Finite Group Theory

David A. Craven

Michaelmas Term, 2010

Contents

Chapter 0

Preliminaries

We assume that the reader is familiar with the concepts of a group, subgroup, normal subgroup, quotient, homomorphism, isomorphism, normalizer, centralizer, centre, simple group.

Definition 0.1 A *p-group* is a group, all of whose elements have order a power of p.

Proposition 0.2 let G be a finite p-group. Then $|G| = p^n$ for some n, and $\mathrm{Z}(G) \neq 1$.

Definition 0.3 Let G be a finite group, and let p be a prime. Suppose that $p^m \mid |G|$, but $p^{m+1} \nmid |G|$. A *Sylow p-subgroup* of G is a subgroup P of G of order p^m.

Theorem 0.4 (Sylow's theorem, 1872) Let G be a finite group, and let p be a prime.

(i) Sylow p-subgroups exist, and the number of them is congruent to 1 modulo p.

(ii) All Sylow p-subgroups are conjugate in G.

(iii) Every p-subgroup is contained in a Sylow p-subgroup.

Definition 0.5 Let G be a group. A *series* for G is a sequence

$$1 = G_0 \trianglelefteqslant G_1 \trianglelefteqslant G_2 \trianglelefteqslant \cdots \trianglelefteqslant G_r = G$$

of subgroups of G with $G_{i-1} \trianglelefteqslant G_i$ for all $1 \leqslant i \leqslant r$. It will sometimes also be denoted (G_i). If G_i/G_{i-1} is abelian, (G_i) is an *abelian* series. If G_i/G_{i-1} is simple, (G_i) is a *composition* series. The *length* of a series is the number of terms in it, so in the example above it has length r.

If a group possesses an abelian series, we say that it is *soluble*.

Theorem 0.6 (Burnside's $p^\alpha q^\beta$-theorem, 1904) Any finite group whose order is of the form $p^\alpha q^\beta$, for primes p and q, is soluble.

Definition 0.7 Let G be a group.

(i) Let h and k be elements of G. The *commutator* of h and k, denoted $[h, k]$, is the element $h^{-1}k^{-1}hk$.

(ii) Let H and K be subgroups of G. The *commutator* of H and K, denoted $[H, K]$, is the **subgroup generated by** all commutators $[h, k]$ for $h \in H$ and $k \in K$. (Note that the elements of $[H, K]$ are products of commutators, and not necessarily commutators $[h, k]$.)

(iii) The *derived subgroup* of G, denoted G', is $[G, G]$. Write $G^{(1)} = G'$ and define $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$.

(iv) By $[x, y, z]$ we mean the *left-normed commutator* $[[x, y], z]$. We extend this notation by induction, so that

$$[x_1, x_2, x_3, \ldots, x_{n-1}, x_n] = \big[[x_1, x_2, \ldots, x_{n-1}], x_n\big] .$$

Definition 0.8 Let G be a finite group. If G possesses a norrmal subgroup K and a subgroup H such that $K \cap H = 1$ and $G = HK$, then G is the (internal) *semidirect product* of K by H.

If K is a finite group and $\phi : H \to \mathrm{Aut}(K)$ is a homomorphism, then we may construct a group G such that $G = K \rtimes H$ and the elements h of H act on K by conjugation as $h\phi \in \mathrm{Aut}(K)$. This is to define a multiplication on the set $H \times K$ by

$$(h', k')(h, k) = (h'h, (k')^{h\phi}k).$$

This group so defined is denoted $G = K \rtimes H$ or $G = H \ltimes K$. This formula is meant to mimic the conjugation formula

$$h'k'hk = h'h(k')^h k$$

in any finite group. This is often referred to as the external semidirect product. If $G = K \rtimes H$ is an external semidirect product, then the natural subgroups $\bar{K} = \{(1, k)\}$ and $\bar{H} = \{(h, 1)\}$ make G into an internal semidirect product, and the other direction is equally easy. Hence from now on we will identify internal and external semidirect products.

Theorem 0.9 Any finite abelian group is the direct product of cyclic groups.

Definition 0.10 Let G be a finite permutation group on a set X.

(i) G is *transitive* if, for any two points x and y in X, there is an element $g \in G$ such that $xg = y$.

(ii) G is *imprimitive* if there is a partition p of X that is preserved by G, and the parts of p are neither X nor singleton sets. G is *primitive* if it is not imprimitive.

(iii) G is *n-transitive* if, for any two n-tuples $\mathbf{x}$ and $\mathbf{y}$ of distinct points in X there is an element $g \in G$ such that $\mathbf{x}g = \mathbf{y}$.

If G is a permutation group on a set X, and $x \in X$, denote by G_x the stabilizer of x in G, i.e., the elements $g \in G$ such that $xg = x$.

Proposition 0.11 Let G be a transitive permutation group on a finite set X.

(i) G is n-transitive if and only if G_x is $(n-1)$-transitive, for some $x \in X$.

(ii) If G is 2-transitive then G is primitive.

(iii) G is primitive if and only if G_x is a maximal subgroup of G, for some (and hence every) $x \in X$.

Proof: If G is n-transitive, then any n-tuple of distinct elements ending in x can be sent to any other n-tuple of distinct elements ending in x, so that (by removing the last term from the n-tuples) we see that G_x is $(n-1)$-transitive.

To see the converse, let $\boldsymbol{x} = (x_1, \dots, x_n)$ and $\boldsymbol{y} = (y_1, \dots, y_n)$ be any two n-tuples of distinct elements. We need to prove that there exists $g \in G$ such that $\boldsymbol{x}g = \boldsymbol{y}$. Since G is transitive, there exists $h, k \in G$ such that $x_n h = y_n k = x$. As G_x is $(n-1)$-transitive, there exists $l \in G_x$ such that

$$(x_1 h, x_2 h, \dots, x_{n-1} h)l = (y_1 k, y_2 k, \dots, y_{n-1} k).$$

The element hlk^{-1} maps $\boldsymbol{x}$ to $\boldsymbol{y}$, proving (i).

Let p be a partition of X that is preserved by G, proving that G is imprimitive. Let x and y be elements of X lying in the same part, and let z be an element not in this part. Since G preserves p, there is no element of G fixing x and mapping y to z, so G is not 2-transitive on X. This proves (ii).

Let H be the stabilizer of a point x in X, and let M be a maximal subgroup of G containing H. As X is the set of cosets of H in G, let the parts of the partition p be given by the cosets of M in G. This partition is clearly preserved by G, and hence G is not primitive. Hence if G is primitive then point stabilizers are maximal subgroups.

The converse is very similar: suppose that $X = X_1 \cup X_2 \cup \cdots X_n$ is a partition of X proving that G is imprimitive. Let x be a point in X_1, and let H be the stabilizer of x. Write M for the stabilizer of X_1. Notice that $M < G$ since $X_1 \neq X$, and since $X_1 \neq \{x\}$ we have $H < M$, so that H is not a maximal subgroup of G. $\square$

Definition 0.12 (i) If V is a vector space, $\mathrm{GL}(V)$ is the set of linear transformations of V. If $V = (\mathbb{F}_q)^n$ we denote $\mathrm{GL}(V)$ by $\mathrm{GL}_n(q)$, and consider it as all invertible $n \times n$ matrices.

(ii) $\mathrm{SL}(V)$ is the subset of $\mathrm{GL}(V)$ consisting of all transformations of determinant 1.

(iii) The *dihedral group* D_{2n} is the group with the presentation

$$\langle x, y \,:\, x^n = y^2 = 1,\, x^y = x^{-1} \rangle.$$

(iv) By C_n we denote the cyclic group of order n.

(v) The symmetric group on n letters is denoted by S_n, and the alternating group on n letters is denoted by A_n.

(vi) By E_{p^n} we mean the *elementary abelian* p-group of order p^n, i.e., the direct product of n copies of C_p.

Proposition 0.13 (i) If $G = C_{p^n}$ then $\mathrm{Aut}\, G$ is abelian, of order $p^{n-1}(p-1)$.

(ii) If $G = E_{p^n}$ then $\mathrm{Aut}\, G \cong \mathrm{GL}_n(p)$.

Theorem 0.14 For $n \geqslant 5$, A_n is simple.

Proposition 0.15 If G is a simple group of order 60 then G is isomorphic with A_5.

Proof: We will show that G has a subgroup of order 12, since in this case the standard homomorphism from G into S_5 must be injective (as G is simple) and lie inside A_5 (again, since G is simple). Notice that G cannot have any subgroups of index less than 5 because S_n has order less than 60 for $n \leqslant 4$. To find a subgroup of order 12, we show that if P is a Sylow 2-subgroup of G then either $\mathrm{N}_G(P)$ or $\mathrm{C}_G(t)$ for some $t \in G$ of order 2, has (at least) order 12. Certainly $|\,\mathrm{N}_G(P)|$ is either 4 or 12, since it is an odd multiple of 4 not greater than 12, so we assume that $P = \mathrm{N}_G(P)$. In this case, there are fifteen Sylow 2-subgroups of G.

Let Q be a Sylow 5-subgroup of G. We see that $\mathrm{N}_G(Q)$ has order at most 10 (since G has no proper subgroups of order greater than 12) and so there are at least six Sylow

5-subgroups of G, yielding at least 24 elements of G of order 5. This implies that at least two Sylow 2-subgroups intersect non-trivially, else there would be 45 elements of order 2 or 4, a contradiction. Let t be an element of order 2 in $P \cap P^g$ for some $g \in G$, and consider $|\,\mathrm{C}_G(x)|$. This contains P, so has order a multiple of 4, and is larger than P, so has order at least 12, completing the proof. $\square$

Definition 0.16 Let G be a finite group, and let H be a subgroup of G, and let $\{x_1, \dots, x_n\}$ be a right transversal to H in G. Let χ be a character of H, and extend χ to a class function (not a character) of G by setting $\chi(g) = 0$ for $g \in G \setminus H$. Define a class function χ^G on G by

$$\chi^G(g) = \sum_{i=1}^{n} \chi(x_i^{-1} g x_i).$$

The class function χ^G is the *induced character* of χ to G.

Definition 0.17 Let G be a finite group. A *G-module* is an abelian group A, together with a group action $\cdot : A \times G \to A$ such that $(a+b) \cdot g = a \cdot g + b \cdot g$.

We will meet G-modules (as opposed to $\mathbb{C}G$-modules) when we deal with cohomology in Chapter 2.

Chapter 1

The 1900s

1.1 $\mathrm{PSL}_n(q)$

Our first result of this course is to produce new simple groups. We know that the alternating groups A_n for $n \geqslant 5$ are simple, and the groups $\mathrm{PSL}_n(q)$ for $(n, q) \neq (2, 2), (2, 3)$ are also simple, as we will prove in this section. This result for prime fields is due to Jordan, in about 1870, but for non-prime fields it is a result of Moore in 1893, and also treated by Burnside in 1894.

The groups $\mathrm{GL}_n(q)$ and $\mathrm{SL}_n(q)$ act on an n-dimensional vector space. If we quotient out by the centre, to get $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$, we no longer get an action on an n-dimensional vector space, but on $(n-1)$-dimensional projective space. Recall that n-dimensional projective space is the set of all lines (1-dimensional subspaces) in an $(n+1)$-dimensional vector space. If V is a vector space, the projective space associated with V is denoted $P(V)$.

Lemma 1.1 Let V be an n-dimensional vector space over $\mathbb{F}_q$. The kernel of the action of $\mathrm{GL}(V)$ on $P(V)$ is $\mathrm{Z}(\mathrm{GL}(V))$.

Proof: Clearly $\mathrm{Z}(\mathrm{GL}(V))$ is the set of all scalar matrices. Firstly, scalar matrices act trivially on $P(V)$ since they fix every line setwise, so the kernel of the action contains every scalar matrix. To see the converse, notice that if a matrix fixes every line then it must be a scalar matrix, since the entire space is a single eigenspace. □

Hence $\mathrm{PGL}(V)$ and $\mathrm{PSL}(V)$ act faithfully on $P(V)$. In order to prove that $\mathrm{PSL}_n(q)$ is simple, we will have to find some generators for it, prove it is perfect, and then use a theorem to prove that it is simple.

Let T be a linear transformation of rank 1. We have two cases: either $\mathrm{im}\, T \cap \ker T = 0$, in which case T is (up to a scalar) a projection; or $\mathrm{im}\, T \subseteq \ker T$, in which case the (invertible) matrix $T + I_n$ is a *transvection*. Denoting the matrix with a 1 in the (i, j) position and 0 elsewhere by $E_{i,j}$, a typical example of a transvection in $\mathrm{SL}_n(q)$ is of the form $I + aE_{i,j}$ for $a \in \mathbb{F}_q \setminus \{0\}$ and $i \neq j$. Notice that if a generator for $\operatorname{im} T$ is x, then we may choose a basis with x as the last basis element, and extend to a basis for the kernel as the last $n-1$ entries, then the matrix form of $I + T$ has a single non-zero entry off the diagonal, in the top-right corner. Hence the set of transvections form a set of conjugacy classes in $\mathrm{GL}_n(q)$, each with a representative of the form $I + aE_{1,n}$. The *centre* of a transvection $I + T$ is the image of T, a line in the vector space.

Lemma 1.2 The group $\mathrm{SL}_n(q)$ is generated by the transvections $I + aE_{i,j}$ for $i \neq j$.

Proof: Notice that if M is a matrix, then multiplying M on the left by the transvection $1 + aE_{i,j}$ is equivalent to adding a copies of the jth row to the ith row of M. It is easy to see, using Gaussian elimination, that one may row reduce a matrix in $\mathrm{SL}_n(q)$ to the identity. The product of these transvections is the original matrix, and hence the transvections generate $\mathrm{SL}_n(q)$, as claimed. $\square$

By expressing transvections as commutators, this proves that $\mathrm{SL}_n(q)$ is perfect.

Proposition 1.3 If q is a prime power, and $q \geqslant 4$ and $n \geqslant 2$, or $n \geqslant 3$, then all transvections are commutators, and so $\mathrm{SL}_n(q)$ is perfect.

Proof: We first deal with the case $n = 2$: let a be a non-zero element of $\mathbb{F}_q$, and let x be an element of $\mathbb{F}_q$. We have the commutator equation

$$\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & (a^2-1)x \\ 0 & 1 \end{pmatrix}.$$

Since $\mathbb{F}_q$ has order at least 4, we may choose $a \neq 0$ so that $a^2 - 1 \neq 0$; by varying x we get all upper unitriangular matrices as commutators. Using the formula $[x, y]^g = [x^g, y^g]$, we get that all transvections are commutators in $\mathrm{SL}_2(q)$.

It remains to deal with the case where $n \geqslant 3$. In this case, we have the commutator identity

$$[I + aE_{1,2}, I + E_{2,n}] = I + aE_{1,n},$$

and since all transvections are conjugate to one of these, this proves that all transvections are commutators. Hence $\mathrm{SL}_n(q)$ is perfect for all $n \geqslant 3$ also. $\square$

In order to prove that a finite perfect group is actually simple, we need a criterion for this, called Iwasawa's lemma.

Theorem 1.4 (Iwasawa's lemma) Let G be a finite primitive permutation group on a set X, and let A be an abelian normal subgroup of the stabilizer of some point $x \in X$. If the G-conjugates of A generate G, then any normal subgroup of G contains G'. In particular, if G is perfect then G is simple.

Proof: Let K be any non-trivial normal subgroup of G, so that K is not contained in G_y for some $y \in X$. By conjugating A, we may assume that $y = x$. Since G is primitive, G_x is a maximal subgroup of G, and so $G = G_x K$. Let $g = hk$ be an element of G, with $h \in G_x$ and $k \in K$. We have

$$A^g = A^{hk} = A^k,$$

as $A \trianglelefteqslant G_x$. As K is a normal subgroup of G, we therefore get that $A^k \leqslant AK$. However, the conjugates of A generate G, and hence $G = AK$.

Since $G = AK$, we have $G/K = AK/K \cong A/(A \cap K)$; as A is abelian, AK/K is abelian, and so K contains G'. This completes the proof. $\square$

Of course, we need to prove that the action of $\mathrm{PSL}_n(q)$ on projective space is primitive in order to apply Iwasawa's lemma. We also need to find a candidate for the abelian normal subgroup of the point stabilizer.

Proposition 1.5 The group $\mathrm{PSL}_n(q)$ acts 2-transitively on projective $(n-1)$-space.

Proof: We prove that $\mathrm{PSL}_n(q)$ is transitive and that the stabilizer of a point is transitive on the remaining points. Let V denote an n-dimensional $\mathbb{F}_q$-vector space, with basis $x_1, \dots, x_n$. Clearly $\mathrm{PSL}_n(q)$ acts transitively on projective $(n-1)$-space, since $\mathrm{GL}_n(q)$ can send any point to any other point. Let α, β and γ be distinct lines in $P(V)$; we wish to find an element that fixes α and sends β to γ. Without loss of generality, we may assume that α is generated by x_1 and β by x_2.

Writing a generator for γ as $a = (a_1, a_2, \dots, a_n)$, any matrix in $\mathrm{SL}(V)$ with second row a and first row $(1, 0, \dots, 0)$ satisfies the requirements. (Notice that we may scale a so that the matrix lies in $\mathrm{SL}(V)$ without affecting its action on $P(V)$.) $\square$

The image of a transvection in $\mathrm{PSL}_n(q)$ is called an *elation*. The *centre* of an elation is the centre of the corresponding transvection, a point in projective space. Hence every elation fixes a specific point in projective space. The elations with a given centre $\alpha \in P(V)$ form a subgroup of G_α isomorphic with $\mathbb{F}_q^\times$, an abelian subgroup. Also, since conjugates of elations are elations, the elations with centre α form an abelian normal subgroup of G_α.

Applying Iwasawa's lemma to this abelian normal subgroup, we get the following theorem.

Theorem 1.6 If $n \geqslant 3$, or $n = 2$ and $q \geqslant 4$, then $\mathrm{PSL}_n(q)$ is simple.

1.2 The Transfer

Most of this course will be spent understanding the concept of fusion and using it.

Definition 1.7 Let G be a group, and H a subgroup of G. Let A and B be non-empty subsets of H. If there is $g \in G$ such that $A^g = B$ but there is no $g \in H$ with this property, then A and B are said to be *fused* in G.

We start this chapter with a simple result of Burnside, which will be used later in this section.

Proposition 1.8 (Burnside, 1900) Let G be a finite group, and P be a Sylow p-subgroup of G. If two elements of $\mathrm{Z}(P)$ are fused in G, then they are fused in $\mathrm{N}_G(P)$. (They cannot be conjugate in P since they lie in the centre of P.)

Proof: Suppose that x and y are elements of $\mathrm{Z}(P)$, and that $x^g = y$. Since $x, y \in \mathrm{Z}(P)$, $P \leqslant \mathrm{C}_G(x)$ and $P \leqslant \mathrm{C}_G(y)$. Also $P^g \leqslant \mathrm{C}_G(x)^g = \mathrm{C}_G(y)$. Thus both P and P^g lie inside $\mathrm{C}_G(y)$, and thus by Sylow's theorem there is some $h \in \mathrm{C}_G(y)$ such that $P^{gh} = P$. Hence $gh \in \mathrm{N}_G(P)$, and

$$x^{gh} = (x^g)^h = y^h = y,$$

since h centralizes y. Thus gh conjugates x to y, as required. $\square$

In the same vein, in Exercise Sheet 1 we see Thompson's transfer lemma.

In this section we will define the transfer homomorphism and give some of its properties. Let G be a group, and let H be a subgroup of G of finite index n. Choose (right) coset representatives x_i for H in G, so that

$$G = \bigcup_{i=1}^{n} Hx_i.$$

Since the right cosets partition the group, for any element $g \in G$, the element $x_i g$ can be written in the form hx_j, for some $h \in H$. For $g \in G$, we use this to get a function ϕ_g mapping i to j. We claim that ϕ_g is a permutation of $\{1, \ldots, n\}$. To see this, suppose that $i\phi_g = j\phi_g$; thus $x_i g = hx_k$ and $x_j g = h'x_k$, and so

$$g^{-1}x_i^{-1}hx_k = 1 = g^{-1}x_j^{-1}h'x_k,$$

which implies that $x_j x_i^{-1} = h'h^{-1}$. Hence x_i and x_j come from the same right coset, and thus $i = j$; so ϕ is a permutation.

Let $\theta : H \to A$ be any homomorphism from H to an abelian group A. We define the *transfer* of θ to be

$$g \mapsto \prod_{i=1}^{n} (x_i g x_{i\phi_g}^{-1})\theta,$$

an element of A. (Notice that each $x_i g x_{i\phi_g}^{-1}$ is an element of H, and so each term in the product is an element of A; thus the order of the product is not important.)

Theorem 1.9 (The transfer, Burnside, 1900 [3]) Let G be a group, and let H be a subgroup of G of index n. Let $\{x_1, \ldots, x_n\}$ be a right transversal to H in G. If $\theta : H \to A$ is a homomorphism from H to an abelian group A, then the transfer of θ is a homomorphism from G to A, and does not depend on the choice of right transversal.

Proof: Let $\{t_1, \ldots, t_n\}$ be another right transversal to H in G, and order the t_i so that $Ht_i = Hx_i$ for all i. In addition, write $t_i = h_i x_i$ for some $h_i \in H$, and note that

$$h_i(x_i g x_{i\phi_g}^{-1})h_{i\phi_g}^{-1} = t_i g t_{i\phi_g}^{-1}.$$

Using this relation, and the fact that the image of θ is abelian, we may reorder the terms in the product to get

$$\prod_{i=1}^{n} \left(h_i(x_i g x_{i\phi_g}^{-1})h_{i\phi_g}^{-1} \right) \theta = \prod_{i=1}^{n} (x_i g x_{i\phi_g}^{-1})\theta \cdot \prod_{i=1}^{n} (h_i h_{i\phi_g}^{-1})\theta.$$

Since ϕ is a permutation, this latter term is clearly 1, and so the transfer of θ does not depend on the choice of transversal.

All that is left is to prove that the transfer of θ is a homomorphism. Let a and b be two elements of G, and write τ for the transfer of θ.

$$\begin{aligned}
(ab)\tau &= \prod_{i=1}^{n} (x_i(ab)x_{i\phi_{ab}}^{-1})\theta \\
&= \prod_{i=1}^{n} \left((x_i a x_{i\phi_a}^{-1})(x_{i\phi_a} b x_{i\phi_{ab}}^{-1}) \right) \theta \\
&= \prod_{i=1}^{n} (x_i a x_{i\phi_a}^{-1})\theta (x_{i\phi_a} b x_{i\phi_{ab}}^{-1})\theta \\
&= \prod_{i=1}^{n} (x_i a x_{i\phi_a}^{-1})\theta \cdot \prod_{i=1}^{n} (x_{\phi_a} b x_{i\phi_{ab}}^{-1})\theta \\
&= (a\tau)(b\tau).
\end{aligned}$$

This proves that τ is a homomorphism, as needed. $\square$

Notice that the transfer is into an abelian group, and so the kernel of it contains G'. Thus if G is perfect the transfer is always trivial.

We have proved that the transfer does not depend on the choice of transversal and so it makes sense to use specific transversals to make calculating it easier. In Exercise Sheet 2 we will calculate the transfer for S_4, so we will not do a specific example here, but we will show a way of making the transversals nice.

Let g be an element of G, and let H be a subgroup of index n in G. Let $\{x_1, \dots, x_n\}$ be a right transversal to H in G. In the proof of Theorem 1.9, the cycle shape of the permutation ϕ_g does not depend on the transversal, and so we order the x_i so that the permutation ϕ_g is

$$\phi_g = (1, 2, \dots, r_1)(r_1 + 1, r_1 + 2, \dots, r_1 + r_2)(r_1 + r_2 + 1, \dots) \dots .$$

Write d for the number of cycles in ϕ_g, and for $1 \leqslant i \leqslant d - 1$ let s_i denote the sum of the first i of the r_j (and write $s_0 = 0$). With this ordering, we have that, for each i,

$$\prod_{j=s_i+1}^{s_{i+1}} (x_j g x_{j\phi_g}^{-1})\theta = (x_{s_i+1} g^{r_{i+1}} x_{s_i+1}^{-1})\theta.$$

In particular, if we set $y_i = x_{s_{i-1}+1}$, we get that

$$g\tau = \prod_{i=1}^{d} (y_i g^{r_i} y_i^{-1})\theta.$$

Also, the sum of the r_i from $i = 1$ to $i = d$ is n, and $y_i g^{r_i} y_i^{-1}$ lies in H.

This yields the following proposition.

Proposition 1.10 Let G be a group and let H be a subgroup of index n, and let $\theta : H \to A$ be a homomorphism to an abelian group A. Write τ for the transfer of θ. Let $\{x_1, \dots, x_n\}$ be a right transversal to H in G, and let $g \in G$. Write d for the number of cycles in ϕ_d. There is a suitable ordering of the x_i, and integers $r_1, \dots, r_d$, such that for $y_i = x_{r_1+\dots+r_{i-1}+1}$, we have:

(i) $y_i g^{r_i} y_i^{-1} \in H$ for $1 \leqslant i \leqslant d$;

(ii) $\displaystyle\sum_{i=1}^{d} r_i = |G : H|$;

(iii) $\displaystyle\left(\prod_{i=1}^{d} y_i g^{r_i} y_i^{-1}\right)\theta = g\tau$.

This result will be used in the proof of Burnside's normal p-complement theorem, which is the content of the next theorem. Before we state it, we define the notion of a normal p-complement: a finite group G is said to have a *normal p-complement* if there exists a normal subgroup K of G such that $p \nmid |K|$ and $|G/K|$ is a power of p, i.e., $G = K \rtimes P$ for some Sylow p-subgroup P of G.

Theorem 1.11 (Burnside normal p-complement theorem, 1900 [4]) Let G be a finite group, and let P be a Sylow p-subgroup of G. If $P \leqslant \mathrm{Z}(\mathrm{N}_G(P))$, then G has a normal p-complement.

Proof: Let P be a Sylow p-subgroup of G, and notice that since $P \leqslant \mathrm{Z}(\mathrm{N}_G(P))$, P is abelian. Let $\theta : P \to P$ denote the identity map and let τ be the transfer of θ. We will show that $\ker\tau \cap P = 1$; then $|G|/|\ker\tau| \geqslant |P|$, but $|\operatorname{im}\tau| \leqslant |P|$, and we get that $G/\ker\tau = P$, proving that $\ker\tau$ is a normal p-complement for G.

Let g be a non-trivial element of P, and consider $g\tau$. As in Proposition 1.10, choose a transversal $x_1, \dots, x_n$ (where $n = |G : P|$) and a subset $y_1, \dots, y_d$ of the x_i, and also the integers $r_1, \dots, r_d$. Since $y_i g^{r_i} y_i^{-1} = h$ lies in P, we see that g^{r_i} and h are G-conjugate elements of P, whence they are $\mathrm{N}_G(P)$-conjugate by Proposition 1.8. Since P lies in the centre of $\mathrm{N}_G(P)$, $g^{r_i} = h$, and so (remembering that $\theta = \mathrm{id}_P$)

$$g\tau = \prod_{i=1}^{d} (x_i g^{r_i} x_i^{-1}) = \prod_{i=1}^{d} g^{r_i} = g^n \neq 1,$$

as n and p are coprime. Thus $g \notin \ker\tau$, as required. □

Cayley proved in 1878 (Exercise 1.3) that if a finite group has cyclic Sylow 2-subgroups then it has a normal 2-complement. Burnside's normal p-complement theorem extends this result to all primes, and we do so now.

Corollary 1.12 Let G be a finite group, and p the smallest prime dividing $|G|$. If the Sylow p-subgroups of G are cyclic then G is not simple; in particular, if G is a simple group then p^2 must divide $|G|$.

Proof: Let P be a Sylow p-subgroup of G. By Proposition 0.13(i), we know that the order of $\operatorname{Aut} C_{p^n}$ is $p^{n-1}(p-1)$. Now recall that $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ is isomorphic to a subgroup of $\operatorname{Aut} P$, and since P is cyclic, $P \leqslant \mathrm{C}_G(P)$. Thus $|\mathrm{N}_G(P)/\mathrm{C}_G(P)|$ is prime to p, and since it divides $p^{n-1}(p-1)$, it must divide $p-1$, which is impossible since p is the smallest prime divisor of G. Hence P cannot be cyclic. □

We can use Burnside's normal p-complement theorem to derive another constraint on the orders of simple groups.

Corollary 1.13 (Burnside, 1895) Let G be a non-abelian simple group, and p be the smallest prime dividing the order of G. Then p^3 divides $|G|$, or $p = 2$ and 12 divides $|G|$.

Proof: By Corollary 1.12, the Sylow p-subgroups cannot be cyclic, so p^2 must divide G. Next, we know that there are only two groups of order p^2: C_{p^2} and E_{p^2}, the elementary abelian group of order p^2. Since the Sylow p-subgroups aren't cyclic, they must be $C_p \times C_p$. By Proposition 0.13(ii) the automorphism group of this is $\mathrm{GL}_2(p)$, which has order $(p^2-1)(p^2-p)$.

Again, we have that $\mathrm{N}_G(P)/\,\mathrm{C}_G(P)$ divides $(p-1)(p^2-1)$ since $P \leqslant \mathrm{C}_G(P)$ (and so $|\,\mathrm{N}_G(P)/\,\mathrm{C}_G(P)|$ is coprime to p). Again, $p-1 < p$, and since p is the smallest prime dividing $|G|$, we must have $|\,\mathrm{N}_G(P)/\,\mathrm{C}_G(P)|$ dividing $p+1$. It cannot be equal to 1 by Burnside's p-complement theorem, and it cannot be between 1 and $p+1$, since again p is the smallest prime dividing $|G|$. So we are forced to take $\mathrm{N}_G(P)/\,\mathrm{C}_G(P) = p+1$, which is a prime by choice of p. Thus p and $p+1$ are primes, giving $p = 2$, and $p^2(p+1) = 12$ divides the order of G. □

We can use this corollary to prove another fact about the possible orders of simple groups.

Corollary 1.14 Let G be a simple group of order p^2qr, where p, q, r are primes. Then $G \cong A_5$.

Proof: By Corollary 1.13, $p = 2$ and either q or r is 3, say $q = 3$. Thus $|G| = 12r$, where r is a prime. Firstly note that $r \leqslant 11$, since the number of Sylow r-subgroups must be congruent to 1 modulo r and divide 12, and so we easily see $r = 11$ or $r = 5$. In the case $r = 5$ we get $|G| = 60$, and by Proposition 0.15 we get $G \cong A_5$. In the case $r = 11$, Burnside's p-complement theorem gives us a contradiction, so we are done. □

Burnside proved that p^3 or 12 divided $|G|$ at the turn of the twentieth century, and made two conjectures: firstly, he conjectured that $p = 2$ for all simple groups – so the order of every non-abelian simple group is even – and he also conjectured that 12 divided the order of every simple group. The first of these conjectures became the 'Feit–Thompson theorem' or the 'odd order theorem', but the second of these conjectures turned out to be incorrect. Suzuki, in [12], proved the existence of an infinite family of simple groups of order $q^2(q^2+1)(q-1)$, where $q = 2^{2n+1}$ is an odd power of 2 not equal to 2 itself. Notice that in this case, 3 cannot divide this order, and so the conjecture was falsified.

As a historical note, some texts (for example [2] and [10]) credit Schur [11] with the development of the transfer in 1902. However, already in 1900 it was used by Burnside, and indeed it was originally developed by him, with several rediscoveries over the years by others. Schur developed lots of new mathematics himself, but this bit isn't one of them.

1.3 p-Groups and Nilpotent Groups

The theory of p-groups and their automorphisms is a large subject, and here we only scratch the surface of what is known. We begin with the Frattini subgroup, which we saw in Exercise 1.5.

Lemma 1.15 Let G be a finite group. The set $\Phi(G)$ consists of all *non-generators* of G; i.e., $\Phi(G)$ consists of all elements $g \in G$ such that, whenever $G = \langle X, g\rangle$, we have that $G = \langle X\rangle$.

Proof: Suppose that g is a non-generator of G, and let M be a maximal subgroup of G. If $g \notin M$ then $G = \langle g, M\rangle$, so $G = \langle M\rangle$ as g is a non-generator, a contradiction. Hence g lies in every maximal subgroup of G, so $g \in \Phi(G)$.

Conversely, suppose that $g \in \Phi(G)$, and suppose that $G = \langle X, g\rangle$ for some subset X of G. If $\langle X\rangle < G$, then $\langle X\rangle \leqslant M$ for some maximal subgroup M; however, since $g \in \Phi(G) \leqslant M$, $\langle X, g\rangle \leqslant M$ as well, a contradiction. Thus $\Phi(G)$ consists of all non-generators of G, as claimed. □

Theorem 1.16 (Burnside basis theorem, 1913) Let G be a finite p-group.

(i) A subset X of G generates G if and only if the image of X in $G/\Phi(G)$ generates $G/\Phi(G)$.

(ii) All minimal (under inclusion) generating sets of G have the same cardinality d, where $|G/\Phi(G)| = p^d$.

Proof: If X is a generating set of G then the image of X generates any quotient group, so one direction is easy. Conversely, suppose that the image of X in $G/\Phi(G)$ generates $G/\Phi(G)$. We claim that $G = \langle \Phi(G), X\rangle$, and then by Lemma 1.15 we have $G = \langle X\rangle$, as required. To see that $G = \langle \Phi(G), X\rangle$ notice that, since $\langle X\rangle$ must contain at least one element from each coset of $\Phi(G)$ (since its image in $G/\Phi(G)$ generates the whole quotient), every coset of $\Phi(G)$ lies in $\langle X, \Phi(G)\rangle$, completing the proof of (i).

To see (ii), we simply note that it is easy to see that all minimal generating sets for an elementary abelian p-group have the same size by identifying elementary abelian p-groups with finite-dimensional vector spaces over $\mathbb{F}_p$, and generating sets with bases. This, plus the previous part of the theorem, completes the proof of (ii), and hence the theorem. □

Proposition 1.17 (Burnside) Let G be a finite p-group. A p'-automorphism $\alpha \in \mathrm{Aut}(G)$ acts trivially on $G/\Phi(G)$ if and only if $\alpha = 1$.

