Group Theory Notes

John L. Manferdelli

These notes started in Berkeley in 1977.
They are clearly not written for third parties (second parties either)
and may be incomplete, inaccurate or even incoherent.
However, you are welcome to use them at your own risk.
I disclaim any and all liability for inaccuracy, infringement of any kind, or anything else.

Please send corrections to:
JohnManferdelli@hotmail.com, jlmucbmath@gmail.com,

Last modified: 26 September 2024 13:54

Chapter 1

Basic Definitions

1.1 Notation, commutator calculus, characteristic subgroups

Definition 1: $Core_G(H) = \bigcap_{g\in G} H^g$ (Can use this to show $|G : Core_G(H)| \leq |G : H|$!). $O^{\mathcal{A}}(G) = \bigcap_{A\lhd G, G/A\in\mathcal{A}} A$. $O_{\mathcal{A}}(G) = \prod_{A\lhd G, A\in\mathcal{A}} A$.

Definition 2: Let $\mathcal{M}_G = \{M : M$ is a non-trivial minimal normal subgroup of $G\}$; the *socle of* G, denoted $soc(G)$, is defined by $soc(G) = \langle M\rangle_{M\in\mathcal{M}}$. $O_\pi(G) =$ maximal normal $\pi-$subgroup of G. $O^\pi(G) =$ smallest normal subgroup of G such that $G/O^\pi(G)$ is a π-group. G is $p-$closed if $O_p(G) \in S_p(G)$.

Definition 3: A homomorphism $\varphi : G \to X$ is *faithful* if it is injective.

Definition 4: $\mathcal{SCN}(P) =$ set of self centralizing normal subgroups of P. $\mathcal{SCN}(p) = \mathcal{SCN}(P)$ where $P \in \mathcal{SCN}(P)$.

Definition 4.5: If $\pi = \{p_1, p_2, \ldots, p_k\}$ is a set of primes, we say G is a π group if the only primes dividing $|G|$ are in π. If G is a finite group and $H \leq G$, we say H is an S_π group if H is a π group and $p \nmid |G : H|$ if $p \in \pi$. $S_\pi(G)$ is the set of all S_π subgroups of G. For $\pi = \{p\}$, we call an S_π group and S_p group and put $S_\pi(G) = S_p(G)$. $S_p(G)$ is just the sylow subgroups of G.

Definition 5: $\mathcal{N}_G(A, \pi) =$ set of all $A-$invariant π subgroups of G. $\mathcal{N}^*_G(A, \pi) =$ maximal subgroups in $\mathcal{N}_G(A, \pi)$. For a $p-$group, P, $\Omega_n(P) = \langle x \in P : x^{p^n} = 1\rangle$ and $\mho_n(P) = \langle x^{p^n} : x \in P\rangle$.

Definition 6: Let $H \subseteq G$ and let S be an H-invariant subset of G; H is said to control fusion in S if for $s \in S$, $s^G \cap S = s^H$. Let $X \leq H \leq G$. X is *weakly closed* in H with respect to G if $X^g \cap H = \{X\}$.

Definition 7: G is *p-constrained* if $P \in S_p(O_{p',p}(G))$ implies $C_G(P) \subseteq O_{p',p}(G)$. Equivalently, if $O_{p'}(G) = 1$ then $C_G(O_p(G)) \subseteq O_p(G)$ and $F(G) = O_p(G)$..

Definition 8: Z is *weakly closed* in P with respect to G if $Z^g \subseteq P \to Z^G = Z$. The *weak closure* of Z in P with respect to G is $wcl_G(Z, P) = \langle Z^g, Z^g \subseteq P\rangle$.

Definition 9: G is *p-stable* if $p \neq 2$ and if $A \in p(N(P))$ with $[P, A, A] = 1$ implies $AC(P)/C(P) \subseteq O_p(N(P)/C(P))$.

Definition 10: $m_p(P)$ is the rank of the largest elementary abelian p-group in P.

Definition 11: $O_\infty(G)$ = largest solvable normal subgroup of G.

Definition 12: $F(G)$, the *Fitting subgroup of* G is the unique maximal, normal, nilpotent subgroup of G and $F(G) = \prod_p O_p(G)$.

Definition 13: (a) If $P \leq H \leq G$, H *controls fusion* in P with respect to G if $\forall x, y \in P : x^g = y, g \in G$, $\exists h \in H : x^h = y$. (b) $A^\pi(G)$ is the unique smallest normal subgroup of G such that $G/A^\pi(G)$ is an abelian π-group. If $P \subseteq H \subseteq G$ then $|G : A^p(G)| \leq |H : A^p(H)|$ if equality holds we say H *controls p-transfer in* G.

Definition 14: G is π-*solvable* if there is a normal series whose factors consist of either π'-groups or a solvable π-groups.

Definition 15: (a) $O_{\mathcal{K}}(G) = \bigcap_{A \lhd G, A \in \mathcal{K}} A$, (b) $O^{\mathcal{K}}(G) = \bigcap_{A \lhd G, G/A \in \mathcal{K}} A$. (c) G is π-*closed* if $G/O_\pi(G)$ is a π' group. (d) G is π-separable iff $O_\pi(G) = O^{\pi'}(G)$.

Definition 16: E_{p^n} denotes the elementary abelian $p-$group of rank n. $m_{2,p}(G) = max\{m_p(H)\}$, where H is 2-local. $e(G) = max\{m_{2,p}(G), p \neq 2\}$ ($e(G)$ is a good approximation of the Lie rank.).

Definition 17: The group A/B is called a section of G if $B \lhd A < G$.

Definition 18: G is π-separable if there are characteristic subgroups $A_0, A_1, \ldots, A_n$: $1 = A_0 < A_1 < \ldots < A_n = G$ such that A_i/A_{i-1} is either a π group or a π' group.

Definition 19: G is p-closed if $O_p(G) = O^{p'}(G)$.

Definition 20: $O_{p'}(G)$ is called the p-*core* of G. $O_{2'}(G)$ is often called the *core* of G and is sometimes denoted by $O(G)$.

Definition 21: G is *metacyclic* if $\exists H \lhd G : G/H, H$ are cyclic.

Notation: Let G be a finite group, $x, y \in G$, $U, V \subseteq G$, $A \subseteq Aut(G)$.

1. $\langle U \rangle$ denotes the smallest subgroup of G containing U.
2. $x^g = g^{-1}xg$.
3. $[x, g] = x^{-1}g^{-1}xg$.
4. $U^g = \{u^g : u \in U\}$
5. $\overline{U} = U/N$.

Theorem 1: $[x, y^{-1}, z][y, z^{-1}, x][z, x^{-1}, y] = 1$ (*Jacobi Identity*). $[ab, c] = [a, c]^b[b, c]$ and $[a, bc] = [a, c][a, b]^c$.

Proof: Straightforward calculations.

Three Subgroups: $A, B, C \subseteq G$ and $N \lhd G$ with $[A, B, C] \subseteq N$ and $[B, C, A] \subseteq N$ then $[C, A, B] \subseteq N$.

Dedekind's Lemma: If $G = HK$ and $H \subseteq G_0$ then $G_0 = H(G_0 \cap K)$.

Proof: $g_0 = hk$ so $g_0 h^{-1} \in G_0 \cap K$ (since $h \in G_0$).

Theorem 2: If $x, y \in G$, $z = [x, y]$, $[z, x] = 1 = [z, y]$ then (1) $[x^n, y^m] = z^{mn}$ and (2) $(yx)^n = z^{(n(n-1))/2} y^n x^n$.

Proof of 1: Claim: Under the conditions of the theorem, $[x^n, y] = z^n$. Proof by induction. It is true for $n = 1$. $[x^{n+1}, y] = x^{-(n+1)} y^{-1} x^{n+1} y = x^{-n} x^{-1} y^{-1} x x^n y$. So $[x^{n+1}, y] = x^{-1} x^{-n} y^{-1} x^n y y^{-1} x y = x^{-1} z^n y^{-1} x y = z^{n+1}$. Proof of theorem is by induction on m. It is true for $m = 1$, by the claim. Now, $[x^n, y^{m+1}] = (x^{-n} y^{-1} x^n y) y^{-1} x^{-n} y^{-m} x^n y^m y = z^n y^{-1} (z^{mn}) y$; so $[x^n, y^{m+1}] = z^n y^{-1} (z^{mn}) y = z^n z^{mn} = z^{n(m+1)}$ which proves the result.

Proof of 2: Again, the proof is by induction on n; it is true for $n = 1$. $(yx)^{n+1} = (yx)^n (yx) = z^{\frac{n(n-1)}{2}} y^n x^n y x = y^{n+1} x^n (x^{-n} y^{-1} x^n y) x = z^{\frac{n(n-1)}{2}} y^{n+1} x^n z^n x = z^{\frac{n(n+1)}{2}} y^{n+1} x^{n+1}$.

Theorem 3: If H *char* K and K *char* G then H *char* G.

Theorem 4: If $H, K < G$, $[H, K] \lhd \langle H, K \rangle$. If $H, K, L \lhd G$ then $[HK, L] = [H, L][K, L]$. $[xy, z] = [x, z][x, z, y][y, z]$. $[x, yz] = [x, z][x, y][x, y, z]$.

Proof: Straightforward.

Theorem 5: If A is a cyclic group of maximal order in an abelian group G, then A is a direct factor of G.

Proof: By induction on $|G|$. G must possess a non-cyclic abelian S_p group for some p. $\exists H : pH = 1, H \cap A = \{1\}$, set $\overline{G} = G/H$. If $|\overline{A}| = |A|$, the result follows by induction so $\overline{G} = \overline{AB}$, $\overline{A} \cap \overline{B} = \{1\}$. Let A and B be the inverse images under the homomorphism. $A \cap B \subseteq H$ but by construction, $H \cap A = \{1\}$ and the result follows.

Theorem 6: If $H \lhd G$ and $(|G : H|, |H|) = 1$ then H *char* G.

Proof: Let ϕ be an automorphism that does not fix H and put $H' = \phi(H)$. HH' is a subgroup of G and $|HH'| > |H|$. $\frac{(HH')}{H} \cong \frac{H'}{H \cap H'}$. Put $k = |HH'|, m = |G : H|, n = |H|, d = |H \cap H'|$, then $1 < k' = \frac{k}{n} = \frac{n}{d}$ and $k' \mid n$. So $dk' = n$ and $(k', d) = 1$, thus $d = 1, H = H'$ and the result follows.

Theorem 7: Let H be an elementary abelian p-group of G and $x \in N_G(H)$ and let ϕ_x be the linear transformation induced by x on H then the minimal polynomial of ϕ_x is $(x - 1)^r$, where $[h, x, \ldots, x] = 1$ and x appears r times.

Proof: Straightforward calculation.

Theorem 8: If G has no non-trivial characteristic subgroups then $G = \bigoplus_{i=1}^{n} H_i$, where $H_1 \cong H_i, \forall i$, and H_i is simple.

Proof: Let H_1 be a minimal normal sugroup of G. If $H_1 = G$, we're done. Now let $H \leq G$ be maximal subject to (a) $H = H_1 H_2 \ldots H_n$, (b) $H_1 \cong H_i$, (c) $H_i \lhd G$ and (d) $H = H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n \cap H_i = 1$. Claim: $H = G$. Observe $1 \neq H$ *char* G; if $\phi \in Aut(G)$, $H_i^\phi \lhd G$. So $H_i^\phi \cap H \lhd G$. If $H_i^\phi \cap H = 1$, H is not maximal and if $H_i^\phi \cap H 1 \geq$, H_1 is not minimal. Thus $H^\phi = H$, H *char* G, so $G = H$.

Corrollary: If G is solvable and $H \leq G$ is characteristically simple, H is an elementary abelian p-group.

Note: This means $O_p(G) \neq 1$ for any solvable group G for some $p \in \pi(G)$.

Definition 23: A group, A acts on a set, Ω, if $\forall x \in \Omega$ and $\forall a \in A$, $x^a \in \Omega$, $x^e = x$, $x^{(a_1 a_2)} = (x^{a_1})^{a_2}$. If, in addition, $\Omega = G$ is a group and $g_1, g_2 \in G$, then $(g_1 g_2)^a = g_1^a g_2^a$.

Lagrange's Theorem: If H is a subgroup of G, $H \leq G$, then $|H| \mid |G|$.

Proof: Cosets of H in G are either dijoint or identical. So G is a disjoint union of sets of order $|H|$.

Chapter 2

Isomorphism Theorems and Series

2.1 Isomorphism Theorems:

Isomorphism Theorem: (1) If $\varphi : G \to H$ is a homomorphism, $G/ker(\varphi) \cong Im(\varphi)$, (2) If $G \triangleright H$ and $G \triangleright N$ and $N \subseteq H \subseteq G$ then $G/H \cong (G/N)/(H/N)$, (3) If $G = HN$, $G \triangleright N$ then $HN/N \cong H/(H \cap N)$.

Proof of 1: Let $N = ker(\phi)$ and define $\psi(Nx) = \phi(x)$. ψ is well defined since $Nx = Ny \to y = nx$ and $\phi(y) = \phi(nx) = \phi(n)\phi(x) = \phi(x)$ and is a homomorphism since ϕ is. If $\psi(Nx) = \psi(Ny)$ then $\phi(xy^{-1}) \in N$ so $Nx = Ny$ and ψ is 1-1. The image of ψ is $Im(\phi)$. So ψ is an isomorphism.

Proof of 2: Define $\psi(Kx) = Hx$. ψ is well defined and is a homomorphism. $ker(\psi) = Kh, h \in H$ so $(G/K)/(H/K) \cong G/H$ by the previous result.

Proof of 3: Define $\psi(Nh) = (H \cap N)h$. ψ is well defined and is a homomorphism. $ker(\psi) = \{h \in H : h \in H \cap N\}$ so $HN/N \cong H/(H \cap N)$ by (1).

Definition 1: A *derived series* is a sequence $G^{[0]} = G$, $G^{[i+1]} = [G^{[i]}, G^{[i]}]$. G is *solvable* iff derived series terminates at 1.

Definition 2: The sequence of homomorphisms $A \to_\alpha B \to_\beta C$ is *exact* if $im(\alpha) = ker(\beta)$. The sequence $1 \to N \to_{id} G \to_\varphi H \to_\epsilon 1$ is a *short exact sequence* if the map id is inclusion and ϵ is the trivial homomorphism and each subsequence is exact; in this case, $G/N \approx H$ by the above.

Definition 3: A *subnormal series* is a sequence of groups G_i such that $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_k = H$, if this happens, we say $G \triangleright \triangleright H$.

Definition 4: A *normal series* is a subnormal series where $G \triangleright G_i, \forall i$.

Definition 5: A *chief series* is a normal series with no repeated terms and no normal subgroup properly lying between two series elements.

Definition 6: A *composition series* is a subnormal series terminating at 1 in which G_i/G_{i-1} is simple.

Lemma 1: If $K \triangleleft H < G$ and $N \triangleleft G$ then $NK \triangleleft NH$.

Proof: Suppose $a, b \in N, h \in H, k \in K$. $[ak, bh] = k^{-1}a^{-1}h^{-1}b^{-1}akbh = k^{-1}a^{-1}(h^{-1}b^{-1}ah)(h^{-1}kh)(h^{-1}bh) \in KNNKN = NK$. So $[NK, NH] \subseteq NK$ and $NK \lhd NH$.

Lemma 2: $A(A^* \cap B) \cap A^* \cap B^* = B(B^* \cap A) \cap A^* \cap B^*$.

Proof: It suffices to show $A(A^* \cap B) \cap B^* = B(B^* \cap A) \cap A^*$. Suppose $x = at \in A(A^* \cap B) \cap B^*, a \in A, t \in (A^* \cap B) \subseteq B^*$. $x = t(t^{-1}at) \in BA \cap B^*$; since $x \in B^*, t^{-1}x \in B^*$ and $t^{-1}at \in B^* \cap A$. Thus $A(A^* \cap B) \cap B^* \subseteq B(B^* \cap A) \cap A^*$. Symmetrically, $A(A^* \cap B) \cap B^* \supseteq B(B^* \cap A) \cap A^*$.

Zassenhaus Butterfly Lemma: If $A \lhd A^*$ and $B \lhd B^*$ then $A(A^* \cap B) \lhd A(A^* \cap B^*)$ and $B(B^* \cap A) \lhd B(B^* \cap A^*)$; further, $\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}$.

Proof: Apply lemma 1 with $N = A$, $K = A^* \cap B$, $H = A^* \cap B^*$, $G = A^*$ to get $A(A^* \cap B) \lhd A(A^* \cap B^*)$. Symmetrically, $B(B^* \cap A) \lhd B(A^* \cap B^*)$. Set $K_1 = A(A^* \cap B)$ and $K_2 = B(B^* \cap A)$. Let $t_1 \in \frac{A(A^* \cap B^*)}{A(A^* \cap B)}, t_2 \in \frac{B(A^* \cap B^*)}{B(B^* \cap A)}$, $t_1 = ayK_1, t_2 = bzK_2$ where $a \in A, b \in B, y, z \in (A^* \cap B^*)$. $ay = y(y^{-1}ay) = ya'$ so $t_1 = yK_1$. Similarly, $t_2 = zK_2$. Define $h : \frac{A(A^* \cap B^*)}{A(A^* \cap B)} \to \frac{B(B^* \cap A^*)}{B(B^* \cap A)}$ by $h(yK_1) = yK_2$. The map is well defined since $yK_1 = zK_1$ iff $z^{-1}y \in A(A^* \cap B^*) \cap A^* \cap B^*$ iff $z^{-1}y \in B(A^* \cap B^*) \cap A^* \cap B^*$ by lemma 2.

Theorem 1: Let G be a finite group. The following are equivalent: (1) G is solvable, (2) G has a normal series terminating at the identity whose factor groups are abelian, (3) G has a subnormal series with cyclic quotients.

Proof: $1 \to 2 \to 3$ is trivial. Suppose $S : 1 = G_r \lhd G_{r-1} \lhd \ldots \lhd G_1 \lhd G_0 = G$ has abelian factors. Claim: $G^{(j)} \leq G_j$. Note that $G' \subseteq G_1$ since G/G_1 is abelian. The claim follows from by an easy induction.

Definition: Two normal series, $G_0 \geq G_1 \geq G_2 \geq \ldots \geq G_n$ and $H_0 \geq H_1 \geq H_2 \geq \ldots \geq H_m$, are *equivalent* if $m = n$ and $G_i/G_{i+1} \cong H_{\pi(i)}/H_{\pi(i)+1}$ for some permutation, π.

Schreier's Theorem: Two normal series for G have equivalent refinements. Two compositions series for G are equivalent.

Proof: By induction on length (l) of shortest such series. If $l = 1$, G is simple. Suppose $G = G_0 \geq G_1 \geq \ldots \geq G_r = 1$ and $H = H_0 \geq H_1 \geq \ldots \geq H_t = 1$ and assume $l = r > t$ and that the theorem is true for all series of length less than l. If $H_1 = G_1$ then we are done by induction on the shortened series. Assume $G_1 \neq H_1$, $H_1 \lhd G, G_1 \lhd G$ then $G_1H_1 = G$ and $G/G_1 \cong H_1/K, K = G_1 \cap H_1$. Consider the two series $G_1 \geq G_2 \ldots \geq G_r = 1$ and $G_1 \geq K \geq K_1 \ldots \geq K_t = 1$. By induction, $r-1 = t+1$ and they are equivalent. Thus, $H_1 \geq H_2 \ldots \geq H_s = 1$ and $H_1 \geq K \geq K_1 \ldots \geq K_{r-2} = 1$ so $r = s$ and they are equivalent.

Jordan-Holder Theorem: If G has a composition series, S, then any subnormal series S^* can be refined to a composition series and any two composition series are equivalent.

Proof: S and S^* have equivalent refinements by Schreier. Remove any repetitions to produce new equivalent refinements. Since a composition series does not have proper refinements, the series are equivalent.

Butterfly Lemma: If $U, V \subseteq G$, $u \lhd U$, and $v \lhd V$ then $u(U \cap v) \lhd u(U \cap V)$, $(u \cap V)v \lhd (U \cap V)v$ and $u(U \cap V)/u(U \cap v) \cong (U \cap V)v/(u \cap V)v$.

Proof: Let $H = (U \cap V)$ [resp. $(U \cap V)v$] and $N = u(U \cap v)$ [resp. $(u \cap V)v$]. We show $N \lhd HN$. Let $x = a_1b_1 \in HN$ and $y = a_2b_2 \in N$, $a_1, a_2 \in u, b_1 \in (U \cap V), b_2 \in (U \cap v)$. $x^{-1}yx = b_1^{-1}a_1^{-1}a_2b_2a_1b_1 = b_1^{-1}a_1^{-1}a_2b_1b_1^{-1}b_2b_1b_1^{-1}a_1b_1 = a_3b_3a_4b_3^{-1}a_1b_3 = a_3b_3a_4$, $a_3, a_4 \in u, b_3 \in (U \cap v)$. So $x^{-1}yx == a_3b_3a_4b_3^{-1}b_3$. Thus $x^{-1}yx \in u(U \cap v)$ and $N \lhd H$. $HN = (U \cap V)u(U \cap v) = u(U \cap V)$. $u(U \cap V)/u(U \cap v) = HN/N \cong H/(H \cap N) = (U \cap V)/(U \cap V \cap u(U \cap v)$. Now we show, $U \cap V \cap u(U \cap v) = (U \cap v)(V \cap u)$. Let $a_1b_1 \in u(U \cap v), a_1 \in u, b_1 \in (U \cap v)$. If $a_1b_1 \in V$, $a_1 \in V$ (since $b_1 \in v \subseteq V$), thus $a_1 \in (u \cap V)$ and $a_1b_2 \in (u \cap V)(U \cap v)$. We've shown, $u(U \cap V)/u(U \cap v) \cong (U \cap V)/(u \cap V)(U \cap v)$. A symmetric aargument shows $(U \cap V)v/(u \cap V)v \cong (U \cap V)/(u \cap V)(U \cap v)$. So $u(U \cap V)/u(U \cap v) \cong (U \cap V)v/(u \cap V)v$, which is what we wanted.

Another proof of Schrier: Let $1 \lhd G_r \lhd \ldots \lhd G_1 = G$ and $1 \lhd H_s \lhd \ldots \lhd H_1 = H$ be normal towers, they have equivalent refinements.

Proof: Put $G_{ij} = G_{i+1}(H_j \cap G_i)$ and $H_{ji} = H_{j+1}(G_i \cap H_j)$. Use the butterfly to show $G_{ij}/G_{i,j+1} \cong H_{ji}/H_{j,i+1}$.

2.2 Indecomposible Groups and Krull Schmidt

Definition 7: ϕ is a *normal endomorphism* iff $\phi(a^{-1}xa) = a^{-1}\phi(x)a$, $\forall x, a \in G$. A group, G, is *indecomposible*, if $G \neq 1$, and if $G = H \times K$ then either $H = 1$ or $K = 1$.

Lemma 1: If ϕ and ψ are normal endomorphisms of a group G then so is their composition and so is ϕ^{-1}.. If ϕ is a normal endomorphism of G and if $H \lhd G$ then $\phi(H) \lhd G$.

Proof: Routine.

Lemma 2: Let $G = H_1 \times \ldots \times H_m$ have projections $\pi_i : G \to H_i$ and inclusions $\lambda_j : H_i \to G$ then the sum of any k distinct $\lambda_i\pi_i$ is a normal endomorphism of G.

Proof: Routine.

Lemma 3: If $H \lhd G$ and both H and G/H have both chain conditions then G has both chain conditions. If $G = H \times K$ and G has both chain conditions then so do H and K.

Proof: If $G_1 \geq G_2 \geq \ldots$ is a chain of normal subgroups of G then $H \cap G_1 \geq H \cap G_2 \geq \ldots$ is a chain of normal subgroups of H and $HG_1/H \geq HG_2/H \geq \ldots$ is a chain of normal subgroups of G/H. $\exists t, s : H \cap G_t = H \cap G_{t+1} = \ldots$ $HG_s/H = HG_{t+1}/H = \ldots$; let $l = max(t, s)$. $G_l = G_{l+1} = \ldots$ so G has ACC. A similar argument holds for DCC.

If $G = H \times K$ then every normal subgroup of H is a normal subgroup of G and every chain of normal subgroups of H is a chain of normal subgroups of G.

Theorem 2: If G satisfies ACC or DCC then G is the direct product of indecomposable groups.

Proof: Call G "good" if it satisfies the conclusion of the theorem. If G is indecomposible, G is good and if A and B are good so is $A \times B$. So if $G = U \times V$ is bad either U is bad or V is bad. Supposed G is bad. Define $H_0 = G$ and by induction, $\exists H_1, H_2, \ldots, H_n$ with H_i a bad proper factor of H_{i+1}. so, $G = H_0 > H_1 > \ldots$. If G has DCC, this must terminate at a bad indecomposible group which is a contradiction.

Lemma 3: If G satisfies ACC (resp. DCC) on normal subgroups and f is a normal endomorphism of G, then f is an injection iff f is an surjection.

Proof: Suppose ϕ is an injection and $g \in \phi(G)$. We prove by induction that $\phi^n(g) \notin \phi^{n+1}(G)$. If not, $\exists h \in G : \phi^n(g) = \phi^{n+1}(h)$ so $\phi(\phi^{n-1}(g)) = \phi(\phi^n(h))$. Since ϕ is injective, $\phi^{n-1}(g) = \phi^n(h)$ which contradicts the inductive hypothesis. Thus $\exists$ a chain $G > \phi(G) > \phi^2(G) > \ldots$. ϕ is normal so ϕ^n is normal and by a previous lemma $\phi^n(G) \lhd G, \forall n$. This violates the DCC condition.

Now assume ϕ is surjective. Define $K_n = ker(\phi^n(G))$ with each $K_n \lhd G$. $1 = K_0 \leq K_1 \leq \ldots$. This chain stops because of ACC. Let t be the smallest integer such that $K_t = K_{t+1} = \ldots$. We claim $t = 0$. If $t \geq 1$ then $\exists x \in K_t$ with $x \notin K_{t-1}$ so $\phi^t(x) \neq 1$ but $\phi^{t+1}(x) = 1$. Since ϕ is a surjection, $\exists g \in G$ with $x = \phi(g)$. Hence $1 = \phi^t(x) = \phi^{t+1}(g)$ so $g \in K_{t+1} = K_t$ and thus $a = \phi(g) = \phi^{t-1}(g)(\phi(g)) = \phi^{t-1}(g)$ which is a contradiction so ϕ is injective.

Definition 8: An endomorphism ϕ of G is nilpotent if $\exists k > 0 : \phi^j = 0$; note $0 : g \mapsto 1$.

Fitting Lemma: Let G satisfy both chain conditions. If ϕ is a normal endomorphism of G with $\phi(H) = H$ and $\phi(K) = K$ then $G = H \times K$ and $\phi_{|K}$ is nilpotent and $\phi_{|H}$ is surjective.

Proof: Let $K_n = ker(\phi^n(G))$ and $H_n = im(\phi^n(G))$. $G \geq H_1 \geq \ldots$ and $1 \leq K_1 \geq \ldots$. Suppose H_i stops at t and K_i stops at s, $l = max(r, s)$. Let $x \in H \cap K$. Since $x \in H, \exists g \in G$ with $x = \phi^l(g)$. $\phi^l(x) = 1$ so $\phi^{2l}(g) = 1$ and $g \in K_{2l} = K_l$. $x \in \phi^l(g) = 1$ and so $H \cap K = 1$. If $g \in G$ then $\phi^l(g) \in H_l = H_{2l}$ so $\exists y \in G : \phi^l(g) = \phi^{2l}(y) = 1$ and $\phi^l(g\phi^l(y^{-1})) = 1$ so $g\phi^l(y^{-1}) \in K_l = K_{2l}$ so $g = (g\phi^l(y^{-1}))\phi^l(y) \in KH$ and $G = K \times H$. Now, $\phi(H) = \phi(H_l) = \phi(\phi^l(G)) = \phi^{l+1}(G) = H_{l+1} = H_j = H$ so ϕ is surjective. Finally, if $x \in K$ then $\phi^l(x) \in K \cap H = 1$ and so $\phi_{|K}$ is nilpotent.

Theorem 3: If G is an indecomposable group satisfying ACC and DCC on normal subgroups and if f is a normal endomorphism then f is nilpotent or an automorphism.

Proof: By Fitting Lemma, $G = K \times H$ with $\phi_{|K}$ and $\phi_{|H}$ surjective. Since G is indecomposible, then either $G = H$ or $G = K$. In the first case, ϕ is nilpotent. In the second case, ϕ is surjective and so by the previous Lemma, ϕ is an automorphism.

Lemma: Let G be an indecomposible group with both chain conditions and suppose ϕ, ψ are two normal, nilpotent endomorphisms of G. If $\phi + \psi$ is an endomorphism of G then it is nilpotent.

Proof: By the previous result, $\phi + \psi$ is either an automorphism or nilpotent. If it is an automorphism, there is an inverse, γ, normal. For each $x \in G$, $x = (\phi + \psi)\gamma(x)) = \phi(\gamma(x)) + (\psi(\gamma(x))$. If $\lambda = \phi\gamma$ and $\mu = \psi\lambda$, $1_G = \lambda + \mu$. In particular, $x = \lambda(x)\mu(x)$ and so $\lambda + \mu = \mu + \lambda \to \lambda\mu = \mu\lambda$. $End(G)$ is generated by μ, λ and $(\lambda + \mu)^m = \sum \binom{m}{i} \phi^i \psi^{m-i}$. Since both ϕ and ψ are nilpotent so are λ and μ and they are not automorphisms. So, $\exists r, s : \lambda^r = \mu^s = 0$. If $m = r + s - 1$ then either $i \geq r$ or $m - i \geq s$ so $1_G^m = 0$ and $G = 1$.

Corollary: Let G be an indecomposible group having both chain conditions. If $\varphi_1, \ldots, \varphi_n$ is a set of normal, nilpotent endomorphisms of G such that every sum of distinct φ's is an endomorphism, then $\varphi_1 + \ldots + \varphi_n$ is nilpotent.

Proof: By induction on n.

Krull-Schmidt Theorem: If G has both chain conditions on normal subgroups and $G = G_1 \times \ldots \times G_s = H_1 \times \ldots \times H_t$ are two decompositions into indecomposable factors then $s = t$ and, after reindexing, $H_i \cong G_i$ and for each $r < t$, $G = G_1 \times G_2 \times \ldots \times G_r \times H_{r+1} \times H_t$.

Proof: Let $P(0)$ be the statement $G = G_1 \times G_2 \times \ldots \times G_s$ and for $1 \leq r \leq min(s,t)$ let $P(r)$ be the statement $G = G_1 \times G_2 \times \ldots \times G_r \times H_{r+1} \times \ldots H_t$. $P(0)$ is true by assumption. Assume $P(r-1)$. Let π_i (resp π_i') be the canonical epimorphisms from $G_1 \times G_2 \times \ldots \times G_s$ (resp. $G_1 \times G_2 \times \ldots \times G_r \times H_{r+1} \times H_t$) and λ_i (resp λ_i') be the inclusion maps, $\varphi_i = \lambda_i \pi_i$ and $\phi_i = \lambda_i' \pi_i'$. $\varphi_r \phi_i = 0_{|G}$ for $i < r$ and $\varphi_1(1_{|G}) = \varphi_r\phi_1 + \ldots + \varphi_r\phi_t = \varphi_r\phi_r + \ldots + \varphi_r\phi_t$ so $(\varphi_r\phi_j)_{|G}$ is an automorphism of G_r. $\varphi_j\phi_r$ must be an automorphism of H_j and $\phi_j : G_r \to H_j$ is and isomorphism and so is $\varphi_r : H_j \to G_r$ reindexing we have the first half of $P(r)$. Let $g = g_1 g_2 \ldots g_{r-1} h_r h_{r+1} \ldots h_t$ define $\theta(g) = g_1 g_2 \ldots g_{r-1} \varphi(h_r) h_{r+1} \ldots h_t$. $G = Im(\theta) = G^* = G_1 \times G_2 \times \ldots \times G_r \times H_{r+1} \times H_t$ which completes the argument.

2.3 Inner Automorphisms

Definitions 9: G is *complete* if it is centerless and every automorphism is inner in which case $G \cong Aut(G)$.

Theorem 4: S_n is complete if $n \neq 2, 3$.

Proof: Let T_k be the set of k disjoint transpostions so $x \in T_k \to x^2 = 1$; note that if $\theta \in Aut(S_n), \theta(T_1) = T_k$ for some k. Also observe that θ preserves transpositions iff $\theta \in Inn(S_n)$. Now we can show $|T_1| = \frac{n(n-1)}{2}$ and $|T_k| = \frac{(n-2k+1)!}{(n-2k)!k!2^k}$. Comparing the two $|T_1| = |T_k|$ is possible only if $k = 2, 3$ and in fact, only if $k = 3$. If $\theta \in Out(S_6)$ and τ is a transposition, $\theta(\tau)$ must be a product of three transpositions and such an automorphism exists.

Theorem 5: If G is a non-abelian simple group, then $Aut(G)$ is complete. If $K \lhd G$ and K is complete, $G = K \times Q$. $Hol(K) \subset S_K$ is $\langle K^l, Aut(K) \rangle$, $K^l \lhd Hol(K)$, $Hol(K)/K^l \cong Aut(K)$ and $C_{Hol(K)}(K^l) = K^r$. If K is a direct factor whenever K is a normal subgroup then K is complete.

Proof: See, Scott.

Chapter 3

Counting and Sylow's Theorem

3.1 Basic Results

Theorem 1: If $X, Y \leq G$, XY is a group iff $XY = YX$.

Proof: Associativity and identity are inherited from G. If $x_1, x_2 \in X$ and $y_1, y_2 \in Y$, $x_1y_1x_2y_2 = x_1x_2'y_1'y_2$ by the equality so XY is closed. Further, $(x_1y_1)^{-1} = (y_1)^{-1}x_1^{-1} = (y_1'x_1')^{-1} \in XY$ so every element in XY has an inverse.

Theorem 2: If $exp(G) = 2$, G is abelian.

Proof: $(xy)^2 = xyxy = 1$ so $x^2yxy = yxy = x$ and $yxy^2 = yx = xy$ so G is abelian.

3.2 Counting

Lagrange's Theorem: If $G > H$ $G = \bigcup Hx_i$ for some $x_i \in G$ and each pair of cosets is disjoint.

Proof: $G = \bigcup_{x \in G} Hx$ since $x \in Hx$. Since any two cosets coincide or are disjoint, this partition can be refined to disjoint sets all of size $|H|$. Thus $|H| \mid |G|$.

Group Actions: A *group action* is a map $\phi : \Omega \times G \to \Omega$ satisfying $\phi(\alpha, 1) = \alpha$, $\phi(\alpha, g_1g_2) = \phi(\phi(\alpha, g_1), g_2)$.

Counting Theorem: $|\alpha^G| = |G : G_\alpha|$.

Proof: Let $G_\alpha g$ be a coset. Every element of the coset maps α into the same element. Further, if $G_\alpha g_1$ and $G_\alpha g_2$ map α into the same element then $g_1g_2^{-1} \in G_\alpha$.

Cauchy's Theorem: If G is abelian and $p \mid |G|$ then $\exists x \in G, x \neq 1 : x^p = 1$.

Proof: By induction on $|G|$; true if $|G| = 1$. If $a \in G$ and $|a| = p^r m$, $(p, m) = 1$ then $b = a^{p^{r-1}m}$ has order p and where done. If $p \nmid |a|$, apply the inductive hypothesis to $G/\langle a \rangle$.

Sylow's Theorem: Let $|G|_p$ denote the largest i such that $p^i \mid |G|$. (1) $\exists S \leq G, |S| = p^{|G|_p}$; (2) Let $S_p(G) = \{S \leq G : |S| = p^{|G|_p}\}$, $|S_p(G)| = 1 \pmod p$ and $|S_p(G)| \mid |G : P|$. All elements of $S_p(G)$ are conjugate.

Proof of (1): By induction on $|G|$; true if $|G| = 1$. Let G act by conjugation on its elements and decompose these into disjoint orbits. We get $|G| = |\mathbb{Z}(G)| + \sum_x |G : C_G(x)|$. If $p \nmid |\mathbb{Z}(G)|$, $p \nmid |C_G(x)|$ for some x and we can apply the induction hypothesis to $C_G(x)$. If $p \mid |G|$, by Cauchy, $\exists a \in \mathbb{Z}(G), a \neq 1, a^p = 1$. $\langle a \rangle \lhd G$. Apply the induction hypothesis to $G/\langle a \rangle$. Let $\Omega = S^G, S \in S_p(G)$. If $R \notin \Omega, R \in S_p(G)$, let R act on Ω. If $R \in N(S)$, $|RS|_p > |S|$, which is a contradiction. Thus, the length of all R-orbits on Ω is divisible by p, which contradicts the fact that $|S_p(G)| = 1 \pmod p$.

Proof of (2, 3): Let G act on $S_p(G)$ by conjugation and $P \in S_p(G)$. P also acts on $S_p(G)$ by conjugation. Let Σ be a G-orbit. $\Sigma = \bigcup \Delta_i$ where each Δ_i is a P-orbit disjoint from $\Delta_j, i \neq j$. If $P \notin \Sigma$ $p \mid |\Delta_i|, \forall i$ so $p \mid |G : N(P)|$ which is a contradiction. So $P \in \Sigma$ for all G-orbits and hence G is transitive on $S_p(G)$. In this decomposition, P is in an orbit by itself and every other orbit has size divisible by p, so $|S_p(G) = |G : N_G(P)| = 1 \pmod p$. Finally, $|S_p(G)| = |G : N_G(P)| \mid |G : P|$.

Frattini Argument: If $H \lhd G$ and $P \in S_p(H)$ then $G = HN_G(P)$.

Proof: Let $g \in G$. $P^g \in H$ so $\exists x \in H : P^x = P^g$. $x^{-1}g \in N(P)$ so $g \in HN(P)$.

Theorem 3: If P is a p-group and $S < P$ then $N_P(S) > S$.

Proof: Let P act on S by conjugation and Σ be the resulting orbit. Now let S act on Σ.

Chapter 4

Nilpotent Groups and Frattini Subgroup

4.1 Series

Definition of lower central series: $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G]$.

Definition 1: G is **nilpotent** if $G^{(n)} = 1$ for some n. Note $G^{(n)}/G^{(n+1)} \subseteq \mathbb{Z}(G/G^{(n+1)})$.

Definition of upper central series: $G^{[0]} = 1$. Define $G^{[n+1]} =$ preimage of $\mathbb{Z}(G/G^{[n]})$.

Definition 2: A normal series, $N_k \subseteq N_{k-1} \subseteq \ldots \subseteq N_1 = G$, is *central* if $[N_i, G] \subseteq N_{i+1}$.

Theorem 1: Let G be a finite group, the following are equivalent: (1) G has a central series which reaches 1; (2) $G^{(n)} = 1$ for some n; (3) $G^{[n]} = G$ for some n; (4) $N_G(H) > H$ if $H \neq G$; (5) Every maximal subgroup of G is normal in G and the quotient group has index p; (6) Every Sylow subgroup of G is normal in G. When these hold, we say G is *nilpotent*.

Proof $1 \to 2$*:* Let $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_n$ with $[G, N_i] \subseteq N_{i+1}$. $G^{(0)} \subseteq N_0$ and $G^{(i+1)} = [G^{(i)}, G] \subseteq [N_i, G] \subseteq N_{i+1}$ so $G^{(n)} = 1$.

Proof $2 \to 3$*:* We prove that $G^{[n-i]} \supseteq G^{(i)}$, $G^{(0)} = G = G^{[n]}$ and $G^{(n)} = 1 = G^{[0]}$.

Proof $3 \to 4$*:* $\exists i$ such that $G^{[i]} \subseteq H$ and $G^{[i+1]} \nsubseteq H$. Then $[G^{[i+1]}, G] \subseteq G^{[i]} \subseteq H$ and there is a $x \in G^{[i+1]}$, $x \notin H$ with $xHx^{-1} = H$.

Proof $4 \to 5$*:* Let M be a maximal subgroup. $N_G(M) > M$ so $G = N_G(M)$.

Proof $5 \to 6$*:* Let M be a maximal subgroup containing $N_G(P)$, $P \in S_p(G)$ then $M \lhd G$ and by Frattini, $G = MN_G(P) = N_G(P)$.

Proof $6 \to 1$*:* Let $P_1, P_2, \ldots, P_n$ be the Sylow subgroups and put $H = P_1P_2 \ldots P_n$, $H \lhd G$. Put $G^* = [P_1, G] = [P_1, P_1] \neq P_1$ and consider $G \supseteq G^*$. G^* has a central series by induction.

Corrollary: If G is nilpotent, $G = \bigoplus_{p||G|} O_p(G)$ and $O_p(G)$ is a Sylow subgroup of G.

4.2 Frattini Subgroup

Lemma: Let $1 \neq H \lhd G$ and J, a p-group in G. If $|H| \neq 1 \pmod{p}$ then $H \cap C_G(J) \neq 1$.

Theorem 2: If G is nilpotent and $1 \neq H \lhd G$ then (1) $[H, G] \not\subseteq H$ and (2) $1 \neq H \cap \mathbb{Z}(G)$.

Proof: (1) If $[H, G] = H$ then $[H, G, G, \ldots, G] = H$. (2) Count!

Definition 3: $\Phi(G) = \bigcap_{M \in \mathcal{M}(G)} M$ where $\mathcal{M}(G)$ is the set of maximal subgroups of G. It is called the *Frattini subgroup* of G.

Theorem 3: (1) If $\langle \Phi(G), X \rangle = G$, $\langle X \rangle = G$. $\Phi(G)$ *char* G; further, (2) $\Phi(G)$ is nilpotent. (3) $F(G)/\Phi(G) = F(G/\Phi(G))$.

Proof: For (1), if not put $H = \langle X \rangle$. H is in some maximal subgroup of G, say M, So $\Phi(G) \subseteq M$ and $\langle \Phi(G), X \rangle \subseteq \langle \Phi(G), H \rangle \subseteq M$, contradiction!. Automorphisms, ϕ, and their inverses take maximal subgroups in G into maximal subgroups in G, so $\bigcap_{M \in \mathcal{M}} M = \bigcap_{M \in \mathcal{M}} \phi(M) = \Phi(G)$. Let $P \in S_p(\Phi(G))$. Since $\Phi(G) \lhd G$, $G = \langle \Phi(G), N_G(P) \rangle = N_G(P)$ and so $P \lhd G$ so $\Phi(G)$ is nilpotent. (3) follows from (2).

Theorem 4: If G is nilpotent, $G' \subseteq \Phi(G)$.

Proof: Suppose G is nilpotent and M is a maximal subgroup of G. $N_G(M) > M$ so $M \lhd G$. If $1 \neq a \in G/M$, $\langle a, M \rangle = G$ so G/M is cyclic and $G' \subseteq M$. This is true for every M so $G' \subseteq \Phi(G)$.

Theorem 4: G is nilpotent iff it is solvable and p-closed $\forall p$.

Proof: If G is nilpotent, $O_p(G) = P \in S_p(G)$ and $G = \bigotimes_{p||G|} O_{p_i}(G)$ and the result follows. The reverse inclusion goes by induction G is solvable, $O_p(G) \neq 1$, some p, applying induction to $\overline{G} = G/O_p(G)$ gives the result.

Theorem 5: If $\Phi(G)$ and $\overline{G} = G/\Phi(G)$ are nilpotent then so is G.

Proof: Let $\overline{P} \in S_p(\overline{G})$ then $\overline{P} \lhd \overline{G}$. Put $N = P\Phi(G) \lhd G$. By Frattini, $P \in S_p(G) \to N_G(P)N = N_G(P)\Phi(G) = N_G(P)$.

Theorem 6: $\Phi(G) \subseteq F(G)$.

Proof: $\Phi(G)$ is nilpotent and so is $F(G)$ and so is their product. Since $F(G)$ is maximal, this product is in $F(G)$.

Theorem 7: If P is a p-group then $\overline{P} = P/\Phi(P)$ is elementary abelian.

Proof: Suppose M is maximal in P. As above, $M \lhd P$ and $P' \subseteq M$. Suppose $\overline{x} \in \overline{P}$. $|x| = p^m$ and there is a the characteristic subgroup N of P with index p must be in M (otherwise $P = NM$). Thus xM has order p. This is true for all M so $\overline{x}$ has order p and as noted $\overline{P}$ is abelian so it is elemenetary abelian.

Theorem 8: $\Phi(G/N) = \Phi(G)N/N$.

Proof: Let $\overline{A} = A/N$, $N \lhd G$. Maximal subgroups of $\overline{G}$ are the maximal subgroups of G containing N.

Theorem 9: If $S \subseteq G$ and $\langle S, \Phi(G) \rangle = G$ then $\langle S \rangle = G$. If $H/\Phi(H)$ is cyclic then H is cyclic.

Proof: Suppose $\langle S \rangle = H < G$. Let M be a maximal subgroup containing H. $\Phi(G) \subseteq M$, so $\langle \Phi(G), S \rangle \subseteq H \neq G$. Contradiction.

Chapter 5

Automorphisms

5.1 Cyclic Groups

Theorem 1: If $G = \langle x \rangle$ and $p^t = n = |x|$. For $p \neq 2$, $|Aut(G)|$ is cyclic of order $(p-1)p^{t-1}$. For $p = 2$, $|Aut(G)| = 2^{t-1}$; moreover, it is a direct product of a group generated by an involution and a cyclic group of order 2^{t-2}.

Proof: Suppose $\sigma \in Aut(G)$. $\sigma(x) = x^r$, so $(p, r) = 1$ and the result follows. If $p \neq 2$, $Aut(G)$ has a unique element of order $p-1$. For $p \neq 2$ $c = 1 + p$ has order p^{t-1} and the first sub-result follows. For $p = 2$, let $c = 5$. c has order 2^{t-2} and $-1 \notin \langle c \rangle$ and the second subresult follows.

Theorem 2: $G = \langle x \rangle$ and $|p^t| = n$. If $p \neq 2, t > 1$, $Aut(G)$ has a unique subgroup of order p generated by by $x \mapsto x^{1+p^{t-1}}$. If $p = 2, t > 2$, there are three subgroups of order 2 generated by $x \mapsto x^{-1}$, $x \mapsto x^{-1+2^{t-1}}$, and $x \mapsto x^{1+p^{t-1}}$.

Proof: Follows directly.

Theorem 3: If $G = \langle x \rangle$ and $|p^t| = n$. Let $G_1 = \langle x^p \rangle$ and $G_2 = \langle x^{p^{t-1}} \rangle$ so $|G_1| = p^{t-1}$ and $|G_2| = p$. Suppose $\sigma \in Aut(G)$ of order p. If σ centralizes G/G_1 or σ centralizes G/G_2, $\sigma = 1$

Proof: Suppose $\sigma(x) = x^r$. If σ centralizes G/G_1, $r = 1 + kp$. If σ centralizes G/G_2, $p^{t-1}(1-r) = 0 \pmod{p^t}$ and again, $r = 1 + kp$. The result follows.

Theorem 4: Suppose G is a p-group of order p^{n+1} with a cyclic subgroup of order p^n then either G is cyclic or $G = \langle x, y \rangle$ with $|x| = p^n$ and one of the following holds for y: (i) $|y| = p$ and $[x, y] = 1$, (ii) $p > 2$ or $p = 2, n > 2$ and $y^{-1}xy = x^{1+p^{n-1}}$; (iii) $p = 2$ and $y^{-1}xy = x^{-1}$ [dihedral], (iv) $p = 2$ and $y^{-1}xy = x^{-1+2^{n-1}}$ [semi-dihedral], or (v) $p = 2$ and $y^2 = x^{2^{n-1}}$, $y^{-1}xy = x^{-1}$ [quaternion]. Moreover, types (i) and (ii) have characteristic abelian subgroups of type (p, p).

Proof: Let $A = \langle x \rangle$, $|G : A| = p$. If A is central, G is abelian. If not, $C(A) = A$. Let $G = \langle x, w \rangle$. $w^p \in C(A)$. Put $w^p = x^r$. Now we examine the action of w on $\langle x \rangle$.

If $x^w = x^{1+ip^{n-1}}$, so $r = ps$ since $|X| = p^n$. $(x^{-s}w)^p = w^p(x^{-s})^{w^p}(x^{-s})^{w^{p-1}} \dots (x^{-s})^w$. Thus $(x^{-s}w)^p = w^p x^{(-s)[p+\frac{p^n(p+1)}{2}]}$. $w^p = x^{sp}$ so $(x^{-s}w)^p = w^p x^{(-s)p^n \frac{p+1}{2}}$. For $p \neq 2$, put $y = x^{-s}w$. $x^y = x^{1+p^{n-1}}$ and $y^p = 1$ and we get (ii). If $p = 2$, put $y = x^{-s(1+2^{n-2}}w$. Again $y^2 = 1$ and we have (ii).

Thus $p = 2$. If $x^w = x^{-1}$, put $y = w$ so $y^2 = 1$ or $y^2 = x^{2^{n-1}}$, giving case (iv).

Finally, put $B = \langle x^{p^{n-1}}, y\rangle$. $[x^{p^{n-1}}, y] = 1$ and each has order p. Every element of order p is in B so B *char* G.

Theorem 5: Suppose G is a p-group and G is not cyclic, dihedral, semi-dihedral or quaternion. Then G has a subgroup of type (p, p).

Proof: Let A be maximal with respect to being normal and cyclic. $|G| \geq p$ and $|A| \geq p$ and $A \neq G$. If $C(A) > A$, $\exists B \subseteq C(A) : |B : A| = p$. B is abelian and non cyclic so it is of type (i) above, which proves it. If $C(A) = A$, G acts by conjugation with kernel $C(A)$ and $G/A \to Aut(A)$ so we're in cases (ii), (iii), (iv) or (v) sp $p = 2$, $|A| = 2^n$ and $x \mapsto x^{1+2^n} \notin A$. Thus $|G : A| = 2$ and $G = B$, so we're in (iii), (iv) or (v).

Theorem 6: Suppose G is a p-group and $\mathbb{Z}(G/\mathbb{Z}(G))$ is cyclic then G is cyclic, dihedral, semi-dihedral or quaternion.

Proof: If G is not cyclic, dihedral, semi-dihedral or quaternion, $\exists D \lhd G$ of type (p, p). $[G, D] < D$ and $[G, [G, D]] = 1$ and $D \subseteq \mathbb{Z}(G/\mathbb{Z}(G))$; hence $\mathbb{Z}(G/\mathbb{Z}(G))$ is not cyclic.

Theorem 7: Suppose G is a p-group and every normal abelian subgroup is cyclic. Then G is cyclic, dihedral, semi-dihedral or quaternion.

Proof:

Theorem 8: Suppose G is a p-group with exactly one subgroup of order p. Then G is cyclic or quaternion.

Proof: $\mathbb{Z}(G/\mathbb{Z}(G))$ is a normal ableian group, so the result follows from Theorem 7. G cannot have a subgroup of type (p, p), so G is cyclic, dihedral, semi-dihedral or quaternion. Looking at generators and relations only the cyclic and quaternion cases are possible. If cyclic, we're done. Let $G = \langle x, y : x^{2^n} = 1, y^2 = x^{2^{n-1}}, y^{-1}xy = x^{-1}\rangle$. Let w be of order 2. If $w \in \langle x\rangle, w = x^{2^{n-1}}$. If not, $w = x^i y$. $1 = w^2 x^i y x^i y = x^i y^2 (y^{-1} x^i y) = y^2 = x^{2^{n-1}}$, which is a contradiction. Thus G has a unique element of order 2.

Theorem 9: If G is quaternion of order 8 then (i) every subgroup is cyclic, (ii) $Aut(G) \cong S_4$, (iii) an element of order 3 transitively permutes the 3 non-central classes of G.

Proof: Let $H < G$, so $|H| \leq 4$. Since G has a unique element of order 2 and H is abelian, H is cyclic and (i) follows. G has three distinct subgroups of order 4: $\langle u\rangle$, $\langle v\rangle$, and $\langle w\rangle$. $u^2 = v^2 = w^2 = z$ and $[u, v] = [w, v] = [u, w] = z$ and $\langle u, v\rangle = \langle u, w\rangle = \langle v, w\rangle = G$. $Sym(u, v, w) \mapsto Aut(G)$. Further, $Sym(u, v, w) \cap Inn(G) = 1$ since $\langle u\rangle, \langle v\rangle, \langle w\rangle$ are normal. But $Inn(u, v, w) \lhd Aut(G)$ and $|Inn(G)| = 4$. $Aut(G)$ contains the semi-direct product of $Inn(G)$ and $Sym(u, v, w)$, which is isomorphic to S_4. Finally, let $\sigma \in Aut(G)$ have order 3, σ permutes u, v, w. If σ fixes one of these, it fixes all of them. So $\sigma(u) = uu^{-1}$ and same for v, w and the result follows.

Theorem 10: If G is quaternion of order > 8 then (i) every subgroup is cyclic or quaternion, (ii) if N is a non-ableian normal subgroup, $|G : N| = 1, 2$, (iii) G has a characteristic cyclic subgroup, A of index 2, $Aut(G)$ is a 2-group, and, (iv) G has three conjugacy classes of elements of order 4, one consists of the two elements of A or order 4 and the other two consist of half the elements of $G \setminus A$.

Proof: Since G has a unique element of order 2, so does every subgroup. Thus subgroups are cyclic or quaternion. $G = \langle x, y : x^{2^n} = 1, y^2 = x^{2^{n-1}}, y^{-1}xy = x^{-1}\rangle$. Let $A = \langle x\rangle$. Every element of $G \setminus A$ has order 4. The generators of A are the only elements of G of order $2^n > 4$ and A *char* G giving (i) and (iii).

Suppose N is a normal, non-abelian subgroup of G and N is not a subgroup of A. Let $w \in N \setminus A$, $w^2 = x^{2^{n-1}}$ and $w^{-1}xw = x^{-1}$. Since $N \lhd G$, N contains $[w, x] = x^2$ and $\langle x^2, w\rangle \subseteq N$ of index 2. So (ii) follows.

Suppose $Aut(G)$ is not a 2 group. $\sigma \in Aut(G)$ of prime order coprime to 2. $\sigma \in Aut(A)$, but $Aut(A)$ is a 2-group, so σ fixes A. $\exists w \in G : \sigma(w) = w$. $G = \langle A, w\rangle$; σ fixes all of G, contradiction and (iv) holds. $\{x^{2^{n-2}}, x^{-2^{n-2}}\}$ are the elements of A of order 4. Let $w \in G \setminus A$, $x^w = w^{-1}$ and $C(w) = \langle x^{2^{n-1}}, w\rangle = \langle w\rangle$ and the result follows.

5.2 Non-cyclic groups

Theorem 1: If $G = E(p^n)$ then $Aut(G) = L_n(p)$.

Theorem 2: If $G = S_n$ then $Aut(G) = S_n$ if $n \neq 6$ and a covering group with factor 2 of S_6 for S_6 (an outer automorphism).

Theorem 3: If G is simple, $1 \to G \to Aut(G)$.

Definition: $Q_8 = \langle \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\rangle$. $Q_8 \in S_2(SL_2(5))$.

Theorem 4: The automorphism group of Q_8 is S_4.

Notation: Suppose G can be represented as a subgroup of $GL_p(V)$. Let ϕ_x be the automorphism induced by x on V in such a representation.

Theorem 5: If $H \lhd G \subseteq GL_p(V)$ then $C_V(H)$ is G-invariant.

Proof: Let $w \in W = C_V(G), h \in H, g \in G$ and let ϕ_x be as above. $g^{-1}hg \in H$ so $\phi_{g^{-1}hg}(w) = 1$. so $\phi_{g^{-1}}\phi_h\phi_g(w) = w$ and so $\phi_h\phi_g(w) = \phi_g(w)$. Thus W is G-invariant.

Theorem 6: Let $P \in p(GL_p(V))$. $\exists v \in V : \phi_x(v) = v, \forall x \in P$.

Proof: By induction on $|P|$. Let $M \lhd P$ be maximal so $|P : M| = p$ and put $W = C_V(M)$. By induction, $W \neq 1$ and is P-invariant. Choose $y \in P \setminus M$ then $y^p \in M$ so the minimal polynomial for y is $x^p - 1 = (x - 1)^p$ so there is a $w \in W : [w, y] = 1$. thus $[w, \langle y, M\rangle] = 1$.

Theorem 7: Let $K \lhd P$ then $K \cap \mathbb{Z}(P) \neq 1$.

Proof: $H = \Omega_1(\mathbb{Z}(K) \neq 1$. H char $K \lhd P$ and H is elementary abelian. Let $\overline{P} = PC_H(P)/C_H(P)$. Then $C_H(\overline{P}) \neq 1$ by Theorem 7. So, $1 \neq H \cap \mathbb{Z}(P) \subseteq \mathbb{Z}(P) \cap K$.

Note: Theorem 7 holds if P is nilpotent.

Theorem 8: Let H be an elementary abelian subgroup of P and $x \in N_P(H)$. Define $H^{(0)} = H$ and $H^{(i+1)} = [H^{(i)}, x]$ then the minimal polynomial for x is $(x - 1)^r$ where $H^{(r)} = 1$.

Proof: Put $\psi_x = \phi_x - 1$. $\psi_x(h)$ represents $[h, x]$ and $\psi_x^n(h)$ represents $[h, x, \ldots, x]$. Since $\phi_x^{p^n} = 1$, $(\phi_x(h) - 1)^r = 0$ for some $r \mid p^n$, wiht r is the least such integer.

Theorem 9: If G has a faithful, irreducible representation over $GF(p)$ then G has no normal p subgroup.

Proof: Suppose $P \lhd G$. $W = C_V(\phi_P) \neq 1$. But ϕ is irreducible so $W = V$. ϕ_P acts trivially on V so $P = 1$ since ϕ faithful.

Chapter 6

Constructions

6.1 Semidirect Product

Definition 1: G is an *extension* of K by Q if $G \triangleright K$ and $G/K \cong Q$. Equivalently, there is a surjective homomorphism $\pi : G \to Q$ (i.e.: $1 \to K \to G \to H \to 1$).

Definition 2: Let $\pi : H \to Aut(K)$, $K \triangleleft G$, $H < G$ and $H \cap K = 1$ define the *semidirect* product of K by H (denoted $H \ltimes K$) as the group with elements $(a, g) \in H \times K$ with the product $(a, g) \cdot (b, h) = (ab, \pi(b)(g)h)$ [or $(ab, (g)^{\pi(b)}h)$]. *Example:* The dihedrael group, $D_n : |D_n| = 2n$ is $H \ltimes K$, where $K = \langle a \rangle, |a| = n$ and H is a group of order 2, the non-identity element is a reflection. $(a, g)^{-1} = (a^{-1}, (g^{-1})^{\pi(a^{-1})})$.

Definition 3: An extension G of K by H *splits* if G is a semidirect product of H and K.

Theorem 1: If $1 \to N \to_i G \to_\varphi Q \to 1$, the following are equivalent (1) $\exists H \subseteq G$ such that $\varphi : H \to Q$ is an isomorphism; (2) $\exists s : Q \to G$ such that $\varphi \cdot s = id$; (3) G is a semidirect product of N by H written $Q \ltimes N$; in this case, we say G is a split extension of N by H.

Proof:

$1 \to 2$: Put $s = \varphi^{-1}_{|H}$, then (2) holds.

$2 \to 3$: Let $H = s(Q)$, $N = ker(\varphi)$. Suppose $x \in G$ and $q = \varphi(x)$. Set $h = s(q)$. $\varphi(xh^{-1}) = \varphi(x)\varphi(h)^{-1} = qq^{-1} = 1$ so $xh^{-1} \in N$ and $x = nh$.

$3 \to 1$: If $G = N \ltimes H$, the map $\varphi_{|H}$ is an isomorphism onto Q and H satisfies the conditions of (1).

6.2 Presentations

Theorem 2: Let $G = \langle x_1, \ldots, x_n | R_1(x_1, \ldots, x_n), R_2(x_1, \ldots, x_n), \ldots R_m(x_1, \ldots, x_n) \rangle$. There is a one to one correspondance between homomorphisms $\rho : G \to H$ and solutions to $R_1(y_1, \ldots, y_n) = 1, R_2(y_1, \ldots, y_n) = 1, \ldots R_m(y_1, \ldots, y_n) = 1, y_i \in H$.

Theorem 3: Two groups are isomorphic iff they admit the same presentation up to renaming.

Theorem 4: Let $G \cong F/R$, F, free. Then for arbitrary abelian A, the transgression map $Hom(R/[F,R], A) \to H^2(G, A)$ is associated with the natural exact sequence $1 \to R/[F,R] \to F/[F,R] \to G \to 1$.

Projective representations and Schur: Let $\rho : G \to GL_n(\mathbb{C})/\mathbb{Z}$ so that $\rho(g)$ is a coset $\pmod{\mathbb{Z}}$. Choose $A(g) \in \rho(g)$ then $\rho(ab) = r_{a,b}\rho(a)\rho(b)$ and $r_{a,b}r_{ab,c} = r_{a,bc}r_{b,c}$ (cocycle identity). Conversely, given an r satisfying the cocycle identity, there is a projective representation of degree $|G| = m$ giving rise to it. If $B(g) \in \rho(g)$ is another, $A(g) = d_g B(g)$, and if $B(ab) = s_{a,b}B(a)B(b)$, $r_{a,b} = \frac{d_a d_b}{d_{ab}} s_{a,b}$ (Relation 1). If r, s satisfy relation 1, they are called *equivalent*.

Theorem 5: Let $\rho^* : H \to GL_n(\mathbb{C})$ be an ordinary irreducible representation of H with $A \leq \mathbb{Z}(H)$ then $\rho^*(a) = j_a I_n$ and we can define $\rho : H/A \to GL_n(\mathbb{C})/\mathbb{Z}$ by $\rho(hA) = \rho^*(h)\mathbb{Z}$. Schur showed the converse: $\exists H : A \leq \mathbb{Z}(H)$ with $H/A \cong G$.

Proof:

Note that if $G = \langle F|R\rangle$ is of rank k, $(F/[F,R])/(R/[F,R]) = G$ and $R/[F,R]$ is central.

6.3 Central Product

Definition of Central Product: $G = \langle G_i\rangle, 1 \leq i \leq n$, $[G_i, G_j] = 1$ for $i \neq j$. Equivalently, $\rho : (x_1, x_2, \ldots, x_n) \mapsto x_1 x_2 \ldots x_n$ is a surjective homomorphism from $D = (G_1 \times G_2 \times \ldots \times G_n)$ to G with $\rho(D_i) = G_i$ with $\pi_i(G_1, \ldots, G_n) = D_i$ and $ker(\rho) \cap D_i = 1$, $ker(\rho) \subseteq \mathbb{Z}(G)$.

Proof of equivalence: Let $\alpha_i : \mathbb{Z}(G_1) \to \mathbb{Z}(G_i)$. $E = \langle z(\alpha_i(z^{-1}))\rangle$. E is a complement to $\mathbb{Z}(D_i)$ in $Z = \langle \mathbb{Z}(D_i)\rangle$ so D/E is a central product. Suppose G is a central product of the G_i with $\mathbb{Z}(G_i) = \mathbb{Z}(G_1)$ and ρ the surjective homomorphism. Let $\beta_i : \mathbb{Z}(D_1) \to \mathbb{Z}(G_i)$ be the composition of $\rho_{|\mathbb{Z}(D_1)}$ and $\rho^{-1}_{|\mathbb{Z}(D_i)} : \mathbb{Z}(G_1) \to \mathbb{Z}(D_i)$ then $ker(\rho) = \langle x\beta_i(z^{-1}), z \in \mathbb{Z}(D_1)\rangle = A$ is a complement to $\mathbb{Z}(D_i)$ in Z and $G \cong D/A$. Define $\gamma \in Aut(D)$ with $\gamma(D_1) = D_i$ and $\gamma(E) = A$. This induces and isomorphism of D/E with D/A. Let $\delta_i = \beta_i(\alpha_i)^{-1}$ then $\gamma_{i|\mathbb{Z}(D_i)} = \delta_i$ and define $\gamma : D \to D$ by $(x_1, x_2, \ldots, x_n) \mapsto (x_1, \gamma_1(x_2), \ldots, \gamma_n(x_n))$.

Example: Both D_8 and Q_8 are central products of Z_2 by $Z_2 \times Z_2$. Note that D_8 is also a direct product but Q_8 is not.

Theorem 6: Let $G_i, 1 \leq i \leq n$ be a family of groups with $Z(G_1) = Z(G_i)$ and $Aut_{G_i}(Z(G_i)) = Aut(Z(G_i))$. The up to isomorphism there is a unique central product with $Z(G_1) = Z(G_i)$.

Proof: By hypothesis, there are isomorphisms $\alpha_i : \mathbb{Z}(D_1) \to \mathbb{Z}(D_i)$, $1 \leq i \leq n$. Let E be the subgroup of D generates by $\{\alpha_i(z^{-1})z, z \in \mathbb{Z}(D_1)$. E is a complement to $\mathbb{Z}(D_i)$ in $Z = \langle \mathbb{Z}(D_i), 1 \leq i \leq n\rangle = \mathbb{Z}(D)$ so D/E is a central product of the G_i with $\mathbb{Z}(G_1) = \mathbb{Z}(G_i)$ by the foregoing equivalence. Now suppose G is a central product of the G_i with $\mathbb{Z}(G_1) = \mathbb{Z}(G_i)$ and let $\pi : D \to G$ be the surjective homomorphism in the equivalence proof. Let $\beta_i : \mathbb{Z}(D_1) \to \mathbb{Z}(D_i)$ be the composition of $\pi_{|\mathbb{Z}(D_1)}$ and $\pi^{-1}_{|\mathbb{Z}(D_i)}$. $ker(\pi) = \langle z\beta_i(Z^{-1}) : z \in \mathbb{Z}(D_1), 1 \leq i \leq n\rangle = A$ is a complement to $\mathbb{Z}(D_i)$ in Z for each i and $G \cong D/A$. Now let $\delta_i = \beta_i\alpha_i^{-1}$ and $\delta_i \in Aut(\mathbb{Z}(D_i))$. By hypothesis, $\exists\gamma_i \in Aut(D_i)$ with $\gamma_{i|\mathbb{Z}(D_i)} = \delta_i$. Define $\gamma : D \to D$ by $(x_1, x_2, \ldots, x_n) \mapsto (x_1, \gamma_2(x_2), \ldots, \gamma_n(x_n))$. $\gamma \in Aut(D)$ and $\alpha_i(\gamma(z^{-1}))z$ so $\gamma(E) = A$ and we're done.

6.4 Wreath Product

Wreath Product: $G^* = G^X$ - maps from X to G. $fg(x) = f(x)g(x)$. Let H act on X: $f^h(x) = f(xh^{-1})$. Let ϕ be the natural action of H induced on $G^{|H|}$, then $G \wr H = H \rtimes_\phi G^*$. If $G_x = \{f : f(y) = 1 \; if \; x \neq y\}$. $G^* = \prod_X G_x$. Put $g_x(y) = g(y)$ if $x = y$, 1 otherwise. Note that ${g_x}^h = g_{xh}$.

Theorem 7: If D and Q are groups with Q finite then the regular wreath product $D \wr_r Q$ contains an isomorphic copy of every extension of D by Q.

Proof: If G is an extension of D by Q then there is a surjective homomorphism $G \to Q$ with kernel D denoted by $a \mapsto \overline{a}$. Choose a transversal $l : Q \to G$. For $a \in G$, define $\sigma_a(x) = l(x)^{-1}al(\overline{a^{-1}x})$. If $a, b \in G$ then $\sigma_a(x)\sigma_b^{\overline{a}}(x) = \sigma_a(x)\sigma_b(\overline{a^{-1}x}) = l(x)^{-1}al(\overline{a^{-1}x})l(x)^{-1}al(\overline{a^{-1}x})l(\overline{a^{-1}x})^{-1}bl(\overline{b^{-1}a^{-1}x}) = l(x)^{-1}abl(\overline{b^{-1}a^{-1}x}) = \sigma_{ab}(x)$. Define $\varphi : G \to D \wr_r Q$ by $\varphi(a) = (\sigma_a, \overline{a}), \forall a \in G$. A simple calculation shows φ is a injective homomorphism.

Theorem 8 (Gaschutz): Let V be an abelian normal subgroup of a p-group, G, $P \in S_p(G)$. G splits over V iff P splits over V.

Proof: $V \leq P$. $P = P \cap G = P \cap HV$ so $P = V(P \cap H)$ by Dedekind.

Chapter 7

Extensions

7.1 Transversals

Definition 1: As before, G is an *extension* of K by Q if $G \triangleright K$ and $G/K \cong Q$ or equivalently $1 \to K \to G \to Q \to 1$.

Extending a group: Suppose G is an extension of N by H and let $\phi : H \to G/N$. Pick $s : H \to G$ such that $s(1) = 1$ and $\phi(h) = Ns(h)$, then $\exists f : H \times H \to N : s(h_1)s(h_2) = f(h_1, h_2)s(h_1h_2)$ and $f(h_1, h_2)f(h_1h_2, h_3) = f(h_2, h_3)^{s(h_1)}f(h_1, h_2h_3)$. Note that $\theta_h : n \mapsto s(h)ns(h)^{-1}$ is in $Aut(N)$ and $\theta_{h_1}(\theta_{h_2}(n)) = \theta_{h_1h_2}(n)^{f(h_1,h_2)}$. Note, here $a^b = bab^{-1}$, usually, we write $a^b = b^{-1}ab$, oh well.

Theorem: Given N, H with $\theta_h \in Aut(N)$ and $\theta_1 = 1$ and a map $f : H \times H \to N$ with $f(1, h) = f(h, 1) = 1$ and $f(h_1, h_2)f(h_1h_2, h_3) = \theta_{h_1}(f(h_2, h_3))f(h_1, h_2h_3)$, suppose f is compatible in the sense that $\theta_{h_1}(\theta_{h_2}(n)) = \theta_{h_1h_2}(n)^{f(h_1,h_2)}$ then the operation $(n_1, h_1) \cdot (n_2, h_2) = (n_1\theta_{h_1}(n_2)f(h_1, h_2), h_1h_2)$ defines a group G which is an extension of N by H. $1 \to N \to G \to H \to 1$ holds with the obvious embedding $n \mapsto (n, 1)$ and $h \mapsto (1, h)$.

> *Proof:* Put $(n, h)^{-1} = \theta^{-1}[n^{-1}f(h, h^{-1})^{-1}], h^{-1})$. $(n, h)^{-1} \cdot (n, h) = (1, 1)$. $(n, h) \cdot (1, 1) = (n, h)$. Associativity is a long calculation but works.

Definition 2: A subset $\mathcal{T}$ consisting of a representative of each coset in G/K is called a *transversal*.

Definition 3: If $\pi : G \to Q$ is a surjective homomorphism with kernel K, $l : Q \to G$ is a *lifting* if $\pi(l(x)) = x$. If $\pi : Q \to G$ is a surjective homomorphism with kernel K and $l : Q \to G$ is a transversal with $l(1) = 0$ then $f : Q \times Q \to K$ defined by $l(x) + l(y) = f(x, y) + l(xy)$ is called a *factor set*. An ordered triple, (Q, K, θ) is called *data* if K is an abelian group, $\theta : Q \to Aut(K)$; a group G is said to *realize* the data if G is and extension of K by Q and for every transversal, $l : Q \to G$ satisfies $xa = \theta_x(a) = l(x) + a - l(x)$. Note additive notation for non-abelian operation.

Theorem 2: Let G be an extension of K by Q and $l : Q \to G$ a transversal. If K is abelian there is a homomorphism $\theta : Q \to Aut(K)$ with $\theta(a) = l(x) + a - l(x), \forall a \in K$; If $l_1 : Q \to G$ is another transversal then $l(x) + a - l(x) = l_1(x) + a - l_1(x)$.

> *Proof:* $K \lhd G$ so $\gamma_{g|K}$ is an automorphism of K (γ_g is conjugation by g). $\mu : G \to Aut(K)$ given by $\mu(g) = \gamma_g$ is a homomorphism with $K \leq ker(\mu)$. μ induces a homomorphism $\mu_\# :$

$G/K \to Aut(K)$ given by $\mu_\#(Kg) = \mu(g)$. The first isomorphism theorem gives the isomorphism $\lambda : Q \to G/K$ and if $l : Q \to G$ is a transversal $\lambda(x) = K + l(x)$. If $l_1 : Q \to G$ is another transversal then $l(x) - l_1(x) \in K$ so $K + l(x) = K + l_1(x), \forall x \in Q$. Thus λ does not depend on the choice of transversal. Put $\theta = \mu_\#\lambda$. $\theta_x = \mu_\#(K + l(x)) = \mu(l(x)) \in Aut(K)$ so for $a \in K : \theta_x(a) = \mu(l(x))(a) = l(x) + a - l(x)$.

Theorem 3: Let $\pi : G \to Q$ be a surjective homomorphism with kernel K and $l : Q \to G$ be a transversal with $l(1) = 0$ and $f : Q \times Q \to K$ the corresponding factor set. $f(1, y) = 0 = f(x, 1), \forall x, y \in Q$ and the *cocycle identity* $xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$ holds $\forall x, y, z \in Q$.

Proof: Definition gives $l(x) + l(y) = f(x, y) + l(xy)$. So $l(1) + l(y) = f(1, y) + l(y)$ and since $l(1) = 0$, $f(1, y) = 0$. Similarly, $f(x, 1) = 0$. $[l(x) + l(y)] + l(z) = f(x, y) + f(xy, z) + l(xyz)$ and $l(x) + [l(y) + l(z)] = xf(y, z) + f(x, yz) + l(xyz)$.

Theorem 4: Let G realize (Q, K, θ) and l and l' be transversals with $l(1) = l'(1) = 0$ giving rise to factor sets f and f' then there is an $h : Q \to K$ with $h(1) = 0$ such that $f'(x, y) - f(x, y) = xh(y) - h(xy) + h(x), \forall x, h \in Q$. The *cocycle identity* $xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$ holds $\forall x, y, z \in Q$.

Proof: By definition, $l(x) + l(y) = f(x, y) + l(xy)$ and $l(1) + l(y) = f(1, y) + l(xy)$; since $l(1) = 0$, this gives $f(1, y) = 0$ similarly $f(x, 1) = 0$. $[l(x) + l(y)] + l(z) = f(x, y) + f(xy, z) + l(xyz)$ and $l(x) + [l(y) + l(z)] = xf(y, z) + l(xy) + l(z) = xf(y, z) + f(xy, z) + l(xyz)$ so the result follows from associativity.

Definition: Given data (Q, K, θ) a *coboundary* is a function $g : Q \times Q \to K$ for which $\exists h : Q \to K$ such that $h(1) = 0$ and $g(x, y) = xh(x) - h(xy) + h(x)$. The set of all coboundaries is $B^2(Q, K, \theta)$. $Z^2(Q, K, \theta)$ is the set of all *factor sets*. $H^2(Q, K, \theta) \cong Z^2(Q, K, \theta)/B^2(Q, K, \theta)$.

Theorem 5: Given data (Q, K, θ) a function $f : Q \times Q \to K$ is a factor set iff it satisfies the cocycle identity.

Proof: The $\to$ direction is the previous theorem. For $\leftarrow$, let G be the set of all ordered pairs, $(a, x) \in K \times Q$ with the operation $(a, x) + (b, y) = (a + xb + f(x, y), xy)$. This is a group with the cocycle identity required for associativity.

Notation: Denote the G constructed in the previous proof as G_f realizing (Q, K, θ) with factor set f arising from $l(x) = (0, x)$.

Definition: Two extensions G, G' realizing (Q, K, θ) with factor sets f, f' are *equivalent* if $f' - f \in B^2(Q, K, \theta)$.

Theorem 6: Two extensions are equivalent if the difference of their two factor sets is in $B^2(Q, K, \theta)$.

Proof: For each $x \in Q$, $l(x)$ and $l'(x)$ are representatives of the same coset of K in G. Thus $\exists h(x) \in K$ with $l'(x) = h(x) + l(x)$. Since $l'(1) = 0 = l(1)$, $h(1) = 0$. We have $l'(x) + l'(y) = (h(x)+l(x))+(h(y)+l(y)) = h(x)+xh(y)+f(x, y)+l(xy) = h(x)+xh(y)+f(x, y)-h(xy)+l'(xy)$. Therefore $f'(, y) = h(x) + xh(y) + f(x, y) - h(xy)$. The conclusion follows since each term is in an abelian group.

Theorem 7: There is a bijection from $H^2(Q, K, \theta)$ to the set, E, of all equivalence classes realizing the data (Q, K, θ) taking the identity to the class of the semidirect product.

Proof: Let the equivalence classes of the extensions realizing the data (Q, K, θ) be denoted by $[G]$. Define $\varphi : H^2(Q, K, \theta) \to E$ by $\varphi(f + B^2(Q, K, \theta)) = G_f$. φ is well defined since if f, g are factor sets, $f - g \in B^2(Q, K, \theta)$ and $[G_f] = [G_g]$. φ is a surjection since if $[G] \in E$ and f is a factor set, $[G] = [G_f]$ and $[G] = \varphi(f + B^2)$. Finally, an extension is a semidirect product off its factor set is in $B^2(Q, K, \theta)$.

Definition: A *projective representation* of a group Q is a homomorphism $\tau : Q \to PGL_n(\mathbb{C})$. We say U has the *projective lifting property* if every projective representation of Q can be lifted to U. If Q is a group then a *cover* (or *representation group*) of Q is a central extension of U of K by Q (for some abelian K) with the projective lifting property and $K \leq U'$.

Definition: The *Schur multiplier* is $M(Q) = H^2(Q, \mathbb{C}^\times)$ (θ is trivial). Here $f(1, y) = f(x, 1) = 1$, $f(x, y)f(xy, z)^{-1}f(x, yz)f(x, y)^{-1} = 1$, $g : Q \times Q \to \mathbb{C}^\times$ is a coboundary iff $\exists h : Q \to \mathbb{C}^\times$ with $h(1) = 1$ such that $g(x, y) = h(y)(h(xy))^{-1}h(x)$.

Schur's Theorem: Every finite group, Q, has a cover U which is a central extension of $M(Q)$ by Q.

Proof: See Rotman.

Definition: $exp(G) = min\{e : x^e = 1, \forall x \in G\}$.

Theorem 8: If Q is finite then $M(Q)$ is a finite abelian group and $exp(M(Q)) \mid |Q|$.

Proof: See Rotman, p 201-211

Theorem 9: If Q is finite p-group then $M(Q)$ is a finite abelian p-group.

Proof: See, Rotman, p 202

Theorem 10: Let G be a group with $G/\mathbb{Z}(G)$ finite, then $G^{(1)}$ is finite.

Proof: Let $n = |G/\mathbb{Z}(G)|$. For $z \in \mathbb{Z}(G)$ and $g, h \in G$: $[g, hz] = [g, h] = [gz, h]$ so the set of commutators, Δ, is of order at most n^2. Claim: $g \in G^{(1)}$ then $g = x_1 x_2 \dots x_m$, $x_i \in \Delta$ and $m \leq n^3$.

Observation: A cyclic extension G of N is one where G/N is cyclic. Solvable groups are built from cyclic extensions.

Definition: G, an extension of K by Q, is a *central extension* if $K < \mathbb{Z}(G)$. Functorially, a central extension G is a pair (H, π) satisfying $\pi : H \to G, ker(\pi) \subseteq \mathbb{Z}(H)$. $\alpha : (H_1, \pi_1) \to (H_2, \pi_2)$ is a morphism in this category. The universal object in this category (if it exists) is called a *universal central extension*. It follows that $(\tilde{G}, \tilde{\pi})$ is universal if $\forall (H, \sigma), \exists! \alpha : (\tilde{G}, \tilde{\pi}) \to (H, \sigma)$.

Theorem 11: Up to isomorphism, there is at most one universal central extension.

Proof: If $(G_1, \pi_i), i = 1, 2$ are universal central extensions of G, $\exists \alpha_1 : (G_i, \pi_i) \to (G_{3-i}, \pi_{3-i})$. $\alpha\alpha_{3-i} = 1$ and by the uniqueness $\alpha_1\alpha_2 = 1 = \alpha_2\alpha_1$. Thus the α_i is an isomorphism.

Theorem 12: If $(\tilde{G}, \pi)$ is a universal central extension of G then both G and $\tilde{G}$ are perfect.

Proof: Let $H = \tilde{G} \times (\tilde{G}/\tilde{G}')$ and define $\alpha : H \to G$ by $\alpha(x, y) = \pi(x)$. Then (H, α) is a central extension of G and $\alpha_i : (\tilde{G}, \pi) \to (H, \alpha)$ are morphisms where $\alpha_1(x) = (x, 1)$ and $\alpha_2(a) = (x, x\tilde{G}')$. By uniqueness, $\alpha_1 = \alpha_2$, hence $\tilde{G} = \tilde{G}'$. Thus $\tilde{G}$ is perfect and so $G = \pi(\tilde{G})$.

Theorem 13: Let G be perfect and H, π be a central extension of G then $H = ker(\pi)H'$ with H' perfect.

Proof: $\pi : H \to G$, $\pi(H') = \pi(H)' = G' = G$ and $ker(\pi) \leq \mathbb{Z}(H)$. $H/H^2 = \mathbb{Z}(H/H^2) = H'/H^2$ is abelian and $H' = H^2$ so H' is perfect.

Theorem 14: G possesses a universal central extension iff G is perfect. If $(\tilde{G}, \pi)$ is a universal central extension then $ker(\pi)$ is called the *Schur multiplier*.

Proof: $\rightarrow$ is easy. For the converse, suppose G is perfect $g \mapsto \overline{g}$ is a bijection, F the free group on the symbols of G, $\Gamma = \{\overline{xyx}^{-1}\overline{y}^{-1}$. $M = \langle\Gamma\rangle \lhd F$, $\Delta = \{[w, z], w \in \Gamma, z \in G\}$, $N = \langle\Delta\rangle \lhd F$. $N = [M, F] \lhd M$, $M/N \leq \mathbb{Z}(F/N)$.. $\exists \pi : F/N \to G$ $\pi(\overline{x}N) = x$, $ker(\pi) \leq \mathbb{Z}(F/N)$. Now let H, σ be any central extension. $w = h(x)h(y)H(xy)^{-1} \in ker(\sigma)$. $ker(\sigma) \leq C_H(h(z))$ and $[w, h(z)] = 1$. $\tilde{G} = (F/N)'$ and $F/N = ker(\pi)\tilde{G}$; further, $\tilde{G}' = \tilde{G}$. $(\tilde{G}, \pi)$ is a universal central extension.

Note: Quasisimple groups are exactly the central extensions of simple groups. $H_2(G, \mathbb{Z}) = \frac{(R \cap F')}{[F,R]}$, further, if Q is perfect then $F'/[F, R]$ is a cover of Q. $SL_k(p)$ is a central extension of $PSL_k(p)$.

Theorem 15: Let (H, α) be a central extension of a group G and (K, β) is a perfect central extension of H then $(K, \alpha\beta)$ is a perfect central extension of G.

Proof: $\alpha\beta : K \to G$ is surjective. Let $x \in ker(\alpha\beta)$ and $y \in K$. $\beta(x) \in ker(\alpha)\mathbb{Z}(H)$, so $\beta([x, y]) = [\beta(x), \beta(y)] = 1$ and $[x, y] \in ker(\beta) \leq \mathbb{Z}(K)$. Thus $[ker(\alpha\beta), K, K] = 1$ so $ker(\alpha\beta) \leq \mathbb{Z}(K)$.

Theorem 16: Let (H, α) and (K, β) be central extensions of G with K with K perfect and $\gamma : (H, \alpha) \to (K, \beta)$ a morphism of central extensions, then (H, α) is a central extension of K. central extension of H then $(K, \beta\alpha)$ is a perfect central extension of

Proof: $\gamma : H \to K$ is a homomorphism with $\alpha = \beta\gamma$. $ker(\gamma) \leq \mathbb{Z}(H)$ so all we have to show is that α is surjective. $K = \gamma(H)ker(\beta)$. $ker(\beta) \leq \mathbb{Z}(H)$, $\gamma(H) \lhd K$ and $K/\mathbb{Z}(H)$ is abelian and thus $K = \gamma(H)$ is perfect.

Theorem 17: Let $\tilde{G}$ be the covering group of a perfect group G and let (H, α) be a perfect central extension of $\tilde{G}$, then α is an isomorphism.

Proof: $\pi : \tilde{G} \to G$ be the universal covering. By previous result, $H(\pi\alpha)$ is a perfect central extension of G. By universality, $\exists \beta : (\tilde{G}, \pi) \to (H, \pi\alpha)$. By uniqueness, $\pi\alpha\beta = \pi$, $\alpha\beta = 1$ and $\beta : \tilde{G} \to H$ is an injection. By previous result, β is surjective. Thus β is an isomorphism, $\alpha\beta = 1$, $\alpha = \beta^{-1}$ is an isomorphism too.

Theorem 18: Let G be perfect and $(\tilde{G}, \pi)$ the universal central extension of G and (H, σ) a perfect central extension of G. Then: (1) There exists a covering $\alpha : \tilde{G} \to H$ with $\pi = \alpha\sigma$; (2) $(\tilde{G}, \alpha)$ is the universal central extension of H; (3) The Schur multiplier of H is a subgroup of the Schur multiplier of G; (4) if $\mathbb{Z}(G) = 1$ then $\mathbb{Z}(\tilde{G})$ is the Schur multiplier of G and $\mathbb{Z}(H) \cong ker(\pi)/ker(\alpha)$ is the quotient of the Schur multiplpier of G by the Schur multiplier of H.

Proof: By the universal property, $\exists \alpha : (\tilde{G}, \pi) \to (H, \sigma)$. α is a covering by previous result. Let $(\tilde{H}, \beta)$ be the universal covering of H. By the universal property, $\exists \gamma : (\tilde{H}, \beta) \to (\tilde{G}, \alpha)$. By previous result, γ is an isomorphism so (2) holds. (3) and (4) are routine.

Theorem 19: Let G be a group with $G/\mathbb{Z}(G)$ finite then G' is finite.

Proof: Let $n = |G/\mathbb{Z}(G)|$, $z \in \mathbb{Z}(G)$, $g, h \in G$. $[g, hz] = [g, h] = [gz, h]$ so the set Δ of commutators has order $\leq n^2$.
Claim: If $g \in G'$ then $g = x_1 x_2 \dots x_m$, $x_i \in \Delta$ then $m \leq n^3$. This and the previous statement proves the theorem.
Proof of Claim: Pick expression of minimal length, m. If $m > n^3$ then, since $|\Delta| \leq n^2$, $\exists d \in \Delta$ with $\Gamma = \{i : x_i = d\}$ of order $k > n$. $x_i x_{i+1} = x_{i+1} x_i^{x_{i+1}} \, x_i^{x_{i+1}} \in \Delta$ and $\Gamma = \{1 \leq i \leq n\}$. Now it STS, d^{n+1} is a product of n commutators which contradicts the minimality of m. Let $d = [x, y]$, $|G/\mathbb{Z}(G)| = n$, $d^n \in \mathbb{Z}(G)$ so $d^{n+1} = (d^n)^x d = (d^{n-1})^x d^x d = (d^x)^{n-1}[x^2, y]$ so d is a product of n commutators.

Theorem 20: Let G be a perfect finite group then the universal covering group of G and the Schur multiplier are both finite.

Proof: Follows from previous result.

Theorem 21: Let (H, σ) be a perfect central extension of a finite group, G, and M the Schur multiplier of G, p, a prime and $P \in S_p(H)$ then $P \cap ker(\sigma) \leq \Phi(P)$.

Proof: By looking at $H/(\Phi(P) \cap ker(\sigma)$, we can assume $\Phi(P)ker(\sigma) = 1$ and show $X = P \cap ker(\sigma) = 1$. $\overline{P} = P/\Phi(P)$ is elementary abelian so $\exists \overline{Y} : \overline{YX} = \overline{P}$, $P = X \times Y$ and P splits by Gaschutz, H splits over X hence, H is perfect, $X \leq \mathbb{Z}(H)$, $X = 1$.

Theorem 22: Let (H, σ) be a perfect finite group and M the Schur multiplier of G, then $\pi(M) \subseteq \pi(G)$.

Proof: Follows from previous result.

Homological version: If $G > N$ and $H > K$ are normal subgroups isomorphic under ϕ, the pullback is (g, h) where $gN = \phi(hK)$. (Q, K, θ) is trivial iff every extension realizing (Q, K, θ) is a central extension. There's a bijection between $H^2(Q, K, \theta)$ and central extensions.

Theorem 23: Assume G is perfect then a central extension (E, ϕ) of G is universal iff (a) E is perfect and (b) all central extensions of E are trivial. In that case, $1 \to R \to F \to G \to 1$, F, free and $E = [F, F][F, R] \to [F, F]/R = G$.

7.2 Miscellaneous Central Extensions

Definition: If K and Q are groups, G is an *extension* of K by Q if $\exists K_1 \cong K$, $K_1 \lhd G$ and $G/K_1 \cong Q$. Let $\pi : G \to Q$ be a surjection. A *lifting* of Q is a map $l : Q \to G : \pi(l(x)) = x$. *Data:* (K, Q, θ), K, abelian, $\theta : Q \to Aut(K)$, for every transversal $l : Q \to G$. G realizes (K, Q, θ) if G is an extension of K by Q, if $\forall : Q \to G$ with $xa = \theta(x)(a) = l(x) + a - l(x)$.

Definition: Let $1 \to K \to G \to Q \to 1$, $l(x)$ are transversals. f is a cocycle if $l(x) + l(y) = f(x, y) + l(xy)$, $f(y, 1) = 0 = f(1, x)$ and $xf(y, z) + f(x, yz) = f(x, y) + f(xy, z)$. f is a *factor* set.

Theorem: Let G be an extension if K by Q, $l : Q \to G$, a transversal. K, abelian, $\theta : Q \to Aut(K)$ then $\theta(x) : a \to l(x) + a - l(x)$. If l_1 is another transversal $l(x) + a - l(x) = l_1(x) + a - l_1(x)$. This gives rise to the a cocycle $xf(y, z) + f(x, yz) = f(xy, z) + f(x, y)$.

Proof: Define $[G_f]$ by $(a, x) * (b, y) = (a + xb + f(x, y), xy)$. We can prove identity, inverse and, using the cocycle identity we get associativity.

Theorem: Let G be an extension, l, l' are transversals, $l(1) = 0 = l'(1)$ giving rise to f, f', $h : Q \to Q$ with $h(1) = 0$ such that $f'(x,y) - f(x,y) = xh(y) = h(xy) + h(x)$.

Proof: If $l'(x) = h(x)+l(x)$, $l'(x)+l'(h) = h(x)+l(x)+h(y)+l(y) = h(x)+xh(y)+f(x,y)+l(xy) = h(x) + xh(y) + f(x,y) - h(xy) + l'(xy)$ and $f'(x,y) = h(x) + xh(y) + f(x,y) - h(xy)$.

Definition: Under the conditions of the previous theorem, the extensions G_f and $G_{[}f']$ are called *equivalent*. Define $Z^2(K,Q,\theta)$ as the set of cocycles under addition. Given (K,Q,θ), $g : Q \times Q \to K$ is a *coboundary*, if $g(x,y) = xh(y) - h(xy) + h(x)$, the set of co-boundaries is denoted $B^2(K,Q,\theta)$. $H^2(K,Q,\theta) = Z^2(K,Q,\theta)/B^2(K,Q,\theta)$. If G and G' realize (K,Q,θ), they are equivalent iff $f' - f \in B^2(K,Q,\theta)$ by the theorem above.

Theorem: Let G and G' be extensions realizing(K,Q,θ) are equivalent if $\exists \gamma : G \to G'$ making the diagrams $1 \to K \to G \to Q \to 1$ and $1 \to K \to G' \to Q \to 1$ commute.

Definition: An extension of K by Q is central iff $K \subseteq \mathbb{Z}(G)$. Q is a finite group U is a *cover* of Q is an extension of K by Q and $K \leq U'$. A *projective representation* of a group Q is a homomorphism $\tau : Q \to PGL_n(\mathbb{C})$. We say U has the *projective lifting property* if every projective representation of Q can be lifted to U.hi (i.e.- $\tau : Q \to PGL_n(\mathbb{C})$ lifts to $\overline{\tau} : Q \to GL_n(\mathbb{C})$.) If Q is a group then a *cover* (or *representation group*) of Q is a central extension of U of K by Q (for some abelian K) with the projective lifting property and $K \leq U'$.

Schrier There is a bijection from $H^2(K,Q,\theta)$ to E, the set of all equivalence classes of extensions realizing (K,Q,θ) taking 0 to the semi-direect product. $H^2(K,Q,\theta) = 0$ iff every extension realizing (K,Q,θ) is a semi-direct product. $\phi : H^2(K,Q,\theta) \to E$ by $\phi(f + B^2(K,Q,\theta)) = G_f$.

Definition: $M(Q) = H^2(K, C^\times, \theta = 1)$. Note under these circumstances, $f(1,y) = 0 = f(x,1)$ and $f(x,y)f(xt,z)^{-1}f(x,yz)f(x,y)^{-1} = 1$.

Theorem: If Q is finite, $M(Q)$ is a finite abelian group, $exp(M(Q)) \mid |Q|$.

Proof: Define $sigma(x) = \prod_z f(x,z)$. From cocycle identity, $\sigma(y)\sigma(xy)^{-1}\sigma(x) = f(x,y)^n$, $n = |Q|$. For $x \in Q$, define $h : Q \to \mathbb{C}$ by $h(1) = 1$ and $h(x)$ an nth root of $\sigma(x)^{-1}$. $g(x,y) = f(x,y)h(y)h(xy)^{-1}h(x)$, $f \sim g$ and $g(x,y)^n = 1$, $f] \in M(Q)$ determines $g : q \times Q \to \mathbb{Z}_n$ and there are only finitely many such g.

Theorem: Every finite group Q has a cover U which is a central extension of $M(Q)$ by Q.

Theorem: If $Q = F/R$ where F is free, $M(Q) = (R \cap F')/[F,R]$.

Theorem: If $\nu : U \to Q$ is a central extension $ker(\nu) = K$ and Q is perfect then U' is perfect and $|nu_{U'} : U' \to Q$ is surjective.

Theorem: If Q is perfect, $Q = F/R$, $M(Q) = (R \cap F')/[F,R]$ and $F'/[F,R]$ is a cover.

Theorem: $U = F'/[F,R]$ is a universal central extension.

Chapter 8

Solvable Groups

8.1 Schur-Zassenhaus

Schur-Zassenhaus Theorem: Let G be a finite group, $N \lhd G$ with $(|N|, |G:N|) = 1$. Suppose further that either N or G/N is solvable. Then G splits over N; that is, $\exists Q < G$ such that $G = QN$. Further, G is transitive on N complements, Q.

Proof of existence: By induction on $|G|$, suppose it holds for all groups of order $< |G|$. Put $|G| = nm$, $(m,n) = 1$, $N \lhd G$ and $|N| = n$. If $\exists K \leq G : |K| = m$ then the theorem is true. For the remainder of the proof, put $P \in S_p(N)$.

Claim 1: Either $P \lhd N$ or the theorem holds by induction.
Proof of Claim 1: If first condition does not hold, $G = N_G(P)N, N_N(P) = N_G(P) \cap N \lhd N_G(P)$ and $m = |G/N| = |N(P)N/N| = |N_G(P)/(N_G(P) \cap N)| = |N_G(P)/N_N(P)|$. Then $N_G(P)$ has a normal Hall group $N_N(P)$ so by induction $\exists K \subseteq N_G(P)$ with $|K| = m$ and $N_N(P)K = N_G(P)$, so $NK = G$.

Claim 2: Either $P = N$ or the theorem holds by induction.
Proof of Claim 2: If first condition does not hold, $|(G/P)/(N/P)| = m$ so $\exists L/P : (N/P)(L/P) = G/P$ and $|L| = m|P|$, $|L \cap N| \mid (|L|, |N|)$. But $(m, |N|) = 1$ so $L \cap N \subset P$ and $L < G$ and $\exists K \subset L : |K| = m$.

Claim 3: Either $P = N$ is abelian or the theorem holds by induction.
Proof of Claim 3: If first condition does not hold, $1 \neq Z = \mathbb{Z}(N)$ *char* $N \lhd G$ and $|(G/Z)/(N/Z)| = m$ so $\exists L/Z : (L/Z)(N/Z) = (G/Z)$. Then $L \cap N = Z, L < G$ and $(|Z|, |L/Z|) = 1$ and L and hence G has the desired subgroup K.

By claims 1-3, we need only prove the result for $P = N \lhd G$, P abelian.
Proof in remaining case: Let $\overline{G} = G/N$. If t, u are two elements in the same G-coset of N. Then $t^{-1}u \in N$ for all such t, u so $tnt^{-1} = unu^{-1}, \forall n \in N$. Thus $\overline{G}$ acts on N - i.e. $\overline{G} \subset Aut(N)$. Define ${}^t x = txt^{-1}, t \in G, x \in N$. Select a transversal $\{t_h | h \in \overline{G}\}$. $t_{h_1h_2}^{-1} N = (t_{h_1h_2}N)^{-1} = (h_1h_2)^{-1} = {h_1}^{-1}{h_2}^{-1}, \forall h_1, h_2 \in \overline{G}$, so $t_{h_1}t_{h_2}t_{h_1h_2}^{-1} \in N$. Define $f : G \times G \to N$ by $f(h_1, h_2)t_{h_1h_2} = t_{h_1}t_{h_2}$. Since $t_{h_1}(t_{h_2}t_{h_3}) = (t_{h_1}t_{h_2})t_{h_3}$, we get ${}^{h_1}f(h_2, h_3) + f(h_1, h_2h_3) = f(h_1, h_2) + f(h_1h_2, h_3)$. Put $m = |\overline{G}|$. If $\exists c : \{t_{h_1}, \ldots, t_{h_m}\} \to N : f(h_1, h_2) = c(h_1h_2) - c(h_1) - {}^{h_1}c(h_2)$, then $c(h_1h_2)t_{h_1h_2} =$

$c(t_1)t_{h_1}c(t_2)t_{h_2}$, this is an isomorphism whose image satisfies the requirements for Q. *Define:* $e : G \to N$ by $e(h) = \sum_{k \in \overline{G}} f(h,k)$ and put $m = |\overline{G}|$. $mf(h_1,h_2) = -e(h_1h_2) + e(h_1) + {}^{h_1}e(h_2)$. Since $(m, |N|) = 1$, $\frac{x}{m}$ is well defined for $x \in N$ and $c(x) = \frac{-1}{m}e(x)$ satisfies the desired properties.

Proof of conjugacy: Suppose $\overline{G} = G/N$ is solvable. Suppose π is the set of primes dividing $|N|$ and $m = |G : N|$. Let $H, K \leq G$ with $|H| = |K| = m$. Set $R = O_\pi(G)$ so that $O_\pi(G/R) = 1$. Let L/N be a minimal normal subgroup of G/N. Then L/N is an elementary abelian $p-$group for some $p \in \pi'$. $H \cap L \in S_p(L)$ and $S = (H \cap L) = (K \cap L)^g = K^g \cap L$. $S \lhd \langle H, K^g \rangle = J$. If $J = G$, $S \lhd J$ and $S \subseteq R$ but then L is a $p'-$group which is a contradiction, concluding the proof in this case. So $J \neq G$ and by induction K, K^g are J-conjugate.
Instead, suppose N is solvable. Again $|H| = |K| = m = |G : N|$. $HN'/N' \cong KN'/N'$ so $H^g \subseteq KN'$ and again by induction, $H^{gk} = K$.

8.2 Alternative proof of abelian case

Definition 1: φ is a crossed homomorphism if $\varphi(xy) = \varphi(x)^y\varphi(y)$. Fix $n \in N$ and define $\varphi : g \mapsto [g, n]$.

Lemma: If φ is a crossed homomorphism and $ker(\varphi) = K$ then (1) $\varphi(1) = 1$, (2) $K < G$, (3) $\varphi(x) = \varphi(y)$ iff $Kx = Ky$ and (4) $|\varphi(G)| = |G : K|$.

Proof: Routine calculation.

Definition 2: Let $\mathcal{T}$ be the set of transversals of N in G. If $S, T \in \mathcal{T}$, define $d(S,T) = \prod_{s=t \,(\mathrm{mod}\ N)} s^{-1}t$.

Lemma: If N is a normal abelian subgroup of G and $S, T, U \in \mathcal{T}$ then (a) $d(S,T)d(T,U) = d(S,U)$, (b) $d(S,T)^g = d(Sg, Tg)$, and (c) $d(S, Sn) = n^{|G:N|}$, $n \in N$.

Proof: Let $T \in \mathcal{T}$ and $\theta(g) = d(T, Tg)$ then θ is a crossed homomorphism. $n \mapsto n^{|G:N|}$ is a permutation of N and $ker(\theta)$ is a complement. Finally, we show $K^n = H$. It suffices to show $K^n \subseteq H$ of $\theta(k^n) = 1$. $m = d(K,T)^k = d(Kk, Tk) = d(K, Tk) = d(K,T)d(T, Tk) = m\theta(k)$. Thus $1 = (m^k)^{-1}m\theta(k) = (m^k)^{-1}\theta(k)m$ so $\theta(k^n) = (m^{-1})^k\theta(k)m$.

Abelian Schur-Zassenhaus Theorem: Let $N \lhd G$, N, abelian and $(|N|, |G : N|) = 1$ then N is complemented in G and all complements are conjugate.

Proof: Fix a transversal, T for N in G and define $\theta(g) = d(T, TG)$. θ is a crossed homomorphism. For $n \in N$, $\theta(n) = n^{|G:N|}$ and by coprimality, $x \mapsto x^{|G:N|}$ is a permutation of the elements of N. Let $H = ker(\theta)$. $H < G$ by the foregoing and $|H| = |G : N|$; this shows H is a complement.

