Chapter 32

MSMYP5 Group Theory

(32.1) Basic Results

(32.1.1) Homomorphisms

Definition 1 *A group is a quadruple $(G, 1, i, m)$ where G is a set, $1 \in G$, i is a unary function, and m is a binary function, and such that*

1. $m(1, x) = x = m(x, 1)$ *for all* $x \in G$.
2. $m(i(x), x) = 1 = m(x, i(x))$ *for all* $x \in G$.
3. $m(m(x, y), z) = m(x, m(y, z))$ *for all* $x, y, z \in G$.

As the notation $m(x, y)$ and $i(x)$ is somewhat laborious, they are abreviated to $m(x, y) = xy$ and $i(x) = x^{-1}$. Further, it is usual to identify G (the set) with the quadruple. It is not actually necessary to specify 1 and i, as they are determined by G and m in the sense that when G and m are given 1 and i can be calculated.

Definition 2 *Let $G = (G, 1_G, i_G, m_G)$ and $H = (H, 1_H, i_H, m_H)$ be groups. H is a subgroup of G if as sets $H \subseteq G$, $1_H = 1_G$, and the functions i_G and m_G restrict to those of H.*

A sufficient condition for a subset H of a group G is that H be non-empty and finite, and closed under m of G. Showing this shows the equivalence of the above definition of a subgroup to the 'usual' one.

Definition 3 *Let G and H be groups. A [group] homomorphism is a function $\theta \colon G \to H$ such that*

1. $\theta(1_G) = 1_H$.
2. $\theta(x^{-1}) = (\theta(x))^{-1}$.
3. $\theta(xy) = \theta(x)\theta(y)$.

Note that s ome definitions take only point 3, the other 2 being deduced from this.

Definition 4 *If G and H are groups and $\theta \colon G \to H$ and $\phi \colon H \to G$ are homomorphisms such that $\phi \circ \theta = \mathrm{Id}_G$ then θ and ϕ are group isomorphisms.*

Definition 5 *Let $N \leqslant G$. N is normal, written $N \trianglelefteq G$ if and only if $g^{-1}ng \in N$ for all $n \in N$ and $g \in G$.*

It can be shown that for $N \leqslant G$ the relation

$$x \sim y \Leftrightarrow y^{-1}x \in N$$

is an equivalence relation with equivalence classes corresponding to the cosets of N. The left and right cosets only coincide when $N \trianglelefteq G$, and in this case a factor group $\frac{G}{N}$ can be formed.

Theorem 6 (Homomorphism) *Let G and H be groups and $\theta\colon G \to H$ be a homomorphirm. Then*

1. $\ker\theta \trianglelefteq G$
2. $\operatorname{Im}\theta \leqslant H$
3. *There is an isomorphism*
$$\overline{\theta}\colon \frac{G}{\ker\theta} \to \operatorname{Im}\theta \quad \textit{defined by} \quad \overline{\theta}\colon gN \mapsto \theta(g)$$

Proof.
1. First of all, $N = \ker\theta \leqslant G$ since
   - $\theta(1_G) = 1_H$ so $1_G \in N$.
   - If $x \in N$ then $\theta(x) = 1_H$. But then $\theta(x^{-1}) = (\theta(x))^{-1} = 1_H^{-1} = 1_H$ and thus $x^{-1} \in N$.
   - If $x, y \in N$ then $\theta(x) = \theta(y) = 1_H$. Then $\theta(xy) = \theta(x)\theta(y) = 1_H 1_H = 1_H$ thus $xy \in N$.

   So N is indeed a subgroup of G. Further, if $g \in G$ and $n \in N$ then
$$\theta(g^{-1}ng) = \theta(g^{-1})\theta(n)\theta(g) = \theta(g^{-1})1_H\theta(g) = (\theta(g))^{-1}\theta(g) = 1_H$$
   thus $g^{-1}ng \in N$ meaning that $N \trianglelefteq G$, as required.
2. Certainly $M = \operatorname{Im}\theta \subseteq H$, so it is now checked for being a group.
   - $\theta(1_G) = 1_H$ so $1_H \in M$.
   - If $h \in M$ then $h = \theta(g)$ for some $g \in G$. But then $\theta(g^{-1}) = (\theta(g))^{-1} = h^{-1} \in M$.
   - If $h, k \in M$ then $h = \theta(g)$ and $k = \theta(f)$ for some $f, g \in G$. Then $hk = \theta(g)\theta(f) = \theta(fg) \in M$.

   Hence $M = \operatorname{Im}\theta \leqslant H$.
3. Define
$$\overline{\theta}\colon \frac{G}{N} \to M \quad \text{by} \quad \overline{\theta}\colon gN \mapsto \theta(g)$$
   First of all it must be shown that $\overline{\theta}$ is well-defined, as each coset gN may be expressed using a different representative, hN say. If $gN = hN$ then $g \in hN$ and so $g = hn$ for some $n \in N$. Then
$$\theta(g) = \theta(hn) = \theta(h)\theta(n) = \theta(h)1_H = \theta(h)$$
   so $\overline{\theta}$ is well defined. $\overline{\theta}$ is a homomorphism since for $g, h \in G$
$$\overline{\theta}(gNhN) = \overline{\theta}(ghN) = \theta(gh) = \theta(g)\theta(h) = \overline{\theta}(gN)\overline{\theta}(hN)$$
   $\overline{\theta}$ is onto for any $\theta(g) \in M$ has a corresponding $gN \in \frac{G}{N}$. Finally, $\overline{\theta}$ is 1-to-1 since if $gN \in \ker\overline{\theta}$ then $\overline{\theta}(gN) = \theta(g) = 1_H$ i.e. $g \in \ker\theta = N$ meaning that $gN = N$. Thus $\ker\overline{\theta} = \{N\}$. □

The Homomorphism Theorem has 2 immediate consequences.

Corollary 7 (First Isomorphism Theorem) *Let $N \trianglelefteq G$ and $H \leqslant G$. Then there is a group homomorphism $\theta\colon H \to \frac{G}{N}$ which is simply the restriction of the cacnonical homomorphism under which $g \mapsto gN$. Then*

1. *$\ker\theta \trianglelefteq H$ and is in fact $H \cap N$ because N is the kernel of the canonical homomorphism.*
2. $\operatorname{Im}\theta = \frac{HN}{N} \leqslant \frac{G}{N}$ *where* $\frac{HN}{N}$ *means* $\{hN \mid h \in H\}$.
3. $\frac{H}{H\cap N} \cong \frac{HN}{N}$

Corollary 8 (Second Isomorphism Theorem) *Let $H \trianglelefteq G$ and $K \trianglelefteq G$ with $K \leqslant H$. Let θ be a homomorphism*
$$\theta\colon \frac{G}{K} \to \frac{G}{H} \quad \textit{defined by} \quad \theta\colon gK \mapsto gH$$

then

$$\ker\theta = \{gK \mid gH = H\} = \{gK \mid g \in H\} = \frac{H}{K}$$

and

$$\operatorname{Im}\theta = \left\{gH \mid gK \in \frac{G}{K}\right\} = \{gH \mid g \in G\} = \frac{G}{H}$$

Hence

1. $\frac{H}{K} \trianglelefteq \frac{G}{H}$.
2. $\frac{G}{H} \leqslant \frac{G}{H}$ *(trivial).*
3. $\frac{\frac{G}{K}}{\frac{H}{K}} \cong \frac{G}{H}$.

