \lhd \lhd G$) to prove what we want. Also, I wanted to mention another Isaacsism I found amusing, which was the statement "For all I know, there are other things I don't know".

8 02-04-10

We begin by stating, and then proving, the Zipper lemma.

Lemma 8.1. If H is not subnormal in G but $H \lhd \lhd X$ whenever $H \subseteq X \subseteq G$ then $H \subseteq M$ for some unique maximal subgroup M of G.

Proof. We proceed by induction on $|G : H|$. We know that H is not normal in G, so let $\mathbf{N}_G(H) \subseteq N \subseteq G$ where N is a maximal subgroup of G. Also, let $H \subseteq M \subseteq G$ where M is maximal in G. We wish to show that $M = N$. We can assume that H is not normal in M or else $M \subseteq \mathbf{N}_G(H) \subseteq N$ and $M = N$ as desired. However, we do know that H is subnormal in M as M is a proper subgroup of G, so we can arrange to have $H \lhd H_1 \lhd H_2 \subseteq M$ where H is not normal in H_2 (delete any intermediate subgroups on the original chain with $H \lhd H_i$). Choose $x \in H_2$ such that $H^x \neq H$. However, since $H_1 \lhd H_2$ we do have that $H_1^x = H_1$; hence $H^x \subseteq H_1 \subseteq \mathbf{N}_G(H) \subseteq N$. Likewise, as $H_2 \subseteq M$ we know that $H^x \subseteq M$. Let $K = HH^x$, which is a sibgroup as both H and H^x are normal in H_1. As $H \neq H^x$, we know that $K > H$ and we established previously that $K \subseteq N$ and $K \subseteq M$. We claim that K satisfies the hypotheses of the theorem. We claim that K is not subnormal in G; this holds since we know that H is not subnormal in G, yet $H \lhd K$. Thus if K were subnormal in G we would have $H \lhd K \lhd \lhd G$, and therefore that $H \lhd \lhd G$. Thus K cannot be subnormal in G. Next, we must show that K IS subnormal in any proper subgroup containing K. So let $K \subseteq Y < G$. Now $H \subseteq K \subseteq Y$ so we know that $H \lhd \lhd Y$. Also, $H^x \subseteq K \subseteq Y$, and so $H \subseteq K^{x^{-1}} \subseteq Y^{x^{-1}}$, and as $|Y| = |Y^{x^{-1}}|$, we must also have that Y is a proper subgroup of G. Thus $H \lhd \lhd Y^{x^{-1}}$ and conjugating both sides of this by x tells us that $H^x \lhd \lhd Y$. From our main theorem last time, we know that the group generated by two subnormal groups is subnormal, so we have that $K = \langle H, H^x \rangle \lhd Y$, establishing that K does in fact satisfy the hypotheses of the problem. As $|G : K| < |G : H|$, we have by induction that

K is contained within a unique maximal subgroup of G. As K is contained in both M and N, we must have that $N = M$, and we are finished. $\square$

The zipper analogy is actually quite visual; it "zips" up all potential subnormalizers into a single entity.

We now continue with a very powerful application of the zipper lemma, Baer's theorem. Isaacs had something interesting to say about this theorem. He said that often in mathematics, people go around inventing definitions and theories and other things and proving things about these new ideas. Although this is grand and wonderful, one key to knowing that you are onto something is when you can take your own definitions and ideas and apply them to something which, on the surface, does not seem to involve this specialized machinery. If you can use these new methods to prove something nontrivial which is NOT self contained, then that is when you know that what you have cooked up is truly useful and worthy of study. Baer's theorem is an example of how subnormality theory can be applied to group theory as a whole in this sort of situation.

Theorem 8.1 (Baer's Theorem)**.** Let $H \subseteq G$ and assume that $\langle H, H^g \rangle$ is nilpotent for all $g \in G$. Then $H \subseteq \mathbf{F}(G)$.

Proof. The first conclusion that we draw is that H is certainly nilpotent, as it is the group generated by H and H. By one of our previous results, it suffices to show that H is subnormal in G. We may therefore asume for contradiction that H is not subnormal in G or else we are done. If $H \subseteq X < G$ and $x \in X$, then $\langle H, H^x \rangle$ is nilpotent by hypothesis. If we work by induction, we can therefore say that the inductive hypothesis applies to X and we conclude that $H \lhd \lhd X$. We may therefore apply to zipper lemma to G and let M be the unique maximal subgroup of G containing H. Let $g \in G$. Now $\langle H, H^g \rangle$ is nilpotent and so if $\langle H, H^g \rangle = G$ then G is in fact nilpotent, and EVERY subgroup of G is known to be subnormal, which is a contadiction. We may therefore assume that $\langle H, H^g \rangle < G$ for all $g \in G$. For an arbitrary $g \in G$, as $\langle H, H^g \rangle < G$, we know that we can find a maximal subgroup of G containing this group, and the uniqueness of M implies that we must have $\langle H, H^g \rangle \subseteq M$ for all $g \in G$. In particular, this gives us that $H^G \subseteq M \subseteq G$, from which we conclude that $H^G < G$ as we can put H^G inside of a proper subgroup. As $H \subseteq H^G$ and $H \lhd \lhd H^G$, and $H^G \lhd G$, we have that $H \lhd \lhd H^G \lhd G$, implying that $H \lhd \lhd G$, which is our contradiction. $\square$

We again note that this is one of those funny proofs in which we prove the property we want by contradiction, and the contradiction that we reach is actually what we wanted to be true in the first place.

Theorem 8.2 (Zenkov's Theorem)**.** Let $A, B \subseteq G$ where A and B are abelian. Let $D = A \cap B^x$ be minimal with respect to containment as x runs over G. Then $D \subseteq \mathbf{F}(G)$.

Proof. Without loss, assume that $D = A \cap B$.[relabel B if necessary]. As every group is generated by its Sylow subgroups, it suffices to show that for $P \in$

$\mathrm{Syl}_p(D)$ that $P \subseteq \mathbf{F}(G)$ for all primes p. By Baer, it is enough to show that $\langle P, P^x \rangle$ is nilpotent for all $g \in G$. Suppose that there exists $g \in G$ such that $\langle P, P^g \rangle$ is NOT nilpotent. In particular, $\langle P, P^g \rangle$ is not a p-group as p-groups are nilpotent. Let $H = \langle A, B^g \rangle$. Suppose first that $H = G$. We know that $A \cap B^g$ is centralized by both A and B^g since A and B^g are abelian, and thus $A \cap B^g \subseteq \mathbf{Z}(G)$. Certainly, $A \cap B^g \subseteq A$. I want to show that $A \cap B^g \subseteq B$. Because $A \cap B^g \subseteq B^g$ we know that $(A \cap B^g)^{g^{-1}} \subseteq B$. But $(A \cap B^g)^{g^{-1}} = A \cap B^g$ since $A \cap B^g$ is central, and therefore $A \cap B^g \subseteq B$, and therefore $A \cap B^g = A \cap B = D$ by the minimality of D; hence D is central in G. As $P \subseteq D \subseteq \mathbf{Z}(G)$, this is a contradiction as we then have $P^g = P$, and we supposed that $\langle P, P^g \rangle = P$ was not a p-group. It therefore cannot be the case that $\langle A, B^g \rangle = G$.

Now $H = \langle A, B^g \rangle < G$. We know that $A \subseteq H$. Let $B_0 = H \cap B$. Now $A \cap B_0 = A \cap (H \cap B) = A \cap B$ since $A \subseteq H$, and we see that $A \cap B_0 = A \cap B$. We wish to show that $A \cap B$ is minimal amongst intersections in H. Suppose for contradiction that $(A \cap B_0^h < A \cap B$ for $h \in H$. Conjugating everything by h^{-1}, we have $A^{h^{-1}} \cap B < D^{h^{-1}}$. Again conjugating both sides by h, we find $A \cap B^h < D$, which is a contradiction since D is minimal amongst intersections in G. This D is minimal amongst intersections in H of A and B_0. Applying the inductive hypothesis in H, we know that $D \subseteq \mathbf{F}(H)$. So $P \subseteq D \subseteq \mathbf{F}(H)$. Now $\mathrm{Syl}_p(\mathbf{F}(H)) = \{\mathbf{O}_p(H)\}$, and as P is a p-group contained in H, we know that we can put P into a Sylow p-subgroup of $\mathbf{F}(H)$. As $\mathbf{F}(H)$ has a unique Sylow p-subgroup, we see that $P \subseteq \mathbf{O}_p(H)$. Since $P \subseteq B$, we know that $P^g \subseteq B^g \subseteq H$. We therefore have that $\langle P, P^g \rangle \subseteq \mathbf{O}_p(H)P^g$. Yet by counting the sizes of sets, we see that $\mathbf{O}_p(H)P^g$ is a p-group, and this is a contradiction as we assumed that $\langle P, P^g \rangle$ was not nilpotent. □

Corollary 8.1. Let G be nonabelian, simple, and let $A \subseteq G$ be abelian. Then $|A| < \sqrt{|G|}$.

Proof. Let D be minimal of the form $A \cap A^g$ for $g \in G$. By Zenkov, we know that $D \subseteq \mathbf{F}(G) = 1$ as G is simple and nonabelian. Thus $A \cap A^g = 1$. Now $G > AA^g$, so $|G| > |A||A^g| = |A|^2$, and the result follows. □

Another corollary to Baer's theorem which will eventually help us in the proof of the $p^a q^b$ theorem is coming up. We state the corollary now, and we prove it next time.

Corollary 8.2. Let $t \in G$ be an involution and asusme that $t \notin \mathbf{O}_2(G)$. Then there exists $g \in G$ of odd prime order such that $g^t = g^{-1}$.

We end with a general fact about involutions. Suppose that $x, y \in G$ with $o(x) = o(y) = 2$. Then $(xy)^x = xxyx = yx = (xy)^{-1}$. Say $o(xy) = n$. Assuming for now that n is not a power of two, take p and odd prime dividing n. Let $g \in \langle xy \rangle$ with $o(g) = p$. Since $(xy)^x = (xy)^{-1}$, we conclude that $g^x = g^{-1}$. With this fact in mind, we note that to prove the corollary it will suffice to show that there exists another involution with $o(xy)$ NOT a power of 2.

9 Problem Set 3

Problem 12. Let $H, K \subseteq G$ and suppose that $|G : H|$ and $|K|$ are relatively prime. Show that if either H or K is subnormal in G, then $K \subseteq H$.

Problem 13. (a) Let $s, t \in G$ be nonconjugate involutions. Show that the elements st has even order and deduce that there exists an involution $z \in G$ that commutes with both s and t.

(b) Suppose that a Sylow 2-subgroup of G is a nonnormal $T.I.$ set. Show that G has exactly one conjugacy class of involutions.

NOTE: There is no result analogous to (b) for elements of odd prime order. This is one of the few circumstances in group theory where the prime 2 makes things easier rather than harder.

Problem 14. Let G be a finite group and let $\mathcal{X}$ be any collection of minimal normal subgroups of G. Let N be the (normal) subgroup of G generated by $\bigcup \mathcal{X}$.

(a) Show that N is the direct product of some members of $\mathcal{X}$.

(b) Show that every minimal normal subgroup of N is simple.

(c) Show that N is a direct product of simple groups.

Problem 15. In the situation of the previous problem, assume that all members of $\mathcal{X}$ are nonabelian. Show that every minimal normal subgroup of G contained in N is a member of $\mathcal{X}$.

HINT: Show that $\mathbf{Z}(N) = 1$.

Problem 16. Let $S \lhd \lhd G$ be nonabelian and simple. Show that $S \subseteq \mathrm{soc}(G)$.

HINT: Work by induction on $|G|$. Let $\mathcal{X}$ be the collection of G-conjugates of S and let N be the group generated by $\bigcup \mathcal{X}$. Note that if $S < G$ then $N < G$. Show that the members of $\mathcal{X}$ are minimal normal in N and that N is minimal normal in G.

Problem 17. Let $A \subseteq G$ and $N \lhd G$ where A is abelian and $\mathbf{C}_A(N) = 1$. Assume, furthermore, that $|A|$ and $|N|$ are coprime. Show that $|A| < |N|$.

HINT: Apply Zenkov's theorem in the group NA.

10 02-09-10

We begin by proving a theorem from last time.

Theorem 10.1. Let $t \in G$ be an involution and assume that $t \notin \mathbf{O}_2(G)$. Then there exists an element $g \in G$ of odd prime order such that $g^t = g^{-1}$.

Proof. We note, as we did last time, that if $x, y \in G$ are involutions, then $(xy)^y = yx = (xy)^{-1}$. If $o(xy)$ is not a power of 2, then take $p|o(xy)$ with p an odd prime. Let $g \in \langle xy \rangle$ with $o(g) = p$. Then $g^y = g^{-1}$ since $g \in \langle xy \rangle$. Therefore if we can show that xy has order not a power of two then we are finished by this fact.

If $\langle t, t^g \rangle$ is a 2-group for all $g \in G$, then $\langle T, T^g \rangle$ is always a 2-group and hence is nilpotent. By Baer, $\langle t \rangle \in \mathbf{F}(G)$ so $t \in \mathbf{O}_2(G)$, a contradiction. We can then conclude that there is some $g \in G$ for which $\langle t, t^g \rangle$ is not a 2-group. Write $s = t^g$, so that $\langle t, s \rangle$ is not a 2-group. Now $\langle t, s \rangle = \langle st \rangle \langle t \rangle$ since $\langle st \rangle \lhd \langle st, t \rangle$; this follows since st normalizes the group generated by st and t normalizes the group generated by st as conjugation by t sends the elements of this group to their inverses. Now $\langle t, s \rangle| = 2o(st)$ since $\langle t, s \rangle = \langle st \rangle \langle t \rangle$. As $|\langle t, s \rangle|$ is not a power of two, we know that $o(st)$ is divisible by p for some odd prime p, and we are done by our original comments.

□

In order to see an application of this theorem, we make a new definition.

Definition 10.1. Given a prime p, a subgroup $H \subseteq G$ is said to be *p-local in* G if $H = \mathbf{N}_G(U)$ where $U \neq 1$ and U is a p-group.

The theorem we prove is an example of a "local to global" type of theorem; that is, we know a local property about a group, and it happens to be strong enough to give us some global information.

Theorem 10.2. Assume for all odd primes p that every p-local subgroup of G has a normal Sylow 2-subgroup. Then G has a normal Sylow 2-subgroup.

Before we prove our theorem, we need a lemma.

Lemma 10.1. Let $N \lhd G$ and write $\overline{G} = G/N$. If $\overline{X}$ is p-local in $\overline{G}$, then $\overline{X} = \overline{Y}$ for some p-local subgroup Y of G.

Proof. We may assume that $N \subseteq X \subseteq G$. We also know that $\overline{X} = \mathbf{N}_{\overline{G}}(\overline{U})$ where $\overline{U} \neq 1$ and $\overline{U}$ is a p-group. From this, we can assume that $N \subseteq U \subseteq G$ as $\overline{U} \subseteq \overline{X}$,we have that $N \subseteq U \subseteq X \subseteq G$ with $U \lhd X$ and $X = \mathbf{N}_G(U)$ by the correspondence theorem. Let $P \in \mathrm{Syl}_p(U)$. We know that P is nontrivial as p divides $|U|$ as $\overline{U} \neq 1$. We claim that $NP = U$. We know that $|U : NP|$ is a p-power as $|U : N|$ is a p-power. yet $|U : NP|$ must also be p' as $P \subseteq NP$ and $|U : P|$ is p'. Hence $|U : NP| = 1$ and we have $U = NP$. [a diagram here is actually quite helpful.]

By the Frattini argument, we see that $X = U\mathbf{N}_X(P) \subseteq U\mathbf{N}_G(P) = (NP)\mathbf{N}_G(P)$. As $P \subseteq \mathbf{N}_G(P)$, we have that $X \subseteq N\mathbf{N}_G(P)$, and applying our homomorphism to this containment, we have that $\overline{X} \subseteq \overline{N\mathbf{N}_G(P)} = \overline{\mathbf{N}_G(P)}$. We now show the other containment, that $\overline{\mathbf{N}_G(P)} \subseteq \overline{X}$. Now $\mathbf{N}_G(P)$ normalizes N as $N \lhd G$ and therefore EVERYTHING normalizes N. Also, $\mathbf{N}_G(P)$ normalizes P, so we have that $\mathbf{N}_G(P)$ normalizes $NP = U$. So $\mathbf{N}_G(P) \subseteq \mathbf{N}_G(U) = X$, and hence $\overline{\mathbf{N}_G(P)} \subseteq \overline{X}$. We therefore have that $\overline{X} = \overline{\mathbf{N}_G(P)}$, which is a p-local subgroup of G. □

Before continuing with the proof of the theorem, we note that the converse of this lemma is NOT necessarily true; that is, a p-local subgroup need not map to a p-local subgroup. As an example, consider the case where $\mathbf{O}_p(G)$ is a Sylow p-subgroup of G and we mod out by $\mathbf{O}_p(G)$.

We now continue with the proof of the theorem.

Proof. First, suppose that $\mathbf{O}_2(G) = 1$. We must show that $|G|$ is odd. If $|G|$ is not odd, then G has even order, and we can find $t \in G$ an involution. Then $t \notin \mathbf{O}_2(G)$ so we know that $g^t = g^{-1}$ for some $g \in G$ with odd prime order, say p. Let $P = \langle g \rangle$. So $t \in \mathbf{N}_G(P)$. By hypothesis, $T \lhd \mathbf{N}_G(P)$ and $P \lhd \mathbf{N}_G(P)$ and $T \cap P = 1$, so we have that T and P commute. In particular, t and g commute. However, this implies that $g^{-1} = g^t = g$, which means that $o(g) = 2$, and this contradicts that $o(g) = p$. Thus of $\mathbf{O}_2(G) = 1$ we know that $|G|$ is odd. Now to prove the theorem in generality, let $T = \mathbf{O}_2(G)$. Let $\overline{G} = G/T$. Now $\overline{G}$ still satisfies the hypotheses of the theorem, yet $\mathbf{O}_2(\overline{G}) = 1$. We check that $\overline{G}$ satisfies the hypotheses of the theorem since if $\overline{X}$ is p-local in $\overline{G}$, then by our lemma we know that $\overline{X} = \overline{Y}$ for some Y p-local in G. So Y by hypothesis has a normal Sylow 2-subgroup S, and $\overline{S}$ is a normal Sylow 2-subgroup of $\overline{Y} = \overline{X}$. Thus $T = \mathbf{O}_2(G)$ is a normal Sylow 2-subgroup of G. □

10.1 Split Extensions

We now switch gears from subnormality theory to the topic of split extensions. Given group G, N, we want to find a group Γ such that $M \lhd \Gamma$, $M \cong N$, and with $\Gamma/M \cong G$. If this happens, then we say that Γ is an *extension of G by N.*

As an example of an extension of G by N, we can let $\Gamma = G \times N$. Then $M = \{(1, n) | n \in N\}$ is isomorphic to N [in the 741 notes, we denoted this M by $\tilde{N}$]. Additionally, we know that $\Gamma/M \cong G$, as we can find $\theta : \Gamma \to G$ having kernel M by considering the standard projection map.

Definition 10.2. If $M \lhd \Gamma$, $H \subseteq \Gamma$, $MH = \Gamma$, and $M \cap H = 1$, then we say that H is a *complement* for M in Γ. If a complement for M exists, we say that Γ is *split*.

We note that although the direct product does indeed give us an example of an extension, it also gives us an example of an extension with a complement which is normal. In general, extensions need not have complements. If they do, these complements certainly need not be normal.

11 02-11-10

We begin with a definition.

Definition 11.1. If $N \lhd G$, we say that H is a *complement* for N in G if $NH = G$ and $N \cap H = 1$.

We note that by the diamond lemma, if a complement H exists, then $H \cong G/N$. If a complement exists, we say that G *splits over* N, and note that if $H \lhd G$ then G is the direct product of H and N.

In general, if H is a complement for N in G, then H acts by conjugation on N. We know that $H \lhd G$ if and only if the corresponding conjugation action is trivial.

Definition 11.2. Given H and N, we say that H *acts on* N *via automorphisms* if H acts on N as a set and $(xy) \cdot h = (x \cdot h)(y \cdot h)$ for all $x, y \in N$ and $h \in H$.

Example 11.1. We give two examples of actions via automorphisms.

- If $N \lhd G$, then G acts via automorphisms on N by conjugation.
- For any group G, $\mathrm{Aut}(G)$ acts via automorphisms on G.

We note that it is standard to write x^h instead of $x \cdot h$ when we have H acting via automorphisms. Then we have the properties that $(xy)^h = x^h y^h$ and that $((x)^h)^k = x^{hk}$.

Theorem 11.1. Let H act on N via automorphisms. Then there exists a group G such that:

1. There exists $\tilde{N} \lhd G$ with $\tilde{N} \cong N$.
2. There exists $\tilde{H} \subseteq G$ such that $\tilde{H} \cong H$.
3. $\tilde{H}$ is a complemenet for $\tilde{N}$ in G.
4. $\tilde{n^h} = \tilde{n}^{\tilde{h}}$.

Proof. Let $\Omega = H \times N$ as a set. Let N act on Ω by $(h, n) \cdot m = (h, nm)$ for $(h, n) \in \Omega$ and $m \in N$. That this is an action is easy since the group multiplication is associative and since $(h, n) \cdot 1 = (h, n)$ for all $(h, n) \in \Omega$. Also, let H act on Ω by $(h, n) \cdot k = (hk, n^k)$ for $(h, n) \in \Omega$ and $k \in H$. This also is a true action as $(h, n) \cdot 1 = (h, n)$ for all $(h, n) \in \Omega$ and since $((h, n) \cdot k) \cdot l = (hk, n^k) \cdot l = (hkl, (n^k)^l) = (h(kl), n^{kl}) = (h, n) \cdot (kl)$.

We see that both actions are faithful since right multiplication is faithful, and we therefore get maps (which by an abuse of notation, we will call both of them tilde) from $N \to \mathrm{Sym}(\Omega)$ and from $H \to \mathrm{Sym}(\Omega)$. As the actions are faithful, we are actually embedding N and H isomorphically into $\mathrm{Sym}(\Omega)$. We call these images $\tilde{N}$ and $\tilde{H}$.

We claim that $\tilde{H} \subseteq \mathbf{N}_{\mathrm{Sym}(\Omega)}(\tilde{N})$. To see this, we actually use a messy element proof. By the definitions of $\tilde{m}$ and $\tilde{k}$, we have that $(h, n)\tilde{m}\tilde{k} = ((h, n) \cdot m) \cdot k$, and by the definitions of each of these actions, we have $((h, n) \cdot m) \cdot k = (h, nm) \cdot k = (hk, (nm)^k)$. Since k originally acted via automorphisms, we have that $(hk, (nm)^k) = (hk, n^k m^k)$. Now working backwards and using the definition of how m and k act, we have $(hk, n^k m^k) = (hk, n^k) \cdot m^k = ((h, n) \cdot k) \cdot m^k$. Finally, by the embedding tilde, we have $((h, n) \cdot k) \cdot m^k = (h, n)\tilde{k}\tilde{m^k}$.

So we have that $\tilde{m}\tilde{k} = \tilde{k}\tilde{m^k}$ and if we multiply (in $\mathrm{Sym}(\Omega)$) on the left by $\tilde{k}^{-1}$, we have that $\tilde{m}^{\tilde{k}} = \tilde{m^k}$, which is an element of $\tilde{N}$. We therefore see that $\tilde{H}$ normalizes $\tilde{N}$ as claimed. Take $G = \tilde{H}\tilde{N}$, which is a group as $\tilde{H}$ normalizes $\tilde{N}$, and note that $\tilde{N} \lhd G$ as $\tilde{N}$ and $\tilde{H}$ are contained in its normalizer. This gives us our first two propositions. If we show that $\tilde{H} \cap \tilde{N} = 1$ then we will also have the third proposition. Note that we have already established the fourth proposition by our above work in showing that $\tilde{H}$ normalizes $\tilde{N}$.

Suppose that $\tilde{m} = \tilde{k}$ for some $m \in N$ and $k \in H$. Then we have that $(h,n)\tilde{m} = (h,n) \cdot m = (h, nm)$ and that $(h,n)\tilde{k} = (h,n) \cdot k = (hk, n^k)$. As $\tilde{m} = \tilde{k}$, we must have $(h, nm) = (hk, n^k)$. This gives us that $h = hk$ and we must have $k = 1$ since the action by k is faithful. This means that $\tilde{k} = 1 = \tilde{m}$, and our intersection is trivial, completing the proof. $\square$

Definition 11.3. We say that G is the *semi-direct product of N by H* with respect to the given action via automorphisms when the above situation happens, and we write $G = N \rtimes H$.

Notice that to have a semi-direct product, we need three things; the groups N, H, AND the action.

Theorem 11.2. Let $G = NH$ with $N \lhd G$, $H \subseteq G$, and $N \cap H = 1$, and let $G_1 = N_1 H_1$ with $N_1 \lhd G_1$, $H_1 \subseteq G_1$ with $N_1 \cap H_1 = 1$. Assume there exists an isomorphsim from $N \to N_1$, from $H \to H_1$, and we use "sub 1" as the name for both maps somewhat ambiguously. Assume that $(n^h)_1 = n_1^{h_1}$ (i.e., the actions agree). Then there exists some isomorphism $\theta : G \to G_1$ such that $\theta(n) = n_1$ and $\theta(h) = h_1$ for $n \in N$ and $h \in H$.

We make a few notes about the previous theorem. First, we are omitting the proof as it is, according to Isaacs, a "follow your nose" proof, which is pretty boring. Also, we note that once such a θ as mentioned above is established, we know that it is unique since if $g = hn$ then $\theta(g) = \theta(hn) = \theta(h)\theta(n) = h_1 n_1$, which is the swine flu :).

We now do an example which gets our hands dirty with the semi-direct product. The write up may not be so nice, as it involves a lot of writing things out in a sort of messy way.

Example 11.2. Given an odd prime p, there exists a group P with $|P| = p^3$ such that P is non-abelian and has *exponent p*, where the exponent of a group is the least common multiple of the orders of the elements.

For our "proof", we begin with N, which is taken to be the direct product of two cyclic subgroups of order p. Without loss, we can take them to be $\mathbb{Z}_p$, so $N = \mathbb{Z}_p \times \mathbb{Z}_p$. Let $\sigma \in \mathrm{Aut}(N)$ be such that $(1,1) \mapsto (b,1)$. That is, σ is the identity on the second component and is multiplication by b in the first component. One should check that σ is actually an automorphism. This can be done using linear algebra thinking of N as a two dimensional vector space over the field of order p. With this representation in mind, we find that σ can be represented as the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. With this is mind, we see that this

matrix, raised to the kth power, is simply $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ and so when we read this modulo p, we see that we have $\sigma^p = 1$. This shows that the order of σ is p.

We now defin $P = N \rtimes \langle \sigma \rangle$, where σ acts as σ. We see then that $|P| = p^3$, and that P is non-abelian since the conjugation action within P is the same as the action of σ, which is non-trivial. The final step of our construction is to show that P has exponent p.

Let $x \in P$. We want to show that $x^p = 1$. We write $x = \tau u$ for $\tau \in \langle \sigma \rangle$ and $u \in N$. Then $(x)^p = (\tau u)(\tau u) \dots (\tau u)$. We want to rearrange and switch the order of the τ's and u's. Notice that $(u\tau) = \tau\tau^{-1}u\tau = \tau u^\tau$. Plugging this in [this is where you need to write things out] we obtain: $\tau^p u^{\tau^{p-1}} u^{\tau^{p-2}} \dots u$, and since $\tau^p = 1$ we have $u^{\tau^{p-1}} \dots u$.

We claim that $u^\tau = ub^k$ for some k; this comes from the fact τ is simply a power of σ and σ is simply multiplication by b. By induction, we can then see that $u^{\tau^m} = ub^{mk}$ and we therefore have that $x^p = u^p b^{(p-1)+(p-2)+\dots+1}$, which is $b^{\frac{p(p-1)}{2}}$. Since $p \neq 2$, we know that 2 must divide $p-1$ and therefore the exponent on b that we have is divisible by p, making b to this power trivial.

12 02-16-10

We begin with two nice theorems involving acting by automorphisms. Recall that an orbit is *regular* means that its point stabilizer is trivial.

Theorem 12.1. Let P be an abelian p-group acting faithfully via automorphisms on a p'-group N. Then P has a regular orbit in N and $|N| > |P|$.