Let K be an arbitrary complement for N in G. K is a transversal. Let $m = d(K,T) \in N$. $\exists n \in N : \theta(n) = m$ and so $\theta(n^{-1}) = m^{-1}$. It suffices to show $K^n \subseteq H$ which is equivalent to $\theta(k^n) = 1, \forall k \in K$. If $k \in K$, $m^k = d(K,T)^k = d(Kk, Tk) = d(K, Tk) = d(K,T)d(T, Tk) = m\theta(k)$, so $1 = (m^k)^{-1}\theta(k)m$ and $\theta(k^n) = \theta(n^{-1}k)^n\theta(n) = \theta(n^{-1}k)m = \theta(n^{-1})^k\theta(k)m = (m^k)^{-1}\theta(k)m = 1$ and we're done.

8.3 Philip Hall's Theorem

Hall's Theorem: Let G be a solvable group and π a set of primes then (i) G has a π-Hall subgroup, (ii) G acts transitively on its Hall π-subgroups via conjugation, (3) any π subgroup is contained in a Hall π subgroup.

Proof: By induction on $|G|$. Let N be a minimal normal subgroup of G then $1 \neq N \lhd G$. N is elementary abelian for some p and $p \mid mn$. If $p \mid m, |G/N| = \frac{m}{p}$ and $\exists L : |L/N| = \frac{m}{p}, |L| = m$ and we're done. If $p \mid n, \exists H : |H/N| = m, |H| = |N|m$. If $|H| < |G|$, we're done by induction. Otherwise $H = G, N \lhd G, |N| = n, |G : N| = m$ and $(m, n) = 1$ so by Schur-Zassenhaus, $\exists K : |K| = m$.

Theorem 1: Let G be a finite group possessing a Hall π' subgroup for each p, then G is solvable.

Proof: This is proved below.

Theorem 2: If A is a maximal abelian normal subgroup of P and $Z = \Omega_1(A)$, then (1) $(C_P(A/Z) \cap C(Z))^{(1)} \leq A$, and (2) if p is odd $\Omega_1(C_P(Z)) \leq C_P(A/Z)$.

Proof: Let $C = C_G(A)$, $A \leq C \lhd G$. $(C_P(A/Z) \cap C(Z)^{(1)} \leq C(A) = A$. Let $p \neq 2$. $|x| = p$, $x \in C_G(Z)$. $X = \langle x, A \rangle$. Let $Y = \langle X, C_A(\langle X, Z \rangle)\rangle/Z$, $cl(Y) \leq 2$. $W = \Omega_1(Y)$ has exponent p and thus $W = \langle X, Z \rangle$ but W *char* Y so $N_X(Y) \leq N_X(W) = Y$ so $X = Y$.

Definition 3: $P_1, \ldots, P_n$ is a *Sylow System* if $\forall i, P_i \in S_{p_i}(G)$, $P_i P_j = P_j P_i, \forall i \neq j$ and $\prod_i P_i = G$. $\Omega_1(P) = \langle x \in P : x^{p^i} = 1 \rangle$.

Theorem 3: The following are equivalent:
(1) G is solvable.
(2) Every π-subgroup of G is contained in an S_π subgroup of G.
(3) G has a Hall $S_{p'}$ subgroup for each p.
(4) G has a Sylow System.

Proof:

$1 \to 2$ (Existence): By induction on $|G|$. Let K be a π-subgroup of G and U be a non-trivial minimal normal subgroup of G. U is an elementary abelian p-group. KU/U is a π-subgroup of G/U. If $KU = G$ we are done by induction, so, we can assume $KU \subseteq L$ and L/U is an S_π subgroup of G/U. If $p \in \pi$, again we are done by induction. So we assume, $p \notin \pi$. U is a normal Hall subgroup of L so $\exists S < L : SU = L, S \cap L = 1$. S is a Hall subgroup of L and hence of G. K and $K \cap SU$ are complements for U in KU, so $\exists g \in U : K = (K \cap SU)^g$ and $K \subseteq S^g$ is an S_π-subgroup of G.

$1 \to 2$ (Conjugacy): Again, the proof is by induction on $|G|$. Let $S, T \in S_\pi(G)$ and U be a non-trivial minimal normal p-subgroup of G. SU/U and TU/U are conjugate in G/U by induction so $\exists g \in G : (SU/U)^g = TU/U$. If $p \in \pi$, $SU = S$ and $TU = U$ so $S^g = T$ and we're done. If $p \notin \pi$, $S^g U = TU$ and S^g and T are normal p-complements to U in TU so $\exists u \in U : S^{gu} = T$. This completes the proof.

$2 \to 3$ is clear.

$3 \to 4$:
Claim: If $(|G : H|, |G : K|) = 1$, then $|G : H \cap K| = |G : H||G : K|$.
Proof of claim: $|G : H \cap K| = |G : H| \cdot |H : H \cap K| = |G : H||G : K||K|$ and $|K| = 1$.

Let $G_{p_i'}$ be an $S_{p_i'}$-subgroup of G, put $G_{\pi'} = \bigcap_{p \in \pi} G_{p_i'}$.

Claim: $G_{\pi'}$ is a Hall $S_{\pi'}$-subgroup of G.
Proof of claim: By induction on $|\pi|$. $G_{\pi'} = G_{(\pi\setminus\{p_1\})'} \cap G_{p_1'}$. Applying the previous claim, we get the result.

Put $G_{p_i} = \bigcap_{j\neq i} G_{p_j'}$ then G_{p_i} is a p_i-Sylow subgroup of G and $G_{p_j}G_{p_i} = G_{(\pi\setminus\{p_i,p_j\})} = G_{p_i}G_{p_j}$.

$4 \to 1$: Let $P_1, P_2, \ldots, P_n$ be a Sylow System. Proof goes by induction on $|G|$.

For $n = 1$, G is nilpotent, hence solvable.
For $n = 2$, this follows from Burnside's Theorem.
For $n \geq 3$, set $H = P_1P_3 \ldots P_n$, $H \neq G$ and H is solvable by induction. Let N be a minimal normal subgroup of H, N is a p_i-group, $i \geq 2$. $G = HP_1$. Let $g = hx, g \in G, h \in H, x \in P_1$. $N \subseteq P_i$ by Sylow and NP_i is a group. $N^g = N^{hx} = N^x$, so $N^x \subseteq P_1P_i$. Put $M = \langle N^g : g \in G\rangle \leq P_1P_i$. $M \lhd G$ and M is solvable. By induction, so is G/N and so G is solvable.

Note on Sylow systems: If $P_1, \ldots, P_n$ and $Q_1, \ldots, Q_n$ are two Sylow Systems, $\exists x \in G : P_i^x = Q_j$. Further, if $H \subseteq G$, G, solvable, and $P_1, \ldots, P_n$ is a Sylow System for H then there is a Sylow system $Q_1, \ldots, Q_n$ for G such that $Q_i \cap H = P_i$.

Theorem 4: Suppose A is a group of operators on a solvable group, X: $(|X|, |A|) = 1$, then (1) Any A-invariant π-subgroup of X is contained in an A-invariant Hall π subgroup of H; (2) any two A-invariant Hall π subgroups of X are conjugate by an element of $C_X(A)$.

Proof: By induction on $|X|$. Let N be a minimal normal subgroup of AX. N is elementary abelian. Set $\overline{X} = X/N$. $\exists \overline{H}$ a Hall subgroup of $\overline{H}$. Let H be the inverse image under the natural homomorphism. If $p \in \pi$, H is an A-invariant Hall subgroup. If $p \notin \pi$, $|X : H|$ is a π' number and any Hall π subgroup of H is a Hall π subgroup of X and so by induction, we can assume $X = H$. By Schur, $\exists H_0 : X = H_0N, N \cap H = 1$. By Frattini, $AX = XN_{AX}(H_0)$ and $N_{AX}(H_0) = A_1N_{AX}(H_0), A_1 \cap X = 1$. So $A_1X = AX$ and $\exists x : A_1^x = A$, $A \subseteq N(H_0^x)$. Thus $A^x, A \subseteq N(H_0^x)$ and $\exists y : A^{xy} = A_1$ but $[xy, A] \subseteq A \cap X$ so $xy \in C_X(A)$ and we're done.

Theorem 5: Suppose V is a non-cyclic abelian group r-group of operators on a p-constrained group X. For $r \neq p$ both prime, $\bigcap_{v\in V^\#} O_{p'}(C_X(v)) \subseteq O_{p'}(X)$.

Proof: Put $\overline{X} = X/O_{p'}(X)$, V-invariant. $C_{\overline{X}}(V) = \overline{C_X(V)}$ and we may assume $O_{p'}(X) = 1$. Let $M \lhd X$. $C_M(V) = M \cap C_X(V) \lhd C_X(V)$ so $C_M(V) \subseteq O_p(C_V(X))$. $[C_M(V), Q] = 1, \forall v \in V^\#$ so $[M, Q] = 1$ and $Q = 1$.

Theorem 6: Let $L = \langle x \in G, x \in p'(G)\rangle$ and $M = G'L$, $S \in S_p(G)$ then (1) G/L is a p-group; (2) $G = SM$, $S \cap M = S \cap G'$; (3) $G/M = S/(S \cap G')$; (4) G has a factor group of order p' iff $S \cap G' \not\subseteq S$.

Proof:
(a) Let $S \in S_p(G)$. By counting, observe $SL = G$. L *char* G so $(SL)/L = G/L \cong S/(S \cap L)$ which is a p-group.
(b) As in (a) $G = SL = S(G'L) = SM$ clearly, $S \cap G' \subseteq S \cap M$. Suppose $x \in M$ and $\overline{x} = xL/L$. $\overline{x}$ is generated by p'-elements in the abelian group $\overline{M}$ so $\overline{x}$ is a p'-element but since $x \in S$ has p order so$\overline{x} = 1$ and $x \in G'$ but $G/M = (SM)/M \cong S/(S \cap M) = S/(S \cap G')$ which proves (c).
(d) Suppose $S \cap G' \not\subseteq S$ then $G/M = \overline{G} \cong S/(S \cap G')$ is a p-group. Let $\overline{H} \lhd \overline{G}$ and let N be the inverse image of $\overline{H}$ then G/N has order p. Conversely, if G/N have order p then $G' \subseteq N$ and every p'-element of G is in N so $M \subseteq N$ thus $S/(S \cap G') \cong (SM)/N = (SN)/N \cong G/N$ since $S/(S \cap G')$ has order p. $S \cap G' \neq S$.

Corollary: G has a factor group of order $p^\alpha, \alpha \geq 1$ iff $S \cap G \not\subseteq S$.

8.4 Hall-Higman

Hall-Higman 1.2.3: Let G be π-solvable and $O_{\pi'}(G) = 1$, then $C_G(O_\pi(G)) \subseteq O_\pi(G)$.

Proof: Set $H = C_G(O_p(G))O_p(G)$. $H \lhd G$ and $O_p(G) = O_p(H)$. Suppose $H > O_p(G)$ then $H/O_p(G)$ is p-solvable and since $O_p(G) = O_p(H)$, if K is the inverse image of $O_{p'}(H/O_p(H)) > O_p(H)$. $O_p(H) \in S_p(K)$ and $K \lhd G$. By Schur-Zassenhaus, $K = LO_p(G)$, L *char* K. If $l \in L$, $[l, O_p(G)] \subseteq O_p(G) \cap K = 1$. Hence $O_{p'}(G) = K > 1$, contradiction!

Hall-Higman: If G is p-solvable, $X = O_{p'}(G)$, $P \in S_p(G)$ with $XP/X = O_p(G/X)$, then $H = G/XP$ acts as faithful p-solvable group of linear operators on $V = P/\Phi(P)$ and H has no non-trivial normal p-subgroups.

8.5 Maximal subgroups of solvable groups

Theorem 7: Let M be a maximal subgroup of a solvable group G and set $L = \bigcap_{x \in G} M^x$. Set $\overline{G} = G/L$, $\overline{F} = F(\overline{G})$, then either $\overline{F} = 1$ or the following holds: (1) $\overline{F}$ is a minimal normal subgroup of $\overline{G}$, (2) $\overline{F}$ is an elementary abelian p-subgroup for some p; (3) $C_{\overline{G}}(\overline{F}) = \overline{F}$; (4) $\overline{F} \cap \overline{M} = 1$; (5) $|\overline{G} : \overline{M}| = p^n$.

Proof: Assume $\overline{F} \neq 1$ so $\mathbb{Z}(\overline{F}) \neq 1$. Let $\overline{P} \neq 1$ be an S_p subgroup of $\Omega_1(\mathbb{Z}(\overline{F}))$ and $\overline{P} \lhd \overline{G}$, $\overline{P}$, elementary abelian. *Claim:* $\overline{G} = \overline{PM}$.
Proof of Claim: Since $\overline{M}$ is maximal, the result will follow if $\overline{P} \not\subseteq \overline{M}$. We show $\overline{M}$ has no non-trivial normal subgroup. If $\overline{N} \lhd \overline{M}$ $\overline{N} \subseteq \overline{M}^x$ whence $N \subseteq \bigcap_{x \in G} M^x = L$. So $\overline{G} = \overline{PM}$.

Now set $\overline{C} = C_{\overline{G}}(\overline{P})$, then $\overline{F} \subseteq \overline{C}$ and $\overline{C} \lhd \overline{G}$ and so $\overline{C} \cap \overline{M} \lhd \overline{M}$. But since $\overline{G} = \overline{PM}$. $\overline{P}$ centralized $\overline{C} \cap \overline{M}$ $\overline{C} \cap \overline{M} \lhd \overline{G}$ and $\overline{C} \cap \overline{M} = 1$. Since $\overline{P} \subseteq \overline{F} \subseteq \overline{C}$ and we have $\overline{G} = \overline{CM}$ with $\overline{C} \cap \overline{M} = \overline{P} \cap \overline{M} = 1$. Then $|\overline{G}| = |\overline{C}||\overline{M}| = |\overline{P}||\overline{M}|$ so $\overline{P} = \overline{F} = \overline{C}$ and this gives 1-4.

Theorem 8: If M is a maximal subgroup of a solvable group G, $|G : M| = p^n$.

Proof: $\overline{F} \neq 1$ so conclusion (5) from the previous result holds.

Theorem 9: In a solvable group the factors of a chief series are elementary abelian of prime power order.

Proof: Let $H \supseteq K$ be a term in the series. Since G is solvable, $H' \subseteq K$ so H/K is abelian. Suppose there are elements of order q and p with $q \neq p$ then the p elements H/K form a characteristic subgroup (since H/K is abelian) which lies properly between H/K and 1. This is a contradiction.

Chapter 9

Specific Groups

9.1 Classical Groups:

Theorem 1: A_n is simple for $n > 4$.

Proof: Suppose $1 \neq H \lhd A_n$.

Claim 1: If $(abc) \in H$ for any $a, b, c, H = A_n$.
Without loss, $(abc) = (123)$. Put $g = (12k), k > 3$. $(123)^g = (12k)$ and these 3-cycles generate A_n.
Claim 2: H contains a 3-cycle.
Let $x \in H$ be the element that moves the fewest points other than the identity. x must move at least 3 points or it would not be in A_n. The cycle structure of x must be one of the following: (1) $(12)(34)$, (2) $(12)(34)(56)(78)\ldots$, (3) $(123)(456)\ldots$, (4) $(12345...)(k, k+1, \ldots)$, (5) (123). Note that all cycles must have the same length otherwise by raising x to the power of the length of the shortest cycle yields an element moving fewer points. In case 1, put $g = (125) \in A_n$. $x^g x = (125)$, so H contains a 3 cycle in this case. In case 2, put $g = (123) \in A_n$. $x^g x = (13)(24)$ which moves fewer points than x contrary to the selection of x, so this can't happen. In case 3, put $g = (234) \in A_n$. $x^g x^{-1} = (12436)(5)$ which moves fewer elements than x so this can't happen. In case 4, put $g = (123)$; then $x^{-1}x^g$ fixes 3 and all elements $\geq k$ so it fixes more elements than x which can't happen. So only case 5 is possible.

Since H contains a 3-cycle by claim 1, it contains all of A_n.

Notation: $L_n(F)$ is the invertible linear transformations in a vector space of dimension n over the field F. $L_n(q) = L_n(F_q)$. $SL_n(F) = \{M \in L_n(F) : det(M) = 1\}$. A *transvection*, τ, is a matrix of the form $\begin{pmatrix} 1 & 0_{n-1} \\ v_{n-1} & I_{n-1} \end{pmatrix}$. Note that $\left[\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & x(a^2-1) \\ 0 & 1 \end{pmatrix}\right]$. Also note that $\tau(x) - x$ is a hyperplane.

There's another way to define transvections. Pick $1 \neq \phi \in \hat{V}$ and $v \in V : \phi(v) = 0$. The set $H = \{y : \phi(y) = 0\}$ is a hyperplane. A transvection can be defined by $\tau_{\phi,v}(x) = x + \phi(x)v$. Note that if $x \in H, \tau_{\phi,v}(x) = x$, since $\phi(v) = 0$, $\forall x \in V, \tau_{\phi,v}(x) - x = \phi(x)v$ and $\phi(phi(x)v)) = \phi(x)\phi(v) = 0$, so $\tau_{\phi,v}(x) - x \in H$. $\tau_{\phi,v}(\tau_{\phi,-v}(x)) = x$. in fact, if ϕ is given and $\phi(v_1) = 0 = \phi(v_2)$, $\tau_{\phi,v_1}(\tau_{\phi,v_2}(x) = \tau_{\phi,v_1+v_2}(x)$. Finally, let $\sigma \in GL_n(F)$, then $\sigma(\tau_{\phi,v}(\sigma^{-1}(x))) = \tau_{\phi\sigma^{-1},\sigma(v)}(x)$. The hyperplane for $\phi\sigma^{-1}$ is $\{y : \phi\sigma^{-1}(y) =$

$0\} = \{\sigma(x) : \phi(x) = 0\} = \sigma H$. Putting, $\psi = \phi\sigma^{-1}, H' = \sigma(H), v' = \sigma(v)$, we get $\sigma(\tau_{\phi,v}(\sigma^{-1}(x))) = \tau_{\psi,v'}(x)$. Going the other way, given H' and v', we can find $\sigma \in GL_n(F) : \sigma(H) = H', \sigma(v) = v'$ and thus a transvection is conjugate to any other transvection in $GL_n(F)$. In fact, if $n \geq 3$, all transvections are conjugate in $SL_n(F)$. All transvections have the same determinant and, furthermore, since $\tau_{\sigma,v_1}\tau_{\sigma,v_2} = \tau_{\sigma,v_1+v_2}$, that common determinant is 1. Commutators of transvections also have determinant 1 so the group generated by transvections in $GL_n(F)$ lies in $SL_n(F)$. Using Theorem 3 below, we see that the transvections actually generate all of $SL_n(F)$, for $n \geq 3$. By theorem 4 below, for $n \geq 3$, the commutator of two transvections is also a transvection and since all transvections are congugate, $SL_n(F)' = SL_n(F)$.

Returning to the matrix form above, we see that the stabilizer of e_1 consists of matricies of the form: $\begin{pmatrix} a_{11} & 0_{n-1} \\ \vec{a}_{n-1} & I_{n-1} \end{pmatrix}$. We will use this stabilizer in conjunction with Iwasawa's theorem to show $PSL_n(F)$ is simple for $n \geq 3$ or $|F| > 3$.

The following theorem is a simplification of Iwasawa's Theorem that is used to show the simplicity of the classical groups.

Theorem 2: (Iwasawa) Suppose G acts faithfully and primitively on a set Ω and $A \lhd G_a$ is abelian. Suppose further $\langle A^G \rangle = G$ and $G = G'$. Then G is simple.

Proof: Suppose $1 \neq N \lhd G$. N is not contained G_a for some a. Since G_a is maximal, $G = NG_a$ so $g = nh, n \in N, h \in G_a$. $gAg^{-1} = nAn^{-1}$, since $A \lhd G_a$, so $gAg^{-1} \subseteq NA$ so $G = \langle A^G \rangle = NA$. But $G/N = A/(A \cap N)$ is abelian so $G' \subseteq N$, however $G = G'$ so $N = G$.

Theorem 3: $SL_n(F)$ is generated by $T_{ij}(b) = I + b(\delta_{ik}\delta_{lj}), i \neq j, b \in F^*$ if $n > 2$. Note: $SL_n(F)$ is also generated by transvections. Note also that $T_{ij}(b)T_{ij}(-b) = I$.

Proof: Note that $det(T_{ij}(b)) = 1$. For $A \in SL_n(F), \exists P, Q \subseteq \langle T_{ij}(b) \rangle : PAQ = diag(d_1, d_2, \ldots, d_n)$ and $d_1 d_2 \ldots d_n = 1$. Also, $\begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \subseteq \langle T_{ij}(b) \rangle$.

Theorem 4: If $n > 2$ or F has more than 3 elements, $SL_n(F) = SL_n(F)'$.

Proof: STS $T_{ij}(b) \in SL_n(F)'$. If $n > 2$ then for $k \neq i, j$: $T_{ij}(b) = T_{ik}(b)T_{kj}(1)T_{ik}(-b)T_{kj}(-1) = T_{ik}(b)T_{kj}(1)T_{ik}(b)^{-1}T_{kj}(1)^{-1}$. If $|F| > 2$, $\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c(d^2-1) \\ 0 & 1 \end{pmatrix}$. Choose $d \neq 0, d^2 \neq 1$. Put $c = (d^2-1)^{-1}b$. This shows $T_{12}(b) \in SL_n(F)'$.

Theorem 5: Let $C_n(F) = \mathbb{Z}(SL_n(F))$, then $C_n(F) = \{\alpha I_n : \alpha^n = 1\}$.

Proof: Note that $GL_n(F)' \subseteq SL_n(F)$ since $GL_n(F)/SL_n(F)$ is abelian. If X commutes with $SL_n(F)$ it must commute with $T_{ij}(1)$, hence $C_n(F) = F^* I_n \cap SL_n(F)$ with $d^n = 1$.

Observation: $GL_n(F)$ and hence $SL_n(F)$ acts on $\mathbb{P}_{n-1}(F)$ whose elements are one dimensional subspaces of $A_n(F)$.

Theorem 6: $SL_n(F)$ is 2-transitive on $\mathbb{P}_{n-1}(F)$ if $n \geq 2$.

Proof: Suppose $Fx_1 \neq Fx_2$ and $Fy_1 \neq Fy_2$. Choose a base $x_1, x_2, \ldots, x_n$ and write $y_k = \sum_j a_{kj}x_j, k = 1, 2$. Add $n-2$ rows to the matrix (a_{ij}) to obtain a matrix with determinant 1. Let T be the linear transformation sending $x_k \to y_k$. If $n = 2$ and $det(A) = a \neq 0$, pick T as $x_1 \to y_1$ and $x_2 \to a^{-1}y_2$.

Theorem 7: $SL_n(F)_{e_1}$ contains an abelian normal subgroup A_{e_1} whose conjugates generate $SL_n(F)$.

Proof: The stabilizer of e_1 is matrix with $a_{11}, \ldots, a_{n1}$ as the first column with all entries of the first row (except possibly a_{11} equal to 0 and any A_{n-1} in the lower right hand corner with $a_{11}det(A_{n-1}) = 1$. Let A_{e_1} denote the matrices with $a_{11} = 1$ and $A_{n-1} = I_{n-1}$ then A_{e_1} is a normal abelian subgroup and $T_{21}(b) \in A_{e_1}$. By conjugating this element, we can get any $T_{ik}(b)$, so $SL_n(F) \subseteq \langle A_{e_1}^g \rangle$.

Theorem 9: $PSL_n(q)$ is simple for $n > 2$ or $q > 3$.

Proof: Apply the above theorem on simplicity to $SL_n(q)$ with the identified A_{e_1}.

Theorem 10: $|PSL_n(q)| = \frac{1}{(q-1)(n,q-1)}(q^n-1)(q^n-q)(q^n-q^2)...(q^n-q^{n-1})$, is simple if $n > 2$ or $q > 3$.

Proof: Let $v_1, \ldots, v_n$ be a base. For $T \in L_n(F_q)$, there are $q^n - 1$ ways to choose $T(v_1)$, $q^n - q$ ways to choose $T(v_2)$, ..., $q^n - q^{n-1}$ ways to choose $T(v_n)$. So $|L_n(F_q)| = (q^n-1)(q^n-q)(q^n-q^2)...(q^n-q^{n-1})$. $|SL_n(F_q)| = \frac{|L_n(F_q)|}{(q-1)}$. There are $(n, q-1)$ solutions in F_q of $d^n = 1$ so $|PSL_n(F_q)| = \frac{|SL_n(F_q)|}{(n,q-1)}$.

Bilinear Forms: $B(x, y)$. A quadratic form is $Q(x) : Q(ax) = a^2Q(x)$ and if $char(F) \neq 2$ the the quadratic form gives rise to the bilinear form $\frac{1}{2}Q(x+y) - Q(x) - Q(y)$. $U_B^{\perp_R} = \{v \in V : (v, u) = 0, \forall u \in V\}$. Matrix for $B(x, y)$ over the basis e_i is $b_{ij} = B(e_i, e_j)$. Bilinear form is *non-degenerate* if $U_B^{\perp_R} = U_B^{\perp_L} = 0$. Bilinear form is *symmetric* if $B(x, y) = B(y, x)$, *hermitian* if $B(x, y) = \overline{B}(y, x)$, and *alternating* if $B(x, y) = -B(y, x)$. If $b_{ij} = (e_i, e_j)$, the *discrimminant* of the bilinear form is $det(b_{ij})$. $\sigma \in L_n(F)$ is an *isometry* with respect to a bilinear form, B, if $B(x, y) = B(\sigma x, \sigma y)$. U is a *non-isotropic* subspace if $dim(U \cap U^{\perp}) = 0$.

Theorem 11: The following three conditions on a bilinear form, B, are equivalent: (1) $V^{\perp_R} = 0$, (2) $V^{\perp_L} = 0$, (3) the matrix of B relative to any basis is invertible.

Proof: Straightforward.

Theorem 12: Let B be a symmetric bilinear form on V over F, $char(F) \neq 2$, then there is a base $(u_1, u_2, \ldots, u_r, z_1, \ldots, z_{n-r})$ such that relative to this base, B has the form $diag(b_1, b_2, \ldots, b_r, 0, 0, \ldots, 0)$.

Proof: This uses the Lagrange reduction which works like this: If $B = 0$, we're done. Choose $u_i : Q(u_i) = b_i \neq 0$. In the inductive step, suppose $V_k = (u_1, u_2, \ldots, u_k)$ be a basis with $(u_i, u_j) = 0, i \neq j$ and $(u_i, u_i) = b_i$. Put $y = x - \sum_{i=1}^{k}(x, u_i)b_i^{-1}u_i$ then $y \in V_k^{\perp}$.

Theorem 13: If B is a non-degenerate bilinear form over V and $U \subseteq V$ is a subspace then $V = U \oplus U^{\perp}$.

Proof: Let $(u_1, \ldots, u_r)$ be a basis for U. Extend U to a basis for V by adding $(u_{r+1}, \ldots, u_n)$. If $(u_i, u_j) = a \neq 0, i \leq r, j > r$, replace u_j with $u'_j = u_j - \frac{a}{(u_i,u_i)}u_i$. This process can continue until we have a basis $(u_1, \ldots, u_r, u'_{r+1}, \ldots, u'_n)$ with the property that $(u_i, u'_j) = 0, i \leq r, j > r$. $\langle u'_{r+1}, \ldots, u'_n \rangle = U^{\perp}$.

Theorem 14: Any non-degenerate symmetric bilinear form on V over F, $char(F) \neq 2$ is equivalent to one with matrix $diag(1, 1, \ldots, 1, d)$, $d = Disc(B)$.

Proof: Use Lagrange diagonalization and take $b_1 = b_2 = \ldots = b_{n-1} = 1$, the last diagonal element must preserve the discrimanent and so must be d.

Theorem 15: (1) The following are equivalent: (i) V is a hyperbolic plane, (ii) V has hyperbolic pair (u, v) as a basis (i.e.- $(u, u) = 0 = (v, v), (u, v) = 1$), (iii) $disc(B) = (-1)(F^*)^2$, (2) any two hyperbolic planes are isometric, (3) any hyperbolic plane contains two one dimensional totally isotropic subspaces, (4) the rotation group of a hyperbolic plane is isomorphic to F^* and every improper transformation on V is a symmetry.

Proof:
(1) If V is a hyperbolic plane, $\exists 0 \neq u \in V : Q(u) = 0$ and since $V^\perp = 0$ and $\exists v \in V : (u, v) \neq 0$. Since $(u, u) = 0$, v is not a multiple of u. Hence (u, v) is a base. Replacing v by a multiple of v, we may assume $(u, v) = 1$. Moreover, if $a \in F$ then $Q(v + au) = Q(v) + a$ so if we replace v with $v - Q(v)u$, we have $Q(v) = 0$ and $(u, v) = 1$ so $(i) \to (ii)$. Assume (ii). The matrix that describes B, is -1. Hence the discriminant of B is $(-1)(F^*)^2$. We have a base (u_1, u_2) such that the matrix for B with respect to (u_1, u_2) is $diag(b_1, b_2)$ where $b_1 b_2 = -c^2 > 0, c \in F$. Let $x = cu_1 + b_1 u_2$, then $Q(x) = \frac{1}{2}c^2 b_1 + \frac{1}{2}b_1^2 b_2 = 0$. Hence V is a hyperbolic plane and we proved $(iii) \to (i)$.
(2) Any two hyperbolic planes have bases (x, y), (x', y') which are hyperbolic pairs. $u \mapsto u', v \mapsto v'$ is an isometry.
(3) Let (u, v) be a base which is a hyperbolic pair, then $Q(au+bv) = ab$. So $au+bv$ is isotropic iff either $a = 0, b \neq 0$ or $a \neq 0, b = 0$ then Fu and Fv are the only one dimensional totally isotropic subspaces of V.
(4) Let η be an orthogonal transformation of the hyperbolic plane V and let Fu and Fv be the two one dimensional totally isotropic subspaces. Then either $\eta(Fu) = Fu$ and $\eta(Fv) = Fv$ or $\eta(Fu) = Fv$ and $\eta(Fv) = Fu$. In the first case, $\eta(u) = au, \eta(v) = bv$ and $ab(u, v) = (\eta(u).\eta(v)) = (u, v)$ gives $ab = 1$ since $(u, v) \neq 0$. Hence $\eta(u) = au$ and $\eta(v) = a^{-1}v$ and η is a rotation. In the second case, $\eta(u) = av$ and $\eta(v) = bu$ and again, $b = a^{-1}$ and η is improper. For any $a \neq 0$, the linear maps $u \mapsto au, v \mapsto a^{-1}v$ and $u \mapsto av, v \mapsto a^{-1}u$ are rotations or improper. The map from F^* into the rotations is an isomorphism of $F^* \to O^+(V, Q)$. Finally, if η is improper, $\eta(u + av) = u + av$ and $\eta(u - av) = -(u - av)$ hence η is the symmetry S_{u-av}.

Theorem 16: An alternate non-degenerate bilinear form is equivalent to one in which the matrix is $diag(H, H, ..., H)$, where $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Proof: By induction. In inductive step, we have u_i, v_i with the properties $(u_i, v_i) = 1 = -(v_i, u_i)$ and $(u_i, u_i) = 0 = (v_i, v_i)$. Put $V_k = \langle u_1, v_1, \ldots, u_k, v_k \rangle$. $V_k \cap V_k^\perp = 0$. Let $y \in V$ then $y = x - \sum_{i=1}^k (x, v_i)u_i + \sum_{i=1}^k (x, u_i)v_i$ then $y \in V_k^\perp$ and we can show $V = V_k \oplus V_k^\perp$.

Witt's Cancellation Theorem: Let Q be a non-degenerate quadratic form and $char(F) \neq 2$ and suppose two subspaces, U_1 and U_2 are isometric, then $U_1^\perp$ and $U_2^\perp$ are isometric.

Proof: By induction on $dim(U_i)$. If $U_i = Fu_i$ and $Q(u_1) \neq 0$, we may assume $Q(u_1) = Q(u_2)$. $Q(u_1 \pm u_2) = 2Q(u_1) \pm (u_1, u_2)$, so either $Q(u_1 + u_2) \neq 0$ or $Q(u_1 - u_2) \neq 0$. Define $S_u : x \mapsto x - \frac{(x,u)}{(u,u)}u$. In the first case, $S_{u_1+u_2}(u_1 - u_2) = u_1 - u_2$ and $S_{u_1+u_2}(u_1 + u_2) = -(u_1 + u_2)$, so $(u_1 - u_2) \perp (u_1 + u_2)$ and a simple calculation shows $S_{u_1+u_2}(Fu_1)^\perp = (Fu_2)^\perp$ and $U_1^\perp$ is isometric to $U_2^\perp$. Now suppose the result is true for $dim(U_i) = n - 1$. Choose a non-isotropic $u_1 \in U_1$ and write $U_1 = Fu_1 \perp W_1$ and $U_2 = Fu_2 \perp W_2$. So $V = Fu_1 \perp W_1 \perp U_1^\perp = Fu_2 \perp W_2 \perp U_2^\perp$. Apply the one-dimensional case to show there is an isometry, η, from $W_1 \perp U_1^\perp$ to $W_2 \perp U_2^\perp$. The induction hypothesis applied to $W_2, \eta(W_1)$ shows $U_2^\perp$ is isometric to $\eta(U_1^\perp)$ which is in turn isometric to $U_1^\perp$.

Theorem 17: Let V be equipped with a non-degenerate form and U be a subspace such that $rad(U) = U \cap U^\perp \neq 0$. Write $U = rad(U) \oplus U'$ and let $z_1, \ldots, z_r$ be a base for $rad(U)$. U can be imbedded in

a non degenerate subspace $U \oplus W$ where W has a base $w_1, \ldots, w_r$ such that z_i, w_i is a hyperbolic pair, $H_i = Fz_i + Fw_i$, and $U \oplus W = U' \perp H_1 \perp \ldots \perp H_r$.

Proof: Let f be a linear function on U with $f(z_1) = 1, f(z_i) = 0, i \neq 1$ and $f(u') = 0, u' \in U'$. $\exists w_1 \in V : f(u) = (u, w_\cdot), u \in U$. Thus $(z_1, w_1) = 1, (z_i, w_1) = 0, i > 1$ and $(u', w_1) = 0, u' \in U'$. Replacing w_1 by $w_1 + az_1$, we may assume $Q(w_1) = 0$ and (z_1, w_1) is a hyperbolic pair. $V = (Fz_1 + Fw_1) \oplus (Fz_1 + Fw_1)^\perp$ and $U_1 = U' + \sum_{j>1} Fz_j \subseteq V_1 = (Fz_1 + Fw_1)^\perp$. $rad(U_1) = \sum j > 1 Fz_j$. If $r > 1$, we take $W = Fw_1$ and we have $U \perp W = U' \perp H_1$, $H_1 = Fz_1 + Fw_1$. If $r > 1$, we replace U, V with U_1, V_1 and note that $rad(U_1) = r - 1$ hence by induction we get $w_2, \ldots, w_n$ such that $U_1 + \sum_j Fw_j = U' \perp H_2 \perp \ldots \perp H_r$ and $H_j = Fz_j + Fw_j$. $W = \sum_{i=1}^r Fw_i$ satisfies the conclusion.

Witt Extension Theorem Let Q be a non-degenerate quadratic form and $char(F) \neq 2$ and suppose two subspaces, U_1 and U_2 are isometric, then the isometry can be extended to all of V.

Proof: Let η be an isometry between U_1 and U_2. If U_1 is non-degenerate, so is U_2 and η can be extended to an orthogonal transformation. If $rad(U) \neq 0$, we apply the previous result, $U_1 = rad(U_1) \oplus U_1'$ and $U_1 + W_1 U_1' \perp H_1 \perp \ldots \perp H_r$ where $H_i = Fz_i + Fw_i$ is a hyperbolic pair. Imbed $U_2 = \eta(U_1)$ in $U_2 + W_2 \eta(U_1') \perp H_1' \perp \ldots \perp H_r'$ where $H_i' = F\eta(z_i) + Fw_i'$ is a hyperbolic pair. $U_1 + W_1 \to U_2 + W_2$ coincides with η on U_1 and sends $w_i \mapsto w_i'$ and is an isometry of $U_1 + W_1$ and $U_2 + W_2$. Since $U_1 + W_1$ is non-degenerate, this can be extended to an orthogonal transformation and thus so can η. If $rad(U) = 0$, Witt's Cancellation Theorem proves it.

Definition 1: A vector v is *isotropic* if $B(v, v) = 0$. The *Witt index* is the common dimension of maximal totally isotropic subspaces. $\tau_{u,c}(x) = x + cB(x, u)u$ are called *symplectic transvections*. Note that by Witt's Theorem all such maximally isotropic subspaces are isometric and that quadratic forms are equivalent if their anisotropic subspaces are. A *symplectic base* is a base $u_1, \ldots, u_r, v_1, \ldots, v_r, 2r = n$ such that $(u_i, u_j) = (v_i, v_j) = 0$ and $(u_i, v_j) = \delta_{ij} = -(v_j, u_i)$. Note that $\eta \in Sp_n(F) \to \eta \tau_{u,c} \eta^{-1} = \tau_{\eta,c}$.

Theorem 19: Any orthogonal transformation is a product of symmetries.

Proof: Let η be orthogonal and $U : Q(u) \neq 0$. As in the proof of Witt's Cancellation Theorem, there is a symmetry, $S_w(x) = x - 2\frac{(x,w)}{(w,w)}w$, $w = u + \epsilon\eta(u)$ such that $\eta'(u) = -\epsilon u$ for $\eta' = S_w\eta$ and $\epsilon = \pm 1$. η' stabilizes $Fu^\perp$ which is non degenerate and of dimension $n - 1$. By induction, $\eta'_{|Fu^\perp} = \overline{S}_{w_1}\overline{S}_{w_2} \ldots \overline{S}_{w_k}$ where $\overline{S}_{w_i}$ is determines by $w_i \in Fu^\perp$. $\overline{S}_{w_i} = S_{w_i|Fu^\perp}$ and $u \perp w_i$ so it fixes u. Then $\eta'' = S_{w_1} S_{w_2} \ldots S_{w_k} \eta$ is the identity on $Fu^\perp$ (reverse order for inverse). Also, $\eta''(u) = \eta'(u) = \pm u$. If $\eta''(u) = u$, $\eta'' = 1$ and if $\eta''(u) = -u$, $\eta'' = S_u$. In either case, η' is a product of symmetries and hence so is $\eta = S_u \eta'$.

Theorem 20: If $dim(V) = n$, any orthogonal transformation is a product of $\leq n$ symmetries.

Proof:
Case 1: $V_1 = Fix(\eta)$ is not totally isotropic.
$\exists u : Q(u) \neq 0$ and η stabilizes $Fu^\perp$, so by induction, $\eta_{Fu^\perp}$) is a product of $n - 1$ symmetries.

Case 2: $\exists u \in V : Q(u) \neq 0$ and $Q(u - \eta(u)) \neq 0$.
As in Witt, $\exists S_w : \eta = S_w \eta'$ fixes u and we're back in Case 1.

Case 3: $dim(V) = 2$
True by above if V is anisotropic so V is a hyperbolic plane, u, v and either $\eta(u) = au, \eta(v) = a^{-1}v$

or $\eta(u) = av, \eta(v) = a^{-1}u$. If $a = 1$ the theorem holds trivially. If $w = u + v$, $w - \eta(w) = (1-a)u + (1-a^{-1}v$ satisfies $Q(w) \neq 0, Q(w - \eta(w)) \neq 0$ and the result holds as before. If $\eta(u) = av, \eta(v) = a^{-1}u$, $w + av$ is fixed by η and $Q(v) \neq 0$ and we're done by case 1.

Case 4: Holds in all other cases, namely: $dim(V) \geq 3$, $V_1 = Fix(\eta)$ is totally isotropic and $Q(u - \eta(u)) = 0, \forall u : Q(u) \neq 0$.
We claim $Q(u - \eta(u)) = 0, \forall u$. STS this for the $w \neq 0 : Q(w) = 0$. Consider $Fw^{\perp}$. $dim(Fw^{\perp}) = n - 1$, $n \geq 3$, $n - 1 > \lfloor \frac{n}{2} \rfloor$ so $Fw^{\perp}$ is not totally isotropic. So $\exists u \neq 0 : u \perp w, Q(u) \neq 0$. Then $(w \pm u) \perp w$, $Q(w \pm u) = Q(u) \neq 0$. Put $\zeta = 1 - \eta$. $Q(\zeta(w)) = Q(w - \eta(w)) = 0$ and $\zeta(V)$ is totally isotropic. Put $V_1 = (\zeta(V))^{\perp}$ then $V_1^{\perp} = \zeta(V)$ and we have both $V_1 \subseteq \zeta(V)^{\perp}$ and $V_1 \subseteq V_1^{\perp} = \zeta(V)^{\perp}$ and $\zeta(V) \subseteq V_1$. Thus $V_1 = \zeta(V)$. If $x \in V$, then $\zeta^2(x) = 0$ and η is unipotent. $n = dim(V_1) + dim(V_1^{\perp}) = 2dim(V_1)$. Now put $\eta' = S_w\eta$ for any symmetry, S_w. η' is improper and is thus a product of $k \leq n$ symmetries; in fact, $k \leq n - 1$ and thus $\eta = S_w\eta'$ is a product of at most n symmetries.

Theorem 21: $Sp_n(F) = \langle \tau_{u,c} \rangle$.

Proof: A symplectic transformation takes a hyperbolic pair into a hyperbolic pair.
Claim: If $\zeta \in Sp_n(F)$ takes the hyperbolic pair $(u, v) \to (u', v')$ then $\zeta \in \langle \tau_{u,c} \rangle$. (Proof: do this in two transvections.)
Note: $\tau_{u,c_1}\tau_{u,c_2} = \tau_{u,c_1+c_2}$ and for $\eta \in Sp(F)$, $\eta\tau_{u,c}\eta^{-1} = \tau_{\eta u,c}$. Given claim, let $\eta : (u, v) \mapsto (u', v')$ and set $\eta' = \zeta^{-1}\eta$ where $\zeta \in \langle \tau_{u,c} : (u, v) \to (u', v') \rangle$ and fixes the rest of V. Then $\eta' = \zeta^{-1}\eta$ fixes (u, v) and stabilizes $(Fu \oplus Fv)^{\perp}$ and by induction, $\eta' \in \langle \tau_{u,c} \rangle$.

Theorem 22: $\mathbb{Z}(Sp_n(F)) = \{1, -1\}$.

Proof: If $T \in \mathbb{Z}(Sp_n(F))$, T commutes with all $\tau_{z,c}$. The fixed points of $\tau_{u,c}, c \neq 0$ is $Fu^{\perp}$ and T maps fixed points into fixed points so T stabilizes $Fu^{\perp}$ but $Fu = rad(Fu^{\perp})$ so T stabilizes Fu and T is a scalar matrix.

Definition: $\mathbb{P}_n(F) = \{(x_1, \ldots, x_{n+1}) : x_i \in F\}$ where not all x_i are 0 and with $(x_1, \ldots, x_{n+1}) \sim \lambda(x_1, \ldots, x_{n+1}), \lambda \in F, \lambda \neq 0$. This is called the projective space of dimension n.

Theorem 23: $Sp_n(F)$ acts primitively on $\mathbb{P}_{n-1}(F)$.

Proof: Let $S = Stab(Sp_n(F))$. We can show $S = \mathbb{P}_{n-1}(F)$. $|S| > 1$. Suppose $(Fx, Fy) : (x, y) \neq 0$. Assume $(x, y) = 1$. Let $Fz \in \mathbb{P}_{n-1}(F)$; if $(x, z) \neq 0$ we may assume $(x, x) = 1$. By Witt, $\exists \eta \in Sp_n(F) : \eta(x) = x, \eta(y) = z$, then $\eta(S) = S$, since $Fx \in S$, $Fz \in S$ and since $F(y) \in S$, $\eta(y) = z$. Now suppose $(x, z) = 0$ and $Fz \neq Fx$ then $\exists Fw \in S$. We have $\zeta \in Sp_n(F) : \zeta(w) = w, \zeta(x) = z$ then $\zeta(S) = S$. $(x, w) = 1 = (x, z)$ since $Fw \in S$, $Fz \in S$ because $Fx \in S$.

Thus $S = \mathbb{P}_{n-1}(F)$ if S contains (Fx, Fy) be a pair of points in $S : (x, y) \neq 0, \exists u \in V$, $(x, u) = 1, (y, u) = 0$. Let $U = (Fx + Fu)^{\perp}$ and let $G < Sp_n(F)$. $\eta(t) = t$ if $t \in Fx + Fu$. These map the set of restrictions $\eta_{|U}$ in the symplectic group on U. Let $z \in U, z \neq 0$. Since $y \in U$ $\exists \eta \in G : \eta(y) = z$. Now $\eta(S) = S$ since $Fx \in S$ and since $Fx, Fy \in S$, we have $Fx \in S$. This shows that every $0 \neq z \in U$, is in S, since U contains a hyperpolic pair, we've reduced to the argument in the first paragraph.

Theorem 24: $Sp_n(F) = Sp_n(F)'$ except for $n = 2, |F| = 2, 3$ or $n = 4, |F| = 2$.

Proof: If $|F| > 3$, given $\tau_{z,c} \neq 1$, pick $d \neq 0$, $d^2 \neq 1$, $b = (1-d^2)^{-1}c$ and $a = -d^2 b$, then $a+b = c$ and $\tau_{z,c} = \tau_{z,a}\tau_{z,b}$. Let η be a symplectic transformation then $\eta\tau_{z,b}^{-1}\eta^{-1} = \eta\tau_{z,-b}\eta^{-1} = \tau_{\eta(z),-b} = \tau_{dz,-b} = \tau_{z,-bd^2} = \tau_{z,a}$ and hence $\tau_{z,c} = \eta\tau_{z,b}^{-1}\eta^{-1}\tau_{z,b}$.

Theorem 25: $Sp_n(F)$ is simple except for $n = 2, |F| = 2, 3$ or $n = 4, |F| = 2$.

Proof: Follows from the two previous results and simplicity theorem.

Theorem 26: $|Sp_n(q)| = q^{n-1}(q^n-1)q^{n-3}(q^{n-2}-1)\dots q(q^2-1)$.

Proof: $|Sp_n(q)| = q^{n-1}(q^n-1)|Sp_{n-2}(q)|$ because there are $q^{n-1}(q^n-1)$ ways to map a hyperbolic pair with respect to a hyperbolic pair and $|Sp_{n-2}(q)|$ ways to map the complementary space. (There are $q^n - 1$) ways to pick the first vector. The second vector has to be a solution to $(x_1)^{(2)} \cdot (y_1)^{(1)} + (y_1)^{(2)} \cdot (x_1)^{(1)} + \dots + (x_k)^{(2)} \cdot (y_k)^{(1)} + (y_k)^{(2)} \cdot (x_k)^{(1)} = 1$. There are q^{n-1} such solutions.)

Theorem 27: $|PSp_{2l}(q)| = \frac{1}{(2,q-1)}q^{l^2}(q^2-1)(q^4-1)...(q^{2l}-1)$, is simple unless $(2l,q) = (2,2), (2,3), (4,2)$.

Proof: $|PSp_{2l}(q)| = \frac{|Sp_{2l}(F)|}{|\mathbb{Z}(Sp_{2l}(F))|}$ and the center is has order 2 or 1 depending on whether $q-1$ is divisible by 2.

Theorem 28: Let $F_1(x_1, y_1, \dots, x_r, y_r) = x_1^2 - y_1^2 + \dots + x_r^2 - y_r^2$, $F_2(x_1, y_1, \dots, x_r, y_r, x_{r+1}) = x_1^2 - y_1^2 + \dots + x_r^2 - y_r^2 - x_{r+1}^2$, and $F_3(x_1, y_1, \dots, x_r, y_r, x_{r+1}) = x_1^2 - y_1^2 + \dots + x_r^2 - y_r^2 - dx_{r+1}^2$. The number of solutions of $F_1(x_1, y_1, \dots, x_r, y_r) = b$ over F_q is $q^{2r-1} + q^r - q^{r-1}$ if $b = 0$ and $q^{2r-1} - q^{r-1}$ if $b \neq 0$. The number of solutions of $F_2(x_1, y_1, \dots, x_r, y_r, x_{r+1}) = b$ over F_q is q^{2r} if $b = 0$, $q^{2r} - q^r$ if $-b \neq 0$ is not a square and $q^{2r} + q^r$ if $-b \neq 0$ is a square. The number of solutions of $F_3(x_1, y_1, \dots, x_r, y_r, x_{r+1}) = b$ over F_q is $q^{2r-1} - q^r + q^{r-1}$ if $b = 0$ and $q^{2r-1} + q^{r-1}$ if $b \neq 0$.

Proof: For $r = 1$, $x^2 - y^2 = b$, put $u = (x-1), v = (x+y)$. So the number of solutions for $b = 0$ is the number of $u, v : uv = 0$; there are $2q-1$ of these. For $b \neq 0$, the number of solutions is $q-1$. Now applying induction, let $b = a + c$, $a = \sum_{i=1}^{r} x_i^2 - y_i^2$ and $c = x_{r+1}^2 - y_{r+1}^2$. $N_q(2(r+1), 0) = (2q-1)N_q(2r, 0) + (q-1)N_q(2r, c), c \neq 0$. The remainder of the proof is similar.

Definition 2: Let Q be a quadratic form. The *orthogonal* group on a vector space, V, denoted $O(V, Q)$ is the group fixing lengths. $O(V, Q)^+$ is the subgroup of *rotations*.

Theorem 28a: Any non-degenerate symmetric form over F_q is equivalent to one of the following:
(a) [even dimension] $diag(1, -1, 1, -1, \dots, 1, -1)$, $(\epsilon = 1)$;
(b) [even dimension] $diag(1, -1, \dots, 1, -d)$, $\frac{-d}{q}) = -1$, $(\epsilon = -1)$;
(c) [odd dimension] $diag(1, -1, 1, -1, \dots, 1, -1, -d), (\frac{-d}{q}) = -1$;
(d) [odd dimension] $diag(1, -1, 1, -1, \dots, 1, -1, -d), (\frac{-d}{q}) = 1$.

Proof: Lagrange reduction. Note that types (c) and (d) yield non-isometric spaces but isomorphic groups. (a) and (b) yield non-isomophic groups.

Notation for orthogonal groups: A vector, x, is called *isotropic* if $(x, x) = 0$. A space, V, is called *anisotropic* if $\forall x \in V, (x, x) \neq 0$. A *symmetry* in V is the linear map $S_u : x \mapsto x - 2\frac{(x,u)}{(u,u)}u$. Note that $\eta S_u \eta^{-1} = S_{\eta(u)}$. Note that S_u is the identity on $Fu^{\perp}$ and the matrix for S_u is $diag(-1, 1, \dots, 1)$ where u is in the first position.

Dimension 2: Let (u,v) be a hyperbolic pair. η_a, $\eta_a(u) = au$ and $\eta_a(v) = a^{-1}v$. The map $a \to \eta_a$ is a map from $F^* \to O^+(V,Q)$. *Improper* transformation, τ_b, $\tau_b(u) = bv$ and $\tau_b(v) = b^{-1}u$. We have $\tau_b\eta_a\tau_b^{-1} = \eta_a^{-1}$. $O(V,Q)$ is a semi-direct product of F^* and Z_2.

Theorem 28b: If B is a symmetric bilinear form and there is a $u \in V, u \neq 0$ such that $(u,u) = 0$ then $(u,u) = b$ has a solution for any b (B is called universal in this case).

Proof: Suppose $\exists u : (u,u) = 0$. Since the form is non-degenerate, $\exists w : (u,w) = \frac{1}{2}$. Put $v = au + w$ and take $a = b - (w,w)$. This gives $(v,v) = b$. For the non-isotropic case, we may assume $B = diag(a,b)$ and we want to solve $ax^2 + by^2 = c$. We can divide and take $a = 1$. If $x^2 + by^2 \neq 0$, then $(\frac{-b}{q}) = -1$. So $x^2 + by^2$ is the norm in K/F. $u \mapsto u^q$ is an automorphism. $N_{K/F}(u) = u^{q+1}$. but K is cyclic with kernel of size $q+1$ and image of size $q-1$. So the automorphism is surjective.

Theorem 28c: If V, $dim(V) = 2$, has a non-degenerate symmetric bilinear form then $\nu(Q) \leq \lfloor \frac{n}{2} \rfloor$.

Proof: Obvious from the definition.

Theorem 28d: $|O_n(q)| = \lambda_n |O_{n-2}(q)|$, λ_n is the number of hyperbolic pairs in V.

Proof: Consider a map, g, from a hyperbolic pair to a hyperbolic pair ($\langle u_1, v_1\rangle \mapsto \langle u_2, v_2\rangle$), extended to all of $O_n(q)$. If $h \in O_n(q)$ is any map taking the first hyperbolic pair into the second, put $t = h^{-1}g$. t is the identity on $\langle u_1, v_1\rangle$; in fact, $t = id_{\langle u_1,v_1\rangle} \perp t'$, $t' \in \langle u_1, v_1\rangle^\perp$, $t' \in O_{n-2}(q)$. λ_n is calculated from Theorem 28. $\lambda_n = q^{n-2}(q^{n-1} - 1)$ if n is odd and $\lambda_n = q^{n-2}(q^{n/2} - \epsilon)(q^{n/2-1} + \epsilon)$, if n is even.

Definition: If $Q(x) = 0$, $u, z \in Fx^\perp$, $dim(V) \geq 3$, define $\eta_{x,u}(z) = z + (z,u)x$. Note that $x \in Fu^\perp$ means $\eta_{x,u}(x) = x$, $\eta_{x,u}^{-1} = \eta_{x,-u}$ and $\eta_{x,u_1+u_2} = \eta_{x,u_1} + \eta_{x,u_2}$. Note also that $Q(z + (z,u)x) = Q(z) + (z,(z,u)x) + (z,u)^2Q(x) = Q(z)$. In the next few theorems, we pick y such that $Q(y) = 0$ and $(x,y) = 1$ so $V = Fx + Fy + U$, $U = (Fx + Fy)^\perp$ and $Fx^\perp = Fx + U$.

Theorem 28e: Let $V, x, u, z, \eta_{x,u}$ be as in the above definition with $(\cdot,\cdot)$, non-degenetate. extends uniquely to an isometry $\rho_{x,u} \in O(V)$. $\rho_{x,u}$ is called a Siegal transformation. Further, $\rho_{x,u_1+u_2} = \rho_{x,u_1} + \rho_{x,u_2}$ and $\eta \in O(V,Q) \to \eta\rho_{x,u}\eta = \rho_{\eta(x),\eta(u)}$.

Proof: Define $\rho_{x,u}(w) = \eta_{x,u}(w)$ if $w \in Fx^\perp$ and $\rho_{x,u}(y) = ax + by + v$, $v \in U$. Note that if $\rho_{x,u}$ is well defined, it's domain is V. If $\rho_{x,u}$ is an isometry, some selection of a, b, v must give $Q(\rho_{x,u}(y)) = Q(y) = 0$ and $(\rho_{x,u}(y), \rho_{x,u}(z)) = (y,z)$ if $z \in Fx^\perp$. The conditions are $Q(\rho_{x,u}(y) = 0$ and $(\rho_{x,u}(y), \rho_{x,u}(z)) = (y,z) = 1$, if $z \in Fx^\perp$. These hold if the following holds: $ab + Q(v) = 0$, $b = 1$ and $(z,u) + (z,v) = 0$. These hold if $b = 1$, $a = -Q(v)$ and $v = -u$. So the definition of $\rho_{x,u}$ becomes $\rho_{x,u}(w) = \eta_{x,u}(w)$ if $w \in Fx^\perp$ and $\rho_{x,u}(y) = -Q(u)x + y - u$ and all conditions are satisfied. The extension is unique because there is a unique solution to the necessary conditions.

Definition: We define the "root" transformations as the transformations $\tau_{u,v,\lambda} : x \mapsto x + \lambda(x,u)v - \lambda(x,v)u$ with (u,v) satisfing $(u,u) = (v,v) = 0$, $(u,v) = 1$. Note that unless $char(F) = 2$, an orthogonal space has no transvections. A *flat* is an isotropic subspace. Define $\mathcal{C} = \{x : Q(x) = 0\}$, a $\mathbb{P}\mathcal{C}$ be the corresponding set in projective space. Let $V, x, u, z, \eta_{x,u}$ be as in the above definition and $dim(V) \geq 3$. Let x be an isotropic vector in V, $H_x = \langle \rho_{x,u} \rangle$, $U = Fy + Fu^\perp$, $y : (x,y) = 1, Q(y) = 0$. *Define* $\Omega = \langle H_x \rangle$, x isotropic.

Lemma 1: Let $V, x, u, z, \eta_{x,u}$ be as in the above definition and $dim(V) \geq 3$. H_x is a normal abelian subgroup of $Stab_{O(V)}(x)$ and $u \mapsto \rho_{x,u}$ is an isomorphism of U^+ with H_x. $\eta H_x \eta^{-1} = H_{\eta(x)}$.

Proof: If $\eta \in O(V,Q)$, $\eta H_x \eta^{-1} = H_{\eta x}$, x, isotropic. $\Omega \lhd Q(V,Q)$. Ω acts on a quadratic cone. Let $\mathcal{C} = \{x : Q(x) = 0\}$ and $e_1, e_2, \ldots, e_n$ a base for V and $x = \sum_i a_i e_i$. $Q(x) = 0 \leftrightarrow \sum_{i,j} b_{i,j} a_i a_j = 0$, $b_{i,j} = (e_i, e_j)$. $\mathcal{C}$ is a cone, $\mathbb{P}\mathcal{C}$ is the cone in $\mathbb{P}_{n-1}(F)$.

Definition 4: $\Omega = \langle H_x \rangle$, x isotropic. Alternative definition: $\Omega_n(q) = O_n(q)'$. Note: $\Omega \lhd O^+(V,Q)$ *char* $O(V,Q)$.

Lemma 2: $Z = \mathbb{Z}(O(V,Q)) = \{1, -1\}$.

Proof: Let $\gamma \in Z$, $Fu = \{x : S_u(x) = -x\}$, $Fu = \{x : S_u(x) = -x\}$. $S_u(\gamma(u) = \gamma(S_u(u)) = -\gamma(u)$. If $u_1, \ldots, u_n$ is an orthonormal basis for V. $\gamma(u_i) = \epsilon_i u_i$. $\gamma(u_i + u_j) = \pm(u_i + u_j)$. $\gamma(u_i + u_j + u_k) = \pm(u_i + u_j + u_k)$.

Lemma 3: If $\eta \in O(V,Q)$ satisfies $\eta(x) \in Fx$ then $\eta = \pm 1$.

Proof: Let (u, v) be a hyperbolic pair and $z \in (Fu + Fv)^\perp$, then $x = z - Q(z)u + v$ is isotropic. Thus, $\eta(u) = c_u u$, $\eta(v) = c_v v$ and $\eta(x) = c_x x$. Then $c_x(z - Q(z)u + v) = \eta(x) = \eta(z) - c_u Q(z) + c_v v$. Since $\eta(z) \in (Fu + Fv)^\perp$, it follows that $\eta(z) = c_x z$ and $c_x = c_u = c_v$. Hence if $c = c_x$, we have $\eta = 1$. Since η is orthogonal, $c = \pm 1$.

Lemma 4: Let $T_x = \mathcal{C} \cap Fx^\perp$, $PT_x = \{Fy \neq 0 : y \in T_x\}$ then H_x acts transitively on the complement of PT_x in $\mathbb{P}\mathcal{C}$.

Proof: This means y, z are isotropic vectors not orthogonal to x. There is a $\rho_{x,u} \in H_x$ such that $\rho_{x,u}(y) \in Fz$. We may assume $(y, x) = (z, x)$. We have $V = Fy + Fx^\perp = Fx \oplus Fy \oplus U$ where $U = (Fx + Fy)^\perp$. $z = ay + bx + u, u \in U$. $(Z, x) = 1, a = 1$ and since $Q(z) = 0$, we have $b + Q(u) = 0$ and so $z = y - Q(u)x + u$. Then $\rho_{x,-u}(y) = z$.

Lemma 5: Ω is transitive on $\mathbb{P}\mathcal{C}$ and on the set of hyperbolic pairs of $\mathbb{P}\mathcal{C}$.

Proof: Let Fx and Fy be distinct points on $\mathbb{P}\mathcal{C}$. $\exists Fz \in \mathbb{P}\mathcal{C}$ such that (Fz, Fx) and (Fx, Fz) are hyperbolic. (Fx, Fy) is hyperbolic and (x, y) is a hyperbolic pair. Let u be a non-isotropic vector is $U = (Fx + Fy)^\perp$. Put $z = x - Q(u)y + u$ then $Q(z) = -Q(u)(x, y) + Q(u) = 0$ and $(z, x) = -Q(u) \neq 0$ and $(z, y) = 1$. So Fz satisfies requirement. Since x, y are linearly independent, there is a linear function mapping $x, y \mapsto 1$ so $\exists z \in V : (x, z) = 1 = (y, z)$. Subtracting a multiple of X from z, we can get $Q(z) = 0$. (Fz, Fx) and (Fz, Fy) are hyperbolic so again we have Fz satisfying the requirement. Apply the previous lemma to get $\eta \in \Omega : \eta(Fx) = Fy$. This gives the transitivity of Ω on $\mathbb{P}\mathcal{C}$. Now let (Fx, Fy) and (Fx', Fy') be hyperbolic planes. $\exists \zeta \in \Omega : \zeta(Fx') = Fx'$ and $\zeta(\eta(Fy)) = Fy'$. Then $\zeta\eta$ maps (Fx, Fy) to (Fx', Fy') proving the second statement.

Lemma 6: Ω acts primitively on $\mathbb{P}\mathcal{C}$ except when $dim(V) = 1, \nu(Q) = 2$.

Proof: Suppose $\nu(Q) = 1$. (Fx, Fy) of $\mathbb{P}\mathcal{C}$ is hyperbolic so by lemma 5 it is 2-transitive on $\mathbb{P}\mathcal{C}$ then the action of Ω is primitive. Assuming $\nu \geq 2$ omitting $dim(V) \neq 4$ so $dim(V) \geq 5$. Let S be one of the sets of a partition of $\mathbb{P}\mathcal{C}$ stabilized by Ω and containing more than one point. Primitivity follows if $S = \mathbb{P}\mathcal{C}$. Suppose $Fx, Fy \in S, (x, y) = 0$ then we can find isotropic z: $(x, z) = 1$, $(y, z) = 0$. $V = (Fx + Fz) \oplus U$ where $U = (Fx + Fz)^\perp$ is at least three dimensional and non-degenerate, Since $y \in U, \exists w \in U : (y, w)$ is a hyperbolic pair. $dim(U) \geq 3$ and U contains isotropic vectors. Applying Lemma 5, to U, $\exists \eta$ which is the product of $\rho_{u,v}, u, v \in U : \eta(Fy) = Fw$. Since $x \in (Fu + Fv)^\perp$, this shows $\eta(Fx) = Fx$. Since $Fx \in S$, $\eta(S) = S$ and since $Fy, Fw \in S$ and (Fy, Fw) is a hyperbolic pair. Let $Fz \in \mathbb{P}\mathcal{C} : Fz \neq Fx$. $\exists Fw : (Fx, Fy)$ and (Fx, Fw), we get $\eta \in \Omega : \eta(Fx) = Fx, \eta(Fy) = Fw, \eta(S) = S$. $Fw, FZ \in S$. Since Fz was arbitrary in $Fx^\perp \in \mathbb{P}\mathcal{C}$, we have $S = \mathbb{P}\mathcal{C}$.

Lemma 7: $O(V,Q)' \subseteq \Omega$.

Proof: Let (x,y) be a hyperbolic pair and u is non-isotropic. $\exists \rho \in \Omega : \rho(u) \in Fx+Fy, u_1 = x + Q(u)y$ satisfies $Q(u_1) = Q(u)$. Hence $\exists \eta \in O(V,Q) : \eta(u_1) = u$. By lemma 5, $\exists \rho \in \Omega : \rho(F(\eta x)) = Fx$ and $\rho(F(\eta y)) = Fx+Fy$. Since $u_1 \in Fx+Fy$, $u = \eta u_1 \in \eta(Fx) + \eta(Fy)$ hence $\rho(u) \in \rho(F(\eta(x))) + \rho(F(\eta(y))) = Fx+Fy$. If S_u is a symmetry, $\exists \rho \in \Omega : \rho S_u \rho^{-1} = S_{u'}, u' \in \rho(u) \in Fx+Fy$. Let $O_{x,y} = \langle s_{u'} : u' \in Fx+Fy \rangle$. Since there is a restriction of $S_{u'}$ to $U = (Fx+Fy)^\perp$ is the identity. $\eta' \to \eta'_{|Fx+Fy}, \eta' \in O_{x,y}$ is an isomorphism between $O_{x,y} \to O(Fx+Fy,V)$ sending $O^+_{x,y} \to O^+(Fx+Fy,Q)$. Let be a rotation in V, $\zeta = S_{u_1} \dots S_{u_{2k}}, u_i$ non-isotropic, $S_0, \exists \rho_i \in \Omega : u'_i = \rho_i u_i \in Fx+Fy$ then $\zeta = (\rho_1 S_{u_1} \rho_1^{-1}) \dots (\rho_{2k} S_{u_{2k}} \rho_{2k}^{-1})$. Since $\Omega \lhd O(V,Q)$ $\zeta = \rho S_{u'_1} \dots S_{u'_{2k}}$ and hence $O^+(V,Q)/\Omega \cong O^+_{x,y}/(O^+_{x,y} \cap \Omega)$ and since $O^+_{x,y} \cong O^+(Fx+Fy,Q)$ and $Fx+Fy$ is a hyperbolic time $O^+_{x,y}$ is abelian so $O^+_{x,y}/\Omega$ is abelian and since $\Omega \supset (O^+(V,Q)')$ and we have $O(V,Q)' = O^+(V,Q)'$ and hence $\Omega \supset O(V,Q)'$.

Dickson-Dieudonne Theorem: Let Q be a non-degenerate quadratic form of Witt index ν in V, $dim(V) \geq 3$ then $P\Omega = O(V,Q)'/\mathbb{Z}(O(V,Q)')$ is simple unless $n=4$ and $\nu = 2$.

Proof: $O(V,Q) \subseteq \Omega \subseteq O(V,Q)$. This also proves $\Omega' = \Omega$. $\forall \rho_{x,u} \in \Omega'$, x isotropic, $u \in Fu^\perp$. Choose $u \in Fx^\perp$ and choose y such that (x,y) is a hyperbolic pair. Let $O_{x,y}$ be as in the lemma. $O_{x,y} = O(Fx+Fy,Q)$ the $\forall a \in F^*, \exists \eta_a \in O_{x,y}$. Also, $\exists \tau \in O_{x,y} : \tau(x) = y, \tau(y) = x$ and $\tau \eta_a^{-1} \tau \eta = \eta_a^2$.

Theorem 29: $\Omega(n,F)$ acts primitively on flat subspaces.

Proof: This is a restatement of Lemma 6.

Notes on orthogonal groups: Orthogonal groups over fields with odd characteristic do not have transvections and $SO_n(q) \neq SO_n(q)'$, in general. $SO_n(q)/\Omega_n(q) = 2$ if q is not even and n is odd. $-I \in \Omega^\epsilon_{2r}(q)$ iff $q^r = \epsilon \pmod 4$.

Theorem 30: $|O_{2r}(q)| = 2q^{r(r-1)}(q^r-1)\prod_{i=1}^{r-1}(q^{2i}-1)$.
$|O_{2r}(q,d)| = q^{r(r-1)}(q^r+1)\prod_{i=1}^{r-1}(q^{2i}-1)$, d, non-square.
$|O_{2r+1}(q)| = 2q^{r^2}\prod_{i=1}^{r}(q^{2i}-1)$.
$|P\Omega_{2r+1}(q)| = \frac{1}{(q-1,2)} q^{r^2}\prod_{i=1}^{r}(q^{2i}-1)$.
$|P\Omega^\epsilon_{2r}(q)| = \frac{1}{(4,q^r-\epsilon)} q^{r(r-1)}(q^r-\epsilon)\prod_{i=1}^{r-1}(q^{2i}-1)$.

Proof: By induction on n. For $n=1$, $O_1(q) = \{1,-1\}$. Assume $n \geq 2$ and pick $x : Q(x) = 1$. $|G| = |x^G||G_x|$ and $G_x \cong O_{n-1}(q)$ on the space $Fx^\perp$. Since G is transitive on vectors of length 1, $|x^G|$ will consist of all the vectors of length 1. Thus, for the case $n=2r$, for example, $|x^G| = (q^{2r-1}-q^{r-1})$. The result follows mutatis mutandis in all cases. Note that $|O_n(q) : SO_n(q)| = 2$, $|SO_n(q) : PSO_n(q)| = 2$, if n is even, 1 otherwise. $|PSO_n(q) : \Omega_n(q)| = 2$.

Theorem 31: If $dim(V) \geq 3$ then $O^+(V,Q) = Q(V,Q)'$.

Proof: Follows from the fact that elements are products of $\leq n$ symmetries and the fact that $\langle S_u S_v)^2 \rangle \lhd O(V,Q)$. *Note:* there is an isomophism $F^* \to \eta_a$.

Theorem 32: $|O^+_n(q)| = \frac{|O_n(q)|}{2}$. Since $\Omega_n(q) \cong O^+_n(q)/O_n(q)'$ and $-1 \in \Omega_n(q) = O_n(q)'$, for n, even but $-1 \notin \Omega_n(q) = O_n(q)'$, for n, odd, we also get the formulas for $P\Omega_n(q)$ and $P\Omega_n(q,d)$.

Proof: For $n = 1$, groups consist of ± 1. Proceed by induction on n. Choose $x \in V$ with $Q(x) = 1$ and consider the orbit Gx, the set of vectors with $Q(y) = 1$. $|G| = |x^G||G_x|$. If $G = O_n(q), n = 2r$ G_x is isomorphic to thr orthogonal group in $Fx^\perp$ relative to the restricted Q and hence $O_{n-1}(q)$. The number of solutions to $Q(y) = 1$ is $q^{2r-1} - q^{r-1}$. We may assume the formula for $n - 1 = 2r - 1$. For $O_n(q, d)$ do the same with $q^{2r-1} + q^{r-1}$. The case $n = 2r + 1$ uses $O_{n-1}(q)$, $n - 1 = 2r$.

Notation: $P\Omega^\epsilon{}_{2l}(q)$ is used with $\epsilon = \pm 1$ to distinguish between the two cases in even order.

Theorem 33: $P\Omega_n(q)$ is simple if $n > 2$, n, odd. $P\Omega^\epsilon{}_{2l}(q)$ is simple if $l > 2$.

Proof: Apply Iwasawa's theorem given that if $G = P\Omega_n(q)$, $G' = G$, G acts primitively on flat spaces and $H \lhd G_u$ $\langle H^G \rangle = G$.

Theorem 34: For $l \geq 2$, q, odd, $P\Omega_{2l+1}(q)$ is not isomorphic to $PSp_{2l}(q)$ despite having the same order.

Proof: $PSp_{2m}(q)$ has $\lfloor \frac{m}{2} \rfloor + 1$ conjugacy classes of elements of order 2. $P\Omega_{2l+1}(q)$ has m conjugacy classes of elements of order 2. If $t \in Sp_{2m}(q)$ with $t^2 = 1$ or $t \in \Omega_{2m}(q)$ with $t^2 = 1$ then $V = V^+ \oplus V^-$ where $vt = \lambda v$ for $v \in V^\lambda$ and V^+ and V^- are orthogonal. There are m possibilities for the subspaces for these subspaces up to isometry; in the symplectic space, it interchanges t and $-t$ in the symplectic case there is another with $t^2 = -1$.

Definition 5: The transformation $\tau_{u,c} : x \mapsto x + c(x, u)u$, u, isotropic, $\overline{c} = -c$, is a *unitary transvection.* For the unitary form, let $\sigma \in F(q^2)/F(q)$ such that $\sigma^2 = 1$ (σ is like the complex conjugate operation over $\mathbb{C}$). $\langle x, y \rangle$ is a *hyperbolic plane* if $(x, y) = 1, (x, x) = (y, y) = 0$. (Fx, Fy) is a *hyperbolic pair* if $(x, y) \neq 0$. For a hyperbolic pair, define η_a by $\eta_a(x) = ax, \eta_a(v) = a^{-1}v$. $K_0 = \{a \in K : \overline{a} = a\}$.

Summary Theorem: (a) All unitary transvections are of the form given above. (b) If V is a unitary space with $dim(V) \geq 2$ then V is isotropic and V is a direct sum of hyperbolic planes. (c) $U_n(q)$ is transitive on $\mathbb{P}\mathcal{C}_n(q^2)$. (d) The unitary transvections generate $SU_n(q)$. (e) $SU_n(q)$ acts primitively on $\mathbb{P}\mathcal{C}_n(q^2)$.

Proof: This is similar to the proofs for the orthogonal case.

Theorem 35: $V = H_1 \perp H_2 \perp \ldots \perp H_r \perp W$; the H_i are hyperplanes and W is anisotropic. $SU_n(F)$ is generated by unitary transvections and acts primitively on isotropic lines. Further, let $A = \langle \tau_{\lambda,u} \rangle$ for fixed u. $A \lhd SU_n(q)_u$ and $A' = 1$.

Proof: This is a straightforward computation.

Theorem 36: $SU_n(F)' = SU_n(F)$.

Proof: Every unitary transvection is a commutator, as in the linear group. These generate $SU_n(q)$.

Theorem 37: $|PSU_n(q^2)| = (n, q + 1)^{-1} q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^{2i} - (-1)^i)$.

Proof: Let y_n be the number of vectors of norm 1 and z_n be the number of vectors of norm 0 in an n dimensional unitary space. $q^{2n} = 1 + z_n + (q - 1)y_n$, $z_0 = z_1 = 0$, $z_{n+1} = z_n + (q^2 - 1)y_n$, so $z_n = (q^n - (-1)^n)(q^{n-1} + (-1)^n)$ $y_n = q^{n-1}(q^n - (-1)^n)$.
$|GU_n(q^2)| = \prod_{i=1}^n q^{i-1}(q^i - (-1)^i) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - (-1)^i)$.
$|GU_n(q^2) : SU_n(q^2)| = q + 1$, $|SU_n(q^2) : PSU_n(q^2)| = (n, q + 1)$.

Another proof: Let $i_n = |\mathbb{P}\mathcal{C}_n(q^2) \cup \{0\}|$ and h_n be the number of hyperbolic planes in V. $i_n = q^{2n} + (-1)^n(q^n - q^{n-1})$. $h_n = q^{2n-3} i_n$. $\mathbb{P}\mathcal{C}_n(q^2)$ is the orbit of $U_n(q)$ on an isotropic vector, u, and $|\mathbb{P}\mathcal{C}_n(q^2)| = q + 1$. The stabiliser of u has order $q(q^2 - 1)$.

Theorem 38: $|PSU_n(q^2)| = \frac{1}{(n,q+1)} q^{\frac{n(n-1)}{2}}(q^2-1)(q^3+1)(q^4-1)...(q^n-(-1)^n)$, is simple unless $(2l,q) = (2,4),(2,9),(3,4)$.

Proof: Apply Iwasawa's theorem given that if $G = PSU_n(q)$, $G' = G$, G acts primitively on isotropic lines and $H \lhd G_u$, where H is the unitary transvections fixing u and $\langle H^G \rangle = G$.

Definition: G is quaternion if $|G| = 8$ and has a single involution. If $x \in G$ and x is neither the identity nor the involution, $|x| = 8$. A generalized quaternion group is a group $G = \langle a, b : a^{2^k} = -1, b^2 = -1, b^{-1}ab = a^{-1} \rangle$. The 2 sylow subgroup of $SL_2(5)$ is quaternion and the 2 sylow subgroups of $SL_2(q), q$, odd are generalized quaternion. The 2 sylow subgroups of $SL_2(2^k)$ are elementary abelian.

Theorem 39: Let $V = A_n(F)$. $GL(V)/SL(V) \cong K^*$. If $t \in Inv(SL(V)), v + v^t \in C_V(t)$. All p-elements of $GL_2(V)$ are in $SL_2(V)$. There are $q+1$ sylow p-subgroups in $GL_2(q), q = p^k$. If $P_1 \neq P_2$ are two Sylow 2 subgroups in $GL_2(V)$ then $SL_2(V) = \langle P_1, P_2 \rangle$.

Proof: These all follow easily from the definitions.

Theorem 40: If $r \neq p$ are two primes, $R \in S_r(SL_2(V))$, then, if $r \neq 2$, R is cyclic; if $r = 2$, R is quaternion.

Proof: Stellmacher 8.6.9.

Theorem 41: If $p \neq 2$, $a \in p(SL(V))$ and R is a $\langle a \rangle$-invariant p'-subgroup of $SL(V)$, such that $1 \neq [R,a]$, then $p = 3$ and R is quaternion of order 8.

Proof: $R = [R,a]C_R(a)$ and $[R,a,a] = [R,a]$. $C_R(a) = \langle z \rangle$ where z is the unique involution.
Claim: $[R,a]$ is quaternion implies $\langle z \rangle = \mathbb{Z}([R,a])$.
Proof of claim: By induction on $|R|$. If $R = [R,a]$, otherwise we can apply induction. So a is a p element and R is an r-group, $r \neq p$. a acts on the cyclic group R so $p \mid (r-1)$ and thus $r \neq 2$ and $r \mid (q+1)$ or $r \mid (q-1)$. If $q = p$ these are inconsistant. If $r \mid (q-1)$, the with $V = Ku + Kw$, Ku and Kw are the only a- invariant subspaces of V and a acts either trivially or transitively, which is a contradiction. If $r \mid (q+1)$, we can extend the underlying field and obtain $R\langle a \rangle$ is isomorphic to the extended linear group. This returns us to the prior contradiction and the claim holds.
Given claim, $\langle z \rangle = \mathbb{Z}([R,a])$ and thus $R = [R,a]$. Hence $R = Q_{2^n}$ For $n \geq 4$, R has a cyclic characteristic group of index 2 and a acts trivially on it and the quotient and thus $R = Q_8$.

Notes: $|A_8| = |PSL_3(4)|$ but the two groups are not isomorphic. Similarly, the infinite families $P\Omega_{2l+1}(q)$ and $PSp_{2l}(q^2)$ have the same orders but are not isomorphic. Here are some "accidental" isomorphisms: $Sp_2(q) \cong SL_2(q)$, $P\Omega_6{}^+(q) \cong PSL_4(q)$, $P\Omega_6{}^-(q) \cong PSU_4(q)$, $P\Omega_5{}^-(q) \cong PSp_4(q)$, $PSL_4(q) \cong A_8$, $L_2(2) \cong S_3$, $L_2(3) \cong A_4$, $L_2(4) \cong L_2(5)$, $PSL_2(7) \cong PSL_3(2)$.

9.2 Groups of Lie Type

Setting: A *complex Lie algebra* is a non-commutative algebra over $\mathbb{C}$ satisfying $x \cdot (y+z) = x \cdot y + x \cdot z$, $(y+z) \cdot x = y \cdot x + z \cdot x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $(\lambda x) \cdot y = \lambda(x \cdot y)$ and $(x \cdot y) \cdot z + (z \cdot x) \cdot y + (y \cdot z) \cdot x = 0$. The simple Lie algebras (ones with no proper ideals) are: $A_n, n \geq 1$ [corresponding to $PSL_{n+1}(q)$], $B_n, n \geq 2$ [corresponding to $O_{2n+1}(q)$], $C_n, n \geq 3$ [corresponding to $Sp_{2n}(q)$], $D_n, n \geq 4$ [corresponding to $O^+_{2n}(q)$], G_2, F_4, E_6, E_7, and E_8. The twisted groups which are groups arising from automorphisms of the Dynkin diagram for the Lie algebra are: ${}^2A_n, n > 1$ [corresponding to $U_{n+1}(q)$], ${}^2D_n, n > 2$ [corresponding to $O^-_{2n}(q)$], ${}^3D_4$, and ${}^2E_6$. Finally, the exceptional families associated with B_2, G_2 and F_4 give rise to (resp), the Suzuki groups ($q = 2^n, n > 1$), the Ree groups of odd type ($q = 3^n, n > 1$), and the Ree groups of eventype ($q = 2^n, n > 1$).

9.3 The centralizer of an involution in the classical simple groups

$PSL_n(q)$: Put $G = PSL_n(q)$ and let $t \in Inv(G)$ and put $C = \{X \in SL_n(q) : XT = \mu TX, \mu \in GF(q)^*\}$. Finally, let $Z = \{\lambda I_n : \lambda^n = 1\}$ so $G = PSL_n(q) = SL_n(q)/Z$; note $|Z| = (n, q-1)$. Let $T = \begin{pmatrix} -I_r & 0 \\ 0 & I_s \end{pmatrix}$. T is an involution corresponding to an involution $t \in G$ of type 1; in fact, $t = TZ/Z$ and $C_G(t) = C/Z$. For odd q, $T^2 = \lambda I_n$ with minimal polynomial $m_t(x) = x^2 - \lambda I_n$. If λ is a quadratic residue in $GF(q)$, $m_t(x) = (x-\rho)(x+\rho)$. If $n = 2m$ is even, $T = \begin{pmatrix} I_m & 0 \\ 0 & \rho I_m \end{pmatrix}$ is also an involution of type 2. For $X \in C$ $X = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$, in the case of a type 1 involution, $det(X_1)det(X_4) = 1$ and $X_2 = 0$, $X_3 = 0$, in the case of a type 2 involution, $det(X_2)det(X_3) = -1$ and $X_1 = 0$, $X_4 = 0$. Let $\delta : X \mapsto det(X)$. $K = ker(\delta) \cong SL_r(q) \times SL_s(q)$. Put $E = KZ/Z \cong K/(K \cap Z)$. E is a central product and $E \lhd C/Z$. $K \cap Z = \lambda I_n$ with $\lambda^r = \lambda^s = 1$ and $|K \cap Z| = (d, s) = (d, r)$, $Z = Z_r \times Z_s$. In fact, given the following lemma, E is a minimal central product.

Lemma: If A and B are cyclic groups with $|\langle A\rangle| = ac$, $|\langle B\rangle| = bc$ and $(a, b) = 1$, then the minimal central product of A and B has order abc. [Proof: $A^a = B^b$ is in the center.]

Now if $N \subseteq C_G(t)$ corresponds to E, $N \lhd C_G(t)$ and $C_G(t)/N$ is cyclic. Since $GF(q)^* = C/Z \mapsto C_G(t)/N$, $\mathbb{Z}(N)$ is also cyclic. This gives the following:

Theorem: Put $G = PSL_n(q)$, q, odd and let $t \in Inv(G)$. If n is odd, $\exists N \lhd : C_G(t)$ and N is a minimal central product of $SL_r(q)$ and $SL_s(q)$ with $r + s = n$. Further, $|C_G(t)/N| \mid q-1$ and $|\mathbb{Z}(N)| \mid q-1$.

Further (considering involutions of type 2, we get:

Theorem: Put $G = PSL_n(q)$, q, odd and let $t \in Inv(G)$. If $n = 2m$ is even, there are involutions corresponding to $r \neq s$ with centralizers as above. For $r = s = m$, the centralizer of an involution either has type i or type ii below. Type i: There subgroup $C_0 \lhd C_G(t), |C_G(t) : C_0| = 2$ such that $r = s = m$ and a subgroup $E \lhd C_G(t)$ where E satisfies the conclusions of the previous result with $C_G(t)/E$ dihedral and C_0/E and $\mathbb{Z}(E)$ cyclic with orders dividing $q-1$. Type ii: There subgroup $C_0 \lhd C_G(t), |C_G(t) : C_0| = 2$ and a subgroup $E \lhd C_G(t)$ with $E/Z(E) \cong PSL_m(q^2)$. $|\mathbb{Z}(E) \mid q+1$ and $C_G(t)/E$ has order $q+1$ or $2(q+1)$.

Here are the results for other simple classical groups.

Theorem: Put $G = PSL_n(q)$, q even and let $t \in Inv(G)$. $\exists E, Q \lhd C_G(t)$ with $C_G(t) \supset E \supset Q \supset 1$ such that $C_G(t)/E$ is a cyclic group with order dividing $q-1$, E/Q is a minimal central product of $SL_r(q)$ and $SL_s(q)$ with $n = 2r + s$ and Q is a 2-group of class at most 2. Further, $C_G(Q) \subseteq Q$.
Here T has the form $\begin{pmatrix} L & 0 & I_r \\ 0 & I_s & L \\ 0 & 0 & I_r \end{pmatrix}$ and for C as above, $X \in C$ has the form $\begin{pmatrix} R & L & M \\ 0 & S & N \\ 0 & 0 & R \end{pmatrix}$ with $det(R)^2 det(S) = 1$, $R \in SL_r(q)$ and $S \in SL_s(q)$

Theorem: Put $G = PSp_{2m}(q)$, q, odd and let $t \in Inv(G)$. $C_G(t)$ has one of the following forms:
(i) $C_G(t)$ is a minimal central product of $Sp_{2r}(q)$ and $Sp_{2s}(q)$, $r + s = m, r \neq s$
(ii) There is a subgroup $C_1 \lhd C_G(t)$ and C_1 is a minimal central product of two copies of $Sp_{2l}(q)$, $2l = m$. Further, $C_G(t) - C_1$ has an involution that exchanges the two copies.
(iii) There is a subgroup $C_1 \lhd C_G(t)$ of index 2 with $C_1 = GL_m(q)/\langle -I\rangle$. Further, $C_G(t) - C_1$ has an involution which induces an automorphism corresponding to $A \mapsto {}^tA^{-1}$ and $q = 1 \pmod 4$.

(iv) There is a subgroup $C_1 \lhd C_G(t)$ of index 2 with $C_1 = U_m(q)/\langle -I \rangle$. Further, $C_G(t) - C_1$ has an involution which induces an automorphism corresponding to $A \mapsto A^\tau$ and $q = 3 \pmod 4$.

Theorem: Put $G = PSp_{2m}(q)$, q, even and let $t \in Inv(G)$. $\exists E \lhd C_G(t)$ where E is a 2-group of class at most 2. $C_G(E) \subseteq Q$ and $C_G(t)/E = G_0 \times Sp_s(q)$ where G_0 is one of: $Sp_r(q)$, $Sp_{r-1}(q)$, or the semidirect product of $Sp_{r-2}(q)$ and a special 2-group, Q, of order q^{r-1}. $2r + s = 2m$.

Theorem: Put $G = PSU_n(q)$, q, odd and let $t \in Inv(G)$. $C_G(t)$ is one or the following:
(i) $\exists N \lhd C_G(t)$ where N is a minimal central product of $SU_r(q)$ and $SU_s(q)$, $r + s = n$. $C_G(t)/N$ and $\mathbb{Z}(N)$ are cyclic with order dividing $q + 1$.
(ii) $n = 2m$ and $\exists C_0 \lhd C_G(t)$ of index 2 and $E \lhd C_G(t)$ with the same structure as (i) and $C_G(t)/E$ is dihedral. There is an involution of $C_G(t) - E$ that exchanges the two factors.
(iii) $n = 2m$ and $\exists C_0 \lhd C_G(t)$ of index 2 and $E \lhd C_G(t)$ with $E/Z(E) = PSL_m(q^2)$, $\mathbb{Z}(E)$ cyclic with order dividing $q - 1$. There is an involution of $C_G(t) - E$ that transforms elements of $PSL_m(q^2)$ as $A \mapsto {}^t(A^\tau)^{-1}$.

Theorem: Put $G = PSU_n(q)$, q, even and let $t \in Inv(G)$. $\exists E, Q : C_G(t) \supset E \supset Q \supset 1$ with $C_G(t)/E$ cyclic whose order divides $q + 1$, E/Q is a minimal central product of $SU_r(q)$ and $SU_s(q)$, $n = 2r + s$, Q is a 2-group of class at most 2 and $C_G(Q) \subseteq Q$.

Theorem: Put $G = P\Omega_n(q)$, q, odd and let $t \in Inv(G)$. $\exists E \lhd C_G(t)$ with $C_G(t)/E$, solvable, $E = E'$ and E is either (i) $SL_m(q)$, $SU_m(q)$ $(2m = n)$ or (ii) a central product of $\Omega_r(q)$ and $\Omega_s(q)$.

Theorem: Put $G = P\Omega_{2m}(q)$, q, even, $m \geq 4$ and let $t \in Inv(G)$. $\exists Q \lhd C_G(t)$, $C_G(Q) \subseteq Q$, where Q is a 2-group and $C_G(t)/Q$ is either (1) $Sp_r(q) \times {\Omega_{2s}}^\epsilon$, $m = r + s$.

Theorem: Put $G = A_n$ and let $t \in Inv(G)$. $C_{S_n}(t) = H_1 \times H_2$. $H_1 = S_k$, $H_2 = S_k$ wr $\mathbb{Z}_2$. So $C_G(t) = \{(a, b), a \in H_2, b \in H_2 : \text{sign}(a) = \text{sign}(b)\}$.

Example special linear group: $G = SL_2(7)$. $|G| = 336$. For $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\langle g \rangle = P \in S_7(G)$. For $t = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$, $\langle t \rangle = R \in S_3(G)$. Let $S = S_2(G)$, $|S| = 16$. $S = \langle a, b \rangle$ where $a = \begin{pmatrix} 1 & 4 \\ 2 & 2 \end{pmatrix}$, and $b = \begin{pmatrix} 1 & 3 \\ 4 & -1 \end{pmatrix}$. $|a| = 8$ and $|b| = 4$. S is generalized quaternion and of course, $T \in S_2(PSL_2(7))$ is dihedrael, with $|Aut(T)| = 2\phi(7)$. $T \cong \langle (1234), (13) \rangle$. S has 1 element of order 1, 1 element of order 2, 10 elements of order 4 and 4 elements of order 8. $N_G(S) = S$, $|N_G(P)| = 42$, and $|N_G(R)| = 12$. G has 1 element of order 1, 1 element of order 2, 56 elements of order 3, 42 elements of order 4, 56 elements of order 6, 48 elements of order 7, 84 elements of order 8, and 14 elements of order 48. $Aut(Q_8) = S_4$.

9.4 Finite Simple Groups

$\mathbb{Z}_p$, Schur Multiplier: 1.
Σ'_n simple if $n > 4$, Schur Multiplier: 6 if $n = 6, 7$, 2 if $n = 5, n > 7$.
$A_n(q) = PSL_{n+1}(q)$ simple if $n \geq 1$, Schur Multiplier: $(n + 1, q - 1)$ except $A_1(4)[2]$, $A_1(9)[6]$, $A_2(4)[48]$, $A_3(2)[2]$.
$B_n(q) = P\Omega_{2n+1}(q)$ simple if $n \geq 1$, Schur Multiplier: $(2, q - 1)$ except $B_2(2)$, $B_3(2)[2]$, $B_2(2)[6]$;
$C_n(q) = PSp_{2n}(q)$ simple if $n > 2$, Schur Multiplier: $(2, q - 1)$ except $C_3(2)[2]$.

$D_n(q) = P\Omega^+_{2n}(q)$ simple if $n \geq 4$, Schur Multiplier: $(2, q-1)$ except $D_4(2)[4]$.
$E_6(q)$ of order $\frac{1}{(3,q-1)}q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$, Schur Multiplier: $(3, q-1)$.
$E_7(q)$ of order $\frac{1}{(3,q-1)}q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$, Schur Multiplier: $(2, q-1)$.
$E_8(q)$ of order $q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$, Schur Multiplier: 1.
$F_4(q)$ of order $q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$, Schur Multiplier: 1 except $F_4(2)[4]$.
$G_2(q)$ simple except $G_2(2)$ of order $q^6(q^6-1)(q^2-1)$, Schur Multiplier: 1 except $G_2(3)[3]$, $G_2(4)[2]$.
${}^2A_n(q^2) = PSU_{n+1}(q)$ simple if $n \geq 2$, Schur Multiplier: $(n+1, q+1)$ except ${}^2A_3(2^2)[2]$, ${}^2A_3(3^2)[36]$, ${}^2A_5(2^2)[12]$.
${}^2D_n(q) = P\Omega^-_{2n}(q)$ simple if $n \geq 4$, Schur Multiplier: $(4, q^n+1)$.
${}^3D_4(q^3)$ of order $q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$, Schur Multiplier: 1 .
${}^2E_6(q)$ of order $q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^2-1)$, Schur Multiplier: $(3, q+1)$ except ${}^2E_6(2^2)[12]$.
${}^2B_2(2^{2m+1}) = Sz(2^{2m+1})$ simple if $m > 1$ of order $q^2(q^2+1)(q-1)$, Schur Multiplier: $1, n > 2$.
${}^2F_4(2^{2m+1})$ (Ree) simple if $m > 1$ of order $q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$, Schur Multiplier: $1, m > 1$.
${}^2G_2(3^{2m+1})$ (Ree) simple if $m > 1$ of order $q^3(q^3+1)(q-1)$, Schur Multiplier: $1, m > 1$.

9.5 Sporadic Groups

M_{11} $(2^4 \cdot 3^2 \cdot 5 \cdot 11)$, Schur: 1.
M_{12} $(2^6 \cdot 3^3 \cdot 7 \cdot 11)$, Schur: 2.
M_{22} $(2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11)$, Schur: 6.
M_{23} $(2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23)$, Schur: 1.
M_{24} $(2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23)$, Schur: 1.
J_1 $(2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19)$, Schur: 1.
$J_2 = HJ$ $(2^7 \cdot 3^3 \cdot 5^2 \cdot 7)$, Schur: 2.
$J_3 = HJM$ $(2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19)$, Schur: 3.
J_4 $(2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43)$, Schur: 1.
Co_1 $(2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23)$, Schur: 2.
Co_2 $(2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23)$, Schur: 1.
Co_3 $(2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23)$, Schur: 1.
HS $(2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11)$, Schur: 2.
Mc $(2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11)$, Schur: 3.
Sz $(2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13)$, Schur: 1.
Ly $(2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67)$, Schur: 1.
He $(2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17)$, Schur: 1.
Ru $(2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29)$, Schur: 1.
$O'N - S$ $(2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31)$, Schur: 3.
F_{22} $(2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13)$, Schur: 6.
F_{23} $(2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23)$, Schur: 1.
F_{24} $(2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29)$, Schur: 3.
F_3 (Thompson) $(2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31)$, Schur: 2.
F_5 (Harada) $(2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19)$, Schur: 1.
F_2 (Baby Monster) $(2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47)$, Schur: 2.
F_1 (Monster) $(2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71)$, Schur: 1.

9.6 Coxeter groups

Definition 6: If G is a finite subgroup of $O(V)$, a subset $F \subset V$ is a *fundamental region* if (1) F is open, (2) $F \cap T_g(F) = \emptyset$ if $g \neq 1$ and (3) $V = \bigcup_{g \in G} T_g(F)^c$ where X^c is the closure of X in V.

Theorem 42: If $dim(V) = 2$ and $G \subseteq O(V), |G| < \infty$, G is cyclic or dihedral.

Proof: Let H be the subgroup of rotations. It has index 1 or 2. Elements of H are parameterized by θ. Pick the minimum θ that generates the (cyclic) group H.

Theorem 43: If $dim(V) = 3$ and T_g is a rotation about an fixed axis, $\vec{v}$, then T_g is a rotation about $\vec{v}$ in $\vec{v}^{\perp}$.

Proof: Since T is a rotation, it preserves length and the determinant is thus 1. Since the dimension is 3, the characteristic equation has at least one real root and hence at least one real eigenvalue which, by the foregoing, must be 1. This proves the result.

Definition 7: If $dim(V) = 3$ and G is a finite subgroup of $O(V)$ the poles of G are the fixed points of the rotations in G. $\mathcal{C}_3^n$ is the cyclic group of order n, $\mathcal{H}_3^n$ is the dihedral group of order $2n$, $\mathcal{T}_3$ is the symmetry group of the tetrahedron, $\mathcal{W}_3$ is the symmetry group of the dodecahedron, and $\mathcal{I}_3$ is the symmetry group of the ichosahedron.

Theorem 44: If $dim(V) = 3$ and $G \subseteq O(V), |G| < \infty$ then G is a permutation group on the poles of G.

Proof: Let γ be the poles. If $x \in \gamma$ fixed by T, $Rx = RTR^{-1}Rx$ and Rx is a pole of RTR^{-1}.

Theorem 45: If $dim(V) = 3$ and $G \subseteq O(V), |G| < \infty$ then G is one of the groups in the prior definition.

Proof: Let G be a finite rotation group, $|G| = n$ and $\gamma = \{x_1, x_2, \ldots, x_k\}$ be the poles. Put $\mathcal{U} = \{(T, x), T \in G, T \neq 1, x \in \gamma\}$. $|\mathcal{U}| = 2(n-1) = \sum_{i=1}^{k} |x_i^G|(|G_{x_i}| - 1)$. Then $2 - \frac{2}{n} = \sum_{i=1}^{k}(1 - \frac{1}{|x_i^G|})$ and $1 \leq 2 - 2/n < 2$, so $k = 2$ or $k = 3$. Putting $n_i = |x_i^G|$, when $k = 2$, $1 = \frac{n}{n_1} + \frac{n}{n_2}$ so $n_1 = n_2 = n$. For $k = 3$, $n_1 = 2$ and $n_2 = 2, 3$, then $n_3 = 3, n = 12$, $n_3 = 4, n = 24$ or $n_3 = 5, n = 60$. $n_5 < 6$.

Theorem 46: If $dim(V) \geq 1$, then V is not the union of a finite number of proper subspaces.

Proof: By induction on $n = dim(V)$. True for $n = 1$. Suppose $V = V_1 \cup \ldots \cup V_m$ and let W be a subspace of dimension $n - 1$ then $W = W \cap V = (W \cap V_1) \cup \ldots \cup (W \cap V_m)$. By induction, $W = V_i$ for some i and in fact, every subspace of dimension $n-1$ must be one of the V_i but there are infinitely many subspaces of dimension $n - 1$ and this is a contradiction.

Definition 8: Let $\mathcal{P}_i$ be the perpendicular bisector of the line segment $\vec{x}_0, \vec{x}_i$. In this case, $\mathcal{P}_i = \{x : d(x, x_0) = d(x, x_i)\}$.

Theorem 47: Let $\vec{x}_i = T_{g_i}(\vec{x}_0)$, $i = 0, 1, \ldots, |G| - 1$. $\mathcal{P}_i = \{\vec{x} \in V : d(\vec{x}, \vec{x}_0) = d(\vec{x}, \vec{x}_i)\}$ and $\mathcal{L}_i = \{\vec{x} \in V : d(\vec{x}, \vec{x}_0) < d(\vec{x}, \vec{x}_i)\}$. $F = \bigcap_{i=0}^{|G|-1} \mathcal{L}_i$ is a fundamental region for G in V.

Proof: Since each $\mathcal{L}_i$ is open, so is F. $T_i(F) = \{T_i x : d(T_i x, T_i x_0) < d(T_i x, T_i T_j x_0)\} = \{y : d(y, x_i) < d(y, T_k x_0)\}$ but $\bigcup_j \{T_i T_j\} = G \setminus \{T_i\}$. So $T(F) = \{x : d(x, x_i) < d(x, x_j), i \neq j\}$. If $x \in F \cap T_i F$ then $d(x, x_i) < d(x, x_0)$ and $d(x, x_i) > d(x, x_0)$ so $F \cap T_i F = \emptyset$. If $x \in V$ choose i such that $d(x, x_i)$ is minimal and so $d(x, x_i) \leq d(x, x_j), \forall j$ and so $x \in T_i(F)^c$ and the union of all these is V.

Definition 9: If G is a finite subgroup of $O(V)$, and r is a unit vector then $s_r(x) = x - 2(x,r)r$ is called a *reflection* through $r^\perp$. $s_r \in O(V)$ and the $\pm r$ are called *roots* of G.

Theorem 48: If r is a root of G then $x = T_g(r)$ is also a root and $s_x = T_g s_r T_g^{-1}$.

Proof: $\mathcal{P} = r^\perp$ and $\mathcal{P}' = T(\mathcal{P}) = T(r)^\perp = x^\perp$. If $y = T(z) \in \mathcal{P}', z \in \mathcal{P}$. $s_x(y) = T s_r T^{-1}(y) = y$.

Definition 10: $V_T = \{x \in V : T(x) = x\}$. $V_0 = V_0(G) = \bigcap_{g \in G} V_{T_g}$. A group $G \leq O(V)$ is *effective* if $V_0(G) = 0$.

Theorem 49: Suppose G is generated by the reflections $s_r, r \in \{r_1, \ldots, r_k\}$. Then G is effective iff $\{r_1, \ldots, r_k\}$ is a basis.

Proof: Set $W = \bigcap r_i^\perp, 1 \leq i \leq k$. Note that each $T \in G$, T is a product of the generating reflections. $T_{|W} = 1$ so $W \subseteq V_0(G)$ but $x \in V_0(G)$, each generating reflection fixes x so $x \in r_i^\perp$ for each i. This $x \in W$ and $W = V_0(G)$ and $W^\perp = V$ but $W^\perp = (\bigcap_{i=1}^k r_i^\perp)^\perp = \sum_{i=1}^k r_i^{\perp\perp}$ and so the r_i span $W^\perp$ and the result holds.

Definition 11: Suppose G is generated by the reflections $s_r, r \in R = \{r_1, \ldots, r_k\}$. $\Delta = \{T_g(r_j), g \in G, 1 \leq j \leq k\}$ is called a *root system*. $\Delta_t^+ = \{r \in \Delta : (t,r) > 0\}$ and $\Delta_t^- = \{r \in \Delta : (t,r) < 0\}$.

Theorem 50: Suppose G is generated by the reflections $s_r, r \in R = \{r_1, \ldots, r_k\}$ and G is effective. If a root system Δ for G is finite, so is G.

Proof: If $T \in G$, $T(\Delta) = \Delta$ and G is a permutation group on Δ. Since Δ is effective, it contains a basis so if $T_{|\Delta} = 1 \to T = 1$ and G is faithful on Δ so G is finite.