Proof: Suppose firstly that α has prime order q (where $q \neq p$), and acts trivially on $G/\Phi(G)$, and write p^m for the order of $\Phi(G)$. Since α fixes each coset of $\Phi(G)$, each of which is a set of order p^m, α must permute the elements of this coset, and hence must fix at least one element in this coset (since if all orbits have length more than 1, they all have length a multiple of q). Hence α fixes an element from each coset of $\Phi(G)$. Let X denote a collection of such fixed points. Clearly the image of X in $G/\Phi(G)$ is the whole of $G/\Phi(G)$, so by Burnside's basis theorem $G = \langle X \rangle$. As α fixes a set of generators for G, $\alpha = 1$, as needed.

Finally, suppose that $o(\alpha)$ is not of prime order, and write $o(\alpha) = qn$, where $n > 1$. Notice that α^n has order q, and acts trivially on $G/\Phi(G)$, so $\alpha^n = 1$ by the previous paragraph. Thus $o(\alpha) = n$, and this contradiction proves the general case. $\square$

(The Burnside basis theorem originally used the derived subgroup rather than the Frattini subgroup, and was cast in its modern form by Philip Hall, in 1934; we will see more of him in the next chapter.)

We move from p-groups to nilpotent groups. These are groups where by quotienting out by the centre repeatedly, one eventually ends up at the trivial group.

Definition 1.18 Let G be a group. A *central series* for G is a series

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

such that $G_i/G_{i-1} \leqslant \mathrm{Z}\,(G_i/G_{i-1})$ for all $1 \leqslant i \leqslant r$. (In other words, G_i is the set of all $g \in G$ such that, for all $x \in G$, we have $[g, x] \in G_{i-1}$.) If G possesses a central series then G is *nilpotent*. The smallest r such that there is a central series for G with $G_r = G$ is the *nilpotence class* of G, or simply the class of G.

Notice that an abelian group is nilpotent of class 1, and all nilpotent groups are soluble. The idea of a nilpotent group is a generalization of a finite p-group, in the sense that finite p-groups are nilpotent. This follows easily from the fact that the centre of a p-group is non-trivial.

Lemma 1.19 Subgroups and quotients of nilpotent groups of class c are nilpotent, of class at most c.

Proof: Let

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

be a central series for G, and let H be a subgroup of G. We claim that if $H_i = H \cap G_i$, then the (H_i) form a central series for H. To see this, notice that $H_i \leqslant G_i$, so that if $g \in H_i$ then for all $x \in H$, we have $[g, x] \in G_{i-1}$. Also, $[g, x] \in H$, so that $[g, x] \in H_{i-1}$, proving that (H_i) is a central series for H.

Let K be a normal subgroup of G, and let $K_i = G_iK/K$. We claim that (K_i) is a central series for G/K. The proof is similar to the above, and is skipped. □

We now introduce two important central series, called the upper and lower central series.

Definition 1.20 Write $\mathrm{Z}_0(G) = 1$, and $\mathrm{Z}_i(G)$ for the preimage in G of $\mathrm{Z}\left(G/\mathrm{Z}_{i-1}(G)\right)$. The series

$$1 = \mathrm{Z}_0(G) \leqslant \mathrm{Z}_1(G) \leqslant \mathrm{Z}_2(G) \leqslant \cdots$$

is called the *upper central series* for G.

Write $L_1(G) = G$ and $L_i(G) = [G, L_{i-1}(G)]$. The series

$$G = L_1(G) \geqslant L_2(G) \geqslant L_3(G) \geqslant \cdots$$

is called the *lower central series* for G.

We have called them the upper and lower central series, suggesting that they actually are central series.

Proposition 1.21 Let G be a nilpotent group of class c. Both the upper and lower central series are central series for G, and both series have length c. Furthermore, if

$$1 = G_0 \trianglelefteqslant G_1 \trianglelefteqslant \cdots \trianglelefteqslant G_r = G$$

is any central series for G, then $G_i \leqslant \mathrm{Z}_i(G)$ and $L_{c+1-i}(G) \leqslant G_i$.

Proof: We proceed by induction on r, the case where $r = 1$ meaning the group G is abelian, and $\mathrm{Z}(G) = G$, $L_2(G) = 1$, and the result holds.

Clearly $G_1 \leqslant \mathrm{Z}(G)$ by definition, and so the result is true $i = 1$. Assume the result is true for $i-1$, so that $G_{i-1} \leqslant \mathrm{Z}_{i-1}(G)$; for all $g \in G_i$ and $x \in G$, we have that $[g, x] \in G_{i-1} \leqslant \mathrm{Z}_{i-1}(G)$, so that $g \in \mathrm{Z}_i(G)$ (as it lies in the centre of $G/\mathrm{Z}_{i-1}(G)$). Hence $G_i \leqslant \mathrm{Z}_i(G)$.

The proof that $L_{c+1-i}(G) \leqslant G_i$ is similar, and left as an exercise. □

We are now able to prove the following result, which offers several characterizations of *finite* nilpotent groups.

Theorem 1.22 Let G be a finite group. The following are equivalent:

(i) G is nilpotent;

(ii) (The normalizer condition) for all $H < G$, we have $H < \mathrm{N}_G(H)$;

(iii) G is the direct product of its Sylow p-subgroups;

Proof: We proceed in stages.

(i) implies (ii) Suppose that G is nilpotent, and let H be a proper subgroup of G. If $\mathrm{Z}(G) \not\leqslant H$ then clearly $H < \mathrm{N}_G(H)$ (as $Z = \mathrm{Z}(G) \neq 1$), so we may assume that $Z \leqslant H$. However, in this case $\mathrm{N}_G(H)/Z = \mathrm{N}_{G/Z}(H/Z)$, and so $H < \mathrm{N}_G(H)$ if and only if $H/Z < \mathrm{N}_{G/Z}(H/Z)$. By induction on the nilpotence class of G, the latter strict inequality holds, and so $H < \mathrm{N}_G(H)$, as claimed.

(ii) implies (iii) Suppose that G has the normalizer condition, and let P be a Sylow p-subgroup of G: the normalizer condition applies to $\mathrm{N}_G(P)$, and so either $\mathrm{N}_G(P) = G$ – i.e., P is normal in G – or $\mathrm{N}_G(P) < \mathrm{N}_G(\mathrm{N}_G(P))$. However, this second possibility cannot occur by Exercise 1.6, and so all Sylow p-subgroups of G are normal in G. Thus G is the direct product of its Sylow p-subgroups.

(iii) implies (i) By Exercise 2.2, the direct product of nilpotent groups is nilpotent, and since p-groups are nilpotent, we see that if G is the direct product of its Sylow p-subgroups then G is nilpotent. $\square$

Notice that the first part of the proof – that nilpotent groups have the normalizer condition – did not require G to be finite. However, in the infinite case, having the normalizer condition is *not* equivalent to being nilpotent. Indeed, there are examples of infinite groups with the normalizer condition but whose centre is the trivial subgroup [7].

1.4 Frobenius Groups

Frobenius groups are an important class of finite group, and they are often minimal configurations in certain classification problems. The general setup is as follows.

Definition 1.23 Let G be a finite group, and let H be a proper, non-trivial subgroup of G.

(i) H is a *TI subgroup* (trivial intersection) if, for all $g \in G$, either $H^g = H$ or $H \cap H^g = 1$.

(ii) G is a *Frobenius group*, with *Frobenius complement* H, if H is a TI subgroup and $H = \mathrm{N}_G(H)$, i.e., $H \cap H^g = 1$ whenever $g \in G \setminus H$.

One of the fundamental applications of character theory to finite groups, as well as Burnside's $p^\alpha q^\beta$-theorem, is the following theorem of Frobenius.

Theorem 1.24 (Frobenius's theorem, 1902) Let G be a Frobenius group, with Frobenius complement H. There exists a normal subgroup K of G such that $G = K \rtimes H$.

The remarkable thing about this theorem is that, to this day, there is no known proof that does not use character theory, while in 1972 Helmut Bender managed to find a proof of Burnside's $p^\alpha q^\beta$-theorem without using character theory. If we are to prove it therefore, we are going to have to use character theory.

We begin with an alternate characterization of Frobenius groups, as permutation groups.

Proposition 1.25 Let G be a finite permutation group acting transitively on a set X.

(i) If only the identity fixes more than one element of X, then G is a Frobenius group, with Frobenius complement G_x for any $x \in X$.

(ii) If G is a Frobenius group with Frobenius complement G_x for some $x \in X$, then only the identity fixes more than one element of X.

Proof: Write $H = G_x$. Let g be an element of G, and suppose that only the identity fixes more than one element of X. We see that if $xg \neq x$ (i.e., $g \notin H$) then $H \cap H^g = G_{x,xg} = 1$. This proves (i).

Conversely, if $H \cap H^g = 1$ for $g \notin H$, then $G_{x,xg} = 1$ for any $g \notin H$; in particular, only the identity fixes more than one letter, as required for (ii). $\square$

Let G be a Frobenius group, with H a Frobenius complement, and we assume that G is a permutation group on X, as in the previous proposition. Notice that $|X| = |G : H|$. Let K denote the subset of all permutations in G that act fixed point freely on X, together with the identity. Since each pair H^g and H^h intersect trivially, we see that there are $n(|H| - 1)$

elements of G that fix exactly one element of X. This proves that K has exactly n elements in it. Also, clearly the conjugates of elements in K are also elements of K, and so it forms a *normal subset* of G. We call K the *Frobenius kernel* of the Frobenius group G. Frobenius's theorem may be restated as follows.

Theorem 1.26 Frobenius kernels are normal subgroups of Frobenius groups.

The general aim is to find a character of a Frobenius group with the Frobenius kernel as its kernel; then it is definitely a normal subgroup, and we are done. In order to do this, we will of course construct various characters of Frobenius groups, and consider the characters for the Frobenius complement and induce them to the whole group.

Let G be a Frobenius group, thought of as a permutation group on a set $X = \{1, \ldots, n\}$. Write $H = G_1$, for a Frobenius complement. Let t_i be an element of G such that $1 = i^{t_i}$, so that $\{t_1, \ldots, t_n\}$ is a right transversal to H in G, and $G_i^{t_i} = H$.

If χ is a character of H then the induced character, χ^G, takes value

$$\chi^G(g) = \sum_{i=1}^{n} \chi(t_i^{-1} g t_i),$$

with the convention that $\chi(g) = 0$ for $g \in G \setminus H$. Let h be a non-trivial element of H, and let $h_i = t_i h t_i^{-1}$ (the conjugate of h by t_i^{-1}), a non-trivial element of H_i.

Lemma 1.27 With the conventions above,

$$\chi^G(h_i) = \chi(h), \qquad \chi^G(k) = 0 \text{ for } k \in K \setminus \{1\}.$$

Proof: The only non-zero terms of the sum for $\chi^G(h_i)$ are when $t_j^{-1} h_i t_j$ lies in H, i.e., $(t_i^{-1} t_j)^{-1} h (t_i^{-1} t_j)$ lies in H. However, h fixes 1, so this conjugate fixes 1 if and only if $i = j$. Hence the only contribution to the sum is $\chi(t_i^{-1} h_i t_i) = \chi(h)$, proving the first statement.

For the second, notice that $t_i^{-1} k t_i$ is always fixed point free (recall that K is a normal subset of G), and so $\chi(t_i^{-1} k t_i) = 0$ for all i. □

Let ϕ denote the deleted permutation character of G; i.e., the permutation character minus the trivial character, the character whose values on $g \in G$ are the number of fixed points of g minus 1. Hence $\phi(1) = n - 1$, $\phi(h_i) = 0$ and $\phi(k) = -1$.

Lemma 1.28 Let χ be an irreducible character of H of degree d. The class function $\zeta = \chi^G - d\phi$ is an irreducible character of G.

Proof: To prove that ζ is an irreducible character, we must show that $\zeta(1) > 0$ and $\langle \zeta, \zeta \rangle = 1$. Notice that $\zeta(1) = nd - (n-1)d = d$, so the first condition is satisfied. To prove that $\langle \zeta, \zeta \rangle = 1$, we must show that

$$\sum_{g \in G} |\zeta(g)|^2 = |G|.$$

Notice that, since χ is irreducible, we have that $\sum_{h \in H^\times} |\chi(h)|^2 = |H| - d^2$, where $H^\times$ denotes the non-trivial elements of H.

Using Lemma 1.27 and the character values of ϕ, we get

$$\zeta(g) = \begin{cases} d & g = 1 \\ \chi(h) & g = h_i \\ d & g \in K^\times \end{cases}.$$

We can use this to calculate (noting that every element of G lies either in $\{1\}$, one of the $H_i^\times$, or $K^\times$, and each H_i has the same character values as H):

$$\begin{aligned} \sum_{g \in G} |\zeta(g)|^2 &= d^2 + n \sum_{h \in H^\times} |\zeta(h)|^2 + \sum_{k \in K^\times} |\zeta(k)|^2 \\ &= d^2 + n(|H| - d^2) + (n-1)d^2 \\ &= n|H| = |G|. \end{aligned}$$

Hence ζ is an irreducible character of G, as needed. □

We are now in a good position to define a character of G with K as its kernel. Let $\chi_1, \dots, \chi_r$ denote a complete set of irreducible characters of H, write $d_i = \chi_i(1)$, and let $\zeta_i = \chi_i^G - d_i\phi$, some irreducible characters of G. Define

$$\theta = \sum_{i=1}^{r} d_i \zeta_i,$$

analogously to the regular character being $\sum_{i=1}^{r} d_i \chi_i$. We claim that $\theta(g) = \theta(1)$ if and only if $g \in K$. One direction of this is clear because, for each i, $\zeta_i(k) = \zeta_i(1) = d_i$. However, if $h \in H^\times$ then

$$\theta(h) = \sum_{i=1}^{d} d_i \zeta_i(h) = \sum_{i=1}^{d} d_i \chi_i(h),$$

and this is simply the value of the regular character of H on h, which is 0. Thus $\theta(h) = 0$ for $h \in H^\times$, and hence for $h \in H_i^\times$. Therefore $\theta(g) = \theta(1)$ if and only if $g \in K$, and the theorem is at last proved.

Let G be a finite group. An automorphism ϕ of G is *fixed point free* if $g\phi = g$ implies $g = 1$. We give a proposition relating Frobenius groups with fixed-point-free automorphisms.

Proposition 1.29 (i) Let G be a Frobenius group with Frobenius kernel K and complement H. If $h \in H$ then the automorphism of K induced by conjugation by h is fixed point free.

(ii) Let K be a finite group and let H be a subgroup of $\operatorname{Aut} K$ consisting of fixed-point-free automorphisms of K (and the identity). The group $K \rtimes H$ is a Frobenius group with Frobenius kernel K and complement H.

Proof: Suppose that $k \in K$ and $h \in H$, and $k^h = k$. Since h and k commute, we see that $H \cap H^k$ contains h, and so either $k \in H$ or $h = 1$, which proves the result in (i).

Assume the notation of (ii), and suppose that $H \cap H^k \neq 1$ for some $k \in K$. Then there exists $h \in H$ such that $h^k = h'$ for some $h' \in H$. We see therefore that $[k, h^{-1}] = h^{-1}h' \in H$, but since $K \trianglelefteq G$, $[k, h^{-1}] \in K$. Hence $h^{-1}h' = 1$, and hence k and h commute, contradicting the fact that h acts fixed point freely on K. Thus $H \cap H^k = 1$ if $k \in K^\times$. If $g = hk$ is an element of $G \setminus H$ then $k \neq 1$, and we see that $H \cap H^g = H \cap H^k = 1$, as claimed. □

We therefore become interested in fixed-point-free automorphisms. An open question for a long time was whether Frobenius kernels are always nilpotent, or equivalently, whether if G is a finite group with a fixed-point-free automorphism of prime order then G is nilpotent. The answer to this question is 'yes', and was proved by John Thompson in his Ph.D. thesis in 1959. The proof of this is will be seen later in this course.

Chapter 2

The 1930s

2.1 The Schur–Zassenhaus Theorem

The Schur–Zassenhaus theorem is one of the fundamental results in finite group theory. It asserts the existence of complements in certain situations, namely when the normal subgroup and the quotient have coprime orders.

Theorem 2.1 (Schur–Zassenhaus theorem, 1937) Let G be a finite group, and let K be a normal subgroup of G such that $|K|$ and $|G/K|$ are coprime. Assume that either K or G/K is soluble. There are complements to K in G, and any two complements to K in G are conjugate in G.

(In the case where G/K is cyclic, the theorem was proved in 1904 by Schur, but the general case we give here was proved by Zassenhaus in 1937.)

We recall briefly some terminology. If G is a finite group and K is a normal subgroup of G, a *complement* to K in G is a subgroup H such that $G = HK$ and $H \cap K = 1$. An extension

$$1 \longrightarrow K \longrightarrow G \xrightarrow{\phi} H \longrightarrow 1$$

splits if there exists a homomorphism $\psi : H \to G$ such that $\phi\psi = \mathrm{id}_H$, or equivalently K has a complement in G. We also say that G is a *semidirect product* of K and H.

We are going to develop the rudiments of *cohomology*: in the guise here, cohomology theory attempts to understand and classify extensions of one group by another, particularly when the kernel is abelian.

Definition 2.2 Let G be a finite group and let M be a G-module. A 2-*cocycle* is a function $\zeta : G \times G \to M$ that satisfies the identity

$$\zeta(x, yz) + \zeta(y, z) = \zeta(xy, z) + \zeta(x, y) \cdot z,$$

and $\zeta(1,y) = \zeta(x,1) = 0$, for all $x, y, z \in G$.

A 2-cocycle looks quite artificial, but it measures how far an extension differs from being a split extension. To see this, let X be a finite group and let M be a normal subgroup. Fix a transversal T to M in X, and write G for the quotient X/M, and $\phi : X \to G$ is the natural quotient map. A transversal can be thought of as a function $\psi : G \to X$ such that $\psi\phi = \mathrm{id}_G$. Notice that X splits over M if and only if we may choose ψ to be a homomorphism. In general, however, we have

$$(x\psi)(y\psi) = (xy\psi)\zeta(x,y),$$

for some $\zeta(x,y) \in M$. We claim that the function $\zeta(x,y)$ is a 2-cocycle. Firstly, write elements in M additively for this proof. Notice that clearly $\zeta(1,y) = 0 = \zeta(x,1)$ for all $x, y \in G$. It remains to check the more complicated condition. The associativity of G is the only thing that we have to use, so let's use it. We have

$$(x\psi+y\psi)+z\psi = (xy)\psi+\zeta(x,y)+z\psi = (xy)\psi+z\psi+\zeta(x,y)\cdot z = (xyz)\psi+\zeta(xy,z)+\zeta(x,y)\cdot z,$$

and

$$x\psi + (y\psi + z\psi) = x\psi + (yz)\psi + \zeta(y,z) = (xyz)\psi + \zeta(x,yz) + \zeta(y,z).$$

This gives $\zeta(x,yz) + \zeta(y,z) = \zeta(xy,z) + \zeta(x,y) \cdot z$, the cocycle identity, as claimed. If G is a finite group and M is a G-module, the set of all 2-cocycles will be denoted by $Z^2(G,M)$.

The next object we need to construct are the 2-coboundaries. A function $\zeta : G \times G \to M$ is a 2-*coboundary* if there exists a function $f : G \to M$ with $f(1) = 0$ such that

$$\zeta(x,y) = f(y) - f(xy) + f(x) \cdot y.$$

It is easy to show, and a simple exercise, that all 2-coboundaries are 2-cocycles. The set of 2-coboundaries will be denoted by $B^2(G,M)$. In fact, we can define an addition operation on $Z^2(G,M)$ by

$$(\zeta + \xi)(x,y) = \zeta(x,y) + \xi(x,y).$$

This turns $Z^2(G,M)$ into an abelian group, and $B^2(G,M)$ into a subgroup of $Z^2(G,M)$. Define the 2-*cohomology group* to be

$$H^2(G,M) = Z^2(G,M)/B^2(G.M).$$

In some sense, $H^2(G,M)$ classifies equivalence classes of extensions of M by G. The next proposition tells us something important is going on when we have that $|G|$ and $|M|$ are coprime.

Proposition 2.3 Let G be a finite group, and let M be a finite G-module. If $|G|$ and $|M|$ are coprime, then $H^2(G, M) = 0$.

Proof: Let $\zeta : G \times G \to M$ be a cocycle. We must show that ζ is a coboundary, for then $H^2(G, M) = 0$. Define $\sigma : G \to M$ by

$$\sigma(g) = \sum_{x \in G} \zeta(x, g).$$

(Since M is abelian this sum makes sense.) As ζ is a cocycle, we have the identity (for $x, y, z \in G$)

$$\zeta(x, yz) + \zeta(y, z) = \zeta(xy, z) + \zeta(x, y) \cdot z.$$

Summing these identities for all $x \in G$, we get

$$\sigma(yz) + n\zeta(y, z) = \sigma(z) + \sigma(y) \cdot z,$$

where $n = |G|$. Let $m = |M|$. As m and n are coprime, there are integers a and b such that $am + bn = 1$. Let $\tau : G \to M$ be defined by $\tau(x) = b\sigma(x)$. We see that $\tau(1) = 0$, and

$$\tau(yz) + (1 - am)\zeta(y, z) = \tau(z) + \tau(y) \cdot z$$

Since $\zeta(x, y)$ is an element of M, $am\zeta(x, y) = 0$, and so $\zeta(x, y)$ satisfies the identity of a coboundary, namely

$$\zeta(y, z) = \tau(z) - \tau(yz) + \tau(y) \cdot z.$$

This proves that $H^2(G, M) = 0$, as claimed. $\square$

The theory of cohomology is extensive, and we will just develop enough to prove our theorem. For this, we just need the following two lemmas.

Lemma 2.4 Let X_1 and X_2 be two extensions of M by G, and let ζ_1 and ζ_2 be the associated 2-cocycles to the extensions. If ζ_1 and ζ_2 lie in the same coset of $H^2(G, M)$, then $X_1 \cong X_2$.

Proof: Write $\psi_i : G \to X_i$ for the transversals yielding ζ_i. Since $\zeta_2 - \zeta_1$ is a coboundary, there exists a function $f : G \to M$ with $f(1) = 0$ such that, for all $x, y \in G$,

$$\zeta_1(x, y) - \zeta_2(x, y) = f(y) - f(xy) + f(x) \cdot y.$$

Each element of X_1 can be expressed uniquely as $(x\psi)a$ with $a \in M$ and $x \in G$, and the multiplication in X_1 is given by

$$[(x\psi_1)a][(y\psi_1)b] = [(x\psi_1)(y\psi_1)][a^{y\psi_1}b] = [(xy)\psi_1][\zeta_1(x, y)][a \cdot y]b.$$

Define $\gamma : X_1 \to X_2$ by $((x\psi_1)a)\gamma = (x\psi_2)f(x)a$. We need to check that this is a homomorphism: the unenlightening computation is as follows.

$$\begin{aligned}((x\psi_1)a)\gamma((y\psi_1)b)\gamma &= (x\psi_2)f(x)a(y\psi_2)f(y)b \\ &= [(x\psi_2)(y\psi_2)]a^{y\psi_2}f(y)b \\ &= [(xy)\psi_2][\zeta_2(x,y)][f(x)\cdot y][a\cdot y][f(y)][b].\end{aligned}$$

$$\begin{aligned}([(x\psi_1)a][(y\psi_2)b])\gamma &= ([(xy)\psi_1][\zeta_1(x,y)(a\cdot y)b])\gamma \\ &= [(xy)\psi_2][f(xy)][\zeta_1(x,y)][(a\cdot y)][b].\end{aligned}$$

For these two expressions to be equal, we may remove $(xy)\psi_2$ and b from both of them: the remaining terms all lie in M, an abelian group, so we may remove $a \cdot y$ from both, and we are left with (written additively since this is an equation solely in M)

$$\zeta_2(x,y) + f(x)\cdot y + f(y) = f(xy) + \zeta_1(x,y).$$

This is a rearrangement of the first equation of this proof, so it holds. Therefore γ is a homomorphism. Finally, we need to know that γ is an injection, since $|X_1| = |X_2|$. However, if $((x\psi)a)\gamma = 1$ then $x = 1$ since else the expression does not lie in M, and $a\gamma = a$ by an easy computation. Thus γ is an isomorphism, as required. □

Lemma 2.5 Let X be an extension of M by G, let T be a transversal to M in X, and let ζ be the associated 2-cocycle to the extension and transversal. If ζ is a 2-coboundary (i.e., the cohomology class is 0) then $X = M \rtimes G$.

Proof: If ζ is identically 0, then T is actually a subgroup of X, so that $X = M \rtimes T$. The rest now follows from Lemma 2.4. □

Since H^2 determines whether an extension splits or not, we get the following corollary to Proposition 2.3 and Lemma 2.5.

Corollary 2.6 Let G be a finite group and let K be an abelian normal subgroup of G. If $|G/K|$ and $|K|$ are coprime then K has a complement in G.

Hence the existence of complements in the Schur–Zassenhaus theorem in the case of K abelian is proved. We will prove the existence of complements in all cases now.

Proof: Let G be a minimal counterexample to the theorem, and let K be a normal subgroup of G such that $|K|$ and $|G/K|$ are coprime. Write $k = |K|$ and $n = |G/K|$.

Step 1: *K is a minimal normal subgroup of G.* We first show that K is a minimal normal subgroup of G, so let M be a normal subgroup of G contained in K. By induction, the theorem holds for G/M, and so since K/M and $G/K = (G/M)/(K/M)$ have coprime orders, there is a complement H/M to K/M in G/M. Taking preimages gives a subgroup H of G such that $HK = G$ and $H \cap K = M$.

Notice that

$$H/M = H/(H \cap K) \cong HK/K = G/K,$$

and so $|H/M| = n$. Therefore, again by induction, since $|M|$ and $|H/M|$ are coprime, M has a complement L in H, which has order n. The subgroup L, having order n, is a complement to K in G, hence $M = 1$ or $M = K$, proving that K is a minimal normal subgroup of G.

Step 2: *K is an elementary abelian p-group, and conclusion.* Let P be a Sylow p-subgroup of K (which is also a Sylow p-subgroup of G), for some $p \mid |K|$. By the Frattini argument (Exercise 1.4) $G = K\,\mathrm{N}_G(P)$. Since $G/K \cong \mathrm{N}_G(P)/(\mathrm{N}_G(P) \cap K)$, and the index of $\mathrm{N}_K(P) = \mathrm{N}_G(P) \cap K$ in $\mathrm{N}_G(P)$ is n, we see that unless $\mathrm{N}_G(P) = G$, $\mathrm{N}_G(P)$ has a complement H to $\mathrm{N}_K(P)$, which therefore has order n, so is a complement to K in G. Hence $P \trianglelefteqslant G$ which means, since K is a minimal normal subgroup, that $K = P$, a p-group. In particular, K is soluble, so K is elementary abelian by Exercise 2.6. However, by Corollary 2.6, K indeed has a complement in G, completing the proof of existence. □

We now turn to conjugacy of the complements. Conjugacy of complements in the case where K is abelian is governed by more cohomology, namely the 1-cohomology group. In Exercises 4.3 and 4.4 we prove some results about 1-cohomology. In particular, we prove that if a finite group X is a split extension of M by G, then all complements to M in G are conjugate if $H^1(G, M) = 0$, and we also prove that if $|G|$ and $|M|$ are coprime then $H^1(G, M) = 0$, so we prove the conjugacy of complements for the case K abelian in the Schur–Zassenhaus theorem.

Suppose now that K is soluble, but not abelian. If H and L are complements to K in G, then HK'/K' and LK'/K' are complements to K' in G/K', whence are conjugate in G/K'. Hence we may assume that $HK' = LK'$, and by induction (as $K' < K$ since K is soluble) H and L are conjugate in HK' since they are both complements to K' in HK'.

Suppose instead that G/K is soluble, and let H and L be two complements to K in G. Let $T = \mathrm{O}_\pi(G)$, where π is the set of primes dividing $|G/K|$. Clearly $T \leqslant H, L$ by consideration of orders, and H and L are conjugate if and only if H/T and L/T are. Thus we may assume that $T = 1$. Let M/K be a minimal normal subgroup of G/K, and let M denote its preimage. Since G/K is soluble, M/K is an elementary abelian p-group for some $p \in \pi$. We claim that $H \cap M$ is a Sylow p-subgroup of M: since H contains a Sylow p-

subgroup of G and $M \trianglelefteq G$, $H \cap M$ contains a Sylow p-subgroup of M, and as H is a π-group, and the only prime in π that divides $|M|$ is p, we prove the claim. Similarly, $L \cap M$ is also a Sylow p-subgroup of M, so there exists $g \in M$ such that $L \cap M = (H \cap M)^g = H^g \cap M$.

Writing $U = L \cap M$, we see that U is normal in $\langle H^g, L\rangle$. If $\langle H^g, L\rangle < G$ then by induction H^g and L are two complements to $H \cap M$ in $\langle H^g, L\rangle$, so are conjugate. Hence $\langle H^g, L\rangle = G$, i.e., $U \trianglelefteq G$. However, we assumed that $\mathrm{O}_\pi(G) = 1$, so $L \cap M = U = 1$. However, this is a contradiction since $M/K \cong U$ and $M/K \neq 1$. This completes the proof of conjugacy if G/K is soluble.

In order to get the clean statement of the Schur–Zassenhaus theorem, we need to know that either K or G/K is always soluble. This is a consequence of the deep and difficult Feit–Thompson theorem, which states that groups of odd order are always soluble. Since one of $|K|$ and $|G/K|$ is definitely odd, we get the final form of the Schur–Zassenhaus theorem, Theorem 2.1.

2.2 Hall's Theorem on Soluble Groups

Definition 2.7 Let G be a finite group and π be a set of primes. A subgroup H of G is a *Hall π-subgroup* of G if H is a π-group and $|G : H|$ is a π'-number.

There is no guarantee that Hall π-subgroups always exist: they do in certain situations and don't in others.

Example 2.8 If $\pi = \{p\}$, then a Hall π-subgroup is a Sylow p-subgroup, and so Hall π-subgroups always exist in this case. If $G = A_5$ and $\pi = \{2, 5\}$, then a Hall π-subgroup of G would have index 3; since A_n has no subgroups of index less than n for $n \geqslant 5$, there is no Hall $\{2, 5\}$-subgroup of G. However, if $\pi = \{2, 3\}$ then a Hall π-subgroup would have order 12, and so the A_4 subgroups are Hall $\{2, 3\}$-subgroups of A_5.

The example of a group without a Hall subgroup was a simple group. The reason we chose an insoluble group for this example is the following proposition, due to Philip Hall.

Proposition 2.9 Let G be a finite soluble group, and let π be a set of primes.

(i) Hall π-subgroups of G exist,

(ii) all Hall π-subgroups of G are conjugate in G, and

(iii) any π-subgroup of G is contained in a Hall π-subgroup of G.

Proof: We proceed by induction on $|G|$. Let K be a minimal normal subgroup of G; by Exercise 2.6, K is an elementary abelian p-group for some prime p. Suppose firstly that $p \in \pi$. The preimage of a Hall π-subgroup of G/K is a Hall π-subgroup of G, so Hall π-subgroups of G exist. Furthermore, by induction, all Hall π-subgroups of G/K are conjugate in G/K, and so their preimages, which are exactly the Hall π-subgroups of G, are conjugate in G. Finally, if H is any π-subgroup of G then HK is also a π-subgroup of G, whence HK/K is contained in a Hall π-subgroup of G/K; the preimage of this subgroup is a Hall π-subgroup of G containing H, completing the proof in this case.

We are left with the case where $p \notin \pi$. In this case, the preimage of a Hall π-subgroup of G/K is a subgroup A of G, with $K \trianglelefteqslant A$ and $|K|, |A/K|$ coprime. Hence by the Schur–Zassenhaus theorem, K has a complement C in A, which is a Hall π-subgroup of G, proving the existence of Hall π-subgroups in this case as well. Letting C and D be Hall π-subgroups of G, the subgroups CK/K and DK/K are G/K-conjugate by induction, whence there exists $g \in G$ such that $(CK)^g = DK$. Furthermore, since $K \trianglelefteqslant G$, $K^g = K$, and so C^g is another complement to K in DK. By the Schur–Zassenhaus theorem again, C^g and D are conjugate in DK, and hence C and D are conjugate, proving conjugacy of Hall π-subgroups.

Finally, let H be any π-subgroup; since HK/K is a π-subgroup of G/K, it is contained in a Hall π-subgroup of G/K, and the preimage of this is a subgroup M of G containing H and K, such that $|K|$ and $|M/K|$ are coprime. Let C be any complement to K in M. We see that $M = CK$ and

$$HK = HK \cap CK = (HK \cap C)K,$$

which shows that the order of H and $HK \cap C$ are equal. Since H and $HK \cap C$ are both complements to K in HK, they are conjugate via some element $g \in HK$ by the Schur–Zassenhaus theorem; hence H is contained in $C^{g^{-1}}$, completing the proof. $\square$

The remarkable result is that the converse holds. In fact, if a finite group possesses Hall p'-subgroups for all primes p, then it is soluble.

Theorem 2.10 (Philip Hall, 1937) Let G be a finite group. Hall p'-subgroups of G exist for all primes p if and only if G is soluble.

Proof: Let G be a finite group. If G is soluble then Hall p'-subgroups of G exist by the previous proposition, so we must prove the converse.

Let G be a minimal counterexample to the statement. By Burnside's $p^\alpha q^\beta$-theorem, at least three distinct primes divide $|G|$.

Let p be a prime dividing $|G|$ and let H be a Hall p'-subgroup of G. Let K be any Hall q'-subgroup of G, for some $q \neq p$; by consideration of orders, $H \cap K$ is a Hall q'-subgroup of H, and so H has Hall q'-subgroups for all primes q dividing $|H|$, so by induction H is soluble. If M is a minimal normal subgroup of H then M is an elementary abelian r-group for some prime $r \neq p$.

Since three distinct primes divide $|G|$, let q be different from both p and r, and let K be a Hall q'-subgroup of G. Clearly a Sylow r-subgroup of K is a Sylow r-subgroup of G, and so M is contained in some conjugate of K; replace K by this conjugate, so we may assume that $M \leqslant K$.

