Algebra and Number Theory : Groups

Outline of questions to be covered in the course :

- Revision of structural properties of groups and certain families of groups (S_n, A_n, D_n).
- How to distinguish groups (numerical invariants and structural invariants)
- How to relate / identify groups (homomorphisms , isomorphisms).
- How to break a group into pieces (distinguished subgroups).
- How to splice groups together (products, ...).
- How to "visualise" groups (action of a group on a set).
- Classification theorems (eg. classify all groups of order $2p$, p prime ; all abelian groups).
- Structural theorems ("Sylow" ; "Orbit-Stabilizer" ; "Cauchy" : p prime divides $|G| \Rightarrow \exists$ subgroup of G of order p).

Central notion this term : Groups.

1 Basics on Groups

Definition : A group $(G, \circ)$ is a pair , where G is a set , and $\circ$ is a binary operation

$$\circ : G \times G \longrightarrow G$$

satisfying the following conditions :

(A) Associativity : $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall a, b, c \in G$

(N) There exists a neutral element e, i.e. $a \circ e = e \circ a = a$, $\forall a \in G$, the identity in G

(I) There exist inverses for any $a \in G$, given $a \in G$, $\exists\, b \in G$ such that $a \circ b = b \circ a = e$

[Recall : such a b is unique and is denoted by a^{-1}]

Recall : A group is called abelian (or commutative) if

$$a \circ b = b \circ a \quad \forall a, b \in G$$

Examples: 0) The trivial group $(G, \circ)$:

$G = \{e\}$, binary operation $\circ : \{e\} \times \{e\} \to \{e\}$
$e \circ e = e$

i) $(\mathbb{Z}_n, +_{\mathbb{Z}_n})$ is a group

$(\mathbb{Z}_n^*, \cdot_{\mathbb{Z}_n})$, where $\mathbb{Z}_n^* = \{ u \in \mathbb{Z}_n \mid u \text{ is a unit} \}$ is also a group.

2) More generally, any ring $(R, +, \cdot)$ gives rise to a group simply by 'forgetting' the multiplicative structure. In fact this group is abelian.

Also $(R^*, \cdot)$ gives a group, which need no longer be abelian

($R = (M_2(\mathbb{R}), +_{mat}, \cdot_{mat})$ has units $GL_2(\mathbb{R})$, the <u>invertible</u> 2×2 matrices with real entries)

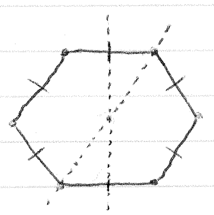
3) — Cyclic groups C_n $(\cong \mathbb{Z}_n)$

[[Also $n = 0$ is allowed, $C_0 \cong \mathbb{Z}_0 := \mathbb{Z}$]]

— Dihedral groups D_n (with $2n$ elements)

D_n: symmetry group of the regular n-gon in the plane.

Eg. $n = 6$



Symmetries: n rotations around the centre of gravity.
n reflections in an axis through distinguished points (midpoints of sides, vertices)

$2n$ symmetries altogether

Binary operation here: composition of symmetries.

ANT : G

4a) Permutation groups, in particular for $n \geq 2$ the Symmetric group S_n on n letters (typically take $1, 2, \dots, n$)

Written in terms of cycle notation, we will multiply cycles from the r[ight]

$$(13)(25734) \in S_{10}$$

where, eg., (25734) means

$$\begin{aligned} 2 &\mapsto 5 \\ 5 &\mapsto 7 \\ 7 &\mapsto 3 \\ 3 &\mapsto 4 \\ 4 &\mapsto 2 \end{aligned}$$

b) The alternating group A_n: half of the permutations in S_n are "even". Any cycle can be written as a product of 2-cycles $(j\ k)$. If the parity of the number of 2-cycles is even, then the cycle is.

[Eg. $(25734) = (24)(23)(27)(25)$ is even]

These even permutations form a group by themselves, denoted A_n.

5) Matrix groups; let $n \geq 2$, then:

$(M_n(\mathbb{R}), +_{mat})$ gives a group

$(GL_n(\mathbb{R}), \circ_{mat})$ gives a group, the invertible matrices in $M_n(\mathbb{R})$

$(O_n(\mathbb{R}), \circ_{mat})$ gives a group, the orthogonal matrices ie. $A \in M_n(\mathbb{R})$ st $A^T = A^{-1}$.

$(U_n(\mathbb{C}), \circ_{mat})$ gives a group, the unitary matrices, ie. U st $\overline{U}^T = U^{-1}$, where $\overline{U}$ is complex conjugation.

6) Geometric symmetry groups: 5 platonic solids (tetrahedron, cube, octahedron, dodecahedron, icosahedron)

Binary operation: composition of symmetries.

7) The unit circle $S^1 = \{ e^{i\theta} \mid \theta \in \mathbb{R} \} \subseteq \mathbb{C}^*$ $(= \mathbb{C} - \{0\})$ forms a group.

Binary operation: multiplication inherited from $\mathbb{C}$.

8) The set $\{ f_1(z), f_2(z), \dots, f_6(z) \}$ (of functions $\mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$)

$$f_1(z) = z, \quad f_2(z) = \frac{1}{z}, \quad f_3(z) = 1 - \frac{1}{z}$$

$$f_4(z) = \frac{z}{z-1}, \quad f_5(z) = \frac{1}{1-z}, \quad f_6(z) = 1 - z$$

forms a group, binary operation: composition of functions.

Eg.

$$\begin{aligned}(f_4 \circ f_3)(z) &= f_4(f_3(z)) \\ &= f_4\left(1 - \frac{1}{z}\right) \\ &= \frac{1 - \frac{1}{z}}{1 - \frac{1}{z} - 1} \\ &= 1 - z \\ &= f_6(z)\end{aligned}$$

9) Geometry: isometry groups of:

- Unit disc $\subset \mathbb{C}$
- Hyperbolic plane (Möbius transformations)
- Euclidean 3-space (rotations, translations, ...)
- Minkowski space-time (physics: Lorentz group, Poincaré group)

10) Number Theory:

On sets of solutions of "Pell's equation":

$$x^2 - dy^2 = 1$$

$d \geq 1$, squarefree, with $x, y \in \mathbb{Z}$.