Corollary 9 (Third Isomorphism Theorem, Zassenhaus, Butterfly Lemma) *Let $H_1, H_2 \leqslant G$, $K_1 \trianglelefteq H_1$ and $K_2 \trianglelefteq H_2$. Then*

$$\frac{(H_1 \cap H_2)K_1}{(H_1 \cap K_2)K_1} \cong \frac{(H_1 \cap H_2)K_2}{(H_2 \cap K_1)K_2}$$

Theorem 10 (Correspondence) *Let G and H be groups and $\theta\colon G \to H$ be a homomorphism. Then there exists a bijection between*

- *Subgroups K of G that contain (as a subgroup) $\ker\theta$; and*
- *subgroups L of H which are contained in (as a subgroup) $\operatorname{Im}\theta$.*

Where the correspondence holds $x \in K \Leftrightarrow \theta(x) \in L$, and furthermore

$$\frac{K}{\ker\theta} \cong L$$

(32.1.2) Group Actions

Definition 11 *A group action of a group G on a set X is a function $f\colon G \times X \to X$ such that*

1. *$f(1_G, x) = x$ for all $x \in X$.*
2. *$f(gh, x) = f(g, f(h, x))$ for all $x \in X$ and $g, h \in G$.*

If X has a group action, then it may be called a G-set. G-sets may have G-homomorphisms between them: If $(X, \cdot)$ and $(Y, \circ)$ are G-sets and $\theta\colon X \to Y$ is a G-homomorphism then $g \circ \theta(x) = \theta(g \cdot x)$.

A common group action is of a group on itself by conjugation, so $x \mapsto gxg^{-1}$ for some chosen $g \in G$ for all $x \in G$.

(32.1.3) Products Of Groups

Groups may be combined to form new groups. The simplest case is the external direct product where the Cartesian product of 2 groups is made into a group by component-wise multiplication.

Let G be a group and H and K be subgroups of G. Define

$$HK = \{hk \mid h \in H, k \in K\}$$

Certainly $HK \subseteq G$ but it is not necessarily the case that $HK \leqslant G$.

If $H \trianglelefteq G$ then

$$(h_1k_1)(h_2k_2) = \underbrace{h_1(k_1h_2k_1^{-1})}_{\in H}\underbrace{(k_1k_2)}_{\in K}$$

and so $HK \leqslant G$. If furthermore $H \cap K = \{1_G\}$ then G is said to be a semi-direct product of H and K, written $G = H \rtimes K$. Similarly, if $K \trianglelefteq G$ then

$$(h_1k_1)(h_2k_2) = \underbrace{(h_1h_2)}_{\in H}\underbrace{(h_2^{-1}k_1h_2)k_2}_{\in K}$$

and so when $H \cap K = \{1_G\}$, $G = H \ltimes K$.

Lemma 12 *If both $H \trianglelefteq G$ and $K \trianglelefteq G$ then $HK \cong H \times K$.*

Proof. Let $h \in H$ and $k \in K$. Since $H \trianglelefteq G$ $k^{-1}hk \in H$ and thus $h^{-1}k^{-1}hk \in H$.

Similarly, since $K \trianglelefteq G$ $h^{-1}k^{-1}h \in K$ and thus $h^{-1}k^{-1}hk \in K$.

But $H \cap K = \{1_G\}$ so $h^{-1}k^{-1}h = 1_G$, *i.e.*, $hk = kh$ and this is so for all $h \in H$ and $k \in K$.

Define now $\theta\colon H \times K \to HK$ by $\theta\colon (h,k) \mapsto hk$. Then

$$\theta((h_1,k_1)(h_2,k_2)) = \theta(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1h_1h_2k_2 = \theta(h_1,k_1)\theta(h_2,k_2)$$

and thus θ is a homomorphism. The image of θ has both H and K as subsets, but since HK is generated by these, θ must be onto.

Finally, θ is 1-to-1 for if $\theta(h,k) = 1$ then $hk = 1$ so $h = k^{-1}$. But then $k^{-1} \in H$ and certainly $k^{-1} \in K$, contradicting $H \cap K = \{1\}$. Thus θ is indeed 1-to-1 and so is the required isomorphism. □

In this case HK is said to be an interal direct product, whereas $H \times K$ is the external direct product. The product is semi-direct if only one of H and K is normal in G, though the condition that $H \cap K = \{1_G\}$ is still required.

The semidirect product also has an 'external' interpretation. Let H and K be groups and that there is an action of H on K that preserves the group structure of K so that for any $x \in H$ the mapping $k \mapsto x(k)$ is an automorphism of K. LEt

$$G = \{(u,x) \mid u \in K, x \in H\}$$

and define a binary operation on G by

$$(u,x)(v,y) = (ux^{-1}(v), xy)$$

This product can be shown to be assoiative, and clearly $(1_K, 1_H)$ is the identity. Also,

$$(u,x)^{-1} = ((x(u))^{-1}, x^{-1})$$

and clearly G has subgoups isomorphic to H and to K,

$$H^* = \{(1_K, x) \mid x \in H\}$$
$$K^* = \{(u, 1_H) \mid u \in K\}$$

Clearly $G = H^*K^*$ and $H^* \cap K^* = (1,1)$. Furthermore, if $K^* \trianglelefteq G$ then H^* acts on K^* by conjugation in the same way that H acts on K.

(32.2) The General Linear Group

(32.2.1) Elementary Abelian Groups

First of all, an alternative definition of a field.

Definition 13 *F is a field if*

1. $(F, 0, -, +)$ *is an abelian group.*
2. $(F^\times, 1, i, \times)$ *is an abelian group. Extend the operation* $\times$ *so that* $0 \times x = 0$ *for all* $x \in G$.
3. *The permutation* $\phi_x \colon F \to F$ *defined by* $\phi_x \colon y \mapsto xy$ *is a group homomorphism for* $(F, 0, -, +)$.

The third property here is a rather convoluted statement of the distributivity property, namely $x(y+z) = xy + xz$.

Perhaps the field of most interest is the integers modulo p for some fixed prime p. This will be denoted $\mathbb{Z}_p$.

Definition 14 *Let G be a group.*

1. *The exponent of G is the least positive integer n such that* $x^n = 1_g$ *for all* $x \in G$.
2. *G is called elementary abelian if G is abelian and the exponent of G is prime.*
3. *G is a p-group if the order of every element of G is a power of the prime p.*
4. *G is an elementary abelian p-group if the order of every element of G divides p (i.e. is 1 or p).*

Note that when G is finite, the exponent of G divides the order of G. Also, the order of the identiry is just 1, hence the apparently odd definition of an elementary abelian p-group. An easy way to make an elementary abelian p-group is to take an abelian group G and form $\frac{G}{pG}$. (It is easy to show that $pG \trianglelefteq G$.)

As interest lies in the general linear group, it is not supprising that matrices with entries from $\mathbb{Z}_p$ will be under consideration. Note, however, than an equivalent way to think of such matrices is to define equivalence $\sim$ with $A \sim B$ if and only if $A - B = pC$ for some matrix C.

(32.2.2) Vector Spaces

Definition 15 *A vector space over the field F is an abelian group* $(V, 0, +, -)$ *together with an action of* $(F, +)$ *on* $(V, +)$ *as a group that restricts to an action of* $(F^\times, \times)$ *on V as a set.*

At this point it is useful to clarify some notation.

- The binary operation of abelian groups will be denoted using additive notation, so that for $g, h \in G$ the 'product' of g and h is written $g + h$.
- Extending the additive notation, if g is operated with itself n times, write ng.
- Elements of the finite field $\mathbb{Z}_p$ will be denoted $[n]$ for $n \in \mathbb{Z}$.

Theorem 16 *Let V be an elementary abelian p-group. Then there exists a unique action of $\mathbb{Z}_p$ on V which makes V into a vector space. Furthermore, if also W is an elementary abelian p-group then a function* $\theta \colon V \to W$ *is linear if and only if θ is a homomorphism of the groups V and W.*

Proof. First of all, define the action of $(F,+)$ on $(V,+)$ by

$$[n]\mathbf{v} \mapsto n\mathbf{v}$$

This is well-defined as if $[n]=[m]$ then $n=m+kp$ for some $k\in\mathbb{Z}$. Then

$$[n]\mathbf{v}=n\mathbf{v}=m\mathbf{v}+k(p\mathbf{v})=m\mathbf{v}=[m]\mathbf{v}$$

Showing that V is a vector space is now merely a case of verifying the axioms.