Definition 12: A finite effective group $G \leq O(V)$ generated by a finite set of reflections $s_r, r \in R = \{r_1, \ldots, r_k\}$ with root system Δ is called a *Coxeter group* with root system Δ. A *t-base* for Δ is a subset $\Pi \subseteq \Delta_t^+$ minimal with respect to the property that every $r \in \Delta_t^+$ is a linear combination of elements of Π with non-negative coefficients.

Theorem 51: If $r_i, r_j \in \Pi, i \neq j$ and $\lambda_i, \lambda_j > 0$ then $x = \lambda_i r_i - \lambda_j r_j$ is neither t-positive nor t-negative.

Proof: If x were positive, $x = \lambda_i r_i = \lambda_j r_j = \sum_{k=1}^m u_k r_k$ with all $u_k \geq 0$. If $\lambda_i \leq u_i$ then $0 = (u_i - \lambda_i) r_i + (u_j + \lambda_j) r_j + \sum u_k r_k, k \neq i, j \geq \lambda_j (t, r_j) > 0$, a contradiction. If $\lambda_i > u_i$ then $(\lambda_i - u_i) r_i = (u_j + \lambda_j) r_j + \sum u_k r_k : k \neq i, j$. So we can express r_i as a non-negative linear combination of elements of $\Pi \setminus \{r_i\}$ contradicting the minimality of Π. Thus x is not positive which is impossible by the above argument with i and j interchanged.

Theorem 52: If $r_i, r_j \in \Pi, i \neq j$ and s_i the reflection along r_i, then $s_i(r_j) \in \Delta^+$ and $(r_i, r_j) \leq 0$.

Proof: Since $s_i(r_j) \in \Delta$, $s_i(r_j)$ is either positive or negative, but $s_i(r_j) = r_j - 2(r_i, r_j) r_i$ with one coefficient positive. By previous result, both must be non-negative, so $(r_i, r_j) \leq 0$ and $s_i(r_j)$ is positive.

Theorem 53: If Π is a t-base for Δ then Π is a basis for V.

Proof: Since G is effective, Δ spans V. Since every $r \in \Delta$ is a linear combination of roots in Π, V is spanned by Π. The elements of Π are linear independent so Π is a basis.

Theorem 54: There is only one t-base for Δ.

Proof: Suppose Π_1 and Π_2 are two different t-bases. Since each root in Π_1 is a non-negative linear combination of roots in Π_2, the roots are related by a matrix A and $B = A^{-1}$. Let $a_1, \ldots, a_n$ be the rows of A and $b_1, \ldots, b_n$ be the rows of B. $AB = I$ and $a_1^\perp b_i, i \neq 1$. There is at most on j for which the jth entry in all the $b_1, \ldots, b_n$ is zero otherwise the b_i would be linearly dependent. A similar argument applies to the columns and so there is exactly one non-zero entry in each row and column and it must be 1 and so A is a permutation matrix and $\Pi_1 = \Pi_2$.

Theorem 55: Suppose $s_r, r \in \Pi$. If $r_i \in \Delta^+, r_i \neq r$ then $s_i(r) \in \Delta^+$.

Proof: If $r \in \Pi$, $s_i(r) \in \Delta^+$. If $r \notin \Pi$, $r = \sum_{i=1}^n \lambda_j r_j$ and at least one of the $\lambda_j > 0$ so $r_i \neq r_1$, $\lambda_1 > 0$ and $s_i(r) = \sum_{j=1}^n \lambda_j s_i(r_j)$. Since $s_i(r) \in \Delta$, it is either positive or negative and since $\lambda_1 > 0$, $s_i(r) \in \Delta^+$.

Definition 13: The reflections $s_r, r \in \Pi$ are called *fundamental reflections.* $H_G = \langle s_i \rangle$, where the s_i are the fundamental reflections.

Theorem 56: If $x \in V, \exists T \in H_G : (T(x), r_i) \geq 0, \forall r_i \in \Pi$.

Proof: Set $x_0 = \frac{1}{2} \sum_{r \in \Delta^+} r$. Since H_G is finite, $\exists T \in H_G$ for which $Tx, x_0)$ is maximal and $s_i(x_0) = x_0 - r_i$. By maximality, $(Tx, x_0) \geq (s_i(T(x)), x_0) = (Tx, x_0) - (Tx, r_i)$ so $(Tx, r_i) > 0$.

Theorem 57: If $r \in \Delta^+$ then $\exists T \in G : T(r) \in \Pi$ for some $T \in H_G$.

Proof: If $r \in \Pi$, set $g = 1$. If $r \notin \Pi$, by previous result, $\exists i : (r, r_i) > 0$ otherwise $\Pi \cup \{r\}$ would be linearly independent. Set $a_1 = s_1(r) = r - 2(r, r_1)r_1$ then $a_1 \in \Delta^+$ by the previous result and $(a_1, t) = (r, t) - 2(r, r_1)(r_1, t) < (r, t)$. If $a_1 \in \Pi$, put $T = s_1 \in H_G$. If $a_1 \notin \Pi$ reapply procedure to get $a_2 = s_2(a_1)$ with $(a_2, t) < (a_1, t)$. Eventually, this process terminates with If $a_k \in \Pi$, $a_k = s_k s_{k-1} \ldots s_1(r)$. Now put $T = s_k s_{k-1} \ldots s_1$ and we're done.

Theorem 58: $H_G = G$.

Proof: Since $G = \langle s_r : r \in \Delta \rangle$. STS $r \in \Delta^+$ then $s_r \in H_G$. Suppose $r \in \Delta^+$ so there is a $T \in G$ such that $T(r) \in \Pi$ say $T(r) = r_i$ and then $s_r = T^{-1} s_i T \in H_G$.

Theorem 59: If $T_g(\Pi) = \Pi$ then $g = 1$.

Proof: Suppose $T \neq 1$, by previous result, $T = s_1 s_2 \ldots s_k$. Assume k is minimal, we have $k > 0$. Since $T(\Pi) = \Pi$, $T(r_k) = s_1 s_2 \ldots s_k(r_k)$ so $s_1 s_2 \ldots s_{k-1} \in \Delta^-$. Put $a_0 = s_1 s_2 \ldots s_{k-1}(r_k)$, $a_1 = s_1(a_0)$, $\ldots$, $a_{k-1} = s_{k-1}(a_{k-2}) = r_k$. Now $a_0 \in \Delta^-$ but $a_{k-1} \in \Delta^+$. Suppose $a_0, a_1, \ldots, a_{j-1} \in \Delta^-$ but $a_j \in \Delta^+$ then $s_j(a_j) = a_{j-1} \in \Delta^-$ so by an earlier result $a_j = r_j$ and so $r_j = s_{j+1} \ldots s_{k-1}(r_k)$. But then $s_j = s_{j+1} \ldots s_{k-1} s_k (s_{j+1} \ldots s_{k-1})^{-1}$ so $T = s_1 s_2 \ldots s_k = s_1 s_2 \ldots s_{j-1} s_{j+1} \ldots s_k$ contradicting minimality.

Theorem 60: $T_g(\Delta_t^+) = \Delta_{T_g(t)}^+$ and $T(\Pi_t) = \Pi_{T(t)}$.

Proof: Every root in $T(\Delta_t^+)$ is a non-negative linear combination of roots in $T(\Pi_t)$. $T(\Delta_t^+) = T(\{r \in \Delta : (t, r) > 0\}) = \{s \in \Delta : (Tt, r) > 0\} = \Delta_{T(t)}^+$.

Theorem 61: If $T_g(\Delta^+) = \Delta^+$ then $g = 1$.

Proof: $\Delta_t^+ = T(\Delta_t^+) = \Delta_{\Pi(t)}^+$ so $\Pi_t = \Pi_{T(t)}$ but then $T(\Pi_t) = \Pi_t$ and $t = 1$.

Definition 14: $F_t = \{x \in V : (x, r_i) > 0, \forall r_i \in \Pi\}$.

Theorem 62: $F = F_t$ is a fundamental region for the Coxeter group G.

Proof: F is open. Suppose $T \in G$ and $x \in F \cap T(F)$ and set $R = T^{-1}$ then $R(x) \in F$ and $(x, r_i) > 0, \forall i$ so $(x, r_i) > 0, r \in \Delta_t^+$. Thus $\Delta_x = \Delta_t$ and $\Pi_t = \Pi_x$ also $\Pi_{R(x)} = \Pi_t$. By a previous result, $\Pi_t = \Pi_{Rx} = R(\Pi_x) = R(\Pi_t)$ and $R = T = 1$. Finally, if $y \in V$ then by a previous result, $\exists T : (Ty, r_i) \geq 0, \forall r_i \in \Pi$ and so $T(y) \in F^c$. Thus $y \in T^{-1}(F^c) = T^{-1}(F)^c$ so $V = \bigcup\{(RF)^c : R \in G\}$ and we're done.

Theorem 63: Every reflection is conjugate to a fundamental reflection.

Proof: Suppose $s_r \in G$ and put $\cap P = r^\perp$. If F is the fundamental region aboive, so is $T(F), T \in G$. If $\mathcal{P} \cap T(F) \neq \emptyset$ for some T, choose $x \in \mathcal{P} \cap T(F)$ and there is a ball, B, of radius ϵ lying entirely in $T(F)$. Since $s_r(x) = x$, $s_r(B) = B$ but $B \nsubseteq \mathcal{P}$ so we can pick $y \in B \setminus \mathcal{P}$. $s_r(y) \in B \subseteq T(F)$ but $s_r(y) \neq y$ contradicting the fact that $T(F)$ is a fundamental region. $\cap P \subseteq V \setminus (\bigcup_{T \in G} T(F)) = \bigcup \mathcal{P}_i$ so $\mathcal{P} = \bigcup_{T \in G} \mathcal{P} \cap T(\mathcal{P}_i)$ or $\mathcal{P} \subseteq T(\mathcal{P}_i)$ for some T and some i. Since both $\mathcal{P}$ and $T(\mathcal{P}_i)$ are both hyperplanes, $\mathcal{P} = T(\mathcal{P}_i)$ and $r = T(r_i)$ or $r = -T(r_i) = T(s_i(r_i))$. In either case, $r \in \Delta$ and $s_r = TS_iT^{-1}$ and we're done.

Theorem 64: If $r_i, r_j \in \Pi$ is a t-base then $\exists p_{ij} \in \mathbb{Z}, p_{ij} \geq 1$ such that $\frac{(r_i, r_j)}{||r_i|| \cdot ||r_j||} = -cos(\frac{\pi}{p_{ij}})$.

Proof: If $i = j$ put $p_{ij} = 1$. If $i \neq j$, put $W = \mathbb{R}r_i + \mathbb{R}r_j$ and $H = \langle s_i, s_j \rangle$. Note that $(s_i)_{|W^\perp} = 1 = (s_j)_{|W^\perp}$ and $H = H_2^m \times 1$ where H_2^m is the dihedral group. $t = t_1 + t_2, t_1 \in W, t_2 \in W^\perp$ and r_i, r_j is a t_1-base for H_2^m in W. If not, $\exists r$, a root of H_2^m such that r, r_j is a t_1'-base for some $t_1' \in W$ and all of r, r_i, r_j are t_1'-positive. If r is a root of G, $r = \lambda_i r_i - \lambda_j r_j$ but this contradicts an earlier proposition. So r_i, r_j is a t_1-base. $(r_i, r_j) = cos(\theta) = cos(\pi - \varphi) = -cos(\varphi) = -cos(\frac{\pi}{p_{ij}})$.

Notation: $M = (m_{ij}), 1 \leq i, j \leq n, m_{ii} = 1, m_{ij} \in \mathbb{Z}, m_{ij} \geq 2$. Associate to each such matrix a graph with nodes $i, 1 \leq i \leq n$, (i, j) is an edge if $m_{ij} > 0$ if $m_{ij} > 2$, label it with $m_{ij} - 2$.

Definition 15: If $\Delta = \{r_1, \ldots, r_n\}, ||r_i|| = 1$ is a root system with unit vectors r_i defining a reflection along its associated hyperplane by $s_r(x) = x - 2(r, x)r$ and $\alpha_{ij} = -cos(\frac{\pi}{p_{ij}}) = (r_i, r_j)$, associate a marked graph with edges labeled by p_{ij} (unmarked edged have $p_{ij} = 3$) and associated quadratic form $Q(\vec{x}) = \sum \alpha_{ij} x_i x_j$.

Theorem 65: The Coxeter group is generated by the involutions s_r and $s_{r_i} s_{r_j}$ has order p_{ij}.

Proof: $s_i s_j$ is a rotation through an angle of $\frac{\pi}{p_{ij}}$.

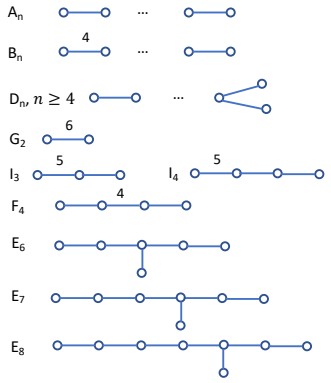
Theorem 66: If G_1 and G_2 are Coxeter groups with the same graph they are related by a similarity $T \in O(V)$ and $TG_1T^{-1} = G_2$.

Proof: Let Π_1 and Π_2 be two bases of unit vectors for the root systems of G_1 and G_2 respectively. Since they have the same graphs, after reordering, $\Pi_1 = \{r_1, \ldots, r_n\}$ and $\Pi_2 = \{r_1', \ldots, r_n'\}$ with $(r_i, r_j) = (r_i', r_j')$. Define $T : r_i \mapsto r_i'$ and extend by linearity. $s_i' = Ts_iT^{-1}$ and the result follows.

Theorem 67: The Coxeter graph of a Coxeter group is positive definite.

Proof: If the roots are unit vectors, then the matrix, A, defining the quadratic form is (a_{ij}) with $a_{ij} = (r_i, r_j)$. If $0 \neq x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, then $\sum_{i=1}^n x_i r_i \neq 0$ since the elements of Π are linearly independent and $Q(x) = \sum_{i,j} (r_i, r_j) x_i x_j = ||\sum_i x_i r_i||^2 > 0$. So Q is positive definite.

Coxeter groups



- If the root system Π is not a union of non-empty orthogonal sets, it is irreducible
- The elements of Π are called fundamental roots.
- G is connected iff G is irreducible
- If G is a connected positive definite Coxeter graph, it has one of the graphs $A_n, B_n, D_n, H_2^n, G_2, I_3, I_4, F_4, E_6, E_7, E_8$.
- G associated with $A_n, B_n, D_n, G_2, F_4, E_6, E_7, E_8$, satisfies the crystallographic condition, so $p_{ij} =$ 1,2,3,4,6.
- Quadratic form for a graph is $P = (c_{ij})$ where $c_{ij} = -\cos(\frac{\pi}{p_{ij}})$ where $p_{ij} = 3$ if two nodes are connected by unlabeled edge and the label if labelled. $c_{ii} = 1$ while $c_{ij} = 0$ if nodes i and j are not connected.
- If $r_i, r_j \in \Pi$, $\frac{(r_i, r_j)}{\|r_i\|\|r_j\|} = -\cos(\frac{\pi}{p_{ij}})$. If s_i, s_j are the reflections associated with r_i, r_j, $|s_i s_j| = p_{ij}$.
- $S_r(x) = x - 2\frac{(x,r)}{(r,r)} r$

Definition 16: A Coxeter group, G, with root system Δ, is *reducible* iff $\Pi = \Pi_1 \cup \Pi_2$, $\Pi_1 \perp \Pi_2$ and $\Pi_1 \neq \emptyset \neq \Pi_2$.

Theorem 69: The Coxeter graph of a Coxeter group is connected iff G is irreducible.

Proof: Clear from definitions.

Theorem 70: A subgraph, H, of a positive definite marked graph, G, is also positive definite.

Proof: Order the nodes of G, $a_1, a_2, \ldots, a_n$ such that $a_1, a_2, \ldots, a_k$ are the nodes of H and let the respective quadratic forms be denoted Q_G and Q_H. If Q_H is not positive define, $\exists x \neq 0, x = \sum_{i=1}^{k} x_k e_k \in \mathbb{R}^k$ such that $Q_H(x) \leq 0$. denoting as y, the extention of x to $\mathbb{R}^n$, $0 \geq Q_H(x) \geq Q_G(y) > 0$ which is a contradiction.

Definition 17: G satisfies the *crystallographic condition* if it fixes a lattice.

Theorem 71: If G satisfies the crystallographic condition, $p_{ij} = 1, 2, 3, 4, 6$.

Proof: $s_i s_j = \begin{pmatrix} A & 0_{n-2} \\ 0 & I_{n-2} \end{pmatrix}$ where $A = \begin{pmatrix} cos(\frac{2\pi}{m}) & -sin(\frac{2\pi}{m}) \\ sin(\frac{2\pi}{m}) & cos(\frac{2\pi}{m}) \end{pmatrix}$. $Tr(A) = 2cos(\frac{2\pi}{m}) + (n-2) \in \mathbb{Z}$ so $Tr(A) = 2cos(\frac{2\pi}{m}) \in \mathbb{Z}$ and $m = 1, 2, 3, 4, 6$.

Theorem 72: If G is a connected positive definite Coxeter graph then G is one of A_n, B_n, D_n, H_2^n, G_2, I_3, I_4, F_4, E_6, E_7, or E_8.

Proof: The graph for G can contain no cycles or the form would not be positive definite. If H_2^n is a subgraph of G, for any $n \geq 7$ then $G = H_2^n$ otherwise U_3 would be in the graph. Similarly, $G = G_2$ if it occurs. We can assume any branch is labeled 3, 4 or 5. Suppose that B_2 is a subgraph of G; it cannot occur more than twice otherwise some S_n would be a subgraph. G cannot have a branch point otherwise T_n would be a subgraph. If H_2^5 is a subgraph then $G = H_2^5$, $G = I_3$ or $G = I_4$. There are no other possibilities otherwise G would have Z_4 or Y_5 as a subgraph. If

B_2 is a subgraph but H_2^5 is not, then G may be B_n for some $n \geq 2$ or F_4. There are no other possibilities otherwise V_5 would be a subgraph of G. In the case that all branches are unmarked then G can have at most one bransh point and only 3 branches can emanate from any branch point otherwise Q_n would occur in G. If there is no branch point $G = A_n$. If G has one branch point, $G = D_n$ for some n or $G = E_6, E_7, E_8$ or R_7, R_8, R_9 would occur in G.

Theorem 73: If G has Coxeter graph A_n, B_n, D_n, H_2^n, G_2, I_3, I_4, F_4, E_6, E_7, or E_8 then G satisfies the crytallographic condition.

Proof: $\mathcal{L} = \sum_{i-1}^{n} k_i r_i$. If $p_{ij} = 3$, $||r_i|| = ||r_j||$ and $(r_i, r_j) = -\frac{1}{2}||r_i|| \cdot ||r_j||$ and $s_i(r_j) = r_i + r_j \in \mathcal{L}$. If $p_{ij} = 4$, $s_i(r_j) = r_j + r_i$ or $s_i(r_j) = r_j + 2r_i$. If $p_{ij} = 6$, $s_i(r_j) = r_j + r_i$ or $s_i(r_j) = r_j + 3r_i$. If $p_{ij} = 1$, $s_i(r_j) = -r_j$. If $p_{ij} = 2$, $s_i(r_j) = r_j$.

Graph	**Base**
A_n	$r_i = e_{i+1} - e_i$, $1 \leq i \leq n$
B_n	$r_1 = e_1$, $r_i = e_i - e_{i-1}$, $2 \leq i \leq n$
D_n	$r_1 = e_1 + e_2$, $r_i = e_{i+1} - e_i$, $2 \leq i \leq n$
H_2^n	$r_i = e_{i+1} - e_i$, $2 \leq i \leq n$
G_2	$r_i = e_2 - e_1$, $r_2 = e_1 - 2e_2 + e_3$
I_3	$r_1 = \beta(2\alpha + 1, 1, -2\alpha)$, $r_2 = \beta(-2\alpha - 1, 1, 2\alpha)$, $r_3 = \beta(2\alpha, -2\alpha - 1, 1)$
I_4	$r_1 = \beta(2\alpha + 1, 1, -2\alpha, 0)$, $r_2 = \beta(-2\alpha - 1, 1, 2\alpha, 0)$, $r_3 = \beta(2\alpha, -2\alpha - 1, 1, 0)$, $r_4 = \beta(2\alpha, 0, -2\alpha - 1, 1)$
F_4	$r_1 = 1\frac{1}{2}(\sum_{i=1}^{4} e_i$, $r_2 = e_1$, $r_3 = e_2 - e_1$, $r_4 = e_3 - e_2$
E_6	$r_1 = 1\frac{1}{2}(\sum_{i=1}^{3} e_i - \sum_{i=4}^{8} e_i)$, $r_i = e_i - e_{i-1}$, $2 \leq i \leq 6$
E_7	$r_1 = 1\frac{1}{2}(\sum_{i=1}^{3} e_i - \sum_{i=4}^{8} e_i)$, $r_i = e_i - e_{i-1}$, $2 \leq i \leq 7$
E_8	$r_1 = 1\frac{1}{2}(\sum_{i=1}^{3} e_i - \sum_{i=4}^{8} e_i)$, $r_i = e_i - e_{i-1}$, $2 \leq i \leq 8$

Base	$\lvert\Delta\rvert$	**Root System**
A_n	$n^2 + n$	$\pm(e_i - e_j)$
B_n	$2n^2$	$\pm e_i$, $\pm e_i \pm e_j$
D_n	$2n(n-1)$	$\pm e_i \pm e_j$
H_2^n	$2n$	$(cos(\frac{j\pi}{n}), sin(\frac{j\pi}{n}))$, $0 \leq j < 2n$
G_2	12	$\pm(e_i - e_j)$, $1 \leq i \leq 3$, $\pm(1, -2, 1)$, $(-2, 1, 1)$, $\pm(1, 1, -2)$
I_3	30	$\pm e_i$, $1 \leq i \leq 3$, $\beta(\pm(2\alpha + 1), \pm 1, \pm 2\alpha)$, and all even permutation of coordinates
I_4	120	$\pm e_i$, $1 \leq i \leq 4$, $\beta(\pm 2\alpha, 0, \pm(2\alpha + 1))$, and all even permutation of coordinates
F_4	48	$\pm e_i$, $\pm e_i \pm e_j$, $1 \leq i \leq 4$
E_8	240	$\pm e_i \pm e_j$, $1 \leq j < i \leq 8$, $\sum_{i=1}^{8} \epsilon_i e_i$, $\epsilon_i = \pm 1$, $\prod_{i=1}^{8} \epsilon_i = -1$
E_7	126	roots of E_8 orthogonal to $u = (1, 1, 1, 1, 1, 1, 1, -1)$
E_6	72	roots of E_8 orthogonal to $r_8 = e_8 - e_7$

Graph	$\lvert G\rvert$
A_n	$(n+1)!$
B_n	$2^n n!$
D_n	$2^{n-1} n!$
H_2^n	$2n$
G_2	12
F_4	$2^7 \cdot 3^2$
I_3	$2^3 \cdot 3 \cdot 5$
I_4	$2^6 \cdot 3^2 \cdot 5^2$
E_6	$2^7 \cdot 3^4 \cdot 5$
E_7	$2^{10} \cdot 3^4 \cdot 5 \cdot 7$
E_8	$2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$

9.7 Mathieu Groups

Construction: M_{11}: $\pi_1 = (123)(456)(789), \pi_2 = (147)(258)(369)$, $\langle \pi_1, \pi_2 \rangle = \mathbb{Z}_3 \times \mathbb{Z}_3$, $\rho_1 = (2437)(5698), \rho_2 = (2539)(4876)$, $\langle \rho_1, \rho_2 \rangle = Q \cong Q_8$. Set $M_9 = \langle \pi_1, \pi_2, \rho_1, \rho_2 \rangle$, $|M_9| = 72$. Now set $\sigma = (1,10)(4,5)(6,8)(7,9)$, $\mu = (4,7)(5,8)(6,9)(10,11)$, $\theta = (4,9)(5,7)(6,8)(11,12)$. $M_{10} = M_9 \cup M_9 \sigma M_9$, $(M_{10})_x = M_9$, $M_{11} = M_{10} \cup M_{10} \mu M_{10}$, $(M_{11})_x = M_{10}$, $M_{12} = M_{11} \cup M_{11} \theta M_{11}$, $(M_{12})_x = M_{11}$. $|M_{11}| = 7920$.

Theorem 74: $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. M_{11} is simple.

> *Proof:* Let N be a non-trivial normal subgroup, it is regular and all Sylow 11 subgroups are contained in it (there are 144 by Sylow) and $|G : N| = 5$. All Sylow 3 subgroups of M_{11} are in N and $\psi = \pi_1 \sigma \pi_2^2 \sigma^{-1}$ has order 5 which is a contradiction. Note that the symmetries of $S(4,5,11)$ also generate it and that $(M_{11})_a = PSL_2(9)$ and $(M_{22})_a = PSL_3(4)$.

9.8 Conway's Groups

Notation: Let $R(C)$ be the row space of C over $GF(2)$. Define the Γ to be the collection of $(v_1, v_2, \ldots, v_{24}) = v \in \mathbb{Z}^{24}$ such that (1) $\sum_{i=1}^{24} v_i = 4m$, (2) $v_i = m \pmod 4$, if $c_i = 0$, (3) $v_i = m + 2 \pmod 4$ if $c_i = 1$.

Definition 18: $L_8 \to \Lambda_8$: $v \in \Gamma_8$ iff $v \in L_8$ and $\sum_{i=1}^{8} v_i = 4m$. Contact number: $112 + 128 = 240$, radius: $\sqrt{2}$. *Alternate definition* of Λ_8: 8-tuples whose spheres are congruent (mod 2) to rows of A_8 or $\overline{A_8}$. Density is $\frac{\pi^4}{4!2^4}$.

Golay: L_8: $v \in L_8$ iff $v \in \mathbb{Z}^8$ and $v_i = a_i \pmod 2$ or $v_i = \overline{a}_i \pmod 2$. Generator matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}.$$

Definition 19: Let $R(C)$ be the row space of $\mathcal{G}_{24}$ over $GF(2)$. Define the *Leech Lattice*, Λ_{24}, as the vectors that satisfy the following conditions: Express coordinates in E_{24} in binary and retain the ones that satisfy the following conditions (a) the 24 1's bits are either all 0 or all 1, (b) the 2's bits form a row in $R(C)$, (c)

4's bits rows have even parity for points with 1's bits that are all 0 and odd otherwise. This is equivalent to the following: Suppose $\vec{c} \in R(C)$ and for $m \in \mathbb{Z}$, define $\vec{c}(m) = \{v \in \mathbb{Z}^{24} : \sum_i v_i = 4m, c_i = 0 \to v_i = m \,(\text{mod } 4), c_i = 1 \to v_i = m + 2 \,(\text{mod } 4)\}$, $\Lambda = \Lambda_{24} = \cup_m \vec{c}(m)$.

Theorem 75: In Λ, lattice points are seperated by a minimum distance of $4\sqrt{2}$. Lattice points a minumum distance from the origin have shapes: $(0^{16}, (\pm 2)^8)$, $(0^{22}, (\pm 4)^2)$, $((\pm 1)^{23}, (\pm 3))$. Hence the contact number is 98256 (lattice point with even parity) + 98304 (lattice point with odd parity) = 196,560; the density is .001929. Each pair of adjacent lattice points is adjacent to 4600 others. *Example:* $(4, 4, 0, \ldots, 0)$ is adjacent to $(4, 0, \ldots, 0)$ - there are 88 of these, $(2, 2, \ldots, 0)$ - there are 77×2^7 of these and $(1, 3, \ldots, 0)$ - there are 2048 of these. For the first Leech packing, the density is $\frac{2^{24}}{2 \times 2^{12}} = 2^{-11}$, first factor of 2 in denominator is from condition that the sum of the coordinates $= 0 \,(\text{mod } 4)$ and so the packing density is .0009647. The Leech lattice doubles this which is about .8 of the Rogers bound.

Noting that there must be an even number of -2's, for the Leech packing, lattice points with even coordinates are:

Shape	**Number**
$0^{16}, (-2)^8$	759
$0^{16}, (-2)^6, 2^2$	$759 \cdot \binom{8}{2} = 21252$
$0^{16}, (-2)^4, 2^4$	$759 \cdot \binom{8}{4} = 53130$
$0^{16}, (-2)^2, 2^6$	$759 \cdot \binom{8}{2} = 21252$
$0^{16}, 2^8$	759
$0^{22}, (-2)^2$	$\binom{24}{2} = 276$
$0^{22}, -2, 2$	$24 \cdot 23 = 552$
$0^{22}, 2^2$	$\binom{24}{2} = 276$
Total	98256

The lattice points with odd coordinates are:

Shape	**Number**
$(-1)^{23}, 3$	24
$(-1)^{16}, (1)^7, -3$	$759 \cdot 8 = 6,072$
$(-1)^{15}, (1)^8, 3$	$759 \cdot 16 = 12,144$
$(-1)^{12}, (1)^{11}, -3$	$2576 \cdot 12 = 30,912$
$(-1)^{11}, (1)^{12}, 3$	$2576 \cdot 12 = 30,912$
$(-1)^8, (1)^{15}, -3$	$759 \cdot 16 = 12,144$
$(-1)^7, (1)^{16}, 3$	$759 \cdot 8 = 6,072$
$(1)^{23}, -3$	24
Total	98304

There are 4600 vertices adjacent to 2 adjacent simplex, 891 vertices adjacent to 3 adjacent simplex, 336 vertices adjacent to 4 adjacent simplex and 170 vertices adjacent to 5 adjacent simplex. This gives a dihedral like estimate on the size of the symmetry group.

Definition of Conway's group: $\cdot\mathbf{O}$ is the set of rotations in $\mathbb{R}^{24}$ fixing O pointwise and Λ setwise.

Notation: $v_S = \sum_{i \in S} v_i$. $Q = \{x^2 : x \in F_{23}\}, N = \Omega \setminus Q$. $A + B = A \setminus B \cup B \setminus A$. $N_i = \{n - i, n \in N\}$. Golay code, $\mathcal{C}$, is generated by N_i, N_Ω. $N_A = \sum_{a \in A} N_a$. $C \in \mathcal{C}$ iff $N_C = 0$. $\Omega = PL(23)$, $\alpha : x \mapsto x + 1$, $\beta : x \mapsto 2x$, $\gamma : x \mapsto \frac{-1}{x}$, $\delta : x \mapsto 9x^3, x \notin Q$ and $\delta : x \mapsto \frac{x^3}{9}, x \in Q$. $L_2(23) = PSL_2(23) = \langle \alpha, \gamma \rangle$,

$M_{24} = \langle \alpha, \gamma, \delta \rangle$. If $\pi \in S_\Omega$, define $(v_i)^\pi = v_{\pi(i)}$. $\epsilon_S(v_i) = -v_i, i \in S$ and $\epsilon_S(v_i) = v_i, i \notin S$.

Theorem 76: The set $G\Lambda = \{2v_K, K \in R(C)\} \cup \{v_\Omega - 4v_\infty\}$ generates Λ. If $v, w \in G\Lambda$, then $v \cdot v = 16n$ and $v \cdot w = 0 \,(\mathrm{mod}\, 8)$. $\Lambda_n = \{x \in \Lambda, x \cdot x = 16n\}$. $\Lambda_1 = \emptyset$, Λ_2 consists of Λ_2^2 of shape $(0^{16}, (\pm 2)^8)$ - there are 97152 of these, Λ_2^3 of shape $((\pm 1)^{23}, (\pm 3)^1)$ - there are $98,304$ of these, Λ_2^4 of shape $(0^{22}, (\pm 4)^2)$ - there are 1104 of these. In tabular form:

Name	Shape	Number
Λ_2^2	$0^{16}, \pm 2^8$	$759 \cdot 2^7$
Λ_2^3	$\pm 1^{22}, \pm 3$	$24 \cdot 2^{12}$
Λ_2^4	$0^{22}, \pm 4^4$	$\binom{24}{2} \cdot 2^2$

Notation: If $S \in R(C)$, $\epsilon_S \in .O$. $E = \langle \epsilon_S \rangle_{S \in R(C)}$, $M = M_{24}$. $N = EM$. $T_0 = \{0, 3, 15, \infty\}$, $T_1 = \{1, 12, 21, 22\}$, $T_2 = \{2, 7, 11, 13\}$, $T_3 = \{4, 10, 16, 17\}$, $T_4 = \{5, 6, 9, 19\}$, $T_5 = \{8, 14, 18, 20\}$, $B = \{T_0, T_1, T_2, T_3, T_4, T_5\}$.

Theorem 77: $\lambda \in .O$ and λ fixes v_i (some i) iff $\lambda \in N$.

Proof of $\rightarrow$: Suppose $\lambda \in .O$ and $\lambda(v_i) = v_i$. If $\lambda(v_j) = w_j, i \neq j$ then $(v_i, w_j) = 0$. Since $4v_i + 4v_j \in \Lambda_2$, $4v_i + 4w_j \in \Lambda_2$. Examining the elements of Λ_2, we see $w_j = \pm v_k$ for some $k \in \Omega$ since $8w_j \in \Lambda$ and $4w_j \notin \Lambda$. Distinct values of j yield distinct values of k. Thus $\lambda = \pi\epsilon_S$, $S \subseteq \Omega, \pi \in S_{24}$. The non-zero coordinates of $\lambda(2v_K), K$ an octet are in the coordinate postions $\pi(K)$, so $\pi(K)$ is an octet and $\pi \in M_{24} = M$. $\lambda(v_\Omega - 4v_\infty)$ is a lattice point of the same shape and the coordinates are $= 1 \,(\mathrm{mod}\, 4)$. $\epsilon_S : v_i \mapsto -v_i, i \in S$ so the coordinates of $\lambda(v_\Omega - 4v_\infty)$ which are $= 3 \,(\mathrm{mod}\, 4)$ are in the places $\pi(S)$ and so $S \in R(C)$. So $\lambda = \pi\epsilon_S \in N$.

Theorem 78: If $\lambda(\Lambda_2^4) = \Lambda_2^4$ then $\lambda \in N$.

Proof: We use the following lemma:
Lemma: If $\lambda \in .O$ and $|\lambda| = p$, a prime then $p \leq 23$ further, no element of $.O$ has order $13 \cdot 23$.

Let H be the symmetries fixing Λ_2^4 as a whole and $x = 4v_i + 4v_j$ and N_x is the subgroup fixing x. N only changes signs and permutes coordinates so $N : \Lambda_2^4 \rightarrow \Lambda_2^4$ and fixes $\Lambda_2^4(x)$ as a whole. There are $2^2\binom{22}{2} = 924$ vectors of the form $\pm 4v_h \pm 4v_k$ are perpendicular to $\pm(4v_i - 4v_j)$ with h, i, j, k distinct and so are $\pm(4v_i - 4v_j)$. These 926 vectors form $\Lambda_2^4(x)$. N_x is 2-transitive so $\exists \sigma : (4v_i - 4v_j) \mapsto \pm(4v_i - 4v_j)$ and no other elements are in this orbit. Thus $\{(4v_i - 4v_j), -(4v_i - 4v_j)\}$ form a single orbit. $N_x \subseteq H_x$ and the orbits of H_x are a union of N_x orbits. As a result, it is either all 926 orbits or the N_x orbits. In the latter case, $|H_x : H_{x,y}| = 926 = 2 \cdot 463$ which contradicts the lemma. So we know H_x has 2 orbits on $\Lambda_2^4(x)$ and maps $(4v_i - 4v_j)$ to itself or it's negative. In the first case, $\lambda(v_i) = v_i$ and $\lambda \in N$ by the previous theorem. In the second case, $\lambda(v_i) = v_j$ and hence $(4v_i + 4v_h) \mapsto (\pm 4v_j \pm 4v_k), h \neq j$ and again $\lambda \in N$. Thus $H_x \subseteq N$ and $H_x \subseteq N_x$ and therefore $H \subseteq N$.

Theorem 79: There is a subgroup isomorphic to $L_2(23)$ which is transitive on octads.

Proof: There is a copy of $L_2(23)$ in M_{24}.

Definition 20: $\epsilon(v_i) = v_i$ if $i \notin Q$ and $-v_i$ if $i \in Q$.

Theorem 80: $N = \langle \alpha, \beta, \gamma, \delta, \epsilon \rangle$.

Proof: Applying permutations from the right, note $\epsilon_K = \epsilon\alpha\delta\alpha\epsilon\alpha^{-1}\delta^{-1}\alpha^{-1}$, $K = \{0, 1, 4, 5, 11, 12, 14, 22\}$. If L is another 8-set and $\theta : K \to L$ then $\epsilon_L = \theta^{-1}\epsilon_K\theta$.

Theorem 81: N is a proper subgroup of $.O$.

Proof: Let $T = T_0$ be any 4-set of Ω. T lies in 5, 8 sets $T + T_1, T + T_2, \ldots, T + T_5$, where T_i is the complement of T in the i-th 8-set. Ω is the disjoint union of 6, 4-sets. $B = \{T_0, T_1, \ldots, T_5\}$. $\eta = \eta_B : v_i \mapsto v_i - \frac{1}{2}v_{T_j}$ and $\zeta_T = \eta\epsilon_T$. $\zeta_T^2 = 1$. $\zeta_T \in .O$ and $\zeta_T \notin N$.

Theorem 82: H_x is transitive on $\Lambda_2(x)$.

Proof: Let $x = v_\Omega - v_\infty$. The order of each orbit of H_x on $\Lambda_2(x)$ has order divisible by 23.

Theorem 83: If $H > N$, H is transitive on Λ_2 and $H = .O$. $|.O| = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 = 8,315,553,613,086,720,000$.

Proof: (1) Λ_2^2, Λ_2^3, Λ_2^4 are all N-orbits. A counting argument shows that the union of two of them can't be an H orbit (otherwise, $p \mid |.O|$ for $p > 23$). Now define $\Lambda_2(x) = \{y : y \in \Lambda_2, y \perp x\}$. Recall H_x is transitive on $\Lambda_2(x)$. Since M_{24} is 5−transitive $|H_x : H_{x,y}| = 926$ and $|.O| = |H| = 196560 \cdot |H_x|$; further, H_x is transitive on $\Lambda_2(x) = \{y : y \perp x\}$. An orbit of H_x has 93150 elements so $|H_x| = (93150)|H_{x,y}|$ and $H_{x,y} = E_{10}M_{22}$. This gives the order of H and shows $H = .O$.

Definition 21: For $x \in \Lambda_2$, define $\{x, -x\}$ is called a diameter. $\overline{\Lambda_2}$ is the set of 98280 diameters. $.1 = .O_d, d = \{x, -x\}, x \in \Lambda_2$

Theorem 84: N is maximal in $.O$. $.O = \langle N, \zeta\rangle$.

Proof: By the theorem, if $H > N$, $H = .O$. The second statement follows from $\zeta \notin N$ and $\zeta \in .O$.

Theorem 85: $.O$ is transitive on ordered pairs of points of vectors of Λ_2 with a given scalar product.

Proof: $\Lambda_2 = \{v \in \Lambda : v \cdot v = 16 \cdot 2\}$. By looking at products of vectors of standard type, the possible products are $0, \pm 8, \pm 16, \pm 32$. Put $\Lambda_2(x, m) = \{y : (x, y) = m\}$. We find orbits of N_x on $\Lambda_2(x, 16)$ and show $\Lambda_2(x, 16)$ is a single orbit of $.O_x$.

Observation: Let φ be an octad, say $\{0, 1, 2, 3, 4, 7, 10, 12\}$, and $i \notin \varphi$; suppose K is the subgroup fixing φ, setwise and $H = K_i$. The subset fixed is of codimension 8 so it has dimension 4. K acts naturally on this 4-dimensional subspace. $K \approx 2^4 L_4(2)$.

Theorem 86: $.1 \cong .O/\mathbb{Z}(.O)$ and $|\mathbb{Z}(.O)| = 2$.

Proof: Suppose $\lambda \notin \{\pm 1\} \in \mathbb{Z}(.O)$. $\theta_i = \alpha^{23-i}\gamma\alpha\gamma\alpha^i$ fixes i and moves all other points of Ω. (1) λ cannot send $v_j \mapsto \pm v_j, \forall j$ since $(v_j)\lambda\alpha = -v_{j+1}$ and $(v_j)\alpha\lambda = v_{j+1}$. (2) λ cannot map $v_i \mapsto \pm v_j, i \neq j$, $(v_i)\lambda\theta_i = \pm(v_j)\theta_i = \pm v_k \neq \pm v_j$, but $(v_i)\theta_i\lambda = \pm(v_j)$. (3) Remaining case, namely, $\lambda : v_i \mapsto w \neq \pm v_j, j \in \Omega$ is impossible too. If $(v_j)\lambda = w \neq \pm v_k$, any k. $(8v_i)\lambda \in \Lambda_4$ and has one of the following form $(0^{23}, \pm 8^1)$, $(\pm 0^{20}, \pm 4^4)$, $(\pm 0^{16}, \pm 2^7, \pm 6^1)$, $(\pm 0^{14}, \pm 2^8, \pm 4^2)$, $(\pm 0^{11}, \pm 2^{12}, \pm 4^1)$, $(\pm 0^8, \pm 2^{16})$, $(\pm 1^{21}, \pm 3^2, \pm 5^1)$, $(\pm 1^{19}, \pm 3^5)$. The only one fixed by θ_i is $8v_i$. Thus $(v_i)\lambda\theta_i = (w)\theta_i \neq w$ but $(v_i)\theta_i\lambda = w$ and the theorem holds.

Theorem 87: $.1$ acts primitively on $\overline{\Lambda_2}$.

Proof: Each element of .1 permutes 98280 diameters. Since $.O$ is transitive on Λ_2, .1 is transitive for diameters. Suppose .1 is imprimitive. $|S_1| \mid 98280$. Let $\overline{x} \in S_1$. Since $|S_1| \geq 1, \exists y \in S_1$ whose orbit under $.1_{\overline{x}}$ has order $4600, 47104, 46575$. Since .1 fixes $\overline{x}$, $.1 : S_1 \to S_1$ and $|S_1| \geq 4601$. None divide 98280 so $\exists \overline{z} \neq \overline{x}$ outside S_1. But then S_1 which has at least $1 + 4600 + 46575 = 51176$ and thus must be all of $\overline{\Lambda_2}$. This contradicts the assumed imprimitivity of .1.

Theorem 88: $.1 = .O/\mathbb{Z}(.O)$ is simple.

Proof: Suppose $\mathbb{Z}(H) \subsetneq H \subsetneq .O$. (1) H is transitive on $\overline{\Lambda_2}$. If not $\exists \overline{x} = \{x, -x\}$ and $y \in \Lambda_2 : \eta(x) = y, \eta \in H$. $.O$ is transitive on $\overline{\Lambda}_2$. Orbits of H in $\overline{\Lambda}_2$ are of equal size. (2) N is not normal in .0. This is proved by looking at B, the 4-subsets defined above. (3) $H = N$. $|H : H_x| = 13 \cdot 7560$. Let $P \in S_{13}$. Since H is normal, all the sylow 13 subgroups of $.O$ are in H so $| > O : N_{.O}(P) = |ccl_{.O}(P)| = |ccl_H(P)| = |H : N_H(P)|$ and $|.O : H| = |N_{.O}(P) : N_H(P)|$ with $N_H(P) = N_{,O}(P) \cap H$. Thus $|.O| = |N_{.O}(P)H| = \frac{|N_{.O}(P)| \cdot |H|}{|N_{.O}(P) \cap H|}$ and $23 \mid |N_{.O}(P)|$ or $23 \mid |H|$. In the former case, put $K = \langle \lambda \rangle$, $P = \langle \mu \rangle$, $|\lambda| = 13$, but then $|PK| = 13 \cdot 23$ which contradicts an earlier lemma. In the latter case, $23 \mid |H|$ so $H \cap N = N$ but N is maximal so $H = N$. Now we have $H \lhd .O$ and $H = N$ but N is not normal and this establishes the result. $\zeta \in .1 : x \mapsto z$, $\lambda \in H : x \mapsto w$. $\zeta(w) = \zeta(\lambda(x)) = \zeta\lambda\zeta^{-1}(z)$ is in orbit of z sinze $\zeta\lambda\zeta^{-1} \in H$. .1 preserves orbits in Λ_2 and the orbits are sets of imprimitivity for .1 on $\overline{\Lambda}_2$ which contradicts the previous result. For $x \in \overline{\Lambda}_2$, $|H : H_x| = |\overline{\Lambda}_2| = 98280 = 13 \cdot 7560$. Let $P \in S_{13}(H)$ all such are H conjugate and $|.O : N_{.O}(P)| = |H : N_H(P)|$.

Conway's other simple groups: $.2 = \{x \in .O,\ x$ stabilizes 2 points $v, w \in \Lambda_2 : |v - w| = 4\sqrt{2}\}$. $.3 = \{x \in .O$, where x stabilizes 2 points $v, w \in \Lambda_2 : |v - w| = 4\sqrt{3}\}$.

9.9 Centralizers of involutions (following Suzuki):

First we'll compute the centralizer of an involution in $G = PSL_n(q)$. Most of the computations happen in $SL_n(q)$. Let $t \in Inv(G)$ and T be the matrix for t. Put $C = \{X : XT = \mu TX\}$ and $Z = \{\lambda I_n\}, \lambda^n = 1$. Finally, if $d = |Z|$, $d = (n, q-1)$. In G, $C_G(t) = C/Z$.

Theorem 1: If $G = PSL_n(q)$, q, odd, and $t \in Inv(G)$.
If n is odd, $n = r + s$, $\exists N \lhd C_G(t)$ such that N is a minimal central product of $SL_r(q)$ and $SL_s(q)$. $C_G(t)/N$ and $\mathbb{Z}(N)$ are cyclic with orders dividing $q-1$. If $n = 2m$ is even, $n = 2m$, in addition to the possibly above, with $r \neq s$, the following two possibilities arise:
(i) $\exists C_0 \lhd C_G(t)$ and $E \lhd C_G(t)$ with $r = s = m$ with $C_G(t)/E$ is dihedral, C_0/E and $\mathbb{Z}(E)$ are cyclic whose order divides $q - 1$. $\exists v \notin C_0, |v| = 2$ that interchanges the factors of E. such that N is a minimal central product of $SL_r(q)$ and $SL_s(q)$. $C_G(t)/N$ and $\mathbb{Z}(N)$ are cyclic with orders dividing $q - 1$.
(ii) $\exists C_0 \lhd C_G(t)$ and $E \lhd C_G(t)$ with $r = s = m$ with $E/F(E) = PSL_m(q^2)$, $\mathbb{Z}(E)$ is cyclic with order dividing $q + 1$, C_0/E is dihedral of order $q + 1$ or $2(q + 1)$ and there is an element of $C_G(t) \setminus C_0$ which acts like the non-identity element of $GF(q^2)$ over $GF(q)$.

Proof: If T is an involutions, $T^2 = \lambda I$. So T has minimal polynomial $(x + \rho)(x - \rho)$ or $x^2 - \lambda$ depending on whether $\sqrt{\lambda} \in GF(q)$. Either (i) $T = \begin{pmatrix} \rho I_r & 0 \\ 0 & -\rho I_s \end{pmatrix}$, or (ii) $T = \begin{pmatrix} 0 & I_m \\ \rho I_m & 0 \end{pmatrix}$.
$X = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$. Either (a) $X_2 = X_3 = 0$ and $det(X_1)det(X_2) = 1$ or (b) $r = s$, $X_1 = X_4 = 0$ and $det(X_2)det(-X_3) = 1$ In case (a), $\delta : X \to det(X_1)$ is a homomorphism and $K = key(\ delta) = SL_r(q) \times SL_s(q)$. Put $E = KZ/Z$ $E \lhd C/Z$ and $E = K/(K \cap Z)$

In case b, $X \to \mu(X)$ is a homomorphism. Put $A = X_1, B = X_2$ then $\begin{pmatrix} \rho I & I \\ -\rho I & I \end{pmatrix}\begin{pmatrix} A & B \\ \lambda B & A \end{pmatrix} = \begin{pmatrix} A+\rho B & 0 \\ 0 & A-\rho B \end{pmatrix}\begin{pmatrix} \rho I & I \\ -\rho I & I \end{pmatrix}$, and $\rho \in GF(q^2)$.
Now we can assume $n = 2m$. Again, T is an involutions, $T^2 = \lambda I$ and either (i) $T = \begin{pmatrix} \rho I_r & 0 \\ 0 & -\rho I_s \end{pmatrix}$, or (ii) $T = \begin{pmatrix} 0 & I_m \\ \lambda I_m & 0 \end{pmatrix}$. Let $J = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} \in C$. In case (i), The matricies X, the form C_1 or $C_1 + C_1 J$, where $C_1 = \{X : X_2 = X_3 = 0, det(X_1)det(X_4) = 1\}$. C_1 has index 2 in C. Again, $\delta : X \to det(X_1)$ is a homomorphism. Again $K = SL_m(q) \times SL_m(q)$ and $J^{-1}\begin{pmatrix} X_1 & 0 \\ 0 & X_4 \end{pmatrix} J = \begin{pmatrix} X_4 & 0 \\ 0 & X_1 \end{pmatrix}$. In case (ii), $X_1 = \mu X_4, \mu X_3 = \lambda X_2, \mu^2 = 1$. $\mu(X)$ is a homomorphism and $\begin{pmatrix} \rho I & I \\ -\rho I & I \end{pmatrix}\begin{pmatrix} A & B \\ \lambda B & A \end{pmatrix} = \begin{pmatrix} A+\rho B & 0 \\ 0 & A-\rho B \end{pmatrix}\begin{pmatrix} \rho I & I \\ -\rho I & I \end{pmatrix}$, $\rho^2 = \lambda$.
$K \lhd C$ and C/K is dihedral.

. **Theorem 2** If $G = PSL_n(q)$, q, even, and $t \in Inv(G)$. $\exists E, Q : E \lhd C_G(t), Q \lhd C_G(t)$, $\{1\} \subset Q \subset E \subset C_G(t)$ with $C_G(t)/E$ is cyclic of order dividing $q-1$, E/Q is a minimal central product of $SL_r(q)$ and $SL_s(q)$ with $n = 2r + s$ and Q is a 2-group of order at most 2. Further, $C_G(Q) \subset Q$.

Proof: $T = \begin{pmatrix} I_r & 0 & I_r \\ 0 & \rho I_s & 0 \\ 0 & 0 & I_r \end{pmatrix}$. $X = \begin{pmatrix} R & L & M \\ 0 & S & N \\ 0 & 0 & R \end{pmatrix}$, $n = 2r + s, det(r)^2 det(S)1$. $\delta : X \to det(R)$ is a homomorphism. If $X \in K$, $R \in SL_r(q)$ and $S \in SL_s(q)$. $X \to SL_r(q) \times SL_s(q)$ is a homomorphism with kernel Q_1. $E = KZ/Z, Q = Q_1 Z/Z$. $E/Q = K/(K \cap Q_1)$. K/Q_1 has matricies of the form $\begin{pmatrix} R & 0 & 0 \\ 0 & S & 0 \\ 0 & 0 & S \end{pmatrix}$. $R = \lambda I_r$, $S = \lambda I_s$, $L = 0$ and $N = 0$.

Now consider the remaining linear groups. Let $G(V, f)$ be the group associated with a bilinear, f, form with $f(\alpha u, \beta v) = \alpha\overline{\beta} f(u, v)$. f can be symplectic, orthogonal, unitary or bilinear. $Z = \mathbb{Z}(G(V, f))$ and $G = G(V, f)/Z$. The simple group associated with G is G itself if f is symplectic, hermitian or unitary and G' if f is orthogonal. **Theorem 3:** $G = PSp_{2m}(q)$, q odd. $t \in Inv(G)$. $C_G(t)$ has one of the following forms:
(i) $C_G(t)$ is a minimal central product of $Sp_{2r}(q)$ and $Sp_{2s}(q)$, $r + s = m$, $r \neq s$
(ii) $\exists C_1 \lhd C_g(t)$ of index 2 where C_1 is a minimal central product of two copies of $SL_{2m}(q)$. $Y \in C = C_1$ interchanges the factors.
(iii) $\exists C_1 \lhd C_g(t)$ of index 2 where $C_1 = GL_m(q)/\langle -1 \rangle$ and $C \setminus C_1$ has a automorphism corresponding to $A = rightarrow""^t A^{-1}$.
(iv) $\exists C_1 \lhd C_g(t)$ of index 2 where $C_1 = U_m(q)/\langle -1 \rangle$ and $q = 3 \pmod 4$.

Proof:

Theorem 4: $G = PSp_{2m}(q)$, q even. $t \in Inv(G)$. $\exists E \lhd C_G(t)$ with E a 2-group of class at most 2, $C_G(R) \subseteq E$, $C_G(t)/E = G_0 \times Sp_s(q)$ where G_0 is (i) $Sp_r(q)$, or (ii) $Sp_{r-1}(q)$, or (iii) the semidirect product of $Sp_{r-2}(q)$ and a special 2-group, Q of order Q^{r-1}

Proof:

Theorem 5 : $G = PSU_n(q)$, q odd. $t \in Inv(G)$. $C_G(t)$ has one of the following forms:
(i) $\exists N \lhd C_G(t)$ which is a minimal central product of $SU_r(q)$ and $SU_s(q)$. $C_G(t)/N$ and N are cyclic groups with orders dividing $q + 1$.

(ii) situation (i) with two factors that are exchanged by an element of $C_G(t) - N$
(iii) $\exists C_0 \lhd C_G(t)$ of index 2 and $E \lhd C_G(t)$ with $E/\mathbb{Z}(E) = PSL_m(q^2)$.

Proof:

Theorem 6: $G = PSU_n(q)$, q even. $t \in Inv(G)$. $C_G(t)$ has one of the following forms:

Proof:

Theorem 7: $G = P\Omega_n(q)$, q odd. $t \in Inv(G)$. $\exists E \lhd C$ with $C_G(t)/E$ solvable. and E is one of $SL_m(q)/\langle -1\rangle$ or $SU_m(q)/\langle -1\rangle$ or a central product of $\Omega_r(q)$ and $\Omega_s(q)$.

Proof:

Theorem 8: $G = P\Omega_{\epsilon,2m}(q)$, q even. $t \in Inv(G)$. $C_G(t)$ has one of the following forms:

Proof:

Chapter 10

Permutation representations

10.1 Basic Results

Lemma 1: Let $H \leq G$ and $Hg_1, ..., Hg_n$ be the cosets; the map $\pi(g) : \langle Hg_1, ..., Hg_n \rangle \mapsto \langle Hg_1 g, ..., Hg_n g \rangle$ is a map from G to Σ_n whose kernel is the largest normal subgroup of G in H; in fact, $ker(\pi) = \bigcap_{i=1}^{n} H^{x_i}$.

Corollary: If G is simple and $G > H$ with $|G : H| = k$ then $|G| \mid k!$. Equivalently, if $|G| \nmid k!$, $|ker(\pi)| > 1$ as above, so G has a normal subgroup.

10.2 Imprimitivity

Definition 1: A *system of imprimitivity for permutation group G:* is a set, $\mathcal{B} = \{\Delta_i\}$ $|\Delta_i| > 1$, with the property that for $\Delta \in \mathcal{B}, g \in G$ either $\Delta \cap g\Delta = \emptyset$ or $\Delta = g\Delta$.

Theorem: 1 If $H < G$ and G is simple then $|G| \mid |G : H|!$.

Proof: Let $\pi : G \to Perm(G/H)$ be the map from G to the permutations on the right cosets of H in G. $G/ker(\pi)$ is an injection into $S_{|G:H|}$ and $ker(\pi) = 1$ so $|G| \mid |G : H|!$.

Definition 2: A permutation is *primitive* if there is no non-trivial set of imprimitivity.

Definition 3: Γ is G invariant if $\Gamma^G = \Gamma$ so Γ is a union of G orbits. $G/G_\Gamma \equiv G^\Gamma$.

Normal Subgroups of Primitive Groups Theorem: Let G be primitive on Ω and $1 \neq N \lhd G$. Then either $N \subseteq G_a$ or N acts transitively on Ω. If the action is regular, N is a minimal normal subgroup.

Proof: Let $\Delta(a) = Na$. If $\Delta(a) = \{a\}$, $N \subseteq G_a$ and we're done. Suppose $a \neq b \in Na$. Since G is transitive, $\exists g \in G : ga = b$ so $g\Delta(a) = gNa = (gNg^{-1})ga = Nb = \Delta(b)$. But $b \in Na$ so $Nb = Na$. Thus $\Delta(a)$ is an imprimitive block. Since G^Ω is primitive, $\Delta(a) = \Omega$ and N is transitive.

Iwasawa's Theorem: Let G be a primitive permutation group and suppose (1) $G' = G$ and (2) $\exists A$ with A solvable and $A \lhd G_a : G = \langle A^G \rangle$ then G is simple.

Proof: Let $1 < N \lhd G$. Since N is transitive by the previous result, $NG_a = G$. Further, $G_a \subseteq N_G(NA)$ and $N \subseteq N_G(NA)$ and so $G = NG_a = N_G(NA)$. So $NA \lhd G$ and $(NA)^G = NA \lhd G$ but $\langle A^G \rangle = G$ so $NA = G$. Since A is solvable, so is G/N and $(G/N)' = (G/N)$ and so $N = G$.

Theorem 2: If $\Delta \subseteq \Omega$ and $\alpha \in \Omega$ then $\psi(\alpha) = \bigcap_{\alpha \in g\Delta} g\Delta$ is a block of a transitive group $G \subseteq Sym(\Omega)$.

Proof: Let $\beta = h\alpha$ and note that $h\psi(\alpha) = \bigcap_{h\alpha \in hg\Delta} hg\Delta = \psi(\beta)$ so $|\psi(\alpha)| = |\psi(\beta)|$. Now suppose $\beta \in \psi(\alpha)$ then $\alpha \in g\Delta \to \beta \in g\Delta$ so $\bigcap_{\beta \in g\Delta} g\Delta \supseteq \bigcap_{\alpha \in g\Delta} g\Delta$ and so, $\psi(\beta) = \psi(\alpha)$ since they both have the same number of elements. We have shown $\beta \in \psi(\alpha) \to \psi(\beta) = \psi(\alpha)$ and thus $\psi(\alpha) \cap \psi(\beta) = \emptyset$ or $\psi(\alpha) = \psi(\beta)$.

Theorem 3: G is primitive iff G_α is maximal. A transitive group is imprimitive iff $\exists Z$: $G_\alpha < Z < G$.

Proof: Suppose $b \neq a$. Suppose $a, b \in \Delta_i$ with $\{\Delta_i\}$ a set of imprimitivity and suppose $ga = b$. Then $g\Delta_i = \Delta_i$ and $\langle g, G_a \rangle > G_a$ stabilises the block containing a. So if G_a is not primitive then G_a is not maximal. If $G > M > G_a$ and M is maximal, Ma is a set of imprimitivity so G is not primitive.

Definition 4: G acts *regularly* on Ω if $\forall \alpha, \beta \in \Omega, \exists! g : \alpha^g = \beta$.

Theorem 4: Let G be $n-$fold transitive on Ω, $n \geq 2$ and N a regular normal subgroup of G then $n \leq 4$ and (1) If $n = 2$, N is an elementary abelian $p-$group; (2) If $n = 3$, N is an elementary abelian $2-$group or $N = C_3$ and $G = S_3$; (3) If $n = 4$, $N = C_2 \times C_2$ and $G = S_4$.

Proof: Let $n \geq 2$ and $\alpha \in \Omega$. G_α is $(n-1)$-fold transitive on $\Omega - \{\alpha\}$ and hence on $N^\#$ so $\exists g : x^g = y, x, y \in N^\#$. Thus every element of $N^\#$ has the same order, p. $N = \mathbb{Z}(N)$ and N is abelian (and hence elementary abelian). If $n \geq 3$, $3 \leq |N| = |\Omega|$. If $n = 3$, $G = S_3$. If $p \geq 3$, $x_1 \neq x_1^{-1} = x_2$. Let x_3 be another element. Then $x_1^g = x_2, x_2^g = x_3$ for some g and this is contradictory so $p = 2$. If $n \geq 4$, N is an elementary abelian 2-group. Let $U = \langle x_1 \rangle \times \langle x_2 \rangle$. If $N \neq U$, put $x_3 = x_1 x_2$ and choose $x_4 \notin U$. Then $\exists g \in G : x_1^g = x_1$, $x_2^g = x_2$, and $x_3^g = x_4$ which is again contradictory.

Definition 5: Define $\mathcal{G}(G, \Omega)$ as the graph of G acting on Ω as follows: G acts on $\Omega \times \Omega$. Diagonal orbital is $\Delta_1 = \{(\alpha, \alpha)\}$. If $\Delta = \{(\alpha, \beta)\}$, $\Delta^* = \{(\beta, \alpha)\}$. Self paired if $\Delta^* = \Delta$. $\Delta(\alpha) = \{\beta : (\alpha, \beta) \in \Delta\}$ — corresponds to orbits of G_α. The *rank of the permutation group* is number of orbitals. $\Delta^p = \{(y, x) : (x, y) \in \Delta\}$ is called the *paired orbit*.

Theorem 5.1: (a) A non-diagonal orbital is self-paired iff (x, y) and (y, x) are in the same orbit.
(b) G has a non-diagonal self paired orbital iff G has even order.
(c) If G is of even order and rank-3, both non-diagonal orbitals are self paired.

Theorem 5.2: On a self-paired orbit Δ, the graph $\mathcal{G} = (G, X, \Delta)$ is symmetric and G is transitive on edges.

Proof: Since Δ is self-paired, the graph is symmetric.

Theorem 6: G is primitive iff $\mathcal{G}$ is connected.

Proof: G is maximal so $G = \langle G_x, G_y \rangle, x \neq y$.

Definition 6: A transitive permutation group is *regular* if $|X| = |G^X|$ or, equivalently $|G_x| = 1, \forall x \in X$ and G^X, transitive.

Theorem 7: Let X be a faithful primitive $G - set$ with G_x simple. Then either G is simple or every non-trivial normal subgroup H of G is a regular normal subgroup.

Proof: Suppose $1 \neq H \lhd G$. Since G is primitive, H is transitive. $H_x = H \cap G_x \lhd G_x$ so, since G_x is simple, $H_x = 1$ of $H_x = G_x$. If $H_x = 1$, H is a regular normal subgroup of G. So $H_x = G_x$ and since H is transitive, $|H : H_x| = |G : G_x|$, so G is simple.

Definition 7: A acts *semi-regularly* on G if $C_G(a) = 1, \forall a \in A^{\#}$.

Theorem 8: Suppose A acts semi-regularly on G. Then (1) $|G| = 1 \,(\mathrm{mod}\, |A|)$, (2) A is semi-regular on each $A-$invariant subgroups factor group of G, (3) $\forall p \in \pi(G)$, $\exists! A-$invariant Sylow $p-$subgroup of G, (4) $\forall a \in A, g \mapsto [g, a]$ is a permutation of G, (5) if $2||A|, \exists t : |t| = 2, t \in A : g^t = g^{-1}, g \in G$ and $G^{(1)} = 1$.

Proof: (1) each orbit of A on $G^{\#}$ has length $|A|$. (2) is clear (second part comes from coprime action). (3) By Schur, the set of A-invariant Sylow p-groups is non-empty. Since $C_G(A) = 1$ is transitive on this set, the subgroup is unique. (4) $[g, a] = [h, a]$ iff $hg^{-1} \in C_G(a)$. The commutator map is already an injection and since G is finite, it is a bijection. (5) Let $t \in Inv(A)$ and $g \in G$. By previous result, $g = [h, t]$ for some $h \in G$ and $g^t = (h^{-1}h^t)^t = g^{-1}$. Therefore $x^t = x^{-1}$ and G is abelian. Finally, if $s \in Inv(A)$, s inverts G so $st \in C_A(G) = 1$ and t is unique.

Theorem 9: Let Δ be an orbit of G and let $\delta \in \Delta$. For each $\gamma \in \Delta$ let $v(\gamma) \in G$ be such that $\delta \mapsto \gamma$. Finally, suppose S generates G. Then $G_\delta = \langle v(\gamma) s v(\gamma^s)^{-1} | \gamma \in \Delta, s \in S \rangle$.

Proof: See, Stellmacher.

10.3 Fixed point free automorphisms

Fixed Point Free: An automorphism, ϕ acting on G is fixed point free if $C_G(\phi) = 1$.

Lemma 1: Let ϕ be a fixed point free automorphism acting on G with $|\phi| = n$. Then (1) $y \in G$ then $y = x^{-1}(x\phi)$ for some x, and (2) $\forall x \in G, x(x\phi)(x\phi^2)\dots(x\phi^{n-1}) = 1$.

Proof: $x^{-1}(x\phi) = y^{-1}(y\phi) \to yx^{-1} = (yx^{-1})\phi$, so $x = y$. Thus $|x^{-1}(x\phi) : x \in G| = |G| - 1$ and (1) holds. Since $\exists y : x = y^{-1}(y\phi)$, so $x(x\phi)(x\phi^2)\dots(x\phi^{n-1}) = y^{-1}(y\phi)(y\phi^2)\dots(y\phi^{n-1})^{n-1}) = y^{-1}y = 1$.

Lemma 2: Let ϕ be a fixed point free automorphism acting on G then ϕ leaves a unique $S_p$subgroup of G invariant.

Proof: Let $Q \in S_p(G), (Q)\phi = y^{-1}Qy$. $y^{-1} = (z\phi)z^{-1}$ and $y = z(z^{-1}]phi)$. $Q\phi = (z\phi)(z^{-1}Qz)(z^{-1}\phi)$ and $(z^{-1}Qz)\phi = z^{-1}Qz$ and thus ϕ leaves $P = z^{-1}Qz$ fixed. If both P, Q are ϕ-invariant and $Q = x^{-1}Px$ then $Q = (x^{-1}\phi)P(x(phi)$ and $(x\phi)x^{-1} \in N(P) = N$ but N is ϕ-invariant and ϕ is fixed point free on N so $\exists z : y = (z\phi)z^{-1}$. $(z\phi)z^{-1} = (x\phi)x^{-1} \to x = z$.

Lemma 3: Let ϕ be a fixed point free automorphism acting on G, $H \lhd G$ and $H = H\phi$ then ϕ is fixed point free on G/H.

Proof: Let $\overline{G} = G/H$ and $\overline{x} = \overline{x}\phi$. $\overline{x}^{-1}(\overline{x}\phi)$ so $y = x^{-1}(x\phi) \in H$. Since ϕ induces a fixed point free automorphism on H, $y = z^{-1}(z\phi)$. So $x = z$, $x \in H$ and $\overline{x} = 1$. Thus ϕ induces a fixed point free automorphism on $\overline{G}$.

Lemma 4: Let ϕ be a fixed point free automorphism acting on G of order 2, then G is abelian.

Proof: Since $x(x\phi) = 1$, $x^{-1} = (x\phi)$. If $x, y \in G$, $y^{-1}x^{-1} = (xy)^{-1} = ((x\phi)(y\phi))^{-1} = x^{-1}y^{-1}$, so G is abelian.

Lemma 5: Let ϕ be a fixed point free automorphism acting on G of order 3, then G is nilpotent and $[x, x\phi] = 1, \forall x \in G$.

Proof: $x(x\phi)(x\phi^2) = 1$, so $x(x\phi) = (x\phi^2)^{-1}$ and x commutes with $x\phi$ for any $x \in G$. Let P be the unique ϕ-invariant S_p subgroup of $G, \forall p \in \pi(G)$. We show $P \lhd G$. Suppose not and $Q \neq P \in S_p(G)$ and pick $x \in Q \setminus P$, put $H = \langle x, x\phi \rangle$. H is a p-group since $[x, x\phi] = 1$ and $H' = 1$ and $H\phi = H$. So $H \subseteq P$ but then $x \in P$.

Thompson: Let G be a transitive permutation group on X and $1 \neq g \in G$ fixes no more than one element then $N = \{g : X_g = \emptyset\}$ is a normal subgroup of G. Thompson showed any finite group having a fixed point free automorphism of prime order is nilpotent.

Proof: Let G be a counterexample of minimal order and ϕ be a fixed point free automorphism of prime order r. G has a proper normal subgroup, $H \neq 1$ with $H\phi = H$. By induction, H is nilpotent and ϕ is a fixed point free automorphism on G/H so G/H is nilpotent and G is solvable. If G has no non-trivial normal subgroup, which is H-invariant. Let $P \in S_p(G), p \neq 2$ with $P\phi = P$. Put $N = N_G(\mathbb{Z}(J(P))), \mathbb{Z}(J(P)))$ *char* P. If $N < G$, N is nilpotent: N has a normal p-complement, K. By the Thompson p-complement theorem, $G = KP$, $K\phi = K$ so $K = 1$ and $P = G$ so G is nilpotent. We may assume G is solvable. Suppose $H_1, H_2 \lhd G$ $H_i\phi = H_i$, $H_1 \cap H_2 = 1$. $\overline{G}_i = G/H_i$ is nilpotent so $\overline{L} = \overline{G}_1 \times \overline{G}_2$ is too. $x\phi = (H_1 x, H_2 x)$. $\psi : G \to \overline{G}_1 \times \overline{G}_2$. $G\psi$ is nilpotent. Let N a minimal normal subgroup of G, N is elementary abelian and $\overline{G} = G/N$ is nilpotent. $\overline{G}$ is not a p-group. Let $\overline{Q} \in S_q(\overline{G})$ with $\overline{Q} = \overline{Q}\phi$, $q \neq p$. Let $\overline{M}$ be a minimal ϕ-invariant subgroup of $\Omega_1(\mathbb{Z}(\overline{Q}))$. $\overline{M} \neq 1$ and $\overline{M} \lhd \overline{G}$ since $\overline{G}$ is nilpotent. Let H be the inverse image of $\overline{M}$ then $H = NM$ and M is a non-trivial elementary abelian q-group. $H \lhd G$, $H\phi = H$ and $M\phi = M$. ϕ acts irreducibly on M. $H \subset G$ then H is nilpotent. M *char* $H \lhd G$ and M and N are two minimal normal ϕ-invariant subgroup and $M \cap N \neq 1$. $C_M(N)\phi = C_M(N)$ since ϕ acts irreducibly on M. Either $C_M(N) = 1$ or $C_M(N) = N$. If $C_M(N) = N$, G is nilpotent so $C_M(N) = 1$. Let G^* be the semidirect product of M by $\langle \phi \rangle$. G^* acts irreducibly on N as a vector space since $C_M(N) = 1$ and ϕ is fixed point free. But G^* is a p'-group $C_{M^*}(M) = M$ and G^*/M has order q so $C_N(\phi) \neq 1$.

O-Nan-Scott: Let G be a finite primitive permutation group of degree n and $H = soc(G)$. Then either (1) H is a regular elementary abelian p group for some p and G is isomorphic to a subgroup of $AGL_m(P)$; or, (2) H is isomorphic to T^m where T is a non-abelian simple group with a bunch of conditions.

10.4 Mathieu groups are simple

We will use one result from a future section here.

Theorem 1: Let N be a finite group $G \subseteq Aut(N)$. Then G acts as a permutation group on $N^{\#}$. Further,
(i) If G is transitive, then N is an elementary abelian p-group.
(ii) If G is 2-transitive, then N is either an elementary abelian 2-group or $|N| = 3$.
(iii) If G is 3-transitive, then $|N| = 4$.
(iv) G cannot be 4-transitive.

Proof: These are all clear.

Theorem 2: Let G be an transitive permutation group and $N \lhd G$. Then N is $\frac{1}{2}$ transitive. If $N \neq 1$ and G is primitive then N is transitive.

Proof: Let B be an orbit of N of minimal length. $B^{Ng} = B^{gN} = B^g$, so B^g is a union of orbits of N. By minimality of $|B|$, B^g is a single N orbit. These form a system of imprimitivity.

Theorem 3: Let G be primitive with no regular normal subgroups. If G_a is simple then G is simple.

Proof: Let $N \lhd G$. $N_a \leq (N \cap G_a) \lhd G_a$ so either $N_a = 1$ or $N = G_a$. If $N_a = 1$, N is a regular normal subgroup.

Theorem 4: Let G be m-transitive on A, $|A| = n$ with a regular normal subgroup, N.
(i) if $m = 2$, then $n = |N| = p^k$
(ii) if $m = 3$, then $n = 3$ or $n = 2^k$ or $n = 3$.
(iii) if $m = 4$, then $n = 4$.
(iv) We cannot have $m > 4$.

Proof:

Theorem 5: Let G be transitive and $H < G$ also be transitive. The $G = HG_a$

Proof: Clear.

Theorem: The Mathieu groups are simple.

Proof:
Step 1: M_{11} is simple.

Put $G = M_{11}$ so $|G| = 11 \cdot 10 \cdot 9 \cdot 8$. Let $P = \langle x \rangle$ be a subgroup of order 11. P acts transitively on Ω. If $P \subseteq A$, A, abelian, then A is transitive and regualr so $A = P$. Thus $C_G(P) = P$. Since $|Aut(P)| = 10$, $|N_G(P)/P| \mid 10$. If $2 \mid N_G(P)$ let $y \in N_G(P), |y| = 2$. y has a fixed point since 11 is odd and $x^y = x^{-1}$. Thus y is a product of 5 transpositions thus $y \notin A_{11}$ which is a contradiction. So $|N_G(P)/P|$ is 1 or 5. Let $1 \neq H \lhd G, H \neq G$. Since G is primitive, H is transitive and $11 \mid |H|, P \subseteq H$. $G = HG_a$ and $G_a \subseteq N_G(P)$ so $G = HN_G(P)$ and $N_G(P) \nsubseteq H$ and $N_H(P) = P$. So, in H, P is in the center of its normalizer and H has a normal 11 complement, K. $K \lhd G$ and $11 \nmid |K|$ so $K = 1$. Thus $H = K$ and $|G| = 55$, which is a contradiction.
Step 2: $PSL_3(4)$ is simple. This was already shown.

Step 3: By the above result, $M_{12}, M_{22}, M_{23}, M_{24}$ cannot ahve a regular normal subgroup. These groups are all 3-transitive. $M_{11} = (M_{12})_a$ so M_{12} is simple. $PSL_3(4) = (M_{22})_a$, $M_{22} = (M_{23})_a$, and $M_{23} = (M_{24})_a$ proving their simplicity.

Chapter 11

Algorithms

11.1 Generators and relations

Notation: X are the generators, R are the relations. Each $R \in R$ is of the form $u_1 u_2 \dots u_k = 1$ where each $u_1 = x, x^{-1}, x \in X$. Write $G = \langle X|R\rangle$ for the generated group. If H is a group and $\varphi : X \to H$, φ can be extended to an homomorphism between H and G.

Definition: F is *free* on X if $i : X \to F$ and $\forall g : X \to G$, $\exists! f : F \to G$ such that $i(f(x)) = g(x)$.

Theorem: Free groups exist. Any group is a homomorphic image of a free group.

11.2 Coset enumeration

Let $G = \langle g_1, g_2, \dots, g_m\rangle$. Let $k_1, k_2, \dots, k_s$ be a group of coset representatives for a subgroup $H < G$. $\overline{g}$ is the coset representative for g in G/H and $k_1 = 1$ then $H = \langle (k_i g_j)\overline{(k_i g_j)^{-1}}\rangle$ for $i = 1, 2, 3, \dots, s$ and $j = 1, 2, 3, \dots, m$.

Coxeter: Maintain following tables: Coset, relation table for each relation, subset table. Column headers are generators, rows are right coset labels. To calculate $|G|$, find cosets of $H < G$ and calculate $|G : H|$.

Definition: $\mathcal{B} = \langle \beta_1, ..., \beta_n\rangle$ is a base for $G \leq Sym(\Omega)$ if $G_{\mathcal{B}} = 1$. If $G^{[i]} = G_{\beta_1,\dots,\beta_i}$ and $G = G^{[1]} \geq ... \geq G^{[m+1]} = 1$ then S is a *strong generating set* relative to $\mathcal{B}$ if it is a generating set and $S \cap G^{[i]} = G^{[i]}$. Can use this to get orbit sizes. Schrier-Sims calculates base and strong generating set.

Theorem: Let G be a group with $G/Z(G)$ finite, then $G^{(1)}$ is finite.

> *Proof:* Let $n = |G/Z(G)|$. For $z \in Z(G)$ and $g, h \in G$: $[g, hz] = [g, h] = [gz, h]$ so the set of commutators, Δ, is of order at most n^2. Claim: $g \in G^{(1)}$ then $g = x_1 x_2 \dots x_m$, $x_i \in \Delta$ and $m \leq n^3$.

Todd Coxeter example: $G = \langle x, y|x^3 = y^3 = (xy)^2 = 1\rangle$. $H = \langle x\rangle$.

Line	Coset	x	x	x	y	y	y	x	y	x	y
1	1	1	1	1	2	3	1	1	2	3	1
2	2	3	5	2	3	1	2	3	1	1	2
3	3	5	2	3	1	2	3	5	6	7	3

Line 1 coincidence: $1y = 2$, $4y = 1$, $4 = 1y^{-1} = 3$. Line 3 coincidence: $7 = 3y^{-1} = 2$, $6 = 2x^{-1} = 5$.

This yields:

Element	1	2	3	5
x	1	3	5	2
y	2	3	1	5

Line 1 coincidence: $1y = 2$, $4y = 1$, $4 = 1y^{-1} = 3$. Line 3 coincidence: $7 = 3y^{-1} = 2$, $6 = 2x^{-1} = 5$.

Chapter 12

Transfer and $p-$complements

12.1 Transfer

Definition 1: Suppose G is a finite group and H is a subgroup, $|G:H| = n$. Let $\langle r_1, \ldots, r_n \rangle$ be a right transversal so $G = \bigcup_{i=1}^{n} Hr_n$ and $Hr_i \cap Hr_j = \emptyset$ if $i \neq j$. Suppose $r_i g = h_i(g) r_j$. The *transfer* map from G to H is defined as $V_{G\to H}(g) = \prod_{i=1}^{n} h_i(g) \pmod{H'}$.

Definition 2: $Foc_G(H) = \langle y^{-1}y^g : y, y^g \in H \rangle$, thus $H' \leq Foc_G(H) \leq H \cap G'$.

Theorem 1: The map $V_{G\to H}$ is well defined and is a homomorphism.

> *Proof:* Let $T = \{t_1, t_2, \ldots, t_n\}$ and $T' = \{t_1', t_2', \ldots, t_n'\}$ be two transversals for G/H. $\exists k_i \in H : t_i' = k_i t_i$. If $t_i g = h_i(g) t_j$ and $t_i' g = h_i'(g) t_j'$, $t_i g = k_i^{-1} h_i(g)' k_j^{-1}$ and $k_i^{-1} h_i(g)' k_j = h_i(g)$. For each g, each k_i^{-1}, k_j occur once when $h_i(g)$ is calculated the cosets. $\prod_{i=1}^{n} h_i(g) = \prod_{i=1}^{n} k_i^{-1} h_i(g)' k_j \pmod{H'}$ but the elements of H commute $\pmod{H'}$ and all the $k_i's$ cancel thus $\prod_{i=1}^{n} h_i(g) = \prod_{i=1}^{n} h_i(g)' \pmod{H'}$ and thus $V_{G\to H}$ is well defined.
>
> Now $V_{G\to H}(g_1 g_2) = \prod_{i=1}^{n} h_i(g_1 g_2) \pmod{H'}$. $t_i g_1 g_2 = h_i(g_1 g_2) t_j = h_i(g_1) t_k g_2 = h_i(g_1) h_k(g_2) t_j$. So $V_{G\to H}(g_1 g_2) = \prod_{i=1}^{n} h_i(g_1 g_2) = \prod_{i=1,k=1}^{n} h_i(g_1) h_k(g_2) \pmod{H'} = (\prod_{i=1}^{n} h_i(g_1) \pmod{H'})$ $(\prod_{k=1}^{n} h_k(g_2) \pmod{H'} = V_{G\to H}(g_1) V_{G\to H}(g_2)$, thus, $V_{G\to H}$ is a homomorphism.

Theorem 2: $V_{G\to H}(g) = \prod_{i=1}^{k} h_j \pmod{H'} = \prod_{i=1}^{k} r_i g^{n_i} {r_i}^{-1} \pmod{H'}$. Further, $\sum_{i=1}^{h} n_i = |G:H|$.

> *Proof:* For fixed $g \in G$, we can pick the transversal $Hr_1, Hr_1, \ldots, Hr_1 g^{n_1 - 1}, Hr_2, Hr_2, \ldots, Hr_2 g^{n_2 - 1}$, $\ldots$, $Hr_k, Hr_k, \ldots, Hr_k g^{n_k - 1}$, where $r_j g^{n_j} = h_j r_j$ for some, $h_j = r_j g^{n_j} {r_j}^{-1}$. So $V_{G\to H}(g) = \prod_{i=1}^{k} h_j \pmod{H'} = \prod_{i=1}^{k} r_i g^{n_i} {r_i}^{-1} \pmod{H'}$. Further, $\sum_{i=1}^{k} n_i = |G:H|$.

Theorem 3: If Z is a central subgroup of G, $|G:Z| = n$ then $V_{G\to Z}(g) = g^n$

> *Proof:* Choose a right transversal, T for Z in G and let $g \in G$. Choose $T_0 \subseteq T$ and integers n_t for $t \in T_0$. For $t \in T_0$, we have $t g^{n_t} t^{-1} \in Z$ and thus $t^{-1} t g^{n_t} t^{-1} t = g^{n_t}$ and the product over all these is $g^{\sum_t n_t} = g^n$.

Lemma A: Let T be a right transversal for $Z = \mathbb{Z}(G)$ in G, then every commutator in G is of the form $[s,t], s, t \in T$. So if $|G:Z|$ is finite, there are only finitely many commutators.

Proof: The second statement follows from the first since $|T| = |G : \mathbb{Z}(G)|$. If $g \in G, g = xs, x \in \mathbb{Z}(G), t \in T$. So it suffices to show $[xs, yt] = [s, t]$ with $x, y \in \mathbb{Z}(G)$ and $s, t \in T$. So $[xs, yt] = [x, yt]^s[s, yt] = [s, yt]$. Also, $[s, yt] = [yt, s]^{-1} = ([y, s]^t[t, s]^{-1} = [t, s]^{-1} = [s, t]$.

Theorem 4: If $|G : \mathbb{Z}(G)| = n$ then $[g, h]^n = 1, \forall g, h \in G$.

Proof: The map $g \mapsto g^n$ is a homomorphism from G into $\mathbb{Z}(G)$ and so G' is in the kernel.

Theorem 5: Let X be a finite subset of G closed under conjugation and suppose $\exists n : x^n = 1, \forall x \in X$ then $\langle X \rangle$ is a finite subgroup of G.

Proof: Let S be the subseteq of G of all products of finitely many elements of X. S is closed under multiplication. Since $x^n = 1$, $x^{n-1} = x^{-1} \in S$ and $\langle X \rangle = S$. *Claim:* Such an expression in S never requires more than $(n-1)|X|$ factors. The result follows from the claim.
Proof of claim: Put $g = x_1 x_2 \dots x_m$. Suppose an element of $x \in X$ occurs k times. We now that g can be rewritten with leading factor x with x occuring no more than k times. To show this, assume t is the smallest index for which $x = x_t$. If $t = 1$, we're done. $x_1 x_2 \dots x_t = x(x_1 \dots x_{t-1})^x = x(x_1^x) \dots (x_{t-1}^x)$, this is a product of t elements of X since X is closed under conjugation. We can continue and extract all copies of x to the front. Since $x^n = 1$, the exponent of x is $\leq n - 1$.

Schur's Theorem: Suppose $|G : \mathbb{Z}(G)| < \infty$ then $|G'| < \infty$.

Proof: Let X be the set of all commutators of G and observe $|X|$ is finite. Also, $[x, y]^g = [x^g, y^g]$. $x^{|G:\mathbb{Z}(G)|} = 1$ and the result follows from the previous result.

Theorem 6: Let $p \mid |G| < \infty$ and $p \mid |G' \cap \mathbb{Z}(G)|$, then the Sylow p-subgroup of G is nonabelian.

Proof: Suppose $P \in S_p(G)$ is abelian and let T be a right transversal. Put $v(g) = V_{G \to P}(g)$. Let $Z = \mathbb{Z}(G)$. $G' \cap Z \cap P > 1$ since $G' \cap Z \lhd G$. For $t \in T, z \in G' \cap Z \cap P$, $Ptz = Pzt = Pt$ so t is the element in Ptz and $t \cdot z = t$. Thus, $tz(t \cdot z)^{-1} = tzt^{-1} = z$ and $v(z) = z^{|T|} = z^{|G:P|}$. We know, since P is abelian that $G' \subseteq ker(v)$. So $z \in G' \to 1 = v(z) = z^{|G:P|}$. Thus $z = 1$. This contradicts the choice of z.

Theorem 7: Let $Z < \mathbb{Z}(\Gamma)$, Γ, finite, then a Sylow p-subgroup of Γ/Z is non-cyclic for all $p \mid |Z|$.

Proof: Let $P \in S_p(\Gamma)$, $p \mid |Z|$ and $Z \subseteq \mathbb{Z}(\Gamma) \cap \Gamma'$ so by the foregoing, P is not abelian. Since $P \cap Z \subseteq \mathbb{Z}(P)$ and P is not abelian, $P/(P \cap Z)$ cannot be cyclic. But $P/(P \cap Z) \cong PZ/Z \in S_p(\Gamma/Z)$ and so Γ/Z has a non-cyclic Sylow p-subgroup.

Observation: Note that Γ is a central extension of G if $\Gamma/Z \cong G$. In the case $Z \cong M(G)$ (the Schur multiplier), Γ is a Schur representation group and if G is perfect, this representation group is unique. If $G = \langle x \rangle, x^4 = 1$, $|M(G)| = 2$. The theorem shows, for example, that $|M(A_5)| = 2$

Definition 3: $A^p(G)$ is the smallest normal subgroup of G such that $G/A^p(G)$ is an abelian p-group. Let $G'(\pi)$ denote the inverse image of $O_{\pi'}(G/G')$.

Focal Subgroup Theorem: If $P \in S_p(G)$, $Foc_G(P) = P \cap G' = P \cap A^p(G) = ker(V_{G \to P})$.

Proof: $Foc_G(P) \subseteq P \cap G' \subseteq P \cap A^p(G) \subseteq ker(V_{G \to P})$ is easy. So if we prove $ker(V_{G \to P}) \subseteq Foc_G(P)$, we're done. Let $x \in ker(V_{G \to P})$, so $x \in P'$. Suppose $\langle Pg_i x, \dots, Pg_i x^{n_i - 1} \rangle$ is an orbit of x acting on Pg_i in G/P. So $Pg_i = Pg_i x^{n_i}$, ${g_i}^{-1} x^{n_i} g_i \in P$, and $x^{n_i} \in P$. We can find a complete set of coset representatives of P in G consisting of such orbits with $g_i \in$

$G, i = 1, 2, \ldots, h$. For each i, $x^{n_i} = {g_i}^{-1} x^{n_i} g_i \pmod{Foc_G(P)}$. So $V_{G\to P}(x) \pmod{Foc_G(P)} = \prod_{i=1}^{h} {g_i}^{-1} x^{n_i} g_i \pmod{Foc_G(P)} = x^{|G:P|} \pmod{Foc_G(P)}$ and $x^{|G:P|} \in Foc_G(P)$. Since $P' \subseteq Foc_G(P) \subseteq P$ and $(|x|, |G:P|) = 1$, $\exists k_1, k_2 : k_1|G:P| + k_2|x| = 1$ so $x = x^{|G:P|k_1} x^{|x|k_2} \in Foc_G(P)$.

Theorem 8: If $P \in S_p(G)$ then $ker(V_{G\to P}) = A^p(G)$.

Proof: Put $K = ker(V_{G\to P})$, $A = A^p(G)$, $A \supseteq K$ by the last result. $|G:K|$ and $|G:A|$ are p-powers. $PK = G = PA$. By FST, $P \cap K = P \cap A$ and $|G:K| = |P:P\cap K| = |P:P\cap A| = |G:A|$. So $|A| = |K|$ and the result holds.

Theorem 9: Let H be a Hall π subgroup of G and $v(g) = V_{G\to H}(g)$ then $v(H) = v(G)$ and $|H : H \cap ker(v)| = |G : ker(v)|$.

Proof: We know $|G : ker(v)| = |v(G)|$ and since $v(G) \subseteq H/H'$, we have $|G : ker(v)| \mid |H|$. $(|G : ker(v)|, |G : H|) = 1$ so $ker(v)H = G$.

Theorem 10: If $P \in S_p(G)$ then $N_G(P)$ controls G-fusion in $C_G(P)$.

Proof: Let $c_1, c_2 \in C_G(P)$ and $c_1^g = c_2$. Then $c_2 = c_1^g \in C_G(P^g)$ We know $c_2 \in C_G(P)$, so $P, P^g \in C_G(c_2)$ and since they are both Sylow subgroups of $C_G(c_2)$ by Sylow, $\exists h \in C_G(c_2) : P^{gh} = P$ and hence $gh \in N_G(P)$. $c_1^{gh} = c_2^h = c_2$ and so c_1 and c_2 fuse in $N_G(P)$.

Theorem 11: Let P be a Hall subgroup of G then $Foc_G(P) = P \cap G'(\pi) = P \cap G'$ and $G/Foc_G(P) \cong G/G'(\pi)$, $ker(V_{G\to P}) = G'(\pi)$ and $P/P' = \overline{P} = \overline{Foc_G(P)} \times Im(V_{G\to P})$.

Proof: $(|P|, |G:P|) = 1$. $V_{G\to P}(\overline{Foc_G(P)}) = \langle \overline{x} \rangle \overline{Foc_G(P)}$ as in the proof of the FST. Conversely, $G'(\pi) \subseteq ker(V_{G\to P})$ and $\overline{P}$ is abelian so $Foc_G(P) \leq P \cap G' = P \cap G'(\pi) \leq P \cap ker(V_{G\to P})$. As before, equality holds $|G/G'(\pi)| \geq |G/ker(V_{G\to P})| = |Im(V_{G\to P})|$. Finally, $P/(P \cap G') \cong G/G'(\pi)$, so $ker(V_{G\to P}) = G'(\pi)$ and $Im(V_{G\to P}) \cong P/Foc_G(P)$. $\overline{P} = \overline{Foc_G(P)} \times Im(V_{G\to P})$.

Corollary: If P is a Hall π group of G, $G/G' = PG'/G' \times O_{\pi'}(G/G')$; hence, if $P \neq Foc_G(P)$, $G \neq O^{\pi'}(G)$.

Proof: Follows from Theorem 11.

Theorem: Let $P \in S_p(G)$. (i) $\exists K \lhd G : G/K \cong P/(P \cap G')$, (ii) If $K \lhd G$ and G/K is an abelian p-group, then $P \cap G' \subseteq K$ and $G/K \cong P/(P \cap G')$.

Proof: (ii): G is abelian so $G' \subseteq K$. $G = KP \cong P/(P \cap K)$. $G' \cap P \subseteq K \cap P$ so $P/(P \cap K)$ is a homomorphic image of $P/(P \cap G')$.
(i) $P \cap G' \in S_P(G')$ and $G' \lhd G$. Put $\overline{G} = G/G'$. $\overline{G}$ is abelian. Let K be the inverse image of $O_{p'}(\overline{G})$. $G' \subseteq K$ so $P \cap G' \subseteq P \cap K$ but $P/(P \cap K)$ is a homomorphic image of $P/(P \cap G')$ so $P \cap K = P \cap G'$.

Theorem: If $P \in S_p(G)$, $Foc_G(P) = P \cap G'$.

Proof: $P' \subseteq Foc_G(P) \subseteq P \cap G'$. $P/Foc_G(P)$ is abelian. Let ϕ be the natural map $P \to P/Foc_G(P)$ and τ the transfer from P to $P/Foc_G(P)$ and put $K = ker(\tau)$. $P/Foc_G(P)$ is a homomorphic image of $P/(P \cap G')$ so $|P/(P \cap G')| > |P/Foc_G(P)|$. Since $Foc_G(P) \subseteq P \cap G'$, this means $Foc_G(P) = P \cap G'$.

Burnside's Lemma: If $P \in S_p(G)$, $A_1, A_2 \subseteq P$ with $(A_i)^x = A_i, \forall x \in P, i = 1, 2$, then if $A_1^g = A_2$, then $\exists h \in N_G(P) : A_1^h = A_2$. ($N(P)$ controls fusion in P.)

Proof: Same as the earlier proof about $N_G(P)$ controlling fusion on $C_G(P)$.

Definition 4: Z is *weakly closed* in P with respect to G if $Z^g \subseteq P \to Z^G = Z$. The *weak closure* of Z in P with respect to G is $wcl_G(Z,P) = \langle Z^g | Z^g \subseteq P \rangle$. $G'(\pi)$ is the inverse image of $O_{\pi'}(G/G')$.

Theorem 12: Let $P \in S_p(G)$ and $Z \subseteq \mathbb{Z}(P)$ is weakly closed in P. Suppose $y \in P$ and $g \in G$ such that $y^g \in P$. The $\exists n \in N_G(Z) : y^g = y^n$.

Proof: Note $y^g \in P \cap P^g$ and $\langle Z, Z^g \rangle \subseteq C_G(y^g)$. By Sylow, $\exists c \in C_G(y^g)$ such that $\langle Z^g, Z^c \rangle$ is a p-group and $\exists h \in G : \langle Z^{gh}, Z^{ch} \rangle \leq P$. Since Z is weakly closed in P, $Z^{gh} = Z^{ch} = Z$. So $n = gc^{-1} \in N_G(Z)$ and since $c \in C(y^g) : y^n = y^g$.

Grun's Theorem: If $P \in S_p(G)$ and $Z \subseteq \mathbb{Z}(P)$ is weakly closed in P then $P/(P \cap G') \approx G/G'(p) \approx N(Z)/N(Z)'$ and so $G \neq O^p(G) \to N(Z) \neq O^p(N(Z))$.

Proof: This follows from Theorem 12 and Theorem 11.

Theorem 13: If $P \in S_p(G)$ and $Z \lhd N(P)$ then the following are equivalent: (1) Z is weakly closed in P with respect to G; (2) $Z \leq R \in S_p(G) \to Z \lhd R$.

Proof:

(1) implies (2): If $Z \leq R = P^{g^{-1}}, g \in G$, then $Z^g \leq P$ and $Z = Z^g$. Hence, $Z^R = Z^{P^{g^{-1}}} = Z$.
(2) implies (1): Let $Z^g \leq P$ so by (2), $\langle Z^g \rangle \lhd P$. By Burnside, $\exists y \in N_G(P)$ such that $Z^y = Z^g$ and thus $Z^y = Z^g = Z$.

Theorem 13a: (1) Let $P \in S_p(G)$ then (1) $\exists K \lhd G : G/K \approx P/P \cap G'$. (2) If $K \lhd G$ such that G/K is an abelian p-group then $P \cap G' \subseteq K$ and G/K is isomorphic to a homomorphic image of $P/P \cap G'$.

Proof: Assume $K \lhd G$ and G/K is an abelian p-group. Then $G' \subseteq K$ and $G = KP$. $P \cap G' \subseteq K$ and so $P/P \cap K$ is a homomorphic image of $P/P \cap G'$ and (2) holds. For 1, put $\overline{G} = G/Foc_G(P)$ and let K be the inverse image of $O_p(\overline{G})$ in G. $P \cap G' \in S_p(G')$. $P \cap G' = P \cap K, K \lhd G$ and G/K is isomorphic to $P/P \cap G'$ and (1) holds.

Burnside's Theorem: If $P \in S_p(G)$ and $P \subseteq \mathbb{Z}(N_G(P))$ then P has a normal p-complement.

Proof: Put $N = N_G(P)$. Note that P is abelian so $P \cap Q' = 1, Q \in S_p(G)$. P is a normal Hall subgroup of N so it has a complement H in N. $N = P \times H$ so $N' = H'$ so $P \cap N' = P \cap H' = 1$ so by Grun, $P \cap G' = 1$. By previous result, $\exists K : G/K \approx P/P \cap G'$ thus K is a p'-group and $K = O_{p'}(G)$.

Another statement of Burnside's Theorem: If $P \in S_p(G)$ and $N_G(P) = C_G(P)$ then G has a normal p complement.

Proof: $P \leq \mathbb{Z}(N_G(P))$.

Theorem 13b: Suppose Sylow p-subgroups of G and G is a semidirect product of $N \lhd G$ and P, $Z \subseteq P$ wiht $Z^g \leq P$. $\exists x \in P : Z^g = Z^x$ so every normal subgroup of P is weakly closed in P.

Proof: $g = yx$, $y \in N$ and $x \in P$. $Z^g \leq P$ so $Z^y \leq P$ so $Z^g = Z^x$. This shows that $\forall z \in Z, [z,y] \in N \cap P = 1$ and so $y \in C_G(Z)$ and the result follows.

Baer's Theorem: X be a p-group of G then either $X \leq O_p(G)$ or $\exists g : \langle X, X^g \rangle$ is not a p-group.

Proof: See the stability section.

Theorem 14: If Q is an abelian Sylow subgroup in G and if $Q \subseteq \mathbb{Z}(G)$ then $V_{G\to Q}(g) = g^{|G:Q|}, \forall g \in G$.

Proof: Let T be the transversal $T = \{Qh_1, Qh_1g, \ldots, Qh_1g^{n_1-1}, Qh_2, Qh_2g^{n_2-1}, \ldots, Qh_mg^{n_t-1}\}$. $V_{G\to Q}(g) = \prod_{k=0}^{t} h_i g_{n_i} h_i^{-1} \pmod{Q'}$. Since $g^{n_i}, h_i g^{n_i} h_i^{-1} \in Q \subseteq \mathbb{Z}(G)$, $V_{G\to Q}(g) = g_{\sum_{i=1}^{t} n_i} = g^{|G:Q|}$.

Theorem 15: If $P \in S_p(G), P' = 1$ then $P \cap G' = P \cap N_G(P)'$.

Proof: As proved earlier, $N_G(P)$ controls fusion on $C_G(P) \supseteq P$ (since P is abelian).

Theorem 16: If $P \in S_p(G)$ is cyclic where p is the smallest prime divisor of $|G|$, then G has a normal p-complement.

Proof: $1 \to N_G(P)/C_G(P) \to Aut(P)$ and since $|P|$ is cyclic it has order $\varphi(|P|)$. If $|P| = p^n$, $\varphi(|P|) = p^{n-1}p$, this is divisible by no prime bigger than p and the index is divisible by no prime smaller than p. Since $p \nmid |N_G(P) : C_G(P)|$ and since P is abelian it has index 1, $C_G(P) = N_G(P)$; thus, $P \subseteq \mathbb{Z}(N_G(P))$ and by Burnside, G has a normal p-complement.

Theorem 17: If all Sylow subgroups of G are cyclic, G is solvable.

Proof: Induction on $|G|$. Let be p be the smallest prime such that $p \mid |G|$. G has a normal p-complement, N, by the previous result. $N < G$ and all the Sylow subgroups of N are cyclic. N is solvable by induction. G/N is a p-group so it is solvable.

Theorem 18: Suppose all Sylow subgroups of G are cyclic then $(|G'|, |G/G'|) = 1$ and both are cyclic.

Proof: G/G' is cyclic. To show G' is cyclic, we proceed by induction on $|G|$. $G' < G$ so G'' is cyclic (by induction). $Aut(G'')$ is thus abelian and $1 \to G/C_G(G'') \to Aut(G'')$ and $G' \subseteq G_G(G'')$ and $G'' \subseteq \mathbb{Z}(G') \to G'$ is abelian and thus G' is cyclic.

Theorem 19: Let P be a cyclic Sylow subgroup of G then p divides at most one of $|G'|$ and $|G/G'|$.

Proof: Let $N = N_G(P)$, $K \subseteq N$ a complement for P in N. $P = [P, K] \times C_P(K)$. If $[P, K] = 1$, $C_P(K) = P$ and P is central in $N = PK$. By Burnside, G has a normal p-complement, M and G/M is a p-group which is cyclic so $G' \subseteq M$ and $p \nmid |G'|$.

Theorem 20: Let P be an abelian Sylow subgroup of G then $G' \cap P \cap \mathbb{Z}(N_G(P)) = 1$.

Proof: Let $v : G \to P$ and $x \in G' \cap P \cap \mathbb{Z}(N_G(P))$ then $x \in G'$ so $1 = v(x) = \prod_{t\in T_0} tx^{n_t}t^{-1} \in P$. $x^{n_t}, tx^{n_t}t^{-1} \in C_G(P)$ and x is central so self conjugate in $N_G(P)$. $x^{n_t} = tx^{n_t}t^{-1}, \forall t \in T_0$, so, since $|G : P| = \sum_t n_t$, $v(x) = x^{|G:P|}$. $1 = x^{|G:P|}$ and since $x \in P$ then $x = 1$.

Theorem 21: Suppose the Sylow 2-subgroups of G, G is nonabelian, are direct products of cyclic groups one of which is strictly larger than the other then G is not simple.

Proof: Let $P \in S_2(G)$. $P = A \times B$ where A is cyclic of order $a \geq 2$ and $x^{a/2} = 1, \forall x \in B$. Let $C = \{x^{a/2} : x \in P\}$ *char* P so there is the unique $t \in C$ is central in $N_G(P)$. $t \notin G'$ so $G' < G$ and the result follows.

Gaschutz: Let K be a normal abelian p-subgroup of a finite group G and let $P \in S_p(G)$. Then K has a complement in G iff K has a complement in P.