There is a group structure on the set of all those (integer) solutions (there are in fact infinitely many such).

ANT : G

Groups are ubiquitous objects all over maths.

Convention: From now on, mostly drop the binary operation in the notation, whenever it is understood.

Structural Properties of Groups

From Core A:

Proposition: Let G be a group

i) The identity element $e \in G$ is unique
ii) The inverse element $a^{-1} \in G$ for a given $a \in G$ is unique
iii) $(ab)^{-1} = b^{-1}a^{-1}$, $\forall a, b \in G$
iv) Cancellation laws:

Let $a, b, g \in G$

If $ga = gb$ then $a = b$
If $ag = bg$ then $a = b$

Notation: Exponents.

For $g \in G$, write:

$$g^n := \underbrace{g \cdot g \cdot \cdots \cdot g}_{n \text{ factors}}, \quad n \geq 1$$

$$g^0 := e$$

$$g^{-n} := (g^n)^{-1}, \quad n \geq 1$$

i) Then we can compute with exponents "as usual".

$$g^m \cdot g^n = g^{m+n}, \quad (g^m)^n = g^{mn}, \quad \forall m, n \in \mathbb{Z}$$

ii) Furthermore, if $g, h \in G$ commute (i.e. if $gh = hg$) then we have

$$(gh)^n = g^n h^n$$

[Proof by induction, for $n = 1$ obvious. Suppose true for n, then deduce for $n+1$:

$$
\begin{aligned}
(gh)^{n+1} &= (gh)^n (gh) \\
&= g^n (h^n g) h \qquad ; \text{ induction assumption} \\
&= g^n g\, h^n h \\
&= g^{n+1} h^{n+1}
\end{aligned}
$$

Subgroups

Definition: A subgroup of a group $(G, \circ)$ is a pair $(H, \circ_H)$ of a subset $H \subset G$, and the binary operation $\circ_H$ is the restriction of $\circ$ to H.

$$
\left(\text{i.e.} \quad \begin{aligned} \circ &: G \times G \longrightarrow G \\ \circ_H &: H \times H \longrightarrow H \end{aligned} \right)
$$

such that $(H, \circ_H)$ itself forms a group.

Notation: $H \leq G$.

Proposition: Subgroup test

$H \subset G$ is a subgroup if

$$
\left.\begin{aligned}
&\text{i)}\ e_G \in H \\
&\text{ii)}\ h_1, h_2 \in H \Rightarrow h_1 h_2 \in H \\
&\text{iii)}\ h \in H \Rightarrow h^{-1} \in H
\end{aligned}\right\} (\text{a priori, in } G)
$$

ie. H is closed under multiplication and under taking inverses.

Examples:

$A_n \leq S_n$, for $n \geq 2$

$n\mathbb{Z} \leq \mathbb{Z}$

$\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$

$S_n \leq S_m$, if $n \leq m$

$\{e\} \leq G$, $G \leq G$ (trivial)

Definition: Let $g \in G$ (a group). Then the <u>subgroup of G generated by g</u> is:

$$\langle g \rangle := \{ g^m \mid m \in \mathbb{Z} \}$$

More generally, the <u>subgroup</u> of G generated by a subset $S \subseteq G$ consists of all the <u>finite</u> products of elements of S and their inverses.

Example: $S = \{\frac{1}{2}, 3, 7\} \subset \mathbb{Q}^*$, then

ANT : G

$$\langle S \rangle = \{ 2^m 3^n 7^r \mid m, n, r \in \mathbb{Z} \}$$

Orders

Definition: i) The order of a group G, denoted $|G|$ is the number of its elements.

ii) The order of an element $g \in G$ is the smallest positive integer m such that $g^m = e$, or if such an m does not exist, the order is infinite.

Examples: i) In $(\mathbb{Z}_{30}, +)$, the class $\overline{24}$ has order 5 since $5 \cdot \overline{24} = \overline{120} = \overline{0}$

$$|\mathbb{Z}_{30}| = 30$$

Note: exponent becomes multiple as we have additive notation.

2) In $(\mathbb{Z}, +)$, the element 1 has infinite order (like any other non-zero element)

3) In $(\mathbb{Z}_p^*, \cdot)$, p prime, $\overline{1}$ has order 1, and all other elements have order dividing $p-1$ (Fermat's little Theorem)

Theorem: (Lagrange)

If $H \leq G$, a finite group, then $|H| \mid |G|$, in particular, the order of any element in G divides the group order $|G|$.

Permutation Groups

Definition: A permutation of a (non-empty) set X is a bijection (i.e. injective and surjective map) from X to itself.

Notation: $S_X := \{ \text{bijections } X \rightarrow X \}$

Fact: $(S_X, \circ)$ becomes a group, where the binary operation $\circ$ is composition of maps.

(A) Associativity holds in general for functions.

(N) Identity element is the identity bijection

$$\mathrm{id} : X \longrightarrow X$$
$$x \longmapsto x$$

(I) To each bijection the inverse map exists and is itself a bijection

In particular, for $X = \{1, 2, \ldots, n\}$, we denote

$$S_n := S_{\{1,2,\ldots,n\}}.$$

Lemma: $|S_n| = n!$

Example: Specific permutations in S_n, for $1 \leq k \leq n$ have:

k-cycles: $(i_1\ i_2\ \cdots\ i_k) = (i_2\ i_3\ \cdots\ i_k\ i_1)$
$= (i_3\ i_4\ \cdots\ i_k\ i_1\ i_2)$

k-fold ambiguity in writing it.