Proof. Let $G = N \rtimes P = NP$ (that is, associate N and P with $\tilde{N}$ and $\tilde{P}$ so that the action is simply conjugation.) We know that $P \in \mathrm{Syl}_p(G)$ and that P is abelian, so there exists $g \in G$ such that $P \cap P^g = \mathbf{O}_p(G)$ by Brodkey's theorem. Now $N \lhd G$, $\mathbf{O}_p(G) \lhd G$, and as the orders of these groups are coprime, we know that $N \cap \mathbf{O}_p(G) = 1$ and therefore the elements of N and the elements of $\mathbf{O}_p(G)$ commute. Alternatively, we can say that $\mathbf{O}_p(G) \subseteq \mathbf{C}_G(N)$, and we therefore know that $\mathbf{O}_p(G)$ acts trivially on N via conjugation. So in the original action, $\mathbf{O}_p(G)$ is a subgroup of P acting trivially on N and we conclude that $\mathbf{O}_p(G) = 1$ since the action of P on N is faithful. So $P \cap P^g = 1$. As $G = PN$, we can write $g = un$ for $u \in P$ and $n \in N$. Thus $P^g = P^{un} = P^n$ since $u \in P$.

We claim that n is a regular P-orbit. We need to show that $P_n = 1$, or equivalently, that $\mathbf{C}_P(n) = 1$. Now $\mathbf{C}_P(n) \subseteq P$, but we also have that $\mathbf{C}_P(n) \subseteq P^n$ since $(\mathbf{C}_P(n))^n \subseteq P^n$ and $(\mathbf{C}_P(n))^n = \mathbf{C}_P(n^n) = \mathbf{C}_P(n)$. Thus $\mathbf{C}_P(n) \subseteq P \cap P^n$ and $\mathbf{C}_P(n) = 1$. So in N, the orbit $\mathcal{O}_n$ has size $|P : \mathbf{C}_P(n)| = |P|$ by the fundamental counting principle. As $|N| \geq 1 + |P|$, we have that $|N| > |P|$. □

Theorem 12.2. Let A be abelian and act faithfully on N via automorphisms. Assume that $\mathbf{F}(N) = 1$. Then there exists a regular A-orbit in N and $|N| > |A|$.

Proof. Let $G = N \rtimes A = NA$. By Zenkov $A \cap A^g \subseteq \mathbf{F}(G)$ for some $g \in G$. Now $N \cap \mathbf{F}(G) \subseteq \mathbf{F}(N) = 1$, so $\mathbf{F}(G)$ is a normal subgroup of G disjoint from N and therefore $\mathbf{F}(G)$ acts trivially on N by conjugation. Therefore $A \cap A^g \subseteq \mathbf{F}(G)$ also acts trivially on N in the original action, and as the original action was faithful, we must have $A \cap A^g = 1$. Write $g = un$ for $u \in A$ and $n \in N$. Then $A^g = A^{un} = A^n$ and we have that $A \cap A^n = 1$. The orbit of n in N is then seen to be the regular A-orbit by the same reasoning as the previous proof. □

We now begin proving the Schur-Zassenhaus theorem. We state the theorem, and then develop the necessary machinery to prove the theorem.

Theorem 12.3. Let $N \lhd G$ and assume that $(|N|, |G : N|) = 1$. Then G splits over N. Also assume that either N or G/N is solvable. Then all complements of N in G are conjugate.

We make a comment about the solvability clause in the above statement. If $(|N|, |G : N|) = 1$, then the prime 2 divides at most one of $|N|$ and $|G/N|$. The Feit-Thompson theorem states that groups of odd order are necessarily solvable, and so the solvability hypothesis is not truly needed. However, the proof of the Feit-Thompson theorem is complex and spans over 250 pages, so in order for our proof to be self contained, we make the extra assumption.

Before beginning with the proof of the Schur-Zassenhaus theorem, we need to develop some machinery.

Definition 12.1. Let G act via automorphisms on N. A map $\theta : G \to N$ is a *crossed homomorphism* if $\theta(xy) = \theta(x)^y\theta(y)$ for all $x, y \in G$.

Example 12.1. We give two brief examples of crossed homomorphisms.

- Clearly, a regular homomorphism is a crossed homomorphism; it is the crossed homomorphism when the action is trivial.
- A more interesting example is when $N \lhd G$ and G acts by conjugation on N. Then we can define $\theta(x) = [x, n] = x^{-1}n^{-1}xn$ which is $n^{x^{-1}}n$. This establishes that $\theta(x) \in N$. We claim that θ is a crossed homomorphism. To see this, we compute:

  $$\theta(xy) = [xy, n] = [x, n]^y[y, n] = \theta(x)^y\theta(x)$$

  We the commutator identity $[xy, n] = [x, n]^y[y, n]$ holds as $[x, n]^y[y, n] = y^{-1}(x^{-1}n^{-1}xn)y(y^{-1}n^{-1}yn) = y^{-1}x^{-1}n^{-1}xyn = [xy, n]$.

Lemma 12.1. Let G act on N via automorphisms and let $\theta : G \to N$ be a crossed homomorphism. Let $K = \ker\theta = \{g \in G | \theta(g) = 1\}$. Then K is a subgroup of G and $\theta(x) = \theta(y)$ if and only if $Kx = Ky$ for $x, y \in G$.

Proof. First, we note that $1 \in K$ since $\theta(1) = \theta(1 \cdot 1) - \theta(1)^1\theta(1) = \theta(1)^2$, which by cancellation shows that $\theta(1) = 1$, and $1 \in K$. Second, let $x, y \in K$. We wish to show that $xy \in K$. Now $\theta(xy) = \theta(x)^y\theta(y) = 1^y \cdot 1 = 1 \cdot 1 = 1$,

and we see that $xy \in K$. For finite groups, this will suffice, but in order to be as general as possible, we show that K is closed under taking inverses. Now $1 = \theta(1) = \theta(x \cdot x^{-1}) = \theta(x)^{x^{-1}}\theta(x^{-1})$. Since $\theta(x) = 1$, we have $1 = 1^{x^{-1}}\theta(x^{-1})$ and thus $1 = \theta(x^{-1})$, showing that $x^{-1} \in K$, and K is a subgroup.

Now let $Kx = Ky$. then $y = kx$ for some $k \in K$. Then $\theta(y) = \theta(k)^x\theta(x) = 1^x\theta(x) = \theta(x)$, and we have that $\theta(y) = \theta(x)$. Now assume that $\theta(x) = \theta(y)$. We compute $\theta(xy^{-1}) = \theta(x)^{y^{-1}}\theta(y^{-1}) = \theta(y)^{y^{-1}}\theta(y^{-1}) = \theta(yy^{-1}) = \theta(1) = 1$. Thus $xy^{-1} \in K$, and multiplying on the right by y we have that $x \in Ky$, showing that the cosets Kx and Ky are equal. □

The importance of the previous lemma is to establish that $|\theta(G)| = |G : K|$ even though K need not be normal.

We proceed in proving the Schur-Zassenhaus theorem under the assumption that N is an abelian group first (This part of the proof was done by Schur). The rest of the proof will come about by reducing to the abelian case.

Now let $N \lhd G$ where N is abelian and let $\mathcal{T}$ be the set of transversals for N in G.[Recall that a *transversal* is a set of representatives of the cosets of N in G].

If $S, T \in \mathcal{T}$ write $s \leftrightarrow t$ if $Ns = Nt$ or equivalently since $N \lhd G$ if $sN = tN$ for $s \in S$ and $t \in T$.

Define $\delta(S, T) = \prod_{s \leftrightarrow t} s^{-1}t$ which is in N.

Note that if $s \leftrightarrow t$ then $sN = tN$ and $t \in sN$ and thus $st^{-1} \in N$. This is well defined since N is abelian and therefore both left and right cosets are the same.

We now pause to see some properties of δ.

- $\delta(S, S) = 1$ since it is the empty product.
- $\delta(S, T)\delta(T, U) = \delta(S, U)$ since if $s \leftrightarrow t$ and $t \leftrightarrow u$ then $s \leftrightarrow u$ since the group N is abelian and we can rearrange the terms of the product to go in order.
- $\delta(S, T) = \delta(T, S)^{-1}$ since $\delta(S, T)\delta(T, S) = \delta(S, S) = 1$ by the first property and thus $\delta(T, S) = \delta(S, T)^{-1}$.
- Notice that if $g \in G$ and $T \in \mathcal{T}$, then $Tg \in \mathcal{T}$ since if $Nt_1g = Nt_2g$ then $Nt_1 = Nt_2$, implying that $t_1 = t_2$ since $t_1, t_2 \in T$ and exactly one coset representative for each coset is in T.
- Using the previous comment, we see that $\delta(Sg, Tg)$ is defined. To compute what $\delta(Sg, Tg)$ is we use our definition of δ:

$$\delta(Sg, Tg) = \prod_{sg \leftrightarrow tg} (sg)^{-1}(tg) = \prod_{sg \leftrightarrow tg} g^{-1}s^{-1}tg$$

Then since $sg \leftrightarrow tg$ if and only if $s \leftrightarrow t$, we see that:

$$\delta(Sg, Tg) = \prod_{s \leftrightarrow t} (s^{-1}t)^g = \left(\prod_{s \leftrightarrow t} s^{-1}t \right)^g = (\delta(S,T))^g$$

Thus $\delta(Sg, Tg) = \delta(S,T)^g$.

- $\delta(S, Sn)$ for $n \in N$. Notice that $s_1 \leftrightarrow s_2 n$ if and only if $s \leftrightarrow s_2$ which means that $s_1 = s_2$ since S is a transversal of the cosets of N in G. Thus $\delta(S, Sn) = \prod_{s \in S} s^{-1}sn = \prod_{s \in S} n = |S|n = |G : N|n$.

13 Problem Set 4

Problem 18. If π is a set of primes, let $\mathbf{O}^\pi(G)$ denote the unique smallest normal subgroup of G whose index is a π-number. (Check that this really exists). Let $H \lhd \lhd G$, where $H = \mathbf{O}^\pi(H)$. Show that $\mathbf{O}_\pi(G)$ normalizes H.

HINT: Without loss, assume $G = H\mathbf{O}_\pi(G)$ and show $H = \mathbf{O}^\pi(G)$.

Problem 19. Let $H \subseteq G$ with $|G : H| = p$ a prime. Show that $\mathbf{O}^{p'}(H) \lhd G$.

HINT:Let $K = \text{core}_G(H)$ and show that $\mathbf{O}^{p'}(H) = \mathbf{O}^{p'}(K)$.

Problem 20. We say that subgroups H and K of G are **strongly conjugate** if they are conjugate in the group that they generate. Show that $H \lhd \lhd G$ if and only if the only subgroup of G that is strongly conjugate to H is H itself.

NOTE: Much more is true. If H is any subgroup if G, then the subgroup generated by all strong conjugates of H in G is subnormal, and is the unique smallest subnormal subgroup of G that contains H.

Problem 21. Let H be arbitrary and let G be the semi-direct product $H \rtimes H$, with H acting by conjugation on itself. Show that $G \equiv H \times H$.

Problem 22. Suppose that a p-group P acts faithfully via automorphisms on a p'-group G. Show that there is a P-orbit in G on which P acts faithfully.

HINT: Use the generalized Brodkey theorem.

NOTE: Recall that an action is **faithful** if its kernel is trivial, i.e. no non-identity element acts trivially. In general, a faithful action on a set need not have a faithful orbit. (Can you find an easy example?)

Problem 23. Let $C = \langle c \rangle$ be a cyclic group of order $4m$, where $m > 1$ is an integer, and let z be the unique element of order 2 in C.

(a) Show that there exists a unique automorphism σ of C such that $c^\sigma = c^{-1}z$, and prove that $o(\sigma) = 2$.

(b) Let $S = C \rtimes \langle \sigma \rangle$ and view C and $\langle \sigma \rangle$ as actual subgroups of S. Prove that half of the elements of $S - C$ have order 2 and that the rest have order 4.

NOTE: The group S is called the **semidihedral** group of order $8m$, though usually it is assumed that m is a 2-power.

14 02-18-10

We begin by restating the facts proved last time about the function δ defined on arbitrary transversals T and S of the cosets of N in G.

1. $\delta(S,T)^{-1} = \delta(T,S)$
2. $\delta(S,T)\delta(T,U) = \delta(S,U)$
3. $\delta(Sg,Tg) = \delta(S,T)^g$
4. $\delta(S,Sn) = n^{|G:N|}$ for $n \in N$.

We note that in the case of the Schur-Zassenhaus theorem, a subgroup $H \subseteq G$ is a complement if and only if $|H| = |G:N|$. This will come up often in our proof. To see why this is true, note that if H is actually a complement then the diamond lemma tells us that $|H| = |G:N|$. Likewise if $|H| = |G:N|$, then $H \cap N = 1$ since $|H| = |G:N|$ and $|N|$ are coprime. Thus NH has the same order as $|G|$ and is contained within G, making $NH = G$.

Theorem 14.1. The Schur-Zassenhaus theorem holds if N is abelian.

Proof. We first prove the existence, and then we prove conjugation. Define $\theta : G \to N$. Fix $T \in \mathcal{T}$, where $\mathcal{T}$ is the set of all transversals of N in G. We set $\theta(g) = \delta(T, Tg)$. We compute $\theta(xy) = \delta(T, Txy) = \delta(T,Ty)\delta(Ty,Txy)$ by property (2) of the δ function listed above. By property (3), $\delta(Ty,Txy) = \delta(T,Tx)^y$, so we have $\theta(xy) = \theta(y)\theta(x)^y = \theta(x)^y\theta(y)$ since N is abelian, and we have that θ is a crossed homomorphism.

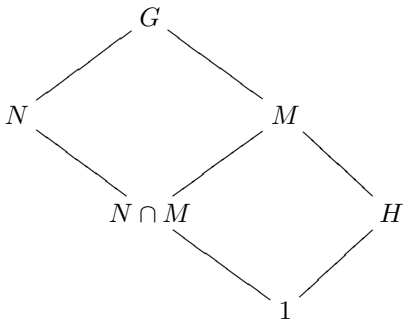
If $n \in N$, note that $\theta(n) = \delta(T,Tn) = n^{|G:N|}$. We claim that θ maps N onto N. As we are assuming that $|N|$ and $|G:N|$ are coprime, so there exists k such that $k|G:N| \equiv 1 \pmod{|N|}$. Given $n \in N$, then $\theta(n^k) = (n^k)^{|G:N|} = n^1 = n$, and θ is onto. Since θ_N is onto N, we know that θ is surjective, and $\theta(G) = N$. Let $K = \ker(\theta)$. We know that $|G:K| = |\theta(G)| = |N|$ by the first homomorphism theorem. It follows that $|K| = |G|/|N| = |G:N|$, and thus K is a complement for N since it has the right size.

We now prove that all complements are conjugate in the case where N is abelian. Let H be an arbitrary complement. Then H is a transversal so $\delta(H,T)$ is defined. Since θ is onto, we know that there exists an $n \in N$ for which $\delta(H,T) = \theta(n)$. Now let $h \in H$. Then $\theta(h) = \delta(T,Th) = \delta(T,H)\delta(H,Th)$ by property 2. By property 1, $\delta(T,H) = \theta(n)^{-1}$, so $\delta(T,H)\delta(H,Th) = \theta(n)^{-1}\delta(Hh,Th)$ and by property 3, we have $\delta(Hh,Th) = \delta(H,T)^h$. Hence $\theta(n)^{-1}\delta(Hh,Th) = \theta(n)^{-1}\delta(T.H)^h = \theta(n)^{-1}\theta(n)^h$. So $\theta(h) = \theta(n)^{-1}\theta(n)^h$ and rearranging this yields $\theta(n)\theta(h) = \theta(n)^h$. Finally, we compute $\theta(h^n)$. Now $\theta(h^n) = \theta(n^{-1}hn) = \theta(n^{-1}h)^n\theta(n)$ since θ is a crossed homomorphism. Yet $\theta(n^{-1}h)^n = \theta(n^{-1}h)$ since N is abelian. So $\theta(n^{-1}h)\theta(n) = \theta(n^{-1})^h\theta(h)\theta(n) = (\theta(n)^h)^{-1}\theta(n)^h$ since we know that $\theta(n)\theta(h) = \theta(n)^h$ and because θ is a regular homomorphism on N, we can interchange conjugation with θ. Again using that θ is a regular homomorphism on N, we see that $(\theta(n)^h)^{-1}\theta(n)^h = \theta(n^h)-1\theta(n^h) = 1$. So we

see that $h^n \in K$ for all $h \in H$. Yet this shows that $H^n \subseteq K$ and since H^n and K have the same order (they are both complements for N), we must have that $H^n = K$. $\square$

We now begin with the generalized case of the Schur-Zassenhaus theorem

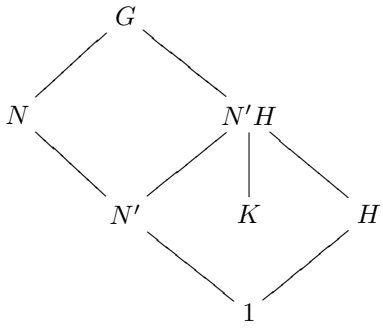
Proof. We proceed by induction on $|G|$. First, assume that N is not nilpotent. Then for some prime p, there exists $P \in \mathrm{Syl}_p(N)$ with P not normal in N. Let $M = \mathbf{N}_N(P)$. By the Frattini argument, $MN = G$. Also, $M < G$ since P is not normal even in N. Then as $M < G$, M satisfies the hypotheses of SZT with respect to $N \cap M \lhd M$ by the diamond lemma. [See the picture below]. By induction, a complement H exists for $N \cap M$ in M. So $|H| = |M : M \cap N| = |G : N|$, and H is in fact a complement for N in G as it has the right size.



Now assume that N is nilpotent. We are ok if $N = 1$ since then G is a complement for N, so assume that $N > 1$. Let $Z = \mathbf{Z}(N) > 1$ since N is nilpotent. Note that Z is characteristic inside of N which is normal in G, making $Z \lhd G$. Write $\overline{G} = G/Z$. Now $|\overline{G}| < |G|$ since $Z > 1$. Also, $|\overline{G} : \overline{N}| = |G : N|$ and $|\overline{N}|$ divides $|N|$, and so we see that $\overline{G}$ satisfies the conditions of the theorem and we can therefore apply induction. This yields a complement $\overline{H}$ in $\overline{G}$. We can assume that $Z \subseteq H$. Now $|H : Z| = |\overline{H}| = |\overline{G} : \overline{N}| = |G : N|$, so $|Z|$ divides $|N|$ and thus $|Z|$ is coprime to $|G : N| = |H : Z|$. So the abelian version of the SZT applies in the group H. This gives a complement $K \subseteq H$ for Z; that is, a group K with $|K| = |H : Z| = |G : N|$. Yet $K \subseteq G$, and this K is a complement for N in G.

We now continue with the proof by proving conjugacy. Again, a picture

will be helpful, and we give it here for reference:



Assume first that N is solvable. Then given K and H both complements of N, we may assume that $N < 1$ or else $H = G = K$. When $N > 1$, we have $N' < N$, where $N' \lhd G$. Write $\overline{G} = G/N'$. Notice that $\overline{G}$ satisfies the hypotheses with respect to $\overline{N}$ since $|\overline{G} : \overline{N}| = |G : N|$ and $|\overline{N}|$ divides $|N|$. Also, $\overline{N}$ is abelian, and we claim that $\overline{H}$ and $\overline{K}$ are complements. This follows since $H \cap N' = 1$ so $|\overline{H}| = |HN'|/|N'| = |H|$. Also, $|\overline{H}| = |H| = |G : N| = |\overline{G} : \overline{N}|$ and similarly for $\overline{K}$. By our previous theorem, this gives us that $\overline{H}$ and $\overline{K}$ are conjugate in $\overline{G}$, and therefore $\overline{H} = \overline{K}^{\bar{g}} = \overline{K^g}$ for some $g \in G$. Replace K with K^g so that we have $\overline{H} = \overline{K}$; know that we can do this since order is all that is important for a complement, and conjugation is an isomorphism. Then $\overline{HN'} = \overline{KN'}$ and therefore $HN' = KN'$ by correspondence. Now $N'H < G$ since $N' < H$. Now we have that $N'H$ satisfies the hypotheses of the theorem with respect to N'. But H and K are both contained in $N'H = N'K$ and are both complements in $N'H$ so they must be conjugate by induction. If H and K are conjugate in $N'H$ then of course they are conjugate in G.

Finally, assume now that G/N is solvable and we work by induction. We can assume that G/N ¿ 1 or else $N = G$ and $H = 1 = K$. Let $U/N \lhd G/N$ with U/N a non-trivial p-group for some prime p; this exists as G/N is solvable. Now $|U \cap H| = |U : N|$ which is a p-power. Note that p does not divide $|N|$ since $(|N, |G : N||) = 1$ and p divides $|G : N|$. Thus $|U : U \cap H| = |N|$ is p' by the diamond lemma. So $U \cap H \in \mathrm{Syl}_p(U)$ and similarly for $K \cap U$. Then by the Sylow-C theorem, we know that $(U \cap K)^g = U \cap H$ for some $g \in U$. So $U \cap H = U \cap K^g$ since $U \lhd G$. Again, replace K by K^g so that we have $U \cap H = U \cap K$, and that $U \cap H \lhd H$ and similarly $U \cap H \lhd K$. Let $M = \mathbf{N}_G(U \cap H)$. Both H and K are contained in M by the previous statement. If $M < G$, note that H and K are complements for $M \cap N$ in M since $|M \cap N|$ is a divisor of $|N|$ which is coprime to $|H|$. So the inductive hypothesis yields $H = K^m$ for some $m \in M$ and we are finished. So assume that $M = G$ so that $H \cap U \lhd G$.

Let $\overline{G} = G/(H \cap U)$ and consider $\overline{H}$ and $\overline{K}$. Note that $|\overline{G}| < |G|$ since $U \cap H$ is a non-trivial Sylow p-subgroup of U. Then $\overline{G}$ satisfies the hypotheses with respect to the normal subgroup $\overline{U}$ and in this situation, $\overline{H}$ and $\overline{K}$ are complements. So $\overline{H} = \overline{K}^{\bar{g}} = \overline{K^g}$, so $(H \cap U)H = (H \cap U)K^g$, but as $H \cap U \subseteq H$

and $U \cap H \subseteq K$ implies that $(U \cap H)^g \subseteq K^g$ but $(H \cap U)^g = H \cap U$ since U is normal. This makes $H = K^g$, as desired. $\square$

15 02-23-10

We take today to prove a few useful results which follow from the Schur-Zassenhaus theorem.

Theorem 15.1. Let G be solvable and let π be any set of primes. Then G has a Hall π-subgroup.

Proof. Induct on $|G|$. Without loss, we can assume that $G > 1$. Let $U \lhd G$ where $U \neq 1$ is a p-group for some prime p, which exists since G is solvable. By the inductive hypothesis, $\overline{G} = G/U$ has a Hall π-subgroup $\overline{H}$ where $U \subseteq H$. If $p \in \pi$, then H is a Hall π-subgroup of G since $|G : H| = |\overline{G} : \overline{H}|$ is a π'-number. So suppose that $p \notin \pi$. Then $|U|$ and $|H : U|$ are coprime since $|H : U|$ is a π-number. The SZT therefore applies in H and implies that a complement K exists. Then the diamond lemma tells us that $|K|$ is a π-number and $|G : K|$ is π' as $|G : K| = |G : H||H : K|$, where $|G : H|$ is π' and $|H : K| = |U|$ is a p-power, and p is π'. $\square$

Note that the theorem we have just proven is like the Sylow-E theorem, only for sets π with more than one prime under the hypothesis that the group is solvable. It is a famous paper of Phillip Hall, with a title something like "On theorems like Sylow's" that the Hall-E, Hall-C, and Hall-D theorems all hold in solvable groups.

We showed earlier in these notes that Hall subgroups need not always exist. However, even when Hall subgroups DO exist, if the group is not solvable there is no guarantee that the Hall-C theorem still applies. In fact, it need not. Isaacs has an example of course, but he said it very quickly and I didn't quite catch it.

Although it doesn't really use the SZT, we prove what is really the converse of the previous theorem. As part of the proof, we will need to assume Burnside's $p^a q^b$ theorem, which we will prove later in the course (and which I already know a character theoretic proof of), so this isn't too much of a cheat.

Theorem 15.2. Suppose that G has a p-complement for all primes p dividing $|G|$. Then G is solvable.

Before getting to the proof of this theorem, we will need a few things.

Lemma 15.1. Let $H, K \subseteq G$ and assume that $(|G : H|, |G : K|) = 1$. Then $HK = G$ and $|H : H \cap K| = |G : K|$.

Proof. Note that $H \cap K \subseteq H \subseteq G$ so $|G : H|$ must divide $|G : H \cap K|$. Similarly, $|G : K|$ divides $|G : H \cap K|$. Then as $|G : H|$ and $|G : K|$ are coprime, we know that $|G : H||G : K|$ divides $|G : H \cap K|$ and throwing away information, we know that $|G : H||G : K| \leq |G : H \cap K|$. Rearranging terms gives us that $|G| \leq (|H||K|)/(|H \cap K) = |HK| \leq |G|$, which means that the set $HK = G$. The relation about the indices is a result of this inequality as well. $\square$

Corollary 15.1. Suppose that H and K are respectively a p-complement and a q-complement in G with $p \neq q$. Then $H \cap K$ is a q-complement in H.

Theorem 15.3. Let $H, K, L \subseteq G$ where H, K, L are solvable and have pairwise coprime indices. Then G is solvable.

Proof. Induct on $|G|$. If there exists N with $1 < N \subseteq G$, let $\overline{G} = G/N$. Then $\overline{H}, \overline{K}$, and $\overline{L}$ are contained in $\overline{G}$, they are solvable, and the have pairwise coprime indices [this can be seen by using the diamond lemma with each of these subgroups and N]. By induction, $\overline{G} = G/N$ is solvable, so it suffices to find a normal subgroup N of G, $N > 1$, and N solvable.

If $L = 1$, then $G = HL \subseteq H$ by the previous lemma and therefore G is solvable as H is assumed to be solvable. So assume that $L > 1$. Let $U \lhd L$, $U \neq 1$ where U is a p-group. WLOG, p does not divide $|G : H|$[this is where we are using the third subgroup] . Let $P \in \mathrm{Syl}_p(H)$. Then $P \in \mathrm{Syl}_p(G)$ since $|G : H|$ is p'. U is a p-group, so $U \subseteq P^g \subseteq H^g$ for some $g \in G$ by the Sylow-D and C theorems. Again without loss, replace that given H of the problem with H^g for convenience, so that $U \subseteq H$. Now $G = LH$ by the lemma, and let $x \in G$. Then $x = lh$ for some $l \in L$ and $h \in H$. Then $U^x = U^{lh} = U^h$ since $U \subseteq L$ and $U \lhd L$. So $U^x \subseteq H$ for all $x \in G$. This gives us that $U^G \subseteq H$. Since $U > 1$ and $U \subseteq U^G$, we know that U^G is nontrivial, $U^G \lhd G$, and since $U^G \subseteq H$ gives us that U^G is solvable, so we have what we want. □

We now give the proof of the theorem.

Proof. Let H_p denote a p-complement in G for p dividing $|G|$. We induct on the number of prime divisors of $|G| = n$. If $n = 1$ then G is a p-group, and we know that p-groups are solvable. If $n = 2$, Burnside theorem applies and tells us the group is solvable. So we can assume that $n \geq 3$ and take p dividing $|G|$. We claim that H_p satisfies the theorem. That is, given a q dividing $|H_p|$, then q divides $|G|$ and by the previous corollary, $H_p \cap H_q$ is a q-complement in H_p. Also, p does not divide $|H_p|$ so the number of prime divisors of $|H_p|$ is $n-1$. So H_p is solvable. Then same can be said for H_q and H_r, where q and r are two other distinct prime divisors of $|G|$. The indices of H_p, H_q, and H_r are pairwise coprime as p, q, r are distinct, and so the previous theorem tells us that G is solvable. □

15.1 Coprime Actions

We now start with a new topic. Let A act on G via automorphisms, and assume that $|A|$ and $|G|$ are coprime. Temporarily, suppose that A is a non-trivial q-group. Then given a prime p dividing $|G|$, we want to find an A-invariant $P \in \mathrm{Syl}_p(G)$. Now A permutes $\mathrm{Syl}_p(G)$ and since q does not divide $|G|$, we know that q does not divide $|\mathrm{Syl}_p(G)|$ since $|\mathrm{Syl}_p(G)| = |G : \mathbf{N}_G(P)|$, a divisor of $|G|$. Yet the A-orbits on $\mathrm{Syl}_p(G)$ have q-power size, but the sum of the orbit sizes must equal $|\mathrm{Syl}_p(G)|$. This means that there exists an orbit $\mathcal{O}$ with size one.

Note that this argument only holds if A is a q-group, and it cannot be generalized to the general case with $(|A|, |G|| = 1$. This is what we will discuss next time.

16 Problem Set 5

Problem 24. Suppose that G has a normal Hall π-subgroup N, and let H be a complement for N in G. Let K be any π'-subgroup of G. Assuming that either N or K is solvable, show that H is G-conjugate to a subgroup of H.

Problem 25. Let $H \subseteq G$.

(a) Assume that $|G : H| = 2m$ where m is odd. Suppose that $t \in G$ is an involution and that no G-conjugate of t lies in H. Show that G has a subgroup of index 2 that does not contain t.

