GROUP THEORY

1. Preliminaries

Definition 1.1. A *group* G is a non-empty set together with an associative binary operation with respect to which there is an identity element, and every element has an inverse.

Note. Unless otherwise specified, we will assume the binary operation is multiplication (of some form), and write 1 (or 1_G) for the identity element of G, ab for the product of elements a and b, and a^{-1} for the inverse of the element a in G.

We make use of the notation x^ϕ as the image of x under ϕ, where $\phi : G \to H$ is a homomorphism and $x \in G$. We also apply functions from left to right: $(1,2,3)(3,4,5) = (1,2,4,5,3)$.

If the binary operation is commutative, that is, if $ab = ba$ for all $a, b \in G$, then the group is said to be *Abelian*. (In this case the binary operation is sometimes assumed to be addition (of some form), and then the identity element is written 0, or 0_G, and the inverse of an element a is written as $-a$).

Proposition 1.2. *If $x^2 = 1$ for each member x in a group G, then G is Abelian.*

Proof. Suppose $x, y \in G$. Then $(xy)^2 = 1$, implying that $xyxy = 1$ and since $x^{-1} = x$, $y^{-1} = y$, it follows that $xy = yx$. Thus, G is Abelian. □

If x and y are elements of a group G, then their *commutator* is the element $x^{-1}y^{-1}xy$, and denoted by $[x, y]$. Note that $p[x, y] = 1$ if and only if x and y commute.

If x is an element of a group G, then the set $[x] = \{g^{-1}xg \mid g \in G\}$ is called the *conjugacy class* of x in G (the equivalence class of x under the conjugacy relation).

The cardinality of a group G is called the *order* of the group, and denoted by $|G|$. Also if a is an element of G then the number of distinct powers of a (including negative powers) is called the *order* of a, and denoted by $o(a)$ (or $|a|$).

A *subgroup* of a group G is a subset H of G which under the same binary operation as G is a group in its own right. In this case we write $H \leq G$. It is easy to prove that a non-empty subset H of G is a subgroup iff $ab^{-1} \in H$ for all $a, b \in H$.

Given a subgroup H and an element a of a group G, the set $Ha = \{ha \mid h \in H\}$ is called the *(right) coset* of H containing a in G. Note that $a = 1a \in Ha$. Left cosets $aH = \{ah \mid h \in H\}$ are defined similarly.

Proposition 1.3. *Any two right cosets of a subgroup H of a group G are equal or disjoint.*

Proof. We claim that if $a \in H$, then $Ha = H$. Suppose $a \in H$. Then $a^{-1} \in H$. If $h \in H$, then $ha^{-1} \in H$. Consequently, $(ha^{-1})a = h$, and so Ha contains H. Clearly H contains Ha, so our claim holds.

Suppose $a, b \in G$ such that $Ha \cap Hb \neq \varnothing$. Then there exists $h \in Ha \cap Hb$. It follows that $h = h_1 a$ and $h = h_2 b$ for some $h_1, h_2 \in H$. Hence, $a = h_1^{-1}h = h_1^{-1}h_2 b$, and so

$$Ha = H(h_1^{-1}h_2 b) = (Hh_1^{-1}h_2)b = Hb.$$

□

There is also a one-to-one correspondence between left and right cosets of H given by $Ha \leftrightarrow a^{-1}H$. The number of distinct right cosets of H in G is called the *index* of H in G and is denoted by $|G : H|$. We have that $(G : H) = \{Hg \mid g \in H\}$.

Theorem 1.4. Lagrange's Theorem. *If $H \leq G$ where G is finite, then $|H|$ divides G and $|G| = |G : H||H|$.*

Proof. Suppose H is a subgroup of a finite group G. Then $\mathscr{H} = \{Hg \mid g \in G\}$ partitions G, where $|H| = |Hg|$ for all $g \in G$ (since $h \mapsto hg$ for $h \in H$ has inverse map by applying g^{-1}). Hence, $|G| = \sum_{g \in G} |Hg| = |G| = |G : H||H|$. □

Example 1.5. Given a group G, a subset H and an element a of G:

(1) $C_G(x) = \left\{h \in G \;\middle|\; h^{-1}xh = x\right\}$ is called the *centraliser* of x in G, and say that g *centralises* x if $g^{-1}xg = x$;
(2) $Z(G) = \{z \in G \mid zg = gz \ \forall g \in G\} = \bigcap_{x \in G} C_G(x)$ is a subgroup called the *centre* of G;
(3) $C_G(H) = \bigcap_{x \in H} C_G(x) = \{g \in G \mid xg = gx \ \forall x \in H\}$ is a subgroup called the *centraliser* of H in G;
(4) $N_G(H) = \left\{g \in G \;\middle|\; g^{-1}Hg = H\right\}$ is a subgroup called the *normaliser* of H in G, and say that g *normalises* H if $g^{-1}Hg = H$;
(5) $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup called the (cyclic) subgroup generated by a in G;
(6) the intersection of all subgroups of G containing H is a subgroup of G, denoted by $\langle H \rangle$ and called the subgroup *generated* by H;
(7) $G' = [G, G] = \langle \{[x, y] \mid x, y \in G\} \rangle$, the subgroup generated by all *commutators* $x^{-1}y^{-1}xy$ of elements x, y in G, is called the *commutator subgroup*, or *derived group*, of G.

Conjecture 1.6. Ore's Conjecture (1950s). *If G is a finite simple group, i.e. only normal subgroups are $\{1\}$ and G, then every element of G is a commutator.*

The symmetry group of a regular n-gon is a group consisting of n rotational and n reflectional symmetries, under composition, and is called the *dihedral group* of order $2n$.

The *tetrahedral* group T: 12 rotational symmetries of a regular tetrahedron ($\mathrm{Rot}(T) \cong A_4$ and $\mathrm{Sym}(T) \cong S_4$). The *octahedral* group: 24 rotational symmetries of a regular octahedron. The *icosahedral* group: 60 rotational symmetries of a regular icosahedron.

The group of all permutations of a set X under composition is called the *symmetric* group on X and denoted by $\mathrm{Sym}(X)$. If X is finite, of cardinality n, then we suppose $X = \{1, 2, \ldots, n\}$ and write S_n for $\mathrm{Sym}(X)$, and call it the *symmetric group of degree n*.

The subgroup of S_n consisting of all permutations $\{1, 2, \ldots, n\}$ which can be written as a product of an even number of transpositions $(\alpha\beta)$ is called the *alternating* group of degree n, and denoted by A_n. For example, $(1, 3, 5)(2, 4, 6) = (1, 5)(3, 5)(2, 6)(4, 6)$.

The *substitution rule*: If $\sigma = (p_1, \ldots, p_k)$ is a k-cycle in S_n and $\pi \in S_n$, then $(p_1^\pi, \ldots, p_k^\pi)$ is a k-cycle of $\sigma^\pi = \pi^{-1}\sigma\pi$. For

$$(p_i^\pi)^{\pi^{-1}\sigma\pi} = (p_i)^{\sigma\pi} = p_{i+1}^\pi.$$

Corollary 1.7. *If σ and τ are* conjugates *in S_n (i.e. $\tau = \pi^{-1}\sigma\pi$ for some $\pi \in S_n$) then σ and τ have exactly the same cycle structure (and vice versa).*

Example 1.8.
- The *general linear* group $\mathrm{GL}(n, F)$ is the multiplicative group of all $n \times n$ matrices over a field F with non-zero determinant (invertible, or non-singular matrices), e.g., $\mathrm{GL}(n, \mathbb{Q})$; we usually write $\mathrm{GL}(n, p)$ for $\mathrm{GL}(n, \mathbb{F}_p)$ when p is prime.
- The *special linear* group $\mathrm{SL}(n, F)$ is the multiplicative group of all $n \times n$ matrices over a field F with determinant 1; we usually write $\mathrm{SL}(n, p)$ for $\mathrm{SL}(n, \mathbb{F}_p)$ when p is prime.
- The *orthogonal* group $O(n, F)$ is the subgroup $\left\{A \in \mathrm{GL}(n, F) \;\middle|\; A^T A = I_n\right\}$ of $\mathrm{GL}(n, F)$ consisting of all $n \times n$ orthogonal matrices over F.
- The *special orthogonal* group $\mathrm{SO}(n, F)$ is the subgroup $\{A \in O(n, F) \mid \det(A) = 1\}$ of $\mathrm{GL}(n, F)$ consisting of all $n \times n$ orthogonal matrices over F of determinant 1; we usually write $O(n)$ and $SO(n)$ for $O(n, \mathbb{R})$ and $SO(n, \mathbb{R})$, respectively.
- The *unitary* group $U(n)$ is the subgroup $\{A \in GL(n, \mathbb{C}) \mid A^* A = I_n\}$ of $GL(n, \mathbb{C})$ made up of all $n \times n$ unitary complex matrices (where A^* is the transpose conjugate of A).
- The *special unitary* group $SU(n)$ is the subgroup $\{A \in U(n) \mid \det(A) = 1\}$ of $GL(n, \mathbb{C})$ consisting of all $n \times n$ unitary complex matrices of determinant 1.

Proposition 1.9. $\mathrm{SL}(2, 2) \cong S_3$.

Proof. One can consider members of $SL(2, 2)$ to consist of two choices from $X = \{(1, 1), (1, 0), (0, 1)\}$ as the rows. That is, all permutations on X. □

A subgroup H of a group G is called *normal* if $Hg = gH$ for all $g \in G$, or equivalently, if $g^{-1}Hg = H$ for all $g \in G$ (so $N_G(H) = G$). In this case we write $H \trianglelefteq G$.

- If $|G : H| = 2$, then $H \trianglelefteq G$ since H has 2 right cosets H and $G \setminus H$;
- If G is Abelian, then $H \trianglelefteq G$ for every subgroup H of G.
- $H = \{(), (1, 2)\}$ is not a normal subgroup of S_3, since $H(1, 3) = \{(1, 3), (1, 2, 3)\}$ yet $(1, 3)H = \{(1, 3), (1, 3, 2)\}$.

If N is a normal subgroup of G, then the set of right cosets of N in G forms a group with multiplication defined by $(Nx)(Ny) = Nxy$ for all $x, y \in G$. This group is called the *quotient* or *factor* group of G by N, and is denoted by G/N. Its identity element is N and the inverse of an element Nx is Nx^{-1}.

Note that $|G/N| = |G : N| = \frac{|G|}{|N|}$.

If G and H are groups, then a mapping $\phi : G \to H$ is called a *homomorphism* if ϕ preserves the group operations, that is, if $(xy)^\phi = x^\phi y^\phi$ for all $x, y \in G$ (alternative notation is $(xy)\phi = (x\phi)(y\phi)$).

A group homomorphism $\phi : G \to H$ is

- *trivial* if $g\phi = 1_H$ for all $g \in G$;
- a *monomorphism* if ϕ is one-to-one;
- an *epimorphism* if ϕ is onto;
- an *isomorphism* if ϕ is bijective, in which case we write $G \cong H$;
- an *endomorphism* of G if $G = H$;
- an *automorphism* if $G = H$ and ϕ is bijective.

Given a group G, the set of all automorphisms of G forms a group under composition, denoted by $\mathrm{Aut}(G)$ and called the *automorphism* group of G.

Example 1.10. The following are homomorphisms:

- $\varphi : G \to H$ given by $g \mapsto 1_H$.
- $\varphi : \mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}^*$ given by $g \mapsto \det(g)$.
- $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $a \mapsto [a]_n$.

Theorem 1.11. (Properties of homomorphisms). *If $\theta : G \to H$ is a group homomorphism, then:*

(1) *θ is one-to-one iff $\ker\theta = \{1_G\}$;*
(2) *θ is onto iff $\mathrm{im}\,(\theta) = H$;*
(3) *the image A^θ of any subgroup A of G is a subgroup of H;*
(4) *the pre-image $\overleftarrow{B}$ of any subgroup B of H is a subgroup of G;*
(5) *if A is a normal subgroup of G then its image A^θ is a normal subgroup of $\mathrm{im}\,(\theta)$;*
(6) *if B is a normal subgroup of H then its pre-image $\overleftarrow{B}$ is normal in G.*

Proof. Suppose θ is one-to-one. Then $\ker\theta = \left\{g \in G \mid g^\theta = 1_H\right\}$ has order at most one. Since $(1_G)^\theta = 1_H$, $\ker\theta = \{1_G\}$. Conversely, suppose $\ker\theta = \{1_G\}$ and that $g^\theta = h^\theta$ for some $g, h \in G$. Then one easily deduces $\left(gh^{-1}\right)^\theta = 1_H$, giving us that $gh^{-1} = 1_G$. It follows that $g = h$, proving (1).

(2) holds by definition.

Suppose that $A \leq G$. Then given any $a, b \in A^\theta$, we get that $a = g^\theta$ and $b = h^\theta$ for some $g, h \in A$. Hence, $gh^{-1} \in A$ because A is a subgroup of G. It follows that $\left(gh^{-1}\right)^\theta = g^\theta\left(h^{-1}\right)^\theta = ab^{-1}$ is a member of A^θ. Moreover, it is clear that A^θ contains 1_H because A contains 1_G, and so this proves (3).

Suppose that B is a subgroup of H. Then the pre-image of B contains 1_G. Say a, b are members of the pre-image of B. Then $a^\theta, b^\theta \in B$, giving us that $\left(ab^{-1}\right)^\theta \in B$ by applying basic group axioms, giving us (4).

Suppose A is a normal subgroup of G. Then $g^{-1}Ag = A$ for each $g \in G$. That is to say, $g^{-1}ag \in A$ for all $a \in A$ and all $g \in G$. Say that $a \in A^\theta$ and $b \in \mathrm{im}\,(\theta)$. Then $a = g^\theta$ and $b = h^\theta$ for some $g \in A$ and $h \in G$. Hence, $h^{-1}gh \in A$, so $\left(h^{-1}gh\right)^\theta = \left(h^\theta\right)^{-1}g^\theta h^\theta \in A^\theta$, giving us that $b^{-1}ab \in A^\theta$. It follows that A^θ is normal.

Suppose that B is a normal subgroup of H, and that $g \in G$ and b is a member of the pre-image of B. Then $\left(g^{-1}bg\right)^\theta \in B$ can be deduced easily, giving us the pre-image of B is indeed normal. □

Given a group homomorphism $\phi : G \to H$, the *image* of ϕ is defined as $\{y \in H \mid y = x\phi \text{ for some } x \in G\}$ and denoted by $\mathrm{im}\,(\phi)$, and the *kernel* of ϕ is defined as $\{x \in G \mid x\phi = 1_H\}$ and denoted by $\ker\phi$.

Theorem 1.12. (First Isomorphism Theorem). *Let $\varphi : G \to H$ be a group homomorphism with kernel K. Then $K \trianglelefteq G$ and $G/K \cong \mathrm{im}\,(\varphi)$.*

Proof. Suppose $g \in G$ and $k \in K$. Then

$$\begin{aligned}\left(g^{-1}kg\right)^\varphi &= \left(g^{-1}k\right)^\varphi g^\varphi \\ &= \left(g^{-1}\right)^\varphi k^\varphi g^\varphi \\ &= \left(g^{-1}\right)^\varphi 1_H g^\varphi \\ &= \left(g^{-1}\right)^\varphi g^\varphi,\end{aligned}$$

and we claim that $\left(g^\varphi\right)^{-1} = \left(g^{-1}\right)^\varphi$, which with this would obviously give us the desired result. The claim can be easily proved by noting $1_H = \left(gg^{-1}\right)^\varphi = g^\varphi\left(g^{-1}\right)^\varphi$.

Now, we claim $\psi : G/K \to \mathrm{im}\,(G)$ defined by $(Kg)^\psi = g^\varphi$ is an isomorphism. We firstly show that ψ is well-defined. To this end, suppose $Kg = Kh$ for some $g, h \in G$. Then $g = kh$ for some $k \in K$, giving us that

$$g^\varphi = (kh)^\varphi = k^\varphi h^\varphi = h^\varphi,$$

as desired. Now, ψ is a homomorphism since

$$(Kgh)^{\psi} = (gh)^{\varphi} = g^{\varphi}h^{\varphi} = (Kg)^{\psi}(Kh)^{\psi}.$$

We note that ψ is onto, since given any $h \in \operatorname{im}(G)$, we have that $h = g^{\varphi}$ for some $g \in G$ and so one simply takes $(Kg)^{\psi}$. Lastly, ψ is one-to-one, since if $(Kg)^{\psi} = (Kh)^{\psi}$, then $g^{\varphi} = h^{\varphi}$ implies that $gh^{-1} \in K$. That is, $g \in Kh$ and so $Kg = Kh$. □

Example 1.13. $\operatorname{SL}(n, \mathbb{F}) \trianglelefteq \operatorname{GL}(n, \mathbb{F})$ and $\operatorname{GL}(n, \mathbb{F})/\operatorname{SL}(n, \mathbb{F}) \cong \mathbb{F}^*$.

Proof. Consider $\varphi : \operatorname{GL}(n, \mathbb{F}) \to \mathbb{F}^*$ given by $g \mapsto \det(g)$. Then we claim φ is a homomorphism with kernel $\operatorname{SL}(n, \mathbb{F})$. Suppose that $g, h \in \operatorname{GL}(n, \mathbb{F})$. Then $\det(g)\det(h) = \det(gh)$ from Linear Algebra, giving us φ is indeed a homomorphism. Moreover, it is clear the kernel is the special linear group, so one needs only apply the First Isomorphism Theorem. □

Also, $\operatorname{im}(\varphi) = \mathbb{F}^* = \mathbb{F} \setminus \{0\}$ since

$$\begin{bmatrix} \lambda & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

has determinant λ.

Example 1.14. Define $\theta : S_n \to \{+1, -1\}$ by

$$\pi^{\theta} = \begin{cases} 1 & \text{if } \pi \text{ is even;} \\ -1 & \text{if } \pi \text{ is odd.} \end{cases}$$

Then θ is a homomorphism, where $\ker\theta = A_n$ and $\operatorname{im}(\theta) = \{+1, -1\} \cong C_2$ and hence $S_n/A_n \cong C_2$.

Theorem 1.15. (Cayley's Theorem). *Every group G is isomorphic to a group of permutations on a set of the same cardinality as G.*

Proof. For each $g \in G$, let μ_g be the right multiplication of G by g (i.e., $x \mapsto xg$). Then μ_g is a bijection/permutation, where $\mu_{g^{-1}}$ is the inverse of μ_g. If we define $\theta : G \to \operatorname{Sym}(G)$ by $g^{\theta} = \mu_g$, then θ is a one-to-one group homomorphism. We have that $(gh)^{\theta} = \mu_{gh}$, where μ_{gh} sends x to xgh. Since $\mu_g\mu_h$ first sends x to xg, then xg to xgh, it follows that $\mu_{gh} = \mu_g\mu_h$, and hence θ is indeed a group homomorphism. Moreover, if μ_g sends x to itself for each $x \in G$, it follows that g is the identity. From this, θ is one-to-one, and so $\ker\theta = \{1_G\}$. Thus, $G \cong G/\{1_G\} \cong \operatorname{im}(\theta) \leq \operatorname{Sym}(G)$. □

Definition 1.16. Suppose $H, K \subseteq G$. Then we define the *product* of H and K to be

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

Lemma 1.17. *Suppose $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.*

Proof. ($\Longrightarrow$) Suppose HK is a subgroup of G, and that $ab \in HK$ for some $a \in H$ and $b \in K$. Then $(ab)^{-1} = b^{-1}a^{-1} \in HK$, since HK is a subgroup of G. It follows that $b^{-1}a^{-1} = cd$ for some $c \in H$ and $d \in K$. Therefore, it follows that

$$ab = \left(b^{-1}a^{-1}\right)^{-1} = (cd)^{-1} = d^{-1}c^{-1} \in KH.$$

Hence, $HK \subseteq KH$.

Now, suppose that $ab \in KH$ for some $a \in K$ and $b \in H$. Then $b^{-1} \in H$ and $a^{-1} \in K$, giving us that $b^{-1}a^{-1} \in HK$. Since HK is a subgroup of G, it follows that $\big(b^{-1}a^{-1}\big)^{-1} = ab \in HK$. Thus, $KH \subseteq HK$ and so $HK = KH$.

($\Longleftarrow$) Suppose $HK = KH$. Since HK contains the identity $1_H 1_K = 1_G 1_G = 1_G$, we know HK is non-empty. Now, suppose that $a, b \in HK$. Then $a = h_1k_1$ and $b = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Therefore,

$$ab^{-1} = (h_1k_1)\big(k_2^{-1}h_2^{-1}\big) = h_1\big(k_1k_2^{-1}\big)h_2^{-1},$$

where $k_1k_2^{-1} \in K$ because K is a subgroup of G. It follows that $h_1\big(k_1k_2^{-1}\big) \in HK$, and since $HK = KH$ we get that $h_1\big(k_1k_2^{-1}\big) = kh$ for some $k \in K$ and $h \in H$. Hence, as we know $hh_2^{-1} \in H$ because $H \leq G$, we get

$$ab^{-1} = k\big(hh_2^{-1}\big) \in KH = HK.$$

Thus, HK is a subgroup of G. □

Corollary 1.18. *Suppose $N \trianglelefteq G$ and $H \leq G$. Then $NH \leq G$.*

Proof. We have that $NH = \bigcup_{h\in H} Nh = \bigcup_{h\in H} hN = HN$, and so $NH \leq G$. □

Corollary 1.19. *If $N \trianglelefteq G$ and $H \leq G$, then $\langle N, H\rangle = NH$.*

Proof. $NH \leq G$ and $N, H \subseteq NH$ and any subgroup of G which contains N and H must contain NH. □

Theorem 1.20. (Correspondence Theorem). *Let G be a group and N be a normal subgroup of G. Then:*

1. *If $N \leq A \leq G$, then $A/N \leq G/N$. Furthermore, if $A \trianglelefteq G$ then $A/N \trianglelefteq G/N$.*
2. *Conversely, each subgroup $H \leq G/N$ has the form $H = A/N$ for some $A \leq G$. Furthermore, if $H \trianglelefteq G/N$ then $A \trianglelefteq G$.*

Proof. Suppose $N \leq A \leq G$. If $N \trianglelefteq G$, then $N \trianglelefteq A$, so A/N exists and $A/N \subseteq G/N$. Then A contains the identity element of G, giving us that N is a member of A/N (so A/N is non-empty). Now, if $Na, Nb \in A/N$, then $(Na)(Nb)^{-1} = N\big(ab^{-1}\big) \in A/N$. Hence, $A/N \leq G/N$. If A is a normal subgroup, and $Na \in A/N$ and $Ng \in G/N$, we get that

$$(Ng)^{-1}(Na)(Ng) = \big(Ng^{-1}\big)(Nag) = N\big(g^{-1}ag\big).$$

Since A is normal, $g^{-1}ag \in A$, so A/N is normal (proving (1)).

Suppose $H \leq G/N$. Then define $\theta : G \to G/N$ by $g^\theta = Ng$. Such a map θ is a group homomorphism, so the pre-image A of H must be a subgroup of G. Also, $A^\theta = \{Na \mid a \in A\} = A/N$, so $H = A/N$. Since the pre-image of any normal group is normal, we are done. □

Theorem 1.21. (Second Isomorphism Theorem). *If $H \leq G$ and $N \trianglelefteq G$, then $(N \cap H) \trianglelefteq H$ and $H/(N \cap H) \cong NH/N$.*

Proof. Define $\theta : H \to G/N$ by $a \mapsto Na$. Then θ is a homomorphism with kernel $\{a \in H \mid Na = N\} = \{a \in H \mid a \in N\} = N \cap H$. Hence, $N \cap H \trianglelefteq H$, and the image $H/(N \cap H) \cong NH/N$. □

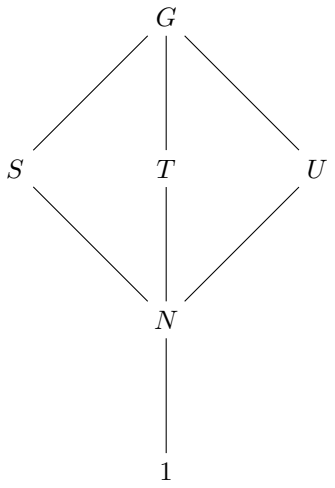
Theorem 1.22. (Third Isomorphism Theorem). *If $K \trianglelefteq G$ and $L \trianglelefteq G$ with $K \leq L$, then $L/K \trianglelefteq G/K$ and $(G/K)/(L/K) \cong G/L$.*

Proof. Let $\theta : G/K \to G/L$ be defined by $(Ka)^\theta = La$. Then θ is well-defined since if $Ka = Kb$, then La contains Ka and Lb contains Kb (which are both non-empty) because $K \leq L$. It follows that $La = Lb$, so θ is well-defined. Moreover, θ is a group homomorphism, as K and L are normal subgroups of G (so the operations are well-defined). Notice that L/K is well-defined because $K \leq L$ and K, L being normal implies that K is a normal subgroup of L. Then $\ker\theta = \{Ka \mid La = L\} = \{Ka \mid a \in L\} = L/K$, giving us $L/K \trianglelefteq G/K$ by the First Isomorphism Theorem. Also, θ is clearly onto, giving us that $(G/K)/(L/K) \cong G/L$ by the First Isomorphism Theorem. □

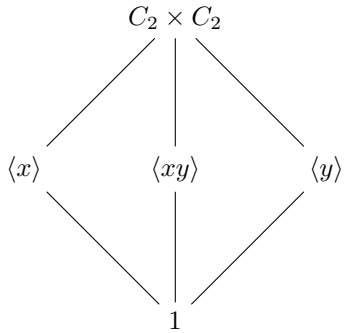
Example 1.23. Suppose $G = D_4 = \langle(1\ 2\ 3\ 4), (1\ 4)(2\ 3)\rangle$. Let $a = (1\ 2\ 3\ 4)$ and $b = (1\ 4)(2\ 3)$ and $N = \langle a^2\rangle = \langle(1\ 3)(2\ 4)\rangle$. Note that $N \trianglelefteq G$, $|G/N| = 4$ and $G/N \cong C_2 \times C_2$. Now, define the following:

$$\begin{aligned} S &= \{1, a, a^2, a^3\} = \langle a\rangle, \\ T &= \{1, b, a^2, ba^2\} = \langle a^2, b\rangle, \quad \text{and} \\ U &= \{1, ba, a^2, ba^3\} = \langle ba\rangle. \end{aligned}$$

We illustrate this with the following diagram.