From Core A

Proposition: i) Every permutation is the product of disjoint cycles in an essentially unique way.

['Essentially unique': two disjoint cycles commute, also note a k-cycle can be written in k different ways]

Example: In S_{10}:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 2 & 1 & 4 & 8 & 9 & 7 & 6 & 10 \end{pmatrix}$$

$$= (1\,5\,4)(2\,3)(6\,8\,7\,9)(10)$$

which can also be written as, eg.

$$= (8\,7\,9\,6)(2\,3)(10)(4\,1\,5)$$

ii) Any $\sigma \in S_n$ factors (non-uniquely) into a product of transpositions (2-cycles)

Example : $(1\,2\,\ldots\,r) = (1\,r)(1\,r-1)\cdots(1\,2)$
$= (1\,2)(2\,3)\cdots(r-1\,r)$

iii) The parity of the number of transpositions in any factorisation as in ii) is the same.

Hence this number is well defined modulo 2, so it makes sense to put:

Definition : Let $\sigma \in S_n$, then $\operatorname{sgn}(\sigma) = (-1)^t$, where t denotes the number of transpositions in a decomposition of σ. (Maybe denoted $\varepsilon(\sigma)$ in Core A).

If t is even σ is called even, otherwise is called odd.

iv) The order of an element $\sigma \in S_n$ with disjoint cycle decomposition of lengths $k_1, \ldots, k_r$ respectively, is

$$\operatorname{lcm}(k_1, \ldots, k_r)$$

Example : In S_{10} the permutation $(1\,2)(3\,4\,5)(6\,7\,8\,9\,10)$ has order $2 \cdot 3 \cdot 5 = 30$.

Definition - Proposition : The set $A_n := \{\sigma \in S_n \mid \sigma \text{ is even, ie } \operatorname{sgn}(\sigma) = 1\}$ forms a subgroup (with usual multiplication in S_n) of S_n

Proof : Note $\quad \operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2) \qquad (*)$

[Just write σ_i as a product of transpositions

$\sigma_1 = \tau_{11} \cdots \tau_{1r}, \quad \operatorname{sgn}(\sigma_1) = (-1)^r$
$\sigma_2 = \tau_{21} \cdots \tau_{2s}, \quad \operatorname{sgn}(\sigma_2) = (-1)^s$

$\operatorname{sgn}(\sigma_1\sigma_2) = (-1)^{r+s} = (-1)^r(-1)^s = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$]

From this we see that

i) $\operatorname{sgn}(e) = 1$; use $(*)$
ii) A_n is closed under multiplication
iii) The inverse of $\sigma \in A_n$ inside S_n has sign 1 ; use $(*)$

Example : $n = 3$

$$S_3 = \{ \underbrace{(1)(2)(3)}_{e},\ \underbrace{(12)(3)}_{\text{odd}},\ \underbrace{(23)(1)}_{\text{odd}},$$

$$\underbrace{(31)(2)}_{\text{odd}},\ (123),\ (132) \}$$

(Discard 1-cycles in the notation)

$$A_3 = \{ e,\ \underbrace{(123)},\ (132) \}$$

$$(123) = (312) = (31)(12)$$

$$(123)^{-1} = (321) = (132)$$

$$(123)^2 = (123)^{3-1} = \underbrace{(123)^3}_{e}(123)^{-1} = (132)$$

Proposition : i) $|A_n| = \frac{1}{2}|S_n|$

ii) A_n is generated by 3-cycles.

Proof : i) Note : $\{ \sigma \in S_n \mid \sigma \text{ even} \} \overset{1:1}{\longleftrightarrow} \{ \sigma \in S_n \mid \sigma \text{ odd} \}$ via $\circ (12)$

ii) Write $\sigma \in A_n$ as a product of an <u>even</u> number of transpositions :

$$(i_1\ j_1)(i_2\ j_2) \cdots (i_{2r}\ j_{2r})$$

Starting from the left combine two successive transpositions

Case 1 : (non-disjoint) : $(i\ j)(j\ k) = (j\ k\ i)$

Case 2 : (disjoint) : $(i\ j)(k\ l) = \underbrace{(i\ j)(j\ k)}\underbrace{(j\ k)(k\ l)}$

now apply case 1.

Example : Some subgroups of A_4

$$\langle (12)(34) \rangle = \{ e,\ (12)(34) \}$$

$\rightsquigarrow$ Cyclic group of order 2.

ANT : G

$\langle (123) \rangle = \{ e, (123), (132) \}$
$\rightsquigarrow$ Cyclic group of order 3

$\langle (12)(34), (13)(24) \rangle = \{ e, (12)(34), (13)(24), (14)(23) \}$
$\rightsquigarrow$ Klein-4-group

Some subgroups of S_4 (not in A_4)

$\langle (12) \rangle$ Cyclic of order 2
$\langle (1234) \rangle$ Cyclic of order 4

$\langle (12), (123) \rangle \cong S_3$ All permutations as in S_3 extended by (4) a 1-cycle.

$\langle \underbrace{r = (1234)}_{\text{order } 4}, \underbrace{h = (12)(34)}_{\text{order } 2} \rangle$ This realises the symmetry group of a square, the dihedral group D_4

Check $r^4 = e$, $h^2 = e$, $hr = r^{-1}h$.

All relations in D_4 follow from these, hence the notation (for more general n)

$$D_n := \langle r, h \mid r^n = e, h^2 = e, hr = r^{-1}h \rangle$$

Direct Product, Homomorphisms and Isomorphisms

Definition: Let $(G, \circ)$, and $(H, *)$ be groups. A map φ, $\varphi : (G, \circ) \longrightarrow (H, *)$ is a <u>homomorphism of groups</u> if

$$\varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2), \quad \forall g_1, g_2 \in G$$

Moreover φ is a <u>group isomorphism</u> if it is bijective.