(b) Let G be simple and have a dihedral Sylow 2-subgroup. Show that G has a unique conjugacy class of involutions.

HINT: Show that t induces an odd permutation on some set.
NOTE: Check that the simple group A_6 has a Sylow 2-subgroup isomorphic to D_8. Thus the situation of (b) really can occur.

Problem 26. Let π be a set of primes. A group G is **π-separable** if it has a series of normal subgroups $1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G - r = G$ such that each factor group G_{i+1}/G_i is either a π-group or a π'-group.

(a) Show that G is π-separable if it has a subnormal series where each factor is either a π-group or a π'-group.

(b) Show that Hall π subgroups of π-separable groups always exist.

HINT: For (a), consider $\mathbf{O}^{\pi}(G)$ and $\mathbf{O}^{\pi'}(G)$.
NOTE: Assertion (b) says that π-separable groups satisfy E_π. Assuming the odd-order theorem, it is not hard to show that π-separable groups also satisfy C_π and D_π.

Problem 27. Let A act via automorphisms on G and suppose that $(|A|, |G|) = 1$ and the either A or G is solvable. Let P be an A-invariant Sylow p-subgroup of G. Show that $P \cap C$ is a Sylow p-subgroup of C, where $C = \mathbf{C}_G(A)$.

Problem 28. Let A, G, and C be as in the previous problem, and assume that $G = HK$, where H and K are A-invariant subgroups. Show that $C = (H \cap C)(K \cap C)$.

HINT: Given $c \in C$, consider the set $\Omega = \{(h, k) | h \in H, k \in K, \text{ and } hk = c\}$.

17 02-25-10

Assume that A acts via automorphisms on G, and that $(|A|, |G|) = 1$. Assume further that either A or G is solvable. We call these hypotheses the *usual hypotheses* throughout the remainder of this discussion.

Lemma 17.1 (Glauberman's Lemma)**.** Assume the usual hypotheses. Assume that G and A each act, although not necessarily via automorphisms, on Ω, where G is acting transitively on Ω. Assume that $(\alpha \cdot g) \cdot a = (\alpha \cdot a) \cdot g^a$ for all $\alpha \in \Omega$, $g \in G$, and $a \in A$. Then:

(a) A has a fixed point in Ω.

(b) If $\alpha, \beta \in \Omega$ are A-fixed there exists $g \in \mathbf{C}_G(A)$ such that $\alpha \cdot g = \beta$.

We make a quick note about some notation that we will use here. We write $\mathbf{C}_G(A)$ to denote the set of elements in G that are fixed by all of A. If $\Gamma = G \rtimes A$, then this is exactly the kernel of the action of A when A acts by conjugation on Γ. However, the semi-direct product is not needed for the statement of this lemma, so we do not introduce it.

Before we give the proof of Glauberman's lemma, we state a corollary of it, which is a way that we go about using Glauberman's lemma.

Theorem 17.1. Assume the usual hypotheses, and let p be a prime. Then:

(a) There exists an A-invariant Sylow p-subgroup of G.

(b) If P and Q are A-invariant Sylow p-subgroups of G, then $P^c = Q$ for some $c \in \mathbf{C}_G(A)$.

Proof. Let $\Omega = \mathrm{Syl}_p(G)$. Then G acts via conjugation on Ω, (note that this action is transitive by the Sylow-C theorem) and A acts on Ω in its natural way. Let $P \in \Omega$, $g \in G$ and $a \in A$. We need to show that $(P^g) \cdot a = (P^a) \cdot g^a$; i.e. we need that $(P^g)^a = (P^a)^{g^a}$ since our dot operations are all just conjugation. Yet this clearly holds since A acts via automorphisms, and we have $(P^g)^a = ((P^a)^{g^a}) = (P^a)^{g^a}$. So Glauberman's lemma applies and part (a) guarantees that there exists an A-fixed P in Ω, and part (b) says that if both P and Q happen to be A-invariant then $P^c = Q$ for some $c \in \mathbf{C}_G(A)$. □

We now give the proof of Glauberman's lemma.

Proof. Let $\Gamma = G \rtimes A = GA$. Now Γ acts on Ω by $\alpha \cdot (ag) = (\alpha \cdot a) \cdot g$. (Note that when dealing with Glauberman's lemma, it is important to interpret which dot corresponds to which action). We first need to check that this defines an action; that is, we need to check that $(\alpha \cdot (ag)) \cdot (bh) = \alpha \cdot (agbh)$. Now $(\alpha \cdot (ag)) \cdot (bh) = ((\alpha \cdot a) \cdot g) \cdot b \cdot h$ by definition, and this is equal to $((\alpha \cdot a) \cdot g \cdot b) \cdot h$ by associativity. As $(\alpha \cdot a) \in \Omega$, we can rewrite $((\alpha \cdot a) \cdot g \cdot b) \cdot h$ as $((\alpha \cdot a) \cdot b \cdot g^b) \cdot h$ by our original compatibility condition. Now we compute:

$$(\alpha \cdot a) \cdot b \cdot g^b \cdot h = \alpha \cdot (ab) \cdot (g^b h) = \alpha \cdot (abg^b h) = \alpha \cdot (agbh)$$

Where all of the above equalities hold since A acts on Ω, G acts on Ω, and since A acts via automorphisms. This shows that Γ too acts on Ω. Pick $\alpha \in \Omega$. We claim that $G\Gamma_\alpha = \Gamma$. To see this, let $x \in \Gamma$. We know that $\alpha \cdot x \in \Omega$ since G is transitive, and we know that $\alpha \cdot x = \alpha \cdot G$ for some $g \in G$. So if we act on both sides by g^{-1}, we see that $\alpha \cdot (xg^{-1}) = \alpha$ and hence $xg^{-1} \in \Gamma_\alpha$. If we now multiply both sides on the right by G, we get that $x \in \Gamma_\alpha G$. Since $x \in \Gamma$ was taken to be arbitrary, we have that $\Gamma = G\Gamma_\alpha$. [Note: this is simply the Frattini argument in disguise]. We notice that $|\Gamma : G| = |A|$ which is coprime by hypothesis to $|G|$. Therefore Γ_α satisfies the hypotheses of the SZT with respect to the group $G \cap \Gamma_\alpha$. So by SZT, we know that there exists a complement H for $G \cap \Gamma_\alpha$ in Γ_α. So $|H| = |\Gamma_\alpha : G \cap \Gamma_\alpha| = |\Gamma : G| - |A|$ [draw a diamond here]. So H is really a complement in Γ for G, and by the conjugacy part of the SZT, we see that $A = H^x$ for some $x \in \Gamma$.

We claim that A fixes $\alpha \cdot x \in \Omega$. To see this, we consider $(\alpha \cdot x) \cdot h^x = \alpha \cdot (xh^x) = \alpha \cdot (hx) = (\alpha \cdot h) \cdot x = \alpha \cdot x$ since $h \in H \subseteq \Gamma_\alpha$. So $A = H^x$ fixes $\alpha \cdot x$ and we have part (a) of the lemma.

For part (b), suppose that $\alpha, \beta \in \Omega$ are both A-fixed. Let $X = \{x \in G | \alpha \cdot x = \beta\}$. We wish to show that there exists an A-fixed element in X; we will apply part (a) of our lemma to obtain (b). First, note that A acts on X. Let $x \in X$ and $a \in A$. We wish to show that $x^a \in X$. So we need to show that $\alpha \cdot x^a = \beta$. Now $\alpha \cdot x^a = (\alpha \cdot a) \cdot x^a$ since α is A-fixed. Yet $(\alpha \cdot a) \cdot x^a = \alpha \cdot x \cdot a = \beta \cdot a = \beta$ since β is also A-fixed. Now the group G_β acts on X by right multiplication, and we need to show that this action is transitive. Now if $x \in X$ and $t \in G_\beta$, we wish to show first that $xt \in X$. Yet $\alpha \cdot xt = \alpha \cdot x \cdot t = \beta \cdot t = \beta$, showing that $xt \in X$. Also, if $x, y \in X$, we want to show that there exists $t \in G_\beta$ with $xt = y$. If this is to be the case, then we must have $t = x^{-1}y$ and it is equivalent, therefore, to show that $x^{-1}y$ stabilizes β. Yet $\beta \cdot (x^{-1}y) = \beta \cdot x^{-1} \cdot y = \alpha \cdot y = \beta$. Also, we must establish that A acts on G_β. So let $t \in G_\beta$ and let $a \in A$. Then t^a must fix β to be in G_β. So $\beta \cdot t^a = \beta \cdot a \cdot t^a$ β is fixed by A. Yet $\beta \cdot a \cdot t^a = \beta \cdot t \cdot a = \beta \cdot a = \beta$ since $t \in G_\beta$ and β is also A-fixed. Finally, we must show that the actions of A and G_β on X are compatible. So let $x \in X$, $t \in G_\beta$, and $a \in A$. We need that $(x \cdot t) \cdot a = (x \cdot a) \cdot t^a$. Yet $(x \cdot t) \cdot a = xt \cdot a = (xt)^a = x^a t^a = (x \cdot a) \cdot t^a$, and we have what we want. Thus by part (a) if this lemma, we have that A has a fixed point $c \in X$ so that $\alpha \cdot c = \beta$ where $c \in X$ and where c is A-fixed, making $c \in \mathbf{C}_G(A)$. □

We now give a direct application of Glauberman's lemma, which we call the Sylow-D theorem "with glasses", to use Isaacs' terminology.

Theorem 17.2. Assume the usual hypotheses. Let $P \subseteq G$ be a p-group which is A-invariant. Then there exists an A-invariant $S \in \mathrm{Syl}_p(G)$ with $P \subseteq S$.

Proof. If false, assume that $|G : P|$ is as small as possible. Let $P \subseteq T$ for $T \in \mathrm{Syl}_p(G)$, which exists by the usual Sylow-D theorem. Note that we must have $P < T$ or we do not have a counterexample. So $\mathbf{N}_T(P) > P$ since normalizers grow in p-groups so $|\mathbf{N}_G(P)|_p > |P|$. Let $N = \mathbf{N}_G(P)$. Then N is A-invariant

since P is A-invariant and N is uniquely determined by P. Let $Q \in \mathrm{Syl}_p(N)$ be A-invariant by the Sylow-E theorem with glasses. Then $P \subseteq Q$ since $P \lhd N$ and therefore $P \subseteq \mathbf{O}_p(N) \subseteq Q$, but $Q > P$ since $|Q| = |N|_p > P$. So $|G : Q| < |G : P|$ and by the minimality of $|G : P|$, we must have that $Q \subseteq S$ for some $S \in \mathrm{Syl}_p(G)$ which is A-invariant. However, $P \subseteq Q \subseteq S$ and so this contradicts that P is a counterexample. □

Theorem 17.3. Assume the usual hypotheses. Let $C = \mathbf{C}_G(A)$. The map $K \mapsto K \cap C$ is a bijection from the set of A-fixed classes of G onto the set of all classes of C.

Proof. Let K be an A-fixed class of G¿ Want $K \cap C \neq 0$. We use Glauberman's lemma with A, G, and $\Omega = K$. By Glauberman, we know that there exists a fixed point making $K \cap C \neq 0$. Part (b) of Glauberman's Lemma says that $K \cap C$ is a class of C. This map is injective since conjugacy classes are disjoint. This map is surjective since conjugacy classes of C are contained in conjugacy classes of G and these can be shown to be A-invariant. □

18 03-02-10

Suppose that A acts on G with $(|A|, |G|) = 1$ with A or G solvable. Suppose that $H \subseteq G$ is A invariant, where A permutes the right cosets of H in G. Then $(Hg)^a = H^a g^a = Hg^a$.

Theorem 18.1. The A-invariant right cosets of H in G are those that contain fixed elements.

Proof. Suppose that X is an A-fixed right coset of H in G. It suffices to show that $X \cap \mathbf{C}_G(A) \neq \emptyset$. Now A permutes X since although X in A-invariant, this does NOT mean that all elements of X are individually fixed. Also, H acts on X by $x \cdot h = h^{-1}x$, where this inverse sign is needed to make this an action. This action is transitive, and to see the compatibility condition, we need that $x \cdot h \cdot a = x \cdot a \cdot h^a$. This means that $x \cdot h \cdot a = (h^{-1}x)^a = ((h^a)^{-1}x^a) = x \cdot a \cdot h^a$ since A acts via automorphisms. Therefore Glauberman's lemma yields an A-fixed element of X, and we have what we need. □

Let us consider what the previous theorem says when H happens to be a normal subgroup of G. Then the permutation action of A on the cosets is an action via automorphisms on the factor group G/H. Then the fixed cosets in this case are $\mathbf{C}_{G/H}(A)$. Write $\overline{G} = G/H$. Then the previous theorem is telling us that $\mathbf{C}_{\overline{G}}(A) = \overline{\mathbf{C}_G(A)}$. This fact is very useful, and will definitely be used later.

18.1 Commutators

We now begin a new section. We define the commutator of x and y, written $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$. We can think about the commutator as sort of

measuring the difference or distance between x and x^y. We see that $[x, y] = 1$ if and only if x and y commute. We state a few useful facts about commutators:

1. $[x, y]^{-1} = [y, x]$
2. $[xy, z] = [x, z]^y[y, z]$
3. $[z, xy] = [xy, z]^{-1} = [z, y][z, x]^y$

Using just these facts, we draw a quick corollary.

Corollary 18.1. Suppose that $g \in G$ and that $[x, g] \in \mathbf{Z}(G)$ for all $x \in G$. Then the map $[\bullet, g] : G \to \mathbf{Z}(G)$ is a homomorphism, and similarly for $[g, \bullet]$.

Proof. Property (1) holds by the second fact listed above about commutators, where $[x, g]^y = [x, g]$ since $[x, g]$ is central. The second statement holds since $[g, \bullet] = [\bullet, g]^{-1}$, and since $\mathbf{Z}(G)$ is abelian we know that the inverse map is a homomorphism. □

We now generalize this definition from elements to subgroups. If $H, K \subseteq G$, we write $[H, K] = \langle [h, k] | h \in H, k \in K \rangle$. We note that the group generated by is absolutely essential, and that it is in fact rarely the case that $[H, K]$ is outright equal to the collection of commutators. We make a few observations. Note that $[H, K] = 1$ if and only if $H \subseteq \mathbf{C}_G(K)$ and that $[H, K] = [K, H]$, the group generated by all of the inverses of the commutators.

Lemma 18.1. Both H and K are contained in $\mathbf{N}_G([H, K])$.

Proof. It suffices to show that $H \subseteq \mathbf{N}_G([H, K])$. Let $x, y \in H$ and let $k \in K$. We compute $[xy, k] = [x, k]^y[y, k]$. Solving this equation for $[x, k]^y$ yields $[xy, k][y, k]^{-1} = [x, y]^k$. As $[xy, k], [y, k] \in [H, K]$, it follows that $[H, K]^y \subseteq [H, K]$ since we have shown that $[x, k]^y \in [H, K]$ for all $[x, k] \in [H, K]$ and $y \in H$. So $H \subseteq \mathbf{N}_G([H, K])$. □

We note that $[G, G] = G'$, the derived subgroup.

Lemma 18.2. $K \subseteq \mathbf{N}_G(H)$ if and only if $[H, K] \subseteq H$.

Proof. Note that $[H, K] \subseteq H$ if and only if $[h, k] \in H$ for all $h \in H$ and $k \in K$. Since $[h, k] = h^{-1}h^k$, this commutator is in H if and only if $h^k \in H$ for all $h \in H$ and $k \in K$, which happens if and only if K normalizes H. □

Suppose that $G \to \overline{G}$ is a homomorphism. Then $[\overline{H}, \overline{K}] = \overline{[H, K]}$. That is, commutators are preserved by homomorphisms.

Corollary 18.2. Let $N \subseteq H \subseteq G$. Then $H/N \subseteq \mathbf{Z}(G/N)$ if and only if $[H, G] \subseteq N$.

Proof. Let $\overline{G} = G/N$. Then $\overline{H} \subseteq \mathbf{Z}(\overline{G})$ if and only if $[\overline{H}, \overline{G}] = 1$. Since $\overline{[H, G]} = [\overline{H}, \overline{G}]$, so we must have $[H, G]$ is contained in the kernel of the bar map, which is N. □

Definition 18.1. We define the *triple commutator* $[x, y, z] = [[x, y], z]$ and similarly, we define $[H, K, L] = [[H, K], L]$. We can of course generalize this to the nth commutator where we associate from the left.

As a HUGE caution, we point on that $[H, K]$ is the *group generated by* commutators $[h, k]$, and we therefore cannot take $[[H, K], L] = \langle [[h, k], l] \rangle$.

Recall that a group G is *nilpotent* if there exists ac central series. A *central series* in G is a normal series where $1 = H_r \subseteq H_{r-1} \subseteq \dots H_1 = G$ where each $H_i/H_{i+1} \subseteq \mathbf{Z}(G/H_{i+1})$ for $1 \leq i < r$. By our previous corollary, we know that this is equivalent to saying that we must have $[H - i, G] \subseteq H_{i+1}$ for all valid i.

Notice that $[G, G] = [H-1, G] \subseteq H_2$, and $[G, G, G] = [[G, G], G] \subseteq [H_2, G] \subseteq H_3$ and so in general, $[G, G, \dots G] \subseteq H_m$, where we have m copies of G on the inside of the commutator on the left hand side. As a shorthand for this, we write G^m to denote $[G, G, \dots, G]$ m times. Note that $G^1 = G$ and $G^2 = G'$, but that $G^3 = [G', G]$, which is NOT G''. So in general, it is NOT the case that $G^m = G^{(m)}$ for the same reason we gave before about $[H, K, L]$. An alternate notation for G^m is $\gamma^m G$, but we use the former in these notes.

For two more remarks, we note that $G = G^1$ contains G^2 which contains G^3, etc. Furthermore, $G^{m+1} = [G^m, G] \subseteq G^m$ since $G^m \lhd G$ so G normalizes G^m and this $[G^m, G] \subseteq G^m$ by a previous corollary.

Definition 18.2. For any subgroup G, we call $\{G^m\}$ the *lower central series* of G.

We defined the lower central series for an arbitrary group G, but we actually have that a group G is nilpotent if and only if this series reaches one eventually; i.e. if there is an integer k for which $G^k = 1$.

There is some logic to why this series is known as the lower central series. We showed earlier that $G^m \subseteq H_m$ where H_m is an arbitrary term in any central series for G, so in a way, the central series obtained by looking at the subgroups G^m is indeed the lowest such series in a sense.

Definition 18.3. We say that a nilpotent group G has *nilpotence class* m if $G^{m+1} = 1$ but $G^m > 1$.

To get a better feel for what the nilpotence class of a group is, we determine the types of groups with nilpotence class 1 and 2. If G has nilpotent class 1, then $G^1 = G \neq 1$ by $G^2 = G' = 1$. These are precisely the abelian groups. If G has nilpotence class 2, then $G^2 = G' \neq 1$ but $G^3 = 1$; that is $[G', G] = 1$ and therefore $G' \subseteq \mathbf{Z}(G)$. Thus $G/\mathbf{Z}(G)$ is abelian but G is not abelian.

Let P be a p-group, and write $\Omega_1(P) = \langle x \in P | x^p = 1 \rangle$. Although it is not true in general that $\Omega_1(P)$ has exponent p, it is a theorem of Phillip Hall that if P has nilpotence class strictly less than p then $\Omega_1(P)$ has exponent p. We will not prove this theorem, but next time we WILL prove the following.

Lemma 18.3. Assume that P has nilpotence class 2 and that $p > 2$. Then $\Omega_1(P)$ has exponent p.

19 03-04-10

We begin today by proving a somewhat baby version of P.Hall's general theorem:

Theorem 19.1. If P is a p-group with nilpotence class less than p then $\{x \in P \mid x^p = 1\}$ forms a subgroup.

Proof. We prove only the case where P has nilpotence class 2 and $p > 2$. Let $x, y \in P$ with $x^p = 1 = y^p$. We want that $(xy)^p = 1$. Now $(xy)^p = (xy)(xy)\dots xy$. The general idea of the proof is to group together all of the x's and y's, at the cost of some commutators, and then examine what we have. Now $yx = xy[y,x]$, so we have $(xy)(xy)\dots xy = xxy[y,x]y(xy)\dots xy$. As P has nilpotence class 2, we know that all commutators are central, so $xxy[y,x]y(xy)\dots xy = xxyy(xy)\dots(xy)[y,x]$. I now repeat my previous action, moving the next x over the y at the cost of the commutator $[y,x]$, which is central. So I have $xxyxy[y,x]\dots xy[y,x]$ which is equal to $xxyxy\dots xy[y,x]^2$. Moving this x across the second y gives me $xxxyyy\dots[y,x]^{1+2}$. So the first x to move across contributed 1 commutator $[y,x]$, then second contributed 2 commutators $[y,x]$, etc. As I have $p-1$ copies of x to move and the ith x contributes i commutators, I end up with $x^p y^p [y,x]^{1+2+\dots+(p-1)}$. As the sum of the first $(p-1)$ integers is $\frac{p(p-1)}{2}$ and both x^p and $y^p = 1$, we have $[y,x]^{p(p-1)/2}$. But $p(p-1)/2$ is divisible by p since $p > 2$. Yet $([y,x]^p)^{(p-1)/2} = ([y^p,x])^{(p-1)/2}$ since the map $[\bullet, x] \to \mathbf{Z}(G)$ is a homomorphism, as we saw last time. Yet $y^p = 1$, so $[y^p, x] = [1,x] = 1$, and so $[y,x]^{p(p-1)/2} = 1$, and we have what we want. □

We now introduce a favorite commutator identity of Isaacs', which is due to Witt.

Lemma 19.1. Let $x, y, z \in G$. Then $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$.

This identity of Witt yields a very nice lemma called the three subgroups lemma. According to Isaacs, any proof that can use the three subgroups lemma is a proof worth knowing; the use of this lemma makes any other proof worthwhile.

Lemma 19.2. Suppose that $H, K, L \subseteq G$ and that both $[H,K,L] = [K,L,H] = 1$. Then $[L,H,K] = 1$.

Proof. We want to prove that $[L,H] \subseteq \mathbf{C}_G(K)$. It is enough to show that $[l,h] \in \mathbf{C}_G(K)$ for all $l \in L$ and $h \in H$. Element wise, what we really want is to show that $[[l,h],k] = 1$. Equivalently, we want to show that $[l,h^{-1},k] = 1$ for all $l \in L, h^{-1} \in H$, and $k \in K$. We have by assumption that $[h,k^{-1},l] = 1$ and therefore that $[h,k^{-1},l]^k = 1$ and that $[k,l^{-1},h] = 1$ and therefore that $[k,l^{-1},h]^l = 1$. Thus by the Witt identity, it follows that $[l,h^{-1}k]^h = 1$, which gives us that $[l,h^{-1},k] = 1$ by conjugating both sides of the previous equation by h^{-1}. □

If we recall that commutators map to commutators under homomorphisms, then we have the following corollary of the three subgroups lemma which is often associated with the three subgroups lemma.

Corollary 19.1. Let $N \lhd G$ and let $H, K, L \subseteq G$. Assume that $[H, K, L] \subseteq N$ and that $[K, L, H] \subseteq N$. Then $[L, H, K] \subseteq N$.

Proof. Apply the three subgroups lemma in $\overline{G} = G/N$ to $\overline{H}, \overline{K}$, and $\overline{L}$. Also, use that $\overline{[H, K, L]} = [\overline{H}, \overline{K}, \overline{L}]$. □

Theorem 19.2. Let G be arbitrary. Then $[G^n, G^m] \subseteq G^{n+m}$.

Proof. Notice that we do NOT have equality here since $[,]$ is NOT associative. We induct on m. If $m = 1$ then we have that $[G^n, G] = G^{n+1}$ by the definition of G^{n+1} so our base case is valid. So assume that $m > 1$ and that the theorem holds for all smaller values. Now $[G^n, G^m] = [G^m, G^n]$ which is $[G^{m-1}, G, G^n]$. We want that $[G^{m-1}, G, G^n] \subseteq G^{n+m}$. Note that G^{n+m} is characteristic in G and therefore it is certainly normal. Now $[G, G^n, G^{m-1}] = [G^{n+1}, G^{m-1}] \subseteq G^{n+m}$ by induction as $m - 1 < m$. Also, $[G, G^{m-1}, G] \subseteq [G^{n+m-1}, G]$ since $[G^n, G^{m-1}] \subseteq G^{n+m-1}$ by induction. But $[G^{n+m-1}, G] = G^{n+m}$, so we have the result by the corollary to the three subgroups lemma. □

Recall that all nilpotent groups are solvable. We can then wonder how that nilpotence class of a group relates to its derived length for a nilpotent group. Recall that we have a sort of asymmetry with our definitions here; if k is the nilpotence class of G, then $G^k \neq 1$ but $G^{k+1} = 1$ and if d is the derived length of G then $G^{(d)} = 1$ but $G^{(d-1)>1}$. To determine this relationship, we make a quick definition.

Definition 19.1. A *weight n commutator* in G is a commutator of n copies of G, just with any association as opposed to left association.

As an important example, we use the derived subgroup. Now $G' = [G, G]$, so $G'' = [G', G'] = [[G, G], [G, G]]$, so we see that G'' is a weight four commutator, and that $G^{(3)} = [G'', G'']$ is therefore a weight $8 = 2^3$ commutator. From here, we notice a pattern; namely, that $G^{(m)}$ is a weight 2^m commutator.

Lemma 19.3. A weight n commutator in G is contained in G^n.

Proof. We induct on n. If $n = 1$, we have $G^1 = G$. If $n > 1$, then the weight n commutator looks like $[W_r, W_s]$, where W_r is a weight r commutator and W_s is a weight s commutator with $r + s = n$. Now both r and s are greater than 0, which makes both r and s less than n. [i.e., there is no such thing as a weight 0 commutator]. By induction, we then have $[W_r, W_s] \subseteq [G^r, G^s] \subseteq G^{r+s} = G^n$ by the previous lemma. □

Returning to our example, we saw that the derived subgroup $G^{(m)}$ had weight 2^m and so by this lemma we know that $G^{(m)} \subseteq G^{2^m}$.

Corollary 19.2. Let G be nilpotent of class k and derived length d. Then $d \leq 1 + \log_2(k)$.

Proof. We know that $1 < G^{(d-1)} \subseteq G^{2^{d-1}}$, so we have that $2^{d-1} \leq k$. Thus $d - 1 \leq \log_2(k)$ and the result follows. □

19.1 Commutators and Actions

Let A act via automorphisms on G. Then $[G, A] \subseteq G$ since G is normal in the semi-direct product of G by A. We can write this subgroup as $\langle g^{-1}g^a \mid g \in G, a \in A \rangle$. Note that this subgroup is A invariant, which again follows by viewing G and A within the semi-direct product and noting that this subgroup is normal. In fact, $[G, A] \subseteq G$ since G is normal in the semidirect product.

We now state a lemma and begin its proof, which we will finish next time.

Lemma 19.4. Let A act via automorphisms on G, and let $H \subseteq G$ be a subgroup. TFAE:

1. A fixes all right cosets of H in G.
2. A fixes all left cosets of H in G.
3. $[G, A] \subseteq H$

Proof. We first show that (1) and (2) are equivalent. Note that $Hx = \{y^{-1} | y \in x^{-1}H\}$ and $xH = \{y^{-1} | y \in Hx^{-1}\}$. Then if Hx is invariant, we know that $(Hx)^{-1}$ is A invariant, and vice versa. □

20 Problem Set 6

Problem 29. Let A act via automorphisms on G and assume that $(|G|, |A|) = 1$ and that one of A or G is solvable. Suppose that $H \subseteq G$ is A-invariant. Show that $|H : H \cap C|$ divides $|G : C|$, where $C = \mathbf{C}_G(A)$.

Problem 30. (a) Let A be maximal among abelian normal subgroups of a finite nilpotent group G. Show that $A = \mathbf{C}_G(A)$ and that $|G : A| \leq |A|!$.

(b) Show that there exists a function $f(n)$ defined on the natural numbers so that if G is a finite group all of whose abelian subgroups have order at most n, then $|G| \leq f(n)$.

Problem 31. Let U and H be groups, where U is nontrivial, and let B be the set of all functions from H into U. Make B into a group be defining multiplication pointwise. Note that B is really just the direct product of $|H|$ many copies of U. Let H act on B by $f^h(x) = f(xh^{-1})$ for $h, x \in H$ and $f \in B$. Then $G = B \rtimes H$ is the **wreath product** of U by H, denoted $U \wr H$. We view B and H as subgroups of G, and we call B the **base group** of the wreath product.

(a) Show that $\mathbf{C}_B(H) \cong U$ and that $\mathbf{C}_H(B) = 1$.

(b) Show that every subgroup of H is $\mathbf{C}_H(f)$ for some $f \in B$.

NOTE: Wreath products can be used to build examples and counterexamples.

Problem 32. Let $A \lhd G$ where A is abelian.