Proof: Let A be a complement of K in $U: = KA, K \cap A = 1$. Let $\mathcal{L}$ be the set of left transversals of U in G and $S_0 \in \mathcal{L}$. Then $\forall L \in \mathcal{L}, l \in L$: $l = s_l k_l a_l, s_l \in S_0, k_l \in K, a_l \in A$ and $s_l U = lU$ and the factorization is unique. Hence $\forall l \in L, \exists! l_0 \in S_0 K : lU = l_0 U$ (i.e. - $l_0 = s_l k_l$). So every $L \in \mathcal{L}$ is associated with $L_0 = \{l_0 : l \in L\}$ in $\mathcal{S} = \{L \in \mathcal{L} : L \subseteq S_0 K\}$ such that $LA = L_0 A$. For $x \in G$ and $xL \in \mathcal{L}$: $(xL)_0 A = xLA = xL_0 A = (xL_0)_0 A$ and thus $(xL)_0 = (xL_0)_0$. Now define $S^x = (x^{-1}S)_0 = (y^{-1}(x^{-1}S))_0 = ((xy)^{-1}S)_0 = S^{xy}$. This defines an action of G on $\mathcal{S}$. Now write $(xS)_0$ instead of $S^{x^{-1}}$. $R|S = \prod_{(r,s) \in R \times S, Kr = Ks}(rs^{-1}), R, S \in \mathcal{S}$. For $kS \subseteq kS_0 K = S_0 K$ and thus $kS = (kS)_0 \in \mathcal{S}$. Further, $(kS)_0 | R = k^{G:K|}(S|R).k \in K, S, R \in \mathcal{S}$. As in Schur-Zassnehaus, $R \sim S \leftrightarrow R|S = 1$ thus defines an equivalence relation on $\mathcal{S}$ and the existance of a complement follows using the action of G and K on $\mathcal{S}/\sim$.

Theorem 22: Let $N \lhd G$ and G be a semidirect product of N with P, $g \in G : Z^g \leq P$. Then $\exists x \in P : Z^g = Z^x$ so every normal subgroup of P is weakly closed in P.

Proof: $g = yx, y \in N, x \in P$ so $Z^g \leq P \rightarrow Z^y \leq P$. Thus, $\forall z \in Z : [z, y] \in N \cap P = 1$ and $y \in C(Z)$ so $Z^g = Z^x$.

Observation: If N is a p-complement in G then $O_{p'}(G) = N = O^p(G)$.

Frobenius Normal $p-$complement Theorem: Let $P \in S_p(G)$ if $\forall U \in p(G)$, $N_G(U)$ has a normal p-complement then G has a normal p -complement. Note: There is a stronger result in which U can be restricted to characteristic p-locals and Thompson's p-complement theorem is a further strengthening.

Proof: G has a normal p-complement if $P = 1$. If $P > 1, Z = \mathbb{Z}(P) > 1$ and $H = N_G(Z)$ has a normal p-complement by hypothesis. Thus $O^p(H) \neq H$.
Claim: Z is weakly closed in P.
Proof of claim: It suffices to show, $Z \leq R \in S_p(N_G(P)) \rightarrow Z \lhd R$. Assume this condition does not hold and choose R such that $S = N_R(Z)$ is maximal. $S < N_R(S)$ and $S < N_T(S)$. Put $M = N_G(S)$ and let $N_T(S) \leq T_1 \in S_p(M)$. By the maximality, $Z \lhd T_1$ Since M has a normal p-complement, the previous result show Z is normal in every Sylow subgroup of M containing it. Hence $Z \lhd N_R(S)$ which contradicts $S < N_R(S)$.
Now Grun's Theorem shows $O^p(G) \neq G$ and by induction on $|G|$, $O^p(G)$ has a normal p-complement, K. $K \lhd G$ and G/K is a p-group, so K is also a normal p-complement of G.

Theorem 23: A finite group G has a normal p complement iff a Sylow p-group controls its own fusion.

Proof:

$\rightarrow$: Let $P \in S_p(G)$ and N be a normal p complement so $G = NP$. Suppose $x, y \in P$ and $x^g = y$. Let $\overline{G} = G/N$ so the isomorphism $G \rightarrow \overline{G}$ induces an isomorphism of P onto $\overline{G}$. $\overline{x}$ and $\overline{y}$ are conjugate in $\overline{G}$ so by the isomorphism, they are P-conjugate and P controls its own fusion.

$\leftarrow$: Let $N = O^p(G)$, $Q = N \cap P$ so $Q \in S_p(N)$. We show $Q = 1$ and hence N is a normal p-complement.
Claim: $N = A^p(N) = N$.
Proof of claim: $A^p(N)$ *char* N so $A^p(N) \lhd G$. Further, $|G : A^p(N)| = |G : N||N : A^p(N)|$, which is a p-power. Thus $N = O^p(G) \subseteq A^p(N)$ and $O^p(N) = A^p(N)$ as claimed.
By the focal subgroup theorem, $Foc_N(Q) = Q \cap A^p(N) = Q \cap N = Q$. Let $x, y \in Q$ be N-conjugate so $x^{-1}y$ is a typical generator in $Foc_N(Q)$. $\exists u \in P : x^u = y$ so $x^{-1}y = [x, u] \in [Q, P]$. So $Q = Foc_N(Q) \subseteq [Q, P]$, so $Q \subseteq [Q, P, P, \ldots, P]$ but $Q \subseteq P$ and P is nilpotent so $[Q, P, \ldots, P] = 1$ eventually and so $Q = 1$.

Theorem 23a: The following are equivalent: (1) G has a normal $p-$complement, (2) Each $p-$local subgroup of G has a normal $p-$complement, (3) $Aut_G(P)$ is a $p-$group $\forall P \in p(G)$.

Proof: $1 \to 2 \to 3$ is easy.
Claim: Assume $N_G(X)/C_G(X)$ is a p-group for every p-group, X, of a finite group G and let $P, Q \in S_p(G)$ then $Q = P^c$ for some $c \in C_G(P \cap Q)$.
Proof of claim: Assume (3). It suffices to show that P controls its own fusion in G. If $x, y \in P$ are conjugate in G, $x^g = y$, $y \in P \cap P^g$ and by the claim, $\exists c \in C_G(P \cap P^g) : (P^G)^c = P$. Since $N_G(P)/C_G(P)$ is a p-group and P is a Sylow p-subgoup of $N_G(P)$, $N_G(P) = C_G(P)P$. We have $gc = tu$, $t \in C_G(P)$ and $u \in P$. Since $x \in P$ and $[x, t] = 1$ and thus $y = y^c = x^{gc} = x^{tu} = x^u$ so x and y are P-conjugate.

Definition 5: G is π-closed if $G/O_\pi(G)$ is a π' group and thus $O_\pi(G) = O^{\pi'}(G)$.

Definition 6: $A^\pi(G)$ is the unique smallest normal subgroup of G such that $G/A^\pi(G)$ is an abelian π-group. If $P \subseteq H \subseteq G$ then $|G : A^p(G)| \leq |H : A^p(H)|$ if equality holds we say H *controls p-transfer in G*.

Burnside p-complement theorem: If $C_G(P) = N_G(P)$ then G has a normal p-complement.

Proof: Obviously, P controls its own fusion in this case and the result follows.

Theorem 24: If $P \in S_p(G)$ and H controls p-fusion in P then H controls p-transfer in G. If $P \in S_p(G)$ is abelian, then $N_G(P)$ controls p-transfer.

Proof: Want to show $|G : V_{G \to P}| = |H : V_{H \to P}|$ this happens iff $P \cap ker(V_{G \to P}) = Foc_G(P) = P \cap ker(V_{H \to P}) = Foc_H(G)$. $Foc_G(P) = Foc_G(H)$ since H controls G-fusion.

Theorem 25: Let $p \neq 2$ and suppose every p-element is central in G then G has a normal p complement.

Proof: This follows from the Frobenius normal p-complement theorem.

Theorem 26: Let G be a finite group $H \leq G$, $(p, |G : H|) = 1, K \lhd H$, H/K abelian, g a $p-$element in $H \setminus K$: $g^{ma} \in g^m K, \forall m$, all $a \in G$ such that $g^{ma} \in H$ then $g \notin G'$.

Proof: See, Stellmacher, p 73.

Definition 7: The action of A on $N \lhd G$ is *Frobenius* if $n^a \neq n$, if $a \neq 1 \neq n$.

Lemma: Let $A < G$ with the TI property for all $g \in G - A$ then $X = \{x : x \neq y, y = a^g\}$, $|X| = |G|/|A|$.

Proof: If $A > 1$, $A = N_G(A)$ since $A^x = a$ then $A \cap A^x = A > 1$, $x \in A$. So A has exactly $|G : A|$ conjugates in G all with the same TI property as A. These contain $|G : A|(|A| - 1)$ non-identity elements of G. $|X| = |G| - |G : A|(|A| - 1) = |G : A|$.

Theorem 27: Let $N \lhd G$ and A is a complement for N in G. The following are equivalent: (1) The conjugate action of A on N is Frobenius; (2) $A \cap A^g = 1$, $\forall g \in G - A$; (3) $C_G(A) \subseteq A$.

Proof: $1 \to 2$: If $A \cap A^x \neq 1$ with $x = an$. $A^x = A^{an} = A^n$ so $A \cap A^n \neq 1$ so $a = a^n$ and $a^n = a \in A \cap A^n = 1$ so $n = 1$ and $x \in A$.
$2 \to 3$: Suppose $g \in C_G(A), g \notin A$ then $g = an$ and $[A, an] = 1$ and $b = b^{an} \in A \cap A^n = 1$ so $n = 1$ by (1).
$3 \to 1$: If $1 \neq a \in A$ by (3), then $C_N(a) = N \cap C_G(a) = 1$ so $a^n \neq a$ for $n \neq 1$.

Chapter 13

Coprime action and p-constraint

13.1 Basic Results

Definition 1: A group of automorphisms A of a group P stabilizes a chain $1 = P_0 \subseteq P_1 \subseteq \ldots \subseteq P_n = P$ if $[A, P_{i+1}] \subseteq P_i$.

Theorem 1: If P is a π group with chain stabilized by A then A is a π group.

Proof: Suppose $a \in A$ is a π' automorphism. Proof is by induction on the length of the chain and so we can assume $[a, P_1] = 1$. $x^a = xy, y \in P_1$. So, $x^{a^{|a|}} = xy^{|a|} = x$, so $y = 1$ and $[a, P_2] = 1$.

Theorem 2: If A is a π' group of automorphisms on a π group P with $[P, A, A] = 1$ then $[P, A] = 1$.

Proof: A stabilizes $[P, A, A] \subseteq [P, A] \subseteq P$.

Theorem 3: Let A be a π' group of automorphisms of a π group P. Let Q be an $A-$invariant normal subgroup of P. Then $C_{P/Q}(A) = (C_P(A)Q)/Q$.

Proof: $C_P(A)Q/Q \subseteq C_{P/Q}(A)$. Suppose xQ is a subset in P fixed by A. QA acts transitively on the set xQ. Let A_1 be the point stabilizer. $|A_1| = |QA|/|xQ| = |A|$. By Schur-Zassenhaus, A and A_1 are conjugate, so $\exists y \in xQ : y^A = y$.

Theorem 4: If P is a π group, A is a π' group, $P = [P, A]C_P(A)$.

Proof: $[P, A] \subseteq P$ and A centralizes $P/[P, A]$.

Lemma A: If the action of A on G is co-prime and U is an A-invariant subgroup of G with $(Ug)^A = Ug$, then $\exists c \in C_G(A)$: $Ug = Uc$.

Proof: $[a, g^{-1}] \in U$ so $A^{g^{-1}} \leq AU$. Both A and $A^{g^{-1}}$ are U complements in AU so by S-Z, $\exists u \in U$: $A^{g^{-1}} = A^u$. Put $c = ug$. $c \in N_{AG}(A) \cap Ug$, so $[A, c] \subseteq A \cap G = 1$.

Theorem: Let N be an A-invariant normal subgroup of G and let A act co-primely on G then (i) $C_{G/N}(A) = C_G(A)N/N$ and (ii) if A acts trivially on N and G/N then A acts trivially on G.

Proof: $C_G(A)N/N \subseteq C_{G/N}(A)$ is obvious. If Ng is in $C_G(A)N/N$, $(Ng)^A = Ng$ and by the lemma, $\exists c \in C_G(A) : Ng = Nc$, proving (i). ii follows directly from the Lemma.

Theorem: Let $Y \lhd X \in \pi$ and $[Y, A] = 1$ $(|A|, |X|) = 1$. If $C_X(Y) \subseteq Y$ then $[X, A] = 1$.

Proof: $[X, Y] \subseteq Y$, so $[X, Y, A] = 1$. $[Y, A, X] = 1$ so $[A, X, Y] = 1$. $[X, A] \subseteq Y$. Thus $[X, A, A] = 1$ and $[X, A] = 1$.

Alternate proof of 2, 4:

Proof: $G/[G, A] = C_{G/[G,A]}(A) = C_G(A)[G, A]/[G, A]$, proving (4). Let $g \in G$ then $g = hk, h \in [G, A], k \in C_G(A)$ by the above. Since $[xy, z] = [x, z]^y[y, z]$, for $a \in A$, $[g, a] = [hk, a] = [h, a]^k[k, a]$. $[k, a] = 1$ since $k \in C_G(A)$. Thus $[g, a] = [h, a]^k \in [G, A, A]$.

Alternate proof of Thompson: Let $A = P \times Q$ act on a p-group G and suppose $C_G(P) \leq C_G(Q)$. Then Q acts trivially on G.

Proof: $C_U(P) \leq C_U(Q)$ for all A-invariant subgroups, U. By induction, we can assume $[U, Q] = 1$ for all proper subgroups. $[G, P, Q] = 1$ and $[P, Q, G] = 1$ so $[Q, G, P] = 1$. Thus $[Q, G] \leq C_G(P) \leq C_G(Q)$ and $[G, Q, Q] = 1$. By the previous result, $[G, Q] = [G, Q, Q] = 1$. $G/[G, A] = C_{G/[G,A]}(A) = C_G(A)[G, A]/[G, A]$.

Theorem 5: P is an abelian π group, A is a π' group. $P = [P, A] \oplus C_P(A)$.

Proof: $\theta = \frac{1}{|A|} \sum_a a$. For $a \in A$, $\theta a = a\theta = \theta$ and $\theta^2 = \theta$. $\theta P \oplus ker(\theta) = P$. $C_P(A) \subseteq \theta P$ and $\theta([x, a]) = 0$, so $[P, A] \subseteq ker(\theta)$. This shows $C_P(A) \cap [P, A] = \emptyset$ and the result follows from the earliler result that $P = [P, A]C_P(A)$.

Theorem 6: If ϕ is a p'-automorphism of a p-group, P, which induces the identity on $P/\Phi(P)$ then $\phi = 1$.

Proof: Let $H = \Phi(P), \overline{P} = P/H, |\overline{P}| = p^r, |H| = p^m$. $|P| = p^{m+r}$ and for any subset $Y = \{y_i, 1 \leq i \leq n\} \subseteq P$, $P = \langle P, Y\rangle$ iff $P = \langle Y\rangle$. Note that $\overline{P}$ and hence P cannot be generated by $< r$ elements. Let $\{x_i\}$ be a minimal generating set for P and $x_i' = h_i x_i$ be another such generating set. Let ϕ be as set forth in the statement of the theorem. Finally, let $\mathcal{M}$ be the collection of all such minimal generating sets. ϕ fixes each coset $Hx_i' = Hx_i$ and $\phi(x_i') = h_i x_i$ so ϕ induces a permutation representation on $\mathcal{M}$. The cycle length, s, of any cycle in this permutation representation of ϕ must divide $t = |\phi|$. Suppose some such cycle had length $s < t$. $\phi_1 = \phi^s$ fixes the elements of this cycle and so fixes some minimal generating set. But then ϕ_1 fixes evely element of P contrary to the fact that $t > s$. Since $\mathcal{M}$ decomposes as a product of disjoint cycles, $t \mid |\mathcal{M}| = p^{mr}$. Since $(t, p) = 1$, $t = 1$ and $\phi = 1$ on P.

$P \times Q$ **lemma:** Let $A = P \times Q$, P a $p-$group, Q a p'-group, act on a p-group G. If $C_G(P) \leq C_G(Q)$ then Q acts trivially on G.

Proof: $C_U(P) \leq C_U(Q)$ for all A-invariant subgroups U. By induction, $[U, A] = 1$ if $U < G$. Now $[G, P] < G$ so $[G, P, Q] = 1$ and since $[P, Q] = 1$, $[P, Q, G] = 1$ so by the three subgroups lemma $[Q, G, P] = 1$ so $[Q, G] \leq C_G(P) \leq C_G(Q)$ and $[G, Q, Q] = 1$ hence $[G, Q] = 1$.

Theorem 7: Suppose M is a p-group and $C_M(P) \leq C_M(Q)$. Then Q acts trivially on M.

Proof: This is just a restatement of the $P \times Q$ Lemma.

Application of $P \times Q$**:** Let $P \in p(X)$, $M = O_p(X)$, $Q = O_{p'}(N_X(P))$. $[P, Q] = 1$ so $P \times Q$ acts on M. Next, $[C_M(P), Q] = 1$ because $[C_M(P), Q] \subseteq M$ and $[C_M(P), Q] \subseteq Q$, since $C_M(P)$ normalizes P so $C_M(P)$ normalizes $Q = O_{p'}(N_X(P))$; as a result, we have, $[C_M(P), Q] = M \cap Q = 1$. Let $x \in C_M(P)$ then $[x, Q] = 1$ so $x \in C(Q)$ and $x \in M$ so $x \in C_M(Q)$. Thus $C_M(P) \subseteq C_M(Q)$ and the $P \times Q$ lemma applies, that is,

$[M,Q]=1$. If X be solvable, we can use this to show $O_{p'}(N_X(P)) \subseteq O_{p'}(X)$, since $C_X(F(X)) \subseteq F(X)$.

Theorem 8: Suppose X acts faithfully on an Abelian group A and $X = \bigcup_{i=0}^{t} X_i$ with $X_i \cap X_j = 1$ for $i \neq j$ then $C_A(X_i) \neq 1$ for some i or $a^t = 1, \forall a \in A$.

Proof: Let $\sigma_i(a) = \prod_{x \in X_i} a^x$ and $\sigma(a) = \prod_{x \in X} a^x$. If the first condition doesn't hold for i, $(\sigma_i(a))^x = \sigma_i(a)$ for all $x \in X_i$, so $\sigma_i(a) = 1$. Similarly, $\sigma(a)$ is fixed by all elements of X and since X acts faithfully, $\sigma(a) = 1$. If $\sigma_i(a) = \sigma(a) = 1, \forall a, i$ then $\prod_{i=0}^{t} \sigma_i(a) = \sigma(a)a^t$, so $a^t = 1$.

Application: $X = \mathbb{Z}_p \times \mathbb{Z}_p$, $|A| \neq 0 \pmod p$.

Theorem 9: If A is abelian and A acts on G, $(|A|, |G|) = 1$ then $G = \langle C_G(A_0) : A/A_0 \text{ is cyclic} \rangle$.

Proof: By induction on $|AG|$. We may assume A acts faithfully otherwise $C_A(G) \neq 1$ and the result holds.

Claim: Under the hypothesis, $\exists P \in S_p(G) : P$ is A-invariant.
Proof of claim: By Frattini, if $P \in S_p(G) \to AG = GN_{AG}(P)$. $\exists A_1 \subset N_{AG}(P) : A_1 \cap G = 1$ and $AG = A_1 N_{AG}(P)$ so $\exists g \in N_{AG}(P) : A_1^g = A$ so $A \subseteq N_G(P)$. This proves the claim.

If G is not a p-group, $\exists P \in S_p(G)$ for each p which are A-invariant. In this case, $|AP| < |AG|$ so by induction, so $\langle C_P(A_0) : A/A_0 \text{ is cyclic} \rangle = P$ for each p and we're done. So G is a p-group. If A is cyclic, the result holds trivially. If not, $\exists A_0 \leq A$ with $A_0 = \mathbb{Z}_q \times \mathbb{Z}_q$. Put $\overline{P} = P/\Phi(P)$ then A_0 acts on $\overline{P}$. By the previous result, $\exists a \in A_0^{\#} : C_{\overline{P}}(a) \neq 1$. Put $\overline{P}_0 = C_{\overline{P}}(a)$. If $\overline{P}_0 = \overline{P}$, $\forall a : [P, a] \subseteq \Phi(P)$ which contradicts the faithfulness hypothesis. So $\overline{P}_0 < \overline{P}$, $\overline{P}_0$ is A-invariant. Since $\overline{P}$ is elementary abelian, $\exists \overline{P}_1$ also A-invariant: $\overline{P} = \overline{P}_0 \times \overline{P}_1$. Thus $P = P_0 P_1$, $P_0 \cap P_1 \subseteq \Phi(P)$ and by induction, $P_i = \langle C_{P_i}(A_0) : A/A_0 \text{ is cyclic } \rangle$ and again we're done by induction.

Theorem 10: Suppose $N \lhd G$, $H < G$, $\overline{G} = G/N$. If $(|N|, |H|) = 1$ and either is solvable then (a) $N_{\overline{G}}(\overline{H}) = \overline{N_G(H)}$ and (b) $C_{\overline{G}}(\overline{H}) = \overline{C_G(H)}$.

Proof: Note that $\overline{N_G(H)} \subseteq N_{\overline{G}}(\overline{H})$ which is the inverse image of $N_G(HN)$. We want to show $N_G(HN) = N_G(H)N$. Let $g \in N_G(HN)$. H, H^g are complements to N in HN so by Schur-Zassenhaus, $H^{gn} = H, n \in N$ and $gn = m \in N_G(H)$ and thus $g \in N_G(H)N$. Let K be the inverse image in G of $C_{\overline{G}}(\overline{H})$ and $K \supseteq N$. We have $K \subseteq KN \subseteq N_G(H)N$ and so by Dedekind, $K = NN_N(H)$. Since $[\overline{K}, \overline{H}] = 1$, $[K, H] \subseteq N$ and $[N_K(H), H] \subseteq N \cap H = 1$. So $N_K(H) \subseteq C_G(H)$ and $K \subseteq C_G(H)N$ and therefore, $C_{\overline{G}}(\overline{H}) = \overline{K} \subseteq \overline{C_G(H)}$. The opposite inclusion obviously holds.

13.2 p-constraint

Definition: G is p-constrained if $O_{p'}(G) = 1$ and $C_G(O_p(G)) \leq O_p(G)$ (So $O_p(G) = F(G)$).

Theorem 11: Suppose G is solvable and $O_{p'}(G) = 1$ then $C_G(O_p(G))) \subseteq O_p(G)$.

Proof: $O_p(G)$ is nilpotent so $O_p(G) \subseteq F(G)$. If $Q \in S_q(F(G))$ then Q *char* $F(G)$ so $Q \lhd G$. Thus $Q = 1$ for $q \neq p$ by hypothesis and $F(G)$ is a p-group and $F(G) = O_p(G)$. Now the result follows since $C_G(F(G)) \subseteq F(G)$.

Note: G acts on $F(G)$ by conjugation so $G/\mathbb{Z}(F(G)) \to Aut(F(G))$.

Theorem 12: If G is p-constrained, $P \in p(G)$ and $P \subseteq G$ then (1) $O_{p'}(N_G(P)) \subseteq O_{p'}(G)$ and (2) $N_G(P)$ is p-constrained.

Proof: (1) Let $\overline{G} = G/O_{p'}(G)$, then, as above, $N_{\overline{G}}(\overline{P}) = \overline{N_G(P)}$. $\overline{O_{p'}(N_G(P))} \subseteq O_{p'}(\overline{N_G(P)}) = O_{p'}(N_{\overline{G}}(\overline{P}))$, so to prove (1), we can assume $O_{p'}(G) = 1$. Let $Q = O_{p'}(N_G(P))$ and $M = O_p(G)$. $[P, Q] \subseteq P \cap Q = 1$ and so $PQ = P \times Q$ acts on M. $[C_M(P), Q] \subseteq M \cap [N_G(P), Q] = 1$ so by the $p \times q$ lemma, $[M, Q] = 1$. Hence $Q \subseteq C_G(M) \subseteq M$ (by p-constraint) and $Q = 1$.
(2) $N_{\overline{G}}(\overline{P}) = \overline{N_G(P)} = N_G(P)/(N_G(P) \cap O_{p'}(G))$. By (1), $O_{p'}(N_G(P)) = N_G(P) \cap O_{p'}(G)$ and so $N_{\overline{G}}(\overline{P}) = N_G(P)/O_{p'}(N_G(P))$ so we may assume $O_{p'}(G) = 1$. Put $M_1 = O_p(N_G(P))$ and $M = O_p(G)$. It suffices to show that $C_G(M_1)$ is a p-group. Let $Q \in S_q(C_G(M_1)), q \neq p$. Since $P \lhd N_G(P)$ and $P \subseteq M_1$ and $P \times Q$ acts on M. $C_M(P) = O_p(G) \cap C_G(P) \subseteq C_G(P)$ and therefore $C_M(P) \subseteq O_p(N_G(P))$. $O_p(C_G(P)) \lhd N_G(P)$ so $O_p(C_G(P)) \subseteq O_p(N_G(P)) = M_1$ and $C_M(P) \subseteq M_1$. Since $Q \subseteq C_G(M)$, we have $[C_M(P), Q] = 1$, thus $[M, Q] = 1$, $Q = 1$, $C_G(M)$ is a p-group.

Theorem 13: Suppose G is p-constrained, $P \in S_p(G)$ and Q is a P-invariant p'-subgroup of G then $Q \subseteq O_{p'}(G)$.

Proof: Reduce to $O_{p'}(G) = 1$ and let $M = O_p(G)$ so $M \subseteq P$. $[M, Q] \subseteq M \cap [P, Q] \subseteq M \cap Q = 1$ and $Q = 1$.

Theorem 14: If $P \in p(G)$ with $N_G(P)$ $p-$constrained then $C_G(P)$ is also $p-$constrained.

Proof: $O_{p'}(N_G(P)) = O_{p'}(C_G(P))$ so by considering factor groups, we may assume $O_{p'}(N_G(P)) = 1$. Let $N = N_G(P)$, $C = C_G(P)$, $Q = O_p(C)$, $R = O_p(N)$. Q *char* $C \lhd N$ and $Q \subseteq R \cap C$, so $Q = R \cap C$. $R \cap C \lhd C$ and $R \cap C \subseteq Q$ so $Q = R \cap C$. Let $x \in C_C(Q)$ be a p' element. $[x, R] \subseteq R \cap C = Q$, so X stabilizes the chain $R \supseteq Q \supset 1$ and so $x \in C_N(R) \subseteq R$ as N is p-constrained. Thus $C_C(Q)$ is a p-group and normal in C hence $C_C(R) \subset Q$.

Example: G solvable and $P_1, \ldots, P_n$ a Sylow system. Let $Q_i = O_{p'}(P_1P_2)$ then $Q_3, \ldots, Q_n$ is a Sylow system for $O_{p'}(G)$.

Theorem 15: Suppose V is a non-cyclic abelian r-group of operators on a p-constrained r' group X. For $r \neq p$ then $\bigcap_{v \in V^\#} O_{p'}(C_X(v)) \subseteq O_{p'}(X)$. p'-subgroup of G then $Q \subseteq O_{p'}(G)$.

Proof: Let $\overline{X} = X/O_{p'}(X)$ be V-invariant. $C_{\overline{X}}(\overline{V}) = \overline{C_X(V)}$. We may asssume $O_{p'}(X) = 1$. Let $M = \langle C_M(V_0) : V/V_0 \rangle = \langle C_M(v), v \in V^\# \rangle$ where V/V_0 is cyclic. The last equality holds since V is non-cyclic. $C_M(v) = M \cap C_X(v) \lhd C_X(v)$ so $C_M(v) \subseteq O_p(C_V(X))$. Now, $Q \subseteq O_{p'}(C_V(X))$ and $[C_M(V), Q] = 1, \forall v \in V^\#$ therefore $[M, Q] = 1$ and so $Q = 1$.

Theorem 16: If G is solvable, $C_G(F(G)) \subseteq F(G)$.

Proof: Let $Z = \mathbb{Z}(F(G))$ and N/Z be a minimal normal subgroup of $C_G(F(G))/Z$ to obtain a contradiction.

Theorem 17 (Another version of the $P \times Q$ Lemma): If P is a p-group and Q is a p' group, and $P \times Q$ acts on a p-group, M then $[M, Q] = 1$.

Proof: For the semi-direct product $(P \times Q)M$ then $P_1 = PM$ is Q-invariant. Put $P_0 = PC_M(P)$. $P_0 \lhd \lhd P_1$, $[P_0, Q] = 1$ so $[M, Q] = 1$.

Theorem 18: Suppose X acts on A, $(|X|,|A|)=1$, A abelian. Then (1) If $A_0 \subseteq A$ is an X-invariant direct factor of A, $\exists A_1 \subseteq A$: A_1 is X invariant and $A = A_0 \times A_1$; and, (b) $A = C_A(X) \times [A,X]$.

Proof: Let $f : A \to A_0$ be any projection. $\exists i : |X|i = 1 \pmod{|A|}$. Put $f_1(a) = \prod_{x\in X}[f(a^x)^{x^{-1}}]^i$. f_1 is an endomorphism, $im(f_1) \subseteq A_0$, if $a_0 \in A_0, f(a_0) = a_0$ and $f_1^2 = f_1$ so $A = A_0 \times ker(f_1)$. $f_1(a^y) = (f_1(a))^y, \forall a \in A, y \in X$ so $ker(f_1)$ is A-invariant which proves (a). For (b), let $f(a) = (\prod_{x\in X} a^x)^i$ then $f(a^y) = f(a)^y$ so $im(f) \subseteq C_A(X)$. If $a \in C_A(X)$ then $f(a) = a$ hence $C_A(X)$ is a direct factor of A. $A = C_A(X) \times A_1$, A_1, X-invariant. $[A,X] \subseteq A_1$ and $A_1 = [A,X]C_{A_1}(X)$ so $[A,X] \subseteq A_1 \subseteq [A_1,X] \subseteq [A,X]$.

Theorem 19: Suppose G is an X-group and $(|[G,X]|,|X|)=1$. (1) $[G,X] = [G,X,X]$; (2) if either X or $[G,X]$ is solvable, $G = [G,X]C_G(X)$; (3) if $[G,X] \subseteq \Phi(G)$ then $[G,X] = 1$.

Proof:
Claim: $[g,x^i] = [g,x]^i \pmod{[G,X,X]}$.
Proof of claim: $[g,x^{i+1}] = [g,x][g,x^i]^x = [g,x][g,x^i][g,x^i,x]$ and this proves the claim.
In particular, $1 = [g,1] = [g,x^{|X|}] = [g,x]^{|X|} \pmod{[G,X,X]}$ so $[G,X]/[G,X,X] = 1$ which proves (1).

For (2), form the semi-direct product, GX. $[G,X] \lhd GX$. Put $G_0 = [G,X]X$.
Claim: $G_0 \lhd G$.
Proof of claim: Suffices to show $[G,G_0] \subseteq G_0$. Let $g \in G, g_0 \in G_0$ and put $g_0 = g_1 x$ then $[g,g_0][g,g_1]^x \in G_0$. G_0 satisfies the Schur-Zassenhaus theorem. Let $g \in G$ then $X^g \subseteq G_0^g = G_0$ and X^g and X are complements so $X^{gg_1} = X, g_1 \in [G,X]$ and $[X, gg_1] \in X \cap G = 1$. $gg_1 \in C_G(X)$ and $g = cg_1^{-1}, c \in C_G(X) \in C_G(X)[G,X]$.

For (3), $G = [G,X]C_G(X)$. If $\Phi(G) \supseteq [G,X]$, $G = \langle [G,X], C_G(X)\rangle \subseteq \langle \Phi(G), C_G(X)\rangle = C_G(X)$, so $[G,X] = 1$.

Theorem 20: If ϕ is an irreducible representation of an abelian group G with kernel K, then G/K is cyclic.

Proof: Claim: If G is abelian and acts irreducibly on V then $gv = \lambda v$.
Proof of claim: $W = \{w \in V : gw = \lambda w\} \neq 0$ is G-invariant, so it is all of V. This proves the claim.
Now G/K acts faithfully and irreducibly its letting λ be the $|G|$-th root of unity in the claim, $g \mapsto \Lambda(g)$. This is an injection into a subgroup of a multiplicative subgroup of F and these subgroups are cyclic.

Corollary: If an abelian group, G, possesses a faithful irreducible representation, then $\mathbb{Z}(G)$ is cyclic.

Proof: Simple application of previous theorem.

Lemma: Let P be an elementary abelian p-group and Q be a non-cyclic abelian q-group of $Aut(P)$, $p \neq q$, then $P = \prod_{x\in Q^\#} C_P(x)$.

Proof: Regard P as a vector space over F_p. Q acts on P as a linear transformation and denote $\varphi : x \mapsto \phi_x$ be the map between Q and the linear transformations under this correspondence. By Maschke, $P = P_1 \oplus \ldots \oplus P_n$, each P_i irreducible. Let $Q_i = ker(\varphi_{|P_i})$ under the restricted map $\varphi_{|P_i} : Q \to P_i$. Q/Q_i must be cyclic and Q is non-cyclic so $Q_i \neq 1$. If $x \in Q_i$ then $P_i \subseteq C_P(x)$.

Theorem 21: Let G be a p-group and $f : Aut(G) \to Aut(G/\Phi(G))$. $ker(f) = \langle \{X : [G,X] \subseteq \Phi(G)\}\rangle$ and so $ker(f) = 1$.

Proof: This is practically the definition.

Theorem 22: If X acts on G, $(|X|, |G|) = 1$ and $G_0 \lhd \lhd G$, $C_G(G_0) \subseteq G_0$ and $[G_0, X] = 1$ then X acts trivially on G.

Proof: Suppose $G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$. Choose i maximal such that $[G_i, X] = 1$ (we want $i = n$). $N_G(G_i)$ is X-invariant. If $N_G(G_i) \not\subseteq G$, we get $[N_G(G_i), X] = 1$; but $G_{i+1} \subseteq N_G(G_i)$ which implies $[G_i, X] = 1$ — a contradiction. $C_G(G_i) \subseteq C_G(G_0) \subseteq G_0 \subseteq G_i$. So $[G_i, X, G] = 1 = [G, G_i, X]$ and by the three subgroups lemma, $[X, G, G_i] = 1$ and $[X, G] \subseteq C_G(G_i) \subseteq G_i$. Therefore, $[G, X, X] = 1$ and hence $[G, X] = 1$.

Definitions: G acts *irreducibly* on V if there are no proper G-invariant subgroups of V. G acts *faithfully* on V if $C_G(V) = 1$. G acts *non-trivially* on V if $C_G(V) \neq G$. For $\alpha \in Aut(G)$, define $\sigma(G) = \sum_{g \in G} \alpha(g)$.

Theorem 23: If G has a faithful, irreducible representation on a vector space V over F, $char(F) = p$ then G has no non-trivial normal p-subgroup.

Proof: Let φ be such a representation and $P \lhd G$. $\varphi(P)$ fixes some $v \neq 0$. Set $W = C_V(\varphi(P))$. W is G-invariant and by irreducibility, $W = G$ and φ acts trivially on G but φ is faithful so $P = 1$.

Theorem 24: Let G act on V, V, abelian with $(|G|, |V|) = 1$ then $C = V_1 \oplus V_2$ is the direct sum of G-invariant subgroups of V with $V_1 = C_V(G)$.

Proof: Let $\sigma = \sigma(G)$. Set $V_1 = C_V(\sigma)$ and $V_2 = im(\sigma)$. V_1 and V_2 are G-invariant and $|V_1| \cdot |V_2| = |V|$. Set $Z = C_V(G)$, Z is G-invariant and $Z \subseteq V_2$. *Claim:* $Z \cap V_1 = 0$. *Proof of claim:* Let $v \in Z \cap V_1$ then $\sigma(v) = |G|v$ and $\sigma(v) = 0$ hence $v = 0$.

Theorem 25: Let G act non-trivially on V, abelian, $(|G|, |V|) = 1$, then $\exists W \subseteq V$, G-invariant, on which G acts non-trivially and irreducibly.

Proof: $V = [G, V] \oplus C_V(G)$ and $[G, V] \neq 1$. By Maschke, $[G, V]$ decomposes into irreducible modules.

Theorem 26: If A is a p'-group of automorphisms of the abelian p-group P which acts trivially on $\Omega_1(P)$ then $A = 1$.

Proof: $P = C \times H$ where $C = C_P(A)$ and $H = [P, A]$. By hypothesis, $\Omega_1(P) \subseteq C$ so $\Omega_1(P) \subseteq \Omega_1(C)$ and $\Omega_1(P) = \Omega_1(C) \times \Omega_1(H)$ so $\Omega_1(H) = 1$. So $H = 1$ and $P = C$ thus A acts trivially on P and $A \subseteq Aut(P)$. and $P = 1$

Theorem 27: If A is a p'-subgroup of $Aut(P)$ and $1 \neq \phi A$, ϕ acts trivially on every proper A-invariant normal subgroup of P, then (1) $P' \subset \mathbb{Z}(P)$; (2) P/P' is an elementary abelian subgroup and A acts irreducibly on P/P'; (3) Either P is elementary abelian or P has class 2, $P' = \mathbb{Z}(P) = \Phi(P)$ is elementary abelian and ϕ acts trivially on P'.

Proof: First, ϕ acts trivially on P' since it is a proper A-invariant normal subgroup of P. ϕ does not act trivially on P/P' because if it were, $P \supset P' \supseteq 1$ of P and $\phi = 1$ which it is not. Suppose $\overline{P} = P/P' = \overline{P}_1 \times \overline{P}_2$ where $\overline{P}_1 \neq 1$ and $\overline{P}_i$ is A-invariant. Then $P = P_1 P_2$ and P_i is a proper A-invariant normal subgroup of P where P_i is the inverse image of $\overline{P}_i$. If ϕ is trivial on P_1 and P_2 then ϕ is trivial on P. Thus we can assume A acts indecomposiblyon $\overline{P}$. If $\Omega_1(\overline{P}) \subset \overline{P}$ then ϕ acts trivially on the inverse image of $\overline{P}$ and A acts trivially on $\Omega_1(\overline{P})$ but then ϕ acts trivially on $\overline{P}$. Thus $\overline{P} = \Omega_1(\overline{P})$. From Maschke, A acts irreducibly on $\overline{P}$. Now, put $B = \langle \phi^A \rangle$. Since ϕ acts

trivially on P', B acts trivially on P'. Set $H = [P, B]$. If $H \subseteq P'$, we have $1 = [H, B] = [H, B, B]$ and so $B = 1$. Thus $H \not\subseteq P'$. Moreover, since B and P are A-invariant and $H \lhd P$ and thus H is A-invariant. If $H \subset P$ then ϕ acts trivially on H and hence on $\overline{H}$ but $\overline{H}$ is a non-trivially of $\overline{P}$ hence $\overline{H} = \overline{P}$ by irreducible action of A on $\overline{P}$ and thus $H = P$. Since B centralizes P' and $P' \lhd P$, $[P', P, B] = 1 = [P, P', B]$ so $[P, B, P'] = 1$. Since $[P, B] = P$ and P' centralizes P and $P' \subseteq \mathbb{Z}(P)$ which proves 1. Assume P is elementary abelian. But $P' \neq 1$ and so $P' \subseteq \mathbb{Z}(P) \subset P$. Now if $Z = \mathbb{Z}(P)$, $\overline{Z}$ is a proper A-invariant subgroup. So $\overline{Z} = 1$ by the A-irreducibility. Hence $\mathbb{Z}(P) = P'$ and $cl(P) = 2$. Since $P' \subseteq \Phi(P)$, $P' = \Phi(P)$. If $x, y \in P$ then $[x, y] = z \in P' = \mathbb{Z}(P)$ so $[x, y^p] = z^p$. But $y^p \in \mathbb{Z}(P)$ and then $z^p = 1$ and $[x, y]^p = 1$. Since P' is abelian, it follows that P' is elementary abelian and the proof is complete.

Theorem 28: Let G be a p'-group acting non-trivially on an abelian p-group V then G acts non-trivially on $V_0 \subseteq V$ with $V_0 = \{v : pv = 0\} = \Omega_1(V)$.

Proof: By induction on $|P|$. If $Q \leq P, \Omega_1(Q) \leq \Omega_1(P)$. So if Q is any proper A-invariant subgroup, the action is trivial on $\Omega_1(Q)$ and P is a special p-group (see chapter 15) and A acts trivially on P' and irreducibly on P/P' so $cl(P) \leq 2$. Hence, $x \in P$ and $\varphi \in A$, implies $(\varphi(x)x^{-1})^p = (\varphi(x))^p x^{-1)^p})$ but then $x^p \in P'$ and φ fixes x^p. Since $[P, A] = \langle \varphi(x)x^{-1} \rangle$, $[P, A] \subseteq \Omega_1(P)$ and A would stabilize the series $P \supseteq \Omega_1(P) \supseteq 1$ and thus $A = 1$.

Theorem 29: Let G act faithfully and irreducibly on an abelian group of V, $(|G|, |V|) = 1$ then $\mathbb{Z}(G)$ is cyclic.

Proof: If $\mathbb{Z}(G)$ is not cyclic it contains a subgroup H of type (p, p) hence by an earlier result, $H = \bigcup_i H_1, H_i \cap H_j = \{0\}$ since $p \nmid |V|$ then $pV \neq \{0\}$, $\exists x_i : C_V(x_i) \neq 0$. Now G acts faithfully so $C_V(x_i) \neq V$ and $C_V(x_i)$ is G-invariant. This is a contradiction.

Theorem 30: Let P be a p-group and Q be a non-cyclic abelian q-group of automorphisms acting on a P, $q \neq p$ then $P = \prod_{x \in Q^\#} C_P(x)$.

Proof: By induction on $|P|$. Let x_j be a fixed ordering of $Q^\#$. Put $Z = \Omega_1(\mathbb{Z}(P))$ and $Z_j = C_Z(x_j)$, some j, then $Z \neq 1$ by the previous result on abelian P. The theorem holds by induction on $\overline{P} = P/Z_j$ and $\overline{C_P(x_i)} = C_{\overline{P}}(x_i)$, so $P = Z_j \prod_{i=1}^n C_P(x_i)$ but $Z_j \subseteq C_P(x_j) \subseteq P$. This proves the result.

Theorem 31: Let φ be a representation of G on a vector space V with $char(F) = 0$ or $(char(F), |G|) = 1$. If $V = V_1 \supset V_2 \supset \ldots \supset V_n \supset V_{n+1} = 0$ a sequence of G-invariant subspaces and $\varphi(G)$ acts trivially on each V_i/V_{i+1} then φ is the trivial representation.

Proof: $V = V_n \oplus W$ and W is G-invariant. $\varphi_{|W}$ is equivalent to the quotient representation, $\overline{\varphi}$ of G on V/V_n but then induction on $dim_F(V)$ yields φ_W is trivial and since φ_{V_n} is also trivial, φ is trivial.

Theorem 32: Let A be a regular group of automorphisms of a p-group P then (1) A is a p'-group; (2) A possesses no non-cyclic abelian subgroups; (3) A subgroup of A of order qr is cyclic.

Proof: Let $B \in S_p(A)$. B acts on $V = \Omega_1(\mathbb{Z}(P))$ which is elementary abelian and so $C_V(B) \neq 1$. Since elements of $A^\#$ only fix $1 \in G$, this forces $B = 1$ and A is a p'-group. (2) follows from the fact that $V = \langle C_V(\varphi) : \varphi \in Q^\# \rangle$ and this forces $C_V(\varphi) \neq 1$ contradicting regularity. For (3), let D be such a subgroup. $q \neq r$ is obvious so assume $q > r$ and $Q \in S_q(D), R \in S_r(D)$. $D = QR$ and $Q \lhd D$. If $C_D(Q) \supset Q$ then $C_Q(D) = D$ and D is abelian and hence cyclic. Hence we can also assume $C_D(Q) = Q$. Applying Thompson's $p \times q$ theorem to the action of D on V gives $C_V(R) \neq 1$ which again contradicts regularity.

13.3 A-invariance

Lemma: If G is a group acting on a group V and $H \lhd G$ then $C_V(H)$ is G-invariant.

Proof: Put $W = C_V(H)$. For $w \in W, h \in H$ and any $x \in G$, $w^{xhx^{-1}} = w$ since $xhx^{-1} \in H$. Thus $(w^x)^h = (w^x)$ and w^x is fixed by h, that is $w^x \in W$.

Theorem 33: Let G be a p-group acting on an elementary abelian p-group V (Hence G is a set of invertible transformations in $GL_n(p)$.) Then $\exists v \in V, v \neq 0 : v \in C_V(G)$.

Proof: By induction on $|G|$. Let M be a maximal subgroup of G. $|G : M| = p$ and $M \lhd G$. Put $W = C_V(M)$. By induction, $W > \{1\}$ and by the lemma, W is G-invariant. Choose $y \in G \setminus M$. The minimal polynomial for y, $min(y) \mid (x^p - 1)$ since $y^p \in M$. So $\exists w_1 \in W, w_1 \neq 0 : w_1^y = w_1$ and we already know $w_1^m = w_1, m \in M$ so $w_1 \in C_V(\langle y, M \rangle) = C_V(G)$ and we're done.

Note: In this section, A acts on G and $(|A|, |G|) = 1$ with either A or G solvable. Note that $A/C_A(G)$ acts faithfully on G.

Theorem 34: Suppose that A is an elementary abelian p-group such that $r(A) \geq 3$. If P, Q are A-invariant p'-groups, $\exists a \in A$ such that $C_P(a) \neq 1$ and $C_Q(a) \neq 1$.

Proof: Let V be a subgroup of type (p, p). Since $P = \langle C_P(v) : v \in V^{\#} \rangle$, $\exists v \in V : C_P(v) \neq 1$. Let $W \subseteq A$ such that W is of type (p, p) and $W \cap \langle v \rangle = 1$. $\exists w \in W : C_P(w) \cap C_P(v) \neq 1$ since $C_P(v)$ is W-invariant. Then $\langle v, w \rangle$ is of type (p, p) and acts on Q. Thus $\exists a \in \langle v, w \rangle^{\#}$ such that $C_Q(a) \neq 1$. Since $C_P(a) \supseteq C_P(w) \cap C_P(v) \neq 1$, we are done.

Theorem 35: If $U \leq G$ is $A-$invariant and g satisfies $(Ug)^A = Ug$ then $\exists c \in C_G(A)$: $Ug = Uc$. If N is an $A-$invariant normal subgroup of G then (1) $C_{G/N}(A) = C_G(A)N/N$ (This shows $G = [G, A]C_G(A)$.) and (2) if A acts trivially on N and G/N then G acts trivially on G. If $p \mid |G|$ (the analogous results hold for π) then (1) $\exists S \in S_p(G) : S^A = S$, (2) all such $A-$invariant Sylow $p-$groups are conjugate under $C_G(A)$, (3) every $A-$invariant p-group of G is contained in an $A-$invariant Sylow $p-$group.

Proof: Suppose $g \in G$ then $(UG)^A = Ug$ so $[g, a] \in U, \forall a \in A$. $A^{g^{-1}} a \subseteq AU$ and A and $A^{g^{-1}}$ are complements U in AU so $\exists n \in U : A = A^{gn}$ and the result holds.

Theorem 36: Let N be an A-invariant normal subgroup of G, $(|A|, |G|) = 1$ then (a) $C_{G/N}(A) = C_G(A)N/N$ and (b) if A acts trivially on N and G/N then A acts trivially on G.

Proof: By the previous result, $\exists c \in C_G(A) : Ng = Nc$. This proves (a).(b) follows from (a).

Theorem 37: Let N be an A-invariant normal subgroup of G, $(|A|, |G|) = 1$ then if A acts trivially on N, it acts trivially on $G/C_G(A)$.

Proof: Since $[N, A] = 1$, $[N, A, G] = 1 = [G, N, A]$ and so $[A, G, N] = 1$.

Theorem 38: Let G act on Ω and $K \lhd G$ with (1) $(|K|, |G/K|) = 1$, (2) K or G/K solvable, (3) K acts transitively on Ω. Then for evey complement, H of K, (1) $C_\Omega(H) \neq \emptyset$ and (2) $C_K(H)$ acts transitively on $C_\Omega(H)$.

Proof: For (a), let $\beta \in \Omega$. Since K is transitive, $|\Omega| \mid |K|$ and $G = KG_\beta$. $G/K \approx G_\beta/(G_\beta \cap K)$. Apply Schur-Zassenhaus to $G_\beta \cap K$ to get a complment H_1 with $\beta \in C_\Omega(H_1)$, $H_1(G_\beta \cap K) = G_\beta$ and $H_1 K = G$. Since all complements conjugate to H_1, (a) is established. For (b), let $\alpha, \beta \in C_\Omega(H), k \in K$ with $\alpha^k = \beta$. H and H^k are two complements of $K \cap G_\beta$ in G_β so $\exists k' \in G_\beta$ such that $\alpha^{kk'} = \beta$. $[kk', H] \leq H \cap K = 1$ so $kk' \in C_K(H)$.

Theorem 39: Let $p \mid |G|$ and suppose the action of A on G is co-prime. (1) There is an A-invariant Sylow p-group of G. (2) The A-invariant Sylow p-groups are conjugate under $C_G(A)$. (3) Every A-invariant p-subgroup is contained in an A-invariant Sylow p-subgroup of G.

Proof: The semi-direct product AG acts on $S_p(G)$ and (1) and (2) follow from previous result. For (3), let U be a maximal A-invariant p-subgroup of G, we show $U \in S_p(G)$. Assume not. Then $U \notin S_p(G_1)$, $G_1 = N_G(U)$. G_1 is A-invariant and $\exists T \in S_p(G_1)$ by (1). $U < T$ which contradicts maximality.

Theorem 40: If $T = \bigcap_{S \in S_p(G), S^A = S} S$, then T is the largest $A-$invariant $p-$subgroup of G normalized by $C_G(A)$.

Proof: By previous result, $\exists S \in S_p(G) : S^A = A$ and $\{P \in S_p(G) : P^A = P\} = \{S^c : c \in C_G(A)\}$, so the intersection of the Sylow groups is A-invariant. By previous result, any A-invariant p-subgroup is contained in an A-invariant Sylow p-group of G. If U is normalized by $C_G(A)$, then U is contained in every A-invariant Sylow p group and hence their intersection.

Theorem 41: If P is an $A-$invariant Sylow $p-$group of G and $H \leq G$ with $H^A = H, H^{C_P(G)} = H$ then $P \cap H \in S_p(H)$. If $A = P \times Q$ acts on M and P, M are $p-$groups and Q is a $p'-$group with $C_M(P) \leq C_M(Q)$ then $[M, Q] = 1$. If A acts trivially on $G/\Phi(G)$ then A acts trivially on G and if $\Phi(G)$ is a $p-$group then so is $A/C_A(G)$.

Proof: $G = \Phi(G)C_G(A)$ so $G = C_G(A)$.

Applying $P \times Q$: If $p \in \pi(G)$ and $\overline{G} = G/O_{p'}(G)$ with $C_{\overline{G}}(O_p(\overline{G})) \leq O_p(\overline{G})$ then $\forall P \in p(G), O_{p'}(N_G(P)) = O_{p'}(G) \cap N_G(P)$.

Thompson: Let a be a p' automorphism of a p group G and suppose X is a p-group of automorphisms of G and $[a, X] = 1 = [a, C_G(X)]$ then $a = 1$.

Proof: Let $N \subseteq G$ be and X-invariant subgroup such that $[a, N] \neq 1$ but $[a, K] = 1$ for all X-invariant proper subgroups K of N. Since $[N, X, a] = 1$ and $[X, a, N] = 1$, $[a, N, X] = 1$, $[N, a] \subseteq C_G(X)$, $[N, a, a] = 1$ and thus $[N, a] = 1$.

Theorem 42: Let a be a π' automorphism of a π group G and suppose $X \lhd \lhd G$ such that $[a, X] = 1 = [a, C_G(X)]$ then $a = 1$.

Proof: Let $X \lhd X_1 \lhd \ldots \lhd X_n = G$ and choose i so that $[a, X_{i+1}] \neq 1$ but $[a, X_i] = 1$. Let $N = N_G(X_i)$. Since $X_{i+1} \subseteq N$, $[a, N] \neq 1$, yet $[X_i, N, a] = 1$ and $[X_i, a, N] = 1$ so $[a, N, X_i] = 1$ and $[N, a] \subseteq C_G(X_i) \subseteq C_G(X)$. Hence $[N, a, a] = 1$ and $[N, a] = 1$.

Theorem 43: If P is a $p-$group and Q a $p'-$ group with $Q \mapsto Aut(P)$ then Q is faithful on $P/\Phi(P)$.

Proof: Suppose $b \in A$ centralizes $G/\Phi(G)$. If $b \neq 1$, there is a non-trivial power of b which is a q-element and which centralizes $G/\Phi(G)$. Let $B = \langle b \rangle$ and $g \in G$. B acts on the coset Xg. $|Fix_B(Xg)| = |X| \pmod q$. $X = \Phi(G)$ has order that is a power of $p \neq 0 \pmod q$, so b centralizes some element $x \in X$. So $G = \langle Y \rangle \leq C_G(B)$ where Y is a set of coset representatives, thus $B = 1$.

Theorem 44: If A acts on G, $(|A|, |G|) = 1$ and G be abelian, A is faithful on $\Omega_1(G)$.

Proof: WLOG, $[A, \Omega_1(G)] = 1$. Let X have order p, $\overline{G} = G/X$. A is faithful on $\Omega_1(G)$ so A is faithful on $\Omega_1(\overline{G})$ so WLOG $\overline{G} = \Omega_1(\overline{G})$. By maximality, $C_{\overline{G}}(A) = 1$ so $X = C_G(A)$, $X = \Omega_1(G)$ and so G is cyclic. This is not possible given the automorphism group of a cyclic group.

13.4 More Results

Definition: G is p-solvable if G has a normal series whose quotients consist of p-groups and p'-groups.

Definition: G is an A_p-group if $\forall S, T \in S_p(G)$, $\exists x \in C(S \cap T)$ such that $S^x = T$. For $X \in p(G)$, define $A_G(X) = N_G(X)/C_G(X)$.

Theorem 45: If G is a solvable group and H is a minimal normal subgroup then H is elementary abelian.

Proof: H is characteristically simple so $H' = 1$ and $\Omega_1(H) = H$ so H is elementary abelian.

Theorem 46: If $\alpha \in Aut(G)$ and α acts trivially on $G/\Phi(G)$ then G acts trivially on G.

Proof: Suffices to assume that α has order $q \neq p$. Let $x_1, x_2, \ldots x_r$ be a minimal generating set. Since α fixes each coset, α acts on each coset. Since $q \neq p$, α must fix an element of each coset. Say y_i is fixed in $\Phi(G)x_i$. $\langle y_1, \ldots y_r \rangle = G$ and the result holds.

1.2.3 Theorem: If G is p-solvable with $O_{p'}(G) = 1$ then $C_G(O_p(G)) \subseteq O_p(G)$.

Proof: Put $H = O_p(G)C_G(O_p(G)) \lhd G$. If $O_{p'}(H) = 1$: if not, $O_{p'}(H) \subseteq O_{p'}(G) = 1$ which is a contradiction. Suppose $H > O_p(G)$. $H/O_p(G)$ is p-solvable. $H/O_p(G)$ cannot have a normal p-group since it would be in $O_p(G)$. Let K be the inverse image of $O_{p'}(H/O_p(G))$. $K \lhd G$ and $K > O_p(G)$. $O_p(G) \in S_p(K)$ so $\exists L \in p'(G)$: $K = LO_p(G)$. Let $x \in L$, $x = yz, y \in O_p(G), z \in C(O_p(G))$. $[x, O_p(G)] = [y, O_p(G)] = 1$ so $K \subseteq O_{p'}(G)$, contradiction.

Theorem 47: If $N \subseteq G$ has a normal p-complement ($G = PN, N \lhd G$) then G is an A_p group. If $X \in p(G)$ then $A(X)$ is a p-group.

Proof: Suppose $S, T \in S_p(G)$, $G = SN = TN$. $\exists y \in N : S^x = T$. Suppose $s \in S \cap T$, $S^y \in T$ so $[s, y] \in T$, so $[s, y] = 1$ and $y \in C(S \cap T)$. Let $X \in p(G)$. $M = N_G(X)$, then $M \cap N$ is a normal p-complement of M. If $x \in X$ and $y \in M \cap N$ then $[x, y] \in X \cap (M \cap N)$, so $y \in C(X)$ and $M \cap N \subseteq C(X)$. Thus y's action is as a p-group and $A(X)$ is a p-group.

Frobenius Theorem: G be group. If $\forall X \in p(G)$, $A_G(X)$ is a p-group then G has a normal p-complement.

Proof: Let G be a minimal counterexample.

1. If $H < G$ then H has a normal p-complement.
Let $X \in p(H)$, $A_H(X) = N_H(X)/C_H(X) \to A_G(X)$, so H satisfies the hypothesis of theorem and H has a normal p-complement.

2. $O_p(G) = 1$.
Let $K = O_p(G)$. $X/K \in p(G/K)$. So $A_G(X) \to A_{G/K}(X/K)$. G/K has a normal p-complement $(M/K)(X/K) = G/K$. $M \lhd G$ and $K \in S_p(M)$, $K \lhd M$, $LK = M$ and $[L, K] \subseteq K$. $M = L \times K$, $L = O_{p'}(M)$, $M \lhd G$ and $L \lhd G$. L is a normal p-complement. Contradiction.

3. G is an A_p-group
Let $P, P_1 \in S_p(G)$. Proof is by induction on $|P : P \cap P_1|$. $P \neq P_1$ and $P \cap P_1 \neq 1$. Put $H = N_G(P \cap P_1)$. Since $O_p(G) = 1$, $H \neq G$ and H has a normal p-complement. If $P > Q$. $N_P(Q) > Q$. Pick $R, R_1 \in S_p(H)$ then $H \cap P \subseteq R$ and $H \cap P_1 \subseteq R_1$. $\exists y \in C_H(R \cap R_1) : R_1 = R^y$. Let $S \in S_p(G)$ with $R \subseteq S$. Set $S_1 = S^y$ so $R_1 \subseteq S_1$. $P \cap S > P \cap P_1$ and $P_1 \cap S_1 > P \cap P_1$ By induction, $\exists u \in C_G(S \cap P), \exists v \in C_G(S_1 \cap P_1) : P^u = S$ and $S_1^v = P_1$. $P^{uyv} = P_1$ and

$uyv \in C(P \cap P_1)$. Since $R \cap R_1$, $S \cap P$ and $S_1 \cap P_1$ all contain $P \cap P_1$, $uyv \in C_G(P \cap P_1)$.

4. Contradiction
Let $P \in S_p(G), g, h \in P$, $h = g^x$ and $h \in P \cap P_1$. Since G is a A-group, $\exists y \in C(P \cap P^x)$ with $P^{xy} = P$, $h^y = h$. Now $xy \in N(P) = C(P)P$. Since G is an $A_G(P)$ is a p-group, $xy = uv$, wtih $u \in C(P)$ and $v \in P$. $g^v = g^{uv} = g^{xy} = h^y = h$. Thus any two elements conjugate in G are conjugate in P so G has a normal p-complement.

Theorem 48: Let G be a group with no normal 2-complement and $Q \in S_2(G)$. Suppose Q has a cyclic subgroup, A of index 2. Then $3 \mid |G|$.

Proof: Since G does not have a normal p-complement, $\exists X \subseteq Q$ such that $N(X)/C(X)$ is not a 2-group. $X \cap A$ is cyclic and $|X : A \cap X|$ is 1 or 2 and X has two generators. $\exists g \in N(X)/C(X)$ of order $q, q \neq 2$ that acts faithfully on X and hence $X/\Phi(X)$. Since X has 2 generators, the Burnside Basis Theorem yields $|X/\Phi(X)| \leq 4$ and $q = 3$.

Definition: Let S be a p-group. For $A : A' = 1$, $m(A)$ is the minimal number of generators of A. $d(P)$ is the maximum value of $m(A)$ for $A \subseteq S$, $A' = 1$. $J(S) = \langle A : m(A) = d(S) \rangle$. $\mathcal{H}(G)$ be a set of p-groups, $H \subseteq G$: $N_G(H)$ does not have a normal p-complement. *Thompson ordering:* For $H, K \in G$, define $H \leq\leq K$ iff (a) $|N_G(H)|_p < |N_G(K)|_p$, or (b) $|N_G(H)|_p = |N_G(K)|_p$ and $H < K$, or (c) $H = K$.

Theorem 49: Let G be a p' group acting non-trivially on an abelian p-group, V with $(|G|, |V|) = 1$. $\exists W \subseteq V$ on which G acts non-trivially and irreducibly.

Proof: $V = V_1 \times V_2$, $V_1 = ker(\sigma)$, $V_2 = im(\sigma)$, where $\sigma(v) = \sum_{g \in G} v^g$. Let V_1 and $V_2 \neq 0$ be as above. Let $W \neq 0$ be a minimal G-invariant subgroup of V_2. Since $W \cap C_G(G) = 0$, G acts nontrivially on W.

Corollary 1: Let G be a p' group acting non-trivially on an abelian p-group, V. Then G acts non-trivially on $V_0 \subseteq V : V_0 = \{v \in V : vp = 0\}$

Corollary 2: Let G act faithfully and irreducibly on an abelian group, V. If $(|G|, |V|) = 1$, then $\mathbb{Z}(G)$ is cyclic.

Proof: If not, G has a central subgroup H which is abelian of type (p, p), some $p \mid |G|$. H is a disjoint union of $p+1$ subgroups $J_0, \ldots, J_p$ of order p. Since $p \nmid |V|$, $vp \neq 0$ and $\exists i : C_V(J_i) \neq 0$. G acts faithfully on V so $C_V(J_i) \neq V$. Since $J_i \lhd G$, $C_V(J_i)$ is a proper G invariant subgroup of V and G does not act irreducibly, contradiction.

Theorem (Thompson): Let p be an odd prime. If $S \in S_p(G)$ and both $C_G(\mathbb{Z}(S))$ and $N_G(J(S))$ have normal p-complements, so does G. There is another proof of this in the stability section.

Proof: Let G be a minimal counterexample of minimal order.

1. $\mathcal{H}(G) \neq \emptyset$ by Frobenius. Let H be maximal in the Thompson ordering of $\mathcal{H}(G)$. Put $N = N_G(H)$. $P \in S_p(N)$ with $H \subseteq P \subseteq S$.

2. $H \neq S$.
If $H = S$ then $N \subseteq N_G(J(S))$ which has a normal p-complement. So N has a normal p-complement. Contradiction.

3. $\overline{N} = N/H$ has a normal p-complement.
$P \in S_p(N)$. Since $H \neq S$, $N_S(H) > H$ and $P > H$. Let $\overline{P}$ be the image of P in $\overline{N}$ then $\overline{P} \in S_p(\overline{N})$. Suppose $\overline{N}$ does not have a normal p-complement. Since $|\overline{N}| < |G|$, either $C_{\overline{N}}(\mathbb{Z}(\overline{P}))$ or $N_{\overline{N}}(J(\overline{P}))$ does not have a normal p-complement. Let K be the complete inverse image of either $\mathbb{Z}(\overline{P})$ or $J(\overline{P})$, which ever one fails. K is a p-group and $N_G(K)$ does not have a normal p-complement. $P \subseteq N_G(K)$ so either $|N_G(K)|_p > |N_G(K)|_p$ or $|N_G(K)|_p = |N_G(K)|_p$ and $|K| > |H|$. So $K \in \mathcal{H}$, $K \geq\geq H$ but $K \neq H$, contradiction.

4. $N = G$.
N satisfies the hypothesis. $H \subseteq P \subseteq S$, $\mathbb{Z}(S) \subseteq N_G(H) = N$. $P\mathbb{Z}(S) \subseteq N \cap S$ and $P\mathbb{Z}(S) = P$. $\mathbb{Z}(S) \subseteq P$ so $\mathbb{Z}(S) \subseteq \mathbb{Z}(P)$ and $C_N(\mathbb{Z}(P)) \subseteq C_G(\mathbb{Z}(P)) \subseteq C_G(\mathbb{Z}(P))$, so $C_N(\mathbb{Z}(P))$ has a normal p-complement and so does $C_N(\mathbb{Z}(P))$. If $P = S$, $N_N(J(P) \subseteq N_G(J(S))$ has a normal p-complement. Now suppose $P < S$. Then $N_S(P) > P$ so $|N_G(J(P)|_p > |N|_p$. By maximality of H, $J(P) \notin \mathcal{H}$ and so $N_G(J(P)$ has a normal p-complement and so does $N_N(J(P))$. If $N \neq G$, since G is minimal, N has a normal p-complement, contradiction. So $N = G$.

5. $O_{p'}(G) = 1$
Put $L = O_{p'}(G)$. We show $\overline{G} = G/L$ satisfies the assumptions of the theorem. Let $K \subseteq S$. We show $\overline{N_G(K)} = N_{\overline{G}}(\overline{K})$. Let $\overline{x} \in N_{\overline{G}}(\overline{K})$. Since $L \lhd KL$, $K \in S_p(KL)$ so $\exists a \in K, b \in L$: $K^x = K^{ab} = K^b$. Hence $xb^{-1} \in N_G(K)$ and $\overline{xb^{-1}} = \overline{x}$. $\overline{N_G(J(S))} = N_{\overline{G}}(J(\overline{S}))$ so $\overline{J(S)} = J(\overline{S})$ and it has a normal p-complement. $\overline{C_G(K)} = C_{\overline{G}}(\overline{K})$. Conversely, let $\overline{x} \in C_{\overline{G}}(\overline{K}) \subseteq N_{\overline{G}}(\overline{K})$, so we can assume $x \in N_G(K)$. Since $[x, K] \subseteq K \cap L = 1$, $x \in C_G(K)$. $\overline{\mathbb{Z}(S)} = \mathbb{Z}(\overline{S})$ so $\overline{C_G(\mathbb{Z}(S)} = C_{\overline{G}(}\mathbb{Z}(\overline{S})$ and it has a normal p-complement. If $|L| > 1$, $|\overline{G}| < |G|$ so $\overline{G}$ has a normal p-complement and its complete inverse image is a normal p-complement of G. Contradiction.

6. $H = O_p(G)$ and G is p-solvable of p-length 2.
Set $K = O_p(G)$ so $H \subseteq K$. Since $G = N_G(K)$has no normal p-complement, $K \in \mathcal{H}$. By the maximality of H in $\mathcal{H}$ and the fact that $G = N_G(K) = N_G(H)$, $H = K$. By 3 and 4, G/H has a normal p-complement, so G is p-solvable of length at most 2.

7. $\overline{G} = G/H = \overline{SM}$ then $\overline{M}$ has a normal p-complement and $\overline{M}$ contains no proper $\overline{S}$-invariant subgroup.
Let $\overline{M} > \overline{M_0} > 1$ and suppose $\overline{M_0}$ is S-invariant. Let M_0 be the complete inverse image of $\overline{M_0}$. Put $G_0 = SM_0$, so $G > G_0$. Since $C_{\overline{G_0}}(\mathbb{Z}(\overline{P}))$ or $N_{\overline{G_0}}(J(\overline{P}))$ have normal p-complements, so does $G_0 = SK_0$. $K_0 \lhd G_0, S \cap K_0 = 1, [H, K_0] \subseteq K_0, [H, K_0] \subseteq H$. Hence $[H, K_0] = 1$ and K_0 centralizes H, this contradicts 5, 6, and 1.2.3.

8. $\overline{M} = \overline{Q}$ is an elementary abelian $q \neq p$ group. $\overline{S}$ acts irreducibly on $\overline{Q}$ and S is a maximal subgroup of G.
Let $q \mid |\overline{M}|$. $\overline{S}$ permutes S_q subgroups of $\overline{M}$ and the number of such subgroups divides $|\overline{M}|$. Some such orbit has size 1, say it contains $\overline{Q}$. By step 7, $\overline{M} = \overline{Q}$. $\overline{Q}$ has no proper G-invariant subgroup so $\overline{S}$ acts irreducibly on $\overline{Q}$. Finally, $G > L > S$ and $\overline{Q} > \overline{Q} \cap \overline{L} > 1$ and $\overline{Q} \cap \overline{L}$ is a proper $\overline{S}$ invariant subgroup of $\overline{Q}$, which is a contradiction. So S is maximal in G.

9. $\exists A$, abelian: $A \subseteq S$ with $m(a) = d(S)$ and with $A \nsubseteq H$. Let A be fixed such group of minimal order. Let $A_0 = A \cap H$ then A/A_0 is elementary abelian.
If $J(S) \subseteq H$, $J(S)$ *char* $H \lhd G$ so $G = N(J(S))$ has a normal p-complement, contradiction. So

$J(S) \not\subseteq H$. Since $J(S) = \langle A \rangle, S \subseteq S$, $A' = 1$ with $m(A) = d(p)$, at least one such $A \not\subseteq H$. Let A be one such of minimal order. Set $A_0 = A \cap H$. $A_1/A_0 = \Omega_1(A/A_0)$, $A_1' = 1$. So $A_1 \not\subseteq H$. Also, $m(A) = m(A_1)$. By minimality, $A = A_1$ and A/A_0 is elementary abelian.

10. Let $\overline{A} = AH/H$ then $\overline{G} = \overline{AQ}$ and $|\overline{A}| = p$.
first, we show $\overline{G} = \overline{AQ}$. Since $\overline{G} = \overline{SQ}$ and $\overline{S} \subseteq N(\overline{Q})$. This is failthful since $H = O_p(G)$ and hence a normal subgroup of $\overline{G}$. $\overline{A} = AH/H \cong A/A_0 \neq 1$.
Now, $\overline{A}$ acts non-trivially and faithfully on some $\overline{Q_1} \subseteq \overline{Q}$ by theorem 49. Let G_1 be the complete inverse image in $\overline{G}$ of $\overline{AQ_1}$. $P_1 \in S_p(G_1)$, $A \subseteq P_1$. $P_1 \subseteq S$. Since $H \subseteq P_1$, and $C_G(H) \subseteq H$, by 1.2.3, $\mathbb{Z}(S) \subseteq C_G(H) \subseteq H \subseteq P_1$ and $\mathbb{Z}(S) \subseteq \mathbb{Z}(P_1)$. Hence $C_G(\mathbb{Z}(P_1)) \subseteq C_G(\mathbb{Z}(S))$ and the latter has a normal p-complement. Since $A \subseteq P_1$ and $m(A) = d(S)$, $D(P_1) = d(S)$. Thus $A \subseteq J(P_1)$. Let $Q_2 \in S_q(N_{G_1}(J(P_1))$. $[A, Q_2] \subseteq [J(P_1), Q_2] \subseteq J(P_1)$ and $[A, Q_2]$ is a p-group. $\overline{Q_2} \subseteq \overline{Q_1}$ so $[\overline{A}, \overline{Q_2}] \subseteq \overline{Q_1}$ is a q-group and $[\overline{A}, \overline{Q_2}] = 1$. $\overline{Q_2}$ is an $\overline{A}$- invariant of Q_1 centralized by $\overline{A}$. So $\overline{Q_2} = 1$ and $Q_2 = 1$. Thus $N_G(J(P)$ is a p-group and has a normal p-complement. If $G_1 < G$, G_1 has a normal p-complement which centralizes H, contradiction. So $G = G_1$, $\overline{G} = \overline{AQ}$. By step 8, $\overline{A}$ acts failthfully and irreducibly on $\overline{Q}$ and $\overline{A}$ is elementary abelian. It is cyclic by the corollary above, so $|\overline{A}| = p$.

11. Set $W = \mathbb{Z}(H)$, $Z \subseteq W : \Omega_1(W) = Z$. If $Q \in S_q(G)$ then $Q \subseteq N(Z)$ but $Q \not\subseteq C(Z)$.
$\mathbb{Z}(S) \subseteq C_G(H) \subseteq H$ so $\mathbb{Z}(S) \subseteq W$. If $[Q, W] = 1$, then it centralizes $\mathbb{Z}(S)$ so $\mathbb{Z}(S)$ is central in G. But then $C_G(\mathbb{Z}(S))$ has a normal p-complement, which is a contradiction. By the corollary above, Q acts non-trivially on W.

12. Contradiction
$Z \lhd G$ and G acts on Z by conjugation. The kernel of the the action acts on $C_G(Z)$ and $H \subseteq C_G(Z)$. $\overline{G}$ acts on Z. Since $\overline{Q}$ is the unique maximal normal subgroup of $\overline{G}$ and $\overline{Q}$ acts non-trivially on Z by 11, $\overline{G}$ acts faithfully on Z. $Z = C \times V$ where $C = C_Z(\overline{Q})$ and V is $\overline{Q}$-invariant, $\overline{Q} \lhd G$. $\overline{G}$ acts faithfully on V. Put $d = d(S)$. Since $|\overline{A}| = p$. $m(A_0) \geq d - 1$. Now put $V_0 = V \cap A_0$, $m(V_0) = t, m(V/V_0) = r, V \subseteq \mathbb{Z}(H)$ and $\langle V, A_0 \rangle$ is abelian. $m(V) = t + r$ $d \geq m(\langle V, A_0 \rangle) = m(V) + m(A_0) = m(V \cap A_0) = t + r + m(A_0) - t \geq d - 1 + r$. So $r = 0$ or $r = 1$. Either $V = V_0$ or V_0 is maximal. Choose $a \in A \setminus A_0$ and $1 \neq \overline{b} \in \overline{Q}$, so $[\overline{a}, \overline{b}] \neq 1$ and $[\overline{a}, V_0] = 1 = [\overline{b}, V_0]$. $\langle \overline{a}, \overline{b} \rangle$ centralizes $V_0 \cap V_0^{\overline{b}}$. $V : V \cap V_0| \leq p^2$ since $\overline{A}$ is maximal in G and $\overline{a}^{\overline{b}} \notin \overline{A}$. $[\overline{G}, V_0 \cap V_0^{\overline{b}}] = 1$ so $V_0 \cap V_0^{\overline{b}} = 1$, $|V| \leq p^2$. $\overline{G}$ is generated by two elements so $\overline{G} \subseteq SL_2(p)$. $\overline{Q}$ is normalized but not centralized by $\overline{A} \subseteq SL_2(p)$, which is a contradiction (Let $N \in p'(SL_2(p)), |P| = p$ if P normalizes but does not centralizer N, then $p = 3$ and $N' = 1$.

Theorem 50a: Let G be a primitive permutation group on Ω and N a normal Hall subgroup. Let H be a transitive complement for N. If either N or H is solvable, $\exists a \in \Omega : N \subseteq G_a$.

Proof: Let $b \in \Omega$. $G = NG_b$ and $N_b = N \cap G_b \lhd G_b$ and that N_b is a Hall subgroup. $G_b/N_b \cong H_b$. Let T be a complement for N_b in G_b. $N \cap T = N \cap G_b \cap T = 1$ and $NT = NN_HT = NG_b = G$ and T is a complement for N is G. By SZ, $\exists g : T^g = H$, so $H \subseteq {G_b}^g = G_a, gb = a$.

Theorem 50b: Let G be a primitive group and G_a a normal Hall subgroup. Let N be a regular normal subgroup and either N or G_a is solvable. Then N is an elementary abelian p group.

Proof: $G = G_aN$ and $N \cap G_a = 1$ so N is also a Hall subgroup of G. Let $P \in S_p(N)$. G permutes the conjugates of P and N acts transitively. By 50a, G_a, G_a normalizes one such $S_p(N)$ group, say P. Let Q be a characteristic subgroup of P. $Q \lhd G_a$ so $G_a \subseteq G_aQ$, which is a subgroup. Since G_a is maximal, $G_aQ = G$ and $N = Q$.

Theorem 50c: Let G be primitive and G_a is nilpotent but not a 2-group then G has a regular normal elementary abelian subgroup, N.

Proof: If $K \lhd G$ and $K \subseteq G_a$, $K = 1$. If $1 < K \lhd G_a$, since G_a is maximal, $N_G(K) = G_a$. There are two cases:

Case 1: $|G_a|$ has at least two prime factors and $1 \neq P \in S_p(G)$.
$N_G(P) = H = G_a$ and $P \in S_p(G)$. H is a Hall subgroup. Let $x, y \in P, x_z = y$ and let $1 \neq Q \in S_q(H)$, $q \neq p$. $x, y \in C_G(Q)$ so $y \in C_G(Q) \cap C_G(Q^z)$, $Q = Q^z u, u \in N_G(Q)$. Put $h = zu$. $x^h = y^u = y$. If $h = h_1 h_2$ with $h_1 \in P, h_2 \in C_G(P)$ (Possible since H is nilpotent.), $x^h = x^{h_2} = y$ and x, y are P conjugate. If $H = \prod P_i$, where P_i is a Sylow system, and $x^z = y$, $\exists h_i \in P_i : y_i = {x_i}^{h_i}$. Put $h = \prod h_i$ and $x^h = y$. So H has a n.p.c.

Case 2: G_a is a p-group.
$p \neq 2$. If $K = \mathbb{Z}(H)$, $1 \neq K \lhd H$ and $N_G(K)$ has a npc. By Thompson, so does G, cll it N. N acts semi-regularly since $N \cap G_a = 1$. $G_a < G$ so $N \neq 1$. Since G is primitive, N is regular and by 50c, N is elementary abelian.

Result: If $G = PSL_2(17)$, $S \in S_2(G)$ is maximal.

Theorem 50: Let H be a maximal subgroup of G and H is nilpotent of odd order then G is solvable.

Proof: By induction on $|G|$. Suppose there is a K: $1 < K < H$ and $K \lhd G$. H/K is maximal in G/K so G/K is solvable. Since K is nilpotent, G is solvable. If no such K exists, G permutes cosets of H in G. Let $a = H$, then $G_a = H$. Let K be the subgroup of G fixing all points. Then $K \subseteq G_a = H$ and $K \lhd G$ so $K = 1$. Since G is primitive, the result follows.

Theorem 51: $\Phi(G) \subseteq F(G)$.

Proof: $\Phi(G)$ is nilpotent (Apply the Frattini argument to $\Phi(G)N_G(P), P \in S_p(\Phi(G))$.) and characteristic in G so $F(G)\Phi(G)$ is nilpotent so $\Phi(G) \subseteq F(G)$.

Definition: H is hyperfocal in G if $H_{n+1} = [G, H_n]$, $H_0 = H$ is a series that terminates in 1.

Theorem 52: Let H is hyperfocal S_π subgroup of G then H has a normal π-complement.

Proof: Induction on $|G|$. $H \neq 1$. Let $L = Foc_G(H)$ so $H' \subseteq L < H$. Let $x \in H \setminus L$. If $(g^r)^x \in H$ then $[g^r, x] \in H \subseteq L$ and $(g^r)^x = g^r \pmod L$ and G has a normal subgroup K such that G/K is a π group. $H \cap K \in S_\pi(G)$ which is hyperfocal in G so, by induction, K has a normal π complement, N. N *char* K so $N \lhd G$. Since G/K is a π number, N is a normal p-complement in G.

Theorem 53: Let H be a nilpotent π - subgroup of G. Suppose any two elements x, y elements of H that are G-conjugate are H-conjugate. Then G has a normal π complement.

Proof: H is hyperfocal in G because it is nilpotent and the result follows.

Theorem 54: Let $P \in S_p(G)$ and suppose $P \subseteq Z(N_G(P))$ then G has a normal p-complement.

Proof: P is nilpotent and the result follows from the previous theorem.

Theorem 55: If every Sylow subgroup of G is cyclic, G is solvable.

Proof: Induction on $|G|$. Let $P \in S_p(G)$ for the smallest prime, $p \mid |G|$. Set $N = N(P)$. N acts on P by conjugation so $\phi : N \to Aut(P)$. Since P is abelian, $Im(\phi)$ is a p' group. But $Aut(P) = p^t(p-1)$, $|P| = p^t$. This is impossible since p is the smallest prime dividing $|G|$.

Theorem 56: If $P \in S_p(G)$ and P is cyclic with $P \not\subseteq G'$, then G has a normal p-complement.

Proof: Put $N = N(P)$ and, again, let N act on P by conjugation. The image is a p' group in $Aut(P)$. $[P, x] \subseteq P \cap G' < P$. If S is a subgroup of P of index p, $g^{-1}g^x = 1 \pmod S$ and $g^x = g$. P is in the center of its normalizer so it has a normal p-complement.

Theorem 57: There are $p + 1$ p-subgroups of $G = SL_2(p)$. A 2-Sylow subgroup of G is quaternion. If P, P_1 are groups of order p in $G = SL_2(p)$ then $\langle P, P_1\rangle = G$.

Proof: Since there are p+1 Sylow subgroups in two orbits of size 1 and p, $\langle P_1, P\rangle = \langle P_1, \ldots P_{p+1}\rangle \lhd SL_2(p)$, so $\langle P_1, P\rangle = SL_2(p)$.

Theorem 58: Suppose A acts trivially on $G/\Phi(G)$. (a) If the action of A on G is coprime, A then A acts trivially on G. (b) If $\Phi(G)$ is a p-group, then so is $A/C_A(G)$.

Proof: (i)$G = \Phi(G)C_G(A)$ so $G = C_G(A)$. (ii) By (i), if $\Phi(G)$ is a p-group, A acts trivially on G.

Theorem 59: Let G be a p-group and $\mathcal{K}$ the set of A-composition factors of G. Suppose the action on of A on G is coprime then $\bigcap_{K\in\mathcal{K}} C_A(K)/C_G(A) = O_p(A/C_A(G))$.

Proof: We may assume, by induction, that A acts failthfully on G. $[K, O_p(G)] = 1$ for all such factor, K. By Theorem 3, every p' subgroup B acts trivially on K and the result follows.

Theorem 60: (a) If $G/\Phi(G)$ is cyclic, G is cyclic. (b) If P is a p-group, $P/\Phi(P)$ is elementary abelian.

Proof: If $G/\Phi(G)$ is cyclic, $\langle g\Phi(P)\rangle = G/\Phi(G)$, so $\langle g, \Phi(P)\rangle = G$ and so $\langle g\rangle = G$. If M is maximal in P, $|P : M| = p$ and $M \lhd P$. Since P/M is abelian, $G' \subseteq M$ for any such M and for $x \in G$, $x^p \in M$ for any such M. The second result follows.

Chapter 14

Fusion

14.1 Definitions

Definition: Let p be a prime, $T \in S_p(G), W \leq T$ with W weakly closed in T with respect to G and $D = C_G(W)$. Then $N_G(W)$ *controls fusion* in D.

Definition: $P \in S_p(G)$. $X \in p(G)$ is a *tame intersection* of $Q, R \in S_p(G)$ if $X = Q \cap R$ and $N_Q(X), N_R(X) \in S_p(N(X))$.

Definition: For $R, Q \in S_p(G)$, write $R \rightarrow_x Q$ if $\exists Q_i \in S_p(G), 1 \leq i \leq n$, and $x_i \in N_G(P \cap Q_i)$ such that (1) $P \cap Q_i$ is a tame intersection of P and Q_i for each $1 \leq i \leq n$, (2) $P \cap R \leq P \cap Q_1$ and $(P \cap R)^{x_1 x_1 \ldots x_i} \leq (P \cap Q_i)$ for each $1 \leq i \leq n$, and (3) $R^x = Q$ where $x = x_1 x_2 \ldots x_n$.

14.2 Alperin's Results

Alperin's Fusion Theorem: If $P \in S_p(G), g \in G$ and $\langle A, A^g \rangle \subseteq P$. Then for $1 \leq i \leq n$, $\exists Q_i \in S_p(G)$ and $x_i \in N(P \cap Q_i)$ such that (1) $g = x_1 x_2 ... x_n$, (2) $P \cap Q_i$ is a tame intersection of P and Q_i for each i, (3) $A \subseteq P \cap Q_1$ and $A^{x_1 x_2 \ldots x_i} \subseteq P \cap Q_{i+1}$.

Lemma 1: $Q \rightarrow P, \forall Q \in S_p(G)$.

Lemma 2: $P \rightarrow P$.

Lemma 3: $\rightarrow$ is transitive.

> *Proof:* Let $\{R_i, y_i : 1 \leq i \leq m\}$ and $\{Q_i, x_i : 1 \leq i \leq n\}$ accomplish $S \rightarrow R$ and $R \rightarrow Q$ respectively. Then $R_1, R_2, \ldots, R_m, Q_1, \ldots, Q_n$ and $y_1, y_2, \ldots, y_m, x_1, \ldots, x_n$ accomplish $A \rightarrow Q$.

Lemma 4: If $S \rightarrow_x P$, $Q^x \rightarrow P$ and $P \cap Q = P \cap S$ then $Q \rightarrow P$.

> *Proof:* It suffices to show $Q \rightarrow Q^x$. Let $\{S_i, x_i : 1 \leq i \leq n\}$ accomplish $S \rightarrow P$ then $\{S_i, x_i : 1 \leq i \leq n\}$ also accomplishes $Q \rightarrow Q^x$.

Lemma 5: If Assume $R, Q \in S_p(G)$ with $R \rightarrow P$ and $P \cap Q < R \cap Q$. Assume further, $\forall S \in S_p(G)$ with $|S \cap P| > |Q \cap P|$ and $S \rightarrow P$. Then $Q \rightarrow P$.

Lemma 6: Assume $P \cap Q$ is tame and $S \to P, \forall S \in S_p(G)$ with $|S \cap P| > |Q \cap P|$ and $S \to P$ then $Q \to P$.

Proof: By Lemma 2, we can assume $Q \neq P$ and thus $P \cap Q < P_0 = N_P(P \cap Q)$ By hypothesis P_0 and $Q_0 = N_Q(P \cap Q)$ are Sylow in $M = N_G(P \cap Q)$ so there is an $x \in M$ with $Q_0^x = P_0$. Hence $Q \to Q_x$ by Q, x; further, $P \cap Q < P_0 \leq P \cap Q^x$ so $Q^x \to P$ and finally by Lemma 3 $Q \to P$.

Proof of Lemma 1: Pick a counterexample Q with $P \cap Q$ of maximal order. By Lemma 2, $P \neq Q$ so $P \cap Q \neq P$ hence $P \cap Q < N_P(P \cap Q)$. Let $S \in S_p(G)$ with $N_P(P \cap Q) < N_S(P \cap Q) \leq P \cap S$, $S \to P$ by the maximality of $P \cap Q$ this there is a $x \in G : S \to_x P$. Now $(P \cap Q)^x \leq q^x$, $P \cap Q \leq S$ and $S^x = P$ so $(P \cap Q)^x \leq P$. Thus $(P \cap Q)^x \leq P \cap Q^x$. If $(P \cap Q)^x \neq P \cap Q^x$ then $|P \cap Q| < |P \cap Q^x|$ so by the maximality of $P \cap Q$, $Q^x \to P$. But then $Q \to P$ by Lemma 4 contradicting the choice of Q. Now we have $(P \cap Q)^x = P \cap Q^x$ and let $T \in S_p(G)$ with $N_{Q^x}(P \cap Q^x) \leq N_T(P \cap Q^x) \in S_p(N_G(P \cap Q^x))$. Again $P \cap Q^x < N_{Q^x}(P \cap Q^x) \leq T$ so $P \cap Q^x < T \cap Q^x$. Hence if $T \to P$, by Lemma 5 $Q^x \to P$ which was already shown false. Thus we do not have $T \to P$ and by the maximality od $|P \cap Q|$, $P \cap Q^x = P \cap T$. By the choice of T and since $P \cap Q^x = P \cap T$, we have $N_T(P \cap T) \in S_p(N_G(P \cap T)$. By the choice of S, $N_S(P \cap Q) \in S_p(N_G(P \cap Q)$. Since $(P \cap Q)^x = (P \cap Q^x) = P \cap T$ and $S^x = P$, we have $N_P(P \cap T) \in S_p(N_G(P \cap T)$. But now, by Lemma 6, $T \to P$, contrary to the previous observation.

Proof of Alperin: By Lemma 1, $P^{g^{-1}} \to P$. Let $Q_i, x_i, 1 \leq i < n$ accomplish $P^{g^{-1}} \to P$. $\langle A, A^{g-1} \rangle \subseteq P \cap P^{g^{-1}}$ so $A \subseteq P \cap P^{g^{-1}} \leq (P \cap Q_1)$ and $A^{x_1 x_2 \ldots x_i} \leq P \cap Q_{i+1}$ for $1 \leq i < n$ setting $x = x_1 x_2 \ldots x_{n-1}$. $P = P^{g^{-1}x}$ so $x_n = x^{-1}g \in N_G(P)$ and $g = x x_n$. Finally, let $Q_n = P$ and note that $A^{x_1 x_2 \ldots x_{n-1}} = A^{g x_n^{-1}} \leq P^{x_n^{-1}} = P = P \cap Q_n$ and the theorem holds.

Chapter 15

Involutions and special p-groups

15.1 Dihedral Groups and Involutions

Theorem 1: If $x, y \in Inv(G)$ then $\langle x, y\rangle$ is a dihedral group of order $2|xy|$.

Proof: Let $u = xy$, $U = \langle u\rangle$ and $|xy| = n$. $U^x = U^y = U$ so $U \lhd D$. $D = U \cup Ux$.

Theorem 2: If $x, y \in Inv(G)$, $n = |xy|$ and $D = \langle x, y\rangle$ then (1) $z \in D \setminus \langle xy\rangle$ is an involution; (2) if n is odd, D is transitive on involutions; (3) if n is even, exactly one of x, y is conjugate to the unique involution in $\langle xy\rangle$; (4) if n is even and z is the unique involution in $\langle xy\rangle$ then xz is conjugate to x in D iff $n = 0 \,(\mathrm{mod}\ 4)$.

Proof: Let $u = xy$, $U = \langle u\rangle$, and $|xy| = n$. $u^x = u^{-1}$ and, in fact, $v \in U \to v^x = v^{-1}$.
(1) If $z \in D \setminus U$, $z = vx$ and $(vx)^2 = vv^x = 1$.
(2) For $w \in U$, $(vx)^w = vx^w = vw^{-1}w^x x = vvw^{-2}x$ so $x^D = \{v^2x : v \in U\}$. If n is odd, U has no involutions, so $x^D = Inv(D) = D \setminus U$.
(3) If $ux = y$, $D \setminus U = \{v^2x : v \in U\} \cup \{v^2ux : v \in U\} = x^D \cup y^D$
(4) $zx \in x^D$ when z is a square in U that is when $n = 0 \,(\mathrm{mod}\ 4)$.

Theorem 3: Let G have even order with $\mathbb{Z}(G) = 1$ and suppose that G has m involutions with $n = |G|/m$ then G has a proper subgroup of index at most $2n^2$.

Proof: Let $I = Inv(G)$, $R = \{g \in G : g^x = g^{-1}, x \in I\}$ and $\{x_i\}$ representatives of the conjugacy classes of G in R for $0 \le i \le k$ and pick $x_0 = 1$. Set $m_i = |x_i^G|$ and $B_i = \{(u, v), u, v \in I : uv = x_i\}$, put $b_i = |B_i|$. If $u, v \in I$ then either $u = v, uv = 1$ or $\langle u, v\rangle$ is dihedral. In either case, $(uv)^u = u^{-1}$ so $uv \in R$. $m^2 = |I \times I| = \sum_{i=0}^{k} m_i b_i$.

Now, $\exists t_i \in Inv(G) : (x_i)^{t_i} = x_i^{-1}$. If $u, v \in B_i, (x_i)^u = x_i^{-1}$ and $(u, v) \mapsto u$ is an injection from B_i into $t_i C_G(t_i)$; thus $b_i \le |C_G(t_i)$ and $m_i b_i \le |G|$, in fact, $m_0 = 1$ and $b_0 = m$ so $m^2 \le m + k|G|$. Let $H < G$ be a subgroup of minimal index, $s = |G/H|$. If $i > 0$ then $x_i \notin \mathbb{Z}(G)$ and $m_i = |G : C_G(x_i)| \ge s$. $|G| \ge \sum_{i=0}^{k} m_i \ge 1 + ks$ and $k \le \frac{(|G|-1)}{s}$. This gives $m^2 \le (|G|\frac{(|G|-1)}{s}) + m$. But $n = \frac{|G|}{m}$ and $m \ge 2$ so $s \le \frac{n(n-m^{-1})}{(1-m^{-1})}$ and $s \le (2n^2)!$.

Theorem 4: The G be a finite simple group of even order and $t \in Inv(G)$ with $n = |C_G(t)|$ then $|G| \le (2n^2)!$.

Proof: By the previous result, $\exists H < G$ such that $|G : H| \le 2n_0^2, n_0 = |G|/m$ where $m = |Inv(G)|$ and $m \ge |t^G| = |G : C_G(t)|$ and so $n_0 \le \frac{|G|}{|G:C_G(t)|} = n$. Representing G as a permutation group

on the cosets $\{Hx\}$, $k = |G/H| \leq 2n^2$. Since G is simple, this representation is faithful and G is isomorphic to a subgroup of S_k and so $|G| \leq k! \leq (2n^2)!$.

Brauer-Fowler Theorem: Let H be a finite group. There are at most finitely many finite simple groups with an involution t such that $H \cong C_G(t)$.

Proof: Follows from previous result.

Thompson Order Formula: Let G be a finite group with $k \geq 2$ conjugacy classes of involutions $\{x_i^G\}$, $i = 1, 2, \ldots, k$. Let n_i be the number of ordered pairs $u \in x_1^G, v \in x_2^G$ and $x_i \in \langle uv \rangle$ then $|G| = |C_G(x_1)||C_G(x_2)| \sum_{i=1}^{k} \frac{n_i}{C_G(x_i)}$.

Proof: Again let $I = Inv(G)$, $\Omega = x_1^G \times x_2^G$. $|\Omega| = |x_1^G||x_2^G| = |G : C_G(x_1)||G : C_G(x_2)|$. For $(u, v) \in \Omega, u \notin v^G$, there is a unique involution $z(u, v) \in \langle uv \rangle$. Let $\Omega_z = \{(u, v) : z = z(u, v)\}$. $\Omega = \bigcup_{z \in I} \Omega_z$ and $|\Omega_z| = |\Omega_{x_i}|$ for $z \in x_i^G$. So $\sum_{z \in I} |\Omega_z| = |G : C_G(x_i)|n_i$ and $|\Omega| = \sum_{i=1}^{k} |G : C_G(x_i)|n_i$.

Remark: n_i can be calculated if $x_i^G \cap C_G(x_i)$ is known so $|G|$ can be calculated by the fusion of involutions in local subgroups.

15.2 Critical subgroup of a p-group:

Definition 1: H *char* G is a *critical subgroup* if $\Phi(H) \leq \mathbb{Z}(H) \geq [G, H]$. $C_G(H) = Z(H)$.

Definition 2: $Mod(p^n) = \langle x \rangle \ltimes \langle y \rangle$, $|x| = p^{n-1}$, $|y| = p$. $D(2^n) = \langle x \rangle \ltimes \langle y \rangle$, $x^y = x^{-1}$. $SD(2^n) = \langle x \rangle \ltimes \langle y \rangle$, $x^y = x^{2^{n-2}-1}$. $Q(2^n) = G/\langle x^{2^{n-2}}, y \rangle$, where $|y| = 4$, $x^y = x^{-1}$, note that $\mathbb{Z}(G) = \langle x^{2^{n-2}}, y \rangle$.

Theorem: Let G be a non-abelian group of order p^n with a cyclic normal subgroup of order p^{n-1} $G \cong Mod(p^{n+1})$, $G \cong D(2^{n+1})$, $G \cong SD(2^{n+1})$, or $G \cong Q(2^{n+1})$.

Proof: Since G is non-abelian, $n \geq 3$. Let X be a cyclic subgroup: $|G : X| = p$. $X = C_G(X)$ and $\exists y \in G \setminus X$ such that y acts non-trivially on X. $y^p \in X$ so y induces an automorphism of order p. $Aut(X)$ has a unique subgroup of order p (case 1) unless $p = 2$ and $n \geq 4$ and in that case $Aut(X)$ has 3 involutions (case 2). In case 1, $x^y = xz$ for some z of order p in X. In case 2, $x^y = x^{-1}z^\epsilon$ where $\epsilon = 0, 1$ and $z \in Inv(X)$. If G splits over X, $G = X \rtimes \langle y \rangle$ and $G \cong Mod(p^n), D(2^n), SD(2^n)$. Otherwise, $C_X(y) = \langle x^p \rangle$ if $x^y = xz$ while $C_X(y) = \langle z \rangle$ otherwise. $y^p \in C_X(y)$ and since G does not split over X, $\langle y, C_X(y) \rangle$ does not split over $C_X(y)$ and hence it is abelian and $C_X(y) = \langle y^p \rangle$ and $y^p = x^p$ if $x^y = xz$ and $y^2 = z$ otherwise. Suppose $x^y = xz$, $z = [y, x] \in C(\langle x, y \rangle)$. So, $yx^{-1})^p = y^p x^{-p} z^{\frac{p(p-1)}{2}}$ but $z^{\frac{p(p-1)}{2}} = 1, p \neq 2$, thus $p = 2$ and $z = x^{2^{n-2}}$ and if $n \geq 4$ then setting $i = 2^{n-3} - 1$ so $(yx^i)^2 = 1$; if $n = 3$, $x^y = x^{-1}$. We're left with $p = 2$, $x^y = x^{-1}z^\epsilon$ and $y^2 = z$. If $\epsilon = 0$, $G \cong Q(2^n)$ but $z \in \mathbb{Z}(G)$, $(yx)^2 = y^2 x^y x = zx^{-1}zx = 1$ so the extension does split.

Theorem 5: If $G = \langle x \rangle$, $|x| = q = p^n$, $A = Aut(G)$. (1) $a \mapsto m(a) \subseteq U(q)$ is an isomorphism on the units of q; (2) the cyclic subgroup of order $p - 1$ is faithful on $\Omega_1(G)$; and, (3) $P \in S_p(A)$ is cyclic and faithful.

Proof: Elementary.

Theorem 6: Let G be a non-abelian group with a cyclic normal subgroup, U, of order p^n and $C_G(U) = U$. Then either (1) $G \cong D(2^{n+1})$, $G \cong SD(2^{n+1})$, or $G \cong Q(2^{n+1})$; or, (2) $M = C_G(\mho^1(U)) \cong Mod(p^{n+1})$ and $E_{p^2} = \Omega_1(M)$ char G.

Proof: Let $\overline{G} = G/U \to Aut(U)$. $\overline{G} \neq 1$ and $n \geq 2$ if $|G| = p$. If $\overline{G} > p$ the conclusion holds by the previous result. $\exists \overline{y} \in \overline{G}$, $|\overline{y}| = p$, $u^y = u^{p^{n-1}+1}$, $U = \langle u \rangle$. $M =< \langle y, u \rangle$. $M = Mod_{p^{n+1}}$, $E = \Omega_1(M) = E_{p^2}$, E *char* G. Since $\overline{G}' = 1$, $\overline{G}$ is cyclic or $p = 2$ and $u^g = u^{-1}$. In the first case, $\Omega_1(\overline{G}) = \overline{M}$, $E = \Omega_1(M) = \Omega_1(G)$ *char* G. In second case, $\mho^1(U) = \langle u^2 \rangle = \langle [u, g] \rangle$ and $G' \subseteq U$. So $G' = \mho^1(U)$ or U *char* G' *char* G. Thus $E = \Omega_1(C_G(\Omega^1(U)))$ *char* G.

Definition: A *critical* subgroup of G is a characteristic subgroup H *char* G such that $\Phi(H) \leq \mathbb{Z}(H) \geq [G, H]$ and $C_G(H) = \mathbb{Z}(H)$ A p-group is *special* if $\Phi(G) = \mathbb{Z}(G) = G^{(1)}$, *extra-special* if the center is cyclic.

Theorem 7: Every $p-$group has a critical subgroup.

Proof: Let S be the set of characteristic subgroups, H, of G with $\Phi(H) \leq \mathbb{Z}(H) \geq [G, H]$ and $C_G(H) = \mathbb{Z}(H)$ and H be a maximal element. Claim: H is critical. If not, set $K = C_G(H)$, $Z = \mathbb{Z}(H)$ and define X by $X/Z = \Omega_1(\mathbb{Z}(G/Z)) \cap K/Z$. The $K \not\leq H$ and $Z = H \cap K$; since $K \lhd G$, $X \neq Z$ but then $XH \in S$ violating the maximality.

Definition: A $p-$group P is **special** if $\Phi(G) = Z(G) = G'$ and **extra-special** if $Z(G)$ is cyclic.

Theorem 8: If G is special, $\mathbb{Z}(G)$ is elementary abelian.

Proof: $g^p \in \Phi(G) = \mathbb{Z}(G)$ $1 = [g^p, h] = [g, h]^p$ so $G^{(1)}$ is elementary so $\mathbb{Z}(G) = G^{(1)}$.

Theorem 9: Let E be an extra-special subgroup of G $[G, E] \leq \mathbb{Z}(G)$, then $G = EC_G(E)$.

Proof: $Z = \langle z \rangle = Z(E)$. $E/Z \leq Aut_G(E) \leq C = C_{Aut(E)}(E/Z)$. Suffices to show $E/Z = C$. Let $\alpha \in C$ and $\langle x_i Z \rangle$ is a basis for E/Z. Then $[x_i, \alpha] = z^{m_i}$, $0 \leq m_i < p$ and $E = \langle x_i, 1 \leq i \leq n \rangle$ and thus $|C| \leq p^n = |E/Z|$.

Definition: A p-group is of symplectic type if it has no non-cyclic characteristic abelian subgroups.

Theorem 10: If G is of symplectic type, $G = E * R$ where (1) $E = 1$ or is extra-special; (2) either R is cyclic or R is dihedral;, semi-dihedral or quaternion of order ≥ 16.

Proof: G has a critical subgroup H, $U = \mathbb{H}$, let Z be a cyclic subgroup of U of order p. $G^* = G/Z$. Put $K^* = \Omega_1(H^*)$ and let E^* be the complement to $\mathbb{Z}(K)^*$ in K^*. We can show K is extraspecial. See Aschbacher p 109 for the rest of the argument.

Theorem 11: Let E be an extra-special p-group with $Z = \mathbb{Z}(G)$, $\overline{E} = E/Z$. Identify Z with $\mathbb{Z}_p$ and $\overline{E}$ as a vector space over Z then (1) $f : \overline{E} \times \overline{E} \to Z$ by $f(\overline{x}, \overline{y}) = [x, y]$ is a symplectic form; (2) $m(\overline{E}) = 2n$; (3) if $p = 2$, then $Q(x) = x^2$ is the associated quadratic form; (4) if $Z \leq U \leq E$, U is extra-special or abelian iff $\overline{U}$ is non-degenerate or totally isotropic, respectively. If $p = 2$, then U is elementary abelian iff $\overline{U}$ is totally singular.

Proof: Aschbacher, p 111.