Note: As for rings:

$$\operatorname{Ker} \varphi = \{ g \in G \mid \varphi(g) = e_H \}, \text{ and}$$
$$\operatorname{Im} \varphi = \{ \varphi(g) \mid g \in G \}$$

are subgroups of G and H respectively.

Examples: 1) $\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +)$
$r \longmapsto r \bmod n$

is a group homomorphism.

$$\operatorname{Ker} \varphi = \{ rk \mid k \in \mathbb{Z} \}$$
$$\operatorname{Im} \varphi = \mathbb{Z}_n$$

2) Let $r \in \mathbb{Z}_{>0}$, then

$$\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{C}^*, \cdot)$$
$$n \longmapsto e^{2\pi i n / r}$$

is a group homomorphism:

$$\begin{aligned} \varphi(n+m) &= e^{2\pi i (n+m)/r} \\ &= e^{2\pi i n/r} e^{2\pi i m/r} \\ &= \varphi(n) \cdot \varphi(m) \end{aligned}$$

$$\begin{aligned} \operatorname{Ker} \varphi &= \{ n \in \mathbb{Z} \mid e^{2\pi i n/r} = 1 \} \\ &= \{ rk \mid k \in \mathbb{Z} \} \end{aligned}$$

3) For $n \geq 2$

$$\operatorname{sgn} : S_n \longrightarrow \{\pm 1\}$$
$$\sigma \longrightarrow \operatorname{sgn}(\sigma)$$

is a homomorphism, with kernel, $\ker(\operatorname{sgn}) = A_n$.

[Explicit form :

$$\operatorname{sgn}(\sigma) = \prod_{n \geq i > j \geq 1} \frac{\sigma(i) - \sigma(j)}{i - j}$$]

4) From Linear Algebra, for $n \geq 1$, we have a homomorphism

$$\varphi_n : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$$
$$A \longmapsto \det(A)$$

$$\begin{aligned} \operatorname{Ker} \varphi_n &= \{ A \in GL_n(\mathbb{R}) \mid \det(A) = 1 \} \\ &= SL_n(\mathbb{R}) \end{aligned}$$

[Use $\det(AB) = \det(A)\det(B)$]

Ideas for 'distinguishing' two groups, ie for checking if they are isomorphic or not.

ANT: G

An isomorphism preserves:

- The order of a group
- The set of orders of elements } Numerical Invariants
- The property of being abelian / non-abelian } Structural Invariant

Examples: 1) S_3 and $\mathbb{Z}_6$ are not isomorphic.

Possible orders in S_3, $\{1, 2, 3\}$
in $\mathbb{Z}_6$, $\{1, 2, 3, \underline{6}\}$

$$\Rightarrow S_3 \not\cong \mathbb{Z}_6$$

2) A_4 and D_6 are not isomorphic.

$$|A_4| = |D_6| = 12$$

Possible orders in A_4, $\{1, 2, 3\}$
in D_6, $\{1, 2, 3, \underline{6}\}$

$$\Rightarrow A_4 \not\cong D_6$$

Definition: The direct product of two groups $(G, \circ)$, and $(H, *)$ is given by the pair $(G \times H, \circledast)$, where $G \times H$ is the Cartesian product of G and H, and the binary operation $\circledast$ is given by

$$(g_1, h_1) \circledast (g_2, h_2) := (g_1 \circ g_2, h_1 * h_2)$$

This forms a group.

Justification: The identity element exists: (e_G, e_H), and (g, h) has an inverse (g^{-1}, h^{-1}).

Example: $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2})$
$(\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$

Where $(\bar{a}, \bar{b})$ means $(a \bmod 2, b \bmod 3)$, with binary operation

$$(\bar{a}, \bar{b}) \circledast (\bar{a}', \bar{b}') = (\bar{a} +_{\mathbb{Z}_2} \bar{a}', \bar{b} +_{\mathbb{Z}_3} \bar{b}')$$

Claim: This is isomorphic to $\mathbb{Z}_6$ (cyclic), a generator is, e.g., $(\bar{1}, \bar{1})$, and an isomorphism is given by

$$\varphi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$$
$$\bar{a} \longmapsto (\bar{a}, \bar{a})$$

Theorem: In general, we have, for $n, m \geq 1$ that

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{nm} \iff \gcd(n,m) = 1$$

Proof: Consider $(\bar{1}, \bar{1}) \in \mathbb{Z}_m \times \mathbb{Z}_n$, it is our candidate for a generator if cyclic.

Suppose $\mathrm{ord}(\bar{1}, \bar{1}) = k$.

$$k(\bar{1}, \bar{1}) = (\bar{0}, \bar{0})$$
$$\Rightarrow \quad m \mid k \quad \text{and} \quad n \mid k.$$

"$\Leftarrow$": Suppose $(m,n) = 1$, then also $mn \mid k$, but $|\mathbb{Z}_{nm}| = mn$, so we also have $k \leq mn$, hence $mn = k$.

"$\Rightarrow$": Suppose $d := (m,n) > 1$, we show then that $\mathbb{Z}_m \times \mathbb{Z}_n$ is <u>not</u> cyclic.

Put $m' = \frac{m}{d}$, $n' = \frac{n}{d}$, so that $(m', n') = 1$.

The order of any element in $G := \mathbb{Z}_{m'd} \times \mathbb{Z}_{n'd}$ is $\leq m'n'd$.

$$m'n'd(\bar{a}, \bar{b}) = (\underbrace{\underbrace{m'd}_{m}(n'\bar{a})}_{\bar{0} \text{ in } \mathbb{Z}_m}, \underbrace{\underbrace{n'd}_{n}(m'\bar{b})}_{\bar{0} \text{ in } \mathbb{Z}_n})$$

$$= (\bar{0}, \bar{0})$$

for any $(\bar{a}, \bar{b}) \in G$.

