ALGEBRA 1, D. CHAN

1. Introduction

[1]Introduction to groups via symmetry. A symmetry of F is a surjective isometry which preserves F.

Definition 1.1. *A set G is a group when given an operation $G \times G \longrightarrow G$, satisfying*
1. *associativity, $(ab)c = a(bc)$,*
2. *identity, there exists a 1 such that $a1 = a$*
3. *inverse, there exists b for all a such that $ba = 1$, we write $b = a^{-1}$.*

Example 1. $G = \mathbb{R} - \{0\}$ the real numbers, with the usual multiplication forms a group.
but $G = \mathbb{Z}$ the integers do not form a group under multiplication, $\mathbb{Z}$ is a group under addition.

2. Symmetry groups

Symmetric group, alternating groups, cycles.
Disjoint cycles commute, and generate the symmetric group.

Example 2.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$$

This can be written as $\sigma = (124)(36)(5) = (124)(36)$

Lemma 2.1. *Any element of Σ_n can be written as a product of disjoint cycles. I.e. Let $\sigma \in \Sigma_n$, then for some set S, where $|S| = n$, we can write $S = \bigcup_i S_i$ such that σ permutes elements of S_i cyclically.*

Proof. see handout. □

Lemma 2.2. *Any element of Σ_n can be written as a product of transpositions.*

Proof. $(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \dots (a_1 a_3)(a_1 a_2)$ □

3. Dihedral groups, subgroups generated by subsets

Consider $\sigma, \tau \in \Sigma_n$, where $\sigma = (12 \dots n)$, and $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & & 1 \end{pmatrix}$, $\tau^2 = \sigma^n = 1_{\Sigma_n}$. What is the smallest subgroup H containing σ and τ? This group is called the dihedral group, D_n.

Definition 3.1.

$$\langle \sigma, \tau \rangle = D_n$$

We will use $\tau\sigma = \sigma^{-1}\tau$ (show this) to simplify products of σ and τ by swapping τ and σ around in the product.

Proposition 3.2. *H is the set of $2n$ elements, $\sigma^i\tau$, σ^i, for $i \in \{0 \dots n-1\}$.*

Proof. Show closure under multiplication, inversion, identity. □

Proposition 3.3. *Let $\{H_i\}$ be a set of subgroups of a group G, then $H = \bigcap_i H_i$ is also a subgroup.*

Proof. Trivial □

Proposition 3.4. *Let $S \subseteq G$, there exists a unique smallest subgroup H containing S, this is called the subgroup generated by S.*

Proof. Use above and take intersections of all subgroups containing S. □

Last lecture. For the dihedral group, D_n, we usually require $n \geqslant 3$, and $|D_n| = 2n$.
Alternating group, abelian groups.
Symmetric function

[1]The first few lectures are a bit sketchy, my apologies.

3.1. **Van der Monde determinant.** ...symmetries of. $(12)\Delta = -\Delta$

Lemma 3.5. *For $\sigma, \tau \in \Sigma_n$, $f(x_1 \dots x_n)$.*

$$(\sigma\tau)f = \sigma(\tau f)$$

Proof. Work from outside in.. □

Definition 3.6. *Let Δ be the difference product, $\sigma \in \Sigma_n$. By proposition in lecture 3, σ can be written as a product of transpositions, $\tau_i \dots \tau_m$. Then*

$$\sigma\Delta = \begin{cases} -\Delta & \text{if } m \text{ is odd} \\ \Delta & \text{if } m \text{ is even} \end{cases}$$

Proof. It suffices to prove that for $\sigma = (ij)$, i.e. $m = 1$, since

$$\sigma\Delta = \tau_1 \dots \tau_m \Delta = \tau_1 \dots \tau_{m-1}(\tau_m \Delta)$$

Now we need to account for all the factors,

- $\sigma(x_i - x_j) = -(x_i - x_j)$
- $\sigma(x_r - x_s) = (x_r - x_s)$
- For $r < i < j$, $\sigma(x_r - x_i)(x_r - x_j) = (x_r - x_j)(x_r - x_i)$
- For $i < r < j$, $\sigma(x_i - x_r)(x_r - x_j) = (x_i - x_r)(x_r - x_j)$
- For $j < i < r$, $\sigma(x_i - x_r)(x_j - x_r) = (x_i - x_r)(x_j - x_r)$

This implies $\sigma\Delta = -\Delta$, and the lemma follows. □

Corollary 3.7. *Let $A_n = \{\sigma \in S_n : \sigma\Delta = \Delta\}$, be all the even permutations. It is a proper subgroup of Σ_n called the alternating group. It is the subgroup generated by the subset,*

$$S = \{\tau_1\tau_2 : \tau_1^2 = \tau_2^2 = 1\}$$

Proof. S clearly contains all the even permutations... □

Abelian groups, cosets and Lagrange's Theorem

Examples. A transposition coset of the alternating group, $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ coset of SL_2

Example 3. (Disjoint union of cosets implies...)

- $Z = \bigcup_{r=0}^{m-1}(r + mZ)$
- $\mathrm{GL}_2 = \bigcup_{d \in R^*} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mathrm{SL}_2$
- $\Sigma_n = A_n \cup \tau A_n$, where τ is any transposition.

Lemma 3.8. *Any left/right coset, gH/Hg of H, has the same cardinality as H.*

Definition 3.9. *(index)*

Theorem 3.10. *(Lagrange)*

Proposition 3.11. *There is a $1-1$ correspondence between the left and right cosets*

Proof. by inversion □

4. Normal groups and Quotient groups

Example 4. Let $G = D_n < S_n$, recall that $D_n = \langle \sigma, \tau \rangle, \sigma = (12 \dots n), \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$. Also $\sigma^n = 1 = \tau^2, \tau\sigma = \sigma^{-1}\tau$. Let

$$\begin{array}{lllll} H & = & \langle \tau \rangle & = & \{1, \tau\} \\ N & = & \langle \sigma \rangle & = & \{\sigma^i\}_{i=0}^{n-1} \\ D_n & = & \langle \tau, \sigma \rangle & = & \{\sigma^i, \sigma^i\tau\}_{i=0}^{n-1} \end{array}$$

Definition 4.1. *Let $N \trianglelefteq G$, then the subset product makes G/N into a group, the quotient group of G mod N.*

Proof. trivial □

Example 5. Modulo arithmetic, $\mathrm{GL}_n(\mathbb{C}) / \mathrm{SL}_n(\mathbb{C})$

5. Isomorphisms and homomorphisms

Definition 5.1. *Let $\varphi : H \longrightarrow G$ be an homomorphism of groups, the following statements are equivalent,*
1. There exists a homomorphism $\varphi' : G \longrightarrow H$ which is an inverse to φ.
2. φ is bijective.
In this case φ is an isomorphism (write $\varphi : G \xrightarrow{\sim} H$, and $G \cong H$ are isomorphic)

Proof. $(2 \Longrightarrow 1)$ φ' is the inverse bijection to φ.
$(1 \Longrightarrow 2)$ Let $\varphi' = \varphi^{-1}$ for $h, h' \in H$ we know that $\varphi(h'h) = \varphi(h')\varphi(h)$. For $g, g' \in G$ let $h = \varphi^{-1}(g), h' = \varphi^{-1}(g')$. $\varphi(\varphi^{-1}(g)\varphi^{-1}(g')) = gg'$. Take inverse to show that φ^{-1} is a homomorphism. □

Example 6. $\varphi : R \longrightarrow H$, where $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(R) : a \in R \right\}$. $\varphi : a \longmapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. φ is a group isomorphism.
Show homormophicity and bijectivity.

Proposition 5.2. *Let $\varphi : H \longrightarrow G$ be an homomorphism of groups.*
1. $\varphi(1_H) = 1_G$
2. $\forall h \in H$, $\varphi(h^{-1}) = \varphi(h)^{-1}$
3. $\varphi(H)$ is a subgroup of G.

Proof. all trivial □

Proposition 5.3. *Let $\varphi : H \longrightarrow G$, $\ker(\varphi) = 1_H \Longrightarrow \varphi$ is injective.*

Proposition 5.4. *Let G be a group, and $g \in G$, then*

$$\begin{array}{lll} Cg & : & G \longrightarrow G \\ & : & h \longmapsto g^{-1}hg \end{array}$$

this is known is the conjugation by g, and is an isomorphism.

Proof. We have Cg^{-1} as the inverse map (check). Check Cg is an homomorphism. □

Example 7. Let $f : S \longrightarrow T$ be a set bijection, then $\mathrm{Perm}(S) \cong \mathrm{Perm}(T)$.

Proof. In fact,

$$\begin{array}{lll} \varphi & : & \mathrm{Perm}(S) \longrightarrow \mathrm{Perm}(T) \\ & : & \sigma \longmapsto f\sigma f^{-1} \end{array}$$

is a group isomorphism, with inverse being $\psi : \tau \longmapsto f^{-1}\tau f$. Exercise, show that the previous calculation implies φ, ψ are inverse isomorphisms. □

Example 8. Let F be an equilateral triangle in R^2, G be the group of symmetries of F, and V be the set of vertices of F. We wish to define an isomorphism

$$\begin{array}{lll} \varphi & : & G \longrightarrow \mathrm{Perm}(V) \cong \Sigma_3 \\ & & \sigma \longmapsto \sigma|_V \end{array}$$

$\varphi : G \longrightarrow \mathrm{Perm}(V) \cong \Sigma_3$.

6. Homomorphims, Quotient Homomorphisms

As for linear maps, we can compose homomorphisms

Proposition 6.1. *Let $\varphi : G \longrightarrow G'$ $\varphi' : G' \longrightarrow G''$ then $\varphi'\varphi : G \longrightarrow G''$ is an homomorphism.*

Proof. For $h, g \in G$ $(\varphi'\varphi)(hg) = \varphi'(\varphi(h)\varphi(g)) = \varphi'\varphi(h)\varphi'\varphi(g)$ □

Example 9. Let $\varphi : \Sigma_n \longrightarrow \mathrm{GL}_n(\mathbb{R})$,

$$\begin{aligned} \varphi(\sigma) \quad &: \quad \mathbb{R}^n \longrightarrow \mathbb{R}^n \\ &\qquad e_i \longmapsto e_{\sigma(i)} \end{aligned}$$

φ is an homomorphism. Let $\varphi' = \det(\mathrm{GL}_n(\mathbb{R})) \longrightarrow \mathbb{R}^*$ what is $\varphi'\varphi : \Sigma_n \longrightarrow \mathbb{R}^*$? ...

$$\begin{aligned} \varphi'\varphi(\sigma) &= (\varphi'\varphi)(\tau_1 \dots \tau_m) \\ &= (\varphi'\varphi)(\tau_1) \dots (\varphi'\varphi)(\tau_m) \\ &= (-1)^m \\ &= \begin{cases} 1 & \sigma \in A_n \\ -1 & \text{otherwise} \end{cases} \end{aligned}$$

Definition 6.2. *A group homomorphism $\varphi : G \longrightarrow G'$ is said to be an*

i. epimorphism if φ is surjective, e.g. det
ii. monomorphism if φ is injective
iii. automorphism if φ is an isomorphism from $G \longrightarrow G$

Definition 6.3. *(Kernel) This gives a condition when injectivity fails. Let $\varphi : G \longrightarrow G'$ be a group homomorphism, then we define the kernel of φ to be*

$$\begin{aligned} \ker(\varphi) &= \varphi^{-1}(1) \\ &= \{g \in G : \varphi(g) = 1\} \end{aligned}$$

Proposition 6.4. *Let φ be as above.*

(1) $\ker(\varphi) \trianglelefteq G$
(2) The non empty fibres of φ is sets of the form, for $g' \in G'$

$$\varphi^{-1}(g') = \{g \in G : \varphi(g) = g'\}$$

are the cosets of $\ker(\varphi)$.
(3) φ is injective iff $\ker(\varphi) = 1_G$.

Proof. (1) $\varphi(1) = 1 \in \ker(\varphi)$, for $h, g \in \ker(\varphi)$, then $\varphi(hg) = \varphi(h)\varphi(g) = (1)(1) = 1 \Longrightarrow hg \in \ker(\varphi)$. $\varphi(g^{-1}) = \varphi(g)^{-1} = 1^{-1} = 1$. So $\ker(\varphi) \leqslant G$.We now check normality, i.e. for any $g \in G$, $g^{-1}\ker(\varphi)g \subseteq \ker(\varphi)$. Let $k \in \ker(\varphi)$

$$\begin{aligned} \varphi(g^{-1}kg) &= \varphi(g)^{-1}(1)\varphi(g) \\ &= 1 \end{aligned}$$

implying $g^{-1}\ker(\varphi)g \subseteq \ker(\varphi)$.

(2) Suppose $g \in \varphi^{-1}(g')$ we must show, $g\ker(\varphi) = \varphi^{-1}(g')$, $K = \ker(\varphi)$

$$\begin{aligned} \varphi(gK) &= \varphi(g)\varphi(K) \\ &= \varphi(g) \\ &= g' \end{aligned}$$

Suppose $h \in \varphi^{-1}(g')$, then

$$\begin{aligned} \varphi(g^{-1}h) &= \varphi(g)^{-1}\varphi(h) \\ &= g'^{-1}g' \\ &= 1 \end{aligned}$$

(3) Follows from 2.

□

Example 10. $\varphi = \det : \mathrm{GL}_2(R) \longrightarrow R^*$. We saw before that $\ker(\varphi) = \mathrm{SL}_2(R)$ is a normal subgroup. We also computed the cosets to be

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mathrm{SL}_2 = \text{set of matrices of determinant } d = \varphi^{-1}(d)$$

clearly φ is not injective.

Example 11. Consider $\varphi'\varphi$ as in example 1, $\varphi'\varphi : \Sigma_n \longrightarrow \mathrm{GL}_n(R) \longrightarrow R^*$. $\ker(\varphi'\varphi) = A_n$, which is a normal subgroup. Fibres of $\varphi'\varphi$ were $A_n, \tau A_n$, where τ is a transposition.

Proposition 6.5. *Let $H \leqslant G$, the inclusion function $H \hookrightarrow G$, $h \longmapsto h$ is a monomorphism. Proof as exercise.*

Proposition 6.6. *(Quotient homomorphism) Let $N \trianglelefteqslant G$, there is an epimorphism*

$$\begin{aligned} \pi &: G \longrightarrow G/N \\ &: g \longmapsto gN \end{aligned}$$

Also $\ker(\pi) = N$. π is called a quotient homomorphism.

Proof. Note that π is surjective. We check that π is a homomorphism, let $h, g \in G$

$$\begin{aligned} \pi(hg) &= \pi(h)\pi(g) \\ &= hNgN \\ &= (hg)N \end{aligned}$$

We check the kernel of π

$$\begin{aligned} \ker(\pi) &= \pi^{-1}(1_{G/N}) \\ &= \pi^{-1}(N) \\ &= \{g : \pi(g) = gN = N\} \\ &= N \end{aligned}$$

□

Example 12. Let V and W be vector spaces, $V \leqslant W$ over some field F. Recall vector spaces can be considered as abelian groups, therefore we can form the quotient group V/W. In fact V/W can be made into a vector space. We describe V/W geometrically, let $V = R^3$, and W be some plane. The cosets of W will be $v + W$ for some $v \in V$, giving a plane parallel to W. So V/W is the set of all these parallel planes.

7. First isomorphism theorem

Remark 1. how much does an homomorphism deviate from being an isomorphism?

Theorem 7.1. *(Universal property for quotient homomorphisms) Let $\varphi : G \longrightarrow G'$ be a group homomorphism, and $N \trianglelefteqslant G$. Let $\pi : G \longrightarrow G/N$ be the quotient homomorphism.*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \\ \pi \downarrow & \nearrow \psi & \\ G/N & & \end{array}$$

If $N \leqslant \ker(\varphi)$ then there is a group homomorphism $\psi : G/N \longrightarrow G'$ such that $\varphi = \psi\pi$. Call ψ the induced homomorphism and say φ factors through ψ or π. In this case, ψ is uniquely defined by (*)

$$\psi(gN) = \varphi(g)$$

Proof. Frist note that if the diagram above commutes, i.e. $\varphi = \psi\pi$ then (*) holds and thus determines ψ uniquely.

- ψ is an homomorphism.
  For $g, h \in G$

$$\begin{aligned} \psi(gNhN) &= \psi(gN)\psi(hN) \\ \psi(gNhN) &= \psi((gh)N) \\ &= \psi(g)\psi(h) \end{aligned}$$

  so ψ is an homomorphism.

- Check (*) is well defined.
  (*) seems to depend on the choice of the coset representative, g, we must show it is independent of this choice, i.e. if $gN = hN$ (for $h \in G$) we require $\varphi(g) = \varphi(h)$. Suppose $h = gn$ for some $n \in N$, $\varphi(h) = \varphi(g)\varphi(n) = \varphi(g)(1) = \varphi(g)$ since $n \in N \leqslant \ker(\varphi)$. Hence φ is well defined.