For the second part of the theorem, trivially any linear map between V and W restricts to a homomorphism between the underlying abelian groups. Conversely, if θ is a group homomorphism then

$$\theta([n]\mathbf{v})=\theta(n\mathbf{v})=n\theta(\mathbf{v})=[n]\theta(\mathbf{v})$$

and thus θ is a linear map. □

Definition 17 *Let* $\mathrm{GL}\,(n,p)$ *be the set of invertible* $n\times n$ *matrices with entries from* $\mathbb{Z}_p$*. With the binary operation of matrix multiplication this is the general linear group.*

Observe that $\det\colon \mathrm{GL}\,(n,p)\to\mathbb{Z}_p^\times$ is a group homomorphism, and that

$$\det A=\sum_{\sigma\in S_n}(-1)^\sigma\prod_{i=1}^{n}A_{i\sigma(i)}$$

Definition 18 *Define the special linear group,* $\mathrm{SL}(n,p)$ *to be*

$$\mathrm{SL}(n,p)=\ker\left(\det\colon \mathrm{GL}\,(n,p)\to\mathbb{Z}_p^\times\right)$$

that is, the matrices whose determinant is 1.

Theorem 19 *The order of* $\mathrm{GL}\,(n,p)$ *is* $\prod_{i=0}^{n-1}p^n-p^i$

Proof. The order of $\mathrm{GL}\,(n,p)$ is the number of $n\times n$ matrices whose columns are linearly independent. Choosing columns one by one where $\mathbf{a}_i$ denotes the ith column:

- The first column can be anything except $\mathbf{0}$. There are p^n-1 such vectors.
- The second column can be anything in $\mathrm{GL}\,(n,P)\setminus\mathrm{Span}\,\{\mathbf{a}_1\}$. Now, $\mathrm{Span}\,\{\mathbf{a}_1\}$ consists of all scalar multiples of $\mathbf{a}_1$ of which there are p, including the zero vector. Thus there are p^n-p choices for $\mathbf{a}_2$.
- $\vdots$
- Suppose that $\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_k$ have been chosen. Then the $(k+1)$th column must be chosen from $\mathrm{GL}\,(n,p)\setminus W$ where $W=\mathrm{Span}\,\{\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_k\}$. But $|W|=p^k$ and so there are p^n-p^k choices for $\mathbf{a}_{k+1}$.

Alltogether ther number of possible matrices is $(p^n-1)(p^n-p)\ldots(p^n-p^{n-1})$. □

Corollary 20 $|\mathrm{SL}(n,p)|=\dfrac{1}{p-1}\prod_{i=0}^{n-1}p^n-p^i$

Theorem 21 *The centre of* $\mathrm{GL}\,(n,p)$ *is the set of scalar matrices* Z*. Moreover, the centre of* $\mathrm{SL}(n,p)$ *is* $Z\cap\mathrm{SL}(n,p)$*.*

Proof. Let $G = \mathrm{GL}\,(n, p)$ and let $M \in G$. Let $E(i, j)$ be the identity matrix with an additional 1 in the (i, j) position ($i \neq j$). If M is central in G then M must commute with each of the $E(i, j)$ for $1 \leqslant i < j \leqslant n$. By commutativity

$$(E(i, j)M)_{ii} = (M)_{ii} + (M)_{ji} = (ME(i, j))_{ii} = (M)_{ii} \tag{22}$$

$$(E(i, j)M)_{ij} = (M)_{ij} + (M)_{jj} = (ME(i, j))_{ij} = (M)_{ii} + (M)_{ij} \tag{23}$$

From (22) it is clear that $(M)_{ji} = 0$ for all $1 \leqslant i < j \leqslant n$, so that M must be upper triangular. Repeating the argument with $E(j, i)$ shows that M must also be lower triangular, so that in fact M must be diagonal. Furthermore, (23) shows that M must be a scalar matrix, and thus Z is precisely the centre of G. □

Definition 24 *The projective general linear group is*

$$\mathrm{PGL}(n, p) = \frac{\mathrm{GL}\,(n, p)}{Z}$$

Similarly for the projective special linear group.

In particular, the projective special linear group is isomorphic to a normal subgroup of the projective general linear group.

(32.2.3) Important Subgroups Of $\mathrm{GL}\,(n, n)$

Definition 25 *Define the following subsets of* $\mathrm{GL}\,(n, p)$*:*

- *Let W be the set of permutation matrices, this is called the Weyl group. Each row(column) contains precisely one 1.*
- *Let $\mathcal{B}$ be the set of upper triangular matrices which are invertible (and so all diagonal entries are non-zero). This is the standard Borel group.*
- *Let T be the set of (invertible) diagonal matrtices. This is called the standard torus.*
- *Let U be the set of unitriangular matrices i.e. upper triangular matrices with all diagonal entries equal to 1. This is the unipotent group.*

Lemma 26 $W \cong S_n$ *with* $A \mapsto \sigma \;\Leftrightarrow\; A\mathbf{e}_i = \mathbf{e}_j$ *where* $\sigma(i) = j$.

Proof. Let θ be the described map. Let $\theta(A) = \sigma$ and $\theta(B) = \tau$. Then

$$(AB)\mathbf{e}_i = A\mathbf{e}_{\tau(i)} = \mathbf{e}_{\sigma(\tau(i))}$$

meaning that $\theta(AB) = \sigma\tau = \theta(A)\theta(B)$ i.e. θ is a homomorphism. Trivially θ is onto, and θ is 1-to-1 since $\ker\theta = \{I_n\}$. Hence θ is an isomorphism. □

Theorem 27 $\mathcal{B}$*, T, and U are all subgroups of* $\mathrm{GL}\,(n, p)$*, and* $\mathcal{B} \cong U \rtimes T$.

Proof. As $\mathrm{GL}\,(n, p)$ is finite, it is sufficient to show that $\mathcal{B}$ adn T are non-empty and closed under multiplication. As I_n is in both $\mathcal{B}$ and T, they are certainly non-empty.

Let $X, Y \in \mathcal{B}$ then $(X)_{ij} = 0 = (Y)_{ij}$ for $i > j$. Now,

$$(XY)_{ik} = \sum_{j=1}^{n} (X)_{ij}(Y)_{jk}$$

Suppose $i > k$

- If $j > k$ then$(Y)_{jk} = 0$ and there is no contribution to the sum.
- If $j < k$ then $i > j$ and so $(X)_{ij} = 0$ and once again there is no contribution to the sum.

Hence for $i > k$, $(XY)_{ik} = 0$ meaning that XY is upper triangular. Thus $\mathcal{B}$ is closed under multiplication, and so $\mathcal{B} \leqslant \mathrm{GL}\,(n, p)$.

To show that $T \leqslant \mathrm{GL}\,(n, p)$ consider the homomorphism

$$\theta\colon B \to T \quad \text{defined by} \quad \theta\colon (A)_{ij} \mapsto \begin{cases} (A)_{ij} & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Hence $\operatorname{Im}\theta = T$ and $\ker\theta = U$.

Now, clearly $U \cap T = \{I_n\}$, $U \trianglelefteq \mathcal{B}$ (because U is the kernel of a homomorphism), and as T is the image of the same homomorphism the conditions are met for $\mathcal{B}$ to be the semi-direct product of T and U, *i.e.*, $\mathcal{B} = U \rtimes T$. □

(32.2.4) Generators

It is of interest to find generators for the variuos subgroups of $\mathrm{GL}\,(n, p)$, and of course for $\mathrm{GL}\,(n, p)$ itself. The aim of this section is to show that $\mathrm{GL}\,(n, p) = \mathcal{B}W\mathcal{B}$ and that this is a disjoint union of the double cosets

$$\mathcal{B}w\mathcal{B} = \{B_1 w B_2 \mid B_1, B_2 \in \mathcal{B}\}$$

Definition 28 *An upper row reduction (or upper transvection) ρ is a row reduction whose correpsonding (elementary) matrix E lies in $\mathcal{B}$, i.e. is upper triangular.*

The action of ρ on a matrix A by its matrix E is on the left, so $\rho(A) = EA$. These operations can be used to scale a row of A by a non-zero factor, or to add a multiple of a row to another row.