Theorem 12: G a p group, A, a p'-group. Let A be a maximal abelian normal subgroup of G, $Z = \Omega_1(A)$ then (1) $A = C_G(A)$, (2) $(C_G(A/Z) \cap C(Z))' \leq A$, (3) if $p \neq 2$, $\Omega_1(C_G(Z)) \leq C_G(A/Z)$.

Proof: Let $C = C_G(A)$ and $a \leq C \lhd G$. If $C \neq A$, $\exists D : |D/A| = p$ and $D/A \subseteq \mathbb{Z}(G/A) \cap C/A$. Then $D \lhd G$ and D is abelian contradicting the maximality of A. $(C_G(A/Z) \cap C(Z)^{(1)} \leq C(A)$ so 1 implies 2. Let $P \neq 2$, $|x| = p$, $x \in C_G(Z)$ and $X = \langle x, A \rangle$ and $Y = \langle x C_A(\langle x, Z \rangle)/Z \rangle$. $cl(Y) \leq 2$ so $W = \Omega_1(Y)$ is of exponent p. Thus $W = \langle x, Z \rangle$. But W *char* Y so $N_X(Y) \leq N_X(W) = Y$ so $Y = X$ and 3 holds.

Theorem 13: G a p group. If $p \neq 2$ and $cl(G) \leq 2$ then $\Omega_1(G)$ is of exponent p.

Proof: Let x, y be elements of order p. $[x, y] = z \in \mathbb{Z}(G)$ so $(xy)^p = x^p y^p z^{\frac{p(p-1)}{2}} = 1$.

Theorem 14: G a p group, A, a p'-group. Let $p \neq 2$ and Z be an elementary abelian normal subgroup of G then $Z = \Omega_1(C_G(Z))$.

Proof: Let $X = \Omega_1(C_G(Z))$. *Claim:* $exp(X) = p$. If claim is true, and $X \neq Z$, $\exists D : |D/A| = p$ and D is elementary abelian, contradicting maximality. *Proof of claim:* Let A be a maximal abelian normal subgroup of G containing Z, then $Z = \Omega_1(A)$. $[X, A] \leq Z$ and so $X^{(1)} \leq A$. Choose $U \leq X$ of minimal order subject to $U = \Omega_1(U)$ and U not of exponent p. $\exists x, y \in U : U = \langle x, y \rangle$ $V = \langle x^U \rangle \neq U$ and so $exp(V) = p$. Hence $z = [x, y]$ has order at most p so $X^{(1)} \leq A, z \in Z$. As $X \leq C(Z)$, $exp(U) = p$ contrary to the choice of U.

Theorem 15: G a p group, A, a p'-group. If G is abelian then A is faithful on $\Omega_1(G)$.

Proof: WLOG, A centralizes $\Omega_1(G)$. Let $|X| = p$ in G and $\overline{G} = G/X$. A is faithful on $\Omega_1(\overline{G})$ and so WLOG, $\overline{G} = \Omega_1(\overline{G})$. We may take, $C_{\overline{G}}(A) = 1$ so $X = \Omega_1(G)$ so G is cyclic. But this contradicts the known structure of the automorphism group.

Theorem 16: Let H be a critical subgroup of G, then (1) A is faithful on H (2) if $p \neq 2$ then A is faithful on $\Omega_1(H)$ and there is a critical subgroup of G such that $\Omega_1(H)$ contains each element of order p in $C_G(\Omega_1(H))$.

Proof: $C_G(H) \leq H$ so by the $p \times q$ lemma (with $P = H, Q = C_A(H)$), $C_A(H) = 1$, proving (1). For (2), see Aschbacher p114.

15.3 More on special p-groups

Lemma: If M is a normal subgroup of a p-group, P, maximal subject to being abelian then $M = C_P(M)$.

Proof: $M \subseteq H = C_P(M)$ since M is abelian. Supose $H \supset M$ and set $\overline{P} = P/M$. $\overline{H} \subset \overline{P}$, $H \lhd P$ and $\overline{H} \neq 1$ so $\overline{H} \cap \mathbb{Z}(\overline{P}) \neq 1$. If $\overline{X}$ is a subgroup of $\overline{H} \cap \mathbb{Z}(\overline{P})$, $X \lhd P$ and $X \subseteq H$. Since H centralizes M, $M \subseteq \mathbb{Z}(X)$. X/M is cyclic of order p and so X is abelian, this is a contradiction.

Theorem 17: A p-group, P, possesses a characteristic subgroup, C, with the following properties: (1) $cl(C) \leq 2$; (2) $[P, C] \subseteq \mathbb{Z}(C)$; (3) $C_P(C) = \mathbb{Z}(C)$; (4) Every nontrivial p' automorphism of P induces a non-trivial automorphism of C.

Proof: Suppose that such a characteristic subgroup C exists. Let ϕ be a p' automorphism of P which acts trivially on C and put $A = \langle \phi \rangle$. $[C, A] = 1$ so $[C, A, P] = 1$ and $[P, C, A] = 1$ so $[A, P, C] = 1$. $[A, P] \subseteq C_P(C)$ and A stabilizes $P \supseteq [A, P] \supseteq 1$ and $A = 1$ so $\phi = 1$ and 3 implies 4. Let M be a normal subgroup of a P, maximal subject to being abelian so $C_P(M) = P$. If M *char* P, $C = M$ satisfies the theorem because $C_P(C) \subseteq C$ and C is of class 1 further $C/\mathbb{Z}(C)$ is trivial and $[P, C] \subseteq C = \mathbb{Z}(C)$ and so 1 and 2 hold.

Let D be a maximal characteristic abelian subgroup of P containing D so $D \subset M$. $M \subseteq H = C_P(D)$ and so $D \subset H$ and H *char* P. Set $\overline{P} = P/D$ then $\overline{H} \neq 1$ so $\overline{C} = \overline{H} \cap \Omega_1(\mathbb{Z}(\overline{P}) \neq 1$ We claim the preimage, C, has the required properties. First the inverse image, K of $\Omega_1(\mathbb{Z}(\overline{P}))$ is characteristic in P and so $C = H \cap K$ *char* P. Since $C \subseteq H = C_P(D)$, $D \subseteq \mathbb{Z}(C)$ but this is characteristic in P so $\mathbb{Z}(C) = D$ by maximality of D. But then $C/\mathbb{Z}(C)$ is elementary abelian and $cl(C) = 2$. Further, since $\overline{C} \subseteq \mathbb{Z}(\overline{P})$, $[\overline{C}, \overline{P}] = 1$ whence $[P, C] \subseteq D$ and C satisfies 1 and 2.

Now set $Q = C_P(C)$ and suppose $Q \not\subseteq C$. $Q \cap C = D$ and $Q \subseteq H$ since Q centralizes D. Thus $\overline{Q} \subseteq \cap\overline{C} = 1$, $\overline{Q} \lhd \overline{P}$ and $\overline{Q} \neq 1$. But $1 \neq \overline{Q} \cap \Omega_1(\mathbb{Z}(\overline{P})) = \overline{C}$ and thus $\overline{Q} \cap \overline{C} \neq 1$, a contradiction. So $Q \subseteq C$ and $Q = \mathbb{Z}(C)$ and 3 holds.

Theorem 18: If P is a p-group then $\Phi(P)$ is the smallest subgroup, H, such that G/H is elementary abelian.

Proof: If M is maximal then $M \lhd G$ and $|G : H| = p$ and $P' \leq M$ so $P' \leq \Phi(P)$ so $P/\Phi(P)$ is abelian. $g^p \in M$ so $g^p\Phi(P)$ hence $P/\Phi(P)$ is elementary abelian.

Theorem 19: Let A be a p' group of automorphisms of a p group P and let $\phi \in A^{\#}$, then P possesses an A-invariant special subgroup Q such that Q acts irreducibly on $Q/\Phi(Q)$, ϕ acts non-trivially on $Q/\Phi(Q)$ and ϕ act trivially on $\Phi(Q)$.

Proof: Suppose $b \in A$, $[b, G/\Phi(G)] = 1$. WTS $b = 1$. If not, there is a power of b that is a q-element. Put $B = \langle b \rangle$ and $g \in G$. B acts on the coset $X = g\Phi(G)$ and the fixed points, $m = |X| \pmod p$, $|X| = |\Phi(G)|$ is a power of p. $|X| \neq 0 \pmod q$ so $[B, x] = 1$ for some $x \in X$ so B centralizes a set, Y of coset representatives for $\Phi(G)$ in G so $G = \langle Y \rangle \leq C_G(B)$ so $B = 1$.

Chapter 16

Stability

16.1 Quadratic Action

Definition 1: G is *π-separable* iff every composition factor of G is either a π-group or a π' group. G is *π-solvable* iff every composition factor of G is either a solvable π-group or a π' group.

Theorem 1: (1) If G is π separable iff the upper and lower π series of G terminate at G.
(2) If G is π-separable (π-solvable) so are subgroups and homomorphic images. G.
(3) If G is π-separable a minimal normal subgroup of G is either a π-group or a π'-group.

Proof: For 3, let K be a minimal normal subgroup of the π separable group G. K is characteristically simple an is thus a direct product of simple groups. There is a composition series in which one of the isomophic subgroups in the direct product is the last term and this must be a π or π' group. For 2, homomorphic and normal subgroups are sutomatically π-separable (or π-solvable). Let $H \leq G$ and K be a minimal normal subgroup of G, $\overline{G} = G/K$. By induction, $\overline{H}$ is π-separable so we only need to show $H \cap K$ is; this follows from 3 since K is either a π' group or a solvable π group. For 1, if the upper or lower series terminate, they can be refined to a composition series and each of the factors is either a π group or a π' group. In either case, G is π separable. Conversely, if G is π-separable and the upper π series of G terminates in the proper subgroup H of G, putting $\overline{G} = G/H$, we have $O_\pi(G) = O_{\pi'}(G) = 1$. But $\overline{G}$ is π separable by 2 and so a minimal normal subgroup $\overline{K}$ is either a π or π' group by 3 and thus either $\overline{K} \subseteq O_\pi(\overline{G})$ or $\overline{K} \subseteq O_{\pi'}(\overline{G})$ and either is a contradiction establishing 1.

Theorem 2: If G is π separable and $\overline{G} = G/O_{\pi'}(G)$ then $C_{\overline{G}}(O_\pi(\overline{G})) \subseteq O_\pi(\overline{G})$.

Proof: STS this when $O_{\pi'}(G) = 1$. Set $H = O_\pi(G)$ and $C = C_G(H)$ so $C \cap Z = \mathbb{Z}(H)$ and we must show $C = \mathbb{Z}(H)$. $O_\pi(C)\, char \lhd G$ so $O_\pi(C) \lhd G$ and hence $O_\pi(C) \subseteq H$. Thus $O_\pi(C) = C \cap H = \mathbb{Z}(H)$. On the other hand, $\mathbb{Z}(H) \lhd G$ and $\mathbb{Z}(H) \subseteq C$ so $\mathbb{Z}(H) \subseteq O_\pi(C)$ and thus $\mathbb{Z}(H) = O_\pi(C)$. Assume, by way of contradiction, that $C \supset \mathbb{Z}(H)$ then $C \supset O_\pi(C)$. C is π-separable so $L = O_{\pi,\pi'}(C) \subset O_\pi(C)$. $L/O_\pi(C)$ is a π' group, $\mathbb{Z}(H) = O_\pi(C)$ is a normal S_p subgroup of L and by Schur-Zassenhaus, $\mathbb{Z}(H)$ has a normal complement, $K \neq 1$ in L which is a normal $S_{\pi'}$ subgroup of L. But $K \subseteq C$ and $[C, \mathbb{Z}(H)] = 1$ so $L = \mathbb{Z}(H) \times K$ and since K is a π' group, $K \lhd G$ and $K \subseteq O_{\pi'}(G) = 1$, a contradiction.

Theorem 3: If G is π-solvable $C_G(P \cap O_{p',p}(G)) \subseteq O_{p',p}(G)$.

Proof: Let $\overline{G} = G/O_{p'}(G)$. $C_{\overline{G}}(\overline{P}) \subseteq O_p(\overline{G})$. By coprime action, $C_{\overline{G}}(\overline{P}) = C_G(P)O_{p'}(G)/O_{p'}(G)$. By Theorem 2, $C_G(O_{p',p}(G)) \subseteq O_{p',p}(G)$ and the result follows.

Theorem 4: Let G be a p-solvable group in which $O_{p'}(G) = 1$ and $H = O_p(G)$, then G/H is faithfully represented on $H/\Phi(H)$.

Proof: Let g act by conjugation on H. If $[g, H] = 1$, $g \in p(G)$ because $O_{p'}(G) = 1$. So gH acts on H and is a p'-element. By the result in the critical subgroups section, if gH acts non-trivially on H then gH acts non-trivially on $H/\Phi(H)$.

Definitions 2: If V is an elementary abelian p-group then a acts quadratically on V if $[V, a, a] = 1$, in which case, $v^{(a-1)^2} = 0$. G is said to be *p-separable* if two non conjugate elements of G remain non-conjugate in some finite p-group endomorphic image of G. The *upper π series* is $\{1\} \subseteq O_\pi(G) \subseteq O_{\pi,\pi'}(G) \subseteq O_{\pi,\pi',\pi}(G) \ldots$ The *lower π series* is $\{1\} \subseteq O_{\pi'}(G) \subseteq O_{\pi',\pi}(G) \subseteq O_{\pi',\pi,\pi'}(G) \ldots$.

Examples of quadratic action:
(a) G a p-group acting on the elementary abelian p-group V: $|V/C_V(G)| = p$;
(b) $G \in S_p(SL(V))$ acting on V the vector space over F_{p^m}; in this case, note $x \in S_p(SL_2(p)) \to (x-1)^2 = 0$.
(c) $V, G \lhd H$, G-abelian, since $[V, G] \subseteq V \cap G$ and $[V \cap G, G] = 1$.

Theorem 5: If G acts quadratically on V then (a) $[v^n, a] = [v, a^n] = [v, a]^n$, (b) $|V| \leq |C_V(a)|^2$, (c) $G/C_G(V)$ is an elementary abelian $p-$group.

Proof: $[v, a^2] = [v, a][v, a]^a$ but quadratic action gives $[v, a]^a = [v, a]$ so $[v, a^2] = [v, a]^2$. $[V, G'] = 1$ so $G' \subseteq C_G(V)$ and so $G/C_G(V))$ is abelian. Since $[v, a^p] = 1$, it is elementary abelian. For (b), note that $V/C_V(G) \cong [V, a] \leq C_V(a)$.

Theorem 6: Let G act on an F_q vector space $W \neq 0$, $q = p^m$. Suppose $G = \langle a, b\rangle$ and a, b act quadratically on W, $G/C_G(W)$ is not a $p-$group, $|ab| = p^e k, k \mid (p-1)$ then $\exists \varphi : G \to SL_2(q)$.

Proof: By induction on $|G| + dim(W)$. If action is not faithful, we're done by induction. Let W_1 be a maximal G-invariant subspace of W. If $G/C_G(W_1)$ is not a p-group,then $C_G(W/W_1)$ is not a p-group; if $W_1 \neq 0$, again we're done by induction. So G acts faithfully and irreducibly on W and if a, b are p-elements, they act quadratically and G is not abelian. By Schur, $\langle ab\rangle$ acts as a scalar on a minimal $\langle ab\rangle$-invariant subspace of W. $\exists 0 \neq W \in W, \lambda \in F_q^* : w^{ab} = \lambda w$. If $w^a \in F_q w$, it is G-invariant and $W = F_q w$ by irreducibility and G is abelian. Contradiction. Thus $W_1 = F_q w + F_q w^a$ is 2-dimensional and we have: $[w, a] \in C_{W_1}(a)$ and $w^{b^{-1}} - w \in C_{W_1}(b)$. So $(w^a)^a \in W_1$, $w^b \in W_1$ and $w^{ab} \in W_1$. so W_1 is G-invariant and $W = W_1$. $G \leq SL(W)$ since $SL_2(q)$ is generated by p-elements a, b.

Definition 3: G is *p-stable* if $\forall a \in G, [V, a, a] = 1$ implies $aC_G(V) \in O_p(G/C_G(V))$.

Example of non-p-stable group: $G = \begin{pmatrix} A & 0 \\ u & 1 \end{pmatrix}$, $A \in SL_2(p), u = (\alpha, \beta)$. V consists of lower triangular matricies. $V = O_p(G)$ and $G/V \cong SL_2(p)$. G is not p-stable.

Question: If V/F_q, $q = p^n$, is a faithful G-module, when does a p element of G have a quadratic minimal polynomial? This is trivial for $p = 1$ and is true for all elements of $SL_2(q)$. Let G be a group and $O_p(G) = 1, p \neq 2$ A faithful representation of G on V, φ is *p-stable* if no p-element of $\varphi(G)$ has a quadratic minimal polynomial. G is p-stable if all such faithful representations of G are p-stable.

Lemma: If G is p-stable and a acts trivially on $[V, a]$ then $\langle A\rangle C_G(V)/C_G(V)$ is a p-group.

Proof: $[V,a,a]=1$ so $aC_G(v)\in O_p(G/C_G(V))$ and $\langle aC_G(V)\rangle=\langle A\rangle\subseteq O_p(G/C_G(V))$.

Theorem 7: Let $p\neq 2$ and G be faithful on V. Suppose (1) $G=\langle a,b\rangle$ where a and b act quadratically on V and (2) G is not a $p-$group then (1) the Sylow 2 subgroups of G are not abelian and (2) If Q is a normal p'-subgroup of G and $[Q,a]\neq 1$ then $p=3$ and there is a section of G isomorphic to $SL_2(3)$. If $p\neq 2$.

Proof: Let $|ab|=p^ek$ and q be a power of p with $k\mid(q-1)$. Write V additively as a vector space over F_p and choose a basis $\langle v_1,v_2,\ldots,v_n\rangle$; the action can be extended to an action of G over W. By the previous result, $\exists\varphi: G\to SL_2(q)$ with $G^\varphi=\langle a^\varphi,b^\varphi\rangle$ and G is not a p-group so it is not p-closed. This gives (a). (b) follows since if Q^φ is an a^φ-invariant p'-subgroup such that $[Q^\varphi,a^\varphi]\neq 1$.

Theorem 8: Suppose $p\neq 2$ and the action of G on V is faithful and not $p-$stable then (1) the Sylow 2-subgroups of G are non-Abelian and (2) if G is $p-$separable then $p=3$ and there is a section of G isomorphic to $SL_2(3)$.

Proof: $\exists a\in G\setminus O_p(G)$ such that $[V,a,a]=1$. Let $\mathcal{K}$ be the G-composition factors of V. $O_p(G)=\bigcap_{W\in\mathcal{K}}C_G(W)$. Hence, $\exists W\in\mathcal{K}, a\notin C_G(W)$ so a $C_G(W)\notin O_p(G/C_G(W))=1$. Thus $G/C_G(W)$ and W satisfy the hypothesis and we can assume $W=V, O_p(G)=1$ by induction. By Baer, $\exists b\in a^G: G_1=\langle a,b\rangle$ is not a p-group. Now (a) follows from the previous result. If G is p-separable, put $Q=O_{p'}(G)$ then $[Q,a]\neq 1$ and b can be chosen in a^Q so we get (b).

Theorem 9: Suppose G acts faithfully on V and E_1,E_2 are two subnormal subgroups of G such that $[V,E_1,E_2]=1$ then $[E_1,E_2]\leq O_p(G)$.

Proof: By hypothesis, $V_1=[V,E_1]$ is invariant under $E=\langle E_1,E_2\rangle$ so $E_0=C_E(V_1)$ and $E^0=C_E(V/V_1)$ are normal in E. $E_0\cap E^0$ acts quadratically on V and is a p-group by the earlier result. Thus $E_0\cap E^0\leq O_p(E)$. $E_1\leq E^0$ and $E_2\leq E_0$ so $[E_1,E_2]\leq[E^0,E_0]\leq E^0\cap E_0\leq O_p(E)$ so E and $O_p(E)$ are subnormal in G and hence, $O_p(E)\leq O_p(G)$.

$Q_8=\langle\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix},\begin{pmatrix} 0 & -1\\ -1 & 0\end{pmatrix}\rangle$.

16.2 Replacement Results

Observation: $A^*=C_A([V,A])$ acts quadratically on V.

Condition $\mathcal{Q}_1$: $|A||C_V(A)|\geq|A^*|C_V(A^*)|,\forall A,A^*$.

Condition $\mathcal{Q}_2$: $A/C_A(V)$ is an elementary abelian p-group.

Definition 4: $\mathcal{A}_V(G)=\{A\leq G: A \text{ satisfies } \mathcal{Q}_1 \text{ and } \mathcal{Q}_2\}$.

Theorem 10: Suppose A acts on an elementary abelian p-group, V, with $A/C_A(V)$ abelian. Let $U\leq V$. Then $\exists A^*\leq A$ such that one of the following holds: (a) $|A||C_V(A)|l|A^*||C_V(A^*)|$, or (b) $A^*=C_A([U,A]), C_V(A^*)=[U,A]C_V(A), |A||C_V(A)|=|A^*||C_V(A^*)|$.

Proof: Assume $\mathcal{Q}_1$ does not hold. $\forall B\leq A$, so $|A||C_V(A)|\geq|B||C_V(B)|$. Put $A^*=C_A([U,A])$. $[U,A,A^*]=1$ and $A/C_A(V)$ is abelian so $[A,A^*,U]=1\to[U,A^*A]=1$ so $[U,A^*]\leq C_V(A)$.

Claim: $|A||C_V(A)|\leq|A^*||[U,A]C_V(A)|$.

Assuming claim, $|A^*||C_V(A^*)| \leq |A||C_V(A)| \leq |A^*||[U,A]C_V(A)| \leq |A^*||C_V(A^*)|$ and we're done.

Proof of claim: Let $Y = C_V(A), X = [U,A]$. We can assume $|U| = p, U = \langle u \rangle$ and $[U,A] = [u,a]$. Let $\varphi : A/A^* \to (XY)/Y$ by $aA^* \mapsto [u,a]Y$ is well defined. $\forall a^* \in A^*$. $[u,a^*,a] = [u,a][u,a^*]^a \in [u,a]Y$. If φ is injective, $|A/A^*| \leq (XY)/Y|$ and the result follows. Let $a_1, a_2 \in A$ such that $[u,a_1]Y = [u,a_2]Y$. $[u,a_1][u,a_2]^{-1} \in Y$ then $[u,a_1a_2^{-1}] \in Y$ so $[u,A,A_1s_2^{-1}] = 1$ and $a_1a_2^{-1} \in C_A([U,A]) = A^*$. Thus φ is injective. Now assume $|U| > p$, $|U : U_1| = p, U = U_1\langle u \rangle$. Put $X_1 = [U_1,A]$, $A_1 = C_A(X_1)$ and $X_2 = [U_2,A]$, $A_2 = C_A(X_2)$. Note $X_1X_2C_V(A) = XC_V(A), A^* = A_1 \cap A_2$ and $X_1C_V(A) \cap X_2C_V(A) \leq C_V(A_1A_2)$. By induction on $|U|$, $|A||C_V(A)| = |A_i||X_i : C_V(A)|$. Hence, $|A||C_V(A)| \geq |A_1A_2||C_V(A_1A_2)| \geq \frac{|A_1||A_2||X_1C_V(A)||X_2C_V(A)|}{|A_1 \cap A_2||X_1C_V(A)||X_2C_V(A)|} = \frac{|A|^2|C_V(A)|^2}{|A^*||XC_V(A)|}$ and this proves the claim.

Theorem 11: $A \in \mathcal{A}_V(G)$ and $A^* = C_A([V,A])$ then $|A/A^*| = |C_V(A^*)/C_V(A)|$ and $C_V(A^*) = [V,A]C_V(A)$.

Proof: By the previous result, every quadratically acting subgroup, A, satisifes $\mathcal{Q}_2$ and the result follows from the second conclusion of that theorem, with $U = V$.

Timmesfeld Replacement Theorem: Let $A \in \mathcal{A}_V(G)$ and $U \leq V$ then $C_A([U,A]) \in \mathcal{A}_V(G)$ and $C_V(C_A([U,A])) = [U,A]C_V(A)$. Moreover, $[V, C_A(([U,A])] \neq 1$ if $[V,A] \neq 1$.

Proof: Let $A^*C_A([U,A])$. Since $A \in \mathcal{A}_V(G)$, we can apply the previous result so $|A^*||C_V(A^*)| = |A||C_V(A)|$ and $C_V(A^*) = [U,A]C_V(A)$. $\forall A_0 \leq A$, $\mathcal{Q}_1$ gives $|A_0||C_V(A_0)| \leq |A^*||C_V(A^*)|$. Hence $A^* \in \mathcal{A}_V(G)$, we may assume $[V,A^*] = 1$ then $V = [U,A]C_V(A) = [V,A]C_V(A)$. In particular, $[V,A,A] = [V,A]$ but then $[V,A] = 1$ since $A/C_A(V)$ is a p-group.

Definition 5: $\mathcal{A}_V(G)_{min} = \{A \in \mathcal{A}(G), [V,A] \neq 1\}$.

Theorem 12: Every element of $\mathcal{A}_V(G)_{min}$ acts quadratically and non-trivially on V.

Proof: Let $A \in \mathcal{A}_V(G)_{min}$. By previous result, $A^* = C_A([V,A])$ is also in $\mathcal{A}_V(G)$ and $[V,A^*] \neq 1$. Minimality forces $A = A^*$ and thus $[V,A,A] = 1$.

Theorem 13: Suppose G is p-stable on V and $O_p(G/C_G(V)) = 1$ then every element of $\mathcal{A}_V(G)_{min}$ acts trivially on V.

Proof: Follows from previous result.

Theorem 14: Let $V = \langle C_V(S), S \in S_p(G) \rangle$ then $O_p(G/C_G(V)) = 1$.

Proof: Let $S \in S_p(G)$, $Z = C_V(S), C = C_G(V)$. $V = \langle Z^G \rangle$. Let $C \leq D \leq G$: $D/C \cong O_p(G/C)$ then $D \cap S \in S_p(D)$ and $D = C(D \cap S)$ and by Frattini: $G = CN_G(D \cap S)$. So $V = \langle Z^{N_G(D \cap S)} \rangle$, so $[V, D \cap S] = 1$ and $D = C$.

Theorem 15: Let $C_G(O_p(G)) \leq O_p(G)$ then $V = \langle \Omega(\mathbb{Z}(S)), S \in S_p(G) \rangle$ is an elementary abelian normal subgroup of G and $O_p(G/C_G(V)) = 1$.

Proof: Let $S \in S_p(G)$ then $\Omega(\mathbb{Z}(S)) \leq C_G(O_p(G)) \leq O_p(G) \leq S$ so V is contained in $\Omega(\mathbb{Z}(O_p(G)))$ and $\Omega(\mathbb{Z}(S)) = C_V(S)$. Now the result follows from the previous result.

Definition 6: Let $\mathcal{E}(G)$ be the set of elementary elementary subgroups of G and m the the size of the element of $\mathcal{E}(G)$ of maximal order. $J(G) = \langle A \in \mathcal{A}(G) : |A| = m \rangle$.

Theorem 16: Let $A \in \mathcal{A}(G)$ act quadratically on V and $A_0 = [V, A]C_A([V, A])$ then A_0 is in $\mathcal{A}(G)$ and acts quadratically on V and if $[V, A] \neq 1$ then $[V, A_0] \neq 1$.

Proof: Let $X = [V, A]$ and $A^* = C_A(X)$ with $A_0 = A^*X$. A_0 is elementary abelian and $[V, A_0, A_0] \leq [V, A, A_0] = 1$. It suffices to show $|A| = |A_0|$ to establish $A_0 \in \mathcal{A}(G)$. The maximality of A gives $C_V(A) = V \cap A = V \cap A^*$ and since $X \cap A = X \cap A^*$, $|A||A \cap V| = |A||C_V(A)| = |A^*||XC_V(A)|$. and so $|A| = \frac{|A^*||XC_V(A)|}{|C_V(A)|} = \frac{|A^*|}{|X \cap C_V(A)|} = \frac{|A^*||X|}{|X \cap A^*|} = |A_0|$.

Theorem 17: (a) $\mathcal{A}(G) \subseteq \mathcal{A}_V(G)$ and (b) $V \not\leq \mathbb{Z}(J(G))$ then $\exists A \in \mathcal{A}(G) : [V, A] \neq 1$.

Proof: Let $A^* \in \mathcal{A}(G)$ then $A^*C_V(A^*) \in \mathcal{E}(G)$ so $|A| \geq |A^*C_V(A^*)| = \frac{|A^*||C_V(A^*)|}{|A^* \cap V|} \geq \frac{|A^*||C_V(A^*)|}{|C_V(A)|}$ and (a) follows. (b) is clear.

Condition $\mathcal{Q}_1'$: $|A/C_A(V)| \geq |V/C_V(A)|$.

Theorem 18: Let $\mathcal{B}$ be the set of subgroups $A \leq G$ satisfying $\mathcal{Q}_1'$ and $\mathcal{Q}_2$. Let $A \in \mathcal{B}$ and suppose that $\forall A^* \leq A, A^* \in \mathcal{B}$, $|A^*/C_{A^*}(V)||C_V(A^*)| \leq |A/C_A(V)||C_V(A)|$ then $A \in \mathcal{A}_V(G)$.

Proof: We need to verify $\mathcal{Q}_1$ for A. Let $A^* \leq A$. If A^* does not satisfy $\mathcal{Q}_1'$ then $A^* \notin \mathcal{B}$ and $|A^*/C_{A^*}(V)||C_V(A^*)| < |V| \leq |A/C_A(V)||C_V(A)|$. So $|A/C_A(V)||C_V(A)| \geq |A^*/C_{A^*}(V)||C_V(A^*)| = |(A^*/C_{A^*}(V))/C_A(V)||C_V(A^*)|$. The inequality also holds for $A^* \in \mathcal{B}$ since the inequality holds. Thus $\forall A^* \leq A$: $|A^*||C_V(A^*)| \leq |A^*C_A(V)||C_V(A^*)| \leq |A||C_V(A)|$ and A satisfies $\mathcal{Q}_1$. Assume $\exists A \in \mathcal{B}$ that act non-trivially on V. Among all such choose it with the property that $|A/C_A(V)||C_V(A)|$ is maximal. Then the inequality in the theorem holds for A. Thus $A \in \mathcal{A}_V(G)$ and $\mathcal{A}(G)_{min} \neq \emptyset$. A previous result insures the existence that act quadratically and non-trivially on V.

Theorem 19: If $\mathcal{K} \in \{N, S, \Pi\}$ then $\forall G : O_{\mathcal{K}}(G) = \langle A : A \in \mathcal{K}, A \lhd \lhd G \rangle$.

Proof: For $A \lhd G$, this is clear. May assume A is not normal in G so $\exists N \lhd G$ with $A \lhd \lhd N < G$. By induction, $A \leq O_{\mathcal{K}}(N)$. $O_{\mathcal{K}}(N) \lhd G$ and $\mathcal{K} \in \{N, S, \Pi\}$. Hence $A \leq O_{\mathcal{K}}(N) \leq O_{\mathcal{K}}(G)$ which proves the result.

16.3 Stability and $SL_2(p)$

Hall's remark on Thompson: If $P \in S_p(K)$ and $K \neq XP$ for any $X \in O_{p'}(K)$, then there is a characteristic subgroup D of P of nilpotence class at most 2 such that $N_K(D)/C_K(D)$ is not a p-group.

Definition 7: Let G be a p-constrained group with $O_{p'}(G) = 1$. G is *p-stable* if $\forall H \lhd G, H \in p(G)$, $[H, x, x] = 1 \to \overline{x} \in O_p(G/C_G(H))$.

Theorem 20: A group is p-separable iff $H < G$ has a non-trivial π-closed factor group or, equivalently G has a normal series $1 = A_0 < A_1 < \ldots < A_n = G$ of characteristic subgroups and A_i/A_{i-1} is a π or π' group.

Proof: Sort of a definition.

Theorem 21: If $p \neq 2$, $O_{p'}(G) = 1$ and G is p-constrained or p-solvable and $SL_2(p)$ is not involved in G, then G is p-stable.

Proof: Suppose $H \lhd G$ is a p-group. $G/C_G(H)$ acts on $H/\Phi(H)$. Let $K = ker(\varphi)$ where $\varphi : G/C_G(H) \to Aut(H/\Phi(H))$.

Claim: K is a p-group.
Proof of claim: It suffices to show that if $\mathbb{Z}_q < G/C_G(H)$ acts non-trivially on H, it acts non-trivially on $H/\Phi(H)$. If $\mathbb{Z}_q$ acts trivially on $H/\Phi(H)$. For each coset, $\Phi(H)x$, by counting, at least one element of the coset is fixed, say x_i. By the Burnside Basis Theorem, $\langle x_i \rangle_i = H$. Thus there is no q-element in K and $|K| = p^m$.

Put $L = G/C_G(H)/K$. L act faithfully on $H/\Phi(H)$. Since $SL_2(p)$ is not involved, K is p stable. Now let $x \in G$ with $[H, x, x] = 1$ and let the canonical map $G/C_G(H) \to L$ be denoted by $\tilde{}$. $[H, x, x] = 1 \to [H, x, x] \in \Phi(H) \to (\tilde{\tilde{x}} - 1)^2 = 0$, so $\tilde{\tilde{x}} \in O_p(G/\tilde{C_G}(H))$ we have $\tilde{\tilde{x}} \in O_p(G/C_G(H))$.

Theorem 21: Let G be a group with no non-trivial normal p-subgroup, $p \neq 2$ which satisfies one of the following: (1) G has odd order; (2) G has an abelian Sylow 2-subgroup; (3) G has a dihedral Sylow 2-subgroup; (4) $G \cong PSL_2(q) = L_2(q)$; (5) G is solvable and $p \geq 5$ or $p = 3$ and $SL_2(3)$ is not involved in G then G is p-stable.

Proof: Generalization of earlier result.

16.4 The Thompson Subgroup

Definition Let $\mathcal{E}(G)$ be the elementary abelian subgroups of G of maximal order. $J(G) = \langle \mathcal{E}(G) \rangle)$.

GL **Lemma:** Let $G = GL_2(p)$, $p \neq 2$, $P \in S_p(G)$. Suppose $L \in p'(G)$ and $P \subseteq N_G(L)$ and if $S \in S_2(G)$, $S' = 1$. Then $P \subseteq C_G(L)$.

Proof: Sublemma: If q is odd, $-I$ is the unique involution in $SL_2(q)$. Let P be a p-group with at most one group of order p. Either P is cyclic or $p = 2$ and P is generalized quaternion.
By induction on $|L|$, we can assume P centralizes every proper subgroup that it stabilizes. Choose $q \mid |L : C_L(P)|$. We can find a P invariant Sylow q subgroup $Q \subseteq L$. Since $Q \neq C_L(P)$, $Q = L$. So L is a q-group. $[L, P] \subseteq P$. If $[L, P] < L$, $[L, P, P] = 1$ and we're done. So $[L, P] = P$, $L \subseteq G' \subseteq SL_2(p)$ since $GL_2(p)/SL_2(p)$ is abelian. If $q = 2$, L is abelian and has a unique involution. L is a cyclic 2-group and so is $Aut(L)$ P cannot act non-trivially on L so $q \neq 2$. $|L| \mid (p-1)p(p+1)$ so $q \mid p-1$ or $q \mid p+1$. This $|L| \leq p+1$. If P acts non-trivially on L then there must be a p-orbit of L of size at least p. $|L| = p+1$ and $|L|$ is even but $|L|$ is a power of q. Contradiction.

Normal P-Theorem: Let $P \in S_p(G)$ and suppose (1) G is p-solvable, (2) $p \neq 2$, (3) if $R \in S_2(G)$, $R' = 1$, (4) $O_{p'}(G) = 1$, and (5) $P = C_G(\mathbb{Z}(P))$ then $P \lhd G$.

Proof: Suppose G is a minimal counter-example. $\exists Q \in S_p(G), P \neq Q : \langle P, Q \rangle G$. $Q = P^g$ and $C_V(Q) = C_V(P)^g$. Put $U = C_V(Q) \cap C_V(P)$. $|V : U| \leq |V : C_V(P)||V : C_V(Q)| = p^2$ and $U \lhd V$. G acts trivially on U: $[U, G] = 1$. G acts on V/U; let K be the kernel of this map. $[V, U] \subseteq U$ and $[V, K, K] = 1$ so K is a p-group. Note $K \subseteq O_p(G)$ so $K \subseteq P$ and $K \subseteq Q$. $\overline{G} = G/K$ has Sylow subgroups $\overline{P}, \overline{Q}$ and $\overline{G}$ acts faithfully on V/U so $[\overline{P}, C_V(P)/U] = 1$. $\overline{G}$ satisfies all the hypothesis of the theorem so $K = 1$ and G acts faithfully on V/U. Replace V by V/U. $|V| \leq p^2$. $G \to Aut(V)$. If V is cyclic, $Aut(V)$ is abelian and so is G therefore $P \lhd G$. So V is elementary

abelian and $Aut(V) = GL_2(p)$ and $O_p(G) = 1$ since $|P| \leq p$ and P is not normal. Let $L = O_{p'}(G)$ and apply the previous lemma. $[P, L] = 1$ so by Hall-Higman, $P \subseteq C_G(L) \subseteq L$ and $P = 1$.

Normal J-Theorem: Let $P \in S_p(G)$ and suppose (1) G is p-solvable, (2) $p \neq 2$, (3) if $R \in S_2(G)$, $R' = 1$, (4) G acts faithfully on some p-group, V and (5) $|V : C_P(V)| \leq p$, then $J(P) \lhd G$.

Proof: Let G be a minimal counterexample. $U = O_p(G) > 1$, $\overline{G} = G/U$, $\overline{L} = O_{p'}(\overline{G})$, where $U \subseteq L$.

Step 1: (a) $\mathbb{Z}(P) \subseteq U$, (b) $U \subseteq H \subseteq G$ implies $O_{p'}(H) = 1$ and (c) $C_{\overline{G}}(\overline{L}) \subseteq \overline{L}$.
Proof: Since G is p-solvable and $O_{p'}(G) = 1$, by 1.2.3, $C_G(U) \subseteq O_p(G) = U$ but $U \subseteq P$ so $\mathbb{Z}(P) \subseteq C_G(U)$, proving (a). Since $U = O_p(G)$ and $O_p(\overline{G}) = 1$, so $C_{\overline{G}}(\overline{L}) \subseteq \overline{L}$ by 1.2.3, proving (c). For (b), let $U \subseteq H \subseteq G$, and put $M = O_{p'}(H)$. $M, U \lhd H$. $M \cap U = 1$, since U is a p-group and M is a p'-group, so $M \subseteq C_G(U) \subseteq U$ and thus $O_{p'}(H) = 1$ and $M = M \cap U = 1$ proving (b).

Step 2: $\exists A \in \mathcal{E}(P) : A \not\subseteq U$.
Proof: If not, all members of $\mathcal{E}(P)$ are contained in U and so $J(P) \subseteq U$. By the GL Lemma, $J(U) = J(P)$ is characteristic in U and since $U \lhd G$, $J(P) \lhd G$, which contradicts the fact that G is a counterexample.

Step 3: Let $UA \subseteq H \subset G$ and $H \cap P \in S_p(H)$ then $\overline{A}$ centralizes $\overline{H \cap L}$.
Proof: H satisfies the first four hypothesis of the theorem. A Sylow 2-group of H is abelian so it meets condition (3). $O_{p'}(H) = 1$ by 1(b). Put $S = H \cap P \in S_p(H)$. Since $\mathbb{Z}(P) \subseteq U \subseteq S \subseteq P$ by 1(a). $\mathbb{Z}(P) \subseteq \mathbb{Z}(S)$ and thus $C_H(\mathbb{Z}(S)) \subseteq C_G(\mathbb{Z}(P)) = P$. So $C_H(\mathbb{Z}(S)) = S$ is a p-group of H containing the Sylow p group S. So $C_H(\mathbb{Z}(S)) = S$ and H satisfies the fifth hypothesis. Since $H < G$, the theorem holds for H and so $J(S) \lhd H$. Since $A \in \mathcal{E}(P)$ and $A \subseteq S \subseteq P$ and $A \in \mathcal{E}(S)$ so $A \subseteq J(S)$. Thus $[H \cap L, A] \subseteq [H \cap L, J(S)] \subseteq (H \cap L) \cap J(S) = L \cap J(S) \subseteq U$ (Reason: $H \cap L$ and $J(S)$ are normal in H and U is the unique Sylow p-subgroup of L). $1 = [\overline{H \cap L}, \overline{A}]$.

Step 4: $G = LA$, $P = UA$.
Proof: $H = LA$ and $UA \in p(H)$. Further, $|H : UA| = |L(UA) : UA| = |L : L \cap UA|$ which divides the p'-number $|L : Y|$. So, $UA \in S_p(H)$, $UA = H \cap P$. If $H < G$ then since $L \subseteq H$, step 3 gives $\overline{A} \subseteq C_{\overline{G}}(\overline{L}) \subseteq \overline{L}$ (by step 1(c)). Since $\overline{A}$ is a p-group and $\overline{L}$ is a p'-group, $\overline{A} = 1$ and $A \subseteq U$. This contradicts the choice of A so $H = G$. Finally, $UA = H \cap P = G \cap P = P$.

Proof: Put $H = LA$, $UA \in p(H)$. $|H : UA| = |LUA : UA| = |L : L \cap UA|$ so $UA \in S_p(H)$ and $UA = H \cap P$. so $UA \in S_p(H)$. If $H \subseteq G$, since $L \subseteq H$, step 3 gives $\overline{A} \subseteq C_{\overline{G}}(\overline{L}) \subseteq \overline{L}$. Since A is a p-group and $\overline{L}$ is a p'-group, $\overline{A} = 1$ and $A \subseteq U$. This contradicts the choice of A so $H = G$. Finally, $UA = H \cap P = G \cap P = P$.

Step 5: $|\overline{A}| = p$.
Proof: $\overline{A} \neq 1$ since $A \not\subseteq U$. $\overline{A}$ is elementary abelian, it STS $\overline{A}$ is cyclic. $\overline{A}$ acts coprimely on $\overline{L}$ and the action is faithful since $C_{\overline{L}}(\overline{L}) \subseteq \overline{L}$ and $\overline{L} \cap \overline{A} = 1$. A previous result shows $\overline{A}$ is cyclic so STS $\overline{A}$ acts trivially on every $\overline{A}$-invariant proper subgroup of $\overline{L}$. Suppose $\overline{M}$ is $\overline{A}$-invariant, $\overline{M} < \overline{L}$, we can assume $U \subseteq M$. $A \subseteq N_G(M)$ so MA is a group $P = UA \subseteq MA$. Since A is a p-group, the p' part of $|MA|$ is equal to the p' part of $|M|$ which is less than the p'-part of $|L|$ since the p' part of$|L : M| > 1$. It follows $MA < G$. Apply step 3 to show $\overline{A}$ centralizes $\overline{MA \cap L} \supseteq M$, proving 5.

Step 6: Let $V = \{z : z \in \mathbb{Z}(U) | z^p = 1\}$. V is an elementary abelian normal subgroup of G so G acts by conjugation on V. Since $V \subseteq \mathbb{Z}(U)$, the action by U is trivial, so $\overline{G} = G/U$ on V. Now we prove: The action of $\overline{G}$ on V is faithful.
Proof: Let $K = C_G(V)$ so $\overline{K}$ is the kernel of the action of $\overline{G}$ on V. We argue K is a p-group. Let $Q \in S_q(K)$, $q \neq p$. Q acts coprimely on $\mathbb{Z}(U)$, so and Q fixes all elements of order p in $\mathbb{Z}(U)$, these make up V. $Q \subseteq K = C_G(V)$. By Fitting, Q acts trivially on $\mathbb{Z}(U)$ but $\mathbb{Z}(P) \subseteq U$ so $\mathbb{Z}(P) \subseteq \mathbb{Z}(U)$ and so $Q \subseteq C_G(\mathbb{Z}(P)) = P$. Thus $Q = 1$ and K is a p-group, as claimed. But $K \lhd G$. So $K \subseteq O_p(G) = U$ and $\overline{K} = 1$ as needed.

Step 7: $|V : V \cap A| \leq p$.
Proof: Put $D = U \cap A$ and $E = V \cap A$. $|V : E| = |V : V \cap D| = |VD : D|$. D is an elementary abelian subgroup of U and V is a central elementary abelian subgroup of U and so VD is elementary abelian. Since $\mathcal{E}(P)$, $|VD| \leq |A|$ and so $|VD : D| \leq |A : D| = |\overline{A}| = p$. We get $|V : E| = |VD : D| \leq p$ as required.

Step 8: Contradiction.
Proof: We apply the Normal-P theorem to the action of $\overline{G}$ on V. $|V : V \cap A| \leq p$. Now, $P = UA$ so $\overline{P} = \overline{A}$. $[\overline{A}, V \cap A] = 1$ since $A' = 1$. So $|V : C_V(\overline{P})| \leq |V : V \cap A| \leq p$. Now we can apply the Normal P theorem, $\overline{P} \lhd \overline{G}$ so $P \lhd G$ and $A \subseteq P \subseteq O_p(G) = U$, which is not the case.

Theorem 22: (1) $J(G)$ *char* G and $J(G) > 1$ if $p \in \pi(G)$; (2) If $J(G) \leq U \leq G$ then $J(G) = J(U)$; (3) $J(G) = \langle J(S) : S \in S_p(G) \rangle$; (4) If $x \in C_G(J(G))$ and $|x| = p$, then $x \in \mathbb{Z}(J(G))$. (5) If $\mathcal{B} \subseteq \mathcal{A}(G)$ then $J(\langle \mathcal{B} \rangle) = \langle \mathcal{B} \rangle$.

Proof: This is straightforward.

Definition 8: G is Thompson factorizable with respect to p if $G = O_{p'}(G) C_G(\Omega(Z(S))) N_G(J(S))$. Note that G is Thompson factorizable iff $G/O_{p'}(G)$ is.

Thompson Factorization: Let $O_{p'}(G) = 1$ and $V = \langle \Omega(\mathbb{Z}(S)) : S \in S_p(G) \rangle$. Then G is Thompson factorizable iff $J(G) \leq C_G(V)$.

Proof: Let $S \in S_p(G)$ and $C = C_G(V)$. Assume that G is Thompson factorizable. $\Omega(\mathbb{Z}(S)) \leq \mathbb{Z}(J(S))$ and so $V \leq \mathbb{Z}(J(S))$ and $C \leq J(G)$. Assume $C \leq J(G)$. The $J(G) \leq C \cap S$. Since $J(S)$ *char* $C \cap S \in S_p(C)$ and $\Omega(\mathbb{Z}(S)) \leq \mathbb{Z}(J(S))$, Frattini yields $G = CN_G(C \cap S) = C_G(\Omega(Z(S)))N_G(J(S))$.

Alternate Thompson subgroup: P a p-group and set $d(P) = sup\{|A| : A \leq P, A' = 1\}$. Let $\mathcal{A}(P) = \{A : |A| = d(P), A' = 1\}$ then $J(P) = \langle A : A \in \mathcal{A}(P) \rangle$.

Lemma: (1) $A \in \mathcal{A}(P) \rightarrow A = C_P(A)$; (2) $C_P(J(P)) = \mathbb{Z}(J(P)) = \bigcap_{A \in \mathcal{A}(P)} A$; (3) $H \leq P$ and $d(H) = d(P) \rightarrow J(H) \leq J(P)$ and $\mathbb{Z}(J(H)) \leq \mathbb{Z}(J(P))$; (4) Suppose $J(P) \subseteq H \subseteq P$ then $J(H) = J(P)$.

Proof: If x centralizes A, $\langle x, A \rangle$ is abelian but then $|\langle x, A \rangle| > |A|$ so $x \in A$; this proves (1). $C_P(J(P)) = \bigcap_{A \in \mathcal{A}(P)} C_P(A)$ since $\langle A \rangle = J(P)$. Thus $C_P(J(P)) = \bigcap_{A \in \mathcal{A}(P)} A \subseteq J(P)$ so $C_P(J(P)) = \mathbb{Z}(J(P))$; this proves (2). (3) and (4) are clear.

Theorem 23: Suppose $O_{p'}(G) = 1$, G is p-stable and $P \in S_p(G)$. If $H \in \mathcal{SCN}(P)$ then $H \subseteq O_p(G)$.

Proof: Put $L = O_p(G)$. Since $L \leq P$, $[L, H] \subseteq H$ and so $[L, H, H] = 1$ so $x \in H \rightarrow [L, x, x] = 1$ and thus $H/C_G(L) \subseteq O_p(G/C_G(L)$. Since L is p-constrained, $C_G(L) \subseteq L$ and thus $H \subseteq L$.

16.5 Glauberman's $Z(J)$ Theorem:

Glauberman Replacement Lemma: If $p \neq 2$, P, a p-group, $B \lhd P$, $A \subseteq P$, $A' = 1$, $B \not\subseteq N_P(A)$ and $A \cap B \supseteq B'$ then $\exists A^* \subseteq P, (A^*)' = 1$ with (1) $A^* \cap B > A \cap B$; (2) $|A^*| = |A|$; (3) $A^* \subseteq N_P(A) \rightarrow [A^*, A, A] = 1$.

Outline of proof: (1) Reduce to $P = AB$, $N_P(A) \lhd P$; (2) $x \in B - N \neq \emptyset, A \cap B \subseteq A \cap A^x$; (3) $u = AA*$, $V = A \cap A^*, W = U \cap B$; (4) $[x, A]$ is abelian; (5) VW is abelian; (6) VW works.

Proof: Proof is by induction $|P|$. If $|P| > |AB|$, we are done by induction, so $P = AB$. Suppose $N = N_P(A)$, $\exists M$ such that $N \leq M \lhd P$ since the maximal subgroups of P are normal. Let $B_1 = B \cap M$ then by Dedekind, $AB_1 = M$ and $B_i \not\subseteq N_M(A)$. Applying induction, we find an A^* such that A^* satisfies (1), (2) and (3) in AB_1. This A^* works in $P = AB$. So we may assume, $N \lhd P$.
Claim: $x \in B - N \rightarrow A \cap B \subseteq A \cap A^x$ and $A^x \leq N$. Proof of claim: $A \cap B \supseteq B' \rightarrow A \cap B \lhd B \rightarrow A \cap B = (A \cap B)^x \rightarrow A \cap B \subseteq A^x \cap B \rightarrow A \cap B \subseteq A \cap A^x$. Now, $A < N$ so $A^x < N^x = N$ by the above and this proves the claim.

Let $U = AA^x < N$, $V = A \cap A^x$, $W = U \cap B$. $A^x \subseteq N_P(A)$ so U is a group and $Z \lhd U$.
Claim: $U' \subseteq V \subseteq \mathbb{Z}(U)$ and $W = [x, A](A \cap B)$. Proof of claim: $A^x \subseteq N, A \subseteq N$ so $A^x A \subseteq N$ and $A^x A, A^x A] \subseteq A \cap A^x$, which proves the claim.
Continuing, $A \cap B \subseteq U \cap B$ and $[x, a] = (a^{-1})^x a \in U$ and $[x, a] = x^{-1}x^a \in B$ so $[x, A](a \cap B) \subseteq W$.
If $y = a_1 a_2^x \in W$, $a_1, a_2 \in A \rightarrow a_1 a_2 [a_2, x] = a_1 a_2^x \in B$ so $a_1 a_2 \in B$ and $y \in [x, A](A \cap B)$.

Major claim: $[x, A]$ is abelian.
Subclaim: U has nilpotence class ≤ 2 ($U' \subseteq \mathbb{Z}(U)$) implies $[ac, b][a, b][c, b]$. This is a calculation.
Let $a, a_1 \in A$. $[x, a, a_1] = [[x, [x, a]^{-1}[x, a], a_1^x]$ but since $[x, a] \in B$, $[x, [x, a]^{-1}] \in B \subseteq A \cap B \subseteq \mathbb{Z}(U)$, $[x, a, a_1]^x = [[x, a], a_1^x]$ by the subclaim. Now, $[[x, a], a_1^x] = [a, a_1^x] = [x, a_1, a]$. So $\forall a, a_1 \in A : [x, a, a_1]^x = [x, a_1, a] \rightarrow [x, a, a_1]^{x^2} = [x, a, a_1]$ (Equation **). Since x has odd order, this becomes $[[x, a], a_1^x] = [x, a, a_1][[x, a], [a_1, x]]$. So $[[x, a], [a_1, x]] = 1$; these two generators of $[x, A]$ commute so $[x, A]$ is abelian.

Claim: VW is abelian: $[x, A] \subseteq U$ is abelian and $A \cap B \subseteq \mathbb{Z}(U)$, so $W = [x, A](A \cap B)$ is abelian. Finally, $V \subseteq \mathbb{Z}(U)$, so VW is abelian.
$A^* = VW$ satisfies the theorem:
(1) $[x, A] \not\subseteq A$ since $x \notin N_P(A)$. $A \cap B < W < B$ so $A^* \cap B > A \cap B$.
(2) $|A^*| = \frac{|V||W|}{|V \cap W|} = \frac{|A \cap A^x||U \cap B|}{|U \cap B \cap A \cap A^x|} = \frac{|A \cap A^x||U \cap B|}{|A \cap B|}$. $|P| = |AB| = \frac{|A||B|}{|A \cap B|} = \frac{|U||B|}{|U \cap B|}$. So $\frac{|U|}{|A|} = \frac{|U \cap B|}{|A \cap B|}$ and $|A^*| = \frac{|A \cap A^x||U|}{|A|}$. $|A^*| = \frac{|A \cap A^x||AA^x|}{|A|} = \frac{|A||A^x|}{|A|} = |A|$.
(3) $A^* \subseteq U$ since $V, W \subseteq U$ and $U \subseteq N$ since $A, A^x \subseteq N$.

Glauberman's $Z(J)$ Theorem: Assume $p \neq 2$ is prime and that G is a p-stable, p-constrained group with $O_{p'}(G) = 1$ and $P \in S_p(G)$ then $\mathbb{Z}(J(P)) \lhd G$.

Proof: Let $Z = \mathbb{Z}(J(P))$ and $H = O_p(G)$. $J(P)$ *char*; P and Z *char* P so $Z \subseteq H$. Let H_0 be a minimal normal p-subgroup of G such that $Z \cap H_0$ is not normal in G. Put $Z_0 = H_0 \cap Z$ and let $K/C_G(H_0) = O_p(G/C_G(H_0))$ so $K \lhd G$. Also put $P_0 = P \cap K \in S_p(K)$.

(1) $K = P_0 C_G(H_0)$. Reason: Since $K/C_G(H_0)$ is a p-group and $P_0 C_G(H_0) \subseteq K$, $K \neq P_0 C_G(H_0)$ implies that $|K/C_G(H_0)| \geq p|(P_0 C_G(H_0))/C_G(H_0) = p\frac{|P_0|}{|P_0 \cap C_G(H_0)|}$. Thus $|P_0| \mid p \cdot |K|$ which

contradicts the fact that $P_0 \in S_p(K)$.
(2) By Frattini, $G = KN_G(P_0)$.
(3) $J(P) \not\subseteq P_0$. Reason: If not, $J(P) < J(P_0) \lhd N_G(P_0)$ so $Z_0 \lhd G$, a contradicton.
(4) $H_0' \subseteq Z_0$. Proof: Since H_0 is a p-group $H_0' < H_0$ so by maximality, $Z \cap H_0' \lhd G$ and $H_0 = \langle Z_0^g \rangle$. $[Z_0, H_0] \subseteq Z_0 \cap H_0' \lhd G$, so $[Z_0, H_0]^g = [H_0, H_0] \subseteq Z_0 H_0'$ and $H_0' \subseteq Z_0 \cap H_0'$.
(5) $H_0 \not\subseteq N_G(A)$ otherwise, $[H_0, A] \subseteq A$ and $[H, A, A] = 1$ which implies $A \subseteq K$ by p-stability.
(6) $H_0 \subseteq \mathbb{Z}(J(P_0))$.

Conclusion: By (1) and (2), $G = N_G(P_0)C_G(H_0)$ so $Z_0^g = Z_0^n, n \in N_G(P_0)$ and $H_0 = \langle Z_0^g \rangle \subseteq \mathbb{Z}(J(P_0)), \forall g \in G$. Therefore $H_0 \subseteq A^*$ and $A^* \subseteq N_G(A)$ so $H_0 \subseteq N_G(A)$ which is a contradiction.

16.6 Alperin-Lyons Proof of Baer

Theorem 24: Suppose x is a p-element of G. $x \in O_p(G)$ iff $\langle x, x^g \rangle$ is a p-group $\forall g \in G$.

Proof: Let $K = \langle x^G \rangle$ and suppose $z, y \in K \to \langle z, y \rangle$ is a p-group. Suppose $K \not\subseteq O_p(G)$.

(1) $\exists P, Q \in S_p(G) : P \cap K \neq Q \cap K$. Reason: If $K \subset R, \forall R \in S_p(G)$ then $K \subseteq \bigcap R^g \lhd G$ so $K \subseteq O_p(G)$.

(2) $|P \cap K| = |Q \cap K|$. Reason: $Q = P^g$ so $Q \cap K = P^g \cap K^g = (P \cap K)^g$ so $|Q \cap K| = |P \cap K|$.

(3) $K \cap P \not\subseteq Q$ and $K \cap Q \not\subseteq P$ for P, Q chosen such that $P \cap K \neq Q \cap K$. If $K \cap P \subseteq Q$, $K \cap P \subseteq K \cap Q$ if since the cardinalities are the same, $K \cap P = K \cap Q$.

(4) We can choose P and Q such that $|K \cap P \cap Q|$ is maximal with respect to $K \cap P \neq K \cap Q$. Put $W = P_0 < P_1 < \ldots < P_n = p$ with $|P_i : P_{i-1}| = p$. Now $P \cap K \not\subseteq W$ (otherwise $\langle P \cap K \rangle \subset P \cap Q$ so $P \cap K \subset Q$ which is a contradiction). Let j be the smallest j such that $P_j \cap K \not\subseteq W \cap K$ ($j \geq 1$). Pick $x \in K \cap P_j - W$.

(5) Claim: $x \in N(W)$. Proof of claim: x normalizes P_{j-1} so $P_{j-1} \cap K$ is normalized by x. By the choice of j, $P_{j-1} \cap K \subseteq W \cap K$ so $P_{j-1} \cap K = W \cap K$. Thus $W = \langle P_{j-1} \cap K \rangle = P_{j-1} \cap K \rangle^x = W^x$ which proves the claim.
For the same reason, $\exists y \notin W : y \in K, y \in N(W)$ and $\langle x, y \rangle$ is a p-group. Thus if $R \in S_p(G)$ with $\langle x, y \rangle W \subset R$, $K \cap P \cap R \supseteq K \cap W \cap \langle x \rangle$ and $|K \cap P \cap R| > |K \cap P \cap Q|$ and symmetrically, $|K \cap Q \cap R| > |K \cap P \cap Q|$ thus $P \cap K = R \cap K = K \cap Q$ concluding the proof.

16.7 Goldschmidt's Proof of Burnside's Theorem for $p \neq 2$

Burnside's Theorem: If $|G| = p^a q^b$ for $p \neq 2 \neq q$ then G is solvable.

Proof: Let G be a minimal counterexample, $r \in \{p, q\}$.

Lemma 1: If $R \in S_r(G)$ then if $1 \neq S \in r'(G)$, $R \not\subseteq N_G(S)$.
Proof: Let $Q \in S_{r'}(G)$ with $S \subseteq Q$. Since $G = RQ$, $\forall g, Q^g = Q^r$ for some $r \in R$. Now suppose $R \subseteq N_G(S)$ then $S \subseteq Q^r$ and thus $1 \neq \bigcap_{r \in R} Q^r = \bigcap_{g \in G} Q^g \lhd G$ which is impossible since G is simple.

Lemma 2: If M is a maximal subgroup of G then $F(M)$ is an r-group.
Proof: From now on, let $F = F(M) = F_p \times F_q$, and $Z = \mathbb{Z}(F) = Z_p \times Z_q$. Observe that if M is maximal, M is solvable and so $O_{p'}(N_M(P)) \subseteq O_{p'}(M)$.

Claim 1: F is not cyclic.
Assume, by way of contradiction, that F is cyclic. Suppose $q > p$ and $Q \in S_q(M)$. Since Q acts on F_p and $q \nmid Aut(F_p)$, $[Q, F_p] = 1$. Q also acts on F_q and $Q/C_Q(F) \to Aut(F_q)$. $C_M(F) \subseteq F$, since M is solvable so $C_M(F) \subseteq F$ and $C_Q(F) \subseteq F_q$. Clearly, $F_q \subseteq C_Q(F)$ since F_q is cyclic. So $Q/F_q \subseteq Aut(F_q)$. Further, $F_q \, char \, Q$ and $N_G(Q) \subseteq N_G(F_q)$. $N_G(Q) \subseteq N_G(F_q) = M$. Examining $N_M(F_q)/C_M(F_q) \subseteq Aut(F_q)$, we see $|N_M(F_q)|_q = |Q|$ so $|N_M(F_q)|_q = |N_G(F_q)|_q$. Thus, $Q \in S_q(G)$, contradicting Lemma 1.

Claim 2: M is the unique maximal subgroup containing Z.
Suppose $Z \subseteq M_1 \neq M$. M_1 a maximal subgroup of G. $M = N_G(Z_p) = N_G(Z_q)$, $Z_p \subseteq O_{q'}(N_{M_1}(Z_q))$ and $Z_q \subseteq O_{p'}(N_{M_1}(Z_p))$. Because M, is solvable, $O_{p'}(N_M(F)) \subseteq O_{p'}(M)$, $Z_p \subseteq F(M_1)_p \subseteq C(Z_q) \subseteq M$ and $Z_q \subseteq F(M_1)_q \subseteq C(Z_p) \subseteq M$ so $F(M_1) \subseteq F(M)$. Since the argument also applies to M_1, $F(M) \subseteq F(M_1)$. So $F(M) = F(M_1)$. This $M = N_G(F(M)) = M_1$, proving the claim.

Now, since F is not cyclic, there is an Abelian subgroup $V \subseteq F$ of type (r, r). $\forall x \in V^{\#}$, $Z \subseteq C(x)$ and by the uniqueness of M, $C(x) \subseteq M$. Let $V \subseteq R \in S_r(M)$. If $Q_0 \in r'(G)$ with $R \subseteq N(Q_0)$. $Q_0 = \prod_{x \in V^{\#}} C_{Q_0}(x) \subseteq M$. It follows that $F_{r'}$ is the unique maximal r'-subgroup of G normalized by R, so $N(R) \subseteq N(F_{r'}) = M$ so $R \in S_r(G)$, contradicting Lemma 1. This proves Lemma 2.

Lemma 3: If $R \in S_r(G)$ then R is contained in a unique maximal subgroup of G. Every maximal subgroup, $M \subseteq G$, contains a Sylow subgroup of G.
Proof: $R \subseteq M$ so $O_{p'}(M) = 1$ by lemma 1. Since M is r-constrained, $O_{r'}(M) = 1$ and M is solvable, M is r-constrained. Once we know M is r-stable, by Glauberman's $Z(J)$ theorem, we have: $M = N_G(\mathbb{Z}(J(R)))$. $p^a q^b$ is odd and $|SL_2(r)| = (r^2-1)r$ which is even, so G is p-stable and $M = N_G(\mathbb{Z}(J(R)))$. So M is unique. Let M_1 be any maximal subgroup of G, we can choose r, such that $O_{r'}(M_1) = 1$. If $R_1 \in S_r(M)$, we have $M_1 = N_G(\mathbb{Z}(J(R_1)))$. Since $\mathbb{Z}(J(R_1))$ *char* R_1, $N_G(R_1) \subseteq M_1$, so $R_1 \in S_r(G)$,proving the second statement.

Lemma 4: If $R \in S_r(G)$ then $\mathbb{Z}(R)$ is contained in a unique maximal subgroup of G.
Proof: Suppose $\mathbb{Z}(R) \subseteq M \cap M_1, M \neq M_1$ with M, M_1 maximal in G. We may assume M_1 is chosen such that $|M \cap M_1|_r$ is maximal. Now, let $R_1 \in S_r(M \cap M_1)$ such that $\mathbb{Z}(R) \subseteq R_1$. By the maximality of $|M \cap M_1|_r$, $N_G(R_1) \subseteq M$ and $R_1 \in S_r(M_1)$ Conjugating R by something in M, we may assume, by lemma 1, $R_1 \subset R$ and M_1 contains a r' sylow subgroup of G. Thus $G = RM_1$ and $1 \neq \mathbb{Z}(R) \subseteq \bigcap_{r \in R} M_1^r = \bigcap_{g \in G} M_1^g \lhd G$, a contradiction.

Lemma 5: $\exists R_1, R_2 \in S_r(G)$ such that $R_1 \cap R_2 = 1$.
Proof: Let $R_1 \in S_r(G)$ and let M be a unique maximal subgroup containing R_1. Pick $R_2 \nsubseteq M$. We can do this since G is simple.

Claim: $R_2 \cap M = 1$.
If not, choose R_2 such that $|R_2 \cap M|$ is as large as possible. Put $R_0 = (R_2 \cap M)$. We can assume, possibly after conjugation in M, $R_0 \subseteq R_1$. $\mathbb{Z}(R_1) \subseteq N(R_0)$. By lemma 4, $N(R_0) \subseteq M$. $R_0 < R_2$ so $N_{R_2}(R_0) > R_0$ and $|R_2 \cap M| > |R_0|$, which is a contradiction. So $R_2 \cap M = 1$.

Conclusion: WLOG, assume $q^b > p^a$ and let $Q_1, Q_2 \in S_q(G)$ with $Q_1 \cap Q_2 = 1$. Then $|G| \geq |Q_1| \cdot |Q_2| > |G|$ which is just plain wrong.

16.8 Thompson Complements

Thompson Normal $p-$Complement: Let $p \neq 2$ and $P \in S_p(G)$. Assume $N_G(J(P))$ and $C_G(\Omega_1(\mathbb{Z}(P)))$ have a normal $p-$complement then so does G.

Proof: Let G be a counterexample of minimum order.

Step 1: Let $\mathcal{H} = \{H \in p(G) : N(H)$ does not have a normal p-complement $\}$. If $H, K \in \mathcal{H}$. We say $H \leq K$ if one of the following holds: (1) $|N(H)|_p < |N(K)|_p$; (2) $|N(H)|_p = |N(K)|_p$ and $|H| < |K|$; or, (3) $|H| = |K|$. Choose H minimal with respect to the ordering and set $N = N(H)$. Let $Q \in S_p(N)$ and $H \subseteq Q \subseteq P$.

Step 2: $H \neq P$
If $H = P$, $N \subseteq N(J(P))$ which is a contradiction.

Step 3: $\overline{N} = N/H$ has a normal p-complement.
Let $\overline{Q} = P/H$ and $\overline{Q} \in S_p(\overline{N})$. Suppose $\overline{N}$ does not have a normal p-complement. Since $|\overline{N}| < |\overline{G}|$, either $C_{\overline{N}}(\mathbb{Z}(\overline{P}))$ or $N_{\overline{N}}(J(\overline{Q}))$ does not have a normal p-complement. Let K be the inverse image of the one that fails to have a normal p-complement. $K \in p(G)$ and $N(K)$ has no normal p-complement. Since $Q \subseteq N(K)$, either $|N(K)|_p > |N(H)|_p$ or $|N(K)|_p = |N(H)|_p$ and $|H| < |K|$. Hence, $K \geq\geq K$. But $K \neq H$ and this contradicts maximality of H in $\mathcal{H}$.

Step 4: $N = G$.
N satisfies the hypothesis of the theorem $H \subseteq Q \subseteq P$ so $\mathbb{Z}(P) \subseteq N(H) = N$. $Q\mathbb{Z}(P) \subseteq N \cap P$ so $Q\mathbb{Z}(Q) = Q$ and $\mathbb{Z}(P) \subseteq Q$ thus $\mathbb{Z}(P) \subseteq \mathbb{Z}(Q)$ and $C_N(\mathbb{Z}(Q)) \subseteq C_G(\mathbb{Z}(Q)) \subseteq C_G(\mathbb{Z}(P))$. If $P = Q$, $N(J(Q)) \subseteq N(J(P))$ has a normal p-complement. Suppose $Q < P$ so $N_P(Q) > Q$ and $|N_G(J(Q))|_p > |N|_p = |N_G(H)|_p$. By the maximality of H in $\mathcal{H}$, $J(Q) \notin \mathcal{H}$ and so $N(J(Q))$ has a normal p-complement and so does $N_N(J(Q))$. If $N \neq G$, then by the minimality of $|G|$, N has a normal p-complement and so $N = G$.

Step 5: $O_{p'}(G) = 1$.
Let $J = O_{p'}(G)$ and $\overline{X} = X/L$. If $K \subset P$, $\overline{N(K)} = N(\overline{K})$, $\overline{J(P)} = J(\overline{P})$, $\overline{C(P)} = C(\overline{P})$, and $\overline{\mathbb{Z}(P)} = \mathbb{Z}(\overline{P})$. So $N(\mathbb{Z}(P))$ has a normal p-complement. If $|\overline{G}| < |G|$, $\overline{G}$ and the inverse image is a normal p-complement of G.

Step 6: $H = O_p(G)$ and G is p-solvable of p-length at most 2.
Set $K = O_p(G), K \subseteq H$. Since G has no a normal p-complement, $N(K) = G$ and $K \in \mathcal{H}$, by steps 3, 4, G/H has a normal p-complement so G has p-length ≤ 2.

Step 7: If $\overline{G} = G/H = \overline{PM}$ where $\overline{M}$ is a normal p-complement and $\overline{M}$ contains no P-invariant subgroup.
Suppose $\overline{M} > \overline{M}_0 > 1$ and $\overline{M}_0$ is P-invariant. Let M_0 be the inverse image and set $G_0 = PM_0$. $G_0 < G$ so G_0 has a normal p-complement and $K_0 \lhd G_0, K_0 \cap P = 1$. $[H, K_0] \subseteq K_0 \cap H = 1$ so $K_0 \subseteq C(H)$. But then $K_0 \subseteq \mathbb{Z}(O_p(G))$ by Hall-Higman which is a contradiction.

Step 8: $\overline{M} = \overline{R}$ is an elementary abelian r-group for some $r \neq p$ and P acts irreducibly on $\overline{R}$. Hence, P is maximal in G.
Let $r \mid |\overline{M}|$. P permutes Sylow r-subgroups and by Sylow, the conjugacy class has size 1. So $\overline{R} \in S_r(\overline{M})$ is P-invariant and since $\overline{R}$ has no non-trivial characteristic subgroups, it is elementary abelian. Since $\overline{M}$ has no proper $\overline{P}$ invariant subgroups, $\overline{P}$ acts irreducibly. If $G > L > P$, $1 \leq \overline{L} \cap \overline{R} < \overline{R}$ and $\overline{L} < \overline{R}$ is a proper $\overline{P}$-invariant subgroup of $\overline{R}$ which is a contradiction.

Step 9: $\exists 1 \neq A \in P$ with A abelian such that $m_p(A) = d(P)$ and $A \not\subseteq H$.
Let A be a fixed one of minimal order. If $A_0 = A \cap H$, A/A_0 is elementary abelian. If $J(P) \subseteq H$ then $J(P)$ *char* H and $J(P) \lhd G$ which is a contradiction. So $J(P) \not\subseteq H$ and such an A exists. Choose A as mentioned and set $A_0 = A \cap H$, $A_1 = \Omega_1(A/A_0)$, $A_1 \not\subseteq H$ and $m(A) = m(A_1)$ so $A = A_1$ and A/A_0 is elementary abelian.

Step 10: Let $\overline{A} = (AH)/H$ then $\overline{G} = \overline{AQ}$ and $|\overline{A}| = p$.
$\overline{G} = \overline{PR}$ and $\overline{P}$ normalizes $\overline{R}$. The action is faithful since $H = O_p(G)$ and the kernel would be a normal p-subgroup of G. Note $\overline{A} = (AH)/H \cong A/A_0 \neq 1$. $\overline{A}$ acts nontrivially on $\overline{R}$ by the previous result an we can find $\overline{R}_1 \subseteq \overline{R}$ on which $\overline{A}$ acts non-trivially and irreducibly. Let G_1 be the inverse image of $\overline{AR}$ and $P_1 \in S_p(G_1)$. $A \subseteq P_1 \subseteq P$. Since $H \subseteq P_1$ and $C_G(H) \subseteq H$, $\mathbb{Z}(P) \subseteq C_G(H) \subseteq H \subseteq P$, and $\mathbb{Z}(P) \subseteq \mathbb{Z}(P_1)$ and the latter has a normal p-complement. Since $A \subseteq P_1$ and $m(A) = d(P)$, $d(P_1) = d(P)$ and $A \subseteq J(P_1)$. Let $R_1 \in S_r(N_G(J(P_1)))$, then $[A, R_1] = [J(P_1), Q_2] \subseteq J(P_1)$ so $[A, R_1]$ is a p group. Since $\overline{R}_2 \subseteq \overline{R}_1$, $[A, \overline{R}_2] \subseteq \overline{R}_1$ is an r-group and so $[A, \overline{R}_2] = 1$. Thus, R_2 is an $\overline{A}$-invariant subgroup of $\overline{R}_1$ centralized by $\overline{A}$ and $\overline{R}_2 = 1$ and $R_2 = 1$. So $N_{G_1}(J(P_1))$ is a p-group and has a normal p-complement. If $G_1 < G$ then G_1 has a normal p-complement and would centralize H. Contradiction. Hence, $G = G_1$ and $\overline{G} = \overline{AR}$ and $\overline{A}$ acts faithfully and irreducibly on $\overline{R}$. $\overline{A}$ is elementary abelian and hence cyclic so $|A| = p$.

Step 11: Set $W = \mathbb{Z}(H), Z = \Omega_1(W)$. If $R \in S_r(G)$ then $[R, Z] \subseteq Z$ but $[R, Z] \neq 1$.
$\mathbb{Z}(P) \subseteq C_G(H) \subseteq H$ so $\mathbb{Z}(P) \subseteq W$. If $[R, W] = 1$, $[R, \mathbb{Z}(P)] = 1$, hence $\mathbb{Z}(P)$ would be central in G which is impossible.

Step 12: Contradiction
$Z \lhd G$ and G acts by conjugation so the kernel of the action is $C(Z) \supset H$ and so $\overline{G}$ acts on Z. Since $\overline{R}$ is the unique minimal normal subgroup of $\overline{G}$ and $\overline{G}$ acts nontrivially, $\overline{G}$ acts irreducibly on Z by step 11. By a previous result, $Z = C_Z(\overline{R}) + V$ where V is $\overline{R}$-invariant. Moreover, $\overline{R} \lhd \overline{G}$ and so V is $\overline{G}$ invariant and $\overline{G}$ acts faithfully on V. Since $|A| = p$, $m(A_0) \geq d(P) - 1$. Set $V_0 = V \cap A_0$ and let $t = m(V_0)$ and $r = m(A/A_0)$. $V \subseteq \mathbb{Z}(H)$ so $\langle V, A_0 \rangle$ is abelian. Since V is elementary, $d(P) \geq m(\langle V, A_0 \rangle) = m(V) + m(A_0) - m(V \cap A_0) = t + r + m(A_0) - t = d(P) - 1 + r$. Hence, $r = 0$ or $r = 1$ and $V_0 = V$ or V_0 is maximal. Choose $a \in A \setminus A_0$, $\overline{b} \in \overline{R}^H$ such that $[a, \overline{b}] \neq 1$, $[\overline{a}, V_0] = 1$ and $[\overline{a}^{\overline{b}}, V_0^{\overline{b}}] = 1$ then $[\langle \overline{a}, \overline{a}^{\overline{b}} \rangle, V_0 \cap V_0^{\overline{b}}] = 1$ and $V_0 \cap V_0^{\overline{b}} \leq p^2$. Since $A = \langle a \rangle$ is maximal in Z and $\overline{a}^{\overline{b}} \notin \overline{A}$, $\overline{G}_1, V_0 \cap V_0^{\overline{b}} = 1$ hence $|V| \leq p^2$. So $\overline{G} \subseteq GL_2(p)$ and since $\overline{G}$ is generated by 2 elements of order p, $\overline{G} \subseteq SL_2(p)$. So we have an abelian p' group, $\overline{R}$, which is normalized but not centralized by $\overline{A} \subseteq SL_2(p)$ of order p and this is impossible.

Theorem (Frobenius): If G is solvable and $|G| > 1$, $\exists p, P \in p(G) : 1 \neq P \lhd G$.

Proof: The proof is by induction. It is clearly true for all p-groups. Since G is solvable, $existsN \lhd G$ and we can assume $|G : N| = p \mid |G|$. By induction, $existsq : Q \in q(N), Q \lhd N$. So $1 \neq O_q(N)\, char\, N \lhd G$.

Theorem 25: If $P \in S_p(G)$, G contains a normal p-complement iff whenever two elements in P are G-conjugate, they are P conjugate.

Proof: See the section on transfer.

Theorem 26: If G has a maximal subgroup, M, which is nilpotent of odd order, then G is solvable.

Proof: See Passman.

Theorem 27: Let $p \neq 2$, $P \in S_p(G)$ and suppose for any $H < G : H \; char; \; P$, $N_G(H)/C_G(H)$ is a p-group, then G has a normal p complement.

Proof: By induction on $|G|$. $N_G(H)$ has a normal p-complement by induction. If $a \in p'(H)$ then $[a, H] = 1$. So H has normal p-complement. The result follows from Thompson's normal p-complement theorem.

Theorem 28: Let $p \neq 2$, $G = SL_2(p)$. The only abelian p'-subgroups of G which are normalized by an S_p subgroup of G lie in $\mathbb{Z}(G)$.

Proof: See earlier.

Chapter 17

Signalizers and Thompson Transitivity

17.1 Thompson Transitivity

Motivation for transitivity: In $\mathcal{N}^*(P,q)$, very often maximal elements are conjugate. $Q \in \mathcal{N}^*(P,q) \rightarrow P \subseteq N(Q)$. If $Q_1, Q_2 \in \mathcal{N}^*(P,q) \rightarrow \exists c \in C(P) : Q_1^c = Q_2$. In common application, $g \in N(P)$ and $Q, Q^g \in \mathcal{N}^*(P,q)$ so $\exists c \in C(P) : Q^{gc} = Q$ and thus $N(P) = C(P)(N(P) \cap N(Q))$.

Theorem 1: Suppose A is an elementary abelian p-group such that $r(A) \geq 3$. If P, Q are A-invariant p'-groups, $\exists a \in A^\# : C_P(a) \neq 1 \neq C_Q(a)$.

Proof: Let V be a subgroup of A of type (p,p). Since $P = \langle C_P(v) : v \in v^\# \rangle$, $\exists v \in V^\# : C_P(v) \neq 1$. Let $W \subseteq A$ be a group of type (p,p) and $W \cap \langle v \rangle = 1$. $\exists w \in W : C_P(w) \cap C_P(v) \neq 1$ since $C_P(v)$ is W-invariant. $\langle v, w \rangle$ is of type (p,p) and acts on Q. $\exists a \in \langle v, w \rangle^\# : C_Q(a) \neq 1$. Since $C_P(a) \supseteq C_P(w) \cap C_P(v) \neq 1$, we are done.

Definition: $\mathcal{N}_G(E,\pi)$ is the set of all E-invariant π-subgroups of G. $\mathcal{N}_G^*(E,\pi)$ is the set of all maximal elements of $\mathcal{N}_G(E,\pi)$. $\mathcal{SCN}(P)$ is the set of self-centralizing normal subgroups of P. $\mathcal{SCN}_G(p) = \mathcal{SCN}(P)$ where $P \in S_p(G)$. $r(P)$ is the rank of the largest elementary abelian subgroup of P.

Theorem 2: Let G be p-constrained. If $p = 2$ assume further that the sylow subgroup has class ≤ 2. Let E be an abelian p subgroup of G with $r(E) \geq 3$ and E contains every p-element of $C = C_G(E)$. Then every E-invariant p' subgroup H of G satisfies $H \subseteq O_{p'}(G)$. In other words, $\langle \mathcal{N}(E,p') \rangle \subseteq O_{p'}(G)$.

Proof: Let G be a minimal counterexample.

Step 1: $O_{p'}(G) = 1$.
If not, set $\overline{G} = G/O_{p'}(G)$. Since $\overline{C_G(E))} = C_{\overline{G}}(\overline{E}))$, $\overline{H} \subseteq O_{p'}(\overline{G}) = 1$ and $H \subseteq O_{p'}(G)$.

Step 2: Set $R = O_p(G)$ and let $Q \neq 1$ be a minimal E-invariant p' subgroup of G then $G = RQE$. If $RQE \subset G$ then $Q \subseteq O_{p'}(RQE)$ by induction hence $[R,Q] \subseteq O_{p'}(RQE) \cap R = 1$. By p-constraint, $C_G(R) \subseteq R$ proving the result.

Let S be a QE-invariant p subgroup of G minimal with respect to $[Q,S] \neq 1$, then S is a

special p-group.

If S is abelian, $S = C_S(Q) \oplus [S,Q]$. But $[S,Q]$ is an E-invariant p group so $C_P(E) \cap [S,Q] \neq 1, P \in S_p(G)$. Thus $E \cap [S,Q] \neq 1$. But $[E \cap [S,Q], Q] \subseteq Q \cap S = 1$ which is a contradiction. So S must be non-abelian. Further, since $[S,Q] \neq 1$ and S is minimal, $S = \Omega_1(S)$ has exponent p.

Suppose p is odd. Define a new group T whose elements are te elements of S and define the operation as follows: Every element of S has a square root since p is odd. Define $x \cdot y = \sqrt{x}y\sqrt{x}$. Then T is elementary abelian and QE acts on T. $Fix(S) = Fix(T)$ and this contradicts what we just showed. So $p = 2$.

Now $p = 2$ and S is non-abelian. $[E,S] \subseteq \mathbb{Z}(S)$ since $cl(SE) \leq 2$. So $[S,E,Q] = 1$, and $[Q,S,E] \subseteq \mathbb{Z}(S)$. If $[E,Q] \neq 1$, then $[E,Q] \subseteq Q$ stabilizes $S \supseteq \mathbb{Z}(S) \supseteq 1$ hence $[E,Q] \subseteq \mathbb{Z}(S)$. But $[E,Q]$ is an E invariant subgroup of Q and by minimality, $Q = [E,Q] \subseteq \mathbb{Z}(S)$ which is a contradiction. So $[E,Q] = 1$. Thus we may assume $[S,E] \subset S$ is Q-invariant and the minimality of S gives $[S,E,Q] = 1$. We also have $[E,Q,S] = 1$ so $[Q,S,E] = [S,E] = 1$, so $S \subseteq E$ and $[S,Q] \subseteq Q \cap S = 1$ and this contradiction concludes the proof.

Observation: If $E \in \mathcal{SCN}(P), P \in S_p(G)$ and $D \in S_p(C_G(E))$. If $Q \in S_p(N_G(E))$ and $D \subseteq Q$, $\exists n \in N_G(E)$: $Q^n = P$ and so $D^n \subseteq P \cap C_G(E) = E$ so $D = E$. Hence $D \in S_p(C_G(E)$ and by Burnside, $C_G(E) = E \times O_{p'}(C_G(E))$.

Thompson Transitivity Theorem (weakened result): Let G be a group in which the normalizer of every non-trivial p-subgroup is p-constrained. If $p = 2$ assume further that the sylow subgroup has class ≤ 2. Let E be an abelian p subgroup of G with $r(E) \geq 3$ and E contains every p-element of $C = C_G(E)$. Then $O_{p'}(C)$ acts transitively on the elements of $\mathcal{N}^*(E,q)$ where $q \neq p$.

Proof: Let $\mathcal{S}_1, \ldots, \mathcal{S}_t$ be $O_{p'}(G)$ orbits of $\mathcal{N}^*(E,Q)$ and suppose $t > 1$; obviously, $\mathcal{N}^*(E,Q) \neq \{1\}$. Let $R \neq 1$ be choosen of minimal order subject to $R = S_i \cap S_j, S_i \in \mathcal{S}_i, S_j \in \mathcal{S}_j, i \neq j$. WLOG $i = 1, j = 2$. $N = N_G(R) \supseteq E$. Put $\overline{N} = N/R$, $T_i = N \cap S_i \supseteq R$. $\overline{T_i}$ is E-invariant so $\exists e \in E^\# : C_{\overline{T_i}}(e) \neq 1$. Since $C_{\overline{T_i}}(e) = \overline{C_{T_i}(e)}$, $C_G(e) \cap T_i \supseteq R$. Since $H = C_G(e)$ is p-constrained, $E \subseteq C_G(e)$.

Let $P_i = T_i \cap H$. $R \subset P_iR$ and $P_i \subseteq N(R)$. P_i is E-invariant so by the previous result, $P_i \subseteq O_{p'}(H)$. Let $L = R(N \cap H)$. $P_i \subseteq O_{p'}(H) \cap N \subseteq O_{p'}(N \cap H)$ so $P_i \subseteq O_{p'}(L)$ since $R \lhd L$ and R is a p' group and thus $RP_i \subseteq O_{p'}(L)$. Now let $Q_i \supseteq Q_iR$ be ab E-invariant Sylow q subgroup of $O_{p'}(L)$. $\exists x \in C_G(E) \cap O_{p'}(L) : Q_1^x = Q_2$. Since $\langle x \rangle$ is an E-invariant p' subgroup of $N_G(E)$ which is p-constrained, another application of the previous result gives $x \in O_{p'}(N_G(E))$ and so $x \in O_{p'}(C_G(E))$. Let $U \in \mathcal{N}_G^*(E,q)$ so $U \supseteq Q_1$. Then $U \cap S_1 \supseteq Q_1 \cap S_1 \supseteq P_1R \supseteq R$. But $U^x \cap S_2 \supseteq Q_1^x \cap S_2 \supseteq P_2R \supseteq R$. Since $x \in C(E)$, U^x is maximal in $\mathcal{N}_G(E,q)$ and by the choice of R, $U^x \in \mathcal{S}_2$ and so $U \in \mathcal{S}_2$ and $\mathcal{S}_1 = \mathcal{S}_2$.

17.2 Signalizers

Let A be a non-cyclic elementary abelian p group acting on G. $C_G(a)$ is A-invariant for $a \in A^\#$. By an earlier theorem, if U is an A-invariant p' group then $U = \langle C_G(a) \cap U, a \in A^\# \rangle$.

Let θ be a map from $A^\#$ into p', A-invariant subgroups of G contained in $C_G(a)$. Define $\theta(C_G(a)) = \theta(a)$.

Define $\mathcal{N}_\theta(A)$ be the solvable A-invariant p' subgroups $U \leq G$ such that $U \cap \theta(C_G(a)) \subseteq \theta(C_G(a)), \forall a \in A^\#$.

If $U \in \mathcal{N}_\theta(A)$, $\langle U \cap \theta(C_G(a)), a \in A^\# \rangle = U$.

θ is solvable if $\theta(C_G(a)) \cap C_G(b) \subseteq \theta(C_G(b)), \forall a, b \in A^\#$. Equivalently, $\theta(C_G(a)) \in \mathcal{N}_\theta(A)$.

θ is complete if $\mathcal{N}_\theta(A)$ contains a unique maximal element E. Clearly, $E = \langle \theta(C_G(a)), a \in A^\# \rangle$ if it exists. So θ is complete iff $E \in \mathcal{N}_\theta(A)$.

Note: If $\theta(G)$ exists and $\theta(G) \neq 1$ and G is simple, $M = N_G(\theta(G))$ contains the normalizers of many p-subgroups of G; this is a uniqueness subgroup. If $\theta(G) = 1$, G is often of characteristic p-type and we can use Thompson factoring.

Definition: Suppose r, prime, G finite and A an abelian $r-$subgroup of G. An $A-$*signalizer* is a map $\theta : A^\# \to \mathcal{N}_\theta(A)$ where $\mathcal{N}_\theta(A)$ is a set of r' $A-$invariant subgroups such that $a, b \in A^\#$ and $\theta(a) \leq C_G(a)$ and $\theta(a) \cap C(b) \leq \theta(b)$. Example: $X \in r'(G)$, $X = \theta(G)$, $\theta(a) = C_X(a), a \in A^\#$.

Example signalizer: $X \in r'(G)$, $A \in r(G)$, $A' = 1$, $X^A = X$, $\theta(a) = C_X(a), a \in A^\#$.

Note: If $P \in S_p(G)$, $A \subseteq P$ then $N_G(A)$ permutes $\mathcal{N}_G(A, q)$ and $C_G(A)$ acts transitively so $N(P)$ normalizes some $Q \in \mathcal{N}_G^*(A, q)$. Pushing up gives $Q \in \mathcal{N}_G^*(P, q)$.

Definition: A signalizer function is solvable if $\theta(C_G(a) \cap C_G(b)) \leq \theta(C_G(b)), \forall a, b \in A^\#$. It is *complete* if $\mathcal{N}_\theta(A)$ contains a unique maximal element.

Motivation for signalizers: Suppose G has no solvable normal subgroups, what is $H = C_G(z), z \in Inv(G)$? $\theta(G, A)$ is a proper p'-group and either (i) $\theta(G, A) \lhd G$ or (ii) $N_G(\theta(G, A))$ is strongly p-embedded. Below, we show $m(A) \geq 3$ then every $A-$signalizer functor is complete. If H is strongly p-embedded then the representation of G on the right cosets of H in G has the property that all the p-elements of G fixes exactly 1 point. Simple groups with strongly p-embedded subgroups were classified by Bender.

Theorem 3: Let p be a prime and $\theta : a \mapsto O_{p'}(C_G(a))$. (1) If $C_G(a)$ is solvable $\forall a \in A^\#$ then θ is a solvable A-signalizer functor on G, (2) Suppose G is solvable then θ is complete and $\theta(G) = O_{p'}(G)$.

> *Proof:* The theorem that if $O_{p'}(G) = 1$ and $C_G(O_p(G)) \leq O_p(G)$ means that for $p \in p(G)$, $O_{p'}(N_G(P)) = O_{p'}(G) \cap N_G(P)$ insures the inclusion property for θ holds It also insures that $O_{p'}(G) = \langle \theta(C_G(a)) : a \in A^\# \rangle$.

Theorem 4: Let $X, Y \in \mathcal{N}_\theta(A)$ and $XY = YX$ and suppose that either (1) $Y \leq N_G(X)$ or (1') XY is solvable, then $XY \in \mathcal{N}_\theta(A)$.

> *Proof:* (1) insures XY is an A-invariant solvable p'-group and so $C_{XY}(a) = C_X(a)C_Y(a) \leq C_a, \forall a \in A^\#$. This proves the result.

Theorem 5: Let N be an A-invariant normal p'-subgroup of G and $\overline{G} = G/N$ then $\overline{\theta} : a \mapsto \overline{\theta}(C_{\overline{G}}(a)) = \overline{C}_a$ is a solvable signalizer functor of $\overline{G}$ and $\overline{\mathcal{N}_\theta(A)} \subseteq \mathcal{N}_{\overline{\theta}}(A)$.

> *Proof:* Let $a, b \in A^\#$ and $M = NC_a$ so $\overline{M} = \overline{\theta}(C_{\overline{G}}(a))$ and $C_{\overline{M}}(b) = \overline{C_M(b)}$. It follows that $C_M(b) = C_N(b)C_{C_a}(b) = C_N(b)(C_a \cap C_G(b)) \leq \overline{\theta}(C_{\overline{G}}(a))$. Similarly for $U \in \mathcal{N}_\theta(A)$ $C_{\overline{U}}(a) = \overline{C_U(a)} = \overline{C_a \cap U} \leq \overline{\theta}(C_{\overline{G}}(a))$. So $\overline{U} \in \mathcal{N}_{\overline{\theta}}(A)$.

Theorem 6: Assume in the previous result that $N \in \mathcal{N}_\theta(A)$ then $\overline{\mathcal{N}_\theta(A)} = \mathcal{N}_{\overline{\theta}}(A)$. In particular, θ is complete iff $\overline{\theta}$ is complete.

Proof: Let $N \leq U < G$ such that $\overline{U} \in \mathcal{N}_{\overline{\theta}}(A)$. STS $U \in \mathcal{N}_\theta(A)$. For $a \in A^\#$, $\overline{C_U(a)} = C_{\overline{U}}(a) \leq \overline{\theta}(C_{\overline{G}}(a)) = \overline{C}_a = C_aN/N$ and thus $C_U(a) \leq NC_a \cap C_G(a) = C_N(a)C_a \leq C_a$ since $N \in \mathcal{N}_\theta(A)$ so $U \in \mathcal{N}_\theta(A)$. Set $\pi(\theta) = \bigcup_{a \in A^\#} \pi(C_a)$.

Theorem 7: Let $U \in \mathcal{N}_\theta(A)$ then $\pi(U) \subseteq \pi(C_a)$.

Proof: This is clear.

Definition: $C_A = \theta(C_G(A))$. If $p \notin \pi$, $C_a = \theta(C_G(a))$ then C_a contains a unique maximal AC_A-invariant π-subgroup denoted by $\theta_\pi(C_G(a))$.

Theorem 8: The mapping $\theta_\pi : a \mapsto \theta_\pi(C_G(a))$ is a solvable A-signalizer functor on G satisfying $\pi(\theta_\pi) \subseteq \pi$ and $\{U \in \mathcal{N}_\theta(A, \pi) : U^{C_A} = U\} \subseteq \mathcal{N}_{\theta_\pi}(A)$.

Proof: Let $a, b \in A^\#$ then $\theta_\pi(C_G(a)) \cap C_G(b)$ is an AC_A-invariant π subgroup of C_b Thus $\theta_\pi(C_G(a)) \cap C_G(b)$ is contained in the unique maximal AC_A-invariant π-subgroup $\theta_\pi(C_G(b))$, This shows that θ_π is a solvable A-signalizer functor on G. Clearly, $\pi(\theta_\pi) \subseteq \pi$ and the other property follows from the uniqueness of $\theta_\pi(C_G(a))$.

Theorem 9: Let $U \in \mathcal{N}_\theta(A)$ then $\pi(U) \subseteq \pi(\theta)$.

Proof: For every $q \in \pi(U)$, there is an A-invariant Sylow q-subgroup Q of U. Moreover, since A is non-cyclic, $\exists a \in A$ such that $C_Q(a) \neq 1$. Thus $C_Q(a) \leq C_U(a) \leq C_a$, we get $q \in \pi(\theta)$.

Theorem 10: Let A be an elementary abelian p-group with $r(A) \geq 3$ that acts on the group X and let $p \neq q \in \pi(X)$. Suppose Q_1 and Q_2 are two A-invariant q-subgroups of X such that for $D = Q_1 \cap Q_2$ $Q_1 \neq D \neq Q_2$ then $\exists a \in A^\#$ such that $N_G(D) \cap C_{Q_i}(a) \not\leq D, i = 1, 2$.

Proof: Since $Q_1 \neq D \neq Q_2$, we get $D < N_{Q_i}(D) = N_i, i = 1, 2$ and $N_i = \langle C_{N_i}(B) \rangle$, $B \leq A$ and $r(A/B) \leq 1$. For $i = 1, 2$ there is a maximal subgroup B_i of A such that $C_{N_i}(B_i) \not\leq D$. Because $r(A) \geq 3$, we get $B_1 \cap B_2 \neq 1$. Now choose $1 \neq a \in B_1 \cap B_2$.

Transitivity Theorem: Let θ be a solvable A-signalizer functor on G, $q \in \pi(\theta)$ and suppose $r(A) \geq 3$ then the elements in $\mathcal{N}^*_\theta(A, q)$ are conjugate in C_A.

Proof: Assume the assertion is false. Among all pairs of elements $\mathcal{N}^*_\theta(A, q)$ that are not conjugate under C_A, we choose Q_1 and Q_2 such that $D = Q_1 \cap Q_2$ is maximal. Set $N = N_G(D)$ and $N_a = N \cap C_a, a \in A^\#$. There is an $a \in A^\#$, such that $N_a \cap Q_1 \not\leq D$ and $N_a \cap Q_2 \not\leq D$. N_a is an A-invariant p'-group, thus $\exists c \in C_{N_a}(A) \leq C_A$ such that $E = \langle (N_a \cap Q_1)^c, N_a \cap Q_2 \rangle$ is an A-invariant q-subgroup. Since D and E are in $\mathcal{N}_\theta(A, q)$. So $\exists Q_3 \in \mathcal{N}^*_\theta(A, q)$ containing DE, so $D < D(N_a \cap Q_1)^c \leq Q_1^c \cap Q_3$ and. $D < D(N_a \cap Q_2) \leq Q_2 \cap Q_3$. The maximal choice of D implies that Q_1^c and Q_3 are conjugate under C_A as well as Q_2 and Q_3. But then also Q_1 and Q_2 are conjugate under C_A, a contradiction.

Theorem 11: Let $q \in \pi(\theta)$ and $Q \in \mathcal{N}^*_\theta(A, q)$ and suppose $r(A) \geq 3$ then (1) $\forall H \in \mathcal{N}_\theta(A)$ $\exists c \in C_A$ such that $Q^c \cap H$ is an A-invariant Sylow q-subgroup of H; and (2) $C_Q(B)$ is an A-invariant Sylow q-subgroup of C_B for every $1 \neq B \leq A$.

Proof: Every A-invariant Sylow q-subgroup, Q_1 of H is in $\mathcal{N}_{\theta_\pi}(A)$ and is thus contained in an element $Q_2 \in \mathcal{N}^*_{\theta_\pi}(A)$. So $\exists c \in C_A : Q_2 = Q^c$ and $Q^c \cap H = Q_1$. Part 2 follows from 1 with $H = C_B$ since $C_A \leq C_B$.

Theorem 12: If $|\pi(\theta)| \leq 1$ and $r(A) \geq 3$ then θ is complete.

Proof: The case $\pi(\theta) = \emptyset$ gives $\theta(G) = 1$. Assume $\pi(\theta) = \{q\}$. Then $\mathcal{N}_\theta(A)\mathcal{N}_\theta(A,q)$, and $\exists Q \in \mathcal{N}_\theta^*(A)$ such that $C_A \leq Q$ and by the previous result, Q is the only element in $\mathcal{N}_\theta^*(A,q)$.

Theorem 13: Let G be a solvable p' group and $q \in \pi(G)$. Suppose U is a q' group of G such that $[U, C_G(B)]$ is a q' group for every maximal subgroup B of A. Then $U \leq O_{p'}(G)$.

Proof: See Stellmacher, p 325.

Glauberman's Theorem: Let θ be a solvable signalizer functor on G and $r(A) \geq 3$ then θ is complete.

Proof: See Stellmacher, p 327.

17.3 Factorizations

Theorem 14a: Suppose the action of A on G is coprime and $G = XY$ with X and Y A-invariant then $C_G(A) = C_X(A)C_Y(A)$.

Proof: Let $g = xy \in G$. $xy = (xy)^a = x^a y^a$. So $x^{-1}x^a = yy^{-a} \in X \cap Y$. $(xU)^a = xU$ and $(Uy)^a = Uy$, so $\exists c \in C_X(A), x = cu$ and $\exists d \in C_Y(A), y = wu$. $cuwd \in C_G(A) \cap X \cap Y$, so $uw \in C_X(A)C_Y(A)$.

Theorem 14: If $p \in \pi(G)$ and $\overline{G} = G/O_{p'}(G)$ and suppose $\overline{G}$ is p-constrained then $\forall P \in p(G)$, $O_{p'}(N_G(P)) = O_{p'}(G) \cap N_G(P)$.

Proof: $C_G(P) \lhd N_G(P) \to O_{p'}(N_G(P)) = O_{p'}(C_G(P))$ so it STS $O_{p'}(G) \cap C_G(P) = O_{p'}(C_G(P))$. Assume $O_{p'}(G) = 1$ and put $Q = O_{p'}(C_G(P))$. $C_G(O_p(G)) \subseteq O_p(G)$ and $[P, Q] = 1$ so we can apply Thompson's $p \times q$ lemma to show Q acts trivially on $C_G(P)$ and $Q \leq C_G(O_p(G)) \leq O_p(G)$ and $Q = 1$.

Theorem 15: Let $P \in p(G)$ and $U \leq O_{p'}(N_G(P))$. Suppose U and P are contained in some solvable group L. Then $U \leq O_{p'}(L)$.

Proof: Todo.

Definition: For $q \in \pi(\theta)$, put $\theta_{q'} = \theta_{\pi(\theta)\setminus Q}$. θ is locally complete if $\theta_{N_G(U)}$ is complete for $U \in \mathcal{N}_\theta(A)$ and $\theta_{q'}$ is complete for all $q \in \pi(\theta)$.

Theorem 16: Let G be a p'-group and X and Y be two A-invariant subgroups if G. Suppose further, (1) $C_G(a) = C_X(a)C_Y(a)$ for all $a \in A^\#$ and (2) X is $C_G(A)$-invariant then $G = XY$.

Proof: By induction. Let q be a prime divisor of $|G|$ and G has a non-trivial q subgroup. $\mathbb{Z}(G) \neq 1$ and since A is non-cyclic, $\exists a \in A : N = C_{\mathbb{Z}(G)}(a) \neq 1$. N is A-invariant. Put $\overline{(G)} = G/N$. By induction, $G = XYN = XNY = XC_G(a)Y = XY$. See Stellmacher, p 312 for the rest.

17.4 More from Thompson

Thompson Transitivity Theorem: If G is a group in which the normalizer of every non-identity p-subgroup is p-constrained and if $A \in \mathcal{SCN}_3(p)$ then $C_G(A)$ permutes all maximal A-invariant q groups of G, $q \neq p$.

Proof: Generalization of earlier result.

Consequence: Under the TTT conditions, if $P \in S_p(G), A \in \mathcal{SCN}_3(P)$ and $\forall q \neq p$, P normalizes some $A-$invariant $q-$subgroup of G; so if P normalizes no p' subgroup of G, neither does A.