□

Example 13. Let $\varphi = \det : \mathrm{GL}_2(R) \longrightarrow R^*$, $\ker(\varphi) = \mathrm{SL}_2 =: N$. The theorem above implies $\exists \psi : \mathrm{GL}_2(R)/\mathrm{SL}_2(R) \longrightarrow R^*$, where ψ maps

$$\psi : \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mathrm{SL}_2 \longmapsto \det \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} = d$$

Example 14. (Classification of cyclic groups) Let $G = \langle g \rangle$ be a cyclic group. Consider the function

$$\begin{aligned} \varphi &: Z \longrightarrow G \\ &: n \longmapsto g^n \end{aligned}$$

Check that φ is a homomorphism. Let N in the theorem be $\ker(\varphi)$, the thereom implies $\exists \psi : Z/N \longrightarrow G$. The claim is that ψ is bijective and therefore an isomorphism.

Proof.
- ψ is surjective, since $\psi(n + N) = \psi(n) = g^n$.
- ψ is injective. Let $n + N \in \ker(\psi)$ i.e. $\psi(n + N) = \psi(n) = 1 \Longrightarrow \ker(\varphi) = N$. $n + N = N = 0_{Z/N}$. So $\ker(\psi) = \{0_{N/Z}\}$.

□

Proposition 7.2. *The subgroups of Z all have form $N = mZ$, where $m \in \mathbb{N}$. (Note that $m = 0 \Longrightarrow N = \{0\}$)*

Proof. Suppose $N = 0$, (otherwise $m = 0$). Closure under negation implies $\exists$ minimum positive integer $m \in N$. Note that N is closed under addition and subtraction, implying $N \geqslant mZ$. Suppose $n \in N$, divide to get $n = qm + r$, with $q, r \in \mathbb{N}$, and $0 \leqslant r < m$. This implies $N \ni n - qm = r$ which contradicts the minimality of m unless $r = 0$, therefore $n = qm \in mZ$, and $N = mZ$. So any cyclic group is isomorphic to Z/mZ and conversely every such group is cyclic, $Z/mZ = \langle 1 + mZ \rangle$. This is part of a more general phenomenon. □

Theorem 7.3. *(First isomorphism theorem) Let $\varphi : G \longrightarrow G'$, be a group homomorphism, $\psi : G/\ker(\varphi) \longrightarrow G'$ be the induced homomorphism as in theorem on universal properties of quotient homomorphisms. Then ψ is a monomorphism and $G/\ker(\varphi) \cong \mathrm{im}(\psi)$.*

Proof. It suffices to check that $\ker(\psi) = 1_{G/\ker(\varphi)} = 1(\ker(\varphi))$. Let $K = \ker(\varphi)$, $gK \in \ker(\varphi)$, i.e.

$$\begin{aligned} \varphi(gK) &= 1 \\ \varphi(gK) &= \varphi(g)(1) \end{aligned}$$

so, $g \in K \Longrightarrow gK = K \Longrightarrow \ker(\psi) = K$, so ψ is injective. □

Corollary 7.4. *(Rank-Nullity Theorem) Let $T : V \longrightarrow W$ be a linear map of vector spaces and $K = \ker(T)$. (Think T as a projection onto a line in R^3) Given a subspace $U < V$, V/U is also a vector space of dimension $\dim(V) - \dim(U)$. We have the induced homomorphism,*

$$\begin{aligned} \psi &: V/K \longrightarrow W \\ V/K &\cong \mathrm{im}(T) \end{aligned}$$

We take dimensions of both sides and we have, $\dim(V) - \mathrm{null}(T) = \mathrm{rank}(T)$.

Corollary 7.5. *(from last week) Any group homomorphism $\varphi : G \longrightarrow G'$ can be factored as*

$$\varphi : G \xrightarrow{\pi} G/\ker(\varphi) \xrightarrow{\sim} G'$$

8. Second and third isomorophism theorems. Subgroups of quotient groups

Proposition 8.1. *Let $\varphi : G \longrightarrow G'$ be a group homomorphism and $H' \leqslant G'$, then*
1. $\varphi^{-1}(H') \leqslant G$
2. *If $H' \trianglelefteqslant G'$ then $\varphi^{-1}(H') \trianglelefteqslant G$*

Proof. (1) $1 \in \varphi^{-1}(1) \subseteq \varphi^{-1}(H')$ (identity). Suppose $g, g' \in \varphi^{-1}(H')$, $\varphi(gg') = \varphi(g)\varphi(g') \in H' \implies gg' \in \varphi^{-1}(H')$ (closure). $g \in \varphi^{-1}(H')$, $\varphi^{-1}(g^{-1}) = \varphi(g)^{-1} \in H' \implies g^{-1} \in \varphi^{-1}(H')$ (inverse). Hence $\varphi^{-1}(H') \leqslant G$.

(2) Let $g \in G, h \in \varphi^{-1}(H')$. We require $g^{-1}hg \in \varphi^{-1}(H')$ for normality. $\varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) \in H'$. therefore $H' \trianglelefteqslant G'$. So $g^{-1}hg \in \varphi^{-1}(H')$ and $\varphi^{-1}(H') \trianglelefteqslant G$.

□

This is analogous to morphisms, continuous maps, in the category of topological spaces. Let $(X, \tau), (X', \tau')$ be topological spaces, suppose

$$f : (X, \tau) \longrightarrow (X', \tau')$$

f is continuous iff $U' \in \tau' \implies f^{-1}(U') \in \tau$. The same applies in morphisms, group homomorphisms, in the category of groups. Let G and G' be groups, suppose

$$\phi : G \longrightarrow G'$$

ϕ is a homomorphism iff $H' \leqslant G' \implies \phi^{-1}(H') \leqslant G$.

Corollary 8.2. *Let $N \trianglelefteqslant G$, $\pi : G \longrightarrow G/N$ be the quotient homomorphism,*
1. *The subgroups $\tilde{H}$ of G/N are the groups of the form H/N where H is such that*

$$N \leqslant H \leqslant G$$

   also, $H = \pi^{-1}(\tilde{H})$
2. *In 1., H is normal in G iff $\tilde{H}$ is normal in G/N.*

Proof. ($\Longleftarrow$)We show $H/N \leqslant G/N$.

$$\begin{array}{rccccc} \varphi & : & H & \overset{i}{\hookrightarrow} & G & \overset{\pi}{\longrightarrow} & G/N \\ & : & h & \longmapsto & h & \longrightarrow & hN \end{array}$$

Then $\mathrm{im}(\varphi)$ is a group which is $\{hN : h \in H\} = H/N$. Check 2. normality if $H \trianglelefteqslant G$. Let $g \in G, h \in H$. we require,

$$(gH)^{-1}(hN)(gH) \in H/N$$

but $(g^{-1}hg)N \in H/N$, (since $H \trianglelefteqslant G$)
($\Longrightarrow$) $H/N \trianglelefteqslant G/N$ if $H \trianglelefteqslant G$. Now $\implies$ for 1. and 2. Consider $H \leqslant G/N$. Then let $H = \pi^{-1}(\tilde{H})$ is a subgroup of G by proposition. We require $\tilde{H} = H/N$.
Now π is surjective implies, $gN \in \tilde{H} \iff gN = hN$ for some $h \in \pi^{-1}(\tilde{H}) = H \iff gN \in H/N$. So $\tilde{H} = H/N$ and H is a subgroup. The previous proposition states that $H \trianglelefteqslant G$ if $H/N = \tilde{H} \trianglelefteqslant G/N$. □

Proposition 8.3. *Let m be a positive integer. The subgroups of Z/mZ are those of the form nZ/mZ where $n|m$, moreover nZ/mZ is cyclic of order n/m.*

Proof. By the previous corollary, subgroups have the form H/mZ where $mZ \leqslant H \leqslant Z$. But all subgroups of Z have the form, nZ for some $n \in Z^+$. So subgroups of Z/mZ has the form nZ/mZ where $nZ \leqslant mZ \iff n|m$. Note that nZ/mZ is generated by $n + mZ$ and therefore has order m/n. □

Note 1. The second and third isomorphism are consequences of the first isomorphism theorem when we have a subgroup $H \leqslant G$. If $N \trianglelefteqslant H \leqslant G$, we can construct 2 subsequent projections onto the quotient groups G/N and $\frac{G/N}{H/N}$ for the second theorem (note that $H/N \trianglelefteqslant G/N$). For the third H does not have to be a subgroup of N, we form an inclusion map form H to G then a projection onto the quotient group G/N.
More precisely, consider $N \trianglelefteqslant G$ as before and let $H \leqslant G$.

i. $\varphi : H \overset{i}{\hookrightarrow} G \longrightarrow G/N$
ii. If $N \trianglelefteqslant H \leqslant G$ then $H/N \trianglelefteqslant G/N$

$$\varphi \quad : \quad G \quad \overset{\pi_N}{\longrightarrow} \quad G/N \quad \overset{\pi_{H/N}}{\longrightarrow} \quad \tfrac{G/N}{H/N}$$

we apply the first isomorphism theorem for the following.

Theorem 8.4. *(Second isomorphism theorem.) Assume the definitions of ii. Then*

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

Proof. We use the first isomorphism theorem. note that

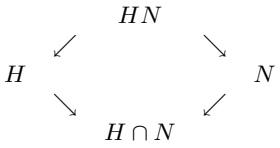
$$\begin{array}{rcccccc} \varphi & : & G & \xrightarrow{\pi_N} & G/N & \xrightarrow{\pi_{H/N}} & \frac{G/N}{H/N} \\ & : & g & \longmapsto & gN & & \end{array}$$

is surjective and π_N and $\pi_{H/N}$ are surjective also. We find $\ker(\varphi)$. Let $g \in \ker(\varphi)$, $gN \in \ker(\pi_{H/N}) = H/N \iff g \in H$, so $\ker(\varphi) = H$. By the first isomorphism theorem, $\frac{G/N}{H/N} = \operatorname{im}(\varphi) \simeq G/\ker(\varphi) = G/H$. □

Theorem 8.5. *(Third isomorphism theorem) Assume the definitions of i. recall that $N \lhd G$, $N \leqslant G$ so $HN \leqslant G$ and $H \cap N \trianglelefteq H$, we have the following*

$$H/H \cap N \simeq HN/N$$

Note: $H \supseteq N \implies HN = H$. A device for remembering this is the following Hasse diagram



Proof. We apply the first isomorphism theorem to

$$\begin{array}{rcccccc} \varphi & : & H & \xhookrightarrow{i} & G & \xrightarrow{\pi} & G/N \\ & : & h & \longmapsto & h & \longmapsto & hN \end{array}$$

Note that $\ker(\varphi) = \varphi^{-1}(N) = i^{-1}(N) = H \cap N \trianglelefteq H$, since $H \cap N$ is a kernel. We require $\operatorname{im}(\varphi) = \{hN : h \in H\} =: \tilde{H} \leqslant G/N$. From the corollary on subgroups of quotient groups

$$\tilde{H} = \pi^{-1}(\tilde{H})/N$$

$\pi^{-1}(\tilde{H}) = \{g : gN = hN, \text{for some } h \in H\} = \bigcup_{h\in H} hN = HN$. (This is necessary since H is not necessarily a subgroup of N) Therefore $\tilde{H} \leqslant G/N \implies HN = \pi^{-1}(\tilde{H}) \leqslant G$ and the first isomorphism theorem implies $HN/N = \pi(\tilde{H})/N = \operatorname{im}(\varphi) \simeq H/\ker(\varphi) = H/H \cap N$. □

9. Products

For groups G_1 and G_2 we wish to construct a bigger group G with a normal subgroup isomorphic to G_1 and $G/G_1 \simeq G_2$. Let I be an index set and G_i be a group for all $i \in I$.
Let $G = \prod G_i = \{(g_i)_{i\in I} : g_i \in G_i\}$. The key example would be $I = \{1 \dots n\}$, $G = G_1 \times G_2 \dots \times G_n = \{(g_1 \dots g_n) : g_i \in G_i\}$.

Proposition 9.1. *Endow G with a multiplication*

$$\begin{array}{rccc} \mu & : & G \times G & \longrightarrow & G \\ & & ((g_i),(g_i')) & \longmapsto & (g_i g_i')_{i\in I} \end{array}$$

Then G is a group called the product of the $G_i's$.

Proof. Check associativitiy. The identity is $1_G = (1_{G_i})_{i\in I}$, indeed $G \ni (g_i)(1_{G_i}) = (g_i 1_{G_i}) = 1_G(g_i)$. For inverse, we let $(g_i)^{-1} = (g_i^{-1})$, it is easy to see this works. □

Example 15. Let

$$G = \mathrm{GL}_n(C) \qquad D = \{\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} : d_i \in C^*\}$$

Claim $\varphi : D \xrightarrow{\sim} C^* \times \dots \times C^*$ n-times, $\varphi : \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \longmapsto (d_1 \dots d_n)$ is an isomorphism.

Proof. Clearly φ is bijective. We require check it is am homomorphism.

$$\begin{aligned}\varphi\left(\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}\begin{pmatrix} e_1 & & 0 \\ & \ddots & \\ 0 & & e_n \end{pmatrix}\right) &= \varphi\begin{pmatrix} d_1e_1 & & 0 \\ & \ddots & \\ 0 & & d_ne_n \end{pmatrix} \\ &= (d_1e_1\dots d_ne_n) \\ &= (d_1\dots d_n)(e_1\dots e_n)\end{aligned}$$

□

Example 16. Canonical injections and projections. Let I be an index set, G_i be a group $\forall i \in I$, $G = \prod_{i\in I} G_i$. consider the canonical maps,

1. Projection

$$\begin{array}{rccc} \pi_i & : & G & \longrightarrow & G_i \\ & & (g_k)_{k\in I} & \longmapsto & g_i \end{array}$$

2. Injection

$$\begin{array}{rccc} \iota_i & : & G_i & \longrightarrow & G \\ & & g & \longmapsto & (1,1,\dots g_i,\dots 1) \end{array}$$

Check that these are group homomorphisms. Consider the case where $G = G_1 \times G_2$, then we have

$$\begin{array}{rccc} \pi_2 & : & G & \longrightarrow & G_2 \\ & & (g_1,g_2) & \longmapsto & g_2 \end{array}$$

is an epimorphism, the first isomorphism theorem states that $G_2 \simeq G/\ker(\pi_2)$. The kernel is normal and $\ker(\pi_2) = \{(g_1,1) : g_i \in G\} = \mathrm{im}(\iota_1 : G_1 \longrightarrow G) \simeq G_1$. In other words, G has a normal subgroup isomorphic to G_1 whose quotient is G_2.

Proposition 9.2. *(Recognising products) Let G be generated by subgroups $G_1 \dots G_n$. Suppose also that*

1. *For $i \neq j$, $g_i \in G_1$, $g_j \in G_j$, $g_ig_j = g_jg_i$.*
2. *Suppose for any i,*

$$G_i \cap \langle G_i : j \neq i\rangle = 1$$

Then $\varphi : G_1 \times G_2 \dots \times G_n \xrightarrow{\sim} G$, $\varphi :\longmapsto (g_i)_{i\in I} \longmapsto \prod_{i\in I} g_i$.

Proof. Check that φ is an homomorphism

$$\begin{aligned}\varphi((g_i)_{i\in I}(g_i')_{i\in I}) &= \prod_{i\in I} g_ig_i' \\ &= \prod_{i\in I} g_i \prod_{i\in I} g_i'\end{aligned}$$

since elements of different G_i's commute. Note that φ is surjective, since the G_i's generate G. We require injectivity, i.e. $\ker(\varphi) = 1$. Let $(g_i)_{i\in I} \in \ker(\varphi)$, then $\prod_{i\in I} g_i = 1$, therefore $g_k^{-1} = \prod_{i\in I, i\neq k} g_k \in G_k \cap \langle G_j : j \neq k\rangle = 1 \Longrightarrow g_i = 1, \forall i \in I$. So $\ker(\varphi) = 1$ implies φ is bijective and hence an isomorphism. □

Definition 9.3. *Let G be a group then the exponent of G is the smallest positive integer, n, such that $g^n = 1, \forall g \in G$.*

Proposition 9.4. *Let G be any finite group. The order of any $g \in G$ divides $|G|$ hence the exponent n, divides $|G|$ as well.*

Proof. Consider $\langle g\rangle \leqslant G$. Lagrange's theorem implies $|\langle g\rangle||o(G)$ but $|\langle g\rangle| = o(g)$. The exponent is the l.c.m. of all $|\langle g\rangle|$ so divides $|G|$ too. □

Example 17. Any finite group G of exponent 2 is isomorphic to $Z/2Z \times Z/2Z \dots \times Z/2Z$.

