Maths 720 Notes

Louis Christie
6652368

May 28, 2018

1 Monday 26^{th} February

$D_3 \simeq S_3 \simeq GL(2, \mathbb{F}_2)$

Definition 1. *V is an elementary p-group if $|g| | p$ for all $g \in V$*

Proposition 2. *If $|G| = p^2$ for some prime p then $Z(G) = G$*

Note when $x = (1234)$, $y = (14)(23)$,

$$D_4 = \langle (1234), (14)(23) \rangle = \{x, x^2, x^3, x^4 = e = y^2, y, xy, yx, x^2y = yx^2\}$$

Claim 3. *D_4 has 5 elements of order 2*

Claim 4. *$Z(G) = \langle (13)(24) \rangle$*

Let $Q_8 \leq S_8 = \langle (1625)(3847), (1423)(5768) \rangle$ then

$$Z(Q_8) = \langle (12)(34)(56)(78) \rangle \qquad |Z(Q_8)| = 2$$

Claim 5. *Q_8 has a unique element of order 2*

Corollary 6. *$Q_8 \simeq D_4$*

Another way of creating Q_8 is as a subgroup of $GL(2, \mathbb{C})$. Set:

$$x = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Then set $Q_8 = \langle x, y \rangle \leq GL(2, \mathbb{C})$.

Definition 7. *Let*

$$\begin{aligned} D_n &= \langle (12 \ldots n), (1, n)(2, n-1) \ldots (\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1) \rangle \\ S_n &= \langle (12), (12 \ldots n) \rangle \\ A_n &= \langle (123) \{n - 1 cycle \text{ or } n - 2 cycle\} \end{aligned}$$

Note $|S_n| = n!$, $|A_n| = n!/2$.

Example 8. *It is clear that:*

$$A_5 = \langle (123), (345) \rangle \qquad |A_5| = 60$$

and

$$A_6 = \langle (123), (23456) \rangle \qquad |A_6| = 360$$

Exercise 9. *Find A_4 and S_4*

Definition 10. *Set $V = \mathbb{F}_q^d$: a d-dimensional vector space over $\mathbb{F}_q$. If $\mathbb{F}$ is finite, then $|\mathbb{F}| = p^e$ for some prime p and $e \in \mathbb{Z}_+$. Now let $GL(V)$ be the group of linear transformations of V.*

Remark 11. *Note $GL(V) \simeq GL(d, \mathbb{F}_q)$.*

Exercise 12. *Find $|GL(d, \mathbb{F}_q)$ (Hint: $GL(2,2) = 6$, $GL(2,3) = 48$, $GL(3,2) = 68$. $GL(2,2) = (q^d - 1) \times ?$)*

2 Tuesday 27^{th} February

Definition 13. *For $H \leq G$ and $x \in G$ we define the cosets of H as:*

$$Hx = \{hx : h \in H\}$$
$$xH = \{xh : h \in H\}$$

Proposition 14. *For any $H \leq G$, we have:*

$$G = \bigcup_{i=0}^{k} Hx_i = \bigcup_{j=0}^{k} x_j H$$

For some $k \in \mathbb{N}$ and $(x_i), (x_j)$.

Definition 15. *We call such k the index of H in G, and write $k = |G : H|$.*

Theorem 16. *If G is a finite group and $H \leq G$ then $|H|\big||G|$.*

Claim 17. *If $H \leq G$ and $x \in G$, then $|H| = |Hx| = |xH|$.*

Definition 18. *We call $H \leq G$ normal in G if $xH = Hx$ for all $x \in G$. We write $H \lhd G$.*

Remark 19. *This is equivalent to $x^{-1}Hx = H$ and $H^x = H$ for all $x \in G$*

Definition 20. *If $H \lhd G$ then we define $Q = G/H = \{Hx : x \in G\}$, i.e. the set of (right) cosets of H.*

Example 21. *Set $G = S_3 = \langle a, b\rangle$, with $a = (123)$ and $b = (12)$, and $H = \langle b\rangle$. Then $H^a = \langle(13)\rangle$, so H is not normal in G. Set $H' = \langle a\rangle$. Then $H' \lhd G$.*

Claim 22. *If $H \leq G$ and $|G : H| = 2$ then $H \lhd G$.*

Definition 23. *Given the set $Q = G/H$, define a multiplication on this set $\cdot : Q \to Q$ by:*

$$(Hx) \cdot (Hy) = H(xy)$$

Proposition 24. *$(G/H, \cdot)$ is a group*

Definition 25. *For groups G, H, We call a function $\phi : G \to H$ a homomorphism if*

$$\phi(xy) = \phi(x)\phi(y)$$

We call a bijective homomorphism an isomorphism. If $\phi : G \to G$ is isomorphic then we call it an automorphism.

Example 26. *Take $G = GL(d, \mathbb{F})$, and $H = \mathbb{F}$. Then $\phi : G \to H$ given by $g \mapsto det(g)$ is a homomorphism.*

Definition 27. *For a homomorphism $\phi : G \to H$, we define $\ker\phi = \{g \in G : \phi(g) = 1\}$.*

Example 28. *Again take $\phi : GL(d, \mathbb{F}) \to \mathbb{F}$ given by $g \mapsto det(g)$. Then*

$$\ker\phi = \{x \in G : \det(x) = 1\} = SL(d, \mathbb{F}) \lhd GL(d, \mathbb{F})$$

We call $SL(d, \mathbb{F})$ the special linear group, and $|SL(n, \mathbb{F}_q)| = |GL(n, \mathbb{F}_q)|/(q-1)$

Definition 29. *For $H \lhd G$, define $\phi : G \to G/H$ by $g \mapsto Hg$.*

Remark 30. *Observe ϕ is a homomorphism. In fact it is the canonical Homomorphism from G to G/H.*

Claim 31. *For any homomorphism $\phi : G \to H$, $\ker\phi \lhd G$.*

Theorem 32 (First Isomorphism Theorem)**.** *Let $K = \ker\phi$, for some surjective homomorphism $\phi : G \to H$. Then $H \simeq G/\ker\phi$.*

Theorem 33 (Correspondence Theorem)**.** *Let G be a group and $N \lhd G$. Then:*

1. *If $N \leq A \leq G$ then $A/N \leq G/N$. If $N \subseteq A \lhd G$, then $A/N \lhd G\ N$.*
2. *Every $A \leq G/N$ has the form B/N for some suitable $B \leq G$. Every $A \lhd G/N$ has the form B/N for some suitable $B \lhd G$.*

(TODO: Add figure)

Proof. For part (1), we claim that if $N \lhd G$ then $N \lhd A$, in which case A/N exists and $A/N \subseteq G/N$. Also, A/N is non-empty (as $N \in A/N$), so take $Na, Nb \in A/N$. Then

$$(Na)(Nb)^{-1} = N(ab^{-1}) \in A/N$$

Thus $A/N \leq G/N$. If $A \lhd G$, then $g^{-1}ag \in A$ for all $g \in G$, so:

$$(Ng)^{-1}(Na)(Ng) = N(g^{-1}ag) \in A/N$$

and thus $A/N \lhd G/N$.

For part (2), it reduces to the First Isomorphism Theorem. □

Definition 34. *Take $H, K \lhd G$, and define*

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

Lemma 35. *$HK \leq G$ if, and only if, $HK = KH$.*

Proof. (TODO : add proof) □

Corollary 36. *If $N \lhd G$ and $H \leq G$, then $NH \leq G$.*

Corollary 37. *If $N \lhd G$ and $H \leq G$, then $\langle N, H\rangle = NH$. This is because clearly $NH \leq \langle N, H\rangle$, but also $NH \leq G$, so as $\langle N, H\rangle = NH$ is the smallest subgroup containing NH, they must be equal.*

Example 38. *Take $G = D_4 = \langle a, b\rangle$ where $a = (1234), b = (14)(23)$. Let $N = \langle a^2\rangle \lhd G$. Then $|G/N| = 4$. Also, $G/N \simeq C_2 \times C_2$. (TODO : add diagram)*

3 Thursday 1^{st} March

Definition 39. *We call $Z(G) = \{y \in G : xy = yx \, \forall x \in G\}$ the center of G.*

Lemma 40. *$Z(G) \lhd G$.*

Remark 41. *Observe that $Z(G)$ is abelian and G is abelian if and only if $Z(G) = G$.*

Example 42. *$Z(S_3) = 1$. In fact, $Z(S_n) = 1$ for every $n \geq 3$. Also, for $G = GL(2, \mathbb{R})$:*

$$A \in Z(G) \implies A = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{i.e.}, \; Z(G) = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : x \in \mathbb{R}\right\}$$

$Z(D_4) = \langle (13)(24) \rangle$.

Definition 43. *We define the centraliser of $g \in G$ as*

$$C_G(g) = \{x \in G : xg = gx\}$$

Remark 44. *Note that $C_G(g) \neq \varnothing$ and $C_G(g) \leq G$.*

Example 45. *$Z(D_4) = \langle (13)(24) \rangle$. Then*

$$C_{D_4}\big((12)(34)\big) = \langle (13)(24), (12)(34) \rangle$$

Exercise 46. *Find $Z(D_n)$ (note that $|Z(D_n)| = 2 - (n\%2)$.*

Proposition 47. *If $\phi : G_1 \to G_2$ is an isomorphism, then*

$$\phi(Z(G_1)) = Z(G_2).$$

If ϕ is an automorphism on G, then $\phi(Z(G)) = Z(G)$. We say Z is fixed under automorphisms.

Definition 48. *We say C is a characteristic of G if $C\phi = C$ for every automorphism ϕ. (TODO : Check with Eamonn) We say $C \leq G$ is a characteristic subgroup of G if $\phi(C) \leq C$ for every $\phi \in Aut(G)$.*

Lemma 49. *The set of automorphisms of G, paired with composition, forms a group.*

Definition 50. *Let $g \in G$. The define the inner automorphism of G generated by g as:*

$$\theta_g(x) = g^{-1}xg = x^g$$

Observe that θ_g does indeed form an automorphism of G. Also define $Inn(G) = \{\theta_g : g \in G\}$.

Lemma 51. *$Inn(G) \lhd Aut(G)$*

Proof. Exercise. □

Remark 52. *Observe that if G is abelian then $Inn(G) = 1$.*

Remark 53. *Characteristic subgroups are fixed under automorphisms, normal subgroups are fixed under inner automorphisms*

Definition 54. *Take*

$$Out(G) = \frac{Aut(G)}{Inn(G)}$$

Note that often $\theta \in Aut(G) \setminus Inn(G)$ is called an outer automorphism, but these are distinct.

Exercise 55. *Show $Inn(G) \simeq G/Z(G)$. (Hint: 1^{st} Isomorphism theorem. Define $\psi : G \to Inn(G)$ with $\ker \psi = Z(G)$.)*

Proposition 56. *For any $\phi \in Aut(G)$, if $G = \langle g \rangle$ then $G = \langle \phi(g) \rangle$.*

Example 57. *Take $(\mathbb{Z}, +)(= \langle x \rangle, x \in \{1, -1\})$. Thus*

$$Aut\big((\mathbb{Z}, +)\big) = \{\phi_a : x \mapsto x, \phi_b : x \mapsto -x\} \simeq \mathbb{Z}_2$$

Lemma 58. *Let $G = \langle x \rangle \simeq \mathbb{Z}_n$. Then take $0 \leq m < n$. Define $\iota_m : G \to G$ by $x \mapsto x^m$. Then*

$$Aut(G) = \{\iota_m : \gcd(m, n) = 1\}$$

Corollary 59. *If p is prime then $Aut(\mathbb{Z}_p) = \mathbb{Z}_{p-1}$.*

Definition 60. *We call G an elementary abelian group if $G \simeq (C_p)^d$.*

Remark 61. *Note that every element of an elementary group has order 1 or p.*

Theorem 62. *Let $G \simeq (C_p)^d$. Then $Aut(G) \simeq GL(d, p)$.*

Remark 63. *Characteristic subgroups are fixed under automorphisms, normal subgroups are fixed under inner automorphisms*

Definition 64. *Let $H \leq G$. Then define the normaliser of H in G as:*

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}$$

Lemma 65. *$N_G(H) \leq G$.*

Remark 66. *$H \lhd G$ if and only if $N_G(H) = G$.*

Example 67. *Let $G = S_3$. Then:*

$$\begin{aligned} H_1 = \langle (12) \rangle &\implies N_G(H_1) = H_1 \\ H_2 = \langle (123) \rangle &\implies N_G(H_2) = H_2 \end{aligned}$$

Definition 68. *Let $x, y \in G$. Then define:*

$$[x, y] = x^{-1}y^{-1}xy$$

We call this the commutator of x, y.

Example 69. *Which $c \in S_3$ are commutators? We know All commutators must have even order, so $x \in A_3 = \{1, (123), (132)\}$. But we also have:*

$$\begin{aligned} [(12), (12)] &= 1 \\ [(12), (23)] &= (123) \\ [(12), (13)] &= (132) \end{aligned}$$

So all elements of A_3 are commutators of S_3

Definition 70. *We derived group $G' \leq G$ is defined as:*

$$G' = \langle [x, y] : x, y \in G \rangle$$

I.e., the group generated by all commutators.

Example 71. *$S_3' = A_3$, as shown. In general $S_n' = A_n$ for all $n \geq 3$. Prove as exercise.*

Lemma 72. *$G' \lhd G$.*

Lemma 73. *Both $Z(G)$ and G' are characteristic subgroups of G. And are both therefore also normal.*

Example 74. *Take $A_4 = G$. $G' = \langle (13)(24), (12)(34) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$. Thus $G' \lhd G$.*

Remark 75. *There exists a group G with order 96. It has 29 commutators, but $|G'| = 32$. This is the smallest group where $\{commutators\} \neq G'$.*

Remark 76. *If G is a finite simple group then every $g \in G' = G$ is a commutator.*

4 Monday 5^{th} March

Lemma 77. *Take $N \lhd G$, then*

$$G/N \textit{is abelian if and only if } G' \leq N$$

Proof. G/N is abelian iff $Nx \cdot Ny = Ny \cdot Nx$ for all $x, y \in G$. Which is equivalent to $N = Nx^{-1}y^{-1}xy$, which implies $[x, y] \in N$. N all commutators, and hence $N \geq G'$. The converse follows exactly in reverse. □

Definition 78. *Take homomorphism $\phi : G \to H$. Then if $U \leq G$,*

$$\phi(U) = \{\phi(u) : u \in U\}$$

if $V \leq H$, then let

$$\phi^{-1}(V) = \{u \in G : \phi(u) \in V\}$$

Remark 79. *Whilst ϕ^{-1} can be defined, there need not be a map ϕ^{-1}*

Lemma 80. *Take homomorphism $\phi : G \to H$.*

1. *If $U \leq G$ Then $\phi(U) \leq H$*
2. *If $V \leq H$ then $\phi^{-1}(V) \leq G$ that contains* $\ker \phi$.

Example 81. *Take $N \lhd G$ and $\phi : G \to G/N$ the canonical homomorphism determined by N: $x \mapsto Nx$. Let $H \leq G$. Then what is $\phi(H)$?. (TODO: Add diagram 1) Observe $NH \leq G$, and $N \lhd NH$. Thus $NH/N \leq G/N$. Now*

$$NH/N = \{Nnh : n \in N, h \in H\} = \{Nh : h \in H\} = \phi(H)$$

Theorem 82 (Second Isomorphism Theorem)**.** *Take $N \lhd G$ and $H \leq G$. Then $N \cap H \lhd H$ and*

$$H/(N \cap H) \simeq NH/N$$

Proof. Define $\phi : G \to G/N$ by $g \mapsto Ng$. Then let ψ be the restriction of ϕ to $H \leq G$. Then ψ is a homomorphism from $H \to \psi(H) = NH/N$. Note that it is surjective. Now

$$\ker \psi = H \cap \ker \phi = H \cap N$$

But also $\ker \psi \lhd H$ and so $H \cap N \lhd H$. By the first isomorphism theorem:

$$H/\ker \psi = H/(H \cap N) \simeq NH/N$$

□

Example 83. *Take $G = S_4 = \langle (1234), (12) \rangle$, take $N = \langle (12)(34), (13)(24) \rangle$, and $H = \langle (1234) \rangle$. Then*

$$H \cap N = \langle (13)(24) \rangle \qquad H/(H \cap N) \simeq \mathbb{Z}_2$$

Also see that:

$$NH/N \simeq \mathbb{Z}_2$$

Lemma 84. *Take homomorphism $\phi : G_1 \to G_2$ where $\phi(N_1) = N2$ for $N_i \lhd G$, $(i = 1, 2)$. Then there exists a homomorphism $\psi : G_1/N_1 \to G_2/N_2$ defined by:*

$$(N_1 x)\psi = N_2(x\phi)$$

for all $x \in G_1$.

Proof. Let $N_1 x = N_1 y$. Then $y = nx$ for some $n \in N_1$. So $y\phi = (nx)\phi = (n\phi)(x\phi) \in N_2(x\phi)$. Thus $N_2(y\phi) = N_1(x\phi)$. Thus the choice of $x \in N_1$ does not matter and the map is well defined.

Now let $g, h \in G_1$. And consider:

$$(N_1 g)\psi(N_1 h)\psi = N_2(g\phi)N_2(h\phi) = N_2(g\phi)(h\phi) = N_2((gh)\phi) = (N_1(gh))\psi$$

Thus ψ is indeed homomorphic. □

Theorem 85 (Third Isomorphism Theorem)**.** *Let $M, N \lhd G$, and $M \geq N$. Then*

$$\frac{G/N}{M/N} \simeq G/M$$

(TODO: add diagram 2)

Proof. Note $N \lhd G$ thus $N \lhd M$ since $M \geq N$. So by the correspondence theorem

$$M/N \trianglelefteq G/N$$

Using the previous lemma, take $G_1 = G$, $N_1 = N$, $G_2 = G/M$, and $N_2 = 1$. Let $\phi : G \to G/M$ and obtain the corresponding ψ from the lemma. Then $\psi : G/N \to G/M$ where $Nx \mapsto Mx$ for all $x \in G$.

Now $\ker\psi \lhd G/N$, and it has the form K/N for some $K \lhd G$ (again by the correspondence theorem). Let $Nx \in K/N$, then $(Nx)\psi = M$. But $Mx = M$ iff $x \in M$, so $K/N \leq M/N$. If $x \in M$ then $(Nx)\psi = M$ and so $Nx \in K/N$. Therefore $K/N \geq M/N$. Hence

$$\ker\psi = M/N \qquad \text{and so} \qquad \frac{G/N}{M/N} \simeq \frac{G}{M}$$

□

Definition 86. *Take G and $\Omega \neq \varnothing$. Assume $g \in G$, and $\alpha \in \Omega$. There is defined a unique $g \cdot \alpha \in \Omega$*

1. *$\alpha \cdot 1_G = \alpha$ for all $\alpha \in \Omega$*
2. *$(\alpha \cdot g) \cdot h = \alpha \cdot (gh)$ for all $\alpha \in \Omega$ and $g, h \in G$.*

Then we say G acts on Ω, and $\cdot$ is an action of G on Ω

Example 87. *Take $\Omega \neq \varnothing$, $G \leq Sym(\Omega)$ then for all $\alpha \in \Omega$ and all $g \in G$,*

$$\alpha \cdot g = \alpha^g \text{ image of } \alpha \text{ under } g$$

1. *is satisfied by definition of the identity of Sym(Ω)*

2. is satisfied by the definition of multiplication in Sym(Ω)

Definition 88. *If $\Omega = G$, then we call is a regular action.*

5 Tuesday 6^{th} March

Corollary 89. *$G \simeq S \leq Sym(\Omega)$.*

Definition 90. *Take a group $G = \Omega$, then take the group action $\alpha \cdot g = g^{-1}\alpha g$. We call this the conjugation action.*

Remark 91. *The group action need not be the same as the the original group multiplication.*

Definition 92. *For a group G and $X \subseteq G$, consider*

$$Xg = \{xg : x \in X\} \qquad \forall g \in G$$

Define an action on $\mathcal{P}(G)$ by:

$$X \cdot g = Xg$$

We call this the action on subsets.