Lemma 29 *The group U of unitriangular matrices is generated by the upper row reductions, i.e. any unitriangular matrix is a product of (finitely many) upper row reductions.*

Proof. If $n = 1$ then there is only 1 unitriangular matrix, (1), and there is nothing to show.

Suppose that $n > 1$ and that the result holds for dimensions lesser than n. Let $E(i, j, \lambda)$ denote the upper row reduction of adding λ times row j to row i. Thus

$$E(i, j, \lambda) = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & \lambda & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}$$

where the λ is in position (i, j) and $i \neq j$. Let A be any $n \times n$ unitriangular matrix, and let A' be the $(n-1) \times (n-1)$ matrix obtained from A be deleting row n and column n. By induction there is a sequence of upper row reductions that takes I_{n-1} to A_1 as in equation (30). For each of these row reductions append a new bottom row and new last column that are all zero except for a 1 in the (n, n) position. Then these are again upper row reductions which take I_n to the form

$$A_1 = \begin{pmatrix} & & & \lambda_1 \\ & & & \lambda_2 \\ & A' & & \vdots \\ & & & \lambda_{n-1} \\ 0\ 0 & \dots & 0 & 1 \end{pmatrix} \tag{30}$$

where A' is unitriangular and $\lambda_1 = \lambda_2 = \cdots = 0$. To form an arbitrary unitriangular matrix apply the row operations

$$P = \prod_{i=1}^{n-1} E(i, n, \lambda_i)$$

Then $A = PA_1$ and the result is shown. □

Corollary 31 *$\mathcal{B}$ is generated by the invertible diagonal matrices (T), and the upper row reductions.*

Proof. By Theorem 27 $\mathcal{B} = U \rtimes T$ and so by Lemma 29 $\mathcal{B}$ is generated by the upper row reductions and the invertible invertible diagonal matrices. □

Lemma 32 *W is generated by the elementary row transpositions.*

Proof. A transposition is a product of adjacent transpositions. □

Lemma 33 *Let A be an invertible $n \times n$ matrix. There is a sequence if upper elementary row operations which reduces A to a matrix C with the following property:*

For each column i there is a row $\pi(i)$ whose first $i - 1$ entries are zero and whose ith entry is non-zero. (34)

Proof. An algorithm for the production of C from A is exhibited.

1. Consider the first column of A. It is not the zero vector since A is invertible. Let i be the row of the last non-zero entry in this column.
2. Multiply row i by $\frac{1}{(A)_{i1}}$ then the last non-zero entry of column 1 is 1 *i.e.*, pre-multiply by $E(i, i, \frac{1}{(A)_{ii})}$.
3. For $1 \leqslant j < i$, add $-(A)_{j1} \times$ row i to row j then column 1 becomes $\mathbf{e}_i$. This may be achieved by pre-multiplying by $E(j, i, -(A)_{j1})$ for $1 \leqslant j < i$. Denote this new matrix by A'.
4. Delete column 1 and row i from A' to give an $(n-1) \times (n-1)$ matrix X. By induction there is a sequence of elementary row operation which transforms X to a matrix X' with property (34).
5. To each of these elementary row operations insert a new first column and new ith row (so that the old row i becomes row $i + 1$) whose ehtries are all zero except for a 1 in the (new) (i, i) position. These operations transform A' to the required matrix C. □

Lemma 35 *Let $\pi, w \in W$ and let $B \in \mathcal{B}$. If $\pi B w \in \mathcal{B}$ then $\pi w = I_n$.*

Proof. By induction on n, the size of the matrix, if $n = 1$ then $\pi = w = B = (1)$ and the result is trivial.

Suppose $n > 1$ and let w have a 1 in column j of row 1, so $w(1) = j$. Note that since w is a permutation matrix it has precisely one 1 in every row and column with all other entries zero. Consider column j of Bw:

- Since $(B)_{11} \neq 0$ and $(w)_{1j} = 1$, $(Bw)_{1j}$ is non-zero.
- Since $(w)_{ij} = 0$ for $i > 1$ and $(B)_{i1} = 0$ for $i > 1$, $(Bw)_{ij} = 0$ for $i > 1$.

Consider now column j of $\pi(Bw)$. Since π is a permutation matrix, this column must be simply a re-arrangement of the elements of column j of Bw. But $\pi B w$ is a product of invertible matrices, and so is invertible. By hypothesis $\pi B w$ is upper triangular and so since column j has only one non-zero element it must be in position (j, j). Therefore π sends row 1 to row j.

Now delete row 1 and column j from both π and w, and delete row 1 abd column 1 from B to give π', w', and B'. By induction $\pi' w' = I_{n-1}$ and so $\pi w = I_n$. □

Corollary 36 *If π and w are distict permutation matrices then $\mathcal{B}\pi\mathcal{B} \cap \mathcal{B}w\mathcal{B} = \emptyset$.*

Proof. Suppse that $B_1\pi B_2 = B_3 w B_4$, then $B_3^{-1}B_1 = wB_4B_2^{-1}\pi^{-1}$. Hence by Lemma 35 $w\pi^{-1} = I_n$. □

Corollary 37 $\mathrm{GL}\,(n, p) = \mathcal{B}W\mathcal{B}$.

Proof. By Lemma 33 there is a sequence of upper elementary row operations that reduces any matrix $C \in \mathrm{GL}\,(n, p)$ to the form wB for some $w \in W$. But a product of upper elementary row operations gives an upper triangular matrix, and so if B' is the inverse of this then $C = B'wB$. □

(32.3) Local Theory

(32.3.1) p-groups

Throughout this section it will be assumed that p is a fixed prime.

Definition 38 *Let p be a prime and n be a positive integer that is not divisible by p. Then where $n = p^k m$, p^k is called the p-local part of n.*

Definition 39 *Let G be a group and $x \in G$. x is a p-element if and only if the order of x is a power of p.*

Definition 40 *A group G is a p-group if and only if all elements of G are p-elements.*

Lemma 41 (Cauchy) *Let G be a group and $p \mid |G|$. Then G has an element of order p.*

Proof. Let Ω be the set of products $x_1 x_2 \ldots x_p$ of elements of G such that $x_1 x_2 \ldots x_p = 1_G$. Now, $|\Omega| = |G|^{p-1}$ because the first $p - 1$ elements of any product can be chosen at will, while the final element must be the inverse of the product of $p - 1$ elements.

Sonsider the action of C_p on Ω. The generator of C_p, $1 + p\mathbb{Z}$, sends $x_1 x_2 \ldots n_p$ to $x_2 x_3 \ldots x_p x_1$ from which it is evident that every orbit is either a fixed point or a cycle of length p. But a fixed point must be a product of the form $x_1 x_1 \ldots x_1$ meaning that x_1 has order p—if any fixed points exist.

Now, Ω is a disjoint union of its orbits, and since each not-fixed point must be in an orbit of cardinality a power of p (by the Orbit-Stabiliser theorem) and so

$$\text{number of fixed points} \equiv |\Omega| \mod p = 0 \mod p$$

But 1_G is a fixed point, and so there must exist at least $p - 1$ others, say $x^p = 1_G$. As p is prime this means that x has order p. □

Corollary 42 *G is a finite p-group if and only if $|G|$ is a power of p.*

Proof. ($\Rightarrow$) Using the contrapositive, suppose that $|G|$ is not a power of p, then there is a prime $q \neq p$ such that $q \mid |G|$, and so by Lemma 41 G has an element of order q. Hence G is not a p-group.

($\Leftarrow$) Following from Lagrange's Theorem, if $x \in G$ then $o(x) \mid |G|$. But G is a power of a prime, thus so must $o(x)$ be. □

Thw following result uses an argument similar to that of Lemma 41.

Theorem 43 *If G is a non-trivial p-group then $Z(G)$ is non-trivial.*

Proof. Let G act on itself by conjugation, so $g \cdot x = gxg^{-1}$. Now, G is a disjoint union of its conjugacy classes which in this case are the orbits of the action. Furthermore, by the Orbit-Stabiliser theorem the cardinality of each orbit must divide $|G|$ (and thus be a power of p). Hence if there is 1 fixed point, there must be at least $p-1$ more.