(a) If $g \in G$, write $[A, g] = \{[a, g] \mid a \in A\}$. Show that $[A, g]$ is a group and that $|[A, g]||\mathbf{C}_A(g)| = |A|$.

(b) If G/A is cyclic, show that every element of G' is a commutator and that $|G'| = |A|/|Z|$, where $Z = \mathbf{Z}(G) \cap A$.

(c) If G/A is cyclic, show that $|G^n| \geq |A|/|Z|^{n-1}$, where Z is as in (b).

Problem 33. Let $G = C \wr C$ where C has prime order p. (The wreath product G thus has order p^{p+1}) and the base group is elementary abelian of order p^p.) Show that G has nilpotence class p and that $G = \Omega_1(G)$ contains an element of order p^2.

NOTE: A group of order p^n always has nilpotence class at most $n-1$. When its class is exactly $n-1$, we say it has **maximal class**.

21 03-08-10

We begin by finishing the lemma we stated last time.

Lemma 21.1. Let A act via autos on G, with $H \subseteq G$. TFAE:

1. All right cosets of H in G are invariant.
2. All left cosets of H in G are invariant.
3. $[G, A] \subseteq H$

Proof. To see that one and two are equivalent, we use the fact that the map $X \mapsto \{x^{-1} | x \in X\}$ swaps left and right cosets. We note that both (2) and (3) imply that H is A-invariant. If (2) holds. then H is A-invariant as H is a left coset of H in G. If (3) holds, we need that $[H, A] \subseteq H$. Yet $[H, A] \subseteq [G, A] \subseteq H$, so H is A-invariant. Now to see that (2) and (3) are equivalent, we can assume now WLOG that H is A-invariant. Now statement (2) happens if and only if $(gH)^a = gH$ for all $g \in G$ and $a \in A$. However, this holds if and only if $g^a H = gH$, or equivalently, that $g^a \in gH$. This will be the case whenever $g^{-1}g^a \in H$, which is to say that $[G, A] \subseteq H$. □

Corollary 21.1. Assume that A acts on G, that $(|A|, |G|) = 1$ and that either A or G is solvable. Then $G = [G, A]\mathbf{C}_G(A)$.

Proof. By the previous lemma, we know that A acts trivially on $G/[G, A]$. Write $\overline{G} = G/[G, A]$. We know that $\mathbf{C}_{\overline{G}}(A) = \overline{\mathbf{C}_G(A)}$ as fixed points come from fixed points. So $\overline{G} = \overline{\mathbf{C}_G(A)}$, and we have that $G = \mathbf{C}_G(A)[G, A]$. □

Theorem 21.1. Let A act on G with $(|A|, |G|) = 1$. Then $[G, A, A] = [G, A]$.

Proof. It is clear that $[G, A, A] \subseteq [G, A]$ since $[G, A] \subseteq G$. We must therefore establish the other containment and it suffices to show that $[g, a] \in [G, A, A]$ for all $g \in G$ and $a \in A$. Since $\langle a \rangle$ is solvable (it is cyclic), we know that $G = [G, \langle a \rangle]\mathbf{C}_G(\langle a \rangle)$ by the previous corollary. Write $g = cx$ for some $c \in \mathbf{C}_G(\langle a \rangle)$ and $x \in [G, \langle a \rangle]$. Compute $[g, a] = [cx, a] = [c, a]^x[x, a] = [x, a]$ since c centralizes $\langle a \rangle$. Yet $[x, a] \in [G, \langle a \rangle, \langle a \rangle] \subseteq [G, A, A]$, as desired. □

We now sway a bit from coprime actions. If A acts on G via automorphisms of course, suppose that $[G, A, A, \ldots, A] = 1$ where we have G bracked with n A's. What can we say about the group A in this case? We give a first easy result.

Corollary 21.2. In the above situation, assume further that G acts faithfully. Then every prime p dividing $|A|$ also divides $|G|$.

Proof. Let $P \in \mathrm{Syl}_p(A)$ with $P > 1$. Then $[G, P, P, \ldots, P] \subseteq [G, A, A, \ldots, A] = 1$. If p does not divide the order of G, then our previous result yields that $1 = [G, P, P, \ldots, P] = [G, P]$. Yet if $[G, P] = 1$ then we know that P acts trivially on G, and P is in the kernel of the action of A. However, we assumed that the action of A was faithful, so $P \subseteq \mathbf{C}_G(A) = 1$, and this is a contradiciton. □

Theorem 21.2. Assume that $[G, A, A, \ldots, A] = 1$ where A appears in this commutator n times, and assume that the action is faithful. Then A is solvable with $dl(A) \leq (n - 1)$.

Proof. Begin by dropping the assumption that A acts faithfully on G. Call K the kernel of the action, so that $K = \mathbf{C}_A(G)$. We will show that $A^{(n-1)} \subseteq K$. Note that in the case where the action is faithful, this yields the result. We induct on n. If $n = 1$, then we need that $A^{(0)} = A \subseteq K$. Yet we have this as $[G, A] = 1$ implies that A acts trivially on G, and then $A = K$. Now assume that $n > 1$ and consider the action of A on $[G, A]$. We have $[[G, A], A, A, \ldots, A] = 1$ with $(n - 1)$ copies of A outside of $[G, A]$ by the left associativity of commutators. By induction, $A^{(n-2)}$ acts trivially on $[G, A]$, so $[G, A, A^{(n-2)}] = 1$. Throwing away information, [at this point, Isaacs said that this part of the proof makes him very sad since he knows he shouldn't throw away information] we have that $[G, A^{(n-2)}, A^{(n-2)}] = 1$. Also, $[A^{(n-2)}, G, A^{(n-2)}] = 1$ since $[A^{(n-2)}, G, A^{(n-2)}] = [G, A^{(n-2)}, A^{(n-2)}]$ because $[G, A^{(n-2)}] = [A^{(n-2)}, G]$. By the three subgroups lemma, this gives us that $[A^{(n-2)}, A^{(n-2)}, G] = 1 = [A^{(n-1)}, G] = 1$, so we see that $A^{(n-1)} \subseteq K$. □

Although the above theorem is true and can be proved quite concisely, there is a theorem of P. Hall which says much more. In the above situation, the group A can actually be shown to be nilpotent, and in this case, the nilpotence class of A is at most $\frac{n(n-1)}{2}$. Since $dl(A) \leq 1 + \log_2(k)$, we would actually have then that $dl(A) \leq 1 + \log_2(\frac{n(n-1)}{2})$, so $dl(A) < 2\log_2(n)$, which is a much better bound.

Theorem 21.3 ((Thompson))**.** Let A act on G where $A = PQ$ where P is a p-group, and where p does not divide $|Q|$.[Note that Q need not be a q-group]. Assume that G is a p-group. Suppose further that $\mathbf{C}_G(P) \subseteq \mathbf{C}_G(Q)$. Then Q acts trivially on G. i.e., $\mathbf{C}_G(Q) = G$.

Proof. We induct on $|G|$. Without loss, $G > 1$. Consider $[G, Q]$. This group is A-invariant since G is A invartiant and Q is A-invariant since $Q \lhd A$. So the action of A on $[G, Q]$ satisfies the hypotheses. If $[G, Q] < G$, then the inductive hypothesis implies that $[G, Q, Q] = 1$. Yet G is a p-group and p does not divide $|Q|$, so by our earlier lemma we know that $[G, Q, Q] = [G, Q]$ so $[G, Q] = 1$. We may therefore assume that $[G, Q] = G$. Note that $[G, P]$ also admits the same action that was allowed on $[G, Q]$ for the same reason; G is A-invariant and P is A-invariant as $P \lhd A$. However, we know that $[G, P] < G$ since $G \rtimes P$ is nilpotent (in fact, it is a p-group as $|G \rtimes P| = |G||P|$). Now $[P, Q, G] = 1$ since $[P, Q] = 1$ and $[G, P, Q] = 1$ by induction. Therefore the three subgroups lemma tells us that $[Q, G, P] = 1$. As $[Q, G] = [G, Q] = G$, we have that $[G, P] = 1$, so Q acts trivially. □

22 03-11-10

Definition 22.1. A group G is π-*separable* if there exist normal subgroups $1 = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_r = G$ where each G_{i+1}/G_i is either a π-group or a π'-group. We say that G is π-*solvable* if, in addition, the G_{i+1}/G_i which are π-groups are solvable.

In the case where $\pi = \{p\}$, then p-solvable is equivalent to being p-separable, as p-groups are necessarily solvable. This leads to some confusion in the literature. Also, we give a short proof that G is solvable if and only if G is p-solvable for all primes p dividing $|G|$.

Proof. Assume that G is p-solvable for all primes p. We want to show that G is solvable. If G is not simple, then there exists $N \lhd G$ with $1 < N \lhd G$ and $N \leq G$. By induction on $|G|$, this gives us that both N and G/N are solvable, and hence G is solvable. If G is simple, then as G must be a p-group by p-solvability. As p-groups are nilpotent and thus solvable, we have the result. Now assume that G is solvable. Then there exists a subnormal chain $1 = K_0 \lhd K_1 \lhd \ldots \lhd K_r = G$ where each factor K_{i+1}/K_i has prime order, so the group is p-solvable as each of these factors is p-solvable. □

As G is π-separable and $G > 1$, the group G_1(WLOG) in the chain is either a normal π-group or a normal π'-group. Hence when we have a nontrivial π-separable group, we know that either $\mathbf{O}_\pi(G)$ or $\mathbf{O}_{\pi'}(G)$ is nontrivial.

The next lemma is from a very popular paper of Hall and Higman. The following lemma is so useful that many people still refer to it by the numbering given in the paper of Hall and Higman. We maintain that notation here.

Lemma 22.1 (1.2.3)**.** Let G be π-separable. Assume that $\mathbf{O}_{\pi'}(G) = 1$. Then $\mathbf{C}_G(\mathbf{O}_\pi(G)) \subseteq \mathbf{O}_\pi(G)$.

Proof. Let $C = \mathbf{C}_G(\mathbf{O}_\pi(G))$, and suppose for the sake of contradiction that $C \nsubseteq \mathbf{O}_\pi(G)$. Let $D = C \cap \mathbf{O}_\pi(G)$. We have under this assumption that $C > 1$ or C would of course be contained within $\mathbf{O}_\pi(G)$, and we have that $C > D$. Now C/D is a non-trivial and π-separable group; note that D is normal as it is the intersection of two normal subgroups. Let $U/D = \mathbf{O}_\pi(C/D)$. Then U/D is a π-group and D is a π-group since $D \subseteq \mathbf{O}_\pi(G)$. Thus U is a π-group. Now $U \lhd G$ (in fact, U is characteristic in G), so $U \subseteq \mathbf{O}_\pi(G)$. Also, $U \subseteq C$, so $U \subseteq D$, and we must have that $(U/D) = 1$; that is, C/D is a group with $\mathbf{O}_\pi(C/D) = 1$. By our above reasoning about π-separable groups, this means that $\mathbf{O}_{\pi'}(C/D) > 1$; write $V/D = \mathbf{O}_{\pi'}(C/D)$. So $V > D$, and by the same reasoning as before, we know that $V \lhd G$. Additionally, we know that $D \lhd V$ with D a π-group and $|V : D|$ being π'. Therefore by the SZT, we know that there exists a complement K for D in V. Note that $D \subseteq \mathbf{Z}(C)$ since C centralizes D because $D \subseteq \mathbf{O}_\pi(G)$ and C centralizes $\mathbf{O}_\pi(G)$. So $D \subseteq \mathbf{Z}(V)$ since $D \subseteq V \subseteq C$ and therefore D normalizes K. So $V = DK \subseteq \mathbf{N}_V(K)$, and we have that K is normal in V. Since $|K| = |V : D|$ is π' and $|V : K| = |D|$ is a π-number, we have that $K \subseteq \mathbf{O}_{\pi'}(V) \subseteq \mathbf{O}_{\pi'}(G)$. This makes $K = 1$ and $D = V$ by the diamond lemma, and this is our contradiction as we know that $V > D$. □

We now proceed to see an application of Thompson's $P \times Q$ theorem.

Theorem 22.1. Assume that G is p-solvable. Let $N \subseteq G$ be p-local, and recall that this means that N is the normalizer in G of P for some nontrivial p-group P. Then $\mathbf{O}_{p'}(N) \subseteq \mathbf{O}_{p'}(G)$.

Proof. Before giving the proof of the theorem, we need a lemma.

Lemma 22.2. Let $K \lhd G$ where p does not divide $|K|$. Write $\overline{G} = G/K$. Let $N \subseteq G$ be p-local. Then $\overline{N}$ is p-local in $\overline{G}$.

Proof. As N is p-local, we know that we can write $N = \mathbf{N}_G(P)$ for $P > 1$ a p-group of G. We will show that $\overline{N} = \mathbf{N}_{\overline{G}}(\overline{P})$. Note that $\overline{P} > 1$ or else we would have $P \subseteq K$ which is a contradiction since $P > 1$ is a p-group and K is a p'-group. Also, we know that $P \lhd N$ and therefore $\overline{P} \lhd \overline{N}$, hence $\overline{N} \subseteq \mathbf{N}_{\overline{G}}(\overline{P})$. We need to show equality. write $\overline{M} = \mathbf{N}_{\overline{G}}(\overline{P})$, where we assume that $K \subseteq M$. We know that $\overline{P} \lhd \overline{M}$ so $\overline{PK} \lhd \overline{M}$ and hence $PK \lhd M$ by the correspondence theorem. Note that $P \in \mathrm{Syl}_p(PK)$. By the Frattini argument, we know that $M = \mathbf{N}_M(P)PK = \mathbf{N}_M(P)K$. Yet $\mathbf{N}_M(P) \subseteq \mathbf{N}_G(P) = N$ so $\mathbf{N}_M(P)K \subseteq NK$ and so $M \subseteq NK$ and $\overline{N} \subseteq \overline{N}$, hence $\overline{N} = \overline{M}$. □

First, assume that $\mathbf{O}_{p'}(G) = 1$. Let $Q = \mathbf{O}_{p'}(N)$ so that p does not divide $|Q|$. Notice that $Q \lhd N$ and that $N = \mathbf{N}_G(P)$ for $P > 1$ a non-trivial p-group since N is assumed to be p-local; hence $P \lhd N$. Thus the group $PQ = P \times Q$. Let $U = \mathbf{O}_p(G) > 1$ since G is p-solvable. PQ acts on U. Look at $\mathbf{C}_U(P)$. Now $\mathbf{C}_U(P) \subseteq \mathbf{N}_U(P) \subseteq \mathbf{N}_G(P) = N$ and in fact $\mathbf{C}_U(P) \subseteq (U \cap N) \lhd N$ since

$U \lhd G$. Also, $N \cap U$ is contained in U so $N \cap U$ is a p-group. So we have $Q \lhd N$ with $(N \cap U) \lhd N$ and $Q \cap (N \cap U) = 1$, so Q centralizes $N \cap U$ as disjoint normal subgroups commute. So $Q \subseteq \mathbf{C}_N(N \cap U) \subseteq \mathbf{C}_G(N \cap U)$. So Q centralizes $\mathbf{C}_U(P)$. By the $P \times Q$ theorem, we have that Q acts trivially on U and $Q \subseteq \mathbf{C}_G(U) \subseteq U$ by lemma 1.2.3, thus $Q = 1$. But $Q = \mathbf{O}_{p'}(N)$, so we have the first part of the theorem. We do the second part of the theorem next time.

□

23 03-16-10

We begin by finishing the theorem we started last time.

Theorem 23.1. Suppose G is p-solvable and N is a p-local subgroup. Then $\mathbf{O}_{p'}(N) \subseteq \mathbf{O}_{p'}(G)$.

Proof. We have the result if $\mathbf{O}_{p'}(G) = 1$. Let $\overline{G} = G/\mathbf{O}_{p'}(G)$. Then $\mathbf{O}_{p'}(\overline{G}) = 1$, $\overline{N}$ is p-local by our lemma from last time. By our result from last time, we know that $\mathbf{O}_{p'}(\overline{N}) \subseteq \mathbf{O}_{p'}(\overline{G}) = 1$. Let $Q = \mathbf{O}_{p'}(N)$. Then $\overline{Q} \lhd \overline{N}$ by the correspondence theorem so $\overline{Q} \subseteq \mathbf{O}_{p'}(\overline{N}) = 1$. hence Q is contained in the kernel of the bar map which is $\mathbf{O}_{p'}(G)$, which is what we want. □

Theorem 23.2 (Fitting)**.** Let A act on G where G is abelian and $(|G|, |A|) = 1$. Then $G = [G, A] \times \mathbf{C}_G(A)$.

Proof. We already know that $G = [G, A]\mathbf{C}_G(A)$ from a lemma on March 9th. It is therefore enough to show that $[G, A] \cap \mathbf{C}_G(A) = 1$ since the normality of both groups is free since G is abelian. Let $\theta : G \to G$ be defined by $\theta(x) = \prod_{a \in A} x^a$. Note that this product is well defined since G is abelian and that $\theta(x)$ is A-invariant, as the action of A on the product simply permutes the order, which is irrelevant since G is abelian. As $\theta(x)$ is A-invariant, we have $\theta(x) \in \mathbf{C}_G(A)$. We claim that θ is actually a homomorphism. All products are assumed to be over all $a \in A$. Now $\theta(xy) = \prod (xy)^a = \prod x^a y^a = \prod x^a \prod y^a$, where this last equality holds since A is abelian, we can separate all the x's and y's. So we see that this is $\theta(x)\theta(y)$ and therefore θ is a homomorphism. Also, $\theta(x^b)$ for $b \in A$ as $\theta(x^b) = \prod_{a \in A} (x^b)^a = \prod x^{ba} = \theta(x)$ since ab runs over all of A. Thus θ is constant on an A-orbit of G. Now what is $\theta([x, b])$ for $x \in G$ and $b \in A$. Well $\theta([x, b]) = \theta(x^{-1}x^b) = \theta(x)^{-1}\theta(x) = 1$, so $[G, A] \subseteq \ker(\theta)$. Now let $x \in [G, A] \cap \mathbf{C}_G(A)$. Then $1 = \theta(x) \prod x^a = x^{|A|}$ since $x \in \mathbf{C}_G(A)$ and so $x^a = x$ for all $a \in A$. Hence $o(x)$ divides $|A|$. But $x \in G$ so $o(x)$ also divides $|G|$ and we must have $o(x) = 1$ and hence $x = 1$. □

Corollary 23.1. Let A be a p'-group acting on an abelian p-group G. Assume that A fixes every element $x \in G$ with $x^p = 1$. Then A acts trivially on G.

Proof. Write $G = [G, A] \times \mathbf{C}_G(A)$. If $o(x) = p$ then $x \in \mathbf{C}_G(A)$, so $x \notin [G, A]$. Thus $[G, A]$ is a p-group with no elements of order P, and this makes $[G, A] = 1$. $\square$

We note that if we drop the assumption that the group G be abelian, we can find a counterexample. If we look at the action of $\mathbb{Z}_3$ on the quaternions, then $\mathbb{Z}_3$ sends i to j, j to k, and k back to i, but this action fixes -1, the only element of order 2. However, this counterexample is slightly phony, as it uses the prime two, which often causes trouble. If we remove the hypothesis that the group G be abelian and then specify that $p \neq 2$, we can obtain a stronger result.

Theorem 23.3. Let A act on a p-group G with $p > 2$. Assume that A is p' and that it fixes all $x \in G$ with $o(x) = p$. Then A acts trivially on G.

Proof. In order to do this proof, we will use something called the **Baer trick**. We state this formally as a lemma.

Lemma 23.1. Let G be a class 2 p-group with $p > 2$. Then there exists a multiplication $\star$ on G such that:

(a) $(G, \star)$ is abelian.

(b) If $xy = yx$ in the original group, then $x \star y = xy$.

(c) $o(x) = o_\star(x)$ for all $x \in G$. That is, the orders of elements are preserved under the new operation.

(d) $\mathrm{Aut}(G) \subseteq \mathrm{Aut}((G, \star))$. This tells us that if A acts on G via automorphisms, that A still acts on the group $(G, \star)$.

Before beginning the "proof" of the lemma, we make a quick note. If $|G|$ is odd, then the map that sends every element to its square is injective, and since G is finite, this makes the square map a bijection, although it need not be a homomorphism. As such, it makes sense to define the square root map for such groups to be the inverse of the squaring map. In this case, if x and y commute, then $\sqrt{xy} = \sqrt{x}\sqrt{y}$ since if x and y commute, we can distribute in ANY power map. With this in mind, we begin a sketchy proof of the Baer trick lemma.

Proof. Let $x \mapsto \sqrt{x}$ be the inverse of the square map. If $H \subseteq G$ and $h \in H$, then $\sqrt{h} \in H$ since for all $h \in H$ we have $h^2 \in H$. Now given $x, y \in G$, define $x \star y = xy\sqrt{[y, x]}$. We prove a few of the above facts, glossing over a few. We first show that $(G, \star)$ is abelian. Now $(y \star x) = yx\sqrt{[x, y]} = xy[yx]\sqrt{[x, y]}$. Now $[y, x] = [x, y]^{-1}$, so we have $y \star x = xy[x, y]^{-1}\sqrt{[x, y]}$. Since G has class two, we have $[x, y]^{-1}$ and $\sqrt{[x, y]}$ commute, so $y \star x = xy\sqrt{[x, y]^{-2}}\sqrt{[x, y]} = xy\sqrt{[x, y]^{-1}} = xy\sqrt{[y, x]}$, which is by definition $x \star y$. We omit the proof that $(\star)$ is associative. By the definition of the star map we have property (b), and we see that $1_\star = 1$ and since x and x^{-1} commute, we have $x \star x^{-1} = xx^{-1} = 1 = 1_\star$, so we have inverses in $(G, \star)$. Also, we get that $x = x_\star^n$ since x commutes with

x^{n-1} and so $x^n = xx^{n-1} = x \star x^{n-1}$. By induction (if we are to be formal), $x^{n-1} = x_\star^{n-1}$, so $x \star x^{n-1} = x \star x_\star^{n-1} = x_\star^n$; therefore (c) holds. We claim that (d) holds since $\star$ is uniquely defined in terms of the group operation; this is the typical argument that things which are uniquely determined remain fixed. This, modulo a hand wave, finishes the proof of the lemma. □

We now proceed to the proof of the theorem. We will induct on $|G|$. By the inductive hypothesis, if $H < G$ is A-invariant, then we have $[H, A] = 1$. Therefore if $[G, A] < G$, then by the above, we know that $[G, A, A] = 1$ since $[G, A]$ is A-invariant. However, $[G, A, A] = [G, A]$ since $|G|$ and $|A|$ are coprime, so we have what we want if $[G, A] < G$. We may therefore assume that $[G, A] = G$. We have that $G' < G$ since G is a p-group, so $[G', A] = 1$ by the above. Throwing away information,we have $[G', A, G] = 1$. Yet $[G, G', A] \subseteq [G, A] = 1$, so the three subgroups lemma tells us that $[A, G, G'] = 1$. However, $[A, G, G'] = [G, G']$ since we are assuming that $[G, A] = [A, G] = G$, so this tells us that $[G, G'] \subseteq \mathbf{Z}(G)$. This tells us that the class of G is less than or equal to 2. We can then construct $(G, \star)$ as in Baer's lemma. By property (d), we have that A still acts on $(G, \star)$ fixing elements of order p since the Baer trick preserves orders. By the abelian case, we know that A acts trivially on $(G, \star)$, and this gives us that A acts trivially on G.

□

24 Problem Set 7

Problem 34. Let A act faithfully via automorphisms on an abelian group B. Assume that A is solvable of derived length n and that $(|A^{(n-1)}|, |B|) = 1$. Show that $G = B \rtimes A$ has derived length $n+1$, and deduce that every positive integer can occur as a derived length.

HINT: If $G^{(n-1)}$ is abelian, show that $[B, A^{(n-1)}, A^{(n-1)}] = 1$.

Problem 35. Suppose that $G = NA$, where $N \lhd G$ and $A \subseteq G$, and let M be the final term in the series $N \supseteq [N, A] \supseteq [N, A, A] \supseteq \ldots$. Also, write A^∞ to denote the final term in the lower central series for A.

(a) Show that $A \lhd\lhd G$ if and only if $M \subseteq A$.

(b) If $M \subseteq A$ show that $M \subseteq A^\infty$.

Problem 36. Let G be π-separable and write $A = \mathbf{O}_\pi(G)$ and $B = \mathbf{O}_{\pi'}(G)$. Show that $AB \subseteq \mathbf{Z}(G)$ if and only if G is abelian.

Problem 37. Let G be a π-separable group and recall that this guarantees that G has a Hall π-subgroup. Suppose that G has an abelian Hall π-subgroup. Show that G has a normal subgroups $N \subseteq M$ such that N and G/M are π'-groups and M/N is a π-group.

NOTE: The conclusion of this problem is what it means to say that G has π **-length** 1.

Problem 38. Let P be a p-group with $|P : \mathbf{Z}(P)| \leq p^n$. Show that $|P'| \leq p^{\frac{n(n-1)}{2}}$.

HINT: Induct on n. If P is nonabelian, choose Q so that $\mathbf{Z}(P) \subseteq Q \subseteq P$ with $|P : Q| = p$. Get a bound on $|Q'|$ and then apply problem 32(b) to the group P/Q'. Note that $(P/Q')' = P'/Q'$.

Problem 39. Let G be p-solvable with $\mathbf{O}_{\pi'}(G) = 1$. Write $P = \mathbf{O}_p(G)$ and $F = \Phi(P)$, so that conjugation by G induces an action of G on P/F. Show that the kernel of this action is exactly P.

25 03-18-10

25.1 Transfer Theory

We now begin a very important subject, which will help us produce a lot of "good theorems" about normal subgroups. Essentially, we are studying homomorphisms from a group to different subgroups and we hope to gain information in this way about the original group.

Let $H \subseteq G$ and take T a right transversal for H in G. So for a coset Ht for $t \in T$, let $g \in G$. Then $Hg = Htg = H(t \cdot g)$, where we write $t \cdot g \in T$ and $t \cdot g$ names the coset Htg. This gives us a dot action of G on T, so $tg \in H(t \cdot g)$ so I can write $tg = h(t \cdot g)$ for some $h \in H$, giving us that $tg(t \cdot g)^{-1} \in H$. Write $V(g) = \prod_{t \in T} tg(t \cdot g)^{-1}$.

Note that since G need not be abelian, $V(g)$ seems to be undefined; to sidestep this issue, we "agree" on a predetermined ordering of the transversal T, and note that in the end we will mod out by a commutator to truly sidestep this issue. We call V a *pretransfer*. Let $v : G \to H \to H/H'$ be the natural map. We call v the *transfer map*. Why v for transfer? The answer is the same as to the question why $\mathbb{Z}$ for integers? It comes from German. For a final piece of notation, if $h, k \in H$, we write $h \equiv k \pmod{H'}$ if $H'h = H'k$.

Theorem 25.1. $v : G \to H/H'$ is a homomorphism.

Proof. Let $x, y \in G$. We want to show that $v(xy) = v(x)v(y)$. I.e., we wish to show that $V(xy) \equiv V(x)V(y) \pmod{H'}$. Now $V(xy) = \prod_{t \in T} txy(t \cdot xy)^{-1} = \prod_{t \in T} tx(t \cdot x)^{-1}(t \cdot x)y((t \cdot x) \cdot y)^{-1}$. Since $tx(t \cdot x)^{-1} \in H$ and $(t \cdot x)y((t \cdot x) \cdot y)^{-1} \in H$, we can interchange the order of multiplication modulo H'. Therefore mod H', this expression simplifies to $\prod_{t \in T} tx(t \cdot x)^{-1} \prod_{t \in T} (t \cdot x)y((t \cdot x) \cdot y)^{-1}$. Since our dot operation is really an action, we have $(t \cdot x)$ ranging over T just as t ranges over T, so again modulo H' this expression simplifies to $\prod_{t \in T} tx(t \cdot x)^{-1} \prod_{t \in T} ty(t \cdot y)^{-1} = V(x)V(y)$. □

We now fill in the gap about just how well defined v is by showing that the transfer homomorphism is independent of the choice of transversal.

Theorem 25.2. The transfer from $G \to H/H'$ is independent of the choice of the transversal T.

Proof. Let S be another right transversal for H in G. Then each $s \in S$ has the form $h_t t$ so that $S = \{h_t t | t \ in T\}$; that is, the members of S and T differ on an element of H; we call that element h_t. We wish to determine what $s \cdot g$ is in terms of our original transversal T. Now $s \cdot g = (h_t t) \cdot g \in H h_t t g$ by definition. But $H h_t t g = H t g = H(t \cdot g)$. Now $t \cdot g$ is an element of T, and we know that the element $(t \cdot g)$ is known in S as $h_{t \cdot g}(t \cdot g)$, so we have the formula $(h_t t) \cdot g = h_{t \cdot g}(t \cdot g)$.