Maximal Subgroup Theorem: If $P \in S_p(G), \mathcal{SCN}_3(P) \neq \emptyset, p \neq 2$ and every element of $\mathcal{N}^*(P)$ is $p-$constrained and $p-$stable and $\exists H, 1 \neq H \lhd P$: $[Q, P] = 1$ if $H \in p'(G)$ and $H^P = H$ then $\mathcal{N}^*(P)$ has a unique maximal element.

Proof: Generalization of earlier result.

Thompson (from N-group paper): G is not solvable iff $\exists x, y, z \in G \setminus \{1\}$ with $(|x|, |y|) = (|y|, |z|) = (|x|, |z|) = 1$ such that $xy = z$. If G is a non-abelian simple group all of whose $p-$locals are solvable then G is isomorphic to one of the following: (1) $PSL_2(q), q > 3$, (2) $Sz(q), q = 2^{2m+1}, m \geq 1$ or (3) A_7, $PSL(2(3)$, $U_3(3)$, or M_{11}.

Proof: The proof is too long for this paper.

Theorem 13: If M is a maximal subgroup of G, $p \in \pi(M)$, $O_{p'}(M) \neq 1$ then all maximal primitive subgroups are conjugate to M.

Thompson Transfer Theorem: Let $S \in S_2(G)$ and suppose $\exists U \leq G$ maximal and $t \in Inv(S) \rightarrow t^G \cap U = \emptyset$ then $t \notin O^2(G)$.

17.5 Bender Uniqueness

Observation: The following uniqueness result is used in the simplification of the odd order result.

Bender's Theorem: Let G be a minimal subgroup of odd order and U be a elementary abelian subgroup of order p^3 then there is one maximal subgroup of G containing U.

Chapter 18

Representations

18.1 $\mathbb{C}G$-modules

Definition: A *representation* of G is a group homomorphism $\rho : G \to GL_n(\mathbb{C})$, n is called the *degree* of ρ. The representation $\rho : G \to GL_n(\mathbb{C})$ is called *faithful* if $ker(\rho) = \{1\}$. Thus ρ is faithful if the only element $g \in G$ with $\rho(g) = I_n$ is the identity of G.

Theorem 1: A representation ρ of G is faithful if and only if $im(\rho) \cong G$.

Proof: We have $G/ker(\rho) \cong im(\rho)$ so if $ker(\rho) = \{1\}$, the isomorphism theorem gives $G \cong im(\rho)$. Conversely if $G \cong im(\rho)$ then these two finite groups have the same order, and so $|ker(\rho)| = 1$.

Definition: A finite-dimensional vector space V over $\mathbb{C}$ is a $\mathbb{C}G$*-module* if a multiplication gv (for all $g \in G$ and $v \in V$) is defined, satisfying the following conditions for all $u, v \in V$, $\lambda \in \mathbb{C}$ and $g \in G$:

(i) $gv \in V$;

(ii) $(gh)v = g(hv)$;

(iii) $1v = v$;

(iv) $g(\lambda v) = \lambda(gv)$;

(v) $g(u + v) = gu + gv$.

Definition: If V is a $\mathbb{C}G$-module, g induces a linear map $\rho(g) : V \to V$; if $\mathcal{B}$ is a basis of V, the matrix for the matrix representing the linear map $\rho(g)$ is denoted by $[g]_{\mathcal{B}}$.

Theorem 2: Let G be a finite group.

(i) Given a representation $\rho : G \to GL_n(\mathbb{C})$, the vector space $V = \mathbb{C}^n$ is a $\mathbb{C}G$-module if we define the multiplication by $gv = \rho(g)v$ for all $g \in G$ and $v \in V$. Moreover, there is a basis $\mathcal{B}$ of V such that $\rho(g) = [g]_{\mathcal{B}}$ for all $g \in G$.

(ii) Given a $\mathbb{C}G$-module V of dimension $n > 0$ with basis $\mathcal{B}$, the function $\rho : G \to GL_n(\mathbb{C})$ defined by $\rho(g) = [g]_{\mathcal{B}}$ is a representation of G.

Proof:

(i) For all $u, v \in \mathbb{C}^n$, $\lambda \in \mathbb{C}$ and $g, h \in G$ we have

$$\begin{aligned} \rho(g)v &\in \mathbb{C}^n, \\ \rho(gh)v &= \rho(g)\rho(h)v, \\ \rho(1)v &= v, \\ \rho(g)(\lambda v) &= \lambda\rho(g)v, \\ \rho(g)(u+v) &= \rho(g)u + \rho(g)v. \end{aligned}$$

Defining $gv = \rho(g)v$ for all $g \in G$ and $v \in \mathbb{C}^n$ makes $\mathbb{C}^n$ into a $\mathbb{C}G$-module. Moreover, if we let $\mathcal{B}$ be the basis

$$100\dot{:}0, \qquad 010\dot{:}0, \qquad \cdots, \qquad 000\dot{:}1$$

of $\mathbb{C}^n$, then we have $\rho(g) = [g]_{\mathcal{B}}$ for all $g \in G$.

(ii) Let V be a $\mathbb{C}G$-module with basis $\mathcal{B}$. Since $(gh)v = g(hv)$ for all $g, h \in G$ and all v in the basis $\mathcal{B}$, it follows that $[gh]_{\mathcal{B}} = [g]_{\mathcal{B}}[h]_{\mathcal{B}}$. In particular, $[1]_{\mathcal{B}} = [g]_{\mathcal{B}}[g^{-1}]_{\mathcal{B}}$ for all $g \in G$. Now we have $1v = v$ for all $v \in V$, so $[1]_{\mathcal{B}}$ is the identity matrix I_n; thus each matrix $[g]_{\mathbb{B}}$ is invertible (with inverse $[g^{-1}]_{\mathcal{B}}$). Hence the function $g \mapsto [g]_{\mathcal{B}}$ is a homomorphism from G to $GL_n(\mathbb{C})$, i.e., a representation of G.

Theorem 3: Let V be a $\mathbb{C}G$-module with basis $\mathcal{B}$, and let ρ be the representation of G defined by $\rho(g) = [g]_{\mathcal{B}}$ for all $g \in G$. Then

(i) if $\mathcal{B}'$ is a basis of V, the representation ϕ of G defined by $\phi(g) = [g]_{\mathcal{B}'}$ for all $g \in G$ is equivalent to ρ;

(ii) if σ is a representation of G which is equivalent to ρ, there is a basis $\mathcal{B}''$ of V such that $\sigma(g) = [g]_{\mathcal{B}''}$ for all $g \in G$.

Proof:

(i) Let T be the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$; then

$$\phi(g) = [g]_{\mathcal{B}'} = T^{-1}[g]_{\mathcal{B}}T = T^{-1}\rho(g)T \qquad \text{for all } g \in G,$$

and so ϕ is equivalent to ρ.

(ii) If σ is equivalent to ρ, then there is an invertible matrix T such that we have $\sigma(g) = T^{-1}\rho(g)T$ for all $g \in G$. If we let $\mathcal{B}''$ be the basis of V such that the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}''$ is T, then

$$\sigma(g) = T^{-1}\rho(g)T = T^{-1}[g]_{\mathcal{B}}T = [g]_{\mathcal{B}''} \qquad \text{for all } g \in G$$

as required.

Lemma: If V and W are $\mathbb{C}G$-modules, then $V \cong W$ if and only if there exist bases $\mathcal{B}_1$ of V and $\mathcal{B}_2$ of W such that $[g]_{\mathcal{B}_1} = [g]_{\mathcal{B}_2}$ for all $g \in G$.

Proof: Suppose that $\theta : V \to W$ is a $\mathbb{C}G$-isomorphism, and let $v_1, \ldots, v_n$ be a basis $\mathcal{B}_1$ of V; then $\theta(v_1), \ldots, \theta(v_n)$ is a basis $\mathcal{B}_2$ of W. Given $g \in G$, write $gv_i = \sum a_{ji} v_j$; then

$$g\theta(v_i) = \theta(gv_i) = \theta\left(\sum a_{ji} v_j\right) = \sum a_{ji}\theta(v_j),$$

and so $[g]_{\mathcal{B}_2} = (a_{ij}) = [g]_{\mathcal{B}_1}$. Conversely, if $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ are bases $\mathcal{B}_1$ of V and $\mathcal{B}_2$ of W such that $[g]_{\mathcal{B}_1} = [g]_{\mathcal{B}_2}$ for all $g \in G$, let $\theta : V \to W$ be the invertible linear map given by $\theta(v_i) = w_i$ for all i. Given $g \in G$, let $[g]_{\mathcal{B}_1} = (a_{ij})$, so that $gv_i = \sum a_{ji} v_j$; then because $[g]_{\mathcal{B}_2} = (a_{ij})$ as well, for all i we have

$$g\theta(v_i) = gw_i = \sum a_{ji} w_j = \sum a_{ji}\theta(v_j) = \theta\left(\sum a_{ji} v_j\right) = \theta(gv_i),$$

and so θ is a $\mathbb{C}G$-isomorphism.

Theorem 4: Let V and W be $\mathbb{C}G$-modules with bases $\mathcal{B}$ and $\mathcal{B}'$; let ρ and σ be the representations of G given by $\rho(g) = [g]_{\mathcal{B}}$ and $\sigma(g) = [g]_{\mathcal{B}'}$ for all $g \in G$. Then $V \cong W$ if and only if ρ and σ are equivalent.

Proof: Assume that V and W are isomorphic $\mathbb{C}G$-modules. By the Lemma, there exist bases $\mathcal{B}_1$ of V and $\mathcal{B}_2$ of W such that $[g]_{\mathcal{B}_1} = [g]_{\mathcal{B}_2}$ for all $g \in G$. Define a representation τ of G by $\tau(g) = [g]_{\mathcal{B}_1}$; then by the Theorem (i), τ is equivalent to both ρ and σ, and so ρ and σ are equivalent. Conversely, if ρ and σ are equivalent, by the Theorem (ii) there is a basis $\mathcal{B}''$ of V such that $\sigma(g) = [g]_{\mathcal{B}''}$ for all $g \in G$, i.e., $[g]_{\mathcal{B}'} = [g]_{\mathcal{B}''}$ for all $g \in G$; thus $V \cong W$ by the Lemma.

18.2 $\mathbb{C}G$-submodules

Definition: Let V be a $\mathbb{C}G$-module. A subset U of V is a *$\mathbb{C}G$-submodule* of V if U is a subspace of the vector space V which satisfies $gu \in U$ for all $g \in G$ and $u \in U$. Thus a $\mathbb{C}G$-submodule of the $\mathbb{C}G$-module V is a subspace U of V such that U is itself a $\mathbb{C}G$-module.

Definition: A non-zero $\mathbb{C}G$-module V is called *irreducible* if it has no $\mathbb{C}G$-submodules apart from $\{0\}$ and V, and *reducible* otherwise. A representation $\rho : G \to GL_n(\mathbb{C})$ is called *irreducible* if the corresponding $\mathbb{C}G$-module $\mathbb{C}^n$, given by $gv = \rho(g)v$ for $g \in G$ and $v \in \mathbb{C}^n$, is *irreducible*, and is *reducible* otherwise.

Theorem 5: If U is a subspace of the complex vector space V with complex inner product $(\ ,\ )$, then $U^\perp$ is a subspace of V, and $U \oplus U^\perp = V$.

Proof: If $v, w \in U^\perp$ and $\lambda \in \mathbb{C}$, then for all $u \in U$ we have $(v, u) = (w, u) = 0$, so

$$(v + w, u) = (v, u) + (w, u) = 0 + 0 = 0, \qquad (\lambda v, u) = \lambda(v, u) = \lambda.0 = 0;$$

thus $v + w, \lambda v \in U^\perp$, and so $U^\perp$ is a subspace of V.

If $u \in U \cap U^\perp$, then $(u, u) = 0$, so $u = 0$ – thus the sum $U + U^\perp$ is direct. To show that $U + U^\perp = V$, take a basis $v_1, \ldots, v_r$ of U, and extend to a basis $v_1, \ldots, v_r, v_{r+1}, \ldots, v_n$ of V. Apply the Gram-Schmidt process to obtain an orthonormal basis $e_1, \ldots, e_r, e_{r+1}, \ldots, e_n$ of V; then $e_1, \ldots, e_r$ form an orthonormal basis of U, and so $e_{r+1}, \ldots, e_n \in U^\perp$ – given $v \in V$ we may write

$$v = \sum_{i=1}^{n} \lambda_i e_i = \sum_{i=1}^{r} \lambda_i e_i + \sum_{i=r+1}^{n} \lambda_i e_i \in U + U^\perp.$$

Maschke's Theorem: If V is a $\mathbb{C}G$-module and U is a $\mathbb{C}G$-submodule, there is a $\mathbb{C}G$-submodule, W, of V such that $V = U \oplus W$.

Proof: Let $\langle\ ,\ \rangle$ be the inner product on V and take the orthogonal complement $U^\perp$ with respect to it then $V = U \oplus U^\perp$. Given $g \in G$ and $v \in U^\perp$, for all $u \in U$ we have $g^{-1}u \in U$ as U is a $\mathbb{C}G$-submodule, so that

$$\langle gv, u\rangle = \langle gv, g(g^{-1}u)\rangle = \langle v, g^{-1}u\rangle = 0;$$

thus $gv \in U^\perp$. This shows that $U^\perp$ is a $\mathbb{C}G$-submodule of V; so taking $W = U^\perp$ gives the $\mathbb{C}G$-module direct sum $V = U \oplus W$ as required.

Alternate Proof: $V = U \oplus W_0$ where W_0 is some not necessarily $\mathbb{C}G$-invariant subspace. Let π_U be the projection operator onto U so $\pi_U(u + w) = u$. Put $\varphi(x) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi_U g(x)$. $U = \varphi(U)$ and φ is a $\mathbb{C}G$-invariant projection. $V = im(\varphi) \oplus ker(\varphi)$. But $im(\varphi) = U$ so $V = U \oplus W$ where $W = ker(\varphi)$.

Definition: A $\mathbb{C}G$-module V is called *completely reducible* if $V = U_1 \oplus \cdots \oplus U_r$ where each U_i is an irreducible $\mathbb{C}G$-submodule of V.

Theorem 6: If V is a non-zero $\mathbb{C}G$-module, then V is completely reducible.

Proof: We use induction on $n = dim(V)$: the result is clear if $n = 1$, as then V is itself irreducible, so assume $n > 1$. The result holds if V is irreducible, so assume V is reducible; then V has a $\mathbb{C}G$-submodule $U \neq \{0\}, V$. Theorem a previous result, V has a $\mathbb{C}G$-submodule W with $V = U \oplus W$; as $dim(U), dim(W) < n$, by induction we have

$$U = U_1 \oplus \cdots \oplus U_r, \qquad W = W_1 \oplus \cdots \oplus W_s,$$

where each U_i and W_j is an irreducible $\mathbb{C}G$-module. It follows that

$$V = U_1 \oplus \cdots \oplus U_r \oplus W_1 \oplus \cdots \oplus W_s$$

as required.

Schur's Theorem: If V, W are irreducible $\mathbb{C}G$-modules and $\theta : V \to W$ is a $\mathbb{C}G$ homomorphism then either $\theta = 0$ or θ is an isomorphism.

Proof: (i) Suppose there exists $v \in V$ with $\theta(v) \neq 0$. Then $im(\theta) \neq \{0\}$; because $im(\theta)$ is a $\mathbb{C}G$-submodule of W, which is irreducible, we must have $im(\theta) = W$. Also $ker(\theta) \neq V$; as $ker(\theta)$ is a $\mathbb{C}G$-submodule of V, which is irreducible, we must have $ker(\theta) = \{0\}$. Thus θ is invertible, and so it is a $\mathbb{C}G$-isomorphism.

(ii) Because V is a vector space over $\mathbb{C}$, the endomorphism θ has an eigenvalue $\lambda \in \mathbb{C}$, and so $ker(\theta - \lambda 1_V) \neq \{0\}$. Since $\theta - \lambda 1_V$ is clearly a $\mathbb{C}G$-homomorphism, $ker(\theta - \lambda 1_V)$ is a $\mathbb{C}G$-submodule of V; because V is irreducible, we must have $ker(\theta - \lambda 1_V) = V$. Thus $(\theta - \lambda 1_V)(v) = 0$ for all $v \in V$, and so $\theta - \lambda 1_V = 0$, i.e., $\theta = \lambda 1_V$ as required.

Theorem 7: If V is a non-zero $\mathbb{C}G$-module such that every $\mathbb{C}G$-homomorphism from V to V is a scalar multiple of 1_V, then V is irreducible.

Proof: Suppose that V is reducible; then it has a $\mathbb{C}G$-submodule U not equal to $\{0\}$ or V. There is a $\mathbb{C}G$-submodule W of V with $V = U \oplus W$. The map $\pi : V \to V$ defined by $\pi(u + w) = u$ for all $u \in U$ and $w \in W$ is a $\mathbb{C}G$-homomorphism; since it is not a scalar multiple of 1_V, this is a contradiction. Thus V must be irreducible.

Corollary: Let $\rho : G \to GL_n(\mathbb{C})$ be a representation of G; then ρ is irreducible if and only if every $n \times n$ matrix A with complex entries which satisfies

$$A\rho(g) = \rho(g)A \qquad \text{for all } g \in G$$

has the form $A = \lambda I_n$ with $\lambda \in \mathbb{C}$.

Proof: Regard $\mathbb{C}^n$ as a $\mathbb{C}G$-module by defining $gv = \rho(g)v$ for all $g \in G$ and $v \in \mathbb{C}^n$. Let A be an $n \times n$ matrix over $\mathbb{C}$. The endomorphism $v \mapsto Av$ of $\mathbb{C}^n$ is a $\mathbb{C}G$-homomorphism if and only if

$$A(gv) = g(Av) \qquad \text{for all } g \in G,\ v \in \mathbb{C}^n;$$

i.e., if and only if

$$A\rho(g) = \rho(g)A \qquad \text{for all } g \in G.$$

The result now follows from the Lemma and an earlier theorem.

Theorem 8: If V, W are $\mathbb{C}G$-module and $\varphi : V \to W$ is a $\mathbb{C}G$-homomorphism then $ker(\varphi)$ and $im(\varphi)$ are $\mathbb{C}G$-modules.

Proof: Straightforward.

Theorem 9: If V is a non-zero $\mathbb{C}G$-module and $\theta : V \to W$ is a $\mathbb{C}G$ module homomorphism, $\exists U$, a $\mathbb{C}G$-submodule of V such that $V = ker(\theta) \oplus U$. $Hom_{\mathbb{C}G}(V, W)$ is a vector space over $\mathbb{C}$.

Proof: $ker(\theta)$ is a $\mathbb{C}G$-module, so by Maschke, there is a $\mathbb{C}G$-module, U such that $V = ker(\theta) \oplus U$. The map $\overline{\theta}(u) = \theta(u)$ is a $\mathbb{C}G$-isomorphism from U into $im(\theta)$. If $u \in ker(\overline{\theta})$, $u \in ker(\theta) \cap U$. If $v \in V$ and $\theta(v) = w$, $v = k + u$, $k \in ker(\theta), u \in U$. $w = \theta(v) = \theta(k) + \overline{\theta}(u) = \theta(u)$ and $Im(\theta) = Im(\overline{\theta})$. $U \cong Im(\theta)$.

18.3 $\mathbb{C}G$-homomorphisms

Definition: Let V and W be $\mathbb{C}G$ modules. θ is a $\mathbb{C}G$ homomorphism if θ is a $\mathbb{C}$ linear map $\theta : V \to W$ with $\theta(gv) = g\theta(v), \forall v \in V$. The set (group) of $\mathbb{C}G$ homomorphisms from V into W is denoted $Hom_{\mathbb{C}G}$.

Theorem 10: If V and W are $\mathbb{C}G$-modules, $\theta, \phi : V \to W$ are $\mathbb{C}G$-homomorphisms and $\lambda \in \mathbb{C}$, then $\theta + \phi, \lambda\theta : V \to W$ are also $\mathbb{C}G$-homomorphisms.

Proof: We know that $\theta + \phi$ and $\lambda\theta$ are linear maps; and for all $g \in G$ and $v \in V$ we have

$$\begin{aligned}(\theta + \phi)(gv) &= \theta(gv) + \phi(gv) = g\theta(v) + g\phi(v) = g(\theta(v) + \phi(v)) = g((\theta + \phi)(v)),\\ (\lambda\theta)(gv) &= \lambda.\theta(gv) = \lambda.g\theta(v) = g(\lambda.\theta(v)) = g(\lambda\theta)(v)\end{aligned}$$

as required.

Definition: If V and W are $\mathbb{C}G$-modules, the vector space of all $\mathbb{C}G$-homomorphisms $\theta : V \to W$ is written $Hom_{\mathbb{C}G}(\mathbb{C}G(V, W))$.

Theorem 11: If V and W are irreducible $\mathbb{C}G$-modules, then $dim(Hom_{\mathbb{C}G}(V, W)) = 1$, if $V \cong W$, and $dim(Hom_{\mathbb{C}G}(V, W)) = 0$, if $V \ncong W$.

Proof: If $V \not\cong W$ this is immediate from Schur's Lemma. If $V \cong W$, let $\theta : V \to W$ be a $\mathbb{C}G$-isomorphism; if $\phi \in Hom_{\mathbb{C}G}(V, W)$, then $\theta^{-1}\phi \in Hom_{\mathbb{C}G}(V, V)$. There exists $\lambda \in \mathbb{C}$ with $\theta^{-1}\phi = \lambda 1_V$; thus $\phi = \lambda\theta$, and so we have $Hom_{\mathbb{C}G}(V, W) = \{\lambda\theta : \lambda \in \mathbb{C}\}$, which is a 1-dimensional vector space.

Theorem 12: Let V, V_1, V_2, W, W_1 and W_2 be $\mathbb{C}G$-modules: then

(i) $dim(Hom_{\mathbb{C}G}(V, W_1 \oplus W_2)) = dim(Hom_{\mathbb{C}G}(V, W_1)) + dim(Hom_{\mathbb{C}G}(V, W_2))$;

(ii) $dim(Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)) = dim(Hom_{\mathbb{C}G}(V_1, W)) + dim(Hom_{\mathbb{C}G}(V_2, W))$.

Proof:

(i) Define the maps $\pi_1 : W_1 \oplus W_2 \to W_1$ and $\pi_2 : W_1 \oplus W_2 \to W_2$ by

$$\pi_1(w_1 + w_2) = w_1, \qquad \pi_2(w_1 + w_2) = w_2 \qquad \text{for all } w_1 \in W_1,\ w_2 \in W_2;$$

then we see that π_1 and π_2 are $\mathbb{C}G$-homomorphisms. Given $\theta \in Hom_{\mathbb{C}G}(V, W_1 \oplus W_2)$, it is easy to see that $\pi_i\theta \in Hom_{\mathbb{C}G}(V, W_i)$ for $i = 1, 2$. We may thus define a map f from the vector space $Hom_{\mathbb{C}G}(V, W_1 \oplus W_2)$ to the vector space direct sum $Hom_{\mathbb{C}G}(V, W_1) \oplus Hom_{\mathbb{C}G}(V, W_2)$ by

$$f(\theta) = (\pi_1\theta, \pi_2\theta) \qquad \text{for all } \theta \in Hom_{\mathbb{C}G}(V, W_1 \oplus W_2).$$

It is clear that f is a linear map; we shall show that it is bijective.

Given $\phi_i \in Hom_{\mathbb{C}G}(V, W_i)$ for $i = 1, 2$, the map $\phi : V \to W_1 \oplus W_2$ defined by $\phi(v) = \phi_1(v) + \phi_2(v)$ for all $v \in V$ lies in $Hom_{\mathbb{C}G}(V, W_1 \oplus W_2)$, and satisfies $f(\phi) = (\phi_1, \phi_2)$; thus f is surjective. If $f(\theta) = 0$, then $\pi_1\theta = 0$ and $\pi_2\theta = 0$, so for all $v \in V$ we have $\theta(v) = \pi_1\theta(v) + \pi_2\theta(v) = 0$; thus $\theta = 0$, and so f is injective. Thus f is an invertible linear map from $Hom_{\mathbb{C}G}(V, W_1 \oplus W_2)$ to the vector space direct sum $Hom_{\mathbb{C}G}(V, W_1) \oplus Hom_{\mathbb{C}G}(V, W_2)$, and so these two spaces have the same dimension as required.

(ii) Given $\theta \in Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$, define $\theta_i : V_i \to W$ for $i = 1, 2$ to be the restriction of θ to V_i, i.e., the map defined by $\theta_i(v) = \theta(v)$ for all $v \in V_i$; then $\theta_i \in Hom_{\mathbb{C}G}(V_i, W)$ for $i = 1, 2$. Now define a map h from the vector space $Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$ to the vector space $Hom_{\mathbb{C}G}(V_1, W) \oplus Hom_{\mathbb{C}G}(V_2, W)$ by

$$h(\theta) = (\theta_1, \theta_2) \qquad \text{for all } \theta \in Hom_{\mathbb{C}G}(V_1 \oplus V_2, W).$$

Clearly h is a linear map, and is injective. Given $\phi_i \in Hom_{\mathbb{C}G}(V_i, W)$ for $i = 1, 2$, the map $\phi : V_1 \oplus V_2 \to W$ defined by $\phi(v_1 + v_2) = \phi_1(v_1) + \phi_2(v_2)$ for all $v_1 \in V_1$, $v_2 \in V_2$ lies in $Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$, and $h(\phi) = (\phi_1, \phi_2)$; thus h is surjective. Thus h is a bijective linear map from $Hom_{\mathbb{C}G}(V_1 \oplus V_2, W)$ to the vector space direct sum $Hom_{\mathbb{C}G}(V_1, W) \oplus Hom_{\mathbb{C}G}(V_2, W)$, and so these two spaces have the same dimension as required.

Corollary: If $V_1, \ldots, V_r, W_1, \ldots W_s$ are $\mathbb{C}G$-modules, then

$$dim(Hom_{\mathbb{C}G}(V_1 \oplus \cdots \oplus V_r, W_1 \oplus \cdots \oplus W_s)) = \sum_{i=1}^{r} \sum_{j=1}^{s} dim(Hom_{\mathbb{C}G}(V_i, W_j)).$$

Proof: For convenience write $W = W_1 \oplus \cdots \oplus W_s$; then by induction, we have

$$\begin{aligned} dim(Hom_{\mathbb{C}G}(V_1 \oplus \cdots \oplus V_r, W)) &= \sum_{i=1}^{r} dim(Hom_{\mathbb{C}G}(V_i, W)) \\ &= \sum_{i=1}^{r} dim(Hom_{\mathbb{C}G}(V_i, W_1 \oplus \cdots \oplus W_s)) \\ &= \sum_{i=1}^{r} \sum_{j=1}^{s} dim(Hom_{\mathbb{C}G}(V_i, W_j)) \end{aligned}$$

as required.

Corollary: Let V be a $\mathbb{C}G$-module with $V = U_1 \oplus \cdots \oplus U_r$ where each U_i is irreducible, and W be any irreducible $\mathbb{C}G$-module; then both $dim(Hom_{\mathbb{C}G}(V, W))$ and $dim(Hom_{\mathbb{C}G}(W, V))$ are equal to the number of terms U_i with $U_i \cong W$.

Proof: By the Corollary, we have

$$\begin{aligned} dim(Hom_{\mathbb{C}G}(V, W)) &= \sum_{i=1}^{r} dim(Hom_{\mathbb{C}G}(U_i, W)), \\ dim(Hom_{\mathbb{C}G}(W, V)) &= \sum_{i=1}^{r} dim(Hom_{\mathbb{C}G}(W, U_i)); \end{aligned}$$

we have

$$dim(Hom_{\mathbb{C}G}(U_i, W)) = dim(Hom_{\mathbb{C}G}(W, U_i)) = 1, \text{ if } U_i \cong W; 0 \text{ if } U_i \ncong W.$$

The result follows.

Theorem 13: Let V be a $\mathbb{C}G$-module, and write $V = U_1 \oplus \cdots \oplus U_r$ where each U_i is an irreducible $\mathbb{C}G$-submodule of V. If U is any irreducible $\mathbb{C}G$-submodule of V, then $U \cong U_i$ for some i.

Proof: Given $u \in U$ we may write $u = u_1 + \cdots + u_r$ for unique vectors $u_i \in U_i$. Define $\pi_i : U \to U_i$ by $\pi_i(u) = u_i$ for $1 \leq i \leq r$; then each π_i is a $\mathbb{C}G$-homomorphism. If we choose i such that $u_i \neq 0$ for some $u \in U$, we have $\pi_i \neq 0$. π_i is a $\mathbb{C}G$-isomorphism, and so $U \cong U_i$.

18.4 Decomposition of $\mathbb{C}G$

Definition: If V is a $\mathbb{C}G$-module and U is an irreducible $\mathbb{C}G$-module, we say that U is a *composition factor* of V if V has a $\mathbb{C}G$-submodule which is isomorphic to U.

Definition: Two $\mathbb{C}G$-modules V and W are said to have a *common composition factor* if there is an irreducible $\mathbb{C}G$-module which is a composition factor of both V and W.

Theorem 14: The $\mathbb{C}G$-modules V and W have a common composition factor if and only if $Hom_{\mathbb{C}G}(V, W) \neq \{0\}$.

Proof: Write $V = V_1 \oplus \cdots \oplus V_r$, $W = W_1 \oplus \cdots \oplus W_s$ with each V_i and W_j irreducible. By the corollary, $\dim(Hom_{\mathbb{C}G}(V, W)) = \sum \sum \dim(Hom_{\mathbb{C}G}(V_i, W_j))$, and, $\dim(Hom_{\mathbb{C}G}(V_i, W_j))$ is 1 if $V_i \cong W_j$, and 0 if $V_i \ncong W_j$. Thus $Hom_{\mathbb{C}G}(V, W) \neq \{0\}$ if and only if some V_i is isomorphic to some W_j.

Definition: The vector space $\mathbb{C}G$, with multiplication defined by

$$\left(\sum_{g\in G}\lambda_g g\right)\left(\sum_{h\in G}\mu_h h\right)=\sum_{g,h\in G}\lambda_g\mu_h(gh) \qquad \text{for all } \lambda_g,\mu_h\in\mathbb{C},$$

is called the *group algebra* of G.

Theorem 15: For all $r,s,t\in\mathbb{C}G$ and $\lambda\in\mathbb{C}$, we have the following:

(i) $rs\in\mathbb{C}G$;

(ii) $r(st)=(rs)t$;

(iii) $r1=1r=r$;

(iv) $(\lambda r)s=\lambda(rs)=r(\lambda s)$;

(v) $r(s+t)=rs+rt$;

(vi) $(r+s)t=rt+st$;

(vii) $r0=0r=0$.

Proof: We prove (ii). Let

$$r=\sum_{g\in G}\lambda_g g, \qquad s=\sum_{h\in G}\mu_h h, \qquad t=\sum_{k\in G}\nu_k k,$$

where $\lambda_g,\mu_h,\nu_k\in\mathbb{C}$ for all $g,h,k\in G$; then

$$(rs)t=\sum_{g,h,k\in G}\lambda_g\mu_h\nu_k(gh)k=\sum_{g,h,k\in G}\lambda_g\mu_h\nu_k g(hk)=r(st).$$

Definition: We now define a $\mathbb{C}G$-module using the group algebra. Let $V=\mathbb{C}G$, so that V is a vector space of dimension $n=|G|$ over $\mathbb{C}$. Given $g\in G$, we may regard g as an element of $\mathbb{C}G$, and so may form the product gv for any $v\in V$; by properties (i), (ii), (iii), (iv) and (v) of an earlier result, for all $g,h\in G$, $\lambda\in\mathbb{C}$ and $u,v\in V$ we have

$$gv\in V, \quad (gh)v=g(hv), \quad 1v=v, \quad g(\lambda v)=\lambda gv, \quad g(u+v)=gu+gv.$$

Thus V is a $\mathbb{C}G$-module. The $\mathbb{C}G$-module $\mathbb{C}G$ is called the *regular* $\mathbb{C}G$-module. The corresponding representation $g\mapsto[g]_{\mathcal{B}}$, where $\mathcal{B}$ is the natural basis of $\mathbb{C}G$, is called the *regular representation* of G. Note that the regular $\mathbb{C}G$-module has dimension $|G|$.

Theorem 16: The regular $\mathbb{C}G$-module is faithful.

Proof: If $g\in G$ with $gv=v$ for all $v\in\mathbb{C}G$, then $g1=1$, and so $g=1$; thus $\mathbb{C}G$ is faithful.

Theorem 17: If V is a $\mathbb{C}G$-module, the following properties hold for all $r,s\in\mathbb{C}G$, $\lambda\in\mathbb{C}$ and $u,v\in V$:

(i) $rv\in V$;

(ii) $(rs)v=r(sv)$;

(iii) $1v = v$;

(iv) $r(\lambda v) = \lambda(rv) = (\lambda r)v$;

(v) $r(u+v) = ru + rv$;

(vi) $(r+s)v = rv + sv$;

(vii) $r0 = 0v = 0$.

Proof: We prove only (ii), leaving the rest as easy exercises (some of whose results we shall assume). Let $r, s \in \mathbb{C}G$ and $v \in V$, and set

$$r = \sum_{g \in G} \lambda_g g, \qquad s = \sum_{h \in G} \mu_h h \qquad \text{with } \lambda_g, \mu_h \in \mathbb{C} \text{ for all } g, h \in G.$$

We then have

$$\begin{aligned}
(rs)v &= \left(\sum_{g,h} \lambda_g \mu_h (gh) \right) v \qquad \text{by definition of the multiplication in } \mathbb{C}G \\
&= \sum_{g,h} \lambda_g \mu_h ((gh)v) \qquad \text{by (iv) and (vi)} \\
&= \sum_{g,h} \lambda_g \mu_h (g(hv)) \qquad \text{by definition of a } \mathbb{C}G\text{-module} \\
&= \left(\sum_{g} \lambda_g g \right) \left(\sum_{h} \mu_h (hv) \right) \qquad \text{by (iv), (v) and (vi)} \\
&= r(sv) \qquad \text{by (iv) and (vi)}
\end{aligned}$$

as required.

Theorem 18: Write the regular $\mathbb{C}G$-module as

$$\mathbb{C}G = U_1 \oplus \cdots \oplus U_r,$$

a direct sum of irreducible $\mathbb{C}G$-submodules; then any irreducible $\mathbb{C}G$-module is isomorphic to one of the U_i.

Proof: Let W be an irreducible $\mathbb{C}G$-module, and choose a non-zero vector $w \in W$. Define $\theta : \mathbb{C}G \to W$ by

$$\theta(r) = rw \qquad \text{for all } r \in \mathbb{C}G;$$

then clearly θ is a linear map. For all $g \in G$ and $r \in \mathbb{C}G$ we have

$$\theta(gr) = (gr)w = g(rw) = g\theta(r);$$

thus θ is a $\mathbb{C}G$-homomorphism. We know that $im(\theta)$ is a $\mathbb{C}G$-submodule of W; since $0 \neq w = 1w = \theta(1) \in im(\theta)$ and W is irreducible, we must have $im(\theta) = W$. There is a $\mathbb{C}G$-submodule U of $\mathbb{C}G$ with

$$\mathbb{C}G = ker(\theta) \oplus U \qquad \text{and} \qquad U \cong im(\theta) = W.$$

We have $U \cong U_i$ for some i, and so it follows that $W \cong U_i$ as required.

Corollary: Up to isomorphism, there are only finitely many irreducible $\mathbb{C}G$-modules.

Proof: Follows immediately from previous result.

Theorem 19: If U is a $\mathbb{C}G$-module, then $dim(Hom_{\mathbb{C}G}(\mathbb{C}G, U)) = dim(U)$.

Proof: Let $dim(U) = d$, and choose a basis $u_1, \ldots, u_d$ of U. For $1 \leq i \leq d$ define $\phi_i : \mathbb{C}G \to U$ by $\phi_i(r) = ru_i$ for all $r \in \mathbb{C}G$. Clearly each ϕ_i is a linear map, and for all $g \in G$ and $r \in \mathbb{C}G$ we have

$$\phi_i(gr) = (gr)u_i = g(ru_i) = g\phi_i(r),$$

so that $\phi_i \in Hom_{\mathbb{C}G}(\mathbb{C}G, U)$. We shall prove that $\phi_1, \ldots, \phi_d$ is a basis of $Hom_{\mathbb{C}G}(\mathbb{C}G, U)$. Given $\phi \in Hom_{\mathbb{C}G}(\mathbb{C}G, U)$, write $\phi(1) = \lambda_1 u_1 + \cdots + \lambda_d u_d$ for some $\lambda_i \in \mathbb{C}$. For all $r \in \mathbb{C}G$ we then have

$$\begin{aligned}\phi(r) &= \phi(r1) = r\phi(1) = r\lambda_1 u_1 + \cdots + r\lambda_d u_d = \lambda_1\phi_1(r) + \cdots + \lambda_d\phi_d(r) \\ &= (\lambda_1\phi_1 + \cdots + \lambda_d\phi_d)(r);\end{aligned}$$

thus $\phi = \lambda_1\phi_1 + \cdots + \lambda_d\phi_d$. Hence $\phi_1, \ldots, \phi_d$ span $Hom_{\mathbb{C}G}(\mathbb{C}G, U)$. Now if $\lambda_1\phi_1 + \cdots + \lambda_d\phi_d = 0$ for some $\lambda_i \in \mathbb{C}$, we have

$$0 = (\lambda_1\phi_1 + \cdots + \lambda_d\phi_d)(1) = \lambda_1 u_1 + \cdots + \lambda_d u_d,$$

so $\lambda_i = 0$ for all i. Thus $\phi_1, \ldots, \phi_d$ is a basis of $Hom_{\mathbb{C}G}(\mathbb{C}G, U)$; it follows that $dim(Hom_{\mathbb{C}G}(\mathbb{C}G, U)) = d$.

Theorem 20: Suppose that $\mathbb{C}G = U_1 \oplus \cdots \oplus U_r$ is a direct sum of irreducible $\mathbb{C}G$-submodules. If U is any irreducible $\mathbb{C}G$-module, then the number of terms U_i isomorphic to U is equal to $dim(U)$.

Proof: $dim(U) = dim(Hom_{\mathbb{C}G}(\mathbb{C}G, U))$, and by the last theorem, this is equal to the number of terms U_i with $U_i \cong U$.

Definition: If $V_1, \ldots, V_k$ are irreducible $\mathbb{C}G$-modules such that no two are isomorphic and any irreducible $\mathbb{C}G$-module is isomorphic to some V_i, we say that the V_i form a *complete set of non-isomorphic irreducible $\mathbb{C}G$-modules*.

Theorem 21: If $V_1, \ldots, V_k$ form a complete set of non-isomorphic irreducible $\mathbb{C}G$-modules, then

$$\sum_{i=1}^{k} (dim V_i)^2 = |G|.$$

Proof: Let $\mathbb{C}G = U_1 \oplus \cdots \oplus U_r$, a direct sum of irreducible $\mathbb{C}G$-modules; set $dim(V_i) = d_i$ for $1 \leq i \leq k$. For each i the number of terms U_j isomorphic to V_i is equal to d_i. Thus

$$dim(\mathbb{C}G) = dim(U_1) + \cdots + dim(U_r) = \sum_{i=1}^{k} d_i(dim(V_i)) = \sum_{i=1}^{k} {d_i}^2.$$

As $dim(\mathbb{C}G) = |G|$, the result follows.

Theorem 22: $dim(Hom_{\mathbb{C}G}(U_1 \oplus \ldots \oplus U_r, W_1 \oplus \ldots \oplus W_s)) = \sum_{i=1,j=1}^{r,s} dim(Hom_{\mathbb{C}G}(V_i, W_j))$. Suppose U is an irreducible $\mathbb{C}G$-module then $dim(Hom_{\mathbb{C}G}(\mathbb{C}G, U)) = dim(U)$.

Proof: Let $d = dim(U)$ and $u_1, u_2, \ldots, u_d$ be a basis for U. Define $r\phi_i = u_i r$. The ϕ_i are a basis for $Hom_{\mathbb{C}G}(\mathbb{C}G, U)$.

Theorem 23: Let V be an $\mathbb{C}G$ module, $V = U_1 \oplus U_2 \oplus \ldots \oplus U_r$ with U_i irreducible; (a) if W is an irreducible $\mathbb{C}G$ module then $dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(V, W)) = dim_{\mathbb{C}}(Hom_{\mathbb{C}G}(W, V))$ is the number of $U_i \cong W$; (b) each U_i is a composition factor in the Jordan Holder series.

Proof: $dim(Hom_{\mathbb{C}G}(U_1 \oplus \ldots \oplus U_r, W) \sum_{i=1}^{r} dim(Hom_{\mathbb{C}G}(V_i, W))$. $dim(Hom_{\mathbb{C}G}(V_i, W)) = 1$ when $U_i \cong W$ and is 0 otherwise. So the sum is just the number of $U_i \cong W$ so is the sum where the U_i and W are reversed.

18.5 Representations of Abelian Groups

Theorem 24: If G is abelian, then every irreducible $\mathbb{C}G$-module has dimension 1.

Proof: Let V be an irreducible $\mathbb{C}G$-module, and take any $x \in G$. Because G is abelian, we have

$$x(gv) = g(xv) \qquad \text{for all } g \in G,\ v \in V,$$

and hence the endomorphism $v \mapsto xv$ of V is a $\mathbb{C}G$-homomorphism. This endomorphism must be a scalar multiple of the identity map 1_V, say $\lambda_x 1_V$; thus $xv = \lambda_x v$ for all $v \in V$. Since this is true for all $x \in G$, we see that every subspace of V is a $\mathbb{C}G$-submodule; so as V is irreducible we must have $dim(V) = 1$.

Theorem 25: Let G be the abelian group $C_{n_1} \times \cdots \times C_{n_r}$. There are $|G|$ irreducible representations of G, and any such is of the form $\rho_{\lambda_1,\ldots,\lambda_r}$; no two of these representations are equivalent.

Proof: The above has shown that any irreducible representation of G must be of the form $\rho_{\lambda_1,\ldots,\lambda_r}$; conversely if λ_i is an n_ith root of unity for $1 \leq i \leq r$, the map $\rho : G \to GL_1(\mathbb{C})$ given by

$$\rho({g_1}^{i_1} \ldots {g_r}^{i_r}) = ({\lambda_1}^{i_1} \ldots {\lambda_r}^{i_r})$$

is clearly an irreducible representation. Since there are n_i choices for each λ_i, the number of representations of the form $\rho_{\lambda_1,\ldots,\lambda_r}$ is $n_1 \ldots n_r = |G|$; no two are equivalent, as $T^{-1}AT = A$ for any 1×1 invertible matrices A and T.

Theorem 26: If every irreducible $\mathbb{C}G$-module has dimension 1, then G is abelian.

Proof: Let V be a faithful $\mathbb{C}G$-module. We can write $V = V_1 \oplus \cdots \oplus V_r$ with each V_i irreducible. By assumption, $\dim(V_i) = 1$ for all i; let $V_i = \langle v_i \rangle$, so that $v_1, \ldots, v_r$ is a basis $\mathcal{B}$ of V. Since each V_i is a $\mathbb{C}G$-submodule, we have $gv_i \in V_i$ for all $g \in G$; thus each matrix $[g]_{\mathcal{B}}$ is diagonal. As diagonal matrices commute, for all $g, h \in G$ we have

$$[gh]_{\mathcal{B}} = [g]_{\mathcal{B}}[h]_{\mathcal{B}} = [h]_{\mathcal{B}}[g]_{\mathcal{B}} = [hg]_{\mathcal{B}},$$

and so as the representation is faithful we have $gh = hg$ – so G is abelian.

Note: The above shows that no non-cyclic abelian group has a faithful representation.

18.6 Characters

Definition: Let $\rho : G \to GL_n(\mathbb{C})$ be a representation of G; then the *character* of ρ is the function $\chi : G \to \mathbb{C}$ given by $\chi(g) = Tr(\rho(g))$ for all $g \in G$.

Remark: Clearly the character of a representation ρ of degree n is "simpler" than ρ itself, in that it involves only $|G|$ values rather than $n^2|G|$ matrix entries. Our next result shows that this "loss of detail" means that we fail to distinguish between equivalent representations.

Theorem 27: Equivalent representations of G have the same character.

Proof: Let $\rho, \sigma : G \to GL_n(\mathbb{C})$ be equivalent representations of G; then there is an invertible matrix T such that for all $g \in G$ we have $\sigma(g) = T^{-1}\rho(g)T$. Thus by the corollary, we have $Tr(\sigma(g)) = Tr((T^{-1}\rho(g)T) = Tr(\rho(g))$.

Definition: Let V be a $\mathbb{C}G$-module, with basis $\mathcal{B}$; then the *character* of V is the function $\chi : G \to \mathbb{C}$ given by $\chi(g) = Tr([g]_{\mathcal{B}})$ for all $g \in G$.

Theorem 28: Isomorphic $\mathbb{C}G$-modules have the same character.

Proof: Combine the two previous results.

Definition: A function $\chi : G \to \mathbb{C}$ is called a *character* if it is the character of some $\mathbb{C}G$-module. A character is called *irreducible* if it is the character of an irreducible $\mathbb{C}G$-module, and *reducible* otherwise.

Theorem 29: If χ is the character of a $\mathbb{C}G$-module V, then $\chi(1) = dim(V)$.

Proof: Let $n = dim(V)$; then the matrix $[1]_{\mathcal{B}}$ is the identity matrix I_n, and so we have $\chi(1) = Tr([1]_{\mathcal{B}}) = Tr(I_n) = n$ as required.

Definition: If χ is the character of the $\mathbb{C}G$-module V, the dimension of V is called the *degree* of χ.

Example: (a) $G = D_8 = \langle a, b | a^4 = b^2 = 1, a^b = a^{-1} \rangle$. $\rho(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
(b) $G = D_6 = S_3 = \langle a, b | a^3 = b^2 = 1, a^b = a^{-1} \rangle$. Basis is $v_0 = 1 + a + a^2$, $w_0 = bv_0$, $v_1 = 1 + \omega^2 a + \omega a^2$, $w_1 = bv_1$, $v_2 = 1 + \omega a + \omega^2 a^2$, $w_2 = bv_2$. $sp(v_0, w_0)$ is reducible as $sp(v_0 + w_0) \oplus sp(v_0 - w_0)$. $sp(v_1, w_2) \cong sp(v_2, w_1)$ and they are irreducible. The characters of D_8 have degree 1, 1, 1, 1, and 2. The characters of S_3 have degrees 1, 1 and 2.

Theorem 30: If χ is a character of G, and $g, h \in G$ are conjugate, then $\chi(g) = \chi(h)$.

Proof: If g and h are conjugate, we have $h = x^{-1}gx$ for some $x \in G$; thus if χ is the character of the $\mathbb{C}G$-module V and $\mathcal{B}$ is a basis for V, we have

$$[h]_{\mathcal{B}} = [x^{-1}gx]_{\mathcal{B}} = [x^{-1}]_{\mathcal{B}}[g]_{\mathcal{B}}[x]_{\mathcal{B}} = ([x]_{\mathcal{B}})^{-1}[g]_{\mathcal{B}}[x]_{\mathcal{B}}.$$

By the corollary, we then have $\chi(h) = Tr([h]_{\mathcal{B}}) = Tr([g]_{\mathcal{B}}) = \chi(g)$ as required.

Theorem 31: If V is a $\mathbb{C}G$-module, then for each $g \in G$ there is a basis $\mathcal{B}$ of V such that the matrix $[g]_{\mathcal{B}}$ is diagonal; if g has order m, the diagonal entries of $[g]_{\mathcal{B}}$ are mth roots of unity.

Proof: Given $g \in G$, let $H = \langle g \rangle$; then H is a cyclic subgroup of G. By restricting the multiplication on V to the elements of H, we may consider V as a $\mathbb{C}H$-module. We may write

$$V = U_1 \oplus \cdots \oplus U_n,$$

where each U_j is an irreducible $\mathbb{C}H$-submodule of V. Each U_j has dimension 1; let u_j be a vector spanning U_j. If we set $\omega = e^{2\pi i/m}$, then for all j there is an integer r_j with $gu_j = \omega^{r_j} u_j$. Thus if we let $\mathcal{B}$ be the basis $u_1, \ldots, u_n$ of V, we have $[g]_{\mathcal{B}} = \begin{pmatrix} \omega^{r_1} & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & \omega^{r_n} \end{pmatrix}$ as required.

Example: Let $G = S_3$, and $g = (1\ 2\ 3) \in G$, so that g has order 3; take V to be the permutation module. We have seen that the matrix of g with respect to the natural basis v_1, v_2, v_3 is not diagonal. However, if we write $\omega = e^{2\pi i/3}$ and set

$$w_1 = v_1 + v_2 + v_3, \qquad w_2 = v_1 + \omega^2 v_2 + \omega v_3, \qquad w_3 = v_1 + \omega v_2 + \omega^2 v_3,$$

then w_1, w_2, w_3 is a basis $\mathcal{B}$ of V, and we have

$$[g]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}.$$

Theorem 32: If χ is a character of G of degree n, and $g \in G$ has order m, then:

(i) $\chi(g)$ is a sum of n mth roots of unity;

(ii) $|\chi(g)| \leq n$;

(iii) $\chi(g^{-1}) = \overline{\chi(g)}$;

(iv) if g is conjugate to g^{-1} then $\chi(g) \in \mathbb{R}$.

Proof: Let V be a $\mathbb{C}G$-module having χ as character. There is a basis $\mathcal{B}$ of V such that

$$[g]_{\mathcal{B}} = \begin{pmatrix} \omega_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \omega_n \end{pmatrix}$$

where each ω_j is an mth root of unity; this proves (i). The triangle inequality gives

$$|\chi(g)| = |\omega_1 + \cdots + \omega_n| \leq |\omega_1| + \cdots + |\omega_n| = 1 + \cdots + 1 = n,$$

which proves (ii). Also we have

$$[g^{-1}]_{\mathcal{B}} = \begin{pmatrix} {\omega_1}^{-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & {\omega_n}^{-1} \end{pmatrix},$$

and so $\chi(g^{-1}) = {\omega_1}^{-1} + \cdots + {\omega_n}^{-1}$. As $\overline{\omega} = \omega^{-1}$ for each root of unity ω, we have $\chi(g^{-1}) = \overline{\omega_1} + \cdots + \overline{\omega_n} = \overline{\chi(g)}$, giving (iii). Finally if g is conjugate to g^{-1} then by Theorem 30 we have $\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$; thus $\chi(g) \in \mathbb{R}$, giving (iv).

Corollary: If $g \in G$ has order 2, and χ is a character of G, then $\chi(g) \in \mathbb{Z}$, and $\chi(g) \equiv \chi(1) \pmod 2$.

Proof:

$$\chi(g) = \omega_1 + \cdots + \omega_n,$$

where $n = \chi(1)$ and each ω_j is a square root of unity. Suppose r terms ω_j are equal to -1; then the remaining $n - r$ are equal to 1, and so

$$\chi(g) = (n - r) - r = n - 2r.$$

Hence $\chi(g) \in \mathbb{Z}$, and $\chi(g) \equiv \chi(1) \pmod 2$ as required.

Theorem 33: Let $\rho : G \to GL_n(\mathbb{C})$ be a representation with character χ. Then:

(i) for $g \in G$ we have $|\chi(g)| = \chi(1)$ if and only if $\rho(g) = \lambda I_n$ for some $\lambda \in \mathbb{C}$;

(ii) $ker(\rho) = \{g \in G : \chi(g) = \chi(1)\}$.

Proof:

(i) Let $g \in G$ have order m. If $\rho(g) = \lambda I_n$ with $\lambda \in \mathbb{C}$, then λ is an mth root of unity, and $\chi(g) = n\lambda$; thus $|\chi(g)| = n = \chi(1)$. Conversely, suppose that $|\chi(g)| = \chi(1)$. We know by Theorem 31 that there is a basis $\mathcal{B}$ of $\mathbb{C}^n$ such that

$$[g]_{\mathcal{B}} = \begin{pmatrix} \omega_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \omega_n \end{pmatrix},$$

where each ω_i is an mth root of unity; thus $\chi(g) = \omega_1 + \cdots + \omega_n$. Since by assumption we have

$$|\omega_1 + \cdots + \omega_n| = |\chi(g)| = \chi(1) = n = |\omega_1| + \cdots + |\omega_n|,$$

each term must have the same argument; so $\omega_i = \omega_j$ for all i, j, and thus

$$[g]_{\mathcal{B}} = \begin{pmatrix} \omega_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \omega_1 \end{pmatrix} = \omega_1 I_n.$$

Hence if $\mathcal{B}'$ is any basis of $\mathbb{C}^n$, there is a change of basis matrix T such that $[g]_{\mathcal{B}'} = T^{-1}[g]_{\mathcal{B}}T = T^{-1}\omega_1 I_n T = \omega_1 I_n$; so $\rho(g) = \omega_1 I_n$ as required.

(ii) Clearly if $g \in ker(\rho)$ then $\rho(g) = I_n$ so that $\chi(g) = n = \chi(1)$. Conversely if $g \in G$ satisfies $\chi(g) = \chi(1)$, then by (i) we have $\rho(g) = \lambda I_n$ for some $\lambda \in \mathbb{C}$; hence $\chi(g) = \lambda\chi(1)$, and so $\lambda = 1$, giving $\rho(g) = I_n$ and so $g \in ker(\rho)$ as required.

Example: Let $G = D_8$, and let χ be the character given above, with values as follows.

g	1	a	a^2	a^3	b	ba	ba^2	ba^3
$\chi(g)$	2	0	-2	0	0	0	0	0

Definition: The *kernel* of the character χ of G is the set $ker(\chi) = \{g \in G : \chi(g) = \chi(1)\}$.

Theorem 34: If χ is a character of G then so is $\bar{\chi}$; if χ is irreducible then so is $\bar{\chi}$.

Proof: Let χ be the character of a representation $\rho : G \to GL_n(\mathbb{C})$; thus $\chi(g) = Tr((\rho(g))$ for all $g \in G$. Now given an $n \times n$ matrix $A = (a_{ij})$ over $\mathbb{C}$, we set $\bar{A} = (\overline{a_{ij}})$; then if $A = (a_{ij})$ and $B = (b_{ij})$ are $n \times n$ matrices over $\mathbb{C}$ we have $\overline{AB} = \overline{A}.\overline{B}$, because

$$(\overline{A}.\overline{B})_{ij} = \sum_{k=1}^{n} \bar{a}_{ik}\bar{b}_{kj} = \sum_{k=1}^{n} \overline{a_{ik}b_{kj}} = \overline{\sum_{k=1}^{n} a_{ik}b_{kj}} = (\overline{AB})_{ij}.$$

Thus the function $\bar{\rho} : G \to GL_n(\mathbb{C})$ defined by $\bar{\rho}(g) = \overline{\rho(g)}$ for all $g \in G$ is a representation of G; as

$$Tr((\bar{\rho}(g)) = Tr((\overline{\rho(g)}) = \overline{Tr((\rho(g))} = \overline{\chi(g)} = \bar{\chi}(g) \qquad \text{for all } g \in G,$$

the character of the representation $\bar{\rho}$ is $\bar{\chi}$. Clearly if ρ is reducible then so is $\bar{\rho}$; thus χ is irreducible if and only if $\bar{\chi}$ is.

Theorem 35: If V is a $\mathbb{C}G$-module and we have $V = U_1 \oplus \cdots \oplus U_r$ with the U_i $\mathbb{C}G$-submodules of V, then the character of V is the sum of the characters of the U_i.

Proof: Let $\mathcal{B}_i$ be a basis of U_i for $1 \leq i \leq r$, and amalgamate the bases $\mathcal{B}_i$ to form a basis $\mathcal{B}$ of V; then for all $g \in G$ we have

$$[g]_{\mathcal{B}} = \begin{pmatrix} [g]_{\mathcal{B}_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [g]_{\mathcal{B}_r} \end{pmatrix}.$$

Thus $Tr([g]_{\mathcal{B}}) = Tr([g]_{\mathcal{B}_1}) + \cdots + Tr([g]_{\mathcal{B}_r})$, i.e., the character of V is the sum of those of the U_i as required.

Example: Let $G = S_3$, and V be the permutation module, with character χ. We saw in section 1.4 that $V = U_1 \oplus U_2$, where $U_1 = \langle v_1 + v_2 + v_3 \rangle$ and $U_2 = \langle v_1 - v_2, v_2 - v_3 \rangle$. If we let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the bases $v_1 + v_2 + v_3$ of U_1 and $v_1 - v_2, v_2 - v_3$ of U_2, then the matrices $[g]_{\mathcal{B}_i}$ are as follows.

g	1	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
$[g]_{\mathcal{B}_1}$	(1)	(1)	(1)	(1)	(1)	(1)
$[g]_{\mathcal{B}_2}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$

Thus if we write χ_i for the character of U_i for $i = 1, 2$, the character values are as follows.

g	1	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
$\chi_1(g)$	1	1	1	1	1	1
$\chi_2(g)$	2	0	0	0	-1	-1
$\chi(g)$	3	1	1	1	0	0

By applying this result when each U_i is irreducible, we see that any character is a sum of irreducible ones. As with representations and $\mathbb{C}G$-modules, this concentrates attention on the irreducible characters.

Definition: A character of degree 1 is called a *linear character*.

Examples:

(i) The three irreducible characters of C_3 are all linear.

(ii) Of the three irreducible characters of D_6, the first two are linear but the third is not, since it has degree 2.

Remark: If V is a 1-dimensional $\mathbb{C}G$-module, then for all $g \in G$ there exists $\lambda_g \in \mathbb{C}$ such that $gv = \lambda_g v$ for all $v \in V$; the linear character χ of V is given by $\chi(g) = \lambda_g$ for all $g \in G$. Any irreducible character of an abelian group is linear. Note that a linear character of any group is certainly irreducible; also a linear character is in fact a homomorphism from G to the multiplicative group of non-zero complex numbers. (It is easy to see that the only characters which are homomorphisms in this way are the linear ones: if χ is a character of degree d which is a homomorphism, we must have $\chi(1)\chi(1) = \chi(1)$, i.e., $d^2 = d$, and so $d = 1$.)

Definition: The character of the trivial representation of G is called the *trivial character* of G, and is written 1_G.

Definition: The character χ is called *faithful* if $ker(\chi) = \{1\}$.

Examples:

(i) The irreducible characters of degree 2 of D_6 and D_8 above are both faithful.

(ii) The two linear characters of D_6 are not faithful, since their kernels are D_6 and $\langle a \rangle \cong C_3$ respectively.

Definition: The character of the regular $\mathbb{C}G$-module $\mathbb{C}G$ is called the *regular character* of G, and is written χ_{reg}.

Theorem 36: Let $V_1, \ldots, V_k$ be a complete set of non-isomorphic irreducible $\mathbb{C}G$-modules, and for $1 \leq i \leq k$ let χ_i be the character of V_i and d_i the dimension of V_i; then $\chi_{reg} = d_1\chi_1 + \cdots + d_k\chi_k$.

Proof:

$$\mathbb{C}G = \underbrace{(V_1 \oplus \cdots \oplus V_1)}_{d_1 \text{ terms}} \oplus \cdots \oplus \underbrace{(V_k \oplus \cdots \oplus V_k)}_{d_k \text{ terms}};$$

the result now follows.

Theorem 37: $\chi_{reg}(1) = |G|$, while $\chi_{reg}(g) = 0$ if $1 \neq g \in G$.

Proof: Let $G = \{g_1, \ldots, g_n\}$, and let $\mathcal{B}$ be the natural basis of $\mathbb{C}G$. We have $\chi_{reg}(1) = n = |G|$. Given $1 \neq g \in G$, for all $1 \leq i \leq n$ we have $gg_i = g_j$ for some $j \neq i$; thus the ith column of $[g]_{\mathcal{B}}$ has zero everywhere except in the jth row, and in particular the (i,i)-entry of $[g]_{\mathcal{B}}$ is zero for all i. Thus $\chi_{reg}(g) = Tr([g]_{\mathcal{B}} = 0$ as required.

Example: Consider $G = D_6$. The irreducible characters are χ_1, χ_2 and χ_3, of degrees 1, 1 and 2. Calculating the values of $\chi_1 + \chi_2 + 2\chi_3$, we get:

g	1	a	a^2	b	ba	ba^2
$\chi_1(g)$	1	1	1	1	1	1
$\chi_2(g)$	1	1	1	-1	-1	-1
$\chi_3(g)$	2	-1	-1	0	0	0
$(\chi_1 + \chi_2 + 2\chi_3)(g)$	6	0	0	0	0	0

$\chi_{reg} = \chi_1 + \chi_2 + 2\chi_3$ and χ_{reg} takes the value $|G|$ at the element 1 and 0 elsewhere.

Definition: If G is a subgroup of S_n, the character of the permutation module for G is called the *permutation character* of G.

Theorem 38: If G is a subgroup of S_n, the function $\nu : G \to \mathbb{C}$ defined by $\nu(g) = |Fix(g)| - 1$ is a character of G.

Proof: Let V be the permutation module for G, and let $v_1, \ldots, v_n$ be the natural basis of V; set $u = v_1 + \cdots + v_n$, and let U be the 1-dimensional subspace of V spanned by u. Since $gu = u$ for all $g \in G$, we see that U is a trivial $\mathbb{C}G$-submodule of V, with character 1_G. There is a $\mathbb{C}G$-submodule W of V such that $V = U \oplus W$; let ν be the character of W. We have

$$\pi = 1_G + \nu,$$

and so $|Fix(g)| = 1 + \nu(g)$ for all $g \in G$; thus $\nu(g) = |Fix(g)| - 1$ for all $g \in G$.

Example: Let $G = A_4$, a subgroup of S_4; then G has four conjugacy classes, represented by 1, (1 2)(3 4), (1 2 3) and (1 3 2). The values of the character ν are as follows.

g	1	(1 2)(3 4)	(1 2 3)	(1 3 2)
$\nu(g)$	3	-1	0	0

18.7 The space of functions $G \to \mathbb{C}$

Definition: Given $\theta : G \to \mathbb{C}$ and $\phi : G \to \mathbb{C}$, we define

$$\langle \theta, \phi \rangle = \frac{1}{|G|} \sum_{g \in G} \theta(g)\overline{\phi(g)}.$$

Theorem 39: If G has precisely ℓ conjugacy classes $C_1, \ldots, C_\ell$, with representatives $g_1, \ldots, g_\ell$, and χ and ψ are characters of G, then

$$\langle \chi, \psi \rangle = \langle \psi, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}) = \frac{1}{|G|} \sum_{i=1}^{\ell} |C_i| \chi(g_i)\overline{\psi(g_i)} = \sum_{i=1}^{\ell} \frac{\chi(g_i)\overline{\psi(g_i)}}{|C_G(g_i)|} \in \mathbb{R}.$$

Proof: We have five things to prove. First note that because $\overline{\psi(g)} = \psi(g^{-1})$ for all $g \in G$ by Theorem 32 (iii), we have

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}).$$

Because g^{-1} runs through G as g does, we also have

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})\psi(g) = \langle \psi, \chi \rangle.$$

Since $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle = \overline{\langle \chi, \psi \rangle}$, we must have $\langle \chi, \psi \rangle \in \mathbb{R}$. Next, because characters are constant on conjugacy classes, we have

$$\sum_{g \in C_i} \chi(g)\overline{\psi(g)} = |C_i| \chi(g_i)\overline{\psi(g_i)};$$

thus as G is the disjoint union of the conjugacy classes C_i, we have

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \frac{1}{|G|} \sum_{i=1}^{\ell} \sum_{g \in C_i} \chi(g)\overline{\psi(g)} = \frac{1}{|G|} \sum_{i=1}^{\ell} |C_i| \chi(g_i)\overline{\psi(g_i)}.$$

Finally, as $|C_i| = |G|/|C_G(g_i)|$, we have

$$\langle \chi, \psi \rangle = \sum_{i=1}^{\ell} \frac{|C_i|}{|G|} \chi(g_i)\overline{\psi(g_i)} = \sum_{i=1}^{\ell} \frac{1}{|C_G(g_i)|} \chi(g_i)\overline{\psi(g_i)}$$

as required.

Example: Let $G = A_4$ then G has four conjugacy classes, with representatives

$$g_1 = 1, \qquad g_2 = (1\ 2)(3\ 4), \qquad g_3 = (1\ 2\ 3), \qquad g_4 = (1\ 3\ 2).$$

The conjugacy class sizes $|C_i|$ are as follows:

$$\begin{array}{ll} C_G(g_1) = G & |C_1| = |G|/|C_G(g_1)| = 1, \\ C_G(g_2) = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, & |C_2| = |G|/|C_G(g_2)| = 3, \\ C_G(g_3) = \{1, (1\ 2\ 3), (1\ 3\ 2)\}, & |C_3| = |G|/|C_G(g_3)| = 4, \\ C_G(g_4) = \{1, (1\ 3\ 2), (1\ 2\ 3)\}, & |C_4| = |G|/|C_G(g_4)| = 4. \end{array}$$

Let $\omega = e^{2\pi i/3}$, then G has characters χ and ψ and:

g	g_1	g_2	g_3	g_4
$\lvert C_G(g)\rvert$	12	4	3	3
$\lvert C_g\rvert$	1	3	4	4
χ	1	1	ω	ω^2
ψ	4	0	ω^2	ω

Since g_2 has a total of 3 conjugates, and g_3 and g_4 have 4 each, we may calculate

$$\langle \chi, \psi \rangle = \frac{1}{12}(1.4 + 1.0 + 1.0 + 1.0 + \omega.\overline{\omega^2} + \omega.\overline{\omega^2} + \omega.\overline{\omega^2} + \omega.\overline{\omega^2} + \omega^2.\overline{\omega} + \omega^2.\overline{\omega} + \omega^2.\overline{\omega} + \omega^2.\overline{\omega}) = 0;$$

however, it is simpler to compute

$$\langle \chi, \psi \rangle = \sum_{i=1}^{\ell} \frac{\chi(g_i)\overline{\psi(g_i)}}{|C_G(g_i)|} = \frac{1.4}{12} + \frac{1.0}{4} + \frac{\omega.\overline{\omega^2}}{3} + \frac{\omega^2.\overline{\omega}}{3} = 0.$$

Note that we also have

$$\langle \psi, \chi \rangle = \sum_{i=1}^{\ell} \frac{\psi(g_i)\overline{\chi(g_i)}}{|C_G(g_i)|} = \frac{4.1}{12} + \frac{0.1}{4} + \frac{\omega^2.\overline{\omega}}{3} + \frac{\omega.\overline{\omega^2}}{3} = 0,$$

so that $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle \in \mathbb{R}$. Similarly we find that

$$\begin{aligned} \langle \chi, \chi \rangle &= \tfrac{1.1}{12} + \tfrac{1.1}{4} + \tfrac{\omega.\overline{\omega}}{3} + \tfrac{\omega^2.\overline{\omega^2}}{3} = 1, \\ \langle \psi, \psi \rangle &= \tfrac{4.4}{12} + \tfrac{0.0}{4} + \tfrac{\omega^2.\overline{\omega^2}}{3} + \tfrac{\omega.\overline{\omega}}{3} = 2. \end{aligned}$$

Remark: Sometimes it is possible to obtain information about class sizes from knowledge of characters and their inner products. Here it tends to be more convenient to use the inner product formula in the form

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{i=1}^{\ell} c_i \chi(g_i) \overline{\psi(g_i)},$$

where $g_1, \ldots, g_\ell$ are representatives of the conjugacy classes, and $c_i = |C_i|$ for $1 \leq i \leq \ell$.

Theorem 40: If $G \lhd N$ and χ is a character of G/N, define $\tilde{\chi}(g) = \chi(gN)$. $\tilde{\chi}$ is a character of G and is irreducile iff χ is irreducible.

Proof: This follows from the natural homomorphism $G \to G/N$.

18.7.1 Orthonormality

Theorem 41: For all $w_1 \in W_1$ and $w_2 \in W_2$ we have

$$e_1 w_1 = w_1, \qquad e_1 w_2 = 0, \qquad e_2 w_1 = 0, \qquad e_2 w_2 = w_2.$$

Proof: Given $w_2 \in W_2$, the map $\theta : W_1 \to W_2$ defined by $\theta(w_1) = w_1 w_2$ for all $w_1 \in W_1$ is clearly a $\mathbb{C}G$-homomorphism. Since W_1 and W_2 have no common composition factor we have $Hom_{\mathbb{C}G}(W_1, W_2) = \{0\}$, and so $\theta = 0$. Thus $w_1 w_2 = 0$ for all $w_1 \in W_1$ and $w_2 \in W_2$; in particular, $e_1 w_2 = 0$ for all $w_2 \in W_2$. Similarly $e_2 w_1 = 0$ for all $w_1 \in W_1$. Since we then have

$$\begin{aligned} w_1 &= 1w_1 = (e_1 + e_2)w_1 = e_1 w_1 \qquad \text{for all } w_1 \in W_1, \\ w_2 &= 1w_2 = (e_1 + e_2)w_2 = e_2 w_2 \qquad \text{for all } w_2 \in W_2, \end{aligned}$$

the result follows.

Corollary: ${e_1}^2 = e_1$, ${e_2}^2 = e_2$ and $e_1 e_2 = e_2 e_1 = 0$.

Proof: Take $w_1 = e_1$ and $w_2 = e_2$ in the previous result.

Definition: An element e with $e^2 = e$ is called an *idempotent*, from the Latin for "same power".

Theorem 42: If χ is the character of W_1, then

$$e_1 = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g.$$

Proof: Let $x \in G$; then the map $\theta : \mathbb{C}G \to \mathbb{C}G$ given by $\theta(w) = x^{-1} e_1 w$ is linear. We shall calculate the trace of θ (i.e., the trace of the matrix of θ with respect to any basis of $\mathbb{C}G$) in two ways; comparing the two answers will give the result.

First, for any $w_1 \in W_1$ and $w_2 \in W_2$ we have

$$\theta(w_1) = x^{-1} e_1 w_1 = x^{-1} w_1, \qquad \theta(w_2) = x^{-1} e_1 w_2 = 0$$

. Writing elements of $W_1 \oplus W_2$ as ordered pairs (w_1, w_2), we have $\theta(w_1, w_2) = (\theta_1(w_1), \theta_2(w_2))$ where $\theta_1(w_1) = x^{-1}w_1$ and $\theta_2 = 0$. Hence

$$Tr(\theta) = Tr(\theta_1) + Tr(\theta_2) = \chi(x^{-1}).$$

Secondly, write $e_1 = \sum_{g\in G} \lambda_g g$. The endomorphism of $\mathbb{C}G$ which sends any element w to $x^{-1}gw$ has trace $|G|$ if $x^{-1}g = 1$, i.e., if $g = x$, and 0 otherwise. Thus as $\theta(w) = \sum_{g\in G} \lambda_g x^{-1}gw$ for all $w \in \mathbb{C}G$, we see that

$$Tr(\theta) = \lambda_x |G|.$$

Comparing the two expressions gives $\lambda_x = \frac{1}{|G|}\chi(x^{-1})$, and so

$$e_1 = \frac{1}{|G|} \sum_{g\in G} \chi(g^{-1})g.$$

Example: With $G = C_3$ and W_1, e_1 as above, the character χ of W_1 is given by $\chi(1) = 1$, $\chi(a) = \omega$ and $\chi(a^2) = \omega^2$; thus $\frac{1}{|G|}\sum_{g\in G} \chi(g^{-1})g = \frac{1}{3}(1 + \omega^2 a + \omega a^2) = e_1$.

Corollary: If χ is the character of W_1, then $\langle \chi, \chi \rangle = \chi(1)$.

Proof: We calculate the coefficient of the basis element 1 in ${e_1}^2$. We have

$${e_1}^2 = \frac{1}{|G|^2} \sum_{g,h\in G} \chi(g^{-1})\chi(h^{-1})gh$$

and so the coefficient of 1 is

$$\frac{1}{|G|^2} \sum_{g\in G} \chi(g^{-1})\chi(g) = \frac{1}{|G|}\langle \chi, \chi \rangle.$$

On the other hand, we have ${e_1}^2 = e_1$ and again the coefficient of 1 in e_1 is $\frac{1}{|G|}\chi(1)$. Thus $\langle \chi, \chi \rangle = \chi(1)$ as required.

Theorem 43: Let U and V be non-isomorphic irreducible $\mathbb{C}G$-modules, with characters χ and ψ; then $\langle \chi, \chi \rangle = 1$ and $\langle \chi, \psi \rangle = 0$.

Proof: We know that $\mathbb{C}G = U_1 \oplus \cdots \oplus U_r$ with the U_i irreducible $\mathbb{C}G$-submodules of $\mathbb{C}G$; let $dim(U) = m$ and $dim(V) = n$, so there are precisely m terms U_i which are isomorphic to U and n which are isomorphic to V. We shall apply the corollary to two different decompositions $\mathbb{C}G = W_1 \oplus W_2$ in which W_1 and W_2 have no common composition factor.

First, let W_1 be the sum of the U_i which are isomorphic to U, and W_2 be the sum of the rest. The character of W_1 is $m\chi$, since W_1 is the direct sum of m $\mathbb{C}G$-submodules each having character χ. Thus by the corollary, we have

$$m\chi(1) = \langle m\chi, m\chi \rangle = m^2 \langle \chi, \chi \rangle;$$

since $\chi(1) = dim(U) = m$ we have $\langle \chi, \chi \rangle = 1$.

Next, let W_1 be the sum of the U_i which are isomorphic to either U or V, and W_2 be the sum of the rest. The character of W_1 is $m\chi + n\psi$. The corollary gives

$$m\chi(1) + n\psi(1) = \langle m\chi + n\psi, m\chi + n\psi\rangle = m^2\langle\chi,\chi\rangle + n^2\langle\psi,\psi\rangle + mn(\langle\chi,\psi\rangle + \langle\psi,\chi\rangle).$$

Since $\langle\chi,\chi\rangle = \langle\psi,\psi\rangle = 1$ by the above, and $\chi(1) = m$ and $\psi(1) = n$, we have

$$\langle\chi,\psi\rangle + \langle\psi,\chi\rangle = 0;$$

as $\langle\chi,\psi\rangle = \langle\psi,\chi\rangle$, we must have $\langle\chi,\psi\rangle = 0$.

Example: Let $G = D_6$, so that the irreducible characters χ_1, χ_2, χ_3 are as follows.

g	1	a	b
$\lvert C_G(g)\rvert$	6	3	2
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

Thus we have

$$\begin{array}{ll} \langle\chi_1,\chi_1\rangle = \frac{1.1}{6} + \frac{1.1}{3} + \frac{1.1}{2} = 1, & \langle\chi_1,\chi_2\rangle = \frac{1.1}{6} + \frac{1.1}{3} + \frac{1.(-1)}{2} = 0, \\ \langle\chi_2,\chi_2\rangle = \frac{1.1}{6} + \frac{1.1}{3} + \frac{(-1).(-1)}{2} = 1, & \langle\chi_1,\chi_3\rangle = \frac{1.2}{6} + \frac{1.(-1)}{3} + \frac{1.0}{2} = 0, \\ \langle\chi_3,\chi_3\rangle = \frac{2.2}{6} + \frac{(-1).(-1)}{3} + \frac{0.0}{2} = 1, & \langle\chi_2,\chi_3\rangle = \frac{1.2}{6} + \frac{1.(-1)}{3} + \frac{(-1).0}{2} = 0. \end{array}$$

Theorem 44: If χ is any character of G, then $\chi = d_1\chi_1 + \cdots + d_k\chi_k$ for some non-negative integers $d_1, \ldots, d_k$; moreover $d_i = \langle\chi,\chi_i\rangle$ for $1 \le i \le k$, and $\langle\chi,\chi\rangle = \sum_{i=1}^{k} {d_i}^2$.

Proof: Let V be a $\mathbb{C}G$-module with character χ. V is a direct sum of irreducible $\mathbb{C}G$-submodules, each of which is isomorphic to some V_i; thus there exist non-negative integers $d_1, \ldots, d_k$ such that

$$V \cong \underbrace{(V_1 \oplus \cdots \oplus V_1)}_{d_1 \text{ terms}} \oplus \cdots \oplus \underbrace{(V_k \oplus \cdots \oplus V_k)}_{d_k \text{ terms}}.$$

Thus the character χ is given by $\chi = d_1\chi_1 + \cdots + d_k\chi_k$. Taking inner products now gives

$$\langle\chi,\chi_i\rangle = \langle d_1\chi_1 + \cdots + d_k\chi_k, \chi_i\rangle = \sum_{j=1}^{k} d_j\langle\chi_j,\chi_i\rangle = d_i,$$

$$\langle\chi,\chi\rangle = \langle d_1\chi_1 + \cdots + d_k\chi_k, d_1\chi_1 + \cdots + d_k\chi_k\rangle = \sum_{i=1}^{k}\sum_{j=1}^{k} d_i d_j\langle\chi_i,\chi_j\rangle = \sum_{i=1}^{k} {d_i}^2$$

as required.

Remark: Thus if we are given any character χ, we can write it as a linear combination of the irreducible characters, and the coefficients can be found simply by calculating inner products. This result motivates the following definition.

Burnside's Algorithm: Let the conjugacy classes of a finite group G be $C_1, C_2, \ldots, C_r$. $C_iC_j = \sum_{s=1}^{r} c_{ijs}C_s$. Thus $(\frac{|C_i|\chi_k(g_i)}{\chi_k(1)})(\frac{|C_j|\chi_k(g_j)}{\chi_k(1)}) = \sum_{s=1}^{r} c_{ijs}(\frac{|C_s|\chi_k(g_s)}{\chi_k(1)})$. Multiply this equation by a_{ki} and sum over i to get:

$(\sum_{i=1}^{r} a_{ki}\frac{|C_i|\chi_k(g_i)}{\chi_k(1)})(\frac{|C_j|\chi_k(g_j)}{\chi_k(1)}) = \sum_{s=1}^{r}(\sum_{i=1}^{r} a_{ki}c_{ijs})\frac{|C_s|\chi_k(g_s)}{\chi_k(1)}$ Put $Y_{ki} = \frac{|C_i|\chi_k(g_i)}{\chi_k(1)}$, $A_k = \sum_{i=1}^{r} a_{ki}Y_{ki}$ and $B_{js}^{(k)} = \sum_{i=1}^{r} c_{ijs}a_{ki}$, for $k = 1, 2, \ldots, r$. Then,

$$\begin{pmatrix} B_{11}^{(k)} & \ldots & B_{1r}^{(k)} \\ \ldots & \ldots & \ldots \\ B_{r1}^{(k)} & \ldots & B_{rr}^{(k)} \end{pmatrix} \begin{pmatrix} Y_{k1} \\ Y_{k2} \\ \ldots \\ Y_{kr} \end{pmatrix} = A_k \begin{pmatrix} Y_{k1} \\ Y_{k2} \\ \ldots \\ Y_{kr} \end{pmatrix}$$

So, we can solve for the Y_{kj} by computing the eigenvalues of $det(B_{is}^{(k)} - \lambda I)$ and finding the corresponding eigenvectors.

Example, S_3:

Let $C_1 = (1)$, $C_2 = (123) + (132)$ and $C_3 = (12) + (13) + (23)$. $C_1C_1 = C_1$, $C_1C_2 = C_2C_1 = C_2$, $C_1C_3 = C_3C_1 = C_3$, $C_2C_3 = C_3C_2 = 2C_3$, $C_2C_2 = C_2C_2 = 2C_1 + C_2$, and $C_3C_3 = C_3C_3 = 3C_1 + 3C_3$. The matricies $m_1 = (C_{1ij})$, $m_2 = (C_{2ij})$, and $m_3 = (C_{3ij})$ are:

$$m_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$m_2 = \begin{pmatrix} 0 & 1 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$m_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 2 \\ 3 & 3 & 0 \end{pmatrix}$$

S_3 character table is $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -1 & 0 \end{pmatrix}$

This is computed as follows: The eigenvalues of the respective matrix are 1; $2, 1, -1$; and $3, -3, 0$. The respective eigenvectors are $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$; $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$, and, $\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$; and, finally, $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}$.

Consider three of the eigenvalues $\begin{pmatrix} \frac{|C_1|\chi_1(1)}{\chi_1(1)} \\ \frac{|C_2|\chi_1((123))}{\chi_1(1)} \\ \frac{|C_3|\chi_1((12))}{\chi_1(1)} \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $\begin{pmatrix} \frac{|C_1|\chi_2(1)}{\chi_2(1)} \\ \frac{|C_2|\chi_2((123))}{\chi_2(1)} \\ \frac{|C_3|\chi_2((12))}{\chi_2(1)} \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}$, and, $\begin{pmatrix} \frac{|C_1|\chi_3(1)}{\chi_3(1)} \\ \frac{|C_2|\chi_3((123))}{\chi_3(1)} \\ \frac{|C_3|\chi_3((12))}{\chi_3(1)} \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$. Remembering $|C_1| = 1$, $|C_2| = 2$, and $|C_3| = 3$, we can solve for the $\chi_k(g_i)$ giving the character table entries.

Definition: If χ is a character of G and we write $\chi = d_1\chi_1 + \cdots + d_k\chi_k$, then we call the irreducible character χ_i a *constituent* of χ if the coefficient d_i is non-zero. Thus χ_i is a constituent of χ if and only if $\langle \chi, \chi_i \rangle > 0$.

Theorem 45: If V is a $\mathbb{C}G$-module with character χ, then V is irreducible if and only if $\langle \chi, \chi \rangle = 1$.

Proof: If V is irreducible, then $\langle \chi, \chi \rangle = 1$. Conversely, assume that $\langle \chi, \chi \rangle = 1$; write

$$V \cong \underbrace{(V_1 \oplus \cdots \oplus V_1)}_{d_1 \text{ terms}} \oplus \cdots \oplus \underbrace{(V_k \oplus \cdots \oplus V_k)}_{d_k \text{ terms}},$$

so that $\chi = d_1\chi_1 + \cdots + d_k\chi_k$, and then we have

$$1 = \langle \chi, \chi \rangle = {d_1}^2 + \cdots + {d_k}^2.$$

As the d_i are non-negative integers, one (say d_j) must be 1 and the remainder 0; then $V \cong V_j$ and so V is irreducible.

Theorem 46: If V and W are $\mathbb{C}G$-modules, with characters χ and ψ respectively, then $V \cong W$ if and only if $\chi = \psi$.

Proof: We know that if $V \cong W$ then $\chi = \psi$; it is the converse which we must show. Thus we assume that $\chi = \psi$, and seek to show that $V \cong W$. There are non-negative integers $c_1, \ldots, c_k$ such that

$$V \cong \underbrace{(V_1 \oplus \cdots \oplus V_1)}_{c_1 \text{ terms}} \oplus \cdots \oplus \underbrace{(V_k \oplus \cdots \oplus V_k)}_{c_k \text{ terms}},$$

and similarly $d_1, \ldots, d_k$ such that

$$W \cong \underbrace{(V_1 \oplus \cdots \oplus V_1)}_{d_1 \text{ terms}} \oplus \cdots \oplus \underbrace{(V_k \oplus \cdots \oplus V_k)}_{d_k \text{ terms}}.$$

Since $\chi = \psi$, for $1 \leq i \leq k$ we have

$$c_i = \langle \chi, \chi_i \rangle = \langle \psi, \chi_i \rangle = d_i,$$

and so $V \cong W$ as required.

Theorem 47: The irreducible characters $\chi_1, \ldots, \chi_k$ are linearly independent vectors in the vector space of functions $G \to \mathbb{C}$.

Proof: Assume that $\lambda_1, \ldots, \lambda_k \in \mathbb{C}$ with

$$\lambda_1\chi_1 + \ldots + \lambda_k\chi_k = 0.$$

Taking inner products with χ_i gives

$$0 = \langle \lambda_1\chi_1 + \ldots + \lambda_k\chi_k, \chi_i \rangle = \lambda_i;$$

since this is true for all $1 \leq i \leq k$, we see that the χ_i are linearly independent.

Theorem 48: If V and W are $\mathbb{C}G$-modules with characters χ and ψ, then we have $dim(Hom_{\mathbb{C}G}(V, W)) = \langle \chi, \psi \rangle$.

Proof: As before there exist non-negative integers $c_1, \ldots, c_k$ and $d_1, \ldots, d_k$ such that

$$V \cong \underbrace{(V_1 \oplus \cdots \oplus V_1)}_{c_1 \text{ terms}} \oplus \cdots \oplus \underbrace{(V_k \oplus \cdots \oplus V_k)}_{c_k \text{ terms}},$$
$$W \cong \underbrace{(V_1 \oplus \cdots \oplus V_1)}_{d_1 \text{ terms}} \oplus \cdots \oplus \underbrace{(V_k \oplus \cdots \oplus V_k)}_{d_k \text{ terms}}.$$

So

$$\begin{aligned} dim(Hom_{\mathbb{C}G}(V,W)) &= \sum_{i=1}^{k}\sum_{j=1}^{k} c_i d_j dim(Hom_{\mathbb{C}G}(V_i,V_j)) \\ &= \sum_{i=1}^{k}\sum_{j=1}^{k} c_i d_j \delta_{ij} = \sum_{i=1}^{k} c_i d_i. \end{aligned}$$

On the other hand, we have $\chi = \sum_{i=1}^{k} c_i \chi_i$ and $\psi = \sum_{j=1}^{k} d_j \chi_j$, and so

$$\langle \chi, \psi \rangle = \sum_{i=1}^{k}\sum_{j=1}^{k} c_i d_j \langle \chi_i, \chi_j \rangle = \sum_{i=1}^{k}\sum_{j=1}^{k} c_i d_j \delta_{ij} = \sum_{i=1}^{k} c_i d_i.$$

The result follows.

18.7.2 Center of the group algebra

Definition: The *center* of the group algebra $\mathbb{C}G$ is the subspace

$$\mathbb{Z}(\mathbb{C}G) = \{z \in \mathbb{C}G : zr = rz \text{ for all } r \in \mathbb{C}G\}.$$

Definition: Let $C_1, \ldots, C_\ell$ be the distinct conjugacy classes of G, and for $1 \leq i \leq \ell$ define

$$\bar{C}_i = \sum_{g \in C_i} g \in \mathbb{C}G;$$

the elements $\bar{C}_1, \ldots, \bar{C}_\ell$ of $\mathbb{C}G$ are called the *class sums*.

Theorem 49: The class sums $\bar{C}_1, \ldots, \bar{C}_\ell$ form a basis of $\mathbb{Z}(\mathbb{C}G)$.

Proof: We first show that each $\bar{C}_i$ lies in $\mathbb{Z}(\mathbb{C}G)$. Let $g \in C_i$, and set $|C_i| = r$; write

$$C_i = \{{y_1}^{-1} g y_1, {y_2}^{-1} g y_2, \ldots, {y_r}^{-1} g y_r\}$$

for some $y_1, \ldots, y_r \in G$, so that $\bar{C}_i = \sum_{j=1}^{r} {y_j}^{-1} g y_j$. For all $h \in G$, we have

$$h^{-1} \bar{C}_i h = \sum_{j=1}^{r} h^{-1} {y_j}^{-1} g y_j h = \sum_{j=1}^{r} (y_j h)^{-1} g (y_j h).$$

This is a sum of r conjugates of g; and they are distinct, since

$$h^{-1}{y_j}^{-1}gy_jh = h^{-1}{y_k}^{-1}gy_kh \iff {y_j}^{-1}gy_j = {y_k}^{-1}gy_k.$$

Thus $h^{-1}\bar{C}_ih = \bar{C}_i$, and so $\bar{C}_ih = h\bar{C}_i$; since this is true for all $h \in G$, we see that $\bar{C}_i$ commutes with all $r \in \mathbb{C}G$, i.e., $\bar{C}_i \in \mathbb{Z}(\mathbb{C}G)$.

Now for $1 \leq i \leq \ell$ let g_i be a representative of C_i. It is clear that the $\bar{C}_i$ are linearly independent, since if $\sum_{i=1}^{\ell} \lambda_i\bar{C}_i = 0$ then considering the coefficient of g_i shows that $\lambda_i = 0$ for all i. Thus we must show that the $\bar{C}_i$ span $\mathbb{Z}(\mathbb{C}G)$. Let $z = \sum_{g\in G} \lambda_g g \in \mathbb{Z}(\mathbb{C}G)$. For all $h \in G$ we have $zh = hz$, and so $h^{-1}zh = z$, i.e.,

$$\sum_{g\in G} \lambda_g h^{-1}gh = \sum_{g\in G} \lambda_g g.$$

Since the coefficient of g in the sum on the left is $\lambda_{hgh^{-1}}$, we must have

$$\lambda_{hgh^{-1}} = \lambda_g \qquad \text{for all } g, h \in G;$$

i.e., the coefficients in z of two conjugate elements g and hgh^{-1} are equal. Thus we have $z = \sum_{i=1}^{\ell} \lambda_{g_i}\bar{C}_i$; so the $\bar{C}_i$ do indeed span $\mathbb{Z}(\mathbb{C}G)$ as required.

Examples:

(i) Let $G = S_3$, then a basis of $\mathbb{Z}(\mathbb{C}G)$ is

$$1, \qquad (1\ 2) + (1\ 3) + (2\ 3), \qquad (1\ 2\ 3) + (1\ 3\ 2).$$

(ii) Let $G = D_8$, then a basis of $\mathbb{Z}(\mathbb{C}G)$ is

$$1, \qquad a^2, \qquad a + a^3, \qquad b + ba^2, \qquad ba + ba^3.$$

Theorem 50: If V is an irreducible $\mathbb{C}G$-module and $z \in \mathbb{Z}(\mathbb{C}G)$, then there exists $\lambda \in \mathbb{C}$ such that $zv = \lambda v$ for all $v \in V$.

Proof: For all $r \in \mathbb{C}G$ and $v \in V$, we have

$$z(rv) = r(zv);$$

thus the map $\theta : V \to V$ defined by $\theta(v) = zv$ is a $\mathbb{C}G$-homomorphism. By a previous Lemma (ii), $\theta = \lambda 1_V$ for some $\lambda \in \mathbb{C}$, i.e., $zv = \lambda v$ for all $v \in V$.

Observation: We may now give our second basis of $\mathbb{Z}(\mathbb{C}G)$. Recall that we have the complete set of non-isomorphic irreducible $\mathbb{C}G$-modules $V_1, \ldots, V_k$. We write

$$\mathbb{C}G = W_1 \oplus \cdots \oplus W_k,$$

where each W_i is isomorphic to a direct sum of copies of V_i; the summands W_i are called the *homogeneous components* of $\mathbb{C}G$. We set

$$1 = e_1 + \cdots + e_k,$$

where $e_i \in W_i$ for $1 \leq i \leq k$.

Theorem 51: The elements $e_1, \ldots, e_k$ form a basis of $\mathbb{Z}(\mathbb{C}G)$.

Proof: We begin by showing that each $e_i \in \mathbb{Z}(\mathbb{C}G)$; it clearly suffices to consider the case $i = 1$. If we set $X = W_2 \oplus \cdots \oplus W_k$, we have

$$\mathbb{C}G = W_1 \oplus X,$$

and W_1 and X have no common composition factor; thus, we see that $w_1 x = 0 = x w_1$ for all $w_1 \in W_1$ and $x \in X$. Thus if we set $e = e_2 + \cdots + e_k \in X$, for all $w_1 \in W_1$ we have

$$w_1 = w_1 1 = w_1(e_1 + e) = w_1 e_1 + w_1 e = w_1 e_1.$$

It follows that we have $e_1 w_1 = w_1 = w_1 e_1$ for all $w_1 \in W_1$, and $e_1 x = 0 = x e_1$ for all $x \in X$; since $\mathbb{C}G = W_1 \oplus X$ we see that $e_1 \in \mathbb{Z}(\mathbb{C}G)$ as required.

Now the e_i are certainly linearly independent, as the sum of the W_i is direct. To show that they span $\mathbb{Z}(\mathbb{C}G)$, take $z \in \mathbb{Z}(\mathbb{C}G)$; then for $1 \leq i \leq k$ there exists $\lambda_i \in \mathbb{C}$ such that

$$zv = \lambda_i v \qquad \text{for all } v \in V_i.$$

Hence $zw = \lambda_i w$ for all $w \in W_i$, and in particular $ze_i = \lambda_i e_i$, for $1 \leq i \leq k$; thus

$$z = z1 = z(e_1 + \cdots + e_k) = ze_1 + \cdots + ze_k = \lambda_1 e_1 + \cdots + \lambda_k e_k.$$

Therefore z is a linear combination of the e_i, so $e_1, \ldots, e_k$ do indeed span $\mathbb{Z}(\mathbb{C}G)$; thus they form a basis of $\mathbb{Z}(\mathbb{C}G)$ as required.

Corollary: The number of irreducible characters of G is equal to the number of conjugacy classes of G.

Proof: We have $k = dim(\mathbb{Z}(\mathbb{C}G)) = \ell$.

Example: Let $G = D_6$; we have $\mathbb{C}G = U_1 \oplus U_2 \oplus U_3 \oplus U_4$ with U_1 the trivial $\mathbb{C}G$-module, U_2 the other 1-dimensional $\mathbb{C}G$-module, and $U_3 \cong U_4$ with $dim(U_3) = dim(U_4) = 2$. We therefore have $W_1 = U_1$, $W_2 = U_2$ and $W_3 = U_3 \oplus U_4$; the elements e_i are

$$e_1 = \tfrac{1}{6}(1 + a + a^2 + b + ba + ba^2), \quad e_2 = \tfrac{1}{6}(1 + a + a^2 - b - ba - ba^2), \quad e_3 = \tfrac{1}{3}(2.1 - a - a^2).$$

If we consider e_3, we have

$$e_3 a = \tfrac{1}{3}(2a - a^2 - 1) = a e_3, \qquad e_3 b = \tfrac{1}{3}(2b - ab - a^2 b) = \tfrac{1}{3}(2b - ba^2 - ba) = b e_3;$$

as a and b generate G we see that $e_3 \in \mathbb{Z}(\mathbb{C}G)$.

18.7.3 The space of class functions

Definition: A *class function* on G is a function $\psi : G \to \mathbb{C}$ with the property that $\psi(g) = \psi(h)$ if $g, h \in G$ are conjugate. The set of class functions on G is written cl. It is clear that cl is a subspace of the vector space of all functions $G \to \mathbb{C}$. Moreover, it is easy to provide a basis of cl.

Definition: If C is a conjugacy class of G, the function $\psi_C : G \to \mathbb{C}$ defined by $\psi_C(g) = 1, g \in C$, $\psi_C(g) = 0, g \notin C$ is called the *characteristic function* of the class C.

Example: Let $G = D_6$, and write $C_1 = \{1\}$, $C_2 = \{a, a^2\}$ and $C_3 = \{b, ba, ba^2\}$ as before; then the characteristic functions ψ_{C_i} are as follows.

	1	a	a^2	b	ba	ba^2
ψ_{C_1}	1	0	0	0	0	0
ψ_{C_2}	0	1	1	0	0	0
ψ_{C_3}	0	0	0	1	1	1

Theorem 52: The characteristic functions $\psi_{C_1}, \ldots, \psi_{C_\ell}$ form a basis of cl.

Proof: It is clear that $\psi_{C_i} \in cl$ for $1 \leq i \leq \ell$. If $\lambda_1\psi_{C_1} + \cdots + \lambda_\ell\psi_{C_\ell} = 0$, evaluating at g_j gives $\lambda_j = 0$; as this is true for all $1 \leq j \leq \ell$, the ψ_{C_i} are linearly independent. Given $\psi \in cl$, set $\lambda_i = \psi(g_i)$ for all i; then $\sum_{i=1}^{\ell} \lambda_i\psi_{C_i}$ is a class function agreeing with ψ on all g_i, so it must be equal to it. Thus the ψ_{C_i} span cl; so they form a basis as required.

Example: If $G = D_6$ as above, the class function ψ given by $\psi(1) = 3$, $\psi(a) = \psi(a^2) = 1$ and $\psi(b) = \psi(ba) = \psi(ba^2) = 0$ is equal to $3\psi_{C_1} + \psi_{C_2}$.

Theorem 53: The irreducible characters $\chi_1, \ldots, \chi_k$ form a basis of cl; indeed if ψ is a class function then $\psi = \sum_{i=1}^{k} \lambda_i\chi_i$, where $\lambda_i = \langle\psi, \chi_i\rangle$ for $1 \leq i \leq k$.

Proof: The χ_i are linearly independent, so they span a subspace of cl of dimension k; since $dim(cl) = \ell = k$, they form a basis of cl. Given $\psi \in cl$ we may therefore write $\psi = \sum_{i=1}^{k} \lambda_i\chi_i$ for some $\lambda_i \in \mathbb{C}$; since $\langle\chi_i, \chi_j\rangle = \delta_{ij}$, taking inner products with χ_i gives $\langle\psi, \chi_i\rangle = \lambda_i$ as required.

Corollary: If $g, h \in G$, then g is conjugate to h if and only if $\chi(g) = \chi(h)$ for all characters χ of G.

Proof: If g is conjugate to h then $\chi(g) = \chi(h)$ for all characters χ of G. Conversely, if $\chi(g) = \chi(h)$ for all characters χ, then by the Theorem, we have $\psi(g) = \psi(h)$ for all $\psi \in cl$. In particular, this is true for the characteristic function ψ_C of the class C containing g; thus $\psi_C(h) = \psi_C(g) = 1$, and so $h \in C$, i.e., h lies in the same conjugacy class as g.

Corollary: If $g \in G$, then g is conjugate to g^{-1} if and only if $\chi(g) \in \mathbb{R}$ for all characters χ of G.

Proof: Since $\chi(g) \in \mathbb{R}$ if and only if $\chi(g) = \overline{\chi(g)} = \chi(g^{-1})$, the result follows immediately from the corollary.

18.7.4 Character tables and orthogonality relations

Definition: The $k \times k$ matrix with (i, j)-entry $\chi_i(g_j)$ is called the *character table* of G.

Definition: The relations

$$\sum_{i=1}^{k} \frac{\chi_r(g_i)\overline{\chi_s(g_i)}}{|C_G(g_i)|} = \delta_{rs}$$

are called the *row orthogonality relations* for G.

Definition: The relations

$$\sum_{i=1}^{k} \chi_i(g_r)\overline{\chi_i(g_s)} = \delta_{rs}|C_G(g_r)|$$

are called the *column orthogonality relations* for G.

Theorem 54: The character table for G satisfies the row and column orthogonality relations.

Proof: We already know that the row orthogonality relations hold. For $1 \leq s \leq k$, we may write the characteristic function ψ_{C_s} as a linear combination of $\chi_1, \ldots, \chi_k$; say $\psi_{C_s} = \lambda_1\chi_1 + \cdots + \lambda_k\chi_k$. Taking inner products with χ_i gives

$$\lambda_i = \langle \psi_{C_s}, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \psi_{C_s}(g)\overline{\chi_i(g)}.$$

Now the only elements g for which $\psi_{C_s}(g) \neq 0$ are those lying in the conjugacy class C_s; since there are $|G|/|C_G(g_s)|$ of them, each having $\psi_{C_s}(g) = 1$, we have

$$\lambda_i = \frac{1}{|G|} \sum_{g \in C_s} \psi_{C_s}(g)\overline{\chi_i(g)} = \frac{\overline{\chi_i(g_s)}}{|C_G(g_s)|}.$$

Thus

$$\delta_{rs} = \psi_{C_s}(g_r) = \sum_{i=1}^{k} \lambda_i \chi_i(g_r) = \sum_{i=1}^{k} \frac{\chi_i(g_r)\overline{\chi_i(g_s)}}{|C_G(g_r)|}.$$

Examples:

(i) Let $G = D_6$.

$$\sum_{i=1}^{3} \chi_i(g_1)\overline{\chi_i(g_1)} = 1.1 + 1.1 + 2.2 = 6, \quad \sum_{i=1}^{3} \chi_i(g_1)\overline{\chi_i(g_2)} = 1.1 + 1.1 + 2.(-1) = 0.$$

(ii) Suppose G is a group of order 12 with four conjugacy classes, and we are given the following part of the character table, in which $\omega = e^{2\pi i/3}$.

g	g_1	g_2	g_3	g_4
$\lvert C_G(g)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4				

We use the column orthogonality relations to determine the final row of the table. The entries in the first column are the degrees of the χ_i, so they are all positive integers. The relation with $r = s = 1$ implies that the sum of the squares of these entries is 12, and so $\chi_4(g_1) = 3$. Next, the relation with $r = 1$ and $s = 2$ yields

$$0 = 1.1 + 1.1 + 1.1 + 3\overline{\chi_4(g_2)};$$

so $\chi_4(g_2) = -1$. Similarly, those with $r = 1$ and $s = 3$ or 4 give $\chi_4(g_3) = 0 = \chi_4(g_4)$. Thus the full character table is:

g	g_1	g_2	g_3	g_4
$\lvert C_G(g)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

Theorem 55: If $N \triangleleft G$ and $\tilde{\chi}$ is a character of G/N, then the function $\chi : G \to \mathbb{C}$ defined by $\chi(g) = \tilde{\chi}(gN)$ for all $g \in G$ is a character of G; the characters χ and $\tilde{\chi}$ have the same degree, and χ is irreducible if and only if $\tilde{\chi}$ is.

Proof: Let $\tilde{\rho} : G/N \to GL_n(\mathbb{C})$ be a representation of G/N with character $\tilde{\chi}$. Define a function $\rho : G \to GL_n(\mathbb{C})$ by

$$\rho(g) = \tilde{\rho}(gN) \qquad \text{for all } g \in G;$$

then $\rho(g)\rho(h) = \tilde{\rho}(gN)\tilde{\rho}(hN) = \tilde{\rho}(gN.hN) = \tilde{\rho}(ghN) = \rho(gh)$, so ρ is a homomorphism, i.e., a representation of G. The character χ of ρ is given by

$$\chi(g) = Tr(\rho(g) = Tr((\tilde{\rho}(gN)) = \tilde{\chi}(gN) \qquad \text{for all } g \in G;$$

moreover $\chi(1) = \tilde{\chi}(N)$ so that χ and $\tilde{\chi}$ have the same degree. Finally, let U be a subspace of the vector space $\mathbb{C}^n$; then by definition of ρ we have $\rho(g)u = \tilde{\rho}(gN)u$ for all $g \in G$ and $u \in U$. Thus

$$\begin{aligned} U \text{ is a } \mathbb{C}G\text{-submodule of } \mathbb{C}^n &\iff \rho(g)u \in U \text{ for all } g \in G,\ u \in U \\ &\iff \tilde{\rho}(gN)u \in U \text{ for all } g \in G,\ u \in U \\ &\iff U \text{ is a } \mathbb{C}(G/N)\text{-submodule of } \mathbb{C}^n; \end{aligned}$$

so the representation ρ is reducible if and only if $\tilde{\rho}$ is, and thus χ is irreducible if and only if $\tilde{\chi}$ is.