Let $x = (1\ 2)$ and $y = (3\ 4)$ such that $C_2 \times C_2 = \langle x, y\rangle$. Then this is illustrated below:



Proposition 1.24. *The centre $Z(G) = \{z \in G \mid zg = gz\ \forall g \in G\}$ of a group G is a normal subgroup of G.*

Proof. By definition of the identity element, $1_G g = g = g1_G$, and so $Z(G)$ is non-empty. If $a, b \in Z(G)$, then given any $g \in G$ we have that $g(ab) = (ga)b = a(gb) =$

$(ab)g$. Also, $ag = ga$ implies $a^{-1}g = ga^{-1}$, so $Z(G)$ is a subgroup of G. Moreover, if $z \in Z(G)$ and $g \in G$, then $gz = zg$ implies $g^{-1}zg = z$, which clearly means that $Z(G)$ is normal. □

Example 1.25.
- $Z(S_n) = \{1\}$ for all $n \geq 3$.
- $Z(D_4) = \langle (1\ 3)(2\ 4) \rangle$, which is a group of order 2.
- $Z(Q_8) = \langle (1\ 2)(3\ 4)(5\ 6)(7\ 8) \rangle$.
- $|D_n|$ is 1 if n is odd and 2 if n is even.

Proposition 1.26. *Let $G = \mathrm{GL}(2, \mathbb{R})$. Then*

$$Z(G) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\middle|\; a \in \mathbb{R} \right\}.$$

Proof. Suppose $M_1 \in Z(G)$ and $M_2 \in G$, where

$$M_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$
$$M_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

Then $M_1M_2 = M_2M_1$:

$$\begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix} = \begin{pmatrix} a_2a_1 + b_2c_1 & a_2b_1 + b_2d_1 \\ c_2a_1 + d_2c_1 & c_2b_1 + d_2d_1 \end{pmatrix},$$

implying that $b_1c_2 = b_2c_1$. Since c_2 and b_2 are arbitrary, we could choose $b_2 = c_2 = 1$, giving us that we must have that $c_1 = b_1$. Moreover, we could choose $c_2 = b_2 + 1$, and so clearly for equality we must have $c_1 = b_1 = 0$. Moreover, $a_1 = d_1$ follows from this. □

Proposition 1.27. *Suppose x is an element of a group G, and H is a subgroup of G. Then $C_G(x) = \{g \in G \mid xg = gx\} \leq G$ and $C_G(H) = \bigcap_{x \in H} C_G(x) \leq G$.*

Proof. Suppose $a, b \in C_G(x)$ (note $C_G(x)$ contains 1_G, and so is non-empty). Then

$$x(ab) = (xa)b = (ax)b = a(xb) = (ab)x,$$

so $ab \in C_G(x)$. Also, $ax = xa$ implies $xa^{-1} = a^{-1}x$, giving us that $C_G(x)$ is closed under inverses. It follows that $C_G(x)$ is a subgroup of G. As the intersection of subgroups is itself a subgroup, we are done. □

Proposition 1.28. *Let $H \leq G$. Then $H \trianglelefteq N_G(H) = \langle g \in G : g^{-1}Hg = H \rangle \leq G$.*

Proof. Since $1_G \in N_G(H)$, it is non-empty. If $a, b \in N_G(H)$ and $h \in H$, then

$$(ab)^{-1}h(ab) = \big(b^{-1}a^{-1}\big)h(ab) = b^{-1}\big(a^{-1}ha\big)b = b^{-1}kb \in H,$$

where $k \in H$. It follows that $ab \in N_G(H)$. Inverses are clear, so $N_G(H) \leq G$.

Now, suppose that $a \in H$ and $g \in N_G(H)$. Notice that $g^{-1}ag \in H$, by definition, so H is a normal subgroup of $N_G(H)$. □

Example 1.29. Suppose $G = S_3$. Then $G' = \langle (1\ 2\ 3) \rangle \cong \mathbb{Z}_3$. Suppose $G = A_4$. Then $G' = \langle (1\ 3)(2\ 4), (1\ 2)(3\ 4) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition 1.30. A subgroup $H \leq G$ is *characteristic* and write $H \operatorname{char} G$ if H is stabilised - that is, fixed as a set but not necessarily point-wise - by all automorphisms of G.

Proposition 1.31. *For any group G, $G' \operatorname{char} G$, where G' is the derived group. Moreover, if $N \trianglelefteq G$ then G/N is Abelian iff $G' \leq N$.*

Proof. Suppose $\varphi \in \mathrm{Aut}(G)$. Since $G' = \langle X \rangle$, where $X = \{[x,y] \mid x,y \in G\}$, we need only show $X^\varphi = X$. We have that $[x,y]^\varphi = [x^\varphi, y^\varphi]$. Since φ is an automorphism, each element has an inverse, and so it is clear $X^\varphi = X$.

Let $N \trianglelefteq G$. Suppose G/N is Abelian, and let $x,y \in G$. Then

$$N[x,y] = \left(Nx^{-1}\right)\left(Ny^{-1}\right)(Nxy) = \left(Ny^{-1}\right)\left(Nx^{-1}\right)(Nxy) = N,$$

giving us that N contains G'. Clearly, this gives us that $G' \leq N$. If on the other hand $G' \leq N$, then

$$(Na)(Nb) = Nab = (Nba)(N[b,a])(N[a,b]) = Nba = (Nb)(Na).$$

□

Definition 1.32. We say that G is an *elementary abelian p-group* if

$$G \cong C_p \times \ldots \times C_p,$$

where C_p denotes the cyclic group of order p.

Theorem 1.33. *Let $G \cong C_p \times \ldots \times C_p$ (d copies) be an elementary abelian p-group. Then*

$$\mathrm{Aut}(G) \cong \mathrm{GL}(d,p).$$

Proof. We identify G with a vector space of dimension d over $\mathrm{GF}(p)$. Observe that we can regard the elements of G as d-component row vectors with entries from $\mathrm{GF}(p)$ and allow $\mathrm{GL}(d,p)$ to act by right multiplication. Note G has a basis $\{v_1, \ldots, v_d\}$, and that any automorphism φ of G has $\{v_1^\varphi, \ldots, v_d^\varphi\}$ as a basis for G. Since each of the other vectors are uniquely determined by the basis vectors, one can associate $\mathrm{Aut}(G)$ with a basis for G. □

We say that G is *simple* if the only normal subgroups of G are G and $\{1_G\}$.

Definition 1.34. Recall that for each $g \in G$, the map $\theta_g : G \to G$ defined by $h^{\theta_g} = g^{-1}hg$ is an automorphism of G. Automorphisms of this form are called *inner automorphisms*. We say that θ_g is the *inner automorphism induced by g*. The set of all inner automorphisms of a group G is $\mathrm{Inn}(G) = \{\theta_g \mid g \in G\}$.

Proposition 1.35. *For any group G,* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof. Certainly $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$, and $\mathrm{Inn}(G)$ is non-empty (it contains the identity). Suppose $\theta_g \in \mathrm{Inn}(G)$. Then $\theta_{g^{-1}}$ is the inverse of θ_g. Moreover, $\theta_g\theta_h$ sends $x \mapsto h^{-1}g^{-1}xgh$, so $\theta_g\theta_h = \theta_{gh}$. This establishes $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Suppose $\varphi \in \mathrm{Aut}(G)$ and $\theta_g \in \mathrm{Inn}(G)$. Then $\varphi^{-1}\theta_g\varphi$ sends x to $\left(g^{-1}\right)^\varphi x g^\varphi$. That is to say, $\varphi^{-1}\theta_g\varphi = \theta_{g^\varphi} \in \mathrm{Inn}(G)$. Thus, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

Note. We call $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ the *group of outer automorphisms*. Also, G is Abelian iff $\mathrm{Inn}(G) = \{\mathrm{id}\}$.

Example 1.36.

- $\mathrm{Aut}(C_n)$? Let G be the cyclic group of order n, say generated by x. If $\theta \in \mathrm{Aut}(G)$, then $\theta : x \mapsto x^\lambda$ for some λ. Since θ is onto, x^λ generated G, so $\gcd(\lambda, n) = 1$ and so $\lambda \in U(n)$. Hence, $|\mathrm{Aut}(C_n)| = |U(n)| = \phi(n)$, where ϕ is Euler's Totient function. Conversely, if $\lambda \in U(n)$, then the maps from G to G given by $x^i \mapsto x^{\lambda i}$ is an automorphism. Also, $\mathrm{Aut}(C_n)$ is Abelian, since $\left(x^\lambda\right)^\mu = x^{\lambda\mu} = (x^\mu)^\lambda$. In some cases, $\mathrm{Aut}(C_n)$ is cyclic; for example if p is prime then $U(p)$ is cyclic of order $p-1$, In this case, $\mathrm{Aut}(C_p) \cong C_{p-1}$. Yet, $\mathrm{Aut}(C_8) \cong U(8) = \{1,3,5,7\} \cong C_2 \times C_2$.
- Let A be an elementary Abelian p-group, where p is prime, (i.e., $A \cong C_p \times \ldots \times C_p = (C_p)^k$ for some k or $A \cong \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$). Then $\mathrm{Aut}(A) = \mathrm{Aut}\left(C_p^k\right) \cong \mathrm{Aut}\left(\mathbb{Z}_p^k\right) \cong \mathrm{GL}(k,p)$ since every automorphism is given by an invertible linear transformation of $(\mathbb{Z}_p)^k$.

- Automorphisms and symmetric groups: A_1, A_2 and S_1 are trivial. $\mathrm{Aut}\,(S_2) \cong \mathrm{Aut}\,(C_2) \cong U(2) \cong \{1\}$. $\mathrm{Aut}\,(S_3)$? If $\theta \in \mathrm{Aut}\,(S_3)$ then it has (1 2 3) sent to (1 2 3) or (1 3 2), and so $\mathrm{Aut}\,(S_3) \cong S_3$, $\mathrm{Aut}\,(A_3) \cong \mathrm{Aut}\,(C_3) \cong U(3) \cong C_2$.

Theorem 1.37. *Automorphism group of S_n is isomorphic to S_n for all $n \geq 3$ except $n = 6$ ($\mathrm{Aut}\,(S_6)$ twice as big as S_6). We also have $\mathrm{Aut}\,(A_n)$ isomorphic to S_n for all $n \geq 4$ except $n = 6$, where $\mathrm{Aut}\,(A_6) \cong \mathrm{Aut}\,(S_6)$.*

What is $\mathrm{Aut}\,(D_n)$? All reflections can be generated by rotations and a single reflection. Hence, $D_n \cong C_n \times C_2$, and so $\mathrm{Aut}\,(D_n) \cong \mathrm{Aut}\,(C_n) \cong U(n)$.

$\mathrm{Inn}\,(G) \cong G/Z(G)$, since $\phi : G \to \mathrm{Inn}(G)$ defined by $g \mapsto \tau_g$ is a homomorphism with kernel $Z(G)$ and is also onto. The factor group $\mathrm{Aut}\,(G)/\mathrm{Inn}(G)$ is called the outer automorphism group of G, and denoted by $\mathrm{Out}(G)$.

Example 1.38. (1) $\mathrm{Inn}(G) \cong C_n/Z(C_n) = C_n/C_n = \{1\}$ and $\mathrm{Out}(C_n) \cong \mathrm{Aut}\,(C_n)/\mathrm{Inn}(C_n) \cong \mathrm{Aut}\,(C_n) \cong U(n)$.

(2) If A is any Abelian group, then $\mathrm{Inn}(A) = \{1\}$, and $\mathrm{Out}(A) \cong \mathrm{Aut}\,(A)$.

(3) In particular, $\mathrm{Out}\left((C_p)^k\right) \cong \mathrm{Aut}\left((C_p)^k\right) \cong \mathrm{GL}\,(k, p)$.

(4) $\mathrm{Inn}\,(A_n) \cong A_n/Z(A_n) \cong A_n/\{1\} \cong A_n$ for all $n \geq 4$. Also,

$$\mathrm{Out}\,(A_n) = \begin{cases} C_2 & \text{when } n \geq 4 \text{ and } n \neq 6; \\ \mathrm{Aut}\,(S_6)/A_6 & \text{if } n = 6. \end{cases}$$

We also get $\mathrm{Inn}\,(S_n) \cong S_n/Z(S_n) \cong S_n$ for all $n \geq 3$, and

$$\mathrm{Out}\,(S_n) \cong \mathrm{Aut}\,(S_n)/\mathrm{Inn}\,(S_n) \cong \begin{cases} S_n/S_n = \{1\} & \text{when } n \geq 3 \text{ but } n \neq 6; \\ C_2 & \text{when } n = 6. \end{cases}$$

Note.
- Every non-inner automorphism of S_6 takes 2-cycles $(\alpha\beta)$ to triple 2-cycles $(ab)(cd)(ef)$ and vice versa.
- Takes 3-cycles $(\alpha\beta\gamma)$ to double 3-cycles $(abc)(def)$.
- Takes 5 cycles to 5 cycles.

Two more things:

(1) A subgroup N of a group G is called *characteristic* in G if $N^\theta = N$ for all automorphisms θ of G, and we write $N \operatorname{char} G$. Note N is normal if $N^\theta = N$ for all $\theta \in \mathrm{Inn}\,(G)$.

(2) If H is a subgroup of G, the conjugation by elements of $N_G(H)$ gives a homomorphism from $N_G(H)$ to $\mathrm{Aut}\,(H)$ with kernel $C_G(H)$. Note $g \in N_G(H)$ we send $g \mapsto \tau_g \mid_H$. Hence, $C_G(H) \trianglelefteq N_G(H)$ and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}\,(G)$.

2. Group Actions

Definition 2.1. A *group action*, or *permutation representation* on a non-empty set Ω, is a homomorphism $\theta : G \to \mathrm{Sym}\,(\Omega)$.

Example 2.2.
- The *trivial representation* is defined by $\theta : g \mapsto 1_\Omega$ for all $g \in G$.
- The *regular representation* of G on itself by defined by $\theta : g \mapsto \mu_g$, where μ_g is the right multiplication by g. By Cayley's Theorem, this is an isomorphism from G to a subgroup of $\mathrm{Sym}\,(G)$.
- The *action in a coset space*: If $H \leq G$ and $(G : H) = \{Hx \mid x \in G\}$ then G acts on $(G : H)$ also by right multiplication $\mu_g : Hx \mapsto Hxg$ for all

$Hx \in (G:H)$. The latter is somtimes called the *natural* permutation representation of G on $(G:H)$. Its kernel is

$$\begin{aligned}\{g \in G \mid Hxg = Hx\ \forall x \in G\} &= \left\{g \in G \;\middle|\; Hxgx^{-1} = H\ \forall x \in G\right\} \\ &= \left\{g \in G \;\middle|\; xgx^{-1} \in H\ \forall x \in G\right\} \\ &= \left\{g \in G \;\middle|\; g \in x^{-1}Hx\ \forall x \in G\right\} \\ &= \bigcap_{x \in G} x^{-1}Hx,\end{aligned}$$

which is the intersection over all the conjugates of H in G, and is called the *core* of H in G, and denoted by $\mathrm{Core}_G(H)$.

Example 2.3. Consider $G = S_3$ and $H = \langle(1\ 2)\rangle = \{(), (1\ 2)\}$. The conjugates of H are the subgroups generated by (1 2), (1 3), (2 3) and as they intersect trivially $\mathrm{Core}_G(H) = \{1\}$. But if $H = A_3$ then $x^{-1}Hx = H$ for all $x \in G$ since $H = A_3 \trianglelefteq S_3$. Therefore, $\mathrm{Core}_{S_3}(A_3) = A_3$. More generally, if $H \trianglelefteq G$ then $\mathrm{Core}_G(H) = H$ and vice versa. In fact, $\mathrm{Core}_G(H)$ is the largest normal subgroup of G contained in H.

Lemma 2.4. *$|G : \mathrm{Core}_G(H)|$ divides $|G:H|!$*

Proof. Let $K = \mathrm{Core}_G(H) = \ker\theta$, where θ is the natural action of G on $(G:H)$. Then $G/K \cong \mathrm{im}(\theta) \leq \mathrm{Sym}(\Omega)$, so $|G:K| = |G/K| = |\mathrm{im}(\theta)|$ divides $|\mathrm{Sym}(\Omega)| = n!$ when $n = |\Omega| = |G:H|$. □

Corollary 2.5. *If $H \leq G$ and $|G:H| = p$, the smallest prime divisors of $|G|$, then $H \trianglelefteq G$.*

Proof. Let $K = \mathrm{Core}_G(H)$. Then $|G:K|$ divides $(|G:K|)! = p!$, but p is smallest prime dividing $|G|$, therefore $p-1$, $p-2$, …, 2 is coprime to $|G|$. Hence, $|G:K|$ divides p, and since $K \leq H$ it follows $|G:K| \geq |G:H|$ implying $|G:K| = p$. Hence, $H = K \trianglelefteq G$. □

Let $\theta : G \to \mathrm{Sym}(\Omega)$ be a group action on the set Ω. Then

- if $x \in \Omega$ then x^g denotes the image of x under the permutation g^θ;
- if $x \in \Omega$ then $x^G = \{x^g \mid g \in G\}$ is called the *orbit* of x under G;
- if $x \in \Omega$ then $G_x = \{g \in G \mid x^g = x\}$ is called the *stabilizer* in G of x;
- $\bigcap_{x\in\Omega} G_x = \{g \in G \mid x^g = x\ \forall x \in \Omega\} = \left\{g \in G \;\middle|\; g^\theta = 1_\Omega\right\} = \ker\theta$;
- If $\ker\theta = \{1_G\}$ then θ is said to be a *faithful* action. Note that in this case, $G \cong G/\{1_G\} \cong G/\ker\theta \cong \mathrm{im}(\theta)$. Hence, G is isomorphic to the permutation group it induces on Ω.
- If $\Omega = x^G$ for some $x \in \Omega$, then for every $y \in \Omega$ there exists $g \in G$ such that $x^g = y$, and we say that the action θ is *transitive* on Ω.
- If for every ordered pairs (α, β) and (γ, δ), *distinct* pairs of Ω, there exists some $g \in G$ such that $(\alpha^g, \beta^g) = (\alpha, \beta)^g = (\gamma, \delta)$ we say the action is 2-*transitive* on Ω.
- Similarly define "k-transitive" using the effect of θ on ordered k-tuples of distinct pairs of Ω.
- If an action is both faithful and transitive, then we say it is *regular*. That is, $x^G = \Omega$ and $\bigcap_{x\in\Omega} G_x$ is trivial.

Proposition 2.6. *Suppose G acts on Ω by θ. Then given any $x \in \Omega$, the stabilizer of x in G denoted G_x is a subgroup of G.*

Proof. Since θ is a homomorphism, $1_G \in G_x$. If $g, h \in G_x$, then $x^{gh^{-1}} = (x^g)^{h^{-1}} = x^{h^{-1}} = x$, implying $gh^{-1} \in G_x$. Note that $x^h = x$ implies $x^{h^{-1}} = x$. □

Example 2.7. (1) Conjugation: If G is a group, then G acts on itself by conjugation $g \mapsto \tau_g$, where $\tau_g : x \mapsto g^{-1}xg$. The image is $\{\tau_g \mid g \in G\} = \operatorname{Inn}(G)$ and the kernel is $\bigcap_{x\in G} C_G(x) = Z(G)$ where $G/Z(G) \cong \operatorname{Inn}(G)$. If $x \in G$, then

$$\begin{aligned} x^G &= \{x^g \mid g \in G\} \\ &= \left\{g^{-1}xg \;\middle|\; g \in G\right\} \\ &= \text{ } \textit{conjugacy class} \text{ of } x \text{ in } G \\ &= \operatorname{im}(\tau_g), \end{aligned}$$

and $G_x = \left\{g \in G \;\middle|\; g^{-1}xg = x\right\} = C_G(x)$ is the stabilizer.

(2) Natural action of G on $(G : H)$, for $H \leq G$. *Image* of this action is $\{\mu_g \mid g \in G\}$, where μ_g is the right multiplication by g on the cosets of H in G, and kernel is $\{g \in G \mid Hxg = Hx \ \forall x \in G\} = \operatorname{Core}_G(H)$ (i.e., μ_g is trivial on $(G : H)$).

$(Hx)^G = \{Hxg \mid g \in G\} = (G : H)$, so this action is transitive. Also, $G_{H_x} = \{g \in G \mid Hxg = Hx\} = x^{-1}Hx$.

(3) Conjugation of subgroups (say $\mathscr{H}$ is a collection of subgroups): $g \mapsto \tau_g$ where $\tau_g : H \mapsto g^{-1}Hg$. No particular name of the image. As for the kernel: $\left\{g \in G \;\middle|\; g^{-1}Hg = H \ \forall H \in \mathscr{H}\right\} = \bigcap_{H\in\mathscr{H}} N_G(H)$. The orbit: $H^G = \left\{g^{-1}Hg \;\middle|\; g \in G\right\}$ is the conjugacy class of H. The stabilizer: $G_H = \left\{g \in G \;\middle|\; g^{-1}Hg = H\right\} = N_G(H)$.

Theorem 2.8. (Orbit-Stabilizer Theorem). *If a finite group G acts on a set Ω, then $|G| = |G_\alpha|\left|\alpha^G\right|$ for every $\alpha \in \Omega$.*

Proof. We count the pairs $(g, \beta) \in G \times \Omega$ such that $\alpha^g = \beta$. On the one hand, for every $g \in G$, there exists a unique β, therefore the number of pairs is $|G|$. On the other hand, let $\beta \in \alpha^G$, say $\beta = \alpha^h$ for some $h \in G$. Then

$$\alpha^g = \beta \iff \alpha^g = \alpha^h \iff \alpha^{gh^{-1}} = \alpha \iff gh^{-1} \in G_\alpha \iff g \in G_\alpha h.$$

So, the number of g from given β is $|G_\alpha h| = |G_\alpha|$. Therefore, the number of pairs is $\left|\alpha^G\right||G_\alpha|$ (since $\left|\alpha^G\right|$ is number choices for β. Hence, $|G| = \left|\alpha^G\right||G_\alpha|$.

Fix $\alpha \in \Omega$. Then $G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$ is a subgroup of G. Then $\alpha^g = \alpha^h$ implies that $\alpha^{gh^{-1}} = \alpha$, giving us that $gh^{-1} \in G_\alpha$. Hence, $g \in G_\alpha h$, and so $G_\alpha g = G_\alpha h$ iff $\alpha^g = \alpha^h$. Therefore, $|G/G_\alpha| = \left|\alpha^G\right|$, and so the result holds by Lagrange's Theorem. □

Example 2.9. Let $\Omega = (G : H)$ with G acting on Ω by right multiplication. If $\alpha = H$, then $\alpha^G = \{Hg \mid g \in G\} = (G : H)$, and $G_\alpha = \{g \in G \mid Hg = H\} = \{g \in G \mid g \in H\} = H$, so $|G| = |G : H||H|$. Hence, Lagrange's Theorem is a consequence of the orbit stabilizer theorem. Conversely, if you take $H = G_\alpha$, then $(G : H) \equiv \Omega$ (and do more work).

Let G be a finite group acting on itself by conjugation. Then for every $x \in G$, we have that $x^G = \left\{g^{-1}xg \;\middle|\; g \in G\right\} = [x]$ is the *conjugacy class* of x in G. Also, $G_x = \left\{g \in G \;\middle|\; g^{-1}xg\right\} = C_G(x)$ is the conjugates of x in G. So, $|G| = |C_G(x)||[x]|$.

Theorem 2.10. (Class equation). *If $x_1, x_2, \ldots, x_k$ are representatives of the k distinct conjugacy classes of elements of the finite group G, then*

$$|G| = \sum_{1\leq i\leq k} \left|x_i^G\right| = \sum_{1\leq i\leq k} |G : C_G(x_i)|.$$

Proof. Observe $G = [x_1] \cup \ldots \cup [x_k]$, since each element of G lies in exactly one of the conjugacy classes. Hence,

$$|G| = \sum_{i=1}^{k} |[x_i]| = \sum_{i=1}^{k} \frac{|G|}{|C_G(x_i)|} = \sum_{i=1}^{k} |G : C_G(x_i)|.$$

□

A finite *p-group* is a finite group of order p^s for some $s \in \mathbb{N}$.