Proof. G is finite implies G is finitely generated. We can pick a minimal set of generators and write $G = \langle g_i\rangle_{i=1}^n$. We require $G \simeq G_1 \times \dots \times G_n$ where $G_i = \langle g_i\rangle$ by applying the previous proposition. Note that g_i has order 2, since G has exponent 2, so $G_i \simeq Z/2Z$.
The G_i's generate G, since $G = \langle g_i\rangle_{i=1}^n$. G is commutative since its exponent is 2, for $a, b \in G$, $(ab)^2 = abab$. If 2. in proposition (recognising products) then $g_i \in \langle G_j : j \neq i\rangle = \langle G_j\rangle = G$, contradicting the minimality of n. Therefore 2 holds and $G \simeq Z/2Z \times Z/2Z \dots \times Z/2Z$. □

Theorem 9.5. *(Universal property of products.) Let I be an index set, G_i be a group $\forall i \in I$, $G = \prod_{i\in I} G_i$. Consider a group H and a homomorphism $\varphi_i : H \longrightarrow G_i$ for each $i \in I$. Then there is a unique group homomorphism $\varphi : H \longrightarrow G$ such that φ_i is the composite*

$$\begin{array}{rccccc} \varphi & : & H & \xrightarrow{\varphi} & G & \xrightarrow{\pi_i} & G_i \\ & & h & \longmapsto & \varphi(h) & \longmapsto & (\varphi(h))_i = \varphi_i(h) \end{array}$$

Proof. If the function φ satisfies the above relation, then φ must be

$$\begin{array}{rccccc} \varphi & : & H & \longrightarrow & G & = & \prod_{i\in I} G_i \\ & & h & \longmapsto & (\varphi_i(h)) & i \in I & \end{array}$$

We require the above is a homomorphism, this is easy to check. □

Remark 2. It is not difficult to show that any group with this universal property is a unique up to isomorphism. This leads to an alternative definition of products.

10. Classification of Isometries

Recall that an isometry is a function $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ such that

$$\|Ta - Tb\| = \|a - b\|$$

Example 18. For $v \in \mathbb{R}^n$, $T_v : \mathbb{R}^n \longrightarrow \mathbb{R}^n$,, $T_v : x \longmapsto x + v$ (translation by v) is an isometry.

Proposition 10.1. *Let $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be an isometry and $v = T(0)$. Then $T = T_v \circ T'$ where T' is an isometry with $T'(0) = 0$.*

Proof. Recall from lecture 1 that

$$T' = T_v^{-1} \circ T$$

is also an isometry (being composite of such) check

$$\begin{aligned} T'(0) &= T_v^{-1}(T(0)) \\ &= T(0) - v \\ &= 0 \end{aligned}$$

□

Theorem 10.2. *Let $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be an isometry with $T(0) = 0$, then T is linear so $T \in O_n$.*
Heuristic argument: recall from lecture that T is injective, also T is continuous. We check additivity and scalar multiplication.

Definition 10.3. *Consider a finte set $V = \{\boldsymbol{v}^i\}_{i=1}^m \subseteq \mathbb{R}^n$, the centre of mass of V is*

$$c(V) = \frac{1}{m}\sum_{i=1}^{m} \boldsymbol{v}^i$$

Proposition 10.4. *Consider the function*

$$\varepsilon_V(\boldsymbol{x}) = \sum_{i=1}^{m} \|\boldsymbol{v}^i - \boldsymbol{x}\|^2$$

$\varepsilon_V(\boldsymbol{x})$ attains a minimum at precisely 1 point, $\boldsymbol{x} = c(V)$.

Proof. Write $\boldsymbol{x} = (x_1, x_2 \dots x_n)$

$$\begin{aligned} \varepsilon_V(x) &= \sum_{i,j} (v_j^i - x_j)^2 \\ &= \sum_{i,j} ((x_j)^2 - 2v_j^i x_j + (v_j^i)^2) \\ &= \sum_{j} (m(x_j)^2 - x_j \left(2\sum_{i=1}^{m} v_j^i\right) + \sum_{i=1}^{m} (v_j^i)^2) \end{aligned}$$

Each (j-th) component is a quadratic in x_j, so the unique minimum occurs when,

$$x_j = \frac{1}{m}\sum_{i=1}^{m} v_j^i$$

i.e. $\boldsymbol{x} = c(V)$ □

Corollary 10.5. *Let $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be an isometry. Suppose $V = \{\boldsymbol{v}^i\}_{i=1}^m \subseteq \mathbb{R}^n$ is a finite set such that $T(V) = V$. Then $T(c(V)) = c(V)$*

Proof.

$$\begin{aligned}\varepsilon_V(T(c(V))) &= \sum_{\boldsymbol{v}^i \in V} \|\boldsymbol{v}^i - T(c(V))\|^2 \\ &= \sum_{\boldsymbol{v}^i \in V} \|T(\boldsymbol{v}^i) - T(c(V))\|^2 \\ &= \sum_{\boldsymbol{v}^i \in V} \|\boldsymbol{v}^i - c(V)\|^2 \\ &= \varepsilon_V(c(V))\end{aligned}$$

line 2 permutes the summands, so by uniqueness of previous proposition. $T(c(V)) = c(V)$ □

Symmetries of regular n-gons. Let F be a regular n-gon in $\mathbb{R}^2$, for $n \geqslant 3$, and G be the group of symmetries of F, i.e. isometries T of $\mathbb{R}^2$ such that $T(F) = F$, such that T preserve $V=$ the set of vertices.
For consistency, we pick coordinates so $c(V) = 0$ and so by corollary $T(0) = 0$ for any $T \in G$. Set the positve x-axis through the midpoint of some side. Label the vertices with $\{1 \dots n\}$, counterclockwise beginning from the positive x-axis.
Recall (from lecture 8) that this labelling induces a natural isomorphism

$$\psi : \Sigma(V) \xrightarrow{\sim} \Sigma_n$$

Each isometry $g \in G$ permutes the element set V giving a function

$$\begin{array}{rccl}\varphi & : & G & \longrightarrow & \Sigma(V) \\ & & g & \longmapsto & (g|_V : v \longmapsto gv)\end{array}$$

Proposition 10.6. *φ is a monomorphism (injective) and the composition*

$$G \xrightarrow{\varphi} \Sigma(V) \xrightarrow{\psi} \Sigma_n$$

gives an isomorphism of G with $\mathrm{im}(\psi \circ \varphi) = D_n \leqslant \Sigma_n$

Proof. We check that φ is an homomorphism, for $g, h \in G$ and $v \in V$

$$\begin{aligned}\varphi(gh)v &= \varphi(gh)|_V v \\ &= (gh)v \\ &= \varphi(g)v\varphi(h)v\end{aligned}$$

Let $g \in \ker(\varphi)$ so g fixes all the vertices, but $g \in O_2$ so $g = 1_{O_2} \implies \varphi$ is injective. Note that $\psi \circ \varphi$ is also injecive, so it induces an isomorphism of G with its image.
We now compute the $\mathrm{im}(\psi \circ \varphi)$. Let $s \in G$ be a rotation such that the vertices permute cyclically, and t be the reflection about the x-axis. We show that this generates G.
Let $g \in G$

$$\begin{array}{lllll}\det(g) = 1 & \implies & g \text{ is a rotation} & \implies & g = s^i \\ \det(g) = -1 & \implies & g \text{ is an improper rotation} & \implies & g = s^i t\end{array}$$

Recall that $D_n = \langle \sigma, \tau \rangle$ for $\sigma^n = 1$, $\tau^2 = 1$. Now note that

$$\begin{aligned}(\psi \circ \varphi)(s) &= \sigma \\ (\psi \circ \varphi)(t) &= \tau \\ (\psi \circ \varphi)(s^i t^j) &= \sigma^i \tau^j \\ \mathrm{im}(\psi \circ \varphi) &= D_n\end{aligned}$$

□

11. Abstract symmetry and group actions

Example 19. (Motivation) Consider the group of symmetries of a smiley face and the roman letter Z, (i.e. let $S_{:)}$ and S_Z be sets of points in $\mathbb{R}^2$). Both of these groups are isomorphic to $\mathbb{Z}/2\mathbb{Z}$, but clearly there is a fundamental difference between these symmetries. The group of symmetries only gives half the picture in a symmetry, we shall see a way to deal with this difference.

Definition 11.1. *Let G be a group. A G-set is a set S and a map*

$$\begin{array}{rccc} \alpha & : & G \times S & \longrightarrow & S \\ & & (g,s) & \longmapsto & \alpha(g,s) \\ & & & & := g \cdot s \end{array}$$

which satisfies

1. *For $s \in S$, $1 \cdot s = s$.*
2. *For $g, h \in G$, $s \in S$*

$$(gh) \cdot s = g \cdot (h \cdot s)$$

This map is called the group action, or the group operation. We also say that G acts or operates on S.

Example 20. Let $G = \mathbb{Z}/2\mathbb{Z} = \{1, \tau\}$, $(x,y) \in S_{:)} = \mathbb{R}^2$. We check that G satisfies the conditions above, (draw the smiley face, :), set the y-axis through the eyes, and the origin halfway between the eyes, τ acts via reflection about the x-axis)

$$\begin{array}{rcl} 1(x,y) & = & (x,y) \\ \tau_*^{i+j}(x,y) & = & (x,(-1)^{i+j}y) \\ & = & \tau_*^i(x,(-1)^j y) \\ & = & \tau_*^i(\tau_*^j(x,y)) \end{array}$$

So $S_{:)}$ is a G-set. Define $\alpha : G \times S \longrightarrow S$ by $\tau^i s = (-1)^i s$ since calculation shows that this is well defined and thus defines a group action.

Example 21. (Conjugation) Let $G = \mathrm{GL}_n(\mathbb{C})$ let $S = M_n(\mathbb{C})$, define $\alpha : G \times S \longrightarrow S$ by $A_* M = AMA^{-1}$. We check the axioms

$$\begin{array}{rcl} I \cdot M & = & M \\ (AB) \cdot (M) & = & A(BMB^{-1})A^{-1} \\ & = & A \cdot (B \cdot M) \end{array}$$

so S is a G-set.

Definition 11.2. *(Orbit) Let G be a group and S a G-set. Define a relation on S by $x \sim y$ iff $x = g_* y$ for some $g \in G$*

Proposition 11.3. *The above relation is an equivalence relation.*

Proof. 1. Reflexivity, $x = 1_* x \iff x \sim x$
2. Symmetry, $x \sim y \iff x = g_* y$ for some $g \in G \iff g_*^{-1} x = y \iff y \sim x$.
3. Transitivity, $x \sim y, y \sim z \iff x = g \cdot y, y = h \cdot z$ for some $g, h \in G \iff x = g \cdot (h \cdot z) = (gh) \cdot z \iff x \sim z$.

□

Corollary 11.4. *We call these equivalence classes of S G-orbits. A G-set S is thus a disjoint union of G-orbits. We write the G-orbit containing $s \in S$ by G_s.*

Note 2. When G is the conjugation map, we call the G orbits conjugacy classes.

Example 22. $G = \mathrm{SO}_3$ and $S = S^2$,

$$\begin{array}{rccc} a & : & G \times S & \longrightarrow & S \\ & & (A,v) & \longmapsto & v \end{array}$$

Consider $v, w \in S$ We can rotate v onto w, i.e. $\exists A \in \mathrm{SO}_3 = G$, such that $Av = w$. There is only 1 G-orbit, the whole of S. (If $S = R^3$, then the G-orbits of containing s are spheres of radius equal to $|s|$.)

Definition 11.5. *(Stabiliser) Let G be a group and S be a G-set, let $x \in S$, then the stabiliser of x is*

$$\mathrm{stab}(x) = \{g \in G : gx = x\} \subseteq G$$

Proposition 11.6. $\mathrm{stab}(x) \leqslant G$.

Proof. We check axioms. $1 \cdot x = x \Longrightarrow 1 \in \mathrm{stab}(x)$. Given $g, h \in \mathrm{stab}(x)$, then $(gh) \cdot x = g \cdot (h \cdot x) = x$, so $gh \in \mathrm{stab}(x)$. Given $g \in \mathrm{stab}(x)$, $g \cdot x = x \iff x = g^{-1} \cdot g \cdot x = g^{-1} \cdot x$ so $g^{-1} \in \mathrm{stab}(x)$. So $\mathrm{stab}(x) \leqslant G$.

□

Example 23. $G = \mathrm{SO}_3$ and S^2, for $x \in S^2$, $\mathrm{stab}(x)$ =rotations about the axis through $x, -x$.

Definition 11.7. *Homomorphisms of G-sets. Let G be a group, and $\varphi : S \longrightarrow S'$ be a function between 2 G-sets. φ is an homomorphism of G-sets if $\forall g \in G$, $s \in S$*

$$\varphi(g \cdot s) = g \cdot \varphi(s)$$

Proposition 11.8. *Let $\varphi : S \longrightarrow S'$ be a bijective homomorphism of G-sets, then φ^{-1} is also an homomorphism of G-sets. We call φ an isomorphism.*

Proof. Same as for isomorphism of groups. □

Example 24. $\mathrm{id} : S \longrightarrow S$ is an homomorphism.

Example 25. We now return to the motivating example. $S_{:)} = S_Z = \mathbb{R}^2$, these are G-sets, for $G = \mathbb{Z}/2\mathbb{Z}$, but they are not isomorphic, hence they represent different symmetries. To show this, suppose

$$\varphi : S_{:)} \longrightarrow S_Z$$

is an isomorphism of G-sets, then φ must preserve fixed points. i) Suppose $x_0 \in S_{:)}$ such that $g_* x_0 = x_0, \forall g \in G$. So $\varphi(g \cdot x_0) = g \cdot \varphi(x_0) \Longrightarrow \varphi(g \cdot x_0) = \varphi(x_0) = g \cdot \varphi(x_0)$, $\varphi(x_0)$ must be a fixed point of S_Z w.r.t. G.
$S_{:)}$ has fixed points along the x-axis and S_Z has a fixed point through the centre of rotation, so there exists no G-set isomorphism between $S_{:)}$ and S_Z.

12. Classification of G-orbits

Definition 12.1. *Suppose $\varphi : S \longrightarrow S'$ is a homomorphism of G-sets, φ is also called a G-equivariant map or one compatible with the group action.*

Note 3. For the rest of this section G will be a group, and X will be a G-set, where there is no ambiguity or indicated otherwise.

Proposition 12.2. *$Y \subseteq X$ is said to be G-stable or a G-subset (G-invariant) if for any $g \in G$, $y \in Y$*

$$g \cdot y \in Y$$

In this case Y inherits from X the structure of a G-set.

Proof. check axioms of subgroups □

Example 26. Any G-orbit

$$Gx = \{g \cdot x | g \in G\} \in X$$

is G-stable. Reason: For $g, g' \in G$, $g \cdot (g' \cdot x) = (gg') \cdot x \in Gx$, therefore Gx is a G-orbit.

Definition 12.3. *We say the group action of G on X is transitive if X is a single orbit.*

Example 27. From last lecture $G = \mathrm{SO}(3)$, and $X = S^2$. The action

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (A, x) & \longmapsto & Ax \end{array}$$

is a group action, the action is transitive as there is only 1 orbit.

The G-set G/H
Let $H \leqslant G$ We can make G/H into a G-set, by defining a group action by $g' \cdot (gH) := g'gH$. We check axioms quickly.

i. $1 \cdot (gH) = gH$
ii. For $g_1, g_2 \in G$, $g_1 \cdot (g_2 \cdot gH) = g_1 \cdot (g_2 gH) = g_1 g_2 gH = (g_1 g_2) \cdot gH$.
iii. Note that $\cdot$is well defined as it is the set product.

Theorem 12.4. *(Classification of G-orbits) Suppose the action of G on X is transitive. Let $x \in X = Gx$. There is a well defined isomorphism of G-sets.*

$$\begin{array}{rccc} \varphi & : & G/H & \longrightarrow & X \\ & & gH & \longmapsto & g \cdot x \end{array}$$

where $H = \mathrm{stab}(x)$. Conversely, every G/H is a G-orbit. (every G-orbit of the form Gx is isomorphic to $G/\mathrm{stab}(x)$)

Proof. We firstly check this is well defined. Let $h \in H$.

$$\begin{aligned}\varphi(g) &= g \cdot x \\ &= g \cdot (h \cdot x) \\ &= (gh) \cdot x\end{aligned}$$

We check G-equivariance, let $g, g' \in G$

$$\begin{aligned}g' \cdot \phi(gH) &= g' \cdot (g \cdot x) \\ &= (g'g) \cdot x \\ &= \varphi(g'gH) \\ &= \varphi(g' \cdot gH)\end{aligned}$$

Surjectivity is clear. We check injectivity. Suppose $\varphi(gH) = g \cdot x = \varphi(g'H) = g' \cdot x$, $g^{-1} \cdot (g' \cdot x) = g^{-1} \cdot g \cdot x = 1$. Therefore $g^{-1}g' \in \operatorname{stab}(x) = H$, so $g' \in g'H$. $g'H = gH$ so φ is injective. The converse is clear. □

Proposition 12.5. *Suppose $x \in X, g \in G$, then $\operatorname{stab}(g \cdot x) = g(\operatorname{stab}(x))g^{-1}$.*

Proof. It suffices to prove $\supseteq$, since applying this result to $g \cdot x$, g^{-1}, giving

$$\begin{array}{ll}\operatorname{stab}(g^{-1} \cdot (g \cdot x)) & \supseteq \; g^{-1} \operatorname{stab}(g \cdot x) g \\ g \operatorname{stab}(x) g^{-1} & \supseteq \; \operatorname{stab}(g \cdot x)\end{array}$$

which is the reverse inclusion. Let's prove $\supseteq$. Let $h \in \operatorname{stab}(x)$

$$\begin{aligned}(ghg^{-1})(g \cdot x) &= (ghg^{-1}g) \cdot x \\ &= g \cdot (h \cdot x) \\ &= g \cdot x\end{aligned}$$

□

13. Application to platonic solids

A platonic solid, X, is a solid such that all faces are congruent to some fixed regular polygon and the same number of faces meet at each vertex. There are 5 such solids.