But the group order $|G|$ is $(m'd)(n'd)$ $= (m'n'd)d > m'n'd$. So G cannot be cyclic.

Notation: For subsets S_1, S_2 of a group G, then

$$S_1 \circ S_2 := \{ h_1 \circ h_2 \mid h_1 \in S_1, h_2 \in S_2 \}$$

Can give a useful criterion to check if a group is a direct product of two other (given) groups.

Theorem: Let H and K be subgroups of a group G such that i) – iii) hold:

i) $H \circ K = G$
ii) $H \cap K = \{e\}$
iii) $hk = kh \quad \forall h \in H, \forall k \in K$

Then we have $G \cong H \times K$.

Proof: Consider a map

$$\begin{aligned} \varphi : H \times K &\longrightarrow G \\ (h, k) &\longmapsto hk \end{aligned}$$

We have:

1) φ is a homomorphism

$$\varphi((h,k)\cdot(h',k')) = \varphi((hh', kk')) = hh' \cdot kk'$$
$$\varphi(h,k)\,\varphi(h',k') = (hk)\cdot(h'k') = hh' \cdot kk' \quad \text{by iii)}$$

2) φ is injective

Let $\varphi(h,k) = e$, i.e. $hk = e$, with $h \neq e$, $k \neq e$, then $k = h^{-1}$ is in H (a subgroup), and is in K, so $H \cap K \supsetneq \{e\}$, violating ii)

3) φ is surjective

As $G = HK$, by i), any $g \in G$ can be written as hk for some $h \in H$, $k \in K$, hence as $\varphi(h,k)$.

Examples: 1) Klein-4-group

$$V_4 = \{e, a_1, a_2, a_3\} \quad \text{with relations}$$

$$a_i^2 = e, \quad i = 1, 2, 3$$
$$a_i a_j = a_k, \quad \text{for } \{i, j, k\} = \{1, 2, 3\} \qquad (*)$$

Two subgroups of order 2 are for example

$$\begin{aligned} H_i &= \{e, a_i\}, \quad i = 1, 2 \\ &\cong C_2 \\ &\cong \mathbb{Z}_2 \end{aligned}$$

And:

$$H_1 \cap H_2 = \{e\}$$
$$H_1 H_2 = \{e \cdot e,\ a_1 e,\ e \cdot a_2,\ a_1 a_2\} = V_4$$
They also commute by $(*)$

Hence we conclude

$$V_4 \cong H_1 \times H_2 \cong C_2 \times C_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

where C_n is the cyclic group of order n.

2) $D_6 = \langle r, h \mid r^6 = h^2 = e,\ rh = hr^{-1} \rangle$ has subgroups

$$H = \langle r^3 \rangle = \{e, r^3\} \cong C_2$$
$$K = \langle r^2, h \rangle = \{e, r^2, r^4, h, hr^2, hr^4\} \cong D_3$$

i) Check — multiply any element in K by r^3, ...
ii) $H \cap K = \{e\}$
iii) $r^3 \cdot (r^{2j} h^i) = (r^{2j} h^i) \cdot r^3 \qquad j = 0, 1, 2, \quad i = 0, 1$

To show:

$i = 0 \qquad r^{3+2j}$ on both sides

$$i = 1 \qquad \text{RHS} = r^{2j}(hr^3) = r^{2j} r^{-3} h = r^{2j} r^3 h = \text{LHS}$$

Conclude using proposition:

$$D_6 \cong H \times K \cong C_2 \times D_3 \cong \mathbb{Z}_2 \times D_3$$

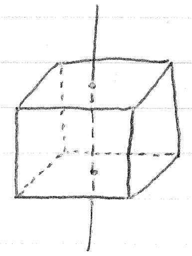
Next aim: Write every group as a subgroup of <u>some</u> permutation group. Motivate with:

Theorem: The group of rotational symmetries of the unit cube in $\mathbb{R}^3$ is isomorphic to S_4

Proof: (Idea)

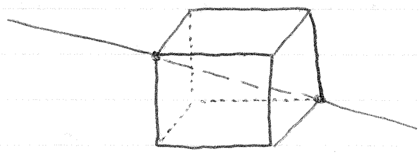
The following rotations exist. Possible axes of rotation

i) Rotation axis through two opposite face centres by angle $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$, (and 0).



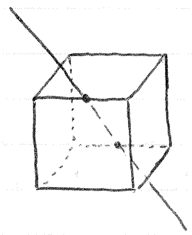
Get $\frac{6}{2}$ (faces) $\cdot$ 3 non-trivial rotations = 9 non-trivial rotatio

ii) Rotation axis through opposite vertices by angle $\frac{2\pi}{3}$, $\frac{4\pi}{3}$, (and 0).



Get $\frac{8}{2}$ (vertices) $\cdot$ 2 non-trivial rotations = 8 non-trivial rotations

iii) Rotation axis through opposite edge mid-points by angle π, (and 0).

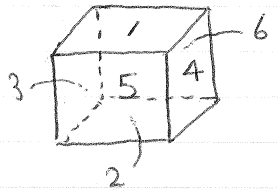


Get $\frac{12}{2}$ (edges) $\cdot$ 1 non-trivial rotation = 6 non-trivial rotations

Overall find $9 + 8 + 6 = 23$ non-trivial rotations, add the trivial one, giving 24 such rotations.

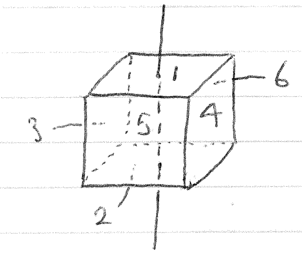
Check: these 24 rotations form a group under composition.

Eg 1) We can label all the faces by different colours / numbers (1,...,6)



Then each rotation permutes the faces and hence these numbers. Produces elements in S_6

Eg.