If $H \leq G$, take $\Omega = \{Hx : x \in G\}$. If $x \in \Omega$, then

$$Xg \in G \qquad since \quad (Hx)g = H(xg).$$

I.e. right multiplication defines an action of G on Ω. We call this the action on subgroups.

Lemma 93. *Take G, and a group action of G on some Ω. For $g \in G$ define $\pi_g : \Omega \to \Omega$ by $\alpha \mapsto \alpha \cdot g$. Then*

$$\pi_g \in Sym(\Omega),$$

and the map $\theta : G \to Sym(\Omega)$ given by $g \mapsto \pi_g$ is a homomorphism. Note that $\ker\theta$ is the kernel of the action.

(TODO : Insert D3)

Proof. For all $g, h \in G$:

$$\begin{aligned}(\alpha)\pi_g\pi_h &= (\alpha \cdot \pi_g)\pi_h \\ &= (\alpha \cdot g) \cdot h \\ &= \alpha \cdot (gh) \\ &= \alpha\pi_{gh}\end{aligned}$$

Also $\alpha\pi_1 = \alpha \cdot 1 = \alpha$ so π_1 is the identity.

For $g \in G$, $\pi_g\pi_{g^{-1}} = \pi_1$ so $\pi_g \in \text{Sym}(\Omega)$.

$$\theta(g)\theta(h) = \pi_g\pi_h = \pi_{gh} = \theta(gh)$$

Thus θ is a homomorphism.

Lastly, for $g \in G$, $g \in \ker\theta$ if and only if $\pi_g = \pi_1$. So $\alpha \cdot g = \alpha$ for all $\alpha \in \Omega$: i.e. $g \in$ kernel of the action. □

Corollary 94. *$\theta : G \to Sym(\Omega)$ is a homomorphism then*

$$K = \ker\theta \lhd G \quad \text{and} \quad G/\ker\theta \simeq Im\theta$$

Theorem 95. *If $H \leq G$, and $|G : H| = n < \infty$, there exists $N \vartriangle G$ such that $N \leq H$ and $|G : N|\big|n!$, if $n > 1$ and $|G| \nmid n!$, then G is not simple.*

Proof. G acts by right multiplication on

$$\Omega = \{Hx : x \in G\} \qquad |\Omega| = n$$

So $\theta : G \to \mathrm{Sym}(n)$. Take $N = \ker\theta$ and so $G/N \simeq \mathrm{Sym}(\Omega)$. Now

$$|S_n| = n! \implies |G : N| = |G/N|\big|n!$$

To see that $N \leq H$, let $x \in N$ and $H \in \Omega$. Then

$$x \in Hx = H \cdot x = H$$

since $x \in N$. Thus $N \leq H$.

If $n > 1$: then $H < G$ and so $N < G$. If $n = 1$ then $|G| = |G/N|\big|n!$. This proves $N > 1$ so G is not finite. □

Corollary 96. *Take $H \leq G$, with G finite. If $|G : H| = p$ and p is the smallest prime divisor of $|G|$, then $H \lhd G$.*

Remark 97. *Take $H \leq G$ with $|G : H| < \infty$. Then there exists $N \vartriangle G$ of finite index with $N \leq H$. We call*

$$N = core_G(H),$$

which is the largest normal subgroup of G contained in H.

Lemma 98. *Take $H \leq G$ of finite index. Then*

$$N = core_G(H) = \bigcap_{x\ inG} H^x$$

If $M \lhd G$ and $M \leq H$, then $M \leq N$.

Proof. (TODO: exercise) □

Example 99. *Take $G = S_4 = \langle(1234), (12)\rangle$. And $H = \langle(13)(24), (34)\rangle \simeq D_4 \leq S_4$. Then $|G : H| = 3|$. Thus there exists a $\theta : G \to Sym(3)$. Take*

$$N = \ker\theta \qquad N = Core_G(H) = H \cap H^{(1234)} \cap H^{(12)} = \langle(12)(34), (14)(23)\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

Also $G/N \simeq Sym(3)$.

Definition 100. *We call a group action $(G, \Omega, \cdot)$ transitive if for every two elements $\alpha, \beta \in \Omega$ there exists a $G \in G$ such that $\alpha \cdot g = \beta$.*

Remark 101. *i.e. the number of orbits is 1*

Example 102. *Take a group G and a regular action. Consider $H \leq G$, and $\Omega = \{Hx : x \in G\}$. Then the action on right cosets is transitive.*

Example 103. *A regular action on G is not necessarily transitive, because only elements of the same order can be conjugates.*

Definition 104. *Take a group action $(G, \Omega, \cdot)$. The orbit of this action are of the form $\{\alpha \cdot g : g \in G\} \subseteq \Omega$. Then the action is transitive if and only if the number of orbits is 1.*

Lemma 105. *Ω is a disjoint union of orbits.*

This is analogus to parition of G under cosets of $H \leq G$.

Example 106. *Conjugation action of G on Ω is equivalent to conjugacy classes of elements of G. I.e. $x \in Z(G) \implies class(x) = \{x\}$.*

Example 107. *S_3, $\Omega = \{1,2,3\}$. This action has one orbit, $x = (123)$ and the conjugacy classes are:*

$$\{e\}, \{(12), (13), (23)\}, \{(123), (132)\}$$

6 Thursday 8^{th} March

Definition 108. *For a group action $(G, \Omega, \cdot)$ we call*

$$G_\alpha = \{g \in G : \alpha \cdot g = \alpha\}$$

the stabiliser of $\alpha \in \Omega$ in G.

Lemma 109. *$G_\alpha \leq G$.*

Example 110. *Consider a congucation action $(G, \Omega, \cdot)$. Then*

$$G_x = \{g \in G : x^g = x\} = C_G(x)$$

Example 111. *Consider a congugation on a subgroup $X \leq G$, given by $X \cdot g = X^g$. THen*

$$G_x = \{g \in G : X^g = X\} = N_G(x)$$

Example 112. *COnsider an action of G on right cosets of $H \leq G$. i.e. $\Omega = \{Hx : x \in G\}$. Then the stabiliser of Hx in G is H^x.*

Theorem 113 (Orbit Stabiliser Theorem)**.** *Take a group action $(G, \Omega, \cdot)$. Then let O_α be the orbit of $\alpha \in \Omega$ under $\cdot$. Let $H = G_\alpha$ be the stabiliser of α in G. Then there exists a bijection*

$$o_\alpha \leftrightarrow \{G_\alpha x : x \in G\}$$

Remark 114. *If G is finite then*

$$|G| = |O_\alpha||G_\alpha|$$

Proof. Define $f : O_\alpha \to \{Hx : x \in G\}$ by the following. Take $\beta \in O_\alpha$, and choose $x \in G$ with $\beta = \alpha \cdot x$, and then give

$$f(\beta) = Hx$$

First consider that if $f(\beta) = Hy$, then we can show that $Hy = Hx$, so f is well defined. Then consider

$$Hx = f(\alpha \cdot x)$$

so f is onto. Lastly, take $f(\beta) = f(\gamma)$. Then $\beta = \alpha \cdot x$ and $\gamma = \alpha \cdot y$, so $Hx = Hy$ and thus $y = hx$ for some $h \in H$. Then

$$\gamma = \alpha \cdot y = \alpha \cdot (hx) = (\alpha \cdot h) \cdot x = \alpha \cdot x = \beta$$

as $h \in H$. Thus f is also injective, and gives us the theorem. □

Corollary 115 (Fundamental Counting Principle)**.** *Suppose G acts on Ω and $|O_\alpha| = |G : G_\alpha|$. Then if G is finite, $|O_\alpha| = |G|/|G_\alpha|$ and $|O_\alpha| \| |G|$.*

Corollary 116. *Take a conjugation action of elements of G. Then*

$$|Cl(g)| = |G : C_G(g)|$$

Exercise 117. *Take finite G and suppose every two non-trivial elements of G are conjugates, then $|G| \leq 2$.*

(TODO : FIX COR BELOW)

Lemma 118. *Let $H, K \leq G$, with H and K finite. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof. $HK = \{hk : h \in H, k \in K\}$, $\Omega = \{Hx : x \in H\}$. Then K acts on Ω by right multiplication. □

Definition 119. *G is a p-group if $|x| = p^k$ for some $k \geq 0$, for all $x \in G$. Then if G is finite, $|G| = p^n$ for some $n \geq 0$.*

Lemma 120. *Take prime p and G a finite p-group with $|G| = p^n$. Then*

$$Z(G) > 1$$

Proof. Let $C_1, C_2, \ldots, C_r$ be conjugacy classes of $G = \Omega$. Then

$$|G| = |C_1| + |C_2| + \cdots + |C_r|$$

Let $C_1 = \{e\}$, so $|C_1| = 1$. Then take $x_i \in C_i$. $|C_i| = |G|/|C_G(x_i)| = p^{j_i}$ where $j_i \geq 0$. If all $j_i \geq 1$ then

$$|G| \cong 0 \mod p$$
$$\sum_{i=1}^{r} \cong 1 \mod p$$

which is a contradiction. Thus $j_i = 0$ for some i, and so $C_G(x_i) = G$ for some $x_i \neq 1$. Thus $Z(G) > 1$. □

Remark 121. *Lagrange implies $p \big| |Z(G)|$.*

Definition 122. *For a standard group action, define:*

$$\chi(g) = |\{\alpha \in \Omega : \alpha \cdot g = \alpha\}|$$

as the number of fixed points under g.

Example 123. *Take $G = S_5$ and $\Omega = \{1, 2, 3, 4, 5\}$. then*

$$g = (123) \qquad \chi(g) = 2$$
$$g = e \qquad \chi(g) = 5$$
$$g = (12345)\chi(g) = 0$$

Example 124. *Take a regular action of G on $\Omega = G$. Then*

$$\chi(g) = \begin{cases} 0 & g \neq 1 \\ |G| & g = 1 \end{cases}$$

Example 125. *Consider a conjugation action of elements. Then*

$$\chi(g) = |C_G(g)|$$

Theorem 126 (C-F)**.** *Let G act on Ω with both G and Ω finite. Then the number of orbits is*

$$\frac{1}{|G|}\sum_{x\in G}\chi(x)$$

Proof. Define $S = \{(\alpha, g) : \alpha \in \Omega, g \in G, \alpha \cdot g = \alpha\}$. Then count the cardinality of this set.

First, for each $\alpha in \Omega$, there exists $|G_\alpha$ elements g such that $(\alpha, g) \in S$. Thus

$$|S| = \sum_{\alpha\in\Omega}|G_\alpha|$$

Secondly, for each $g \in G$, the number of elements of $\alpha \in \Omega$ paired with g is $\chi(g)$. So

$$|S| = \sum_{g\in G}\chi(g)$$

Combining these gives:

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{\alpha\in\Omega}|G_\alpha| = \sum_{\alpha\in\Omega}\frac{1}{|O_\alpha|}$$

□

7 Monday 12^{th} March

Corollary 127. *If G is finite and $|\Omega| > 1$ then there exists an element $g \in G$ with $\chi(g) = 0$.*

Example 128. *Conisder D_4 acting on $\Omega = \{1,2,3,4\}$. Then $\chi(e) = 4$, $\chi(24) = \chi(13) = 2$ and also other characters vanish. Hence the number of orbits of this action is $\frac{1}{8}(8) = 1$.*

Example 129. *Consider D_4 again, this time acting by conjugation. Then $\chi(e) = \chi((13)(24)) = 8$ and all other elements have $\chi(g) = 4$. Thus this action has $\frac{1}{8}40 = 5$ orbits.*

7.1 Sylow Theorems

Theorem 130 (Lagrange)**.** *If G is finite, and $H \leq G$ then $|H|\,\big|\,|G|$.*

We want to understand a form of converse: if $m\,\big|\,|G|$ then does there exist a subgroup $H \leq G$ with $|H| = m$?

Exercise 131. *Does there exist a subgroup of A_4 of order 6?*

Lemma 132. *Let $n = p^a m$. Then ${}^nC_{p^a} \equiv m \mod p$*

Proof. Let $f(x), g(x) \in \mathbb{Z}[x]$. $f(x) \equiv g(x) \mod p$ if and only if the coefficients of each x^j are congruent mod p. Observe that $(x+1)^p \equiv (x^p + 1) \mod p$ since ${}^pC_j \equiv 0 \mod p$ for $1 \leq j \leq p-1$. Therefore it follows from a simple induction that

$$(x+1)^{p^a} \equiv (x^{p^a} + 1) \mod p$$

And thus

$$(x+1)^n = (x+1)^{p^a m} \equiv (x^{p^a} + 1)^m \mod p$$

Then compare coefficients to get

$$\binom{n}{n-p^a} = \binom{n}{p^a} \equiv \binom{m}{1} \equiv m \mod p$$

□

Theorem 133 (Sylow I)**.** *If G is a finite group with $|G| = p^a m$ for some prime p and m with $\gcd(p,m) = 1$. Then G has a subgroup of order p^a.*

Proof. Take $\Omega = \{X \subset G : |X| = p^a\}$. Then $|Omega| =^{|G|} C_{p^a} \equiv m \neq 0 \mod p$. Let G act on Ω by right multiplication (which is well defined as $|Xg| = |X|$). Then p does not divide $|\Omega|$ so there exists some orbit O where p does not divide $|O|$. Let $x \in O$. By the fundamental counting principle, $|O||G_x| = |G|$. Considering divisibility of $|G|$ by p^a gives $p^a\,\big|\,|G_x|$ so $p^a \leq |G_x|$. Now for any $X \in \Omega$ with $X \supseteq \{x\}$ and $y \in X$ and $h \in G_x$, $yh \in Xh = X$. Thus $xG_x \subseteq X$, so $|G_x| = |xG_x| \leq |X| = p^a$, and hence $|G_x| \leq p^a$. Thus G_x has order p^a, giving us the desired subgroup. □

Definition 134. *Let G have $|G| = p^a m < \infty$ for prime p and $\gcd(p,m) = 1$. Then a **Sylow-**p subgroup of G is any $P \leq G$ such that $|P| = p^a$. We call the set of such subgroups*

$$Syl_p(G) = \{P \leq G : |P| = p^a\}$$

Corollary 135. *If $|G|$ is finite and $p\,\big|\,|G|$ for prime p then G has an element of order p.*

Proof. There exists some $P \in \mathrm{Syl}_p(G)$ by Sylow I. Choose $x \in P \setminus \{1\}$. Then $|x| = p^a$ for some $a \geq 1$, and so $|x^{p^{a-1}}| = p$. □

Definition 136. *A group P is a p-group if every element has finite order that is a power of p.*

Corollary 137. *A finite group is a p-group if its order is a power of p.*

Proof. Apply Cauchy and Lagrange □

Example 138. *Take $G = Sym(4)$. Then $|G| = 24 = 2^3 \cdot 3$. We have*

$$S = \langle (12), (13)(24) \rangle$$
$$T = \langle (13), (12)(34) \rangle$$

As Sylow 2-groups of G, and:

$$A = \langle (142) \rangle$$
$$B = \langle (123) \rangle$$
$$C = \langle (243) \rangle$$
$$D = \langle (143) \rangle$$

are the Sylow 3-groups of G.

Remark 139. *If $S \leq G$ is a Sylow p-subgroup then as $|S^g| = |S|$, S^g is also a sylow p-subgroup of G. Hence $Syl_p(G)$ is closed under conjugation.*

Theorem 140 (Sylow II)**.** *Let G be a finite group. Then $Syl_p(G)$ is a single conjugacy class of subgroups of G.*

8 Tuesday 13^{th} March

$|G| = p^a m$ with $\gcd(p, m) = 1$, then there exists an $H \leq G$ with $|H| = p^a$. $\mathrm{Syl}_p(G)$ is a single conjugacy class of G.

Theorem 141. *G finite, $P \leq G$ a p-subgroup and $S \in Syl_p(G)$ then $P \subseteq S^x$ for some $x \in G$. I.e., every p-subgroups is contained in some sylow p-subgroup of G*

Proof. Let $\Omega = \{Sx : x \in G\}$. Let P act on Ω by right multiplication.

$$(Sx) \cdot y = S(xy)$$

$|\Omega| = |G : S|$ is not divisible by p since $S \in \mathrm{Syl}_p(G)$. Thus some orbit of the action of P on Ω must have size not divisible by p. But P is a p-group, so all those orbits have p-power size by FCP. Since only p-power not divisible by p is 1, there exists some orbit of size 1. Therefore P stabilisies Sx for some $x \in G$. Let $y \in P$, so $Sx = Sx \cdot y = S(xy)$. Thus

$$S^x = x^{-1}Sx = x^{-1}Sxy = S^x y$$

so $y \in S^x$. Thus $P \subseteq S^x$. □

Sylow II. Take $S \in \mathrm{Syl}_p(G)$. Then $|S^x| = |S|$ only if $S^x \in \mathrm{Syl}_p(G)$. If P is a p-subgroup of G then $P \subseteq$ some sylow p-group. Thus $P \leq S^x$ for some $x \in G$. But then $|P| = |S^x|$ so $P = S^x$. Therefore there exists just one conjugacy class of Sylow p-subgroups. □

Corollary 142. *$\#Syl_p(G) = |G : N_G(P)|$ for $P \in Syl_p(G)$. Also $\#Syl_p(G) \big| |G : P|$.*

Corollary 143. *Let $S \in Syl_p(G)$ TFAE. Then*

1. *$S \lhd G$*
2. *S is unqiue Sylow p-subgroup of G*
3. *Every p-subgroup of G is contained in S*
4. *S characteristic subgroup of G*

Proof. (1) implies (2) by the prior corollary. (2) implies (3) as $S = S^x$. (3) implies (4) as automorphisms fix sylow subgroups. (4) implies (1) trivially. □

Remark 144. *This means that we can prove that a group is not simple by showing that G has a unique Sylow p-subgroup.*

Example 145. *Take $|G| = 360 = 2^3 \cdot 3^2 \cdot 5$. Then $N_p(G) = \#Syl_p(G)$ thus*

$$N_3(G) \big| 2^3 \cdot 5$$

Thus

$$N_3(G) \in \{1, 2, 4, 8, 5, 10, 20, 40\}$$

Theorem 146 (Sylow III)**.** *If G is a finite group, then*

$$N_p(G) = \#Syl_p(G) \quad and \quad N_p(G) \cong 1 \mod p$$

Lemma 147. *Take finite G, $S \in Syl_p(G)$. Let P be a p-subgroup of $N_G(S)$. Then $P \subseteq S$.*

Proof. S a Sylow p-subgroup with $S \leq N_P(S)$ implies $S \in \mathrm{Syl}_P(N_G(S))$. But by definition $S \lhd N_G(S)$ so S is unique, and thus $P \subseteq S$ by the previous corollary. □

Claim 148. $N_P(S) \leq S$

Claim. Take G; $S \in \mathrm{Syl}_p(G)$. $N_p(S) \leq P$ only if $N_p(S)$ is a p-group. Which implies $N_p(S)$ is a p-subgroup of $N_G(S)$, and thus $N_P(S) \leq S$. □

Theorem. Let $P \in \mathrm{Syl}_p(G)$. Let P act by conjugation on $\mathrm{Syl}_p(G)$. Since P stabilises itself under conjugation, $\{P\}$ is an orbit under the action. If there is just one orbit, then we are done. Otherwise, let $S \in \mathrm{Syl}_p(G)$ where $S \neq P$. Let O be the orbit of S. Then $|O| = |P : N_P(S)|$. Now $N_P(S) \leq S$ from the claim above, and $N_P(S) \leq P$, so $N_P(S) \leq P \cap S$. But also $x \in P \cap S$ only if $x \in S$, so x normalises S, and so $N_P(S) \geq P \cap S$. Therefore $|O| = |P : P \cap S|$. But $S \neq P$, so $|P : P \cap S| = p^e$ for some $e \geq 1$. Thus

$$N_P(S) = 1 + \sum_i p^{e_i} \quad \text{and} \quad N_P(S) \cong 1 \mod p$$

□

9 Thursday 15^{th} March

Example 149. *Take $G = Sym(4) = \langle(1234),(12)\rangle$ (with $|G| = 24 = 2^3 \cdot 3$. Then the factors of 3 are only 1 and 3, which are both congruent to $1 \mod 2 = p$. We can construct three subgroups of order 8:*

$$S = \langle(12),(13)(24)\rangle$$
$$T = \langle(24),(14)(23)\rangle$$
$$U = \langle(14),(13)(24)\rangle$$

thus $n_2 = 3$. Note that $U = S^{(24)}$ and $T = U^{(12)}$ so $T = (S^{(24)})^{(12)} = S^{(241)}$.