Now we determine $V_s(g) \equiv \prod_{t \in T} (h_t t) g ((h_t t) \cdot g)^{-1} = \prod_{t \in T} (h_t t) g (h_{t \cdot g}(t \cdot g))^{-1} = \prod_{t \in T} h_t t g (t \cdot g)^{-1} h_{t \cdot g}^{-1}$. Again notice that $h_t \in H$, $t g (t \cdot g)^{-1} \in H$, and that $h_{t \cdot g}^{-1} \in H$, so we can again rearrange the orders of these elements modulo H'. Therefore the previously obtained expression is equivalent mod H' to $\prod_{t \in T} t g (t \cdot g)^{-1} \prod_{t \in t} h_t \prod_{t \in T} h_{t \cdot g}^{-1} \equiv V(t) \pmod{H'}$, where the last equivalence holds because $t \cdot g$ is ranging over T as t ranges over T, and we can rearrange all of these terms to stand next to their inverses modulo H'. □

We now digress a bit from introductions in order to show an application of transfer theory.

Theorem 25.3. Let $P \in \mathrm{Syl}_p(G)$ and assume that P is abelian. Then $P \cap \mathbf{Z}(G) \cap G' = 1$.

Proof. Notice that $v = V$ on abelian groups and that $v : G \to H$ in the case where H is abelian as $H' = 1$. Let $v : G \to P$ be the transfer map. Let $u \in P \cap \mathbf{Z}(G) \cap G'$. Then $1 = v(u)$ since $u \in G'$ and P is abelian. [Again notice that the kernel of the transfer homomorphism always contains the commutator subgroup of G]. So $1 = v(u) = \prod_{t \in T} t u (t \cdot u)^{-1}$. Now $t \cdot u \in Ptu$ by definition; but $Ptu = Put = Pt$ since $u \in \mathbf{Z}(G)$ and since $u \in P$. So $t \cdot u = t$, and we have $1 = v(u) = \prod_{t \in T} t u t^{-1} = \prod_{t \in T} u$ again since u is central. However, $1 = v(t) = \prod_{t \in T} u = u^{|T|} = u^{|G:P|}$. This tells us that $o(u)$ divides $|G : P|$, which is p' since $P \in \mathrm{Syl}_p(G)$. However, $u \in P$, so $o(u)$ must also divide $|P|$ which is a p-power. This gives us that $o(u) = 1$ and therefore that $u = 1$, proving the result. □

We now begin a brief digression. Given a group G, I want to find a group Γ with $Z \subseteq \mathbf{Z}(\Gamma)$ such that $\Gamma/Z \cong G$. Additionally, I want $Z \subseteq \Gamma'$. Among all pairs (Γ, Z) with $Z \subseteq \mathbf{Z}(\Gamma) \cap \Gamma'$ and with $\Gamma/Z \cong G$, There is a unique largest

Z and all other such $Z's$ are homomorphic images of Z. This largest such Z is called the *Schur multiplier*, and we denote it by $M(G)$. It is a fact, proven in the Character Theory book, that $M(G) = H^2(G, \mathbb{C}^\times)$.

Although it is true that the largest Z is unique, it is NOT true that the Γ is unique. As an example, both D_8 and Q_8 have Schur multiplier $\mathbb{Z}_2 \times \mathbb{Z}_2$, the Klein four group.

Theorem 25.4. Suppose G has a cyclic Sylow p-subgroup. Then p does not divide $|M(G)|$.

Proof. Let $Z \subseteq \Gamma' \cap \mathbf{Z}(\Gamma)$ with $\Gamma/Z \cong G$ and $Z = M(G)$. Let $P \in \mathrm{Syl}_p(\Gamma)$. Then $P/(P \cap Z) \cong Q$ for $Q \in \mathrm{Syl}_p(G)$, so we see that $P/(P \cap Z)$ is cyclic. But $P \cap Z$ is central, so P is abelian. By our previous theorem, this tells us that $P \cap \mathbf{Z}(\Gamma) \cap \Gamma' = 1$, so p does not divide the order of $\Gamma' \cap \mathbf{Z}(\Gamma)$. However, $Z \subseteq (\mathbf{Z}(\Gamma) \cap \Gamma')$, so p does not divide the order of $Z = M(G)$. □

26 03-23-10

We now return to transfer theory and prove a very useful lemma, the transfer evaluation lemma, which we will abbreviate TEL.

Lemma 26.1 (Transfer Evaluation Lemma)**.** Let $H \subseteq G$ with T a right transversal and let $g \in G$. Then there exists some $T_0 \subseteq T$ and positive integers n_t for $t \in T_0$ such that:

(a) $tg^{n_t}t^{-q} \in H$ for all $t \in T_0$.

(b) $V(g) \equiv \prod_{t \in T_0} tg^{n_t}t^{-1} \pmod{H'}$

(c) $\sum n_t = |T| = |G :: H|$

(d) n_t divides $o(g)$ for all $t \in T_0$.

Proof. The element g induces a permutation on T via the dotting action. We write this permutation in cycle notation, including the one cycles. Let T_0 be the set of first entries in all of the cycles [the first here is irrelevant], and let n_t be the size of the cycle containing t. Then $\sum n_t = |T| = |G : H|$, proving statement (c).

Let $t \in T_0$ with corresponding cycle $(t, t \cdot g, t \cdot g^2, \ldots, t \cdot g^{n_t - 1})$. We compute the contribution to $V(g)$ coming from this cycle. Recall that $V(g) = \prod_{t \in T} tg(t \cdot g)^{-1}$. The contribution from our cycle is:

$$[tg(t \cdot g)^{-1}][(t \cdot g)g(t \cdot g^2)^{-1}][(t \cdot g^2)g(t \cdot g^3)^{-1}] \ldots [(t \cdot g^{n_t - 1})gt^{-1}] = tg^{n_t}t^{-1}$$

Since every one if these factors lies in H, we have that their product lies in H, so $tg^{n_t}t^{-1} \in H$, proving (a). Multiplying over all cycles, we get that

$V(g) \equiv \prod_{t \in T_0} tg^{n_t}t^{-1} \pmod{H'}$, where the mod H' is necessary due to ordering issues, and this gives us (b). Finally, we have that (d) holds by the FCP. In other words, the cycle lengths n_t divide the order of the induced permutation, which divides $o(g)$. □

Theorem 26.1. Let $Z = \mathbf{Z}(G)$, and write $n = |G : Z|$. Then the map $g \mapsto g^n$ is a homomorphism from G to Z.

Proof. Note that the nth power map indeed maps G into Z since G/Z has order n and therefore all elements of G/Z raised to the nth power are trivial; i.e., they lie in Z. Let $V : G \to Z$ be the transfer map. Because Z is abelian, $v = V$. So $v(G) = \prod_{t \in T_0} tg^{n_t}t^{-1} \pmod{Z}' = \prod_{t \in T_0} tg^{n_t}t^{-1}$ since $Z' = 1$. Also, $tg^{n_t}t^{-1} \in Z$ by part (a) of the TEL, so $(tg^{n_t}t^{-1}) = (tg^{n_t}t^{-1})^t = g^{n_t}$. So $v(g) = \prod_{t \in T_0} g^{n_t} = g^{\sum n_t} = g^{|G:Z|} = g^n$. As we already know that the transfer map is a homomorphism, this gives us the result. □

Corollary 26.1. If $x \in G'$ then $x^n = 1$, where $n = |G : \mathbf{Z}(G)|$.

Proof. Since G' is contained in the kernel of every transfer map and the nth power map is now known to be a transfer map. □

Assume that $|G : \mathbf{Z}(G)| = n$. The question now is, how many commutators are there in G? Let T be a transversal for $\mathbf{Z}(G)$ in G. Then all commutators in G have the form $[s, t]$ for $s, t \in T$. To verify this is a calculation: if $x, y \in G$ then we can write $x = zs$ and $y = ut$ for some $z, u \in \mathbf{Z}(G)$ and $s, t \in T$. Then:

$$[x, y] = [zs, ut] = [z, ut]^s[s, ut] = ([z, t][z, u]^t)^s[s, t][s, u]^t$$

Notice that $[s, u], [z, u]$, and $[z, t]$ are all trivial since $z, u \in \mathbf{Z}(G)$, proving that $[x, y] = [s, t]$ for $s, t \in T$ and $x, y \in G$ arbitrary. Therefore the number of commutators is less than n^2 and e each one of these commutators has order at most n.

The fact, due to Schur, is that even in infinite groups, we can get a bound on the number of commutators in the group. The following bound, although certainly not the best possible, can be easily justified.

Claim. $|G'| \leq (n^2)^{(n^2)^n}$.

Proof. If $t \in G'$, we can write $t = u_1u_2 \dots u_r$ where the u_i are commutators. We claim that $r \leq (n^2)^n$, which proves the above claim. Assume that r is minimal such that $t = u_1u_2 \dots u_r$. We now claim that no u_i appears more than n times. We need to move all other $u_i = u_1$ across intermediate commutators. We can do this, bu at a price; the price is that $uv = vu^v$. But u^v is a commutator since $[s, t]^v = [s^v, t^v]$, so we can rearrange the product of u_j without changing the number of commutators; however, then all of the u_i which happen to be u_1 can be put next to one another and as there are now more than n of them,

they cancel out, contradicting the minimality of r. Therefore we know that each commutator cannot appear in this decomposition of t more than n times, and as there are at most n^2 commutators, the claim holds. □

Suppose $v : G \to H/H'$ and let $x \in H$. Then $V(x) \equiv \prod_{t \in T_0} t x^{n_t} t^{-1}$ where $x^{n_t} \in H$ and so is $t x^{n_t} t^{-1}$, yet t is only known to be in G. We therefore know that the elements of H x^{n_t} and $t^{-1} x^{n_t} t^{-1}$ are conjugate in G, although there is no reason to believe they may be conjugate in H.

Definition 26.1. If $H \subseteq G$, then conjugacy classes of G are said to be *fused* in G if they are in the same conjugacy class in G.

Definition 26.2. Let $H \subseteq K \subseteq G$. Then K *controls G-fusion* in H if whenever x and y are conjugate in G then they are already conjugate in K.

To demonstrate these new definitions, we prove the following lemma, where $H = \mathbf{C}_G(P)$, $K = \mathbf{N}_G(P)$, and $G = G$.

Lemma 26.2 (Burnside)**.** Let $P \in \mathrm{Syl}_p(G)$. Then $\mathbf{N}_G(P)$ controls G-fusion in $\mathbf{C}_G(P)$.

Proof. Let $x, y \in \mathbf{C}_G(P)$. We want to assume that $y = x^g$ for some $g \in G$ and show that $y = x^n$ for some $n \in \mathbf{N}_G(P)$. We have that $P \subseteq \mathbf{C}_G(y)$. Also, $P \subseteq \mathbf{C}_G(x)$ so $P^g \subseteq \mathbf{C}_G(x)^g = \mathbf{C}_G(x^g) = \mathbf{C}_G(y)$, so we have both $P, P^g \subseteq \mathbf{C}_G(y)$. In fact, P and P^g must both be Sylow p-subgroups of $\mathbf{C}_G(y)$ since they are already Sylow p-subgroups of G. Hence there exists $c \in \mathbf{C}_G(y)$ such that $(P^g)^c = P$; i.e. that $P^{gc} = P$. This places $gc \in \mathbf{N}_G(P)$, and we must simply show that $x^{gc} = y$ to finish the proof. Yet $x^{gc} = y^c = y$ since $c \in \mathbf{C}_G(y)$, so we have what we want. □

27 Problem Set 8

Problem 40. Let A be a group of odd order that acts on a 2-group P, and assume that A fixes every element of order 2 and every element of order 4 in P. Prove that A acts trivially on P.

HINT: If P is a counterexample of minimal possible order, show that $[P, A] = P$. Deduce that there is no A-invariant subgroup Q such that $P' < Q < P$ and that $x^2 \in P'$ for all $x \in P$. Also, show that $P' \subseteq \mathbf{Z}(P)$ and deduce that $x^2 = 1$ for all $x \in P'$.

Problem 41. Let $N \lhd G$ and assume that $\mathbf{C}_G(N) \subseteq N$. Let A act on G and assume that $N \subseteq \mathbf{C}_G(A)$. If $(|A|, |G|) = 1$, show that A acts trivially on G.

HINT: Show that $[G, A] \subseteq N$.

NOTE: We know several examples of normal subgroups N that contain their own centralizers. If G is solvable, we could take $N = \mathbf{F}(G)$ (see theorem 3 of notes 3) or if G is π-separable and $\mathbf{O}_{\pi'}(G) = 1$ we could take $N = \mathbf{O}_\pi(G)$. (this is Lemma 1.2.3.)

Problem 42. Let G be p-solvable, and assume that a Sylow p-subgroup of G is cyclic. Let $K \subseteq G$ have p'-order, and assume that p divides $|\mathbf{N}_G(K)|$. Show that $K \subseteq \mathbf{O}_{p'}(G)$.

HINT: First handle the case where $\mathbf{O}_{p'}(G) = 1$.

Problem 43. Let A act faithfully on G, and let

$$G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_r = 1$$

be a series of normal subgroups of G. Assume that $[N_i, A] \subseteq N_{i+1}$ for all i with $0 \leq i < r$. Prove that A is nilpotent, and that its nilpotence class in at most $r - 1$.

Problem 44. Let A act on G, and write $Z = \mathbf{Z}([G, A])$. Note that Z is A-invariant, and let $B = \mathbf{C}_Z(A)$. Show that $B \lhd G$.

HINT: Show that $[B, G] \subseteq B$.

Problem 45. Suppose that G'/G'' is cyclic and that G''/G''' is cyclic. Show that G'/G'' is abelian, and deduce that $G'' = G'''$.

HINT: Note that $\mathrm{Aut}(G''/G''')$ is abelian.

28 03-25-10

We begin by proving what is historically the first or second main theorem in transfer theory.

Theorem 28.1 (Burnside)**.** Suppose $P \in \mathrm{Syl}_p(G)$. Assume that $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$. Then G has a normal p-complement.

Proof. We recall that a p-complement is a Hall p'-subgroup, or alternatively, a subgroup $H \subseteq G$ such that $|G : H|$ is the order of a Sylow p-subgroup. Let $v : G \to P$ be the transfer map (again, no P/P' since P is abelian). Let $x \in P$. Then $v(x) = \prod_{t \in T_0} tx^{n_t}t^{-1}$ and where both x^{n_t} and $tx^{n_t}t^{-1}$ are in P by the transfer evaluation lemma. Thus both x^{n_t} and $tx^{n_t}t^{-1} \in P \subseteq \mathbf{C}_G(P)$ since $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$, so the elements are conjugate in $\mathbf{N}_G(P)$. These two elements are actually central in $\mathbf{N}_G(P)$, so we conclude that they must be equal. Therefore $v(x) = \prod_{t \in T_0} tx^{n_t}t^{-1} = \prod_{t \in T_0} x^{n_t} = x^{\sum n_t} = x^{|G:P|}$. We have therefore established that on P, v maps $x \in P$ to $x^{|G:P|}$. Since $(|P|, |G : P|) = 1$, this map is surjective, So $V : G \to P$ is a surjective homomorphism. Let $K = \ker(v)$. Then $G/K \cong P$, $K \lhd G$, and $|G : K| = P$, so K is a normal p-complement. $\square$

Corollary 28.1. Let $P \in \mathrm{Syl}_p(G)$, where p is the smallest prime divisor of $|G|$. Assume that P is cyclic. Then G has a normal p-complement.

Proof. We want to show that $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$ in order to apply the previous theorem. We know from the N/C theorem that $\mathbf{N}_G(P)/\mathbf{C}_G(P)$ is isomorphically embedded in $\mathrm{Aut}(P)$ So $|\mathbf{N}_G(P) : \mathbf{C}_G(P)|$ divides $\varphi(|P|) = p^a(p-1)$, where $|P| = p^a$. But this index is divisible by no prime less than or equal to p which happens to also divide $|G|$ since P is a Sylow p-subgroup and $P \subseteq \mathbf{C}_G(P)$. So $\mathbf{C}_G(P)$ must equal $\mathbf{N}_G(P)$ and thus $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$. □

Corollary 28.2. Assume that all Sylow p-subgroups of G are cyclic. Then G is solvable.

Proof. Let p be the smallest prime divisor of $|G|$. By the previous corollary, we know that G has a normal p-complement K. Then all Sylows of K are cyclic and by induction, K is solvable. But $G/K \cong P$ which is cyclic and thus solvable so G is solvable. □

Corollary 28.3. If $|G| = \prod p_i$ for p_i distinct primes, then G is solvable and if p is the largest prime dividing $|G|$, then $P \in \mathrm{Syl}_p(G)$ is normal in G.

Proof. Repeat the process of the previous corollary and use that normal p-complements are characteristic. □

We now give a useful definition. Note, however, that the notation we use seems to be solely Isaacs' notation, and is not so common to other texts.

Definition 28.1. For any group, we define $\mathbf{A}^p(G)$ to be the unique smallest normal subgroup M such that G/M is an abelian p-group.

To see why such a group should exist, note that any such M will have to contain G' if G/M is to be abelian, and normal p-complements always exist in abelian groups. It is a fact, although we do not prove it, that $\mathbf{A}^p(G) = G'\mathbf{O}^p(G)$.

We note that if $P \in \mathrm{Syl}_p(G)$, then the transfer map $v : G \to P/P'$ has image an abelian p-group so we must have that $\mathbf{A}^p(G) \subseteq \ker(v)$ by the minimality of $\mathbf{A}^p(G)$.

Theorem 28.2 (Generalized Burnside Theorem)**.** Let $P \in \mathrm{Syl}_p(G)$. Assume that P is abelian. Let $Z \subseteq (P \cap \mathbf{Z}(\mathbf{N}_G(P)))$. Then $Z \cap \mathbf{A}^p(G) = 1$.

Proof. Let $v : G \to P$ be the transfer map and let $z \in Z \cap \mathbf{A}^P(G)$. Now $v(z) = 1$ since $z \in \mathbf{A^p(G)} \subseteq \ker(v)$ by our statements preceding this theorem. Also, we have by definition that $v(z) = \prod_{t \in T_0} tz^{n_t}t^{-1}$, where each $tz^{n_t}t^{-1} \in P \subseteq \mathbf{C}_G(P)$ since P is abelian and each $z^{n_t} \in \mathbf{C}_G(P)$. By the fusion lemma, we therefore know that z^{n_t} and $tz^{n_t}t^{-1}$ are conjugate in $\mathbf{N}_G(P)$, but since $z^{n_t} \in Z \subseteq \mathbf{Z}(\mathbf{N}_G(P))$, the action of $\mathbf{N}_G(P)$ is trivial on z^{n_t}, and we must have $z^{n_t} = tz^{n_t}t^{-1}$ and so we have $1 = v(z) = \prod z^{n_t} = z^{\sum n_t} = z^{|G:P|}$, which tells us that $o(z)$ divides $|G : P|$. But $z \in P$, so $o(z)$ must divide $|P|$. This gives us that $o(z) = 1$ and so we must have $z = 1$. □

We now outline how to deduce Burnside's first theorem from this theorem. Take $Z = P$. By the generalized Burnside theorem, we know that $P \cap \mathbf{A}^p(G) = 1$ so 1 is a Sylow p-subgroup of $\mathbf{A}^p(G)$. Therefore p does not divide $|\mathbf{A}^p(G)|$ and we know that $|G : \mathbf{A}^p(G)|$ is a power of p, so $\mathbf{A}^P(G)$ ends up being a normal p-complement.

We now turn our attention to two-groups.

Theorem 28.3. Let $P \in \mathrm{Syl}_2(G)$. Assume that P is abelian and that $P = C \times D$ where C is cyclic and $\exp(D) < |C|$. Then $C \cap \mathbf{A}^2(G) = 1$.

Proof. Write $|C| = 2^n$. Now let $U = \{x^{2^{n-1}} | x \in P\}$. Because P is abelian, we know that U is a characteristic subgroup of P, so $U \lhd \mathbf{N}_G(P)$. Also, $|U| = 2$ so U is *the* subgroup of order 2 in C. [To see why U has order 2, take $x \in P$ and write $x = cd$. Then $x^{2^{n-1}}$ is just $c^{2^{n-1}}$]. This puts $U \subseteq \mathbf{Z}(\mathbf{N}_G(P))$ since $|U| = 2$ and $U \lhd \mathbf{N}_G(P)$.[This is where we are using the 2-ness]. So $U \cap \mathbf{A}^2(G) = 1$, and in fact $C \cap \mathbf{A}^2(G) = 1$ since otherwise $C \cap \mathbf{A}^2(G)$ would have to contain U since C has a unique element of order 2. □

Theorem 28.4. Let $P \in \mathrm{Syl}_2(G)$. Assume that $P = C_{2^a} \times C_{2^b}$ where $a > b$. Then G has a normal 2-complement.

Proof. Write $P = C \times D$, where $C \cong C_{2^a}$ and $D \cong C_{2^b}$. Then the previous theorem yields that $C \cap \mathbf{A}^2(G) = 1$. Let $B = \mathbf{A}^2(G) \cap P$. Then we can think of B as $B/B \cap C$ since $B \cap C = 1$. But $B/B \cap C \cong BC/C \subseteq P/C \cong D$ by the first isomorphism theorem. This tells us that B is cyclic and $B \in \mathrm{Syl}_2(\mathbf{A}^2(G))$. But by Burnside's theorem, we know that $\mathbf{A}^2(G)$ has a normal 2-complement which *is* a normal 2-complement of G. Since it is characteristic in a normal subgroup, and so is normal in G. □

29 04-06-10

We now begin a new subtopic within transfer theory. In this section, there are a lot of pictures that make everything clearer. I've put some pictures in, I just hope that they are helpful. Before we can really begin, we need a definition.

Definition 29.1. Let $H \subseteq G$. Then the *focal subgroup*, written $\mathrm{Foc}_G(H) = \langle h^{-1}h^g \,|\, h \in H, g \in G, h^g \in H \rangle$.

Note that if $g \in H$ then $h^g \in H$ and in fact $h^{-1}h^g = [h, g]$. Thus H' is clearly seen to be contained within $\mathrm{Foc}_G(H)$. Also, all generators of $\mathrm{Foc}_G(H)$ are commutators so $\mathrm{Foc}_G(H) \subseteq G'$, so $\mathrm{Foc}_G(H) \subseteq (G' \cap H)$.

Theorem 29.1 (Focal Subgroup Theorem)**.** Let $P \in \mathrm{Syl}_p(G)$. Then:

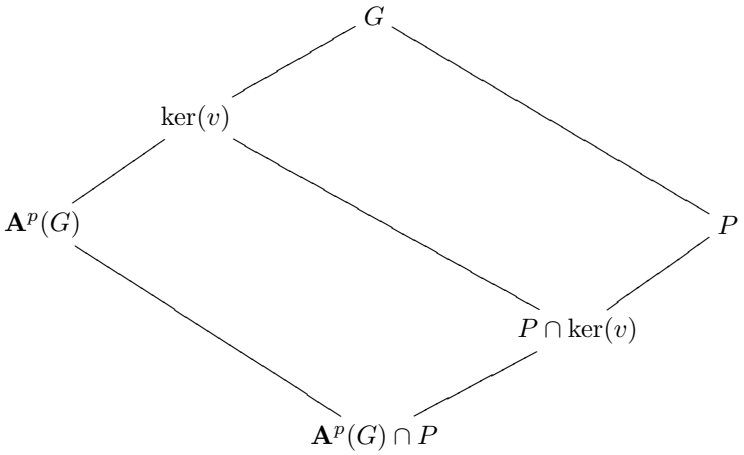
$$\mathrm{Foc}_G(P) = P \cap G' = P \cap \mathbf{A}^p(G) = P \cap \ker(v)$$

where $v : G \to P/P'$ is the transfer map.

Proof. We have $\mathrm{Foc}_G(P) \subseteq P \cap G' \subseteq P \cap \mathbf{A}^p(G) \subseteq P \cap \ker(v)$, and so the prove equality it suffices to show that $P \cap \ker(v) \subseteq \mathrm{Foc}_G(P)$. Let $x \in P \cap \ker(v)$. Since $x \in \ker(v)$, we have that $V(x)$, the pretransfer, is contained in $P' \subseteq \mathrm{Foc}_G(P)$. By the transfer evaluation lemma, we know that we can write $V(x) \equiv \prod_{t \in T_0} tx^{n_t}t^{-1} \pmod{P'}$, so $\prod_{t \in T_0} tx^{n_t}t^{-1} \in \mathrm{Foc}_G(P)$ since $P' \subseteq \mathrm{Foc}_G(P)$. Also, $x^{n_t} \in P$ since $x \in P$ and therefore $x^{-n_t}tx^{n_t}t^{-1} \in \mathrm{Foc}_G(P)$ by the definition of the focal subgroup of P for each $t \in T_0$. Hence $\prod_{t \in T_0} x^{-n_t}tx^{n_t}t^{-1} \in \mathrm{Foc}_G(P)$. Because $P' \subseteq \mathrm{Foc}_G(P)$, we can rearrange the order of this product and NOT change the fact that the product lies in $\mathrm{Foc}_G(P)$. Hence we have that $\prod_{t \in T_0} x^{-n_t} \prod_{t \in T_0} t^{-1}x^{n_t}t^{-1}$ is contained in $\mathrm{Foc}_G(P)$, and since $\prod_{t \in T_0} tx^{n_t}t^{-1} \in \mathrm{Foc}_G(P)$, we have $\prod_{t \in T_0} x^{-n_t} \in \mathrm{Foc}_G(P)$ and $\prod_{t \in T_0} x^{n_t} \in \mathrm{Foc}_G(P)$. However, $\prod_{t \in T_0} x^{n_t} = x^{\sum n_t} = x^{|G:P|}$, so we have $x^{|G:P|} \in \mathrm{Foc}_G(P)$. Since this integer is coprime to $o(x)$, we then have $x \in \mathrm{Foc}_G(P)$, giving us the result. □

Corollary 29.1. $\mathbf{A}^p(G) = \ker(v)$, where v is the transfer from G to P/P' and where $P \in \mathrm{Syl}_p(G)$.

Proof. Here is one place that a picture is helpful.



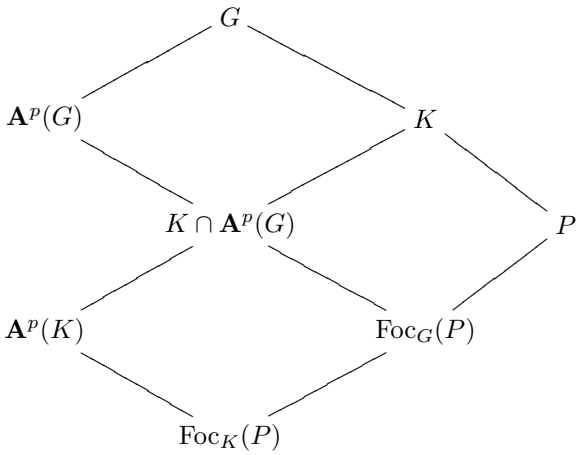
We know that $|\ker(v) : \mathbf{A}^p(G)| = |P \cap \ker(v) : P \cap \mathbf{A}^p(G)| = 1$ by the previous theorem. □

We note that If $P \subseteq K \subseteq G$, then $\mathbf{A}^p(K) \subseteq \mathbf{A}^p(G) \cap K$. When we have equality, something good is happening.

Definition 29.2. Let $P \subseteq K \subseteq G$. We say that K *controls p-transfer* in G if $\mathbf{A}^P(G) \cap K = \mathbf{A}^p(K)$.

Theorem 29.2. Let $P \subseteq K \subseteq G$ where $P \in \mathrm{Syl}_p(G)$. Assume that K controls G-fusion in P. Then K controls p-transfer.

Proof. To prove that $\mathbf{A}^p(K) = \mathbf{A}^p(G) \cap K$, it suffices to show that $\mathrm{Foc}_K(P) = \mathrm{Foc}_G(P)$. That this is true follows from the Focal subgroup theorem and the following picture:



By definition, $\mathrm{Foc}_G(P) = \langle x^{-1}x^g \mid x \in P, g \in G, x^g \in P\rangle$. But K controls G-fusion in P, so this is equal to $\langle x^{-1}x^k \mid x \in P, k \in K, x^k \in P\rangle = \mathrm{Foc}_K(P)$. □

We will see later on that although controling P-fusion gives us control of p-transfer, it is not necessary.

Corollary 29.2. Assume that $P \in \mathrm{Syl}_p(G)$ is abelian. Then $\mathbf{N}_G(P)$ controls p-transfer.

Proof. Since P is abelian, $P \subseteq \mathbf{C}_G(P)$ and we know that $\mathbf{N}_G(P)$ controls fusion in $\mathbf{C}_G(P)$, which contains P, so $\mathbf{N}_G(P)$ controls p-transfer in P by the previous theorem. □

We now state a few theorems which we will not prove, but which are quite helpful.

Theorem 29.3 (Hall-Wielandt)**.** Let $P \in \mathrm{Syl}_p(G)$ and assume that the nilpotence class of P is less than p. Then $\mathbf{N}_G(p)$ controls p-transfer.