T	:=	tetrahedron	4 triangular faces
C	:=	cube	6 square
O	:=	octahedron	8 triangular
D	:=	dodecahedron	12 pentagonal
I	:=	isocahedron	20 triangular

Definition 13.1. *Let X be a platonic solid and assume in $\mathbb{R}^3$ with centre of mass at $\mathbf{0}$. The rotational symmetric group consists of those symmetries which are (exclusively) in $\mathrm{SO}(3)$, i.e. the proper rotations.*

Corollary 13.2. *(..to classification theorem) Let G be the rotational symmetry group of X (a platonic solid). Then $|G| = (f)(s)$, where f is the number of faces of X, and s is the number of sides of X, i.e.*

	T	C	O	D	I
$\lvert G\rvert$	12	24	24	60	60

Proof. Let $F = \{F_i\}_{i=1}^f$ be the faces of X, G permutes these faces giving a G-set, namely, for $T \in G, T \cdot F_i := T(F_i)$. Exercise: check that this is a G-set. Note that this action is transitive (one can rotate any face onto another). Therefore $F = G \cdot F$. Let l be the axis through the centre of F_1. $\operatorname{stab}(F_1)$ =rotations in G about $l \simeq \mathbb{Z}/s\mathbb{Z}$ (spin each of the edges around), so $|\operatorname{stab}(F_1)| = s$. The classification theorem implies $F \simeq G/\operatorname{stab}(F)$,

$$\begin{aligned}|F| &= |G/\operatorname{stab}(F_1)| \\ &= |G|/|\operatorname{stab}(F_1) \\ &= |G|/s \\ sf &= |G|\end{aligned}$$

as required. □

Remark 3. Turns out, rotational symmetry groups are

	T	C	O	D	I
G	$4!/2$	$4!$	$4!$	$5!/2$	$5!/2$
$\|G\|$	A_4	S_4	S_4	A_5	A_5

Counting number of orbits and permutation representations
Let G be a group and X be a G-set.

Definition 13.3. *Let $J \subseteq G$ the fixed point set of J is defined as*

$$X^J = \{x \in X | g \cdot x = x, \forall g \in J\} \subseteq X$$

Proposition 13.4. *If $H = \langle J \rangle$, then $X^J = X^H$.*

Theorem 13.5. *(Number of orbits) Let G be a finite group, and X be a finite G-set. Then the number of orbits in X is*

$$n = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Proof. Suppose $X = \bigcup X_i$, is the disjoint union of G-stable subsets of X_i.

$$l.h.s = \sum_i \text{number of orbits of } X_i$$

since $X^g = \bigcup X_i^g$.

$$r.h.s = \sum_i \frac{1}{|G|} \sum_{g \in G} |X_i^g|$$

It suffices to prove equality for X_i's. Now X is a disjoint union of G-orbits and these are isomorphic to G-sets of the form G/H, so w.l.o.g. we let $X_i = G/H$, for some $H \leqslant G$.

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} |X_i^g| &= \frac{1}{|G|} |\{(g, x) \in G \times X_i | g \cdot x = x\}| \\ &= \frac{1}{|G|} \sum_{x \in G/H} |\operatorname{stab}(x)| \end{aligned}$$

this is analogous to switching the sum over G to over $X_i \simeq G/H$. Note that the action is transitive, so a previous proposition implies $\operatorname{stab}(x)$ are all conjugate to each other, hence, $\operatorname{stab}(1 \cdot H) = H$.

$$\begin{aligned} &= \frac{1}{|G|} \sum_{x \in G/H} |H| \\ &= \frac{1}{|G|} |G/H| \cdot |H| \\ &= 1 \\ &= \text{number of orbits of } G/H \end{aligned}$$

this gives the theorem. □

Example 28. (Cake) In each of 8 equal sectors, we place a white or orange candle at centre. How many different ways are there of doing this? (two arrangements are the same if we can rotate the cake to get the other). Formulation: Let $G = \langle \sigma \rangle = \mathbb{Z}/8\mathbb{Z}$, $X = (\mathbb{Z}/2\mathbb{Z})^8$. Define a group action by

$$\sigma \cdot (x_1 \dots x_8) = (x_2 \dots x_8, x_1)$$

Check that this makes X a G-set. The question becomes, how many orbits are there? Using the above theorem. n =number of orbits= $\frac{1}{|G|}\sum_{\sigma^i\in G}|X^{\sigma^i}|$

$$\begin{aligned}
X^1 &= X\\
|X^1| &= 2^8\\
|X^\sigma| &= |\{(x_1\dots x_8)|x_1=0,1,\text{all } x_i=x_j\}|\\
&= 2\\
|X^{\sigma^2}| &= |\{(x_1\dots x_8)|x_1,x_2=0,1,x_{2i}=x_2,x_{2i+1}=x_1\}|\\
&= 4\\
|X^{\sigma^3}| &= 2\\
|X^{\sigma^4}| &= 2^4\\
|X^{\sigma^5}| &= 2\\
|X^{\sigma^6}| &= 4\\
|X^{\sigma^7}| &= 2\\
n &= \frac{1}{|G|}\sum_{\sigma^i\in G}|X^{\sigma^i}|\\
&= \frac{1}{2^3}(2^8+2+4+2+2^4+2+4+2)\\
&= 36
\end{aligned}$$

14. Permutation Representations

Definition 14.1. *Let G be a group, X be a set. A premutation representation is a group homomorphism*

$$\varphi : G \longrightarrow \Sigma(X)$$

There is a 1:1 correspondence between G-sets and permutation representations, which is as follows.

Permutation representation -set.
Let $\varphi : G \longrightarrow \Sigma(X)$ be an homomorphism. Define a corresponding G-set as a set X with its group action defined by

$$\begin{array}{ccc} G\times X & \longrightarrow & X\\ (g,x) & \longmapsto & \varphi(g)x\end{array}$$

We check the axioms

1. $1\cdot x=\varphi(1)x=\mathrm{id}\,x=x$.
2. Associativity. For $g,g'\in G, x\in X$, $g'(gx)=\varphi(g')(\varphi(g)x)=\varphi(g')\varphi(g)x=\varphi(g'g)x$.

So X is a G-set.
G-set$\longrightarrow$Permutation representation
Suppose X is a G-set, we require a group homomorphism,

$$\begin{array}{ccccc}\varphi & : & G & \longrightarrow & \Sigma(X)\\ & & g & \longmapsto & \varphi(g)\end{array}$$

Let $\varphi(g)$ be defined by

$$\begin{array}{ccccc}\varphi(g) & : & X & \longrightarrow & X\\ & & x & \longmapsto & g\cdot x\end{array}$$

We require $\varphi(g)\in\Sigma(X)$. $\varphi(g)$ has inverse $\varphi(g^{-1})$, since $\varphi(g^{-1})\varphi(g)\cdot x=g^{-1}\cdot(g\cdot x)=x$. So $\varphi(g)\varphi(g^{-1})=\mathrm{id}$. We now check φ is a homomorphism. Suppose $g,g'\in G$, $x\in X$

$$\begin{aligned}\varphi(g'g)x &= (g'g)\cdot x\\ &= g'\cdot(g\cdot x)\\ &= \varphi(g)(\varphi(g')x)\end{aligned}$$

Therefore φ is a permutation representation. Exercise: check these constructions are inverses of each other. The key to the correspondence is $g\cdot x=\varphi(g)x$.

Example 29. Refer to alglec7.tm, smiley face example. Consider the G-set, $S_{:)}$, $G=\{1,\sigma\}\simeq\mathbb{Z}/2\mathbb{Z}$. $\varphi(x,y)^T=(x,-y)^T$, $1(x,y)^T=(x,y)^T$. We seek the corresponding permutation representation. The

composition

$$\begin{array}{ccccc} G & \longrightarrow & \mathrm{GL}_2(\mathbb{R}) & \longrightarrow & \Sigma(\mathbb{R}) \\ 1 & \longmapsto & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & & \\ \varphi & \longmapsto & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & & \end{array}$$

We check the action of φ

$$\begin{aligned} \varphi(x,y) &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= (x,-y) \end{aligned}$$

Definition 14.2. *A permutation representation $\varphi : G \longrightarrow \Sigma(X)$ is faithful if φ is injective.*

Theorem 14.3. *(Cayley) Let G be a finite group, then G is isomorphic to a subgroup of $\Sigma(G)$, (i.e. if $n = |G| < \infty$, then G is isomorphic to Σ_n??).*

Proof. Consider G-set, $G(= G/H \text{ with } H = 1)$ gives premutation representation

$$\varphi : G \longrightarrow \Sigma(G)$$

It suffices to check φ is faithful by the first isomorphism theorem. Let $g \in \ker(\varphi)$. $g = g \cdot 1 = \varphi(g) \cdot 1 = \mathrm{id}\, 1 = 1$. Thereofore $\ker(\varphi) = 1$ so φ is injective. The first isomorphism theorem gives correspondence with a subgroup of $\Sigma(G)$. □

15. Finite groups of isometries

Let (A for affine) $A\,\mathrm{GL}_n$ =set of isometries of $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ of $\mathbb{R}^n = V$. $A\,\mathrm{GL}_n \subseteq \Sigma(V)$. Let $G \leqslant A\,\mathrm{GL}_n$ be a finite subgroup. The inclusion homomorphism $G \hookrightarrow \Sigma(V)$ defines a permutation representation. The corresponding G-set V, has action, $T \in G, x \in V = \mathbb{R}^n$, $T \cdot x = T(x)$.

Proposition 15.1. *Let finite $G < A\,\mathrm{GL}_n$ act on V as above. Then V^G is nonempty and changing coordinates so that a fixed point is 0, we see that G is isomorphic to a subgroup of O_n.*

Proof. Consider any G-orbit $F = Gv$. F is finite so G fixes the centre of mass c of F, therefore $c \in V^G$. From previous lecture, any isometry T with $T(0) = 0$ is linear, so G is isomorphic to a subgroup of O_n. □

Theorem 15.2. *Let $G < O_2$ be finite, then G is either cyclic or dihedral (recall $D_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$)*

Proof. Let $H = \mathrm{SO}_2 \cap G$. We claim that H is cyclic. H is a finite subgroup of SO_2 =set of proper rotations in the plane. Let $h \in H$ be a rotation by θ such that θ is minimally positive. Suppose $h' \in H$ rotates by θ' where $n\theta \leqslant \theta' < (n+1)\theta$ for some $n \in \mathbb{Z}$. Note that $h'h^{-n}$ rotates by $0 \leqslant \theta' - n\theta < \theta$ Minimality of θ implies that $\theta' - n\theta = 0$, so $h' = h^n \iff H = \langle h \rangle$ is cyclic.
Suppose $G \nsubseteq \mathrm{SO}_2$, let $\tau \in G - \mathrm{SO}_2$, note that $\mathrm{SO}_2 \lhd O_2$ since $[O_2 : \mathrm{SO}_2] = 2$. The third isomorphism theorem implies

$$\frac{G}{H} = \frac{G}{G \cap \mathrm{SO}_2} \simeq \frac{(G)(\mathrm{SO}_2)}{\mathrm{SO}_2} \leqslant \frac{O_2}{\mathrm{SO}_2} = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$$

Since $H \neq G$, $G/H \simeq \mathbb{Z}/2\mathbb{Z}$, therefore $G = H \cup \tau H$. Now τ is a reflection in $O_2 - \mathrm{SO}_2$. Changing coordinates such that this is a reflection about the x-axis. Consider a regular n-gon, H is a cyclic group of rotations of the n-gon. So G is the set of $2n$ symmetries of the regular n-gon. Therefore $G \simeq D_{2n}$, at least for $n \geqslant 3$. Exercise: check the degenerate case, $n = 2$. □

Definition 15.3. *Poles. Let $G < \mathrm{SO}_3$ be finite. Consider a G-set $\mathbb{R}^2 = V$. Note that $W = S^2$ be the unit sphere in $\mathbb{R}^3$ is a G-stable subset. A point $x \in W$ is a pole if $\mathrm{stab}(x) \neq 1$. The set $X \subset R^3 = V$ of poles is G-stable since for $x \in X$, $g \in G$, $\mathrm{stab}(g \cdot x) = g\,\mathrm{stab}(x)g^{-1} \neq 1$.*

Theorem 15.4. *The finite subgroups of SO_3 are the cyclic groups, dihedral groups, or the rotational groups of symmetries of a Platonic solids.*

Proof. We prove the case for platonic solids. Let G be the group of rotational symmetries of the Platonic solid S with centre of mass $\mathbf{0}$. It seems we have poles through the centres of opposite faces, opposite vertices, and midpoints of opposite edges. Note that for $x \in X$, $\mathrm{stab}(x)$ is a cyclic group of rotations about the axis $\{\pm x\}$. So it is reasonable to surmise that the 3 orbits correpsond to $\{\text{face poles}\}$, $\{\text{edge poles}\}$, and $\{\text{vertex poles}\}$. We also require the concept of duality (draw a picture :¿), which maps faces to vertices of dual solids. Since an isometry of a Platonic solid preserves the centres of faces, the rotational symmetry groups of dual solids are isomorphic.

Let $G < \mathrm{SO}_3$ be finite, $X = G$-set of poles. From last lecture we have a formula for the number of orbits, r. Suppose $X = Gx_1 \cup Gx_2 \cup \ldots \cup Gx_r$, then

$$\begin{aligned}
r &= \frac{1}{|G|}\sum_{g\in G}|X^g| \\
X^g &= \begin{cases} X & \text{if} \quad g = 1 \\ \text{pair of poles of } g & \text{if} \quad g \neq 1 \end{cases} \\
r &= \frac{1}{|G|}((|G|-1)2 + |X|) \\
&= \frac{1}{|G|}\left((|G|-1)2 + \sum_{i=1}^{r}|Gx_i|\right) \\
&= \left(\left(1-\frac{1}{|G|}\right)2 + \sum_{i=1}^{r}\frac{1}{|\operatorname{stab}(x)|}\right) \\
2-\frac{2}{|G|} &= r - \sum_{i=1}^{r}\frac{1}{|\operatorname{stab}(x)|} \\
&= \sum_{i=1}^{r} 1 - \frac{1}{|\operatorname{stab}(x)|} \\
1-\frac{1}{|\operatorname{stab}(x)|} &> 1-\frac{1}{2} = \frac{1}{2} \\
\text{so } r &\leqslant 3
\end{aligned}$$

$r \neq 1$, since the formula above fails. If $r = 2$, then G is cyclic. Since

$$\begin{aligned}
r &= \frac{1}{|G|}((|G|-1)2 + |X|) \\
2 &= 2 - \frac{2}{|G|} + \frac{|X|}{|G|} \\
|X| &= 2
\end{aligned}$$

therefore there are only 2 poles, say $\pm x$, G mmust be some cyclic group of rotations about the axis $x, -x$. For $r = 3$, let $n_i = |\operatorname{stab}(x)|$, the equation bounds the n_i's as follows.
If $n_1 \leqslant n_2 \leqslant n_3$, (n_1, n_2, n_3) is a Platonic triple, i.e. (we require $|G| \in \mathbb{Z}^+$)

a. $(2, 2, n) \quad n \geqslant 2$
b. $(2, 3, 3)$
c. $(2, 3, 4)$
d. $(2, 3, 5)$

We examine case *d*, $(n_1, n_2, n_3) = (2, 3, 5) \iff |G| = 60$. Let us consider $Gx_3 \simeq G/\operatorname{stab}(x_3)$. $|Gx_3| = \frac{60}{n_3} = 12$ =number of vertices of isocahedron I. The claim is Gx_3 are the vertices of the same I.

$$\operatorname{stab}(x_3) \quad \simeq \quad \mathbb{Z}/5\mathbb{Z} \quad = \quad \langle g\rangle$$

since $g \in \operatorname{stab}(x_3)$. If $y \in Gx_3 - \{\pm x_3\}$, then we get distinct $\{y, g(y), \ldots, g^4(y)\}$. But $|Gx_3| = 12$. the only possible configuration for Gx_3 is as in picture ... so

$$Gx_3 = \{\pm x_3, y, g(y), \ldots, g^4(y), z, g(z), \ldots g^4(z)\}$$

the corners of an isocahedron. Note that $\|x_3 - y\| < \|x_3 - z\|$, and $\|x_3 - y\| = \|x_3 - g(y)\| = \ldots = \|x_3 - g^4(y)\|$. This correpsonds to saying 'adjacent' vertices are the same distance apart. Since x_3 can be an arbitrary element of Gx_3, this will show adjacent vertices are the same distance apart. From the picture we see 5 equilateral triangles meet at each vertex. Therefore Gx_3 is the set of vertices of an isocahedron I, and G is a subgroup of rotational symmetries of I since Gx_3 is G-stable, but $|G| = 60$ and the group of rotational symmetries of I is 60, the equality holds.
For case *c*, $(n_1, n_2, n_3) = (2, 3, 4)$, the formula implies $|G| = 24$.

$$|Gx_3| = |G/\operatorname{stab}(x_3)| = 6$$

Suppose $\langle g\rangle = \operatorname{stab}(x_3) = \mathbb{Z}/4\mathbb{Z}$. Symmetry implies for y on the equator, we can see as before, that Gx_3 is the set of vertices of an octahedron O, and G is a group of rotational symmetries of G.
For case *b*, $(n_1, n_2, n_3) = (2, 3, 3)$, the formula implies $|G| = 12$.

$$|Gx_3| = |G/\operatorname{stab}(x_3)| = 4$$

Suppose $\langle g\rangle = \operatorname{stab}(x_3) = \mathbb{Z}/3\mathbb{Z}$. Check that we have a tetrahedron, as before.