Consider all G-conjugates of M: as M is a normal subgroup of H, it is normalized by H. Also, $M \leqslant K$, so any K-conjugate of M lies inside K. However, G is generated by H and K (since K contains a Sylow p-subgroup of G and H contains all other Sylow subgroups), so that all G-conjugates of M are subgroups of K. This implies that the normal closure N of M in G (see Exercise 2.8) is contained in K.

Since K is soluble, N is soluble, and is a normal subgroup of G. By induction, and that fact that if L is a Hall π-subgroup of G then LN/N is a Hall π-subgroup of G/N, we see that G/N is soluble, so that G is soluble, as needed. $\square$

2.3 The Fitting Subgroup

In this section we consider nilpotent subgroups of a finite group, particularly nilpotent normal subgroups. The following result of Fitting is the basis for studying normal nilpotent subgroups.

Theorem 2.11 (Fitting's theorem) Let G be a finite group, and let H and K be nilpotent normal subgroups, of class c and d respectively. The product HK is nilpotent, of class at most $c+d$.

Proof: By Exercise 2.4, we have $[xy,z]=[x,z]^y[y,z]$ and $[x,yz]=[x,z][x,y]^z$, and so if X, Y and Z are normal subgroups then $[XY,Z]=[X,Z][Y,Z]$ and $[X,YZ]=[X,Y][X,Z]$. Consider the $(c+d+1)$-fold commutator $[HK,HK,\dots,HK]=L_{c+d+1}(HK)$. By using the commutator expansions we just described, we may write this commutator as

$$\prod_{X_i\in\{H,K\}}[X_1,X_2,\dots,X_{c+d+1}].$$

Notice that in each of the expressions in the product, either (at least) $c+1$ of the X_i are H, or $d+1$ of the X_i are K. Notice also that removing terms from a multiple commutator can only make the subgroup larger, and so each term is contained in either a $(c+1)$-fold commutator $L_{c+1}(H)$ or a $(d+1)$-fold commutator $L_{d+1}(K)$, both of which are trivial since H has class c and K has class d. Hence each term in the product is trivial, and so the $(c+d+1)$-fold commutator of HK is trivial. Thus HK is a normal nilpotent subgroup of class at most $c+d$, as required. □

Hence the product of all normal nilpotent subgroups is normal and nilpotent, so it makes sense to give the following definition.

Definition 2.12 Let G be a group. The *Fitting subgroup* of G, denoted $F(G)$, is the product of all normal nilpotent subgroups of G.

The Fitting subgroup is obvious a characteristic subgroup of a group, and is particularly important for soluble groups, where we have the following result.

Theorem 2.13 (Philip Hall) Let G be a soluble group. We have $\mathrm{C}_G(F(G))\leqslant F(G)$.

Proof: Let N be a normal subgroup of G. We claim that N contains some normal abelian subgroup of G: if G has derived length n, then the subgroup $G^{(n-1)}\cap N$ is a normal subgroup of G, and $G^{(n-1)}$ is abelian, so our claim is correct. Now write $F=F(G)$, $C=\mathrm{C}_G(F)$, and suppose that $C \nleqslant F$. There exists an abelian normal subgroup A/F of G/F contained in CF/F. Since $F \leqslant A$, by the modular law, Exercise 1.8,

$$A = A \cap (CF) = (A \cap C)F,$$

and $L_3(A \cap C) \leqslant [[A, A], C] = [A', C] \leqslant [F, C] = 1$. Hence $A \cap C$ is nilpotent, so $A \cap C \leqslant F$: therefore $A \leqslant F$ by the displayed equation, and this is a contradiction. Thus $\mathrm{C}_G(F(G)) \leqslant F(G)$, as needed. □

The Frattini subgroup, the intersection of all maximal subgroups, is actually a nilpotent subgroup. In fact, more is true.

Proposition 2.14 (Gäschutz) Let G be a finite group. The subgroup $\Phi(G)$ is nilpotent, and $F(G/\Phi(G)) = F(G)/\Phi(G)$.

Proof: We first show that if H is a subgroup of G containing $\Phi(G)$, and $H/\Phi(G)$ is nilpotent, then H is nilpotent. Let P be a Sylow p-subgroup of H: by assumption $P\Phi(G)/\Phi(G)$ is a Sylow p-subgroup of $H/\Phi(G)$, whence is characteristic in $H/\Phi(G) \trianglelefteqslant G/\Phi(G)$. In particular, $P\Phi(G) \trianglelefteqslant G$. The Frattini argument now yields that $G = (P\Phi(G))\,\mathrm{N}_G(P)$, and since $P \leqslant \mathrm{N}_G(P)$ and $\Phi(G)$ consists of all non-generators of G by Lemma 1.15, we see that $G = \mathrm{N}_G(P)$; i.e., we see that $P \trianglelefteqslant G$. Therefore all Sylow subgroups of H are normal in H, so H is nilpotent.

Applying this to $H = \Phi(G)$ gives that $\Phi(G)$ is nilpotent. Applying this to the preimage H of $F(G/\Phi(G))$ in G yields that H is nilpotent, so $F(G)/\Phi(G) \geqslant F(G/\Phi(G))$. The converse is clear, since images of nilpotent normal subgroups are nilpotent and normal, so we have equality, as required. □

Another interaction between the Frattini subgroup and nilpotence is the following result, due to Wielandt.

Proposition 2.15 (Wielandt) If G is a finite group, then $G' \leqslant \Phi(G)$ if and only if G is nilpotent.

Proof: If G is nilpotent then G is the direct product of its Sylow p_i-subgroups P_i. Clearly $\Phi(G)$ is the direct product of the $\Phi(P_i)$ and G' is the direct product of the P_i', so one direction is true.

Conversely, suppose that $G' \leqslant \Phi(G)$. By Exercise 2.7, if every maximal subgroup of G is normal then G is nilpotent; however, G/G' is abelian so every overgroup of G' is normal in G. In particular, the maximal subgroups of G, all of which contain G', are normal in G, proving the result. □

The last theorem that we will see in this section is a theorem of Philip Hall from 1958. We know that if K and G/K are soluble then G is soluble, but the same is not true with nilpotent in place of soluble. However, we do have something similar. We should start with a lemma.

Lemma 2.16 Let G be a finite group, and let K be a normal subgroup of G. Suppose that K is the product of normal subgroups K_i of G for $i = 1, \dots, n$. If L is another normal subgroup of G then

$$[K, L] = \prod_{i=1}^{n} [K_i, L].$$

Proof: This follows easily from the commutator identity $[xy, z] = [x, z]^y [y, z]$, as seen in Exercise 2.4. □

Theorem 2.17 (Philip Hall [6, Theorem 7]) Let G be a group and let K be a normal subgroup of G. If both K and G/K' are nilpotent, of classes c and d respectively, then G is nilpotent of class at most $f(c) = c(c+1)d/2 - c(c-1)/2$.

Proof: For this proof, write γXY for $[X, Y]$ and in general, $\gamma^m X_1 X_2 \dots X_{m+1}$ for the $(m+1)$-fold commutator

$$\gamma^m X_1 X_2 \dots X_{m+1} = [X_1, X_2, \dots, X_{m+1}].$$

Furthermore, if X is a subgroup of G, write $X_n = \gamma^n X G^n$.

Step 1: *For any two normal subgroups $X, Y \leqslant G$, $(\gamma YX)_n \leqslant \prod_{j=0}^{n} (\gamma Y_j X_{n-j})$ for all $n \geqslant 1$.* The three subgroup lemma says that

$$[Y, X, G] \leqslant [X, G, Y][G, Y, X].$$

By rewriting the terms in the commutator, this gives

$$(\gamma YX)_1 \leqslant (\gamma Y_0 X_1)(\gamma Y_1 X_0),$$

so the case $n = 1$ holds. Assume that the claim holds for $n < 1$: then by Lemma 2.16,

$$(\gamma YX)_n = [(\gamma YX)_{n-1}, G] \leqslant \prod_{j=0}^{n-1} [(\gamma Y_j X_{n-1-j}), G].$$

Finally, by the three subgroups lemma, we have that

$$[(\gamma Y_j X_{n-1-j}), G] = [Y_j, X_{n-1-j}, G] \leqslant [Y_{j+1}, X_{n-1-j}][Y_j, X_{n-j}].$$

This proves that $(\gamma YX)_n$ is contained in the product of the $\gamma Y_j X_{n-j}$, as required.

Step 2: *If X is a normal subgroup of G and $\gamma^m XG^m \leqslant X'$, then $(\gamma^{i-1}X^i)_{im-i+1} = \gamma^{im}X^iG^{im-i+1} \leqslant \gamma^i X^{i+1}$ for all $i \geqslant 1$.* By induction, assume the result is true for $i-1$. In the formula of Step 1, set $n = im - i + 1$ and $Y = \gamma^{i-2}X^{i-1}$, we get

$$(\gamma^{i-1}X^i)_{im-i+1} = (\gamma YX)_{im-i+1} \leqslant \prod_{j=0}^{im-i+1} [Y_j, X_{im+1-i-j}].$$

Consider the factors of the product. By induction hypothesis, $Y_{n-m+1} \leqslant [Y, X]$, and so for $j \geqslant n-m+1$ we have that $[Y_j, X_{n-j}] \leqslant [Y, X, X]$. For $j \leqslant n-m$, we have that $n-j \geqslant m \geqslant 1$, and so $X_{n-j} \leqslant X'$. Finally, $Y_j \leqslant Y$, so $[Y_j, X_{n-j}] \leqslant [Y, [X, X]]$. By the three subgroups lemma, $[Y, [X, X]] \leqslant [Y, X, X]$, and so

$$(\gamma^{i-1}X^i)_{im-i+1} \leqslant [Y, X, X] = \gamma^i X^{i+1},$$

proving the claim.

Step 3: *The conclusion.* Notice that, since G/K' is nilpotent of class d, $\gamma^d KG \leqslant K'$. Therefore, by Step 2,

$$(\gamma^{i-1}K^i)_{id-i+1} \leqslant \gamma^i K^{i+1}$$

for all $i \geqslant 1$. Notice that $f(j) - f(j-1) = jd - j + 1$, so we have, by induction, that

$$\gamma^{f(j)}G^{f(j)+1} \leqslant \gamma^{jd-j+1}(\gamma^{j-1}K^j)G^{jd-j+1} \leqslant \gamma^j K^{j+1}.$$

In particular, for $j = c$ we get that $\gamma^{f(c)}G^{f(c)+1} = 1$, as claimed. □

Chapter 3

The 1960s

3.1 Nilpotence of Frobenius Kernels

In this section we will use interchangeably the notations $x\phi$ and x^ϕ for the image of x under ϕ, in order to make the formulae easier to read. (For example, we write $x^{-1}x^\phi$ but $(x\phi)^{-1}$.)

Definition 3.1 Let G be a group. An automorphism ϕ of G is *fixed point free* if $x\phi = x$ implies $x = 1$.

As easy examples of fixed-point-free automorphisms, we have the non-trivial automorphism of C_3, and the automorphism of V_4 of order 3. Clearly, if a finite group G has a fixed-point-free automorphism of order p, then $|G| \equiv 1 \mod p$.

Lemma 3.2 Let G be a finite group, and let ϕ be a fixed-point-free automorphism of order n. We have that every element of G can be written in the form $x^{-1}(x\phi)$ or $(x\phi)x^{-1}$), and for all $x \in G$,

$$x(x^\phi)(x^{\phi^2})\dots(x^{\phi^{n-1}}) = 1.$$

Proof: If $x^{-1}x^\phi = y^{-1}y^\phi$ then $yx^{-1} = (y\phi)(x\phi)^{-1} = (yx^{-1})\phi$, so that $y = x$. Hence the map $x \mapsto x^{-1}x^\phi$ is an injection, so is a bijection as $|G|$ is finite: this proves the first part.

To see the second, write $x = y^{-1}y^\phi$: then

$$x(x^\phi)(x^{\phi^2})\dots(x^{\phi^{n-1}}) = (y^{-1}y^\phi)(y^{-1}y^\phi)^\phi\dots(y^{-1}y^\phi)^{\phi^{n-1}} = y^{-1}y^{\phi^n} = 1,$$

as the middle terms cancel each other off, and ϕ has order n. $\square$

The next lemma follows from Exercise 4.5, using the fact that $\mathrm{C}_G(\langle\phi\rangle) = 1$ if ϕ is fixed point free, but here we give a self-contained proof.

Lemma 3.3 Let G be a finite group, and let ϕ be a fixed-point-free automorphism of G. If p is a prime dividing $|G|$, then ϕ fixes a unique Sylow p-subgroup P of G.

Proof: If P is a Sylow p-subgroup of G, then $P\phi$ is also a Sylow p-subgroup of G. Therefore, $P\phi = x^{-1}Px$ for some $x \in G$. Thus for any $y \in G$,

$$(y^{-1}Py)\phi = (y^\phi)^{-1}x^{-1}Px(y^\phi).$$

However, every element of G can be expressed as $x^\phi x^{-1}$ by Lemma 3.2 and so choose y such that $y^\phi y^{-1} = x^{-1}$; then P^y is fixed under ϕ, as required.

Now suppose that P and P^x are fixed by ϕ. Therefore, $x^\phi x^{-1} \in \mathrm{N}_G(P)$. Again, since $x^\phi x^{-1}$ is in $\mathrm{N}_G(P)$, we see that (as $\mathrm{N}_G(P)$ is ϕ-invariant) there is an element $y \in \mathrm{N}_G(P)$ such that

$$x^\phi x^{-1} = y^\phi y^{-1}.$$

Since the map $x \mapsto x^\phi x^{-1}$ is a bijection, $x = y$, and so $P^x = P$, as needed. $\square$

If G is a group, then the map $x \mapsto x^{-1}$ is an *anti-automorphism*; that is, it is a map ϕ such that $(xy)^\phi = y^\phi x^\phi$. If G is abelian, then all anti-automorphisms are automorphisms, and so any abelian group of odd order has a fixed-point-free automorphism of order 2.

Lemma 3.4 Suppose that $\phi : G \to G$ is a bijection that is both an automorphism and an anti-automorphism. Then G is abelian.

Proof: Let x and y be elements of G. Since ϕ is a bijection, there are elements x' and y' such that $x'\phi = x$ and $y'\phi = y$. Since ϕ is both an automorphism and an anti-automorphism, we have

$$xy = (x'\phi)(y'\phi) = (x'y')\phi = (y'\phi)(x'\phi) = yx,$$

as G is abelian. $\square$

Corollary 3.5 Suppose that G has a fixed-point-free automorphism ϕ of order 2. Then G is an abelian group of odd order.

Proof: The map ϕ satisfies $x(x^\phi) = 1$, by Lemma 3.2. This implies that $x^\phi = x^{-1}$, and so this map is an automorphism. It is also an anti-automorphism, and so G possesses an automorphism that is also an anti-automorphism; thus G is abelian. $\square$

We need a technical result to prove the main result of this section, about semidirect products of automorphisms.

Lemma 3.6 Let G be a finite abelian group, and suppose that H is a subgroup of $\mathrm{Aut}(G)$ of the form $K \rtimes \langle \phi \rangle$. Suppose that, for all $k \in K$, the element $k\phi$ is fixed point free and of prime order p, and that $|K|$ and $|G|$ are coprime. Then K fixes some non-trivial element of G.

Proof: For each $k \in K$, and $x \in G$ the element

$$x^{1+(k\phi)+(k\phi)^2+\cdots+(k\phi)^{p-1}} = 1,$$

by Lemma 3.2. If $x \in G$, then we can multiply these together for all $k \in K$, and have

$$1 = \prod_{k \in K} \prod_{i=0}^{p-1} x^{(k\phi)^i} = x^{|K|} \prod_{i=1}^{p-1} \prod_{k \in K} x^{(k\phi)^i}.$$

Notice that clearly $\{k\phi^i \,:\, k \in K,\, 1 \leqslant i \leqslant p-1\} = H \setminus K$, but we claim also that

$$\{(k\phi)^i \,:\, k \in K,\, 1 \leqslant i \leqslant p-1\} = H \setminus K.$$

To see this, suppose that $(k\phi)^i = (l\phi)^j$, for some $1 \leqslant i, j \leqslant p-1$ and $k, l \in K$. The image of these maps in H/K is $K\phi^i$ and $K\phi^j$, so that $i = j$. Since $k\phi$ has order p, by raising to a certain power i' such that $ii' \equiv 1 \pmod p$, we get $(k\phi)^{ii'} = k\phi = l\phi = (l\phi)^{ii'}$, so that clearly $k = l$.

Applying this to the product above, we get that

$$1 = x^{|K|} \prod_{i=1}^{p-1} \prod_{k \in K} x^{(k\phi)^i} = x^{|K|} \prod_{i=1}^{p-1} \prod_{k \in K} x^{k\phi^i}.$$

Clearly, $\prod_{k \in K} x^{k\phi^i}$ is a fixed point of G under the action of all $k \in K$, and since $x^{|K|}$ is not the identity, one of the terms in the product must also not be the identity. Hence there is a fixed point of G under the action of K. □

Corollary 3.7 Let G be a finite abelian group, and let A be a homocyclic group of automorphisms of G, all of whose non-trivial elements act fixed-point-freely. Then A is cyclic.

Theorem 3.8 Let G be a finite soluble group. If G admits a fixed-point-free automorphism of prime order, then G is nilpotent.

Proof: Let G be a minimal counterexample. If $\mathrm{Z}(G) > 1$, then ϕ induces a fixed-point-free automorphism on $G/\mathrm{Z}(G)$, which is nilpotent by choice of G, and so G is nilpotent. Hence $\mathrm{Z}(G) = 1$.

Let ϕ be a fixed-point-free automorphism of order p of the soluble group G, and let Q be a minimal ϕ-invariant normal subgroup of G (lying in $G \rtimes \langle \phi \rangle$). Then Q is an elementary abelian q-subgroup, and clearly $p \neq q$.

If G is a q-group, then G is nilpotent, so let $r \neq q$ be a prime dividing $|G|$, and let R be the ϕ-invariant Sylow r-subgroup. Consider the subgroup QR; if $QR < G$, then by induction QR is nilpotent, and so Q and R centralize each other. This is true for all $r \neq q$ dividing $|G|$, and so $\mathrm{C}_G(Q)$ has index a power of q. In particular, $\mathrm{Z}(G) \neq 1$, since if S is a Sylow q-subgroup of G, then $1 \neq Q \cap \mathrm{Z}(S) \leqslant \mathrm{Z}(G)$.

Thus $G = Q \rtimes R$. Let K be the subgroup of $\mathrm{Aut}(Q)$ induced by the action of R on it, and let H be the semidirect product of K by $\langle \phi \rangle$. Then it is clear that $k\phi$ acts fixed point freely and has the same order as ϕ itself for any $k \in K$, and so K fixes a point of R by Lemma 3.6. Equivalently, there is a non-identity element $z \in Q$ such that $R \leqslant \mathrm{C}_G(z)$; clearly, $z \in \mathrm{Z}(G)$ as Q is abelian, and this again contradicts the choice of minimal counterexample, completing the proof. □

In order to prove the general case, we need the following definition and theorem.

Definition 3.9 Let G be a finite group. The *Thompson subgroup* of G, denoted $J(G)$, is the subgroup generated by all elementary abelian subgroups of G of maximal order.

Thompson's normal p-complement theorem will be proved later, as the culmination of the course. For now we simply state it.

Theorem 3.10 (Thompson, 1963) Let G be a group, and let p be an odd prime with $p \mid |G|$. If P is a Sylow p-subgroup of G, then G has a normal p-complement if and only if both $\mathrm{C}_G(\mathrm{Z}(P))$ and $\mathrm{N}_G(J(P))$ have normal p-complements.

With this theorem we can now prove the result.

Theorem 3.11 (Thompson, 1959) Suppose that a finite group G possesses a fixed-point-free automorphism ϕ of prime order. Then G is nilpotent.

Proof: We assume that G is a minimal counterexample, and prove that G is soluble, whence we are done by Theorem 3.8. If G is a 2-group then G is nilpotent, so choose q to be an odd prime dividing $|G|$, and let P denote a ϕ-invariant Sylow q-subgroup of G. Since both $Z = \mathrm{Z}(P)$ and $J = J(P)$ are characteristic in P, they are ϕ-invariant. If either Z or J is normal in G, then ϕ induces a fixed-point-free automorphism on G/Z or G/J, which are by induction nilpotent, and thus G is soluble.

The other possibility is that $\mathrm{N}_G(J)$ and $\mathrm{N}_G(Z)$ are both proper in G. By choice of minimal counterexample, both $\mathrm{C}_G(Z)$ and $\mathrm{N}_G(J)$ are nilpotent (as normalizers and centralizers of ϕ-invariant subgroups are ϕ-invariant), and so have normal q-complements. Therefore, G has a normal q-complement, say Q. Since Q is characteristic (a normal Hall q'-subgroup is characteristic) it is ϕ-invariant, and so is nilpotent by induction, and G is soluble. □

We finish discussing fixed-point-free automorphisms with a result on the structure of groups of automorphisms all elements of which act fixed-point-freely.

Theorem 3.12 (Burnside) Let G be a finite group and suppose that G accepts a group A of automorphisms, each (non-trivial) element of which acts fixed-point-freely. Then $|G|$ and $|A|$ are coprime, and all Sylow p-subgroups of A are of p-rank 1.

Proof: Suppose that p divides both $|G|$ and $|A|$, and let ϕ be an element of A of order p. Then ϕ fixes a Sylow p-subgroup of G, and so acts fixed-point-freely on P. However, counting ϕ-orbits yields an easy contradiction.

Now let P be a Sylow p-subgroup of A, and let S be a subgroup of P of order p^2. We will show that S is cyclic, proving our result. We claim that G possesses an S-invariant Sylow q-subgroup Q, where $q \mid |G|$ is a prime. If this is true, then let $K = \mathrm{Z}(Q)$, and apply Corollary 3.7: then S is an homocyclic group of automorphisms of an abelian group K, whence it is cyclic, as required.

It remains to prove that if P is a p-group acting on a group G with $p \nmid |G|$, then there is a P-invariant Sylow q-subgroup Q for all primes q dividing $|G|$. To see this, let R be any Sylow q-subgroup of G, and write $H = G \rtimes P$. Then, by the Frattini argument, $H = \mathrm{N}_H(R)G$. A Sylow p-subgroup $\bar{P}$ of $\mathrm{N}_H(R)$ is a Sylow p-subgroup of H, and hence there is an element g such that $\bar{P}^g = P$. Then

$$P = \bar{P}^g \leqslant \mathrm{N}_H(R^g),$$

and so $Q = R^g$ is a P-invariant Sylow q-subgroup, finishing the proof. □

Since nilpotent groups are direct products of their Sylow p-subgroups, each of which is clearly characteristic, we see that we need to understand fixed-point-free automorphisms of p-groups. The nilpotence class was proved to be finite by Higman, and the bound below was given by Kreknin and Kostrikin.

Theorem 3.13 (Higman, Kreknin, Kostrikin) Let G be a nilpotent group possessing a fixed-point-free automorphism of order p. The nilpotence class of G is bounded by the function $h(p)$, where

$$h(p) \leqslant \frac{(p-1)^{2^{p-1}-1} - 1}{p-2}.$$

3.2 Alperin's Fusion Theorem

Alperin's fusion theorem is one of the fundamental results on fusion in finite groups, and in some sense gives justification to the goal of local finite group theory. One of the main ideas in finite group theory, during the 1960s in particular, is that the structure of *p-local subgroups* – normalizers of non-trivial p-subgroups of a finite group – should determine the global structure of a finite simple group, or more generally an arbitrary finite group, in some sense. Thompson's normal p-complement theorem is an examplee of this, where the presence of normal p-complements in two different local subgroups implies the presence of a normal p-complement in the whole group.

Alperin's fusion theorem is the ultimate justification of this approach, at least in terms of fusion of p-elements, because it tells you that if x and y are two elements of a Sylow p-subgroup P, then you can tell whether x and y are conjugate in G by only looking at p-local subgroups.

Definition 3.14 Let G be a finite group, and let P and Q be Sylow p-subgroups of G. We say that $R = P \cap Q$ is a *tame intersection* if both $\mathrm{N}_P(R)$ and $\mathrm{N}_Q(R)$ are Sylow p-subgroups of $\mathrm{N}_G(R)$.

Examples of tame intersections are when the intersection is of index p in one (and hence both) of the Sylow subgroups, and more generally if the intersection is normal in both Sylow subgroups. Extremal subgroups were introduced in Exercise Sheet 2. In Exercise 2.9, we proved that every subgroup A of a Sylow p-subgroup P is conjugate to an extremal subgroup B, and in fact we can choose $g \in G$ such that $A^g = B$ so that $\mathrm{N}_P(A)^g \leqslant \mathrm{N}_P(B)$.

Lemma 3.15 Let G be a finite group, and let P be a Sylow p-subgroup of G. Let $g \in G$, and write $A = P \cap P^g$. The intersection $P \cap P^{g^{-1}}$ is tame if and only if both A and A^g are extremal in P with respect to G.

Proof: Since A is extremal in P with respect to G, $\mathrm{N}_P(A)$ is a Sylow p-subgroup of $\mathrm{N}_G(A)$. Also, since A^g is extremal, $\mathrm{N}_P(A^g)$ is a Sylow p-subgroup of $\mathrm{N}_G(A^g)$, so that $\mathrm{N}_{P^{g^{-1}}}(A)$ is a Sylow p-subgroup of $\mathrm{N}_G(A)$, as needed. □

Exercise 2.10 introduced the 'arrow notation' $A \xrightarrow{g} B$, which we will use in a very similar way to that exercise. Let P be a Sylow p-subgroup of a finite group G. a *family* $\mathscr{F}$ is a collection of subgroups of P. If $\mathscr{F}$ is a family and $A, B \subseteq P$ with $A^g = B$ for some $g \in G$, then we write $A \xrightarrow{g} B$ with respect to $\mathscr{F}$ if there are subgroups $R_1, \dots, R_n \in \mathscr{F}$ and elements $x_i \in \mathrm{N}_G(R_i)$ and $y \in \mathrm{N}_G(P)$, such that

(i) $g = x_1 x_2 \dots x_n y$, and

(ii) $A^{x_1x_2\dots x_i}$ is a subset of R_i and R_{i+1} for all $0 \leqslant i \leqslant n-1$.

A family $\mathscr{F}$ is a *conjugation family* if, whenever A and B are subsets of P such that $A = B^g$, we have that $A \xrightarrow{g} B$ with respect to $\mathscr{F}$. If the family under consideration is obvious, we will drop the 'with respect to $\mathscr{F}$'. In Exercise 2.10 we proved that the family of all subgroups of P is a conjugation family. Alperin's fusion theorem is better.

Theorem 3.16 (Alperin's fusion theorem [1]) Let G be a finite group, and let P be a Sylow p-subgroup of G. Let A and B be two subsets of P such that $A = B^g$. There exist Sylow p-subgroups $S_1, \dots, S_n$ of G, elements $x_1, \dots, x_n$ of G, and an element $y \in \mathrm{N}_G(P)$ such that

(i) $g = x_1x_2\dots x_ny$;

(ii) $P \cap S_i$ is a tame intersection for all i;

(iii) x_i is an element of $\mathrm{N}_G(P \cap S_i)$ for all i;

(iv) $A^{x_1x_2\dots x_i}$ is a subset of $P \cap S_{i+1}$ for all $0 \leqslant i \leqslant n-1$.

In other words, the collection of all tame intersections $P \cap S$ where $S \in \mathrm{Syl}_p(G)$ is a conjugation family.

Proof: Let $\mathscr{F}$ be the family of all tame intersections. We will show that, if A and B are two subsets of P and $g \in G$ is such that $A^g = B$, then $A \xrightarrow{g} B$ (with respect to $\mathscr{F}$). Note that if $A \xrightarrow{g} B$ and $C \subseteq A$, then $C \xrightarrow{g} C^g$, and if $A \xrightarrow{g} B$ and $B \xrightarrow{h} C$, then $A \xrightarrow{gh} C$ and $B \xrightarrow{g^{-1}} A$.

We may assume that A and B are subgroups of P, since $A \xrightarrow{g} B$ if and only if $\langle A \rangle \xrightarrow{g} \langle B \rangle$. We proceed by induction on $m = |P : A|$. If $m = 1$ then $A = P$, whence $g \in \mathrm{N}_G(P)$, and $P \xrightarrow{g} P$, so we may suppose that $m > 1$. In fact, we may assume that $A = P \cap P^{g^{-1}}$, an intersection of two Sylow p-subgroups of G, since if $A < P \cap P^{g^{-1}}$ then by induction $P \cap P^{g^{-1}} \xrightarrow{g} P \cap P^g$, whence $A \xrightarrow{g} B$ since $A \subseteq P \cap P^{g^{-1}}$. Hence from now on we let $R = P^{g^{-1}}$, and note that $A = R \cap P$.

Step 1: *The case where $R \cap P$ is a tame intersection.* Suppose that $R \cap P$ is a tame intersection. Clearly $B = (R \cap P)^g = P \cap P^g$ is also a tame intersection, and hence both A and B are extremal in P with respect to G. Hence there exists $h \in G$ such that $A^h = B$ and $\mathrm{N}_P(A)^h = \mathrm{N}_P(B)$ by Exercise 2.9, and hence by induction $\mathrm{N}_P(A) \xrightarrow{h} \mathrm{N}_P(B)$ and so $A \xrightarrow{h} B$. Clearly, $h^{-1}g \in \mathrm{N}_G(B)$, $B \xrightarrow{h^{-1}g} B$, and so $A \xrightarrow{g} B$, as needed.

Step 2: *The general case.* By hypothesis $A < P$, and so $A < \mathrm{N}_P(A)$. Choose C a subgroup of P that is G-conjugate to A and extremal in P with respect to G. By Exercise 2.9, we may choose $h \in G$ such that $A^h = C$ and $\mathrm{N}_P(A)^h \leqslant \mathrm{N}_P(C)$, so that by induction $\mathrm{N}_P(A) \xrightarrow{h} (\mathrm{N}_P(A))^h$ and hence $A \xrightarrow{h} C$. Similarly, there exists $k \in G$ such that $B \xrightarrow{k} C$. We see therefore that $x = h^{-1}gk$ normalizes C. If $X = P \cap P^{x^{-1}}$ properly contains C then by induction $X \xrightarrow{x} X^x$ so $C \xrightarrow{x} C$, whence

$$A \xrightarrow{h} C \xrightarrow{x} C \xrightarrow{k} B,$$

and so $A \xrightarrow{g} B$. Therefore $X = C$, so that C is the intersection of P and $P^{x^{-1}}$. As C and $C = C^x$ are both extremal in P with respect to G, by Lemma 3.15 we see that C is a tame intersection, whence by Step 1, $C \xrightarrow{x} C$, as needed. $\square$

In Exercise Sheet 6 we will prove more facts about conjugation families, and in fact classify them.

3.3 Focal Subgroup Theorem

The focal subgroup theorem proves that abelian quotients of a finite group that are p-groups are locally determined.

Definition 3.17 Let G be a finite group, and let P be a Sylow p-subgroup of G. Denote by $A^p(G)$ the subgroup $G' \mathrm{O}^p(G)$, or equivalently the smallest normal subgroup of G whose quotient is an abelian p-group.

Lemma 3.18 Let G be a finite group, and let P be a Sylow p-subgroup of G. We have $P \cap A^p(G) = P \cap G'$ and

$$G/A^p(G) \cong P/(P \cap G').$$

Proof: Since $A^p(G) = G' \mathrm{O}^p(G)$, by the second isomorphism theorem we have

$$G/A^p(G) = PA^p(G)/A^p(G) \cong P/(P \cap A^p(G)) = P/(P \cap G'),$$

with the last equality due to the fact that $p \nmid |A^p(G) : G'|$, so that $P \cap A^p(G) = P \cap G'$. $\square$

The subgroup $P \cap G'$ is the *focal subgroup* of P in G.

Theorem 3.19 (Focal subgroup theorem, D. Higman [8]) If G is a finite group with Sylow p-subgroup P, then

$$\begin{aligned} P \cap G' &= \langle [x, g] \,:\, x, x^g \in P,\ g \in G \rangle \\ &= \langle x^{-1}y \,:\, x, y \in P,\ y = x^g \text{ for some } g \in G \rangle \end{aligned}$$

Proof: Let $Q = \langle x^{-1}y \,:\, x, y \in P,\ y = x^g \text{ for some } g \in G\rangle$. Notice that $P' \leqslant Q$ since Q contains $[x, g]$ for $x, g \in P$. In particular, $Q \trianglelefteq P$ and P/Q is abelian. Also, clearly $Q \leqslant G'$ so that $P' \leqslant Q \leqslant P \cap G'$. Let $\theta : P \to P/Q$ be the natural map, and let τ denote the transfer of θ, so that $\tau \in \mathrm{Hom}(G, P/Q)$.

Let $x \in P$ and let $\{t_1, \dots, t_n\}$ denote a transversal to P in G, where $n = |G : P|$. Choose the first d of the t_i and the integers r_i with $\sum_{i=1}^{d} r_i$ so that the transfer τ becomes (using Proposition 1.10)

$$x\tau = \prod_{i=1}^{d} (t_i x^{r_i} t_i^{-1})\theta = Q\left(\prod_{i=1}^{d} (t_i x^{r_i} t_i^{-1})\right).$$

Since P/Q is abelian,

$$x\tau = Q\left(\prod_{i=1}^{d} (t_i x^{r_i} t_i^{-1})\right) = Q\left(\prod_{i=1}^{d} x^{r_i}\right)\left(\prod_{i=1}^{d} (x^{-r_i} t_i x^{r_i} t_i^{-1})\right).$$

The second product is of commutators $[x^{r_i}, t_1^{-1}]$, which lie in Q by definition, and so

$$x\tau = Q\left(\prod_{i=1}^{d} x^{r_i}\right) = Qx^{\sum r_i} = Qx^n.$$

Since n and p are coprime, $Qx^n = Q$ if and only if $x \in Q$. Hence $\ker\tau \cap P = Q$. Since $G/\ker\tau$ is an abelian p-group, $A^p(G) \leqslant \ker\tau$, so that $P \cap A^p(G) = P \cap G' \leqslant P \cap \ker\tau = Q$. Hence $P \cap G' = Q$, as claimed. □

The next result on the generation of the focal subgroup is sometimes useful.