Similarly, n_3 must be a factor of 8, i.e., $n_3 \in \{1,2,4,8\}$. But is must also be congruent to $1 \mod 3$, so it cannot be 2 or 8. Again, we can construct at least two subgroups of order 3, so $n_3 = 4$.

Definition 150. *A group G is simple if and only if its only normal subgroups are 1 and G.*

Example 151. *Cyclic groups of prime order are simple, and are in fact the only simple abelian groups.*

Example 152. *If G is simple, non-abelian, and such that $|G| < 1000$ then there are only five possibilities:*

$$|G| \in \{60,168,360,504,660\}$$

Most of these are of the form $PSL(2,q) = SL(2,q)/Z(SL(2,q))$.

Lemma 153. *Let G be such that $|G| = p^a m$ for prime p with $\gcd(p,m) = 1$. If G is simple then $n_p(G)$ satisfies all of the following:*

1. $n_p|m$
2. $n_p \equiv 1 \mod p$
3. $|G|\,\big|\,n_p!$

Proof. We have:

1. $|\text{Orbit of Sylow } p\text{-subgroups}|\,\big|\,|G|$. Thus $|O||N_G(P)| = |G|$ and $|O|\,\big|\,|G:P|$.
2. This is just Sylow III
3. Take $S \in \text{Syl}_p(G)$ and $H = N_G(S)$. Then as G os simple and $1 < S < G$, S is not normal in G so $n_p > 1$. Let G act on $\Omega = \{Hx : x \in G\}$ by right multiplication. Then $|\Omega| = n_p > 1$. Define a homomorphism $\phi : G \to \text{Sym}(n_p)$. Then $\ker\phi \lhd G$ only if $\ker\phi = \{1\}$. So as G is isomorphic to a subgroup of $\text{Sym}(n_p)$ we must have $|G|\,\big|\,n_p! = |\text{Sym}(n_p)|$.

□

Example 154. *Let $|G| = 10^6 = 2^6 \cdot 5^6$. Then G is not simple. To see this, consider $n_5|2^6$ and $n_5 \equiv 1 \mod 5$, so $n_5 \in \{1,16\}$. If G were simple, then $|G|\,\big|\,16!$, but this is clearly false. Hence G is not simple.*

Example 155. *Let $|G| = 21 = 3 \cdot 7$. $n_7|3$ and $n_7 \equiv 1 \mod 7$ thus $n_7 = 1$, so G has a unique sylow 7-subgroup. $P \in Syl_y(G)$. Then $G/P \simeq C_3$, thus $G' \leq P$. Suppose $Q \lhd G$ and $|Q| = 3$. Then $G' \leq Q$, which implies $G' \leq P \cap Q = \{1\}$. Hence there only exists such a Q is G is abelian. If G is non-abelian, then G has a unique Sylow 7-subgroup and 7 Sylow 3-subgroups.*

Lemma 156. *Let $|G| = pq$ for distinct primes $p > q$. Then:*

1. *G has a normal Sylow p-subgroup; and*

2. *If G is non-abelian, then $q|p-1$ and G has exactly p sylow q-subgroups.*

Example 157. *let $|G| = 12$. By our usual considerations $n_3 \in \{1,4\}$. If $n_3 = 1$, then G has a normal 3-subgroup. So suppose $n_3 = 4$. Then the 4 Sylow 3-subgroups contain the 8 elements of order 3 (in G), as well as the identity element. There must exist a Sylow 2-subgroup of order 4, must can only contain the remaining 3 elements, and so must be unique.*

Lemma 158. *If $|G| = p^2 \cdot q$ with distinct primes p, q, then either G has a normal Sylow p-subgroup or it has a normal q-subgroup.*

Example 159. *If $|G| = 30 = 2 \cdot 3 \cdot 5$ then G is not simple.*

10 Monday 19^{th} March

10.1 Finite Abelian Groups

Take groups G, H. Then define

$$G \times H = \{(g,h) : g \in G \ h \in H\}$$

Call this the external direct product, and it is a group when $(g,h) \cdot (a,b) = (ga, hb)$. We want to understand when a group G can be written as a direct product $G \simeq H \times K$, for some $H, K \leq G$.

Theorem 160. *Let the group G have subgroups G_i for $1 \leq i \leq n$ where:*

1. *G_i commute with G_j element wise;*
2. *$G = G_1 G_2 \cdots G_n$; and*
3. *$G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_n) = \{e\}$.*

Then $G \simeq G_1 \times G_2 \times \cdots \times G_n$.

Proof. Let $g \in G$. Then by (2) every $g \in G$ can be written $g = g_1 g_2 \cdots g_n$. Suppose that also $g = g_1' \cdots g_n'$. Then by (1), $g_i (g_i')^{-1} = g_1^1 g_1' \cdots g_{i-1}^{-1} g_{i-1}' g_{i+1}^{-1} g_{i+1}' \cdots g_n^{-1} g_n'$. The left hand side is in G_i and the other side is in $G_1 \cdots G_{i-1} G_{i+1} \cdots G_n$ so by (3) $g_i (g_i')^{-1} = 1$, or rather $g_i = g_i'$. Hence the representation of g is unique.

Now define $\phi ; G \to G_1 \times G_2 \times \cdots \times G_n$ by $g \mapsto (g_1, g_2, \ldots, g_n)$. Exercise: show that ϕ is an isomorphism. □

Remark 161. *(1) is equivalent to (1'): $G_i \lhd G$ for all $1 \leq i \leq n$.*

Corollary 162. *If $G = MN$ for $N, M \lhd G$ with $M \cap N = \{1\}$. Then $G = M \times N$.*

Definition 163. *Take a finite group G, with $S_p \lhd G$ for all $p \big| |G|$. Then we say G nilpotent.*

Remark 164. *All abelian groups are nilpotent.*

Theorem 165. *Let G be a finite nilpotent group. Then*

$$G = S_{p_1} \times S_{p_2} \times \cdots S_{p_k}$$

for where $P = \{p_i : 1 \leq i \leq k\}$ list the primes dividing $|G|$.

Proof. (1') is satisfied by the definition of nilpotent groups. Then consider $S_{p_1} S_{p_2} \cdots S_{p_k} \leq G$. Note that $|S_p| \big| |S_{p_1} \cdots S_{p_k}|$ for all $p \in P$. Thus

$$\prod_{p \in P} |S_p| \Big| |S_{p_1} \cdots S_{p_k}|$$

But then $|G| = \prod_{p \in P} |S_p|$ so $G = S_{p_1} \cdots S_{p_k}$. So (2) is satisfied. Let $q \in P$. Then

$$\left| \prod_{p \in P \setminus \{q\}} S_p \right| \quad \text{divides} \quad \prod_{p \in P \setminus \{q\}} |S_p|$$

But q does not divide $\prod_{p \in P \setminus \{q\}} |S_p|$ so q does not divide $\left| \prod_{p \in P \setminus \{q\}} S_p \right|$ either. But $S_q \cap \prod_{p \in P \setminus \{q\}} S_p \leq S_q$ is a group of q-power order. Thus $S_q \cap \prod_{p \in P \setminus \{q\}} S_p = \{1\}$ and so (3) is satisfied too. Hence applying the previous theorem gives

$$G = S_{p_1} S_{p_2} \cdots S_{p_k}$$

□

Theorem 166. *Let G be a finite abelian p group. Let $C \leq G$ be a cyclic subgroup of maximum possible order. Then $G = C \times B$ for some $B \leq G$.*

Proof. If $C = G$ then take $B = \{1\}$ and we are done. Otherwise, $C < G$. Take $x \in G \setminus C$ of smallest possible order, with $x \neq 1$. Now $|x^p| < |x|$ so $x^p \in C$. If $C = \langle x^p \rangle$ then $|x| = p|C|$ but this contradicts the choice of C. Therefore $x^p = y^p$ for some $y \in C$. But $x \notin C$ so $xy^{-1} \notin C$, so $|x| \leq |xy^{-1}|$. But $(xy^{-1})^p = x^p(y^p)^{-1} = 1$ as G is abelian. Thus $|xy^{-1}| = p$ and so $|x| = p$.

Take $X = \langle x \rangle$ and define $\phi : G \to G/X$. As $|X| = p$, $C \cap X = \{1\}$. Thus $\phi(C) = XC/X \simeq C/(C \cap X) \simeq C$. Hence $\phi|_C$ is an isomorphism. $\phi(C)$ is a cyclic subgroup of maximum order in G/X (as otherwise it would contradict our choice of C). Since $|G/X| < |G|$ we can then apply induction on $|G|$ and conclude that $\phi(C)$ is direct factor of G/X. To see this:

By the correspondence theorem, every subgroup of G/X has the form B/X for some $X \leq B \leq G$. By the inductive hypothesis, we can find $X \leq B \leq G$ such that $G/X \simeq \phi(C) \times (B/X)$. Since $G/X = \phi(C)(B/X)$, $G = CB$, and also $\phi(C) \cap (B/X) = \{1\}$ and so $C \cap B \subseteq X, C$ so $C \cap B \subseteq C \cap X = \{1\}$. Thus $G = C \times B$. □

11 Tuesday 27^{th} February

Theorem 167 (Fundemental Theorem of Fintie Abelian Groups)**.** *Let G be a finite abelian group. Then $G = C_1 \times C_2 \times \cdots \times C_n$ where the C_i are cyclic p_i-groups for various primes p_i.*

Proof. Consider an induction argument on the order of G. If G is decomposable: i.e. $G = A \times B$ for $A, B < G$, then our by our inductive hypothesis is each of A and B are products of cyclic p-groups and so G is too. Otherwise, by our previous theorems G is a (finite abelian) p-group. Then our other result implies that G is cyclic. □

Theorem 168. *Let $n_1, n_2, \ldots, n_r$ and $m_1, m_2, \ldots, m_s$ be non trivial prime powers. Then take $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r} \simeq C_{m_1} \times C_{m_2} \times \cdots \times C_{m_s}$. Then $r = s$ and, after a suitable renumbering (if necessary), $n_i = m_i$ for all $1 \leq i \leq r$.*

Proof. See Krull-Schmidt Theorem. □

Lemma 169. *Take coprime $n, m \in \mathbb{N}$. Then $C_{nm} \simeq C_n \times C_m$.*

Proof. Exercise □

Exercise 170. *Every infinite abelian cyclic group is isomorphic to $(\mathbb{Z}, +)$.*

Definition 171. *We say a group G is torsion-free if no element of G other than the identity has finite order.*

Example 172. $(\mathbb{Z}, +)$ *is torsion free.*

Theorem 173. *A non-trivial torsion-free finitely generated abelian group is isomorphic to the direct sum of a set of infinite cyclic groups*

Proof. Let A be an appropriate group. Choose a generating set $A = \langle a_1, \ldots, a_n \rangle$ with minimal n (which exists as A is finitely generated). A is also torsion free, so we cannot have

$$m_1 a_1 + m_2 a_2 + \cdots + m_n a_n = 0$$

for non-vanishing m_i, as otherwise we could construct a generating set with fewer than n elements - a contradiction. Now let $A_i = \langle a_i \rangle$. Observe that $A_i \lhd A$ as A is abelian. Also see that

$$A = A_i + A_2 + \cdots + A_n$$

from the definitions of our generating set and A_is, and that

$$A_i \cap (A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots A_n) = 0,$$

which can be seen from a similar argument as before. Therefore by our previous result:

$$A \simeq A_1 \oplus A_2 \oplus \cdots \oplus A_n$$

□

Definition 174. *We call G periodic if every element of G has finite order.*

Lemma 175. *Let G be an arbitrary abelian group. The elements of finite order in G form a subgroup P (called the periodic subgroup) and G/P is torsion free.*

Proof. Note that the identity has finite order, so $P \neq \varnothing$. Then take $x, y \in P$. $x^t = y^s = 1$, so $(xy^{-1})^{ts} = 1$ and thus $xy^{-1} \in P$. Hence $P \lhd G$. Now consider elements $Pg \in G/P$. If $|Pg| = m < \infty$, then $g^m \in P$, so g has finite order. Thus $g \in P$ and so $Pg = P$ - i.e. the only element of G/P of finite order is the identity and so it is torsion free. □

Remark 176. *P as defined above need not be a subgroup unless G is abelian*

Remark 177. *Elements of infinite order need not generate a subgroup. Consider $b \in G$ with finite order and $c \in G$ of infinite order. Then bc and c^{-1} both have infinite order but bcc^{-1} has finite order.*

Theorem 178. *Let G be a finitely generated abelian group with periodic subgroup P. Then $G = P \oplus T$ where T is torsion free.*

Proof. By our previous result, G/P is torsion free. Assume it is non trivial. Then $G/P \simeq \oplus_{n=1}^{n} \mathbb{Z}_i$ generated by $p_{g_1}, p_{g_2}, \dots, p_{g_n}$. Then let $T = \langle g_1, g_2, \dots, g_n \rangle$. It is an excerise to show that $T \cap P = 0$, so T is torsion free. Suppose there exists a nontrivial relation

$$m_1 g_1 + \dots + m_n g_n = b$$

for some $b \in P$. Then $(P_{g_1})^{m_1} \cdots (P_{g_n})^{m_n} = P$ as $Pb = P$. But G/P is torsion free so $m_i = 0$ for all i. Thus $b = 0$. So again using our previous result $G \simeq P \times T$. □

12 Thursday 22^{nd} March

Corollary 179. *Periodic subgroup of a finitely generated abelian group is finitely generated.*

Proof. $P \simeq G/T$ so we are done. □

Remark 180. *We have:*

1. *P is uniquely determined*
2. *T is determined up to isomorphism $T \simeq G/P$.*
3. *If G is not finitely generared then it is not necesarily the case that P is a direct summand.*

Theorem 181. *A finitely generated abelian group G is isomorphic to the direct sum of finite or infinite cyclic groups.*

Proof. Take $G = P \times T$. Then expand each of P and T. □

Definition 182. *The rank of a finitely generated abelian group is the number of infinite direct summands in the direct sum decomposition.*

Theorem 183. *The rank of a finitely generated abelian group is an invariant*

Definition 184. *A finite group G has exponent m if m is the smallest integer such that every element of G has order dividing m.*

Exercise 185. *Take G a finite abelian group. Show that G has an element with order equal to it's exponent.*

12.1 Finitely Presented Groups

We now move to finitely presented groups, and begin with an example.

Example 186. *Let*

$$Q_8 = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle \simeq \langle a, b : a^2 = b^2 = (ab)^2 \rangle$$

Definition 187. *Take some set $X \neq \varnothing$ with index set Λ. So $X = \{x_\lambda : \lambda \in \Lambda\}$. Then define*

$$X^{-1} = \{x_\lambda^{-1} : \lambda \in \Lambda\}$$

Definition 188. *A word in $X \cup X^{-1}$ is an ordered set of $n \geq 0$ elements each from $X \cup X^{-1}$ with repetitions allowed. The length of the word is n.*

Example 189. *Words look like:*

$$x_{\lambda_1}^{\epsilon_1} x_{\lambda_2}^{\epsilon_2} \cdots x_{\lambda_n}^{\epsilon_n} \quad \text{where } \epsilon_i = \pm 1$$

If $n = 0$ the the word is trivial.

Example 190. *If $X = \{x, y\}$ then some words are:*

$$xyx^{-1}y, \qquad yx^{-1}yxy^{-1}$$

Definition 191. *For words, u, v, w of X, we define the product $\cdot$ as:*

$$w \cdot 1 = 1 \cdot w = w$$

And if $u = x_{\lambda_1}^{\epsilon_1} x_{\lambda_2}^{\epsilon_2} \cdots x_{\lambda_n}^{\epsilon_n}$ and $v = x_{\mu_1}^{\delta_1} x_{\mu_2}^{\delta_2} \cdots x_{\mu_m}^{\delta_m}$ then

$$u \cdot v = x_{\lambda_1}^{\epsilon_1} x_{\lambda_2}^{\epsilon_2} \cdots x_{\lambda_n}^{\epsilon_n} x_{\mu_1}^{\delta_1} x_{\mu_2}^{\delta_2} \cdots x_{\mu_m}^{\delta_m}$$

i.e. it is the concatenation of the words

Remark 192. *The set of all words on $X \cup X^{-1}$ with this product can be regarded as a semi-group (not a group as there are no inverses, yet), which are objects of study in computer science.*

Definition 193. *We say two words u, v on $X \cup X^{-1}$ are adjacent if there exist words ζ_1, ζ_2 on $X \cup X^{-1}$ and $a \in X \cup X^{-1}$ for which either*

$$u = \zeta_1\zeta_2 \qquad \textit{and} \qquad v = \zeta_1 a a^{-1} \zeta_2; \textit{or} \tag{1}$$

$$u = \zeta_1 a a^{-1} \zeta_2 \qquad \textit{and} \qquad v = \zeta_1\zeta_2 \tag{2}$$

Example 194. *$x^{-1}xyy^{-1}$ os adjacent to both yy^{-1} and $x^{-1}x$.*

Remark 195. *u is adjacent to v only if v is adjacent to u.*

Definition 196. *Let u, v be words on $X \cup X^{-1}$. We call u equivalent to v ($u \sim v$) if there exist some ζ_i for $1 \leq i \leq n$ on $X \cup X^{-1}$ such that $u = \zeta_1$, $v = \zeta_n$ and ζ_i is adjacent to ζ_{i+1} for all $1 \leq i < n$.*

Lemma 197. *$\sim$ is an equivalence relation on the set of all words on $X \cup X^{-1}$.*

Definition 198. *For words u, v on $X \cup X^{-1}$, with equivalent classes $[u], [v]$ under $\sim$. Then define the product of the classes as*

$$[u][v] = [uv]$$

Theorem 199. *The product of classes of words is well defined. The set of classes, with this product forms a group.*

Proof. Suppose $[u] = [u']$ and $[v] = [v']$. Then $u \sim u'$ and $v \sim v'$ so

$$[uv] = [u'v] = [u'v']$$

It is an exercise to show that this then satisfies the group axioms. □

Definition 200. *The free group on a non-empty set X is the set of equivalence classes of words on $X \cup X^{-1}$ with the product given above. Often write this as $F(X)$ or just F*

13 Monday 26^{th} March

Definition 201. *A word in $X \cap X^{-1}$ is called reduced if it has the form $x_{\lambda_1}^{\epsilon_1} x_{\lambda_2}^{\epsilon_2} \cdots x_{\lambda_n}^{\epsilon_n}$ where $x_{\lambda_i}^{\epsilon_i} \neq x_{\lambda_{i+1}}^{-\epsilon_{i+1}}$ for all $i < n-1$.*

Theorem 202. *Each equivalence class of words in $X \cap X^{-1}$ contains one and only one reduced word.*

Proof. Let w be a word on $X \cup X^{-1}$. If w is not reduced, then it is adjacent to a word u which is shorter. Then by induction we obtain the equivalent reduced word for w. Hence $[w]$ contains a reduced word. For uniqueness, let $w = a_1 \cdots a_n$. Define $w_0 = 1$, $w_1 = a_1$. Define

$$w_{i+1} = \begin{cases} w_i a_{i+1} & \text{if the last term of } w_i \neq a_{i+1}^{-1} \\ z & \text{if } w_i = z a_{i+1}^{-1} \text{ for some word } z \end{cases}$$

Consequently, w_i is reduced and $w_i \sim a_1 \cdots a_i$ for all $0 \leq i \leq n$. Thus $[w_n] = [w]$ and if w is already reduced then $w_n = w$.