For case a, $(n_1, n_2, n_3) = (2, 2, n)$. Assume $n > 2$ to avoid the non degenerate case, the formula implies $|G| = 2n$. Consider $Gx_3 \simeq G/\operatorname{stab}(x_3)$

$$|Gx_3| = |G/\operatorname{stab}(x_3)| = \frac{2n}{n} = 2$$

$\operatorname{stab}(x_3) = \langle\sigma\rangle \simeq \mathbb{Z}/n\mathbb{Z}$, let $y \in Gx_3 - \{\pm x_3\}$, then $Gx_3 \supset \{\pm x_3, y, g(y)\ldots\}$, but $|Gx_3| = 2$, so we are left with $Gx_3 = \{\pm x_3\}$. Consider $Gx_2 \simeq G/\operatorname{stab}(x_2)$

$$|Gx_2| = |G/\operatorname{stab}(x_2)| = \frac{2n}{2} = n$$

$\operatorname{stab}(x_2) = \langle\tau\rangle = \{1, \tau\}$. Now $\tau(x_3) \in Gx_3 = \{\pm x_3\}$, implying x_2 is on the equator w.r.t. the poles $x_3, -x_3$ since $G(x_3) = \{\pm x_3\}$. Similarly x_1 is on the equator as well. $\operatorname{stab}(x_3)$ is a group of order index 2

$$\begin{aligned} G &= \langle\sigma\rangle \cup \tau\langle\sigma\rangle \\ &= \text{symmetries of the } n-\text{gon}, \{x_2, g(x_2), \ldots, g^{n-1}(x_2)\} \end{aligned}$$

exercise: check the degenerate case, $n = 2$.
This finishes the proof of the theorem. □

Lemma 15.5. *The formula* $r = \frac{1}{|G|}\left((|G| - 1)2 + |X|\right)$ *and* $r = 3$ *implies* $(n_1, n_2, n_3) \in \{(2, 2, n), (2, 3, 3), (2, 3, 4), (2, 3, 5)\}$.

Proof. The formula implies

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} > 1$$

if $n_3 \geqslant 6$

$$\begin{aligned} \frac{1}{n_1} + \frac{1}{n_2} &> 1 - \frac{1}{6} \\ &= \frac{5}{6} \\ &= \frac{1}{2} + \frac{1}{3} \\ n_1 = n_2 &= 2 \end{aligned}$$

if $n_3 = 3, 4, 5$.

$$\begin{aligned} \frac{1}{n_1} + \frac{1}{n_2} &> 1 - \frac{1}{6} \\ &= 1 - \frac{1}{3} \\ &= \frac{2}{3} \end{aligned}$$

finish as exercise.. □

16. Class equation and conjugacy

Aim: study of groups via symmetry. Let $\operatorname{Aut}(G)$ be the set of automorphisms of G, $\operatorname{Aut}(G) \subseteq \operatorname{Perm}(G)$.

Proposition 16.1. $\operatorname{Aut}(G) \leqslant \operatorname{Perm}(G)$. *Proof is trivial.*

Definition 16.2. *Let $g, h \in G$. Define $C_g(h) = ghg^{-1}$, called conjugation by g. Recall that $C_g : G \longrightarrow G$ is an automorphism of G. If $H \leqslant G$, then $C_g(H) = gHg^{-1}$ is a subgroup of G, called a conjugate of H.*

Proposition 16.3. *The canonical map $C : G \longrightarrow \operatorname{Aut}(G)$ is a group homomorphism.*

Proof. For $g_1, g_2, h \in G$, $C_{g_1g_2}(h) = g_1g_2hg_2^{-1}g_1^{-1} = C_{g_1}(g_2hg_2^{-1}) = C_{g_1}C_{g_2}(h)$ for all h. □

Consider the composite group homomorphism

$$G \xrightarrow{C} \operatorname{Aut}(G) \xhookrightarrow{\iota} \operatorname{Perm}(G)$$

this defines a permutation representation. The corresponding G-set is G with action defined by (for $g, g' \in G$)

$$g \cdot g' = C_g(g') = gg'g^{-1}$$

we say the group G acts on itself by conjugation.

Definition 16.4. *Let G act on G by conjugation. The G-orbits are called conjugacy classes, which we denote by $G \cdot x$ to distinguish it from Gx. The set of fixed points is called the centre, denoted, $Z = Z(G)$.*

Note 4. We can write the centre as

$$\begin{aligned} Z(G) &= \{z \in G \mid gzg^{-1} = z, \text{for any } g \in G\} \\ &= \{z \in G \mid |G \cdot z| = 1\} \\ &= \{z \in G \mid gz = zg, \text{for any } g \in G\} \\ &= \{z \in G \mid g = zgz^{-1} = C_z(g), \text{for any } g \in G\} \\ &= \{z \in G \mid C_z = \mathrm{id}\} \\ &= \ker(C : G \longrightarrow \mathrm{Aut}(G)) \end{aligned}$$

Corollary 16.5. *$Z(G) \trianglelefteq G$ and $Z(G) = G$ iff G is abelian.*

Example 30. What is the centre of $G = \mathrm{GL}_2(\mathbb{R})$?

Proof. The claim is $Z(G) = \{aI | a \in \mathbb{R}^*\}$. Note that $\supseteq$ holds. Suppose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z$. We know that $AB = BA$ for any $B \in G$ and by continuity it is true for any 2×2 real B. Sub in $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} &= \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 0 \\ d & b \end{pmatrix} \end{aligned}$$

so $a = d$, and A is scalar so the claim is true. □

Definition 16.6. *(Class equation) Let (finite) G act on itself by conjugation. Decomposition into orbits gives*

$$G = Z \dot\cup G \cdot x_1 \dot\cup \ldots \dot\cup G \cdot x_r$$

where $G \cdot x_i$ are orbits with $|G \cdot x_i| > 1$. Note that these are disjoint unions. Using the classification of orbits, and the disjoint union, we have

$$|G| = |Z| + \sum_{i=1}^{r} \frac{|G|}{|\operatorname{stab}(x_i)|}$$

Definition 16.7. *(p-group and Sylow p-group) A group H is said to be a p-group, where p is a prime, if the $o(H)$ is a power of p. Suppose G is a finite group with $|G| = p^l q$ and $\gcd(p, q) = 1$. Then $H \leqslant G$ is said to be a Sylow p-subgroup if $|H| = p^l$. I.e. a Sylow p-subgroup G is a maximal p group of G.*

Example 31. The conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

Proposition 16.8. *Let H be a nontrivial ($H \neq 1$) p-group, then $Z(H) \neq 1$.*

Proof. (by class equation)

$$|H| = |Z| + \sum_{i=1}^{r} \frac{|H|}{|\operatorname{stab}(x_i)|}$$

p divides $|H|, |\operatorname{stab}(x_i)|$ by Lagrange's theorem, and in fact $\frac{|H|}{|\operatorname{stab}(x_i)|} \neq 1$. Therefore $p||Z|$ and $Z(G) \neq 1$. □

Corollary 16.9. *Suppose p is prime, then if $|G|$ is*

a) *p, then $G \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. Let $g \in G - \{1\}$, Lagrange's theorem implies $|\langle g\rangle| \mid p$ therefore $p = |\langle g\rangle|$. So $G = \langle g\rangle$ is cyclic, hence $G \simeq \mathbb{Z}/p\mathbb{Z}$. □

b) *p^2, then $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proof. Suppose $G \ncong \mathbb{Z}/p^2\mathbb{Z}$, let $z \in Z(G) - \{1\}$ (exists by proposition). We assumed $\langle z\rangle \neq G$ so Lagrange's theorem implies $|\langle z\rangle| = p$, so $\langle z\rangle \simeq \mathbb{Z}/p\mathbb{Z}$. Let $x \in G - \langle z\rangle$, again by the same argument, $\langle x\rangle \simeq \mathbb{Z}/p\mathbb{Z}$.

Claim $G \simeq \langle z\rangle \times \langle x\rangle$. It suffices to check criterion for products from lecture 12

- Since $\langle z\rangle < Z(G)$, elements of $\langle z\rangle$ and $\langle x\rangle$ commute.
- $|\langle z,x\rangle| > |\langle z\rangle| + 1 = p+1$. Lagrange's theorem implies $|\langle z,x\rangle| = p^2$, then z, x generates G, i.e. $\langle z,x\rangle = G$
- Lagrange's theorem implies $|\langle z\rangle \cap \langle x\rangle| = 1$ so $\langle z\rangle \cap \langle x\rangle = 1$. Proposition from lecture 12 implies $G \simeq \langle z\rangle \times \langle x\rangle$ we should check that $\langle z\rangle \times \langle x\rangle \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

□

Theorem 16.10. *(Sylow) Let G be a group of order $p^l q$ with p prime and $\gcd(p,q) = 1$, let $\mathrm{Cl}(K)$ denote the conjugacy class of $K \subseteq G$, and $\mathrm{Syl}_p(G)$ be the collection of all Sylow p-subgroups of G.*

1. *$\mathrm{Syl}_p(G)$ is nonempty, suppose $P \in \mathrm{Syl}_p(G)$.*
2. *Let $H \leqslant G$ be a p-subgroup, then it is contained in a conjugate of P. In particular, $\mathrm{Cl}(P) = \mathrm{Syl}_p(G)$, and hence the members of $\mathrm{Syl}_p(G)$ isomorphic.*
3. *Let $m = |\mathrm{Syl}_p(G)|$, then $m | o(G)$ and $m = 1 + kp$ for some $k \in \mathbb{N}$.*

Example 32. Let p be prime and $G = D_p = \langle \sigma, \tau\rangle$ with $\sigma^p = \tau^2 = 1$, $\tau\sigma = \sigma^{-1}\tau$. Then the only Sylow p-subgroup is $\langle\sigma\rangle$, the Sylow 2-subgroups are $\langle\tau\rangle, \langle\tau\sigma^i\rangle$.

17. Proof of Sylow's theorem

Proof. Recall that $|G| = p^l q$, and $\gcd(p,q) = 1$.

1. Let $X = \{A \subseteq G \mid |A| = p^l\}$, then $|X| = \binom{p^l q}{p^l}$. Let G act on X by left translation, check that this makes X a G-set.

   Lemma 17.1. *$p \nmid |X|$.*

   Proof. For $i \in \{1 \dots p^l\}$ the same powers of p divides i as divides $p^l q - i$,
   $$\binom{p^l q}{p^l} = \frac{(p^l q)!}{(p^l(q-1))! p^l!}$$
   □

   Write X as its orbit decomposition $X = \dot{\bigcup} G \cdot X_i$, and by above, there exists X_i such that $p \nmid |G \cdot X_i|$. The claim is that $P = \mathrm{stab}(X_i)$ is a Sylow p-subgroup.
   - $p \nmid |G \cdot X_i|$, and $|G \cdot X_i| = |G|/|P| = p^l q/|P|$ implies $p^l \mid |P|$, since $|P|$ has to kill the p^l factor.
   - Let $x \in X_i$ then $Px \subseteq PX_i = X_i$. Therefore $|P| \leqslant |X_i x^{-1}| = p^l$, containment gives equality then P is a Sylow p-subgroup. (or the fact that $|G|/|P|$ is an integer.)
2. We have to show that all Sylow p-subgroups are conjugate, with $|P| = p^l$, and maximal.

   Lemma 17.2. *Let H be a p-group acting on a set S. Then $p \mid |S| - |S^H|$*

   Proof. First note that $|S| - |S^H| = |S - S^H|$. S^H is the fixed point group of H in S. $S - S^H$ is the set of all points not fixed by H, so is an orbit, which we denote $H\, s_i$. By classification of orbits, this is isomorphic to $H/\mathrm{stab}(s_i)$. Lagrange's theorem implies $p \mid |H/\mathrm{stab}(s_i)|$ therefore $p \mid |S - S^H|$. □

   Let $H \leqslant G$ be a p-group, and P a Sylow p-subgroup. Consider H-set G/P where the action is given by left translation,
   $$h \cdot gP = hgP$$
   for $h \in H, g \in G$. Check that this is an H-set. $|G/P| = p^l q/p^l = q$ so $p \nmid |G/P|$, the lemma above implies $1 \leqslant |(G/P)^H| < p$, so $(G/P)^H$ is non-empty.

   Let $gP \in (G/P)^H$, so for any $h \in H$, $hgP = gP$, therefore $g^{-1}hg \in P$, and $h \in gPg^{-1}$. h is arbitrary implies $H \subseteq gPg^{-1}$, with equality iff $|H| = |P|$, i.e. equality occurs iff H is a Sylow p-subgroup. Therefore $\mathrm{Cl}(P) = \mathrm{Syl}_p(G)$.
3. Let by above. Both G and P act on S by conjugation, namely for $h \in G$ or P and $g \in G$.
   $$\begin{aligned} h \cdot (gPg^{-1}) &:= C_h(gPg^{-1}) \\ &= hgPg^{-1}h^{-1} \end{aligned}$$
   Check that this is an action. The action of G on S is transitive, so $S \simeq G/\mathrm{stab}(P)$ therefore $|S| \mid |G|/|\mathrm{stab}(P)| = q \implies |S| \nmid p$. It remains to show $|S| = 1 + kp$ for some $k \in \mathbb{N}$.

   Consider now P-action on S. By above lemma, $p \mid |S - S^P|$ so it suffices to show that $|S^P| = 1$ or $S^P = \{P\}$. Note that P is fixed by P-action, so $P \in S^P$. Suppose $P' \in \mathrm{Syl}_p(G)$ with $P' \neq P$, we require $J := \mathrm{stab}(P') \leqslant P$. Given $j \in J$, $jP'j^{-1} = P'$ implies $jP' = P'j$ so $JP' = P'J$. We now need JP' to be a p-group.

   Proof. We check that this is a subgroup
   - $1 \in JP'$

- $JP'JP' = JJP'P' = JP'$ so JP' is closed under product.
- Let $j \in J, h \in P$ then $(jh)^{-1} = h^{-1}j^{-1} = P'J = JP'$ so we have closure under inverses.

We need $|JP'|$ to be a power of p.

$$\begin{aligned} |JP'| &= |P'||JP'/P'| \\ 3\,\text{rd isomorphism theorem} &= p^l \left| \frac{J}{J \cap P'} \right| \\ &\mid p^{2l} \end{aligned}$$

So JP' is a p-subgroup but $JP' \geqslant P'$, together with $|P'| = p^l$ implying that $JP' = P'$. So $J \leqslant P' \cap P$ therefore $J \neq P$ and $P' \notin S^P$. This completes the proof of 3. □

□

Corollary 17.3. *Let p be an odd prime. Suppose G is a group of order $2p$ then*

$$G \simeq \begin{cases} \mathbb{Z}/2p\mathbb{Z} \\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ or } D_p \end{cases}$$

Proof. Assume G is not cyclic, then by Sylow's theorem $\exists P \in \mathrm{Syl}_p(G)$ with $o(P) = p \Longrightarrow P \simeq \mathbb{Z}/p\mathbb{Z}$. So $P = \langle \sigma \rangle$ for some $\sigma \in P$. Let $\tau \in G - P$, note that $|G/P| = 2$ so $G = P \dot\cup \tau P$. Also $P \lhd G$ as $[G : P] = 2$. Let e be the order of τ. τP has order 2 so $2|e$. Also $e \neq 2p$ as G is not cyclic. Lagrange's theorem implies $e|2p$ so $e = 2$. Similarly, the order of $\tau\sigma$ is 2, i.e. $\tau\sigma\tau\sigma = 1 \Longrightarrow \tau\sigma = \sigma^{-1}\tau$. This gives the same multiplication table for D_p, so $G \simeq D_p$. □

Note 5. Compositions of G-set homomorphisms are G-set homomorphisms.

18. Abelian groups

Let $\{A_i\}_{i \in I}$ be a family of abelian groups indexed by I.

Definition 18.1. *The direct sum of the A_i's is the subgroup of $\Pi_{i \in I} A_i$,*

$$\bigoplus_{i \in I} A_i = \{(a_i \in \Pi_{i \in I} A_i | \text{ only finitely many } A_i \neq 0\}$$

Check that this is a subgroup.