The theorem by Hall and Wieldant tells us that we do not actually need the assumption that P is abelian in order to get a control on p-transfer. A theorem of Yoshida actually implies the theorem of Hall and Wielandt, but we do not prove this theorem either.

Theorem 29.4 (Yoshida)**.** Let $P \in \mathrm{Syl}_p(G)$. Assume $C_p \wr C_p$ is not a homomorphic image of P. Then $\mathbf{N}_G(P)$ controls p-transfer.

Theorem 29.5 (Tate's theorem)**.** If $\mathbf{A}^p(G) \cap K = \mathbf{A}^p(K)$ then $\mathbf{O}^p(G) \cap K = \mathbf{O}^p(K)$.

30 Problem Set 9

Problem 46. Let $P \in \mathrm{Syl}_p(G)$, where P is cyclic. If $P \cap G' > 1$, show that $P \subseteq G'$.

HINT: Let $N = \mathbf{N}_G(P)$ and write $N = PK$, where $P \cap K = 1$. Note that if $[P, K] = P$ then $P \subseteq G'$.

Problem 47. Suppose that every Sylow p-subgroup of G is cyclic.

(a) If $G > 1$, show that G/G' is a nontrivial cyclic group.

(b) Show that G' is cyclic.

(c) Show that G' is a Hall subgroup of G, and thus G splits over G'.

HINT: For (b), work by induction on $|G|$ and use Problem 45.

NOTE: This problem shows that if all Sylow subgroups of G are cyclic, then G could be constructed as the semidirect product of a cyclic group acted on by a cyclic group of coprime order.

Problem 48. A group G is **supersolvable** if there exists a normal series in G in which the factors of consecutive terms are all cyclic. It is easy to show that all subgroups and factor groups of a supersolvable group are supersolvable.

(a) Show that the minimal normal subgroups of a supersolvable group all have prime order.

(b) Show that the maximal subgroups of a supersolvable group all have prime index.

(c) Let p be the smallest prime divisor of $|G|$, where G is supersolvable. Show that G has a normal p-complement.

HINT: For (b) and (c), work by induction on $|G|$ and apply the inductive hypothesis to G/N, where N is minimal normal in G.

Problem 49. Suppose that every maximal subgroup of some group G has prime index. Show that a Sylow p-subgroup of G for the largest prime divisor of $|G|$ is normal, and deduce that G is solvable.

NOTE: In fact, G must be supersolvable, but that is harder to prove. This problem can be used to construct an alternative proof for Problem 48(c).

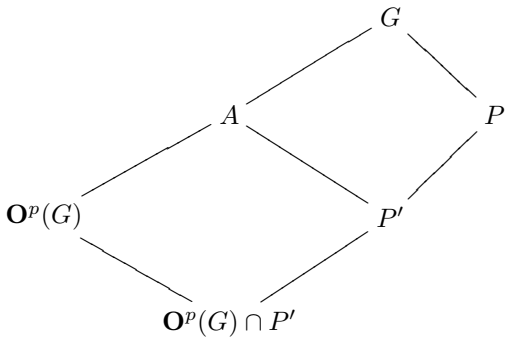
31 04-08-10

We begin by restating Tate's theorem. We will be using it without proof, although a proof can be found in the character theory book.

Theorem 31.1 (Tate)**.** Assume that $\mathbf{A}^p(K) = \mathbf{A}^p(G) \cap K$. Then $\mathbf{O}^p(K) = \mathbf{O}^p(G) \cap K$.

Corollary 31.1. Let $P \in \mathrm{Syl}_p(G)$. If $\mathbf{O}^p(G) \cap P \subseteq P'$ then $\mathbf{O}^p(G) \cap P = 1$ and so G has a normal p-complement.

Proof. The following picture is useful (although I don't know why the lines are skewed):



Let $A = \mathbf{O}^p(G)P'$. Note that $A \lhd G$ since P normalizes $\mathbf{O}^p(G)$ and P' so P normalizes anything that they uniquely determine, so P normalizes A. since A normalizes A and $G = AP$, we see that $A \lhd G$. This gives us that $G/A \cong P/P'$ which is an abelian p-group, so $\mathbf{A}^p(G) \subseteq A$. But we also have that $\mathbf{O}^p(G) \subseteq \mathbf{A}^p(G)$ and $P' \subseteq G' \subseteq \mathbf{A}^p(G)$, so we have $A \subseteq \mathbf{A}^p(G)$ and therefore $A = \mathbf{A}^p(G)$. Now applying Tate's theorem with $K = P$ gives us that $\mathbf{O}^p(G) \cap P = \mathbf{O}^p(P) = 1$. □

Theorem 31.2. Let $P \in \mathrm{Syl}_p(G)$. Assume that G controls its own G-fusion. Then G has a normal p-complement.

Proof. Let $N = \mathbf{O}^p(G)$. We want $N \cap P = 1$, which will give us that N is a normal p-complement. Let $S = N \cap P$, and note that $S \in \mathrm{Syl}_p(N)$. Note also that $\mathbf{A}^p(N) = N$ since $\mathbf{A}^p(N) \lhd G$ with $|G : \mathbf{A}^p(N)|$ a power of p. By the Focal subgroup theorem applied in N, we know that $\mathrm{Foc}(S) = S \cap \mathbf{A}^p(N) = S \cap N = S$. Now $\mathrm{Foc}_N(S)$ is generated by elements of the form $x^{-1}x^n$ for $x \in S$, $n \in N$, and $x^n \in S$. Both x and x^n are in $S \subseteq P$ so x and x^n are two elements of P which are conjugate in G. Since P controls its own G-fusion by hypothesis, there is some $u \in P$ with $x^n = x^u$. So the generators of $\mathrm{Foc}_N(S)$ can all be written as $x^{-1}x^u = [x, u] \subseteq [S, P]$. Hence $S = \mathrm{Foc}_N(S) \subseteq [S, P]$. Note that $S = N \cap P \lhd P$ by the diamond lemma, so $[S, P] \subseteq S$ automatically and we then have $S = [S, P] = [S, P, P] = [S, P, P, P] \ldots$. Yet $[S, P, P, \ldots] \subseteq [P, P, P, \ldots] =$ 1with enough dot dot dots since P is nilpotent; this gives us that $S = 1$ and we then have what we want. □

We pause now to state that the converse of this theorem is also true. Suppose that G has a normal p-complement N. Then P controls its own fusion. Let $\overline{G} = G/N$. Then $\overline{G} = \overline{NP} = \overline{P}$, so the bar map maps P onto $\overline{G}$. Since $P \cap N$ is the same as P intersected with the kernel of the bar map, we have that $P \cap N = 1$, and then the isomorphism theorem gives us that P is isomorphic to

$\overline{G}$. If $x, y \in P$ are G-conjugate, we then have that $\bar{x}$ and $\bar{y}$ are conjugate in $\overline{G}$. Thus x and y are conjugate in P due to this isomorphism.

We now state a very powerful result due to Frobenius which helps us to determine when a group G has a normal p-complement.

Theorem 31.3 (Frobenius)**.** The following are equivalent.

(1) G has a normal p-complement.

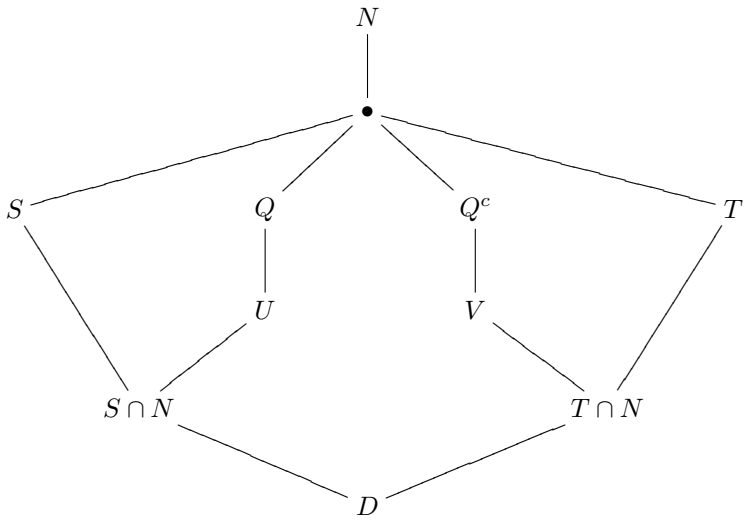
(2) Every p-local subgroup of G has a normal p-complement.

(3) For every p-subgroup $U \subseteq G$ we have $\mathbf{N}_G(U)/\mathbf{C}_G(U)$ a p-group.

Proof. We first show that (1) $\to$ (2). Here, it suffices to show that if G has a normal p-complement and $H \subseteq G$ then H has a normal p-complement. Write N for the normal p-complement in G. Then $N \cap H \lhd H$ since $N \lhd G$. Also $|N \cap H|$ is p' since it is contained in N which has p' order. Also, $|H : H \cap N|$ is a p-power by the diamond lemma, so we see that $H \cap N$ is a normal p-complement in H.

We now show that (2) $\to$ (3). Let $U \subseteq G$ be a p-group [U can even be trivial] and we need to show that $\mathbf{N}_G(U)/\mathbf{C}_G(U)$ is a p-group. We are alright if $U = 1$ since then this quotient space is also trivial, so we can assume that $U > 1$. By definition, we then have that $\mathbf{N}_G(U)$ is p-local, so $\mathbf{N}_G(U)$ has a normal p-complement K. So $K \lhd \mathbf{N}_G(U)$ and $U \lhd \mathbf{N}_G(U)$, yet $U \cap K = 1$ since K is a p' subgroup and U is a p-group. Thus K and U commute, so $K \subseteq \mathbf{C}_G(U)$. So $|\mathbf{N}_G(U) : \mathbf{C}_G(U)|$ divides $|\mathbf{N}_G(U) : K|$ which is a p-power.

For (3) $\to$ (1), we will need a lemma that Isaacs' calls the "antler's lemma" due to the accompanying picture. You should really draw it as you go, and it will look more like antlers. Here is my redition:



Lemma 31.1. Assume $\mathbf{N}_G(U)/\mathbf{C}_G(U)$ is a p-group for all $U \subseteq G$ with U a p-subgroup. Let $S, T \in \mathrm{Syl}_p(G)$. Then $T = S^c$ for $c \in \mathbf{C}_G(S \cap T)$.

Proof. Write $D = S \cap T$, and induct on $|S : D| = |T : D|$. If $|S : D| = 1$, then $S = D = T$ and we can take $c = 1$. We can therefore assume that $D < S$ and $D < T$. Let $N = \mathbf{N}_G(D)$. Since normalizes grow in p-groups, we have $S \cap N > D$ and $T \cap N > D$. We know that we have $S \cap N \subseteq U \in \mathrm{Syl}_p(N)$ and $T \cap N \subseteq V \in \mathrm{Syl}_p(N)$ by the Sylow-D theorem. Let $U \subseteq Q \in \mathrm{Syl}_p(G)$. We can write $V = U^n$ for some $n \in N$. By assumption, we know that $|\mathbf{N}_G(D) : \mathbf{C}_G(D)|$ is a p-power, so we have $U\mathbf{C}_G(D) = N$. Write $n = uc$ for $u \in U$ and $c \in \mathbf{C}_G(D)$. Then I have $U^n = V$ implies $U^{uc} = U^c = V$. Thus $Q^c \in \mathrm{Syl}_p(G)$ and $V \subseteq Q^c$. Now $Q \cap S \supseteq N \cap S > D$ by construction and similarly, $Q^c \cap T \supseteq N \cap T > D$. The inductive hypothesis applies then to the pair S and Q and so $Q = S^x$ for some $x \in \mathbf{C}_G(S \cap Q) \subseteq \mathbf{C}_G(D)$ since $D \subseteq S \cap Q$. Similarly, $(Q^c)^y = T$ for some $y \in \mathbf{C}_G(T \cap Q^c) \subseteq \mathbf{C}_G(D)$. This tells us that $S^{xcy} = Q^{cy} = T$. But each of $x, c, y \in \mathbf{C}_G(D)$, so $xcy \in \mathbf{C}_G(D) = \mathbf{C}_G(S \cap T)$. □

Finally, we show that (3) → (1). Let $P \in \mathrm{Syl}_p(G)$. It suffices to show that P controls G-fusion in P. Let $x, y \in P$ where $y = x^g$ for some $g \in G$. We have that $y \in P$ and also since $y = x^g$ and $x \in P$ we have $y \in P^g$. Note that now $y \in P \cap P^g$ and so by the lemma, there exists c such that $P^{gc} = P$ for $c \in \mathbf{C}_G(P \cap P^g) \subseteq \mathbf{C}_G(y)$; hence $gc \in \mathbf{N}_G(P)$. By (3) again, we can write $\mathbf{N}_G(P) = P\mathbf{C}_G(P)$; this follows since this group has the correct order. So $gc = tb$ for $t \in P$ and $b \in \mathbf{C}_G(P)$. Now $t = gcb^{-1}$, so $x^t = x^{gcb^{-1}} = y^{cb^{-1}} = y$ since both $c, b^{-1} \in \mathbf{C}_G(y)$. Thus P controls its own G-fusion, and a normal p-complement exists. □

32 04-13-10

In this lesson, we draw a few quick corollaries of Frobenius' theorem.

Corollary 32.1. Suppose that every proper subgroup of G is nilpotent. Then G is solvable.

Proof. Suppose for contradiction that G is a minimal counter-example. Suppose that $1 < N < G$ with $N \lhd G$. Then N is nilpotent. Also, G/N satisfies the hypotheses, so by the minimality of G, we know that G/N is not a counter-example. So N is solvable and G/N is solvable, giving us that G is solvable. Therefore no such N can exist, and G is simple. Also, as G is a counterexample, we know that G is not abelian; hence G is not a p-group. By simplicity, G does not have a normal p-complement. Let $H \subseteq G$ be p-local, so that $H = \mathbf{N}_G(U)$ for some nontrivial p-group U. Note that $H < G$ or else we would have $U \lhd G$ and $1 < U < G$. As H is a proper subgroup of G, we know that H is nilpotent by hypothesis and so H has a normal p-complement since nilpotent groups are the direct product of their Sylow p-subgroups. So by Frobenius' theorem, we know that G has a normal p-complement. This is a contradiction, so G cannot be a counterexample, and the theorem holds. □

Corollary 32.2. Let $p \neq 2$ and assume every element of order p in G is central. Then G has a normal p-complement.

Proof. Let $U \subseteq G$ be a p-subgroup. We want to show that $\mathbf{N}_G(U)/\mathbf{C}_G(U)$ is a p-group. If this is not true, then choose $Q \in \mathrm{Syl}_p(\mathbf{N}_G(U))$ such that Q does not centralize U with $q \neq p$. Then Q acts on U and fixes all elements of order p since the elements of order p are central in G. However, this is a coprime action, so we have a theorem stating that this means that Q acts trivially on all of U, and hence $Q \subseteq \mathbf{C}_G(U)$. However, this is a contradiction, so no such Q exists. □

Corollary 32.3. Let $|G| = p^a m$ where p does not divide m. Assume that there does not exist a prime q dividing $|G|$ such that q divides $p^b - 1$ for all $0 < b \leq a$. Then G has a normal p-complement.

Proof. Let $U \subseteq G$ be a p-group. If suffices to show that if $Q \subseteq G$ is a q-group with $a \neq p$ and $Q \subseteq \mathbf{N}_G(U)$ then $Q \subseteq \mathbf{C}_G(U)$ for the same reason as the previous corollary. So suppose that Q exists and $Q \nsubseteq \mathbf{C}_G(U)$ but that $Q \subseteq \mathbf{N}_G(U)$. We know that $|U| = p^e$ for some $e \leq a$ and that $|\mathbf{C}_U(Q)| = p^f$ for $f < e$. So the *set* $U - \mathbf{C}_U(Q)$ is the union of the non-trivial Q-orbits, each of size divisible by q giving us that $q \Big| |U - \mathbf{C}_U(Q)|$. Yet the size of this set is $p^e - p^f = p^f(p^{e-f} - 1)$. So q must divide $(p^{e-f} - 1)$ since q does not divide p^f, but this is contrary to what we assumed; hence no such Q can exist. □

We make a few comments about this corollary. First, note what happens if G is a group with $|G|_2 = 4$. Then if all of the remaining primes dividing $|G|$ are greater than 3, i.e. if 3 does not divide $|G|$, then we meet the requirements of this corollary and we can deduce that G is not simple. Similarly, if $|G|_2 = 8$, we are in this situation if neither 3 nor 7 divides the order of the group. This is a helpful tool for determining when groups are not simple. With these remarks, we close the chapter on transfer.

32.1 Frobenius Actions

We now reach the sixth main topic of the course, Frobenius actions. We begin with a definition.

Definition 32.1. Let A act on N via automorphisms. Then the action is a *Frobenius action* if $\mathbf{C}_N(a) = 1$ for all $a \in A$ with $a \neq 1$.

Equivalently, we can say that $\mathbf{C}_A(n) = 1$ for $n \in N$ and $n \neq 1$, or we could say that all A-orbits on N other than $\{1\}$ have size $|A|$.

33 04-15-10

We begin with a few observations about Frobenius actions. As always, suppose that A acts via automorphisms on N and that the action is Frobenius, that is,

$\mathbf{C}_N(a) = 1$ for all $a \in A$ with $a \neq 1$. Since this action is Frobenius, we have $|N| \equiv 1 \pmod{|A|}$ and so $|N|$ and $|A|$ are coprime.

If the action of A on N is a Frobenius action and $X \subseteq N$ admits the action of A, then the action of A on X is also a Frobenius action. If $M \lhd N$ and M is A-invariant, then the action of A on N/M is Frobenius since with coprime actions, we know that fixed points come from fixed points.

We now prove a little lemma to familiarize ourselves with Frobenius actions.

Lemma 33.1. Let A act on N such that the action is Frobenius, and assume $|A|$ is even. Then N is abelian. Also, if $N > 1$ then A contains a unique involution.

Proof. Let $t \in A$ be an involution. Map N to N by $x \mapsto x^{-1}x^t$. We claim that this map is injective. So suppose $x, y \in N$ are such that $x^{-1}x^t = y^{-1}y^t$. Then $yx^{-1} = y^t(x^t)^{-1} = (yx^{-1})^t$ since t acts via automorphisms. But since the action is Frobenius, we have $yx^{-1} = 1$, giving us that $x = y$. Since $|N| < \infty$ this map is also a surjective map. So let $n \in N$. Then $n = x^{-1}x^t$ for some $x \in N$. Now consider $n^t = (x^{-1}x^t)^t = (x^{-1})^t x$ since t is an involution, so $n^t = n^{-1}$. Now let $m, n \in N$. Then $(mn)^t = (mn)^{-1} = n^{-t}m^{-1} = n^t m^t = (nm)^t$, so by the injectivity of t, we have $nm = mn$, making N abelian. Now let $s \in A$ be an involution. Then $n^s - n^{-1}$ for all $n \in N$ by our work above. Hence $n^s = n^t$ and we have $n^{st^{-1}} = n$. We can assume that $n \neq 1$, in which case we must have $st^{-1} = 1$ and $t = s$, proving the uniqueness of the involution t if A is not the group of order 2. □

We note that in the case of Frobenius actions, the group A is almost always solvable, although it does not HAVE to be solvable; a counterexample exists for the group $A = \mathrm{SL}(2, 5)$ acting on an elementary abelian group of order 121.

Lemma 33.2. Assume that A acts on N and let $G\ N \rtimes H = NH$. Then the action is Frobenius if and only if $H \cap H^g = 1$ for all $g \in G - H$.

Proof. Assume that the action is Frobenius, and let $g \in G - H$. We want to show that $H \cap H^g = 1$. Write $g = hn$ for $h \in H$ and $n \in N$, where $n \neq 1$ since $g \notin H$. Then $H^g = H^{hn} = H^n$, so we really want to show that $H \cap H^n = 1$. Let $y \in H \cap H^n$ and write $y = x^n$ for some $x \in H$. Now $x^{-1}y \in H$ since both $x, y \in H$ but $x^{-1}y = x^{-1}x^n = [x, n]$, so we have $[x, n] \in H$. Since $N \lhd G$, we have $[x, n] \in N$ so $[x, n] \in N \cap H = 1$ so $x = y$. Then $x = y = x^n$ implies that $x = 1$ since $n \neq 1$ and so $y = 1^n = 1$ also.

Now assume that $H \cap H^g = 1$ whenever $g \notin H$. So given $h \in H$ with $h \neq 1$, we want $\mathbf{C}_N(h)$ to be trivial. So suppose $n \in \mathbf{C}_N(h)$. Then $h \in H$ and $h \in H^n$, so we have $h \in H \cap H^n$. Since $h \neq 1$, we must have $n \in \mathbf{N}_G(H) = H$ by assumption, and thus $n \in H \cap N = 1$. □

We now make a few more definitions and observations.

Definition 33.1. In the above lemma, if the action is Frobenius, then we say that $G = N \rtimes H = NH$ is a *Frobenius group*, provided that $N > 1$ and $H > 1$.

If $G = NH$ is a Frobenius group, then N is called the *Frobenius kernel* and the conjugates of H are called the *Frobenius complements* of G.

Lemma 33.3. Let $H \subseteq G$ and assume that $H \cap H^g = 1$ for all $g \in G - H$. Let $K = G - \left(\bigcup_{g \in G} H^g \right) \cup \{1\}$. Then $|K| = |G : H|$.

Proof. The number of conjugates if H in G is $|G : \mathbf{N}_G(H)| = |G : H|$ by the FCP and since every two distinct conjugates of H intersect trivially. Then the number of nonidentity elements in $\bigcup_{g \in G} H^g$ is $|G : H|(|H| - 1) = |G| - |G : H|$. So the number of non-identity elements in K is $(|G| - 1) = (|G| - |G : H|)$, making $|K| = (|G| - 1) - (|G| - |G : H|) + 1 = |G : H|$. □

Lemma 33.4. Let G be a Frobenius group with kernel N and complement H. Then $N = K$.

Proof. N does not contain any non-identity element of ANY conjugate of H; hence $N \subseteq K$. Yet $|N| = |G : H| = |K|$, so we must have equality. □

It is a theorem of (who else) Frobenius that if *ever* there exists $H \subseteq G$ with $H \cap H^g = 1$ for all $g \in G - H$ then G is a Frobenius group. However, all known proofs of this use character theory (see ch.7 of Isaacs' book).

Definition 33.2. Let Π be a set of subgroups of G. Suppose that $\cup\Pi = G$ and that if $X, Y \in \Pi$ with $X \neq Y$ then we have $X \cap Y = 1$. Then Π is said to be a *partition* of G.

If G is a Frobenius group, then G is partitioned by the Frobenius kernel and all of the complements. As a final example of a partitioned group, take $C_p \times C_p$, which is partitioned by its cyclic subgroups.

34 04-20-10

Let G be a group with Π a set of subgroups. Then Π is a *partition* if $\cup\Pi = G$ and when $X, Y \in \Pi$ with $X \neq Y$ then we have $X \cap Y = 1$. We have seen that if $G = NA$ is a Frobenius group then we have a partition Π consisting of N and all of the conjugates of A in G. From this, we conclude that $|\Pi| = 1 + |G : A| = 1 + |N|$ since there are $|G : A|$ G-conjugates of A by definition.

Lemma 34.1. Let G be partitioned by Π with $|\Pi| = 1 + n$. Assume that G acts on an abelian group A. Assume that there exists an $a \in A$ such that $a^n \neq 1$. Then there exists $X \in \Pi$ such that $\mathbf{C}_A(X) \neq 1$.

Proof. Given a subgroup $H \subseteq G$ and an element $t \in A$, write $t^H = \left(\prod_{h \in H} t^h \right) \in A$. Note that each $t^h \in A$ also, and that this product is well defined since A

is abelian. Additionally, we have $t^H \in \mathbf{C}_A(H)$ since applying any $h \in H$ to t^H simply permutes the factors. Applying this definition across the partition allows us to compute a^G, and we obtain the formula $a^n a^G = \prod_{X \in \Pi} a^X$, where we have a copy of a^n on the left hand side to balance out the overcounting of a on the right. Now $a^n \neq 1$ by hypothesis, so it must be the case that either $a^G \neq 1$ or $a^X \neq 1$ for some $X \in \Pi$. If $a^X \neq 1$ for some $X \in \Pi$, then we know that $1 \neq a^X \in \mathbf{C}_A(X)$ and we are done. So assume that $a^X = 1$ for all $X \in \Pi$. Then we must have that $a^G \neq 1$, so $\mathbf{C}_A(G) > 1$ since a^G is certainly centralized by G. But if $\mathbf{C}_A(G) > 1$ then we have certainly have $\mathbf{C}_A(X) > 1$ for some $X \in \Pi$, and this is a contradiction. Therefore the only case that can happen has $\mathbf{C}_A(X) > 1$ for some $X \in \Pi$, as desired. □

We now draw a few corollaries from this lemma about what groups can induce a Frobenius action. Isaacs' referred to this next corollary as "A prohibition on partitioned groups acting Frobeniusly". He also said that I should never write the phrase "acts Frobeniusly", but I just can't help myself.

Corollary 34.1. Let A act on N where the action is Frobenius with $N \neq 1$. Assume that A is solvable. Then A cannot be partitioned by Π if $|\Pi| = 1 + n$ where $(n, |N|) = 1$ with all members of Π nontrivial.

Proof. Assume that Π is a partition of A with the above conditions. Let p divide $|N|$ for some prime p and let $P \in \mathrm{Syl}_p(N)$ chosen such that P is A-invariant; this uses our Sylow-E theorem with glasses which comes from Glauberman's lemma. Write $Z = \mathbf{Z}(P)$. We know that $Z > 1$ since non-trivial p-groups have non-trivial centers, and we know that Z is A-invariant since A acts via automorphisms and automorphisms must fix characteristic subgroups. Since p divides $|N|$, we know that $(n, p) = 1$ so $z^n \neq 1$ for all $z \in Z$ with $z \neq 1$. By the previous lemma, we know then that there exists $X \in \Pi$ such that $\mathbf{C}_A(X) > 1$. But $X \subseteq A$ with X non-trivial [by hypothesis] and the action of A is Frobenius on N and therefore also on P and Z. We have therefore reached a contradiction, so no such partition can exist. □

Corollary 34.2. Let $A = C_p \times C_p$. Then there does not exist a Frobenius action of A on ANY non-trivial group.

Proof. The group $C_p \times C_p$ is solvable and can be partitioned by its cyclic subgroups. When we do this, we find that $|\Pi| = 1 + p$; this number arises from counting the number of non-identity elements and using the fact that each cyclic subgroup has exactly $p - 1$ generators. All members of Π are therefore non-trivial, and if A acts on N with a Frobenius action, then we have seen that $(|N|, |A|) = 1$. Since $|A| = p^2$, we know that $(|N|, p) = 1$, but this would give a counter-example to our previous corollary. Hence no such Frobenius action can exist. □

Theorem 34.1. Let A induce a Frobenius action on N with $N > 1$. Let $P \in \mathrm{Syl}_p(A)$. Then P contains at most one subgroup of order p.

Proof. If this is not the case, then let $Z \subseteq \mathbf{Z}(P)$ with $|Z| = p$ and let $U \subseteq P$ with $|U| = p$ and $U \neq Z$. Then UZ is a group having order p^2 and it is not a cyclic group; hence $UZ \equiv C_p \times C_p$. We then know by our previous corollary that UZ cannot induce a Frobenius action on any non-trivial group. However, it does, since we already assumed that the action of A on N is Frobenius, and therefore the action of any subgroup of A on N is Frobenius. We have therefore found our contradiction. □

It is a fact that if P is a p-group with exactly one subgroup of order p, then P is either cyclic or $p = 2$ and P is a generalized quaternion group. A *generalized quaternion group* is a 2-group with a large cyclic subgroup of index 2 such that every element NOT in the cyclic subgroup has order 4. A result of this fact if A induces a Frobenius action on N and 2 does not divide $|A|$ then A has all or its Sylow subgroups cyclic and therefore A is solvable. In fact, we saw in a homework assignment that the group A is metacyclic, meaning that it has derived length at most 2.

Theorem 34.2. Let $A > 1$ act on N where the action is Frobenius. Assume that N is solvable. Then N is nilpotent.

Proof. Suppose that the theorem is false, and let $|N|$ be smallest for a counterexample. Then if $H < N$ and H admits the action of A then H is nilpotent. Also, if $M > 1$ and $M \lhd N$ with M being A-invariant then N/M has smaller order than N and admits the action of A, so N/M is nilpotent. So if any such M exists, then we can conclude that N^∞, the last term in the central series for N, is contained in M. Now $\mathbf{O}_p(N) \neq 1$ for some prime p since N is solvable, so we have that $N^\infty \subseteq \mathbf{O}_p(N)$. If it were also the case that $\mathbf{O}_q(N) \neq 1$, then the same reasoning implies that $N^\infty \subseteq \mathbf{O}_q(N)$. However, we cannot have $N^\infty \subseteq \mathbf{O}_q(N)$ since we would then have $N^\infty \subseteq \mathbf{O}_p(N) \cap \mathbf{O}_q(N) = 1$ and since N is not nilpotent we know $N^\infty \neq 1$. Hence $\mathbf{O}_p(N)$ is the ONLY nontrivial $\mathbf{O}_q(N)$ for any prime q.