Let u and v be adjacent words:

$$u = a_1 \cdots a_i a_{i+1} \cdots a_n$$
$$v = a_1 \cdots a_i x x^{-1} a_{i+1} \cdots a_n$$

The reduction procedure described previously give $u_j = v_j$ for all $j \leq i$. Now consider two cases: either u_i ends with x^{-1} or it does not. In the first case, $u_i = zx^{-1}$ (note z does not end with x), so $v_{i+1} = z$ and $v_{i+2} = zx^{-1} = u_i$. In the second, $v_{i+1} = u_i x$ and $v_{i+2} = u_i$. Thus in both cases $v_{i+2} = u_i$. Then continuing gives $u_{j+i} = v_{j+2+i}$ for $i < n - i$, and in particular, $u_n = v_{n+2}$.

Now suppose u and v are two reduced words in $[w]$. Then $u \sim v$ by a sequence of adjacent words k_i. But then the reduced forms of each of these adjacent words are identical, so u and v must be too. □

Corollary 203. *if $|X| = |Y|$ then $F(X) \simeq F(Y)$. I.e., the cardinality of X is an invariant of $F(X)$, and we (sometimes) call this the rank of $F(X)$.*

Lemma 204. *Every free group is torsion free.*

Proof. Suppose $[a] \in F \setminus \{1\}$ has finite order $|[a]| = n$. Take a reduced form of $a = b_r^{-1} \cdots b_1^{-1} a_1 \cdots a_s b_1 \cdots b_r$ where $a_1 \neq a_s^{-1}$ for some $r \geq 0$. Then $a^n = b_r^{-1} \cdots b_1^{-1} (a_1 \cdots a_s)^n b_1 \cdots b_r \in [a]^n = 1$ is also a reduced word of length $2r + ns = 0$. But this contradicts $n \geq 1$, so a must be the empty word. □

Remark 205. *We see:*

1. *if $X = \{x\}$ then $F(X)$ is the infinite cyclic group.*
2. *is $|X| > 1$ then $F(X)$ is non-abelian*

13.1 Free Generators

Let $X = \{x, y\}$, and $F = F(X)$. Then X has the property that any reduced word on $X \cap X^{-1}$ which is in the identity class in F must be the empty word. But consider $Y = \{[x], [x^{-1}yx]\}$. Then $\langle Y \rangle$ contains both $[x]$ and $[y]$ and so equals F. Reduced words in $[x], [y^x]$ is the conjugate of a reduced word in $[x]$ and $[y]$.

Definition 206. *A free basis for a free group F is a generating set for F with the property that the only reduced words in them inside the identity class is the empty word*

Observe that F can have many free bases, but that not every generating set is a free basis.

14 Tuesday 27^{th} March

Theorem 207. *Let $F = F(X)$ where $X = \{x_\lambda : \lambda \in \Lambda\}$. Take an arbitrary group G. If $\{g_\lambda : \lambda \in \Lambda\} \subseteq G$ then there exists a unique homomorphism $\phi : F \to G$ with $x_\lambda \mapsto g_\lambda$ for all $\lambda in \Lambda$.*

Proof. Define $\phi_0 : X \to G$ by $s_\lambda \mapsto g_\lambda$. Take $[w] \in F$ where $w = x_{\lambda_1}^{\epsilon_1} \cdots x_{\lambda_n}^{\epsilon_n}$. Define $\phi : F \to G$ by $[w] \mapsto g_{\lambda_1}^{\epsilon_1} \cdots g_{\lambda_n}^{\epsilon_n}$. It is instructive to check that ϕ is well defined: if $[u] = [v]$ then $\phi([u]) = \phi([v])$, and that it is a homomorphism. Uniqueness then follows from the fact that the images of the reduced words in $X \cup X^{-1}$ agree with the images of x_λ specified. □

Theorem 208. *Take F_m and F_n as free groups of rank m and n respecetively. Then $F_m \simeq F_n$ if and only if $m = n$.*

Proof. If $m = n$ then it is easy to show $F_m \simeq F_n$. Consider the converse; suppose $F_m \simeq F_n$. Let $G = \langle g : g^2 = 1 \rangle (\simeq \mathbb{Z}_2)$. Consider a homomorphism $\phi : F_m \to G$. This is completely determined by the images of each $x_i \in F_m$: either $x_i \mapsto g \neq 1$ or $x_i \mapsto g^0 = 1$. Thus the number of nontrivial homomorphisms from F_m onto G is $2^m - 1$ (there is also one trivial one). Suppose ϕ is non-trivial. Then $K = \ker \phi \lhd F_m$ and $F_m / K \simeq \mathbb{Z}_2$ by the first isomorphism theorem. In fact every normal subgroup of index 2 is of the form $\ker \phi$ for some non trivial ϕ. Therefore F_m has $2^m - 1$ normal subgroups of index 2. Similarly F_n has $2^n - 1$ subgroups of index 2. Thus as $F_m \simeq F_n$ we have $2^m - 1 = 2^n - 1$ and we are done. □

Corollary 209. *Every free basis for F_n has precisely n elements.*

Theorem 210. *Let $G = \langle g_\lambda : \lambda \in \Lambda \rangle$ have the property that any group H containing a subset $\{h_\lambda : \lambda \in \Lambda\}$ the map $\theta : g_\lambda \mapsto h_\lambda$ can be uniquely extended to a homomorphism of G into H. Then G is a free group and $\{g_\lambda ; \lambda \in \Lambda\}$ is a free basis of G.*

Proof. Choose H to be the free group with free basis $\{h_\lambda : \lambda \in \Lambda\}$. There exists a unique homomorphism $\phi : H \to G$ with $h_\lambda \mapsto g_\lambda$. Thus $\theta\phi h_\lambda = h_\lambda$ and $\phi\theta g_\lambda = g_\lambda$. Thus θ is an isomorphism and so G is the free group with free basis $\{g_\lambda : \lambda \in \Lambda\}$. □

Definition 211. *A group F is free on $X \subseteq F$ if, given an arbitrary group H and map $\theta : F \to H$, there exists a unique homomorphism $\theta' : F \to G$ extending θ.*

Theorem 212. *Every group is isomorphic to a factor group of a suitable free group. Every group with n generators is isomorphic to a quotient of F_n.*

Proof. Let $G = \langle g_\lambda : \lambda \in \Lambda \rangle$ and $X = \{x_\lambda : \lambda \in \Lambda\}$. Then there is a 1-1 correspondence between X and G. Let $F = F(X)$, with free basis X. There exists a surjective homomorphism $\phi : F \to G$ with $x_\lambda \mapsto g_\lambda$. Then $G \simeq F / \ker \phi$. If $|\Lambda| = n$ then F has rank n. □

Definition 213. *Let X be a set and let Δ be a set of words on $X \cup X^{-1}$. A group G has* ***Generators*** *X and* ***Relators*** *Δ if $G \simeq F/R$ where $F = F(X)$ and R is the normal closure of Δ (i.e., the smallest normal subgroup of F containing Δ). We say G has presentation $\{X : \Delta\}$ and $G = \langle X : \Delta \rangle$.*

Example 214. *Take $G = \mathbb{Z}_6 = \langle x : x^6 = 1 \rangle$. Then $G \simeq F_1 / \langle\langle x^6 \rangle\rangle^G$. x^6 is a relator. $x^6 = 1$ is a relation.*

Example 215. *$G = D_n = \langle x, y : x^n = 1, y^2 = 1, x^y = x^-1 \rangle$. Then $G \simeq F_2 / \langle\langle x^n, y^2, x^y x \rangle\rangle^G$.*

Example 216. *$Q_8 = \langle x, y : x^2 = y^2, (xy)^2 = y^2 \rangle$. Then $Q_8 \simeq F_2 / \langle\langle x^2 y^{-2}, (xy)^2 y^{-2} \rangle\rangle^G$.*

15 Thursday 29^{th} March

15.1 Group Presentations

Example 217. *Consider*

$$Q_8 = \left\langle a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle \leq GL(2, \mathbb{C})$$

Then $a^2 = b^2 = (ab^2)$. Now let F be the free group of rank 2: $F = Free\{x, y\}$. Define $\phi : F \mapsto Q_8$ by $x \mapsto a$ and $y \mapsto b$. Then $\phi(y^2x^{-2}) = 1$ and $\phi((xy)^2y^{-2}) = 1$ so $x^2y^{-2}, (xy)^2y^{-2} \in \ker\phi$. Set $K = \langle x^2y^{-2}, (xy)^2y^{-2}\rangle^F$. We claim $K = \ker phi$. Thus we can write

$$Q_8 = \langle x, y : x^2 = y^2, (xy)^2 = y^2\rangle$$

Lemma 218. *Every group has presentation (although not necessarily finite)*

Proof. Let $G = \langle X\rangle$. Then G is isomorphic to some quotient of $F = F(X)$. Declare any homomorphism $\theta : F \to G$. Let $R \subseteq F$ such that $\ker\phi = \langle R\rangle^F$. Now $G \simeq F/\ker\theta$ and so G has presentation $\{X : R\}$. □

Theorem 219 (Von Dyck's Theorem (1882))**.** *Let $G = \langle X : W_1\rangle$ and let $H = \langle X : W_2\rangle$ where $W_1 \subseteq W_2$. Then H is isomorphic to a factor group of G.*

Proof. Let $K_1 = \langle W_1\rangle^F$ and $K_2 = \langle W_2\rangle^F$. Note that $K_1 \leq K2$, and that $G \simeq F/K_1$ and $H \simeq F/K_2$. Using the third isomorphism theorem, we then have:

$$H \simeq \frac{F}{K_2} \simeq \frac{F/K_1}{K_2/K_1} \simeq \frac{G}{N}$$

□

Example 220. *Let $G = \langle a, b : a^2 = b^2\rangle$ and $H = \langle a, b : a^2 = b^2, (ab)^2 = b^2\rangle$. Then $H \simeq Q_8$ is a quotient of G. So is $H_2 = \langle a, b : a^2 = b^2, b^2 = 1\rangle$ (this is called the infinite dihedral group).*

Our strategy for using Von Dyck's theorem is:

1. Show $|G| \leq n$
2. Exhibit quotient H of order at least n
3. Deduce $|G| = n$

For $G = \langle X : R\rangle$ and $H = \langle X : R, \dots\rangle$.

Example 221. *Define $G = \langle a, b, c, d : ab = c, bc = d, cd = a, da = b\rangle$. We show that $|G| \leq 5$ by consideration of the relations. Then define $\phi : F = \langle a, b, c, d\rangle \to \mathbb{Z}/5 \simeq \mathbb{Z}_5 \simeq H$ by*

$$a \mapsto [1]$$
$$b \mapsto [3]$$
$$c \mapsto [4]$$
$$d \mapsto [2]$$

It is clear that $abc^{-1}, \dots dab^{-1} \in \ker \phi$ *so by Von Dyck's* H *is isomorphic to a quotient of* G. $|G| \geq 5$ *and so we are done.*

Example 222. *Let* $G = \langle a, b : a^4 = b^2, b^{-1}ab = a^{-1} \rangle$. *We note that* a^4 *is central in* G*; it is a power of both* a *and* b *and so commute with both. Then* $a^4 = b^{-1}a^4b = (b^{-1}ab)^{-1} = (a^{-1})^4$, *so* $a^8 = 1$. *Hence* $\langle a \rangle^G \lhd G$. *Note that* $|\langle a \rangle| \leq 8$ *so* $|G| \leq 16$.

Now, let

$$H = \left\langle A = \begin{pmatrix} 3 & 3 \\ -3 & 3 \end{pmatrix}, B = \begin{pmatrix} 0 & 4 \\ 4 & 0 \end{pmatrix} \right\rangle \leq GL(2, 17)$$

We claim $|H| = 16$. *We also claim that* $A^4 = B^2$ *and* $B^{-1}AB = A^{-1}$. *Thus we can use Von Dyck, and* $|G| = 16$.

16 Monday 16^{th} April

Lemma 223. *D_n is the dihedral group of order $2n$ (for $n \geq 3$) then*

$$D_n \simeq \langle s, t : s^n = 1, t^2 = 1, s^t = s^{-1} \rangle$$

Theorem 224. *Let G be a finite group generated by 2 involutions (elements of order 2). Then $G \simeq D_n$ for some n.*

Proof. If G is finite, then $|ab| = n$ for involutions a, b. Let $s = ab$. Then

$$asa = aaba = ba = (ab)^{-1} = s^{-1}$$

Hence:

$$|\langle a, b \rangle| = |\langle a, s \rangle| = m$$

for some m. Suppose for a contradiction that $as^i = 1$ for some $i \geq 0$. Choose minimal i with $as^i = 1$. $i \neq 0$ and $a \neq 1$. But also $i \neq 1$ as else $1 = as = aab = b$. But also $1 = as^i = aabs^{i-1} = bs^{i-1}$. Then conjugation by b gives

$$1 = s^{i-1}b = s^{i-2}abb = s^{i-2}a$$

Then conjugation by a gives $1 = as^{i-2}$ which contradicts the minimality of i. Thus as^ineq1 for all $i \geq 0$, and so $as^i \neq s^j$ for all $i \neq j$. Thus

$$\langle a, b \rangle \geq \langle s \rangle \cup a\langle s \rangle$$

and so $|\langle a, b \rangle| = |\langle a, s \rangle| \geq 2n$. Now define

$$H = \{a^j s^i : 0 \leq j < 2, 0 \leq i < n\} \leq G$$

Then $|H| = 2n$ and $\langle a, s \rangle \leq H$ so $|\langle a, b \rangle| = |langlea, s\rangle| = 2n$, and so $\langle a, b \rangle \simeq D_n$. □

Theorem 225. *Let p be prime. Then every group G of order $2p$ is either cyclic or dihedral.*

Proof. If $p = 2$, then $|G| = 4$ for which the claim is true. Otherwise, p is odd and so G has an element s of order p and an element t of order 2. Let $H = \langle s \rangle$, so $|G : H| = 2$ and $H \lhd G$. Thus $t^{-1}st = tst = s^i$ for some i. Thus $s = t^2st^2 = ts^it = s^{i^2}$, and so $i^2 \equiv 1 \mod p$. But as p is prime, $1 \equiv \pm 1 \mod p$. Therefor $tst = s$ or $tst = s^{-1}$. In the first case,

$$\langle s, t : tsts6{-}1, t^2, s^p \rangle \simeq \mathbb{Z}_{2p}$$

In the second,

$$\langle s, t : tsts, t^2, s^p \rangle \simeq D_p$$

□

Theorem 226. *If $|G| = pq$ for distinct primes $p > q$. Either*

1. *G is cyclic*
2. *$G = \langle a, b : a^p = 1, b^q = 1, b^a = b^m \rangle$ where $m^q \equiv 1 \mod p$ and $m \neq 1 \mod p$*

And, if q does not divide $p - 1$, then the second case does not exist.

16.1 Classification of 2-generated groups of order 8

Let $x \in G$ of maximal order m. Then $m \in \{2, 4, 8\}$ by Lagrange. If $m = 8$, then G is cyclic so $m \neq 8$. If $m = 2$, then G is abelian. Suppose $m = 4$ let $H = \langle x \rangle$ so $|H| = 4$. Then $H \lhd G$. Let $y \in G/H$. Then $y^2 \in H$, and $x^y \in H$ and H is normal in G. Observe this means $y^2 = x^i$ and $x^y = x^j$ for some $i, j \in \{0, 1, 2, 3\}$. if $i = 1$ or $i = 3$, then $|y| = 8$ which is a contradiction, so $i \in \{0, 2\}$. Also $j \in \{1, 3\}$ as the orders are the same for conjugate pairs. Thus there are 4 posibilities:

1. $R = \{x^4, y^2, x^y = x\}$
2. $R = \{x^4, y^2 = x^2, x^y = x\}$
3. $R = \{x^4, y^2, x^y = x^3\}$
4. $R = \{x^4, y^2 = x^2, x^y = x^3\}$

The first two cases give groups isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$. The third gives D_4, and the final case gives the Quaternion group. The last two cases can be seen by applications of von Dyck's theorem.

16.2 Free Abelian Groups

Take an abelian group G. Take $x_1, \dots x_r \in G$. Then any integral linear combination (i.e, a linear combination over $\mathbb{Z}$) is an element of G. Define a basis for G as a generating set X such that any finite sequence of elements of X, the only vanishing integral linear combination is the trivial one. If an abelian group has a basis, then it is a free abelian group.

Example 227. *Consider $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (with n terms). This has natural basis $e_i = (0, \dots, 1, \dots, 0)$ with the one in the i^{th} position.*

17 Tuesday 17^{th} April

17.0.1 Subgroups of $\mathbb{Z}^n$

Take $H \leq \mathbb{Z}^n$. Then H is generated by at most n elements, call this number m. We can represent H as an $m \times n$ matrix A whose rows generate H.

Definition 228. *$S(A)$ is the set of all linear combinations of the rows of A. i.e.,*

$$S(A) = \{uA : u \in \mathbb{Z}^{n*}\}$$

We want to solve the decidability of membership in H, or equivalently membership in $S(A)$ for a given $m \times n$ matrix A. Our approach is to use row-equivalence to get a matrix B with $S(A) = S(B)$, but which is easier to describe.

Definition 229. *Two matrices A and B are **Row-equivalent** (and write $A \sim B$) if one can be transformed to the other using the operations:*

1. *Interchang rows;*
2. *Multiplying a row by -1; or*
3. *Adding an integral multiple of one row to another (distinct) row.*

*We call these the **Integral Row Operators**.*

Lemma 230. *If A is row-equivalent to B then $S(A) = S(B)$, and the subgroups generated by A and B are identical.*

Definition 231. *A is in **Row Hermite Normal Form** if:*

1. *First r rows of A are non-zero;*
2. *For $1 \leq i \leq r$, the index of the first non-zero entry in row i, j_i, satisfies $j_1 < j_2 < j_3 < \dots j_r$;*
3. *$A_{i,j_i} > 0$ for $1 \leq i \leq r$; and*
4. *If $1 \leq k < l < r$ then $0 \leq A_{k,j_k} < A_{l,j_l}$.*

Example 232. *The matrix:*

$$A = \begin{bmatrix} 2 & 1 & 5 & 0 & -1 & 1 & -1 \\ 0 & 3 & -1 & 2 & 4 & 0 & 2 \\ 0 & 0 & 0 & 4 & 7 & 1 & 8 \\ 0 & 0 & 0 & 0 & 0 & 2 & 5 \end{bmatrix}$$

is in row-hermite form. Consider $v = (6, 0, 16, 6, 4, 13, 31)$, is $v \in S(A)$? This is equivalent to there being a $u = (a, b, c, d) \in \mathbb{Z}^4$ such that $uA = v$. Thus $2a = b$, $a + 3b = 0$, $2b + 4c = b$, $a + c + 2d = 13$. Solving these shows that indeed $v \in S(A)$.

Theorem 233. *Given an integral matrix B, there exists a unique matrix A in row hermite normal form with $B \sim A$.*

Example 234. *Take $G = \mathbb{Z}^4 = \langle g_1, g_2, g_3, g_4 \rangle$, and $H = \langle g_1 + 2g_2 + g_4, 3g_1 + g_2 + 2g_3 - g_4, -2g_1 + g_2 + 4g_4 \rangle$. Then let $v = 7g_1 + 6g_3 - 3g_4$. Is $v \in H$? We take the representation of H:*

$$B = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 3 & 1 & 2 & -1 \\ -2 & 1 & 0 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 4 & 6 \\ 0 & 0 & 8 & 10 \end{bmatrix} = A$$

Then $(7, 0, -1)A = v$ so $v \in S(A) = S(B)$.