Proposition 3.20 Let P be a Sylow p-subgroup of the finite group G. The focal subgroup $P \cap G'$ is generated by the subgroups $[R, \mathrm{N}_G(R)]$, as R ranges over all non-trivial tame intersections R of P with respect to G.

Proof: Let S be the subgroup generated by the subgroups of the form $[R, \mathrm{N}_G(R)]$, where R is a non-trivial extremal subgroup of P as in the statement. Certainly S is contained within G', and since $[R, \mathrm{N}_G(R)] \leqslant R \leqslant P$, we have that $S \leqslant P \cap G'$.

By the focal subgroup theorem, if we can show that $a^{-1}b$ lies in S for all a and b in P that are G-conjugate, we are done. We will use Alperin's fusion theorem to prove this result: by this theorem, there are tame intersections $R_i = P \cap S_i$ for $S_i \in \mathrm{Syl}_p(G)$, and elements $x_1, \dots, x_r$, with $x_i \in \mathrm{N}_G(R_i)$ for all i, such that

$$(x_1 \dots x_i)^{-1} a (x_1 \dots x_i) \in R_{i+1}$$

for all $i < r$, and $x_1 \dots x_r = g$. (Here we have used the fact that P is a tame intersection, and so may be one of the R_i.)

Let $a_0 = a$ and $a_i = a_{i-1}^{x_i}$, so that $a_r = b$; then both a_{i-1} and a_i lie in R_i (since a_{i-1} lies in R_i by assumption and x_i normalizes R_i), and $a_{i-1}^{x_i} = a_i$, with $x_i \in \mathrm{N}_G(R_i)$. Therefore

$$a_{i-1}^{-1} a_i = a_{i-1}^{-1} x_i^{-1} a_{i-1} x_i \in [R, \mathrm{N}_G(R_i)],$$

and since

$$a^{-1}b = a_0^{-1} a_r = (a_0^{-1} a_1) \dots (a_{r-1}^{-1} a_r),$$

we have that $a^{-1}b \in S$, as needed. □

Using the focal subgroup theorem, we may prove Frobenius's normal p-complement theorem, which we proved directly using the transfer in Exercise Sheet 3.

Theorem 3.21 (Frobenius's normal p-complement theorem) Let G be a finite group and let P be a Sylow p-subgroup of G. The following are equivalent:

(i) G possesses a normal p-complement;

(ii) P controls fusion in P with respect to G;

(iii) for every p-subgroup Q of G, $\mathrm{Aut}_G(Q)$ is a p-group.

Proof: Exercise 3.6 proves that (ii) and (iii) are equivalent, and Exercise 3.5 proves that (i) implies (iii), so it remains to assume (ii) and prove (i). We will show firstly that G has a non-trivial p-factor group; we will prove that $P \cap G' = P'$, and so G has a non-trivial p-factor group. By (ii) the G-conjugates of elements of P are simply the P-conjugates of elements of P. The focal subgroup theorem says that

$$\begin{aligned} P \cap G' &= \langle x^{-1}y \,:\, y = x^g \text{ for some } g \in G\rangle \\ &= \langle x^{-1}y \,:\, y = x^g \text{ for some } g \in P\rangle \\ &= \langle [x,g] \,:\, x, g \in G\rangle \\ &= P'. \end{aligned}$$

Since $P' < P$, we see that G has a non-trivial p-factor group. The rest of the proof follows Exercise 3.7(ii), yielding that (i) is true. □

Just as the maximal abelian p-factor group can be written, via the second isomorphism theorem, as a quotient of P by some naturally defined subgroup, the same is true for the maximal p-factor group. Indeed, since $G/\mathrm{O}^p(G)$ is a p-group, we have that $G = P\,\mathrm{O}^p(G)$, and so

$$G/\mathrm{O}^p(G) \cong P/(P \cap \mathrm{O}^p(G)).$$

Just as the maximal abelian p-factor group can be detected in the fusion system, the same is true for the maximal p-factor group. This the content of Puig's hyperfocal subgroup theorem. Define the *hyperfocal subgroup* of P in G to be the subgroup $P \cap \mathrm{O}^p(G)$.

Theorem 3.22 (Hyperfocal subgroup theorem, Puig [9]) Let G be a finite group, and let P be a Sylow p-subgroup of G. Then

$$\begin{aligned} P \cap \mathrm{O}^p(G) &= \langle [x,g] \,:\, x \in Q \leqslant P,\, g \in \mathrm{N}_G(Q),\, g \text{ has } p'\text{-order}\rangle \\ &= \langle x^{-1}(x\phi) \,:\, x \in Q \leqslant P,\, \phi \in \mathrm{O}^p(\mathrm{N}_G(Q))\rangle \\ &= \langle x^{-1}(x\phi) \,:\, x \in Q \leqslant P,\, \phi \in \mathrm{O}^p(\mathrm{Aut}_G(Q))\rangle \end{aligned}$$

Proof: Firstly notice that the subgroups on the right-hand side are all the same, and so it suffices to check the theorem for any one of them; write S for this subgroup of P. Firstly,

$S \leqslant P \cap \mathrm{O}^p(G)$, since if Q is a subgroup of P, if $x \in Q$ and $y \in \mathrm{O}^p(\mathrm{N}_G(Q))$, then $[x, y] \in \mathrm{O}^p(G)$, and it also lies in Q. Therefore it remains to show that $P \cap \mathrm{O}^p(G)$ is contained in S.

Let $H = \mathrm{O}^p(G)$ and $Q = P \cap H$; since H has no non-trivial p-quotients, $Q \cap H' = Q$, and by Proposition 3.20 this subgroup is generated by the subgroups $[R, \mathrm{N}_H(R)]$, where R is a subgroup of Q extremal in Q with respect to H.

Also, $\mathrm{N}_H(R)$ is generated by $\mathrm{O}^p(\mathrm{N}_H(R))$ and a Sylow p-subgroup of $\mathrm{N}_H(R)$, such as $\mathrm{N}_Q(R)$ (as R is extremal). Therefore, $[R, \mathrm{N}_H(R)]$ is generated by $[R, \mathrm{O}^p(\mathrm{N}_H(R))]$ and $[R, \mathrm{N}_Q(R)] \leqslant Q'$. Hence Q is generated by subgroups of the form $[R, \mathrm{O}^p(\mathrm{N}_H(R))]$, each of which is contained within S, and Q', so $Q = \langle S, Q' \rangle$; since S is a normal subgroup of Q, this means that Q/S is perfect, a contradiction unless Q/S is trivial, as needed. $\square$

3.4 The Generalized Fitting Subgroup

If G is a finite soluble group then we saw that $\mathrm{C}_G(F(G)) \leqslant F(G)$. However, if G is not soluble, we do not get that $\mathrm{C}_G(F(G)) \leqslant F(G)$ in general. As an obvious example, if G is a simple group, $F(G) = 1$.

Definition 3.23 Let G be a finite group. We say that G is *quasisimple* if G is perfect and $G/\mathrm{Z}(G)$ is simple. If H is quasisimple and subnormal in G then H is a *component* of G. The set of components of G is denoted $\mathrm{Comp}(G)$.

Components are the obstructions to the statement $\mathrm{C}_G(F(G)) \leqslant F(G)$, in the sense that if $\mathrm{C}_G(F(G)) \nleqslant F(G)$ then G has a component (Lemma 3.29), and if one includes the components into $F(G)$ one gets a normal subgroup X such that $\mathrm{C}_G(X) \leqslant X$ (Theorem 3.30). We start with a trivial lemma, before proving that components often commute with subnormal subgroups.

Lemma 3.24 Let H be a subnormal subgroup of a finite group G. Then $\mathrm{Comp}(H)$ is the set of components of G lying in H.

Lemma 3.25 Let C be a component of a finite group G. If H is a subnormal subgroup of G, then either C is a component of H or C and H commute.

Proof: Let G be a minimal counterexample to the lemma. If $C = G$ then H is a subnormal subgroup of C, so that $H \leqslant \mathrm{Z}(C)$, and H commutes with C. Hence $C < G$, so in particular the normal closure X of C is a proper subgroup of G. Similarly, if $H = G$ then C is a component of H, so that $H < G$, so the normal closure Y of H in G is a proper subgroup. As X and Y are normal subgroups of G, $X \cap Y$ is a normal subgroup of X. Since C is a component of X, either C is a component of $X \cap Y$ or C and $X \cap Y$ commute.

If C is a component of $X \cap Y$ then C is a component of Y by Lemma 3.24. Since $H \leqslant Y < G$, the lemma holds for Y, and so either $[C, H] = 1$ or $C \in \mathrm{Comp}(H)$, as needed. Thus $[C, X \cap Y] = 1$. Therefore, since $[Y, C] \leqslant [Y, X] \leqslant X \cap Y$, we have

$$[Y, C, C] \leqslant [X \cap Y, C] = 1.$$

Using the three subgroups lemma, we have that $[Y, C, C] = [C, Y, C] = 1$, and so $[C, Y] = [C, C, Y] = 1$, as needed. $\square$

Corollary 3.26 Let G be a finite group.

(i) If H and K are two different components of G then $[H, K] = 1$.

(ii) If H is a component of G then $[H, F(G)] = 1$.

This follows easily because $F(G)$ is a nilpotent group, and hence has no quasisimple subgroups at all.

Since any two components H and K of G centralize one another, they normalize one another, and so HK is a subgroup of G. Notice that if L is any other component of G, then L commutes with H and K, so commutes with HK, and we may form the subgroup HKL. Continuing in this way, if $C_1, \ldots, C_d$ are the components of G, we see that for $I \subseteq \{1, \ldots, d\}$,

$$\langle C_i : i \in I \rangle = \prod_{i \in I} C_i,$$

and for $j \notin I$, C_j commutes with this subgroup.

Definition 3.27 Let G be a finite group. Denote by $E(G)$ the subgroup generated by all components of G, called the *Bender subgroup*. Denote by $F^*(G)$ the product $E(G)F(G)$, the *generalized Fitting subgroup* of G.

Notice that conjugation by $g \in G$ permutes the components of G, so normalizes the subgroup generated by them, so $E(G) \trianglelefteq G$ and hence $F^*(G) \trianglelefteq G$. By the remarks above, $E(G)$ is the product of the components of G, and in fact $E(G)$ is the central product of the components of G. As $E(G)$ commutes with $F(G)$, $F^*(G)$ is the central product of $E(G)$ and $F(G)$.

Corollary 3.28 $E(G)$ is the central product of the components of G. $F^*(G)$ is the central product of $E(G)$ and $F(G)$.

Notice that $F^*(G) > 1$, since any minimal normal subgroup of G lies in $F^*(G)$. As claimed, $E(G)$ contains the obstructions to a group G satisfying $\mathrm{C}_G(F(G)) \leqslant F(G)$.

Lemma 3.29 Let G be a finite group. If $\mathrm{C}_G(\mathrm{F}(G)) \nleqslant \mathrm{F}(G)$ then $E(G) \neq 1$.

Proof: Write $C = \mathrm{C}_G(F(G))$ and $Z = \mathrm{Z}(F(G)) = F(G) \cap C$. Let $\bar{C} = C/Z$, and let $\bar{S}$ be the *socle* of $\bar{C}$, that is, the product of all minimal normal subgroups of C/Z. The subgroup $\bar{S}$ has no soluble normal subgroups, as if it had one, say $\bar{X}$, the preimage X of $\bar{X}$ in G would be a soluble normal subgroup of G with $\mathrm{C}_X(F(X)) \nleqslant F(X)$, a contradiction. Thus $\bar{S}$ is a direct product of non-abelian simple groups

$$\bar{S}_1 \times \cdots \times \bar{S}_r.$$

Let $S_1, \ldots, S_r$ be the full preimages in C of $\bar{S}_1, \ldots, \bar{S}_r$. Thus, each S_i is subnormal in G, and S_i/Z is simple. Hence S_i' is quasisimple and S_i' is subnormal in G, so are components of G, as needed. $\square$

Using this result, we can extend our statement that for soluble groups $\mathrm{C}_G(F(G)) \leqslant F(G)$ to all finite groups, replacing $F(G)$ by $F^*(G)$.

Theorem 3.30 (Bender) Let G be a finite group. We have $\mathrm{C}_G(F^*(G)) = \mathrm{Z}(F^*(G)) \leqslant F^*(G)$.

Proof: By Lemma 3.29, we may assume that $E(G) \neq 1$. Write $C = \mathrm{C}_G(E(G))$, so that $E(C) \leqslant E(G)$ by Lemma 3.24. Also, as $C \cap E(G) \leqslant \mathrm{Z}(E(G))$, we have $E(C) = 1$; hence $F(G) = F(C)$. Since $E(C) = 1$, we have $\mathrm{C}_C(F(C)) \leqslant F(C)$ by Lemma 3.29. Thus

$$\begin{aligned} \mathrm{C}_G(F^*(G)) &= \mathrm{C}_G(F(G)) \cap \mathrm{C}_G(E(G)) \\ &= \mathrm{C}_G(F(G)) \cap C = \mathrm{C}_G(F(C)) \cap C \\ &= \mathrm{C}_C(F(C)) \leqslant F(C) = F(G) \leqslant F^*(G), \end{aligned}$$

as needed. □

As $F^*(G)$ is a normal subgroup of G, we see that $F^*(G)/\mathrm{C}_G(F^*(G)) = F^*(G)/\mathrm{Z}(F^*(G))$ is a subgroup of $\mathrm{Aut}(F^*(G))$. If we simplify things, say by assuming that $F(G) = 1$, then $F^*(G)$ is a direct product of simple groups. Hence we want to understand $\mathrm{Aut}(S)$ for S a finite simple group, and then $\mathrm{Aut}(S_1 \times \cdots \times S_n)$, where the S_i are simple groups.

If G is a finite group then $\mathrm{Inn}(G) = G/\mathrm{Z}(G)$ is a subgroup of $\mathrm{Aut}(G)$, called the *inner automorphism group*, and $\mathrm{Aut}(G)/\mathrm{Inn}(G) = \mathrm{Out}(G)$ is called the *outer automorphism group*. Note that elements of $\mathrm{Out}(G)$ are not automorphisms, but cosets of $\mathrm{Inn}(G)$, so an element of $\mathrm{Out}(G)$ is only determined up to conjugation by some element of G. If G is a group such that $\mathrm{Z}(G) = 1$ (e.g., G is simple) then G embeds naturally in $\mathrm{Aut}(G)$, so for any subgroup A of $\mathrm{Out}(G)$ there is a group X, containing G as a normal subgroup, such that X induces A on G by conjugation.

Theorem 3.31 (Schreier conjecture) If G is a finite simple group, then $\mathrm{Out}(G)$ is a soluble group.

This theorem requires the classification of the finite simple groups. Using the classification, it simply becomes a matter of determining $\mathrm{Out}(S)$ for S a finite simple group. Although determining this for all finite simple groups is well beyond the scope of this course, we will do this for alternating groups.

Let $G = A_n$ for $n \geqslant 5$. The symmetric group S_n is a finite group such that A_n is a normal subgroup of S_n, and conjugation by (for example) $(1,2)$ induces an outer automorphism of A_n. Hence $S_n \leqslant \mathrm{Aut}(A_n)$. If $S_n < \mathrm{Aut}(A_n)$, then the elements of $\mathrm{Aut}(A_n)$ also induce outer automorphisms on S_n.

Lemma 3.32 Let $\rho \in \mathrm{Aut}(S_n)$ be an automorphism that sends transpositions to transpositions. Then ρ is inner.

Proof: A generating set for S_n are the transpositions $x_i = (i, i+1)$. Notice that $(a, b)(c, d)$ has order 1 if $\{a, b\} = \{c, d\}$, 3 if $\{a, b\} \cap \{c, d\}$ has size 1, and order 2 if $\{a, b\}$ and $\{c, d\}$ are disjoint. This will be used to get information on $x_i\rho$, given that we have determined $x_j\rho$ for $j < i$.

The transposition $x_1 = (1, 2)$ may be sent to any of the $n(n-1)/2$ transpositions, which we may label so that $x_1\rho = (1, 2)$. The image of $x_2 = (2, 3)$ is either $(1, a)$ or $(2, a)$, where $3 \leqslant a \leqslant n$, yielding $2(n-2)$ choices for $x_2\rho$. Again, we may label $a = 3$ without loss of generality.

From then on, since x_i and x_j commute for $j < i-1$, this means that $x_i\rho = (i, a_i)$ (as it does not commute with $x_{i-1}\rho = (i-1, i)$, but does commute with $x_{i-2}\rho = (i-2, i-1)$, so that i is moved by $x_i\rho$). This yields $n-i$ choices for $x_i\rho$, and so the total number of choices is

$$\left(\frac{n(n-1)}{2}\right)\big(2(n-2)\big)\prod_{i=3}^{n-1}(n-i) = n!.$$

This proves that the total number of such automorphism is $n!$, the size of $\mathrm{Inn}(S_n)$. □

Theorem 3.33 If $n \neq 2, 6$ then $\mathrm{Aut}(S_n) = S_n$.

Proof: If the size of the conjugacy class of transpositions, $n(n-1)/2$, is different from all other sizes of conjugacy classes of elements of order 2 (i.e., products of transpositions), then any automorphism of S_n sends transpositions to transpositions, and so is inner by Lemma 3.32. For $n = 3, 4, 5$, this is clear by an easy calculation, whereas for $n = 6$ the conjugacy classes of $(1, 2)$ and $(1, 2)(3, 4)(5, 6)$ have the same size.

Hence we assume that $n \geqslant 7$, and let t be the product of k transpositions of S_n, with m conjugates. We prove that $m \geqslant n(n-1)/2$, and is equal to that for t a transposition. There are

$$\left(\frac{n(n-1)}{2}\right)\cdot\left(\frac{(n-2)(n-3)}{2}\right)\cdots\left(\frac{(n-2k-2)(n-2k-1)}{2}\right)$$

k-tuples of disjoint transpositions, and since disjoint transpositions commute, we have

$$m = n(n-1)(n-2)\dots(n-2k-1)/k!2^k.$$

Since we ask whether $m = n(n-1)/2$, we seek n and $k > 1$ such that

$$(n-2)\dots(n-2k-1) = k!2^{k-1}.$$

Since $n \geqslant 2k$, the left-hand side is minimized when $n = 2k$, in which case it becomes

$$(2k-2)\dots 1 = k!2^{k-1},$$

and this becomes $(2k-2)! = k!2^{k-1}$. It is easy to show that for $k \geqslant 4$ the left-hand side is strictly greater than 1, and so we may assume that t is the product of either two or three transpositions. There are $n(n-1)(n-2)(n-3)/8$ double transpositions, and this is greater than $n(n-1)/2$ for $n \geqslant 7$, as is the number of triple transpositions for $n \geqslant 7$. Hence the result is proved.

$$m \geqslant \frac{(n-d)(n-d-1)}{2} \cdot \binom{n}{d} = \frac{n(n-1)}{2}\binom{n-2}{d}.$$

The right hand side is greater than $n(n-1)/2$ for $d > 0$ and so the proof is complete. $\square$

The cases $n = 2, 6$ are genuine exceptions. If $n = 2$ then $S_n = C_2$, so $\mathrm{Aut}(S_2) = 1$. When $n = 6$ there is an exceptional outer automorphism of S_n, which is a freak of nature. It comes from the fact that there are six Sylow 5-subgroups of S_5.

The fact that there are six Sylow 5-subgroups of S_5 means that there is a transitive action of S_5 on six points, and hence an embedding H of S_5 into $G = S_6$, which is not the stabilizer of a point. Consider the permutation representation of G on the cosets of H, which is an isomorphism $\rho : G \to G$. To see that this is not an inner isomorphism, notice that the image of $(1, 2)$ is the product of *three* transpositions, so this must be an outer automorphism.

Finally, to see that $\mathrm{Out}(S_6) = C_2$, we see that any automorphism must either send transpositions to themselves, so is inner, or to triple transpositions, whence the product of this automorphism with ρ is inner, so that $\mathrm{Inn}(S_6)\rho$ is the only other coset of $\mathrm{Inn}(S_6)$ in $\mathrm{Aut}(S_6)$.

If G is a sporadic simple group then $\mathrm{Out}(G)$ has order either 1 or 2, and if G is a group of Lie type (e.g., $\mathrm{PSL}_n(q)$) then there are three types of outer automorphism – diagonal, graph and field – and the structure of $\mathrm{Out}(G)$ is known.

Chapter 4

The 1990s

4.1 Saturated Fusion Systems

By the 1990s Puig had finished formulating the notion of a *fusion system*, which encodes in an abstract sense the conjugation and fusion properties inherent in the Sylow p-subgroup of a finite group.

We need a quick reminder about categories, which aren't anything complicated, but are a useful definition for things in an abstract setting. We give an approximate definition of a category (without bothering with set-theoretic nonsense).

Definition 4.1 A *category* $\mathscr{C}$ consists of a set of *objects*, and for every two objects x and y in $\mathscr{C}$ a set $\mathrm{Hom}_{\mathscr{C}}(x, y)$ of *morphisms*. The morphisms should have a composition

$$\mathrm{Hom}_{\mathscr{C}}(x, y) \times \mathrm{Hom}_{\mathscr{C}}(y, z) \to \mathrm{Hom}_{\mathscr{C}}(x, z)$$

that is associative, and there should be an element $\mathrm{id}_x : x \to x$ that acts like the identity morphism.

In our case, the objects of our category will be all subgroups of a finite p-group, and the morphisms will be injective homomorphisms between them, so that composition between them is obvious.

Definition 4.2 Let G be a finite group and let P be a Sylow p-subgroup of G. the *fusion system* of G on P, denoted $\mathcal{F}_P(G)$, is a category, whose objects are all subgroups of P, and whose morphisms are given by

$$\mathrm{Hom}_{\mathcal{F}_P(G)}(Q, R) = \{\, c_g : Q \to R \mid Q^g \leqslant R \,\}.$$

The fusion system of a group is a convenient language for talking about all of the notions of fusion that we have seen before in this course, such as Alperin's fusion theorem, the focal subgroup theorem, Burnside's normal p-complement theorem, Frobenius's normal p-complement theorem, and so on. We start understanding this with a lemma. For this, we need the notion of an isomorphism of a fusion system. If $\theta : P \to Q$ is an isomorphism, and $A, B \leqslant P$ with an injective homomorphism $\phi : A \to B$, then θ induces a map $\phi^\theta = \theta^{-1}\phi\theta : A\phi \to B\phi$ given by

$$\phi^\theta : a\theta \mapsto (a\phi)\theta.$$

An *isomorphism* $\mathcal{F}_P(G) \to \mathcal{F}_Q(H)$ is an isomorphism $\theta : P \to Q$ such that, for all $A, B \leqslant P$, the map $\mathrm{Hom}_{\mathcal{F}_P(G)}(A, B) \to \mathrm{Hom}_{\mathcal{F}_Q(H)}(A\theta, B\theta)$ given by $\phi \mapsto \phi^\theta$ is a bijection.

Lemma 4.3 Let G be a finite group, and let P be a Sylow p-subgroup of G. Let $H = \mathrm{O}_{p'}(G)$, and write Q for the image of P in G/H. The homomorphism $\phi : G \to G/H$ induces an isomorphism $\theta : P \to Q$, and this induces an isomorphism of fusion systems $\mathcal{F}_P(G) \to \mathcal{F}_Q(G/H)$.

Proof: See Exercise 7.1. $\square$

The fusion system $\mathcal{F}_P(G)$ allows us to express control of fusion statements easily. Notice that if H is a subgroup of G and $P \cap H$ is a Sylow p-subgroup of H (e.g., if $P \leqslant H$ or if $H \trianglelefteq G$) then $\mathcal{F}_{P\cap H}(H)$ is naturally a 'subsystem' of $\mathcal{F}_P(G)$. We give two earlier theorems from the course, dressed in the language of fusion systems.

Proposition 4.4 (Frobenius's normal p-complement theorem) $\mathcal{F}_P(G) = \mathcal{F}_P(P)$ if and only if G has a normal p-complement.

Proposition 4.5 (Burnside) If P is abelian then $\mathcal{F}_P(G) = \mathcal{F}_P(\mathrm{N}_G(P))$.

(Later on we will construct a normalizer subsystem $\mathrm{N}_\mathcal{F}(Q)$ of a subgroup Q, and $\mathrm{N}_\mathcal{F}(Q)$ will be the subsystem corresponding to $\mathrm{N}_G(Q)$.)

A fusion system of a finite group is a nice way of expressing control of fusion and normal p-complement theorems, but fusion systems have become a powerful tool because there is an abstract theory of them. To develop this theory we need an abstract definition of a fusion system, which we give now.

Definition 4.6 Let P be a finite p-group. A *fusion system* $\mathcal{F}$ on P is a category, whose objects are all subgroups of P and whose morphisms $\mathrm{Hom}_\mathcal{F}(Q, R)$ are a subset of all injective homomorphisms $Q \to R$, with composition the usual composition of homomorphisms. The category $\mathcal{F}$ should satisfy the following three axioms:

(i) if $x \in P$ is such that $Q^x \leqslant R$ then $c_x : Q \to R$ lies in $\mathrm{Hom}_\mathcal{F}(Q, R)$ (i.e., $\mathcal{F}_P(P) \subseteq \mathcal{F}$);

(ii) if $\phi \in \mathrm{Hom}_{\mathcal{F}}(Q,R)$ then the associated isomorphism $\phi' : Q \to Q\phi$ lies in $\mathrm{Hom}_{\mathcal{F}}(Q,Q\phi)$;

(iii) if $\phi \in \mathrm{Hom}_{\mathcal{F}}(Q,R)$ is an isomorphism then ϕ^{-1} lies in $\mathrm{Hom}_{\mathcal{F}}(R,Q)$.

For $Q \leqslant P$, write $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Hom}_{\mathcal{F}}(Q,Q)$.

This definition looks quite abstract, and as it stands isn't all that useful, because the conditions we have applied haven't really restricted things: what this means is that if we have *any* collection of injective homomorphisms between subgroups of P then there is a fusion system containing them.

Example 4.7 If G is a finite group with Sylow p-subgroup P, then $\mathcal{F}_P(G)$ is a fusion system on P. Note that $\mathrm{Aut}_{\mathcal{F}_P(G)}(Q) = \mathrm{Aut}_G(Q)$.

Example 4.8 If P is a finite p-group, define $\mathcal{U}(P)$ to be the fusion system on P, where $\mathrm{Hom}_{\mathcal{U}(P)}(A,B)$ consists of *all* injective homomorphisms $A \to B$. This is called the *universal fusion system* on P, and obviously contains all other fusion systems on P.

To get the rigid structure that we need, we will have to define a *saturated* fusion system. This definition looks technical, but it captures enough of the structure of a finite group to be useful. It embodies two concepts: firstly, that p-automorphisms of subgroups Q of a Sylow p-subgroup P should be inherited from P itself (as P is a maximal p-subgroup of G), and we should be able to use induction on the index of a subgroup of P, so we need a way of extending (some) isomorphisms $A \to B$ to overgroups of A.

Let $\mathcal{F}$ be a fusion system on a finite p-group P. The first concept suggested above is easy to codify: a subgroup Q of P is *fully $\mathcal{F}$-automized* if $\mathrm{Aut}_P(Q)$ is a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{F}}(Q)$.

In the fusion system $\mathcal{F}_P(G)$, examples of fully automized subgroups have been seen before.

Example 4.9 Let G be a finite p-group, and let P be a Sylow p-subgroup of G. If Q is extremal in P with respect to G then Q is fully $\mathcal{F}_P(G)$-automized. This is true because by definition $\mathrm{N}_P(Q)$ is a Sylow p-subgroup of $\mathrm{N}_G(Q)$, and so the image of $\mathrm{N}_P(Q)$ in $\mathrm{Aut}_G(Q)$, namely $\mathrm{Aut}_P(Q)$, is a Sylow p-subgroup of $\mathrm{Aut}_G(Q) = \mathrm{Aut}_{\mathcal{F}_P(G)}(Q)$.

The next concept that we will need is that of a receptive subgroup. If $\phi : A \to B$ is an isomorphism, then ϕ induces a map $\phi^* : \mathrm{Aut}(A) \to \mathrm{Aut}(B)$, given by $\phi^* : \theta \mapsto \theta^\phi = \phi^{-1}\theta\phi$. Notice that, if $\mathcal{F}$ is a fusion system on a finite p-group P, and $\phi : A \to B$ is an isomorphism in $\mathcal{F}$, then ϕ induces an isomorphism $\phi^* : \mathrm{Aut}_{\mathcal{F}}(A) \to \mathrm{Aut}_{\mathcal{F}}(B)$.

In Exercise 6.8 we proved that if $\phi : A \to B$ is an isomorphism in $\mathcal{F}$, and $A \trianglelefteqslant N \leqslant P$, then a necessary condition for ϕ to extend to a map $\bar{\phi} : N \to \mathrm{N}_P(B)$ is that the image of

$\mathrm{Aut}_N(A)$, under ϕ^*, is contained in $\mathrm{Aut}_P(B)$. A receptive subgroup of P is one where this map *will* always extend.

Definition 4.10 Let $\mathcal{F}$ be a fusion system on a finite p-group P. A subgroup Q is *receptive* if, for all $R \leqslant P$ and isomorphisms $\phi : R \to Q$ in $\mathcal{F}$, whenever $R \leqslant N \leqslant \mathrm{N}_P(R)$ is such that $\mathrm{Aut}_N(R)\phi^* \leqslant \mathrm{Aut}_P(Q)$, there is a morphism $\bar{\phi} : N \to \mathrm{N}_P(Q)$ extending ϕ.

In other words, a receptive subgroup is one where any isomorphism to it, that has the possibility to extend to a subgroup of its normalizer, does so. Let $\phi : A \to B$ be an isomorphism in $\mathcal{F}$. We write N_ϕ for the preimage in $\mathrm{N}_P(A)$ of $\mathrm{Aut}_P(A) \cap \mathrm{Aut}_P(B)^{\phi^{-1}}$; this is the largest subgroup of $\mathrm{N}_P(A)$ to which ϕ might extend. Notice that we always have $A\,\mathrm{C}_P(A) \leqslant N_\phi$.

Our extremal subgroups also yield examples of receptive subgroups.

Example 4.11 Let G be a finite p-group, and let P be a Sylow p-subgroup of G. If Q is extremal in P with respect to G then Q is receptive in $\mathcal{F}_P(G)$. To see this, let $c_g = \phi : R \to Q$ be an isomorphism in $\mathcal{F}_P(G)$, so that $R^g = Q$. Let $R \leqslant N \leqslant \mathrm{N}_P(R)$, and suppose that $\mathrm{Aut}_N(R)\phi^* \leqslant \mathrm{Aut}_P(Q)$. This latter statement means, taking preimages in P, that $(N\,\mathrm{C}_P(R))^g \leqslant \mathrm{N}_P(Q)$. Hence $N^g \leqslant \mathrm{N}_P(Q)$, so ϕ extends to $\psi = c_g : N \to \mathrm{N}_P(Q)$; thus Q is receptive in $\mathcal{F}_P(G)$.

We may now state our definition of a saturated fusion system. Two subgroups of P are *$\mathcal{F}$-conjugate* if there is an isomorphism in $\mathcal{F}$ between them. Hence for $\mathcal{F}_P(G)$, two subgroups of P are $\mathcal{F}_P(G)$-conjugate if and only if they are G-conjugate.

Definition 4.12 Let $\mathcal{F}$ be a fusion system on a finite p-group P. We say that $\mathcal{F}$ is *saturated* if every subgroup of P is $\mathcal{F}$-conjugate to a fully $\mathcal{F}$-automized subgroup that is also receptive in $\mathcal{F}$.

Example 4.13 Fusion systems of groups are saturated because every subgroup of P is G-conjugate to an extremal subgroup by Exercise 2.9(i), and extremal subgroups are fully $\mathcal{F}_P(G)$-automized and receptive in $\mathcal{F}_P(G)$, by the above two examples.

4.2 Normalizers and Quotients

In order to do finite group theory we need homomorphisms, and in order to do local finite group theory we need normalizers and centralizers. Building analogues of these for saturated fusion systems is the objective of this section.

We begin with trying to understand morphisms of fusion systems. In order to do this, we will introduce strongly closed subgroups.

Definition 4.14 Let $\mathcal{F}$ be a fusion system on a finite p-group P. A subgroup T of P is *strongly $\mathcal{F}$-closed* if, whenever $A \leqslant T$ and $\phi : A \to P$ is a morphism in $\mathcal{F}$, then $A\phi \leqslant T$. In other words, T is strongly $\mathcal{F}$-closed if all $\mathcal{F}$-conjugates of subgroups of T are also subgroups of T.

As an easy consequence, a strongly $\mathcal{F}$-closed subgroup is only $\mathcal{F}$-conjugate to itself, and so all strongly $\mathcal{F}$-closed subgroups are normal in P. If T is a strongly $\mathcal{F}$-closed subgroup of P, then one may construct a quotient fusion system, which we denote by $\mathcal{F}/T$. If $\theta : P \to P/T$ is the natural quotient map, and $\phi : A \to B$ is a morphism with $A, B \geqslant T$, then ϕ induces a map (since T is normal) $\phi^\theta : A/T \to B/T$ given by $(Ta)\phi^\theta = T(a\phi)$. This induced homomorphism will be used in the next definition.

Definition 4.15 Let $\mathcal{F}$ be a fusion system on a finite p-group P, and let T be a strongly $\mathcal{F}$-closed subgroup of P. Write θ for the natural map $P \to P/T$. The *factor system*, $\mathcal{F}/T$, of $\mathcal{F}$, is the fusion system on P/T, where for $T \leqslant A, B \leqslant P$, we have

$$\mathrm{Hom}_{\mathcal{F}/T}(A, B) = \{\, \phi^\theta : A/T \to B/T \mid \phi \in \mathrm{Hom}_{\mathcal{F}}(A, B) \,\}.$$

It is easy to see that $\mathcal{F}/T$ is a fusion system on P/T. The proof of the next theorem is much harder however, and is omitted from this course.