We now give a name to this subgroup, writing $U = \mathbf{O}_p(N) > 1$. Since $|N/U| < |N|$, we know that N/U is nilpotent, where U is A-invariant since U is characteristic in N which is normal in the semi-direct product. But $\mathbf{O}_p(N/U) = 1$, and since N/U is nilpotent this means that p does not divide $|N/U|$. We therefore conclude that $U \in \mathrm{Syl}_p(N)$.

We claim that U is abelian. To see this, consider $\Phi(N)$, the Frattini subgroup. If $\Phi(N) > 1$ then $N/\Phi(N)$ is nilpotent. But if $N/\Phi(N)$ is nilpotent then N is nilpotent, and since we are assuming that this is not the case we can deduce that $\Phi(N) = 1$. Now $U \lhd N$ so by a homework problem we know that $\Phi(U) \subseteq \Phi(N)$ and we have that $\Phi(U) = 1$. But $U' \subseteq \Phi(U)$ since all maximal subgroups of a p-group are normal and have index p, making the factor group abelian. So $U' \subseteq \Phi(U) = 1$ and U is abelian, as claimed.

Let $G = N \rtimes A = NA$. Also, UA/U acts on N/U inside of G/U simply by conjugation. Note that this conjugation action is Frobenius since $UA/U \cong A$ since $U \cap A \subseteq N \cap A = 1$ and Frobenius actions carry over to quotients. Thus G/U is a Frobenius group with kernel N/U and complement UA/U [Draw the

diamonds here, its very helpful]. Since Frobenius groups have partitions, we have a partition of G/U into $1+|N/U|$ pieces, namely N/U and the conjugates of UA/U. Also, G/U acts on U since G acts on U and the action of U on U is trivial since U is abelian. But $|U|$ is coprime to $|N/U|$ since $U \in \mathrm{Syl}_p(N)$, so we can conclude that some partitioning subgroup has a non-trivial fixed point in U from our very first lemma in this section.

Now we know that $\mathbf{C}_U(UA/U) = \mathbf{C}_U(A) = 1$, thus no conjugate of UA/U has a non-trivial fixed point in U. Thus $\mathbf{C}_U(N/U) > 1$ since N/U is the only partition element left. But $\mathbf{C}_U(N/U) = \mathbf{C}_U(N) \subseteq \mathbf{Z}(N)$. Thus $\mathbf{Z}(N) > 1$, and since the center of N is characteristic, we know $\mathbf{Z}(N)$ is A-invariant and can conclude that $N/\mathbf{Z}(N)$ is nilpotent. But $N/\mathbf{Z}(N)$ being nilpotent implies that N is nilpotent since we would have a central series for N obtained by taking a central series for $N/\mathbf{Z}(N)$ and adding on a term involving $\mathbf{Z}(N)$. Another way to see this is to see that $[\overline{N}, \overline{N}, \ldots, \overline{N}] = 1$, telling us that $[N, N, N, \ldots, N] \subseteq \mathbf{Z}(N)$, making $[N, N, N, \ldots, N, N] \subseteq [\mathbf{Z}(N), N] = 1$. □

35 Problem Set 10

Problem 50. Let $W \subseteq P \in \mathrm{Syl}_p(G)$. We say that W is **weakly closed** in P with respect to G if the only G-conjugate of W contained in P is W itself.

(a) Show that W is weakly closed in P if and only if it is normal in every Sylow p-subgroup that contains it and it is also normal in $\mathbf{N}_G(P)$.

(b) Suppose W is weakly closed in P and that $W \subseteq K \subseteq G$. Show that every G-conjugate of W contained in K is K-conjugate to W.

(c) Suppose $W \subseteq \mathbf{Z}(P)$ is weakly closed in P. Show that $\mathbf{N}_G(W)$ controls G-fusion in P.

NOTE: Problem 50(c) is Grün's theorem.

Problem 51. Let $P \in \mathrm{Syl}_p(G)$ and suppose that P is a maximal subgroup of G.

(a) If P' is contained in some Sylow p-subgroup of G different from P, show that G is not simple.

(b) If P is nontrivial and has nilpotence class at most 2, show that G is not simple.

HINT: Use Problem 50 for (b).

NOTE: Simple groups in which a Sylow 2-subgroup is maximal actually do exist, but this cannot happen if $p > 2$. This follows from Thompson's normal p-complement theorem, which we will discuss.

Problem 52. Suppose that every proper subgroup of G is supersolvable. Prove that G is solvable.

HINT: Use problem 48(c).

Problem 53. Suppose that for some prime p, every two-generator subgroup of G has a normal p-complement. Show that G has a normal p-complement.

HINT: If U is a p-subgroup of G, consider the subgroups of the form $\langle u, v\rangle$ where $u \in U$ and $v \in \mathbf{N}_G(U)$.

Problem 54. Let G be a Frobenius group with Frobenius complement A and Frobenius kernel N. If $M \lhd G$ and $M \not\subseteq N$, show that M is a Frobenius group.

36 04-22-10

We established last time that if A acts on N via a Frobenius action, $N > 1$, and N is known to be solvable, then we actually have that N is nilpotent. We now move on to the proof of Thompson's theorem.

Theorem 36.1 (Thompson)**.** Let $P \in \mathrm{Syl}_p(G)$ with $p \neq 2$. Assume that $\mathbf{N}_G(U)$ has a normal p-complement for all $U \neq 1$ with U characteristic in P. Then G has a normal p-complement.

The proof of this theorem of Thompson will have to wait until we establish some more machinery. This theorem of Thompson was essentially his thesis, and there was an awesomely hilarious article about it in the New York times. The title of the article was "50 year problem in math solved". If I knew how, I would link to it here.

It should be noted that the theorem IS false if $p = 2$, and there is a counterexample, which I think is A_5, but if that isn't true then I would check a wreath product.

Assuming the above theorem of Thompson, we can prove the following.

Theorem 36.2. Let A act on N where the action is Frobenius and $A > 1$. Then N is nilpotent.

Proof. Observe that it is no loss to assume that $|A| = r$ where r is prime since subgroups of A will also "act Frobeniusly". We again assume that the statement is false and take N such that $|N|$ is smallest for a counterexample. If $1 < M < N$ where M is characteristic in N, then M is acted upon by A where the action is Frobenius and A acts on the quotient N/M in a Frobenius manner. By the minimality of N, we have that both M and N/M are nilpotent and therefore certainly solvable, making N solvable. Then by our previous theorem, this implies that N is nilpotent, and therefore we have a contradiction to N being a counterexample. So no such M exists [Note that this does not mean that N is simple, it means that N lacks nontrivial characteristic subgroups]. We also know that N is not a p-group for any prime p since we are assuming that N is not nilpotent. Thus $|N|$ is divisible by at least 2 primes, one of which, say p, is not 2. Now $\mathbf{O}_p(N) < N$ since N is not a p-group. Thus $\mathbf{O}_p(N) = 1$. Let $P \in \mathrm{Syl}_p(N)$ be A-invariant, where we know that such a P exists by the

"magic eyeglasses" theorem. Let $1 < U$ be a characteristic subgroup of P. Now A stabilizes U since U is characteristic in P and P is A-invariant, and since U uniquely determines its normalizer, we can conclude that $\mathbf{N}_N(U)$ is A-invariant. But U is not normal in N since $\mathbf{O}_p(N) = 1$ and U is a p-group, so $\mathbf{N}_N(U) < N$. The minimality of N implies that $\mathbf{N}_N(U)$ is nilpotent and therefore has a normal p-complement. By Thompson's theorem, we can therefore conclude that N has a normal p-complement M. However, $1 < M < N$ and M is characteristic in N, and this is a contradiction. □

36.1 The Thompson Subgroup

We now enter what is chapter 7 in Isaacs' book.

Given P a p-group, then Thompson subgroup $\mathbf{J}(P)$ is a subgroup such that if we know $P > 1$ then we know $\mathbf{J}(P) > 1$. The point of introducing $\mathbf{J}(P)$ is to eventually prove the following crucial theorem of Thompson.

Theorem 36.3 (Thompson, 1964)**.** Let $P \in \mathrm{Syl}_p(G)$ with $p \neq 2$. Assume that $\mathbf{C}_G(\mathbf{Z}(P))$ and $\mathbf{N}_G(\mathbf{J}(P))$ have normal p-complements. Then G has a normal p-complement.

We now give the definition of the Thompson subgroup, although calling it THE definition is misleading, since there are actually three different Thompson subgroups that work. The definition we give is NOT Thompson's original definition. Given a p-group P, let $\mathcal{E}(P)$ be the set of elementary abelian subgroups of largest possible order.

Definition 36.1. We define $\mathbf{J}(P) = \langle E | E \in \mathcal{E}(P) \rangle$.

Lemma 36.1. Let A be abelian, non-cyclic, and act on L where $(|A|, |L|) = 1$. Then $L = \langle \mathbf{C}_L(a) | a \in A,\ a \neq 1 \rangle$.

Proof. Let $M = \langle \mathbf{C}_L(a) | a \in A,\ a \neq 1 \rangle$. Assume for contradiction that $M < L$. Choose a prime p dividing $|L : M|$, and let $P \in \mathrm{Syl}_p(L)$ be A-invariant. Now P is not contained in M since p divides $|L : M|$, so let $X = P \cap M$, noting that $X < P$. Also note that M is A-invariant since by definition, each $\mathbf{C}_L(a)$ and the action of A on the generators of M simply permutes them. Write $Y = \mathbf{N}_P(X)$. We know that $Y > X$ since $X < P$ and normalizers grow in p-groups. Also, Y is A-invariant since X is A-invariant, where X is a-invariant as it is the intersection of two A-invariant subgroups. Therefore A acts on Y/X, and we claim that this action is Frobenius. Let $a \in A$ with $a \neq 1$. We compute $\mathbf{C}_{Y/X}(a) = \dfrac{X\mathbf{C}_Y(a)}{X} = X/X = 1$ since fixed points come from fixed points. But $\mathbf{C}_Y(a) \subseteq \mathbf{C}_L(a) \subseteq M$, but $\mathbf{C}_Y(a) \subseteq P$ by its definition, so $\mathbf{C}_Y(a) \subseteq M \cap P = X$. This tells us that $(X\mathbf{C}_Y(a))/X = X/X = 1$, giving us that the action is Frobenius. However, the action cannot be Frobenius since A is not cyclic, since the only abelian groups which are not cyclic contain a copy of $C_q \times C_q$ for some prime q, and we know that these groups cannot act Frobeniusly. □

37 04-27-10

Recall last time that we found that if A is abelian and non-cyclic, A acts on L and the action is coprime, then $L = \langle \mathbf{C}_L(a) | a \in A,\ a \neq 1 \rangle$. We now draw a quick and useful corollary of this fact.

Corollary 37.1. Assume that A is abelian and acts faithfully on L, where $(|A|, |L|) = 1$. Assume A acts trivially on M for all A-invariant $M < L$. Then A is cyclic.

Proof. If $a \in A$, then $\mathbf{C}_L(a)$ is A-invariant since A is abelian. If $a \neq 1$, then $\mathbf{C}_L(a) < L$ since the action of A is faithful. So A centralizes $\mathbf{C}_L(a)$ by hypothesis, and so A acts trivially on L if A is not cyclic, and this would be a contradiction. Hence A is cyclic. □

We now need to list a few linear algebra facts. Let $G = \mathrm{GL}(2, p)$. Then by counting row choices, we see that we have $p^2 - 1$ choices for the first row (cannot pick (0,0)) and $p^2 - p$ choices for the second row, since we cannot pick any of p scalar multiples of the first row. Thus $|G| = (p^2 - 1)(p^2 - p) = p(p-1)^2(p+1)$. Now $S = \mathrm{SL}(2, p)$ is the collection of determinant one matrices in G, so G/S is isomorphic to the multiplicative group of the field of order p, which is cyclic and has order $(p-1)$. We conclude that $G' \subseteq S$ and from the first isomorphism theorem we have that $|S| = p(p-1)(p+1)$. Also, if $p \neq 2$, then we have that S has a unique involution, the negative of the identity matrix. With these facts in hand, we proceed to a technical lemma.

Lemma 37.1. Let $L \subseteq \mathrm{GL}(2, p)$ where p is prime and p does not divide $|L|$. Let $P \in \mathrm{Syl}_p(\mathrm{GL}(2, p))$. Assume that $P \subseteq \mathbf{N}_{\mathrm{GL}(L)}$. Assume that $p \neq 2$ and that a Sylow 2-subgroup of L is abelian. Then $P \subseteq \mathbf{C}_{\mathrm{GL}}(L)$.

Proof. We may assume by induction that $P \subseteq \mathbf{C}_{GL}(M)$ for $M < L$ with $P \subseteq \mathbf{N}_{GL}(M)$. We can assume by the coprimeness that L is a q-group for some prime q with $q \neq p$. Also, if $[L, P] < L$ then $[L, P, P] = 1$. But $[L, P] = [L, P, P] = 1$ and this is what we want, so we can assume that $[L, P] = L$. So $L \subseteq \mathrm{GL}(2, p)' \subseteq \mathrm{SL}2, p$. If $q = 2$, then L is a 2-group so L is abelian by hypothesis so L is an abelian subgroup having only one involution. This implies that L is cyclic, so p does not divide $|\mathrm{Aut}(L)|$ and we conclude that P acts trivially. So we may assume that q is odd. Now $|L|$ divides $p(p-1)(p+1)$ and $|L| = q^e$ for some e. Since $q \neq 2$, we cannot have q dividing both $(p-1)$ and $(p+1)$ so q^e must divide one or the other, but not both. Either way, we know $|L| \leq p + 1$, and in fact $|L| < p + 1$ since $p + 1$ is even. There is therefore no room in L for a non-trivial P-orbit, so we are done. □

We now start the proof of Thompson's theorem, which is broken up into 3 main theorems, each of which has some parts.

Theorem 37.1 (Normal-P)**.** Let G act faithfully via automorphisms on a p-group V. Let $P \in \mathrm{Syl}_p(G)$. Assume that $|V : \mathbf{C}_V(P)| \leq p$. Assume:

(1) G is p-solvable.

(2) $p \neq 2$.

(3) A Sylow 2-subgroup of G is abelian.

Then $P \lhd G$.

Proof. Assume false, and let $|G|$ be minimal for a counter-example. Let $Q \neq P$ with $Q \in \mathrm{Syl}_p(G)$. Now $\langle P, Q\rangle$ satisfies the hypotheses; subgroups of p-solvable groups are p-solvable, $p \neq 2$, a Sylow 2-subgroup of $\langle P, Q\rangle$ is a subgroup of a Sylow 2-subgroup of G and this therefore abelian. Subgroups of G will also act faithfully and since the order of a Sylow p-subgroup of G is the order of a Sylow p-subgroup of $\langle P, Q\rangle$, we do satisfy all hypotheses. [In the future, we will not check so rigorously]. By conjugating everything by an element of G, we can see that $|V : \mathbf{C}_V(Q)| = |V : \mathbf{C}_V(P)| \leq p$. Let $U = \mathbf{C}_V(P) \cap \mathbf{C}_V(Q)$. We conclude that $|V : U| \leq p^2$, so G acts trivially on U. Now V/U is elementary abelian [due to its order and that we know it is not cyclic as $\mathbf{C}_V(P)$ and $\mathbf{C}_V(Q)$ are two subgroups of order p]. Let $K = \mathbf{C}_G(V/U)$. We then have that $[V, K] \subseteq U$ so $[V, K, K] \subseteq [U, K] = 1$ since $K \subseteq G$ and G acts trivially on U.

We claim that K is a p-group. To see this, let $S \in \mathrm{Syl}_q(K)$ for $q \neq p$. We want to show that $S = 1$. Now $[V, S, S] \subseteq [V, K, K] = 1$. But since the action of V on S is coprime, we have $[V, S, S] = [V, S]$, and thus $[V, S] = 1$. We can then conclude that $S = 1$ since $S \subseteq K \subseteq G$ and G acts faithfully on V. Now $K \subseteq P$ and $K \subseteq Q$, and we write $\overline{G} = G/K$. [We can mod out by K since it is the kernel of an action]. Notice that $\overline{P} \neq \overline{Q}$ since P and Q both contain K and that $\overline{P}, \overline{Q} \in \mathrm{Syl}_p(\overline{G})$. Also, we know that $\overline{G}$ acts faithfully on V/U. From these observations, we conclude that we can replace V by V/U and G by $\overline{G}$ and we still have a counterexample which satisfies the hypotheses. However, we have gained the extra assumption that V is an elementary abelian p-group of order p^2, since we do NOT have a counterexample if $V = 1$ or $|V| = p$.

We can also now make the assumption that $G \subseteq \mathrm{GL}(2, p)$ since elementary abelian groups of order p^2 can be though of as a vector space over the field of order p [Think of $V = C_p \times C_p$ externally, so that it is in the form (c, b)]. So $|P| = q = |Q|$ since we know the order of $\mathrm{Gl}(2, p)$. If P and Q are to be different, then $P \cap Q = 1$ and thus $\mathbf{O}_p(G) = \cap_{P \in \mathrm{Syl}_p(G)} P = 1$. Let $L = \mathbf{O}_{p'}(G)$. We know that $L > 1$ since G is p-solvable and $P \subseteq \mathbf{N}_G(L)$ since $L \lhd G$. Therefore our previous technical lemma gives us that $P \subseteq \mathbf{C}_G(L)$. But by lemma 1.2.3, we know that $\mathbf{C}_G(L) \subseteq L = \mathbf{O}_{p'}(G)$ and $P > 1$, and this is our contradiction. □

Theorem 37.2 (Normal-J)**.** Let $P \in \mathrm{Syl}_p(G)$. Assume:

(1) G is p-solvable.

(2) $p \neq 2$.

(3) A Sylow 2-subgroup of G is abelian.

(4) $\mathbf{O}_{p'}(G) = 1$.

(5) $\mathbf{C}_G(\mathbf{Z}(P)) = P$.

Then $\mathbf{J}(P) \lhd G$.

Proof. We again argue for contradiction, and assume that $|G|$ is minimal for a counterexample. Let $U = \mathbf{O}_p(G) > 1$ since G is p-solvable and $\mathbf{O}_{p'}(G) = 1$ by assumption (4). So write $\overline{G} = G/U$. Write $\overline{L} = L/U$ for $\mathbf{O}_{p'}(G/U)$. We break up this proof into steps.

Step 1. There exists $A \in \mathcal{E}(P)$, the collection of elementary abelian subgroups of P with largest possible order, with A not contained in U.

For the proof or step 1, we argue for contradiction. If this were not the case, then we would have $\mathbf{J}(P) \subseteq U$. But this makes $\mathbf{J}(P) \subseteq \mathbf{J}(U)$ [as it will make $\mathcal{E}(P) = \mathcal{E}(U)$], and since $\mathbf{J}(U)$ is characteristic inside U which is normal in G, this would make $\mathbf{J}(P) \lhd G$, which contradicts that we are in a counter-example.

Step 2. The following hold.

(a) $\mathbf{Z}(P) \subseteq U$.

(b) If $U \subseteq H \subseteq G$ then $\mathbf{O}_{p'}(H) = 1$.

(c) $\mathbf{C}_{\overline{G}}(\overline{L}) \subseteq \overline{L}$.

The proof of each of these statements is simply an application of lemma 1.2.3. Part (a) follows as $\mathbf{Z}(P) \subseteq \mathbf{C}_G(U)$ and $\mathbf{C}_G(U) \subseteq U$ by 1.2.3. Part (b) follows since when $U \subseteq H \subseteq G$, we have $U \lhd H$, $\mathbf{O}_{p'}(H) \lhd H$, and disjoint normal subgroups commute, putting $\mathbf{O}_{p'}(H) \subseteq U$ by lemma 1.2.3, and this implies that we must have $\mathbf{O}_{p'}(H) = 1$ since U is a p-group. Finally, part (c) follows directly by applying lemma 1.2.3 in $\overline{G}$.

We continue with this proof next time. □

38 04-29-10

We continue today with the proof of the normal J-theorem. We restate both the theorem and the first two steps, which were proved last time.

Theorem 38.1 (Normal-J)**.** Let $P \in \mathrm{Syl}_p(G)$. Assume:

(1) G is p-solvable.

(2) $p \neq 2$.

(3) A Sylow 2-subgroup of G is abelian.

(4) $\mathbf{O}_{p'}(G) = 1$.

(5) $\mathbf{C}_G(\mathbf{Z}(P)) \lhd G$.

Then $\mathbf{J}(P) \lhd G$.

Proof. We are assuming that $|G|$ is smallest for a counter-example, and we have $U = \mathbf{O}_p(G)$ and L such that $\overline{L} = \mathbf{O}_{p'}(\overline{G})$. Steps 1 and 2, which we list below, were proven last time:

Step 1. There exists $A \in \mathbf{E}(P)$ with $A \not\subseteq U$.

Step 2. The following hold:

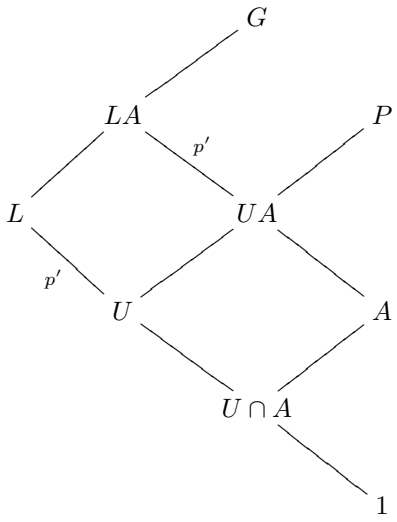
(a) $\mathbf{Z}(P) \subseteq U$.

(b) If $U \subseteq H \subseteq G$ then $\mathbf{O}_{p'}(H) = 1$.

(c) $\mathbf{C}_{\overline{G}}(\overline{L}) \subseteq \overline{L}$.

Step 3. $LA = G$ and $UA = P$.

We begin by proving step 3. We find the following picture helpful:



Now $|LA : UA| = |L : U|$ is p', so $UA \in \mathrm{Syl}_p(LA)$, and thus $UA = LA \cap P$. It therefore suffices to show that $LA = G$, and the diamond lemma will give us that $UA = P$. So suppose for contradiction that $LA < G$. We check that LA satisfies the hypotheses of the theorem. The first three of the hypotheses are clearly satisfied, and the hypothesis (4) is satisfied by step (2) claim (b). We need to check that (5) holds in the group LA; that is, we need to show that $\mathbf{C}_{LA}(\mathbf{Z}(UA)) = UA$. Now we know by step (2) part (a) that $\mathbf{Z}(P) \subseteq U$, so $\mathbf{Z}(P) \subseteq UA$, and $\mathbf{Z}(P) \subseteq \mathbf{Z}(UA)$. So $P = \mathbf{C}_G(P) \supseteq \mathbf{C}_G(\mathbf{Z}(UA))$. In words, we know that anything in G which centralizes the center of UA will also centralize $\mathbf{Z}(P)$ since $\mathbf{Z}(P) \subseteq \mathbf{Z}(UA)$. Now $UA \subseteq \mathbf{C}_{LA}(\mathbf{Z}(UA)) \subseteq P \cap LA = UA$, so we see that (5) holds. By the minimality of G as a counter-example, we have that $\mathbf{J}(UA) \lhd LA$. Mod U, we therefore have that $\overline{\mathbf{J}(UA)} \lhd \overline{LA}$ and $\overline{L} \lhd \overline{LA}$, and we know that $\overline{\mathbf{J}(UA)} \cap \overline{L} = 1$ since $\overline{L}$ is p' and $\overline{JUA}$ is a p-group. Since disjoint normal subgroups commute, we have that $\overline{J(UA)} \subseteq \mathbf{C}_{\overline{G}}(\overline{L}) \subseteq \overline{L}$ by step

(2) part (c). But U is the unique Sylow p-subgroup of L, so $\mathbf{J}(UA) \subseteq U$. But $A \subseteq \mathbf{J}(UA) \subseteq U$, and this is contradiction to step (1), and we have step 3.

Step 4. Let $U \subseteq M < L$ and assume that M is A-invariant. Then $[M, A] \subseteq U$.

We look at $MA < G$, where MA is a group since A normalizes M. We wish to check the hypotheses and see that they apply to the group MA. We again have that property (4) holds by step (2) part (b), and here (5) holds since $P \in \mathrm{Syl}_p(MA)$ and we are assuming that the properties hold for P. Therefore MA satisfies the theorem and $MA < G$, and we have that $\mathbf{J}(P) \lhd MA$. Now $[M, A] \subseteq M$ since N is A-invariant. But $[M, A] \subseteq [M, \mathbf{J}(P)] \subseteq \mathbf{J}(P)$ since $A \in \mathcal{E}(P)$ and $\mathbf{J}(P) \lhd MA$. This therefore gives us that $[M, A] \subseteq M \cap \mathbf{J}(P) \subseteq M \cap P \subseteq U$. Since $\mathbf{J}(P)$ is a p-group and U is the unique Sylow p-subgroup of M.

Step 5. $|\overline{A}| = p$.

We know that $\overline{A}$ acts faithfully on $\overline{L}$ by step (2) part (c). By step 4, we know that $\overline{A}$ centralizes and therefore acts trivially on all proper subgroups of $\overline{L}$ on which it acts. By a previous corollary, we know that $\overline{A}$ is cyclic. But $A \in \mathbf{E}(P)$ implies that A is an elementary abelian subgroup, and we conclude that $|\overline{A}| = p$ since the only elementary abelian cyclic subgroups are those of order p.

Before starting step 6, we introduce a small bit of notation. Let $V = \Omega_1(\mathbf{Z}(U))$; i.e. V is the group generated by the elements of order p in $\mathbf{Z}(U)$. It is important to note that V is elementary abelian.

Step 6. $\mathbf{C}_G(V) = U$.

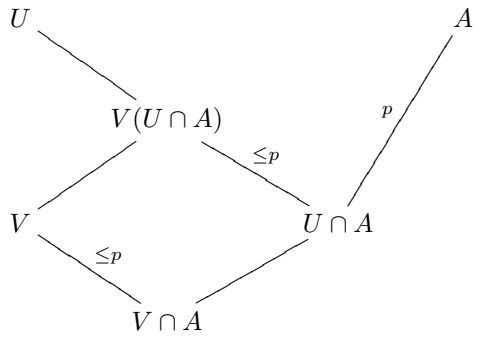
The one containment here is obvious. To show that $\mathbf{C}_G(V) \subseteq U$, we work as follows. Write $C = \mathbf{C}_G(V)$. Now $C \lhd G$ as it is the kernel of an action. Therefore, if we can show that C is a p-group then we will have that $C \subseteq U$ since $U = \mathbf{O}_p(G)$. So let $Q \in \mathrm{Syl}_q(C)$ for $q \neq p$. We want to show that $Q = 1$.

Now Q acts on $\mathbf{Z}(U)$ and Q fixes all elements of order p in $\mathbf{Z}(U)$ since Q is a subgroup of C. By Fitting's theorem, we know that Q acts trivially on $\mathbf{Z}(U)$. By step (2) part (a), we know that $\mathbf{Z}(P) \subseteq U$ and therefore $\mathbf{Z}(P) \subseteq \mathbf{Z}(U)$ as $U \subseteq P$. So $Q \subseteq \mathbf{C}_G(\mathbf{Z}(U)) \subseteq \mathbf{C}_G(\mathbf{Z}(P)) = P$ by hypothesis (5). So Q, a q-group is contained in P a p-group, and we have that $Q = 1$. This shows us that $\overline{G}$ acts faithfully on V since U is exactly the kernel of the action of G on V.

Step 7. $|V : \mathbf{C}_V(P)| \leq p$.

This step is the key step in the argument. Note that the group $V(U \cap A)$ is elementary abelian since V and $U \cap A$ are both elementary abelian and the factors centralize each other. [$U \cap A \subseteq A \in \mathcal{E}(P)$, V is elementary abelian by definition, V centralizes U and $U \cap A \subseteq U$]. By the maximality of A in $\mathbf{E}(P)$, we cannot have that $|V(U \cap A) : U \cap A| > p$ since $|A : U \cap A|$ is p. Hence $|V(U \cap A)|U \cap A| \leq p$. Recall that $P = UA$. Now U acts trivially on V, so $\mathbf{C}_V(P) = \mathbf{C}_G(UA) = \mathbf{C}_V(A) \supseteq (V \cap A)$. So $|V : \mathbf{C}_V(P)| \leq |V : V \cap A| = |V(U \cap A) : U \cap A| \leq p$.