Corollary 2.11. *Centres of a non-trivial p-groups are non-trivial.*

Proof. We show that if P is a non-trivial p-group, then $Z(P)$ is also non-trivial.

Observe that

$$|P| = \sum_{i=1}^{k} |P : C_P(x_i)|,$$

where $x_1, x_2, \ldots, x_k$ are the conjugacy class representations, and if $x_i \in Z(P)$, then $C_P(x_i) = P$ and so $|P : C_P(x_i)| = 1$, and while if $x_i \notin Z(P)$, then $C_P(x_i)$ is a proper subgroup of P. Therefore, $|P : C_P(x_i)|$ is a non-trivial power of p, say $r_i > 0$ (by Lagrange's). Now, while

$$|P| = \sum_{i \text{ s.t. } zx_i \in Z(P)} 1 + \sum_{i \text{ s.t. } zx_i \notin Z(P)} p^{r_i} = |Z(p)| + pk,$$

where $k \in \mathbb{N}$. Taking modulo p on both sides implies that $|Z(p)|$ is divisible by p, so $|Z(p)| \neq 1$. □

Example 2.12. The number of conjugates of a subgroup of a group G. Let G be a finite group, and let $H \leq G$. Then let G act on Ω, the set of all subgroups of G, by conjugation. Then

$$|G| = |C_H| \left| H^G \right|$$

where

$$G_H = \left\{ g \in G \;\middle|\; g^{-1} H g = H \right\} = N_G(H).$$

Hence, $\left|H^G\right|$ is the number of conjugates of H, which is

$$\left|H^G\right| = \frac{|G|}{|G_H|} = \frac{|G|}{|N_G(H)|} = |G : N_G(H)|.$$

Lemma 2.13. (Burnside's Lemma). *If the finite group G acts on the set Ω, with exactly m orbits, and $F_\Omega(g) = \{\alpha \in \Omega \mid \alpha^g = \alpha\}$ is the set of fixed points of each $g \in G$, then*

$$|G| = \frac{1}{m} \sum_{g \in G} |F_\Omega(g)|.$$

Note. We let $\chi(g) = |F_\Omega(g)|$, which we sometimes call the *permutation character* of G.

Proof. Count in two diffeerent ways the number of pairs $(\alpha, g) \in \Omega \times G$ such that $\alpha^g = \alpha$. On the one hand, for each $\alpha \in \Omega$, the number of g is $|G_\alpha| = \frac{|G|}{|\alpha^G|}$ by the Orbit Stabilizer theorem. On the other hand, for each $g \in G$, the number of α is $\chi(g)$. Hence,

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

so

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

If the orbits are $\Delta_1, \ldots, \Delta_m$ where $\Delta_i = \alpha_i^G$, then each Δ_i has

$$\sum_{\alpha \in \Delta_i} \frac{1}{|\alpha^G|} = \sum_{\alpha \in \Delta_i} \frac{1}{|\Delta_i|} = |\Delta_i| \frac{1}{|\Delta_i|} = 1.$$

Thus,

$$|\alpha \in \Omega| \frac{1}{|\alpha^G|} = m.$$

□

Corollary 2.14. *If G is a transitive group on some set Ω, then there exists $g \in G$ with no fixed points.*

3. Sylow Theory

Definition 3.1. A *p-group* is a group if order p^s for some prime p and $s \in \mathbb{N}$.

Some properties:

- Every subgroup of a p-group is a p-group (apply Lagrange).
- Every quotient of a p-group is a p-group (i.e., $|P/N| = \frac{|P|}{|N|}$, which divides $|P|$).
- If P has prime order, then P is simple, and cyclic. If $H \trianglelefteq P$ and $H \neq \{1_P\}$, then $|H| = |P| = p$ (prime) by Lagrange, and therefore $H = P$ and so only subgroups are $\{1_P\}$ and P (implying P is simple). In particular, if $x \neq 1_P \in P$, then $\langle x \rangle = P$, and thus P is cyclic generated by x.
- If P is a non-trivial p-group, then it has non-trivial centre $Z(P)$ by the Class equation.

Corollary 3.2. *If $|P| = p^2$ where p is prime, then P is Abelian.*

Proof. We know that $Z(P)$ is non-trivial, by the above. Hence, $|Z(P)| = p$ or p^2 by Lagrange. If $|Z(P)| = p^2$ then $Z(p) = P$, implying P is Abelian. Finally, suppose $|Z(P)| = p$. Then also $|P/Z(P)| = p$. Hence, both $Z(P)$ and $P/Z(P)$ are cyclic, and then P is Abelian due to a general property that doesn't depend on the orders of $|P|$ and $|Z(P)|$, which we prove in the proposition below. □

Proposition 3.3. *Suppose G is a finite group, with $Z(G)$ and $G/Z(G)$ both cyclic. Then G is Abelian.*

Proof. Suppose $Z(G)$ is generated by $x \in G$ and $G/Z(G)$ is generated by Ny, where $N = Z(P)$. Then every element of N is is expressed as x^i for some i and every element of G/N is expressed as $(Ny)^j = Ny^j$ for some j. Therefore, every element of G is expressed by $x^i y^j$ for some i, j. Since $x \in Z(G) = N$, we have $\left(x^i y^j\right)\left(x^k y^\ell\right) = \left(x^k y^\ell\right)\left(x^i y^j\right)$ by simple rearrangement. Thus, G is Abelian. □

There are three Sylow theorems, which concern the existence and properties of p-subgroups of finite groups (subgroups that are p-groups).

The first one says that if p^s is the largest power of p that divides $|G| = p^s m$ for some m coprime to p, then there exists a subgroup of order p^s in G. This is one case where the converse of Lagrange's theorem holds. But the converse of Lagrange's theorem does not always hold. If $n \geq 4$, A_n has no subgroup of order $\frac{n!}{4}$ (and index 2).

Proof. Suppose the contrary, and H is a subgroup of A_n of order $\frac{n!}{4} = \frac{|A_n|}{2}$. Then H has 2 cosets in A_n; H and A_n/H. So, H is a normal subgroup of A_n with $A_n/H \cong C_2$. Now, every element of order 3 in A_n must lie in H (since there are no elements of order 3 in C_2 by Lagrange). Therefore, A_n cannot be generated by the 3-cycles, a contradiction. □

Theorem 3.4. (Sylow's First Theorem). *Let G be a finite group of order $p^s m$ where p is prime and $s, m \in \mathbb{Z}^+$, with p coprime to m. Then there exists a subgroup P in G of order p^s (called a Sylow p-subgroup of G).*

Proof. Let Ω be the set of all subsets of G of size p^s. Then G acts on Ω by right multiplication:

$$\text{if } T \subseteq G \text{ with } |T| = p^s \text{ then also } Tg \subseteq G \text{ with } |Tg| = |T| = p^s.$$

Also note that

$$|\Omega| = \binom{|G|}{p^s} = \binom{p^s m}{p^s} = \frac{p^s m(p^s m - 1)\dots(p^s m - p^s + 1)}{p^s(p^s - 1)\dots(p^s - p^s + 1)},$$

and is not divisible by p. Since if one term $p^s - k$ of the denominator is divisible by p^r (where $1 \le r \le s$), then p^r divides $p^s m - k$. So every power of p that divides the denominator also divides the numerator.

Next, because p does not divide $|\Omega|$, we know that p does not divide the order of some orbit Δ of G on Ω (since the order of Ω is the sum of sizes of all orbits). Suppose Δ is the orbit containing the subset E of G, i.e., $\Delta = \{Eg \mid g \in G\}$, and let $P = G_E$ be the stabilizer in G of E ($\{g \in G \mid Eg = E\}$). By the Orbit-Stabilizer theorem,

$$|G| = |G_E|\left|E^G\right| = |P||\Delta| = p^s m,$$

yet $|\Delta|$ is not divisible by p, implying that $|P|$ is divisible by p^s. But also $P = G_E$ acts on E by right multiplication (as $Eg = E$ for all $g \in P$), and if $x \in E$ then $P_x = \{g \in P \mid xg = x\} = \{1\}$. Therefore, by the Orbit-Stabilizer theorem

$$|P| = |P_x|\left|x^P\right| = \left|x^P\right|.$$

Therefore, every orbit of P in E has size $|P|$, so $p^s = |E|$ equal to the union of orbits of P in E which is sum of these sizes of $|P|$. So p^s is a multiple of $|P|$. Thus, $|P| = p^s$, and $P \le G$, so P is a Sylow p-subgroup of G. □

Theorem 3.5. (Sylow's Second Theorem). *Let G be a finite group of order $p^s m$ where p is prime and $s, m \in \mathbb{Z}^+$, with p coprime to m. If P is a Sylow p-subgroup of G, and Q is any p-subgroup of G, then $Q \le x^{-1}Px$ for some $x \in G$. In particular, all Sylow p-subgroups of G are conjugate to each other (i.e., equality takes place).*

Proof. Consider the group action of Q on the orbit $\Delta = E^G$, where E is a subset of G of size p^s. By the Orbit-Stabilizer Theorem, each such orbit has size a power of p. Also, we chose Δ (in the proof of Sylow's first theorem) such that $|\Delta| \not\equiv 0 \mod p$. So at least one of the orbits of Q on Δ must have size 1 (as $|\Delta|$ is a sum of powers of p, but not divisible by p). Therefore, Q must fix some members of $\Delta = E^G$, say E_g (where $g \in G$). Therefore, $Q \le \mathrm{Stab}_G(E_g) = g^{-1}\mathrm{Stab}_G(E)g = g^{-1}Pg$. In particular, also if R is any Sylow p-subgroup of G, then $R \le h^{-1}Ph$ for some $h \in G$. Hence, we get $R = h^{-1}Ph$ (by comparing orders). Therefore,

$$Q \le g^{-1}Pg = x^{-1}Rx,$$

where $x = h^{-1}g \in G$. The rest follows easily. □

Theorem 3.6. (Sylow's Third Theorem). *Let G be a finite group of order $p^s m$ where p is prime and $s, m \in \mathbb{Z}^+$, with p coprime to m. $\left|\mathrm{Syl}_p(G)\right|$ is the number of Sylow p-subgroups of G is a divisor of $|G|$, and is congruent to 1 modulo p. In fact, if we define $n_p = \left|\mathrm{Syl}_p(G)\right|$, then $n_p = |G : N_G(P)|$ for every $P \in \mathrm{Syl}_p(G)$.*

Proof. By Sylow's second theorem, G acts transitively by conjugation on $\mathrm{Syl}_p(G)$ (i.e., if $Q, R \in \mathrm{Syl}_p(G)$ then there exists $x \in G$ such that $Q = x^{-1}Rx$). Therefore, by the Orbit-Stabilizer theorem,

$$|G| = |G_P|\left|P^G\right| = |N_G(P)|\left|\mathrm{Syl}_p(G)\right| = |N_G(P)|n_p,$$

so n_p divides $|G|$ and $n_p = \frac{|G|}{|N_G(P)|}$.

Now we prove the first part. Let $\Delta_1, \Delta_2, \ldots, \Delta_t$ be the orbits of G on Ω (under right multiplication). If $S \in \Delta_i$, then let $x \in S$, and we have $1_G = xx^{-1} \in Sx^{-1} \in S^G = \Delta_i$. So now choose $E_1, E_2, \ldots, E_t \in \Delta_1, \Delta_2, \ldots, \Delta_t$ (respectively) such that $1_G \in E_i$ and define $P_i = \mathrm{Stab}_G(E_i) = G_{E_i}$. Next, for any say $y \in P_i$ we have $E_i y = E_i$, and therefore $y = 1_G y \in E_i y = E_i$. Hence, $P_i = E_i$. And conversely, if $P_i = E_i$ then $|E_i| = |P_i| = p^s$ so $P_i \in \mathrm{Syl}_p(G)$. Thus, $P_i \in \mathrm{Syl}_p(G)$ iff $P_i = E_i$.

Also, if $x \in E_i$, and $g \in P_i = G_{E_i}$, then $xg \in E_i g = E_i$, and therefore $P_i \subseteq E_i$. Hence, E_i is a union of left cosets of P_i. In particular, $|E_i|$ is a multiple of $|P_i|$ (equal to the size of each such coset). Therefore, $|P_i|$ divides $|E_i| = p^s$. In particular, P_i is a p-subgroup of G. Moreover, by the Orbit-Stabilizer theorem,

$$|G| = |G_{E_i}|\left|E_i^G\right| = |P_i||\Delta_i|,$$

so

$$|\Delta_i| = \frac{|G|}{|P_i|} = |G : P_i| = \begin{cases} m & \text{if } P_i \in \mathrm{Syl}_p(G), \text{ or equivalently } P_i = E_i; \\ p^{r_i} m & \text{if } P_i \notin \mathrm{Syl}_p(G), \text{ where } r_i > 0. \end{cases}$$

It follows that

$$\binom{p^s m}{p^s} = |\Omega| = |\Delta_1 \cup \Delta_2 \cup \ldots \cup \Delta_t| = \sum_{i=1}^{t} |\Delta_i| = n_p m + pk,$$

where $k \in \mathbb{Z}$, since the number of Δ_i of size m is equal to the number of Sylow p-subgroups (of which there n_p), and the rest are of size multiple of p. Hence,

$$\binom{p^s m}{p^s} \equiv n_p m \mod p.$$

Now, this equivalence holds for every group G of order $p^s m$. In particular, it holds for the cyclic group of order $p^s m$, which has only one subgroup of each possible order, and hence only one Sylow p-subgroup. Thus,

$$n_p m \equiv \binom{p^s m}{p^s} \equiv m \mod p,$$

and so $(n_p - 1)m \equiv 0 \mod p$. But $p \nmid m$ (by hypothesis) and consequently $n_p - 1 \equiv 0 \mod p$ and rearranging yields $n_p \equiv 1 \mod p$, as desired. □

Corollary 3.7. Cauchy's Theorem. *If G is a group of order divisible by p, then G has at least one element of order p.*

Proof. Let $P \in \mathrm{Syl}_p(G)$, which exists by Sylow's first theorem, and is non-trivial. So take any non-identity element $x \in P$, then the order of x is a power of p (by Lagrange), say p^k where $k \geq 1$. Then $y = x^{p^{k-1}}$ has order p. □

Example 3.8. If G is a group of order 15, then G is cyclic.

Proof. $n_3 \equiv 1 \mod 3$ and $n_3 \mid 15$, so $n_3 \in \{1, 3, 5, 15\}$, yet clearly $3, 5, 15$ do not satisfy this so $n_3 = 1$, and similarly holds for $n_5 = 1$. Hence, G has 1 element of order 1, 2 elements of order 3, 4 elements of order 5, and rest 8 elements have order 15 (so G is cyclic). □

Proposition 3.9. *If G is a group of order pq where p, q are primes such that $p < q$, then G has a normal subgroup of order q. Hence, G is not simple.*

Proof. $n_q \mid pq$, so $n_q = 1, p, q$ or pq. But $n_q \equiv 1 \mod q$, so $n_q \neq p, q, pq$ (not equal to p since $p < q$). Therefore, $n_q = 1$. Hence, there exists only one Sylow q-subgroup and this must be normal in G (or every conjugate of a Sylow q-subgroup is a Sylow q-subgroup and equal to Q). □

Proposition 3.10. *If G is a group of order p^2q where p and q are distinct primes, then G cannot be simple.*

Note. Burnside's $p^\alpha q^\beta$ theorem says even when $\alpha \geq 1$ and $\beta \geq 1$, the result holds.

Proof. First, $n_p \equiv 1 \mod p$ and $n_p \mid q$, therefore $n_p = 1$ or 1. Assume $n_p = q$ (then $q > p$), and note if $n_p = 1$, then G has a normal subgroup of order p^2 (implying G is not simple). Hence, G has q subgroups of order p^2.

Next, $n_q \equiv 1 \mod q$ and $n_q \mid p^2$ implies $n_q = 1$, p or p^2. Assume $n_q \neq 1$ (for otherwise we are done). Then $n_q = p$ or p^2, and $n_q \neq p$ since $p \not\equiv 1 \mod q$ (we have $q > p$). Hence, $n_q = p^2$. So, we have p^2 cyclic subgroups of order q. Any two such subgroups have trivial intersection (since q is prime). Therefore, we have $p^2(q-1) = p^2q - p^2$ elements of order q in G. This leaves p^2 other elements in G, and they must lie in a Sylow p-subgroup of order p^2. Hence, $n_p = 1$, a contradiction. □

Proposition 3.11. *If G is a group of order pqr, where p, q, r are distinct primes, then G cannot be simple.*

Proof. Without loss of generality, suppose $p < q < r$. Then $n_r \mid pqr$, so $n_r \in \{1, p, q, r, pq, pr, qr, pqr\}$. But also $n_r \equiv 1 \mod r$, implying $n_r \neq p, q, r, pr, qr, pqr$, so n_r is 1 or pq. Suppose $n_r = pq$, for if $n_r = 1$ the result follows. Hence, there are pq subgroups of order r in G (and also $pq > r$). Any two such subgroups have trivial intersection (since r is prime). Therefore, we have $pq(r-1) = pqr - pq$ elements of order r in G. This leaves pq other elements of G.

Similarly, $n_q \mid pqr$, so $n_q \in \{1, p, q, r, pq, pr, qr, pqr\}$. But also $n_q \equiv 1 \mod q$, implying $n_q \neq p, q, pq, qr, pqr$, so $n_q \in \{1, r, pr\}$. Suppose $n_q = r$, so that G has r subgroups of order q in G. Then $r(q-1) = rq - r$ elements of order q. □

Theorem 3.12. (Frattini Argument). *If K is a normal subgroup of G, and $P \in \mathrm{Syl}_p(K)$, then $G = N_G(P)K$ (where G is finite).*

Proof. First, $K \subseteq G$ and $N_G(P) \subseteq G$, therefore $N_G(P)K \subseteq G$. Conversely, if $g \in G$, consider $Q = g^{-1}Pg$. (Then Q is a Sylow p-subgroup of G). Then $Q \leq g^{-1}Kg = K$ and $|Q| = |P|$ implies $Q \in \mathrm{Syl}_p(K)$. So, by Sylow's second theorem we get $Q = x^{-1}Px$ for some $x \in K$. Hence, $g^{-1}Pg = Q = x^{-1}Px$ implying $xg^{-1}Pgx^{-1} = P$, so $gx^{-1} \in N_G(P)$. Hence, $g = \left(gx^{-1}\right)x \in N_G(P)K$. Thus, $G = N_G(P)K$. □

Theorem 3.13. *If $P \in \mathrm{Syl}_p(G)$, then if $N_G(P) \leq H \leq G$, then H is* self-normalizing *(i.e., $N_G(H) = H$). In particular, we get $N_G(N_G(P)) = N_G(P)$.*

Proof. Suppose $N_G(P) \leq H \leq G$. Then $H \leq N_G(H)$, so we show $N_G(H) \subseteq H$. Let $g \in N_G(H)$, so that $g^{-1}Hg = H$. Then since $P \leq N_G(P) \leq H$, we get that $g^{-1}Pg \leq g^{-1}Hg = H$. Therefore, $g^{-1}Pg$ is a Sylow p-subgroup of H. Therefore, $g^{-1}Pg = x^{-1}Px$ for some $x \in H$ (by Sylow's second theorem). Once again, we get $xg^{-1}Pgx^{-1} = P$ so that $gx^{-1} \in N_G(P)$. Therefore, $gx^{-1} \in H$ and so $g = \left(gx^{-1}\right)x \in H$, and hence $N_G(H) \subseteq H$ implies $N_G(H) = H$. □

4. Finite abelian groups

4.1. Direct Products.

Definition 4.1. *External direct product*;

$$G = M \times N = \{(x, y) \mid x \in M, y \in N\}$$

with component-wise group operation.

Internal direct product; if $M \trianglelefteq G$, $N \trianglelefteq G$ and $G \cong M \times N$.

Direct powers; if M is a group, then $M^r = \overbrace{M \times M \times \ldots \times M}^{r \text{ copies}}$.

Theorem 4.2. *If M and N are normal subgroups of G such that $G = MN$ and $M \cap N = \{1_G\}$, then*

(1) *$[M, N] = \{1_G\}$, i.e. M commutes with N, $\{[x, y] \mid x \in M, y \in N\} = \{1_G\}$;*
(2) *$G \cong M \times N$;*
(3) *$G/M \cong N$ and $G/N \cong M$.*

Proof. If $x \in M$ and $y \in N$ then $[x, y] = x^{-1}y^{-1}xy$, where $x^{-1}, y^{-1}xy \in M$ (since M is normal) and $x^{-1}y^{-1}x, y \in N$ (since N is normal), implying that $[x, y] \in M \cap N = \{1_G\}$ (proving (1)).

Define $\theta : G \to M \times N$ as follows: if $g \in G$, then $g = xy$ for some $x \in M$ and $y \in N$ (since $G = MN$) and we may set $g^\theta = (x, y)$. This is well-defined, since if $xy = g = uv$ (where $x, u \in M$ and $y, v \in N$) then we get $u^{-1}x = vy^{-1}$, where $u^{-1}x \in M$ and $vy^{-1} \in N$. Hence, $u^{-1}x = vy^{-1} \in M \cap N = \{1_G\}$, giving us $u = x$ and $v = y$ (so well-defined).

Next, θ is a homomorphism (easy, since $[M, N] = \{1_G\}$). Also,

$$\ker \theta = \{g \in G \mid g = xy \text{ with } x = 1_M \text{ and } y = 1_N\} = \{1_G\}.$$

Hence, θ is an isomorphism. Moreover,

$$\{(x, 1_N) \mid x \in M\}, \{(1_M, x) \mid x \in N\} \subseteq \text{im}\,(\theta)$$

implying

$$\{(x, y) \mid x \in M, y \in N\} = M \times N$$

and so $G \cong \text{im}\,(\theta) \cong M \times N$ (proving (2)).

Composing θ with the projections $\pi_M : M \times N \to M$ (taking $(x, y) \mapsto x$) and $\pi_N : M \times N \to N$ (taking $(x, y) \mapsto y$) we get homomorphisms $\theta_{\pi_M} : G \to M$ with image M and kernel N, and $\theta_{\pi_N} : G \to N$ with image N and kernel M. Therefore, $G/M \cong N$ and $G/N \cong M$. □

Proposition 4.3. *If A, B and C are normal subgroups of G such that $AB = AC$, then $B = C$.*

Proof. Observe that $AB = AC$ implies $AB = CA$, so that $B \subseteq ABA^{-1} = C$. Similarly, $C \subseteq ACA^{-1} = B$, so $B = C$. □

Theorem 4.4. *If $G \cong M \times N$, then $G' = [G, G] \cong M' \times N'$ and $Z(G) \cong Z(M) \times Z(N)$.*

Proof. Let $\theta : G \to M \times N$ be an isomorphism. Restricting θ to $Z(G)$ obviously preserves commutativity. Similarly, one restricts θ to G'. □

Theorem 4.5. *If $n = m_1 m_2 \ldots m_k$ where the m_i are positive integers, then $C_n \cong C_{m_1} \times C_{m_2} \times \ldots \times C_{m_k}$ iff the m_i are pairwise coprime.*

Note. For example, $C_2 \times C_3 \times C_6$, but $C_5 \times C_5$ is not cyclic since every element has order 1 or 5.

Proof. $C_n \cong C_{m_1} \times C_{m_2} \times \ldots \times C_{m_k}$ iff the RHS has an element of order $n = m_1 m_2 \ldots m_k$. But if x_i has order r_i (in C_{m_i}) for $1 \leq i \leq k$, then $(x_1, x_2, \ldots, x_k) \in C_{m_1} \times C_{m_2} \times \ldots \times C_{m_k}$ has order $\text{LCM}(r_1, \ldots, r_k)$. Therefore, has order n iff $\text{LCM}(r_1, \ldots, r_k) = n$. Hence, $C_{m_1} \times C_{m_2} \times \ldots \times C_{m_k}$ is cyclic (of order n) iff $\text{LCM}(m_1, \ldots, m_k) = n$ iff the m_i are pairwise coprime. □

Theorem 4.6. (The Chinese Remainder Theorem). *If $m_1, m_2, \ldots, m_k$ are pairwise coprime positive integers, then for any integers $r_1, r_2, \ldots, r_k$ (where $0 \leq r_i < m_i$ for all i), there exists an integer s such that $s \equiv r_i \mod m_i$ (for all $1 \leq i \leq k$), i.e., any set of remainders (modulo the m_i) is achievable.*

Note. For example, $m_1 = 6$, $m_2 = 5$, $r_1 = 3$ and $r_2 = 1$ has $s = 21$.