17.1 Abelian Quotients

Recall for group G, $G' = \langle [x, y] : x, y \in G \rangle$ is called the derived group of G

Lemma 235. *$G' \triangleleft G$. $H = G/G'$ is abelian. If $N \triangleleft G$, G/N is abelian if and only if $N \geq G'$. Thus G/G' is the largest abelian quotient of G.*

Lemma 236. *For a given $G = \langle \{x_1, \dots, x_r\} : R \rangle$, define $C = \{[x_i, x_j] : i \leq i < j \leq r\}$. Then $G_{ab} = \langle X : R, C \rangle$.*

Proof. It suffices to prove that G' coincides with the normal closure $\overline{C}$ of C in G. Since the generators of G_{ab} all commute, G_{ab} is abelian and so $G' \subseteq \overline{C}$. But by definition $\overline{C} \subseteq G'$ so $\overline{C} = G'$. Thus $G_{ab} = \langle X : R, C \rangle$. □

17.2 Finitely Generated Abelian Groups

For an abelian group $G = \langle g_1, \dots, g_n \rangle$, define a surjection $f : \mathbb{Z}^n \to G$ by:

$$(a_1, \dots a_n) \mapsto a_1 g_1 + \dots + a_n g_n$$

Observes that f is a homomorphism, and that

$$G \simeq \mathbb{Z}^n / \ker f$$

Let $H = \ker f$. $H \leq \mathbb{Z}^n$ so H is finitely generated too, and so we can represent H by a matrix A where $H = S(A)$.

Example 237. *$f : \mathbb{Z}^5 \to \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z} \oplus \mathbb{Z}$ with*

$$(a, b, c, d, e) \mapsto ([a]_2, [b]_4, [c]_{12}, d, e)$$

Then $kerf = \{(a, b, c, d, e) : 2|a, 4|b, 12|c, d = e = 0\}$. Set

$$A = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 12 & 0 & 0 \end{bmatrix}$$

Then $H = S(A)$, and

$$\mathbb{Z}^5 / H \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z} \oplus \mathbb{Z}$$

18 Thursday 19^{th} April

Definition 238. *Two matrices A and B are equivalent (over $\mathbb{Z}$) if one can be obtained from the other using elementary row and column operations. We write $A \sim B$.*

Remark 239. *This is equivalent to there being matrices P and Q with $A = PBQ$ with* $\det P, \det Q = \pm 1$.

Lemma 240. *$A \sim B$ if and only if*

$$\frac{\mathbb{Z}^n}{S(A)} \simeq \frac{\mathbb{Z}^n}{S(B)}$$

Definition 241. *A $m \times n$ integral matrix A is in **Smith Normal Form** if for some $k \geq 0$ the entries $d_i = A_{ii}$ are positive for $1 \leq i \leq k$ and $d_i | d_{i+1}$.*

Lemma 242. *If*

$$A = \begin{bmatrix} d_1 & & & & & & & \\ & d_2 & & & & & & \\ & & \ddots & & & & & \\ & & & d_k & & & & \\ & & & & \ddots & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 0 \end{bmatrix}$$

Then

$$\frac{\mathbb{Z}^n}{S(A)} \simeq \mathbb{Z}_{d_1} \oplus \mathbb{Z}^{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^{n-k}$$

Lemma 243 (Smith Normal Form Construction)**.** *Let M be an $l \times m$ matrix over $\mathbb{Z}$ (with $l \geq n$). Then there exists invertible matrices $P \in GL(n, \mathbb{Z})$ and $Q \in GL(l, \mathbb{Z})$ such that $D = QMP$ is diagonal with non-negative integer entries $d_1, \dots, d_n$ with $d_i | d_{i+1}$ for all $i \leq n-1$. The matrix D is in Smith Normal Form.*

Example 244.

$$A = \begin{pmatrix} 4 & 2 & 1 & 8 \\ -4 & 4 & 2 & -8 \\ 4 & -1 & 1 & 2 \\ 4 & 5 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & & & \\ & 3 & & \\ & & 12 & \\ & & & 0 \end{pmatrix}$$

Example 245. *Take $G = \langle x, y : (xy^3x^{-2})^2, y^{-1}x^2y^2 \rangle$. What is G/G'?*

$$\begin{aligned} \frac{G}{G'} &= \langle x, y : \dots, [x, y] = 1 \rangle \\ &= \langle x, y : 2x + 6y - 4x, -y + 2x + 2y \rangle \\ &= \langle x, y : -2x + 6y, 2x + y \rangle \\ &\simeq \mathbb{Z}^/ \langle -2x + 6y, 2x + y \rangle \end{aligned}$$

The matrix $A = \begin{pmatrix} -2 & 6 \\ 2 & 1 \end{pmatrix}$ is the relation matrix describing H, i.e. $S(A) = H$. A has Smith Normal Form $B = \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix}$. Thus

$$\frac{G}{G'} \simeq \frac{\mathbb{Z}^2}{S(A)} \simeq \frac{\mathbb{Z}^2}{S(B)} \simeq \mathbb{Z}_{14}$$

Example 246. *Take $G = \langle a,b,c : a^2c^{-1}, bc^2b, cab^4\rangle$. Then*

$$\frac{G}{G'} \simeq \frac{\mathbb{Z}^3}{S(A)} \qquad \text{where } A = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & 2 \\ 1 & 4 & 1 \end{pmatrix} \sim B = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 10 \end{pmatrix}$$

Thus $G/G' \simeq \mathbb{Z}_{10}$

Example 247. *Take $G = \langle x,y,z : (xyz^{-1})^2, (x^{-1}y^2z)^2, (xy^{-2}z^{-1})^2\rangle$ Then*

$$A = \begin{pmatrix} 2 & 2 & -2 \\ -2 & 4 & 2 \\ 2 & -4 & -2 \end{pmatrix} \sim \begin{pmatrix} 2 & & \\ & 6 & \\ & & 0 \end{pmatrix}$$

So $G/G' \simeq \mathbb{Z}_2 \times \mathbb{Z}_6 \simeq \mathbb{Z}$.

Theorem 248 (Basis Theorem for Finitely Generated Abelian Groups)**.** *Given a finitely generated abelian group G, there exist integers $k, n \geq 0$ and $d_i \geq 2$ for $1 \leq i \leq k$ where $d_i | d_{i+1}$ for $1 \leq i \leq k$, such that*

$$G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^{n-k}$$

Note k, n, d_i are determined with the isomorphism type of G.

Example 249. *If $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$ then $G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{36}$*

18.1 Deficiency of Presentations

Definition 250. *Let $G = \langle X : R\rangle$ with $|X|, |R| < \infty$. Define the **Deficiency** of G as Def$(G) = |X| - |R|$*

Example 251. *We have:*

1. *$G = \langle x : x^2\rangle$ has deficiency of 0*
2. *$H = \langle x : x^2, x^4\rangle \simeq G$ has deficiency -1*
3. *$A = \langle x : x^6\rangle$ has deficiency of 0*
4. *$B = \langle x,y : x^2, y^3, [x,y]\rangle \simeq A$ has deficiency of -1*
5. *$P = \langle x,y : x = (xy)^3, y = (xy)^4\rangle$ has deficiency of 0*

Lemma 252. *Take $G = \langle X : R\rangle$ with X and R finite. If G is finite then $|X| \leq |R|$.*

Proof. Assume $|X| > |R|$. Then the relation matrix for this presentation has fewer rows than columns The number of d_i for G_{ab} is less than $|X|$. Thus there exists one infinite cyclic factor in G/G'. Thus G_{ab} is infinite, and so G must be too. □

Corollary 253. *Every group with $|X| > |R|$ (i.e., positive deficiency) is infinite.*

Remark 254. *The converse is not true, i.e., if a group has negative deficiency it need not be finite.*

19 Monday 24^{rd} April

19.1 Residually Finite Groups

Definition 255. *Let P be a property, and say G has property P* ***residually*** *if for all $x \in G \setminus \{1\}$, there exists a normal subgroup $N_x \lhd G$ such that $x \notin N_x$, and g/N_x has property P.*

Remark 256. *We will only consider the property that P is finite. I.e., G is residually finite if for all $x \in G \setminus \{1\}$ there exists a normal subgroup N_x such that $x \notin N_x$ and $|G : N_x| < \infty$.*

Theorem 257. *Every free group is residually finite.*

Proof. Let F have free basis $\{x_\lambda : \lambda \in \Lambda\}$. Take a reduced word $x = x_{\lambda_1}^{\epsilon_1} \cdots x_{\lambda_n}^{\epsilon_n}$. Let $S = \mathrm{Sym}(n+1)$. Define a homomorphism $\phi : F \to S$. Let $x_{\lambda_i} \mapsto \sigma_{\lambda_i} \in S$ where $\sigma_{\lambda_i}^{\epsilon_i}$ maps i to $i+1$. Then $\phi(x_\lambda) = 1$ if $\lambda \notin \{\lambda_1, \ldots, \lambda_n\}$. Thus σ_{λ_i} maps $i = i+1$ if $\epsilon_i = 1$ and $i+1$ to i if $\epsilon_i = -1$. This map is injective, as otherwise we get a contradiction on the reduced words. By the universal property, this map then extended to a (unique) homomorphism $\phi : F \to S$. It is then easy to check that $x \notin \ker\phi$ and $F/\ker\phi \simeq S$ and so is finite. □

Corollary 258. *The intersection of all subgroups of finite index in a free group is $\{1\}$.*

Proof. Let x be in the intersection of all subgroups of finite index. If $x \neq 1$, then there exists a normal subgroup N_x of finite index not containing x, a contradiction. □

19.2 Structure of (Finite) Groups

Recall that if $H \leq G$ and $N \lhd G$ then $HN \leq G$, and $H/(H \cap N) \simeq NH/N$ by the second Isomorphism Theorem. If $N, M \lhd G$ and $N \leq M$ then $\frac{G/N}{M/N} \simeq G/M$ by the correspondence theorem.

Definition 259. *A* ***Subnormal Series*** *of a group G, is a finite series of subgroups $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = 1$.*

Example 260. *Take $G = S_3$. Then a subnormal series is $S_3 \rhd \langle(123)\rangle \rhd \{e\}$. If $G = S_4$, we could take*

$$G \rhd V = \langle(12)(34), (13)(24)\rangle \rhd U = \langle(12)(34)\rangle \rhd 1$$

Definition 261. *If G has two subnormal series, then we say that the second is a refinement of the first if each member of the first is also a member of the second.*

Example 262. *The subnormal series $S_4 \rhd A_4 \rhd V \rhd U \rhd 1$ is a refinement of previous example.*

Definition 263.

$$\{G_{i-1}/G_i : 1 \leq i \leq r\} \quad \textit{and} \quad \{H_{i-1}/H_i : 1 \leq i \leq s\}$$

such that corresponding factor groups are isomorphic.

Example 264. *The group $\mathbb{Z}_6$ has isomorphic subnormal series:*

$$\mathbb{Z}_6 \rhd \mathbb{Z}_3 \rhd 1$$
$$\mathbb{Z}_6 \rhd \mathbb{Z}_2 \rhd 1$$

Theorem 265 (Refinement Theorem)**.** *Any two subnormal series of a given group G have isomorphic refinements.*

Definition 266. *A composition series of G is a subnormal series without repetitions which cannot be further refined.*

Proposition 267. *If $G \rhd G_1 \rhd \cdots G_r = 1$ is a composition series then G_i/G_{i+1} is simple.*

Example 268. *The most refined subnormal series of S_4 from the previous example is a composition series.*

20 Tuesday 24^{th} April

Lemma 269 (Zassenhaus / Butterfly Lemma)**.** *Given $A, B \leq G$ and $X \lhd A$ and $Y \lhd B$:*

1. $X(A \cap Y) \lhd X(A \cap B)$;
2. $Y(B \cap X) \lhd Y(A \cap B)$; *and*
3. $\dfrac{X(A \cap B)}{X(A \cap Y)} \simeq \dfrac{Y(A \cap B)}{Y(B \cap X)}$

Proof. We leave the proof of (1) and (2) as an exercise. Since $A \cap B \leq A$ and $X \lhd A$, $X(A \cap B) \leq A$. But also $X \lhd X(X \cap B)$, so by the second isomorphism theorem,

$$\frac{X(A \cap B)}{X} \simeq \frac{A \cap B}{X \cap B}$$

Then applying the third isomorphism theorem gives us that $\frac{A \cap B}{(X \cap B)(A \cap Y)}$ is isomorphic to a factor group of $\frac{A \cap B}{X \cap B} \simeq \frac{X(A \cap B)}{X}$. If we can define $\phi : \frac{X(A \cap B)}{X} \to \frac{A \cap B}{(A \cap Y)(B \cap X)}$ such that $\ker \phi = \frac{X(A \cap Y)}{X}$, then:

$$\frac{X(A \cap B}{X(A \cap Y)} \simeq \frac{A \cap B}{(X \cap B)(A \cap Y)} \simeq \frac{Y(A \cap B)}{Y(B \cap X)}$$

If $Xk \in \ker \phi$, with $k \in A \cap B$, then $k \in (A \cap Y)(X \cap B)$, and so it follows that $K \leq X(A \cap Y)$ (as $K \geq X$). Conversely take, $k \in X(A \cap Y) \subseteq X(A \cap B)$ whose image is trivial. Then $\frac{K}{X} = \frac{X(A \cap Y)}{X}$ and thus $\ker \phi = \frac{X(A \cap Y)}{X}$. □

Proof of Refinement Theorem. Let the two subnormal series be:

$$\begin{aligned} G &= G_0 \rhd G_1 \rhd \cdots \rhd G_{i-1} \rhd G_i \rhd \cdots \rhd G_r = 1 && (1) \\ &= H_0 \rhd H_1 \rhd \cdots \rhd H_{j-1} \rhd H_j \rhd \cdots \rhd H_s = 1 && (2) \end{aligned}$$

We construct a refinement of (1) by inserting between G_{i-1} and G_i the following:

$$G_{i-1} = G_i(G_{i-1} \cap H_0) \rhd G_i(G_{i-1} \cap H_1) \rhd \cdots \rhd G_i(G_{i-1} \cap H_s) = G_i$$

Now the butterfly lemma implies that $G_i(G_{i-1} \cap H_{j-1} \rhd G_i(G_{i-1} \cap H_j)$, so this is indeed a refinement of (1). Similarly, construct a refinement of H by inserting

$$H_{j-1} = H_j(H_{j-1} \cap G_0) \rhd H_j(H_{j-1} \cap G_1) \rhd \cdots \rhd H_i(H_{j-1} \cap G_r) = H_j$$

and again the butterfly lemma show that this is a refinement. Both of these refinements are of length rs. Now we again apply the butterfly lemma to get:

$$\frac{G_i(G_{i-1} \cap H_{j-1})}{G_i(G_{i-1} \cap H_j} \simeq \frac{H_j(G_{i-1} \cap H_{j-1})}{H_j(G_i \cap H_{j-1})}$$

for $1 \leq 1 \leq r$ and $1 \leq j \leq s$. □

Theorem 270 (Jordan-Hölder Theorem)**.** *In a group G with a composition series, every composition series for G is isomorphic to the given one.*

Proof. From the refinement theorem there exists isomorphic refinements of any to subnormal series, and since composition series cannot be further refined, they must be isomorphic. □

Corollary 271. *The composition factors and their multiplicities are a group invariant.*

Remark 272. *If G is a finite abelian group, then the composition factors are abelian groups and hence are cyclic of prime order.*

Remark 273. *It is not the case that knowledge of the composition factors gives knowledge of the group isomorphism type. For example, $\mathbb{Z}_4 \rhd \mathbb{Z}_2 \vartriangle 1$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \rhd \mathbb{Z}_2 \rhd 1$ have the same composition factors.*

Lemma 274. *Any composition factor of a group is a simple group.*

Proof. Take $G \rhd \cdots \rhd G_{i-1} \rhd G_i \rhd \cdots \rhd 1$, and suppose G_{i-1}/G_i is not simple. Then there exists some $N/G_i \lhd G_{i-1}/G_i$ and by the correspondence theorem $G_{i-1} \rhd N \rhd G_i$, which contradicts the definition of a composition series. □

Lemma 275. *A simple abelian group is cyclic of prime order. A composition factor of a finite abelian group is cyclic of prime order.*

Proof. If G is a simple abelian group, then for $1 \neq x \in G$ we have $\langle x \rangle G$ and $\langle x^2 \rangle \leq \langle x \rangle$. But G is simple, so there are two cases: if $\langle x^2 \rangle = 1$ then $G = \mathbb{Z}_2$; else $\langle x^2 \rangle = G$, so $x \in \langle x^2 \rangle$ and thus x^{2n} for some $n \in \mathbb{N}$. Thus $|x|$ is finite and so G is finite. Take $p||G|$. Then there exists some $H \lhd G$ with $|H| = p$ and so $|G| = p$. □

21 Thursday 26^{th} April

Remark 276. *Not every group has a composition series, for example* $(\mathbb{Z},+)$*. There certainly exist subnormal series, but every one can be refined.*

21.1 Soluble groups

These are also sometimes called solvable groups.

Definition 277. *A group* G *has a* ***normal series*** *if the series:*

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

with $G_i \lhd G$*.*

Example 278. $S_4 \rhd A_4 \rhd V \rhd 1$ *(with* V *from the previous context) is a normal series.*

Definition 279. *A group* G *is* ***soluble*** *if it has a normal series:*

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

where G_i/G_{i+1} *is abelian for all* $1 \leq i \leq r-1$*.*

Remark 280. *If* G *is abelian, then* G *is soluble.*

Example 281. S_3*, which has the series* $S_3 \rhd A_3 \rhd 1$*, is soluble.*

Remark 282. *Recall that if* G/N *is abelian then* $G' \leq N$*. So* G_i/G_{i+1} *then* $G_i' \leq G_{i+1}$*.*

Definition 283. *The derived series of* G *is a descending series of subgroups*

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(r)} = 1$$

Where $G^{(1)} = [G^{(0)}, G^{(0)}] = G'$ *and* $G^{(i+1)} = [[G^{(i)}, G^{(i)}]$*.*

Example 284. $S_4 \rhd A_4 \rhd V \rhd 1$ *(with* V *from the previous context) is the derived series of* G*.*

Lemma 285. *IF* $\{G^{(i)}$ *is a derived series for* G *then:*

1. $G^{(i)}$ *is characteristic in* G *for all* i*;*
2. $G^{(i)}/G^{(i+1)}$ *is abelian; and*
3. *If* $G_0 \rhd G_1 \rhd \cdots \rhd G_n = G$ *be an abelian series, then* $G^{(i)} \leq G_i$ *for each* i

Proof.

1. Induction
2. Direct by the previous remark
3. The base case is clear, the induct on the indices. as $G^{(i+1)} = G^{(i)\prime} \leq (G_i)' \leq G_{i+1}$ because G_i/G_{i+1} is abelian.

□

Definition 286. *If* $G^{(n)} = 1$ *for some* n*, then the smallest such* n *is called the* ***Derived Length*** *of* G*. We write* $dl(G) = n$*.*

Corollary 287. *G is soluble if and only if there exists an n such that $G^{(n)} = 1$.*

Corollary 288. *If G is soluble then $dl(G)$ is the minimum length of any abelian series for G.*

Theorem 289. *The following are equivalent:*

1. *G is soluble;*
2. *G has a subnormal series $\{G_j\}$ such that each G_i/G_{i+1} is abelian.*
3. *There exists an n such that $G^{(n)} = 1$.*

Proof. (1) implies (2) by definition. (2) implies (3) through a simple inductive argument. (3) implies (1) as the derived series is a normal series with abelian factors. □

Example 290. *Take $G = SL(2,3)$. Then $G \triangleright G' \triangleright G'' = Z(G) \triangleright G^{(3)} = 1$, and hence $SL(2,3)$ is a soluble group.*

Exercise 291. *Is $G = SL(2,5)$ soluble?*

Theorem 292. *Subgroups and factor groups of a soluble group are themselves soluble.*

Proof. If $S \leq G$ then $S^{(\mathrm{dl}(G))} \leq G^{(\mathrm{dl}(G))} = 1$ so S is soluble.