As 1_G is a fixed point, there are at least $p-1$ more. Let x be one of these fixed points, then $gxg^{-1} = x$ $\forall g \in G$, *i.e.*, $xg = gx$ $\forall g \in G$ and thus $1_G \neq x \in Z(G)$. □

Lemma 44 (Not Burnside's Lemma) *Let G be a finite group acting on a set X. If G has t orbits on X then*

$$t = \sum_{g\in G} |\operatorname{fix} g|$$

Proof. Consider the set $E = \{(g,x) \in G \times X \mid x \in \operatorname{fix} g\}$ then

$$\begin{aligned} \operatorname{fix} g &= \{x \in X \mid (g,x) \in E\} \\ \operatorname{stab}_G(x) &= \{g \in G \mid (g,x) \in E\} \end{aligned}$$

Hence

$$\sum_{g\in G} |\operatorname{fix} g| = \sum_{x\in X} |\operatorname{stab}_G(x)|$$

Let $x_1, x_2, \ldots, x_t$ representatives of the orbits $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_t$, then if x is in the same orbit as x_i there exists $g \in G$ such that $g(x) = x_i$ and therefore

$$g^{-1}(\operatorname{stab}_G(x_i))g = \operatorname{stab}_G(x)$$

so $|\operatorname{stab}_G(x)| = |\operatorname{stab}_G(x_i)|$. Hence

$$\begin{aligned} \sum_{g\in G} |\operatorname{fix} g| &= \sum_{i=1}^{t} \sum_{x\in\mathcal{O}_i} |\operatorname{stab}_G(x)| \\ &= \sum_{i=1}^{t} |\mathcal{O}_i||\operatorname{stab}_G(x_i)| \\ &= \sum_{i=1}^{t} |G| \quad \text{by the orbit-stabiliser theorem} \\ &= t|G| \end{aligned}$$

□

(32.3.2) Sylow Subgroups

Definition 45 *Let G be a finite group of order $|G| = p^k m$ where p is prime and $p \nmid m$. Let H be a p-subgroup of G, then H is a Sylow p-subgroup if and only if $|H| = p^k$.*

Lemma 46 $\dbinom{p^k m}{p^k} = m \mod p$.

Proof. Let $G = \Pi_{p^k m}$ and $H = \Pi_{p^k}$ so $H \leqslant G$. Let

$$\Omega = \{X \subseteq G \mid |X| = p^k\}$$

then H acts on Ω by multiplication on the elements of some X thus producing a different element of Ω. Now, Ω is a disjoint union of its orbits under H, and by the Orbit Stabiliser Theorem the cardinality of each of these orbits must divide $|H| = p^k$. Now, fix H is the set of all fixed points. By the Orbit-Stabiliser theorem the cardinality of all orbits under the action of H must divide $|H| = p^k$ and hence

$$|\Omega| \equiv |\operatorname{fix} H| \mod p \tag{47}$$

Claim that X is fixed by H if and only if $X = Hx$ for some $x \in G$.

- ($\Rightarrow$) Suppose that $X \in \Omega$ is fixed by H, then $\forall h \in H\ \forall x \in X\ hx \in X$. Therefore $Hx \subseteq X$ for chosen $x \in X$. But $|Hx| = |H| = p^k = |X|$ and therefore $Hx = X$.
- ($\Leftarrow$) If $X = Hx$ then for any $h \in H$ and $y \in X$, $y = h'x$ for some $h' \in H$ and therefore $hy = hh'x = h''x \in Hx = X$ and so X is fixed by H.

Thus the number of fixed points in Ω is equal to the number of cosets of H in G, namely

$$\frac{|G|}{|H|} = \frac{p^k m}{p^k} = m$$

Now, $|\Omega| = \binom{p^k m}{p^k}$ and hence by equation (47) the result is shown. □

(32.3.3) Sylow's Theorem

Theorem 48 (Sylow) *Let G be a group of order $p^a m$ where p is prime and $p \nmid m$. Then*

1. *G has a Sylow p-subgroup, H say.*
2. *If G has k Sylow p-subgroups then $k \equiv 1 \mod p$.*
3. *K is a Sylow p-subgroup of G if and only if $K = gHg^{-1}$ for some $g \in G$.*
4. *If G has k Sylow p-subgroups then $k \,|\, m$.*

Proof. Let $\Omega = \{X \subseteq G \mid |X| = p^a\}$ then G acts on Ω by translation.

1. By Lemma 46, $|\Omega| = \binom{p^a m}{p^a} \equiv m \mod p$. Since Ω is a disjoint union of its orbits, there must be at least one orbit, $\mathcal{O}$ say, for which $p \nmid |\mathcal{O}|$. Let $X \in \mathcal{O}$ and $1_G \in X$, and let $H = \operatorname{stab}_G(X)$.
   By the Orbit Stabiliser Theorem $|\mathcal{O}| = \left|\frac{G}{H}\right|$. But $p \nmid |\mathcal{O}|$ and $p^a \,|\, G$, therefore $p^a \,|\, |H|$ so that $|H| \geqslant p^a$.
   On the other hand, if $h \in H = \operatorname{stab}_G(X)$ then since $1_G \in X$, $h = h1_G \in hX = X$ and hence $|H| \subseteq |X| = p^a$.
   By the preceeding two paragraphs, $|H| = p^a$ and thus G does indeed have a Sylow p-subgroup.
2. From above given an orbit $\mathcal{O}$ such that $p \nmid |\mathcal{O}|$ a Sylow p-subgroup can be constructed: namely the stabiliser of $X \in \mathcal{O}$ with $1_G \in X$. Now, $H \subseteq X$, but since $|H| = p^a$, $H = X$. Hence

   $$g \cdot X = \{gh \mid h \in X\} = \{gh \mid h \in H\} = gH$$

   so $\mathcal{O} = \frac{G}{H}$.
   However, if H is a Sylpw p-subgroup then $\left|\frac{G}{H}\right| = m$ and is an orbit in Ω (whose cardinality is indivisible by p). But then this orbit gives rise to a Sylow p-subgroup, which must be H. Hence there is a bijection

   $$\{\text{Sylow } p\text{-subgroups}\} \leftrightarrow \{\text{Orbits in } \Omega \text{ with cardinality indivisible by } p\} \tag{49}$$

Thus Sylow p-subgroups may be counted by counting the orbits in Ω with cardinlaity not divisible by p.

$$\begin{aligned}
|\Omega| &= \sum_{\text{all orbits, } \mathcal{O}} |\mathcal{O}| \\
&\equiv \sum_{\{\mathcal{O} | p \nmid |\mathcal{O}|\}} |\mathcal{O}| \mod p \\
&\equiv \sum_{\{\mathcal{O} | p \nmid |\mathcal{O}|\}} m \mod p \\
&\equiv km \mod p
\end{aligned}$$

where there are k orbits of cardinality indivisible by p, and thus by equation (49), there are k Sylow p-subgroups. But by Lemma 46 $\Omega \equiv m \mod p$,

$$\begin{aligned}
\text{so } km &\equiv m \mod p \\
\text{so } k &\equiv 1 \mod p
\end{aligned}$$

as required.

3. Let H be the Sylow p-subgroup constructed above, and let K be another Sylow p-subgroup. Now, K may act on $\frac{G}{H}$ by $gH \mapsto kgH$. Let

$$F = \text{fix}_{\frac{G}{H}}(K) = \left\{ gH \in \frac{G}{H} \mid kgH = gH \; \forall k \in K \right\}$$

Now, $\frac{G}{H}$ is a disjoint union of K-orbits and the cardinality of each orbit must (by the Orbit Stabiliser Theorem) divide $|K| = p^a$. But $p \nmid m = \left|\frac{G}{H}\right|$ and therefore F is non-empty and

$$m = |\mathcal{O}| \equiv \left| \text{fix}_{\frac{G}{H}}(K) \right| \mod p$$

Suppose $gH \in F$ then

$$\begin{aligned}
kgH &= gH \; \forall k \in K \\
\Leftrightarrow \; k(gHg^{-1}) &= gHg^{-1} \; \forall k \in K \\
\Leftrightarrow \; k &\in gHg^{-1} \; \forall k \in K
\end{aligned}$$

Hence $K \leqslant gHg^{-1}$. But $|K| = |gHg^{-1}| = p^a$ and so K is a conjugate of H. As K was any Sylow p-subgroup, all Sylow p-subgroups are conjugate.