Proof. Let $n = m_1 m_2 \ldots m_k$ (which is equal to the lowest common multiple of the m_i). Define $\theta : \mathbb{Z}_n \to \mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_k}$ by letting $\theta : v \mapsto (\overline{v_1}, \ldots, \overline{v_k})$ where $\overline{v_i}$ is the remainder of v up to dividing m_i. This is a homomorphism with trivial kernel, since

$$\ker \theta = \{v \in \mathbb{Z}_n \mid v \equiv 0 \mod m_i \ \forall i\} = \{v \in \mathbb{Z}_n \mid v \equiv 0 \mod n\} = \{0\}.$$

So, θ is one-to-one. Therefore, $n = |\mathbb{Z}_n| = |\mathrm{im}\,(\theta)|$, but

$$|\mathbb{Z}_{m_1} \oplus \ldots \oplus \mathbb{Z}_{m_k}| = m_1 \ldots m_k = n.$$

Hence, θ is onto, implying any $(r_1, \ldots, r_k)$ is achievable. □

Theorem 4.7. *If the finite group G has exactly one Sylow p-subgroup for every $p \mid |G|$, then G is the (internal) direct product of its Sylow p-subgroup.*

Proof. Observe

- Every Sylow-subgroup is normal in G (because it is unique for the corresponding prime p, using Sylow's second theorem);
- Any two Sylow subgroups have trivial intersection (because for $P \in \mathrm{Syl}_p\,(G)$ and $Q \in \mathrm{Syl}_q(G)$ we get $P \cap Q$ is a p-subgroup and a q-subgroup for primes p and q, that is, $|P \cap Q|$ is a power of p and power of q, implying it equals 1.

Thus, $G \cong$ direct product of its Sylow subgroups (and any group with this property is called *Nilpotent*). □

For example, finite abelian groups are nilpotent.

4.2. **Abelian groups.**

Definition 4.8. The *exponent* of a finite group (not necessarily Abelian) is the lowest common multiple of the order of its elements.

Example 4.9.
- $\exp\,(C_n) = n$;
- $\exp\,(S_3) = 6$;
- $\exp\,(S_n)$ is the lowest common multiple of the divisors of $n!$ for $n \geq 3$.

Theorem 4.10. *Let G be a finite Abelian group.*

(1) *If $\exp\,(G) = m$, then G has an element of order m.*
(2) *If $|G| = mn$ where m and n are coprime, then $G \cong M \times N$ where $M = \{x \in G \mid x^m = 1\}$ and $N = \{x \in G \mid x^n = 1\}$.*
(3) *G is nilpotent.*

Proof. Write $m = m_1 m_2 \ldots m_k$ as the prime powers factorisation of m. As m is the LCM of the orders of elements of G, there exists $x_i \in G$ with $o(x_i) = m_i$ for each $1 \leq i \leq k$. Now, $x = x_1 x_2 \ldots x_k$ has order $m_1 m_2 \ldots m_k = m$, since any two x_i commute and two m_i are pairwise coprime (proving (1)).

Define M and N as given. Then $M \leq G$ (using the fact G is Abelian). Moreover, M is normal in G (since G is Abelian). Similarly, $N \lhd G$. Also, M and N intersect trivially, since the order of any element of $M \cap N$ divides $\gcd\,(m, n) = 1$. Finally, we claim $G = MN$. Let $x \in G$. Then $o(x)$ divides $|G| = mn$ by Lagrange, and so

$o(x^m)$ divides n and $o(x^n)$ divides m. Also, $\gcd(m,n)=1$. Therefore, $1=am+bn$ by Bezout's Theorem, implying

$$x = x^1 = x^{am+bn} = x^{bn}x^{am} = (x^n)^b(x^m)^a \in MN,$$

so $G \subseteq MN$, where $x^m \in N$ and $x^n \in M$. Therefore, $G \cong M \times N$. □

Theorem 4.11. *Let G be a finite Abelian group of prime-power order $q = p^k$ (where p is prime) and exponent m, and let x be an element of G of order m. Then $G \cong \langle x \rangle \times K$, for some $K \leq G$.*

Proof. Since G is Abelian, every subgroup is normal. Since G has exponent m and prime-power order p^k, it follows m divides p^k by Lagrange. Hence, $m = p^s$ for some $0 < s \leq k$ (i.e., $\langle x \rangle$ is a cyclic p subgroup of G). Consider

$$K = \left\{ g \in G \;\middle|\; g^{p^{k-s}} = 1 \right\}.$$

Clearly K contains the identity, so K is non-empty. Also, if $g, h \in K$, then since G is Abelian, it follows that $gh^{-1} \in K$ (i.e., K is a subgroup of G).

Then $g \in K \cap \langle x \rangle$ implies $g = x^i$ for some i such that $\left(x^i\right)^{p^{k-s}} = 1$. Clearly g has order at most p^s, and is a power of p. □

Corollary 4.12. *Every finite Abelian group of prime-power order is (isomorphic to) to a direct product of cyclic groups.*

Proof. □

Lemma 4.13. *Let G be a finite Abelian group of prime-power order. If $G \cong H_1 \times H_2 \times \ldots \times H_r$ and $G \cong K_1 \times K_2 \times \ldots \times K_s$, where each H_i and each K_j is a cyclic subgroup of G, and also $|H_1| \geq |H_2| \geq \ldots \geq |H_r|$ and $|K_1| \geq |K_2| \geq \ldots \geq |K_s|$, then $r = s$ and $H_i \cong K_i$ for all i.*

Proof. □

Theorem 4.14. (Fundamental Theorem of Finite Abelian Groups). *Every finite Abelian group is expressible as a direct product/sum of cyclic groups of prime power order (also, this product/sum is unique up to rearrangement of the cyclic subgroup).*

Proof. □

Corollary 4.15. *Finite Abelian groups are* converse Lagrange *groups, i.e., there exists a subgroup of every possible order dividing the order of the group.*

Note. For example, $C_8 \times C_9 \times C_{125}$ has order $8 \times 9 \times 125$, and want a subgroup of $2 \times 9 \times 5$, simply take $C_2 \times C_9 \times C_5$.

A_5 has no subgroup of orders 5, 12 or 30.

5. Presentations

Example 5.1. We have

$$\langle x \mid x^6 = 1 \rangle$$

is the *largest* group generated by an element x such that $x^6 = 1$. There are four such groups: C_1, C_2, C_3, and C_6, and since C_6 is largest, $C_6 \cong \langle x \mid x^6 = 1 \rangle$. Observe C_1, C_2, C_3 are all quotients of C_6. Note that $C_1 = \langle x \mid x = 1 \rangle$, $C_2 = \langle x \mid x^2 = 1 \rangle$ and $C_3 = \langle x \mid x^3 = 1 \rangle$.

As a second example, $G = \langle x, y \mid x^2 = y^3 = 1 \rangle$ has C_1, C_2, C_3, C_6 as quotients, but also S_3 and A_4 as a quotients (for S_3 take $(1,2)$ and $(1,2,3)$, for A_4 take $(1,2)(3,4), (1,2,3)$. Also, A_n and S_n for all $n \geq 9$. Note that G is infinite and isomorphic to $\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm I\}$.

A group presentation is of the form $\langle X \mid R\rangle$ where members of X are generators and R are relations the generators must satisfy. A free group is a group with "no relations" (other than consequences of the group axioms). That is, we use notation $\langle X \mid \varnothing\rangle$.

5.1. **Free Groups.** Let X be a set, and consider it as a set of symbols (for example $X = \{x, y\}$ or $\{a, b, c\}$ etc.), which we call an *alphabet*. Also let X^{-1} denote the set of symbols of the form x^{-1} for $x \in X$. We define a *word* on $X \cup X^{-1}$ as an expression of the form $x_1^{\epsilon_1} \dots x_k^{\epsilon_k}$ where $x_1, \dots, x_k \in X$ and each $\epsilon_i \in \{\pm 1\}$ (note we let x^1 denote x for any $x \in X$). We say this word has *length* k.

For example, if $X = \{a, b, c\}$, we have these words (among others):

- empty word, length 0, sometimes denoted by 1;
- $a, b, c, a^{-1}, b^{-1}, c^{-1}$ words of length 1;
- $aa, ab, ac, aa^{-1}, ab^{-1}, ac^{-1}, ba, \dots$ words of length 2 (of which there are 36).

Next, we say a word $w = x_1^{\epsilon_1} \dots x_k^{\epsilon_k}$ is *reduced* if

$$\left(x_i^{\epsilon_i}, x_{i+1}^{\epsilon_{i+1}}\right) \neq \left(x_i^{\epsilon_i}, x_i^{-\epsilon_i}\right)$$

for all i. That is, if it is not the case that $x_i = x_{i+1}$ and $\epsilon_i = -\epsilon_{i+1}$ for some i.

For example, $ab^{-1}c$ is reduced, but $aa^{-1}cabac^{-1}c$ is not.

Lemma 5.2. *Any word can be reduced to a (unique) reduced word by eliminating subwords of the form $x_i^{\epsilon_i} x_{i+1}^{\epsilon_{i+1}}$ with $x_i = x_{i+1}$ and $\epsilon_i = -\epsilon_{i+1}$.*

Proof. By equivalence relation that says whether two words can be transferred to each other by reduction or its reverse. □

Given an alphabet X, the *free group* $F(X)$ is the group consisting of all reduced words on $X \cup X^{-1}$, and the following operation: if u, v are reduced words on $X \cup X^{-1}$ then uv is the reduced form of uv.

For example, $\left(ab^{-1}c\right)\left(c^{-1}bab\right) = ab^{-1}cc^{-1}bab = aab$.

Is this a group? Yes:

- Non-empty set, since $1 \in F(X)$;
- Binary operation, well-defined by uniqueness of reduction;
- Has identity element 1 (empty word);
- Associative (in assignment 2);
- Inverses: $(x_1^{\epsilon_1} \dots x_k^{\epsilon_k})^{-1} = x_k^{-\epsilon_k} \dots x_1^{-\epsilon_1}$.

Note: there are no relations in this group except the ones obtained by the reduction. Some notation:

- The rank of $F(X)$ is $|X|$ (typically rank in group theory is the number of generators);
- If $|X| = n$, then $F(x)$ can be denoted by F_n, i.e., F_n is the free group on $\{x_1, \dots, x_n\}$.

Define $F_n = F(X) = F(x_1, x_2, \dots, x_n)$ when $X = \{x_1, x_2, \dots, x_n\}$. Then $F_1 = F\left(1, x, x^{-1}, \dots\right) = \langle X\rangle$ is infinite cyclic.

$F_2 = F(x, y) = \left\{1, x, x^{-1}, y, y^{-1}, xy, \dots\right\}$. This is also infinite, but not cyclic, not even Abelian as $xy \neq yx$.

$F_3 = F(x, y, z)$ contains $F(x, y)$ which contains $F(x)$ and $F(y)$. But also F_3 is isomorphic to a subgroup of F_2 (which is isomorphic to a subgroup of F_3) but not equal.

Question: which elements of $F(X)$ have finite order? For example, $F_1 \cong (\mathbb{Z}, +)$ has only one element of finite order namely 0 under addition. Then if $X \neq \varnothing$, then the only *torsion* element of $F(X)$ is the identity element (i.e., element of finite order).

Proof. Let g be an element of finite order in $F(X)$. Suppose $g \neq 1$. If we can write $g = b^{-1}ab$ where a and b are reduced words, then $bgb^{-1} = a$ and will also have finite order. So, wlog $b = 1$. But then $a^n = aa\dots a$ with no reductions possible, where RHS is reduced and LHS is 1. Therefore, 1 iff $n = 0$ in which case $o(a) = 1$. Therefore, a is $1_{F(X)}$, so g is $1_{F(X)}$. We say $F(X)$ is "torsion free" (meaning that it contains no non-trivial element of finite order). □

Definition 5.3. If B is a set of elements in $F(X)$ such that $\langle B\rangle = F(X)$ and the only reduced word in $B \cup B^{-1}$ that is equal to $1_{F(X)}$ is the empty word, then we call B a *free basis* for $F(X)$. In other words, the elements of B satisfy no non-trivial relations, then B is a free basis for $F(X)$, and vice versa.

Example 5.4. $\{x\}$ and $\{x^{-1}\}$ are the only free basis for $F(x)$. Note $\langle x^i\rangle \neq F(x)$ when $|i| \neq 1$. And also, $\langle x^2, x^3\rangle = F(x)$, but also $(x^2)^3(x^3)^{-2}$ is a reduced word on $\{x^2, x^3\}$ giving us the identity element of $F(x)$ (so not free basis).

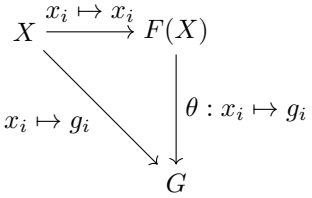
$\{x, x^{-1}yx\}$ is a free basis for $F(x, y)$ since $y = x(x^{-1}yx)x^{-1}$, and also taking $u = x$, $v = x^{-1}yx$ we have

$$u^{k_1}v^{\ell_1}\dots u^{k_r}v^{\ell_r} = x^{k_1-1}y^{\ell_1}x^{k_2}\dots x^{k_r}y^{\ell_r}x \neq 1.$$

Theorem 5.5. (The Universal Property of Free Groups). *Let $X = (x_i)_{i\in I}$ be any alphabet indexed by a set I. Then for any group G, finite or infinite, if $(g_i)_{i\in I}$ is a family of elements of G indexed by the same set I, then there exists a unique homomorphism $\theta : F(X) \to G$ with the property that $\theta : x_i \to y_i$ for all $i \in I$.*

Proof. Obvious, just define θ as follows: if $w = x_{i_1}^{\epsilon_1}\dots x_{i_k}^{\epsilon_k}$ where $i_j \in I$ and $\epsilon_j \in \{\pm 1\}$, then $\theta : w \mapsto g_{i_1}^{\epsilon_1}\dots g_{i_k}^{\epsilon_k}$. □

We have that the diagram commutes:



Theorem 5.6. *$F(X) \cong F(Y)$ iff $|X| = |Y|$.*

Proof. Let $X = (x_i)_{i\in I}$ and $Y = (y_j)_{j\in J}$.

($\Longleftarrow$) If $|X| = |Y|$, then we may assume w.l.o.g. that $I = J$. Hence, define $\theta : F(X) \to F(Y)$ given by $x_{i_1}^{\epsilon_1}\dots x_{i_k}^{\epsilon_k}$ mapping to $y_{i_1}^{\epsilon_1}\dots y_{i_k}^{\epsilon_k}$. This is an isomorphism.

($\Longrightarrow$) (Finite) Suppose $|X| = m$ and $|Y| = n$. Then, by the Universal Property, with say $G = \overbrace{C_2 \times C_2 \times \dots \times C_2}^{m}$, if $g = (g_1, g_2, \dots, g_m)$ is any element of G, then there exists a unique homomorphism from $F(X) \to G$ taking $(x_1, x_2, \dots, x_m) \mapsto (g_1, g_2, \dots, g_n)$. Note there are 2^m choices for g, therefore there are 2^m such homomorphism. Similarly, there are 2^n such homomorphisms from $F(Y)$ to $\overbrace{C_2 \times C_2 \times \dots \times C_2}^{n}$, but none onto $(C_2)^{m+1}$. If $m < n$, then $F(Y)$ will have some such G that is not a homomorphic image of $F(X)$, since every homomorphic image of $F(X)$ has rank $\leq m$. With some homomorphic image of $F(Y)$ have rank $n > m$. For $F(X) \cong F(Y)$ via ρ (assume $m < n$) then ρ^θ is a homomorphism from $F(X)$ onto $(C_2)^n$. Every homomorphic image of $F(X)$ is generated by the images of the x_i, therefore has rank $\leq m$, while $F(Y)$ has smallest generating set of size m (where $n > m$).

(Infinite) Let's assume cardinals are linearly ordered and WLOG suppose $|X| < |Y|$. Now, define G as the group of all "Y-tuples" $(a_y)_{y\in Y}$ where $a_y = \pm 1$ for all $y \in Y$, under component-wise multiplication. Then $|G| = 2^{|Y|} > 2^{|X|}$ and G has rank $|Y|$. By a standard argument, using "basis" tuples $e_z = (a_y)_{y\in Y}$ with $a_y = -1$ if $y = z$ and $a_y = 1$ otherwise. Then G is a quotient of $F(Y)$ but not of $F(X)$. Therefore, $F(X) \ncong F(Y)$. □

Corollary 5.7. *Every group is a quotient (factor group) of some free group.*

Proof. Let $(g_i)_{i\in I}$ be a generating set given group G and apply the Universal Property of Free Groups, noting that θ is surjective (since $(g_i)_{i\in I}$ generates G). For example, we can take $I = G$, and then $(g_i)_{i\in I}$ is just the family of every member of G. Or instead take $I = G \setminus \{1_G\}$, so get every non-trivial element. □

Corollary 5.8. *If G is a free group, and B is any free basis for G then $G \cong F(B)$.*

Proof. Suppose $G = F(X)$, where $X = (x_i)_{i\in I}$. Then $B = (b_i)_{i\in I}$ and by the Universal Property of Free Groups, there exists homomorphisms $\theta : G \to \langle G\rangle$ taking g_i to b_i for all $i \in I$. Conversely, $\langle B\rangle$ is free on B, therefore $\langle B\rangle \cong F(B)$ and there exists a homomorphism $\phi : \langle B\rangle \to G$ taking b_i to g_i for all $i \in I$. Clearly θ and ϕ are natural inverses, therefore θ is an isomorphism and so $G \cong \langle B\rangle = F(B)$. □

5.2. **Group Presentations.** Let $X = (x_i)_{i\in I}$ be an alphabet, and let R be a set of words called *relators* on X. The notation $\langle X \mid R\rangle$ is going to mean the "largest" group G that can be generated by a set $(g_i)_{i\in I}$ such that when each occurrence of any element $x_i \in X$ in any word $r \in R$ is replaced by $g_i \in G$ then we can get the identity element G (will formally define soon).

Example 5.9. $G = \langle x \mid x^n\rangle$. G could be any cyclic group where generator g satisfies the relation $g^n = 1$. Therefore, G could be the cyclic group of order k for some k dividing n. But we want the largest one, therefore $G = C_n$.

$G = \langle x, y \mid x^k, y^m, [x, y]\rangle$. So G is generated by a pair of commuting elements x and y of orders dividing k and m. So G has largest such group, therefore $G \cong C_k \times C_m \cong \mathbb{Z}_k \oplus \mathbb{Z}_m$. Note if $k = 2$ and $m = 6$ then also $C_1, C_2, C_3, C_6 \cong C_2 \times C_3, C_2 \times C_2$ possibilities, but all smaller than $C_2 \times C_6$.

Note. If $G = \langle X \mid R\rangle = \langle R\rangle^{F(X)}$ then there exists homomorphism θ from $F(X)$ to G taking x_i to g_i for all $i \in I$. Question: What is the kernel of θ? If $K = \ker\theta$, then $F(X)/K \cong \operatorname{im}(\theta) = G$ by the First Isomorphism Theorem. Therefore, $G \cong F(X)/K$. This gives a way of defining $G = \langle X \mid R\rangle$. How? Clearly K contains R because $\theta : r \mapsto 1_G$ for all $r \in R$. Since $G = \langle X \mid R\rangle$ is to be the largest group generated by a set of elements satisfying all $r \in R$, it follows that K is the smallest normal subgroup of $F(X)$ containing R. Called the "normal closure" of R in $F(X)$.

Definition 5.10. If S is a subset of a group G, then the *normal closure* of S in G is the smallest normal subgroup of G containing S (therefore equals the intersection of all normal subgroups of G that contains S). We denote this normal closure by $\langle S\rangle^G$.

For example, let $G = C_{24} = \langle c\rangle$. Normal closure of $\{c^4, c^6\} = \langle c^2\rangle$ since $c^2 = c^6(c^4)^{-1}$.

Theorem 5.11. *Every group G has a presentation.*

Proof. Let G be any group.

(1) Let $(g_i)_{i\in I}$ (or just $(g)_{g\in G}$) be an indexed set consisting of the elements of G. Let $X = (x_i)_{i\in I}$ be a corresponding alphabet, and define $R = \{x_i x_j x_k^{-1} \mid g_i g_j = g_k \text{ in } G\}$.

Then there exists $\theta : F(X) \to G$ taking $x_i \mapsto g_i$ for all $i \in I$. Clearly, $R \subseteq \ker\theta$ and so $\langle R\rangle^{F(X)} \leq \ker\theta$, and its not hard to see that any word in $F(X)$ that gets taken to 1_G under θ can be expressed as a product of elements of the form given by the definition of K. In fact, R determines the multiplication table for G.

(2) We know that G is a quotient of some free group, say $F(X)$, and so $G \cong F(X)/K$ for some normal subgroup K of $F(X)$. So take $R = K$ and then since $K \trianglelefteq F(X)$ we know that $K = \langle K\rangle^{F(X)} = \langle R\rangle^{F(X)}$. Therefore, $G \cong F(X)/\langle R\rangle^{F(X)} = \langle X \mid R\rangle$. □

Example 5.12. We have already seen cyclic groups. We provide some other examples.

(1) Dihedral groups D_n is symmetry group of regular n-gon with n rotations and n reflections such that $|D_n| = 2n$. We claim that

$$D_n \cong \left\langle x, y \mid x^2, y^n, (xy)^n \right\rangle$$

via $x = (1,2)(3,n)(4,n-1)\ldots$ and $y = (1,2,3,\ldots,n)$. For example, $n = 5$ we get $x = (1,2)(3,5)(4)$ and for $n = 6$ we get $x = (1,2)(3,6)(4,5)$. So, $xy = (1,3)(2)(4,n)\ldots$.

Proof of claim: First, it's easy to see that D_n is a quotient of the group $G = \left\langle x, y \mid x^2, y^n, (xy)^2 \right\rangle$ because it contains elements satisfying the relations (with x as a reflection of order 2 and y as a rotation of order n). Also, these elements generate D_n since there exists n powers of y $\left(1, y, y^2, \ldots, y^{n-1}\right)$ and n elements $\left(x, xy, xy^2, \ldots, xy^{n-1}\right)$, and no xy^i lies in $\langle y\rangle$ for otherwise $x \in \langle y\rangle$ which is impossible. Thus, $|G| \geq |D_n| = 2n$.

On the other hand, consider elements of G itself. We see that G contains powers of y, namely $1, y, y^2, \ldots, y^{n-1}$ with $y^n = 1$, even if we don't yet know these elements are distinct. Similarly G contains $x, xy, xy^2, \ldots, xy^{n-1}$ even if we don't yet know that these are distinct.

Claim: Every element of G lies in one of these two lists. Why? $(xy)^2 = 1$ in G, therefore $xyx = y^{-1}$ and so $yx = x^{-1}y^{-1} = xy^{-1}$. Now take any element w of G we can we can write w as $x^{\alpha_1}y^{\beta_1}\ldots x^{\alpha_k}y^{\alpha_k}$ where $\alpha_i \in \{0,1\}$ and $\beta_i \in \{0,\ldots,n-1\}$ (since $x^2 = 1 = y^n$). In fact we can suppose $1 = \alpha_2 = \alpha_3 = \ldots = \alpha_k$, since otherwise cancel, and similarly that $\beta \in \{1,2,\ldots,n-1\}$ for $i = 1,2,\ldots,k-1$. Thus, $w = x^{\alpha_1}y^{\beta_1}xy^{\beta_2}x\ldots xy^{\beta_{k-1}}xy^{\beta_k}$. But $y^\beta x = y^{\beta-1}yx = y^{\beta-1}xy^{-1} = xy^{-\beta}$ for all $\beta \geq 1$. By induction therefore we can write w as x^uy^v for some $u, v \in \mathbb{Z}$ and then replace u by 0 or 1 and v by $0,\ldots,n-1$ respectively. Hence, $|G|$ is at most $2n$ implying $|G| \leq 2n$, so $|G| = 2n = |D_n|$. Thus, $G \cong D_n$.

(2) $G = \left\langle x, y \mid x^4, y^4, x^2y^2, y^{-1}xyx \right\rangle$. Then same kind of argument in (1) shows that every element of the two group can be written as x^uy^v where $u, v \in \{0,1,2,3\}$ (since $y^{-1}xyx = 1$ therefore $yx = x^{-1}y$). So has order at most 16. Also, $x^2 = \left(y^2\right)^{-1} = y^{-2} = y^2$, therefore we can reduce further say that $u \in \{0,1\}$ and $v \in \{0,1,2,3\}$. For example, $x^3y^v = xx^2y^v = xy^{v\pm 2 \mod 4}$ and $x^2y^v = y^2y^v = y^{v+2 \mod 4}$, so $|G| \leq 2 \times 4 = 8$. What quotients does G have? C_1, C_2, $C_2 \times C_2$ all work, C_4 does not.

"Rabbit out of a hat" Define $Q \leq S_8$ by letting $a = (1,2,3,4)(5,6,7,8)$ and b such that $b^{-1}ab = (5,8,7,6)(3,2,1,4) = a^{-1}$, so $b^{-1}aba = 1$. Can be checked Q is a quotient of G since a^4, b^4, a^2b^2 is trivial. But also $|Q| \geq 8$ since $|Q|$ is divisible by $o(b) = 4$ but $a \notin \langle b\rangle$ and so $|Q| \geq 2 \times 4 = 8$. Therefore, $|G| = 8 = |Q|$, so $G \cong Q$ where Q is Q_8 called the quaternion group of order 8.

These two examples are typical of an approach that often works to figure out which group is known group determined by a given presentation:

(1) Use the presentation $G = \langle X \mid R\rangle$ to work out properties of G, and get a bound of the form $|G| \leq m$.
(2) Find a known group of order m that is a quotient of G.

Next time, use "coset enumeration" on

$$\left\langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \right\rangle$$

and

$$\left\langle x, y \mid x^2 = y^3 = (xy)^4 = 1 \right\rangle.$$

Example 5.13. Let $G = \left\langle x, y \mid x^2, y^3, (xy)^3 \right\rangle$, and $H = \langle y\rangle$ in G and consider cosets of H in G. First, $Hy = H = Hy^{-1}$ since $y \in H$. Also, $x^2 = 1$ so we'll consider multiplication of right cosets Hg by $x = x^{-1}$, y and y^{-1}. Next, $(Hx)x = Hx^2 = H1 = H$ and $(Hxy)y = Hxy^2 = Hxy^{-1}$. Also, $\left(Hxy^{-1}\right)y^{-1} = Hxy^{-2} = Hxy$.