If $N \triangleleft G$ and ϕ is the canonical homomorphism from G to G/N, then $\phi(G^{(k)}) = (G/N)^{(k)}$ (which can be seen by a simple induction), and so

$$1 = \phi(\{1\}) = \phi(G^{(\mathrm{dl}(G))}) = (G/N)^{(\mathrm{dl}(G))}$$

and thus G/N is soluble. □

Lemma 293. *Suppose $N \triangleleft G$, and that G/N and N are both soluble. Then G is soluble and $dl(G) = dl(G/N) + dl(N)$.*

Proof. Take

$$\frac{G}{N} = \frac{G_0}{N} \geq \cdots \geq \frac{G_s}{N} = \frac{N}{N}$$
$$N = N_0 \geq N_1 \geq \cdots \geq N_t = 1$$

Then each G_i contains N, and $G_i \triangleleft G_{i-1}$. G_{i-1}/G_i is abelian because it is isomorphic to $\frac{G_{i-1}/N}{G_i/N}$ by the third isomorphism theorem. Hence

$$G = G_0 \geq \cdots \geq G_{s-1} \geq N_0 \geq \cdots \geq N_t = 1$$

□

Remark 294. *Just because G/N and N are abelian, G need not be abelian. Consider $G = S_3$ and $N = A_3$.*

22 Monday 30^{th} April

Lemma 295. *The direct product of a finite set of soluble groups is soluble.*

Proof. Take $G = G_1 \times G_2$. Since G_1 is soluble $G/G_1 \simeq G_2$ is soluble, and so G is soluble. □

Remark 296. *A finite group need not be soluble even if all its subgroups are soluble. Consider A_5, for example.*

22.1 Chief Series

Definition 297. *A* ***Chief Series*** *of G is a series of normal subgroups*

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

such that each factor G_i/G_{i+1} is a minimal normal subgroup of G/G_{i+1} for $0 \leq i < r$.

Remark 298. *This is a normal series that cannot be further refined, analogous to how a composition series is a subnormal series that cannot be further refined.*

Example 299. *Take $S_4 \leq A_4 \leq V \leq 1$ as a chief factors of S_4, with chief factors $\mathbb{Z}_2, \mathbb{Z}_3$, and $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Remark 300. *The refinement theorem and Jordan / Hölder theorem's have analogues in normal / chief series:*

- *Any two normal series have isomorphic refinements; and*
- *The chief series of G is unique.*

The proofs are also analogous.

Lemma 301. *Let N be a minimal normal subgroup of a group G that is finite and soluble. Then N is an elementary abelian p-group for some prime p.*

Exercise 302. *If $N \lhd G$ and K characteristic in G then $K \lhd G$.*

Proof. As $N > 1$ and N is soluble, $N' < N$, and $N' \lhd G$. But then as N is minimal, so $N' = 1$ and hence N is abelian.

Now take $p \big| |N|$ and let $A = \{x \in N : x^p = 1\}$. Then $1 < A < N$ as N is abelian, and A is characteristic in N, so it is normal in G. But then again N is mininal, so we must have $A = N$, and so N is a p-group. □

Corollary 303. *All chief factors of finite soluble groups are elementary abelian p-groups for various primes p.*

Definition 304. *A group G is* **characteristically simple** *if the only characteristic subgroups of G are 1 and G.*

Lemma 305. *Every chief factor of a group G is characteristically simple.*

Proof. $G_i/G_{i+1} \lhd G/G_{i+1}$, so if K/G_{i+1} is characteristic in G_i/G_{i+1} then it is normal in G/G_{i+1}, so $K \lhd G$ and so either $K = G_i$ or $K = G_{i+1}$. □

Theorem 306. *A finite characteristically simple group is a direct product of isomorphic simple groups.*

The proof is left as an exercise. We have already done this for finite simple G.

Theorem 307. *Let M be a proper maximal subgroup of a finite soluble group G. Then $|G : M|$ is a prime power.*

Proof. Let L be maximal among normal subgroups of G contained in M, i.e. $L = \mathrm{Core}_G(M)$. Since $L \lhd G$, take K/L as a chief factor of G (Take K such that K/L is minimal in G/L). Then $K > L$ and $K \lhd G$, so K is not contained in M. Thus $KM > M$ and so $KM = G$. By the second isomorphism theorem, $|G : M| = |K : K \cap M||K : L|$. But K/L is a chief factor, and hence is an elementary abelian group and so $|K : L|$ is a prime power, and so $|G : M|$ is too. □

Remark 308. *The last result does not hold without the soluble hypothesis, as otherwise we cannot claim K/L is a chief factor. Consider again A_5 with 3 conjugacy classes of maximal subgroups with indices* $5, 6, 10$. *Also $PSL(2,7) = SL(2,7)/\mathbb{Z}$ has maximal subgroups of indices* 7 *and* 8.

23 Tuesday 1^{st} May

Nilpotent Groups

Recall that a finite group G is called nilpotent if all its Sylow p-subgroups are normal in G. In this case:

$$G = \prod_{p \in \pi} S_p \qquad \text{where } \pi = \{\, \text{primes dividing } |G|\}$$

We now generalise.

Definition 309. *A group G is nilotent if G has a finite series*

$$G = G_o > G_1 > \cdots > G_r = 1$$

where $G_i/G_{i+1} \leq Z(G/G_{i+1})$ for $0 \leq i < r$.

Remark 310. *Such a series is a normal series, as $G_i/G_{i+1} \leq Z(G/G_{i+1})$ implies $G_i/G_{i+1} \lhd G/G_{i+1}$ and so $G_i \lhd G$.*

Example 311. *Abelian groups are nilpotent, which can be seen by taking the series $G = G_0 \rhd G_1 = 1$.*

Example 312. *Consider $G = D_4 = \langle (1234), (14)(23) \rangle$. Then the series $D_4 > Z(D_4) = \langle (13)(24) \rangle > 1$ show that D_4 is nilpotent.*

Example 313. *The series*

$$D_8 > \langle (1753)(2864) \rangle > \langle (15)(26)(37)(48) \rangle > 1$$

show D_8 is nilpotent.

Example 314. *We can show S_3 is not nilpotent as this would imply A_3 is in the center of S_3, but this is just the trivial subgroup. In general nilpotent groups cannot have a trivial centre.*

Remark 315. *Nilpotency implies solubility.*

Lemma 316. *Let $G = G_0 \rhd \cdots \rhd G_r = 1$ be a normal series for G. It is a central series if and only if $[G_i, G] \leq G_{i+1}$ for $0 \leq i < r$.*

Proof. $G_i/G_{i+1} \leq Z(G/G_{i+1})$ if and only if $[xG_{i+1}, yG_{i+1}] = G_{i+1}$ for $x \in G_i$ and $y \in G$. But this is equivalent to $[x,y]G_{i+1} = G_{i+1}$, or $[x,y] \in G_{i+1}$. Hence $[G_i, G] \leq G_{i+1}$. □

Lemma 317. *Subgroups and factors groups of nilpotent groups are nilpotent.*

Proof. Take a central series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = 1$. Let $S \leq G$. Then the series

$$S = S \cap G_0 \geq S_1 = S \cap G_1 \geq \cdots \geq S \cap G_i \geq \cdots \geq S \cap G_r = 1$$

has $S_i = S \cap G_i \lhd S$. and $[S_i, S] \leq S_{i+1}$, so this is a central series of S. Now take $N \lhd G$. Then consider the series

$$\frac{G}{N} = \frac{G_0 N}{N} \geq \frac{G_1 N}{N} \geq \cdots \frac{G_r N}{N} = N$$

For each i, $G_iN/N \trianglerighteq G_{i+1}N/N$, so for $x \in G$ and $y \in G_{i-1}$ we have $[yN, xN] = [y,x]N \in G_iN/N$. Thus $[G_{i-1}N/N, G/N] \leq G_iN/N$. □

Lemma 318. *The direct product of a finite set of nilpotent groups is nilpotent*

Proof. Take nilpotent groups H, K with respective central series:

$$H = H_0 \geq \cdots \geq H_r = 1$$
$$K = K_0 \geq \cdots \geq K_r = 1$$

Then the series

$$H_0 \times K_0 \geq H_1 \times K_1 \geq \cdots \geq H_r \times K_r = 1$$

is a central series for $H \times K$. It is easy to show that $G_i = H_i \times K_i \lhd G = H \times K$. We can also see that $[G_i, G] \leq G_{i+1}$ as

$$H_i \times K_i, H \times K] = [H_i, H] \times [K_i, K] \leq H_{i+1} \times K_{i+1} = G_{i+1}$$

□

Remark 319. *The direct product of an arbitrary set of nilpotent groups is not necessarily nilpotent.*

Definition 320. *The* ***Nilpotency Class*** *of a group G is the length of the shortest central series for G. If G is nilpotent then $cl(G) < c$ for some $c \in \mathbb{N}$.*

Example 321. *Consider the collection of groups G_i where each G_i has $cl(G_i) = i$, then the product:*

$$G = \prod_{n \in \mathbb{N}} G_n$$

is not nilpotent as its nilpotency class is infinite.

Lemma 322. *Let G be a finite group with $Z(G/M) > 1$ for every proper $M \lhd G$. Then G is nilpotent.*

Proof. Define a series $Z_0 = 1$, and $Z_1 = Z(G)$. The define $Z_i \leq G$ such that $Z_i/Z_{i-1} = Z(G/Z_{i-1})$. By our hypothesis if $Z_i < G$ then $Z_{i+1} > Z_i$. Since G is finite, the $Z_n = G$ for some $n \in \mathbb{N}$ (as we run out of elements eventually). This is the clearly a central series (with appropriate relabelling) and so G is nilpotent. □

Corollary 323. *A finite p-group is nilpotent*

Proof. $Z(P)$ is nontrivial for any finite P-group P. □

24 Thursday 3^{rd} May

Lemma 324 (Frattini Lemma)**.** *Let $N \lhd G$ with N finite, and let $P \in Syl_p(N)$. Then $G = N_G(P)N$.*

Proof. Let $g \in G$, and consider $P^g \subseteq N^g = N$. Since $|P^g| = |P|$, $P^g \in \mathrm{Syl}_p(N)$. Thus there exists some $n \in N$ such that $P^{gn} = P$. Thus $gn \in N_G(P)$, or equivalently $g \in N_G(P)n^{-1} \subseteq N_G(P)N$. Since g was arbitrary, we then get $G = N_G(P)N$. □

Theorem 325. *Let G be finite. Then the following are equivalent:*

1. *G is nilpotent;*
2. *$N_G(H) > H$ if $H < G$;*
3. *Every maximal subgroup of G is normal in G;*
4. *Every Sylow p-subgroup is normal in G; and*
5. *G is isomorphic to a direct product of p-groups for all $p\big||G|$.*

Remark 326. *(1) - (4) are equivalent when G is infinite, but 5 does not hold.*

Proof. If G is nilpotent, take the central series $G_0 \geq G_1 \geq \cdots G_r = 1$. Take $H \leq G$ and suppose $G_k \leq H$ for some $k > 0$ (with k minimal, so $G_{k-1} \nleq H$). Then $[G_{k-1}, G] \leq G_k \leq H$, so $[G_{k-1}, H] \leq H$, and so G_{k-1} normalises H. But $G_{k-1} > H$, so we get (1) implies (2).

Now let $M < G$ be a maximal subgroup. Then $N_G(M) > M$ (by (2)) so $N_G(M) = G$, and so $M \lhd G$. Thus (2) implies (3).

Let $P \in \mathrm{Syl}_p(G)$. If $N_G(P) < G$, then choose a maximal subgroup $M < G$ with $N_G(P) \leq M$, so that $P \in \mathrm{Syl}_p(M)$. By (3), $M \lhd G$, so by the Frattini Lemma $G = N_G(P)M$. But $M \geq N_G(P)$ so $N_G(P)M = M$, a contradiction. Thus $N_G(P) = G$ and so $P \lhd G$.

We have already proved that (4) implies (5) and (5) implies (1), so we are done. □

Remark 327. *If M is a maximal subgroup of G, a finite soluble group, then $|G : M|$ is a prime power.*

If $M < G$ has $|G : M| = p$ then M is a maximal subgroup of G, however the converse of this does not hold (consider S_4

Lemma 328. *Let G be a nilpotent group and let M be a maximal subgroup of G. Then G/M has prime order.*

Proof. This follows from the previous lemma, a the fact that G/M can have no proper subgroup (by the third isomorphism theorem). □

Remark 329. *A nilpotent group need not have any maximal subgroups. Consider $\mathbb{Z}_p^\infty = \{z \in \mathbb{C} : z^{p^n} = 1\}$ where $n \in \mathbb{P}$ under multiplication in $\mathbb{C}$ (this is called a Prüfer group), a countable abelian group. Then $H_n = \left(\frac{1}{p^n}\right)\mathbb{Z}/\mathbb{Z}$, the cyclic subgroup of $\mathbb{Z}_p^\infty$ with p^n elements (those with order dividing p^n. Then $H_i \subsetneq H_{i+1} \subsetneq \mathbb{Z}_p^\infty$ for all $i \in \mathbb{N}$, so $\mathbb{Z}_p^\infty$ has no maximal subgroup.*

24.1 General Central Series

Definition 330. *Take a group G and define $\gamma_1(G) = G$. Then let $\gamma_i(G) = [\gamma_{i-1}(G), G]$. If $\gamma_{c+1} = 1$ for some $c \geq 0$, then G has a **Lower Central Series** given by*

$$G = \gamma_1(G) \geq \cdots \geq \gamma_{c+1}(G) = 1$$

Lemma 331. *A lower central series for G is a central series*

Proof. excercise □

Definition 332. *Take a group G and let $Z_0(G) = 1$, then define $Z_i(G)$ by $Z_i(G)/Z_{i+1}(G) = Z(G/Z_{i-1}(G))$. If $Z_r(G) = G$ for some $r \geq 0$, then G has **Upper Central Series***

$$G = Z_r(G) \geq \cdots \geq Z_0 = 1$$

Lemma 333. *An upper central series is a central series*

Proof. Trivial. □

Exercise 334. *Find the upper and lower central series of D_4.*

Example 335. $D_4 \leq \gamma_1(D_4) = D_4 > \gamma_2 = G' = \langle(13)(24)\rangle > \gamma_3 = [\gamma_2, G] = 1$

25 Monday 7^{th} May

Example 336. *The two composition series of $Q_8 = \langle a, b \rangle = \langle (1625)(3847), (1423)(4768) \rangle$ are*

$$Q_8 > \langle a \rangle > \langle a^2 \rangle > 1 \qquad \textit{and} \qquad Q_8 > \langle b \rangle > \langle b^2 \rangle > 1$$

The upper and lower central series for this group are both:

$$Q_8 > Q_8' = \langle (12)(34)(56)(78) \rangle > 1$$

Theorem 337. *If G has a central series $G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$. Then:*

- *$G_{r-i} \leq Z_i$ for $0 \leq i \leq r$; and*
- *$G_i \geq \gamma_{i+1}$ for $0 \leq i \leq r-1$.*

Remark 338. *Colloquially, this means that the upper central series goes up as fast as any others, whilst the lower central series goes down as fast as any others.*

Proof. Left as an exercise, use induction. □

Corollary 339. *If a group is nilpotent, then its Upper central series and lower central series have the same length.*

Proof. Assume G has nilpotency class r. Then it has a central series of length r. This central series is at least as long as the Upper Central Series and Lower Central Series. But both of these are central series, so they must have the same length. □

Example 340. *Consider $g = Q_8 \times \mathbb{Z}_2 = \langle a, b, c : a^2 = b^2 = (ab)^2, c^2 = 1 \rangle$. We see that*

$$\gamma_1 = G > \gamma_2 = \langle a^2 \rangle > \gamma_3 = 1$$

whilst

$$Z_0 = 1 < Z_1 = Z(G) = \langle a^2, c \rangle < Z_2(G) = G$$

25.1 Minimal Normal Subgroup

We have seen that if G is a soluble group, then its minimal normal subgroup is an elementary abelian p-group.

Lemma 341. *Let N be a non-trivial normal subgroup of a finite nilpotent group G. Then $N \cap Z(G) > 1$.*

Proof. G is nilpotent, so G has an upper central series $Z_0 < \cdots < Z_{m-1} < Z_m < \cdots < Z_c$. Let $N \lhd G$. Then exists a minimal m such that $N \cap Z_m \neq 1$. Then consider $[N \cap Z_m, G] \leq N \cap [Z_m, G] \leq N \cap Z_{m-1} = 1$. Thus $N \cap Z_m \neq 1$ is central in G and so $N \cap Z(G) > 1$. □

Corollary 342. *A minimal normal subgroup of a finite nilpotent group is of prime order.*

Proof. $N < Z(G)$, so N has prime order. □

25.2 Finite p-Groups

Lemma 343. *A finite simple p-group P must have order p*

Proof. $1 < Z(P) \lhd P$ so $Z(P) = P$. Thus P is abelian and so $|P| = p$. □

Lemma 344. *Let P be a finite p-group. Then every composition factor and chief factor of P has order p.*

Proof. P is nilpotent, take its UCS. Refine until you have an abelian composition series. □

Lemma 345. *Take a finite non-trivial p-group P. P has a subgroup of index p and every such subgroup is normal.*

Proof. $P > 1$, so choose a maximal normal subgroup $N \lhd P$. P/N is simple, so $|P : N| = p$. Then $N_P(G) > N$ and so $N \lhd P$. □

Lemma 346. *Every maximal subgroup of P is normal and has index p.*

Proof. Let $H < P$ be a maximal subgroup of P. Then $N_P(H) > H$ so $H \lhd P$. Also, since H is maximal, P/H has no nontrivial subgroups, and so P/H has prime order. □

Lemma 347. *Let P be a finite p-group. Let $N < M$ be normal subgroups of P. Then there exists an $L \lhd P$ such that $N \leq L \leq M$ and $|L : N| = p$.*

Proof. Let $\overline{P} = P/N$. $\overline{M}$ is a nontrivial subgroup and $\overline{M} \lhd \overline{P}$. Observe that $Z(\overline{P}) \cap \overline{M} \neq 1$ as $\overline{P}$ is nilpotent. Hence this intersection contains an element x of order p. Then set $\overline{L} = \langle x \rangle \lhd \overline{P}$, so pulling back via the correspondence theorem gives $N \leq L \leq M$, $L \lhd P$, and $|L : N| = p$. □

26 Tuesday 8^{th} May

26.1 Finite p-groups

Corollary 348. *Given a finite abelian p-group P with $|P| = p^n$, for every $b \in \{0, \ldots, n\}$ there exists an $L_b \lhd P$ with $|L_b| = p^b$.*

Proof. This is trivially true for $b = 0$. If it is true for some b, then apply the previous lemma with $N = L_b$ and $M = P$ to get L_{b+1} with $N \leq L_{b+1} \leq M$ with $L_{b+1} \lhd P$ and $|L_{b+1} : L_b| = p$. Hence $|L_{b+1}| = p^{b+1}$, so by induction we are done. □

Corollary 349. *With G be a finite group with $p^b||G|$, ($b \in \mathbb{N}$ and p prime). Then G has a subgroup of order p^b.*

This is a stronger version of the Sylow existence theorem.

26.2 Largest Nilpotent Subgroup

Let G be a finite group and $S \in \mathrm{Syl}_p(G)$. Consider $\mathrm{Core}_G(S) = \cap_{g \in G} S^g = \cap_{T \in \mathrm{Syl}_G(p)} T$. Let $N \lhd G$, so that $S \cap N \in \mathrm{Syl}_p(N)$. In particular, if N is a p-subgroup of G, then $N \leq S$. Hence $\mathrm{Core}_G(S)$ contains every normal p-subgroup of G.

Definition 350. *We define $o_p(G) = Core_G(S) = \cap Syl_p(G)$.*

Remark 351. *$o_p(G)$ contains every normal p-subgroups of G, and it is the largest normal p-subgroup of G.*

Lemma 352. *$o_p(G)$ is characteristic in G.*

By taking direct products of $o_p(G)$ for each $p\big|\,|G|$ gives the largest nilpotent subgroup.

26.3 Frattini Subgroup

Definition 353. *Let G be a finite group. Define the **Frattini Subgroup** of G as*

$$\Phi(G) = \bigcap_{M <\cdot G} M$$

i.e., the intersection of all maximal subgroups

Exercise 354. *$\Phi(G)$ is characteristic in G*

Lemma 355. *The following are equivalent:*

1. *G is nilpotent;*
2. *$G/\Phi(G)$ is abelian; and*
3. *$G/\Phi(G)$ is nilpotent.*

Proof. Suppose G is niloptent, any maximal subgroup M is normal in G and G/M has prime order and is hence abelian. Thus $G' \leq M$ and so $G' \leq \Phi(G)$, giving us an abelian $G/\Phi(G)$.