This picture may be helpful:



Finally, we can complete the proof. We now satisfy all of the requirements for the normal p-theorem, and we know then that $\overline{P} \lhd \overline{G}$, which tells us that $P \lhd G$ by the correspondence theorem. But $\mathbf{J}(P)$ is characteristic in P which is normal in G, so $\mathbf{J}(P) \lhd G$, and this is our contradiction as G was taken to be a counterexample.

□

We now move towards the proof of Thompson's theorem. Before getting there, we need a lemma along the lines of fixed points come from fixed points.

Lemma 38.1. Let $M \lhd G$ be a p'-group. Write $\overline{G} = G/M$. Let $U \subseteq G$ be a p-group.

(a) $\mathbf{N}_{\overline{G}}(\overline{U}) = \overline{\mathbf{N}_G(U)}$

(b) $\mathbf{C}_{\overline{G}}(\overline{U}) = \overline{\mathbf{C}_G(U)}$

Proof. We did part (a) previously.

For part (b), we know that we already have one containment, namely that $\overline{\mathbf{C}_G(U)} \subseteq \mathbf{C}_{\overline{G}}(\overline{U})$. That is, everything that already commuted with U will still commute with the image of U under the bar map. For the other direction, note that $\mathbf{C}_{\overline{G}}(\overline{U}) \subseteq \mathbf{N}_{\overline{G}}(\overline{U}) = \overline{\mathbf{N}_G(U)}$ by part (a). So $\mathbf{C}_{\overline{G}}(\overline{U})$ can be written as $\overline{X}$ for some $X \subseteq \mathbf{N}_G(U)$. Now $[X, U] \subseteq U$ since X normalizes U. Therefore $\overline{[X, U]} = [\overline{X}, \overline{U}] = 1$ since $\overline{X} = \mathbf{C}_{\overline{G}}(\overline{U})$. Thus $[X, U] \subseteq M$. This makes $[X, U] \subseteq (M \cap U) = 1$ since M is a p'-group and U is a p-group. This tells us that $X \subseteq \mathbf{C}_G(U)$, and therefore $\overline{X} \subseteq \overline{\mathbf{C}_G(U)}$. As $\mathbf{C}_{\overline{G}}(\overline{U}) = \overline{X}$, this gives us the second containment, and we have equality. □

We now proceed to the proof of Thompson's theorem.

Theorem 38.2 (Thompson, 1964)**.** Let $P \in \mathrm{Syl}_p(G)$ with $p \neq 2$. Write $Z = \mathbf{Z}(P)$ and $J = \mathbf{J}(P)$. Assume that $\mathbf{N}_G(J)$ and $\mathbf{C}_G(Z)$ have normal p-complements. Then G has a normal p-complement.

Proof. As we did with our other important theorems, assume that the theorem is false, and let $|G|$ be minimal for a counter-example. By Frobenius' theorem, we then know that there exists a p-subgroup $U > 1$ such that $\mathbf{N}_G(U)$ does NOT have a normal p-complement. There may be many such U's, so among the U's that work, choose U such that the p-part of $|\mathbf{N}_G(U)|$ is as large as possible. Again, there may be many such U's with this property, so among the U's which yield a maximal p-part of the normalizer, select U to be maximal with respect to order.

NOTE: This is a very subtle induction. As with the case of the normal J-theorem, we proceed in steps.

□

39 05-04-10

We continue with the proof of Thompson's theorem.

Proof.

Step 1. $\mathbf{O}_{p'}(G) = 1$.

For the proof of step 1, let $M = \mathbf{O}_{p'}(G)$. Assume that $M > 1$. Then $\overline{G} = G/M$ is not a counterexample. To see why this is true, we check to see that $\overline{G}$ satisfies all of our hypotheses. Now $P \cong \overline{P}$ since M is a p'-subgroup. Notice that $\overline{J} = \mathbf{J}(\overline{P})$ and that $\overline{Z} = \mathbf{Z}(\overline{P})$. Also, $\mathbf{N}_{\overline{G}}(\overline{J}) = \overline{\mathbf{N}_G(J)}$ has a normal p-complement and $\mathbf{C}_{\overline{G}}(\overline{Z}) = \overline{\mathbf{C}_G(Z)}$ has a normal p-complement, so the minimality of G implies that $\overline{G}$ has a normal p-complement. However, M is a p'-subgroup, and so a normal p-complement in $\overline{G}$ pulls back to a normal p-complement in G, and this is a contradiction. Thus $|M| = |\mathbf{O}_{p'}(G)| = 1$.

Step 2. $U \lhd G$. In fact, $U = \mathbf{O}_p(G)$.

Let $N = \mathbf{N}_G(U)$. Suppose for contradiction that $N < G$. Now N does NOT have a normal p-complement since G is a counter-example. Let $S \in \mathrm{Syl}_p(N)$. WLOG, we can assume that $S \subseteq P$. If $S = P$, then $\mathbf{J}(S) = J$ and $\mathbf{Z}(S) = Z$ implying that $\mathbf{N}_G(\mathbf{J}(S)) = \mathbf{N}_G(J)$ and $\mathbf{C}_G(\mathbf{Z}(S) = \mathbf{C}_G(Z)$ have normal p-complements. So $\mathbf{N}_N(\mathbf{J}(S))$ and $\mathbf{C}_N(\mathbf{Z}(S))$ have normal p-complements as the property of having normal p-complements is inherited by subgroups. Induction would then give us that N has a normal p-complement, and this is a contradiction. Thus $S < P$, so $\mathbf{N}_P(S) > S$ since normalizers grow, and therefore $|\mathbf{N}_G(U)|_p = |S| < |\mathbf{N}_P(S)|$. Write X for either $\mathbf{J}(S)$ or $\mathbf{Z}(S)$. Then X is characteristic in S which is normal in $\mathbf{N}_P(S)$ and so $X \lhd \mathbf{N}_P(S)$. Therefore $|\mathbf{N}_G(X)|_p > |S| = |\mathbf{N}_G(U)|_p$, and we conclude by the way that we chose U that $\mathbf{N}_G(X)$ has a normal p-complement. So $\mathbf{N}_N(X)$ has a normal p-complement [and thus if $X = \mathbf{Z}(S)$ so does $\mathbf{C}_N(S)$ since subgroups have normal p-complements], and N therefore has a normal p-complement by the minimality of G. This is our contradiction, so $N = G$ and $U \lhd G$ as claimed.

Step 3. Let $U < U_1$ where $U_1 \lhd P$. Then $\mathbf{N}_G(U_1)$ has a normal p-complement.

Now $|G|_p = |\mathbf{N}_G(U)|_p = |P| = \mathbf{N}_G(U_1)$ by step 2, and we know that $|U| < |U_1|$. Therefore by our choice of U, we conclude that $\mathbf{N}_G(U_1)$ has a normal p-complement.

Step 4. G/U has a normal p-complement.

Since $U > 1$, we know that $|G/U| < |G|$. If G/U is a p'-group then we are trivially done, so we can assume that p divides $|G/U|$ so that $U < P$. Write J_1/U for $\mathbf{J}(P/U)$ and Z_1/U for $\mathbf{Z}(P/U)$. Both J_1/U and Z_1/U are non-trivial since P/U is non-trivial, so $U < J_1$ and $U < Z_1$. In fact, the correspondence theorem gives us that J_1 and Z_1 are normal in P. By step 3, we know that $\mathbf{N}_G(J_1)$ and $\mathbf{N}_G(Z_1)$ have normal p-complements. Thus $\mathbf{N}_{G/U}(J_1/U) = \mathbf{N}_G(J_1)/U$ and $\mathbf{N}_{G/U}(Z_1/U) = \mathbf{N}_G(Z_1)/U$ have normal p-complements. If $\mathbf{N}_{G/U}(Z_1/U)$ has a normal p-complement then we know that $\mathbf{C}_{G/U}(Z_1/U)$ has a normal p-complement as having a p-complement is a property inherited by subgroups. Thus G/U satisfies the hypotheses of our theorem and $|G/U| < |G|$, so we can conclude that G/U has a normal p-complement.

Write L so that L/U is the normal p=complement of G/U. We then have $U \subseteq L \subseteq G$ with U, L both normal in G and $|G : L|$ a p-power, $|L : U|$ a p'-number, and $|U|$ a p-power. This establishes that this minimal counter-example for the normal J-theorem is in fact a p-solvable group.

Step 5. P is maximal in G.

Let $P \subseteq H < G$, and check that H satisfies the hypotheses of the theorem [$P \subseteq H$ so $\mathbf{J}(P)$ in H is the original J that we started with, etc.]. Note that $\mathbf{N}_H(J) = \mathbf{N}_G(J)$. This tells us that H has a normal p-complement, say M, so that $U \lhd H$ and $M \lhd H$ with $U \cap M = 1$. Since disjoint normal subgroups commute, we have that $M \subseteq \mathbf{C}_G(U)$. But we know that $\mathbf{O}_{p'}(G) = 1$ by step 1 and that G is p-solvable by the previous step, so by Lemma 1.2.3, we have $\mathbf{C}_G(\mathbf{O}_p(G)) \subseteq \mathbf{O}_p(G)$. Since $U = \mathbf{O}_p(G)$, we have $M \subseteq \mathbf{C}_G(U) \subseteq U$, and since M is a p'-group we must have that $M = 1$. This gives us that H is a p-group and hence $P = H$ as P is a full Sylow p-subgroup of G.

Step 6. $P = \mathbf{C}_G(Z)$.

Since $Z = \mathbf{Z}(P)$, we know that $P \subseteq \mathbf{C}_G(Z)$. By the maximality of P, we must either have that $P = \mathbf{C}_G(Z)$ or $\mathbf{C}_G(Z) = G$. However, $\mathbf{C}_G(Z)$ has a normal p-complement by assumption and G does not, so we cannot have $\mathbf{C}_G(Z) = G$, and we conclude that $\mathbf{C}_G(Z) = P$.

Step 7. L/U is abelian, and therefore a Sylow 2-subgroup of G is abelian.

Suppose that $U \subseteq Y < L$ and $P \subseteq \mathbf{N}_G(Y)$. We then have that PY is a group, so either $PY = G$ or $PY = P$ by the maximality of P. We cannot, however, have that $PY = G$ since $|PY| < |PL| = |G|$. So $PY = P$ and we have $Y \subseteq P$. Since L/U is a p'-group, we must have that $Y = U$ if Y is to be contained in P. In other words, nothing inside of L/U is P-invariant under the conjugation action of P on L/U except for the identity. To elaborate further, P is acting by conjugation on L/U since both L and U are normal

in G. If Y/U is a subgroup of L/U which is P-invariant, then P normalizes Y/U and therefore $P \subseteq \mathbf{N}_G(Y)$. Now choose a prime q dividing $|L/U|$ and choose a p-invariant Sylow q-subgroup of L/U, which can be done using the Sylow-E theorem with glasses. By our previous statements, we can conclude that this P-invariant subgroup is all of L/U since this Sylow subgroup is not trivial. Then $\mathbf{Z}(L/U) > 1$, P-invariant since it is characteristic in L/U, and so $\mathbf{Z}(L/U) = L/U$. This makes all of L/U abelian, as claimed. Thus a Sylow 2-subgroup of G is isomorphic to a Sylow 2-subgroup of L/U since $p \neq 2$, and hence a Sylow 2-subgroup i s abelian. By the normal J-theorem, $J \lhd G$ so $\mathbf{N}_G(J) = G$, but this is a contradiction since $\mathbf{N}_G(J)$ does have a normal p-complement.

□

This concludes the chapter on Thompson's work, although the final theorem we prove is along the same lines. We conclude with a proof of Burnside's $p^a q^b$ theorem.

40 05-06-10

Theorem 40.1. If $|G| = p^a q^b$ where p and q are prime, then G is solvable.

Proof. As always, assume that the theorem is false, and that $|G|$ is the smallest for a counter-example. Then if there exists $N \lhd G$ with $1 < N < G$, then by induction we have that N is solvable and G/N is solvable so G is solvable. We can thus assume that G is a simple group. We proceed in steps.

Step 1. Let $K \subseteq G$ with $K = K_p \times K_q$; i.e. take K to be nilpotent, where K_p and K_q are both non-trivial. Also assume that $\mathbf{N}_G(K) = M$ is maximal in G. Then M is the unique maximal subgroup of G containing K.

Suppose for contradiction that this is false, and let K be a maximal counter-example. Let $K \subseteq X$ where X is maximal in G. We want to show that $X = M$. Now $M = \mathbf{N}_G(K)$, but $\mathbf{N}_G(K_p)$ since K_p is characteristic in K which is normal in M, but K_p is not normal in G since G is simple and K_p is non-trivial. So $M \cap X = \mathbf{N}_X(K_p)$, so $M \cap X$ is p-local in X. So $\mathbf{O}_{p'}(M \cap X) \subseteq \mathbf{O}_{p'}(X)$; i.e. $\mathbf{O}_q(M \cap X) \subseteq \mathbf{O}_q(X)$ by Thompson's $P \times Q$ theorem and since $|G| = p^a q^b$. We claim that $K_q \subseteq \mathbf{O}_q(M \cap X)$. Since $K_q \subseteq M \cap X$ and K_q is a q-group and $K_q \lhd M$, we have that $K_q \subseteq \mathbf{O}_q(X)$. Similarly, we have that $K_p \subseteq \mathbf{O}_p(X)$. Let $L = \mathbf{F}(X)$. Then $L = L_p \times L_q \supseteq K_p \times K_q = K$. So $K \subseteq L$. Now $X = \mathbf{N}_G(L)$ since X is maximal in G and G is simple. Also, $L_q \subseteq \mathbf{C}_G(L_p) \subseteq \mathbf{C}_G(K_p) \subseteq \mathbf{N}_G(K_p) = M$. An analogous argument shows that $L_p \subseteq M$, so we have that $L \subseteq M$. So $K \subseteq L \subseteq (X \cap M)$. This makes L a counter-example, so $K \subseteq L$ but we cannot have that L is strictly larger than K, so we must have that $L = K$. But $X = \mathbf{N}_G(L) = \mathbf{N}_G(K) = M$, and we therefore do not have that K is a counter-example as X was taken to be arbitrary.

Step 2. Suppose $G = XY$ where $X, Y \subseteq G$ and $Y < G$. Then X normalizes no non-identity subgroup of Y.

Let $U \subseteq Y$ with $X \subseteq \mathbf{N}_G(U)$. We wish to show that U is trivial. Let $g \in G$, and write $g = xy$ for $x \in X$ and $y \in Y$. Then $U^g = U^{xy} = U^y \subseteq Y$ since $U \subseteq Y$ and $y \in Y$. Thus $U^g \subseteq Y < G$. But $U^G \lhd G$ and as we have shown $U^g \in Y$ for all $g \in G$, we have $U^G \lhd G$ and $U^G < G$. Since G is simple, we must have that $U^G = 1$, and since $U \subseteq U^G$, we conclude that U is trivial, as wanted.

Step 3. Let $M \subseteq G$ with $|G : M|$ a q-power. Then $\mathbf{O}_q(M) = 1$.

Since $\mathbf{O}_q(M)$ is a q-group, we have $\mathbf{O}_q(M) \subseteq Q \in \mathrm{Syl}_q(G)$ for some Q. By an order/index argument, we know that $QM = G$. But M normalizes $\mathbf{O}_q(M) \subseteq Q$, so we must have that $\mathbf{O}_q(M) = 1$ by step 2.

Note that maximal subgroups of G are solvable by the minimality of G, and are therefore p-solvable. In p-solvable groups, we know that either $\mathbf{O}_p$ or $\mathbf{O}_{p'}$ [in this case $\mathbf{O}_q$] is nontrivial. It is also possible with p-solvable groups for both subgroups to be non-trivial. Then next case shows us that in our case, we cannot have this last option.

The next two steps of this proof are very tricky, and in fact, are the crux of the argument.

Step 4. Let M be a maximal subgroup of G. Then either $\mathbf{O}_p(M)$ or $\mathbf{O}_q(M)$ is trivial.

Suppose again for contradiction that the statement is false. Let $Z_p = \mathbf{Z}(\mathbf{O}_p(M))$ and let $Z_q = \mathbf{Z}(\mathbf{O}_q(M))$. Note that since $\mathbf{O}_p(M)$ and $\mathbf{O}_q(M)$ are both assumed to be non-trivial, both Z_p and Z_q are non-trivial. write $Z = Z_p \times Z_q$. By simplicity, M is the normalizer of Z_p, Z_q, and Z since we know M is maximal and all of these subgroups are normal in M. By step 1, M is the unique maximal subgroup of G containing Z. Now $|G : M|$ is not a q-power by step 3, so let $S \in \mathrm{Syl}_p(M)$, so that $S < P$ for some $P \in \mathrm{Syl}_p(G)$. Since normalizers grow in p-groups, we know $\mathbf{N}_P(S) > S$, so there exists $g \in G$ such that $M^g \neq M$ but such that $S^g = S$. Now $Z_p \subseteq S = S^g \subseteq M^g$. We want to get $Z_q \subseteq M^g$ so that we can obtain a contradiction by having Z contained in two distinct maximal subgroups.

Look at $Z_p^g \subseteq S^g = S \subseteq M$. Now Z_q is normal in M, so Z_p^g acts on Z_q by conjugation. Temporarily write $A = Z_p^g$ to stress that this group is an *acting* group, so A is acting on Z_q. Suppose $a \in A$ with $a \neq 1$. Then $Z^g \subseteq \mathbf{C}_G(a)$ since Z^g is an abelian group containing a. Also, M^g is the unique maximal subgroup containing Z^g since Z^g is contained in M^g, Z^g is nilpotent, and M^g is maximal. Thus $\mathbf{C}_G(a) \subseteq M^g$ since $\mathbf{C}_G(a)$ must be contained in some maximal subgroup of G and $Z^g \subseteq \mathbf{C}_G(a)$. If A is not cyclic, then by on old lemma we have $Z_q = \langle \mathbf{C}_{Z_q}(a) | a \in A, a \neq 1 \rangle \subseteq M^g$. Also, we get the same result even if A IS cyclic if the action is not faithful. This shows us that $Z_q \subseteq M^g$ unless A is a cyclic group acting faithfully on Z_q. So unless A is cyclic and acts faithfully, we have Z_p, Z_q, and Z contained in both M and M^g with $M \neq M^g$, and this is our contradiction. Thus A can be assumed to be cyclic and to act faithfully

on Z_q. Yet $A = Z_p^g$ being cyclic implies that Z_p is cyclic, and interchanging the roles of the primes p and q [this is what Marty Isaacs called "by magic"] we also have that Z_q is cyclic. So A acts faithfully on a cyclic group, and we have that A is isomorphic to a subgroup of the automorphism group of Z_q, which has size $q^{a-1}(q-1)$ for some integer a. Since p does not divide q^{a-1}, we see that we must have p dividing $q-1$. However, if we again interchange the roles of p and q, we find that we must have q dividing $p-1$, and these two things cannot happen simultaneously. We have therefore reached the desired contradiction, and we have step 4.

Before beginning step 5, another tricky step, we introduce a bit of notation. If M is a maximal subgroup of G, we now know by step 4 that exactly one of $\mathbf{O}_p(M)$ or $\mathbf{O}_q(M)$ is non-trivial. We say that M is of *p-type* if $\mathbf{O}_p(M) > 1$ and similarly for q. Also, we say that an element $x \in G$ is *p-central* if $x \neq 1$ but $x \in \mathbf{Z}(P)$ for some $P \in \mathrm{Syl}_p(G)$. Again, a similar definition holds for q-central. Finally, if $V \subseteq G$ is a p-subgroup, let $V^* = \langle x \in V | x \text{ is } p\text{-central} \rangle$. Note that V^* can be trivial, and notice that $\mathbf{N}_G(V)$ normalizes V^* since conjugation simply permutes p-central elements.

Step 5. Let $y \in G$ be q-central and suppose that y normalizes some p-group V. Then V^* is trivial.

If this statement is false, let $W \subseteq G$ be a p-group normalized by y with $W = W^*$[i.e. we can take the W to be V^* if necessary since $(V^*)^* = V^*$] and where $|W|$ is maximal. In particular, W is definitely non-trivial. Let $N = \mathbf{N}_G(W)$. Now $y \in N$, so let $Q \in \mathrm{Syl}_q(G)$ with $y \in \mathbf{Z}(Q)$.

We claim that $NQ \neq G$. This holds because $\langle y \rangle \subseteq N$ and Q normalizes $\langle y \rangle$ since y is central in Q, and step two tells us that this cannot be the case if $G = NQ$. So $NQ \neq G$. Let $S \in \mathrm{Syl}_p(N)$. Again, we have that $S < R$ for $R \in \mathrm{Syl}_p(G)$ since $RQ = G$, so if $S = R$ then we would have $G = QS \subseteq NQ$, which is a contradiction. So a Sylow p-subgroup of N must be smaller than a Sylow subgroup of G. Again, we have that normalizers grow in p-groups so there exists $g \in G$ with $S^g = S$ but $g \notin N$, so that $W^g \neq W$. Note that $W \subseteq S$ since W is a p-group with $W \lhd N$ and thus N is contained in every Sylow p-subgroup of N.

As W is generated by p-centrals, there exists $x \in W$ which is p-central and such that $x^g \notin W$, or else we would have $W = W^g$. So $x^g \in W^g \subseteq S^g = S \subseteq N$. Also, x is p-central so there exists $P \in \mathrm{Syl}_p(G)$ with $x \in \mathbf{Z}(P)$. Also, $y \in \mathbf{Z}(Q)$ for $Q \in \mathrm{Syl}_q(G)$ and $PQ = G$. So write $g = ab$ for $a \in P$ and $b \in Q$. So $x^g = x^{ab} = x^b$ since $a \in P$ and x is central in P. Also, $x^b \in W^b$ as $x \in W$. Now $y \in \mathbf{N}_G(W)$ so $y^b \in \mathbf{N}_G(W^b)$. But $y^b = y$ since $b \in Q$ and y is central in Q. So $y \in \mathbf{N}_G(W^b)$. It follows that y normalizes $N \cap W^b$. now $W(N \cap W^b)$ is a group because $W \lhd N$ and $N \cap W^b \subseteq N$. In fact, $W(N \cap W^b)$ is a p-group since W and W^b are both p-groups. So in summary, we have:

- y normalizes W and $N \cap W^b$ so y normalizes anything uniquely determined by these groups; in particular, y normalizes $W(N \cap W^b)$.

- $(W(N \cap W^b))^* = W(N \cap W^b)$
- x and x^g are contained in the group $W(N \cap W^b)$ and x^g is NOT in W, so $W(N \cap W^b) > W$

This tells us that the group $W(N \cap W^b)$ is a strictly larger group with the properties we want, and this is a contradiction to the maximality of W, and step 5 holds.

Step 6. Let M be a maximal subgroup of G of p-type. Then M does not contain any q-central element.

Let $V = \mathbf{O}_p(M)$. We want to know that V^* is non-trivial. There exists $x \in G$ which is p-central with $x \in \mathbf{C}_G(V) \subseteq \mathbf{N}_G(V) = M$ by the Sylow-D theorem and the fact that p-groups have non-trivial centers. Also, M is solvable since $|M| < |G|$, and we know that $\mathbf{O}_q(M) = \mathbf{O}_{p'}(M) = 1$ by step 4. Thus $x \in \mathbf{C}_M(V)$ since $x \in M$ by Lemma 1.2.3; that is, we know $\mathbf{C}_M(V) \subseteq V$ and this makes $x \in V$. Yet V is not normalized by a q-central by step 5, so M cannot contain any q-central elements at all since all elements of M normalize V.

Step 7. Let $y \in \mathbf{N}_G(V)$ where y is q-central and V is a p-group. Then $V = 1$.

Suppose that $V > 1$ with this property. Then $\mathbf{N}_G(V) \subseteq M < G$ for some maximal subgroup M and $y \in M$. By step 6, this tells us that M must be of q-type. However, we also have that M contains a p-central element because V is a p-group, so V lives inside a full Sylow p-subgroup of G which has a non-trivial center, and any such element will certainly normalize V. This is our contradiction, so V must be trivial.

Step 8. $p, q \neq 2$

Suppose (say) that $q = 2$. Then let t be a q-central involution [an element of order two in the center of some Sylow subgroup]. Now $t \notin \mathbf{O}_2(G)$ since $\mathbf{O}_2(G) = 1$. SO there exists a subgroup or order p, say U, such that t acts on U by sending each element of U to its inverse. This puts $t \in \mathbf{N}_G(U)$, and this is a contradiction to step 7. Note also that this means that $p \neq 2$.

We now move on to the crux of the argument, step 9.

Step 9. Let M be a p-type maximal subgroup of G and let $S \in \mathrm{Syl}_p(M)$. Then $\mathbf{J}(S) \lhd M$ and $S \in \mathrm{Syl}_p(G)$.

Write $V = \mathbf{O}_p(M)$ where $V > 1$ since M is of p-type. Also, $V \subseteq S \subseteq P$ for some $P \in \mathrm{Syl}_p(G)$. Then $\mathbf{Z}(P)$ centralizes V so $\mathbf{Z}(P) \subseteq \mathbf{C}_G(V) \subseteq \mathbf{N}_G(V) = M$, so we know that the center of P is actually contained in M. This means that $\mathbf{Z}(P) \subseteq \mathbf{C}_M(V) \subseteq V$ by Lemma 1.2.3 since M has $\mathbf{O}_q(M) = 1$ by step 4 (i.e. M is of p-type). So $\mathbf{Z}(P) \subseteq \mathbf{Z}(S) \subseteq S$ and so $\mathbf{Z}(S)$ contains some p-central elements of G. To apply the normal J-theorem in M, we need $\mathbf{C}_M(\mathbf{Z}(S)) = S$. If this is not the case, then $\mathbf{C}_M(\mathbf{Z}(S)) > S$ and so there exists a q-central element of M, say $y \in \mathbf{C}_M(\mathbf{Z}(S))$, with $o(y) = q$. We therefore have $\mathbf{Z}(S)$ centralizing and

hence normalizing $\langle y \rangle$. A p-central element therefore normalizes $\langle y \rangle$, but this is a contradiction to step 8, giving us that $\mathbf{C}_M(\mathbf{Z}(S)) = S$. We can then get that $\mathbf{J}(S) \lhd M$ from the normal J-theorem. Thus $M = \mathbf{N}_G(\mathbf{J}(S))$. If $S < P$, then since normalizers grow in p-groups we would have $\mathbf{N}_P(S) > S$ and so S would contain elements NOT in M, making $\mathbf{N}_G(\mathbf{J}(S)) > M$, which is also a contradiction. Hence $S = P$, as claimed.

Step 10. We have a contradiction.

At long last, we break the symmetry of the primes p and q. Without loss, we know that $|G|_p > |G|_q$. If $S, T \in \mathrm{Syl}_p(G)$, then $|G| \geq |S||T|$ since G contains the set ST. But $|ST| = (|S||T|)/|S \cap T| > (|S||Q|)/|S \cap T| = |G|/|S \cap T|$, so this tells us that $|G| > |G|/|S \cap T|$ and therefore $|S \cap T| > 1$. Now it is a fact that there exists $S, T \in \mathrm{Syl}_p(G)$ with $S \neq T$ and such that $\mathbf{J}(S) \neq \mathbf{J}(T)$ since if this were not the case, we would have $\mathbf{J}(S) = \mathbf{J}(T)$ for all $S, T \in \mathrm{Syl}_p(G)$, making $\mathbf{J}(S) = \mathbf{J}(S^g) = \mathbf{J}(S)^g$ for all $g \in G$. This would make $\mathbf{J}(S) \lhd G$ with $1 < \mathbf{J}(S) < G$, and this is a contradiction. Knowing that such an S and T exist, choose $S, T \in \mathrm{Syl}_p(G)$ such that $\mathbf{J}(S) \neq \mathbf{J}(T)$ and so that $S \cap T$ is maximal with respect to containment (actually, with either definition of maximal). Let $D = S \cap T$. We know that $D > 1$ by our earlier remarks. Let M be a maximal subgroup of G which contains $\mathbf{N}_G(D)$. Then there exists a p-central element in M since $\mathbf{Z}(S) \subseteq \mathbf{N}_G(D) \subseteq M$ so we know that M is of p-type. Let $U \in \mathrm{Syl}_p(M)$ so that U contains $M \cap S > D$ since normalizers grow in p-groups. Choose $m \in M$ so that U^m contains $M \cap T > D$. By step 9, we know that both U and U^m are Sylow p-subgroups of G, so we know that $\mathbf{J}(S) = \mathbf{J}(U)$ since $S \cap U > D$ and $S, U \in \mathrm{Syl}_p(G)$. Also by step 9, we have that $\mathbf{J}(U) \lhd M$. But this makes $\mathbf{J}(U) = \mathbf{J}(U)^m = \mathbf{J}(T)$ since $U^m, T \in \mathrm{Syl}_p(G)$ with $U^m \cap T > D$. However, this gives us that $\mathbf{J}(S) = \mathbf{J}(U) = \mathbf{J}(T)$, and this is a contradiction. $\square$