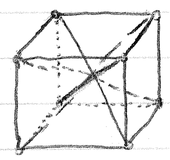


rotating around this by $\frac{\pi}{2}$ gives $(1)(2)(3546)$

2) Can also label the vertices, find rotations encoded as an element in S_8, or rather $S_X \cong S_8$, where $X = \{$ set of 8 vertices $\}$.

3) Or label the edges, get rotation as an element in $S_X \cong S_{12}$, where $X = \{$ set of 12 edges $\}$

4) Most economic set; the set of 4 principle diagonals.



Get for each rotation an element in $S_X \cong S_4$ where $X = \{$ set of 4 principle diagonals $\}$.

Remark: The geometric interpretation of the rotational symmetries of a cube give rise to natural maps

$$\{\text{rotational symmetries of a cube}\} \longrightarrow S_X$$

where X is, for example, the set of

— faces $\rightsquigarrow S_6$
— vertices $\rightsquigarrow S_8$
— edges $\rightsquigarrow S_{12}$
— principle diagonals $\rightsquigarrow S_4$

These are instances of a more general statement.

Theorem: (Cayley)

Any group $(G, \circ)$ is isomorphic to a subgroup of a permutation group

Proof: Idea: attach to each $g \in G$ a permutation, "left translation"

$$L_g : G \longrightarrow G$$
$$h \longmapsto gh, \quad \forall h \in G$$

[Check L_g is indeed a bijection

Injectivity: $L_g(h_1) = L_g(h_2)$
$\Rightarrow gh_1 = gh_2$
$\Rightarrow h_1 = h_2$; left cancel

Surjectivity: for $k \in G$, take $h = g^{-1}k$, then $L_g(h) = gh = gg^{-1}k = k$.]

Now put $G' := \{ L_g \in S_G \mid g \in G \}$, this is a subset of S_G.

Claim: G' is indeed a group.

[Need to check:

- G' non-empty, clear, contains L_e, identity bijection
- $L_g, L_h \in G'$, show $L_g \circ L_h = L_k$ for some $k \in G$

$$\begin{aligned} L_g \circ L_h(r) &= L_g(L_h(r)) \\ &= L_g(hr) \\ &= ghr \\ &= L_{gh}(r) \quad \forall r \in G \qquad (*) \end{aligned}$$

- $L_g \in G'$, show $(L_g)^{-1} \in G'$

$L_{g^{-1}} \circ L_g = L_e$
$\Rightarrow L_{g^{-1}}$ indeed in G', is the inverse of L_g]

And we have shown

$$\psi : G \rightarrow G'$$
$$g \mapsto L_g$$

is a homomorphism of groups (cf $(*)$)

Claim: ψ is in fact an isomorphism of groups

[Injectivity: $\Psi(g_1) = \Psi(g_2)$
$\Rightarrow L_{g_1} = L_{g_2}$

In particular $L_{g_1}(e) = L_{g_2}(e)$
$\Rightarrow g_1 = g_2$

Surjectivity : By construction]

This proves the Theorem.

Example: Consider the Klein-4-group

$X := V_4 = \{e, a_1, a_2, a_3\}$, with relations
$a_i^2 = e$, $a_i a_j = a_k$ $\{i, j, k\} = \{1, 2, 3\}$.

Want to show:

$G := V_4$ is isomorphic to a subgroup of S_X ($\cong S_4$
by labelling the elements of X by $1, \dots, 4$ as:

$$\begin{array}{cccc} e & a_1 & a_2 & a_3 \\ 1 & 2 & 3 & 4 \end{array}$$)

Proof of the Theorem suggests to proceed as follows

$$e \longmapsto L_e$$
$$a_1 \longmapsto L_{a_1}$$

where
$$\begin{aligned} L_{a_1} : V_4 &\longrightarrow V_4 \\ e &\longmapsto a_1 e = a_1 \\ a_1 &\longmapsto a_1 a_1 = e \\ a_2 &\longmapsto a_1 a_2 = a_3 \\ a_3 &\longmapsto a_1 a_3 = a_2 \end{aligned}$$

Encode as permutations of the circled indices, so

$$\begin{aligned} L_{a_1} : V_4 &\longrightarrow V_4 \\ 1 &\longmapsto 2 \\ 2 &\longmapsto 1 \\ 3 &\longmapsto 4 \\ 4 &\longmapsto 3 \end{aligned}$$

i.e. as $(12)(34) \in S_4$.

Similarly, $a_2 \longmapsto L_{a_2}$ corresponding to $(13)(24)$
$a_3 \longmapsto L_{a_3}$ corresponding to $(14)(23)$

Altogether V_4 is 'identified' as the subgroup

$$V_4 = \{ e, (12)(34), (13)(24), (14)(23) \}$$

of S_4.

From the Theorem get, for any group G, a homomorphism $G \to S_G$.

In particular every $g \in G$ is realised as a permutation of G.

In the example of the rotational symmetries of the cube we saw homomorphisms $\{\text{rotational symmetries}\} \longrightarrow S_X$, for some set X.

This leads to Group Actions.

2 Group Actions

Definition: An action of a group G on a (non-empty) set X is a homomorphism

$$\varphi : G \longrightarrow S_X$$

In other words; for any $g \in G$ assign a permutation $\varphi(g)$ such that

$$\varphi(g)\varphi(h) = \varphi(gh)$$

Note: φ need neither be injective nor surjective.

We say "G acts on X (via φ)".

Examples: 1) (Additive notation!)

The infinite cyclic group $\mathbb{Z}$ acting on $\mathbb{R}$, acting by translation.

To each $n \in \mathbb{Z}$ attach:

$$\varphi(n) : \mathbb{R} \to \mathbb{R}$$
$$r \mapsto n + r$$

Can check

$$(\varphi(n) \circ \varphi(m))(r) = \varphi(n)(m+r)$$
$$= n + (m+r)$$

$$\varphi(n+m)(r) = (n+m) + r$$

These agree, by associativity for $\mathbb{R}$.