Note 6. If I is finite then $\bigoplus_{i \in I} A_i = \Pi_{i \in I} A_i$.

Recall from lecture 12, the canonical injections

$$\begin{array}{rccc} \iota_j & : & A_j & \hookrightarrow & \Pi_{i \in I} A_i \\ & & a & \longmapsto & (a_i) \end{array}$$

$$a_i = \begin{cases} 0 & i \neq j \\ a & i = j \end{cases}$$

The image lies in $\bigoplus_{i \in I} A_i$, so we have a canonical injection $A_j \hookrightarrow \bigoplus_{i \in I} A_i$. We sometimes use this to identify A_j with a subgroup of $\bigoplus_{i \in I} A_i$. Hence $\bigoplus_{i \in I} A_i$ is also the set of formal finite sums

$$a_{j1} + a_{j2} + \ldots + a_{j\,r}$$

where j_i's are all distinct and $a_{j\,i} \in A_{j\,i}$.

Theorem 18.2. *(Universal property for direct sums) Let $\{A_i\}_{i \in I}$, B be abelian groups. Further let $\lambda : \bigoplus_{i \in I} A_i \longrightarrow B$ be a group homomorphism. Then the restrictions to A_j*

$$\lambda|_{A_j} \quad : \quad A_j \quad \longrightarrow \quad B$$

are group homomorphisms. Conversely, given a family of group homomorphisms, $\lambda_i : A_i \longrightarrow B, i \in I$, the map

$$\begin{array}{rccc} \lambda & : & \bigoplus_{i \in I} A_i & \longrightarrow & B \\ & & (a_i) & \longmapsto & \sum_{i \in I} \lambda_i(a_i) \end{array}$$

this makes sense as all but finitely many a_i's are zero, so λ is a homomorphism. There is a 1-1 correspondence between group homomorphisms $\bigoplus_{i \in I} A_i \longrightarrow B$ and families of group homomorphisms $\lambda_i : A_i \longrightarrow B, i \in I$

Proof. Routine. □

Definition 18.3. *Let A, B be abelian groups. Define the Hom group* $\mathrm{Hom}(A, B)$ *to be the set of group homomorphisms $\lambda : A \longrightarrow B$.*

Proposition 18.4. *The Hom group is an abelian group when endowed with addition, for $g, h \in \mathrm{Hom}(A, B)$, $(f + g)(a) = f(a) + g(a)$.*

Proof. As for vector spaces. □

Definition 18.5. *An abelian group, F, is free abelian if there exists a group isomorphism $\lambda : \bigoplus_{i \in I} \mathbb{Z} \xrightarrow{\sim} F$. Let $1_i \in \bigoplus \mathbb{Z}$ be the element with 1 in the i-th slot and 0's elsewhere. The set $\{\lambda(1_i)\}_{i \in I}$ is called a basis of F.*

Proposition 18.6. *Let A be an abelian group, then*

(1) $\mathrm{Hom}(\mathbb{Z}, A) \underset{\Psi}{\overset{\Phi}{\leftrightarrows}} A$, $f \overset{\Psi}{\longmapsto} f(1)$, $a \overset{\Phi}{\longmapsto} (f : n \longrightarrow n\,a)$ *are inverse homomorphisms.*

Proof. Exercise, check group homomorphism □

(2) There is an isomorphism of groups

$$\mathrm{Hom}(\mathbb{Z}^s, A) \xrightarrow{\sim} A^s$$

with correspondence given by

$$\text{left mul } x \in \mathbb{Z}^s \text{ by} (a_1 \dots a_s) \longleftrightarrow (a_1 \dots a_s)$$

Proof. Exercise, universal property. □

Example 33. $\mathrm{Hom}(\mathbb{Z}^s, \mathbb{Z}^t)$ is just $t \times s$-matrices over $\mathbb{Z}$.

Corollary 18.7.

1. $\mathrm{Aut}(\mathbb{Z}^n) = \mathrm{GL}_n(\mathbb{Z}) = \{A \in \mathrm{GL}_n(\mathbb{Q}) \mid A^{-1} \text{ have integer entries}\}$.

   Proof. Follows from proposition. □

2. *If $\mathbb{Z}^m \simeq \mathbb{Z}^n$ then $m = n$.*

   Proof. Suppose we have inverse isomorphisms $\mathbb{Z}^m \longrightarrow \mathbb{Z}^n$ and $\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ given by $m \times n$ matrix M and $n \times m$ matrix N. Then $M\,N = I$ and $N\,M = I$ so N and M are square and $m = n$. □

Definition 18.8. *Let A be an abelian group. The torsion subgroup is*

$$A_{\mathrm{tors}} = \{a \in A \mid a \text{ has finite order}, n\,a = 0, \text{for some } n \geqslant 1\}$$

Also define

$$A_n = \{a \in A \mid n\,a = 0, n \in \mathbb{N}\}$$

For prime p,

$$A_{p^\infty} = \{a \in A \mid p^r a = 0, \text{for some } r\}$$

I.e. order of a is some power of p.

Proposition 18.9. *A_{tors}, A_n and A_{p^∞} are subgroups.*

Proof. (For A_{p^∞}.) Suppose $a, b \in A_{p^\infty}$, say $p^m a = 0 = p^n b$. W.l.o.g. $m \geqslant n$ then $p^m(a+b) = p^m a + p^m b = 0$, so $a + b \in A_{p^\infty}$. The proofs of the others follow similarly, note that this depends on abelian property. □

Example 34. $(\mathbb{C}^*)_{\mathrm{tors}} = \mu$, group of roots of unity.

Definition 18.10. *An abelian group A is said to be*

$$\left\{ \begin{array}{c} \text{torsion} \\ \text{torsion free} \end{array} \right\} \text{if } A_{\mathrm{tors}} = \left\{ \begin{array}{c} A \\ 0 \end{array} \right\}$$

Example 35. $\mathbb{Z}, \mathbb{Q}$ are torsion-free, $\mathbb{Z}/n\mathbb{Z}$ is torsion.

Proposition 18.11. *Let A be an abelian group, then $B = A/A_{\mathrm{tors}}$ is torsion free.*

Proof. Let $a + A_{\text{tors}} \in (A/A_{\text{tors}})_{\text{tors}}$, i.e. $\exists n \in \mathbb{Z}^+$ such that $n\,a \in A_{\text{tors}}$. Hence $n\,a$ has finite order and $\exists m \in \mathbb{Z}^+$ with $m\,n\,a = 0$, this implies $a \in A_{\text{tors}}$ and $a + A_{\text{tors}} = A_{\text{tors}} = 0_B$. Therefore $B_{\text{tors}} = 0$ so B is torsion free. □

Proposition 18.12. *Let $f : A \longrightarrow B$ be an homomorphism of abelian groups. Then $f(A_{\text{tors}}) \subseteq B_{\text{tors}}$. The universal property of quotients, applied to $A \longrightarrow B \longrightarrow B/B_{\text{tors}}$, shows that there is an induced map*

$$\tilde{f} : A/A_{\text{tors}} \longrightarrow B/B_{\text{tors}}$$

Hence if f is an isomorphism, $f|_{A_{\text{tors}}} : A_{\text{tors}} \longrightarrow B_{\text{tors}}$ and $\tilde{f} : A/A_{\text{tors}} \longrightarrow B/B_{\text{tors}}$ are isomorphisms.

Proof. Let $a \in A_{\text{tors}}$ say $n\,a = 0$ for $n \in \mathbb{Z}^+$. Then $n\,f(a) = f(n\,a) = 0$ so $f(a) \in B_{\text{tors}}$. Therefore $f(A_{\text{tors}}) \subseteq B_{\text{tors}}$. If f is an isomorphism, f^{-1} induces an inverse isomorphism

$$f^{-1}|_{B_{\text{tors}}} : B_{\text{tors}} \longrightarrow A_{\text{tors}}$$

to $f|_{A_{\text{tors}}}$, and

$$\widetilde{f^{-1}} : B/B_{\text{tors}} \longrightarrow A/A_{\text{tors}}$$

to $\tilde{f}$. □

19. Structure of finitely generated abelian groups

Theorem 19.1. *Let A be a finitely generated abelian group, then*

$$A \simeq \mathbb{Z}/h_1\mathbb{Z} \times \mathbb{Z}/h_2\mathbb{Z} \times \ldots \times \mathbb{Z}/h_r\mathbb{Z} \times \mathbb{Z}^s$$

where $h_i | h_{i+1}, i \in \{1 \ldots r-1\}$.

Proof. (by linear algebra over $\mathbb{Z}$) Let $A = \langle a_1 \ldots a_n \rangle$. By proposition above (8 by texmacs numbering, 2 if you are reading pdf), there exists a surjective group homomorphism

$$f : \mathbb{Z}^n \overset{(a_1 \ldots a_n)}{\longrightarrow} A$$

Write $f = (a_1 \ldots a_n)$ and let $K = \ker(f)$, such that $A \simeq \mathbb{Z}^n/K$. Thus proof of the above amounts to proving the following lemma.

Lemma 19.2. *Let $K \leqslant \mathbb{Z}^n$. By changing the basis of $\mathbb{Z}^n$, K is generated by $r \leqslant n$ elements of the form*

$$\begin{pmatrix} h_1 \\ 0 \\ \vdots \\ \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ h_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \ldots \begin{pmatrix} \vdots \\ 0 \\ h_r \\ 0 \\ \vdots \end{pmatrix}$$

Proof. Assume firstly $K \leqslant Z^n$ is finitely generated[†]. Let $K = \langle a_1 \ldots a_r \rangle$. Write the generators of K in vector form and form a matrix, A, with these vectors. Clearly $A : \mathbb{Z}^r \longrightarrow \mathbb{Z}^n$ and $K = \text{im}(A)$. A change of basis in $\mathbb{Z}^n$ corresponds to left multiplication by some $M \in \text{GL}_n(\mathbb{Z})$. Note also that for $N \in \text{GL}_r(\mathbb{Z})$, $\text{im}(A\,N) = \text{im}(A) = K$. Rephrasing this, □

Lemma 19.3. *There exist $M \in \text{GL}_n(\mathbb{Z}), N \in \text{GL}_r(\mathbb{Z})$ such that*

$$M\,A\,N = \begin{pmatrix} h_1 & & \\ & \ddots & \\ & & h_r \end{pmatrix}$$

where $h_i | h_{i+1}$, note that we allow $h_j = 0$.

Note 7. After the n-th column, all entries are zero so $\text{im}(A\,N)$ is generated by $\leqslant n$ elements.

Recall that $\text{GL}_m(\mathbb{Z})$ contains elementary matrices, $E_{i\,j}(\alpha), P_{i\,j}, S_i$ for multiplying rows by a constant, α, swapping two rows, and negating a row respectively. Left and right multiplication by these correspond to elementary row operations (ERO's) and elementary column operations (ECO's).

Definition 19.4. *For a matrix B with entries as integers define*

$$\gcd(B) = \gcd(\{b_{ij}\})$$

Lemma 19.5. *Let $M \in \mathrm{GL}_m(\mathbb{Z}), N \in \mathrm{GL}_s(\mathbb{Z})$, B is an $m \times s$ matrix with integer entries, then* $\gcd(M\,B\,N) = \gcd(B)$.

Proof. Entries of $M\,B\,N$ are integer linear combinations of the $b_{i\,j}$'s and is a multiple of $\gcd(B)$, this is true for every entry so $\gcd(B) \mid \gcd(M\,B\,N)$ and similarly $\gcd(M\,B\,N) \mid \gcd(B)$. □

Lemma 19.6. *Let $x \in \mathbb{Z}^m$, then $\exists M \in \mathrm{GL}_m(\mathbb{Z})$ such that $M\,x = (\gcd(x), 0 \dots 0)^T$.*

Proof. (sketch) Apply (integer) ERO's to $x = (x_1 \dots x_n)^T$ to reduce $\sum |x_i|$ until there is only 1 non zero entry remaining, and swap it up to top. The following example illustrates this procedure.

Example 36.

$$\begin{pmatrix} 6 \\ -9 \\ 12 \end{pmatrix} \longrightarrow \begin{pmatrix} 6 \\ -3 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}$$

□

Lemma 19.7. *A is an $n \times r$ matrix as before, there exists $N \in \mathrm{GL}_r(\mathbb{Z})$ so that the first column of $A\,N$, say a, satisfies*

$$\gcd(a) = \min\{\gcd(A\,x) | x \in \mathbb{Z}^r\}$$

we will later see that this is equal to $\gcd(A)$.

Proof. Let y be such that $\gcd(A\,y)$ minimises $\gcd(A\,x)$. Note $\gcd(y) = 1$, otherwise we can replace y with $\frac{y}{\gcd(y)} \in Z^r$ and $\gcd\left(\frac{A\,y}{\gcd(y)}\right) < \gcd(A\,y)$ would contradict minimality of $\gcd(A\,y)$. By the previous lemma, $\exists N \in \mathrm{GL}_r(\mathbb{Z})$ with $N^{-1}y = (1, 0 \dots 0)^T$. Then the first column of $A\,N$ is

$$a = A\,N(1, 0 \dots 0)^T = A\,N\,N^{-1}y = A\,y$$

□

By this, $a = A\,N\,e_1$ is such that $h_1 := \gcd(a) = \min\{\gcd(A\,x)\}$. We use M from the second previous lemma, so

$$\begin{aligned} M\,a &= (h_1, 0 \dots 0)^T \\ B &= M\,A\,N \\ &= \begin{pmatrix} h_1 & b_{12} & & h_{1r} \\ 0 & b_{22} & & \\ \vdots & & \dots & \\ 0 & b_{m2} & & b_{mr} \end{pmatrix} \end{aligned}$$

Using ECO's we can replace b_{1j}'s with remainders modulo h_1. But the third previous lemma, $\gcd(M\,B\,N) = \gcd(B)$, and $h_1 = \min\{\gcd(A\,x)\} \implies 0 = h_{12} = h_{13} \dots = h_{1r}$, giving

$$M\,A\,N = \begin{pmatrix} h_1 & 0 & \dots & 0 \\ 0 & b_{22} & & b_{2r} \\ \vdots & & \ddots & \\ 0 & b_{m2} & & b_{m\,r} \end{pmatrix}$$

Applying elementary row and column operations, we can replace any $b_{i\,j}$'s by remainders mod h_1, this implies $h_1 | b_{i\,j}$ for all i, j. Therefore we can modify M and N such that

$$\begin{aligned} B &= M\,A\,N \\ &= \begin{pmatrix} h_1 & \mathbf{0}^T \\ \mathbf{0} & h_1 B' \end{pmatrix} \end{aligned}$$

Now use induction on the size of A to rewrite B' in diagonal form, this completes proof of the key lemma, and proves the theorem. We are left to show that,

Lemma 19.8. *$^\dagger K \leqslant \mathbb{Z}^n$ is finitely generated.*

Proof. Let $\{(a_1 \dots a_n) \in \mathbb{Z}^n \mid a_n = 0\} = A \leqslant \mathbb{Z}^n$, so $A \simeq \mathbb{Z}^{n-1}$. We argue by induction.
Suppose $K \cap A = \langle a_1 \dots a_l \rangle \leqslant A \simeq \mathbb{Z}^{n-1}$. By the 3rd isomorphism theorem, we have

$$\frac{K}{K \cap A} \simeq \frac{K\,A}{A}$$

so there exists an epimorphism

$$\frac{K}{K \cap A} \longrightarrow \mathbb{Z}^n / A \simeq \mathbb{Z}$$

thus $\frac{K}{K\cap A} \leqslant \mathbb{Z}$. Classification of subgroups of $\mathbb{Z}$ shows that $\frac{K}{K\cap A}$ is cyclic, say generated by $a_0 + K \cap A$, for some $a_0 \in K$.
We require $a_0 \dots a_l$ to generate K. Let $a \in K$, $a + K \cap A = n_0 a_0 + K \cap A$ for some $n_0 \in \mathbb{Z}$. Therefore $a - n_0 a_0 \in K \cap A$, this implies $a - n_0 a_0 = \sum_{i=1}^{l} n_i a_i$, $a = \sum_{i=0}^{l} n_i a_i \in \langle a_0, \dots, a_l \rangle$. So K is finitely generated. □

□

20. Solvable Groups

G will denote a finite group for this section.

Definition 20.1. *A normal series (normal chain of subgroups) of G, is defined as*

$$G_* := 1 = G_0 \lhd G_1 \lhd \dots \lhd G_r = G$$

The quotients G_{i+1}/G_i are called factors.

Note 8. It is possible that G_1 is not normal in G_{i+2} or higher indecies.

Example 37. Let $G = H \times J \times K$ where H, J, K are groups. Note that $H \times J \times 1 = \ker(\pi_3) \lhd G$, where $\pi_3 : H \times J \times K \longrightarrow K$ is the canonical projection. Similarly $H \times 1 \times 1 \lhd H \times J \times 1$, we have a normal series,

$$1 \lhd H \times 1 \times 1 \lhd H \times J \times 1 \lhd H \times J \times K \lhd G$$

The factors are H, J and K respectively.