4. G acts transitively (by conjugation) on its Sylow p-subgroups and hence by the Orbit-Stabiliser theorem $k \,|\, |G|$. But $|G| = p^a m$ and $k \equiv 1 \mod p$ therefore $k \nmid p$ and hence $k \,|\, m$. □

(32.3.4) Applications Of Sylow's Theorem

Example 50 *Let p and q be primes with $p < q$. If G is a group of order pq then $G \cong C_p \rtimes C_q$. Furthermore, if $q \not\equiv 1 \mod p$ then $G \cong C_{pq}$*

Proof. Solution Let G be a group of order pq, let N be a Sylow p-subgroup, and H be a Sylow q-subgroup. Then $|N| = p$ and $|H| = q$ and so both groups are cyclic.

Let $x \in N \cap H$, then $o(x)$ is a power of p, and is a power of q too. Since p and q are different primes, $x = 1_G$

and hence $N \cap H = \{1_G\}$.

Since $N \cap H = \{1_G\}$, $NH = \{nh \mid n \in N, h \in H\}$ is a set of pq distinct elements. But $NH \subseteq G$, so since $|NH| = |G|$, $NH = G$, *i.e.*, $G = \langle N, H \rangle$.

Let k_p and k_q be the numbers of Sylow p- and q-subgroups respectively. Now, by Theorem 48 (Sylow) $k_q \mid p$, so $k_q = 1$ or $k_q = p$.

By Theorem 48 (Sylow), $k_q \equiv 1 \mod q$, so if $k_q = p$ then $p = 1 + kq$ for some $k \in \mathbb{N}$, which contradicts that $p < q$. Therefore $k_q = 1$.

By Theorem 48 (Sylow), all Sylow q-subgroups are conjugate and thefore since $k_q = 1$, $N \trianglelefteq G$. Hence since $G = \langle N, H \rangle$ and $N \cap H = \{1_G\}$ the conditions are met for $G \cong N \rtimes H$.

Consider now k_p and by hypothgesis, assume that $q \not\equiv 1 \mod p$. By Theorem 48 (Sylow) $k_p \mid q$ and $k_p \equiv 1 \mod p$ and therefore $k_p = 1$ or $k_p = q$. To avoid a contradiction $k_p = 1$ so that $H \trianglelefteq G$ and hence $G \cong H \times N \cong C_p \times C_q \cong C_{pq}$. □

Example 51 *If p and q are distinct primes then there is no simple group of order p^2q.*

Proof. Solution Suppose that G is a simple group of order p^2q and consider the Sylow p- and q-subgroups of G, say they number k_p and k_q repectively.

By Theorem 48 (Sylow) $k_p \mid q$. Since G is simple this gives $k_p = q$. Also,

$$q = k_p \equiv 1 \mod p \;\Rightarrow\; q > p \tag{52}$$

Similarly, $k_q \mid p^2$ and $k_q \equiv 1 \mod q$

- If $k_q = 1$ then G is not simple, a contradiction, so $k_q \neq 1$.
- If $k_q = p$ then it is required that $p \equiv 1 \mod q$ and therefore $p > q$, in contradiction with observation 52). Hence $k_q \neq p$¿
- If $k_q = p^2$ then it is required that $p^2 \equiv 1 \mod q$ and so $q \mid p^2 - 1 = (p+1)(p-1)$. By observation (52) $q = p + 1$ and hence $q = 3$ and $p = 2$.

Let G be a group of order $12 = 2^2 3$ then the number of Sylow 2-subgroups, k say, must satisfy $k \mid 3$ and $k \equiv 1 \mod 2$. Therefore $k = 1$ and thus the Sylow 2-subgroup of G is normal in G, the contradiction required to complete the proof. □

Example 53 *A finite group of order p^2 is Abelian.*

Proof. Let G have order p^2, then G is a p-group and so has non-trivial centre, Z say. By Lagrange's Theorem, either $Z = G$ or $|Z| = p$. In the former case the result is trivial.

Suppose that $|Z| = p$, then $\left|\frac{G}{Z}\right| = p$ and so is cyclic. Say $\frac{G}{Z}$ is generated by xZ for some $x \in G$ then the elements of G must be of the form $x^i y$ whence said element lies in the coset $x^i Z$ and $y \in Z$. Take another such element, $x^j z$ say, then

$$(x^i y)(x^j z) = x^{i+j} yz = (x^j z)(x^i y)$$

and thus G is Abelian. But this is a contradiction, since were G Abelian, $Z(G) = G$ and in this case $|Z| = p < |G| = p^2$. Hence the former case, $Z = G$ must hold *i.e.*, G is Abelian. □

Definition 54 *Let $x \in \mathbb{N}$. Define $\mathrm{ord}_p x$ to be the number of times p appears in the prime factorisation of x.*

Theorem 55 *Let G be a finite group, $N \trianglelefteq G$, and Q be a Sylow p-subgroup of G. Then*

1. *$\frac{QN}{N}$ is a Sylow p-subgroup of $\frac{G}{N}$.*
2. *$Q \cap N$ is a Sylow p-subgroup of N.*

Proof. 1. By Corollary 7 (First Isomorphism Theorem) $\frac{QN}{N} \cong \frac{Q}{Q\cap N}$. Now,

$$\left|\frac{QN}{N}\right| = \left|\frac{Q}{Q\cap N}\right| = \frac{|Q|}{|Q\cap N|}$$

Since $|Q|$ is a power of p and by Lagrange's Theorem $|Q \cap N| \mid |Q|$, $\left|\frac{QN}{Q}\right|$ is also a power of p and thus is a p-group.

Now, $Q \leqslant QN \leqslant G$ so by Lagrange's Theorem $|Q| \mid |QN|$ and $|QN| \mid |G|$. As Q is a Sylow p-subgroup of G, $\mathrm{ord}_p(|Q|) = \mathrm{ord}_p(|G|)$ and therefore $\mathrm{ord}_p(|QN|) = \mathrm{ord}_p(|G|)$. So

$$\begin{aligned}
\mathrm{ord}_p\left(\left|\frac{QN}{N}\right|\right) &= \mathrm{ord}_p\left(\frac{|QN|}{|N|}\right) \\
&= \mathrm{ord}_p(|QN|) - \mathrm{ord}_p(|N|) \\
&= \mathrm{ord}_p(|G|) - \mathrm{ord}_p(|N|) \qquad (56) \\
&= \mathrm{ord}_p\left(\left|\frac{G}{N}\right|\right)
\end{aligned}$$

and hence $\frac{QN}{N}$ is a Sylow p-subgroup of $\frac{G}{N}$.

2. By Corollary 7 (First Isomorphism Theorem) and equation (56) above,

$$\mathrm{ord}_p\left(\left|\frac{Q}{Q\cap N}\right|\right) = \mathrm{ord}_p(|G|) - \mathrm{ord}_p(|N|) \qquad (57)$$

But also

$$\begin{aligned}
\mathrm{ord}_p\left(\left|\frac{Q}{Q\cap N}\right|\right) &= \mathrm{ord}_p(|Q|) - \mathrm{ord}_p(|Q\cap N|) \\
&= \mathrm{ord}_p(|G|) - \mathrm{ord}_p(|Q\cap N|) \qquad (58)
\end{aligned}$$

Thus equating equation (57) with equation (58) gives

$$\mathrm{ord}_p(|N|) = \mathrm{ord}_p(|Q\cap N|)$$

and hence $Q \cap N$ is a Sylow p-subgroup of N. □

(32.3.5) The Frattini Argument

Theorem 59 (Frattini Argument) *Let G be a finite group and $N \trianglelefteq G$. Let P be a Sylow p-subgroup of N, then $G = N_G(P)N$.*

Proof. Let Ω be the set of Sylow p-subgroups of N. If $Q \in \Omega$ and $g \in G$ then since N is normal and $Q \leqslant N$, $gQg^{-1} \leqslant N$. But $|gQg^{-1}| = |Q|$ and thus $gQg^{-1} \in \Omega$ for all $g \in G$. Thus G acts on Ω by conjugation.