2) $\mathbb{Z}$ acts on $\mathbb{R}$ in a completely different way as follows:

For $n \in \mathbb{Z}$ attach $\varphi(n) : \mathbb{R} \to \mathbb{R}$
$r \mapsto (-1)^n r$

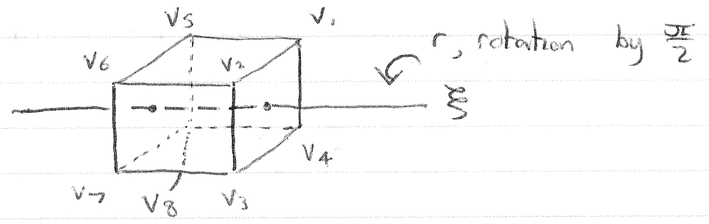
Also gives a group action:

$$(\varphi(n)\varphi(m))(r) = \varphi(n)((-1)^m r) = (-1)^n((-1)^m r)$$
$$\varphi(n+m)(r) = (-1)^{n+m} r$$

agree.

3) (More geometric)

$X = \{$ vertices of a cube $\}$
$G = \{$ rotations of a cube around an axis ξ connecting two opposite face centres with angle in $\frac{\pi}{2}\mathbb{Z}\}$



Claim: $G = \langle r \rangle \cong \mathbb{Z}_4 = \langle T \rangle$

$$\begin{aligned} \varphi: e &\longmapsto (v_1)(v_2)(v_3)(v_4) \mid (v_5)(v_6)(v_7)(v_8) \\ r &\longmapsto (v_1\, v_2\, v_3\, v_4) \mid (v_5\, v_6\, v_7\, v_8) \\ r^2 &\longmapsto (v_1\, v_3)(v_2\, v_4) \mid (v_5\, v_7)(v_6\, v_8) \\ r^3 &\longmapsto (v_4\, v_3\, v_2\, v_1) \mid (v_8\, v_7\, v_6\, v_5) \end{aligned}$$

Remark: $v_1 \dots v_4$ never 'mix' with $v_5 \dots v_8$

Definition: Let G act on a set X via $\varphi: G \to S_X$

Then for any $x \in X$

1) The set:
$$G(x) := \{ \underbrace{\varphi(g)}_{\text{permutation}}(x) \in X \mid g \in G \}$$

is called the <u>(G-) orbit</u> of x inside X.

2) The set:
$$G_x := \{ g \in G \mid \varphi(g)(x) = x \}$$

is called the <u>stabilizer</u> of x in G.

Lemma: G_x is in fact a <u>subgroup</u>.

Proof: G_x is:

i) non-empty, eg. $\varphi(e)$ is the identity permutation of X, so in particular fixes $x \in X$.

ii) closed under taking products.

$g, h \in G_x \Rightarrow \varphi(g)(x) = x, \quad \varphi(h)(x) = x$

$$\begin{aligned} \varphi(gh)(x) &= (\varphi(g)\varphi(h))(x) \quad ; \varphi \text{ homomorphism} \\ &= \underbrace{\varphi(g)(\underbrace{\varphi(h)(x)}_{x})}_{x} \\ &= x \end{aligned}$$

Conclusion : $gh \in G_x$

iii) closed under taking inverses.

For $g \in G_x$, to show $g^{-1} \in G_x$

$$\begin{aligned} \varphi(g^{-1})(x) &= \varphi(g^{-1})(\varphi(g)(x)) \quad ; g \in G_x \\ &= (\varphi(g^{-1})\varphi(g))(x) \\ &= \varphi(g^{-1}g)(x) \\ &= \varphi(e)(x) \\ &= x. \end{aligned}$$

Examples : 1) (Revisited)

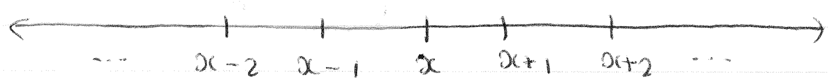
$(\mathbb{Z}, +)$ acts on $\mathbb{R}$ by "translation".

$$\begin{aligned} \varphi : \mathbb{Z} &\to S_{\mathbb{R}} \\ n &\mapsto \varphi(n) : \mathbb{R} \to \mathbb{R} \\ & \qquad\qquad x \mapsto n + x \end{aligned}$$

Orbits? Call $G = \mathbb{Z}$, $X = \mathbb{R}$

Orbit of $x \in X = \mathbb{R}$ is :

$$\begin{aligned} G(x) &:= \{ \varphi(g)(x) \mid g \in G \} \\ &= \{ g + x \mid g \in \mathbb{Z} \} \end{aligned}$$



[If $x \in \mathbb{Z} \subset \mathbb{R}$, then in particular $G(x) = \mathbb{Z}$]

Stabilizers of $x \in X = \mathbb{R}$

$$G_x := \{ g \in G \mid \varphi(g)(x) = x \}$$
$$= \{ g \in \mathbb{Z} \mid g + x = x \}$$
$$= \{ 0 \}.$$

2) (Revisited)

$(\mathbb{Z}, +)$ acting on $\mathbb{R}$ by

$$\varphi : \mathbb{Z} \longrightarrow S_{\mathbb{R}}$$
$$n \longmapsto \varphi(n) : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto (-1)^n x$$

Orbits of $x \in \mathbb{R}$. Call $G = \mathbb{Z}$, $X = \mathbb{R}$.

$$G(x) = \{ (-1)^n x \mid n \in \mathbb{Z} \}$$
$$= \{ -x, x \}.$$

For $x = 0$, $G(0) = \{0\}$
$x \neq 0$, $G(x) = \{x, -x\}$, a 2 element set

Stabilizers of x:

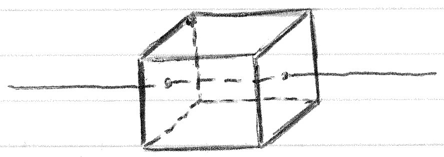
$$G_x = \{ n \in \mathbb{Z} \mid (-1)^n x = x \}$$

For $x = 0$ get $G_0 = \mathbb{Z}$
$x \neq 0$ get $G_x = \{ n \in \mathbb{Z}, n \text{ even} \} = 2\mathbb{Z}$.