Example 38. Let $G = \mathbb{Z}/n\mathbb{Z}$, where $n \in \mathbb{Z}^+$, consider the prime factorisation of n,

$$n = p_1 p_2 \dots p_n$$

with p_i's not necessarily distinct. The series

$$n\mathbb{Z} = p_1 p_2 \dots p_n \mathbb{Z} \leqslant p_1 p_2 \dots p_{n-1}\mathbb{Z} \leqslant \dots$$

gives a normal chain of subgroups

$$0 \lhd p_1 p_2 \dots p_n \mathbb{Z}/n\mathbb{Z} \lhd p_1 p_2 \dots p_{n-1}\mathbb{Z}/n\mathbb{Z} \lhd \dots \lhd \mathbb{Z}/n\mathbb{Z} = G$$

The factors are

$$\frac{p_1 p_2 \dots p_{i-1}\mathbb{Z}/n\mathbb{Z}}{p_1 p_2 \dots p_i \mathbb{Z}/n\mathbb{Z}} \simeq \frac{p_1 p_2 \dots p_{i-1}\mathbb{Z}}{p_1 p_2 \dots p_i \mathbb{Z}} \simeq \mathbb{Z}/p_i\mathbb{Z}$$

Definition 20.2. *A finite group G is solvable if there exists a normal series with all factors (cyclic) of prime order.*

Example 39. $\mathbb{Z}/n\mathbb{Z}$ is solvable.

Lemma 20.3. *Let G be a finite group and $N \lhd G$, then G is solvable iff N and G/N are both solvable.*

Proof. ($\Longrightarrow$) Suppose G is solvable, consider a normal series as defined above, with factors of prime order. It suffices to show that the series
a) $1 = N \cap G_0 \leqslant N \cap G_1 \leqslant \dots \leqslant N \cap G_r = N$
b) $1 = G_0 N/N \lhd G_1 N/N \lhd \dots \lhd G_r N/N = GN$
are both normal series with factors $\mathbb{Z}/p_i\mathbb{Z}$ or 0.
Recall the third isomorphism theorem states that $\tilde{H} \leqslant \tilde{G}, \tilde{N} \lhd \tilde{G}$, $\frac{\tilde{H}}{\tilde{H}\cap\tilde{N}} \simeq \frac{\tilde{H}\tilde{N}}{\tilde{N}}$.
We show a) using the third isomorphism theorem with $\tilde{H} = N \cap G_i, \tilde{N} = G_{i-1}$

$$\frac{N \cap G_i}{N \cap G_{i-1}} \simeq \frac{(G_i \cap N)G_{i-1}}{G_{i-1}} \leqslant G_i/G_{i-1}$$

Lagrange's theorem implies the factor group is either $\mathbb{Z}/p\mathbb{Z}$ or 0. b can be proved by a similar approach.
($\Longleftarrow$) Suppose

$$\begin{array}{ll} H_* & 1 = N_0 \lhd N_1 \lhd \dots \lhd N_r = N \\ G/N_* & 1 = N/N \lhd H_1/N \lhd \dots \lhd H_s/N = G \end{array}$$

have prime factors, then

$$1 = N_0 \lhd N_1 \lhd \dots \lhd N_r = N \lhd H_1 \lhd H_2 \lhd \dots \lhd H_s = G$$

is a normal series with prime power quotients. □

Note 9. There is a kind of 'induction' that is often used in arguments in group theory. If a property P holds for all groups of order less than $o(G)$, and if whenever there exists a normal subgroup $N \trianglelefteqslant G$ such that $N, G/N$ satisfying P implies G satisfies P, then if G has a nontrivial proper normal subgroup, then G satisfies P.

Proposition 20.4. *A finite group G is solvable iff there exists a normal series with abelian factors.*

Proof. ($\Longrightarrow$) By definition
($\Longleftarrow$) By induction on $|G|$. If $r > 1$ and G_i's distinct. If G_{r-1} and G_r/G_{r-1} are solvable then G_r is solvable. Suppose $r = 1$ so G is abelian. Pick $g \in G - \{1\}$, let $H = \langle g \rangle$ then G/H is solvable by induction and H is solvable since it is cyclic. G is thus solvable by the previous proposition. □

Proposition 20.5. *A p-group is solvable.*

Proof. It was proved previously that the centre of a p group is non trivial. If $Z(G)$ is abelian then G is solvable. By induction $G/Z(G)$ is also a p-group, so it is solvable. Hence G is also solvable. □

Definition 20.6. *Let $g, h \in G$, we define the commutator of G to be*

$$[g, h] = g^{-1}h^{-1}gh$$

The commutator, or derived group, $G' = [G, G]$ is the subgroup of G generated by all such commutators.

Note 10. $G' = 1$ iff G is abelian.

Proposition 20.7. $G' \lhd G$

Proof. For $k \in G$

$$\begin{aligned} k[g, h]k^{-1} &= [kgk^{-1}, kh\,k^{-1}] \\ &\in G' \end{aligned}$$

implying $kG'k^{-1} = G'$ i.e. $G' \lhd G$ □

Note 11. G/G' is abelian and is called the abelianisation of G.

Proposition 20.8. *Let G be a group, A be an abelian group and $f : G \longrightarrow A$ be an homomorphism. Then $\ker(f) \geqslant G'$. So f factors through some homomorphism, $\tilde{f}$*

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ \pi \searrow & & \nearrow \tilde{f} \\ & G/G' & \end{array}$$

Proof.

$$\begin{aligned} f([g, h]) &= f(g^{-1})f(h^{-1})f(g)f(h) \\ &= 1 \\ [g, h] &\in \ker(f) \end{aligned}$$

as required. □

Corollary 20.9. *G/N is abelian iff $N \geqslant G'$.*

Proposition 20.10. *For $n \geqslant 5$, $G = A_n$ is not solvable.*

Proof. Suppose the contrary, and

$$G_* := 1 = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$$

has abelian factors. We arrive at a contradiction if we can show by downward induction on r, that all G_i contain every 3-cycle. G_r contains all 3 cycles since 3-cycles are even.
Suppose G_i contains all 3-cycles. G_i/G_{i-1} is abelian implies $G_{i-1} \geqslant G_i'$ by previous proposition applied to $G_i \longrightarrow G_i/G_{i-1}$. Let $a, b, c, d, e \in \{1 \ldots n\}$ be distinct,

$$(abc)^{-1}(cde)^{-1}(abc)(cde) = (ecb) \in G_{i-1}$$

therefore G_{i-1} contains all 3-cycles and we have a contradiction. □

21. Jordan Holder Theorem

c.f. http://www.uoregon.edu/~brundan/math647fall99/ch1.pdf
Let G be a finite group, and we have a normal series

$$G_* := 1 = G_0 \lhd G_1 \lhd \ldots \lhd G_i \lhd G_{i+1} \lhd \ldots \lhd G_r = G$$

Suppose $H/G_{n-1} \lhd G_{i+1}/G_i$ is non trivial, then we can obtain a non trivial refinement of the series,

$$1 = G_0 \lhd G_1 \lhd \ldots \lhd G_i \lhd H \lhd G_{i+1} \lhd \ldots \lhd G_r = G$$

The process can be repeated but must stop since G is finite.

Definition 21.1. *A series G_* is called a composition series if no such non trivial refinement exists, i.e. all the factors G_{i+1}/G_i are simple, in the sense that they have no nontrivial normal subgroups, and are not 1.*

Example 40. $G = \mathbb{Z}/6\mathbb{Z}$ there are composition series

$$0 \lhd 3\mathbb{Z}/6\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z}$$

The factors are $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. Also

$$0 \lhd 2\mathbb{Z}/6\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z}$$

with factors being $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$. Both these factors are clearly simple.

Definition 21.2. *The factors of a composition series are called composition factors. In the above example, they are the same in both series up to permutation.*

We will see that this is true in general.

Theorem 21.3. *(Jordan Holder) Let G be a finite group, and consider 2 composition series,*

$$G_* := 1 = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$$
$$H_* := 1 = H_0 \lhd H_1 \lhd \ldots \lhd H_s = G$$

Then $r = s$ (called the length of G) and composition factors of G_* and H_* are the same up to isomorphism and permutation.

Lemma 21.4. *(Zassenhaus' Butterfly lemma) Let G be a group, and*

$$\begin{array}{ccccc} U_1 & & V_1 & \leqslant & G \\ \nabla & & \nabla & & \\ U_0 & & V_0 & & \end{array}$$

where the triangles stand for $\trianglelefteqslant$ on its side. Clearly we have the following Hasse diagram.
DIAGRAM 1
Whenever two groups are connected by a segment to a point lying directly above, this point above represents their product. Whenever .. directly below, this represents their interesection. The double lines indicate normal subgroup inclusion.
Then,

1. *Note that the following are groups as $U_0 \trianglelefteqslant U_1, V_0 \trianglelefteqslant V_1$*
   a) $(U_1 \cap V_0)U_0 \trianglelefteqslant (U_1 \cap V_1)U_0$
   b) $(U_0 \cap V_1)V_0 \trianglelefteqslant (U_1 \cap V_1)V_0$
2. *The quotient groups formed along the three central vertical double lines are all isomorphic, namely*

$$\frac{(U_1 \cap V_1)U_0}{(U_1 \cap V_0)U_0} \simeq \frac{U_1 \cap V_1}{(U_1 \cap V_0)(U_0 \cap V_1)} \simeq \frac{(U_1 \cap V_1)V_0}{(U_0 \cap V_1)V_0}$$

Proof. By symmetry it suffices to show 1a, and the following, †

$$\frac{(U_1 \cap V_1)U_0}{(U_1 \cap V_0)U_0} \simeq \frac{U_1 \cap V_1}{(U_1 \cap V_0)(U_0 \cap V_1)}$$

(1a) Let $a \in U_1 \cap V_1, b \in U_0$, we require $ab(U_1 \cap V_0)U_0b^{-1}a^{-1} = (U_1 \cap V_0)U_0$ for $(U_1 \cap V_0)U_0 \trianglelefteqslant (U_1 \cap V_1)U_0$. Rememeber that N is normal in G imply that $xNx^{-1} = N, \forall x \in G$.

$$\begin{aligned} ab(U_1 \cap V_0)U_0b^{-1}a^{-1} &= ab(U_1 \cap V_0)b^{-1}bU_0b^{-1}a^{-1} \\ &= a(U_1 \cap V_0)U_0a^{-1} \\ &= (a(U_1 \cap V_0)a^{-1})(aU_0a^{-1}) \\ &= (U_1 \cap V_0)U_0 \end{aligned}$$

as required (since $a \in U_1$ and $U_0 \lhd U_1$). For † we require the following lemma.

Lemma 21.5.

$$(U_1 \cap V_0)U_0 \cap (U_1 \cap V_1) = (U_1 \cap V_0)(U_0 \cap V_1)$$

Proof. $\supseteq$ is clear. For $\subseteq$, let $a \in U_1 \cap V_0, b \in U_0$ suppose $ab \in U_1 \cap V_1$. We require $ab \in r.h.s$. Note $a^{-1}(U_1 \cap V_1) \subseteq V_1$

$$\begin{aligned} b &\in a^{-1}(U_1 \cap V_1) \cap U_0 \\ &\subseteq V_1 \cap U_0 \end{aligned}$$

Therefore $ab \in (U_1 \cap V_0)(V_1 \cap U_0) = r.h.s$. □

To finish off the butterfly lemma apply the third isomorphism theorem with $G = (U_1 \cap V_1)U_0, N = (U_1 \cap V_0)U_0, H = U_1 \cap V_1$. This gives †. □

Proof. (Of Jordan Holder) Define

$$\begin{aligned} G_{ij} &= (G_{i+1} \cap H_j)G_i \\ H_{ij} &= (H_{i+1} \cap G_j)H_i \end{aligned}$$

This gives the following (usually trivial) refinement of G_*, G_{**} :

$$\begin{array}{ccccccccccccc} 1 = G_0 & = & G_{00} & \trianglelefteq & G_{01} & \trianglelefteq & G_{02} & \trianglelefteq & \dots & \trianglelefteq & G_1 & = & G_{0s} \\ & & G_{10} & \trianglelefteq & G_{11} & & & & & \trianglelefteq & G_2 & & \\ & & & & & & & & & & \vdots & & \\ & & & & & & & & & & G_r & & \end{array}$$

we have a similar refinement H_{**} of H_*. The composition factors of $\left\{ \begin{array}{c} G_* \\ H_* \end{array} \right\}$ are the non trivial factors of $\left\{ \begin{array}{c} G_{**} \\ H_{**} \end{array} \right\}$. It remains only to show that factors of G_{**} are the same as those for H_{**}. By the butterfly lemma

$$\frac{(U_1 \cap V_1)U_0}{(U_1 \cap V_0)U_0} \simeq \frac{(U_1 \cap V_1)V_0}{(U_0 \cap V_1)V_0}$$

We let $U_1 = G_{i+1}, U_0 = G_i, V_1 = H_{j+1}, V_0 = H_j$

$$\frac{G_{i,j+1}}{G_{i,j}} \simeq \frac{H_{j,j+1}}{H_{j,i}}$$

This proves the Jordan Holder theorem. □

22. Free groups

Let X be a set, formally define a set $X^{-1} = \{x^{-1} \mid x \in X\}$, where $(X^{-1})^{-1} = X$.

Definition 22.1. *A word in X is an expression of the form*

$$w = x_1 x_2 \dots x_n$$

with $n \geqslant 0, x_i \in X \cup X^{-1}$, note that $n = 0$ gives an empty word denoted 1.

Say w is reduced if $x_i \neq x_{i+1}^{-1}$ for any i. the set of reduced words is denoted $W(X)$.
Define a mutiplication map

$$\begin{array}{rccc} \mu & : & W(X) \times W(X) & \longrightarrow & W(X) \\ & & (x_1 \dots x_n, y_1 \dots y_n) & \longmapsto & x_1 \dots x_n y_1 y_n \end{array}$$

Note that μ is a associative and 1 is an identity. For inverses, we need an equivalent relation on $W(X)$. For $v, w \in W(X)$, write $v \sim w$ iff we can obtain v from w by insertion or deletion of adjacent pairs of xx^{-1} where $x \in X \cup X^{-1}$.
We will denote equivalence classes of w by $[w]$ (the square brackets are usually omitted.)

Proposition 22.2. *The free group generated by X is $F(X) = W(X)/\sim$. μ descends to a well defined multiplication on $F(X)$.*

$$\begin{array}{rccc} \tilde{\mu} & : & F(X) \times F(X) & \longrightarrow & F(X) \\ & & ([w_1], [w_2]) & \longmapsto & [\mu(w_1, w_2)] \end{array}$$

which makes $F(X)$ a group.

Proof. For $\tilde{\mu}$ to be well defined we require

$$w_1 \sim w_1', w_2 \sim w_2' \Longrightarrow \mu(w_1, w_2) \sim \mu(w_1', w_2')$$

This is easy to see from any example.

$$w_1 \sim w_1 x^{-1} x, w_2 \sim y^{-1} y w_2 \text{ for } x, y \in X \cup X^{-1}$$

Note

$$\begin{aligned} \mu(w_1, w_2) &= w_1 w_2 \\ &\sim w_1 x^{-1} x y^{-1} y w_2 \\ &= \mu(w_1 x^{-1} x, y^{-1} y w_2) \end{aligned}$$

For group axioms, note μ is associative implies $\tilde{\mu}$ is associative. [1] is an identity as before. We check inverse, and it is easy to see

$$[x_1 x_2 \dots x_n]^{-1} = [x_n^{-1} x_{n-1}^{-1} \dots x_1^{-1}]$$

This ends the proof. □

Example 41. Let $X = \{x\}, F(X) = \{x^n | n \in \mathbb{Z}\} \simeq \mathbb{Z}$

Proposition 22.3. *(Universal property) Let X be a set and G be a group, and $f : X \longrightarrow G$ be a (set) map. Then*

$$\begin{array}{rccc} \tilde{f} & : & F(X) & \longrightarrow & G \\ & & x_1^{\pm 1} x_2^{\pm 1} \dots x_n^{\pm 1} & \longmapsto & f(x_1)^{\pm 1} f(x_2)^{\pm 1} \dots f(x_n)^{\pm 1} \end{array}$$

with $x_i \in X$ is a well defined group homomorphism.

Proof. (sketch) If $\tilde{f}$ is well defined, it is multiplicative. Showing $\tilde{f}$ is well defined is easy. □

Example 42.

$$\begin{aligned} \tilde{f}(w_1 x x^{-1} w_2) &= \tilde{f}(w_1) f(x) f(x)^{-1} \tilde{f}(w_2) \\ &= \tilde{f}(w_1) \tilde{f}(w_2) \\ &= \tilde{f}(w_1 w_2) \end{aligned}$$

Defining groups by generators and relations. Recall that we defined a dihedral group by its two generators, σ, τ, and the relation $\sigma\tau = \tau\sigma^{-1}$. Generally we can define groups in this fashion.