We have not yet used $(xy)^3 = 1$. Observe that

$$Hxyx = Hxyxyxyy^{-1}x^{-1}y^{-1} = H(xy)^3y^{-1}xy^{-1} = Hxy^{-1}$$

since $(xy)^3 = 1$ and $y^{-1} \in H$. We now have the coset table:

	x	y	y^{-1}
$H : 1$	2	1	1
$Hx : 2$	1	3	4
$Hxy : 3$	4	4	2
$Hxy^{-1} : 4$	3	2	3

Can get $Hxyx = Hxy^{-1}$ another way:

.	x	.	y	.	x	.	y	.	x	.	y	.
1	.	2	.	3	.	?	4	2	.	1	.	1

Gives $3x = 4$, i.e., $Hxyx = Hxy^{-1}$.

So now have all cosets. Finally, as we know G acts transitively on the right coset space $(G : H)$, it follows that $|G : H| = |(G : H)| \leq 4$. If we multiply any of the four cosets we get one of the four cosets. Thus, $|G| = |G : H||H| \leq 4 \times 3 = 12$. Next, A_4 is a quotient of this group. The coset table now gives permutations $x = (1, 2)(3, 4)$, $y = (1)(2, 3, 4)$ and these generate A_4 of order 12. Hence, $|G| \geq |A_4| = 12$ and so $|G| = 12$ implying $G \cong A_4$.

Note. Exercises: Read examples 5.3.3 on Q_8, 5.3.9 on S_8, 5.3.10 on $F(2, 5) \cong C_5$ (a Fibonacci group), 5.3.11 on group order 16.

A group is *finitely generated* if $G = \langle S\rangle$ for some finite subset $S \subseteq G$. A group G is *finitely presented* if $G \cong \langle X \mid R\rangle$ for some finite set X and some finite set R of words on X. Note: Every finite group is finitely generated $G = \langle G\rangle$ and finitely presented $G = \langle G \mid$ "multiplication table"$\rangle$.

Theorem 5.14. (Von Dyck's Theorem). *If $G = \langle X \mid R\rangle$ and $K = \langle S\rangle^{F(X)}$ for some $S \subseteq F(X)$, then $G/K \cong \langle X \mid R \cup S\rangle$.*

Proof. Let $L = \langle R\rangle^{F(X)}$ and let $M = \langle R \cup S\rangle^{F(X)}$. Then $K \leq M$ and $L \leq M$, and all of M, K, L are normal in $F(X)$. So,

$$\langle X \mid R \cup S\rangle \cong F(X)/\langle R \cup S\rangle^{F(X)} = F(X)/M \cong (F(X)/L)/(M/L) = \left(F(X)/\langle R\rangle^{F(X)}\right)/(M/L) = G/K,$$

since $K \cong M/L$ (exercise). See also Theorem 5.3.7 in coursebook. □

Example: $C_{12} = \langle x \mid x^{12} \rangle$, $C_4 = \langle x \mid x^4 \rangle$ and $C_{12}/\langle C_{x^4} \rangle \cong C_4$.

Theorem 5.15. *If G is any group generated by two elements of order 2, then G is dihedral (two sided).*

Proof. Suppose G is generated by $\langle a, b \rangle$ where $a^2 = b^2 = 1$, and suppose $o(ab) = n$. Let $c = ab$. Then

$$a^{-1}ca = a^{-1}aba = ba = b^{-1}a^{-1} = (ab)^{-1} = c.$$

Therefore, $G = \langle a, c \rangle$ with $a^2 = c^n = 1$ and $a^{-1}ca = c^{-1}$.

Conversely, if $x^2 = y^n = 1$ and $x^{-1}yx = y^{-1}$, then $\langle x, y \rangle$ is also generated by x and xy where $(xy)^2 = xyxy = x^{-1}yxy = y^{-1}y = 1$, therefore generated by 2 elements of order 2. Thus, $D_n \cong \langle x, y \mid x^2, y^n, xyxy \rangle \cong \langle a, b \mid a^2, b^2, (ab)^n \rangle$. □

More exercises:

(1) Show that if p is prime, then every group of order $2p$ is either cyclic (C_{2p}) or dihedral (D_p). Hint: the group has a cyclic normal subgroup N of order p; two cases, $p = 2$ and p odd.
(2) Show that if p and q are primes with $p < q$ then every group of order pq is either cyclic or generated by two elements x and y such that $x^p = y^q = 1$ and $x^{-1}yx = y^k$ for some k. In this case, $N = \langle y \rangle$ is normal in the group G with $N \cong C_q$ and $G/N \cong C_p$.

5.3. **The Modular Group.** Note that $\langle X \mid R \rangle$ with $|X| > |R|$ is infinite, whereas if $|X| < |R|$ it is not necessarily finite since $\left\langle x, y \mid x^2, y^3, (xy)^7, [x, y]^9 \right\rangle$ is infinite.

Note. $PSL(2, \mathbb{Z})$ is *highly* infinite - it is "residually infinite" and it is "SQ-universal" i.e., every countable group occurs as a subgroup of some quotient of $PSL(2, \mathbb{Z})$.

We will show $\langle x, y \mid x^2, y^3 \rangle \cong PSL(2, \mathbb{Z}) = SL(2, \mathbb{Z})/Z(SL(2, \mathbb{Z})) = SL(2, \mathbb{Z})/\{pm1\}$ starting with $SL(2, \mathbb{Z})$. In $SL(2, \mathbb{Z})$, the elements $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are called *transvections* (generally a transvection in $SL(n, \mathbb{R})$ is a matrix of the form $I_n + E_{ij}$ where E_{ij} is the (i, j)th elementary matrix with 1 in (i, j)th entry and zeroes everwhere else). Observe $L^2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, and by induction $L^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$ for all $k \in \mathbb{Z}$, since $L^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Similarly, $U^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ for all $k \in \mathbb{Z}$.

Proposition 5.16. *$SL(2, \mathbb{Z})$ is generated by $X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $Y = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.*

Proof. First note that $X^2 = -I_2$ and $Y^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$, so $Y^3 = -I_2$. Therefore, $X^4 = Y^6 = I_2$, and $X^2 = Y^3 = -I_2$. Also, $YX = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = L$ and $Y^2X = YL = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = U$.

Next, [Defn] for any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$, let $N(A) = |c|$ (*norm* of A). We claim every $A \in SL(2, \mathbb{Z})$ can be written as a word in the alphabet $\{X, Y\}$, i.e., $SL(2, \mathbb{Z}) = \langle X, Y \rangle$ (since $X, Y \in SL(2, \mathbb{Z})$). This will then prove the proposition. So, proof of claim: By induction on $N(A)$. If $N(A) = 0$, then $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with

$1 = \det(A) = ad$, so $a = d = \pm 1$. Either $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = U^b = \left(Y^2X\right)^b$ or $a = d = -1$ so

$$A = \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = -U^{-b} = -\left(Y^2X\right)^{-b} = X^2\left(Y^2X\right)^{-b}.$$

Now, (inductive step), suppose $N(A) = |c| > 0$. Trick: Divide a by c to get $a = qc + r$ for some $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ with $0 \leq r < |c|$. Then

$$\left(Y^2X\right)^{-q} A = U^{-q}A = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a - qc & b - qd \\ c & d \end{pmatrix}.$$

Therefore,

$$X\left(Y^2X\right)^{-q} A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a - qc & b - qd \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ q - qc & b - qd \end{pmatrix} =: B$$

with $N(B) = |a - qd| = |r| < |c|$. Therefore, by induction $B \in \langle X, Y \rangle$ and so $A = \left(Y^2X\right)^q X^{-1} B \in \langle X, Y \rangle$. Thus, $SL(2, \mathbb{Z})$ generated by just two elements. □

Corollary 5.17. *$SL(2, \mathbb{Z})$ is generated by L and U.*

Proof. We know $YX = L$ and $Y^2X = U$. Therefore,

$$Y = \left(Y^2X\right)(YX)^{-1} = UL^{-1}$$

and

$$X = Y^{-1}L = \left(UL^{-1}\right)^{-1} = LU^{-1}L.$$

Therefore, $\langle L, U \rangle = \langle X, Y \rangle = SL(2, \mathbb{Z})$. □

In fact, $SL(2, \mathbb{Z})$ is generated by its transvections, for all $n \geq 2$. What about presentations?

Theorem 5.18. *$SL(2, \mathbb{Z}) \cong \langle x, y \mid x^2 = y^3, x^4 = 1 \rangle =: F$ (which is isomorphic to $\langle x, y \mid x^4 = y^6 = 1, x^2 = y^3 \rangle$).*

Proof. For this, we define the set

$$T = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \;\middle|\; a \geq 1, b \geq 0, c \geq 0, d \geq 1, b + c \geq 1 \right\}.$$

Easy to see T is closed under multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

with $ab' + bd' \geq b' + b$ and $ca' + dc' \geq c + c'$, so follows it is in T. We know that X and Y satisfy $X^2 = Y^3 = -I_2$ and $X^4 = I_2$, therefore $SL(2, \mathbb{Z})$ is a quotient of F. Indeed, there exists a homomorphism $\theta : F \to SL(2, \mathbb{Z})$ taking $x \mapsto X$ and $y \mapsto Y$. Let K be the kernel of θ. We'll show K is trivial by assuming the contrary, i.e., assuming that some non-trivial element g of F is taken by θ to I_2. Since $x^2 = y^3 = z$, for some z, z is central (commutes with x and y) we can write g as $x^\alpha w$ where $\alpha \in \{0, 1\}$ and w is a word on $\left\{x, y, y^2\right\}$. Conjugating if necessary, we can suppose $g = x^r (yx)^{s_1} \left(y^2x\right)^{t_1} \dots (yx)^{s_m} \left(y^2x\right)^{t_m}$ where $r = 0, 1, 2$ or 3, each $s_i \geq 0$ and each $t_i \geq 0$. Applying θ, $X^{-r} = (YX)^{s_1} \left(Y^2X\right)^{t_1} \dots (YX)^{s_m} \left(Y^2X\right)^{t_m}$ since $g^\theta = I_2$. But $YX = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in T$ and $Y^2X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Therefore, RHS lies in T, so $X^{-r} \in T$. But $X^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \notin T$, $X^{-2} = X^2 = -I_2 \notin T$, $X^{-3} = X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \notin T$, a contradiction, unless $m = 0$. But in this case,

$g = x^r \mapsto X^r$, so $r = 0$ and hence $g = x^0 = 1$. Hence, $\ker\theta$ is trivial and we have an isomorphism. □

Corollary 5.19. $\langle x, y \mid x^2, y^3\rangle \cong SL(2,\mathbb{Z})/\{\pm I_2\} = PSL(2,\mathbb{Z})$.

Proof. Apply Von Dyck's Theorem with $PSL(2,\mathbb{Z}) \cong \langle x, y \mid x^2y^{-3}, x^4\rangle/\langle x^2\rangle$ which is isomorphic to $\langle x, y \mid x^2y^{-3}, x^4, x^2\rangle \cong \langle x, y \mid x^2, y^3\rangle$. □

Corollary 5.20. *$SL(2,\mathbb{Z}) \cong C_2 * C_3$, which is the* free product *of $\langle x\rangle \cong C_2$ and $\langle y\rangle \cong C_3$ (i.e., no other relations except ones from C_2 and C_3).*

5.4. **Residual finiteness.** Given a group "property" P (such as being finite, or being Abelian, being a p-group etc.), we say G is *residually P* if it has the property for every non-trivial element $x \in G$, there exists a normal subgroup $N \lhd G$ such that

(1) $x \notin G$, and
(2) G/N has property P.

G is residually-finite iff there exists a finite index normal subgroup $N \lhd G$ such that $x \notin N$ (so that the image of x in G/N is non-trivial) i.e. iff G has a finite quotient in which the image of x is non-trivial.

Aside: A group is *virtually P* if it has a subgroup H of finite index such that H has property P (e.g., virtually abelian means there exists an abelian subgroup of finite index). Maths joke: Finite groups are virtually trivial.

Theorem 5.21. *Every free group is residually finite.*

Proof. Trivial for free groups of rank 0 ($F_0 = \{1\}$ vacuously holds) and rank 1 ($F_1 \cong (\mathbb{Z}, +)$, if $n \in \mathbb{Z}$, then for any $m > n$, the subgroup $m\mathbb{Z}$ is normal in $\mathbb{Z}$ and does not contain n, since n is not multiple of m). Hence, we may suppose $F = F(X)$ with $|X| > 1$.

We'll prove that F is residually finite by showing that if x is a reduced word on X of length $n \geq 2$, then there exists a homomorphism $\theta : F \to S_{n+1}$ such that x^θ is non-trivial and therefore $x \notin \ker\theta$ (where $K = \ker\theta$ of finite index dividing $(n+1)!$ by using first isomorphism theorem since $|F/K| = |\mathrm{im}\,(\theta)|$ which divides $|S_{n+1}| = (n+1)!$).

Suppose $x = x_{\lambda_1}^{\epsilon_1} \dots x_{\lambda_n}^{\epsilon_n}$, where each $x_{\lambda_i} \in X$ and $\epsilon_i = \pm 1$ for $1 \leq i \leq n$. For any λ in $\{\lambda_1, \dots, \lambda_n\}$, say $\lambda = \lambda_i$, choose a permutation σ_λ in S_{n+1} such that $j^{\sigma_\lambda} = j+1$ if $(\lambda_j, \epsilon_j) = (\lambda_i, 1) = (\lambda, 1)$ and $(j+1)^{\sigma_\lambda} = j$ if $(\lambda_j, \epsilon_j) = (\lambda_i, -1) = (\lambda, -1)$. Now, let $\sigma_x = \sigma_{\lambda_1} \dots \sigma_{\lambda_n}$ when $x = x_{\lambda_1}^{\epsilon_1} \dots x_{\lambda_n}^{\epsilon_n}$. Then

$$1 \overset{\sigma_{\lambda_1}}{\mapsto} 2 \mapsto \dots \overset{\sigma_{\lambda_n}}{\mapsto} n+1,$$

true whether $\epsilon_i = \pm 1$. Thus, $\sigma_x : 1 \mapsto n+1$. Therefore, σ_x is a non-trivial permutation. Finally, define $\theta : F(X) \to S_{n+1}$ by letting $\theta : x \mapsto \sigma_x$. Then θ is a homomorphism, and $x \notin \ker\theta$. □

Corollary 5.22. *In any free group $F(X)$, the intersection of all subgroups of finite index is trivial.*

Proof. Let J be the intersection of all subgroups of finite index in $F(X)$ and suppose $g \in J$. If $g \neq 1_{F(X)}$, then there exists $N \lhd F(X)$ such that $|F(X) : N|$ is finite and $g \notin N$, since $F(X)$ is residually finite. But now by definition of J, we know that $J \leq N$ (since N normal subgroup finite index). Therefore, $g \in J \leq N$, so $g \in N$, a contradiction, so $g = 1_{F(X)}$. Then, $J = \{1_{F(X)}\}$. □

6. Abelian Groups

6.1. **Free abelian groups.** G, Abelian: $x_1, \ldots, x_r$ elements of G. Then

$$\sum_{i=1}^{r} m_i x_i, \quad m_i \in \mathbb{Z}.$$

Basis for G: generating set X for G such that any two finite sequence of elements of X the only way to express 0 as linear combination is to take all $m_i = 0$. If Abelian group has a basis, we say free Abelian.

Example 6.1. $\mathbb{Z}^n = \oplus_{i=1}^n \mathbb{Z}$, $x \in \mathbb{Z}^n$ where $x = (a_1, \ldots, a_n)$ each $a_i \in \mathbb{Z}$. Basis for $\mathbb{Z}^n$ is $e_1 = (1, 0, \ldots, 0)$, ..., $e_n = (0, \ldots, 0, 1)$. Then $\{e_1, \ldots, e_n\}$ is basis for $\mathbb{Z}^n$.

Theorem 6.2. *Every finitely generated free Abelian group G is isomorphic to $\mathbb{Z}^n$ for some n.*

Proof. $\{x_1, \ldots, x_n\}$ basis for G. Define map $\varphi : \mathbb{Z}^n \to G$ mapping $(m_1, \ldots, m_n) \mapsto \sum_{i=1}^r m_i x_i$. Claim φ is an isomorphism. □

Definition 6.3. The *rank* of a free Abelian group is the cardinality of its basis (and note that it is an invariant).

Lemma 6.4. *$H \leq \mathbb{Z}^n$. H has generating set of cardinality at most n.*

Proof. Induction. Let $N = \langle e_1 \rangle \lhd \mathbb{Z}^n$. Define $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n/N$ as canonical homomorphism. Observe $\mathbb{Z}^n/N \cong \mathbb{Z}^{n-1}$. Consider $\varphi(H) \leq \mathbb{Z}^{n-1}$. By inductive hypothesis, $\varphi(H)$ has generating set at most $n-1$. Suppose $y_1, \ldots, y_{n-1}$. Take x_i such that $\varphi(x_i) = y_i$ for $1 \leq i \leq m$, $H = \langle x_1, \ldots, x_m, x_{m+1} \rangle$, of $N \cap H$. □

Representing subgroups of $\mathbb{Z}^n$. $H \leq \mathbb{Z}^n$ implies H has say $m \leq n$ generators. Represent H as $m \times n$ matrix A whose rows generate H. Define $S(A)$ as the set of all integral linear combinations of rows of A. These are the vectors uA where u ranges over $\mathbb{Z}^n$.

Task: decide membership in H. To do this, use row operations.

Definition 6.5. Two matrices over $\mathbb{Z}$ are *row equivalent* (RE) if one can be transformed from on to the other via integral row operations: interchanging rows, multiply row by -1, add integral multiple of one row to the second.

Lemma 6.6. *A row equivalent to B implies $S(A) = S(B)$ implies H remains fixed.*

Proof. B is obtained from A via row operations, so rows of B contained inside of $S(A)$, and therefore $S(B) \subseteq S(A)$. Similarly, $S(A) \subseteq S(B)$ and so $S(A) = S(B)$. □

Definition 6.7. $A \in M_{m \times n}(\mathbb{Z})$ is in (row) *Hermite form* if

1. first r rows of A are non-zero;
2. for $1 \leq i \leq r$ let j_i be index of first non-zero entry row i. Then require $j_1 < j_2 < \ldots < j_r$.
3. $A_{i,j_i} > 0$ for $1 \leq i \leq r$.
4. $1 \leq k < i \leq r$, $A_{k,j_i} < A_{i,j_i}$.

Theorem 6.8. *B $m \times n$ integral matrix. There exists unique matrix A in Hermite form which is row-equivalent to B.*

Example 6.9. For example,

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

take $v = (6, 0, 16, 6, 4, 13, 31)$ and $v \in S(A)$. Does there exist a, b, c, d such that such that $uA = v$? Take $u = (a, b, c, d) \in \mathbb{Z}^4$. Compute entries of uA corresponding to that of A without pivot entries: $2a = 6$, $a + 3b = 0$, $2b + 4c = 6$, $a + c + 2d = 13$ implies (a, b, c, d) equals $(3, -1, 2, 4)$.

Example 6.10. $G = \mathbb{Z}^4 = \langle g_1, g_2, g_3, g_4 \rangle$. $H = \langle g_1 + 2g_3 + g_4, 3g_1 + g_2 + 2g_3 - g_4, -2g_1 + g_2 + 4g_4 \rangle$. Then

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 3 & 1 & 2 & -1 \\ -2 & 1 & 0 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 4^6 & \\ 0 & 0 & 8 & 10 \end{pmatrix} = Bv = 7g_1 + 6g_3 - 3g_4.$$

So, $v = (7, 0, 6, -3)$. Does there exist u such that $uB = v$, $u = (a, b, c)$? $(7, 0, -1)B = v$ so $v \in H$.

$G = \langle g_1, \ldots, g_n \rangle$ Abelian written additively. $f : \mathbb{Z}^n \to G$ where $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i g_i$ is a homomorphism. By first isomorphism theorem, $G \cong \mathbb{Z}^n / H$, where $H = \ker f$.

Note. G free Abelian group with basis X. H any Abelian group. Every map from X to H has unique extension to a homomorphism from G to H. If the image of X generates H then the homomorphism is onto, and H isomorphic to quotient of G.

Every finitely generated Abelian group is a quotient of a free group. $H \leq \mathbb{Z}^n$ implies H is finitely generated. Represent H by matrix A such that $H = S(A)$.

Example 6.11. $f : \mathbb{Z}^5 \to \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}^2$ where $(a, b, c, d, e) \mapsto ([a]_2, [b]_4, [c]_{12}, d, e)$, and $H = \ker f$ is all vectors (a, b, c, d, e) where $2 \mid a$, $4 \mid b$, $12 \mid c$ and $d = e = 0$. So, $H = S(A)$ and $\mathbb{Z}^5 / H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}^2$, where $A = \begin{pmatrix} 2 & & & & \\ & 4 & & & \\ & & 12 & 0 & 0 \end{pmatrix}$. This is an example of Smith-Normal form.

Definition 6.12. Two $m \times n$ matrices A and B are equivalent over $\mathbb{Z}$ if one can be obtained from the other by row and column operations. Equivalently, there exists $P \in \mathrm{GL}(m, \mathbb{Z})$ and $Q \in \mathrm{GL}(n, \mathbb{Z})$ such that $A = PBQ$.

Lemma 6.13. *If A and B are row/column equivalent, then $\mathbb{Z}^n / S(A) \cong \mathbb{Z}^n / S(B)$.*

Note. Column operations correspond to automorphisms of $\mathbb{Z}^n$.

Definition 6.14. A is in *smith normal form* if for some $k \geq 0$ the entries $d_i = A_{ii}$ for $1 \leq i \leq k$ are positive and $d_i \mid d_{i+1}$ for $1 \leq i \leq k$ and all other entries zero, so

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

Lemma 6.15. *If A is an $n \times n$ matrix in smith-normal form and $s = n - k$, then $\mathbb{Z}^n / S(A) \cong \mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^s$.*

Theorem 6.16. (Basis Theorem). *Given finitely generated Abelian group G, there exists $k, n \geq 0$ and $d_i \geq 2$ for $1 \leq i \leq k$ and $d_i \mid d_{i+1}$ for $1 \leq i \leq k$ such that $G = \mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^s$ where $s = n - k$. The k, n and d_i are determined by G.*

Corollary 6.17. *G finitely Abelian group, $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ where $n_1, \ldots, n_r > 1$ and $n_i \mid n_{i+1}$ for $1 \leq i \leq r - 1$.*

For example, $G = C_4 \times C_4 \times C_4 \times C_3 \times C_9 \cong C_4 \times C_{12} \times C_{36}$.

Lemma 6.18. *G group, $G' \lhd G$. $H = G/G'$ is abelian. $N \lhd G$, G/N Abelian if and only if $N \geq G'$.*

G/G' is largest Abelian quotient of G. Question: $G = \langle X \mid R \rangle$, what is $G/G' =: G_{ab}$? Structure of G_{ab}?

Remark: $G = \langle X \mid R \rangle$ and $C = \{[x_i, x_j] \mid 1 \leq i \leq j \leq r\}$, where $|X| = r$.

Lemma 6.19. *$G' = C$.*

Proof. Suffices to prove G' coincides with normal closure $\overline{C}$ of C in G. Since generators of $G_{ab} = \langle X \mid R, C \rangle = G/\overline{C}$ all commute, G_{ab} is abelian, so $G' \subseteq \overline{C}$. But $G' \lhd G$. Since $\overline{C}$ is smallest normal subgroup of G containing C, implies $G' \geq \overline{C}$ and so $G' = C$. □

$G \to G_{ab}/S(A)$, A goes to smith normal form of A . Read off $G_{ab} = G/G'$.

For example, $G = \left\langle x, y \mid \left(xy^3x^{-2}\right)^2, y^{-1}x^2y^2 \right\rangle$. $G/G' = \langle x, y \mid \ldots, \ldots, [x, y] = 1 \rangle$, so $G/G' = \langle x, y \mid -2x + 6y, 2x + y \rangle$.

Also, $H = \langle (-2, 6), (2, 1) \rangle \leq \mathbb{Z}^2$ and $B = \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix}$. $A = \begin{pmatrix} -2 & 6 \\ 2 & 1 \end{pmatrix}$, $S(A) = H$.

Now, $\mathbb{Z}^2/H \cong \mathbb{Z}^2/S(A) \cong \mathbb{Z}^2/S(B)$. $P = \begin{pmatrix} -2 & 1 \\ -5 & 2 \end{pmatrix}$ and $Q = \begin{pmatrix} 2 & -11 \\ 1 & -6 \end{pmatrix}$ both in $\mathrm{GL}(2, \mathbb{Z})$ gives us $PAQ = B$.

Example 6.20. $G = \left\langle x, y, z \mid \left(xyz^{-1}\right)^2, \left(x^{-1}y^2z\right)^2, \left(xy^{-2}z^{-1}\right)^2 \right\rangle$. $A = \begin{pmatrix} 2 & 2 & -2 \\ -2 & 4 & 2 \\ 2 & -4 & -2 \end{pmatrix}$ goes to diagonal entries $2, 6, 0$. So, $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}$, so infinite group.