(2) implies (3) trivially; abelian groups are nilpotent. Now suppose $G/\Phi(G)$ is nilpotent. Let M be any maximal subgroup, which must then contain $\Phi(G)$. $M/\Phi(G)$ is maximal in $G/\Phi(G)$, which is nilpotent, so $M/\Phi(G) \lhd G/\Phi(G)$. Thus $M \lhd G$ and so G is nilpotent. □

Lemma 356. *Let P be a finite p-group. Then $P/\Phi(P)$ is a elementary abelian p-group.*

Proof. If $M < \cdot P$ then P/M is cyclic of prime order, so $P' \leq M$ and $x^p \in M$ for all $x \in P$. Thus $P' \leq \Phi(P)$ and $x^p \in \Phi(P)$ for all $x \in P$, giving us the result. □

Remark 357. *If P is a finite p-group, then byt Burnside basis theorem says that P needs precisely d elements to generate it (where $|P : \Phi(P)| = p^d$.*

$\Phi(P)$ consists of non-generators; elements that can always be removed from generating sets without changing the structure.

26.4 Simplicity of A_n for $n \geq 5$

Remark 358. *A_5 is not abelian, as we can find two elements which do not commute (exercise).*

If $N \lhd G$ then N is a union of conjugacy classes of G, so if G is simple then it is a complete union of conjugacy classes.

Proposition 359. *A_5 is simple.*

Proof. Consider the size of the conjugacy classes of 1, (12)(34), (123), (12345) and (13452): respectively, 1, 15, 20, 12, and 12. So if $N \lhd A_5$ then $|N| = 1$ or $|N| = 60$. □

Lemma 360. *Let $n \geq 3$. Every element of A_5 can be written as a product of 3-cycles.*

Proof. Every element of A_n is a product of transpositions. Take two transpositions $h_1 = (ab)$ and $h_2 = (cd)$. If $h_1 = h_2$ then $h_!h_2 = 1$. If they share one element (WLOG $b = c$) then $h_1h_2 = (adb)$. Otherwise $h_1h_2 = (abc)(adc)$ Thus every element of A_5 is a product of three cycles. □

Lemma 361. *$Z(S_n) = 1$ for all $n \geq 3$.*

27 Thursday 10^{th} May

Lemma 362. *Let G act transitively on Ω. Then $\{G_\alpha : \alpha \in \Omega\}$ is a single conjugacy class of subgroups. Each G_α is called a one-point stabiliser.*

Proof. Let $\alpha \in \Omega$ and $g \in G$. Let $\beta = \alpha \cdot g$, then if $x \in G$ fixes α then

$$\beta \cdot x^g = (\alpha \cdot g) \cdot x^g = \alpha \cdot (xg) = \alpha \cdot g = \beta$$

i.e., x^g fixes β. Thus every conjugate of G_α is another one-point-stabiliser. Also, if $\alpha, \beta \in \Omega$, then by the transitivity of the action of G, there exists a $g \in G$ such that $\alpha \cdot g = \beta$ and $(G_\alpha)^g = G_\beta$. Hence every two one-point-stabilisers are conjugate. □

Lemma 363. *A_5 is simple.*

Proof. Let $N \lhd G = A_5$. Suppose $3 \| |N|$. Then N contains a Sylow 3-subgroup. Since $N \lhd G$, it contains all Sylow 3-subgroups, which collectively contain 20 elements of order 3, and so $|N|$ must exceed 20. Similarly, if $5 \| |N|$, then $|N| > 24$ and so must be 30. But then it must contain 20 elements of order 3 as well, and so would have to have at least 44 elements: a contradiction. Hence neither 3 nor 5 divides $|N|$. So $|N|$ is either 2 or 4. If it were 4, it would be the unique sylow 2-subgroup and would contain 15 elements of order 2: another contradiction. Lastly, if $|N| = 2$, then take $x \in N$, which must have some fixed point. So $N = \{1, x\} \le G_\alpha$ where $\alpha \in \{1, \ldots, 5\} = \Omega$. But then $G_\beta = (G_\alpha)^y$ so $N \le G_\beta$ for all $\beta \in \Omega$. But x cannot fix every point, another contradiction, so there are no options for non-trivial normal subgroups of A_5. □

Lemma 364. *The only normal subgroup of A_n that contains a 3-cycle is A_n.*

Proof. Let $N \lhd A_n$. This is easy to check for $n = 3$ and $n = 4$. Take $n \ge 5$. Let π be the 3-cycle in N. Recall that all 3-cycles are conjugate in S_n. Now there exists an odd permutation which centralises π (seen as the support of π contains three points, and so there are at least 2 point remaining that can be transposed, and that transposition fixes π). Thus $C_{S_n}(\pi) > C_{A_n}(\pi) = C_{S_n}(\pi) \cap A_n$, and $A_n C_{S_n}(\pi) = S_n$.

Then $|C_{S_n}(\pi) : C_{A_n}(\pi)| = |C_{S_n}(\pi) : C_{S_n}(\pi) \cap A_n| = |A_n C_{S_n}(\pi) : A_n| = |S_n : A_n| = 2$, so $|A_n : C_{A_n}(\pi)| = |S_n : C_{S_n}(\pi)|$. Hence all three cycles are contained in A_n, and so all three cycles are contained in N, which then implies that $N = A_n$. □

Theorem 365. *A_n is simple for $n \ge 5$.*

Proof. We have already shown this for $n = 5$. Take $n \ge 6$, and suppose that A_{n-1} is simple. Take $N \lhd A_n$. N contains an element which fixes some $i \in \{1, \ldots, n\}$. Suppose every non-identity element of N has no fixed points. Let $\pi \in N$ and let $a = \pi(1) \ne 1$. Choose b, c such that $c = \pi(b) \ne b$ and $b, c \ne 1, a$. Since $n \ge 6$, there exist $d, e \notin \{1, a, b, c\}$. Let $\rho = (1a)(bcde) \in A_n$. Then $\rho^{-1} = (1a)(bedc)$. Since N is normal in A_n, $\rho\pi\rho^{-1} \in N$, and so $\rho\pi\rho^{-1}(a) = 1$ and $\rho\pi\rho^{-1}(c) = d$. Thus $\rho\pi\rho^{-1}\pi(1) = 1$ and $\rho\pi\rho^{-1}\pi(b) = d$. Thus $\rho\pi\rho^{-1}\pi$ is a non-trivial element of N which fixes 1.

Let $B \le A_n$ consist of all permutations which fix i, so $B \simeq A_{n-1}$. Let $N_i = N \cap B \lhd B$. But by the inductive hypothesis, $A_{n-1} = B$ is simple, so $N_i = 1$ or B. But N_i is nontrivial (as it contains $\rho\pi\rho^{-1}\pi$, and so $N_i = B$; or equivalently, $B \le N$. Since $n \ge 6$, B contains a 3-cycle, so N contains a three cycle, and by our previous lemma must therefor contain all three cycles. Thus $N = A_n$. □

28 Monday 14^{th} May

Alternative Proof for $n > 5$. Take $N \lhd A_n = G$, assume A_{n-1} is simple. Let $H = G_\alpha$ for some $\alpha \in \{1, \dots, n\}$, so $H = A_{n-1}$ is simple. Then $N \cap H \lhd H$, so there are two cases. If $N \cap H = H$, then $H \leq N$. Now $G_\alpha \sim G_\beta$ and so all one point stabilsers are in N. Thus N contains every element of A_n that fixes a point, so it must contain every product of two transpositions, and so $N \geq A_n$.

Otherwise $N \cap H = 1$, so the only element of N that fixes a point is 1. If $N > 1$, then take some non trivial $x \in N$. Either x contains an m-cycle for some $m \geq 3$ or it consists entirely of transpositions. i.e., $x = (12)(34)\dots$ or $x = (12\dots)(\dots)$. Let $y = x^{(356)} \in N$. Then $y = (12)(54)\dots$ or $y = (125\dots)(\dots)$. Thus xy^{-1} is a non trivial element of N that fixes 1, a contradiction. Thus $N = 1$. □

Corollary 366. *For $n \geq 5$, the only normal subgroups of S_n are $1, A_n$ and S_n.*

Proof. Let $N \lhd S_n$. Then $N \cap A_n \lhd A_n$, so by the simplicity of A_n either $N \cap A_n = A_n$ or 1. In the first case, we must have $A_n N = A_n$ or S_n, in which case we are done (TODO: Check). Otherwise take $N \cap A_n = 1$. Then $|N| \leq |S_n : A_n| = 2$. if $|N| = 2$ then $N \leq Z(S_n) = 1$, a contradiction, so $N = 1$. □

Remark 367. *A_n is perfect, i.e., $A_n = A_n'$. Thus S_n is insoluble.*

Exercise 368. *Show that the only subgroup of S_n of index less than n is A_n.*

28.1 Classification of Finite Simple Groups

Theorem 369. *The finite simple groups are:*

1. *Cyclic of prime order;*

2. *A_n for $n \geq 5$;*

3. *16 families of groups; and*

4. *26 sporadic groups.*

Example 370. *$PSL(n, q) = SL(n, q)/Z(GL(n, q))$ except $(n, q) \in \{(2, 2), (2, 3)\}$. Other families include $PSp(n, q)$, $U(n, q)$, and $\Omega(n, q)$ - sets of matricies that preserve a particular forms. There are also the exceptional groups $E_6(q), E_7(q)$, and $E_8(q)$.*

Example 371. *Some of the sporadic groups are M_{11}, a useful group in graph theory. $\mathbb{M}$, the monster group, has $\sim 10^{53}$ elements, and contains many of the other sporadic groups, such as $C_{\mathbb{M}}(x)$.*

Theorem 372 (Feit - Thompson Theorem)**.** *Every finite group of odd order is soluble (and therefor not simple).*

28.2 Group Constructions

We have already seen that the direct product allows us to form new groups, and if $G = H \times K$ then the following are equivalent:

1. $H, K \lhd G$;

2. $H \cap K = 1$; and

3. $KH = G$.

Definition 373. *We define G as the semi direct product of H and K if*

1. *$H \lhd G$;*

2. *$H \cap K = 1$; and*

3. *$KH = G$.*

*And write $G = H \rtimes K$, and so G is a semidirect product **of** H **by** K. We might also say K is the complement of H in G if (2) and (3) hold. G is the **Split Extension** of N by H.*

Remark 374. *If $G = N \rtimes H$ then*

$$\frac{G}{N} = \frac{NH}{N} \simeq \frac{H}{H \cap N} = \frac{H}{1}$$

so $G/N \simeq H$

Example 375. *Take $D_4 = \langle x, y : x^4 = y^2 = 1, x^y = x^{-1} \rangle$. Then $N = \langle x \rangle \lhd D_4$ and $H = \langle y \rangle$ has $N \cap H = 1$, and $NH = D_4$, so $D_4 = N \rtimes H$.*

Example 376. *Take $S_3 = \langle a, b : a^3 = b^2 = 1, a^b = a^{-1} \rangle$. Then set $N = \langle a \rangle$ and $H = \langle b \rangle$. Then $S_3 = N \rtimes H$.*

Example 377. *$\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2 = \langle a, b : a^3, b^2, a^b = a \rangle$.*

Remark 378. *Ever direct product (DP) is a semi direct product (SDP).*

Example 379. *$D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$ and $S_n = A_n \rtimes \mathbb{Z}_2$.*

Example 380. *Q_8 cannot be a split extension of any N, H with $|N| = 4$, as N would then have to contain the unique element of order 2.*

29 Tuesday 15^{th} May

Lemma 381. *Let $G = N \rtimes H$. For each $h \in H$, define $\theta_h : N \to N$ by $n \mapsto n^h = hnh^{-1}$. Then $\theta_h \in Aut(N)$. The map $\theta : H \to Aut(N)$ given by $h \mapsto \theta_h$ is a homomorphism.*

Proof. For the first claim, see that $N \lhd G$ so $n^h \in N$. θ_h is indeed Homomorpic, injective, and surjective (as $\theta_h(h^{-1}nh) = n$).

Then $\theta(h_1h_2)(n) = (h_1h_2)n(h_1h_2)^{-1} = \theta_{h_1} \circ \theta_{h_2}(n) = \theta(h_1) \circ \theta(h_2)(n)$, so θ is indeed a homomorphism. □

Example 382. *Take $N = \mathbb{Z}_3$ and $H = \mathbb{Z}_2 \simeq Aut(N)$. Then both $\mathbb{Z}_6$ and S_3 are semi direct products of N by H.*

29.1 External Semi Direct Products

Definition 383. *$N \lhd G$, $H \leq G$, $\theta : H \to Aut(N)$ given by $h \mapsto \theta_h$. Then we say $G = N \rtimes H$ **Realises** θ if for all $h \in H$ and $n \in N$, then $\theta_h(n) = n^h$.*

Example 384. *If θ is the trivial map, then G is the direect product of N and H.*

Lemma 385. *If $N \lhd G$, and H is complement to N in G, then every $g \in G$ has a unique expression $g = nh$ with $n \in N$ and $h \in H$.*

Proof. Take $g = G$ and suppose that it has expressions $g = n_1h_1 = n_2h_2$. Then $n^{-1}n_2 = h_1h_2^{-1} = 1$ (as $N \cap H = 1$), so $n_1 = n_2$ and $h_1 = h_2$. □

Definition 386. *Given N, H, $\theta : H \to Aut(N)$ with $h \mapsto \theta_h = (n \mapsto hnh^{-1})$, we define $G = N \rtimes_\theta H$ to be the set of ordered pairs*

$$\{(n,h) : n \in N, h \in H\}$$

equipped with the opperation:

$$(n_1,h_1) \cdot (n_2,h_2) = (n_1\theta_{h_1}(n_2), h_1, h_2)$$

Remark 387. *If θ maps $h \mapsto 1$ for all $h \in H$, then $N \rtimes_{theta} H = N \times H$.*

Theorem 388. *Let N and H be groups, and let $\theta : H \to Aut(N)$. Set $G = \{(n,h) : n \in N, h \in H\}$, $N_0 = \{(n,1) : n \in N\}$, and $H_0 = \{(1,h) : h \in H\}$. Then:*

1. *G equiped with the product in the previous definition is a group*
2. *$N_0 \lhd G$ and $N_0 \simeq N$;*
3. *$H_0 \leq G$ and $H_0 \simeq H$; and*
4. *$G = N_0 \rtimes H_0$.*

Proof. G is closed under the given opperation. It is associative, as

$$(a,x)((b,y)(c,z)) = (a\theta_x(b)\theta_y(c), xyz) = ((a,x)(b,y))(c,z))$$

Then it has identity as

$$(n,h)(1,1) = (n\theta_h(1),h) = (n,h)$$

And it has an inverse as

$$(n,h)(\theta_{h^{-1}}(n^{-1}),h^{-1}) = (n\theta_h\theta_{h^{-1}}(n^{-1}),hh^{-1}) = (1,1)$$

Now $(1,h_1)(1,h_2) = (1,h_1h_2) \in H_0$ so $H_0 \leq G$. $(n_1,1)(n_2,1) = (n_1n_2,1) \in N$ so $N_0 \leq G$. Then take any $(n,h) \in G$. Then $(n,h) = (n,1)(1,h)$ so $G = N_0H_0$, and it is clear that $N_0 \cap H_0 = 1$. Lastly, see that $N_0 \lhd G$ as

$$(m,h)(n,1)(m,h)^{-1} = \cdots = (n_0,1) \in N_0$$

□

Remark 389. *Given $G = N \rtimes H$, there exists a $\theta : H \to Aut(N)$ with $h \mapsto \theta_h$. If $G = N \rtimes H$, then $g = nh$, so*

$$g_1g_2 = n_1h_1n_2h_2 = n_1\theta_{h_1}(n_2)h_1h_2$$

29.2 Remarks on Automorphisms

Remark 390. *If $G = \langle x\rangle \simeq \mathbb{Z}_n$ and $\theta_m : G \to G$ has $x \mapsto x^m$ then $Aut(G) = \{\theta_m : m \neq 0 \text{ and } \gcd(m,n) = 1\}$. Thus $Aut(G) \simeq$ the group of units of $\mathbb{Z}_n$, $U(n)$.*

Remark 391. *$\mathbb{Z}_p$ has $Aut(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$.*

Remark 392. *If $G = \mathbb{Z}_p \times \cdots \mathbb{Z}_p$ be an elementary abelian group of rank d. Then $Aut(G) \simeq GL(d,p)$.*

This is because we can create an isomorphism from G to a vector space V of dimension d over the field $\mathbb{Z}_p$, and the autmorphisms of G then correspond to the linear transformations on V.

Remark 393. *Let A, B be groups, and $\phi : A \to B$ be a homomorphism. If $a \to b$ then $|b| \,\big|\, |a|$.*

30 Thursday 17^{th} May

Example 394. *Let $N = \mathbb{Z}_3 = \langle y \rangle$, $H = \mathbb{Z}_2 = \langle x \rangle$. Define the homomorphism $\theta : H \to Aut(N)$ with either $x \mapsto \theta_x = (y \mapsto y^2)$ or $x \mapsto \theta_{Id} = (y \mapsto y)$. In the second case, we see $(n_1,h_1)(n_2,h_2) = (n_1n_2,h_1h_2)$, so the external direct product generates $\mathbb{Z}_3 \times \mathbb{Z}_2$. In the first case, $(n_1,h_1)(n_2,h_2) = (n_1\theta_{h_1}n_2,h_1h_2)$ which means we have S_3.*

We could also consider these with their presentations.

Example 395. *Let $N = \mathbb{Z}_3 = \langle n : n^3 = 1 \rangle$ and $H = \mathbb{Z}_3 = \langle h : h^3 = 1 \rangle$. The order of $Aut(N)$ is 2, containing the identity and inverting automorphisms. We must have $|\phi(H)|\big||Aut(N)| = 2$, so θ must map h to the identity. Thus*

$$N \rtimes H = N \times H = \langle n,h : n^3 = h^3 = 1, n^h = n \rangle.$$

Example 396. *Let $N = \mathbb{Z}_5 = \langle n : n^5 = 1 \rangle$ and $H = \langle h : h^2 = 1 \rangle$. Then $Aut(N) = \{\phi_1,\dots,\phi_4\}$ where $\phi_iL : n \mapsto n^i$. We must have $h \mapsto \phi_1,\phi_4$ as $|\phi_2| = |\phi_3| = 4$. Thus*

$$N \rtimes_\theta = \langle n,h : n^5 = h^2 = 1, n^h = \theta_h(n) \rangle$$

Where $\theta : hmapsto\theta_h = \phi_1,\phi_4$. In the first case, we get the direct product $\mathbb{Z}_5 \times \mathbb{Z}_2$ and in the second we get D_5.