Theorem 4.16 Let $\mathcal{F}$ be a fusion system on a finite p-group P, and let T be a strongly $\mathcal{F}$-closed subgroup of P. If $\mathcal{F}$ is saturated then $\mathcal{F}/T$ is saturated.

Having dealt with quotients, we move on to morphisms. A morphism should be a homomorphism $P \to Q$ that induces a map on fusion systems. Notice that if $\theta : P \to Q$ is a homomorphism, with kernel K, and $\phi : A \to B$ is a morphism of $\mathcal{F}$ on P, then θ induces a homomorphism $\phi^\theta : A\theta \to B\theta$; however, the map ϕ^θ need not be an injection. (As $A\theta$ can be identified with AK/K, ϕ^θ can be thought of as a map $AK/K \to BK/K$.)

Definition 4.17 Let $\mathcal{F}$ be a fusion system on a finite p-group P, and let $\mathcal{E}$ be a fusion system on a finite p-group Q. A homomorphism $\theta : P \to Q$ induces a *morphism* of fusion systems $\theta : \mathcal{F} \to \mathcal{E}$ if ϕ^θ is a morphism in $\mathcal{E}$, for all morphisms ϕ in $\mathcal{F}$.

We will often conflate the group homomorphism and the morphism of fusion systems, since each determines the other, and write the same symbol for both.

Not all group homomorphisms yield morphisms of fusion systems; indeed, if $\theta : P \to Q$ is a homomorphism inducing a morphism of fusion systems, then we can say a lot about $\ker\theta$.

Proposition 4.18 Let $\mathcal{F}$ be a fusion system on a finite p-group P, and let $\theta : P \to Q$ be a homomorphism. The kernel T of θ is strongly $\mathcal{F}$-closed if and only if, whenever ϕ is a map in $\mathcal{F}$, the image ϕ^θ is an injection.

Proof: Suppose that T is strongly $\mathcal{F}$-closed, and let $\phi : A \to B$ be a morphism in $\mathcal{F}$, so that in particular it is injective. Let $a \in A$, and suppose that $(a\theta)\phi^\theta = 1$. We have $(a\theta)\phi^\theta = (a\phi)\theta$, so that $a\phi \in \ker\theta = T$: since T is strongly $\mathcal{F}$-closed, and $a\phi \in T$, we must have that $a \in T$, so that $a\theta = 1$. Hence ϕ^θ is an injection.

Conversely, suppose that ϕ^θ is an injection for all ϕ in $\mathcal{F}$, and let B be a subgroup of T. Let $\phi : A \to B$ be an isomorphism in $\mathcal{F}$. Since $B \leqslant T$, the image of ϕ^θ is trivial, so its domain must be trivial as well; hence $A \leqslant T$, and so T is strongly $\mathcal{F}$-closed. $\square$

This proposition has the following immediate corollary.

Corollary 4.19 Let $\mathcal{F}$ be a fusion system on a finite p-group P, and let $\theta : P \to Q$ be a homomorphism. We have that $\ker\theta$ is strongly $\mathcal{F}$-closed if and only if θ induces a morphism of fusion systems $\mathcal{F} \to \mathcal{U}(Q)$, and in particular the kernel of any morphism of fusion systems is strongly $\mathcal{F}$-closed.

The next result ties in morphisms and factor systems.

Theorem 4.20 (Puig) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P, and let T be a strongly $\mathcal{F}$-closed subgroup. Let $\theta : P \to P/T$ denote the natural quotient map. The map θ induces a morphism of fusion systems $\mathcal{F} \to \mathcal{F}/T$, and this morphism is surjective, in the sense that every morphism in $\mathcal{F}/T$ is of the form ϕ^θ, for some morphism ϕ of $\mathcal{F}$.

The proof of this, while not particularly difficult, is too long for our course, and so will be omitted again. This theorem can be restated as the following corollary, the first isomorphism theorem for fusion systems.

Corollary 4.21 (First isomorphism theorem, Puig) Let $\mathcal{F}$ and $\mathcal{E}$ be saturated fusion systems on finite p-groups P and Q respectively, and let $\theta : \mathcal{F} \to \mathcal{E}$ be a morphism of fusion systems. Then

$$\mathcal{F}/\ker\theta \cong \operatorname{im}\theta.$$

Analogues of the second and third isomorphism theorems do hold by work of the author [5].

Theorem 4.22 (Second isomorphism theorem, Craven) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P, and let $\mathcal{E}$ be a saturated subsystem of $\mathcal{F}$, defined on the subgroup Q of P. Let T be a strongly $\mathcal{F}$-closed subgroup of P. Denoting by $\mathcal{E}T/T$ the image of $\mathcal{E}$ under the morphism $\mathcal{F} \to \mathcal{F}/T$, we have

$$\mathcal{E}T/T \cong \mathcal{E}/(Q \cap T).$$

Theorem 4.23 (Third isomorphism theorem, Craven) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P, and let T and U be strongly $\mathcal{F}$-closed subgroups of P, with $T \leqslant U$. We have

$$(\mathcal{F}/T)/(U/T) \cong \mathcal{F}/U.$$

The other objects that we introduce in this section are normalizers and centralizers.

Definition 4.24 Let $\mathcal{F}$ be a fusion system on a finite p-group P.

(i) A subgroup Q of P is *fully $\mathcal{F}$-normalized* if, whenever R is $\mathcal{F}$-conjugate to Q,

$$|\,\mathrm{N}_{\mathcal{F}}(Q)| \geqslant |\,\mathrm{N}_{\mathcal{F}}(R)|.$$

(ii) A subgroup Q of P is *fully $\mathcal{F}$-centralized* if, whenever R is $\mathcal{F}$-conjugate to Q,

$$|\,\mathrm{C}_{\mathcal{F}}(Q)| \geqslant |\,\mathrm{C}_{\mathcal{F}}(R)|.$$

In Exercise 7.2 we prove that a receptive subgroup is fully centralized, and a receptive fully automized subgroup is fully normalized. In saturated fusion systems the converse is true, as we see in Exercise 7.3.

Definition 4.25 Let $\mathcal{F}$ be a fusion system on a finite p-group P, and let Q be a subgroup of P.

(i) The *normalizer subsystem* $\mathrm{N}_{\mathcal{F}}(Q)$ is the fusion system on $\mathrm{N}_P(Q)$, where $\mathrm{Hom}_{\mathrm{N}_{\mathcal{F}}(Q)}(A,B)$ is the set of all $\phi \in \mathrm{Hom}_{\mathcal{F}}(A,B)$ such that ϕ extends to $\psi : QA \to QB$ with $Q\phi = Q$.

(ii) The *centralizer subsystem* $\mathrm{C}_{\mathcal{F}}(Q)$ is the fusion system on $\mathrm{C}_P(Q)$, where $\mathrm{Hom}_{\mathrm{C}_{\mathcal{F}}(Q)}(A,B)$ is the set of all $\phi \in \mathrm{Hom}_{\mathcal{F}}(A,B)$ such that ϕ extends to $\psi : QA \to QB$ with $\phi|_Q = 1$.

(iii) If $Q \trianglelefteq P$, then the subsystem $P\,\mathrm{C}_{\mathcal{F}}(Q)$ is the fusion system on P, where $\mathrm{Hom}_{P\,\mathrm{C}_{\mathcal{F}}(Q)}(A,B)$ is the set of all $\phi \in \mathrm{Hom}_{\mathcal{F}}(A,B)$ such that ϕ extends to $\psi : QA \to QB$ with $\phi|_Q \in \mathrm{Aut}_P(Q)$.

Theorem 4.26 (Puig) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P, and let Q be a subgroup of P. If Q is fully $\mathcal{F}$-centralized then $\mathrm{C}_{\mathcal{F}}(Q)$ is saturated, and if Q is fully $\mathcal{F}$-normalized then $\mathrm{N}_{\mathcal{F}}(Q)$ is saturated. If $Q \trianglelefteqslant P$ then $P\,\mathrm{C}_{\mathcal{F}}(Q)$ is saturated.

If $\mathcal{F} = \mathrm{N}_{\mathcal{F}}(Q)$ for some subgroup Q, then this should correspond to a normal p-subgroup. We say that Q is *normal* in $\mathcal{F}$, and write $Q \trianglelefteqslant \mathcal{F}$, if $\mathcal{F} = \mathrm{N}_{\mathcal{F}}(Q)$.

Lemma 4.27 Let $\mathcal{F}$ be a fusion system on a finite p-group P. If Q and R are normal subgroups of $\mathcal{F}$ then QR is a normal subgroup of $\mathcal{F}$.

Proof: Let $\phi : A \to B$ be any morphism in $\mathcal{F}$. Since $Q \trianglelefteqslant \mathcal{F}$, ϕ extends to $\psi : QA \to QB$ such that $Q\psi = Q$, and since $R \trianglelefteqslant \mathcal{F}$, ψ extends to $\theta : QRA \to QRB$ such that $R\theta = R$. Hence ϕ extends to $\theta : (QR)A \to (QR)B$ such that $(QR)\theta = QR$, and so $QR \trianglelefteqslant \mathcal{F}$, as needed. $\square$

The largest normal subgroup of a fusion system will be denoted by $\mathrm{O}_p(\mathcal{F})$, just as for groups.

Back in the 1930s, we saw that for soluble groups, $\mathrm{C}_G(F(G)) \leqslant F(G)$: in a fusion system, we may assume that $\mathrm{O}_{p'}(G) = 1$, so that the analogue of $F(G)$ is simply $\mathrm{O}_p(G)$. Hence we might well be interested in the statement of whether $\mathrm{C}_P(\mathrm{O}_p(\mathcal{F})) \leqslant \mathrm{O}_p(\mathcal{F})$. If this holds, we say that $\mathcal{F}$ is *constrained*. The fundamental theorem on constrained fusion systems was proved by Broto, Castellana, Grodal, Levi and Oliver, in 2005.

Theorem 4.28 Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P. If $\mathcal{F}$ is constrained then there exists a unique finite group G such that $\mathrm{O}_{p'}(G) = 1$, $\mathcal{F} = \mathcal{F}_P(G)$, and $\mathrm{C}_G(\mathrm{O}_p(G)) \leqslant \mathrm{O}_p(G)$.

4.3 Alperin's Fusion Theorem

Alperin's fusion theorem for finite groups has an analogue for fusion systems, but the two statements are not equivalent: the theorem for groups cannot imply the theorem for fusion systems, since there are fusion systems that do not come from finite groups! The theorem for fusion systems does not imply the theorem for groups because tame intersections cannot be detected by the fusion system, and the fusion system 'ignores' elements of G that centralize p-subgroups, so we can never hope to express g as a product of elements of normalizers, and simply express c_g as a product of automorphisms of subgroups of P.

Definition 4.29 Let $\mathcal{F}$ be a fusion system on a finite p-group P. A subgroup Q of P is *$\mathcal{F}$-radical* if $\mathrm{O}_p(\mathrm{Aut}_{\mathcal{F}}(Q)) = \mathrm{Inn}(Q)$.

With this definition, together with the definition of a centric subgroup on Exercise Sheet 6 (Q is $\mathcal{F}$-centric if $\mathrm{C}_P(R) \leqslant R$ whenever R is $\mathcal{F}$-conjugate to Q), we can state a version of Alperin's fusion theorem for fusion systems.

Let $\mathscr{C}$ be a family of subgroups of P. For an isomorphism $\phi \in \mathrm{Hom}_{\mathcal{F}}(A, B)$, write $A \xrightarrow{\phi} B$ with respect to $\mathscr{C}$ if there exist subgroups $Q_1, \dots, Q_n \in \mathscr{C}$ and automorphisms $\psi_i \in \mathrm{Aut}_{\mathcal{F}}(Q_i)$ such that $A \leqslant Q_1$ and, writing $A_i = A_{i-1}\phi_i$, we have that $B = A_{n+1}$ and

$$\phi = \psi_1|_{A_1} \circ \psi_2|_{A_2} \circ \cdots \circ \psi_n|_{A_n}.$$

This is very similar to the definition of a conjugation family for a finite group, but if $\mathcal{F} = \mathcal{F}_P(G)$ then the conjugation family for $\mathcal{F}$ only yields that conjugation by $g \in G$ is the same as conjugation by some product of elements from the conjugation family for $\mathcal{F}$.

A *conjugation family* for $\mathcal{F}$ is a family such that $A \xrightarrow{\phi} B$ for all A and B, and all isomorphisms $\phi \in \mathrm{Hom}_{\mathcal{F}}(A, B)$.

As with the proof of the original Alperin's fusion theorem in the previous chapter, if $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ then $A \xrightarrow{\phi\psi} C$ and $B \xrightarrow{\phi^{-1}} A$, and if $D \subseteq A$ then $D \xrightarrow{\phi} D\phi$.

Theorem 4.30 (Alperin's fusion theorem) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P. Let $\mathscr{C}$ be the set of all fully $\mathcal{F}$-normalized, $\mathcal{F}$-centric, $\mathcal{F}$-radical subgroups of P. We have that $\mathcal{F}$ is generated by $\mathrm{Aut}_{\mathcal{F}}(Q)$, for $Q \in \mathscr{C}$; in other words, $\mathscr{C}$ is a conjugation family for $\mathcal{F}$.

Proof: Let $\phi \in \mathrm{Hom}_{\mathcal{F}}(A, B)$ be an isomorphism. We proceed by induction on $m = |P : A|$, noting that if $A \in \mathscr{C}$ then $A \xrightarrow{\phi} A$ for any $\phi \in \mathrm{Aut}_{\mathcal{F}}(A)$. This implies the case $m = 1$, so that $A < P$. Let C be a fully $\mathcal{F}$-normalized subgroup of P that is $\mathcal{F}$-conjugate to A (and hence to B). By Exercise 7.6 there exist maps $\psi : A \to C$ and $\theta : B \to C$ with $N_\psi = \mathrm{N}_P(A)$

and $N_\theta = \mathrm{N}_P(B)$. Since $\mathcal{F}$ is saturated, ψ and θ extend to these overgroups, and so by induction $A \xrightarrow{\psi} C$ and $B \xrightarrow{\theta} C$. Thus, writing $\chi = \psi^{-1}\phi\theta \in \mathrm{Aut}_{\mathcal{F}}(C)$, if $C \xrightarrow{\chi} C$ then

$$A \xrightarrow{\psi} C \xrightarrow{\chi} C \xrightarrow{\theta} B,$$

so that $A \xrightarrow{\phi} B$, as needed.

As C is fully normalized, χ extends to N_χ, so if $C < N_\chi$ then $C \xrightarrow{\chi} C$ by induction; hence we may assume that $N_\chi = C$. As $\mathrm{C}_P(C) \leqslant N_\chi$, this implies that $\mathrm{C}_P(C) = \mathrm{Z}(C)$. However, as C is fully normalized it is fully centralized, so that all $\mathcal{F}$-conjugates D of C have $|\,\mathrm{C}_P(D)| \leqslant |\,\mathrm{C}_P(C)| = |\,\mathrm{Z}(C)\,| = |\,\mathrm{Z}(D)\,|$. Hence $\mathrm{C}_P(D) = \mathrm{Z}(D)$, and C is $\mathcal{F}$-centric. Finally, as $N_\phi = C$, this means that $\mathrm{Aut}_P(C) \cap \mathrm{Aut}_P(C)^{\chi^{-1}} = \mathrm{Inn}(C)$: as the two terms in the intersection are Sylow p-subgroups of $\mathrm{Aut}_{\mathcal{F}}(C)$, we see that $\mathrm{O}_p(\mathrm{Aut}_{\mathcal{F}}(C)) = \mathrm{Inn}(C)$, so that C is also radical. Hence $C \in \mathscr{C}$, and $C \xrightarrow{\chi} C$, as needed. □

As we saw on Exercise Sheet 6, there is a characterization of all conjugation families for groups: a collection $\mathscr{F}$ of subgroups of P is a conjugation family if it contains a representative of every G-conjugacy class of subgroups Q such that $\mathrm{N}_G(Q)/Q$ contains a strongly p-embedded subgroup.

For fusion systems, there is a similar classification. A subgroup Q of P is *$\mathcal{F}$-essential* if Q is $\mathcal{F}$-centric, and $\mathrm{Out}_{\mathcal{F}}(Q) = \mathrm{Aut}_{\mathcal{F}}(Q)/\mathrm{Inn}(Q)$ contains a strongly p-embedded subgroup. Notice that being $\mathcal{F}$-essential is invariant under $\mathcal{F}$-conjugacy.

Theorem 4.31 (Puig) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P. A family $\mathscr{C}$ of subgroups of P is a conjugation family if and only if it contains a representative from each $\mathcal{F}$-conjugacy class of $\mathcal{F}$-essential subgroups.

The proof of this theorem follows a similar strategy to the proof of the theorem for groups, which we did in Exercise Sheet 6, and we leave the details to the reader.

Using Alperin's fusion theorem, we can give a characterization of subgroups of P that are normal in a fusion system.

Corollary 4.32 Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P. A strongly $\mathcal{F}$-closed subgroup Q of P is normal in $\mathcal{F}$ if and only if it is contained in every fully normalized, centric, radical subgroup of $\mathcal{F}$.

Proof: Suppose that Q is contained in every fully normalized, centric, radical subgroup of P and let $\phi \in \mathrm{Hom}_{\mathcal{F}}(A,B)$ be a morphism. By Alperin's fusion theorem, ϕ can be written as the restriction of the composition of $\psi_i \in \mathrm{Aut}_{\mathcal{F}}(R_i)$, with the R_i fully normalized, centric, radical subgroups. As $Q \leqslant R_i$ and Q is strongly closed, $Q\psi_i = Q$, so that ϕ can be extended to include Q in its domain.

Conversely, suppose that Q is normal in $\mathcal{F}$, and let R be a centric, radical subgroup of P. We claim that $\mathrm{Aut}_Q(R)$ is a normal subgroup of $\mathrm{Aut}_{\mathcal{F}}(R)$: if this is true, then since R is $\mathcal{F}$-radical, $\mathrm{Aut}_Q(R) \leqslant \mathrm{Inn}(R)$, so that $Q \leqslant R\,\mathrm{C}_P(R) = R$.

We now prove the claim. Let $c_g \in \mathrm{Aut}_Q(R)$, let $\phi \in \mathrm{Aut}_{\mathcal{F}}(R)$, and let $\psi \in \mathrm{Aut}_{\mathcal{F}}(QR)$ be an extension of ϕ. Since both Q and R are ψ-invariant, $\mathrm{N}_Q(R) = Q \cap \mathrm{N}_Q\,R(R)$ is ψ-invariant. For $x \in Q$, x normalizes R if and only if $c_x \in \mathrm{Aut}(R)$, so it suffices to show that, if $c_g \in \mathrm{Aut}_Q(R)$ then $(c_g)^\psi \in \mathrm{Aut}_Q(R)$. However, $(c_g)^\psi = c_{g\psi}$, and $g\psi \in \mathrm{N}_Q(R)$ as $g \in \mathrm{N}_Q(R)$.

□

We end with a useful result of Stancu.

Lemma 4.33 (Stancu) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P, and write $Q = \mathrm{O}_p(\mathcal{F})$. We have

$$\mathcal{F} = \langle \mathrm{N}_{\mathcal{F}}(Q\,\mathrm{C}_P(Q)), P\,\mathrm{C}_{\mathcal{F}}(Q)\rangle,$$

where the fusion system generated by a collection of morphisms is the smallest fusion system containing them.

Proof: Let R be a fully normalized, centric, radical subgroup of P, and let ϕ be an $\mathcal{F}$-automorphism of R. We see that Q is contained in R by Corollary 4.32. Since $\mathcal{F} = \mathrm{N}_{\mathcal{F}}(Q)$, Q is strongly $\mathcal{F}$-closed, and so $\psi = \phi|_Q$ is an $\mathcal{F}$-automorphism of Q. Certainly $R \leqslant N_\psi$, and it is always true that $Q\,\mathrm{C}_P(Q) \leqslant N_\psi$. Thus there is a homomorphism $\theta \in \mathrm{Hom}_{\mathcal{F}}(RQ\,\mathrm{C}_P(Q), P)$ such that $\theta|_Q = \psi$; hence

$$\phi = \theta|_R \circ \left((\theta|_R)^{-1} \circ \phi\right).$$

The morphism $\theta|_R$ is a morphism in $\mathrm{N}_{\mathcal{F}}(Q\,\mathrm{C}_P(Q))$ (since θ acts as an automorphism on $Q\,\mathrm{C}_P(Q)$), and $\theta|_R^{-1} \circ \phi$ lies in $P\,\mathrm{C}_{\mathcal{F}}(Q)$. Thus $\phi \in \langle P\,\mathrm{C}_{\mathcal{F}}(Q), \mathrm{N}_{\mathcal{F}}(Q\,\mathrm{C}_P(Q))\rangle$, and by Alperin's fusion theorem we get the result. □

4.4 Thompson's Normal p-Complement Theorem

Our aim is to prove Thompson's p-nilpotence theorem for fusion systems directly, hopefully improving on the proof for groups. We need a lemma.

Lemma 4.34 Let $\mathcal{F}$ be a constrained, saturated fusion system on a finite p-group P, and let $Q = \mathrm{O}_p(\mathcal{F})$. If H is a subgroup of $\mathrm{Out}_\mathcal{F}(Q)$ such that $H \cap \mathrm{Out}_P(Q)$ is a Sylow p-subgroup of H, then there exists a saturated subsystem $\mathcal{E}$ of $\mathcal{F}$, on a subgroup of P containing Q, such that $\mathrm{Out}_\mathcal{E}(Q) = H$.

Proof: This follows easily from Theorem 4.28.

Let R be the preimage of $H \cap \mathrm{Out}_P(Q)$ in P. We define a subsystem $\mathcal{E}$ of $\mathcal{F}$ on R as follows: if A and B are subgroups of R containing Q, then let $\mathrm{Hom}_\mathcal{E}(A, B)$ be all morphisms ϕ in $\mathrm{Hom}_\mathcal{F}(A, B)$ such that $\phi|_Q$ has image in H, taken as an element of $\mathrm{Out}_\mathcal{F}(Q)$. In general, $\mathrm{Hom}_\mathcal{E}(A, B)$ consists of the restrictions to A of all maps in $\mathrm{Hom}_\mathcal{E}(QA, QB)$. This is clearly a subsystem of $\mathcal{F}$, and we claim that it is saturated.

Notice that, since any $\mathcal{F}$-centric subgroup is fully $\mathcal{F}$-centralized it is receptive in $\mathcal{F}$, and any $\mathcal{F}$-centric subgroup is $\mathcal{E}$-centric. Any subgroup of R containing Q is $\mathcal{F}$-centric (since Q is), and so is $\mathcal{E}$-centric. If $\phi \in \mathrm{Hom}_\mathcal{E}(A, B)$ is an isomorphism between subgroups of R containing Q then ϕ extends to $\bar\phi \in \mathrm{Hom}_\mathcal{F}(N_\phi, P)$, and this restricts to a map $\bar\phi \in \mathrm{Hom}_\mathcal{F}(N_\phi \cap R, R)$. Finally, since $\bar\phi|_Q = \phi|_Q$, it lies in $\mathcal{E}$, so that every subgroup of R containing Q is receptive in $\mathcal{E}$.

Suppose that A and B are two subgroups of R containing Q. If A and B are $\mathcal{F}$-conjugate via ϕ, then $\mathrm{Aut}_A(Q)$ and $\mathrm{Aut}_B(Q)$ are $\mathrm{Aut}_\mathcal{F}(Q)$-conjugate via $\phi|_Q$, and if $\mathrm{Aut}_A(Q)$ and $\mathrm{Aut}_B(Q)$ are $\mathrm{Aut}_\mathcal{F}(Q)$-conjugate via ψ, then (as A is receptive in $\mathcal{E}$ and $\mathcal{F}$) there exists an $\mathcal{F}$-isomorphism $\phi : A \to B$ such that $\phi|_Q = \psi$.

Let A be a subgroup of R containing Q. The restriction map $\theta : \mathrm{Aut}_\mathcal{F}(A) \to \mathrm{N}_{\mathrm{Aut}_\mathcal{F}(Q)}(\mathrm{Aut}_A(Q))$ has kernel all those elements of $\mathrm{Aut}_\mathcal{F}(A)$ that act trivially on Q; we claim that this is a p-group, and has order $|\,\mathrm{Z}(Q)\,/\,\mathrm{Z}(A)\,|$; to see this, let $\phi \in \mathrm{Aut}_\mathcal{F}(A)$ act trivially on Q, and notice that therefore the induced action of $\phi|_Q$ is trivial on $\mathrm{N}_P(Q)/\,\mathrm{C}_P(Q) = P/\,\mathrm{Z}(Q)$, so that ϕ acts trivially on A/Q. Hence ϕ is a p-element, so that $\ker\theta$ is a p-group.

Notice that $\mathrm{Aut}_R(Q)$ is a Sylow p-subgroup of $\mathrm{Aut}_\mathcal{E}(Q)$ by assumption:

Kernel is a p-group. Want to show that $\mathrm{Aut}_R(A)$ is a Sylow p-subgroup of $\mathrm{Aut}_\mathcal{E}(A)$,

notice that $\mathrm{N}_R(A)/Q = \mathrm{N}_{R/Q}(A/Q)$, so that $\mathrm{Aut}_{\mathrm{N}_R(A)}(Q) = \mathrm{N}_{\mathrm{Aut}_R(Q)}(\mathrm{Aut}_A(Q))$. THIS NEEDS TO SHOW THAT FULLY NORMALIZED MEANS THAT AUT OF N R A IS A SYLOW OF AUT E A.

Suppose that B is fully $\mathcal{F}$-normalized, and that $\phi \in \mathrm{Hom}_{\mathcal{E}}(A, B)$. Since $\mathcal{F}$ is saturated, B is fully $\mathcal{F}$-normalized and receptive in $\mathcal{F}$, there exists an extension

Let A and B be $\mathcal{E}$-conjugate, and

Let A be an abitrary fully $\mathcal{E}$-normalized subgroup of R, and let $\bar{A} = AQ$. If we let X be a fully $\mathcal{E}$-normalized subgroup of R that is $\mathcal{E}$-conjugate to $\bar{A}$, then there is a map $\phi : \bar{A} \to X$ such that $N_\phi = \mathrm{N}_R(\bar{A})$, which contains $\mathrm{N}_R(A)$. This yields a map $\mathrm{N}_R(A) \to \mathrm{N}_R(A\phi)$, so that by replacing A by $A\phi$ we may assume that both A and $\bar{A}$ is fully $\mathcal{E}$-normalized.

There is a natural surjective map $\theta : \mathrm{Aut}_{\mathcal{E}}(\bar{A}) \to \mathrm{Aut}_{\mathcal{E}}(A)$, obtained from restricting an automorphism of $\bar{A}$ to A. As θ is surjective, the image of a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{E}}(\bar{A})$ is a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{E}}(A)$; since $\bar{A}$ is fully $\mathcal{E}$-normalized, $\mathrm{Aut}_R(\bar{A})$ is a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{E}}(\bar{A})$, and the image of this map is clearly a subgroup of (in fact equal to since $Q \trianglelefteqslant R$) $\mathrm{Aut}_R(A)$, so that A is fully automized.

Let $\phi \in \mathrm{Hom}_{\mathcal{E}}(B, A)$ be an isomorphism, and let $\psi \in \mathrm{Hom}_{\mathcal{E}}(QB, QA)$ be an extension of ϕ: if we can show that N_ψ contains $N = N_\phi$ then, since $QA = \bar{A}$ is receptive, ψ must extend to $\bar{\psi} \in \mathrm{Hom}_{\mathcal{E}}(N_\psi, R)$, so the restriction to N is the required extension of ϕ to N.

Notice that $\mathrm{Aut}_N(B)^\psi = \mathrm{Aut}_N(B)^\phi \leqslant \mathrm{Aut}_N(A)$, so that $\mathrm{Aut}_N(BQ)^\psi$ is a subset of $\mathrm{Aut}_{\mathcal{F}}(AQ)$ that acts like a subset of $\mathrm{Aut}_R(A)$ on A. If there exists an element $\chi \in \ker\theta$ such that $(\mathrm{Aut}_R(AQ)^\psi)^\chi \leqslant \mathrm{Aut}_R(AQ)$ then $N_\phi \leqslant N_{\psi\chi}$, and since $\psi\chi|_A = \phi$, $\psi\chi$ is indeed an extension of ϕ.

Let $g \in N_\phi$, so that $(c_g)^\phi = c_h$ for some $h \in \mathrm{N}_R(A)$. Consider the automorphism $(c_g)^\psi$ of QA: it agrees with c_h on A, and acts as a p-automorphism of Q. The difference $\chi = (c_g)^\psi(c_h)^{-1}$ acts trivially on A, so lies in the kernel of θ.

If χ is a p-automorphism then there exists $\kappa \in \ker\theta$ such that $\chi^\kappa \in \mathrm{Aut}_R(QA) \cap \ker\theta = \mathrm{Aut}_{\mathrm{C}_R(A)}(QA)$; hence $[(c_g)^\psi(c_h)^{-1}]^\kappa = c_x$ lies in $\mathrm{Aut}_{\mathrm{C}_R(A)}(QA)$, and $c_g^{\psi\kappa} = c_x c_h^\kappa$

□

A saturated fusion system is *sparse* if the only saturated subsystems of $\mathcal{F}$ on P itself are $\mathcal{F}$ and $\mathcal{F}_P(P)$.

Theorem 4.35 (Thompson's normal p-complement theorem) Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P. Suppose that $\mathrm{C}_{\mathcal{F}}(\mathrm{Z}(P))$ and $\mathrm{N}_{\mathcal{F}}(J(P))$ are trivial. If p is odd then $\mathcal{F}$ is trivial.

Proof: Let $\mathcal{F}$ be a minimal counterexample firstly in terms of $|P|$, then in terms of the number of morphisms in $\mathcal{F}$.

Step 1: *$\mathcal{F}$ is sparse, $\mathrm{N}_{\mathcal{F}}(P) = \mathcal{F}_P(P)$, and if $\mathrm{Z}(P) \leqslant X \leqslant P$ and $\mathcal{E} \leqslant \mathcal{F}$ is defined on an overgroup of X, then $\mathrm{C}_{\mathcal{E}}(X)$ is trivial.* The first part is true, since any proper subsystem of

$\mathcal{F}$ on P satisfies the conditions of the result, so is $\mathcal{F}_P(P)$; the second part is true since else $P \trianglelefteq \mathcal{F}$ and so $J(P) \trianglelefteq \mathcal{F}$, a contradiction; the third part is clear.

Step 2: *If* $Q = \mathrm{O}_p(\mathcal{F})$ *then* $\mathcal{F}/Q$ *is trivial.* By Alperin's fusion theorem, since $\mathcal{F}$ is not trivial, there is some subgroup Q of P such that $\mathrm{N}_{\mathcal{F}}(Q)$ is non-trivial. Choose Q so that $|\mathrm{N}_P(Q)|$ is maximal such that $\mathrm{N}_{\mathcal{F}}(Q)$ is non-trivial. We claim that $\mathrm{N}_P(Q) = P$. To see this, write $N = \mathrm{N}_P(Q)$ and $\mathcal{N} = \mathrm{N}_{\mathcal{F}}(Q)$, and we show that $\mathrm{N}_{\mathcal{N}}(J(N))$ and $\mathrm{C}_{\mathcal{N}}(\mathrm{Z}(N))$ are trivial, and so since $\mathcal{N}$ is non-trivial, we must have by induction that $\mathcal{N} = \mathcal{F}$.

Since $\mathrm{Z}(P) \leqslant \mathrm{Z}(N)$, $\mathrm{C}_{\mathcal{N}}(\mathrm{Z}(N))$ is trivial by Step 1. If $N = P$ then $\mathrm{N}_{\mathcal{N}}(J(N)) = \mathrm{N}_{\mathcal{N}}(P)$ is trivial by Step 1, so assume that $N < P$. Since $J(N) \operatorname{char} N \trianglelefteq \mathrm{N}_P(N)$, we see that $\mathrm{N}_P(J(N)) > N$, and so by choice of Q, we must have that $\mathrm{N}_{\mathcal{F}}(J(N))$ is trivial. Hence $\mathrm{N}_{\mathcal{N}}(J(N))$ is trivial. This completes the proof, and so $\mathrm{N}_{\mathcal{F}}(Q) = \mathcal{F}$. Hence $\mathrm{O}_p(\mathcal{F}) > 1$, so let $Q = \mathrm{O}_p(\mathcal{F})$.

If $Q < W \trianglelefteq P$, then $\mathrm{N}_{\mathcal{F}}(W) < \mathcal{F}$, so $\mathrm{N}_{\mathcal{F}}(W)$ is trivial. Write $\bar{\cdot}$ for quotienting by Q. Since P cannot be normal in $\mathcal{F}$, $\bar{P} \neq 1$. Notice that if W is the preimage of $J(\bar{P})$ or $\mathrm{Z}\left(\bar{P}\right)$ in P, then $Q < W \trianglelefteq P$, and so $\mathrm{N}_{\mathcal{F}}(W)$ is trivial. Thus $\mathrm{N}_{\bar{\mathcal{F}}}(\bar{W}) = \mathrm{N}_{\mathcal{F}}(W)/Q$ is also trivial, and therefore so is $\mathrm{C}_{\bar{\mathcal{F}}}(\bar{W})$. In particular, $\mathrm{N}_{\bar{\mathcal{F}}}(J(\bar{P}))$ and $\mathrm{C}_{\bar{\mathcal{F}}}(\mathrm{Z}\left(\bar{P}\right))$ are trivial, so by induction $\bar{\mathcal{F}}$ is trivial, as needed.

Step 3: $\mathcal{F}$ *is constrained.* Lemma 4.33 states that $\mathcal{F} = \langle P\,\mathrm{C}_{\mathcal{F}}(Q), \mathrm{N}_{\mathcal{F}}(Q\,\mathrm{C}_P(Q)\rangle$. By Step 1, both of these are either $\mathcal{F}_P(P)$ or $\mathcal{F}$. If both are $\mathcal{F}_P(P)$ then $\mathcal{F} = \mathcal{F}_P(P)$, so at least one of them is $\mathcal{F}$.