Definition: If $N \triangleleft G$ and $\tilde{\chi}$ is a character of G/N, then the character χ of G defined by

$$\chi(g) = \tilde{\chi}(gN) \qquad \text{for all } g \in G$$

is called the *lift* of $\tilde{\chi}$ to G.

Example: Let $G = S_4$; then if we write v_{ij} for $v_{\{i,j\}}$, the second permutation module for G has basis $v_{12}, v_{13}, v_{14}, v_{23}, v_{24}, v_{34}$. If we take conjugacy class representatives 1, (1 2), (1 2)(3 4), (1 2 3) and (1 2 3 4), then 1 fixes all six basis elements, (1 2) and (1 2)(3 4) each fix just v_{12} and v_{34}, while (1 2 3) and (1 2 3 4) both fail to fix any basis elements. Thus the values of the second permutation character are as follows.

	1	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3 4)
π_2	6	2	2	0	0

Together with the first permutation character, lifts from the quotient $S_4/A_4 \cong C_2$ and the orthogonality relations, this enables us to obtain the full character table of G.

	1	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3 4)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	1	-1	0	-1
χ_5	3	-1	-1	0	1

We may also define the *third permutation character* of G by considering unordered triples, and so on.

The third method applies when we have a non-trivial linear character of G.

Theorem 56: If χ and λ are characters of G and λ is linear, then the function $\lambda\chi : G \to \mathbb{C}$ defined by $\lambda\chi(g) = \lambda(g)\chi(g)$ for all $g \in G$ is a character of G; if χ is irreducible, so is $\lambda\chi$.

Proof: Let $\rho : G \to GL_n(\mathbb{C})$ be a representation of G with character χ, and define a map $\lambda\rho : G \to GL_n(\mathbb{C})$ by

$$(\lambda\rho)(g) = \lambda(g)\rho(g) \qquad \text{for all } g \in G;$$

thus $(\lambda\rho)(g)$ is the matrix obtained by multiplying $\rho(g)$ by the complex number $\lambda(g)$. For all $g, h \in G$ we have

$$\begin{aligned}(\lambda\rho)(gh) &= \lambda(gh)\rho(gh)\\ &= \lambda(g)\lambda(h)\rho(g)\rho(h)\\ &= \lambda(g)\rho(g)\lambda(h)\rho(h)\\ &= (\lambda\rho)(g)(\lambda\rho)(h),\end{aligned}$$

and so $\lambda\rho$ is a homomorphism, i.e., a representation of G. The trace of the matrix $(\lambda\rho)(g)$ is $\lambda(g)Tr(\rho(g) = \lambda(g)\chi(g)$; thus $\lambda\chi$ is the character of the representation $\lambda\rho$. For irreducibility, we note that for all $g \in G$ the complex number $\lambda(g)$ is a root of unity, and so $\lambda(g)\overline{\lambda(g)} = 1$; thus

$$\langle \lambda\chi, \lambda\chi\rangle = \frac{1}{|G|}\sum_{g\in G} \lambda(g)\chi(g)\overline{\lambda(g)\chi(g)} = \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\chi(g)} = \langle \chi, \chi\rangle,$$

so χ is irreducible if and only if $\lambda\chi$ is.

Examples:

(i) Let $G = S_4$. We obtain a non-trivial linear character of G by lifting from the quotient $S_4/A_4 \cong C_2$; this gives the character χ_2 (which corresponds to the sign homomorphism). If we write $\lambda = \chi_2$, we see that

$$\lambda\chi_1 = \chi_2, \quad \lambda\chi_2 = \chi_1, \quad \lambda\chi_3 = \chi_3, \quad \lambda\chi_4 = \chi_5, \quad \lambda\chi_5 = \chi_4.$$

(ii) Let $G = A_4$, we have two non-trivial linear characters, χ_2 and χ_3. If we set $\lambda = \chi_2$, we have

$$\lambda\chi_1 = \chi_2, \quad \lambda\chi_2 = \chi_3, \quad \lambda\chi_3 = \chi_1, \quad \lambda\chi_4 = \chi_4.$$

Example: Let $G = S_5$; then G has seven conjugacy classes, with representatives

$$1, \quad (1\ 2), \quad (1\ 2)(3\ 4), \quad (1\ 2\ 3), \quad (1\ 2\ 3\ 4), \quad (1\ 2\ 3\ 4\ 5), \quad (1\ 2\ 3)(4\ 5),$$

and centralizer sizes 120, 12, 8, 6, 4, 5 and 6 respectively. We have the trivial character 1_G and we have the normal subgroup A_5 with quotient $S_5/A_5 \cong C_2$, so we may lift the non-trivial irreducible character of C_2 to G to obtain a second linear character λ (which again corresponds to the sign homomorphism). We also have the first and second permutation characters π_1 and π_2; the values of the characters found so far are as follows.

	1	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2 3)(4 5)
1_G	1	1	1	1	1	1	1
λ	1	−1	1	1	−1	1	−1
π_1	5	3	1	2	1	0	0
π_2	10	4	2	1	0	0	1

Of these, 1_G and λ are irreducible, and shall be called χ_1 and χ_2 respectively. We find that $\langle \pi_1, \chi_1\rangle = 1$, and so $\nu_1 = \pi_1 - \chi_1$ is a character; then $\langle \nu_1, \nu_1\rangle = 1$, so that ν_1 is a third irreducible character χ_3. Since $\lambda\nu_1 \neq \nu_1$, we have a fourth irreducible character $\chi_4 = \lambda\nu_1$. We then find that

$$\langle \pi_2, \chi_1\rangle = \langle \pi_2, \chi_3\rangle = 1,$$

and so $\nu_2 = \pi_2 - \chi_1 - \chi_3$ is a character; as $\langle \nu_2, \nu_2 \rangle = 1$, we see that ν_2 is a fifth irreducible character χ_5. Again, $\lambda\nu_2 \neq \nu_2$, so we have a sixth irreducible character $\chi_6 = \lambda\nu_2$. Finally, the seventh irreducible character may be determined using the orthogonality relations; the full character table is as follows.

	1	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3 4)	(1 2 3 4 5)	(1 2 3)(4 5)
χ_1	1	1	1	1	1	1	1
χ_2	1	−1	1	1	−1	1	−1
χ_3	4	2	0	1	0	−1	−1
χ_4	4	−2	0	1	0	−1	1
χ_5	5	1	1	−1	−1	0	1
χ_6	5	−1	1	−1	1	0	−1
χ_7	6	0	−2	0	0	1	0

18.8 Characters and group structure

Observation: The character table determines the normal subgroups and the nilpotent groups. General procedure for calculating characters: (1) Derive a faithful representation, (2) generate group elements, (3) determine conjugacy classes, (4) determine structure constants ($|C_i||C_j| = \sum_k \alpha_{ijk}|C_k|$), (5) get characters from structure constants.

Theorem 57: If χ is an irreducible character, $\chi(1) \mid |G|$

Proof: If g_i is in the i-th conjugacy class, $\frac{|G|}{|C_G(g_i)|}\frac{\chi(g_i)}{\chi(1)}$ and $\overline{\chi(g)}$ are algebraic integers so $\sum_{i=1}^{k} \frac{|G|}{|C_G(g_i)|}\frac{\chi(g_i)}{\chi(1)}\overline{\chi(g)} = \frac{|G|}{\chi(1)}$ is and algebraic integer. Since it is rational, it must be in $\mathbb{Z}$.

Theorem 58: If $G \subseteq S_n$, $\alpha : G \to \mathbb{C}$ by $\alpha(g) = |Fix(g)| - 1$, then α is a character of G. Define $ker(\rho) = \{g : \chi_\rho(g) = \chi_\rho(1)\}$. ρ is faithful iff $ker(\rho) = 1$. $N = \{n : |\chi(n)| = \chi(1)\} \lhd G$.

Proof: This is easy.

Theorem 59: $N \lhd G, \exists \chi_i : \bigcap_{i=1}^{r} ker(\chi_i) = N$. $g \sim h$ iff $\chi(g) = \chi(h), \forall \chi$.

Proof: If g, h are conjugate, it's clear $\chi(g) = \chi(h), \forall \chi$. If $\chi(g) = \chi(h), \forall \chi$, it's also true for any class function. Pick the class function which is 1 in $ccl_G(g)$ and 0 elsewhere and the result follows.

Theorem 60: $ccl_{A_n}(x) = ccl_{S_n}(x)$ otherwise $ccl_{S_n}(x)$ splits into two conjugacy classes in A_n.

Proof: $S_n = A_n \cup A_n(12)$ and the result follows.

Theorem 61: Let $C_i = \sum_{x \in ccl(y)} x$ then the C_i form a basis for $\mathbb{Z}(FG)$. There are $|G/G'|$ inequivalent linear representations (characters) of G.

Proof: If A is abelian, there are $|A|$ inequivalent linear representations (characters) of G by the decomposition results. Each gives rise to an inequivalent linear representation of G/G'. So G/G' has at least $|G/G'|$ inequivalent linear representations.

Theorem 62: $\chi(g)$ is real iff $\chi(g) = \chi(g^{-1}), \forall \chi$. $N \lhd G$ iff $\exists \chi_i, i = 1, \ldots, k$ such that $\bigcap_{i=1}^{k} ker(\chi_i) = N$.

Proof: In $\mathbb{C}$, $\chi(g^{-1}) = \overline{\chi(g)}$.

Theorem 63: G is not simple iff $\exists \chi, g \neq 1 : \chi(g) = \chi(1)$.

Proof: If such a g exists, it is in the kernel of χ.

Theorem 64: G has $|G/G'|$ linear characters. If all irreducible representations of G have dimension 1, G is abelian.

Proof: Every linear character, χ, has $G' \subseteq ker(\chi)$. Further, if $N \lhd G$, $G' \subseteq N$ means G/N is abelian. Further, every linear character of G is a lift of linear character of G/G'.

Theorem 65: Let H be the kernel of θ then (i) $|\theta(g)| \leq \theta(1)$, (ii) $\theta(g) = \theta(1)$, iff $g \in H$, (iii) $|\theta(g)| = \theta(1)$, iff gH is in the center of G/H.

Proof: $\theta(g)$ is the sum of $\theta(1)$ roots of unity showing (i). (ii) is the definition.

Definition: Define $(\theta, \eta) = \frac{1}{|G|} \sum_g \theta(g)\overline{\eta(g)}$.

Theorem 66: If $U = U_1 \otimes ... \otimes U_s$, the number of these similar to U_1 is $\frac{(\theta,\eta)}{(\eta,\eta)}$. $(\theta, \rho_G) = \theta(1)$, $(\chi_i, \chi_j) = \delta_{ij}$, $\sum_g \chi(g) = |G|\delta_{i1}$, $\sum_i \chi_i^2(1) = |G|$. $\omega_i(R_j) = |r_j|\chi_i(g)/\chi_i(1)$, $\omega_t(R_i)\omega_t(R_j) = \sum_s a_{ijs}\omega_t(R_s)$. $\sum_t \chi_t(g_i)\overline{\chi}_t(g_j) = \frac{|G|}{|R_j|}\delta_{ij}$.

Proof: Calculations based on the decomposition theorem.

Theorem 67: The number of conjugacy classes = number of irreducible representations. $\omega_i(R_j)$ is an algebraic integer.

Proof: Each element of the representation affording each ω is an algebraic integer and a character is just field operations of these elements.

18.9 Some applications of character theory

Theorem 70: Suppose χ is a character of a $\mathbb{C}G$-module, V, and $g \in G$ has order m then (1) $\chi(1) = dim(V)$, (2) $\chi(g)$ is a sum of m-th roots of unity, (3) $\chi(g^{-1}) = \overline{\chi(g)}$ and (4) $\chi(g)$ is real iff $g \sim g^{-1}$.

Proof: (a) is trivial. For (b), put the matrix affording χ into Jordan form (maybe by extending the field). Raising the matrix to the n-th power (where $g^n = 1$), we get the identity. The character of g is thus the sum of roots of 1.

Burnside's Lemma: $|\frac{\chi(g)}{\chi(1)}| \leq 1$. If $|\frac{\chi(g)}{\chi(1)}| \neq 1$ it is not an algebraic integer.

Proof: $\chi(g)$ is the sum of $\chi(1)$ roots of unity.

Theorem 71: Let χ be an irreducible character and R a conjugacy class. If $(\chi(1), |R|) = 1$ then either $|\chi(g)| = \chi(1)$ (equivalently, $R \subseteq \mathbb{Z}(\chi)$) or $\chi(g) = 0$.

Proof: $\exists s, t \in \mathbb{Z} : s|R| + t\chi(1) = 1$, so, $s|R|\chi(g) + t\chi(1)\chi(g) = \chi(g)$. $a_1 = \frac{\chi(g)}{\chi(1)}$ is an algebraic integer. Let its conjugates be $a_2, \ldots a_m$. For each a_1, $|a_i| \leq 1$ and $\prod_{i=1}^m |a_i| \leq 1$ is a rational integer so $\prod_{i=1}^m |a_i| = 0$ or $\prod_{i=1}^m |a_i| = 1$. In the former case, $\chi(g) = 0$ and in the latter case, $|\chi(g)| = \chi(1)$.

Theorem 72: Let p be a prime and G a finite group with conjugacy class of size $p^r, r \geq 1$, then G is not a non-abelian simple group.

Proof: Let $g \in R$. Every non-principal irreducible character $\chi_i, i > 1$ of G is faithful. $\sum_{i=2}^{k} \chi_i(1)\chi_i(g) + 1 = 0$ so $\exists i : \chi_i(g)\chi_i(g) \neq 0 \pmod{p}$. Thus $(|R|, \chi_i(1)) = 1$ and since $\chi_i(g) \neq 0$, applying the previous result, we have $g \in \mathbb{Z}(G)$.

Burnside's Theorem: Every group of order $p^a q^b$ is solvable.

Proof: Let G be a minimal counterexample. If G is abelian, the theorem is true. If not, some element of G has a conjugacy class of prime power order. This contradicts the previous result.

Theorem 73: The number of real irreducible characters of G is the number of real conjugacy classes in G,

Proof: Let X be the character table of G. Since $\overline{X}$ is also a matrix of irreducible characters so $PX = \overline{X}$, where P is a permutation matrix. Similarly, $XQ = \overline{X}$ and $Q = X^{-1}PX$. The number of irreducible real characters of G is $tr(X)$ and the number of irreducible conjugacy classes is $tr(Q)$, and the result holds.

Corollary: G has a non-trivial real irreducible character iff G has even order.

Proof: Straightforward.

18.10 Feit's moduleless treatment

Maschke: If $char(F)$ does not divide $|G|$, then F-representations of G are completely reducible. For ϕ irreducible, if $\exists S : \forall g, S\phi(g) = \phi(g)S$ then S is non-singular.

Theorem 74: If $A(g), B(g)$ are k-irreducible then (i) if A is not similar to B, and, $\sum_g a_{is}(g)b_{tj}(g^{-1}) = 0$; or, (ii) A, B are absolutely irreducible and $\sum_g a_{is}(g^{-1})a_{tj}(g) = \frac{|G|}{n}\delta_{ij}\delta_{st}$, where $n \times n$ is the dimension of $(a_{is}(g))$.

Theorem 75: If A^s is absolutely irreducible then $a^s_{ij}(g)$ are linearly independent and $\sum_{s=1}^{k} n_s^2 \leq |G|$.

18.11 Induced Representations and Characters

Theorem 76: Let U be a $\mathbb{C}H$ submodule then the map $\theta(x) = xr, r \in \mathbb{C}G$ is a $\mathbb{C}H$-homomorphism from U into $\mathbb{C}G$. Any $\mathbb{C}H$ homomorphism into $\mathbb{C}G$ can be represented this way.

Proof: The first statement is obvious. If θ is a $\mathbb{C}H$ homomorphism into $\mathbb{C}G$, $\mathbb{C}H = U \oplus W$ for some $\mathbb{C}H$ invariant, W. Define $\varphi(u + w) = \theta(u)$ then $\varphi(u) = \theta(u), u \in U$. If $r = \varphi(1)$, $\varphi(u) = \varphi(u \cdot 1) = u\varphi(1) = ur$.

Definition: If $X \subseteq \mathbb{C}G$, define $X(\mathbb{C}G) = span\{xg, g \in G, x \in X\}$. If $H \leq G$ and U is a $\mathbb{C}H$ module, further define the induced representation $U^G = U(\mathbb{C}G)$.

Theorem 77: If U, V are isomorphic $\mathbb{C}H$ modules, U^G, V^G are isomorphic $\mathbb{C}G$ modules.

Proof: Straightforward.

Theorem 78: If U, V are $\mathbb{C}H$ modules and $U \cap V = \{0\}$, then $U^G \cap V^G = \{0\}$.

Proof: Let $\theta : U \to W$ be a $\mathbb{C}H$-homomorphism. $\exists r \in \mathbb{C}G : \theta(u) = ru$ and $\exists s \in \mathbb{C}G : \theta^{-1}(v) = sv$. If $a \in U^G$, a is a linear combination of the elements ug. So ra is a linear combination of elements rug and $ra \in V^G$. Moreover, $\phi \in Hom_{\mathbb{C}G}$, $a\phi(g) = \phi(ag)$. $sra = a$ and $rsb = b$ so $b \mapsto sb$ is ϕ^{-1}. So ϕ is a $\mathbb{C}G$ isomorphism.

Theorem 79: If U is a $\mathbb{C}H$ module of $\mathbb{C}H$ and If V is a $\mathbb{C}G$ module of $\mathbb{C}G$ then $dim(Hom_{\mathbb{C}G}(U^G, V)) = dim(Hom_{\mathbb{C}H}(U, V_{|H}))$

Proof: If $\theta \in Hom_{\mathbb{C}G}(U^G, V))$, $\exists r \in \mathbb{C}G$: $\theta(s) = sr, s \in U^G$. Define $\overline{\theta} = \theta_{|H}$. The map $\theta \mapsto \overline{\theta}$ is a linear transformation from $Hom_{\mathbb{C}G}(U^G, V)$ to $Hom_{\mathbb{C}H}(U, V_{|H})$. First we show it is invertible: If $\varphi \in Hom_{\mathbb{C}H}(U, V_{|H})$, $\exists r \in \mathbb{C}G : \varphi(u) = ur$. Define $\theta : U^G \to \mathbb{C}G$ by $\theta(s) = sr, s \in U^G$ then $\theta \in Hom_{\mathbb{C}G}(U^G, V)$ and $\overline{\theta} = \varphi$. Now the transformation is injective because if $r_1, r_2 \in \mathbb{C}G$ and $ur_1 = ur_2, \forall u \in U$, then $r_1 s = r_2 s, \forall s \in U^G$.

Definition: If $H \leq G$ and φ a class function on H, $\varphi^G(g) = \frac{1}{|H|} \sum_{x \in G} \varphi^*(x^{-1}gx)$ is called an *induced character*, where $\varphi^*(x) = 0, x \notin H$ and $\varphi^*(x) = \varphi(x), x \in H$. It actually is a character.

Frobenius Reciprocity Theorem: $(\varphi^G, \theta) = (\varphi, \theta_{|H})$.

Proof: Suppose first that (φ and θ are irreducible with underlying representation modules U and V. Then $(\varphi^G, \theta)_G = dim(Hom_{\mathbb{C}G}(U^G, V))$ and $(\varphi, \theta_{|H})_H = dim(Hom_{\mathbb{C}H}(U, V_{|H})$ and the result follows from the earlier theorem. Since any character is the linear combination of irreducible characters, the result follows from the bilinearity of the form.

Remark: Note that $deg(\phi^G) = \phi^G(1) = \frac{|G|}{|H|}\phi(1)$. We define $f_x^G(y) = 1$, if $y \in x^G$ and $f_x^G(y) = 0$, otherwise.

Theorem 80: $(\chi, f_x^G) = \frac{\chi(x)}{|C_G(x)|}$. If no element of g^G lies in H then $\phi^G(g) = 0$. If some element of g^G lies in H then $\phi^G(g) = |C_G(g)|(\frac{\phi(x_1)}{|C_H(x_1)|} + \ldots + \frac{\phi(x_m)}{|C_H(x_m)|})$ where $(f_g^G)_{|H} = f_{x_1}^H + \ldots + f_{x_m}^H$.

Proof: $(\chi, {f_x}^G) = \frac{1}{|G|} \sum_{g \in G} \chi(g) {f_x}^G(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g) {f_x}^G(g) = \frac{|x^G|}{|G|}\chi(x) = \frac{\chi(g)}{|C_G(x)|}$.

Brauer's Characterization of Characters: p-elementary groups are the products of a cyclic p' group and p group. Every irreducible character is an induced character of a linear character of a p elementary subgroup for some p.

Proof:

Step 1: Let $\chi_1, \ldots, \chi_h$ be the irreducible characters of G over $\mathbb{C}$ and let $X_R(G) = \{\sum a_i \chi_i\}$, $V_R(G) = \{\sum r_i \phi_1, \phi_i$ and irreducible character of an elementary abelian subgroup of $G\}$, $U_R(G) = \{\chi : G \to \mathbb{C}\}$ where χ is a class function of an elementary abelian subgroup E of G, $\chi_{|E} \in X_R(E)$.

Step 2: $V_R(G) \subseteq X_R(G) \subseteq U_R(G)$ and $V_R(G)$ is an ideal in $U_R(G)$.

Step 3: Let $E = A \times B$ be elementary with $(|A|, |B|) = 1$. $\exists \psi = \psi_a \in V_S(G)$ such that (1) $\psi(g) \in \mathbb{Z}, \forall g \in G$, (2) if g is not conjugate to an element of gB then $\psi(g) = 0$ and (3) $\psi(a) = |C(a) : B|$.

Step 4: Let $\mathcal{C}_\infty, \mathcal{C}_\infty, \ldots, \mathcal{C}_\parallel$ be the conjugacy classes of G which consist of p'-elements then $\forall i, 1 \leq i \leq k$, $\exists \tau_i \in V_S(G)$: (1) $\tau_i(g) \in Z, g \in G$, (2) $\tau_i(g) = 0$ if the p' part of g is not in $\mathcal{C}_i$, (3) $\tau_i(g) = 1 \pmod p$ if the p' part of $g \in \mathcal{C}_i$.

Step 5: If p is prime, $\exists \phi \in V_S(G)$ such that $\forall g \in G, \phi(g) \in Z$ and $\phi(g) = 1 \pmod p$.

Step 6: If $\alpha : G \to \mathbb{C}$ is a class function and $\alpha(g) \in |G|S, \forall g \in G$ then $\alpha \in V_S(G)$.

Step 7: $|G| = p^n g_0$, $p \nmid g_0$ then $\alpha(x) = g_0 \in V_S(G)$.

Step 8: $1 \in V_S(G)$.

Step 9: $1 \in V_Z(G)$.

Step 10: $1 \in V_Z(G) \leq V_R(G)$ so by step 2, $V_R(G) = X_R(G) = U_R(G)$.

RSK correspondence for representations of the symmetric group: $\exists$ bijection between S_n and the set of ordered tableau of the same shape $g \leftrightarrow (S, T)$, further $g^{-1} \leftrightarrow (T, S)$.

Young's diagram: $D(\lambda)$, $n = n_1 + n_2 + \ldots + n_k$, $n_1 \geq n_2 \geq \ldots \geq n_k$. Number of tableaus with shape λ: $f_\lambda = \frac{n!}{\prod_{i,j \in D(\lambda)} h(i,j)}$, where $h(i,j) =$ number of cells in hook $H_{i,j}$.

18.12 Miscellaneous

Theorem: Let χ be an irrecucible character of G then $\chi(1) \mid |G : \mathbb{Z}(G)|$. If $|\theta(g)| = \theta(1)$ then $gker(\theta) \in \mathbb{Z}(G/ker(\theta))$.

Proof:

Character Table: Let $\chi_1, \chi_2, \ldots, \chi_s$ be the irreducible characters of G and $R_1, R_2, \ldots, R_s$ be the conjugacy classes. $X = (\chi_i(g_j))$ is the character table.

Theorem: If $N \lhd G$, $N \subseteq ker(\rho_{G/N})$. If $H < G$ and θ is a character that vanishes on $H^\#$ then $|H| \mid \theta(1)$. If χ is a non-linear irreducible character of G then $\exists g \in G : \chi(g) = 0$.

Proof: $\frac{\theta(1)}{|H|} = \frac{1}{|H|} \sum_h \theta(h)$ which is an integer.

Theorem: Let $A(g) = (a_{ij}(g))$ and $B(g) = (b_{ij}(g))$ be $F-$irreducible representations of G. (a) If $A \nsim B$ then $\sum_g a_{is}(g) b_{tj}(g^{-1}) = 0$. (b) If A is absolutely irreducible, $\sum_g a_{is}(g) a_{tj}(g^{-1}) = \frac{|G|}{n} \delta_{ij} \delta_{st}$, where $n = deg(A)$. If A affords χ and B affords η, $(\chi, \eta) = 0$ and $(\chi, \chi) = 1$.

Proof: Put $f(S) = \sum_g A(g^{-1}) S B(g)$. $A(h) f(S) = F(S) B(h), \forall h$, so by Schur, $f(S)$ is 0. Put $E_{ij} = (\delta_{ij})$. $f(E_{ij}) = 0$. This gives (a). Since $A = B$ is absolutely irreducible, $f(E_{st}) = \lambda I_n$. $e_{st} \delta_{ij} = \sum_g a_{is}(g^{-1}) a_{tj}(g)$ or $\sum_g a_{is}(g^{-1}) a_{tj}(g) = \frac{|G|}{n\lambda} \delta_{ij} \delta_{tj}$. This gives b. Summing over i, j, s, t gives $(\chi, \eta) = 0$. Summing over i, we get $\sum_g a_{ss}(g^{-1}) a_{tj}(g) = \frac{|G|}{n\lambda} \delta_{sj} \delta_{tj}$. Summing over j, we get $\sum_g a_{ss}(g^{-1}) a_{tt}(g) = \frac{|G|}{n\lambda} \delta_{ts}$. Finally, summing over t, s, we get $\sum_g a_{ss}(g^{-1}) a_{tt}(g) = \frac{|G|}{n\lambda} \delta_{ts}$. Finally, summing over t, s, we get $\sum_g \chi(g^{-1}) \chi(g) = \frac{|G|}{n\lambda} \delta_{ts}$. Finally, summing over t, s, with $\lambda = 1$, we get $\sum_g \chi(g^{-1}) \chi(g) = |G|$.

18.13 Some character tables

If $n = 2k$, D_{2n} has $k + 3$ conjugacy classes. If $n = 2k + 1$, D_{2n} has $k + 2$ conjugacy classes.

C_3			
$\lvert ccl(g)\rvert$	1	1	1
$\lvert C_G(g)\rvert$	3	3	3
g	1	a	a^2
$\chi_1(g)$	1	1	1
$\chi_2(g)$	1	ω	ω^2
$\chi_3(g)$	1	ω^2	ω

S_3			
$\lvert ccl(g)\rvert$	1	2	3
$\lvert C_G(g)\rvert$	6	2	3
g	1	(123)	(12)
$\chi_1(g)$	1	1	1
$\chi_2(g)$	1	1	-1
$\chi_3(g)$	2	-1	0

A_4				
$\lvert ccl(g)\rvert$	1	3	4	4
$\lvert C_G(g)\rvert$	12	4	3	3
g	1	(12)(34)	(123)	(132)
$\chi_1(g)$	1	1	1	1
$\chi_2(g)$	3	-1	0	0
$\chi_3(g)$	1	1	ω	ω^2
$\chi_4(g)$	1	1	ω^2	ω

S_4					
$\lvert ccl(g)\rvert$	1	6	8	3	6
$\lvert C_G(g)\rvert$	24	4	3	8	4
g	1	(12)	(123)	(12)(34)	(1234)
$\chi_1(g)$	1	1	1	1	1
$\chi_2(g)$	1	-1	1	1	-1
$\chi_3(g)$	2	0	-1	2	0
$\chi_4(g)$	3	1	0	-1	-1
$\chi_5(g)$	3	-1	0	-1	1

A_5					
$\lvert ccl(g)\rvert$	1	20	15	12	12
$\lvert C_G(g)\rvert$	60	3	4	5	5
g	1	(123)	(12)(34)	(12345)	(21345)
$\chi_1(g)$	1	1	1	1	1
$\chi_2(g)$	4	1	0	-1	-1
$\chi_3(g)$	5	-1	1	0	0
$\chi_4(g)$	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
$\chi_5(g)$	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

S_5							
$\lvert ccl(g)\rvert$	1	10	20	15	30	20	24
$\lvert C_G(g)\rvert$	120	12	6	8	4	6	5
g	1	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
$\chi_1(g)$	1	1	1	1	1	1	1
$\chi_2(g)$	1	-1	1	1	-1	-1	1
$\chi_3(g)$	4	2	1	0	0	-1	-1
$\chi_4(g)$	4	-2	1	-2	0	1	-1
$\chi_5(g)$	6	0	0	1	0	0	1
$\chi_6(g)$	5	1	-1	1	-1	1	0
$\chi_7(g)$	5	-1	-1	1	1	-1	0

Chapter 19

Frobenius Groups

19.1 Sylow analysis

Theorem 1: If G is a finite group, $P \in S_p(G)$, with $n_p = |G : N_G(P)| \neq 1 \pmod{p^2}$, then there are distinct Sylow subgroups P, R of G such that $P \cap R$ is of index p in both P and R.

Proof: Let P act on P^G yielding several orbits. The orbit with P has one element. If $p^2 \mid |P : P \cap R|$ for all p-Sylow subgroups $R \neq P$, p^2 divides the size of every orbit not containing P. Thus $n_p = 1 + kp^2$, which is a contradiction. So there is some R for which $|P : P \cap R| = p$.

Result: If $p \neq q$ and every subgroup of order pq is cyclic then $p \mid q - 1$. In this case, $p \mid |N_G(Q)|$ and for som p-group, P, of order p, $P \leq N_G(Q)$ and $PQ \leq N_G(Q)$ is abelian so $q \mid |N_G(P)|$.

Application: No group, G, of order $1785 = 3 \cdot 5 \cdot 7 \cdot 17$ is simple.

If G is simple, $n_{17} = 35$. Let $Q \in S_{17}(G)$, $|G : N_G(Q)| = 35$ and $|N_G(Q)| = 3 \cdot 17$. Let $P \in S_3(N_G(Q))$. PQ is abelian since $3 \nmid (17 - 1)$ so $Q \leq N_G(P)$ and $17 \mid |N_G(P)|$. The only possibilities for n_3 are $7, 85, 595$ and the last two are eliminated because $17 \mid |N_G(P)|$. On the other hand, if $|G : N_G(P)| = 7$ it violates the lower bound on the index of a subgroups of G by the permutation bound so we're done.

Application: No group, G, of order $3675 = 3 \cdot 5^2 \cdot 7^2$ is simple.

If G is simple, $n_7 = 15$, $Q \in S_7(G)$, $|G : N_G(Q)| = 15$ and $|N_G(Q)| = 5 \cdot 7^2$. Put $N = N_G(Q)$ and let $P \in S_5(N)$. $P \lhd N$ and P is contained in a Sylow p group P^*. $P^* \leq N_G(P)$ and $\langle N, P^* \rangle = N_G(P)$. $3^2 \cdot 7^2 \mid |N_G(P)|$ and $n_p = 3$ but this violates the permutation bound on the index of subgroups in G.

Application: No group, G, of order $3159 = 3^4 \cdot 13$ is simple.

$13 \neq 1 \pmod{3^2}$ so $\exists P, R \in S_3(G)$: $|P : P \cap R| = 3$. Put $N = N_G(P \cap R)$, $P, R \leq N$, so $3^4 \mid |N|$ since $|N| > 3^4$, $G = N$ and $P \cap R \lhd G$.

19.2 Frobenius groups

Definition: G is $\frac{3}{2}$ transitive on A if G is transitive on A and G_a has orbits of the same size on $A \setminus \{a\}$. If further, $G_a = 1$, G is called *semiregular* and if, further, G_a is transitive on $A \setminus \{a\}$, then G is called *regular*.

If G is $\frac{3}{2}$ transitive on A, $G_a \neq 1$ and G_a is semiregular on $A \setminus \{a\}$ then G is called a *Frobenius group*. So G is Frobenius iff $G_a \neq 1$ and $G_{a,b} = 1$.

Example: A_4 is a Frobenius group with kernel V_4. $SL(q)$ is Frobenius: $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. D_{2n} is Frobenius with complement of order 2.

Theorem 2:
(1) $\sum_{g \in G} |A_g| = t|G|$, where t is the number of orbits of G on A.
(2) If H is a transitive abelian group then H is regular.
(3) If G is transitive of prime degree, G is primitive.
(4) If G is transitive, G is primitive iff G_a is maximal.

Proof: (1) is just Burnside's theorem. (4) is Theorem 3 in the permutation chapter. For (2), if $a \neq b$, since H is transitive, $\exists h : h(a) = b$. $H_b = H_{h(a)} = (H_a)^h$ so H_b also fixes a. Letting b vary, we get H_a fixes all points so $H_a = 1$. For (3), if $B_1, \ldots, B_k$ is a system of imprimitivity, $|B_i| \mid |A|$ which is impossible if $|A|$ is a prime.

Theorem 3: If G is $\frac{3}{2}$ transitive then G is either primitive or Frobenius.

Proof: Put $G_C = \{g \in G : g(c) = c, \forall c \in C\}$ and $G_{\langle C \rangle}$ be the elements that fix C setwise. Suppose G has a system of imprimitivity, $B_1, \ldots, B_r$ with $|B_i| = k$. The orbits of G_α all have the same size (m) except the orbit consisting of just α, so $k = 1 \pmod m$ so $(k, m) = 1$. If $\alpha \notin B_i$, $m \mid |B_i^{G_\alpha}|$ and $k \mid |B_i^{G_\alpha}|$ so $km \mid |B_i^{G_\alpha}|$ and $|G_\alpha : G_{\alpha,\beta}| = m$ but then $G_{B_i} = G_{\alpha_i,\alpha_j} = G_{\alpha_j,\alpha_i} = G_{B_j}$. Fixing i and letting j vary, $G_{B_i} = G_A = 1$ for $a \neq b$. $G_{a,b} = G_{a_i,a_j} = 1$ and G is Frobenius.

Theorem 4: G has a faithful permutation representation in which it is Frobenius iff it has a proper subgroup, H which is a "TI" set with $N_G(H) = H$.

Proof: Suppose G is Frobenius and put $H = G_a$. $1 < H < G$. If $g \in G - H$ then $H^g = G_a^g = G_{a^g} = G_b$ where $b = a^g \neq a$. Thus $H^g \cap H = G_a \cap G_b = G_{a,b} = 1$. Hence H is a TI set and $N(H) = H$. Conversely, given G, H then G permutes the right cosets of H transitively by right multiplication. Suppose $\langle x_1, x_2, \ldots, x_n \rangle$ is a set of coset representatives of H then we have a homomorphism $\varphi : G \to Sym(\langle Hx_i \rangle)$. Let $a - Hx_i$, $b = Hx_j$ with $i \neq j$. $G_{a,b} = H^{x_i} \cap H^{x_j}$ and $x_j x_i^{-1} \notin H = N(H)$ and so $H^{x_i} \neq H^{x_j}$. Since H is a TI set, $G_{a,b} = 1$. Thus the representation is faithful and G is a Frobenius group.

Theorem 5: If G is Frobenius, it contains a regular normal subgroup, N called a Frobenius kernel.

Proof: Put $N = \{g \in G : g = 1 \text{ or } |A_g| = 0\}$ and $H = G_\alpha$. H is a TI set, $N_G(H) = H$. Finally, put $\alpha^*(g) = (ind_H)^G(g)$. $(\alpha^*, \beta^*)_G = (\alpha, \beta)_H$. Let $\phi_0, \phi_1, \ldots, \phi_k$ be the irreducible characters of H with $\phi_0 = 1_H$. For $i \neq 0$, put $\alpha_i = f_i 1_G - \phi_i$, where $f_i = deg(\phi_i)$. $(\alpha_i, \alpha_i) = {f_i}^2 + 1$, but $({\alpha_i}^*, 1_G)_G = (\alpha_i, 1_H)_H = f_i$. So, ${\alpha_i}^* = f_i + \chi_i$, where χ_i is a generalized character of G. Since $||{\alpha_i}^*|| = {f_i}^2 + 1$, ${\alpha_i}^* = f_i 1_H + \chi_i$ where χ_i is an *irreducible* character of G. Further, $(\chi_i)_H = \phi_i$. Put $K = \cap_i ker(\chi_i)$ so $K \lhd G$ and $|K| \leq |G : H|$. If $g \in N$, since no conjugate of an element of $H^\#$ lies in H, ${\alpha_i}^*(g) = 0$. Thus, for $g \in N$, $\chi_i(g) = f_i = \phi_i(1)$ so $g \in ker(\chi_i)$ and $g \in K$. $|N| = |G : H| \geq |K|$ and $N = K$. N is normal and regular.

Theorem 6: Let G be a Frobenius group with $|G_a|$, even. Then G has an abelian regular normal subgroup.

Theorem 7: Let G be a Frobenius group of degree n of maximal order $[n(n-1)]$. The $n = p^k$ and G has a regular normal abelian subgroup.

Proof: Let $p \mid |N|$, where N is the Frobenius kernel of G. $|N| = n$. Since $|G_a| = n-1$, $p \nmid |G_a|$ for any a and $x \in N$. Since G is Frobenius, $C_G(x) \leq N$ and $|G| = |G_a| \cdot |N| geq |C_G(x)| \cdot |G_a| = n(n-1)$ and $|C_g(x)| \leq |N|$ and thus $\frac{|G|}{C_G(x)} \geq |G_a| = n-1$. As a result, $|G : C_G(x)| \geq n-1$ and hence the conjugacy class containing x in G which is inside N has at least $n-1$ elements and must be all of N except for 1. Thus all non-identity elements of N have order p and $|N| = p^k$. N is a regular normal subgroup that acts on $ccl_G(x)$ and so it is transitive. So all non-identity elements of N are conjugate and have common order, p, so N is an elementary abelian subgroup.

Note: Frobenius groups are semi-direct products. $N = Fit(G)$.

Theorem 8: Let G be a group. The following are equivalent:
(a) G is Frobenius with kernel N of order n and complement H of order m.
(b) G has a normal subgroup N with $1 < N < G$. If $C_G(g) \leq N$, $|N| = n$ and $|G| = mn$.
(c) $|G| = mn$, $(m, n) = 1$. If either $g \in G$ then either $g^m = 1$ or $g^n = 1$. If $N = \{g \in G, g^n = 1\}$, then $N \lhd G$ with $1 < N < G$.

Proof:
(a) $\rightarrow$ (b): $1 < N < G$. Suppose, by way of contradiction, $g \in N^{\#}, C_G(g) \not\subseteq N$. $G = N \cup \bigcup_{x \in G} (H^{\#})^x$. Taking conjugates, we can assume $h \in H^{\#}$ and $h \in C_G(g)$ then $h \in H \cap H^g$ so $H \cap h^g \neq 1$, a contradiction.

(b) $\rightarrow$ (c): First, we show N is a Hall subgroup. Let $P \in S_p(N)$ extend P to a sylow subgroup P^* of G. $\mathbb{Z}(P^*) \subseteq C_G(P^{\#})$ and $\mathbb{Z}(P^*) \subseteq N$ also $P^* \subseteq C_G(\mathbb{Z}(P^*) i^{\#})$. So, $P^* \subseteq N$, $P = P^*$ and N is a Hall subgroup. $|N| = mn$, $(m, n) = 1$ and $N \lhd G$ with $N = \{g : g^n = 1\}$. Let $g \in G$ and suppose $g^m \neq 1$. Then $g^m \in N^{\#}$. By (b) $G \in C_G(g^m) \subseteq N$ and $g^n = 1$.

(c) $\rightarrow$ (a): Since $N \lhd G$ is a Hall subgroup, by Schur-Zassenhaus, $\exists H, |H| = m$ with $G = HN, H \cap N = 1$. As $G = HN$ we can assume $g \in N$. If $1 \neq h \in H \cap H^g$, $ghg^{-1} \in H$ and so $[g, h] \in H$ but $[g, h] \in N$ and $[g, h] \in H \cap N = 1$, so $hg = gh$. If $|g| = n_1$ and $|h| = m_1$ and $|hg| = m_1 n_1$. By (c), $m_1 \neq 1$, $n_1 = 1$ and $g = 1$. So H is a TU set with $N_G(H) = H$.

Theorem 9: Let G be a Frobenius group with kernel N, $K < G$ if $K \not\leq N$ and $K \cap N \neq 1$ then K is Frobenius with Frobenius kernel $K \cap N$. If $a < K < N$ and $K \lhd G$ then G/K

Proof: $K > K \cap N > 1$ and $K \cap N \lhd K$. If $g \in (K \cap N)^{\#}$, by (b) above, $C_K(g) = K \cap C_G(g) \subseteq K \cap N$ so K is Frobenius and the result follows from (c).

Theorem 10: Thompson: Frobenius kernels are nilpotent.

Proof: Let G be a Frobenius group with kernel N. We show N is nilpotent by induction on $|G|$. By Previous result, we can assume $|G : N| = p$ and $|H| = p$.

Suppose first that $\mathbb{Z}(N) \neq 1$. If $\mathbb{Z}(N) = N$, N is nilpotent. If $\mathbb{Z}(N) < N$, $N/\mathbb{Z}(N)$ is nilpotent by induction and thre result follows.

Now suppose $\mathbb{Z}(N) = 1$. For some $p \neq q$, N does not have a normal q complement for some q. First lets assume q is odd. If $q \neq 2$ and $p \nmid |N|$ and H permutes sylow q-subgroups of N. Since $(q, p) = 1, \exists Q \in S_q(N), H \subseteq N(Q)$. If $Q_0 = \mathbb{Z}(Q)$ or $Q_0 = \mathcal{T}(Q)$, in either case $Q_0 \, char \, Q$ and

$Q_0 \lhd Q$ and $H \subseteq N_N(Q_0)$ and by the previous result, $K = HN_N(Q_0)$ is Frobenius with kernel $N_N(Q_0)$. If $N_N(Q_0) \neq N$, $N_N(Q_0)$ is nilpotent and has a normal q complement. By Thompson's normal p-complement theorem, this can't be the case for both $\mathbb{Z}(Q)$ and $\mathcal{T}(Q)$. Since $G = HN$, $Q_0 \lhd G$. By induction, N/Q_0 is nilpotent and $Q/Q_0 \lhd N/Q_0$ so $Q \lhd N$. On the other hand, if N has a normal q complement for all q odd dividing $|N|$, then $2 \mid |N|$ and N has a normal Sylow-2 subgroup.
In any case, we have, for some q and $Q \in S_q(G)$, $Q \lhd N$ and $\mathbb{Z}(Q), C_G(\mathbb{Z}(Q)) \lhd G$. Put $\overline{G} = G/C_G(\mathbb{Z}(Q))$. By a previous result, $\overline{G} = \overline{N} \bigcup_{\overline{g} \in \overline{G}} \overline{H}^{\overline{g}}$ which is a disjoint (except for 1) union of $|\overline{N}| + 1$ subgroups. G acts on $\mathbb{Z}(Q)$ with kernel $C_G(\mathbb{Z}(Q))$, so $\overline{G}$ acts faithfully on $\mathbb{Z}(Q)$. Since $Q \subseteq C_G(\mathbb{Z}(Q))$, $(t, q) = 1$. By a result in the coprime action section, $\exists v \in \mathbb{Z}(Q)^{\#}$ which is centralized by either $\overline{N}$ or $\overline{H}^{\overline{g}}$. Since $\mathbb{Z}(N) = 1$, $[v, \overline{N}] \neq 1$ and by a previous result, v cannot be centralized by any non identity element of $\overline{H}^{\overline{g}}$. This contradiction establishes the result.

Additional fact: Frobenius groups with non abelian kernels exist.

Theorem 11: Let G be a $\frac{3}{2}$ transitive group with a regular normal subgroup, N. If G is not Frobenius then N is an elementary abelian p-subgroup and N is the unique minimal normal subgroup of G.

Proof: N is transitive and N and $N' = 1$. $N_a = 1$ and any characteristic subgroup, T, of N is normal in G and transitive which is impossible.

Theorem 12: If G is Frobenius with non-solvable complement H, H has a normal subgroup of index 2 that is isomorphic to $M \times SL_2(5)$ where M is metacyclic and $(|M|, 30) = 1$.

19.3 Character theory of Frobenius groups

Theorem 13: Let G be a Frobenius group of order $q^a p$ with elementary abelian Frobenius kernel Q and a cyclic group of G/Q acts irreducibly by conjugation on Q, then
(1) $G = QP$, $P \in S_p(G)$. Every non-identity element of G has order p or q. Every element of P is conjugate to one in P and every element of order q in in Q. There are $p - 1$ conjugacy classes of order p of size q^a. There are $\frac{q^a - 1}{p}$ conjugacy classes of order q of size p.
(2) $G' = Q$ so the number of characters of degree 1 of G is p contains Q in its kernel.
(3) If ϕ is a non-principal irreducible character of Q, then ${ind_Q}^G(\phi)$ is an irredicible character of G. Every irreducible character of of G degree > 1 is equal to ${ind_Q}^G(\phi)$ for some non-principal irreducible character of G has either degree 1 or p and the number of irreducible characters of degree p is $\frac{q^a - 1}{p}$.

Proof: $G = QP$ and $C_G(h) = Q$ if $1 \neq h \in Q$. If $|x| = pq$, x^p has oorder q, so $x^p \in Q$ but then $[x, x^p] = 1$ and $x \in C_G(x^p) = Q$, which is a contradiction. Put $\overline{G} = G/Q$ and $\overline{G}$ is abelian. $\overline{g^{-1}xg} = \overline{y}$. So $\overline{x} = \overline{y}$ since $P \cong \overline{P}$. There are $p - 1$ conjugacy classes of elements of order p. If $1 \neq x \in P$, $C_G(x) = Q$ and $|G : P| = q^a$. If $1 \neq h \in Q : C_G(h) = Q$, $ccl(h) = \langle h, h^x, \ldots, h^{x^{p-1}} \rangle$. $P = \langle x \rangle$. This proves (1).

G/Q is abelian so $Q \subseteq G'$ but Q is a minimal normal subgroup so $Q = G'$. Let ψ be a non-principal irreducible character of Q and $\phi = {ind_Q}^*(\psi)$. Let $1, x, \ldots, x^{p-1}$ be coset representatives for G/Q. $||\phi||^2 = \frac{1}{|G|} \sum_{h \in Q} \phi(h)\overline{\phi(h)} = \frac{1}{|G|} \sum_{h \in Q} \sum_{i=0}^{p-1} \phi(x^i h x^{-i})\overline{\phi(x^i h x^{-i})} = \frac{p}{|G|} \sum_{h \in Q} \phi(h)\overline{\phi(h)} = \frac{p|Q|}{|G|} = 1$ so ϕ is irreducible.

P acts on irreducible characters of degree > 1, $\mathcal{C}$ as follows. For $\psi \in \mathcal{C}$, $\psi^x(h) = \psi(xhx^{-1}), h \in Q$. Let $P = \langle x \rangle$ so ${ind_Q}^G(\psi)(h) = \psi(h) + \psi^x(h) + \ldots + \psi^{x^{p-1}}(h)$. If ψ_1 and ψ_2 are in two different orbits, ${ind_H}^G(\psi_1)$ and ${ind_H}^G(\psi_2)$ restrict to different Q-classes. Q has $q^a - 1$ irreducible, non-principal characters and so $\mathcal{C}| = q^a - 1$, $|P| = p$ and there are $\frac{q^q-1}{p}$ P-orbits. This accounts for all non-principal irreducible characters so they all have degree p.

Application: You can use this to calculate the characters of D_{10}, a non-abelian group of order 57, a non-abelian group of order 56 with a normal elementary abelian Sylow 2 subgroup.

Lemma 13.1: Let $1 \neq Z \subseteq \mathbb{Z}(G)$ with $|G : Z| = m$ and ψ a character of Z, then ${ind_Z}^G(\psi)(g) = m\psi(g), g \in Z, 0$ otherwise.

19.4 Frobenius groups in CN classification

The main result is that there is no simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$ using a method similar to the method of Feit, Hall, Thompson to show CN groups of odd order are solvable.

Lemma 13.2: Let G be a Frobenius group of with kernel Q and suppose Q and G/Q are abelian but G is not abalian. Let $|Q| = n, |G : Q| = m$. Then

(1) G/Q is cyclic and $G = QC$ for some cyclic groups C, $C \cap Q = 1$.

(2) $(m, n) = 1$.

(3) G has no elements of order pq, $q \mid n$, $p \mid m$,

(4) The number of non-identity conjugacy classes of G in Q is $\frac{n-1}{m}$ and each has size m.

(5) No two distinct elements of C are G-conjugate. So there are $m-1$ representatives of distinct conjugacy classes in C, each of size n. Every element of $G \setminus Q$ is conjugate to some element of C. G has $m + \frac{n-1}{m}$ conjugacy classes.

(6) $G' = Q$ and G has m distinct linear characters.

(7) If ψ is a non-principal irreducible character of Q, ${ind_Q}^G(\psi)$ is an irreducible character of G. Every irreducible character of degree > 1 is ${ind_Q}^G(\psi)$ for some non-principal character of Q. Every irreducible character has degree 1 or m and the number of degree m is $\frac{n-1}{m}$.

Proof:

(1) Let $q \mid n$ and let G/Q act by conjugation on the elementary abelian subgroup $\Omega_1(Q)$. If ϕ is a faithful irreducible character then the center is cyclic

(2) If $p \mid |Q|$ and $p \mid |G : Q|$. Let $P \in S_p(G)$, then $P \cap Q \lhd P$ and $P \cap Q$ is a Sylow subgroup of Q. $C_G(\mathbb{Z}(P) \cap Q)$

(3) and (4) Argue as in theorem 13.

(5) If $g_1^x = g_2$; $g_1, g_2 \in C$ and we cam pick $x \in Q$. $[g_2, x] \in C \cap C^x \cap Q = 1$. So $g_2 \in C(x), x \in Q$ which contradicts the fact that G is Frobenius.

(6) $Q \leq G'$ since G/Q is abelian. Let $C = \langle x \rangle$. $h \mapsto [x, h]$ is a homomorphism with trivial kernel.

(7) Argue as in theorem 13.

19.5 Frobenius groups in CN classification

The main result is that there is no simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$ using a method similar to the method of Feit, Hall, Thompson to show CN groups of odd order are solvable.

Theorem 14: Let G be a simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$.

(1) $q_1 = 3$: $Q_1 \in S_3(G)$, $N_1 = N_G(Q_1)$. Q_1 is elementary abelian. $|N_1| = 3^3 \cdot 13$ and N_1 is Frobenius.

(2) $q_2 = 7$: $Q_2 \in S_7(G)$, $N_2 = N_G(Q_2)$. Q_2 is cyclic. $|N_2| = 3 \cdot 7$ and N_2 is Frobenius.

(3) $q_3 = 13$: $Q_3 \in S_{13}(G)$, $N_3 = N_G(Q_3)$. Q_3 is cyclic. $|N_3| = 3 \cdot 13$ and N_3 is Frobenius.

(4) $q_4 = 409$: $Q_4 \in S_{409}(G)$, $N_4 = N_G(Q_4)$. Q_4 is cyclic. $|N_4| = 3 \cdot 409$ and N_4 is non-abelian.

(5) Every non-identity element of G has prime order and $Q_i \cap {Q_i}^g = 1, g \in G \setminus Q_i$. Further, for $1 \leq i \leq 4$: $Q_i \cap {Q_i}^g = 1$, if $g \in G \setminus N_i$.

The non-identity conjugacy classes of G are:

(a) 2 classes of elements of order 3, each of size $7 \cdot 13 \cdot 409$.

(b) 2 classes of elements of order 7, each of size $3^3 \cdot 13 \cdot 409$.

(c) 4 classes of elements of order 13, each of size $3^3 \cdot 7 \cdot 409$.

(d) 136 classes of elements of order 409, each of size $3^3 \cdot 7 \cdot 13$.

From here on, for any subgroup $H < G$ with generalized character μ of H, put $\mu^* = (ind_H)^G(\mu)$. Thus,

(i) N_1 has 2 irreducible characters of degree 13.

(ii) N_2 has 2 irreducible characters of degree 3.

(iii) N_3 has 4 irreducible characters of degree 3.

(iv) N_4 has 136 irreducible characters of degree 3.

Proof: Note that by theorem 8, G is Frobenius with kernel Q, if $Q \lhd G$ and $C_G(x) \leq Q, 1 \neq x \in Q$.

Let n_i be the size of $S_{q_i}(G)$.

Besides 1 (which is impossible since G is simple), $n_4 \mid 3^3 \cdot 7 \cdot 13$ and $n_4 = 1 \pmod{409}$ leaves only $n_4 = 819$ and $|N_4| = 3 \cdot 409$. $Q_4 \lhd N_4$ and N_4 is a semidirect product of Q_4 and a cyclic group of order 3.

No element of order 409 divides $|N_3|$, so $n_3 \mid 3^3 \cdot 7 \cdot 13$ and $n_3 = 1 \pmod{13}$. The only possibilities are $n_3 = 27$ or $n_3 = 9 \cdot 7 \cdot 409$. So $n_3 = 9 \cdot 7 \cdot 409$, $|N_3| = 3 \cdot 13$.

No element of order 13 or 409 can divide $|N_2|$, so $n_2 \mid 3^3 \cdot 13 \cdot 409$. $n_2 = 3^2 \cdot 13 \cdot 409$ and $|N_2| = 3 \cdot 7$.

Based on what we know so far, there are $s_{409} = 408 \cdot 9 \cdot 7 \cdot 13 = 334,152$ elements of order 409 in G, $s_{13} = 12 \cdot 9 \cdot 7 \cdot 409 = 309,204$ elements of order 13, $s_7 = 6 \cdot 9 \cdot 7 \cdot 409 = 287,118$ elements of order 7 and $s_1 = 1$ element of order 1. $|G| = 3^3 \cdot 7 \cdot 13 \cdot 409 = 1,004,913$; there are $r = |G| - s_1 - s_7 - s_{13} - s_{409} = 74,438$ remaining elements. Neither N_4, N_3 nor N_2 can be abelian otherwise a Sylow subgroup would lie in the center of its normalizer and G would have a normal p complement by Burnside. Let x be an element of order 3 that lies in the center of Q_1. $|C_G(x)|$ cannot contain a element of order 409, 13 or 7 because of the structure of the normalizers of their Sylow subgroups. $Q_1 \subseteq C_G(x)$ so $|G : C_G(x)| = 7 \cdot 13 \cdot 409 = 37,219$, there are also $37,219$ conjugates of x^2 which also has order 3 and thus $74,438$ elements of order 3, this accounts for all the remaining elements of G. As a result, every element of Q_1 has order 3 and Q_1 is an elementary abelian group of order 3^3. $|Aut(Q_1)| = (3^3-1)(3^3-3)(3^3-3^2) = 26 \cdot 24 \cdot 18 = 2^5 \cdot 3^3 \cdot 13$. $|N_G(Q_1)/C_G(Q_1)|$ must be either 1 or 13. Again, Burnside rules out 1 so $|N_G(Q_1)| = 3^3 \cdot 13$ and $N_1 = N_G(Q_1)$ is nonabelian. For each $Q = Q_i, i = 1,2,3,4$, $x \in Q$ implies $C_G(x) \leq Q$ so N_1, N_2, N_3 and N_4 are all Frobenius. $n_1 = \frac{|G|}{|N_1|} = 7 \cdot 13 \cdot 409$.

The character results follow from theorem 13, completing the proof.

Lemma 14.1: For $1 \leq j \leq 4$, $q = q_i$, $Q = Q_i$, $N = N_i$, $p = |N : Q|$. Let $\phi_1, \ldots, \phi_k$ be any exceptional characters of N of degree p. Put $\alpha = \phi_1 - \phi_2$, $\beta = \phi_3 - \phi_4$, then α, β are generalized characters of N with $\alpha(g) = 0 = \beta(g)$, if $g \in N, |g| \neq q$. α^*, β^* are generalized characters of G with the same property. $(\alpha^*, \beta^*)_G = (\alpha, \beta)_N$.

Proof: $\exists \lambda_1, \ldots . \lambda_4$ irreducible, linear cahracters of Q, $\psi_j = {ind_Q}^G(\lambda_j)$. $\psi_j(x) = 0$ if $x \in N \setminus Q$ since $Q \lhd N$ and so do α and β. $\psi_j^*(1) = p$ and $\alpha(1) = \beta(1) = 0$. ${\psi_j}^* = {ind_N}^G(\lambda_j) = {ind_Q}^N(\lambda_j)$. ψ_j^* vanishes on all elements not conjugate to an element of Q and so do α^* and β^*. $deg(\psi_j^*) = |G : Q|$. $\alpha^*(x) = \beta^*(x) = 0$ if $|x| \neq q$. Let $\langle g_1, g_2, \ldots, g_k \rangle$ be coset representatives for G/N. $Q \cap Q^x = 1, k > 1$. $(\alpha^*, \beta^*)_G = \frac{1}{|G|} \sum_{x \in G} \alpha^*(x)\overline{\beta^*(x)} = \frac{1}{|G|} \sum_{x \in G, |x| = q} \alpha^*(x)\overline{\beta^*(x)} = \frac{1}{|G|} \sum_{x \in N, |x| = q} |G : N| \alpha^*(x)\overline{\beta^*(x)} = \frac{1}{|N|} \sum_{x \in N} \alpha(x)\overline{\beta(x)} = (\alpha, \beta)_N$.

Lemma 14.2: Under the same assumptions as Lemma 14.1, let $\psi_1, \ldots, \psi_k$ be dictinct irreducible characters of N of degree p. $\exists \chi_1, \chi_2, \ldots, \chi_k$ which are irreducible characters of G of the same degree $\phi_1^* = \phi_j^* = \epsilon_j(\chi_1 - \chi_j)$, $\epsilon_j = \pm 1$, $2 \leq j \leq k$. These ψ_j^* are called the exceptional representations associated with Q_j.

Proof: Let $q = q_i$, $N = N_i$, $p = |N : Q|$. Let $\psi_1, \ldots, \psi_k$ be irreducible representations of Q. Put $\alpha_j = \psi_1 - \psi_j, j = 2, \ldots, k$. $2 = ||\alpha_j||^2 = (\alpha_i, \alpha_j)_N = ||\alpha_j^*||^2$. So α_j^* has two irreducible characters of G as constituents; since $\alpha_j^*(1) = 0$, these must be characters of the same degree. The lemma holds for $k = 1, 2$ so assume $k > 2$. $\alpha_2^* = \psi_1^* - \psi_2^* = \epsilon(\chi - \chi')$ and $\alpha_3^* = \psi_1^* - \psi_3^* = \epsilon(\theta - \theta')$ and $\theta, \theta', \chi, \chi' \in Irred(G)$. $\chi \neq \chi'$ and $\theta \neq \theta'$. $\alpha_3^* - \alpha_2^* = \psi_2^* - \psi_3^* = \epsilon(\theta - \theta' + \chi' - \chi)$. By 14.1, $\psi_2^* - \psi_3^* = (\psi_2 - \psi_3)^*$ has two constituents and $\theta = \chi$ or $\theta' = \chi'$. $\alpha_2^* = (\chi - \chi')$ and $\alpha_3^* = (\chi - \theta')$; put $\chi_1 = \chi, \chi_2 = \chi', \chi_3 = \theta$. $\exists \chi_j : \alpha_j^* = \psi_1^* - \psi_j^* = \epsilon(\chi_1 - \chi_j)$. $\chi_1, \ldots, \chi_k$ are all distinct, proving the lemma.

Lemma 14.3: The exceptional characters associated with Q_i are distinct from the exceptional characters associated with Q_j.

Proof: Let χ be an exceptional character associated with Q_i and Let θ be an exceptional character associated with Q_j. There are distinct, irreducible characters of Q_i with $\psi^* - \psi'^* = \chi - \chi'$ and distinct, irreducible characters of Q_j with $\lambda^* - \lambda'^* = \theta - \theta'$. Put $\alpha = \psi - \psi'$ and $\beta = \lambda - \lambda'$. α^* is 0 on all elements with order different from q_i and β^* is 0 on all elements with order different from q_j. So $(\alpha^*, \beta^*)_G = 0$ and the pairwise constituents are pairwise orthogonal.

Lemma 14.4: The permutation character of the group G in theorem 14 of degree 819 with G actinng on left cosets of N_4 decomposes as $\chi_0 + \gamma + \gamma'$ where χ_0 is the principal character, and γ, γ' are irreducible characters of degree 409.

Theorem 15: Let G be a group of order $3^3 \cdot 7 \cdot 13 \cdot 409$, then G is not simple.

Proof: Let d_i be the common degree of the characters associated with Q_i. These characters represent irreducible, non-principal characters of G; together with the principal character. These form all the irreducible characters of G. $1+2d_1^2+2d_2^2+4d_3^2+136d_4^2 = 1004913$. $d_1^2+d_2^2+2d_3^2+68d_4^2 = 502456$ (Equation *). All of these are irredicible and faithful and the smallest degree is 13, so $d_i \geq 13$ and $d_4 \leq \sqrt{50245668} < 86, d_4 \mid |G|$, so $d_4 = \langle 13, 21, 27, 39, 63 \rangle$. As a result equation * has no solution.

Chapter 20

Note on Strongly Embedded subgoups

20.1 Main result

Definition: $H < G$ is strongly embedded if (a) H is a roper subgroup of G of even order and (2) $\forall x \in G \setminus H$, $|H \cap H^x|$ is odd.

Bender's Theorem: If G has a strongly embedded subgroup then either:
(1) every S_2 subgroup has a unique involution, $C_G(t)$ is a proper subgroup and any proper subgroup containing $C_G(t)$ is strongly embedded; or,
(2) There is a normal series $\{1\} \lhd M \lhd L \lhd G$ such that G/L and M have odd order and L/M is $PSL_2(2^n)$, $Sz(2^n)$ or $PSU_3(2^n)$ and every strongly embedded subgroup is of the form $H = N_G(S)O_{2'}(G)$, $S \in S_2(G)$.

A characterization: If G is a group of even order and H is a proper subgroup of G, either:
(1) H is strongly embedded,
(2) $|H|$ is even and $N_G(Q) \subseteq H$ for any $Q \in 2(H)$; or,
(3) $H \subseteq T \in S_2(G)$ and $N_G(T) \subseteq H$ and $C_G(t) \subseteq H, t \in Inv(H)$.

If H is strongly embedded in G, all involutions of G, are conjugate and all involutions in H are $H-$conjugate. If $u \in Inv(H)$ and $x, y \in Inv(G)$ and $xy \in C_G(u)$, $x, y \in H$. If $x \in G \setminus H$, $C_G(u)x$ contains exactly one element of $Inv(G)$.

Chapter 21

Components

21.1 Subnormal Subgroups

Definition: G is *semi-simple* if it is the direct product of non-abelian simple groups.

Theorem 1: If $G = \prod K_i$ is semisimple and $N \lhd G$ then N is aproduct of some of the K_i.

Theorem 2: If $G_1, G_2 \lhd G$ are semi-simple, so is G_1G_2 and $G_1 \cap G_2$.

Theorem 3: If H is a minimal normal subgroup of G then H is either semi-simple or an elementary abelian p-group.

Theorem 4: If $A \lhd \lhd G$ and $B \lhd \lhd G$ then $\langle A, B\rangle \lhd \lhd G$.

Proof: The proof is by induction on $|G|$. We have: $A = A_1 \lhd A_2 \lhd \ldots \lhd A_n \lhd G$ and $B = B_1 \lhd B_2 \lhd \ldots \lhd B_m \lhd G$. $A_nB_m \lhd G$. If $A_nB_m < G$. $\langle A, B\rangle \lhd \lhd \langle A_n, B_m\rangle \lhd G$ where the subnormality in the product group follows by induction and the result follows. If $\langle A, B\rangle = G$ the result is trivial. Let B_l be the first subgroup in the subnormal sequence for B in G: $B_lA_n = G$. The $N = B_{l-1}A_n \lhd B_lA_m = G$. $\langle A, B\rangle \lhd N \lhd G$ and the result follows.

Theorem 5: Let Σ be a set of subnormal subgroups of G satisfying $\Sigma^G = \Sigma$ and $\exists \Sigma : \Sigma > \Sigma_0$ then $\exists X \in \Sigma \setminus \Sigma_0$ such that $\Sigma_0^X = \Sigma_0$.

Proof: By the previous result $\langle \Sigma_0\rangle \lhd \lhd G$. Assume $\langle \Sigma_0\rangle \neq G$ then $\exists G_1 \lhd G : \langle \Sigma_0\rangle \subseteq G_1$, hence the induction claim applies to G_1 provided $\Sigma_1 = \{U : U \leq G_1\} \neq \Sigma_0$. We can assume $\Sigma_1 = \Sigma_0$. Then $\Sigma_1^G = \Sigma_1$, $G_1^G = G_1$ and $\Sigma_G = \Sigma$ and so $\langle \Sigma_0\rangle = \langle \Sigma_1\rangle \lhd G$.

Theorem 6: Let $A < G$ and $\mathcal{U}$ be a collection of non-empty subsets of G For $U \in \mathcal{U}$, $\emptyset \neq \Sigma_U : \Sigma_U = \{A^g : g \in G, A^g \lhd \lhd U\}$. Suppose that $\forall U, \tilde{U} \in \mathcal{U}$ such that (1) $A \in \Sigma_U$, (2) $\{B : B \in \Sigma\tilde{U} : B \leq U\} \subseteq \Sigma_U$, (3) $\exists \hat{U} \in \mathcal{U} : N_G(\langle \Sigma_U \cap \Sigma\tilde{U}\rangle)$ then $\mathcal{U}$ contains a unique maximal element.

Proof: Set $\Sigma = \bigcup_{U\in\mathcal{U}} \Sigma_U, U \in \mathcal{U}$. Assume $U_1 \neq U_2$ are two maximal elements of $\mathcal{U}$ and $\Sigma_0 = \Sigma_{U_1} \cap \Sigma_{U_2}$ is maximal. According to (3), $N_G(\langle \Sigma_0\rangle) \subseteq U_3^{max}, < \Sigma_{U_i} \lhd U_i$ and the maximality of U_i gives $U_i = N_G(\langle \Sigma_{U_i}\rangle)$. Suppose $\Sigma_0 \subseteq \Sigma_{U_i}$. By the previous result, $\exists X \in \Sigma_{U_i} \setminus \Sigma_0$ with $\langle \Sigma_0\rangle^X = \langle \Sigma_0\rangle$. So $X \in \Sigma_{U_3}$ and $\Sigma_0 \subset \Sigma_{U_3} \cap \Sigma_{U_i}$ and $U_2 \neq U_1 = U_3$. Then $\Sigma_0 = \Sigma_{U_1}$ and since $U_i = N_G(\langle \Sigma_{U_i}\rangle)$, $U_1 = N_G(\langle \Sigma_{U_i}\rangle) \leq U_3$. This is a contradiction.

Theorem 7: If $A \lhd \lhd \langle A, A^g \rangle, \forall g \in G$ then $A \lhd \lhd G$.

Proof: $A \lhd \lhd \langle A, A^{gx^{-1}} \rangle$ so $A^x \lhd \lhd \langle A^x, A^g \rangle$. Proceed by induction on $|G|$ and assume A is not subnormal in G. Let $\mathcal{U}$ be the proper subgroups of G containing A. $\langle A, A^g \rangle \in \mathcal{U}, \forall g \in G$. By induction, $\Sigma_U = \{A^x : A^x \leq U, x \in G\} \lhd \lhd U$. $\Sigma_0 \subseteq \Sigma_U$ and $A \in \Sigma_0$, $A \lhd \lhd \langle \Sigma_0 \rangle$. So $\langle \Sigma_0 \rangle$ is not normal in G and $N_G(\langle \Sigma_0 \rangle) \in \mathcal{U}$ and $\mathcal{U}$ satisfies the hypothesis of the previous theorem. Let M be the unique maximal subgroup. that contains $\langle A, A^g \rangle, \forall g \in G$. $A \lhd \lhd, \langle \Sigma_M \rangle \lhd G$ and thus $A \lhd \lhd G$.

21.2 Basic Results and definitions

Generalized Fitting Subgroup Motivation: Since $C(F^*(G)) \subseteq F^*(G)$, $G \to Aut(G)$ has kernel $Z(F^*(G))$; further, $F^*(G)$ is uncomplicated and its embedding in G is well behaved. Want to study relationship of $F^*(G)$ and its $p-$locals. Hard when $F^*(G)$ is a $p-group$ but then we can use Thompson factorization.

Definition: L is *quasi-simple* if $L' = L$ and $L/Z(L)$ is simple.

Definition: L is a *component* of H if $L \lhd \lhd H$ and L is quasi-simple.

Definition: $Comp(G) = \{H : H \text{ is a component of } G\}$.

Definition: $E(G) = \langle Comp(G) \rangle$ where H is a component of G. $E(G) \lhd G$.

Definition: $F^*(G) = F(G)E(G)$ is called the *Generalized Fitting Group.*

Theorem 8: Let $H \lhd \lhd G$ then $Comp(H) = Comp(G) \cap H$.

Proof: If $L \in Comp(H)$, $L \lhd \lhd H \lhd \lhd G$ so $L \in Comp(G)$. If $L \lhd \lhd G$ and $L \in Comp(G) \cap H$, $L \lhd \lhd H$ and the result follows.

Theorem 9: Let $L \in Comp(G)$ and $H \lhd \lhd G$ then either $L \in Comp(H)$ or $[L, H] = 1$.

Proof: If $L \notin Comp(H)$, $L \cap H < L$ and $L \neq [L, H] \lhd L$, so $[L, H] \subseteq \mathbb{Z}(L)$. $[L, H, L] = 1 = [H, L, L]$ so $[L, L, H] = [L, H] = 1$ by the three subgroups lemma.

Theorem 10: Distinct components commute.

Proof: $[L_1, L_2] \leq L_1 \cap L_2$. Since $L_1 \neq L_2$ $[L_1 \cap L_2] \subseteq \mathbb{Z}(L_1) \cap \mathbb{Z}(L_2)$. So $[L_1, L_2, L_2] = 1$ and $[L_2, L_1, L_2] = 1$ so $[L_2, L_2, L_1] = [L_2, L_1] = 1$.

Theorem 11: Let $L \in Comp(G)$ and H be an L-invariant subgroup of G then (1) either $L \in Comp(H)$ or $[L, H] = 1$ and (2) if H is solvable, $[L, H] = 1$

Proof: $H \lhd \langle H, L \rangle$. If $L \subseteq H$, $L \in Comp(H)$, otherwise, $[L, H] = 1$ by the earlier result. If H is solvable, it cannot have a simple non-abelian subgroup, L so $L \notin Comp(H)$.

Lemma: If K_1 and K_2 are components either $K_1 = K_2$ or $[K_1, K_2] = 1$.

Proof: By previous result, if $[K_1, K_2] \neq 1$, $K_1 \leq K_2$ symmetrically, $K_1 \geq K_2$ and $K_1 = K_2$,

Theorem 12: Let $E = E(G)$, $Z = \mathbb{Z}(E)$, $\overline{E} = E/Z$. Then (1) $Z = \langle \mathbb{Z}(L) : L \in Comp(G) \rangle$ (2) $\overline{E}$ is the direct product of the groups $\overline{L}, L \in Comp(G)$, (3) E is a central product of its components.

Proof: $Z_0 = \prod_{i=1}^{n} Z_i$. $E(G) = \prod_{i=0}^{n} (Z_0 K_i)$. $K_i Z_0 \cap \prod_{i \neq j} K_j Z_0 = Z_0$.

Theorem 13: $O_\infty(C_G(F(G))) = \mathbb{Z}(F(G))$.

Proof: Let $Z = \mathbb{Z}(F(G))$, $\overline{G} = G/Z$ and $H = O_\infty(C_G(F(G)))$. Assume $\overline{H} \neq 1$ and $\overline{X}$ a minimal normal subgroup of $\overline{H}$. $\overline{X}$ is a p-group so $X = PZ$, $P \in S_p(X)$ and X centralized Z so $P \lhd X$. Thus $P \leq O_p(G) \leq F(G)$ so $P \leq C_G(F(G)) = Z$, a contradiction.

Theorem 14: Let $Z = \mathbb{Z}(F(G))$, $\overline{G} = G/Z$, $\overline{S} = soc(C_G(F(G)))$ then $E = S^{(1)}$ and $S = E(G)Z$.

Proof: Let $H = C_G(F(G))$. $O_\infty(\overline{H}) = 1$ so each minimal normal subgroup of $\overline{H}$ is the direct product ofnonabelian simple subgroups and these are components of $\overline{H}$. So $\overline{S} \leq E(\overline{H})$. Let $\overline{K}$ be a component of $\overline{H}$. So $K = K^{(1)}Z$ with $K^{(1)}$ quasisimple. $K \in Comp(G)$ so $S \leq E(G)Z$ and $S \leq E(G)Z$, thus $E(G) \leq H$. Let $L \in Comp(G)$ and $M = \langle L^H \rangle$ then $\overline{M}$ is a minimal normal simple subgroup of $\overline{H}$ so $M \leq S$. Thus $S = E(G)Z$ so $E(G) = S^{(1)}$.

Definition: $F^*(G) = E(G)F(G)$.

Theorem 15: $C_G(F^*(G)) \leq F^*(G)$.

Proof: Let $H = C_G(F^*(G)), K = C_G(F(G)), Z = \mathbb{Z}(F(G))$ and $\overline{G} = G/Z$. $\overline{H} \lhd \overline{K}$, so if $\overline{H} \neq 1$ then $1 \neq \overline{H} \cap soc(\overline{K})$ and thus $H \cap E(G) \neq Z$, a contradiction.

Definition: $O_{p',E}(G)$ is defined by $O_{p',E}(G)/O_{p'}(G) = E(G/O_{p'}(G))$.

Theorem 16: $P \in p(G)$ then (1) $O_{p',E}(N_G(P)) \leq C_G(O_p(G))$ and (2) if $P \leq O_p(G)$ then $O^p(F^*(N_G(P)) = O^p(F^*(G))$.

Proof: Todo.

Theorem 17: If G is solvable and $p \in p(G)$ then $O_{p'}(N_G(P)) \leq O_{p'}(G)$.

Proof: This was proved in the Coprime section.

Theorem 18: Let $X/Z(X)$ be a non-abelian simple group then $X = X'Z(X)$ and X' is quasi-simple.

Proof: Let $Y = X'$ and $X^* = X/Z(X)$. $Y^* \lhd X^*$ and X^* is simple so $Y^* = 1$ or $Y^* = X^*$. In the latter case, $X = YZ(X)$ and in the former X^* is abelian which is a contradiction. So $X = YZ(X)$ and X/Y' is abelian thus $Y = Y'$. Further, $Y/Z(Y) = X^*$ is simple so Y^* is quasi-simple.

Definition: G is of *characteristic $p-$type* if $F^*(H) = O_p(H)$ for every $p-$local, H (Groups of Lie type over characteristic p are, for example).

Theorem 19: $E(G) = \langle K | K$ is a component of $G \rangle$. $F^*(G)F(G)E(G)$, $[F(G), E(G)] = 1$. $F^*(G)$ contains every minimal subgroup of G; in particular, $\langle K^G \rangle$ is the direct product of components conjugate to K.

Proof: See section on components.

Theorem 20: $E(G) \neq 1$ and $K_1, K_2, \ldots, K_n$ be components of G. Set $Z = Z(E(G)), Z_i = Z(K_i), E_i K_i Z/Z$. $E(G)$ is the central product of K_i, $Z = Z_1 Z_2 \ldots Z_n$. $E(G)/Z = E_1 \times E_2 \times \ldots \times E_n$.

Proof: See section on components.

Theorem 21: Let $L \lhd \lhd G$ then (1) if $L \leq F^*(G)$ then $L = (L \cap F(G))(L \cap E(G))$, (2) $F^*(L) = F^*(G) \cap L$, (3) $E(L)C_{E(G)}(L) = E(G)$, $E(L) \lhd E(G)$.

21.3 Characteristic $p-$type

Definition: G is of characteristic $p-$type if $P \in p(G), N = N_G(P) \to F^*(N) = O_p(N)$. $PSL_n(p^m)$ is of characteristic $p-$type.

Theorem 22: Let G be a non-abelian simple group, G is of characteristic $p-$type iff $F^*(N(P)) = O_p(N(P))$ for every maximal $p-$local. If $F^*(G)$ is a $p-$group then so is $F^*(N(P)), \forall P \in p(G)$ (use $P \times Q$).

Definition: Let Ω be a collection of subgroups. Define $\mathcal{D}(\Omega)$ as the graph formed by joining $A, B \in \Omega$ if $[A, B] = 1$. If $k > 0$ let, $\mathcal{E}_k^p(G)$ be the elementary abelian subgroups of p-rank at least k. G is said to be $k - connected$ for prime p if $\mathcal{D}(\mathcal{E}_k^p(G))$ is connected.

Theorem 23: If G is a non-abelian finite simple group with $m_2(G) \leq 2$ then either (1) a Sylow 2-group is either dihedral, semi-dihedral or $Z_{2^n} \wr Z_2$ and $G \cong L_2(q)$, $G \cong L_3(q)$, $G \cong U_3(q)$ q, odd, or M_{11}; or, (2) $G \cong U_3(4)$. Note that $Q_8 \in S_2(SL_2(3))$ and $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ is the unique involution.

21.4 Strongly Embedded Groups

Definition: H is *strongly-embedded* in X if $N_X(T) \subseteq H$ if $T \in 2(X)$.

bf Lemma: If H is *strongly-embedded* in X then (a) $S \in S_2(H)$ then $S \in S_2(X)$, (b) $x \in x - H$ then $|H \cap H^g|$ is odd and (c) In the permutation representation of X on $\{H^g\}$, the 1-point stabilizer of a point has even order and the 2-point stabilizer has odd order.

Observation: Induction on SE groups uses the following: *Lemma 1:* If H is strongly embedded in X and $Y \leq H$ and $|Y \cap H|$ and $|Y \cap H^g|$ for some $g \in G - H$, then $Y \cap H$ is strongly embedded in Y.
Lemma 2: If $Y \leq H$ lies in at least three distinct conjugates of H, $|C_H(Y)|$ is odd and acts transitively on conjugates of H.

Definition: M is *strongly-embedded* if $|M|_2 > 1$ and $|M \cap M^g|_2 = 1, \forall g \in G \setminus M$.

Theorem 24: $C_L(O_2(L)) \leq O_2(L)$ for all 2-locals, L.

Bender's Theorem: For any group X, we have $C_X(F^*(X)) \leq F^*(X)$ and if $W \lhd X$ and $C_X(W) \leq W$ then $E(X) \leq W$. If $O_{p'}(X) = 1$ then $F(X) = O_p(X)$ and every component of X has order divisible by p so X is p-constrained iff $E(X) = 1$ or, equivalently, $C_X(O_p(X)) \leq O_p(X)$.

Definition: Let $\overline{X} = E(X/O_{p'}(X))$, L is a minimal normal subgroup subject to $\overline{L} = E(\overline{X})$, $\overline{L_i}$ is a component of $E(\overline{X})$, $L_i = O^{p'}(L_i)$, $[L_i, L_i] = L_i$ and $[L_i, L_j] \leq O_{p'}(X)$, L is called the *p-layer.*

Theorem 25: $F^*(X)$ controls embedding of X of p'-cores and the p-layer of every p-local. $O_\pi((X/O_\pi(X))) = 1$.

Theorem 26: If $O_\pi(X) = 1$ then $F(X)$ is divisible by $p \in \pi$ and every component is divisible by some $p \in \pi'$.

Signalizer Motivation: The idea is that $A-$invariant p' subgroups of G can be glued into a single p' subgroup $\theta(G, A)$ which is either normal or strongly $p-$embedded in G. $M \subseteq G$ is *strongly $p-$embedded* if $p||M|$ but p does not divide $|M \cap M^g|$ for $g \in G - M$.

Tightly embedded: $p = 2$. If M is strongly embedded, G fixes one point when acting on the cosets of M. Bender identified all simple groups with strongly 2-embedded subgroups, namely, $SL_2(2^n), Sz(2^n), PSU_3(2^n)$.

Definition: No simple group of $p - rank \geq 3$ has a strongly $2-$embedded $2'$ local subgroup.

Bender's Theorem: Let G be a finite simple group and $S \in S_2(G)$ then one of the following holds: (a) S is dihedral, (b) S is semidihedral, (c) G has a strongly embedded subgroup, (d) S has a non-cyclic characteristic elementary abelian subgroup, A, and $E = N_G(A)$ has conjugacy classes, $\langle z_i^G \rangle$, that do not fuse in G such that $G = \langle E, C_G(z_i) \rangle$.

Definition: If G is a finite simple group and $H < G$ with $\mathbb{Z}(H)$ of even order and $h \approx C_H(z)$ then G is said to be of H-type. Note we can construct a faithful transitive permutation representation of G given a presentation of H. A group has an H-satellite if there are non-isomorphic groups of H-type.

Definition: A finite simple group, G, is uniquely determined by $C_H(z)$ for a $2-$central involution, z, if G does not have any non-isomorphic H-satellites.

Definition: G is of characteristic 2-type, $F^*(H)$ is a 2-group for all 2-locals, H.

Definition: G is balenced, if for every 2-local, H, $L_{2'}(h) \leq L_{2'}(G)$.

L-Balence Theorem: (Walter). Every finite group is balenced.

B-Theorem: $L_{2'}(C_G(z)) = E(C_G(z))$.

Bender: $H/Z(F(H))$ acts faithfully as a group of automorphisms of $F^*(H)$ and, in particular $|H| \leq |F^*(H)|!$.

Proof: Follows from properties of $F^*(G)$.

Problem Suppose that G is a finite group containing an involution t such that $C_G(t) = \langle t \rangle \times L$, with $L \cong S_n$, $n \geq 5$. Suppose further that if t_i is a transposition in L, then $C_G(t_i) = \langle t_i \rangle \times L_i \cong C_G(t)$. Prove that $G \cong S_{n+2}$.

Problem Show that if S is a Sylow 2-subgroup of $N_G(D)$ with $S < U$, then there exists a nonidentity characteristic subgroup C of S with $C \lhd N_G(D)$. If this is the case, then we can "push up" $N_G(D)$ to $N_G(C)$ which contains a larger 2-group than S, namely $N_U(C)$.

Global $C(G,T)$ Theorem Let G be a finite simple group of characteristic 2-type having 2-rank at least 3. Let T be a Sylow 2-subgroup of G and let $C(G,T)$ denote the subgroup of G generated by the normalizers of all nonidentity characteristic subgroups of T. If $C(G,T) < G$, then $C(G,T)$ is a strongly embedded subgroup of G and so $G \cong SL(2,2n), Sz(2n), PSU(3,2n)$.

Gorenstein-Lyons Trichotomy Theorem Let G be a simple group of characteristic 2-type with $e(G) \geq 4$ in which all proper subgroups have known simple composition factors. Then one of the following alternatives holds:
1. There is an odd prime p and an element x of G of order p such that $C_G(x)$ has a normal quasisimple subgroup L with $L/Z(L)$ a group of Lie type in characteristic 2; or
2. G has a maximal 2-local subgroup M which is a p-uniqueness subgroup for some odd prime p such that M has p-rank at least 4; or
3. G is of $GF(2)$-type.

The Feit-Thompson Uniqueness Theorem Let G be a finite group of odd order in which every proper subgroup is solvable. Suppose that K is a proper subgroup of G such that either $r(K) \geq 3$ or $r(C_G(K)) \geq 3$. Then K is contained in a unique maximal subgroup of G. (Here $r(K)$ denotes the maximum rank of an abelian p-subgroup of K, as p ranges over all prime divisors of $|K|$.)

Theorem 27: Let G be 2-transitive on Ω, $|\Omega| = 1 \pmod 2$ and for $\alpha, \beta \in \Omega$, $|G_{\alpha\beta}|$ is odd and $G_{\alpha\beta}$ has a normal complement, Q, in G_α which acts regularly on $\Omega \setminus \{\alpha\}$. Then $G = PSL_2(s^n), SZ(2^{2n+1}, PSI_3(2^n)$.

Theorem 28: Let G be a finite simple group and every element of G is either an involution or is of odd order. Then $G \cong SL_2(2^n)$.

G is a CA group if $1 \neq g \in G$ then $C_G(g)$ is abelian.

Aschbacher's Component Theorem: Let G be a finite simple group and suppose the B-theorem holds. Suppose $E(C_G(t)) \neq 1$ for some $t \in Inv(G)$. Then there is an involution, z and a quasi-simple standard component, K of $C = C_G(z)$ such that $C_G(K)$ either has 2-rank 1 or is solvable with and elementary abelian or dihedral Sylow 2-subgroup. So G has at most two components and $K \lhd G$ or K has 2-rank 1.

Chapter 22

CN groups

22.1 Basic Results

Definition: G is a CN-group if $1 \neq x \in G$ then $C_G(x)$ is nilpotent.

Theorem: If H is a non trivial CN-group then $H > g$ is a CN-group and $C_G(H)$ is nilpotent.

Proof: Subgroups of nilpotent groups are nilpotent.

Theorem: If G is a CN-group and $P \in S_p(G)$ and $Q \in S_q(G)$, $p \neq q$. If $x \in P^{\#}$ and $y \in Q^{\#}$ and $[x, y] = 1$ then $[P, Q] = 1$.

Proof: If H is nilpotent and a, b are p and q elements with $p \neq q$ then $[a, b] = 1$. $\langle y, \mathbb{Z}(P)\rangle \subseteq C(x)$. Since $C(x)$ is nilpotent, $[y, \mathbb{Z}(P)] = 1$. Let $t \in \mathbb{Z}(P)^{\#}$. $\langle y, P\rangle \subseteq C(t)$ so $[P, y] = 1$. Analogously, $[Q, x] = 1$. Now, let $u \in \mathbb{Z}(Q)^{\#}$, $\langle y, Q\rangle \subseteq C(u)$ so $[y, Q] = 1$. Thus $\langle P, Q\rangle \subseteq C(y)$ and $[P, Q] = 1$.

Theorem: If G is a CN-group and $H \lhd G$ is solvable then G/H is a CN-group.

Proof: First, prove it for H elementary abelian. If L is a characteristically simple subgroup of H, L is elementary abelian since H is solvable. G/L is nilpotent by the previous result. $(G/L)/(H/L) = G/H$ and the result holds by induction.

Definition: G is a 3-step group with respect to p provided:
(1) $O_{p,p'}(G)$ is Frobenius with kernel $O_p(G)$ and a cyclic complement;
(2) $G = O_{p,p',p}(G)$
(3) $G/O_p(G)$ is Frobenius.

Theorem: A 3-step group is a solvable CN-group.

Proof: $H = O_p(G)$, $O_{p,p'}(g) = HA$. G/HA is a p-group.

Theorem: If G is a solvable CN-group then one of the following holds: (1) G is nilpotent; (2) G is Frobenius whose complement is either cyclic or a direct product of a cyclic group of odd order and a generalized quaternion group; (3) G is a 3-step group.

Proof: $F = F(G)$ so $C_G(F) \subseteq F$.

Theorem: If G is a CN-group and $O_p(G) \neq 1$ then either $O_p(G)$ is an S_p group of G or G is a 3-step group.

Proof:

Theorem: If G is a non-solvable CN-group of minimal order, then G is simple and all its proper subgroups are solvable.

Proof: By induction. If $H \lhd G$ and M/H is maximal so G/H is solvable. If $M = 1$ then $|G| = p$ so $M \neq 1$ and let $P \in S_p(M)$, $N = N_G(P)$. $M \subseteq N$ so $M = N$ and $P \in S_p(G)$. Similarly, $M = N_G(\mathbb{Z}(J(P)))$, so $M = O^p(M)P, \forall p$. Put $\bigcap_p O^p(M)$. $K \lhd G$ and $G = PO^p(M)$ with $O^p(M) \cap P = 1$ so K contains all p' elements so $G = KM$ and $K \cap M = 1$. If K is nilpotent, were done. Choose $x \in \mathbb{Z}(P)$. $M \subseteq C_G(x)$ so $C = M$ and x centralizes np p'-element and x induces by conjugation a fixed point free automorphism and G is nilpotent by Thompson.

Theorem: If G is a non-solvable CN-group of minimal odd order then no proper subgroup of G is a 3-step group.

Theorem: If G is a non-solvable CN-group of minimal odd order then no proper subgroup of G is a 3-step group.

Definition: Let G be a CN-group $\mathcal{H}$ is the set of subgroups $H < G$ which are maximal with respect to being nilpotent.

Theorem: Let G be a minimal simple CN-group of odd order, $H \in \mathcal{H}$, then (1) H is a Hall group of G and is disjoint from its conjugates, (2) $N_G(H)$ is Frobenius with kernel H and is maximal. Conversely, every maximal subgroup of G is a Frobenius whose kernel is in $\mathcal{H}$.

Theorem: Let G be a minimal simple CN-group of odd order, $H_{,1}, H_2 \in \mathcal{H}$ then $(|H_1|, |H_2|) = 1$.

Definition: Let G be a minimal simple CN-group of odd order. $p\ q$ if $\exists x \in p(G), y \in q(g) : [x, y] = 1$.

Theorem: Let G be a minimal simple CN-group of odd order then (a) is an equivalence relation, (b) if π_i is an equivalence class under then G possesses nilpotent S_{π_i} subgroups H_i, $H_i \in \mathcal{H}$ which is disjoint from its conjugates, (c) every maximal subgroup of G is conjugate to $N_G(H_i)$ for some i, (d) every element of G lies in a conjugate of H_i for some $1 \leq i \leq r$.

Theorem: Let G be a minimal simple CN-group of odd order and $H \in \mathcal{H}$ then (1) H is a Hall group of G; (2) If $|H|$ is not a of prime power order then H is disjoint from its conjugates; (3) If H is disjoint from its conjugates then $C_G(x) \subseteq H, \forall x \in H^{\#}$; (4) If H is disjoint from its conjugates and H has even order then $C_G(x) \subseteq H, \forall x \in H^{\#}$.

Theorem: Let G be a minimal simple CN-group of odd order, H_i are representatives of the conjugacy classes of the elements of $\mathcal{H}$. Put $h_i = |H_i|$ and $|N(H_i)| = n_i h_i$. Then (1) $n_i > 1$, $n_i \mid (h_i - 1)$, $n_i h_i \mid |G|$, $(h_i, h_j) = 1$ if $i \neq j$, and (2) $\sum_{i=1}^{r} \frac{h_i - 1}{h_i n_i} = 1 - \frac{1}{|G|}$.

Hall-Feit-Thompson: CN-groups of odd order are solvable.

Proof: By induction. Let G be a minimal simple CN-group of odd order. Set $M_i = N_G(H_i), 1 \leq i \leq r$. We derive properties of the irreducible characters of the M_i. These properties show that $|G| = p^a q^b$ and so G is solvable by Burnside's theorem.

22.2 More on $SL_2(p)$

Lemma: $|SL_2(5)| = 2^3 \cdot 3 \cdot 5$, $|SL_2(7)| = 2^4 \cdot 3 \cdot 7$, $|SL_2(17)| = 2^5 \cdot 3^2 \cdot 17$. In $SL_2(17)$, let $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $v = \begin{pmatrix} 3 & 0 \\ 0 & 6 \end{pmatrix}$, $w = \begin{pmatrix} 1 & 1 \\ 5 & 6 \end{pmatrix}$. Then $|u| = 17$, $|v| = 16$ and $|w| = 3^2$. $\begin{pmatrix} 14 & 0 \\ 0 & 11 \end{pmatrix}^{16} = \begin{pmatrix} 3 & 0 \\ 0 & 6 \end{pmatrix}^{16} = \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix}^{16} = 1$.

22.3 Role in classification

The induction step in a classification (in particular the odd order theorem) for G can use the following (1) minimal normal subgroups of a maximal subgroup of G are p-groups so (2) every proper subgroup is a p-local. Thus maximal subgroups are actually maximal p-locals and we can use "local methods" to push up to a maximal subgroup. Then we can study the embedding of the maximal subgroups (often using Thompson transitivity) to get a contradiction. The maximal subgroups usually have a Bruhat structure fixed by character theory. The final contradiction can often be obtained from generators and relations.

Sometimes important subgroups are Frobenius and we can use the following: **Frobenius:** G has Frobenius kernel, K, consisting of fixed point free automorphisms. A is the Frobenius complement and $|A| \mid (|K| - 1)$. K is nilpotent. Frobenius groups allow an action on congugates od A since $A \cap A^g = 1$ if $g \in G \setminus A$. In fact, G is Frobenius if G act transitively on Ω, $G_\alpha \neq 1$ but $G_\alpha \cap G_\beta = 1$ for $\alpha \neq \beta$, $A = G_\alpha$ and $|\Omega| = |K| = |G : A| = 1 \pmod{|H|}$.

Bruhat structure: $P \in S_p(G)$ and $B = N_G(P)$ (This is the Borel group.) Let H be a complement of P in B. $B \cap N = H \lhd N$ and $W = N/H$ is generated by reflections (W is the Weyl group). $G = BNB$. We often construct a strongly embedded subgroup M of G and can determine the structure of the p-locals of M and use this to determine the Bruhat structure of M.

Example: Put $G = GL_2(5)$, $|G| = 2^5 \cdot 3 \cdot 5$. $P = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F_5\}$. $N(P) = \{\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} : x \in F_5, a, b \in {F_5}^*\}$. $|N(P)| = 5 \cdot 16$. $O_5(N(P)) = P$. $H = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in {F_5}^*\}$, $|H| = 16$. $N(P) = HP$. G has other 2-elements like $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and a 3-element, $g = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$.

Chapter 23

Notes on odd order techniques

23.1 An idea

In CA groups of odd order, the maximal abelian subgroups are TI (Reason: from character theory every such subgroup, A, is of the form $C_G(x), 1 \neq x \in A$). For each such A, $M = N_G(A)$ is maximal and M is Frobenius. This gives characters of G which lead to a contradiction.

In the general odd order case, a minimal counterexample, G, has the property that every elementary abelian subgroup of order p^3 is in a unique maximal subgroup (by the Uniqueness Theorem). This allows us to determine the structure of such maximal subgroups of G and their embeddings in G. This is the origin of $SCN_k(P), P \in S_p(G)$. For these groups, $A = C_G(A)$ and $C_G(A) = A \times D$ with $D = O_{p'}(N(A))$. This in turn takes advantage of the fact that for $m(A) \geq 3$, $C_G(A)$ acts transitively on the set of maximal p' groups normalized by A. If G is a group of odd order thet doesn't contain any elementary abelian subgroup of order p^3 for any p, it is solvable and G' is nilpotent.

If $SCN_3(P)$ is empty, P is generated by 3 elements. Then $P \subseteq M'$ where M is a maximal subgroup of $N_G(P)$. These p^2 groups restrict the structure and embedding of the maximal subgroups which, coupled with the Uniqueness result provides contradictory evidence for the existance of G. Finally, an argument using generators and relations leads to a contradiction.

$PSL_3(7)$ has an elementary abelian p^2 groups as an example. $PSL_2(11)$ has a single conjugacy class of involutions and the centralizer of an involution is dihedral of order 12; it has an elementary abelian group of order 4 but the transitivity theorem doesn't hold. $|PSL_2(11)| = 1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$.

Lemma: If $q = p^n$, $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(q)$ and $|x| = 4$, $a = -d$ and $a^2 + bc = -1 \pmod{p}$.

If x has order 4, $x^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. So either $a = d = 0$ and $bc = -1$ or $d = -a \neq 0$ and $a^2 + bc = -1 \pmod{p}$.

Lemma: Let $G = SL_2(11)$. $S \in S_2(G)$ is quaternion. G has one element of order 2, and 110 elements of order 4. If x has order 4, $C_G(x)$ is dihedral of order 12. $PSL_2(11)$ has elementary abelian Sylow 2 subgroups. There are 55 involutions in $PSL_2(11)$; all involutions are conjugate in $PSL_2(11)$. $A_1 = \begin{pmatrix} 0 & 4 \\ 8 & 0 \end{pmatrix}$ has order

4 and so does $A_2 = \begin{pmatrix} 1 & 3 \\ 3 & -1 \end{pmatrix}$. $B = \begin{pmatrix} 5 & 1 \\ 2 & 5 \end{pmatrix}$ has order 3. $[A_1, B] = 1$ and $C_G(A_1) = \langle A_1, B \rangle$. $|C_G(A_1)| = 12$. $C = \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$ has order 10.

There are 110 solutions to $a^2 + bc = -1 \pmod{11}$. Let $H = G' = PSL_2(11)$. $S \in S_2(H)$ is elementary abelian and since H is simple, $N_H(S) > C_H(S)$ and all the involutions of S are conjugate. Most of the remaining results are direct calculations. Note that $PSL_2(11) \subseteq PSL_2(11^2)$. Let $\phi : SL_2(11^2) \to PSL_2(11^2)$ be the usual homomorphism. If $\phi(A)$ is an involution in $PSL_2(11^2)$, $\phi(A)^2 = \mu I$. $\exists B : A = B^{-1} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} B$, ${\lambda_1}^2 = {\lambda_2}^2 = \mu$ so $\mu = \pm 1$. If $\mu = 1$, $\phi(A)$ is not an involution, so $\mu = -1$. A has order 4 in $SL_2(11^2)$ so $A = C^{-1} \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} C$ for some C. These two possibilities are conjugate in $SL_2(11^2)$.

23.2 Guide to Feit-Thompson

If G is a minimal counterexample to the Odd Order conjecture, we'd like to prove something like the following (which is nor quite true).

Goal: For every maximal subgroup, M of G, $\exists M_0 \lhd M$ such that:
(1) $C_{M_0}(a) = 1$ for $a \in M \setminus M_0$;
(2) $M \cap M^g = 1$ for $g \in G \setminus M$;
(3) M_0 is nilpotent;
(4) $M/M0$ is cyclic;
(5) $\forall 1 \neq x \in G$, x lies in exactly one sucb M_0.

If all that happened, the M_0 would form a partition of G. In the real argument, such M are either almost Frobenius or 3-step groups (see section on CN-groups). In the real case, if E is a complement of M_0 in M, $r(E) \leq 2$ and two elements of a nilpotent Hall subgroup H are $G-$conjugate iff they are $N_G(H)$-conjugate ($N_G(H)$ controls fusion).

Chapter 24

Primitive groups, pairs and amalgams

24.1 Primitive Groups

Definition 1: $M < G$ is *primitive* if $M = N_G(A), \forall A \lhd M$. $1 \neq M < G$ is *strongly p-embedded* if $|M \cap M^g|_p = 1$ for $g \in G \setminus M$. $H < G$ is a p-local subgroup of G if $M = N_G(P), P \in p(G)$.

Comment: Bender classified groups with strongly embedded 2-subgroups.

Theorem 1: Let $N \lhd G$, be abelian. If G/N is perfect then G' is perfect.

Proof: $(G/N) = (G/N)'$ so $G = G'N$ and $G/N \approx G'/(G' \cap N)$. So $G'/(G' \cap N) = (G'/(G' \cap N))'$ and thus $G = G''N$ so $G/G'' \approx N/(G'' \cap N)$. Since this is abelian, $G' \subseteq G''$.

Theorem 2: $C_M(O_p(M)) \subseteq O_p(M)$ is equivalent to $F^*(M) = O_p(M)$ and $O_{p'}(M) = 1$.

Proof: Clear.

Theorem 3: If $M < G$ is maximal and $N \lhd G$ then M/N is a maximal subgroup of G/N.

Proof: Clear.

Comment: The forgoing theorem let's us assume a maximal subgroup contains no normal subgroup of G.

Theorem 4: Let $L \lhd \lhd G$. If $L \leq F^*(G)$ then (a) $L = (L \cap F(G))(L \cap E(G))$; (b) $F^*(L) = F^*(G) \cap L$; (c) $E(L)C_{E(G)}(L) = E(G)$. $E(L) \lhd E(G)$.

Proof: Every component of L is a component of G and $F(L) \leq F(G)$. Since $[F(G), E(G)] = 1$.

Theorem 5: The action of G by right conjugation on cosets of primitive groups is primitive.

Proof: The action is obviously transitive and $Mg = M \rightarrow g \in M$ which is maximal so the action is primitive.

Theorem 6: If $M < G$ is primitive, $N \lhd G$ and $M \cap N \neq 1$ then $C_G(N) = 1$.

Proof: $C_G(N) \lhd G$ and $C_G(N) < M \cap N$ then $C_G(N) = 1$.

Theorem 7: Let M be a primitive subgroup of G. No non-trivial subnormal subgroup of G is contained in M. $F(G) \cap M = 1$.

Proof: Suppose $L \lhd \lhd G, 1 \neq L \leq M$. Pick a minimal one, $L \leq F^*(G)$. By the previous result, $\mathbb{Z}(F^*(G)) = 1$. So $F(G) = 1$ and L is a component of G. $\langle L^M \rangle \lhd E(G)$ and by primitivity, $E(G) \leq M$. So $E(G) = 1$, which is a contradiction.

Theorem 8: If $M < G$ is a primitive subgroup, $p \in \pi(M)$, $N \lhd G$. Suppose $M \cap N = 1$ and $O_p(M) \neq 1$. (a) $p \notin \pi(N)$, (b) $\forall q \in \pi(N), \exists$ an M-invariant subgroup Sylow q-subgroup of N; (c) if $|\pi(N)| \geq 2$ then M is a maximal subgroup of G.