Definition 6.21. The *deficiency* of $G = \langle X \mid R \rangle$ is $\mathrm{Def}(G) = |X| - |R|$, not invariant since consider $\langle x \mid x^2 \rangle = \langle x \mid x^2, x^4 \rangle$.

Lemma 6.22. *If $G = \langle X \mid R \rangle$ where X, R finite and G finite then $|X| \leq |R|$.*

Proof. If $|X| > |R|$, then can show certain rows in smith normal form are zero, implying G/G' is infinite and so G is infinite (a contradiction). □

7. Normal structure

A *subnormal series* of a group G is a finite series of subgroups

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

where $G_i \lhd G_{i-1}$ for all $1 \leq i \leq r$.

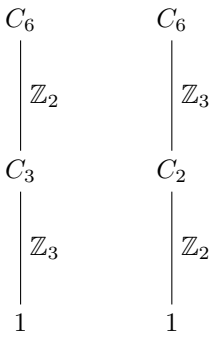
For example, $S_3 \rhd A_3 \rhd 1$. Also, $S_4 \rhd V = \langle (12)(34), (13)(24) \rangle$, $V \rhd U = \langle (12)(34) \rangle$ and $U \rhd 1$.

Given

$$\begin{aligned} G = G_0 &\rhd \ldots \rhd G_r = 1 \\ = H_0 &\rhd \ldots \rhd H_s = 1, \end{aligned}$$

we say the *subnormal series are isomorphic* if there exists one-to-one correspondence between sets of non-trivial factor groups G_{i-1}/G_i and H_{j-1}/H_j such that the corresponding factors are isomorphic groups.

For example, taking $G = C_6$, consider the following.



Lemma 7.1. (Butterfly Lemma). *Let $A, B \leq G$, $X \lhd A$ and $Y \lhd B$. Then*

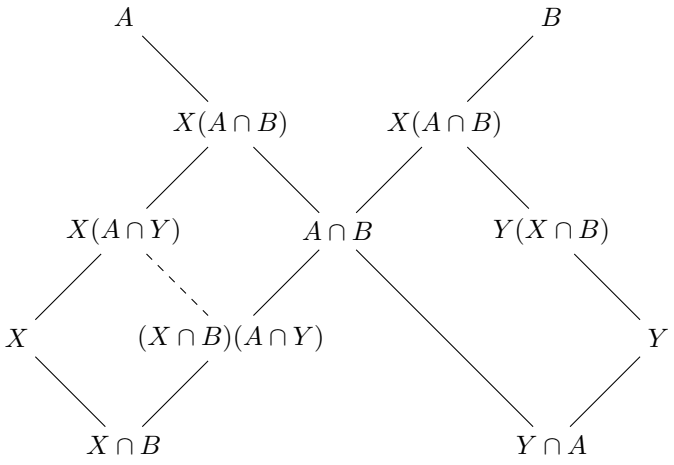
(1) $X(A \cap Y) \lhd X(A \cap B)$;
(2) $Y(X \cap B) \lhd Y(A \cap B)$;
(3) $\frac{X(A\cap B)}{X(A\cap Y)} \cong \frac{Y(A\cap B)}{Y(X\cap B)}$.

Proof. Since $A \cap B \leq A$ and $X \lhd A$, follows $X(A \cap B) \leq A$. Similarly, $A \cap Y \leq A$ and $X \lhd A$, so $X(A \cap Y) \leq A$. It follows that $X(A \cap Y) = (A \cap Y)X$. Since $X(A \cap Y) \subseteq X(A \cap B)$, follows $X(A \cap Y) \leq X(A \cap B)$. Moreover, $A \cap B \leq B$ and $Y \lhd B$ implies $A \cap Y \lhd A \cap B$. Now, this means elements of $A \cap B$ commute with $A \cap Y$ and X, and X absorbs elements from itself; it is easy to check (1) holds ((2) similar).

Now, we show $\frac{X(A\cap B)}{X(A\cap Y)} \cong \frac{A\cap B}{(A\cap Y)(X\cap B)}$. Since $A \cap B \leq A$ and $X \lhd A$, it follows $X(A \cap B) \leq A$. Moreover, $X \lhd X(A \cap B)$, so by the second isomorphism theorem it follows that $\frac{X(A\cap B)}{X} \cong \frac{A\cap B}{X\cap B}$. By the third isomorphism theorem,

$$\frac{H}{N_1N_2} \cong \frac{H/N_2}{N_1N_2/N_2}$$

for $N_1, N_2 \lhd H$, $H = A \cap B$, $N_1 = A \cap Y$, $N_2 = X \cap B$. Hence, $\frac{A\cap B}{(X\cap B)(A\cap Y)}$ is isomorphic to a quotient of $\frac{A\cap B}{X\cap B} \cong \frac{X(A\cap B)}{X}$. Therefore, there exists $\varphi : \frac{X(A\cap B)}{X} \to \frac{A\cap B}{(X\cap B)(A\cap Y)}$. Claim: $\ker\varphi = \frac{X(A\cap Y)}{X}$. Hence, by first isomorphism theorem, $\frac{X(A\cap B)}{X(A\cap Y)} \cong \frac{A\cap B}{(X\cap B)(A\cap Y)}$. Now, repeat with Y and B and deduce second half (proving (3)). □



Theorem 7.2. (Schreier). *Any two subnormal series of G have isomorphic refinements.*

Proof. Let

$$\begin{aligned} G &= G_0 \rhd \ldots \rhd G_r = 1 \\ &= H_0 \rhd \ldots \rhd H_s = 1. \end{aligned}$$

Construct refinement of the first by inserting between G_{i-1} and G_i for each i the following:

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

By the Butterfly Lemma, $G_i(G_{i-1} \cap H_j) \lhd G_i(G_{i-1} \cap H_{j-1})$, so we obtain refinement of length rs. Carry out similar refinement for the second series by inserting between H_{j-1} and H_j the series

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

so we obtain refinement of length rs. By the Butterfly Lemma,

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

□

Note. Natural next step: refine subnormal series to obtain one which cannot be further refined, which is called a *composition series*.

Theorem 7.3. (Jordan-Holder). *In a group with a composition series, every composition series is isomorphic to the other.*

Proof. Apply the refinement theorem to two composition series. □

Lemma 7.4. *Any composition factor of a group is a simple group.*

Proof. Suppose G_i/G_{i+1} is not simple. Then there exists $N/G_{i+1} \lhd G_i/G_{i+1}$, so there exists $N \lhd G_i$ such that $G_{i+1} \lhd N \lhd G_i$ (contradiction). □

Given finite group G of $\{G_i/G_{i+1} \mid 1 \leq i \leq r\}$ set of composition factors of G (composition series $G = G_0 \rhd \ldots \rhd G_r = 1$).

For example, $\mathbb{Z}_4$ v.s. $\mathbb{Z}_2 \times \mathbb{Z}_2$ and S_3 v.s. $\mathbb{Z}_2 \times \mathbb{Z}_3$ (S_3 non-Abelian and $\mathbb{Z}_2 \times \mathbb{Z}_3$ Abelian).

Lemma 7.5. *A simple abelian group is cyclic of prime order.*

Note. A composition factor of a finite abelian group is cyclic of prime order.

Proof. Take G simple abelian group. Let $x \neq 1 \in G$. Then $\langle x \rangle \lhd G$. Also, $\langle x^2 \rangle \leq \langle x \rangle$. If $x^2 = 1$, then $G = C_2$ else $\langle x^2 \rangle \lhd G$. G simple, so $x \in \langle x^2 \rangle$ implies $x = x^{2n}$ for some n. Therefore, $|x| < \infty$. Let $p \mid |G|$. Apply Cauchy implies there exists $H \leq G$ such that $|H| = p$ and $H \lhd G$ so $|G| = p$ (since G simple). □

Example 7.6. $G = S_4 \rhd A_4 \rhd C_2 \rhd 1$. Composition factors, $(\mathbb{Z}_2)^3$, $(\mathbb{Z}_3)^1$, subnormal $G_{i+1} \lhd G_i$.

Definition 7.7. *Normal series* if $G_i \lhd G$ for all i. Note we will refine normal series to obtain chief series (similar concept to composition factors).

Example 7.8. $G = (\mathbb{Z}, +)$ has no composition series. Suppose G has a composition series $1 = G_r \lhd G_{r-1} \lhd \ldots \lhd G_0 = G$. Then $G_{r-1} = \langle x^s \rangle$ for some $s \in \mathbb{N}$, where G_{r-1} infinite cyclic. Then $1 \neq \langle x^{2s} \rangle < G_{r-1}$, so could extend (contradiction).

8. Soluble groups

Often we define soluble group as one all whose composition factors are abelian (implies cyclic of prime order).

Definition 8.1. A normal series for a group G, $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = 1$ is *abelian* if G_i/G_{i+1} is abelian for $0 \leq i < r$. Note $G_n \lhd G$.

Definition 8.2. A group is *soluble* if it has an abelian normal series. Note all abelian groups are soluble.

Definition 8.3. The *derived series* of G is the descending series of subgroups $G = G^{(0)}$, $G^{(1)}$, ..., $G^{(r)} = 1$ where $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for each $i \geq 0$. Note $G^{(1)} = \left[G^{(0)}, G^{(0)}\right] = [G, G] = G'$.

Example 8.4. $G = S_4$, $G' = A_4$, $V = \langle (14)(23), (12)(34) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, 1 is such a derived series.

Lemma 8.5. *Let G be a group. Then*

(1) *$G^{(i)}$ $\operatorname{char} G$.*
(2) *$G^{(i)}/G^{(i+1)}$ is abelian.*
(3) *Let $1 = G_n \leq G_{n-1} \leq \ldots \leq G_0 = G$ be an abelian (normal) series. Then $G^{(i)} \leq G_i$ for each $i = 0, \ldots, n$.*

Proof. Recall $N \lhd G$, G/N abelian iff $N \geq G'$. For (1), $G^{(1)} = G' \operatorname{char} G$. Proof by induction, $G^{(i)} \lhd G$ and $G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right] = \left(G^{(i)}\right)'$. Hence, $G^{(i)}/G^{(i+1)}$ is abelian. This finishes (1) and (2).

For (3), induction $i = 0$. $G^{(i+1)} = \left(G^{(i)}\right)' \leq G_i' \leq G_{i+1}$ (so derived series is an abelian normal series). □

Example 8.6. $G = S_3 \geq G' = A_3 = \langle (1, 2, 3) \rangle \geq G^{(2)} = 1$.

Theorem 8.7. *The following are equivalent:*

(1) *G is soluble;*
(2) *G has subnormal series where G_i/G_{i+1} is abelian.*
(3) *G has derived series (i.e., exists n such that $G^{(n)} = 1$).*

Proof. ((1) $\Longrightarrow$ (2)). By definition.

((2) $\Longrightarrow$ (3)). G_i/G_{i+1} abelian implies $G_i' \leq G_{i+1}$. Use induction to deduce that $G^{(k+1)} \leq G_{k+1}$. $G^{(k)} \leq G_k$ implies $G^{k+1} \leq \left(G^{(k)}\right)' \leq G_k' \leq G_{k+1}$.

((3) $\Longrightarrow$ (1)). Derived series is abelian normal series. □

Definition 8.8. If $G^{(n)} = 1$ and n is smallest such integer then G has *derived length* n, denoted $dl(G) = n$.

For example, G is abelian implies $dl(G) = 1$.

Corollary 8.9. *G soluble iff exists n s.t. $G^{(n)} = 1$.*

Corollary 8.10. *G soluble. Then $dl(G)$ is minimum length of abelian normal series for G.*

So, G has a composition series and G_i/G_{i+1} is abelian implies cyclic implies G is soluble. G has an abelian normal series implies soluble which is equivalent to G has derived series. Note G soluble implies $G' \lhd G$ (in fact, G' characteristic in G). Yet, $G' \neq G$, since otherwise each of the terms in a proposed 'derived series' would be equal to G (and so would not terminate). If $G = G'$, we say G is *perfect*.

Theorem 8.11. *Subgroups and factor groups of soluble groups are soluble.*

Proof. Suppose $H \leq G$. G is soluble implies $G^{(r)} = 1$ for some r. But $H^{(r)} \leq G^{(r)}$, so $H^{(r)} = 1$, implying H is soluble.

Suppose $N \lhd G$, $\phi : G \to G/N$. Observe $\phi\big(G^{(k)}\big) = (G/N)^{(k)}$. $G^{(r)} = 1$ therefore implies that its image $(G/N)^{(1)} = 1$, so G/N is soluble. □

Theorem 8.12. *Let $G = G_0 \rhd \ldots \rhd G_r = 1$ be a composition series. Then G is soluble iff G_i/G_{i+1} has prime order.*

Proof. ($\Longleftarrow$) Suppose G_i/G_{i+1} has prime order. This implies G_i/G_{i+1} is abelian, and hence $G_i' \leq G_{i+1}$. Hence, $G^{(r)} \leq G_r = 1$, implying G is soluble.

($\Longrightarrow$) Suppose G is soluble. G_i/G_{i+1} is soluble by applying previous theorem twice (first on G_i, then noting $G_{i+1} \lhd G_i$). But they are composition factors and hence simple, so implies they are abelian giving us they are cyclic ($G' \lhd G$). Thus, they have prime order. □

Lemma 8.13. *G/N, N soluble for some $N \lhd G$ implies G is soluble. Moreover, $dl(G/N) = s$ and $dl(N) = t$ implies $dl(G) = s + t$.*

Proof. $G/N = G_0/N \rhd \ldots \rhd G_s/N = 1$ and $N = N_0 \rhd \ldots \rhd N_t = 1$. G_i contains $G_s = N$. $G_i \lhd G_{i-1}$ for $1 \leq i \leq s$. Since $G_i/N \lhd G_{i-1}/N$, by correspondence theorem obtain G_{i-1}/G_i is abelian. By third isomorphism theorem, $\frac{G_{i-1}/N}{G_i/N} \cong G_{i-1}/G_i$ where LHS abelian implies RHS abelian. Take $G = G_0 \rhd G_1 \rhd \ldots \rhd G_{s-1} \rhd N_0 \ldots \rhd N_t = 1$, which is an abelian normal series for G. Hence, G is soluble. □

Note that $N \lhd G$ and G/N both having properties, does not imply in general that G has said property. Take $G = S_3$ and $N = A_3$, one finds A_3 cyclic order 3 and S_3/A_3 cyclic order 2, yet S_3 is not cyclic. So both cyclic/abelian not general true. Also, simple not true either: take $G = \mathbb{Z}_6$ and $N = \mathbb{Z}_2$. Then $G/N = \mathbb{Z}_3$ and N both simple, yet G is not. Good counterexamples are A_5, S_4, A_4, S_3, A_3.

Theorem 8.14. *Direct product of a finite set of soluble groups is soluble.*

Proof. $G = G_1 \times G_2$, both G_1, G_2 soluble. Then G_1 soluble and $G_1 \lhd G$ implies $G/G_1 \cong G_2$ soluble, so G is soluble. □

Note. Infinite direct product of soluble groups not necessarily soluble (find counterexample).

Definition 8.15. A finite abelian p-group is *elementary* if every element of G has order dividing p (for e.g., $(p, p, \ldots, p)$ for $G \cong (\mathbb{Z}_p)^d$ for $d \geq 1$).

Definition 8.16. A *chief series* is a normal series $G = G_0 \lhd \ldots \lhd G_r = 1$ such that each *chief factor* G_i/G_{i+1} is a minimal non-trivial normal subgroup of G/G_{i+1}. This is equivalent to there exists no subgroup $N \lhd G$ with $G_i > N > G_{i+1}$. We write $\{G_i/G_{i+1} \mid 0 \leq i < r\}$ as sequence of chief factors.

Note. Chief series can not be further refined. For example, $A_4 - V - 1$ has $A_4/V \cong \mathbb{Z}_3$ and $V/1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is elementary abelian p-group.

Chief factors need not be simple. Any two chief series have isomorphic refinements.

Lemma 8.17. *Let N be a minimal normal subgroup of a group G, and assume N is finite and soluble. Then N is elementary abelian p-group for some prime p.*

Proof. $N > 1$, N soluble implies $N' < N$. Recall given a group G and $N \lhd G$, $K < N < G$ with $K \mathrm{char} N$ implies $K \lhd G$ (in fact characteristic). Hence, $N' \lhd G$ implies $N' = 1$ implies N is abelian. Let $p \mid |N|$. $A = \{x \mid x^p = 1\}$. Claim: $A \lhd N$, since N abelian. $A \mathrm{char} G$ and $N \lhd G$ implies $A \lhd G$ implies $A = N$. □

Corollary 8.18. *Every chief factor of a finite soluble group is elementary abelian for some prime p.*

Definition 8.19. G is *characteristically simple* if its only characteristic subgroups (i.e., fixed by automorphisms) are 1 and G).

Lemma 8.20. *Every chief factor of G is characteristically simple.*

Proof. Let G_i/G_{i+1} be a chief factor. Suppose K/G_{i+1} characteristic in G_i/G_{i+1}. Therefore, $K/G_{i+1} \lhd G/G_{i+1}$ implies $K \lhd G$ (a contradiction). □

Theorem 8.21. *A finite characteristically simple group G is a direct product of isomorphic simple groups, i.e., $G = G_1 \times \ldots \times G_n$ where $G_i \cong G_j$ finite simple.*

Theorem 8.22. *Let $M < G$ be a maximal proper subgroup, where G is finite soluble. Then $|G : M|$ is a prime power.*

Proof. Let L be maximal among normal subgroups of M. Then $L = \mathrm{Core}_G(M)$. $L \lhd G$ by definition, let K/L be a chief factor of G. Choose K such that K/L minimal normal in G/L. $K > L$, $K \lhd G$ and therefore $K \not\leq M$ implying $KM > M$. Yet M is maximal, so follows $KM = G$. Therefore, $|G : M| = |K : K \cap M|$, where RHS divides $|K : L|$ by second isomorphism theorem which is a prime power, since K/L is a chief factor of a finite soluble group. Thus, $|G : M|$ is a power of a prime. □

The above requires soluble hypothesis. For example, A_5 has 3 conjugacy classes of maximal subgroups: these have indices 5, 6 and 10.

Definition 8.23. G is *supersoluble* if it has a chief series with cyclic factors. Not every soluble group is supersoluble. For example, S_3 is supersoluble, yet A_4 is not supersoluble (one of its chief factors is $\mathbb{Z}_2 \times \mathbb{Z}_2$).

9. Nilpotent groups

G finite: G nilpotent if all of its Sylow p-subgroups are normal. That is, $G = \prod_{p||G|} S_p$.

Definition 9.1. G is *nilpotent* if it has a normal series $G = G_0 \rhd \ldots \rhd G_r = 1$ where $G_i/G_{i+1} \leq Z(G/G_{i+1})$ $0 \leq i \leq r-1$. Such a series is called a *central series*. Observe that this implies the centre of G is non-trivial, by considering $G_{r-1} \cong G_{r-1}/G_r \leq Z(G/G_r) \cong Z(G)$.

For example, G abelian implies G is nilpotent (take $G = G_0 \rhd G_1 = 1$). Also, $D_8 = \langle (1234), (14)(32) \rangle$, $N = Z(D_8) = \langle (13)(24) \rangle$, 1 is an example.

Definition 9.2. The minimum length of a central series of G is its *nilpotency class.*

For example, G abelian has $ncl(G) = 1$, $ncl(D_8) = 2$ and the quaternion group order 8 has $ncl(Q_8) = 2$. Note that nilpotent implies soluble. Yet, soluble does not imply nilpotent. For $Z(S_n) = 1$ for all $n \geq 3$. S_3 is soluble since it has trivial centre, so not nilpotent.

Lemma 9.3. *Let $G = G_0 \rhd \ldots \rhd G_r = 1$ be a normal series ($G_i \lhd G$). It is a central series iff $[G_i, G] \leq G_{i+1}$ for $0 \leq i < r$.*

Proof. $G_i/G_{i+1} \leq Z(G/G_{i+1})$ iff $[yG_{i+1}, xG_{i+1}]$ where $y \in G_i$ and $x \in G$ iff $[y, x]G_{i+1} = G_{i+1}$ iff $[y, x] \in G_{i+1}$ iff $[G_i, G] \leq G_{i+1}$. □

Lemma 9.4. *All subgroup and factor groups of nilpotent groups are nilpotent. Further, G has $ncl = r$ implies subgroups/quotients have $ncl \leq r$.*

Proof. $G = G_0 \rhd \ldots \rhd G_r = 1$ central series. Suppose $S \leq G$. Then take $S = S \cap G = S_0 \geq S_1 \geq \ldots \geq S_r = 1$, $S_i = S \cap G_i$. Is this central? Well, $S_i \lhd S$ since $G_i \lhd G$. Is $[S_{i-1}, S] \leq S_i$? Well, $S_{i-1} \leq G_{i-1}$, $S \leq G$ implies $[S_{i-1}, S] \leq [G_{i-1}, G] \leq G_i$. Also, $[S_{i-1}, S] \leq S$ implies $[S_{i-1}, S] \leq S \cap G_i = S_i$ implies S has central series at length most r.

Suppose G/N factor group of G. Take □

For example, S_n for $n \geq 3$ is not nilpotent. $S_3 \leq S_n$ for $n \geq 3$ and S_3 is not nilpotent. Remark: class of nilpotent groups is not closed under extensions. For example, $A_3 \lhd S_3$ and S_3/A_3 nilpotent, but S_3 is not.

Lemma 9.5. *Direct product of a finite set of nilpotent groups is nilpotent.*

Proof. $H = H_0 \rhd \ldots \rhd H_r = 1$ and $K = K_0 \rhd \ldots \rhd K_s = 1$ central series. If $s < r$ implies we can extend with identity to get both same length. Now, $G = H \times K$ has central series $G_i = H_i \times K_i$ for $0 \leq i < r$. Claim: $G_i = H_i \times K_i$, $[H_i \times K_i, H \times K] = [H_i, H] \times [K_i, K] \leq H_{i+1} \times K_{i+1} = G_{i+1}$ implies G has central series. □

Example 9.6. G_i nilpotent group of class $> i$. $G = \prod_{i \in \mathbb{N}} G_i$ direct product. If G is nilpotent, implies $ncl(G) = c$. But $G_c \subseteq G$ and $ncl(G_c) > c$, contradiction.

Lemma 9.7. *G finite, assume $Z(G/M) > 1$ for every proper normal subgroup M of G. Then G is nilpotent.*

Proof. Define a sequence of subgroups of G; $Z_0 = 1$, $Z_1 = Z(G) \lhd G$, $Z_2 \leq G$ such that $Z_2/Z_1 = Z(G/Z_1)$, and so on. By hypothesis, if $Z_i \leq G$ then $Z_{i+1} > Z_i$. Also, G finite implies $Z_n = G$ for some n. □

Corollary 9.8. *A finite p-group is nilpotent.*

Proof. $Z(P) > 1$ for P finite p-group. □

Recall the Frattini argument; $N \lhd G$ finite, $P \in \mathrm{Syl}_p(N)$ implies $G = N_G(P)N$.

Theorem 9.9. *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.*
(4) *Every Sylow p-subgroup of G is normal.*
(5) *G is isomorphic to product of Slow p-subgroups for $p \mid |G|$.*

Proof. ((1) $\Longrightarrow$ (2)). Let $H < G$. Suppose $G_k \leq H$ and $G_{k-1} \leq H$. Then $[G_{k-1}, G] \leq G_k \leq H$ implies $[G_{k-1}, H] \leq H$ implies G_{k-1} normalises H and $G_{k-1} \neq H$.

((2) $\Longrightarrow$ (3)). Let M be proper maximal subgroup of G, $N_G(M) > M$ implies $N_G(M) = G$ implies $M \lhd G$.

((3) $\Longrightarrow$ (4)). Let $P \in \mathrm{Syl}_p(G)$. If $N_G(P) < G$, choose M maximal in G such that $M \geq N_G(P)$ implies by (3) that $M \lhd G$. Also, $P \in \mathrm{Syl}_p(M)$, and so by Frattini $G = MN_G(P) = M$, a contradiction implying $N_G(P) = G$, and thus $P \lhd G$.

((4) $\Longrightarrow$ (5)). In direct product section.

((5) $\Longrightarrow$ (1)). Direct product implies nilpotent group. □

Note. $M < G$ and $|G : M| = p$ prime implies M maximal proper subgroup of G. But index of maximal subgroups need not be prime. For example, $M = \langle (234), (34) \rangle \cong S_3$ maximal subgroup of S_4 and $|G : M| = 4$. But the Theorem depending stronger result for nilpotent group.