Suppose that $\mathcal{F} = P\,\mathrm{C}_{\mathcal{F}}(Q)$, and let ϕ be a p'-automorphism of a fully normalized, centric, radical subgroup R of P. By Corollary 4.32, $Q \leqslant R$. Consider $\phi|_Q$: since $\mathcal{F} = P\,\mathrm{C}_{\mathcal{F}}(Q)$, $\phi|_Q = c_g$, but ϕ is a p'-automorphism, so $g = 1$, and $\phi|_Q$ is trivial. Also, if $\theta : \mathcal{F} \to \mathcal{F}/Q$ is the natural morphism of fusion systems, then ϕ^θ is trivial, since it is a p'-automorphism of a subgroup in $\mathcal{F}_{P/Q}(P/Q)$. this means that ϕ acts trivially on R/Q, so that $\phi = 1$ by Exercise 2.3. Thus by Alperin's fusion theorem, $\mathcal{F} = \mathcal{F}_P(P)$.

Thus $\mathcal{F} = \mathrm{N}_{\mathcal{F}}(Q\,\mathrm{C}_P(Q))$, and so $\mathcal{F}$ is constrained.

Step 4: $\mathrm{Out}_{\mathcal{F}}(Q) = H \rtimes \mathrm{Out}_P(Q)$, *where H is an elementary abelian q-group for some $q \neq p$. Furthermore,* $\mathrm{Out}_P(Q)$ *is maximal in* $\mathrm{Out}_{\mathcal{F}}(Q)$*, and every non-trivial normal subgroup of* $\mathrm{Out}_{\mathcal{F}}(Q)$ *contains H.* Write $G = \mathrm{Out}_{\mathcal{F}}(Q)$: by Step 2, $G = H \rtimes \mathrm{Out}_P(Q)$ for some p'-group H, and since $\mathcal{F}$ is sparse, $\mathrm{Out}_P(Q)$ is maximal in $\mathrm{Out}_{\mathcal{F}}(Q)$. Let $q \neq p$ be a prime dividing $|H|$, let R be a Sylow q-subgroup of H and $R_0 = \Omega_1(\mathrm{Z}(R))$. By the Frattini argument, $G = \mathrm{N}_G(R)H$, so $\mathrm{N}_G(R)$ contains a Sylow p-subgroup of G, namely a conjugate X of $\mathrm{Out}_P(Q)$, which is maximal in G. Since $R_0 \operatorname{char} R$, $R_0 \trianglelefteq \mathrm{N}_G(R)$, so that R_0X is a subgroup of G. By maximality of X, $R_0X = G$, so that $R_0 = H$, as claimed. Finally, if

K is normal in $\mathrm{Out}_{\mathcal{F}}(Q)$, as $H \operatorname{char} \mathrm{Out}_{\mathcal{F}}(Q)$ we have $H \cap K \operatorname{char} K \trianglelefteqslant \mathrm{Out}_{\mathcal{F}}(Q)$, so that $H \cap K = H$ or $H \cap K = 1$. If $H \cap K = 1$ then K is a normal p-subgroup, contradicting the fact that $Q = \mathrm{O}_p(\mathcal{F})$, and so $H \leqslant K$, as claimed.

Since $\mathrm{N}_{\mathcal{F}}(J(P))$ is trivial, we cannot have that $J(P) \leqslant Q$, since else $J(P) = J(Q) \operatorname{char} Q$, and so $J(Q) \trianglelefteqslant \mathcal{F}$. Hence there exists some elementary abelian p-subgroup A of maximal order in P such that $A \nleqslant Q$. We may choose A to be fully $\mathcal{F}$-normalized.

Step 5: *$P = QA$ and $P/Q \cong A/(A \cap Q)$ has order p.* Write B for the image of A in $\mathrm{Out}_P(Q)$. Since $H \trianglelefteqslant \mathrm{Out}_P(Q)$, $[H, B]$ is a subgroup of H normalized by B, so is normal in HB (as H is abelian, so normalizes $[H, B]$). Let H_1 be a minimal normal subgroup of HB contained in $[H, B]$. Let $\mathcal{E}$ be the saturated subsystem of $\mathcal{F}$ such that $\mathrm{Out}_{\mathcal{E}}(Q) = H_1 B$. Clearly $\mathcal{E}$ is non-trivial, and $\mathcal{E}$ is defined on QA. By Step 1, $\mathrm{C}_{\mathcal{E}}(\mathrm{Z}(QA))$ is trivial. Let $\phi \in \mathrm{N}_{\mathcal{E}}(J(QA))$; let ψ be an extension of ϕ to an $\mathcal{E}$-automorphism of $J(QA)Q$ (as $\mathcal{E} = \mathrm{N}_{\mathcal{E}}(Q)$). Since $A \leqslant J(QA)$, if ψ normalizes QA then $A\psi \leqslant QA$. Since $Q\psi \leqslant QA$, we see that $(QA)\psi = QA$. If ψ is not a p-automorphism, by raising to an appropriate power, we may assume that ψ is a p'-automorphism of QA in $\mathcal{E}$.

As ψ is a p'-automorphism, if $\psi|_Q$ is trivial, then since $\mathrm{C}_P(Q) \leqslant Q$, ψ is trivial; thus $\psi|_Q$ is non-trivial. We consider the image of ψ in $\mathrm{Out}_P(Q)$. Since ψ normalizes QA, $[B, \psi] \leqslant B$, and since $\psi \in H$ we have that $[B, \psi] \leqslant H$, so that $[B, \psi] = 1$. Hence $\psi \in \mathrm{C}_H(B)$; as $\psi \in [H, B]$ we get that $\psi \in [H, B] \cap \mathrm{C}_H(B) = 1$ (by Exercise 6.2). Thus $\mathrm{N}_{\mathcal{E}}(QA)$ is trivial, and so by choice of minimal counterexample, $\mathcal{E} = \mathcal{F}$. In particular, $P = QA$.

Notice that H is a simple, faithful, $\mathbb{F}_q(P/Q)$-module, and since P/Q is abelian we must have that P/Q is cyclic. Thus $A/(A \cap Q)$ has order p.

Write $Z = \mathrm{Z}(Q)$. Since $\mathrm{Z}(P) \leqslant Z$ (as $\mathrm{C}_P(Q) \leqslant Q$) we see by Step 1 that $\mathrm{C}_{\mathcal{F}}(Z)$ is a trivial fusion system on $\mathrm{C}_P(Z)$. By Exercise 6.2, $Z = \mathrm{C}_Z(H) \times [Z, H]$, and so if $[Z, H] = 1$ then H centralizes Z, impossible since $\mathrm{C}_{\mathcal{F}}(Z) = \mathcal{F}_P(P)$. Hence $[H, Z] \neq 1$. Let $V = \Omega_1([H, Z])$, an elementary abelian p-group. Also, as $Q \trianglelefteqslant \mathcal{F}$, $Z \trianglelefteqslant \mathcal{F}$, and so $[H, Z] \trianglelefteqslant \mathcal{F}$, and $\Omega_1([H, Z]) \trianglelefteqslant \mathcal{F}$.

Step 6: *$|V| \leqslant p^3$.* Let $A_0 = A \cap Q$; as AQ/Q has order p, A/A_0 has order p. As $V \leqslant \mathrm{Z}(Q)$, $A_0 V$ is elementary abelian, and so $|A_0 V| \leqslant |A|$, so that $|V/(V \cap A_0)| = |A_0 V : A_0| \leqslant p$. If $\phi \in \mathrm{Aut}_{\mathcal{F}}(Q)$, then $V\phi = V$, and so $V/(V \cap A_0)\phi$ has order at most p. If $|V| \geqslant p^3$ then $X = V \cap A_0 \cap A_0\phi \neq 1$. As A is abelian, $\mathrm{Aut}_A(Q)$ acts trivially on X, as does $\mathrm{Inn}(Q)$ since $X \leqslant \mathrm{Z}(Q)$. As $\mathrm{Aut}_A(Q)$ centralizes A_0, $\mathrm{Aut}_A(Q)^\phi$ centralizes $A_0\phi \geqslant X$, and so X is centralized by $\langle \mathrm{Aut}_A(Q), \mathrm{Aut}_A(Q)^\phi, \mathrm{Inn}(Q) \rangle = \mathrm{Aut}_{\mathcal{F}}(Q)$. Hence $X \leqslant \mathrm{C}_H(Z)$, which as $X \leqslant [H, Z]$ gives $X \leqslant \mathrm{C}_H(Z) \cap [H, Z] = 1$, a contradiction. Thus $|V| \leqslant p^2$.

Step 7: *$\mathrm{Aut}_{\mathcal{F}}(Q) \cong \mathrm{SL}_2(p)$ and contradiction.* If we can show that $C = \mathrm{C}_{\mathrm{Aut}_{\mathcal{F}}(Q)}(V) =$

$\mathrm{Inn}(Q)$ then $\mathrm{Out}_{\mathcal{F}}(Q)$ may be embedded in $\mathrm{Aut}(V) = \mathrm{GL}_2(p)$. By Step 4, $\mathrm{Out}_{\mathcal{F}}(Q)$ has at least two Sylow p-subgroups, so $\mathrm{Out}_{\mathcal{F}}(Q) \geqslant \mathrm{SL}_2(p)$ by Exercise 5.2. However, Sylow p-subgroups are not maximal in an overgroup of $\mathrm{SL}_2(p)$, contradicting the fact that $\mathrm{Out}_P(Q)$ is maximal in $\mathrm{Out}_{\mathcal{F}}(Q)$.

Since V is normalized by $\mathrm{Aut}_{\mathcal{F}}(Q)$, $C \trianglelefteqslant \mathrm{Aut}_{\mathcal{F}}(Q)$, whence $C/\mathrm{Inn}(Q)$ is a normal subgroup of $\mathrm{Out}_{\mathcal{F}}(Q)$. By Step 2, if $C > \mathrm{Inn}(Q)$ then it contains H, so that $V \leqslant \mathrm{C}_Z(H) \cap [H, Z] = 1$; hence $C = \mathrm{Inn}(Q)$, as claimed. □

The case where $p = 2$ requires us to not consider *all* fusion systems. As the fusion system of S_4 satisfies $\mathrm{N}_{\mathcal{F}}(J(P)) = \mathrm{C}_{\mathcal{F}}(\mathrm{Z}(P))) = \mathcal{F}_P(P)$ but $\mathrm{O}_{2'}(S_4) = 1$, we do need to exclude some finite groups for the prime 2.

It turns out that if G is a finite group, then G is S_4-free (i.e., there is no subgroup H of G, and normal subgroup K of H, such that $H/K \cong S_4$) if and only if $\mathcal{F}_P(G)$ is S_3-free (i.e., $\mathrm{Aut}_{\mathcal{F}}(Q)$ is S_3-free for all $Q \leqslant P$). The only time we needed p odd in the theorem is in Step 7, and if $\mathcal{F}$ is S_3-free then this step holds in this case as well.

Specializing to the case where $\mathcal{F} = \mathcal{F}_P(G)$, we get the following theorem.

Theorem 4.36 Let G be a finite group, and let p be an odd prime, or $p = 2$ and let G be S_4-free. Let P be a Sylow p-subgroup of G. If $\mathrm{N}_G(J(P))$ and $\mathrm{C}_G(\mathrm{Z}(P)))$ have normal p-complements then G has a normal p-complement.

Chapter 5

Exercise Sheets

1 Sheet 1

In all questions, G is a finite group.

1.1. A subgroup H of G is *characteristic* in G (denoted $H \operatorname{char} G$) if, whenever ϕ is an automorphism of G, $H\phi = H$. Let H and K be subgroups of G, with $H \leqslant K$. Prove that if $H \operatorname{char} K \trianglelefteq G$ then $H \trianglelefteq G$, and if $H \operatorname{char} K \operatorname{char} G$ then $H \operatorname{char} G$.

1.2. Let π be a set of primes. Denote by $\mathrm{O}_\pi(G)$ the largest normal π-subgroup of G, and by $\mathrm{O}^\pi(G)$ the smallest normal subgroup of G such that $G/\mathrm{O}^\pi(G)$ is a π-group. If $\pi = \{p\}$, we denote them by $\mathrm{O}_p(G)$ and $\mathrm{O}^p(G)$ respectively. If π is a set of primes, π' denotes all primes not in π. A π-*element* is an element of G whose order is a product of primes from π.

(i) Given the definitions above, prove that $\mathrm{O}_\pi(G)$ and $\mathrm{O}^\pi(G)$ are well-defined subgroups of G (i.e., there exist unique largest and smallest such normal subgroups respectively).

(ii) Prove that $\mathrm{O}_\pi(G)$ and $\mathrm{O}^\pi(G)$ are characteristic subgroups of G.

(iii) Prove that $\mathrm{O}^\pi(G)$ is generated by all π'-elements of G.

1.3. Suppose that G has cyclic Sylow 2-subgroups.

(i) Prove that G possesses a subgroup of index 2.

(ii) Prove that $\mathrm{O}^2(G) = \mathrm{O}_{2'}(G)$, i.e., G possesses a normal subgroup K such that $|K|$ is odd and $|G : K|$ is a power of 2.

1.4. Let H be a normal subgroup of G. Let P denote a Sylow p-subgroup of H. Prove that every element $g \in G$ may be expressed as $g = hk$, where $h \in H$ and $k \in \mathrm{N}_G(P)$. This is called the *Frattini argument*, and is (of course) due to Frattini.

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

(i) Prove that $\Phi(G)$ is characteristic in G.

(ii) Prove (by induction or otherwise) that a maximal subgroup of a finite p-group G is of index p and normal in G. (Hint: consider a central subgroup of order p.)

(iii) Suppose that G is a finite p-group. Prove that $G/\Phi(G)$ is elementary abelian.

(iv) Suppose that H is a normal subgroup of the finite p-group G, and G/H is elementary abelian. Prove that $\Phi(G) \leqslant H$.

1.6. Let P be a Sylow p-subgroup of G. Prove that $\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P)$.

1.7. Let N be a normal subgroup of G and let H be a subgroup of G with $N \leqslant H \leqslant G$. Prove that $\mathrm{N}_G(H)/N = \mathrm{N}_{G/N}(H/N)$.

1.8. This result is normally called the modular law, or Dedekind's lemma. Let A, B and C be subgroups of G, and suppose that $A \leqslant C$. Prove that (as sets)

$$A(B \cap C) = AB \cap C.$$

1.9. (Thompson's transfer lemma, MFoCS) Suppose that $|G|$ is even, and let P be a Sylow 2-subgroup of G. Assume that G contains no (normal) subgroup of index 2, i.e., that $G = \mathrm{O}^2(G)$. Prove that, if M is a maximal subgroup of P, then every involution of G is conjugate to one in M. (An *involution* in a group G is an element of order 2.)

2 Sheet 2

2.1. Let G be the group S_4 and let $P = \langle (1,2), (1,3,2,4) \rangle$ denote a Sylow 2-subgroup of G. Let θ denote the standard quotient map $P \to P/P'$, and let τ denote the transfer of θ with respect to G. Calculate the image of $(1,2,3)$ and $(1,2)$. What can you deduce about $\mathrm{O}^2(G)$?

2.2. Prove that the direct product of two nilpotent groups is nilpotent. Give an example to show that the semidirect product of nilpotent groups need not be nilpotent.

2.3. Let G be a finite p-group, let α be a p'-automorphism of G, and let H be an α-invariant normal subgroup of G. If α acts trivially on H and G/H prove that $\alpha = 1$.

2.4. Let G be a group, and let x, y and z be elements of G. Prove the following equalities.

(i) $[x,y] = [y,x]^{-1}$.

(ii) $[xy,z] = [x,z]^y[y,z] = [x,z][x,z,y][y,z]$.

(iii) $[x,yz] = [x,z][x,y]^z = [x,z][x,y][x,y,z]$.

(iv) (Hall–Witt identity) $[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$.

(Hint: for the final calculation, let $u = xzx^{-1}yx$, $v = yxy^{-1}zy$ and $w = zyz^{-1}xz$.)

Deduce the *three subgroups lemma*: Let X, Y and Z be three subgroups of a group G, and let N be a normal subgroup of G. If $[X,Y,Z]$ and $[Y,Z,X]$ are both contained within N, then so is $[Z,X,Y]$.

2.5. Let G be a group, and let H and K be subgroups of G. Let

$$H = H_0 \geqslant H_1 \geqslant \cdots \geqslant H_n \geqslant \cdots$$

be a chain of normal subgroups of H with $[H_r,K] \leqslant H_{r+1}$ for each r. Prove that $[H_r, L_n(K)] \leqslant H_{r+n}$ for all $r \geqslant 1$ and $n \geqslant 1$.

Deduce the following inequalities, for all r, s and all groups G:

(i) $[L_r(G), L_s(G)] \leqslant L_{r+s}(G)$;

(ii) $[L_r(G), \mathrm{Z}_s(G)] \leqslant \mathrm{Z}_{s-r}(G)$ for $s \geqslant r$;

(iii) $[L_r(G), \mathrm{Z}_r(G)] = 1$; and

(iv) $L_{2^n}(G) \geqslant G^{(n)}$ for all n.

2.6. Let G be a finite group, and let M be a minimal normal subgroup of G (i.e., a non-trivial normal subgroup of G minimal with respect to inclusion). Prove that M is a direct product of isomorphic simple groups, and hence if G is soluble then M is elementary abelian.

2.7. Let G be a finite group. Prove that G is nilpotent if and only if every maximal subgroup of G is normal in G.

2.8. Let G be a group and let H be a subgroup of G.

(i) Prove that the product of all normal subgroups of G contained in H is equal to the intersection of all conjugates H^g of H for $g \in G$. This subgroup is often denoted H_G and is called the *core* of H in G.

(ii) Prove that the intersection of all normal subgroups of G containing H is equal to the subgroup generated by all conjugates H^g of H for $g \in G$. This subgroup is often denoted H^G and is called the *normal closure* of H in G.

2.9. (MFoCS) Let G and let P be a Sylow p-subgroup of G. A subgroup is *extremal* if $\mathrm{N}_P(A)$ is a Sylow p-subgroup of $\mathrm{N}_G(A)$.

(i) Prove that every subgroup of P is conjugate in G to an extremal subgroup.

(ii) Let B be an extremal subgroup of P that is G-conjugate to A. Prove that there exists $g \in G$ such that $\mathrm{N}_P(A)^g \leqslant \mathrm{N}_P(B)$ and $A^g = B$.

2.10. (MFoCS) Let G be a finite group, and let P be a Sylow p-subgroup of G. Let A and B be any subgroups of P, and let $g \in G$ be such that $A^g = B$. Write $A \xrightarrow{g} B$ if there exist, for $1 \leqslant i \leqslant n$, extremal subgroups R_i of P and elements $x_i \in \mathrm{N}_G(R_i)$ such that $g = x_1 x_2 \dots x_n$, and $A^{x_1 \dots x_i} \leqslant R_i, R_{i+1}$ (and $A \leqslant R_1$).

(i) Prove that, if $A \xrightarrow{g} B$ and $D \subseteq A$, then $D \xrightarrow{g} D^g$, and that, if $A \xrightarrow{g} B$ and $B \xrightarrow{h} C$, then $A \xrightarrow{gh} C$ and $B \xrightarrow{g^{-1}} A$.

(ii) Prove that if B is extremal then $A \xrightarrow{g} B$. (Proceed by induction on $|P : A|$)

(iii) Prove that $A \xrightarrow{g} B$ in all cases.

3 Sheet 3

In all questions, G is a finite group, and P is a Sylow p-subgroup of G.

3.1. Let A be a normal subgroup of G such that A is cyclic and G/A is non-abelian simple. Prove that $A = \mathrm{Z}(G)$.

3.2. Let H and K be normal subgroups of G such that $[H, K] = 1$ and $G = HK$. Prove that there exists a central subgroup Z of $X = H \times K$, such that $X/Z \cong G$, with Z having trivial intersection with both direct factors, and with the images of HZ/Z and KZ/Z in X/Z being H and K (as subgroups of G) respectively.

Such a group G is said to be a *central product* of H and K.

3.3. Let H be a subgroup of G. If ψ is a character of G, the *restriction* of G to H is the character ψ_H of H with $\psi_H(h) = \psi(h)$ for $h \in H$. Let ψ be a character of G and χ be a character of H.

(i) Prove that
$$\chi^G(x) = \frac{1}{|H|} \sum_{g \in G} \chi(g^{-1}xg),$$
where $\chi(x) = 0$ for $x \in G \setminus H$, and $\chi^G(x)$ is the induced character of χ to G.

(ii) Prove that $\langle \psi, \chi^G \rangle = \langle \psi_H, \chi \rangle$. (Hint: for fixed $g \in G$, set $y = g^{-1}xg$ to depend on $x \in G$, and notice that if x ranges over all elements of G, so does y.)

The equality $\langle \chi, \psi^G \rangle = \langle \chi_H, \psi \rangle$ is known as *Frobenius reciprocity*, and is of fundamental importance in character theory.

3.4. Prove that the intersection of all Sylow p-subgroups of G is $\mathrm{O}_p(G)$. (In fact, it can be shown (using complicated stuff) that $\mathrm{O}_p(G)$ is the intersection of at most three Sylow p-subgroups of G, and it is 'usually' the intersection of two.)

3.5. Suppose that G has a normal p-complement. Prove that $\mathrm{Aut}_G(Q) = \mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is a p-group for all subgroups Q of P.

3.6. (MFoCS) Prove that the following are equivalent:

(i) $\mathrm{Aut}_G(Q) = \mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is a p-group for all subgroups Q of P.

(ii) P controls fusion in P with respect to G.

Deduce that, if H is a normal subgroup of G, and P controls fusion in P with respect to G, then $H \cap P$ controls fusion in $H \cap P$ with respect to H.

3.7. (MFoCS) Suppose that P controls fusion in P with respect to G. Let $\theta : P \to P/P'$ be the natural quotient map, and let τ be the transfer of θ.

(i) Prove that $\ker \tau < G$.

(ii) Deduce that G has a normal p-complement.

The statement that G has a normal p-complement if and only if P controls fusion in P with respect to G is known as *Frobenius's normal p-complement theorem.*

4 Sheet 4

4.1. Let G be a finite group and let M be a G-module. A 1-*cocycle* is a map $\gamma : G \to M$ that satisfies the identity
$$\gamma(xy) = \gamma(x) \cdot y + \gamma(y).$$

Let X be a split extension of M by G, and turn M into a G-module via conjugation. Identify M and G with their images in X.

(i) If γ is a 1-cocycle, prove that the set $\{x\gamma(x) : x \in G\}$ is a complement to M in X.

(ii) If H is a complement to M in X, prove that there exists a 1-cocycle γ such that $H = \{x\gamma(x) : x \in G\}$.

(iii) Prove that if H and K are two complements to M in G, and $H = K^g$ for some $g \in X$, then there exists $v \in M$ such that $H = K^v$.

The set of all 1-cocycles is denoted $Z^1(G, M)$.

4.2. Let G and M be as in Exercise 4.1. A 1-*coboundary* is a function $\gamma : G \to M$ such that there exists $v \in M$ with $\gamma(x) = v - v\cdot x$. Denote by $B^1(G, M)$ the set of 1-coboundaries. Define an addition on $Z^1(G, M)$ by $(\gamma + \delta)(x) = \gamma(x) + \delta(x)$.

(i) Prove that $Z^1(G, M)$ forms an abelian group.

(ii) Prove that $B^1(G, M)$ forms a subgroup of $Z^1(G, M)$.

The quotient $Z^1(G, M)/B^1(G, M)$ is denoted $H^1(G, M)$ and called the 1-*cohomology* of G and M.

4.3. Let G and M be as in Exercise 4.1, and suppose that $|G|$ and $|M|$ are coprime. Prove that $H^1(G, M) = 0$.

4.4. Let G, M and X be as in Exercise 4.1. Let H and K be two complements to M in X. Prove that H and K are X-conjugate if and only if the corresponding 1-cocycles lie in the same 1-cohomology class. Deduce that all complements to M in X are conjugate if and only if $H^1(G, M) = 0$.

4.5. Let G be a finite group, and let A be a group of automorphisms of G, with $|A|$ and $|G|$ coprime. Let $p \mid |G|$ be a prime.

(i) Prove that there exists an A-invariant Sylow p-subgroup of G.

(ii) Prove that every A-invariant p-subgroup of G is contained in an A-invariant Sylow p-subgroup of G.

(iii) (MFoCS) Prove that $\mathrm{C}_G(A)$ acts transitively by conjugation on the set of A-invariant Sylow p-subgroups of G.

5 Sheet 5

5.1. Let M be the group C_4 (written additively), and $G = C_2$; turn M into a non-trivial G-module in the unique way, by $m \cdot g = -m$ for $1 \neq g \in G$ and $m \in M$. Prove that $H^1(G, M)$ and $H^2(G, M)$ are non-zero.

5.2. Let $p \geqslant 5$. Prove that the set of upper unitriangular matrices in $\mathrm{GL}_2(p)$ forms a Sylow p-subgroup of $\mathrm{GL}_2(p)$. Prove that, if G is a subgroup of $\mathrm{GL}_2(p)$ with at least two Sylow p-subgroups, then G contains $\mathrm{SL}_2(p)$. (Optional. For $p = 2, 3$ the result still holds: prove it.)

5.3. Let p be the smallest prime dividing $|G|$. If H is a subgroup of index p, prove that $H \trianglelefteqslant G$.

5.4. Let H and K be subgroups of G. Let $\mathrm{Aut}_K(H)$ denote the set of all automorphisms of H induced by conjugation by elements of K. Let $\mathrm{Inn}(H) = \mathrm{Aut}_H(H)$ (the *inner automorphisms* of H).

(i) Prove that $\mathrm{Inn}(H) \trianglelefteqslant \mathrm{Aut}(H)$.

(ii) Prove that $\mathrm{Aut}_K(H)$ is naturally isomorphic to $\mathrm{N}_K(H)/\mathrm{C}_K(H)$.

(iii) Prove that $\mathrm{Inn}(H) \cong H/\mathrm{Z}(H)$.

(iv) Define $\mathrm{Out}(H)$ to be $\mathrm{Aut}(H)/\mathrm{Inn}(H)$, and $\mathrm{Out}_K(H)$ to be the image of $\mathrm{Aut}_K(H)$ in $\mathrm{Out}(H)$. Prove that $\mathrm{Out}_K(H)$ is naturally isomorphic to $\mathrm{N}_K(H)/(H \cap K)\,\mathrm{C}_K(H)$.

(v) Prove that if G is a simple group then G naturally embeds in $\mathrm{Aut}(G)$.

(vi) (MFoCS) Prove that $\mathrm{Aut}(A_4) \cong S_4$ and $\mathrm{Aut}(A_5) \cong S_5$.

5.5. Let $g \in G$. An intersection $A = P \cap P^{g^{-1}}$ is *domestic* if it is tame, and whenever $x \in \mathrm{C}_G(A)$ we have $P \cap P^{(xg)^{-1}} = A$. Let A be a domestic intersection.

(i) Prove that $\mathrm{C}_P(A) = \mathrm{Z}(A)$, and indeed $\mathrm{C}_G(A) = \mathrm{Z}(A) \times \mathrm{O}_{p'}(\mathrm{C}_G(A))$. (Hint: for the second part, use a normal p-complement theorem.)

(ii) Prove that $\mathrm{O}_p(\mathrm{Aut}_G(A)) = \mathrm{Inn}(A)$.

5.6. A *strongly p-embedded subgroup* of G is a subgroup M, containing P (or a conjugate) such that $M \cap M^g$ is a p'-group for all $g \in G \setminus M$. Let $A_p(G)$ be the graph with vertices all non-trivial p-subgroups of G, and a line connecting two vertices if and only if the corresponding subgroups Q and R satisfy $Q \leqslant R$ (or $R \leqslant Q$). Prove that G has a strongly p-embedded subgroup if and only if $A_p(G)$ is disconnected.

5.7. (MFoCS) Let A be an extremal subgroup of P with respect to G, with $\mathrm{C}_G(A) = \mathrm{Z}(A) \times \mathrm{O}_{p'}(\mathrm{C}_G(A))$. Suppose that $\mathrm{Out}_G(A)$ has a strongly p-embedded subgroup. Prove that A is a domestic intersection.

6 Sheet 6

In all questions, let G be a finite group and let P be a Sylow p-subgroup of G.

6.1. The *exponent* of a group G is the smallest integer n such that, for all $g \in G$, $g^n = 1$. (It need not be finite.)

Let G be a not-necessarily-finite group.

(i) Let $X_i = L_i(G)/L_{i+1}(G)$. Prove that the map (not homomorphism) $\phi : G \times G \to G$ given by $(x, y) \mapsto [x, y]$ induces a bilinear map $\bar{\phi}_i : X_i \times X_1 \to X_{i+1}$. (Bilinear here means that $(ab, x)\bar{\phi}_i = (a, x)\bar{\phi}_i \cdot (b, x)\bar{\phi}_i$ and $(a, xy)\bar{\phi}_i = (a, x)\bar{\phi}_i \cdot (a, y)\bar{\phi}_i$.)

(ii) Prove that if G/G' is finitely generated then X_i is finitely generated for all $i \geqslant 1$.

(iii) Suppose that G/G' has exponent n. Prove that $L_i(G)/L_{i+1}(G)$ has exponent at most n for all i.

(iv) Prove that every finitely generated nilpotent group is either finite or has a surjective homomorphism to $\mathbb{Z}$.

6.2. Let G be a finite group with an abelian Sylow p-subgroup P, and write $N = \mathrm{N}_G(P)$.

(i) Prove that $P \cap G' = [P, N]$.

(ii) Prove that $P = \mathrm{C}_P(N) \times [P, N]$.

This clearly implies that, if H is a p'-group of automorphisms of P, then $P = \mathrm{C}_P(H) \times [P, H]$.

6.3. Let Q be an extremal subgroup of P.

(i) Prove that every element of $\mathrm{Aut}_G(Q)$ may be expressible as a product of p-automorphisms of Q and the restriction of an automorphism of a subgroup R of P with $Q < R$.

(ii) Deduce that, for any conjugation family $\mathscr{F}$, the elements $x_i \in S_i$ (for $S_i \in \mathscr{F}$) may be chosen to be p-elements, unless $S_i = P$.

6.4. In this and the next question we relax slightly the definition of a conjugation family, and allow multiple occurrences of elements of $\mathrm{N}_G(P)$ in the decomposition; alternatively, we delete the element $y \in \mathrm{N}_G(P)$ at the end of the decomposition, and let $P \in \mathscr{F}$.

Let $\mathscr{F}$ be a conjugation family. Prove that, if $\mathscr{F}'$ is a subset of $\mathscr{F}$ containing a representative from every G-conjugacy class of subgroups of P that have a representative in $\mathscr{F}$, then $\mathscr{F}'$ is also a conjugation family.

6.5. We make the same relaxation of the definition of a conjugation family as in the previous question.

Let $\mathscr{F}$ be a conjugation family. Let Q be an extremal subgroup of P. Let X be the subgroup of $\mathrm{N}_G(Q)$ generated by those $g \in \mathrm{N}_G(Q)$ that normalize some $Q < R \leqslant \mathrm{N}_P(Q)$.

(i) Prove that $\mathrm{N}_G(Q)/Q$ contains a strongly p-embedded subgroup, namely X/Q, if and only if $X < \mathrm{N}_G(Q)$.

(ii) If $X < \mathrm{N}_G(Q)$, prove that Q is a tame intersection.

(iii) Suppose that $X = \mathrm{N}_G(Q)$. If $\mathscr{F}$ contains Q, prove that $\mathscr{F} \setminus \{Q\}$ is also a conjugation family.

(iv) Deduce that a family $\mathscr{F}$ of subgroups of P is a conjugation family if and only if it contains a representative from every G-conjugacy class of subgroups $R \leqslant P$ such that $\mathrm{N}_G(R)/R$ has a strongly p-embedded subgroup, together with P.

6.6. Suppose that P is a dihedral 2-group.

(i) Use Alperin's fusion theorem to determine the three possibilities for fusion in P.

(ii) Use the focal subgroup theorem to calculate the maximal abelian 2-quotient $G/A^p(G)$ of G in each ease.

(iii) Deduce that, if $\mathrm{O}^2(G) = G$, then all involutions in G are conjugate.

6.7. Let ϕ be an automorphism of G. Let H be a subgroup of G and let $H \leqslant K \leqslant \mathrm{N}_G(H)$.

(i) Prove that ϕ induces a natural isomorphism $\phi^* : \mathrm{Aut}(H) \to \mathrm{Aut}(H\phi)$.

(ii) Let $g \in \mathrm{N}_G(H)$. Prove that, $g\phi \in \mathrm{N}_G(H\phi)$, and as an element of $\mathrm{Aut}(H)$, $c_g\phi^* = c_{g\phi}$.

(iii) Deduce that

$$\mathrm{Aut}_K(H)\phi^* = \mathrm{Aut}_{K\phi}(H\phi).$$

6.8. Let A and B be subgroups of P, and suppose that there is an isomorphism $\phi : A \to B$. Let N be a subgroup of $\mathrm{N}_P(A)$ containing A. If there exists an injective homomorphism $\psi : N \to \mathrm{N}_P(B)$, such that $\psi|_A = \phi$, prove that $\mathrm{Aut}_N(A)\phi^* \leqslant \mathrm{Aut}_P(B)$. (Use the previous question!)

7 Sheet 7

In all questions, P is a finite p-group, G is a finite group with Sylow p-subgroup P, and $\mathcal{F}$ is a fusion system on P.

7.1. Prove Lemma 4.3.

7.2. A subgroup Q of P is *fully $\mathcal{F}$-normalized* if, whenever R is $\mathcal{F}$-conjugate to Q, $|\,\mathrm{N}_P(Q)| \geqslant |\,\mathrm{N}_P(R)|$. Similarly, Q is *fully $\mathcal{F}$-centralized* if, whenever R is $\mathcal{F}$-conjugate to Q, $|\,\mathrm{C}_P(Q)| \geqslant |\,\mathrm{C}_P(R)|$.