Proof: (a) Put $P = O_p(M)$ then $M = N_G(P)$ and $P \in S_p(NP)$ since $N \cap P = 1$ thus $p \notin \pi(N)$. For (b), PN acts on $\Omega = S_q(N)$. by conjugation and N is a transitive normal subgroup of PN so $C_\Omega(P) \neq \emptyset$ and $C_N(P)$ is transitive on $C_\Omega(P)$. Now $C_N(P) \leq M \cap N = 1$ gives $|C_\Omega(P)| = 1$ and $C_\Omega(P) = C_\Omega(M)$ since $P \lhd M$. For (c), $\exists M$-invariant $Q \in S_q(N)$. Since $Q < N$, $M < QM < NM \leq G$.

Theorem 9: Let $M < G$ be a primitive subgroup, $N \lhd G$: $M \cap F^*(N) \neq 1$ then $F(G) = 1$, $F^*(N) = F^*(G) = E(G)$. Every minimal normal subgroup of G is contained in M.

Proof: $F^*(N) \leq F^*(G)$ and by a previous result, $\mathbb{Z}(R(G)) = 1$ and so $F(G) = 1.F^*(N) = E(N)$ and $F^*(G) = C_{F^*(G)}(E(N))E(N)$. Applying the result again, $F^*(G) = E(N) = F^*(N)$.

Theorem 10: Suppose G contains a primitive maximal subgroup M then one of the following holds: (F1) $F(G) = F^*(G)$ and M is a complement of $F(G)$ in G; (F2) G contains exactly two minimal normal subgroups N_1, N_2 which are non-abelian $F^*(G) = N_1 \times N_2 = E(G)$; (F3) $F^*(G)$ is a minimal non-abelian subgroup of G.

Proof: See Stellmacher, 6.6.4.

Theorem 11: If F1 holds and $p \in \pi(M), O_p(M) \neq 1$ then all primitive maximal subgroups of G are conjugate.

Proof: Put $P = O_p(M), F = F^*(G)$ then $M = N_G(P)$, $FP \lhd G$ and $S_p(M) \subseteq S_p(G)$. Let H be another primitive maximal subgroup. H is also a complement of F so $|H| = |M|$. $\exists g : P \leq P^g$. $P = H^g \cap FP \lhd H^g$ so $H^g = N_G(P) = M$.

Theorem 12: Suppose F2 holds. There is an M-isomorphism $\alpha : N_1 \to N_2$ such that $M \cap F^*G) = \{xx^\alpha : x \in N_1\}$.

Proof: Let $D = M \cap F^*(G)$ then by a previous result ($C_G(N) = 1$), $D \cap N_1 = 1 = D \cap N_2$. Since $G = N_i M$, $F^*(G) = N_i D$ and $\forall x_1 \in N_1, \exists! x_2 \in N_2 : x_1 x_2 \in D$. The mapping $\alpha : N_1 \to N_2, x_1 \mapsto x_2$ is an isomorphism. The isomorphism commutes with elements of M since N_1, N_2, D are all M-invariant.

Theorem 13: Let F be a minimal normal subgroup of G, $N < G$, $G = FM$. (a) Suppose $U \subseteq F$ and $U^M = U$, then $UM < G$.

Proof: (b) follows from (a). For (a), assume the contrary, $G = UM$. Then $U \lhd G$ and F is not a minimal normal subgroups of G.

24.2 Primitive pairs

Definition 2: $M < G$ is *primitive* if $M = N_G(A), \forall A \lhd M$. $1 \neq M < G$ is *strongly p-embedded* if $|M \cap M^g|_p = 1$ for $g \in G \setminus M$. A group M is of characteristic p if $C_M(O_p(M)) \leq O_p(M)$ (If M is p-separable

then $O_{p'}(M) = 1$).

Theorem 14: Let M be a group of characteristic p. Suppose $U \leq M$ and $U \lhd \lhd M$ or $O_p(M) \leq U$ then U has characteristic p.

Proof: The case $O_p(M) \leq$ is clear. In the other case, apply $F^*(L) = F^*(G) \cap L$.

Definition 3: M_1, M_2 is called a *primitive pair* if $1 \neq A \lhd M_i$, $A \leq M_1 \cap M_2 \rightarrow N_{M_j}(A) = M_1 \cap M_2$. The pair is respectively (solvable or characteristic p if each are. The property $\mathcal{P}(M_1, M_2, A)$ is $1 \neq A \lhd M_i$, $A \leq M_1 \cap M_2$.

Theorem 15: Let M_1, M_2 be two different maximal p-local subgroups of G that both have characteristic p. Suppose M_1 and M_2 have a common Sylow p-subgroup, then (M_1, M_2) is a primitive pair of characteristic p.

Proof: Let $1 \neq A \lhd M_i, A \leq M_i \cap M_j, i \neq j$. By previous result, $1 \neq O_p(A) \lhd M_i$ and the maximality of M_i gives $M_i = N_G(O_p(A))$. So $N_{M_j}(A) = M_i \cap M_j$ has property $\mathcal{P}$. Let S be a common Sylow subgroup of M_1 and M_2 then $O_p(M_1)O_p(M_2) \leq S \leq M_1 \cap M_2$.

Theorem 16: Suppose $p \in \pi(G)$, every p-local has characteristic p and $O_p(G) = 1$ then either (a) there is a primitive pair of characteristic p or (b) every maximal p-local subgroup of G is strongly embedded in G.

Proof: Let M be a maximal p-local of G, then $O_p(M) \neq 1$ and $N_G(M) \leq N_G(O_p(M)) = M < G$ so $M^g \neq M, g \in G - M$. M^g is a maximal p-local. Among all such, choose one, $L \neq M$ with $|M \cap L|_p$ maximal. If $|M \cap L|_p > 1$ then $T \in S_p(M \cap L)$ and $U = N_G(T)$. Since U is a p-local, there is a maximal p-local $H \subseteq G$, maximal with $U \subseteq H$. If $H \neq M$, let $T \in S_p(M)$. If $T < S$, $T < N_S(T) \leq H \cap M$ which contradicts the maximality of $|M \cap L|_p$. This $T \in S_p(M)$. $\exists S_1 \in S_p(L), g \in S_1 - T$ such that $T^g = T$ and $M \neq M^g$. By the previous result, (M, M^g) is a primitive pair of characteristic p. We've shown (a) holds if $|M \cap L|_p = 1$ when M, L are two different p-locals. If $|M \cap M^g|_p = 1, \forall g \in G - M$, M is strongly p-embedded.

Bender's Little Theorem: Let (M_1, M_2) be a primitive pair of G. Suppose $F^*(M_1) \leq M_2$ and $F^*(M_2) \leq M_1$ then $\exists p : (M_1, M_2)$ has characteristic p.

Proof: See Stellmacher, 10.1.4.

Theorem 17: Let (M_1, M_2) be a primitive pair of G of characteristic p then $\exists i \in \{1, 2\}$ such that either (1) The action of M_i on $O_p(M_i/\Phi(M_i))$ is not p-solvable or (2) W_i is elementary abelian and the action of M_i on W_i is not p-stable.

Proof: See Stellmacher, 10.1.5.

Theorem 18: Let (M_1, M_2) be a primitive pair of characteristic p, then M_1 or M_2 has a non-abelian Sylow 2-subgroup.

Proof: If $p \neq 2$, it follows from the previous result and p-stability for groups with abelian 2-syslow subgroups. For $p = 2$, if the Sylow 2-groups are abelian, then $O_2(M_1) = O_2(M_2)$ and (M_1, M_2) is not primitive.

Theorem 19: Let M be p-saperable and A a p-subgroup of M satisfying $Phi(A) \leq O_p(M)$ and $A \not\leq O_p(M)$ then $\exists x \in O_{p,p'}(M)$ such that for $L = \langle A, A^x \rangle$, (a) $x \in O^p(L) \leq O_{p,p'}(M)$, (b) $[O^P(L), A] = O^p(L)$, and (c) $|A/(A \cap O_p(L))| = p$ and $[A \cap O_p(L), L] \leq O_p(M)$.

Proof: $\exists L$ with property (a). Choose L maximal among all such groups then (b) follows. $\overline{L} = L/O_p(L)$, $\overline{Q} = O_{p'}(\overline{L})$ so $\overline{L} = \overline{AQ}$. A is an elementary abelian p-group and $\Phi(A) \leq O_p(M) \cap L \leq O_p(L)$. Let $\mathcal{B}$ be the set of maximal subgroups of A. $\overline{Q} = \langle C_{\overline{Q}}(\overline{U}) : U \in \mathcal{B} \rangle$ so $[C_{\overline{Q}}(\overline{U}), A] \neq 1$ for some $U \in \mathcal{B}$ since A acts non-trivially on $\overline{Q}$. This implies $U = A \cap O_p(L)$ and $[U, O^p(L)] \leq O_p(L) \cap O_{pp'}(M) \leq O_p(M)$ and (c) follows.

Theorem 20: Let M be a group of characteristic 2 that possesses a section isomorphic to S_4 then M possesses a section isomorphic to S_4 .

Proof: Let M be a minimal counterexample. $O_2(S_3) = 1$ and $M/O_2(M) \leq N \lhd X < M$ and $X/N \approx S_3$. $X = M$ by minimality. Let $\overline{M} = M/N$ and $D \in S_3(M)$, $\overline{D} \approx C_3 \lhd M$. By Frattini, $M = N_M(D)N$. There are 2-elements that act nontrivially on the 3 group D. Let $t \in N_M(D)$ of minimal order. $\exists d \in D : |d| = 3, d^t = d^{-1}$, $\langle d, t \rangle / \langle t^2 \rangle \approx S_3$. Minimality of M shows $M = O_2(M)\langle d, t \rangle$ and $t^2 \in_2 (M)$. $\Phi(O_2(M)) = 1$ and $C_{O_2(M)}(d) = 1$. Thus $t^2 = 1$ and $\exists 1 \neq Z \in C_{O_2(M)}(t)$. $V = \langle z, z^d, Z^{d^2} \rangle$ and $|V| \leq 8$ and $V \lhd M$. Hence $V = C_2 \times C_2$ and $V\langle d, t \rangle \approx S_4$ so M is not a minimal counterexample.

Notation: $\mathcal{Q}(Z, X) = \{A \leq X : [Z, A, A] = 1 \neq [Z, A]\}$. $q(Z, X) = 0$ if $\mathcal{Q}(Z, X) = \emptyset$; $q(Z, X) = min\{e \in \mathbb{R} : |A/C_A(Z)|^e = |Z/C_Z(A)|, A \in \mathcal{Q}(Z, X)\}$, otherwise.

Theorem 21: Let M act faithfully on an elementary abelian 2-group, V and let A be an elementary abelian 2-subgroup of M. Suppose $C_M(O_{2'}(M)) \leq O_{2'}(M)$ and $|V/C_V(A)| < |A|^2$. Then M posseses a section isomorphic to S_3.

Proof: Among all the elementary abelian 2-subgroups that satisfy the condition, choose A of minimal order. Assume $|A| = 2$, then $A \in \mathcal{A}_V(M)$ and the result follows from Glauberman's theorem. If $|A| > 2$,$C_M(O_{2'}(M) \leq O_{2'}(M)$ means A acts non-trivially on $O_{2'}(M)$. Let $Q \subseteq O_{2'}(M)$ be minimal. $Q^A = Q$ and $[Q, A] \neq 1$ so $A_0 = C_A(Q)$ is a maximal subgroup of A and QA/A_0 acts faithfully on $C_V(A_0)$. The conclusion follows from the $|A| = 2$ case if $|C_V(A_0)/C_V(A)| \leq |A/A_0|^2 = 4$ which in turn follows from the minimality of A since $|V/C_V(A)| < |A|^2 \leq 4|V/C_V(A_0)|$.

Theorem 22: Let M be a group and V an elementary abelian normal p-subgroup of M; let $Z \leq V$ with $V = \langle Z^M \rangle$ and $Z \lhd O_p(M)$. Suppose $\exists A \leq O_p(M)$ with $[V, A, A] = 1$. Then $|A/C_A(V)|^q \leq |V/C_V(A)|$ where $q = q(Z, O_p(M))$.

Proof: See Stellmacher, 10.1.10.

Theorem 23: Let (M_1, M_2) be a solvable primitive pair of characteristic 2, then M_1 or M_2 has a section isomorphic to S_4.

Proof: See Stellmacher, 10.1.11.

Theorem 24: Let G be a group of even order, $O_2(G) = 1$. Suppose that for every 2-local M of G, (1) M has characteristic 2 and is solvable and (2) M does not possess a section isomorphic to S_4 then every maximal 2 local of G is strongly 2-embedded in G.

Proof: This is a direct consequence of the result preceeding Bender's theorem and the previous result.

24.3 Amalgam Graphs

Definition 4: $P_1, P_2 \leq G$, $|P_i| < \infty$. Construct a graph $\Gamma(G, P_1, P_2) = \Gamma$ as follows: Γ has verticies consisting of right cosets of P_1 and P_2; the verticies $P_i g_j$ and $P_n g_m$ are joined by an edge if $P_i g_j \neq P_n g_m$ and $P_i g_j \cap P_n g_m \neq \emptyset$. $\Delta(\alpha)$ denotes the verticies adjacent to α. G acts on graph by right multiplication on cosets. $\Delta(\alpha)$ is a set of vertices adjacent to α. $G \to Aut(\Gamma)$.

Theorem 25: Suppose G has two orbits and P_1, P_2 are representatives. Every vertex stabilizer G_α is a G-conjugate of P_1 or P_2 then (a) G acts transitively on Γ and every edge stabilizer in G is a G-conjugate of $P_1 \cap P_2$, (b) G_α acts transitively on $\Delta(\alpha)$, (c) $|\Delta(\alpha)| = |G_\alpha : G_{\alpha,\beta}|$, (d) $P_1 \cap P_2$ is the kernel of the action on Γ.

Proof: (a) For $P_i x \in \Gamma$ and $g \in G$, $P_i x g = P_i x$ is equivalent to $P_i g^{x^{-1}} = P_i$ is equivalent $g \in P_i^x$. (b) Let $\langle P_1 x, P_2 y \rangle$ be an edge. $\exists z \in P_1 x \cap P_2 y$. Hence $P_1 x = P_1 z$ and $P_1 x = P_1 z$ so z^{-1} conjugates $(P_1 x, P_2 y)$ to (P_1, P_2). The stabilizer of $(P_1 z, P_2 z)$ is in $P_1^z \cap P_2^z = (P_1 \cap P_2)^z$. (c) By (a), we can assume $\alpha = P_1$ then $\Delta(\alpha) = \{P_2 y : P_2 \cap P_1 \neq \emptyset\} = \{P_2 y : y \in P_1\}$ thus P_1 is transitive on $\Delta(\alpha)$. (d) By (a), any normal subgroup of G is contained in $P_1 \cap P_2$ fixes every vertex of Γ.

Theorem 26: Γ is connected iff $G = \langle P_1, P_2 \rangle$.

Proof: Assume $G = \langle P_1, P_2 \rangle$ and let Δ be a connected component of Γ that contains P_1. Since P_1 and P_2 are adjacent, $P_2 \in \Delta$. Since different components are disjoint, $\Delta = \Delta^{\langle P_1, P_2 \rangle} = \Delta^G$ and thus $\Delta = \Gamma$ by (a) above. Now assume Γ is connected and let $G_0 = \langle P_1, P_2 \rangle$ and $\Gamma_0 = \{P_1 x : x \in G_0\} \cup \{P_x x : x \in G_0\}$ be the coset graph of G_0 with respect to P_1, P_2. Γ_0 is connected. If $\Gamma = \Gamma_0$ then $G = G_0$. Assume $\Gamma \neq \Gamma_0$. Since Γ is connected, $\exists \alpha, \beta \in \Gamma$ such that $\alpha \in \Gamma_0, \beta \in \Gamma - \Gamma_0$. By (c) above, β and all other elements of $\Delta(\alpha)$ are in $\Gamma - \Gamma_0$. Hence Γ is not connected. Contradiction.

Theorem 27: Let $G = \langle P_1, P_2 \rangle$, $U \leq G_\alpha \cap G_\beta$ and (α, β) is an edge. The (1) $N_{G_\delta}(U)$ acts transitively on $\Delta(\delta), \delta \in \{\alpha, \beta\}$ and (2) if $U \leq G_\alpha \cap G_\beta$ then U acts trivially on Γ.

Proof: (2) together with (c) implies (1) so we may assume (1) holds. Let $\Gamma_0 = \alpha^{N_G(U)} \cup \beta^{N_G(U)}$. U fixes Γ_0. If $\gamma \in \Gamma_0$, $\exists g \in N_G(U)$ and $\delta \in \{\alpha, \beta\}$ such that $\gamma = \delta^g$. Then $\Delta(\delta^g) = \Delta(\gamma)$ and $N_{G_\gamma}(U) = N_{G_\delta}(U)^g$. By (1), $N_G(U)$ is transitive on $\Delta(\delta^g) = \Delta(\gamma)$. One of α^g, β^g is adjacent to γ and $\{\alpha^g, \beta^g\} \subseteq \Gamma_0$. It follows that $\Delta(\gamma) \subseteq \Gamma_0$. By the previous result, Γ is connected and we must have $\Gamma = \Gamma_0$ so U stabilizes every vertex in Γ.

Condition $\mathcal{A}$: Let G be a finite group generated by P_1, P_2, $T = P_1 \cap P_2$ satisfying: $C_{P_i}(O_2(P_i)) \leq O_2(P_i)$, $T \in S_2(P_i)$, $T_G = 1$, $P_i/O_2(P_i) \approx S_3$ and $[\Omega(Z(T)), P_i] \neq 1$.

Theorem 28: Let $\mathcal{A}$ holds and (α, β) be an edge of Γ. (a) $|G_\alpha : G_{\alpha,\beta}| = 3$ and is a Sylow 2 subgroup of G_α. $G_\alpha = \langle t, G_{\alpha,\beta} \rangle$ for $t \in G_\alpha - G_\beta$. (b) $|\Delta(\alpha)| = 3$ and $O_2(G_\alpha) = \bigcap_{\delta \in \Delta(\alpha)} (G_\alpha \cap G_\beta)$, (c) G_α acts 2-transitively on $\Delta(\alpha)$.

Proof: (a) follows from $P_1/O_2(P_i) \approx S_3$ and (b) and (c) follows from a previous result.

Notation: For the remainder of the section, $Q_\alpha = O_2(G_\alpha)$ and $Z_\alpha = \langle \Omega(Z(T)) : T \in S_2(G_\alpha) \rangle$.

Theorem 29: Suppose $\mathcal{A}$ holds and $\alpha \in \Gamma$, $V \lhd G_\alpha$, $T \in S_2(G_\alpha)$ and $\Omega(Z(T)) \leq V \leq \Omega(Z(Q_\alpha))$ and $|V : \Omega(Z(T))| = 2$ then $V = C_V(G_\alpha) \times W$, $W = [V, G_\alpha]$. $W = C_2 \times C_2$, $C_{G_\alpha}(W) = Q_\alpha$.

Proof: Let $D \in S_3(G_\alpha)$. $V = C_V(D) \times W$, $W = [V, D]$. By $\mathcal{A}$, since $G_\alpha = DT$, $W \neq 1$ and thus $|W| \geq 4$. Let $d \in D^\#$, $|V/\Omega(Z(T))| = 2 = |V/\Omega(Z(T^d))|$. $G_\alpha = \langle T, T^d \rangle$ means $|V/C_V(G_\alpha)| \leq 4$ so $C_V(G_\alpha) = C_V(D)$ and $|W| = 4$. The remainder follows from $\mathcal{A}$.

Theorem 30: Let $\mathcal{A}$ hold and (α, β) be an edge of Γ; (a) $Z_\alpha \leq \Omega(Z(Q_\alpha))$; (b) $Q_\alpha Q_\beta = G_\alpha \cap G_\beta \in S_2(G)$; (c) $C_{G_\alpha}(Z_\alpha) = Q_\alpha$; (d) $Z_\alpha Z_\eta \lhd G_\alpha$ iff $\exists \gamma \in \Delta(\alpha) - \{\beta\}$ such that $Z_\alpha Z_\beta = Z_\alpha Z_\gamma$.

Proof: (a) Let $T \in S_2(G_\alpha)$ then $Q_\alpha \leq T$ and $\mathcal{A}$ implies $\Omega(Z(Y)) \leq Z(Q_\alpha)$. (b) By $\mathcal{A}$ and a previous result, Q_α and Q_β have index 2 in $G_\alpha \cap G_\beta$ so it STS $Q_\alpha \neq Q_\beta$. If $Q_\alpha = Q_\beta$, now two previous results show G acts failthfully on Γ, and this contradicts $\mathcal{A}$.

Theorem 31: Let $\mathcal{A}$ hold and (α, β) be an edge of Γ. The following are equivalent: (1) the conclusion of Goldschmidt's Theorem holds; (2) $Z \leq Q_\beta$.

Proof: Assume the conclusion of Goldschmidt's theorem holds. For $\delta \in \{\alpha\beta\}$, either (i) $G_\delta = S_4$ and $Q_\delta \approx S_4 \times C_2$, or (ii) $G_\delta = S_4 \times C_2$ and $Q_\delta \approx C_2 \times C_2 \times C_2$. In either case, $Z_\delta - Q_\delta$ and by the previous result $Z_\alpha \not\leq Q_\beta$. Set $T = Q_\alpha Q_\beta$ and $E = Q_\alpha \cap Q_\beta$. The previous result gives $T \in S_2(G_\delta)$ and $|T/Q_\delta| = 2$. Thus $|Q_\alpha : E| = 2 = |Q_\beta : E|$ and $T = Q_\beta Z_\alpha$ and $Q_\alpha = EZ_\alpha$. Todo, more.

Definition 5: α, α' is a *critical pair* if $Z_\alpha \not\leq Q_{\alpha'}$ and $b = d(\alpha, \alpha')$. Let b be minimal.

Theorem 32: Suppose $\mathcal{A}$ holds and (a) (α, α') is a critical pair; (b) $G_\alpha \cap G_{\alpha+1} = Z_{\alpha'} Q_\alpha$, $G_{\alpha'-1} \cap G_{\alpha'} = Z_\alpha Q_{\alpha'}$; (c) $R \leq Z(G_\alpha) \cap Z(G_{\alpha+1}) \cap Z(G_{\alpha'}) \cap Z(G_{\alpha'-1})$ and $R = [Z(G_\alpha), G_{\alpha+1}) \cap G_\alpha] = [Z(G_{\alpha'}), G_{\alpha'-1}) \cap G_{\alpha'}]$ (d) $Z_\alpha = [Z_\alpha, G_\alpha] \times \Omega(Z(G_\alpha))]$ and $[Z_\alpha, G_\alpha] = C_2 \times C_2$; (e) $|Z_\alpha : \Omega(Z(Y))| = 2$ for $Y \in S_2(G_\alpha)$.

Proof: Minimality of (b) implies $Z_\alpha \leq Q_{\alpha'-1} \leq G_{\alpha'-1} \cap G_{\alpha'}$ and $Z_{\alpha'} \leq Q_{\alpha+1} \leq G_{\alpha+1} \cap G_\alpha$. $Z_\alpha \not\leq Q_{\alpha'}$ shows that $G_{\alpha'-1} \cap G_{\alpha'} = Z_\alpha Q_\alpha$ since $Q_{\alpha'}$ has index 2 in $G_{\alpha'-1} \cap G_{\alpha'}$. $Z_\alpha \lhd G_\alpha$ and $Z_{\alpha'} \lhd G_{\alpha'}$ so $R \leq Z_\alpha \cap Z_{\alpha'}$. By a previous result, $R \neq 1$ and so $Z_{\alpha'} \not\leq Q_\alpha$ and $G_{\alpha+1} \cap G_\alpha = Z_{\alpha'} Q_\alpha$. (a) and (b) follow and (c) follows from $R \leq Z_\alpha \cap Z_{\alpha'}$ and a previous result. These also show $|Z_\alpha / C_\alpha(Z_{\alpha'}(Z_\alpha) = |Z_{\alpha'}/Z_{\alpha'} Z(Z_\alpha) = 2$ and $C_{Z_\alpha}(Z_{\alpha'}) = \Omega(Z(G_{\alpha+1} \cap G_\alpha)$ which gives (d) and (f) and, with a previous result (e).

Theorem 33: Let $\alpha - 1 \in \Delta(\alpha) - \{\alpha + 1\}$. Suppose $(\alpha - 1, \alpha' - 1)$ is not a critical pair. Then (1) $Z_\alpha Z_{\alpha+1} = Z_\alpha Z_{\alpha-1}$; (2) $Q_\alpha \cap Q_\beta \lhd G_\alpha, \beta \in \Delta(\alpha)$; (3) α and α' are conjugate and b is even.

Proof: Since $(\alpha - 1, \alpha' - 1)$ is not critical, $Z_{\alpha-1}, Z_{\alpha'}] \leq R \leq Z_\alpha$, so $\langle Z_{\alpha'}, G_\alpha \cap G_{\alpha-1} \rangle \subseteq N(Z_{\alpha-1} Z_\alpha)$. The previous result gives (a). (b) follows by a previous result and the fact that G_α is transisitve on $\Delta(\alpha)$. Either $\alpha \in (\alpha')^G$ or $\alpha \in (\alpha' - 1)^G$, so the former holds and b is even. For (c), note α and $\alpha' - 1$ are conjugate so G_α and $G_{\alpha'-1}$ are conjugate. Then (b) gives $Z_\alpha \leq Q_{\alpha'-2} \cap Q_{\alpha'-1} = Q_{\alpha'-1} \cap Q_{\alpha'}$. This contradicts $Z_\alpha \not\leq Q_{\alpha'}$.

Theorem 34: Suppose $\alpha - 1 \in \Delta(\alpha) - \{\alpha + 1\}$ such that $(\alpha - 1, \alpha' - 1)$ is a critical pair then $b = 1$.

Proof: Put $R_1 = [Z_{\alpha-1}, Z_{\alpha'-1}]$. Assume $b > 1$. $Z_\alpha \leq Q_{\alpha+1}$ and $Z_{\alpha'} \leq Q_{\alpha'-1}$. $(\alpha - 1, \alpha' - 1)$ is a critical pair so $|R_1'| = 2$. $R_1 = [Z_{\alpha-1}, G_{\alpha-1} \cap G_\alpha] \leq (Z(G_{\alpha-1} \cap Z(G_\alpha)) \cap (Z(G_{\alpha'-2} \cap Z(G_{\alpha'-1}))$. $R_1 \leq [Z_{\alpha-1}, Z_{\alpha'-1}]$, so $[R_1, Z_{\alpha'}] = 1$. $\langle Z_{\alpha'}, G_{\alpha-1} \cap G_\alpha \rangle = G_\alpha$.

(1) $R_1 \leq Z(G_\alpha)$.
Let $\alpha - 2 \in \Delta(\alpha - 1) \setminus \{\alpha\}$. Now we show

(2) $(\alpha - 2, \alpha' - 2)$ is a critical pair.

If not, $Z_{\alpha+1}Z_\alpha = Z_{\alpha-1}Z_\delta, \delta \in \Delta(\alpha-1)$ $Z_{\alpha+1}Z_\alpha = Z_{\alpha+1}Z_{\alpha+2}$. Minimality of b gives $Z_{\alpha+1}Z_{\alpha+2} \leq Q_{\alpha'}$ and $Z_\alpha \leq Q_{\alpha'}$, so (α, α') is not a critical pair. Now put $R_2 = [Z_{\alpha-2}, Z_{\alpha'-2}]$. $\alpha - 2$ and (α, α') satisfy the hypothesis, hence $|R_2| = 2$.

(3) $R_2 = [Z_{\alpha-2}, G_{\alpha-2} \cap G_{\alpha-1}] \leq Z(G_{\alpha-1})$.
$\exists y \in G_{\alpha-1}, x \in G_\alpha : (\alpha-2)^y = \alpha$ and $(\alpha+1)^x = \alpha-1$. $[Z_\alpha, G_{\alpha-1} \cap G_\alpha] = [Z_{\alpha-2}, G_{\alpha-2} \cap G_{\alpha-1}] = (R_1)^y \leq Z_{\alpha-1}$. $R^x = [Z_\alpha, G_{\alpha+1} \cap G_\alpha]^x = [Z_\alpha, G_\alpha \cap G_{\alpha-1}] = (R_2)^y \leq Z(G_{\alpha-1})$. It follows that

(4) $R \leq Z(G_{\alpha+1})$, so

(5) $R \cap R_1 = 1$.
If not, $Z_{\alpha'} \leq Q_{\alpha'-2}$, $[R_2, Z_{\alpha'}] = 1 = [R_2, G_{\alpha-1}]$, so $R_2 = 1$. This contradicts $|R_2| = 2$.

(6) $b = 2$
If $b > 2$, $V_\alpha = \langle Z_\beta, \beta \in \Delta(\alpha) \rangle \lhd G_\alpha$. $V_{\alpha+1} = \langle Z_\beta, \beta \in \Delta(\alpha+1) \rangle \lhd G_{\alpha+1}$. $V_\alpha \leq Q_\alpha$, $V_{\alpha+1} \leq Q_{\alpha+1}$, and $Z_\alpha = \langle \Omega(Z(G_{\alpha+1} \cap G_\alpha)^{G_\alpha} \rangle \leq V_\alpha$. $Z_{\alpha+1} \leq Q_{\alpha+1}$, so

(7) $Z_\alpha Z_{\alpha+1} \leq V_\alpha \cap V_{\alpha+1}$.
Since $R_1 \leq Z(G_\alpha)$ is a 2-transitive action of G_α on $\Delta(\alpha)$. ${V_\alpha}' = R_1 \leq Z(G_\alpha)$. We show V_α is abelian and V_α is generated by involutions. V_α/R_1 is elementary abelian so $R_1 = \Phi(V_\alpha)$ and $R = \Phi(V_{\alpha+1})$, put $\overline{V_\alpha} = V_\alpha/Z_\alpha$. We get $Z_\beta/(Z_\alpha \cap Z_\beta) = 2, \forall \beta \in \Delta(\alpha)$, so $|\overline{Z_\beta}| = 2$. $\overline{V_\alpha} = \langle Z_\beta, \beta \in \Delta(\alpha) \rangle$, so $|\overline{V_\alpha}| \leq 8$. Set $W = V_\alpha \cap V_{\alpha+1} \lhd G_\alpha \cap G_{\alpha+1}$ then $Z_\alpha Z_{\alpha+1} \leq W$ and

(8) $V_\alpha = \langle W^{G_\alpha} \rangle$.
$\Phi(W) \leq \Phi(V_\alpha) \cap \Phi(V_{\alpha+1}) = R_1 \cap R = 1$ and W is elementary abelian ${V_\alpha}' \neq 1$ and $|V_\alpha/W| \geq 2$. The kernel of the action of G_α on $\overline{V_\alpha}$ contains Q_α since $[Z_{\alpha-1}, G_\alpha \cap G_{\alpha-1}] \leq R_1 \leq Z_\alpha$. $\overline{V_0} = [\overline{V_\alpha}, O^2(G_\alpha)]$. If $\overline{V_0} = 1$ $W \lhd G_\alpha$ and ${V_\alpha}' = 1$ but this contradicts ${V_\alpha}' = R_1$ and $|R_1| = 2$. Now suppose $\overline{V_0} \neq 1$ since $|\overline{V_\alpha}| \leq 8$,

(9) $|\overline{V_0}| = 4$.
Assume $|V_\alpha/W| = 2$. Let $x \in G_\alpha$ st $W^x \neq W$ then $V_\alpha = WW^x$. $W \cap W^x = Z(V_\alpha)$ and $|V_\alpha(W \cap W^x)| = 4$. Let $D \in S_3(G_\alpha)$, D acts non-trivially on $V_\alpha/(W \cap W^x)$ so all maximal subgroups of V_α that contain $W \cap W^x$ are D-conjugate. Every $x \in V^\#$ is an involution, V_α is elementary abelian contradicts ${V_\alpha}' = R_1$. We have shown $|V_\alpha/W| \geq 4$ so $|\overline{V_\alpha}| \leq 8$.

(10) $|V_\alpha| = 8$, $W = Z_\alpha Z_{\alpha+1}$ and $|\overline{W}| = 2$.
$Z_{\alpha'} \leq G_\alpha$, $Z_{\alpha'} \not\leq Q_\alpha$, we get $[\overline{V_0}, Z'_\alpha] \neq 1$. But $b = 2$, so $[V_\alpha, Z_\alpha] \leq [V_\alpha, V_{\alpha+1}] \leq W$. $\overline{W} = [\overline{V_0}, Z_{\alpha'}], \langle \overline{W}^{G_\alpha} \rangle = \overline{V_0}$, which contradicts (8), (9) and (10).

Goldschmidt's Theorem: If $\mathcal{A}$ holds either (i) $P_1 \approx P_2 \approx S_4$ or (ii) $P_1 \approx P_2 \approx C_2 \times S_4$.

Proof: Let G be a counter example and choose (G, P_1, P_2, T) with $|T|$ minimal. $b > 1$ and $(\alpha - 1, \alpha' - 1)$ is not a critical pair $\forall \alpha - 1 \in \Delta(\alpha) \setminus \{\alpha + 1\}$.

(1) $b = 0 \pmod 2$, $X = Q_\alpha \cap Q_{\alpha+1} \lhd G_\alpha$.
$|Q_\alpha : X| = |Q_{\alpha+1}| = 2$. Let $D \in S_3(G_\alpha)$, $\overline{G_\alpha} = G_\alpha/X$. $|\overline{G_\alpha}| = 12$, $\overline{Q_\alpha} \leq \overline{G_\alpha}$ and $|\overline{Q_\alpha}| = 2$ so $\overline{D} \lhd \overline{G_\alpha}$.

We get (2a) $L \lhd G_\alpha$, $|G_\alpha : L| = 2$,

(2b) $\overline{L} = S_3$,
(2c) $S_2(L) = \langle Q_\beta : \beta \in \Delta(\alpha)\rangle$,
(2d) $O_2(L) = X = Q_\alpha \cap Q_\beta, \forall \beta \in \Delta(\alpha)$,
(2e) $Q_{\alpha+1} = Z_{\alpha'} O_2(L))$, (f) $C_L(O_2(L)) \leq O_2(L)$.
$Z_\alpha \leq G_\alpha$, $Z_\alpha \leq Q_{\alpha+1} \leq O_2(L)$. $C_L(O_2(L)) \leq C_L(Z_\alpha) \leq Q_\alpha \cap L \leq O_2(L)$. By $A2$, $\exists t \in G_{\alpha+1} \setminus Q_{\alpha+1}, \alpha^t = \alpha + 2$ and $t^2 \in Q_{\alpha+1}$ $Q_{\alpha+1}, Q_\alpha^t \in S_2(L) \leq G_\alpha$, $L^t \leq G_{\alpha+2}$.

(3) $O_2(L)$ is not elementary abelian.
$A_1 = O_2(L)$, $A_2 = O_2(L^t)$ are elementary abelian of index 2 in $Q_{\alpha+1}$. If $A_1 = A_2$, $A_1 \lhd \langle G_\alpha, G_{\alpha+2}\rangle$. $\langle G_\alpha, G_\alpha \cap G_{\alpha+1}, G_{\alpha+1} \cap G_{\alpha+2}\rangle = \langle G_\alpha, G_{\alpha+1}\rangle = G$ such that $A_1 \neq A_2$, $Q_{\alpha+1}$ is non-abelian. $A = A_1 \cap A_2 = Z(Q_{\alpha+1})$, $|(Q_{\alpha+1}/A)| = 4$. $\langle G_\alpha, O^2(G_{\alpha+1}\rangle = N_G(A_1)$, which is a contradiction. $O^2(G_{\alpha+1})$ acts transitively on $(Q_{\alpha+1}/A)^\#$, its elements are involutions and $Q_{\alpha+1}$ is elementary abelian. $G_0 = \langle L, L^t\rangle$. Denote the largest normal subgroup of G_0 in $Q_{\alpha+1}$ by Q. ${G_0}^t = G_0, Q^t = Q$.

(4) We show $[Q, D] \neq 1$.
Suppose not put $\tilde{G_0} = G_0/Q$. $Q_{\alpha+1} \in S_2(L) \cap S_2(L^t)$. $(\tilde{G_0}, \tilde{L}, \tilde{L^t}, \tilde{Q_{\alpha+1}})$ satisfy $\mathcal{A}_\in$, $\mathcal{A}_\ni$, $\mathcal{A}_\triangle$. $\tilde{W} = [\tilde{Z_\alpha}, \tilde{D}] \neq 1$. $C_{\tilde{L}}(O_2(\tilde{L})) \leq O_2(\tilde{L})$, so $\mathcal{A}_\infty$ and $\mathcal{A}_\triangledown$ hold. Because of the minimality of $|T|$ and $|Q_{\alpha+1}| < |T|$, $\tilde{L} = S_4$ or $\tilde{L} = C_2 \times S_4$. $\tilde{W} = [O_2((\tilde{L}), O^2(\tilde{L})]$ is not contained in $O_2(\tilde{L}^t)$ and $\tilde{W} \leq \tilde{Z_\alpha}$ and so $O_2(L) = (O_2(L) \cap O_2(L^t))Z_\alpha$. Since $Z_\alpha \leq \Omega(Z(O_2(L)))$, $\Phi(O_2(L)) = \Phi(O_2(L) \cap O_2(L^t))$ and thus $\Phi(O_2(L)) = \Phi(O_2(L^t))$. $\Phi(O_2(L)) \lhd \langle G_\alpha, G_{\alpha+2}\rangle = G$ and $\mathcal{A}_\ni$ gives $\Phi(O_2(L)) = 1$ which contradicts (3) and (4).

(5) Let $\beta \in \Delta(\alpha) \setminus \{\alpha\}$, then $\langle Z_\alpha, Z_\gamma\rangle$ is not normal in L.
Put $\Delta(\beta) = \{\alpha, \delta, \gamma\}$ and $V_\beta = \langle Z_\alpha, Z_\beta, Z_\gamma\rangle \lhd G_\beta$. If $x \in Q_\alpha \setminus Q_\beta$ interchanges γ and δ and normalized L. If $\langle Z_\alpha, Z_\gamma\rangle$ is normal in L and also $\langle Z_\alpha, Z_\delta\rangle = \langle Z_\alpha, Z_\gamma^x\rangle$ is normal in L. Thus V_β is normal in L (which is not contained in $G_\alpha \cap G_\beta$) which contradiction!

(6) Let $b \geq 4, \alpha - 1 \in \Delta(\alpha) \setminus \{\alpha + 1\}$ and $\alpha - 2 \in \Delta(\alpha - 1) \setminus \{\alpha\}$ then $(\alpha - 2, \alpha' - 2)$ is a critical pair.
Assume not. $Z_{\alpha-2} \leq Q_{\alpha'-3} \cap Q_{\alpha'-2}$. Since $\alpha' - 2$ is conjugate to α, $Z_{\alpha-2} \leq Q_{\alpha'-3} \cap Q_{\alpha'-2} = Q_{\alpha'-2} \cap Q_{\alpha'-1} \leq G_{\alpha'-1} \cap G_{\alpha'} = Z_\alpha Q_{\alpha'}$. So $[Z_{\alpha-2}, Z_{\alpha'}] \leq [Z_\alpha, Z_{\alpha'}] \leq Z_\alpha$ and so $Z_{\alpha-2}Z_\alpha \leq Q_\alpha \cap Q_{\alpha-1}$ is normalized by $Z_{\alpha'}$ is normal in L which contradicts (5).

$\alpha - 1 \in \Delta(\alpha) \setminus \{\alpha + 1\}, x \in L \leq G_\alpha$ with $(\alpha - 1 = (\alpha + 1)^x$. Thus $\alpha - 2 = (\alpha + 2)^x$, which is adjacent to $\alpha - 1$. If $b \geq 4$, $(\alpha - 2, \alpha' - 2)$ is critical. Hence $R_2 = [Z_{\alpha-2}, Z_{\alpha'-2}] \leq Z(G_{\alpha-2} \cap G_{\alpha-1}) \cap Z_{\alpha'-2}$. Also, $b \geq 4$ also implies $Z_{\alpha'} \leq Q_{\alpha'-2}$ and $[R_2, Z_{\alpha'}] = 1$ and so $[R_2, L] = 1$ and $R_2 \leq Z(G_{\alpha+2} \cap G_{\alpha+1}$ since $x \in L$.
Now (α', α) is also a critical pair so $\exists \alpha' + 2$ such that $d(\alpha', \alpha' + 2) = 2$ and $(\alpha' + 2, \alpha + 2)$ is also critical. So $Z_{\alpha'+2} \leq Q_{\alpha'-2}$ and so $[R_2, Z_{\alpha'+2}] = 1$ since $R_2 \leq Z_{\alpha'-2}$. Hence $G_{\alpha+2} \cap G_{\alpha+3} = Q_{\alpha+2}Z_{\alpha'+2}$ is centralized by R_2. But then $R_2 \leq Z(G_{\alpha+2})$ and $R_2 \leq Z(G_{\alpha-2})$ after conjugation. This contradicts the action of $Z_{\alpha'-2}$ on $Z_{\alpha+2}$. This proves:
(7) $b \leq 4$
Finally, $Q \leq O_2(L^t) \leq Q_{\alpha+2}] = 1$.

Case a: $Z_{\alpha+2}$ is not contained in $O_2(L)$.
$Q_{\alpha+1} \leq O_2(L)Z_{\alpha+2}$ and $L = \langle (Z_{\alpha+2})^L\rangle O_2(L) = C_L(O_2(L))O_2(L)$. So $O^2(L) \leq C_L(Q)$ since $Q \lhd L$ but then $[Q, D] = 1$ which contradicts (4).

Case b: $Z_{\alpha+2} \leq O_2(L)$
$Z_{\alpha+2} \leq Q_\alpha$ and (7) implies $b = 4$. (6) then implies $Z_{\alpha+2}$ is not contained in $Q_{\alpha-2} = Q_{(\alpha+2)^x}$ and L^{tx} is normal of index 2 in $G_{\alpha-2}$. $\langle (Z_{\alpha+2})^{L^{tx}} \rangle \leq G_0$ has a Sylow 3 subgroup, D_2 of $G_{\alpha-2}$. But then $Q \lhd G_0$ shows $[Q, D] = 1$ which contradicts (4). This contradicts (4) since D_2 is a G_0 conjugate of $D \in S_3(G_\alpha)$. Assume $(\alpha - 2, \alpha' - 2)$ is not normal in L.

Amalgam example 1: $G = S_6$, $a = (12)$, $b = (12)(34)(56)$. $P_1 = C_G(a)$, $P_2 = C_G(b)$. $P_1 = \langle a \rangle \times \langle (34)(56) \rangle \times \langle (35)(46) \rangle$.

Amalgam example 2: $G = SL_3(2)$, $|G| = 168$. $P_1 = \{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}\}$. $P_2 = \{\begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{pmatrix}\}$. $G = \langle P_1, P_2 \rangle$. $P_1 \cong P_2 \cong S_4$. $P_1 \cap P_2 = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\}$. If M_1, M_2 are a solvable primitive pair oc characteristic 2, either M_1 or M_2 possesses a section isomorphic to S_4.

24.4 ONan

Theorem: Let M be a primitive maximal subgroup of G then either (1) $F^*(G) = F(G)$ [Example: $G = S_4$, $M = S_3$], (2) $F(G) = 1$ and $F^*(G) = N_1 \times N_2$ where N_1 and N_2 are the only minimal normal subgroups [G involves A_5] or (3) $F(G) = 1$ and $F^*(G)$ is the unique minimal subgroup pf G.

Chapter 25

Applications of Signalizers and Amalgams for groups with solvable proper subgroups

25.1 Outline and definitions

We refer to the major classification theorems in the Classification of Finite Simple Groups section. The goal here is to classify the N-groups, as defined below by reducing to these cases.

N-group: Non solvable groups all of whose 2-local subgroups are solvable.

Condition Z: $N_G(\Omega(\mathbb{Z}(S))) \leq N_G(S)$ for $S \in S_2(G)$.

Definition ZN-group: An N-group which satisfies condition Z.

Condition C: G is of even order and $C(t)$ is solvable $\forall t \in Inv(G)$.

Recall: M is *strongly-embedded* if $|M|_2 > 1$ and $|M \cap M^g|_2 = 1, \forall g \in G \setminus M$. $C_L(O_2(L)) \leq O_2(L)$ for all 2-locals, L.

Lemma: Let G be p-separable, $p \in \pi(G)$ and $P \in S_p(O_{p',p}(G))$ then $O_{p'}(G) = 1 \rightarrow C_G(O_p(G)) \subseteq O_p(G)$.

Proof: Given the definition of p-separable, this was proved earlier.

Observation: For an N-group, $O_{2'}(L) = 1$ for all 2-locals, L.

Modified ZN Theorem (Theorem 1): Let G be a ZN-group with $O_{2'}(G) = 1 = O_2(G)$ and $S \in S_2(G)$. Put $Z = O^2(G)$, $R = S \cap H$. One of the following holds:
(1) H contains a strongly embedded subgroup.
(2) R is dihedral or semi-dihedral.
(3) $Z \cap R \cong C_2$ and $Z \cap R$ is weakly closed in R with respect to H.
(4) $\Omega(R) = Z = C_2 \times C_2$.
The first outcome is handled by Bender's classification. The second by the Gorenstein-Walter classification

and the Alperin-Brauer-Gorenstein classification. The third case is handled by the Z^* theorem and the fourth case is handled by Goldschmidt's classification of groups with a strongly-closed abelian 2-subgroup.

Definition: G has local characteristic 2-type if $|G|$ has even order and $C_L(O_2(L)) \leq O_2(L)$.

Theorem 2: Let G be a ZC-group with $O_{2'}(G) = 1 = O_2(G)$ then case (1), (3) or (4) of the Modified ZN Theorem holds or $O^2(G)\Omega(\mathbb{Z}(S))$ has local characteristic 2.

Theorem 3: Let G be a ZN-group with $O_2(G) = 1$ then either (a) G possesses a strongly embedded subgroup or (b) there are two maximal 2-local subgroups, M_1, M_2 of $O^2(G)$ such that $M_1 \cong M_2 \cong S_4$ and $M_1 \cap M_2 \in S_2(M_i), i = 1, 2$.

Note: Conclusion (b) of theorem 3 implies case (2) of theorem 1.

25.2 Application of the Completeness Results

Theorem: Suppose G satisfies $\mathcal{C}$ and $O_{2'}(C(t)) \neq 1, \forall t \in Inv(G)$, then G has local characteristic 2-type.

Theorem: Let $\mathcal{B}$ be the set of maximal Abelian 2-subgroups of G that contain an elementary abelian subgroup of rank 3 then $\theta_B : a \mapsto O_{2'}(C_G(a)), a \in \Omega(B)^\#$ for $B \in \mathcal{B}$ is a solvable signalizer function. Denote its maximal element as $\theta_B(G)$.

Now we begin the proof of theorem 2 above.

Condition S: G is a ZC group with $O(G) = O_2(G) = 1$. $H = O^2(G)$ and $S \in S_2(G), Z = \Omega(\mathbb{Z}(S)), T = S \cap H \in S_2(H)$. $\mathcal{B}(G)$ is the set of maximal abelian 2-groups of G that contain a subgroup of order 8. For $B \in \mathcal{B}(G)$, $\theta_B(G) : a \mapsto O_{2'}(C_G(a)), a \in \Omega(B)^\#$. θ_B is a solvable $\Omega(B)$ signalizer functor. For $R = \theta_B(G)$, (1) $C_R(a) = O_{2'}(C_G(a)), a \in B^\#$, (2) $C_R(B_0) = O_{2'}(C_G(B_0)), 1 \neq B_0 \leq B$, (3) $R = \langle O_{2'}(C_G(a)), a \in B^\# \rangle$, (4) $R^g = \theta_{B^g}(G)$ for $g \in G$ so $N_G(B) \leq N_G(R)$.

25.3 $J(T)$-Components

Theorem 3: Let G be a ZN-group ofl local characteristic 2 with $O_2(G) = 1$ then G possesses a strongly embedded subgroup or there are two maximal 2-locals M_1 and M_2 of $O^2(G)$ such that $M_1 \cong S_2 \cong M_2$ and $M_1 \cap M_2 \in S_2(M_i)$.

25.4 N-groups of characteristic 2-type

G is a ZN-group of local characteristic 2-type with $O_2(G) = 1$, $S \in S_2(G), Z = \Omega(Z(S))$ and M is a 2-local containing $N_G(J(S))$.

Definition: $\mathcal{T}(M)$ is a set of 2 subgroups $T \leq M$ such that there is a 2-local L, $T \leq L \leq G$ and $L \not\leq M$.

Theorem: M is strongly embedded in G iff $\mathcal{T}(M) = \emptyset$.

Proof: If $\mathcal{T}(M) = \emptyset$ then M is strongly embedded. Suppose $\mathcal{T}(M) \neq \emptyset$ and M is strongly embedded. $N_G(T) \leq M, T \in \mathcal{T}(M)$. Choose $T \in \mathcal{T}(M)$ with $|M|$ maximal and let $T \leq L \leq G$ and $L \not\leq M$. $N_{N_0}(T) \leq M \cap L$ for $T \leq T_0 \in S_2(L)$ so $T = N_{T_0}(T) = T_0$ by maximality. $O_2(L) \leq T_0 \leq M \cap L$ so $O_2(L) \in \mathcal{T}(M)$ thus $L \leq N_G(O_2(L)) \leq M$, a contradiction. Apply Thompson Transfer lemma.

The Amalgam results give.

Theorem: Let $T \in \mathcal{T}(M)$. There exist two different maximal 2-locals, P_1, P_2 with $P_i \in S_2(T), i = 1, 2$ and either $P_1 \cong P_2 \cong S_4$ or $P_1 \cong P_2 \cong S_4 \times \mathbb{Z}_2$.

Proof of theorem 3

Assume M is not strongly embedded. Suffices to show $M_1 \cong M_2 \cong S_4$

Proof of theorem 1

We may assume HZ has local characteristic 2. If HZ has a strongly embedded subgroup, we're done. Otherwise, H contains a maximal 2-local, $P \cong S_4$. $O_2(P) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $P = N_H(O_2(P))$. $D \in S_2(P)$ is dihedral of order 8. After conjugation, $D \leq S \cap H = R$. Put $Z^* = \Omega(Z(R))$. $Z^* \leq O_2(P)$ and $\exists t \in Inv(O_2(P))$ with $O_2(P) = Z^* \times \langle t \rangle$. Thus $C_R(t) = C_R(O_2(P)) = O_2(P)$ and R is dihedral or semi dihedral.

Chapter 26

Classification of Finite Simple Groups

26.1 Early Results

Feit-Thompson (FT): The only finite simple groups of odd order are $\mathbb{Z}_p, p \neq 2$. The proof follows the CN classification which follows Suzuki's CA classification.

Proof of FT is similar to the proof that all CA groups are solvable. (In a CA-group, the centralizer of any element is abelian.). The plan is to try and prove the following: Let G be a minimal counterexample, for every maximal subgroup $M < G$, $\exists M_0 \lhd M$, such that:
(a) $C_{M_0}(a) = 1, a \in M - M_0$;
(b) $M \cap {M_0}^g = 1$ for $g \in G - M$;
(c) M_0 is nilpotent;
(d) M/M_0 is cyclic;
(e) the union of all such M_0's is a partition of G.
The notion of stability shortens the original proof.

Glauberman ZJ: If $C_G(O_p(G)) \leq O_p(G)$ and the action of G on its chief factors of G is $p-$stable then $G = N_G(Z(J(S)))$.

Glauberman's Z^* Theorem: Let G be a finite group and t and involution in G which is weakly closed in $C(t)$. Then $t^* \in Z(G^*)$ where $G^* = G/O_{2'}(G)$.

26.2 Centralizers of involutions

Basic question: Let G be a finite simple group and $N = C_G(t)$ for the central involution, t, of a Sylow subgroup. Can you show any simple group with this centralizer has to be G? This requires knowing the core of N which is trivial or a cyclic group in which $|N : C_H(O(N))| = 2$. $O(N)$ is trivial when G is a Lie group over characteristic 2, $A_m, m = 0, 1, 2 \,(\mathrm{mod}\ 4)$ and sporadic groups but is non trivial in Lie groups over odd characteristics. Walter showed that if G has 2-rank ≥ 5, and $O(G) = 1$, and $C_G(t)$ is 2-constrained, then $O(C_G(t)) = 1$. This started the interest in signalizers.

Glauberman 1: If $S \in S_2(G), z \in Inv(G)$ and z is not conjugate to any other involution in S then $zO(G) \in \mathbb{Z}(G/O(G))$.

Glauberman 2: Suppose $O_{p'}(H) = 1$ and $O_p(H) \neq 1$, p, odd, $P \in S_p(H)$. If H is p-constrained and p-stable, then $\mathbb{Z}(J(P)) \lhd H$.

Application of Glauberman 2: Let H be a p-local of G, $H \subseteq M = N_G(\mathbb{Z}(J(P))$. Suppose $R \in S_p(G), P \subseteq R$. If $P = R$, H contains a Sylow p-subgroup of G. If not, $Q = N_G(\mathbb{Z}(J(P))) > P$ and Q normalizes $\mathbb{Z}(J(P))$. $Q \subseteq M$ and a p-subgroup of M contains P properly. If M is p-constrained and p-stable with $O_{p'}(M) = 1$ we can repeat this argument. Thus we can "push-up" from a p-local to a Sylow p-subgroup. So every maximal p-local is conjugate to $N_G(\mathbb{Z}(J(P))$.

26.3 Recognition Problem

Motivation: Let (B, N) be the Bruhat structure of a simple group G^* then $G^* \cong G$ for any simple group G with the same Bruhat structure.

Define a $G^*(q)$ as a Lie group type over q. W is Coxeter if $w = \langle w_i \rangle, 1 \leq i \leq t$ and t is the rank and $(w_i w_j)^{k_{ij}} = 1$. Let $P \in S_p(G^*(q)), B = N_G(P)$ and let H be the complement of P in B. $\exists N$: (1) $B \cap N = H \lhd N$, (2) $G = \bigcup_{u \in N} BuB$, (3) $BuBu_iB \subseteq BuB \cup Buu_iB$, (4) $B^{u_i} \neq B$. $W = N/H$ is the Weyl group.

Setting: For some non-cyclic abelian 2-group, A, of G (I) $W_A = \langle O(C_G(a)), a \in Inv(A) \rangle$ has odd order and (II) if $W_A \neq 1$, $M = N_G(AW_A)$ is strongly embedded.

26.4 Major Classification Results

Brauer, Suzuki: Suppose the Sylow 2-subgroups of G are quaternion then $\mathbb{Z}^*(G)/O_{2'}(G) \cong C_2$.

Gorenstein, Walter: Suppose $O_{2'}(G) = 1$ and that the sylow 2 subgroups of G are dihedral then $F^*(G)$ is isomorphic to $PSL_2(q), q = 1 \pmod 2$ or A_7.

Alperin, Brauer, Gorenstein: Suppose G is simple and the Sylow 2-subgroups are semi-dihedral then G is isomorphic to $PSL_3(q), q = -1 \pmod 4$, $PSU_3(q), q = 1 \pmod 4$, or M_{11}.

Bender: Suppose G possesses a strongly embedded subgroup then the Sylow 2-subgroups of G are cyclic or quaternion or G possesses a normal series $1 \lhd M \lhd L \lhd G$ such that M, and G/L have odd order and L/M is isomorphic to $PSL_2(2^n)$, $Sz(2^{2n-1})$, or $PSU_3(2^n), n \geq 2$.

Goldschmidt: Suppose $S \in S_2(G)$ and A and Abelian subgroup of S such that $a \in A, a^g \in S \to a^g \in A$. Suppose that $G = \langle A^G \rangle$ and $O_{2'}(G) = 1$ then $G = F^*(G)$, $A = O_2(G)\Omega(T)$ and for every component K of G, the factor group $K/\mathbb{Z}(K)$ is isomorphic to $PSL_2(2^n)$, $Sz(2^{2n-1})$, $PSU_3(2^n), n \geq 2$, $PSL_2(q), q = 3, 5 \pmod 8$, $R(3^{2n+1})$, or J_1.

Thompson: Suppose G is a non-solvable group all of whose 2-locals are solvable $\forall p \in \pi(G)$, then $F^*(G)$ is isomorphic to $PSL_2(q), q > 3$, $Sz(2^{2n-1})$, $PSU_3(2^n), n \geq 2$, A_7, M_{11}, $PSL_3(3)$, $PSU_3(3)$ or ${}^2F_4(2)'$.

Gorenstein, Lyons, Janko, Smith: Suppose G is a non-solvable group all of whose 2-locals are solvable, then $F^*(G)$ is isomorphic to $PSL_2(q), q > 3$, $Sz(2^{2n-1})$, $PSU_3(2^n), n \geq 2$, A_7, M_{11}, $PSL_3(3)$, $PSU_3(3)$ or

${}^2F_4(2)'$.

Walter: Let G be a group with 2 rank ≥ 5 and $O_{2'}(G) = 1$ with the property that the centralizer of every involution is $2-$constrained then $O_{2'}(C(x)) = 1$ for every involution x.

Example of groups of semi-simple type: $GL_n(q)$, q, odd, $t \in Inv(G)$ has form $t = \begin{pmatrix} -I_m & 0 \\ 0 & I_r \end{pmatrix}, n = m + r$ and $C_G(t) = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, $A \cong GL_m(q)$ and $B \cong GL_r(q)$.

Definition: $e(G) = max\{m_p(H), H \leq G \text{ is a } 2-\text{local and } p \neq 2\}$. A group G is *quasi-thin* if $m_2(G) \geq 3$ but every $e(G) \leq 2$.

Classification decomposes as follows: (1) Minimal counterexample has characteristic 2-type ($C_H(O_p(H)) \leq O_p(H)$) where H is a 2-local (Lie type $q = 2^n$) small groups are quasi-thin (2) G is not of characteristic 2-type, small groups have $m_2(G) \leq 2$.

26.5 Connected Groups

Definition: Let Ω_G be a collection of subgroups of G *define* $\mathcal{D}(\Omega_G)$ as the graph with points Ω_G; two points $A, B \in \Omega_G$ are joined by an edge if $[A, B] = 1$. Note that G acts as a group of automorphisms on $\mathcal{D}(\Omega_G)$ via conjugation.

Theorem: Let Δ be a G-invariant collection of subgroups of G and $H < G$. The following are equivalent: (1) H controls fusion in $H \cap \Delta$ and $N_G(X) \leq H$ for $x \in H \cap \Delta$; (2) $H \cap H^g \cap \Delta = \emptyset$ if $g \in G \setminus H$; (3) the members of $H \cap \Delta$ fix a unique point in the permutation representation of G on G/H by right multiplication; (4) $H \cap \Delta$ is the uniion of a set, Γ, of connected components of $\mathcal{D}(\Delta)$ and $\Gamma \cap \Gamma^g = \emptyset$ if $g \in G \setminus H$.

Proof:

$1 \to 2$: Let $g \in G$ with $H \cap H^g \cap \Delta \neq \emptyset$. $\exists X \in H \cap \Delta$ with $X^g \leq H$ so H controls fusion in $H \cap \Delta$ and $X^{gh} = X, h \in H$. $gh \in N_G(X) \leq H$ so $g \in H$.

$2 \to 3$: Consider the representation $G \to G/H$. $X \in H \cap \Delta$ fixes Hg iff $X \leq H^g$ which happens iff $g \in H$.

$3 \to 4$: For $A \in H \cap \Delta$, $\{H\} = Fix(A)$ so $N_G(A) \leq H$. If $B \in \Delta$ is incident to A in $\mathcal{D}(\Delta)$ then $B \leq C(A) \leq H$ so $B \in H \cap \Delta$ and $H \cap \Delta$ is the union of some set Γ of connected components of $\mathcal{D}(\Delta)$. Further, if $A \in \theta \in \Gamma$ and $\theta^g \in \Gamma$ then $A^g \leq H$ so $\{H\} = Fix(A^g) = \{Hg\}$ and $g \in H$.

$4 \to 1$: If $X \in H \cap \Delta$ and $g \in G$ with $X^g \leq H$ then $X \in \theta \in \Gamma$ and $X^g \in \theta' \in \Gamma$, so $\theta' = \theta^g \in \Gamma \cap \Gamma^g$ hence $g \in H$.

Definition: Define $\mathcal{E}_k^p(G)$ to be the set of all elementary abelian p-subgroups of G of p-rank at least k. G is said to be *k-connected* for the prime p if $\mathcal{D}(\mathcal{E}_k^p(G))$ is connected. Define $\Gamma_{P,k}(G) = \langle N_G(X), X \rangle \leq P, m(X) \geq k \rangle$ and $\Gamma_{P,k}^0(G) = \langle N_G(X), X \leq P, m(X) \geq k, m(XC_P(X)) > k \rangle$. If $P \in S_p(G)$ then $\Gamma_{P,k}(G)$ is called the *k-generated p-core of G*.

Theorem: Let P be a p-group. Then (1) P is 1-connected for the prime p; (2) If $m(P) > 2$, $\exists E_{p^2} \cong U \lhd P$ and $X \in \mathcal{E}_2^p(P)$ is in the same connected component of $\mathcal{D}(\mathcal{E}_k^p(P))$ as U when $m(C_P(X)) > 2$; (3) If $p = 2$ and $\exists E_8 \cong U \lhd P$ then P is 2-connected for the prime 2; (4) If $p = 3$ and $m(P) > 3$ then P is 2-connected for the prime 3.

Proof: (1) follows from $\mathbb{Z}(G) \neq 1$. Assume $m(G) > 2$ then there is an $E_{p^2} \cong U \lhd G$ and $G/C_G(U) \leq SL_2(p)$ and $SL_2(p)$ is of p-rank 1. If $A \in \mathcal{E}_3^2(G)$ then $m(C_A(U)) \geq 2$ so $m(UC_A(U)) > 2$ and $m(C_A(U)) > 2$. If $U \neq E \in \mathcal{E}_2^p(G)$ is in the same connected component as U, then $\exists D : E \neq D \in \mathcal{E}_2^p(G)$ and E is adjacent to D and further, $m(C_G(E)) \geq m(DE) \geq 3$. All we need to show is that $A \in \mathcal{E}_2^p(G)$ is in the same connected component as U. But $\langle A, C_A(U), UC_A(U), U\rangle$ is in a path of $\mathcal{D}(\mathcal{E}_2^p(G))$ completing 2. Assume $p = 2$ and $E_8 \cong V \lhd G$ and let $E \in \mathcal{E}_2^p(G)$, we must show there is a path from E to V. For $e \in E : m(C_V(e)) \geq 2$ and so we can assume $e \in E \setminus V$ so $\langle E, \langle e, C_V(E)\rangle, C_V(e), V\rangle$ is a path in $\mathcal{D}(\mathcal{E}_2^p(G))$. $\exists E_8 \cong V \lhd G$ and the argument above establishes 4.

Theorem: Let $H \leq G, P \in S_p(H)$ and $k \in \mathbb{Z}^+$. Then (1) If $m(p) \geq k$ and $\Gamma_{P,k}(G) \leq H$ then $P \in S_p(G)$; and (2) If $m(p) > k$ and $\Gamma_{P,k}^0(G) \leq H$ then $P \in S_p(G)$.

Proof: Follows from previous result.

Theorem: Let $H \leq G$, $P \in S_p(G)$ and $m(p) \geq k$. Then the following are equivalent: (1) $\Gamma_{P,k}(G) < H$; (2) H controls fusion in $\mathcal{E}_k^p(H)$ and $N_G(X) \leq H$ for $x \in \mathcal{E}_k^p(H)$; (3) $m(H \cap H^g) < k$ for $g \in G \setminus H$; (4) each member of $\mathcal{E}_k^p(H)$ fixes a unique point in the permutation representation of G on G/H.

Proof: Parts 2, 3, 4 are equivalent by the above result except $\mathcal{E}_k^p(G)$ should be $\mathcal{E}_k^p(H)$. It remains to show 1 implies 2. Assume $\Gamma_{P,k}(G) \leq H$ and $X \in \mathcal{E}_k^p(H)$. It STS that if $g \in G$ with $X^g \leq H$ then $g \in H$. By Sylow, $\langle P, P^g\rangle \leq P$ and by the above $P \in S_p(G)$. By Alperin, $\exists P_i \in S_p(G), 1 \leq i \leq n$ and $g_i \in N_G(P \cap P_i)$ with $g = g_1 g_2 \dots g_n$, $X \leq P_1$ and $X^{g_1 g_2 \cdots g_i} \leq P \cap P_i$ and $m(P \cap P_i) \geq k$ so $g_i \in N_G(P \cap P_i) \leq \Gamma_{P,k}(G) \leq H$ and so $g = g_1 g_2 \dots g_n \in H$ and 2 holds.

Definition: If $k = 1$ in any of the above equivalent conditions we say H is *strongly p-embedded in G*.

Theorem: Let $P \in S_p(G)$ and suppose P is k-connected then (1) $\mathcal{E}_k^p(\Gamma_{P,k}(G))$ is a connected component of $\mathcal{D}(\mathcal{E}_k^p(G))$ and $\Gamma_{P,k}(G))$ is the stabiliser of that component; (2) G is k-disconnected for the prime p iff G has a proper k-generated p-core.

Proof: 1 implies 2. Let $H = \Gamma_{P,k}(G)$. By the earlier resutls, $\mathcal{E}_k^p(G)$ is a union of connected components of $\mathcal{D}(\mathcal{E}_2^p(G))$ while $\mathcal{E}_k^p(P)$ is contained in some component since P is k-connected and $H \leq N_G(\Delta)$. Hence $\mathcal{E}_k^p(H) \subseteq \Delta$ by Sylow. Thus $\Delta = \mathcal{E}_k^p(H)$ and $H = N_G(\Delta)$ and 2 holds.

Theorem: G posseses a strongly p-embedded subgroup iff G is 1-disconnected for the prime p.

Proof: Follows from previous result.

Theorem: Let $m_p(G) > 2, P \in S_p(G)$ and $\mathcal{E}_k^p(G)^0$ be the set of subgroups $X \in \mathcal{E}_k^p(G)$ with $m_p(XC_G(X)) > 2$. Then (1) $\mathcal{E}_k^p(G)^0$ is the set of points that are not isolated in $\mathcal{D}(\mathcal{E}_k^p(G))$; (2) $\mathcal{E}_2^p(\Gamma_{P,2}^0(G))^0$ is a connected component of $\mathcal{D}(\mathcal{E}_2^p(G))$ and $\Gamma_{P,2}^0(G))$ is the stabilizer of this connected component; (3) $\mathcal{D}(\mathcal{E}_2^p(G))^0$ is connected iff $G = \Gamma_{P,2}^0(G))$.

Proof: 1 is trivial and 3 easily follows from 2. By the previous result, $\mathcal{E}_2^p(G)^0$ is contained in a connected component Δ of $\mathcal{D}(\mathcal{E}_2^p(G))$. Thus $H = \Gamma_{P,2}^0(G) \leq N_G(\Delta)$. Let $\Gamma = \mathcal{E}_2^p(G)^0$. Since $\mathcal{E}_2^p(G)^0 \subseteq \Delta$ and H acts on Δ, $\Gamma \subseteq \Delta$ by Sylow. If $\Delta \neq \Gamma$, $\exists x \in \Gamma$, $Y \in \Delta \setminus \Gamma$

with X and Y are adjacent $\mathcal{D}(\Delta)$. WLOG, $X \in \mathcal{E}_2^p(G)^0$, so $Y \leq C_G(X) \leq H$ and hence $m_P(C_H(Y)) \geq m_P(XY) \geq 3$, $Y \in \Gamma$, a contradiction. So $\Delta = \Gamma$, it remains to show that if $X, X^g \in \Gamma$ then $g \in G$. Suppose $X, X^g \in \Gamma$ then $N_G(X) \leq H \geq N_G(X^g)$ so there is a $E_{p^3} \cong A \leq C_G(X) \leq H$ and $A^g \leq H$. So by Sylow take A, $A^g \leq P$. Now apply Alperin, using $\Gamma_{P,3}(G) \leq \Gamma_{P,2}(G)^0 \leq H$ to conclude $g \in H$.

Theorem: Let Γ be the elements $a \in G$ of order p with $m_p(C_G(a)) > 2$ and $\theta : \Gamma \to p'(G)$ such that $\forall a, b \in \Gamma, [a, b] = 1$ and all $g \in G : \theta(a^g) = \theta(a)^g$ and $\theta(a) \cap C_G(b) \leq \theta(b)$. Let $P \in S_p(G)$ and assume $G = \Gamma_{P,2}(G)$ and $O_{p'}(G) = 1$ and finally assume that either $\theta(a)$ is solvable for each $a \in \Gamma$ or the Signalizer Functor Theorem holds on G then $\theta(a) = 1, \forall a \in \Gamma$.

Proof: For $A \in \mathcal{E}_3^p(G)$, θ is an A-signalizer functor. For $B \in \mathcal{E}_2^p(G)$, define $W_B = \langle \theta(b) : b \in B^\# \rangle$. Then $\exists A \in \mathcal{E}_3^p(G)$ with $B \leq A$ and hence $W_B = W_A$ and $\Gamma_{A,2}(G) \leq N_G(W_A)$. In particular, if B, D are distinct members of $\mathcal{E}_2^p(G)$ adjacent in $\mathcal{D}(\mathcal{E}_2^p(G))$, $BD \in \mathcal{E}_2^p(G)$ so $W_B = W_{BD} = W_D$. Thus $G = \Gamma_{P,k}^0(G) \leq N_G(W)$ since $N_G(B) \leq \Gamma_{A,2}(G) \leq N_G(W)$. But by 1 and the solvable signalizer functor theorem, W is a p' group so $W \leq O_{p'}(G)$. Since $O_{p'}(G) = 1$ and $\theta(a) \leq W, \forall a \in \Gamma$, the lemma is proved.

Theorem: Let Γ be the elements $a \in G$ of order p with $m_p(C_G(a)) > 2$ and $P \in S_p(G)$ and assume $G = \Gamma_{P,2}(G)$ and $O_{p'}(G) = 1$, $C_G(a)$ is balenced for the prime p and for each $a \in \Gamma$ either $O_{p'}(C_G(a))$ is solvable or the Signalizer Functor Theorem holds on G then $O_{p'}(C_G(a)) = 1, \forall a \in \Gamma$.

Proof: For $a \in \Gamma$, let $\theta(a) = O_{p'}(C_G(a))$ and we know $\theta(a) \cap C_G(b) \leq \theta(b), \forall a, b \in \Gamma$ with $[a, b] = 1$ and applying the previous result, we're done.

26.6 Aschbacher's Plan

Definition: $m_{2,p}(G) = max_H\{m_p(H)\}$, where H is a 2-local of G. $e(G) = max\{m_{2,p}(G)\}, p$ odd.

Definition: $O_{p',E}(G)/O_{p'}(G) = E(G/O_{p'}(G))$.

Theorem: $P \in p(G)$ then (1) $O_{p',E}(N_G(P)) \leq C_G(O_p(G))$ and (2) if $P \leq O_p(G)$ then $O^p(F^*(N_G(P)) = O^p(F^*(G))$.

Proof: Todo.

Definition: G is *balenced* for p, prime if $O_{p'}(C_G(X)) \leq O_{p'}(G), \forall X < G : |X| = p$. $m_{2,p}(G) = max_H\{m_p(H)\}$, where H is a 2-local of G. $e(G) = max\{m_{2,p}(G)\}, p$ odd.

Theorem: Let $O_{p'}(G) = 1$ and $Aut_H(L)$ is balenced for the prime p for each $L \in Comp(G)$ and for each $L \in Comp(G)$ and each $H \leq G$ with $L \lhd H$ then G is balenced for the prime p.

Theorem: If G is a non-abelian simple group with $m_2(G) \leq 2$ then either (1) a Sylow 2-group of G is dihedrael, semi-dihedral, or $\mathbb{Z}_{2^n} \wr \mathbb{Z}_2$ and $G \cong L_2(q), L_3(q), U_3(q), q$, odd, or M_{11}; or (2) $G \cong U_3(4)$.

Theorem: If G is a non-abelian simple group with $m_2(G) > 2$ and G has a proper 2-generated 2-core then either G is of Lie type of characteristic 2 and Lie rank 1 ($L_2(2^n), L_2(2^n), Sz(2^n)$ or J_1).

Definition of B_p property: Let p be a prime and $O_{p'}(G) = 1$ and x and element of order p in G then $O_{p',E}(C_G(x)) = O_{p'}(C_G(x))E(C_G(x))$.

Theorem: Let $p \neq 2$ and suppose G contains no normal abelian subgroups of rank 3 then G has p-rank ≤ 2.

Theorem: If G is a non-abelian simple group with $m_2(G) \leq 2$ then either (1) a Sylow 2-group of G is dihedrael, semi-dihedral, or $\mathbb{Z}_{2^n} \wr \mathbb{Z}$ and $G \cong L_2(q), L_3(q), U_3(q), q$, odd, or M_{11}; or (2) $G \cong U_3(4)$.

Theorem: If G is a non-abelian simple group with $m_2(G) > 2$ and G has a proper 2-generated 2-core then either G is of Lie type of characteristic 2 and Lie rank 1 ($L_2(2^n), L_2(2^n), Sz(2^n)$ or J_1.

Definition of B_p property: Let p be a prime and $O_{p'}(G) = 1$ and x and element of order p in G then $O_{p',E}(C_G(x)) = O_{p'}(C_G(x))E(C_G(x))$.

Unbalenced Group Theorem: If G is a group with $F^*(G)$, simple which is unbalenced for the prime 2, then $F^*(G)$ is a group of Lie type and odd characteristic A_{2n+1}, $L_3(4)$ or He.

Component Theorem: Let G be a group with $F^*(G)$ simple satisfying the B_2 property and possessing an involutions, t, such that $O_{2',E}(C_G(t)) \neq O_{2'}(C_G(t))$ then G posseses a standard subgroup for the prime 2.

Standard Form Problem for (L, r): Determine all finite groups G possessing a standard subgroup H for the prime r: $E(H) \cong L$.

Theorem: Let G be a minimal counterexample to the classification theorem and assume G is generic of even characteristic then one of the following holds: (1) G possesses a standard subgroup for some $p \in \sigma(G)$, (2) there is a symplectic involution, t, such that $F^*(C_G(t))$ is a 2-group of symplectic type or (3) G is in the uniqueness case.

Aschbacher: Suppose G is a finite simple group, the B-Theorem holds, and $E(C_G(t)) \neq 1$ for some $t \in Inv(G)$. $\exists x \in Inv(G)$ and a quasi-simple group, K of $C(z)$ such that $C_{C(z)}(K)$ either has 2-rank 1 or is solvable with elementary abelian or dihedral 2-Sylow subgroups.

Standard form: Suppose $x \in Inv(G)$ and $H = C(x)$ has a normal quasi-simple subgroup L, of Lie type with odd characteristic such that $C_H(L)$ has 2-rank 1. We say H is in standard form with standard component L.

26.7 Outline of Thompson

J.G. Thompson proved that Frobenius kernels are nilpotent. It is enough to prove that a finite group which admits a fixed-point free automorphism α of prime order p is nilpotent, which Thompson did in his thesis.

Before Thompson's, it was known that a finite solvable group which admits a fixed-point free automorphism of prime order is nilpotent. This was proved by G. Higman and J. Witt. Here is a quick outline, making use of the more modern version of the normal p-complement theorems (and standard properties of coprime automorphisms).

Theorem 1: Let G be a finite group which admits a fixed-point-free automorphism α of prime order p such that G is not nilpotent, and let G have minimal order subject to this. Then $|G| = 1 \,(\mathrm{mod}\ p)$.

Proof: We may assume that G is not solvable. Hence we may choose an odd prime divisor q of $|G|$. Then G has an α-invariant Sylow q-subgroup Q, and $N(Z(J(Q)))$ is also α-invariant.

If $Z(J(Q)) \lhd G$ then α induces a fixed-point free automorphism on $G/Z(J(Q))$ so, by induction, $G/Z(J(Q))$ is nilpotent, and G is solvable, contrary to assumption. Hence $N(Z(J(Q)))$ is a proper subgroup of G, which is nilpotent by the minimality of G. The Thompson's normal q-complement theorem shows that G has a normal q-complement too. Since q was an arbitrary odd prime divisor of $|G|$, G has a normal Sylow 2-subgroup U and G/U is nilpotent by minimality of G. So G is again solvable, contrary to assumption.
This now reduces to proving the result in the case that G is solvable which reduces to representation theory. Further reducing to the case that $Q = F(G)$ is a minimal normal subgroup of G. This means Q is an elementary Abelian q-group for some prime q. Furthermore, G/M is an elementary Abelian r-group for some prime r. Let R be an α-invariant Sylow r-subgroup of G. Consider the semi-direct product $H = G\langle\alpha\rangle = QR\langle\alpha\rangle$. $R\langle\alpha\rangle$ is a Frobenius group of order $p|R|$, and acts faithfully as a group of automorphisms of Q. Now by Clifford's theorem, α can't act without non-trivial fixed-points on Q, contrary to the assumption that it does.

26.8 Dickson's Theorem

Theorem 2: (i) $SL_2(q)$ has cyclic groups of order $q-1$ and $q+1$, (ii) $P \in S_2(SL_2(q))$ is elementary abelian if q is even and generalized quaternion if q is odd.

Proof: $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ shows (i). Identify the two dimensional space over $GF(q)$ with the additive group of $GF(q^2)$; now look at the kernel of *det* into the cyclic group of order q^2-1 in $GF_2(q)$. The kernel has order $q+1$.

Theorem: Let λ be a generator for $GF(p^r)$, $p \neq 2$ and put $L = \langle \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$. Then, either (i) $L = SL_2(p^r)$ or (ii) $p^r = 9$, $L/Z(L) \cong A_5$, and L contains a subgroup isomorphic to $SL_2(3)$.

Proof: Gorenstein 2.8.4

26.9 Simplifying CN-theorem

Theorem 1: Suppose G is a minimal simple CNgroup of odd order and $P, Q \in S_p(G)$ with $P \cap Q \neq 1$ Then $P = Q$.

Theorem 2: Suppose G is a minimal simple CNgroup of odd order and $P \in S_p(G)$ then $P \subseteq N(P)'$.

From Theorem 1, it is clear the minimal counterexample cant be a 3-step group which gives 14.2.2 in Gorenstein. With these two theorems, we can use $N_G(P)$ in place of $N_G(Z(J(P)))$ in 14.2.3.

26.10 Some Bender Results

Theorem 3: Suppose G is a group in which every normalizer of a p subgroup is p-constrained. If $p = 2$ assume $cl(P) \leq 2$, $P \in S_p(G)$. Let E be an abelian p groups with $r(E) \geq 3$ such that E contains every p-element of $C_G(E)$. Then $O_{p'}(C_G(E))$ acts transitively on $\mathcal{N}_G^*(E, q)$, $p \neq q$.

Definition: $S \in S_2(G), S' = 1$ is an A^* group if there is a normal series $1 \subseteq N \subseteq M \subseteq G$ where N and G/M have odd order and M/N is a direct product of 2-group and $L_2(q)$ or JR.

Bender Uniqueness Theorem: Let G be a minimal simple group of odd order and U an elementary abelian subgroup with $|U| = p^3$. Then there is one and only one maximal subgroup $U < M < G$.

Bender A: Let G be an group with abelian S_2 subgroups then G is an A^* group.

Theorem 6: If G is p-solvable and $R \in p(G)$ is p-stable if $p \geq 5$ or $SL_2(3)$ is not involved.

Theorem 7: If $T \in p(G)$ and $M \in p'(G)$ with $M \lhd G$. Write $\overline{X} = XM/M$. $C_{\overline{G}}(\overline{T}) = \overline{C_G(T)}$ and $N_{\overline{G}}(\overline{T}) = \overline{N_G(T)}$.

Proof: Let $C^*/M = C_{G/M}(TM/M)$ and $N^*/M = N_{G/M}(TM/M)$. $NM \subseteq N^*$. If $x \in N^*$, $T^x \in S_p(TM)$, so $\exists y \in M : T^x = T^y$ and $xy^{-1} \in N(T)$. $xy^{-1})y = x \in NM$. So $N^* = NM$. $CM \subseteq C^* \subseteq N^* = NM$. Since $T \cap M = 1$, $C^* \cap N = C$ and $C^* = (C^* \cap N)M = CM$.

Theorem 8: If G is solvable and $R \in p(G)$ then $O_{p'}(C_G(R)) \subseteq O_{p'}(G)$.

Proof: By previous result, $O_{p'}(G) = 1$. Put $M = O_p(C_G(R))$, $T = O_p(G)$. $RM = R \times M$. $[C_{RT}(R), M] \subseteq M \cap RT = 1$. Put $C = C_{RT}(M)$. $C_{RT}(C) \subseteq C_{RT}(R) \subseteq C$. $[M, T] = 1$ and $T = F(G)$. $C_G(T) \subseteq T \cap M = 1$. So $M = 1$.

Theorem 9: If G is solvable of odd order and $O_p(G) = 1$, then $O_{p',p}(G)$ contains every normal abelian subgroup in $S \in S_p(G)$.

Proof: We can assume $O_{p'}(G) = 1$. $R = O_p(G)$, $V = R/\Phi(R)$, $\overline{G} = G/R$. $\overline{G}$ acts faithfully on V. $O_p(\overline{G}) = 1$. Let A be an abelian normal subgroup of $P \in S_q(G)$. $[P, A] \subseteq A$ so $[P, A, A] = 1$ and $[P, A] = 1$ so $[R, A, A] = 1$ and $\overline{A}$ has minimal polynomial $(x-1)^2$. Since G is p-stable, the minimal polynomial is $x - 1$.

Theorem 6a: If A acts on G, a p-group, with $(|G|, |A|) = 1$, $C = C_G(A)$. If $C_G(C) \subseteq C$ then $[A, G] = 1$.

Proof: Take $x \in N_G(C), y \in C$. $(x^{-1}yx)^a = x^{-1}yx$ and $x^a x^{-1}$ centralized y. So $x^a x^{-1} \in C_G(C) \subseteq C$. Thus A centralizes $N_G(C)/C$ stabilizing $1 \subseteq C \subseteq N_G(C)$ and A acts trivially in $N_G(C)$. Thus $N_G(C) \subseteq C$. Since G is nilpotent, $G = C$ and A acts trivially on G.

Bender B: If $A \neq B$ are two maximal subgroups of a simple group G with $F^*(A) \subseteq B$ and $F^*(B) \subseteq A$ then $F^*(A)$ and $F^*(B)$ are p-groups.

Theorem: If G has a fixed-point-free automorphism of prime order, p then G is nilpotent.

Theorem: G is p-stable iff $G/O_{p'}(G)$ is p-stable.

Theorem: Let G be a group with no non-trivial normal p-subgroups, $p \neq 2$ which satisfies one of the following:
(a) $|G|$ is odd;
(b) $S \in S_2(G)$ is abelian;
(c) $S \in S_2(G)$ is dihedral;
(d) $G \cong PSL_2(q)$;
(e) G is solvable and either $p \geq 5$ or $SL_2(3)$ is not involved in G;
then G is p-stable.

Hall-Higman Theorem: Let G be p-solvable with $O_p(G) = 1$ acting on V over $GF(p)$. Let x be an element of order p^n. The the minimal polynomial for x is $(x-1)^r$ where (i) $r = p^n$ or (ii) $\exists n_0 \leq n$ such that $p^{n_0} - 1 = q^k$ for which $Q \in S_q(G)$ are non-abelian and n_0 is the least such integer and $p^{n-n_0}(p^{n_0}-1) \leq r \leq p^n$.

This was the genisis of p-stability when looking identifying groups with $r = 2$. If x, y are conjugate p-elements but $\langle x, y \rangle$ is not a p-group and x can be represented over $GF(p)$ with quadratic polynomial then $SL_2(3)$ is involved. Consider A_8 and the elementary abelian subgroup of order 3^8.

Chapter 27

Motivation for Classification Plan

27.1 Semisimple and unipotent elements

Canonical group: $GL_n(q), q = p^k$ is a good prototype example of an "almost simple" group. Doing computations in $GL_n(q)$ is also easier than doing them in $PSL_n(q)$. There are two kinds of elements in $GL_n(q)$: *semisimple* elements are diagonalizable and have order co-prime to p while *unipotent* elements are upper (or lower) triangular and have centralizers that are nilpotent.

For example,

$$s = \begin{pmatrix} aI_r & 0_r \\ 0_{n-r} & bI_{n-r} \end{pmatrix}$$

is semisimple and its centralizer has the form

$$C(s) = \begin{pmatrix} GL_r(q) & 0_r \\ 0_{n-r} & GL_{n-r}(q) \end{pmatrix}$$

. The element

$$u = \begin{pmatrix} I_{r\times r} & 0_{r\times n-2r} & 0_{r\times r} \\ 0_{n-2r\times r} & I_{n-2r\times n-2r} & 0_{n-2r\times r} \\ I_{r\times r} & 0_{r\times n-2r} & I_{r\times r} \end{pmatrix}$$

is unipotent and its centralizer has the form

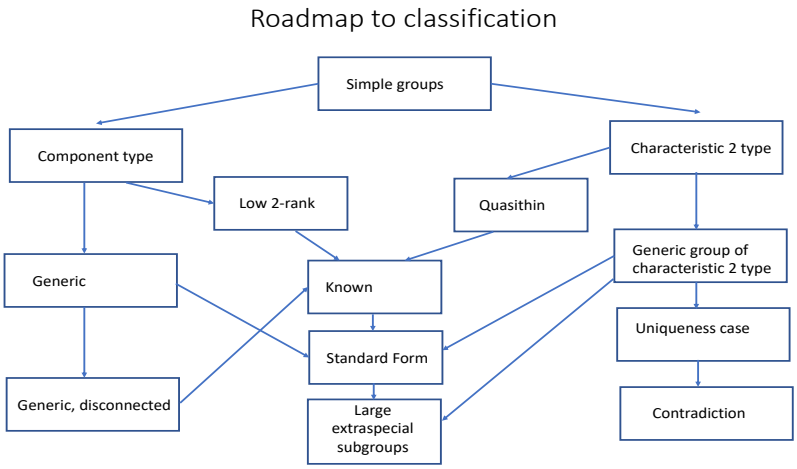
$$C(u) = \begin{pmatrix} X_{r\times r} & 0_{r\times n-2r} & 0_{r\times r} \\ P_{n-2r\times r} & Y_{n-2r\times n-2r} & 0_{n-2r\times r} \\ Q_{r\times r} & R_{r\times n-2r} & X_{r\times r} \end{pmatrix}$$

which is nilpotent. Further,

$$O_p(C(u)) = \begin{pmatrix} I_r & 0_r & 0_r \\ P & I_{n-2r} & 0_{n-2r} \\ Q & R & I_r \end{pmatrix}$$

.

Thus centralizers of semisimple elements are almost simple and have quasisimple components which dominate the structure of G. The centralizers of unipotent elements are dominated by a large normal p-group. This motivates the definition of $E(G)$ we saw earlier.



Definition: $C_G(x)$ is in *standard form* if $C_G(x)$ has one component, L, and $C_G(L)$ is small (often cyclic). An example is $C_G(s) = GL_1(q) \times GL_{n-1}(q)$. Finite simple groups can be determined by a centralizer in standard form.

Theorem 1: Let G be a finite group with $O_{2'}(G) = 1$, $s \in Inv(G)$ such that G has one component, L and $C_G(L)$ has a cyclic Sylow 2-group then either (1) $G = C_G(x)$, (2) $H \leq G \leq Aut(H)$, H simple, or (3) $L \times L \leq G \leq Aut(L \times L)$, L, simple.

Theorem 2: If u is unipotent $C(u) \cap C(O_p(C(u))) \leq O_p(C(u))$.

Definition: G is of characteristic p-type if for all p local subgroups, H, $C_H(O_p(H)) \leq O_p(H)$. It is usually difficult to determine G from $C(u)$ in characteristic 2-type groups. Lie groups of even characteristic are of characteristic 2-type.

Plan: First we try to show the centralizer of an involution in G is in standard form (i.e- is a Lie group of odd characteristic or A_{2k+1}). If not, G is of characteristic 2-type. If G is not of characteristic 2-type, G has an involution, x and $C(x)/O(C(x))$ has a component. This is a group of *component* type. Note that if G is not of component type, G is 2 constrained.

Applying signalizers: What are the components of $C(a)/O(C(a))$, $a \in A^{\#}$. Either $\theta(a) = O(C(a))$ is an A-signalizer or for some $a, b \in A^{\#}$, there is a b-invariant component, $\overline{L}$ of $\overline{C(a)} = C(a)/O(C(a))$: $O(Aut_{\overline{C(a)}}(\overline{L})) \cap C(\overline{b}) \neq 1$.

Definition: G is *balenced* if $O(C(x)) \leq O(G), x \in Inv(G)$.

Unbalenced group conjecture: Let $L \leq G \leq Aut(L)$, L, simple. If G is unbalenced (1) L is of Lie type with odd characteristic, (2) $L = A_{2k+1}$ or, $G = L_3(4), He$.

Component group conjecture: Let H be simple with $H \leq G \leq Aut(H)$, $x \in Inv(G)$. Let $\overline{L}$ be a

component of $\overline{C(x)} = C(x)/O(C(x))$ which is a known simple group, then G is a known simple group.

Now let G be a minimal counterexample then either G is balenced or there is an unbalenced component, $\overline{L}$.

Definition: A quasisimple group, L, is a *standard subgroup* of G, if $K = C_G(L)$ is tightly embedded in G, $N_G(K) = N_G(L)$ and L commutes with none of its conjugates. K is tightly embedded in G if $|K|$ is even and $|K \cap K^g|$ is odd if $K^g \neq K$.

Standard Form Problem for X: If H is simple, $H \leq G \leq Aut(H)$ and L is a standard subgroup of G with $L/Z(L) = H$ then H is a known simple group.

Fisher: G is a finite group, $\mathcal{D}$ a collection of subgroups or elements permuted by conjugation, $G = \langle \mathcal{D} \rangle$. Let $a, b \in \mathcal{D}$, A and elementary abelian group of $q = p^e$, $X = \langle a, b \rangle$, then X is either (1) elementary abelian of order q^2, (2) isomorphic to $SL_2(q)$ or (3) if order q^3, $[a, b] \in \mathcal{D}$. Originally, $q = 1$ and (3) does not occur (like symplectic or unitary groups over $GF(2)$ $|ab| = 3$. $M(22), M(23), M(24)'$ were found this way.

$\mathcal{G}$ is a graph with vertex set $\mathcal{D}$. $G(a)$ denotes the points adjacent to a. $A^\perp = A \cup G(A)$. $\mathcal{G}^c$ is the complementary graph.

The *triangle property* $A, B, C \in \mathcal{D}$, $C \in \mathcal{G}(A)$, $A, C \in \mathcal{G}^c(B)$. If C is conjugate to A in $\langle \langle A, B, C \rangle \cap B^\perp$; this is like a 3-transposition.

Let $\mathcal{G}$ and $\mathcal{G}^c$ be connected, G, simple, $\mathcal{D}$ is locally congugate ($[A, B] = 1$ or $A \cong B$ in $\langle A, B \rangle$) then $\langle A^\perp$ is transitive on $\mathcal{G}(A)$ and $\mathcal{G}^c(A)$ then G has a rank 3 permutation group.

Let $\mathcal{D}$ be a conjugacy class of 3-transpositions and G', simple. Then $\mathcal{G}$ and $\mathcal{G}^c$ are connected and G is simple.

We want to show $x \in G, |x| = p$ with $C_G(X) = H$ in standard form with $O_{p'}(H)$ small.

B_p **Conjecture:** Let G be a group with $O_{p'}(G) = 1$ then for all p elements, $x \in G$ $E(C(x)/(O_{p'}(C(x))) = E(C(x))O_{p'}(C(x))/O_{p'}(C(x))$.

We use a signalizer to analyze $O_{p'}(H)$. $\theta(A) \lhd G$. Consider $\mathcal{D}(G, \Omega)$ with A, B adjacent iff $[A, B] = 1$. For $B, D \in \Omega$ adjacent, $\theta(B) = \theta(BD) = \theta(D)$ then $\theta(A) = \theta(A)^g$ so $\theta(A) \lhd G$.

Chapter 28

Miscellaneous Results

28.1 Thompson like characterization

Netto: Let $x, y \in S_n$ be selected randomly. $Pr[\langle x, y\rangle = S_n] = \frac{3}{4}$.

Thompson Order Formula: Suppose G has $s \geq 2$ classes of involutions, $C_1, \ldots, C_s$. Put $d_{ijk} = |\{(u, v) : u \in C_i, v \in C_j, w = (uv)^m, w \in C_k\}|$. Put $n_i = \frac{|G|}{|C_i|}$ then $|G| = n_i n_j \sum_k d_{ijk}$. (Proved earlier)

Sample characterization of S_5: If G is a finite group with two conjugacy classes of involutions (ccl_1, ccl_2) having centralizers, $C_1 = C(u_1) = \langle u_1\rangle \times S_3$ and $C_2 = C(u_2) = D_8$ then $G = S_5$.
In S_5, $u_1 = (12)$, $u_2 = (12)(34)$.

1. $C_2 \in S_2(G)$.

2. After conjugation, we can assume, $u_1 \in C_2, u_2 \in C_1$. Let $x_1 \in ccl_1, x_2 \in ccl_2$ be involutions. Let $S_i = \{(u, v) : u \in x_1^G, v \in x_2^G, x_i \in \langle u, v\rangle\}$. Put $s_i = |S_i|$. $|G| = s_1|C_G(x_2)| + s_2|C_G(x_1)|$. (In the real G, $|ccl_G(u_1)| = 10$ and $|ccl_G(u_2)| = 15$.) Note that if $x \in x_1^G$ and $y \in x_2^G$, $|xy|$ is even (otherwise they would be conjugate), $x, y \in C((xy)^{\frac{|xy|}{2}})$.

3. $C_2 \cong D_8$ has three conjugacy classes of involutions. $D_8 = \langle u, v\rangle$, $u^2 = v^2 = 1$, $t = uv$ and $|t| = 4$. $C_2 = \langle (12), (14)(23)\rangle$, $t = (1324)$. $u_2 = (12)(34)$. $ccl_{C_2}((14)(23)) = \{(14)(23), (13)(24)\}$, $ccl_{C_2}((12)) = \{(12), (34)\}$, $ccl_{C_2}((12)(34)) = \{(12)(34)\}$. If $x \neq u_2$, $x \sim xu_2$. G contains a non-cyclic group, V, of order 4. $V = ccl_{C_2}((14)(23)) \cup \{1\} \cup ccl_{C_2}((12)(34))$. Since G has two classes of involutions, $s_2 = 0$ or $s_2 = 4$ and all the involutions in V are G-conjugate.

4. C_1 has three conjugacy classes of involutions. $x \neq u_1 \to x \nsim xu_1$. $\langle u_1\rangle \times S_3$. $ccl_{C_1}((12)) = \{(12)\}$, $ccl_{C_1}((12)(34)) = \{(12)(34), (12)(35), (12)(45), \}$, $ccl_{C_1}((34)) = \{(34), (35), (45)\}$. If $x \neq u_1$, $x \nsim xu_1$. Since G has two classes of involutions and for any $u_1 \neq x \in Inv(C_1)$, exactly one of x or xu_1 is conjugate to u_1, $s_1 = 9$.

5. $|G| = 9 \cdot 8 + 4 \cdot 12 = 120$, if $s_2 = 4$ or $|G| = 9 \cdot 8 = 72$, if $s_2 = 0$.

6. $|G| \neq 72$: If $|G| = 72$, let $P \in S_3(C_1)$, $P \subseteq Q \in S_3(G)$. $|Q| = 9$ and $\langle C_1, Q\rangle \subseteq N(P)$, $36 \mid |N(P)|$.

$\exists H : C(P) \subset H : |H| = 36$. $u_1 \in H$ and u_2 is a square in H. $H \lhd G$ and H contains all involutions in G hence $C_2 \cap H$ contains all involutions of C_2 but $|C_2 \cap H| = 4$ and there are 5 involutions in C_2.

7. By 3, C_2 has a normal four-group, V, with $u_2 \in V$ and all the involutions in V are G-conjugate. Let $x \in G$ then $x^{-1}u_2x \neq u_2$, $x^{-1}u_2x \in V$ then $x^{-1}C_2x \neq C_2$ and $u_2 \in C(x^{-1}u_2x) = x^{-1}C_2x$.

8. By 7, $N(V)$ contains at least two Sylow subgroups of G.

9. $C(V) = V$. $N(V)/V \cong S_3$ (permutes all 3 involutions of V), by 7 above, and $|N(V)| = 24$.

10. $G : N(V) = 5$. Let $\phi : G \to \{N(V)x_i\}$ be the permutation representation on the cosets of $N(V)$ in G. $ker(\phi) = 1$ so $G \cong S_5$. If $g \in G$ is an element of order 5, g acts as a 5-cycle on the cosets. If t is an element of order 2, it is of the form (12) or (12)(34).

28.2 Isaac's treatment of central extensions

Definition: A central extension of G is a pair (Γ, π) with $\pi : \Gamma \to G$ and $ker(\pi) = \mathbb{Z}(\Gamma)$.

Theorem 1: Let (Γ, π) be a central extension of G, $A = ker(\pi)$ and let $X = \{x_g | g \in G\}$ be coset representatives for Γ/A. Define α by $x_g x_h = \alpha(g,h)x_{gh}$, then $\alpha \in Z(G, A)$ is well defined and the resulting multiplication is associative.

Proof: Compute $x_g x_h x_k$ both ways and compare. Put $y_g = \mu(g)x_g$ then $y_g y_h = \mu(g)\mu(h)\mu(gh)^{-1}\alpha(g,h)$.

Definition: A divisible if $\forall a \in A, n \in \mathbb{Z}^+, \exists b \in A : b^n = a$. $M(G) = H(G, \mathbb{C}^\times)$. $\hat{A}$ is the set of linear characters of A.

Theorem 2: Let A be abelian, $Q \subseteq A$, Q, divisible and $|A : Q| < \infty$ then Q is complemented in A.

Proof: By induction on $|A : Q|$. True if $|A : Q| = 1$. Choose $a \in G \setminus A$. $n = |aQ|$ in A/Q. $u = a^n$, $v \in Q : v^n = u$. Put $b = av^{-1}$ and $\langle b \rangle \cap Q = 1$. $\overline{A} = A/\langle b \rangle$. $\overline{Q} = Q\langle b \rangle / \langle b \rangle$ and $\overline{Q} = Q$. $|\overline{A} : \overline{Q}| = |A : Q\langle b \rangle| < |A : Q|$, so $\overline{Q}$ is complemented by induction and $\exists B \subseteq A : B \cap Q\langle b \rangle = \langle b \rangle$ and $QB = A$. $Q \cap B = Q \cap Q\langle b \rangle \cap B = Q \cap \langle b \rangle = 1$.

Theorem 3: If F is algebraically closed and G is finite, $|H(G, A)| \mid |G|$.

Proof: Claim: $B(G, F^\times)$ is divisible: $B(G, F^\times)$ is complemented in $Z(G, F^\times)$. For $\beta \in B(G, F^\times)$, $\beta = \delta(\mu)$ for some $\mu : G \to F^\times$. Choose $\nu(g) \in F^\times : \nu(g)^n = \mu(g)$, we can do this since F is algebraically closed. $\delta(\nu)^n = \delta(\mu) = \beta$. We can apply previous lemma and once we show $|H(G, F^\times)| < \infty$.

For $\alpha \in Z(G, F^\times)$, put $\mu(g) = \prod_{x \in G} \alpha(g, x)$. $\alpha(g, hx)\alpha(h, x) = \alpha(gh, x)\alpha(g, h)$ so $\prod_{x \in G} \alpha(g, hx)\alpha(h, x) = \prod_{x \in G} \alpha(gh, x)\alpha(g, h)$ so $\mu(g)\mu(h) = \mu(gh)\alpha(g, h)^{|G|}$. $\alpha(g, h)^{|G|} \in B(G, F^\times)$ and $exp(H(G, F^\times)) \mid |G|$. Putting $U = \{\alpha \in Z(G, F^\times) : \alpha^{|G|} = 1\}$ and $A = \langle B(G, F^\times), \alpha \rangle$. $|A : B(G, F^\times)| \mid |G|$. By the previous result, $B(G, F^\times)$ is complemented in $Z(G, F^\times)$ so $B(G, F^\times)U = Z(G, F^\times)$. $\forall u \in U, u : G \times G \to \{y \in F : y^{|G|} = 1\}$. $|H(G, F^\times)| = B(G, F^\times)U : B(G, F^\times)| \leq |U| < \infty$, and we can apply the previous result, proving the lemma.

Definition: Choose a set of coset representatives in Γ/A, as before and $\pi(x_g) = g$. Let $\alpha \in Z(G, A)$, defined by $x_g x_h = \alpha(g,h)x_{gh}$. For $\lambda \in \hat{A}$, define $\eta(\lambda) = \overline{\lambda(\alpha)}$. $\lambda(\alpha)(g,h) = \lambda(\alpha(g,h))$. Bar is the canonical map

from $Z(G, \mathbb{C}^\times)$ to $H(G, \mathbb{C}^\times) = M(G)$. $\eta : \hat{A} \to M(G)$ is defined by that map, called the *standard map.*

Theorem 4 (Schur): Given G and A, abelian, there is a central extension with $ker(\pi) = A = M(G)$

Proof: Let M be a complement of $B(G, F^\times)$ in $Z(G, F^\times)$. Let $M = \hat{A}$. Define $\alpha(g, h)$ by $\alpha(g, h)(\gamma) = \gamma(g, h), \gamma \in M$. $\alpha(g, h) \in A$. $\alpha(gh, k)\alpha(g, h)(\gamma) = \gamma(gh, k)\gamma(g, h)$. Since γ runs over factor sets, $\alpha \in Z(G, F^\times)$. Let Γ, G, X be as in the earlier results. $\lambda(\alpha(g, h))) = \alpha(g, h)(\gamma) = \gamma(g, h)$ and $\lambda(\alpha) = \gamma$. $|A| = |\hat{A}| \geq |\eta(\hat{(}A))| = |M(G)| = |A|$.