Example 397. *Let $|G| = pq$ where p,q are distinct primes, and assume that $p > q$. Then either:*

1. *$C_p \times C_q$ (given by $C_p \rtimes_1 C_q$); or*
2. *if $q|p-1$, then there exists a non-trivial HM θ with $G = C_p \rtimes_\theta C_p$.*

Example 398. *Let $N = \mathbb{Z}_5$ and $H = \mathbb{Z}_4$. Then h could map to any ϕ_i, so there are 4 possible groups. If $1_H \mapsto \phi_1$ then we have $N \times H$. If $1_H \mapsto \phi_4$ then we have $N \rtimes H \simeq D_{10}$. Otherwise, we have groups isomorphic to $\langle n,h : n^5 = h^4 = 1, n^h = \theta_i(n) \rangle$.*

Example 399. *$D_4 \simeq \mathbb{Z}_4 \rtimes \mathbb{Z}_2$. $Aut(\mathbb{Z}_4) = \mathbb{Z}_2$. So let θ map $x \mapsto (a \mapsto a^{-1})$. Then*

$$\mathbb{Z}_4 \rtimes_\theta \mathbb{Z}_2 = \langle a,x : a^4 = x^2 = 1, a^x = a^{-1} \rangle$$

We can also see $D_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2 = N \rtimes H = \langle a,b : a^2 = b^2 = [a,b] = 1 \rangle \rtimes \langle x : x^2 \rangle$. $Aut(N) = GL(2,2)$. Define $\theta : H \to GL(2,2)$ by $x \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = M$. Then $M^2 = 1$. Then the external product becomes

$$\langle a,b,x : a^2 = b^2 = x^2 = [a,b] = 1, a^x = a, b^x = ab \rangle$$

Remark 400. *A group need not be a non-trivial semidirect product, and a group can be a semi-direct product in more than one way.*

Exercise 401. *Replace the 2s with some odd prime p in the previous example.*

Example 402. *Let $T = \langle a,b : a^6, b^2 = a^3 = (ab)^2 \rangle$. We will show that a non-abelian group G of order 12 is isomorphic to either A_4, D_6 or T. Suppose $G \not\simeq A_4$ Let $K \in Syl_3(G)$ then $K = \langle k \rangle \lhd G$. Let $P \in Syl_2(G)$, so $|P| = 4$. Thus $G = KP$, and so either $P \simeq \mathbb{Z}_4$ or $P \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. In the second case, $G \simeq D_4 = S_3 \times \mathbb{Z}_2$.*

Otherwise, take $P \simeq \mathbb{Z}_4 = \langle x \rangle$*, and* $\mathbb{Z}_3 = \langle a \rangle$*. Define* $\theta : \mathbb{Z}_4 \to Aut(\mathbb{Z}_3) \simeq \mathbb{Z}_2$ *by* $x \mapsto (a \mapsto a^{-1})$*. Consider* $u = (a^2, x^2)$ *and* $v = (1, x)$*. Then* $u^6 = 1$ *and* $v^2 = u^3 = (uv)^2$*, and* $u, v \in \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_4$*. Thus* $G = \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_4 \simeq T$*.*

31 Monday 21^{st} May

31.1 Holomorph of N

Take N and $H = \mathrm{Aut}(N)$. Set $G = N \rtimes \mathrm{Aut}(N)$. This is called the **Holomorph** of N.

Example 403. *Take $N = \mathbb{Z}_3$, so $H = Aut(N) \simeq \mathbb{Z}_2$. Then $|Hol(N)| = 6$ and $Hol(N) \simeq \mathbb{Z}_3 \rtimes \mathbb{Z}_2$. If θ is the identity map on $H = \{1, phi = (x \mapsto x^{-1})\}$, then*

$$(n, \phi)(n^2, 11) = (n\phi(n^2), \phi 1) = (n^2, \phi)$$

and

$$(n^2, 1)(n, \phi) = (n^2 1(n), 1\phi) = (1, \phi)$$

Thus the holomorph of $\mathbb{Z}_3$ does not commute, and so is isomorphic to S_3.

31.2 Affine General Linear Group

Let F be a field, and $V = F^n$ be an n-dimensional vector space over F (representing them as row vectors). Take $A \in GL(n, F)$ and $b \in F^n$. Define a map $T_{A,b} : V \to V$ by $x \mapsto xA + b$. This is called an **Affine Linear Transformation** of V. The set of all such transformations forms a group under composition. We call this group $AGL(n, F) = \{T_{A,b} : A \in GL(n, F), b \in F^n\} = AGL(V)$.

This is indeed a group, as we see that $T_{A,b}T_{C,d} = T_{AC,bC+d} \in AGL(n, F)$, and $(T_{A,b})^{-1} = T_{A^{-1},-bA^{-1}}$. In fact, this forms a subgroup of $\mathrm{Sym}(V)$.

We define the normal subgroup $T(V) = \{T_{I,b} : b \in F^n\} \lhd AGL(n, F)$ (i.e., the translation subgroup). Define $\phi : AGL(V) \to GL(V)$ by $T_{A,b} \mapsto A$. Then ϕ is an epimorphism from $AGL(V)$ onto $GL(V)$. $T(V) = \ker \phi$, and $AGL(V) = T(V) \rtimes GL(V)$.

Example 404. *Let $N = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \simeq V = GF(p)^n$. Then $GL(n, p) \simeq Aut(N)$. $AGL(n, F) = V \rtimes Aut(V) = Hol(N)$.*

Example 405. *If $n = p = 2$, then $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $Aut(V) \simeq GL(2, 2)$. $AGL(V) = V \rtimes Aut(V) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3 = Sym(4)$.*

31.3 Wreath Products

Definition 406. *Take G, $N = G^n$, and $H \leq Sym(n)$ finite. Then the **Permutation Wreath Product** is*

$$GpwrH = N \rtimes_\theta H$$

The elements of N are n-tuples of elements of G, $(g_1, g_2, \ldots, g_n) \in N$ with each $g_i \in G$. θ_h then maps each g_i to $g_{h(i)}$. We claim that $\theta_h \in \mathrm{Aut}(N)$ (which is trivial), so $\theta : H \to \mathrm{Aut}(N)$ is a homomorphism. H acts on N by permuting the n direct factors.

Remark 407. $|GpwrH| = |G|^n|H|$

Example 408. *Take $G = S_3$ and $H = S_4$. Then $|GpwrH| = 6^4 \cdot 4$.*

Definition 409. *Let H be a finite group of order n. Then the* ***Regular Representation*** *of H is as a subgroup of Sym(n). (note the this follows from Cayley's theorem).*

Definition 410. *Take G, and a finite group $H \leq$ Sym$(|H|)$. Then we define the* ***Regular Wreath Product*** *as*

$$GrwrH = (G^n) \rtimes_\theta H$$

Example 411. *With $G = S_3$ and $H \simeq S_4$. Then $|GrwrH| = |G|^{24}|H|$.*

The regular wreath product is a subcase of the permutation wreath product.

Example 412. *Let $G = \mathbb{Z}_2 = \langle x : x^2 = 1\rangle$ and $H = \mathbb{Z}_2 = \langle h = (12)\rangle$. Then $GrwrH = GpwrH = G \wr H = W$. We see that $N = G \times G = \{(1,1),(1,x),(x,1),(x,x)\}$. Take $\theta : H \to Aut(N)$ with $h \mapsto \theta_h$. Then θ_h must have $(1,1) \mapsto (1,1)$, $(1,x) \mapsto (x,1)$, $(x,1) \mapsto (1,x)$ and $(x,x) \mapsto (x,x)$.*

Then $|N \rtimes H| = 2^2 \cdot 2 = 8$. We see that

$$((1,x),h) \cdot ((1,x).h) = ((1,x)\theta_h((1,x)), hh) = ((1,x)(x,1),1) = ((x,x),1) \neq 1$$

Continue, to see that $|((1,x),h)| = 4$. Then set $a = ((1,x),h)$ and $b = ((1,1),h)$, so that $|b| = 2$. Also see that $a^{-1} = b^{-1}ab$. Then $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ satisfies the presentation

$$\{a, b : a^4, b^2, a^b = a^{-1}\}$$

so $W \simeq D_4$.

32 Tuesday 22^{nd} May

We typically call $N = G^n$ the **Base Group** of the wreath product.

32.1 Orders of Iterated Wreath Products

It is clear that $|C_p \wr C_p| = p^p \cdot p = p^{p+1}$. The $|(C_p \wr C_p) \wr C_p| = (p^{p+1})^p \cdot p = p^{p^2+p+1}$.

Lemma 413. *Let $W_k(C_p)$ be the iterated wreath product of C_p with itself k times. That is, Set $W_1(C_p) = C_p$ and $W_i(C_p) = W_{i-1}(C_p) \wr C_p$. Then*

$$|W_k(C_p)| = p^{r(p)} \qquad \text{where } r(p) = p^{k-1} + p^{k-2} + \cdots + p + 1$$

Remark 414. *Is the wreath product commutative? Associative?*

Lemma 415. *Let $p^{r(n)}$ be the highest power of the prime p dividing $(p^n)!$. Then*

$$r(n) = p^{n-1} + p^{n-2} + \cdots + p + 1 = p^{n-1} + r(n-1)$$

Corollary 416. *Let $G = Sym(p^n)$. Then $|Syl_p(G)| = p^{r(n)}$.*

Example 417. *If $p^n = 2^3 = 8$. Then $|Syl_2(S_8)| = 2^{2^2+2^1+1} = 2^7$.*

Theorem 418. *Let p be a prime number, k a positive integer. Then*

$$Syl_p(Sym(p^k)) = W_k(C_p)$$

Proof. Induction on k. The base is trivial as $\mathrm{Syl}_p(C_p) = C_p$. Then we have already observed that the highest power of p dividing $p^n!$ is $p^{r(n)}$, so $|W_k(C_p)| = |\mathrm{Syl}_p(\mathrm{Sym}(p^k))|$. Now we want to show that $W_{k+1}(C_p)$ can be embedded as a subgroup of $\mathrm{Sym}(p^{k+1})$, if given that W_k can.

First, we let N be the direct product of p copies of $\mathrm{Sym}(p^k)$. These copies act on disjoint sets, so they commute. $N = \prod_p \mathrm{Sym}(p^k) \le \mathrm{Sym}(p^{k+1})$. Let $H \le \mathrm{Sym}(p^{k+1})$ where $H = \langle h : h^p = 1 \rangle$ and $h = \prod_{i=1}^{p^k}(i, i+p^k, \cdots, i+(p-1)p^k)$. h has p^k cycles of length p. $|H| = p$. Thus there exists a $\theta : H \to \mathrm{Aut}(N)$ so that $N \rtimes_\theta H \le \mathrm{Sym}(p^{k+1})$.

Then we have $\mathrm{Syl}_p(N \rtimes H) = \mathrm{Syl}_p(N) \rtimes \mathrm{Syl}_p(H) = \mathrm{Syl}_p(N) \rtimes H$. But N is a direct product of $\mathrm{Sym}(p^k)$, so $\mathrm{Syl}_p(N) = \prod \mathrm{Syl}_p(\mathrm{Sym}(p^k))$. By our inductive hypothesis, this means that $N = W_k$, and $G = N \rtimes H = W_k \rtimes C_p = W_{k+1}$, so we are done. □

Corollary 419. *Let p be a prime. Let $n \in \mathbb{N}$ be a positive integer, and take*

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$$

where $0 \le a_i \le p-1$ be the expansion of n to base p. Then each Sylow p subgroup of S_n is a direct product

$$T_1^{a_1} \times T_2^{a_2} \times \cdots \times T_k^{a_k}$$

where T_i is a Sylow p-subgroup of $Sym(p^i)$, i.e., $T_i = W_i(C_p) = Syl_p(Sym(p^i))$.

Proof. Calculate the order of p dividing $n!$. The number of integers between 1 and n divisible by p is $[n/p]$. The number of these divisible by p^2 is $[n/p^2]$. Therefor $p^m|n$ where $m = [n/p] + [n/p^2] + \cdots$. So

$$\begin{aligned} m &= (a_1 p + a_2 p^2 + \cdots a_k p^k) + (a_2 p_2 + \cdots + a_k p^k) + \cdots + (a_k p^k) \\ &= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots \end{aligned}$$

Thus p^m is the order of $T_1^{a_1} \times \cdots \times T_k^{a_k}$. Then, as in the proof of the theorem, divide the set of size n into disjoint subsets, with each corresponding to some a_i with size p^i. The symetric groups of these sets are then $W_i(C_p)$. We can then argue as in the theorem to see that this is isomorphic to subgroup of S_n. □

Example 420. *Let $G = Sym(5)$. $5 = 1 \cdot 2^0 + 0 \cdot 2 + 1 \cdot 2^2$. Then $Syl_2(G) = T_4 = Syl(Sym(4)) = C_2 \wr C_2 \simeq D_4$.*

33 Thursday 24^{th} May

Example 421. *Taek $p^3 = 27$. Then $N = Sym(9) \times Sym(9) \times Sym(9)$ and $H = C_3$. Then $G = N \rtimes H \leq S_{27}$.*

Then $Syl_3(G) = Syl_3(N) \rtimes H = \prod Syl_3(S_9) \rtimes H$. This equals

$$(C_3 \wr C_3) \times (C_3 \wr C_3) \times (C_3 \wr C_3)) \rtimes C_3 = (C_3 \wr C_3) \wr C_3$$

Example 422. *Take $G = S_{10}$. $10 = 0 + 1 \times 2 + 1 \times 2^3$. The 2 terms corresponds to S_2, so $T_2 = \mathbb{Z}_2$. The 2^3 term corresponds to S_{2^3}, with Sylow 2-subgroup $(\mathbb{Z}_2 \wr \mathbb{Z}_2)$. Thus*

$$Syl_2(G) = \mathbb{Z}_2 \times ((\mathbb{Z}_2 \wr \mathbb{Z}_2) \wr \mathbb{Z}_2)$$

Similarly, $10 = 1 + 3^2$ so $Syl_3(G) = \mathbb{Z}_3 \wr \mathbb{Z}_3$. Lastly, $10 = 2 \times 5$ so $Syl_5(G) = \mathbb{Z}_5 \times \mathbb{Z}_5$.

Example 423. *Let $G = S_{34}$. $34 = 1 + 2 \cdot 3 + 3^3$. Thus*

$$Syl_3(G) = T_{3^1}^2 \times T_{3^3}^1 = (\mathbb{Z}_3 \times \mathbb{Z}_3) \times ((\mathbb{Z}_3 \wr \mathbb{Z}_3) \wr \mathbb{Z}_3)$$

33.1 General Construction of Wreath Products

Take $G \leq \mathrm{Sym}(\Lambda)$, $H \leq \mathrm{Sym}(\Omega)$, and set $W = G \wr H \leq \mathrm{Sym}(\Lambda \times \Omega)$. Given some $g \in G$ and $w \in \Omega$, define a permutation of g_w^* of $\Lambda \times \Omega$ as follows: for $(\lambda, \omega) \in \Lambda \times \Omega$ define

$$g_w^*(\lambda, \omega) = \begin{cases} (\lambda^g, \omega) & \text{if } \omega = w \\ (\lambda, \omega) & \text{Otherwise} \end{cases}$$

From this, note that $g_w^*(g')_w^* = (gg')_w^*$ for all $g, g' \in G$. Define $G_w^* = \{g_w^* : g \in G\} \leq \mathrm{Sym}(\Lambda \times \Omega)$. The the map $G \to G_w^*$ taking g to g_w^* is a isomorphism for all $w \in \Omega$. Also define h^* as the permutation of $\Lambda \times \Omega$ taking (λ, ω) to (λ, ω^h), and $H^* = \{h^* : h \in H\}$. Similarly, $h \mapsto h^*$ is an isomorphism.

Theorem 424. *Given $G \leq Sym(\Lambda)$, and $H \leq Sym(\Omega)$ (where Ω is finite), the wreath product*

$$G \wr H \simeq W = \langle G_w^*, H^* : w \in \Omega \rangle \leq Sym(\Lambda \times \Omega)$$

Proof. Define $K^* = \langle \cup_{w \in \Omega} G_w^* \rangle$. We claim that this is equal to the direct product

$$K^* = \prod_{w \in \Omega} G_w^*$$

note that G_w^* centralises G_ω^* for all $\omega \neq w$. Thus $G_w^* \lhd K^*$, and $G_w^* \cap \langle \cup_{\omega \in \Omega \setminus \{w\}} G_\omega^* \rangle = 1$, proving the claim. Now take $h \in H$ and $w \in \Omega$. We have $h^* g_w^* (h^*)^{-1} = g_{w^h}^* \in K^*$, thus $h^* K^* (h^*)^{-1} \leq K^*$ for all $h \in H$, and thus $K^* \lhd W = \langle K^*, H^* \rangle$. Therefor $W = K^* H^*$.

Take some element $x \in K^* \cap H^*$. This must fix the point (λ, ω), so it must be the identity. Thus

$$W = \langle G_w^*, H^* : w \in \Omega \rangle = \langle K^*, H^* \rangle = K^* \rtimes H^* = \left(\prod_{\omega \in \Omega} G_\omega^* \right) \rtimes H^*$$

Then the map $\phi : G \wr H \to W$ given by $(g_\omega)_{\omega \in \Omega} h \mapsto (g_\omega^*) h^*$ is an isomorphism. □

Example 425. *Take $G = H = C_2$, set $\Lambda = \{1,2\}$ and $\Omega = \{3,4\}$. Then label the elements of $\Lambda \times \Omega$ as*

$$\{a = (1,3), b = (2,3), c = (1,4), d = (2,4)\}$$

Set $g = (12)$, so then the permutation g_3^* has

$$\begin{aligned} a = (1,3) &\mapsto (1^g,3) = (2,3) = b \\ b = (2,3) &\mapsto (2^g,3) = (1,3) = a \\ c = (1,4) &\mapsto (1,4) = c \\ d = (2,4) &\mapsto (2,4) = d \end{aligned}$$

or equivalently, $g_3^* = (ab)$. Similarly $g_4^* = (cd)$. Lastly, h^* fixes the first component and permutes the second, so $h^* = (ac)(bd)$. So we have

$$W = (\langle (ab) \rangle \times \langle (cd) \rangle) \rtimes \langle (ac)(bd) \rangle = \langle (ab), (cd), (ac), (bd) \rangle \leq Sym(\{a,b,c,d\})$$

Computing this out show that $W \simeq D_4$.

34 Monday 28^{th} May

Example 426. *Take $G = C_2 = \langle(12)\rangle$ and $H = C_3 = \langle(345)\rangle$, $\Lambda = \{1,2\}$ and $\Omega = \{3,4,5\}$. Label*

$$\Lambda \times \Omega = \{a = (1,3), b = (2,3), c = (1,4), d = (2,4), e = (1,5), f = (2,5)\}$$

Take $\omega \in \Omega$. Then g^*_ω has $g^*_3 = (ab)$, $g^*_4 = (cd)$ and $g^*_5 = (ef)$. If $h = (345)$, then $h^* = (ace)(bdf)$. Thus $W = G \wr H = \langle(ab),(cd),(ef),(ace)(bdf)\rangle \le S_6$, and $|W| = |G|^n|H| = 2^3 \cdot 3$.

Example 427. *Consider $W = C_3 \wr C_2 = \langle(123)\rangle \wr \langle(45)\rangle$. Then*

$$\Lambda \times \Omega = \{1,2,3\} \times \{4,5\} = \{a = (1,4), b = (2,4), c = (3,4), d = (1,5), e = (2,5), f = (3,5)\}$$

$g = (123)$ so $g^*_4 = (abc)$ and $g^*_5 = (def)$. $h = (45)$ so $h^* = (ad)(be)(cf)$. Thus

$$W = \langle(abc),(def),(ad)(be)(cf)\rangle$$

with order $3^2 \cdot 2$.

Example 428. *Take $P(n)$ to be the group of permutation matrices. So $P(n) \simeq S_n$. e.g., for $n = 3$,*

$$(123) \sim \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Also define the group $B(n)$ as the group generated by permutation matrices where single non-zero entry can be ± 1. This is sometimes called the Monomial group or the Hyper octahedral group. Observe that $B(n)$ has a normal subgroup D consisting of diagonal matrices with ± 1 on the diagonal. Each matrix in $B(n)$ can be written as a product of a diagonal matrix and a permutation matrix. Thus $B(n) = D \rtimes P(n)$. Observe that $D \simeq (Z_2)^n$, so $B(n) = \mathbb{Z}_2 \wr S_n$, and so $|B(n)| = 2^n n!$.

Remark 429. *Recall the Prüfer group $\mathbb{Z}_p^\infty = \{z \in \mathbb{C} : z^{p^k} = 1 \text{ for some } k \in \mathbb{N}\}$. Note that this is abelian because $\mathbb{C}$ is. The only proper subgroups are cyclic of the form $T_n = \{z \in \mathbb{Z}_p^\infty : z^{p^n} = 1\}$. There is no maximal subgroup. The group $W = \mathbb{Z}_p \wr \mathbb{Z}_p^\infty$ is thus an infinite group with trivial center, and is not nilpotent.*