Let Q be a subgroup of P. Prove that if Q is receptive in $\mathcal{F}$ then Q is fully $\mathcal{F}$-centralized. Prove that if Q is in addition fully $\mathcal{F}$-automized, then Q is fully $\mathcal{F}$-normalized.

7.3. Suppose that $\mathcal{F}$ is saturated. Prove that every fully $\mathcal{F}$-centralized subgroup is receptive, and that every fully $\mathcal{F}$-normalized subgroup is both fully $\mathcal{F}$-automized and receptive.

7.4. A subgroup Q of $\mathcal{F}$ is *$\mathcal{F}$-centric* if, whenever R is $\mathcal{F}$-conjugate to Q, we have that $\mathrm{C}_P(R) \leqslant R$ (in particular $R = Q$). Prove that, if $\mathcal{F} = \mathcal{F}_P(G)$, then Q is $\mathcal{F}$-centric if and only if

$$\mathrm{C}_G(Q) = \mathrm{Z}\,(Q) \times \mathrm{O}_{p'}(\mathrm{C}_G(Q)).$$

7.5. Prove that if Q is fully $\mathcal{F}$-centralized then $Q\,\mathrm{C}_P(Q)$ is $\mathcal{F}$-centric, and that if Q is $\mathcal{F}$-centric and $R \geqslant Q$ then R is $\mathcal{F}$-centric.

7.6. Suppose that $\mathcal{F}$ is saturated, let Q be a fully $\mathcal{F}$-normalized subgroup of P, and let R be a subgroup of P that is $\mathcal{F}$-conjugate to Q. Prove that there is a morphism $\phi : R \to Q$ that extends to an $\mathcal{F}$-morphism $\bar{\phi} : \mathrm{N}_P(R) \to \mathrm{N}_P(Q)$.

7.7. A subgroup Q is *weakly $\mathcal{F}$-closed* if $\{Q\}$ is the $\mathcal{F}$-conjugacy class containing Q. Prove that the product of two weakly closed subgroups is weakly closed.

Chapter 6

Solutions to Exercises

1 Sheet 1

1.1. Let $g \in G$. Since $K \trianglelefteq G$, conjugation by g induces an automorphism of K, namely $\phi : x \mapsto x^g$. As $H \operatorname{char} K$, $H\phi = H$, and so $H^g = H$. If ϕ is any automorphism of G and $K \operatorname{char} G$, then $K\phi = K$, and so as above ϕ induces an automorphism of K. As above, since $H \operatorname{char} K$ we see that $H\phi = H$, so that $H \operatorname{char} G$.

1.2. (a) If H and K are normal π-subgroup of G then HK is, using the order formula $|H| \cdot |K| = |HK| \cdot |H \cap K|$. Hence the product of all normal π-subgroups is a normal π-subgroup, so $\mathrm{O}_\pi(G)$ is well defined. Similarly, if H and K are normal subgroups such that G/H and G/K are π-groups, then the intersection $H \cap K$ is a normal subgroup, and the order formula says that

$$|G|/|H \cap K| = \frac{|G| \cdot |HK|}{|H| \cdot |K|} = \frac{|G|}{|H|} \cdot \frac{|HK|}{|K|}.$$

The first term is a π-element, and since $HK/K \leqslant G/K$, it is also a π-group. Hence the intersection of all normal subgroups whose quotient is a π-group is a normal subgroup whose quotient is a π-group. Thus $\mathrm{O}^\pi(G)$ is well defined.

(b) Let ϕ be an automorphism of G. Notice that $\mathrm{O}_\pi(G)\phi$ is a normal π-subgroup of G, so that $\mathrm{O}_\pi(G)\phi \leqslant \mathrm{O}_\pi(G)$ (so they are equal), proving that $\mathrm{O}_\pi(G) \operatorname{char} G$. Similarly, $\mathrm{O}^\pi(G)\phi$ is a normal subgroup such that $G/(\mathrm{O}^\pi(G)\phi)$ is a π-group, so that $\mathrm{O}^\pi(G) \leqslant \mathrm{O}^\pi(G)\phi$, proving again that $\mathrm{O}^\pi(G) \operatorname{char} G$.

(c) Notice that every π'-element of G must lie in $\mathrm{O}^\pi(G)$, since the image of it in $G/\mathrm{O}^\pi(G)$ is a π'-element in a π-group. Let H be the subgroup generated by all π'-elements, so that $H \leqslant \mathrm{O}^\pi(G)$. If $g \in G$ then conjugation by g permutes the π'-elements of G, so that conjugation by g fixes the subgroup generated by all π'-elements. Thus $H \trianglelefteqslant G$.

If G/H is not a π-group, then there exists an element $x \in G$, such that the order of Hx in G/H is a π'-element. Write $o(x) = ab$, where a is a π-element and b is a π'-element. The element Hx^a in G/H must be a π'-element, since it is a power of Hx, and is non-trivial since a is a π-number; thus $x^a \notin H$. However, x^a is a π'-element, so lies in H, a contradiction. Thus G/H is a π-group, so $\mathrm{O}^{\pi}(G) \leqslant H$, completing the proof.

1.3. (a) Let x be a generator for $P \in \mathrm{Syl}_2(G)$, and consider the regular representation ρ of G. Since x has order 2^n for some n, each cycle of $x\rho$ has length 2^m. As $|G| = n = 2^m a$ for odd a, there are a cycles of length 2^n. Each of these cycles is odd, and so $x\rho$ is odd. Hence $\operatorname{im}\rho \cap A_n$ has index 2 in $\operatorname{im}\rho$, so that G possesses a subgroup H of index 2.

(b) The subgroup H has cyclic Sylow 2-subgroups, and so $\mathrm{O}_2(H) = \mathrm{O}^2(H) = K$ is an odd-order subgroup. By the previous exercise, all elements of odd order in G lie in H, and all elements of odd order in H lie in K, so that all odd-order elements of G lie in K. Hence $\mathrm{O}^2(G) \leqslant K$. However, $|K| = a$, whereas $|\,\mathrm{O}^2(G)| = 2^i a$ for some $i \geqslant 0$, so that $\mathrm{O}^2(G) = K$; this proves that G has a normal 2-complement, as claimed.

1.4. Let $g \in G$. Since $P^g \leqslant H$, it is a Sylow p-subgroup of H, and so there exists $h \in H$ such that $P^g = P^h$. Therefore $P^{h^{-1}g} = P$, and hence ?? lies in $\mathrm{N}_G(P)$. Thus $g = h(h^{-1}g)$

1.5. (a) Let ϕ be an automorphism of G. If M is a maximal subgroup of G then so is $M\phi$, so that ϕ permutes the maximal subgroups of G; thus ϕ fixes their intersection, proving that $\Phi(G) = \Phi(G)\phi$. Hence $\Phi(G) \operatorname{char} G$.

(b) Proceed by induction on n, where $|G| = p^n$. We know that $\mathrm{Z}(G) \neq 1$, so let Z be a central subgroup of order p, which is normal in G. Let M be a maximal subgroup of G. If $Z \leqslant M$ then M/Z is a maximal subgroup of G/Z, hence normal in G/Z and of index p, proving the result in this case. Otherwise $M < MZ \leqslant G$, so since M is maximal, $G = MZ$, so again M has index p as $M \cap Z = 1$. Also, since $Z \leqslant \mathrm{N}_G(M)$, $G = \mathrm{N}_G(M)$, so in this case $M \trianglelefteqslant G$.

(c) Let M be a maximal subgroup of G. Since $G/M \cong C_p$ it is abelian, so that $G' \leqslant M$. Hence G' is contained in every maximal subgroup, so in $\Phi(G)$. Hence $G/\Phi(G)$ is abelian. In addition, if $x \in G$ then $(Mx)^p = Mx^p = M$ (as G/M has order p). Thus for all $x \in G$, $x^p \in \Phi(G)$, so that all elements of $G/\Phi(G)$ have order 1 or p.

By the classification of finite abelian groups, this means that $G/\Phi(G)$ is elementary abelian.

(d) As G/H is elementary abelian, there is a collection of maximal subgroups of G/H whose intersection is trivial, and taking preimages in G there is a collection of maximal subgroups of G (containing H) whose intersection is H. In particular, H contains the intersection of *all* maximal subgroups of G, so that $\Phi(G) \leqslant H$.

1.6. Notice that $P \trianglelefteqslant \mathrm{N}_G(P)$, and so by Sylow's theorem $\mathrm{N}_G(P)$ has a unique Sylow p-subgroup, so that $P \operatorname{char} \mathrm{N}_G(P)$. Hence

$$P \operatorname{char} \mathrm{N}_G(P) \trianglelefteqslant \mathrm{N}_G(\mathrm{N}_G(P)),$$

so that $P \trianglelefteqslant \mathrm{N}_G(\mathrm{N}_G(P))$ by Exercise 1.1. By the definition of $\mathrm{N}_G(P)$, we have the result.

1.7. Suppose that $x \in \mathrm{N}_G(H)$; then Nx normalizes Hx, so that $Nx \in \mathrm{N}_{G/N}(H/N)$. Hence $\mathrm{N}_G(H)/N \subseteq \mathrm{N}_{G/N}(H/N)$. Conversely, suppose that $x \in G$ and Nx normalizes Hx; then, as $N \leqslant H$,

$$Hx = Hx^{Nx} = (Nx)^{-1}(Hx)(Nx) = x^{-1}NHxNx = x^{-1}(Hx)x,$$

since $N \trianglelefteqslant G$ and therefore $xN = Nx$, and $NHN = H$. Hence $Hx = x^{-1}(Hx)x$, so that $H = x^{-1}Hx$; i.e., x normalizes H, so that $x \in \mathrm{N}_G(H)$.

1.8. Let x be an element of $A(B \cap C)$. We see that $x = ab$ where $a \in A \leqslant C$ and $b \in B \cap C$. Hence $a, b \in C$ so that $x \in C$ and $ab \in AB$, proving that $A(B \cap C) \subseteq AB \cap C$. Convesely, if $x = ab$ with $a \in A \leqslant C$, $b \in B$ and $x \in C$. Since a and x lie in C, $b \in C$, so that $b \in B \cap C$. This proves that $ab \in A(B \cap C)$, proving the opposite conclusion.

1.9. Let $|G| = 2^n m$, where m is odd. Then $|G : M| = 2m$. Consider the action of G on the cosets of M. This is a homomorphism from G to S_{2m}. The set of all elements of the image that are even permutations is a subgroup of index at most 2 in this image, and since G contains no subgroup of index 2, the image of G consists solely of even permutations.

Suppose that g is any involution in G. The image of g in A_{2m} is a product of disjoint transpositions, and since g is an even permutation and there are $2m$ points with m odd, this permutation must fix a point, Mx say. Hence $Mxg = Mx$, and so $x^{-1}gx \in M$, as required.

2 Sheet 2

2.1. This is a simple calculation: choose the transversal $\{1, (1,2,3), (1,3,2)\}$, and write t_i for the ith element of the set. Firstly let $g = (1,2,3)$. We have

$$t_i \cdot (1,2,3) = 1 \cdot t_{i+1},$$

with the index of t_i taken modulo 3. The transfer is therefore $1 \cdot 1\dot{1} = 1$. Now let $g = (1,2)$, and we have

$$1 \cdot (1,2) = (1,2) \cdot 1, \qquad (1,2,3)(1,2) = (1,2)(1,3,2), \qquad (1,3,2)(1,2) = (1,2)(1,2,3).$$

Hence the transfer is therefore $(1,2) \cdot (1,2) \cdot (1,2) = (1,2)$.

Since the image of the transfer is non-trivial, we have that $\ker \tau < G$, so that $\mathrm{O}^2(G) < G$.

2.2. Let G and H be nilpotent groups. Notice that $\mathrm{Z}(G \times H) = \mathrm{Z}(G) \times \mathrm{Z}(H)$, and clearly

$$(G \times H)/(\mathrm{Z}(G) \times \mathrm{Z}(H)) = G/\mathrm{Z}(G) \times H/\mathrm{Z}(H).$$

By induction, $G/\mathrm{Z}(G) \times H/\mathrm{Z}(H)$ is a nilpotent group, and so $G \times H$ is, completing the proof.

An example of a semidirect product of two nilpotent groups that is not nilpotent is $S_3 = C_3 \rtimes C_2$, which is not nilpotent since it has no centre.

2.3. Suppose firstly that α has prime order q (where $q \neq p$), and acts trivially on H and G/H, and write p^m for the order of H. Since α fixes each coset of H, each of which is a set of order p^m, α must permute the elements of this coset, and hence must fix at least one element in this coset (since if all orbits have length more than 1, they all have length a multiple of q). Hence α fixes an element from each coset of H. Let X denote a collection of such fixed points. Since α fixes every element of H and X, it acts trivially on $\langle X, H \rangle = G$, as needed.

Finally, suppose that $o(\alpha)$ is not of prime order, and write $o(\alpha) = qn$, where $n > 1$. Notice that α^n has order q, and acts trivially on H and G/H, so $\alpha^n = 1$ by the previous paragraph. Thus $o(\alpha) = n$, and this contradiction proves the general case.

2.4. (a) $[x,y] = x^{-1}y^{-1}xy = \left(y^{-1}x^{-1}yx\right)^{-1} = [y,x]^{-1}$. (b) $[xy,z] = y^{-1}x^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}x\left(zyy^{-1}z^{-1}\right)yz = [x,z]^y[y,z]$. For the second equality, notice that

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

(c) $[x, yz] = [yz, x]^{-1} = ([y, x]^z[z, x])^{-1} = [z, x]^{-1}([y, x]^z)^{-1} = [x, z][x, y]^z$, proving the first inequality. The second inequality follows the same as the previous part.

(d) Notice that

$$\begin{aligned}[x, y^{-1}, z]^y &= y^{-1}[x, y^{-1}]^{-1}z^{-1}[x, y^{-1}]zy \\ &= y^{-1}\left(x^{-1}yxy^{-1}\right)^{-1}z^{-1}x^{-1}yx^{-1}y^{-1}zy \\ &= \left(y^{-1}y\right)\left(x^{-1}y^{-1}xz^{-1}x^{-1}\right)\left(yx^{-1}y^{-1}zy\right) = u^{-1}v.\end{aligned}$$

Cycling x, y, and z, we get $[y, z^{-1}, x]^z = v^{-1}w$ and $[z, x^{-1}, y]^x = w^{-1}u$, so that

$$[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = u^{-1}vv^{-1}ww^{-1}u = 1.$$

The three subgroups lemma is now clear, since if X, Y and Z are all normal subgroups of G then $[X, Y, Z]$ is a normal subgroup of G, and the Hall–Witt identity.

2.5. The case $n = 1$ is fine, so we proceed by induction. Assume true for $n-1$ (and all r). We have $H_{r+n} \trianglelefteqslant H$,

$$[H_{r+n}, K] \leqslant H_{r+n+1} \leqslant H_{r+n},$$

so $K \leqslant \mathrm{N}_G(H_{r+n})$, and $H_{r+n} \trianglelefteqslant \langle H, K\rangle$. We apply the three subgroups lemma with $L = \langle H, K\rangle$ and $N = H_{r+n}$. We want $[L_n(K), H_r] \leqslant N$.

Now, $[K, H_r, L_{n-1}(K)] \leqslant [H_{r+1}, L_{n-1}(K)] \leqslant H_{r+n}$ by induction hypothesis. Also

$$[H_r, L_{n-1}(K), K] \leqslant [H_{r+n-1}, K] \leqslant H_{r+n}$$

by induction. Thus by the three subgroups lemma, N contains

$$[L_{n-1}(K), K, H_r] = [L_n(K), H_r],$$

as required.

2.6. Let M be a minimal normal subgroup of G. If M is simple then we are finished, so we may assume that M is not simple, and let N be a minimal normal subgroup of M. By induction, N is a direct product of isomorphic simple groups S. As M is normal in G, $N^g \trianglelefteqslant M$ for all $g \in G$. Let $N_1, \dots, N_r$ denote all of these conjugates, each isomorphic to N. We claim that M is the direct product of the N_i, proving that M is the direct product of copies of S. To see this, since all elements of G permute the N_i they must normalize the subgroup generated by then, so that $X = \langle N_1, \dots, N_r\rangle \trianglelefteqslant G$. Since M is a minimal normal subgroup of G, $X = N$. To see that N is the direct product of some of the N_i, we see that, if $\hat{N}_i$ is the product of all of the N_j for $j \neq i$, then $N_i \cap \hat{N}_i$

is a normal subgroup of M, hence either $N_i \cap \hat{N}_i = 1$ or $N_i \leqslant \hat{N}_i$. If the latter is true, remove N_i from the collection of the N_i and try again. Eventually, we see that X is the product of some of the N_i, concluding the proof.

If G is soluble then these simple groups S must be C_p for some prime p, and so M is the direct product of copies of C_p, so elementary abelian.

2.7. By Theorem 1.22, if G is nilpotent then all maximal subgroups are normal, since G satisfies the normalizer condition. Conversely, suppose that every maximal subgroup of G is normal in G. Let P be a Sylow p-subgroup of G. If P is not normal in G then $\mathrm{N}_G(P) < G$, so that $\mathrm{N}_G(P) \leqslant M$ for some maximal subgroup M. However, $M \trianglelefteq G$, so a Frattini argument shows that $G = M\,\mathrm{N}_G(P) = M$, a contradiction. Hence all Sylow p-subgroups of G are normal in G, and G is nilpotent by Theorem 1.22 again.

2.8. (a) Let X be the intersection of all conjugates H^g, and let Y be the product of all normal subgroups of G contained in H. Since $X \leqslant H$ and is a normal subgroup of G, $X \leqslant Y$. Conversely, notice that $X \leqslant H$ and so $X = X^g \leqslant H^g$, so that $X \leqslant Y$.

(b) Let X denote the intersection of all normal subgroups of G containing H, and let Y denote the subgroup generated by all conjugates H^g. Since Y is a normal subgroup containing H, $X \leqslant Y$. Conversely, as $H \leqslant X$, $H^g \leqslant X^g = X$, so that $Y \leqslant X$.

2.9. Let A be a subgroup of P. Let Q be a Sylow p-subgroup of $\mathrm{N}_G(A)$, and let $g \in G$ be such that $Q^g \leqslant P$, and write $B = A^g$. Notice that $\mathrm{N}_G(A^g) = \mathrm{N}_G(A)^g$, so the order of a Sylow p-subgroup of $\mathrm{N}_G(B)$ is the same as $|Q|$. Hence, since $Q \leqslant \mathrm{N}_P(B)$, we see that $Q = \mathrm{N}_P(B)$, proving that B is extremal.

If B is extremal and G-conjugate to A, let $g \in G$ be such that $A^g = B$. We have that $\mathrm{N}_P(A)^g \leqslant \mathrm{N}_G(B)$, so that $\mathrm{N}_P(A)^g$ is a p-subgroup of $\mathrm{N}_G(B)$. Since $\mathrm{N}_P(B)$ is a Sylow p-subgroup of $\mathrm{N}_G(B)$, there exists $h \in \mathrm{N}_G(B)$ such that $\left(\mathrm{N}_P(A)^g\right)^h \leqslant \mathrm{N}_P(B)$, proving the second part.

2.10. (a) That $D \xrightarrow{g} D^g$ is clear, since the same subgroups and elements proving that $A \xrightarrow{g} B$ will work. For $B \xrightarrow{g^{-1}} A$ we reverse the sequence of subgroups of elements, and for $A \xrightarrow{gh} C$ we concatenate the two sequences.

(b) Proceed by induction on $n = |P : A|$, the case where $n = 1$ being obvious since then $g \in \mathrm{N}_G(P)$ (and P is extremal). If B is extremal, then there exists $x \in G$ such that $A^x = B$ and $\mathrm{N}_P(A)^x \leqslant \mathrm{N}_P(B)$ by Exercise 2.9. By induction $\mathrm{N}_P(A) \xrightarrow{x} \mathrm{N}_P(A)^g$, so $A \xrightarrow{x} B$. In addition, $x^{-1}g$ normalizes B, so trivially $B \xrightarrow{x^{-1}g} B$, which proves that $A \xrightarrow{g} B$, as needed.

(c) Suppose that $A^g = B$. Choose C an extremal subgroup that is G-conjugate to A, and let $A^h = C$. By the previous part, $A \xrightarrow{h} C$ and $B \xrightarrow{g^{-1}h} C$, so by the first part $A \xrightarrow{g} B$, as needed.

3 Sheet 3

3.1. Consider $\mathrm{C}_G(A)$, which contains A. As $A \trianglelefteqslant G$, $G/\mathrm{C}_G(A)$ is a quotient of G/A, a non-abelian simple group, so that $A = \mathrm{C}_G(A)$ or $G = \mathrm{C}_G(A)$. If $A = \mathrm{C}_G(A)$ then G/A embeds in $\mathrm{Aut}(A)$, an abelian group as A is cyclic; this contradiction proves that $\mathrm{C}_G(A) = G$, i.e., that $A \leqslant \mathrm{Z}(G)$. To see that $A = \mathrm{Z}(G)$, notice that $\mathrm{Z}(G)$ is a normal subgroup of G containing A, so is either A or G. As G is non-abelian, $\mathrm{Z}(G) = A$, as needed.

3.2. Let H and K be as in the question, and let $\bar{H}$ and $\bar{K}$ denote groups isomorphic to H and K respectively. (We make these definitions to avoid ambiguity.) Let $\phi : \bar{H} \times \bar{K} \to G$ be given by $(h,k)\phi = hk$. Since $[H,K] = 1$, this is a homomorphism, as

$$((h_1,k_1)(h_2,k_2))\,\phi = h_1h_2k_1k_2 = h_1k_1h_2k_2 = ((h_1,k_1)\phi)\,((h_2,k_2))\,\phi.$$

The homomorphism is clearly also surjective, and $\bar{H}\phi = H$ and $\bar{K}\phi = K$, so it remains to show that $Z = \ker\phi$ is a central subgroup of G. Also, since ϕ is an isomorphism on both factors, $Z \cap \bar{H} = Z \cap \bar{K} = 1$.

If $z = (h,k)$ lies in Z, then $z\phi = (h\phi)(k\phi) = 1$, so that $h\phi, k\phi \in H \cap K$. In particular, $[h\phi, H] = 1$, so that since $\bar{H}\phi = H$ is an isomorphism, $[h,\bar{H}] = 1$. Thus $h \in \mathrm{Z}\left(\bar{H} \times \bar{K}\right)$, and similarly k is also central in $\bar{G} \times \bar{K}$, so that z is, as claimed.

3.3. (a) Let $h \in H$, and let $\{t_1, \dots, t_n\}$ be a right transversal to H in G. Notice that the set $\{t_1h, \dots, t_nh\}$ is also a right transversal to H in G, since $Ht_ih = Ht_2h$ implies that $Ht_1 = Ht_2$. Hence

$$\chi^G(x) = \sum_{i=1}^{n} \chi(h^{-1}t_i^{-1}xt_ih).$$

By running over all $h \in H$, we get

$$|H|\chi^G(x) = \sum_{h\in H}\sum_{i=1}^{n} \chi(h^{-1}t_i^{-1}xt_ih) = \sum_{g\in G}\chi(g^{-1}xg),$$

since as $h \in H$ and $1 \leqslant i \leqslant n$, t_ih runs over all elements of G. This completes the proof.

(b) Using the previous part, we have

$$\begin{aligned}\langle \chi^G, \psi\rangle &= \frac{1}{|G|}\sum_{x\in G}\chi^G(x)\overline{\psi(x)}\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{x\in G}\sum_{g\in G}\chi(g^{-1}xg)\overline{\psi(x)}\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{y\in G}\sum_{g\in G}\chi(y)\overline{\psi(y^{g^{-1}})}.\end{aligned}$$

Since ψ is a character of G, $\psi(y^{g^{-1}}) = \psi(y)$, and so the sum is independent of g. Thus

$$\begin{aligned}&= \frac{1}{|G|}\frac{1}{|H|}\sum_{y\in G}|G|\chi(y)\overline{\psi(y)}\\ &= \frac{1}{|H|}\sum_{y\in G}\chi(y)\overline{\psi(y)}.\end{aligned}$$

As $\chi(y) = 0$ for $y \in G \setminus H$, we can restrict the sum to $y \in H$, to get

$$= \frac{1}{|H|}\sum_{y\in H}\chi(y)\overline{\psi(y)} = \langle \chi, \psi_H\rangle.$$

This completes the proof.

3.4. Let Q be a normal p-subgroup of G, contained in some Sylow p-subgroup P of G. If $g \in G$ then $Q = Q^g \leqslant P^g$, and since G acts transitively on the Sylow p-subgroups, Q lies in every one. Conversely, letting R denote the intersection of all Sylow p-subgroups P, R^g is also the intersection of all Sylow p-subgroups P^g, so $R = R^g$ and $R \trianglelefteqslant G$. Thus $\mathrm{O}_p(G)$ is the intersection of all Sylow p-subgroups of G, as claimed.

3.5. Let K be a normal p-complement for G, and notice that $L = K \cap \mathrm{N}_G(Q)$ is a normal p-complement for $\mathrm{N}_G(Q)$ (as L is a p'-group and $\mathrm{N}_G(Q)/L$ is a p-group by the second isomorphism theorem). As $Q, L \trianglelefteqslant \mathrm{N}_G(Q)$, $[Q, L] \leqslant Q \cap L = 1$, and so $L \leqslant \mathrm{C}_G(Q)$. Thus $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is a p-group, as it is a quotient of $\mathrm{N}_G(Q)/L$.

3.6. Suppose that $\mathrm{Aut}_G(Q)$ is a p-group for all $Q \leqslant P$, so that if Q is extremal then $\mathrm{Aut}_G(Q) = \mathrm{Aut}_P(Q)$. By Exercise 2.10, if $A, B \subseteq P$ and $g \in G$ is such that $A^g = B$, then $A \xrightarrow{g} B$, so that $g = x_1x_2\dots x_n$, where $x_i \in \mathrm{N}_G(R_i)$ for R_i an extremal subgroup of P, and $A^{x_1\dots x_i} \leqslant R_i, R_{i+1}$. Since $\mathrm{Aut}_G(R_i) = \mathrm{Aut}_P(R_i)$, we may write $x_i = c_ir_i$, where $c_i \in \mathrm{C}_G(R_i)$ and $r_i \in \mathrm{N}_P(R_i)$. Finally,

$$Ac_g = Ac_{x_1\dots x_n} = Ac_{c_1r_1\dots c_nr_n} = Ac_{r_1\dots r_n} = Ac_r,$$

where $r \in P$, and we may remove the c_i since the centralize R_i. Thus P control fusion in P with respect to G.

Conversely, suppose that P controls fusion in P with respect to G, and let Q be a subgroup of P of smallest index such that $\mathrm{Aut}_G(Q)$ is not a p-group. By Exercise 2.9, and the fact that $\mathrm{Aut}_G(Q)^g = \mathrm{Aut}_G(Q^g)$, we may assume that $\mathrm{N}_P(Q)$ is a Sylow p-subgroup of $\mathrm{N}_G(Q)$, and hence $\mathrm{Aut}_P(Q)$ is a Sylow p-subgroup of $\mathrm{Aut}_G(Q)$. If $g \in \mathrm{N}_G(Q)$ has p'-order, then there exists $x \in P$ such that g and x induce the same conjugation action on Q. Since g is a p'-element the induced automorphism $c_g \in \mathrm{Aut}_G(Q)$ has order prime to p, but $c_g = c_x$ so that it has order a power of p. Hence $c_g = 1$ and $g \in \mathrm{C}_G(Q)$. By Exercise 1.1, as $\mathrm{C}_G(Q)$ contains all p'-elements of $\mathrm{N}_G(Q)$, $\mathrm{O}^p(\mathrm{N}_G(Q)) \leqslant \mathrm{C}_G(Q)$, and the result is proved.

To see the consequence, notice that for $Q \leqslant H$, we have $\mathrm{N}_H(Q) = \mathrm{N}_G(Q) \cap H$ and $\mathrm{C}_H(Q) = \mathrm{C}_G(Q) \cap H$, so that

$$\begin{aligned}\frac{|\mathrm{N}_H(Q)|}{|\mathrm{C}_H(Q)|} &= \frac{|\mathrm{N}_G(Q) \cap H|}{|\mathrm{C}_G(Q) \cap H|} = \frac{|\mathrm{N}_G(Q) \cap H|/|H|}{|\mathrm{C}_G(Q) \cap H|/|H|} \\ &= \frac{|\mathrm{N}_G(Q)|/|H\,\mathrm{N}_G(Q)|}{|\mathrm{C}_G(Q)|/|H\,\mathrm{C}_G(Q)|} = \frac{|\mathrm{C}_G(Q)H|}{|\mathrm{N}_G(Q)H|}\frac{|\mathrm{N}_G(Q)|}{|\mathrm{C}_G(Q)|}.\end{aligned}$$

The second term is a p-group by assumption and the first part, and $\mathrm{N}_G(Q)H/\mathrm{C}_G(Q)H$ is a p-group because it is the image of $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ in G/H. Hence $\mathrm{N}_H(Q)/\mathrm{C}_H(Q)$ is a p-group, so that $P \cap H$ controls fusion in $P \cap H$ with respect to G, by the first part again.

3.7. (a) Let $\{x_1, \dots, x_n\}$ be a transversal for P in G. Choose d, $y_1 \dots, y_d$, and $r-1, \dots, r-d$ as in Proposition 1.10. For $x \in P$, we have

$$x\tau = \prod P' y_i x^{r_i} y_i^{-1}.$$

As P controls fusion in P with respect to G, there exists $g \in P$ such that $a_i = y_i x^{r_i} y_i^{-1} = g x^{r_i} g^{-1}$, whence $a_i (x^{r_i})^{-1} = [g^{-1}, (x^{r_i})^{-1}]$ lies in P'. In particular, $P' y_i x^{r_i} y_i^{-1} = P' x^{r_i}$, so that

$$x\tau = \prod_{i=1}^{d} P' y_i x^{r_i} y_i^{-1} = \prod_{i=1}^{d} P' x^{r_i} = P' x^n.$$

Since n is prime to p, $P'x^n = P'$ if and only if $P'x = P'$, i.e., $x \in P'$, so that if $x \in P \setminus P'$ then $x \notin \ker\tau$. In particular, $\ker\tau < P$, so that $\mathrm{O}^p(G) < G$.

(b) By the previous part, $\mathrm{O}^p(G) < G$, and by the previous exercise, $P \cap \mathrm{O}^p(G)$ controls fusion in $P \cap \mathrm{O}^p(G)$ with respect to G, so by induction $\mathrm{O}^p(G)$ has a normal p-complement K. Obviously K is a normal p-complement for G, completing the proof.

4 Sheet 4

4.1. (a) Let γ be a 1-cocycle, and let $S = \{x\gamma(x) : x \in G\}$. If $x\gamma(x)$ and $y\gamma(y)$ are elements of S, then

$$(x\gamma(x))(y\gamma(y)) = xy\gamma(x)^y\gamma(y) = xy\gamma(xy) \in S.$$

Hence S is closed under products, so since S is finite, it is a subgroup of X. If $g \in S \cap M$, then $g = x\gamma(x)$, and as $\gamma(x) \in M$, $x \in M$, so is 1. Thus $S \cap M = 1$. To prove that S is a complement to M, we must show that the map $x \mapsto x\gamma(x)$ is an injection. If $x\gamma(x) = y\gamma(y)$, then since $x, y \in G$ and $\gamma(x), \gamma(y) \in M$, and $X = GM$, we must have that $x = y$, so that $x \mapsto x\gamma(x)$ is an injection.

(b) Let H be a complement to M in X. Since G is a complement to M in X, every element h of H may be written as $h = xv$, for $x \in G$ and $v \in M$. Set $v = \gamma(x)$. We claim this is a 1-cocycle: clearly $H = \{x\gamma(x) : x \in G\}$, so this will complete the proof.

Let $x, y \in G$, and let $h = x\gamma(x)$ and $k = y\gamma(y)$, so that $h, k \in H$. We have $hk = x\gamma(x)y\gamma(y)$, and so

$$hk = x\gamma(x)y\gamma(y) = xy\gamma(x)^y\gamma(y).$$

However, since $hk \in H$, we have that $hk = (xy)\gamma(xy)$, and so

$$\gamma(xy) = \gamma(x)^y\gamma(y)$$

in X, and written additively in M this is the 1-cocycle identity.

(c) Let $g \in X$ be such that $H = K^g$, and write $g = hv$, for $v \in M$ and $k \in K$. (We can do this since $X = KV$.) As $K^k = K$, $K^g = K^v$, and this completes the proof.

4.2. (a) The sum of two 1-cocycles is a 1-cocycle because

$$(\gamma+\delta)(xy) = \gamma(xy)+\delta(xy) = \gamma(x)\cdot y+\delta(x)\cdot y+\gamma(y)+\delta(y) = (\gamma+\delta)(x)\cdot y+(\gamma+\delta)(y).$$

It is clearly commutative, and associativity is induced from the associativity of M. The identity is the zero 1-cocycle $\gamma(x) = 0$, and inverses are $\gamma(x) = -x$.

(b) Firstly we must show that every 1-coboundary is a 1-cocycle: let $\gamma(x) = v - v \cdot x$ for some $v \in M$. We have

$$\gamma(xy) = v-v\cdot(xy) = v-(v\cdot x)\cdot y+v\cdot y-v\cdot y = (v-v\cdot x)\cdot y+v-v\cdot y = \gamma(x)\cdot y+\gamma(y).$$

Secondly, we must show that the sum of two 1-coboundaries is a 1-coboundary: if $\gamma(x) = v - v \cdot x$ and $\delta(x) = w - w \cdot x$ are two 1-coboundaries then

$$(\gamma + \delta)(x) = \gamma(x) + \delta(x) = v - v \cdot x + w - w \cdot x = (v + w) - (v + w) \cdot x.$$

This completes the proof.