Lemma 22.4. *Let G be a group and $\{N_i\}_{i \in I}$ be normal subgroups. Then $N = \cap_{i \in I} N_i \lhd G$. Hence given a subset $S \subseteq G$ the intersection of all normal subgroups of G containing S is the smallest normal subgroup of G containing S. This is known as the normaliser of S, denoted $N(S)$.*

Proof. For $g \in G$

$$\begin{aligned} g \left(\bigcap_{i \in I} N_i \right) g^{-1} &= \bigcap_{i \in I} g N_i g^{-1} \\ &= \bigcap_{i \in I} N_i \end{aligned}$$

□

Let X be a set of generators. Consider a set of relations $\{w_i = v_i\}_{i \in I}$ where $w_i, v_i \in F(X)$.

Definition 22.5. *The group generated by X with defining relations $\{w_i = v_i\}_{i \in I}$ is*

$$\langle X \mid w_i = v_i, i \in I \rangle = F(X)/N$$

where N is the smallest normal subgroup of $F(X)$ containing $\{w_i v_i^{-1}\}_{i \in I}$.

Note 12. $F(X)/N$ is generated by the image of X in $F(X)/N$ and the relations $w_i = v_i$ hold on them

Proposition 22.6. *(Universal property) Use notation as defined above. Let G be a group and $f : X \longrightarrow G$ a map of sets, so we have an induced group homomorphism*

$$\tilde{f} \quad : \quad F(X) \quad \longrightarrow \quad G$$

Then $\tilde{f}$ induces a group homomorphism

$$\begin{array}{rccc} \hat{f} & : & F(X)/N & \longrightarrow & G \\ & & wN & \longmapsto & \tilde{f}(w) \end{array}$$

iff $\tilde{f}(w_i) = \tilde{f}(v_i), \forall i$

Proof. Use universal property of quotient groups. Note that $\tilde{f}(w_i) = \tilde{f}(v_i), \forall i$ iff $w_i v^{-1} \in \ker(f), \forall i$ □

Example 43.

$$D_n \simeq \langle g, h \mid g^n = h^2 = 1, gh = hg^{-1} \rangle := H$$

Proof. Here $H = F(X)/N$ where $X = \{g, h\}$. Use universal property on

$$\begin{array}{ccc} X & \longrightarrow & G \\ g & \longmapsto & \sigma \\ h & \longmapsto & \tau \end{array}$$

gives a surjective group homomorphism, because σ, τ are generates D_n.

$$H \quad : \quad F(X)/N \quad \longrightarrow \quad G$$

To show that this is an isomorphism, it suffices to show that $|H| \leqslant 2n$. □

Note 13. Any $k \in N$ can be written using relations in the form g^i or hg^i where $i \in \{0 \dots n-1\}$. There are only $2n$ such elements so the map is an isomorphism.

Theorem 22.7. *(Normal Form) Let X be a set. Every element of $F(X)$ can be written uniquely as a reduced word. This implies, for example if $X = \{x, y\}$.*

$$xyx \neq yxx$$

reduced words are distinct.

23. Graphs

DIAGRAM 1
A graph $\Gamma = \Gamma(V, E)$ is a set of vertices, V, a set of edges, E, and three maps

$$\begin{array}{cccc} \tilde{\cdot} & : & E & \longrightarrow & E \\ s, t & : & E & \longrightarrow & V \end{array}$$

satisfying two axioms
1. $\tilde{\tilde{\alpha}} = \alpha, \forall \alpha \in E$
2. $s(\alpha) = t(\tilde{\alpha}), \forall \alpha \in E$.

In the above example.

$$s(\varepsilon) \quad = \quad c \quad \text{and} \quad t(\varepsilon) \quad = \quad d$$

Definition 23.1. *Let $\Gamma = \Gamma(V, E)$ be a graph. A path in Γ is a string of edges*

$$p = \alpha_1 \alpha_2 \dots \alpha_n, n \geqslant 0$$

where $t(\alpha_i) = s(\alpha_{i+1})$ for each i. Sometimes we write

$$s(\alpha_i) \quad \xrightarrow{p} \quad t(\alpha_n)$$

we say that the path, p, is irreducible if $\alpha_i \neq \tilde{\alpha}_{i+1}$ for any i. (read no loops)

Example 44. In above picture, $\alpha\tilde{\beta}\beta$ is not irreducible.

Definition 23.2. *A graph $\Gamma = \Gamma(V, E)$ is connected if for any $v, w \in V$ there exists a path $v \xrightarrow{p} w$. A connected graph is called a tree if for each $v, w \in V$ there is a unique irreducible p with $v \xrightarrow{p} w$.*

Example 45. DIAGRAM 2
is not a tree as

$$\begin{array}{ccc} a & \xrightarrow{\alpha\beta\gamma} & a \\ a & \xrightarrow{\text{empty path}} & a \end{array}$$

DIAGRAM 3
is a tree

Definition 23.3. *Let $\Gamma = \Gamma(V, E)$ be a graph. A subgraph $\Lambda(V', E')$ of Γ is a pair of subsets $V' \subseteq V, E' \subseteq E$ such that $\tilde{E'} \subseteq E'$ and $s(E'), t(E') \subseteq V'$.*

Example 46. DIAGRAM 4
is a subgraph of
DIAGRAM 5

Proposition 23.4. *Let $\Gamma = \Gamma(V, E)$ be a connected graph, there exists a subgraph $\Lambda(V', E')$ which is a tree and is maximal (i.e. there exists no subgraph $\Lambda''(V'', E'')$ with $V' \subseteq V'', E' \subseteq E''$ one of these not equal and Λ'' a tree)*

Aside on partial order and total order.

Lemma 23.5. *(Zorn) Let S be a nonempty set, partially ordered by $\leqslant$. Suppose every nonempty chain has an upper bound in S, then S has a maximal element.*

Note 14. This is equivalent to the axiom of choice.

Proof. (of proposition) Let T the set of subgraphs of $\Gamma = \Gamma(V, E)$ which are trees. Consider a partial order $\leqslant$ defined by

$$\Lambda_1(V_1, E_1) \leqslant \Lambda_2(V_2, E_2) \iff V_1 \subseteq V_2, E_1 \subseteq E_2$$

Check tha this is a partial order, we require the maximal element of this poset.
Let $\{\Lambda_i(E_i, V_i)\})_{i \in I} \subseteq T$, which is totally ordered, we require an upper bound, the candidate is

$$\tilde{\Lambda} = \tilde{\Lambda}(\tilde{V}, \tilde{E})$$

such that $\tilde{V} = \bigcup V_i, \tilde{U} = \bigcup U_i$. It suffices to check that $\tilde{\Lambda}$ is a subgraph and a tree. The method is similar for both so we demonstrate the latter.
Suppose we have irreducible paths.
DIAGRAM 6
note since Λ_i's are totally ordered, p_1, p_2 actually lie in some Λ_i. But Λ_i is a tree so $p_1 = p_2$ as desired. Now Zorn's lemma gives the existence of a maximal subtree. Let $\Lambda'(V', E')$ be one such subtree, we require $V' = V$. We can show maximality easily. □

24. Fundamental group

Let $\Gamma = \Gamma(V, E)$ and $p = \alpha_1 \dots \alpha_m, q = \beta_1 \dots \beta_n$ be two paths in Γ. Suppose $u \xrightarrow{p} v \xrightarrow{q} w$, then we can define the product of p and q to be their concatenation, $pq = \alpha_1 \dots \alpha_m \beta_1 \dots \beta_n$. We require an equivalent relation on paths in Γ which have the same source and target.

Definition 24.1. *(Homotopy, graph) Let $p = \alpha_1 \dots \alpha_m, q = \beta_1 \dots \beta_n$ be two paths in Γ with $s(\alpha_1) = s(\beta_1), t(\alpha_m) = t(\beta_n)$. We say that p and q are homotopic if we can obtain p from q by inserting or deleting a sequence of paths of the form $\alpha\tilde{\alpha}$.*
Alternatively, we can say that two paths p and q in Γ are edge related if we can write them as

$$\begin{aligned} p &= p_1 p_2 \\ q &= p_1 \alpha \tilde{\alpha} p_2 \end{aligned}$$

for some $\alpha \in E$. Two paths p and q in Γ are homotopic if there exists a sequence of paths

$$p = p_0, p_1, \dots, p_r = q$$

where p_i is edge related to p_{i-1} for $i \in \{1 \dots r\}$.

Proposition 24.2. *The homotopy relation is an equivalence relation.*

Definition 24.3. *(Fundamental group) Let $\Omega(a) = \{p \in E \mid s(p) = t(p) = a\}$, the set of paths which begin and end at a, then the fundamental group is defined as $\pi_1(\Gamma, a) = \Omega(a)/\sim$.*

Proposition 24.4. *The multiplication of paths descends to a multiplication map*

$$\mu \quad : \quad \pi_1(\Gamma, a) \times \pi_1(\Gamma, a) \quad \longrightarrow \quad \pi_1(\Gamma, a)$$

which makes $\pi_1(\Gamma, a)$ a group. Moreover, the isomorphism class of this group is independent of a.

Remark 4. This independence on a means we can write $\pi_1(\Gamma) \simeq \pi_1(\Gamma, a)$.

Proof. The path multiplication making $\pi_1(\Gamma, a)$ a group is analogous to free groups.
Independence on a. We require $\pi_1(\Gamma, a) \simeq \pi_1(\Gamma, b)$, since Γ is connected, there exists $p = \alpha_1 \dots \alpha_n$ from a to b. We wish to show that

$$\begin{aligned} \phi \quad : \quad \pi_1(\Gamma, a) &\longrightarrow \pi_1(\Gamma, b) \\ q &\longmapsto \tilde{p} q p \\ \text{and} \quad \psi \quad : \quad \pi_1(\Gamma, b) &\longrightarrow \pi_1(\Gamma, a) \\ q &\longmapsto p q \tilde{p} \end{aligned}$$

are inverse homomorphisms. Note that both are well defined. First we show that ϕ is a group homomorphism, let q and q' be paths in Γ, then

$$\phi(qq') = \tilde{p} q q' p \sim \tilde{p} q p \tilde{p} q' p = \phi(q)\phi(q')$$

therefore ϕ is a group homomorphism. To see that the maps defined are inverses, note

$$\psi\phi(q) = p\tilde{p}qp\tilde{p} \sim q$$

so $\psi\phi = \mathrm{id}$. We can reverse p and $\tilde{p}$ to see that $\phi\psi = \mathrm{id}$. Therefore ϕ and ψ are inverse group homomorphisms, and the isomorphism class of $\pi_1(\Gamma, a)$ is independent of a. □

Lemma 24.5. *Let $\Lambda = \Lambda(V, E)$ be a tree. Any two paths p, q from a to b $a \xrightarrow{p,q} b$ are homotopic.*

Proof. Delete $\alpha\tilde{\alpha}$'s, with $\alpha \in E$, from p until we have an irreducible path, $a \xrightarrow{\hat{p}} b$. Note that $p \sim \hat{p}$. Similarly we can an find irreducible path $a \xrightarrow{\hat{q}} b$ such that $q \sim \hat{q}$. Uniqueness property for irreducible paths in trees imply that $\hat{p} = \hat{q}$ so $p \sim q$. □

Corollary 24.6. *If Λ is a tree, $\pi_1(\Lambda) = 1$.*

Proof. All paths $a \xrightarrow{p} a$ are homotopic to the empty path. □

Theorem 24.7. *Let $\Gamma = \Gamma(V, E)$ be a connected graph. Pick a maximal subtree $\Gamma' = \Gamma'(V, E')$ as in proposition in last lecture. For each pair $\{\alpha, \tilde{\alpha}\}$ of edges not in Γ', pick one, say α, and let X be the set of such α's, then*

$$\pi_1(\Gamma) \simeq F(X)$$

Proof. Denote $\alpha^{-1} = \tilde{\alpha}$ for convenience. (We require a set map from the generators to the edges.) Pick, for each $v \in V$ a path $a \xrightarrow{f_v} v$ which is in Γ'. Define a set map

$$\begin{array}{cccccc} \varphi & : & X & \longrightarrow & \pi_1(\Gamma) \\ \dagger & & \left(v \xrightarrow{\alpha} w\right) & \longmapsto & f_v \alpha \widetilde{f_w} \\ & & & & a \to v \to w \to a \end{array}$$

The universal property shows that this extends to a group homomorphism

$$\tilde{\varphi} \quad : \quad F(X) \quad \longrightarrow \quad \pi_1(\Gamma, a)$$

Note that $\tilde{\varphi}(\alpha^{-1}) = f_w \alpha^{-1} \widetilde{f}_v$, so † gives $\tilde{\varphi}$ for $\alpha \in X^{-1}$ as well. It suffices now to show that $\tilde{\varphi}$ is an isomorphism by exhibiting an inverse, ψ. Consider a path $p \in \Omega$ $(t(p) = s(p) = a)$, we write

$$w_0 \xrightarrow{p_0} v_0 \xrightarrow{p_1} w_1 \xrightarrow{p_2} v_1 \xrightarrow{p_3} w_2 \xrightarrow{p_4} \ldots \longrightarrow w_{n-1} \xrightarrow{p_{2n-1}} v_n$$

where $\alpha_i \in X \cup X^{-1}$ and p_i's are paths in Γ'. Note that by lemma, $\sim$

$$a = w_0 \xrightarrow{f_{v_1}} v_1 \xrightarrow{\alpha_1} w_1 \xrightarrow{\widetilde{f_{w_1}} f_{v_2}} v_2 \xrightarrow{\alpha_2} w_2 \ldots$$

with $w_1 \to q \to v_2$.

$$\begin{array}{rcl} & = & \tilde{\varphi}(\alpha_1)\tilde{\varphi}(\alpha_2) \\ & = & \tilde{\varphi}(\alpha_1\alpha_2 \ldots \alpha_{n-1}) \end{array}$$

The candidate for the inverse is

$$\psi \quad : \quad p \quad \longmapsto \quad \alpha_1\alpha_2 \ldots \alpha_{n-1}$$

This is an inverse provided it is well defined. If we changed p in the homotopy class by inserting or deleting $\alpha\tilde{\alpha}$ with

1. $\alpha \in \Gamma'$ then the expression $\alpha_1\alpha_2 \ldots \alpha_{n-1}$ does not change
2. $\alpha \in X \cup X^{-1}$

Then we have inserted $\alpha\alpha^{-1}$ into the expression which is the same element in the free gorup, then it is well defined. This completes the theorem □

25. Nielsen-Schreier Theorem

Theorem 25.1. *(N-S) Any subgroup H of a free group say $G = F(X)$ generated by X is a free group.*

Proof. We construct a graph, $\Gamma = \mathrm{BH} = \mathrm{BH}(V, E)$, as follows. Let $V = H \setminus G$ be the set of right cosets of H in G, and $E = \{Hg \overset{\alpha_{Hg,x}}{\longrightarrow} Hgx \mid x \in X, Hg \in H \setminus G\} \cup \{\tilde{\alpha}_{Hg,x} = Hgx \overset{\alpha_{Hg,x}^{-1}}{\longrightarrow} Hg \mid x \in X, Hg \in H \setminus G\}$. We will abbreviate the notation to $Hg \overset{x}{\longrightarrow} Hgx$.

Example 47. Let $\mathbb{Z} \simeq \langle x \rangle = F(\{x\}) \geqslant H = \langle x^3 \rangle$, we determine BH. We have $V = \mathbb{Z}/3\mathbb{Z}$, and we have the edges $H \longrightarrow Hx \longrightarrow Hx^2 \longrightarrow H$.

To prove the theorem, it suffices by the previous theorem to show that $H \simeq \pi_1(\mathrm{BH})$
Define a group homomorphism

$$\varphi \quad : \quad \pi_1(\mathrm{BH}) \quad \longrightarrow H$$

First let $a = H$ be the base point, and consider paths from H to H (forming the set Ω).

$$H \overset{x_1}{\longrightarrow} Hx_1 \overset{x_2}{\longrightarrow} Hx_1x_2 \overset{x_3}{\longrightarrow} \ldots \overset{x_n}{\longrightarrow} Hx_1 \ldots x_n = H$$

where $x_i \in X \cup X^{-1}$. Note $x_1 \ldots x_n \in H$. We require $\varphi(p) = x_1 \ldots x_n$, note that this is well defined as adding and deleting a path of the form xx^{-1} does not change the *r.h.s.* Also note that φ is a group homomorphism. It suffices now to construct an inverse $\psi : H \longrightarrow \pi_1(\mathrm{BH}, H)$. Let $x_1 \ldots x_n \in H$ with $x_i \in H \cup H^{-1}$, let $\psi(x_1 \ldots x_n)$ be the path

$$H \overset{x_1}{\longrightarrow} Hx_1 \overset{x_2}{\longrightarrow} Hx_1x_2 \overset{x_3}{\longrightarrow} \ldots \overset{x_n}{\longrightarrow} Hx_1 \ldots x_n = H$$

which represents an element of $\pi_1(\mathrm{BH})$, clearly the inverse is well defined. We check this by inserting $xx^{-1}, x \in X \cup X^{-1}$ into the word $x_1 \ldots x_n$ to obtain a new word w, then $\psi(w)$ changes only in homotopy class. This proves the Nielsen-Schreier theorem. □