Lemma 9.10. *G nilpotent, M maximal subgroup of G implies $M \lhd G$ and G/M has prime order.*

Proof. M maximal subgroup of G, $N_G(M) > M$ implies $N \lhd G$. Since nilpotent implies soluble, simply take G/M to be composition factor (which then we know has prime order). □

Example 9.11. $\mathbb{Z}_p^\infty \subseteq \mathbb{C}$ where p prime, take $\mathbb{Z}_p^\infty = \left\{ e^{\frac{2\pi i m}{p^m}} \;\middle|\; 0 \leq m < p^n, n \in \mathbb{N} \right\}$ group over complex numbers equal to $\left\{ z \in \mathbb{C} \;\middle|\; z^{p^n} = 1 \right\}$ (all p^n-th roots of unity as n ranges over $\mathbb{N}$). This is the *Prufer* group, countable abelian group. Then $\mathbb{Z}_p^\infty = \langle g_1, g_2, g_3, \ldots \mid g_1^p = 1, g_2^p = g_1, g_3^p = g_2, \ldots \rangle$. Take $H_n \leq \mathbb{Z}_p^\infty$ cyclic subgroup of $\mathbb{Z}_p^\infty$ with p^n elements, those whose orders divide p^n. This is the set of p^n-th roots of unity. Only subgroups $\frac{1}{p} \subset \frac{1}{p^2} \subset \ldots \subset \mathbb{Z}_p^\infty$, no maximal subgroup.

Definition 9.12. G has a *lower central series* if $G = \gamma_1(G) \geq \gamma_2(G) \geq \ldots \geq \gamma_{r+1}(G) = 1$ where $\gamma_{i+1}(G) = [G, \gamma_i(G)]$, and has an *upper central series* $G = Z_r(G) \geq \ldots \geq Z_0(G) = 1$ where $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$. Observe $Z_1 = Z(G)$, and $\gamma_2(G) = G'$.

Theorem 9.13. *Lower and upper central series are central series.*

Proof. Observe $\gamma_2(G) = [G, G] = G'$ char in G. So, γ_i char G by induction. Also, $Z_{r-1} = Z(G)$ char in G, so Z_i char G by induction. $\gamma_{i+1} \geq [\gamma_i, G]$ implies γ is central series. □

Example 9.14. D_8, Q_8; find lower/upper central series. We have that $D_8 = \gamma_1 = G$, $\gamma_2 = G' = \langle (1,3)(2,4) \rangle$, $\gamma_3 = [\gamma_2, G] = 1$, and $D_8 = Z_2$, $Z_1 = Z(D_8)$, $Z_0 = 1$.

Theorem 9.15. *G has a central series $G = G_0 \rhd \ldots \rhd G_r = 1$. Then $G_{r-i} \leq Z_i$ and $G_i \geq \gamma_{i+1}$ for $0 \leq i \leq r$.*

Proof. By induction; base case for $i = r$ is trivial, since $G = G_0 \geq Z_r$. Now, suppose $G_{r-i} \geq Z_i$ for some $0 < i \leq r$. Then $G_{r-i+1} \geq G_{r-i} \geq Z_i \geq Z_{i-1}$, so by induction result follows. For base case $i = 0$, we get $G = G_0 \geq \gamma_1$. So, IH yields $G_i \geq \gamma_{i+1}$ for some $0 \leq i < r$, so $G_{i+1} \geq G_i \geq \gamma_{i+1} \geq \gamma_{i+2}$, so by induction result follows. □

Corollary 9.16. *If a group is nilpotent, then its upper and lower central series have the same length (called nilpotency class of G).*

Proof. Suppose G has central series of length r. This series is of length as long as upper/lower central series. But upper/lower central series are themselves central series, there each is as long as the other, and hence equal in length. □

Example 9.17. $G = Q_8 \times \mathbb{Z}_2 = \left\langle a, b, c \mid a^2 = b^2 = (ab)^2, c^2 = [a, c] = [b, c] = 1 \right\rangle$. Take $\gamma_1 = G$, $\gamma_2 = \left\langle a^2 \right\rangle$, $\gamma_3 = 1$ and $Z_0 = 1$, $Z_1 = \left\langle a^2, c \right\rangle$, $Z_2 = G$.

Note that the derived series and (γ_i) are different - and can have different lengths (derived length can be much smaller).

Lemma 9.18. *Let $1 \neq N \lhd G$ be nilpotent. Then $N \cap Z(G) > 1$.*

Proof. G is nilpotent implies G has upper central series $G = Z_c \geq \ldots \geq Z_0 = 1$. Let $1 \neq N \lhd G$. There exists minimal m such that $N \cap Z_m \neq 1$. Observe $[N \cap Z_m, G] \leq N \cap [Z_m, G] \leq N \cap Z_{m-1} = 1$, implying $N \cap Z_m$ is central and $1 \neq N \cap Z_m \leq N \cap Z(G)$. □

Corollary 9.19. *A minimal normal subgroup of a nilpotent group has prime order.*

Proof. N minimal normal subgroup of G implies $N \leq Z(G)$ implies N is abelian and also simple, so N has prime order. □

Note. Compare: finite soluble groups. Recall Klein V has chief factor $\mathbb{Z}_2 \times \mathbb{Z}_2$.

10. The finite simple groups

Lemma 10.1. *P finite simple p-group implies $|P| = p$ prime.*

Proof. $1 < Z(G) \lhd P$ implies $Z(P) = P$ implies P is abelian. P is simple, so $|P| = p$. □

Lemma 10.2. *G finite p-group. Every composition factor and every chief factor has order p.*

Proof. We know from previous result that every composition factor has prime order, and so clearly has order p. Every chief factor G_i/G_{i+1} is minimal non-trivial normal subgroup of G/G_{i+1}, and G/G_{i+1} is nilpotent since it is a p-group, implying by previous result G_i/G_{i+1} has prime order. □

Lemma 10.3. *P finite p-group. P has a subgroup of index p and every such subgroup is normal.*

Proof. $P > 1$. Choose maximal normal subgroup N of P. There does not exist M such that $N < M \lhd P$. Hence, P/N is simple, and therefore $|P : N| = p$. Given $M < P$, $|P : M| = p$, and $N_P(M) > M$, implying $N_P(M) = P$ and thus $M \lhd P$. □

Lemma 10.4. *Every maximal subgroup of finite p-group P is normal and has index p.*

Proof. H maximal subgroup of P. $N_P(H) > H$, implying $H \lhd P$. Now, also have P/H has no non-trivial proper subgroup by maximality of H, so P/H has prime order. □

Lemma 10.5. *P finite p-group. Let $N < M$ be normal subgroups of P. Then there exists $L \lhd P$ such that $N \leq L \leq M$ and $|L : M| = p$.*

Proof. Canonical homomorphism: $\varphi : P \to P/N$. Let $\overline{P} = P/N$ and $\overline{M} = M/N$. $\overline{M}$ is non-trivial and $\overline{M} \lhd \overline{P}$. Know $\left|Z\left(\overline{P}\right) \cap \overline{M}\right| > 1$, therefore it contains some x of order p. x is central and of order p, therefore $\overline{L} = \langle x \rangle \lhd \overline{P}$. Now, $N \subseteq L$ and $\overline{L} \subseteq \overline{M}$, so $N \subseteq L \subseteq M$. $\overline{L} \lhd \overline{P}$ implies $L \lhd P$, and $|L : N| = p$. □

Corollary 10.6. *P finite p-group of order p^n. For every b such that $0 \leq b \leq n$, exists $L \lhd P$ such that $|L| = p^b$.*

Proof. Induction on b. Trivial for $b = 0$. Assume $b > 0$. By IH, exists $N \lhd P$ s.t. $|N| = p^{b-1}$. Apply above lemma to produce $L \lhd P$ s.t. $|L : N| = p$. Therefore, $|L| = p^b$. □

Corollary 10.7. *G finite. $p^b \mid |G|$, where p prime, implies that there exists $H \leq G$ such that $|H| = p^b$.*

Question: given G and $A, B \leq G$ with property P. When does AB or $\langle A, B \rangle$ have property P?

Lemma 10.8. *$H \lhd G$ if and only if H is a union of conjugacy classes.*

Proof. ($\Longrightarrow$) Observe $H = \bigcup_{x \in H} [x]$, since RHS clearly contains H, and by normality of H equality follows.

($\Longleftarrow$) If $H = \bigcup_{x \in H} [x]$, then $g^{-1}xg \in [x]$ implies $g^{-1}xg \in H$ and normality easily follows. □

Theorem 10.9. *A_5 is non-abelian simple.*

Proof. Non-abelian: take $x = (1,2,3)$ and $y = (12)(34)$, then $xy \neq yx$. A_5 has conjugacy classes [1], $[(1,2)(3,4)]$, $[(1,2,3)]$, $[(1,2,3,4,5)]$, $[(1,3,4,5,2)]$ of sizes 1, 15, 20, 12 and 12, respectively. Thus, we find the only unions of these classes which divide $|A_5| = 60$ is taking union of all classes, and taking only trivial class. Hence, A_5 is simple by Lagrange and previous result. □

Lemma 10.10. *$n \geq 3$. Every element of A_n can be written as a product of 3-cycles.*

Proof. Every element of A_n can be written as a product of 2-cycles, say $h_1 h_2 \dots h_{2s}$. Show product of 2 transpositions is a 3-cycle. $h_i = h_j$ implies $h_i h_j = 1$. h_i and h_j have one point in common, implies $(a,b)(b,c) = (a,c,b)$. h_i and h_j have no point in common, then $(a,b)(c,d) = (a,b,c)(a,d,c)$. □

Lemma 10.11. *If $H \leq G$, then $C_H(x) = C_G(x) \cap H$ for all $x \in G$.*

Lemma 10.12. *The only normal subgroup of A_n that contains a 3-cycle is A_n ($n \geq 3$).*

Proof. Let $N \lhd A_n$. Assume N contains a 3-cycle π. Then $n = 3$ and $n = 4$ are trivial. Assume $n \geq 5$. $N \lhd A_n$ implies N contains conjugacy class of π in A_n. Aim to show that the conjugacy class of π in A_n contains all 3-cycles (implies N contains all 3-cycles and hence $N = A_n$). Since $n \geq 5$, exists odd permutation which centralises π (for example in S_5, $\pi = (1,2,3)$ and $\sigma = (4,5)$ then $\pi\sigma = \sigma\pi$, where $\sigma \in S_5 \setminus A_5$). π has *support* (number elements moved) 3 implies exists 2 points distinct from π and distinct cycles commute. Therefore, $C_{S_n}(\pi) > C_{A_n}(\pi)$, and so $C_{A_n}(\pi) = C_{S_n}(\pi) \cap A_n$. Hence, $A_n < A_n C(S_n)(\pi) \leq S_n$ (since A_n normal in S_n) implying $A_n C_{S_n}(\pi) = S_n$ by maximality of A_n. Consequently, $|C_{S_n}(\pi) : C_{A_n}(\pi)| = |S_n : A_n| = 2$ implies $|A_n : C_{A_n}(\pi)| = |S_n : C_{S_n}(\pi)|$. Therefore, number of conjugates of π in $A_n = S_n$ and so N contains all 3-cycles. Thus, $N = A_n$. □

Note. We ask given group order, what is the number of subgroups? If G has order p^n, then number of subgroups is approximately $O\left(p^{\frac{2n}{27}}\right)$. For orders $2, 2^2, 2^3, \dots, 2^{10}$, they have $1, 2, 5, 14, 51, 267, 2328, 56092, 10414291$ and approximately 50 billion subgroups, respectively.

10.1. **Characteristic subgroups.** Let G be a group and $S \leq G$. $\mathrm{Core}_G(S) = \bigcap_{g \in G} S^g \lhd G$, is the largest normal subgroup of G contains in S. Take G finite and $S \in \mathrm{Syl}_p(G)$. Define $O_p(G) := \mathrm{Core}_G(S) = \bigcap_{g \in G} S^g = \bigcap \mathrm{Syl}_p(G)$.

Proposition 10.13. *If G finite, $S \in \mathrm{Syl}_p(G)$ and $N \lhd G$, then $S \cap N$ is a Sylow p-subgroup of N.*

Proof. Suppose K is a Sylow p-subgroup of N. By Sylow's second theorem, exists $g \in G$ such that $K \leq g^{-1} S g$. Hence, $K \leq g^{-1} S g \cap N$, and by normality of N easy follows that $K \leq g^{-1}(S \cap N)g$ (and so result follows). □

Theorem 10.14. *$O_p(G)$ contains every normal p-subgroup of G. It is the largest normal p-subgroup of G and is characteristic in G.*

Proof. Take p-group $N \lhd G$. Then $S \cap N \in \mathrm{Syl}_p(N)$. But N is a p-group, therefore $N = S \cap N \leq S$. But $N \lhd G$, so $N = N^g \leq S^g$ for all $g \in G$. Therefore, $N \subseteq \bigcap_{g \in G} S^g = O_p(G)$. Therefore, $O_p(G)$ contains every normal p-subgroup of G. □

Note. Uniqueness important for characteristic, since image must have same property.

Definition 10.15. The *Fitting subgroup* of a finite group G is the product of the subgroups $O_p(G)$ where p runs over $\Pi = \{r \mid r \text{ prime and divides order of } G\}$. Define $\mathrm{Fit}(G) := \prod_{p\in\Pi} O_p(G)$. Claim: This is a direct product, since intersection is trivial.

Proposition 10.16. $\mathrm{Fit}(G)$ *is nilpotent. It contains every normal nilpotent subgroup of* G*. It is characteristic in* G*.*

Definition 10.17. G finite group. $\mathrm{Rad}(G)$ is the largest normal soluble subgroup of G.

Proposition 10.18. $\mathrm{Rad}(G)$ *is characteristic in* G*, and contains every normal soluble subgroup of* G*.*

Theorem 10.19. A_n *is simple* $n \geq 5$*.*

Proof. By induction on n. $n = 5$ done by conjugacy classes. Now, $n \geq 6$ and $N \lhd A_n$, we claim N contains element which fixes some $i \in \{1, \ldots, n\}$. Suppose every non-identity element of N has no fixed points. Let $\pi \in N$. Then $\pi : 1 \mapsto a$ where $a \neq 1$. Choose b, c such that $b \mapsto c$ and $b \neq c$. Since $n \geq 6$, exists $d, e \neq 1, a, b, c$. $\rho = (1, a)(b, c, d, e) \in A_n$. Observe $\rho^{-1} = (1, a)(b, e, d, c)$. Since $N \lhd A_n$, $\rho\pi\rho^{-1} \in N$ and $\rho\pi\rho^{-1}(a) = 1$ and $\rho\pi\rho^{-1}(c) = d$. So, $\rho\pi\rho^{-1}\pi(1) = 1$ and $\rho\pi\rho^{-1}\pi(b) = d$, implying $\rho\pi\rho^{-1}\pi$ is a non-identity element fixing 1 (a contradiction). So, claim follows and hence exists element of N which fixes integer i.

Now, let A_i be the subgroup of A_n which fixes i, implying $A_i \cong A_{n-1}$ and $A_i \leq A_n$. Therefore, $N_i = N \cap A_i \lhd A_i$ is simple by IH, implying $N = 1$ or A_i. But N contains non-identity element which fixes i, so $N_i \neq 1$ implying $N_i = A_i$. Therefore, $A_i \leq N \lhd A_n$. Since $A_i \cong A_{n-1}$, A_i contains a 3-cycle, so N contains a 3-cycle, and therefore N contains all 3-cycles. Thus, $N = A_n$. □

Corollary 10.20. *The only normal subgroups of* S_n *are* 1*,* A_n*,* S_n *for* $n \geq 5$*.*

Proof. Let $N \lhd S_n$ implying $N \cap A_n \lhd A_n$ and therefore $N \cap A_n = A_n$ or $N \cap A_n = 1$. If $N \cap A_n = A_n$, then $A_n N = S_n$ or $A_n N = A_n$. If $N \cap A_n = 1$, then $|N| \leq |S_n : A_n| = 2$. Either $|N| = 2$ or $|N| = 1$. If $|N| = 2$, implies N is a minimal normal subgroup of S_n and $N \leq Z(S_n)$. But $Z(S_n) = 1$, so $N = 1$. □

Lemma 10.21. $K \lhd G$ *and* $|K| = 2$ *implies* $K \leq Z(G)$*.*

Proof. If $K = \langle k \rangle$, then $k^g = k$ for all $g \in G$, so $k \in Z(G)$. □

Corollary 10.22. S_n *is insoluble for* $n \geq 5$*.*

Proof. Composition series is $S_n \rhd A_n \rhd 1$, where $S_n/A_n \cong \mathbb{Z}_2$ and $A_n/1 \cong A_n$, and since A_n non-abelian we are done. Alternatively, assume S_n soluble which implies A_n soluble. But A_n is perfect (i.e., $[A_n, A_n] = A_n$), so no derived series implies A_n insoluble. □

Corollary 10.23. *Only subgroups of* S_n *of index* $< n$ *is* A_n*.*

Note. A_5 is the smallest non-abelian simple group.

Theorem 10.24. (Burnside) $|G| = p^a q^b$ *where* p, q *primes and* $a, b \in \mathbb{N}$ *implies* G *is soluble.*

Theorem 10.25. (Classification; Aschbacher, Gorenstein, Solomon). G *is finite simple, then either*

(1) G *is cyclic of prime order.*
(2) $G \cong A_n$ *for* $n \geq 5$*.*
(3) G *is one of* 16 *families of groups.*

(4) *G is one of* 26 *sporadic groups.*

Note. For (3), $G = \mathrm{SL}(n, F_q)$ $n \geq 2$ and F_q finite field size q. Also, $Z(G)$ has size $\gcd(n, q-1)$ and $G/Z(G) = \mathrm{PSL}(n, q)$ (except for $n = 2$ and $q = 2$ since $\mathrm{GL}(2,2) \cong S_3 \cong D_3 \cong \mathrm{SL}(2,2) \cong \mathrm{PSL}(2,2)$; $n = 2$ and $q = 3$ is also an exception, as it is group of order 12 and soluble). Also get $E_8(q)$, where for $q = 2$ get 248×248 matrices.

The Sporadic groups (by Mathieu) has $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ and others, where M_{11} has order 7920 (orders increasing). We have $\mathbb{B}$ and $\mathbb{M}$ as groups, where $\mathbb{M}$ is called *the monster*, and consists of approximately 10^{53} elements of 196482×196482 matrices over GF(2).

Theorem 10.26. (Odd Order Theorem; Feit and Thompson (1963)). *G non-abelian simple implies $|G|$ is even.*

Does composition factors of G have property?

11. Group constructions

11.1. **Semidirect products.** G is a *semi-direct product* if there exists $N, H < G$ such that

(1) $N \lhd G$
(2) $NH = G$
(3) $N \cap H = 1$

and we say H is *complement to N in G*. We write $G = N \rtimes H$. This also means *G is a SDP of N by H*, *G splits over N* and *G is a split extension of N by H*.

Example 11.1. $S_3 = \langle a, b \mid a^3, b^2, a^b = a^{-1} \rangle$. Then $S_3 \rtimes \mathbb{Z}_2 = \langle a \rangle \rtimes \langle b \rangle$. Also have $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.

For $D_{2n} = \mathbb{Z}_n \rtimes \mathbb{Z}_2 = \langle a, b \mid a^n, b^2, a^b = a^{-1} \rangle = \langle a \rangle \rtimes \langle b \rangle$.

Q_8 is not semi-direct product (quaternion group of order 8). Observe $Q_8 \neq$ (group of order 4) $\rtimes$ (group of order 2), since D_8 has 5 elements of order 2 yet Q_8 has 1 element of order 2. So there does not exist H such that $N \cap H = 1$ where $|H| = 2$, since $Z(Q_8) \cong C_2$ and so any group of order 4 must contain H (since only one element of order 2).

$D_6 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ and $\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$.

Lemma 11.2. *$G = N \rtimes H$. For $h \in H$, $\theta_h : N \to N$ defined by $\theta_h : n \mapsto n^h$ is an automorphism of N, i.e., $\theta_h \in \mathrm{Aut}(N)$. The map $\theta : H \to \mathrm{Aut}(N)$ defined by $\theta : h \mapsto \theta_h$ is a homomorphism.*

Note. We use $n^h := hnh^{-1}$.

Proof. $N \lhd G$ implies $n^h \in N$. θ_h is a HM:

$$\theta_h(n_1 n_2) = h n_1 n_2 h^{-1} = h n_1 h^{-1} h n_2 h^{-1} = \theta_h(n_1)\theta_h(n_2).$$

θ_h is one-to-one $\theta_h(n_1) = \theta_h(n_2)$ implies $n_1 = n_2$ and also θ_h is onto since $\theta_h\big(h^{-1}nh\big) = n$. Hence, $\theta_h \in \mathrm{Aut}(N)$.

θ is a HM:

$$\theta(h_1 h_2)(n) = h_1 h_2 n (h_1 h_2)^{-1} = \theta(h_1)\theta(h_2)(n).$$

□

Lemma 11.3. *$N \lhd G$, H complement to N in G. Every $g \in G$ has a unique expression $g = nh$ where $n \in N$ and $h \in H$.*

Proof. $G = NH$ implies $g = nh$. If $g = n_1 h_1$ then $nh = n_1 h_1$ has $n_1^{-1} n = h_1 h^{-1}$ where LHS in N and RHS in H, but intersection is trivial ($N \cap H = 1$), so representation is unique. □

Definition 11.4. Given N, H, $\theta : H \to \mathrm{Aut}(N)$ and $h \mapsto \theta_h$, define $G = N \rtimes_\theta H$ to be the set of ordered pairs (n, h) with $n \in N$ and $h \in H$ with operation $\cdot$

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

called *semi-direct external product.*

Theorem 11.5. *$(G, \cdot)$ is a group. Furthermore, $N_0 = \{(n, 1) \mid n \in N\} \leq G$ and $H_0 = \{(1, h) \mid h \in H\} \leq G$ where $N_0 \cong N$ and $H_0 \cong H$. Finally, $G = N_0 \rtimes H_0$.*

Proof. Closure, associativity both hold. For the identity element, simply take $(1, 1)$, such that

$$(n, h) \cdot (1, 1) = (n\theta_h(1), h) = (n, h) = (\theta_1(n), h) = (1, 1) \cdot (n, h).$$

Also obtain

$$(n, h) \cdot \left(\theta_h^{-1}\left(n^{-1}, h^{-1}\right)\right) = \left(n\theta_h\theta_h^{-1}\left(n^{-1}\right), 1\right) = \left(nn^{-1}, 1\right) = (1, 1),$$

so G is a group.

Now, $(1, h_1) \cdot (1, h_2) = (1, h_1 h_2)$ implies $H_0 \leq G$. Furthermore, $(1, h) \mapsto h$ yields $H_0 \cong H$.

Similarly, $(n_1, 1)(n_2, 1) = (n_1 n_2, 1)$ implies $N_0 \leq G$ and $N_0 \cong N$.

Observe $(n, h) = (n, 1)(1, h)$ implying $G = N_0 H_0$. Furthermore, $N_0 \cap H_0 = 1$, and notice

$$(n, h)(n_1, 1)(n, h)^{-1} = (n_2, 1) \in N,$$

so $N \lhd G$, and thus $G = N_0 \rtimes H_0$. □

We say G *realises* as SDP N, H $\theta : H \to \mathrm{Aut}(N)$.

11.2. **Automorphisms (of cyclic groups).**

Lemma 11.6. *$G = \langle x \rangle = \mathbb{Z}_n$ for some $n \in \mathbb{N}$. Let σ_m be the endomorphism of G sending x to x^m. $\mathrm{Aut}(G) = \{\sigma_m \mid m \neq 0$ and $\gcd(m, n) = 1\}$.*

Corollary 11.7. *p prime, $\mathrm{Aut}(\mathbb{Z}_p)$ has order $p - 1$. $\mathrm{Aut}(\mathbb{Z}_p)$ is cyclic of order $p - 1$.*

Example 11.8. $\mathbb{Z}_5 = \left\langle x \mid x^5 = 1 \right\rangle$. $\mathrm{Aut}(\mathbb{Z}_5)$ has $x \mapsto x^i$ for $i \in \{1, 2, 3, 4\}$.

Theorem 11.9. *$E = \overbrace{C_p \times \ldots \times C_p}^{d \text{ copies}}$ elementary abelian group of order p^d. Then $\mathrm{Aut}(E) \cong GL(d, p)$.*

Proof. Identify E with $V = \mathrm{GF}(p)^d$, d-dimensional vector space over $\mathrm{GF}(p)$. Then $x \cdot y \mapsto x + y$ and $x^\alpha \mapsto \alpha \cdot x$. □

11.3. **External SDP.**

Example 11.10. $N, H, \theta : H \to \mathrm{Aut}(N)$ take $h \mapsto$ id aut of N such that $(n_1, h_2) \cdot (n_2, h_2) = (n_1 n_2, h_1 h_2)$, implying $G = N \rtimes_\theta H = N \times H$.

Example 11.11. $N = \mathbb{Z}_3 = \left\langle y \mid y^3 = 1 \right\rangle$, $H = \mathbb{Z}_2 = \left\langle x \mid x^2 = 1 \right\rangle$; consider $N \rtimes_\theta$ where $\theta : H \to \mathrm{Aut}(N)$. Can take $\theta_a = \mathrm{id}$ so $y \mapsto y$ (such that θ_a is an element of order 1), and $\theta_b = \mathrm{inv}$ so $y \mapsto y^{-1}$ (such that θ_b is an element of order 2). Can define $h \mapsto \theta_a$ or $h \mapsto \theta_b$. $\{(y, , x) \mid y \in N, x \in H\}$. $(y_1, x_1) \cdot (y_2, x_2) = (y_1 \theta_a(y_2), x_1 x_2)$ or $(y_1 \theta_b(y_2), x_1 x_2)$, which is $(y_1 y_2, x_1 x_2)$ or $\left(y_1 y_2^{-1}, x_1 x_2\right)$ respectively. For θ_a, obtain abelian group of order 6 implying $\mathbb{Z}_3 \times \mathbb{Z}_2$, and for θ_b obtain non-abelian group of order 6 (implying isomorphic to S_3). Note this is because we get $(y_1, x_1)(y_2, x_2) \neq (y_2, x_2)(y_1, x_1)$ in general for θ_b.