4.3. Define $\sigma \in M$ by $\sigma = \sum_{x \in G} \gamma(x)$. Let $|G| = n$ and $|M| = m$. Summing the 1-cocycle identity for all $g \in G$ we get

$$\sigma = \sigma \cdot y + n\gamma(y).$$

Hence we see that $\sigma - \sigma \cdot y = n\gamma(y)$. Since n and m are coprime, there exist integers a and b such that $am + bn = 1$. Let $v = b\sigma \in M$. We have

$$v - v \cdot y = bn\gamma(y) = \gamma(y)$$

(since $bn = 1 - am = 1$ modulo $m = |M|$). Hence γ is a 1-coboundary, and $H^1(G, M) = 0$.

4.4. Let γ and δ be associated to the complements H and K respectively.

If $\gamma(x) - \delta(x) = v - v \cdot x$ for some $v \in M$, we claim that $H = K^v$. To see this, notice that, in X, $v - v \cdot x = vx^{-1}v^{-1}x$, and so

$$\gamma(x) = vx^{-1}v^{-1}x\delta(x).$$

From this we get that $vxv^{-1}\gamma(x) = x\delta(x)$. However, $\gamma(x) \in M$, so that $\gamma(x) = \gamma(x)^v$, and so we see that

$$x^{v^{-1}}\gamma(x)^{v^{-1}} = x\delta(x),$$

which implies $x\gamma(x) = (x\delta(x))^v$. As H is the set of all $x\gamma(x)$ and K is the set of all $x\delta(x)$, we get the result.

Conversely, if $H = K^v$ for some $v \in M$ (by Exercise 4.1(c) we may assume this), then

$$x\gamma(x) = h = k^v = (x\delta(x))^v,$$

for each $x \in G$, and reversing the argument above we get $\gamma(x)\delta(x)^{-1} = vx^{-1}v^{-1}x$; written additively in M,

$$\gamma(x) - \delta(x) = v - v \cdot x,$$

as claimed.

4.5. (a) Let $X = G \rtimes A$. Let $p \mid |G|$ and let P be a Sylow p-subgroup of G (hence of X). By the Frattini argument, $X = G\,\mathrm{N}_X(P)$. Also, $\mathrm{N}_G(P) = G \cap \mathrm{N}_X(P)$ is a normal subgroup of $\mathrm{N}_X(P)$, and $|\,\mathrm{N}_X(P) : \mathrm{N}_G(P)| \mid |X : G|$ is prime to $|G|$, so by the Schur–Zassenhaus theorem there exists a complement L to $\mathrm{N}_G(P)$ in $\mathrm{N}_X(P)$. Hence

$$X = G\,\mathrm{N}_X(P) = G\,\mathrm{N}_G(P)L = GL,$$

so that L is a complement to G in X. By the Schur–Zassenhaus theorem again, $L^x = A$ for some $x \in X$, and so A normalizes P^x, since L normalizes P. This proves the claim.

(b) Let Q be a maximal A-invariant p-subgroup. If Q is not a Sylow p-subgroup of G, then Q is contained in a (not A-invariant) Sylow p-subgroup P of G, hence $\mathrm{N}_P(Q) > Q$. In particular, this proves that Q is not a Sylow p-subgroup of $\mathrm{N}_G(Q)$, which is A-invariant since Q is. However, by the previous part there is an A-invariant Sylow p-subgroup R of $\mathrm{N}_G(Q)$, which contains Q since $Q \trianglelefteq \mathrm{N}_G(Q)$ (using Exercise 3.4). Hence Q is not a maximal A-invariant p-subgroup, and this contradiction proves that Q is a Sylow p-subgroup of G, as needed.

(c) Let P and Q be A-invariant Sylow p-subgroups. There exists $g \in G$ such that $P^g = Q$. Since $A, A^g \leqslant \mathrm{C}_X(Q)$, we see that both A and A^g are complements to $\mathrm{C}_X(Q) \cap G = \mathrm{C}_G(Q)$ in $\mathrm{C}_X(Q)$. Hence, by the Schur–Zassenhaus theorem, there exists $x \in \mathrm{C}_X(A)$ such that $A^{gx} = A$. In fact, by Exercise 4.1(c), we may choose $x \in \mathrm{C}_G(A)$, so that $gx \in G$. As $G \trianglelefteq X$, $[gx, A] \leqslant G$, but since gx normalizes A, $[gx, A] \leqslant A$, so that $[gx, A] \leqslant A \cap G = 1$. Hence gx centralizes A. Also, since $x \in \mathrm{C}_G(Q)$, $P^{xg} = Q$, so that $\mathrm{C}_G(A)$ acts transitively on the A-invariant Sylow p-subgroups of G.

5 Sheet 5

5.1. The group Q_8 is a non-split extension of C_4 by C_2, with the correct conjugation action; hence $H^2(G, M) \neq 0$. In D_8, there are two non-central conjugacy classes of elements of order 2, and so $H^1(G, M) \neq 0$.

5.2. Clearly the element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has order p, and hence forms a Sylow p-subgroup of $\mathrm{GL}_2(p)$, since the order of $\mathrm{GL}_2(p)$ is $p(p+1)(p-1)^2$.

Since $|\,\mathrm{GL}_2(p) : \mathrm{SL}_2(p)| = p - 1$, any Sylow p-subgroup P of $\mathrm{SL}_2(p)$ is a Sylow p-subgroup of $\mathrm{GL}_2(p)$. Since $\mathrm{SL}_2(p)$ is normal in $\mathrm{GL}_2(p)$, all Sylow p-subgroups of $\mathrm{GL}_2(p)$ are contained in $\mathrm{SL}_2(p)$. Let P denote the upper unitriangular matrices. Notice that every upper triangular matrix normalizes P, and hence $\mathrm{N}_{\mathrm{SL}_2(p)}(P)$ has order at least $p(p-1)$. There are at least $p+1$ Sylow p-subgroups of $\mathrm{SL}_2(p)$, and so by the fact that $|\,\mathrm{SL}_2(p)| = p(p+1)(p-1)$, we see that the normalizer has order exactly $p(p-1)$ and there are exactly $p+1$ Sylow p-subgroups. In particular, all Sylow p-subgroups of $\mathrm{SL}_2(p)$ are Sylow p-subgroups of G.

We aim to show that $\mathrm{SL}_2(p) \leqslant G$, so we may intersect G with $\mathrm{SL}_2(p)$, and assume that G is a subgroup of $\mathrm{SL}_2(p)$. Hence the above argument proves that $|G| \geqslant p(p+1)$, and so G has index at most $p-1$ in $\mathrm{SL}_2(p)$. Let ϕ be the homomorphism from $\mathrm{SL}_2(p)$ to S_{p-1} given by acting on the cosets of G. Since $p \nmid |S_{p-1}|$, we see that all $p+1$ Sylow p-subgroups of $\mathrm{SL}_2(p)$ lie inside $\ker\phi$. Hence $|\ker\phi| \geqslant p(p+1)$.

Since $p \geqslant 5$, $\mathrm{PSL}_2(p)$ is simple, and so the composition factors of $\mathrm{SL}_2(p)$ are $\mathrm{PSL}_2(p)$ and C_2. As $\ker\phi \trianglelefteq G$ and has order at least $p(p+1)$, either $\ker\phi = G$ or $\ker\phi$ has index 2 (as $\mathrm{PSL}_2(p)$ is a composition factor of $\ker\phi$). Since $\mathrm{SL}_2(p)$ is perfect, it has no subgroups of index 2: as $\mathrm{SL}_2(p) = \ker\phi \leqslant G$, we get the result.

5.3. Consider the map $\rho : G \to \mathrm{Sym}(p)$, given by acting on the cosets of H. Since $|Sym(p)| = p \cdot (p-1)!$, and $|G| = p \cdot n$, where all prime divisors of n are at least p, we see that $\operatorname{im}\rho$ has order p. Hence the core of H in G, the kernel of ρ, must have index p, so equals H. Thus $H \trianglelefteq G$.

5.4. i) In general, if c_x denotes conjugation by $x \in H$ and $\phi \in \mathrm{Aut}(H)$, then $\phi^{-1}c_x\phi = c_{x\phi}$. To see this, simply calculate for $h \in H$:

$$h(\phi^{-1}c_x\phi) = (x^{-1}(h\phi^{-1})x)\phi = (x^{-1}\phi)(h\phi^{-1}\phi)(x\phi) = (x\phi)^{-1}h(x\phi).$$

Since $H\phi = H$, we see that $\mathrm{Inn}(H)^\phi = \mathrm{Inn}(H)$, as required.

ii) The map $\theta\, \mathrm{N}_K(H) \to \mathrm{Aut}(H)$ given by $\theta : k \mapsto c_k$ is a homomorphism, with kernel $\mathrm{C}_K(H)$ and image $\mathrm{Aut}_K(H)$, which proves the result.

iii) Apply the previous part to $H = K$, noting that $\mathrm{C}_H(H) = \mathrm{Z}(H)$.

iv) The image of $(H \cap K)\,\mathrm{C}_K(H)$ under θ is the set $\mathrm{Inn}(H) \cap \mathrm{Aut}_K(H)$, and so $\mathrm{N}_K(H)/(H \cap K)\,\mathrm{C}_K(H)$ is naturally isomorphic to $\mathrm{Aut}_K(H)/(\mathrm{Inn}(H) \cap \mathrm{Aut}_K(H)) \cong \mathrm{Aut}_K(H)\,\mathrm{Inn}(H)/\,\mathrm{Inn}(H) = \mathrm{Out}_K(H)$.

v) As $\mathrm{Z}(G) = 1$, $G \cong \mathrm{Inn}(G)$, and so G may be embedded naturally in $\mathrm{Aut}(G)$.

vi) Let $G = A_4$. This group is generated by $(1,2,3)$ and $(1,2)(3,4)$. The first element has eight possible images under an automorphism, and the second has three, so that $|\mathrm{Aut}(A_4)| \leqslant 24$. However, $|S_4| = 24$, so this proves that $\mathrm{Aut}(A_4) = S_4$, since $S_4 \leqslant \mathrm{Aut}(A_4)$ clearly.

Now let $G = A_5$. A subgroup of index 5 has order 12, so cannot be a transitive subgroup of A_4; hence all subgroups of order 12 in A_5 are isomorphic with A_4 and are point stabilizers. There are five of these, so $|\mathrm{Aut}(A_5)| = 5 \cdot |\mathrm{Aut}(A_4)| = 5 \cdot |S_4| = |S_5|$. As clearly $\mathrm{Aut}(A_5)$ contains S_5, we are done.

5.5. i) Since $A \leqslant P$ and $A \leqslant P^{g^{-1}}$, $A^g = A$, and so $\mathrm{C}_G(A)^g = \mathrm{C}_G(A)$. As A is extremal in P with respect to G, $\mathrm{N}_P(A)$ is a Sylow p-subgroup of $\mathrm{N}_G(A)$, so that (as $\mathrm{C}_G(A) \trianglelefteqslant \mathrm{N}_G(A)$) $\mathrm{C}_P(A) = \mathrm{C}_G(A) \cap \mathrm{N}_P(A)$ is a Sylow p-subgroup of $\mathrm{C}_G(A)$.

Since $\mathrm{C}_P(A)$ is a Sylow p-subgroup of $\mathrm{C}_G(A)$, $\mathrm{C}_P(A)^{g^{-1}}$ and $\mathrm{C}_P(A)$ are $\mathrm{C}_G(A)$-conjugate. Thus there exists $x \in \mathrm{C}_G(A)$ such that $\mathrm{C}_P(A)^x = \mathrm{C}_P(A)^{g^{-1}}$. Therefore

$$(A\,\mathrm{C}_P(A))^{xg} = A^{xg}\,\mathrm{C}_P(A)^{xg} = A\,\mathrm{C}_P(A).$$

However, by the definition of a domestic intersection, we must have $A\,\mathrm{C}_P(A) = A$, so that $\mathrm{C}_P(A) \leqslant A$; hence $\mathrm{C}_P(A) = \mathrm{Z}(A)$.

Finally, using Burnside's normal p-complement theorem, since $\mathrm{Z}(A)$ is a Sylow p-subgroup of $\mathrm{C}_G(A)$, and is clearly in the centre of $\mathrm{C}_G(A)$, we have that $\mathrm{C}_G(A)$ has a normal p-complement $K = \mathrm{O}_{p'}(\mathrm{C}_G(A))$. As $\mathrm{Z}(A)$ is central, it is also a normal subgroupp, so we have a direct product.

ii) Since A is a tame intersection, $R = \mathrm{N}_P(A)$ and $S = \mathrm{N}_{P^{g^{-1}}}(A)$ are Sylow p-subgroups of $\mathrm{N}_G(A)$, so that A is the intersection of two Sylow p-subgroups of $\mathrm{N}_G(A)$. Hence $\mathrm{O}_p(\mathrm{N}_G(A)) = A$. Taking images under the natural surjective map $\mathrm{N}_G(A) \to \mathrm{Aut}_G(A)$, we see that $\mathrm{O}_p(\mathrm{Aut}_G(A)) = \mathrm{Inn}(A)$, as needed.

5.6. Suppose that G has a strongly p-embedded subgroup, M, containing a Sylow p-subgroup P. Let g be an element of $G \setminus M$, and consider P^g. We claim that P^g and P lie in different components of $\mathcal{A}_p(G)$. Since $M \cap M^g$ is a p'-group, we see that $P \cap P^g = 1$. Suppose that $Q = Q_0, Q_1, \dots, Q_n = Q^g$ is a path of minimal length linking $Q \leqslant P$ and $Q^g \leqslant P^g$, as we range over all subgroups of P and all paths. Since $Q \leqslant P$ and $Q \cap Q_1 \neq 1$, we must have that Q_1 is contained within P, contradicting the minimal length claim. Thus P and P^g lie in different components, as claimed.

Now suppose that $\mathcal{A}_p(G)$ is disconnected, and let P be a Sylow p-subgroup of G. Since $\mathcal{A}_p(G)$ is disconnected, this splits $\mathrm{Syl}_p(G)$ into (at least two) components (else all p-subgroups, which are contained in Sylow p-subgroups, would be connected to each other), and let $\mathcal{S}$ denote the subset of $\mathrm{Syl}_p(G)$ lying in the same component as P. Let M denote the set of all $g \in G$ such that $P^g \in \mathcal{S}$. The claim is that M is a strongly p-embedded subgroup of G. Firstly, M is clearly a subgroup, and contains a Sylow p-subgroup of G. Furthermore, if $g \notin M$, then for any (non-trivial) p-subgroup Q of M, we have that Q and Q^g are not connected in $\mathcal{A}_p(G)$, so certainly $Q \cap Q^g = 1$. Hence $M \cap M^g$ is a p'-group, as required.

5.7. Since $\mathrm{C}_G(A) = \mathrm{Z}(A) \times \mathrm{O}_{p'}(\mathrm{C}_G(A))$, $\mathrm{C}_P(A) \leqslant A$. Hence, as A is extremal, $\mathrm{N}_P(A)/A \cong \mathrm{Out}_P(A)$ is a Sylow subgroup of $\mathrm{Out}_G(A)$. Since $\mathrm{Out}_G(A)$ has a strongly p-embedded subgroup, there are two Sylow p-subgroups of it, which we may take to be $\mathrm{Out}_P(A)$ and another S, which lie in different connected components of $\mathcal{A}_p(\mathrm{Out}_G(A))$. Taking preimages in $\mathrm{N}_G(A)$, we see that there exists $g \in \mathrm{N}_G(A)$ such that $\mathrm{N}_P(A) \cap \mathrm{N}_P(A)^{g^{-1}} = A$. This proves that A is a tame intersection.

Now assume that $x \in \mathrm{C}_G(A)$, and write $x = ab$, where $a \in \mathrm{Z}(A)$ and $b \in \mathrm{O}_{p'}(\mathrm{C}_G(A))$. Write $X = P \cap P^{(xg)^{-1}} \geqslant A$, and suppose that $X > A$. Set $Y = \mathrm{N}_X(A)$, and notice that $A < Y$. As $A \trianglelefteqslant Y$, we have that $Y \leqslant \mathrm{N}_P(A)$, and since $Y \leqslant P^{(xg)^{-1}}$ we see that $Y \leqslant \mathrm{N}_{P^{(xg)^{-1}}}(A)$. However, taking images in $\mathrm{Aut}_G(A)$, we see that $\mathrm{Out}_Y(A) \leqslant \mathrm{Out}_P(A) \cap S = 1$. Thus $\mathrm{Aut}_Y(A) \leqslant \mathrm{Inn}(A)$ and Y is a p-subgroup of $A\,\mathrm{C}_G(A)$, so contained in A, a contradiction.

6 Sheet 6

6.1. (i) Exercise 2.4 yields the identity $[xy, z] = [x, z][x, z, y][y, z]$. If $x, y \in L_i(G)$ and $z \in G$ then $[xy, z]$, $[y, z]$ and $[x, z]$ lie in $L_{i+1}(G)$ and $[x, z, y] \in L_{i+2}(G)$. Hence, $L_{i+2}(G)[xy, z] = L_{i+2}(G)[x, z][y, z]$, which is the requirement for being linear in the first variable. Being linear in the second variable follows similarly, using the identity $[x, yz] = [x, z][x, y][x, y, z]$ and the fact that the X_i are abelian groups.

(ii) Suppose that, for $1 \leqslant j \leqslant i$, the subgroup $L_j(G)$ is generated by the finite set S_j modulo $L_{j+1}(G)$. The group $L_{i+1}(G)$ is generated by elements of the form $[a, x]$, where $x \in G$ and $a \in L_i(G)$. By (i), modulo $L_{i+2}(G)$, we may write this as aproduct of commutators $[b, y]$, where $b \in S_j$ and $y \in S_1$, so that X_{i+1} is generated by at most $|S_j| \cdot |S_1|$ elements, a finite number.

(iii) Since X_i is an abelian group, it suffices to show that a generating set for X_i consists of elements of order dividing n. By (ii), these have the form (the images in X_i of) $[a, x]$, where x lies in S_1 and a lies in S_{i-1}, each of which has order dividing n modulo lower terms in the central series. Since $(a, x) \mapsto [a, x]$ is bilinear, $[a, x]^n = [a^n, x] = [1, x] = 1$ modulo $L_{i+1}(G)$, and so X_i has exponent dividing n.

(iv) A finitely generated abelian group of finite exponent is finite. Hence, if the exponent of G/G' is finite, and G is finitely generated, then each X_i is finite, so G is finite. Otherwise, G/G' is infinite and finitely generated, so has a quotient isomorphic to $\mathbb{Z}$, as required.

6.2. (i) By the focal subgroup theorem, $P \cap G'$ is generated by all elements of the form $x^{-1}x^g$, where $x \in P$ and $g \in G$ are such that $x^g \in P$. By Burnside's theorem, since P is abelian, we may assume that $g \in \mathrm{N}_G(P)$, and so $P \cap G'$ is generated by all elements of the form $[x, g]$ for $x \in P$ and $g \in \mathrm{N}_G(P)$. Hence $P \cap G' = [P, N]$, as claimed.

(ii) Let $\theta : P \to P$ be the identity, and let $\tau : G \to P$ be the transfer. By the focal subgroup theorem, $\ker \tau \cap P$ contains $P \cap G' = [P, N]$. If $x \in \mathrm{C}_P(N)$ then x is centralized by all elements of the normalizer $\mathrm{N}_G(P)$, which controls fusion in P by Burnside's theorem. Hence $\{x\} = P \cap x^G$; i.e., x is the only G-conjugate of itself that lies in P.

In the modified version of the transfer, in Proposition 1.10, $x\tau$ is a product of n conjugates of x, each of which lies in P, where $n = |G : P|$. Hence $x\tau = x^{|G:P|} \neq 1$ as $|G : P|$ is prime to p. Thus $\mathrm{C}_P(N) \cap \ker \tau = 1$, so that $\mathrm{C}_P(N) \cap [P, N] = 1$. Since both are clearly normal subgroups of P, it remains to show that every element of P may be expressed as a product of an element from $\mathrm{C}_P(N)$ and an element from $[P, N]$.

Let x be a non-trivial element of P, with n conjugates in $\mathrm{N}_G(P)$. Since P is abelian, $|\,\mathrm{C}_N(x)|$ has p'-index, so $p \nmid n$. If $g_1, \dots, g_n$ are elements of $\mathrm{N}_G(P)$ such that the x^{g_i} are the various conjugates of x, then for each i,

$$x = x^{g_i} \left(x^{g_i}\right)^{-1} x = x^{g_i}[g_i, x].$$

Write m for an integer such that $mn \equiv 1 \bmod p$, and taking the product over all i we get

$$x = x^{nm} = \left(\prod_{i=1}^{n} x^{g_i}\right)^m \cdot \left(\prod_{i=1}^{n} [g_i, x]\right)^m.$$

The first term, since it is the product of all N-conjugates of x, lies in $\mathrm{C}_P(N)$, and the second term clearly lies in $[N, P]$, completing the proof.

6.3. (i) Let $X = \mathrm{N}_G(Q)$ and $S = \mathrm{N}_P(Q)$, a Sylow p-subgroup of X. Let $Y = \mathrm{O}^{p'}(X)$, which is generated by p-elements; hence $S \in \mathrm{Syl}_p(Y)$. By the Frattini argument, $X = Y\,\mathrm{N}_X(S)$. If $g \in \mathrm{N}_G(Q)$ lies in $\mathrm{N}_X(S)$ then it normalizes $S = \mathrm{N}_P(Q)$, so that $\mathrm{N}_P(Q)^g = \mathrm{N}_P(Q)$. This proves that every element of $\mathrm{N}_G(Q)$ is expressible as a product of p-elements of $\mathrm{N}_G(Q)$, and an element that normalizes a subgroup of P of strictly larger order.

(ii) Let S_i be an element of $\mathscr{F}$. If S_i is extremal then (i) proves the statement. If S_i is not extremal then there is an extremal subgroup T such that $T^g = S_i$ and $\mathrm{N}_P(T)^g = \mathrm{N}_P(S_i)$ by Exercise 2.9. As $\mathrm{N}_G(T)^g = \mathrm{N}_G(S_i)$, and the result holds for

$\mathrm{N}_G(T)$, we may pass the decomposition in (i) for any element of $\mathrm{N}_G(T)$ through the conjugation by g.

6.4. It suffices to show this when $\mathscr{F}'$ is obtained from $\mathscr{F}$ by altering a single G-conjugacy class. Let $\mathcal{Q}$ be the G-conjugacy class so altered, and let Q be a subgroup in $\mathcal{Q}$ lying in $\mathscr{F}'$. If we show that $R \xrightarrow{g} R$ with respect to $\mathscr{F}'$ for all $R \in \mathcal{Q}$ and $g \in \mathrm{N}_G(R)$, then $\mathscr{F}'$ is a conjugation family: we have only removed elements of $\mathcal{Q}$ from $\mathscr{F}$, so in any expression of $g \in G$ as a product of $x_i \in \mathrm{N}_G(S_i)$, if $S_i \in \mathscr{F}$ then we may replace them with the sequence obtained above proving that $S_i \xrightarrow{x_i} S_i$ with respect to $\mathscr{F}'$.

It suffices therefore to prove that $R \xrightarrow{g} R$ with respect to $\mathscr{F}'$ for all $R \in \mathcal{Q}$ and $g \in \mathrm{N}_G(R)$. Since $\mathscr{F}$ and $\mathscr{F}'$ coincide on subgroups of P of smaller index than $|P : Q|$, and there exists $h \in G$ such that $R^h = Q$, we must have by assumption $R \xrightarrow{h} Q$ with respect to $\mathscr{F}$, and hence $R \xrightarrow{h} Q$ with respect to $\mathscr{F}'$, for *some* choice of $h \in G$ with $R^h = Q$. Notice that $x = h^{-1}gh \in \mathrm{N}_G(Q)$, so $Q \xrightarrow{x} Q$ with respect to $\mathscr{F}'$ as $Q \in \mathscr{F}'$. Hence

$$R \xrightarrow{h} Q \xrightarrow{h^{-1}gh} Q \xrightarrow{h^{-1}} R,$$

and so $R \xrightarrow{g} R$, as neeed.

6.5. (i) Notice that if either $Norm_G(Q)/Q$ contains a strongly p-embedded subgroup, or $X < \mathrm{N}_G(Q)$, then $\mathrm{O}_p(\mathrm{N}_G(Q)) = Q$, so we may assume this.

Consider $X \cap X^{g^{-1}}$ for some $g \in \mathrm{N}_G(Q) \setminus X$. If S is a p-subgroup of this intersection containing Q and contained in $\mathrm{N}_P(Q)$ (a Sylow p-subgroup of X), then $S \leqslant X$ and $S \leqslant X^{g^{-1}}$, so that S and S^g are p-subgroups of $\mathrm{N}_P(Q)$ strictly containing Q. Hence by Alperin's fusion theorem, applied to $\mathrm{N}_G(Q)/Q$ and $\mathrm{N}_P(Q)/Q$, we may write Qg, and hence g, as a product of elements that normalize subgroups of $\mathrm{N}_P(Q)$ strictly containing Q. However, each of these lies in X, so that $g \in X$.

Consider $X \cap X^{g^{-1}}$ for some $g \in \mathrm{N}_G(Q)$. Let S be a Sylow p-subgroup of this intersection, and choose S to be contained in $\mathrm{N}_P(Q)$; note that $Q \leqslant S \leqslant \mathrm{N}_P(Q)$. Since $S \leqslant X$ and $S \leqslant X^{g^{-1}}$, we have that S and S^g are p-subgroups of $\mathrm{N}_P(Q)$ containing Q. Hence by Alperin's fusion theorem, applied to $\mathrm{N}_G(Q)$ and $\mathrm{N}_P(Q)$, we may write g as a product of elements that normalize subgroups of $\mathrm{N}_P(Q)$ containing S.

If $S > Q$ then the elements g each lie in X, so that $g \in X$. Hence $g \in \mathrm{N}_G(Q) \setminus X$ if and only if $X \cap X^{g^{-1}}$ has Q as a Sylow p-subgroup, i.e., $X \cap X^{g^{-1}}/Q$ is a p'-group. This is equivalent to saying that $X < \mathrm{N}_G(Q)$ if and only if X/Q is a strongly p-embedded subgroup of $\mathrm{N}_G(Q)/Q$, as claimed.

(ii) Let $g \in \mathrm{N}_G(Q)$ be an element such that $X \cap X^{g^{-1}}/Q$ is a p'-group. Since $\mathrm{N}_P(Q) \leqslant X$, this implies that $\mathrm{N}_P(Q) \cap \mathrm{N}_P(Q)^{g^{-1}} = Q$. If $P \cap P^{g^{-1}} > Q$, then there is a subgroup of $P \cap P^{g^{-1}}$ strictly containing Q in which Q is normal, which contradicts the fact that $\mathrm{N}_P(Q) \cap \mathrm{N}_P(Q)^{g^{-1}} = Q$. Hence $Q = P \cap P^{g^{-1}}$. By assumption $Q = Q^g$ is extremal in P with respect to G, and so $P \cap P^{g^{-1}}$ is a tame intersection, by Lemma 3.15.

(iii) As in the previous question, we must show that, for $g \in \mathrm{N}_G(Q)$, $Q \xrightarrow{g} Q$ with respect to $\mathscr{F}'$. However, as $g \in X$, we may write g as a product $x_1 x_2 \dots x_n$ of elements of G that normalize subgroups $R_1, \dots, R_n$ of P of strictly smaller index in P than $|P : Q|$. Since $\mathscr{F}$ is a conjugation family, $R_i \xrightarrow{x_i} R_i$ with respect to $\mathscr{F}$ for all i, and since $\mathscr{F}'$ differs from $\mathscr{F}$ only in the exclusion of Q, we have that $R_i \xrightarrow{x_i} R_i$ with respect to $\mathscr{F}'$ for all i; hence $Q \xrightarrow{g} Q$ with respect to $\mathscr{F}'$, as needed.

(iv) The set of all subgroups of P is a conjugation family, by Alperin's fusion theorem, and we may remove all those subgroups Q of P for which $\mathrm{N}_G(Q)/Q$ does not have a strongly p-embedded subgroup, by (iii). Finally, by the previous question, we may take any representatives of the remaining G-conjugacy classes, completing the proof of one direction.

Conversely, let Q be a subgroup of P such that $\mathrm{N}_G(Q)/Q$ has a strongly p-embedded subgroup, and let $\mathscr{F}$ consist of all subgroups of P that are not G-conjugate to Q. We will show that $\mathscr{F}$ is not a conjugation family, which will complete the proof. Let $g \in \mathrm{N}_G(Q) \setminus X$, and suppose that $Q \xrightarrow{g} Q$ with respect to $\mathscr{F}$. In this case, we have that $g = x_1 x_2 \dots x_n$, with $x_i \in \mathrm{N}_G(R_i)$, and since no G-conjugate of Q lies in $\mathscr{F}$, $|P : R_i| < |P : Q|$. Write $Q_i = Q^{x_1 \dots x_i}$, and write $Q_i = Q^{h_i}$ for $1 \leqslant i \leqslant n-1$. Let $h_0 = h_n = 1$, so that $Q_i = Q^{h_i}$ in all cases.

Notice that $Q_{i-1}^{x_i} = Q_i$, so that $y_i = h_{i-1} x_i h_i^{-1}$ maps Q to Q_{i-1} to Q_i to Q; hence $y_i \in \mathrm{N}_G(Q)$. Also,

$$g = x_1 x_2 \dots x_n = (h_0 x_1 h_1^{-1})(h_1 x_2 h_2^{-1}) \dots (h_{n-1} x_n h_n^{-1}) = y_1 \dots y_n.$$

Hence if each y_i lies in X, g lies in X, a contradiction.

Writing $S_i = R_i^{h_i^{-1}}$, we see that as R_i normalizes Q_i and strictly contains it, S_i normalizes Q and strictly contains it. Hence $Q < S_i \leqslant \mathrm{N}_G(Q)$; finally, $S_{i-1}^{y_i} = S_i$, so by Alperin's fusion theorem y_i can be expressed as a product of elements of $\mathrm{N}_G(Q)$ normalizing strictly larger subgroups of $\mathrm{N}_P(Q)$ than Q, so lie in X. Hence $y_i \in X$, and $g \in X$, a contradiction.

6.6. (i) Let P be generated by two elements a and b of order 2. The subgroups of D_{2^n} are cyclic 2-groups, dihedral 2-groups of order at least 8, and Klein four subgroups. There are two conjugacy classes of subgroups of P isomorphic with V_4, with representatives Q and R. By Alperin's fusion theorem, the possibilities for the fusion in P are determined by whether one of Q and R, both, or neither, have automorphisms of odd order.

(ii) If neither has an automorphism of odd order then $\emptyset$ is a conjugation family for G, so that G has a normal p-complement by Frobenius's normal p-complement theorem. Hence $G/A^p(G)$ is Klein four. Suppose that Q has an automorphism of odd order, but not R. By the focal subgroup theorem, $P \cap G'$ is generated by $[x, g]$, for $g \in G$ and $x \in P$, with $x^g \in P$. If $g \in G$ induces an automorphism of order 3 on Q, then $[x, g]$ ranges over the elements of Q as x ranges over the elements of Q. Hence the focal subgroup is generated by P' and Q, which is a subgroup of index 2 in P, so that $G/A^p(G)$ has order 2.

The final case is where Q and R both have an automorphism of order 3, in which case the focal subgroup is generated by P', Q and R, which is P itself. This implies that $P \cap G' = P$, so that $G = \mathrm{O}^2(G)$ by the focal subgroup theorem.

(iii) In this case, all involutions in Q are G-conjugate, as are all involutions in R, and so all involutions in P are G-conjugate. As all Sylow 2-subgroups of G are conjugate, and every involution lies in some Sylow 2-subgroup, this implies that all involutions of G are conjugate.

6.7. (i) The isomorphism is, if $\psi \in \mathrm{Aut}(H)$, $\phi^* : \psi \mapsto \phi^{-1}\psi\phi$. This is clearly a bijection, and it is a homomorphism because

$$(\psi_1\phi^*)(\psi_2\phi^*) = \phi^{-1}\psi_1\phi\phi^{-1}\psi_2\phi = \phi^{-1}\psi_1\psi_2\phi = (\psi_1\psi_2)\phi^*.$$

(ii) As $g^{-1}Hg = H$, applying ϕ we get $(g\phi)^{-1}(H\phi)(g\phi) = (H\phi)$, so that $g\phi$ normalizes $H\phi$. Also,

$$h(c_g\phi^*) = (h^g)\phi = (h\phi)^{g\phi} = (h\phi)c_{g\phi},$$

as needed.

(iii) Apply (ii) to all $g \in \mathrm{N}_K(H)$.

6.8. As above, for $g \in N$, we have that $c_g\psi^* = c_{g\psi} \in \mathrm{Aut}_P(B)$, and $c_g\psi^* = c_g\phi^*$, so that in order for ψ to exist, it must map $\mathrm{Aut}_N(A)$ into $\mathrm{Aut}_P(B)$.

Bibliography

[1] Jonathan Alperin, *Sylow intersections and fusion*, J. Algebra **6** (1967), 222–241.

[2] Kenneth Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer–Verlag, New York, 1994.

[3] William Burnside, *On transitive groups of degree n and class $n-1$*, Proc. London Math. Soc. **32** (1901), 240–246.

[4] ———, *Some properties of groups of odd order*, Proc. London Math. Soc. **33** (1901), 162–185, 257–268.

[5] David A. Craven, *Control of fusion and solubility in fusion systems*, J. Algebra **323** (2010), 2429–2448.

[6] Philip Hall, *Some sufficient conditions for a group to be nilpotent*, Illinois J. Math. **2** (1958), 787–801.

[7] Hermann Heineken and Ismail Mohamed, *A group with trivial centre satisfying the normalizer condition*, J. Algebra **10** (1968), 368–376.

[8] Donald Higman, *Focal series in finite groups*, Canadian J. Math. **5** (1953), 477–497.

[9] Lluís Puig, *The hyperfocal subalgebra of a block*, Invent. Math. **141** (2000), 365–397.

[10] Joseph Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer–Verlag, New York, 1995.

[11] Issai Schur, *Neuer Beweis eines Satzes über endliche Gruppen*, S.-B. Preuss. Akad. Berlin **1902** (1902), 1013–1019.

[12] Michio Suzuki, *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), 105–145.