For any $P \in \Omega$ and $g \in G$ $gPg^{-1} \in \Omega$ but since all Sylow p-subgroups of N are N-conjugate, $\exists n \in N$ such that $n(gPg^{-1})n^{-1} = P$, so that $gn \in N_G(P)$. Thus $g \in NN_G(P)$ and since g was arbitrary, $G \subseteq NN_G(P)$. Certainly $NN_G(P) \subseteq G$ and thus the theorem is proven. □

(32.3.6) Nilpotent Groups

Definition 60 *A group G is nilpotent if and only if every Sylow subgroup of G is normal.*

The objective of this section is to arrive at the following equivalence.

$$G \text{ nilpotent} \overset{\text{Corollary 70}}{\Rightarrow} G \text{ has property } N \overset{\text{Theorem 71}}{\Rightarrow} (H \leqslant G \text{ maximal} \Rightarrow H \trianglelefteq G) \overset{\text{Theorem 63}}{\Rightarrow} G \text{ nilpotent}$$

Theorem 61 *A nilpotent group is a direct product of its Sylow subgroups.*

Proof. Let $|G| = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$ and let P_i be the Sylow j_i-subgroup, which is unique by nilpotency. Define

$$H_i = P_1 P_2 \dots P_i \quad \text{and} \quad H_0 = \{1_G\}$$

then trivially $H_0 \trianglelefteq G$. Suppose that $H_i \trianglelefteq G$ and consider forming H_{i+1}. Now,

$$|H_i| = p_1^{j_1} p_2^{j_2} \dots p_i^{j_i} \quad \text{and} \quad |P_{i+1}| = p_{i+1}^{j_{i+1}}$$

and both of these are coprime. Thus if $x \in H_i \cap P_{i+1}$ then $o(x)$ must be a divisor of both these *i.e.*, $o(x) = 1$ and thus $x = 1_G$ so that $H_i \cap P_{i+1} = \{1_G\}$. Hence by Lemma 12 $H_i P_{i+1}$ is a direct product and so by induction the result is shown. □

Theorem 62 *The Frattini subgroup of a finite group G,* $\Phi = \bigcap_{\substack{H \leqslant G \\ H \text{ maximal}}} H$ *is nilpotent.*

Proof. Let P be a Sylow p-subgroup of Φ and suppose that $N_G(P) \neq G$, then there is a maximal subgroup of G, H say, such that $N_G(P) \leqslant H$.

But by definition, $\Phi \leqslant H$ and thus $N_G(P)\Phi \leqslant H < G$. But by Theorem 59 (the Frattini argument) $N_G(P)\Phi = G$.

The proof now assumes that $\Phi \trianglelefteq G$, but this is not revealed until later?

□

Theorem 63 *Let G be a finite group such that every maximal subgroup is normal. Then G is nilpotent.*

Proof. Let P be a Sylow p-subgroup of G that is not normal. Then there exists a maximal subgroup, H say, such that $N_G(P) \leqslant H$. Now, P is also a Sylow p-subgrpup of H because $P \leqslant N_G(P) \leqslant H$ and by hypothesis $H \trianglelefteq G$ and hence by Theorem 59 (the Frattini argument) $G = N_G(P)H$.

However, $N_G(P) \leqslant H$ and thus $N_G(P)H = H$. But then from above $H = G$, which contradicts that H is a maximal normal subgroup of G. Thus $N_G(P) = G$ so that no maximal subgroup containing $N_G(P)$ can exist. □

Lemma 64 *If G is nilpotent and $H \leqslant G$ then H is nilpotent. Furthermore, if P is the Sylow p-subgroup of G then $H \cap P$ is the Sylow p-subgroup of H.*

Proof. Let Q be a Sylow p-subgroup of H, then Q is a p-subgroup of G and since all Sylow p-subgroups of G are conjugate, $\exists g \in G$ such that $Q \leqslant gPg^{-1}$, but by nilpotency $gPg^{-1} = P$ so that $Q \leqslant P$. Thus $Q \leqslant H \cap P$.

Now, $H \cap P$ is a p-subgroup of H, and thus $|H \cap P| \leqslant |Q|$. By above, $Q = H \cap P$.

But this can be done for any Sylow p-subgroup of H, and so $H \cap P$ must be the unique Sylow p-subgroup of H. □

Corollary 65 *Let G be nilpotent, so by Theorem 61 $G = P_1 P_2 \dots P_k$. Then the subgroups of G are the groups of the form $Q_1 Q_2 \dots Q_k$ for $Q_i \leqslant P_i$.*

Proof. Trivially, if $Q_i \leqslant P_i$ for $1 \leqslant i \leqslant k$ then $Q_1 Q_2 \dots Q_k \leqslant P$.

Converseley, if $H \leqslant G$ then by Lemma 64 H is also nilpotent and so by Theorem 61 is a product of its Sylow subgroups, which by Lemma 64 are subgroups of the Sylow subgroups of G. □

Definition 66 *Let G be a finite group and let $G_0 = G$. Define $G_{i+1} = \frac{G_i}{Z(G_i)}$. Define G to have property N if and only if $\exists n \in \mathbb{N}$ such that $G_n = \{1_G\}$.*

Theorem 67 *If G is a finite p-group then G has property N.*

Proof. If $|G| = 1$ then the result is trivial. Suppose that $|G| > 1$ and that the result holds for groups of smaller order. By Theorem 43 G has a non-trivial centre, Z say. But then $G_1 = \frac{G}{Z}$ is again a p-group and so by hypothesis has property N. But then G has property N. □

Lemma 68 *Let G be a finite nilpotent group with Sylow subgroups $P_1, P_2, \dots, P_k$. Then the centre of G is given by $Z_1 Z_2 \dots Z_k$ where $Z_i = Z(P_i)$.*

Proof. Let $z \in Z = Z(G)$, then z has an expression of the form $z = z_1 z_2 \dots z_k$ where $z_i \in P_i$. Then

$$z_i = z_{i-1}^{-1} z_{i-1}^{-1} \dots z_1^{-1} z z_k^{-1} z_{k-1}^{-1} \dots z_{i+1}^{-1} \tag{69}$$

Since G is formed as a direct product, the proof of Lemma 12 shows that if $g \in P_i$ then g commutes with elements of P_j for $j \neq i$. Since $z \in Z$, g commutes with z and thus by equation (69) g commutes with z_i. Hence $z \in Z_i = Z(P_i)$ and thus $Z \subseteq Z_1 Z_2 \dots Z_k$.

Converseley, let $z_i \in Z_i$ and $g \in G$. Then g has an expression $g = g_1 g_2 \dots g_k$ for $g_j \in P_j$. Once again by Lemma 12 z_i and g_j commute for $i \neq j$. Also, g_i and z_i commute becuase $z_i \in Z_i$. Thus g comutes with z_i and hence $Z_i \subseteq Z$. But then $Z_1 Z_2 \dots Z_k \subseteq Z$ and by above the result is shown. □

Corollary 70 *If G is a finite nilpotent group then G has property N.*

Proof. If $|G| = 1$ the result is trivial. Let G be a nilpotent group with $|G| > 1$ and suppose the result holds for groups of smaller order. By Lemma 68 the centre of G is a direct product of the centres of its Sylow subgroups, each of which is a p_i-group and so by Theorem 43 has a non-trivial centre. Hence the centre of G is non-trivial and thus by induction $G_1 = \frac{G}{Z(G)}$ has property N. □

Theorem 71 *Let G be a finite group that has property N. If H is a maximal subgroup of G then $H \trianglelefteq G$.*

Proof. If $|G| = 1$ then the result is trivial. Suppose that $|G| > 1$ and that the result holds for groups of smaller order. Let $Z = Z(G)$ and consider HZ. Since H is maximal, either $ZH = G$ or $HZ = H$.