Example 11.12. $N = \langle n \mid n^3 = 1\rangle$, $H = \langle h \mid h^2 = 1\rangle$, $\theta : H \to \mathrm{Aut}(\mathbb{Z}_3)$, $\theta : h \mapsto \theta_h$ where $|h| = 2$ implying $|\theta_h| = 1$ or 2. As $\theta : H \to \mathrm{Aut}(N)$ and $\mathrm{Aut}(N) \cong \mathbb{Z}_2$, follows we only have inverse and identity automorphism. For identity, we get $G_1 = \langle n, h \mid n^3 = 1, h^2 = 1, n^h = n\rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_2$, and for $G_2 = \langle n, h \mid n^3 = 1, h^2 = 1, n^h = n^{-1}\rangle \cong S_3$.

Example 11.13. $N = \mathbb{Z}_3 = \langle n \mid n^3 = 1\rangle$, $H = \langle h \mid h^3 = 1\rangle$. Then $\langle n, h \mid n^3, h^3, n^h = n\rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Example 11.14. $N = \mathbb{Z}_5 = \langle x \mid x^5 = 1\rangle$, $H = \mathbb{Z}_2 = \langle h \mid h^2 = 1\rangle$. Then we have $\theta_1 : x \mapsto x$, $\theta_2 : x \mapsto x^2$, $\theta_3 : x \mapsto x^3$, $\theta_4 : x \mapsto x^{-1}$, which have orders 1, 4, 4, 2, respectively. Since h has order 2, $h \mapsto \theta_1$ or θ_4 only valid options, so $G_i = \langle n, h \mid n^5, n^h = \theta_i(n)\rangle$ where $G_2 \cong G_3$.

Example 11.15. $N = \langle n \mid n^p = 1\rangle$, $H = \langle h \mid h^q = 1\rangle$ with p, q distinct primes and assume $p > q$. Then we get $C_p \times C_q$; $q \mid p - 1$ implies exists non-trivial HM $\theta : H \to \mathrm{Aut}(N)$ with $C_p \rtimes_\theta C_q$.

Example 11.16. $D_8 \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2$ where $N := \langle a\rangle = \mathbb{Z}_4$ and $H := \langle h\rangle = \mathbb{Z}_2$. Then $\mathrm{Aut}(N)$ has identity and inverse automorphisms; if you take $\theta : H \to \mathrm{Aut}(N)$, $h \mapsto \mathrm{id}$ we get $\langle a, h \mid a^4, h^2, a^h = a\rangle$. If you take $h \mapsto$ inv aut, then $\langle a, h \mid a^4, h^2, a^h = a^{-1}\rangle$.

Example 11.17. $D_8 = (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ with $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a, b \mid a^2 = b^2 = [a, b] = 1\rangle$ and $\mathbb{Z}_2 = \langle x \mid x^2 = 1\rangle$. So, $N = \mathbb{Z}_2 \times \mathbb{Z}_2$ yields $\mathrm{Aut}(N) \cong \mathrm{GL}(2, 2) \cong S_3$, where automorphisms of $\mathrm{Aut}(N)$ correspond to identity matrix I, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ which are the elements of $\mathrm{GL}(2, 2)$ of order dividing 2.

Taking the identity:

$$\langle a, b, x \mid a^2 = b^2 = x^2 = 1, [a, b] = 1, a^x = a^1 b^0 = a, b^x = a^0 b^1 = b\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

and taking $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$:

$$\langle a, b, x \mid a^2 = b^2 = x^2 = [a, b] = 1, a^x = a^1 b^1 = ab, b^x = a^0 b^1 = b\rangle.$$

11.4. **Groups of order 12.** We have $\mathbb{Z}_4 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ as the abelian groups of order 12 (follows from fundamental theorem of finite abelian groups).

For the non-abelian finite groups of order 12, we claim that there are only three: A_4, D_{12} and $T = \left\langle a, b \mid a^6 = 1, b^2 = a^3 = (ab)^2\right\rangle$. Assume G is a finite non-abelian group of order 12, and that $G \ncong A_4$. Then G has a Sylow-3-subgroup P, of index 4. If we assume K is not normal, then we may consider the action of G on the (right) cosets of K; since the kernel of the action is $\mathrm{Core}_G(K)$ and we assume K not normal, follows that the kernel is trivial (i.e., map is 1-to-1). But K has order 3, and so obviously image a 3-cycle, implying $G \cong A_4$, a contradiction. Now, K is normal. Take P to be a Sylow 2-subgroup of G, which has order 4 and index 3 (and consequently maximal). Then $K \cap P = 1$, and $KP = G$, giving us $G = K \rtimes P$.

Now, $P \cong \mathbb{Z}_4$ or $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. If $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we consider x, y to be generators of P so that θ_x is the inverse automorphism and θ_y is the identity automorphism. Then $s = \left(n^2, y\right)$ and $t = (n, x)$ satisfy the relations of D_{12}, i.e., $\langle s, t \mid s^6, t^2, stst\rangle$. On the other hand, if $P \cong \mathbb{Z}_4$, we consider x to be the generator of P so that θ_x is the inverting automorphism, and choose $s = \left(a^2, x^2\right)$ and $t = (1, x)$ which satisfy the relations of T with $\left\langle s, t \mid s^6 = 1, t^2 = s^3 = (st)^2\right\rangle$.

11.5. **Holomorphs and affine groups.**

Definition 11.18. N, $H := \mathrm{Aut}\,(N)$. Then take $\mathrm{Hol}\,(N) = N \rtimes_\theta H$ to be the *holomorph* of N, with θ the identity automorphism.

Example 11.19. $N = \mathbb{Z}_3$, $H := \mathrm{Aut}\,(\mathbb{Z}_3) = \mathbb{Z}_2$. Then $\theta_1 : n \mapsto n$ and $\theta_2 : n \mapsto n^{-1}$ such that $|\mathrm{Hol}\,(N)| = 6$. Observe

$$(n, \theta_2)\big(n^2, \theta_1\big) = \big(n^2, \theta_2\big)$$

and

$$\big(n^2, \theta_1\big)(n, \theta_2) = (1, \theta_2),$$

implying $\mathrm{Hol}\,(N)$ is non-abelian of order 6, and consequently isomorphic to S_3.

F field, $V = F^n$ vector space of $1 \times n$ row vectors over F. Given $A \in \mathrm{GL}\,(n, F)$, $b \in F^n$. Define $T_{A,b} : V \to V$ by $x \mapsto Ax + b$. Then $T_{A,b} = T_{A',b'}$ if and only if $A = A'$, $b = b'$. These maps $T_{A,b}$ are the *affine linear transformations of* V $\mathrm{AGL}(n, F) := \{T_{A,b} \mid A \in \mathrm{GL}\,(n, F), b \in F^n\}$. Define $T_{A,b} \cdot T_{C,d} = T_{AC,bC+d}$, which is a group under operation $\cdot$. Note $(T_{A,b})^{-1} = T_{A^{-1},-bA^{-1}}$. Define $\phi : \mathrm{AGL}(V) \to \mathrm{GL}(V)$. $T_{A,b} \to A$; ϕ is an epimorphism onto $\mathrm{GL}(V)$ where $\ker\phi = \{T_{I,b} \mid b \in F^n\}$. Observe $\mathrm{AGL}(V) \rhd T(V) = \ker\phi$ implying $\frac{\mathrm{AGL}(V)}{T(V)} \cong \mathrm{GL}(V)$. Furthermore, $\mathrm{AGL}(V) = T(V) \rtimes \mathrm{GL}(V)$. Every affine linear transformation is composed of a linear transformation followed by a translation $T_{I,b}$. Note $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$.

$|F| = n$, V rank n implies V isomorphic to elementary abelian group E of order p^n. $V \rtimes \mathrm{GL}(V) \to \mathrm{Hol}\,(V)$ where $\mathrm{GL}(V) \cong \mathrm{Aut}\,(E)$. $V = \mathrm{GF}(p^n)$, $\mathrm{Aut}\,(V) = \mathrm{GL}(V) \cong \mathrm{GL}\,(n, F)$. $\mathrm{AGL}(V) = \mathrm{Hol}\,(V)$, so $|\mathrm{AGL}(n, F)| = p^n|\mathrm{GL}\,(n, F)|$.

Example 11.20. $V = \mathbb{Z}_2 \times \mathbb{Z}_2 \cong F_2^2$ where $\mathrm{Aut}\,(V) \cong \mathrm{GL}\,(2, 2, \cong)S_3$ and so $\mathrm{AGL}(2, 2) \cong \mathrm{Hol}\,(V_4)$ (where V_4 klein-four-group) implying $\mathrm{Hol}\,(V) = V_4 \rtimes S_3$ (a group of order 24).

Example 11.21. $N = \big\langle n_1, n_2 \mid n_1^2 = n_2^2 = [n_1, n_2] = 1\big\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Let

$$H = \Big\langle h_1, h_2 \mid h_1^2 = h_2^3 = 1, h_2^{h_1} = h_2^{-1}\Big\rangle \cong S_3,$$

where $h_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $h_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Using the matrices, obtain $n_1^{h_1} = n_1$, $n_1^{h_2} = n_1$, $n_2^{h_1} = n_1 n_2$, $n_2^{h_2} = n_1 n_2$. Now, let R be the relators of those found in N and H, and also those from the matrix. Hence, $\mathrm{Hol}\,(\mathbb{Z}_2 \times \mathbb{Z}_2) = \langle n_1, n_2, h_1, h_2 \mid R\rangle$, which is isomorphic to S_4.

11.6. **Wreath product.** Given group G and $H \leq \mathrm{Sym}(n)$. Define $N = G \times \ldots \times G$ (n copies) and $\theta : H \to \mathrm{Aut}\,(N)$ with $h \mapsto \theta_h$ where $\theta_h((g_1, \ldots, g_n)) = (g_{1^h}, \ldots, g_{n^h})$ and 1^h is image of 1 under h and so on. Claim: $\theta_h \in \mathrm{Aut}\,(N)$.

Definition 11.22. $W := N \rtimes_\theta H$. We say W is a *wreath product* of G by H. $N := G \times \ldots \times G$ is the *base* of wreath product.

Say $|G| = m$, $|H| = n$. Then $|W| = m^n \cdot n$.

May also say $W := N \rtimes H = G$ pwr $H = G \wr H$, but note different to G wr H (will define later).

Example 11.23. $G = \mathbb{Z}_2$, $H = \mathbb{Z}_2 \leq \mathrm{Sym}(2)$ with $G = \big\langle x \mid x^2 = 1\big\rangle$ and $H = \langle(1, 2)\rangle$. What is $G \wr H$? Well, $|G \wr H| = 2^2 \times 2 = 8$. $N := G \times G\{(1, 1), (1, x), (x, 1), (x, x)\}$ and $H = \{h_1 = \mathrm{id}, h_2 = (1, 2)\}$. Then $\theta_h : (1, 2) \mapsto (2, 1)$, so $\theta_h(g_1, g_2) = (g_2, g_1)$. Note θ_h fixes $(1, 1)$, (x, x) and swaps $(1, x)$ and $(x, 1)$. $N = \mathbb{Z}_2 \times \mathbb{Z}_2$, $H = \mathbb{Z}_2$. So,

$$((1, x), h)^2 = \big((1, x)\theta_h((1, x)), h^2\big) = ((1, x)(x, 1), 1) = ((x, x), 1),$$

where $a = ((1,x),h)$ has order 4 and $b = ((1,1),h)$ is of order 2 and $a^b = a^{-1}$ implying $N \rtimes H \cong \langle a, b \mid a^4, b^2, b^{-1}ab = a^{-1}\rangle$. Thus, $W = \mathbb{Z}_2 \wr \mathbb{Z}_2 \cong D_8$.

Example 11.24. $G = \mathbb{Z}_2$, $H = S_3 = \langle (1,2,3),(1,2)\rangle$. What is $G \wr H$? Well, $N = G \times G \times G$, $W := N \rtimes H$ so $|W| = 2^3 \cdot 6 = 48$.

Example 11.25. $G = \mathbb{Z}_2$ and H regular representation of H (from Cayley's theorem). $H = \langle (1,2,4),(3,6,5),(1,3)\rangle \leq \mathrm{Sym}(6)$. $G \wr H$? $N = G \times \ldots \times G$ (6 copies), with $|W| = |G|^6|H| = 2^6 \times 6$. Written G rwr H and G wr H means to take regular representation. If H is cyclic, then the two coincide. That is, does not matter if we take regular or other permutation groups (so can take $(1,\ldots,n)$).

Example 11.26. $G = \mathbb{Z}_2$ and $H = \mathbb{Z}_3 = \langle (1,2,3)\rangle$ then $|G \wr H| = 2^3 \cdot 3$ but $|H \wr G| = 3^2 \cdot 2$, so S is not commutative.

11.7. **Iterated wreath products.** $C_p \wr C_p$ where $|W| = p^p \cdot p = p^{p+1}$. We may then consider iterating, i.e., next would be $(C_p \wr C_p) \wr C_p$ where $|W| = \left(p^{p+1}\right)^p \cdot p = p^{p^2+p+1}$. So, $\wr_k C_p$ has $|W| = p^{r(k)}$ where $r(k) = p^{k-1} + p^{k-2} + \ldots + p + 1$.

Lemma 11.27. *Let $p^{r(n)}$ be the highest power prime p dividing $(p^n)!$. Then $r(n) = p^{n-1} + p^{n-2} + \ldots + p + 1$ $\left[r(n) = p^{n-1} + r(n-1)\right]$.*

Proof. $(p^n)! = 1 \cdot 2 \ldots p^n$. Contribution to $r(n)$ comes from p, $2p$, …, $(p-1)p$, …, p^n. There are p^{n-1} such terms of the p^{n-1}, a total of p^{n-2} terms are divisible by p^2 of the p^{n-2} so p^{n-3} by p^3, and hence $r(n) = p^{n-1} + \ldots + 1$. □

Corollary 11.28. *$G = \mathrm{Sym}\,(p^n)$, $S :=$ Sylow p-subgroup of G, then $|S| = p^{r(n)}$.*

Example 11.29. $G = S_8$. Then $\left|\mathrm{Syl}_p\,(2)G\right| = 2^{2^2+2+1} = 128$.

Theorem 11.30. *Let p be prime, $k \in \mathbb{N}$. $\mathrm{Syl}_p\left(\mathrm{Sym}\left(p^k\right)\right)$ is the k-fold iterated wreath product of C_p.*

Proof. Show that $\wr_k C_p \leq \mathrm{Sym}\left(p^k\right)$. Base case: $k = 1$, $C_p = \langle (1,\ldots,p)\rangle \leq \mathrm{Sym}\,(p)$. Suppose claim is true for k. Let $P = \mathrm{Sym}\left(p^{k+1}\right)$, $A = \mathrm{Sym}\left(p^k\right)$. Take p copies of A acting on disjoint sets

$$\left\{1,\ldots,p^k\right\}, \left\{1+p^k,\ldots,2p^k\right\}, \ldots, \left\{(p-1)p^k+1,\ldots,p^{k+1}\right\}.$$

Since copies of A act on disjoint sets on support (points which A acts on) of P, therefore they commute. $N := \prod_{i=1}^p A \leq P$, $\overbrace{A \times \ldots \times A}^{p} \leq P$.

Define $h := \prod_i^{p^k} \left(i, i+p^k, i+2p^k, \ldots, i+(p-1)p^k\right) \in P$ where $H \leq \langle h\rangle \leq P$. H acts to permute the copies of A. Let $G = N \rtimes H \leq P$, claim $\mathrm{Syl}_p\,(G) = \mathrm{Syl}_p\,(N) \rtimes \mathrm{Syl}_p\,(H)$. Therefore, $\mathrm{Syl}_p\,(G) = (\wr_k C_p)^p \rtimes C_p = \wr_{k+1} C_p \leq \mathrm{Sym}\left(p^{k+1}\right)$ by IH. □

Lemma 11.31. *Suppose $G = N \rtimes H$. Then $\mathrm{Syl}_p\,(G) = \mathrm{Syl}_p\,(N) \rtimes \mathrm{Syl}_p\,(H)$.*

Proof. □

Corollary 11.32. *Let p be a prime, $n \in \mathbb{N}$. Let $n = \sum_{i=0}^k a_i p^i$ $0 \leq a_i \leq p-1$. Each Sylow p-subgroup of S_n is a direct product $T_1^{a_1} \times T_2^{a_2} \times \ldots \times T_k^{a_k}$, $T_i = \wr_i C_p$ is Sylow p-subgroup of $\mathrm{Sym}\left(p^i\right)$.*

Proof. Calculate powers p dividing $n!$ number of integers between 1 and n divisible by p is $\left\lfloor \frac{n}{p} \right\rfloor$. The number of these elements by p^2 is $\left\lfloor \frac{n}{p^2} \right\rfloor$ implying $p^m \mid n$ where $m = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$, therefore

$$m = \left(a_1 + a_2 p + \ldots + a_k p^{k-1}\right) + \left(a_2 p + \ldots + a_k p^{k-2}\right) + \ldots,$$

and so $m = a_1 + a_2(p+1) + a_3\big(p^2+p+1\big) + \ldots$. Therefore, p^m is the order of $T_1^{a_1} \times T_2^{a_2} + \times \ldots \times T_k^{a_k}$. Now, we show S_n has a subgroup isomorphic to $\prod T_i^{a_i}$. As in theorem, divide set with n elements into disjoint subsets (where a_i size p^i maps to $\wr_i C_p$ for $0 \leq i \leq k$, and proof follows similar way. □

Example 11.33. S_5, $n = 5$, $p = 2$, $5 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2$, so get $\mathrm{Syl}_2(\mathrm{Sym}\,(4))$ giving us $C_2 \wr C_2 \cong D_8$.

Example 11.34. $G = \mathrm{Sym}\,(10)$, $10 = 1 \times 2 + 1 \times 2^3$ where we get $\mathbb{Z}_2$ from the '2' and $\mathrm{Syl}_2(\mathrm{Sym}\,(8)) = \wr_3\mathbb{Z}_2$ from the '2^3'. Hence, get $\mathbb{Z}_2 \times (\wr_3\mathbb{Z}_2)$. Now, $|\mathrm{Syl}_2(G)| = 2 \times 2^7 = 2^8$. Claim $\mathrm{Syl}_3(G) = C_3 \wr C_3$. Well, $10 = 1 + 1 \times 3^2$ where we get $\mathrm{Syl}_3\big(\mathrm{Sym}\,\big(3^2\big)\big) = C_3 \wr C_3$.

Example 11.35. S_{34}, $\mathrm{Syl}_3(S_{34})$? Well, $34 = 1 + 2 \times 3 + 1 \times 3^3$, so we get two copies of C_3 and one copy of $\wr_3 C_3$. So, $S := (C_3)^2 \times (\wr_3 C_3)$ with order 3^{15}.

11.8. **General construction of wreath product.** G, H, want $G \wr H$. G acts on Λ and H acts on Ω. So, $G \wr H$ acts on $\Lambda \times \Omega$.

Given $g \in G$, $\omega \in \Omega$ we define g_ω^* of $\Lambda \times \Omega$ as follows: for $(\lambda, \omega') \in \Lambda \times \Omega$ define

$$g_\omega^* = \begin{cases} (\lambda^g, \omega') & \text{if } \omega' = \omega; \\ (\lambda, \omega') & \text{if } \omega' \neq \omega. \end{cases}$$

Observe $g_\omega^*(g')_\omega^* = (gg')_\omega^*$ where $g, g' \in G$. Hence, $G_\omega^* = \{g_\omega^* \mid g \in G\} \leq \mathrm{Sym}\,(\Lambda \times \Omega)$.

The map $G \to G_\omega^*$ defined $g \mapsto g_\omega^*$ is an isomorphism (i.e., $G \cong G_\omega^*$, $\omega \in \Omega$). For $h \in H$, define permutation h^* of $\Lambda \times \Omega$ by $h^*(\lambda, \omega) = \big(\lambda, \omega^h\big)$. $H^* = \{h^* \mid h \in H\}$, $H^* \leq \mathrm{Sym}\,(\Lambda \times \Omega)$. Map $H \to H^*$ by $h \mapsto h^*$ is an isomorphism, so $H \cong H^*$.

Theorem 11.36. *G acts on Λ, H acts on finite set Ω. $G \wr H \cong W$ where $W := \langle G_\omega^*, H^* \mid \omega \in \Omega\rangle \leq \mathrm{Sym}\,(\Lambda \times \Omega)$.*

Note. Want to show $W = N \rtimes H$, $N = G \times \ldots G$ where $N \lhd W$, $NH = W$.

Proof. $K^* = \big\langle \bigcup_{\omega\in\Omega} G_\omega^* \big\rangle = \prod_{\omega\in\Omega} G_\omega^*$ direct product. G_ω^* centralises $G_{\omega'}^*$ for all $\omega \neq \omega'$ implying $G_\omega^* \lhd K^*$. $K^* \lhd W$: $h^* g_\omega^* (h^*)^{-1} = g_\omega^* h$ (claim), implying $(K^*)^{h^*} \leq K^*$ so $K^* \lhd W = \langle K^*, H^*\rangle$.

Now, we check $K^* \cap H^* = 1$. $g^*(\lambda, \omega')$ fixes second component and $h^*(\lambda, \omega')$ fixes first component so element common to both K^*, H^* must be $(1, 1)$.

Therefore, $W = K^* \rtimes H^*$. Define isomorphism from $\phi : G \wr H \to W$ by $(g_\omega)_{\omega\in\Omega} h \mapsto (g_\omega^*)h^*$ where ϕ is an isomorphism. □

Note. $G \times \ldots \times G$ $|\Omega|$ times.

Example 11.37. $G = \mathbb{Z}_2 = \langle(1, 2)\rangle$ and $H = \mathbb{Z}_2 = \langle(3, 4)\rangle$ where $\Lambda = \{1, 2\}$ and $\Omega = \{3, 4\}$. Then $\Lambda \times \Omega = (a = (1, 3), b = (2, 3), c = (1, 4), d = (2, 4))$. Let $g = (1, 2)$ and $\omega = 3$. Then $g_\omega^* : (1, 3) \mapsto (1^g, 3) = (2, 3)$, $(2, 3) \mapsto (2^g, 3) = (1, 3)$, $(1, 4) \mapsto (1, 4)$, $(2, 4) \mapsto (2, 4)$. That is, $g_3^* = (a, b)$.

$\omega = 4$: $(1, 3) \mapsto (1, 3)$, $(2, 3) \mapsto (2, 3)$, $(1, 4) \mapsto (2, 4)$, $(2, 4) \mapsto (1, 4)$ so $g_4^* = (c, d)$.

Now, $h = (3, 4)$ so $h^* : (2, 3) \mapsto (2, 4)$, $(1, 4) \mapsto (1, 3)$, $(2, 4) \mapsto (2, 3)$, $(1, 3) \mapsto (1, 4)$. Therefore, $h^* = (a, c)(b, d)$. $W := \langle G_3^*, G_4^*, H^*\rangle = \langle g_3^*, g_4^*, h^*\rangle$ and so $W = \langle(a, b), (c, d), (a, c)(b, d)\rangle$. Therefore, $W := \langle(1, 2), (3, 4), (1, 3)(2, 4)\rangle \cong D_8$.

Example 11.38. $G = C_2 = \langle(1, 2)\rangle$ $\Lambda = \{1, 2\}$ and $H = S_3 = \langle(3, 4, 5), (3, 4)\rangle$ $\Omega = \{3, 4, 5\}$. $\Lambda \times \Omega = \{a = (1, 3), b = (2, 3), c = (1, 4), d = (2, 4), e = (1, 5), f = (2, 5)\}$. Let $g = (1, 2)$ and $\omega = 3$. Then g_3^* where $(1, 3) \mapsto (2, 3)$ and vice versa fixing all others so get (a, b). For $\omega = 4$, get (c, d) and $\omega = 5$ gets (e, f). Now, consider $h = (3, 4, 5)$. Get $(1, 3) \mapsto (1, 4) \mapsto (1, 5)$ and $(2, 3) \mapsto (2, 4) \mapsto (2, 5)$ so

get $(a,c,e)(b,d,f)$. For $h = (3,4)$ get $(1,3) \mapsto (1,4)$ and $(2,3) \mapsto (2,4)$ so get $(a,c)(b,d)$.

$$W = G \wr H = \left\langle \overbrace{(a,b),(c,d),(e,f)}^{C_2 \times C_2 \times C_2}, \overbrace{(a,c,e)(b,d,f),(a,c)(b,d)}^{\text{permute the copies}} \right\rangle.$$

Hence, $|W| = |G|^n |H| = 8 \cdot 6 = 48$.

Example 11.39. $H \leq \mathrm{Sym}\,(6)$ $H = \langle (3,5,7)(4,6,8), (3,6)(4,7)(5,8) \rangle$ $\Omega = \{3, \ldots, 8\}$ with $G \wr H \leq \mathrm{Sym}\,(12)$. So, $|G \wr H| = |G|^n |H| = 2^6 \cdot 6 = 384$.

Note. C_2 wreath product with the Prufer group infinite group.