3) (Revisited).

$X = \{$ edges of a cube $\}$
$G = \{$ rotations by angle in $\frac{\pi}{2}\mathbb{Z}$ through axis ξ $\}$

Produces three orbits of same size, 4 (different colours)



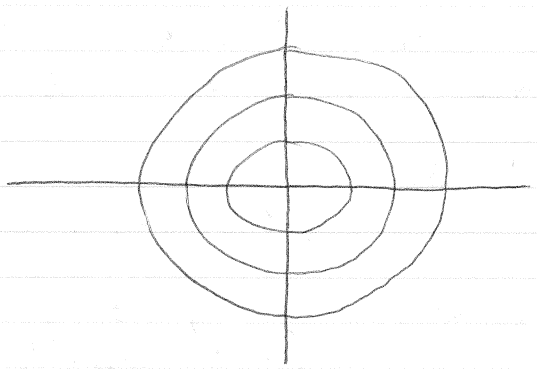
Stabilizers: $G_x = \{e\}$ for any edge $x \in X$.

4) Check for yourself:

$\mathbb{R}$ acting on $\mathbb{C}$ by

$$r \longmapsto \varphi(r) : \mathbb{C} \longrightarrow \mathbb{C}$$
$$x \longmapsto e^{ir} x.$$

What are orbits and stabilizers for given $x \in \mathbb{C}$?



Clumsy notation, introduce shorthand: We usually leave out 'φ' in the notation of an action.

Example: For $\varphi : G \longrightarrow S_X$, replace $\varphi(g)(x)$ by $g(x)$ $\forall g \in G$, $\forall x \in X$.

Example: $G_x := \{ g \in G \mid g(x) = x \}$

$\varphi(g)(\varphi(h)(x))$ now $g(h(x))$.

Proposition: Let G act on a set X, then the G-orbits partition X i.e.

i) Each orbit is non-empty
ii) any $x \in X$ lies in some G-orbit
iii) two orbits are either disjoint or coincide.

Proof: i) Clear since $e(x) = x$ lies in $G(x)$.
ii) $x \in X$ lies in its own orbit $G(x)$
iii) Suppose $z \in G(x) \cap G(y)$

Need to show $G(x) = G(y)$.

Have $z = g_1(x)$ and $z = g_2(y)$.

But then $x = g_1^{-1}(\underbrace{g_1(x)}_{z = g_2(y)}) = g_1^{-1}(g_2(y)) \in G(y)$

In fact any $w \in G(x)$ lies in $G(y)$.

$$w = g_3(x) \Rightarrow w = g_3(g_1^{-1}(g_2(y))) \in G(y)$$

Swapping the roles of x and y, get also $G(y) \subseteq G(x)$

Conclusion $G(y) = G(x)$.

Introduce equivalence relations:

Definition: A binary relation $\sim$ on X (i.e. a subset Σ of $X \times X$) is an equivalence relation on X if

(R) Reflexivity: $x \sim x \quad \forall x \in X$
$[\leftrightarrow (x,x) \in \Sigma]$

(S) Symmetry: $x \sim y \Rightarrow y \sim x$
$[\leftrightarrow (x,y) \in \Sigma \Rightarrow (y,x) \in \Sigma]$

(T) Transitivity: If $x \sim y$ and $y \sim z \Rightarrow x \sim z$
$[\leftrightarrow (x,y) \in \Sigma$ and $(y,z) \in \Sigma \Rightarrow (x,z) \in \Sigma]$

Example: For G acting on a set X, we have subsets of X given, for any x

$$G(x) = \{ g(x) \mid g \in G \}.$$

Then "$y \in G(x)$" is an equivalence relation

S) $x \sim y \iff y \in G(x)$.
$\iff x \in G(y)$; proof of proposition
$\iff y \sim x$.

R) Also have indeed $x \sim x$, ie. $x \in G(x)$.

T) And $x \sim y$ and $y \sim z$ imply

$x \in G(y)$, $x = g_1(y)$ for some $g_1 \in G$
$y \in G(z)$, $y = g_2(z)$ for some $g_2 \in G$

$\Rightarrow x = g_1(y) = g_1(g_2(z)) = (g_1 g_2)(z)$
$\Rightarrow x \in G(z)$.

$\Rightarrow x \sim z$

Remark: To be in the same orbit under a group action defines an <u>equivalence relation</u>

In particular, we can choose $X = G$, so G acts on itself in different ways, eg.

a) By left translation (cf proof of Cayley's Theorem)

$g \in G$ acts on G by

$$L_g : \begin{aligned} G &\longrightarrow G \\ h &\longmapsto gh \end{aligned}$$

b) By 'Conjugation' (Important!)

$$\varphi : \begin{aligned} G &\longrightarrow S_G \\ g &\longmapsto (\varphi(g) : h \longmapsto ghg^{-1}) \end{aligned}$$

In other words, using shorthand

g acts on $h \in X = G$ via

$$g(h) = ghg^{-1}.$$

Check: This gives indeed a homomorphism.

Let $g, g' \in G$

$$\begin{aligned} \underbrace{(gg')}_{\varphi(gg')}(h) &= (gg') \cdot h \cdot (gg')^{-1} \\ &= gg'hg'^{-1}g^{-1} \\ &= \underbrace{g\underbrace{(g'hg'^{-1})}_{g'(h)}g^{-1}}_{g(g'(h))} \\ &= \underbrace{g}_{\varphi(g)\varphi(g')}(g'(h)) \end{aligned}$$