- If $HZ = G$ observe that $H \subseteq N_G(H)$ and $Z \subseteq N_G(H)$ and therefore $G = HZ \subseteq N_G(H)$ so $G = N_G(H)$ which means that $H \trianglelefteq G$.
- If $HZ = H$ then $Z \subseteq H$. By Theorem 10 (Correspondence) $\frac{H}{Z}$ is maximal in $\frac{G}{Z}$ and thus by induction $\frac{H}{Z} \trianglelefteq \frac{G}{Z}$ but then applying Theorem 10 again gives $H \trianglelefteq G$.

Both cases are covered, so the result is shown. □

(32.4) Solubility

The merit of studying soluble groups is to reduce questions about a group G to questions about the groups N and $\frac{G}{N}$ for $N \trianglelefteq G$. As these are smaller groups, the questions should be simpler to answer. For example,

1. G is a p-group if and only if N and $\frac{G}{N}$ are both p-groups.
2. If $N \leqslant Z(G)$ then G is nilpotent if and only if $\frac{G}{N}$ is nilpotent.

Definition 72 *A normal series for a finite group G is a sequence of subgroups of G, $H_0, H_1, \ldots, H_k$ such that $H_0 = \{1_G\}$, $H_k = G$, $H_i \leqslant H_{i+1}$, and $H_i \trianglelefteq G$ for all i.*

Normal series are not particularly interesting. However, they are readily modified to provde more information about a group.

Definition 73 *A subnormal series for a finite group G is a sequence of sungroups of G, $H_0, H_1, \ldots, H_k$ such that $H_0 = \{1_G\}$, $H_k = G$, and $H_i \trianglelefteq H_{i+1}$.*

1. *The integer k is called the length of the series.*
2. *The quotient groups $\frac{H_{i+1}}{H_i}$ are called the factors of the series.*
3. *A subnormal series with simple factors is called a composition series.*

Note that the condition that the factors are simple is equivalent to requiring that H_i is a maximal normal subgroup of H_{i+1}. Note also that two subnormal series are equal if they have the same factors, which need not occur in the same order.

Theorem 74 *If G is a finite group, then G has a composition series.*

Proof. If $|G| = 1$ then the result is trivial. Suppose that $|G| > 1$ and that the result holds for groups of smaller order. Let X be the set of proper normal subgroups of G, then since G is finite so is X. X is non-empty for $\{1_G\} \in X$ and thus since X is finite it has an element N of maximal cardinality.

By induction, N has a composition series, $H_0, H_1, \ldots, H_k$ say, where $H_k = N$. But then $H_0, H_1, \ldots, H_k, G$ is a composition series for G. $\square$

Theorem 75 (Jordan-Hölder) *Let $H_0, H_1, \ldots, H_n$ and $K_0, K_1, \ldots, K_m$ be composition series for a group G. If S is any simple group then the number of factors $\frac{H_{i+1}}{H_i}$ isomorphic to S is equal to the number of factors $\frac{K_{i+1}}{K_i}$ isomorphic to S.*

Theorem 75 (Jordan-Hölder: Traditional Statement) *Let $H_0, H_1, \ldots, H_n$ and $K_0, K_1, \ldots, K_m$ be composition series for a group G. Then $n = m$ and there exists a permutation $\sigma \in S_n$ such that $\frac{H_{i+1}}{H_i} \cong \frac{K_{j+1}}{K_j}$ where $\sigma(i) = j$.*

Proof. If $|G| = 1$ the result is trivial. Let $|G| > 1$ and assume the result for groups of smaller order. Consider 2 composition series

$$H_0 < H_1 < \cdots < H_{n-1} < H_n = G \tag{76}$$

$$K_0 < K_1 < \cdots < K_{m-1} < K_m = G \tag{77}$$

Write $H = H_{n-1}$ and $K = K_{m-1}$ then H and K are both maximal proper normal subgroups of G. Consider HK which is again a normal subgroup of G, and $H \leqslant HK \leqslant G$ and thus either $HK = H$ or $HK = G$.

If $HK = H$ then $K \leqslant H$, but since H and K are both maximal and normal, this gives $H = K$. Furthermore, $|H| < |G|$ and so by induction the result holds for H. But then equations (76) and (77) are identical, *i.e.,* the result holds.

If $HK = G$ then $H \neq K$. Consider $N = H \cap K$ which is a normal subgroup of G. Let $N_0, N_1, \ldots, N_k = N$ be a composition series for N. Using Corollary 7 (First Isomorphism Theorem),

$$\frac{H}{N} = \frac{H}{H \cap K} \cong \frac{HK}{K} = \frac{G}{K}$$

But since equation (77) is a composition series, $\frac{G}{K}$ is simple, and thus so is $\frac{H}{N}$. Therefore

$$N_0, N_1, \ldots, N_k, H, G \tag{78}$$

is a composition series for G and has the same factors as (76). Similarly,

$$\frac{K}{N} = \frac{K}{H \cap K} \cong \frac{KH}{H} = \frac{G}{H}$$

and thus

$$N_0, N_1, \ldots, N_k, K, G \tag{79}$$

is a composition series for G and is the same as (76). But (79) and (78) have the same factors, (in the same order except the last two which are transposed) and hence the composition series are the same, that is

$$(76) \leftrightarrow (78) \leftrightarrow (79) \leftrightarrow (77)$$

and so the result is shown. □

Definition 80 *A subgroup H of a group G is called characteristic if $\phi(H) = H$ for all $\phi \in \mathrm{Aut}(G)$,* i.e., *is invariant under all automorphisms of G.*

Theorem 81 *A finite group G that has no characteristic subgroups (is characteristically simple) is a direct product of isomorphic simple groups.*

Proof. Trivially, the result holds if $|G| = 1$. Let $|G| > 1$ and assume that the result holds for characteristically simple groups of smaller order. Let G be a characteristically simple group, and let N be a minimal non-trivial normal subgroup of G.

If $N = G$ then G is simple and there is nothing more to show.

Suppose $N < G$ then N is also characteristically simple, for any automorphism of N can be extended to an automorphism of G by defining $\phi(g) = g$ for $g \in G \setminus N$. Hence by induction N is a direct product of isomorphic simple groups.

Now, for any $\phi \in \mathrm{Aut}(G)$, $\phi(N)$ is also a minimal normal subgroup of G, and is isomorphic to N. Hence each $\phi(N)$ is isomorphic to the direct product of isomorphic simple groups to which N is isomorphic.

Let M be a normal subgroup of G that is a direct product of some images of N under some subset of $\mathrm{Aut}(G)$, so

$$M = \prod_{\substack{\phi \in \Phi \\ \Phi \subseteq \mathrm{Aut}(G)}} \phi(N)$$

Note that N is such a group. Let M be maximal amongst such subgroups of G, and consider $\phi(N) \cap M$ for some $\phi \in \mathrm{Aut}(G)$.

If $\phi(N) \cap M = \{1_G\}$ then $\phi(N) \times M$ is a direct product, and is again normal. But $M \leqslant \phi(N) \times M$ and thus by the maximility of M, $M = \phi(M) \times M$ and so $\phi(N) \subseteq M$ which contradicts $\phi(N) \cap M = \{1_G\}$. Thus this cannot be the case.

If $\phi(N) \cap M = \phi(N)$ then $\phi(N) \subseteq M$. But as this must hold for any ϕ,

$$\prod_{\phi \in \mathrm{Aut}(G)} \phi(N) \subseteq M$$

but by the definition of M this must be equality.

Now, M is a direct product of all images under $\mathrm{Aut}(G)$ of N, thus applying any automorphism of G to M will simply 'permute' the order of this direct product. Thus when the direct product is treat as being internal, M is characteristic in G. But G is characteristically simple, and thus $M = G$. Hence from above G is a direct product of isomorphic simple groups. $\square$