

UiO : Department of Mathematics
University of Oslo

MAT2200 Spring 2023

Revision on groups

Binary algebraic structures

A **binary operation** on a set S is a map

$$* \colon S \times S \to S$$

$$\text{Notation} : *(a, b) = a * b.$$

A pair $(S, *)$ of a set S and a binary operation on $*$ is a **binary algebraic structure**.

Further concepts

- $*$ is **associative** if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.
- $*$ is **commutative** if $a * b = b * a$ for all $a, b \in S$.
- $e \in S$ is an **identity element** if $e * a = a * e = a$ for all $a \in S$.
- $a \in S$ is **inverse** to $b \in S$ if $a * b = b * a = e$.

Isomorphisms

A map $\varphi\colon (S, *) \to (S', *')$ is an **isomorphism** if φ is a bijection and

$$\varphi(a * b) = \varphi(a) *' \varphi(b) \qquad \forall a, b \in S$$

Write $(S, *) \simeq (S', *')$, say that these are **isomorphic**.

All important ("structural") properties are preserved under isomorphism – if $(S, *)$ has the property then $(S', *')$ has it, e.g. "S has identity element", "$*$ is associative", "$*$ is commutative", S is finite, $(S, *)$ is a group, $(S, *)$ is a cyclic group, "In $(S, *)$, every element satisfies $x * x = e$", ...

Groups

A binary algebraic structure $(G, *)$ is a **group** if

1. $*$ is associative.
2. G has an identity element e.
3. For every $a \in G$, there is an element $a^{-1} \in G$ such that

$$a * a^{-1} = a^{-1} * a = e.$$

The identity element and the inverses are unique – there is exactly one identity element $e \in G$ and for each a, exactly one inverse a^{-1}.

Two words

- A group is **abelian** if $*$ is commutative.
- The **order** of a group is the number of elements.

Examples of groups

- These sets, with the operation of addition, are groups:

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}^n$$

- These sets, with the operation of multiplication, are groups:

$$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, GL(n, \mathbb{R}) = \{(n \times n) \text{ invertible matrices}\}$$

- $\mathbb{Z}_n = \{0, \ldots, n-1\}$ with operation

$$a +_n b = \begin{cases} a + b \text{ if } \ a + b \leq n - 1 \\ a + b - n \text{ if } \ a + b \geq n \end{cases},$$

"the integers modulo n".

Group notation

In a group $(G, *)$, typically write ab instead of $a * b$. For n a positive integer:

$$a^n = \overbrace{a \cdots a}^{n}, \quad a^{-n} = \overbrace{a^{-1} \cdots a^{-1}}^{n}, \quad a^0 = e$$

Then have

$$a^m a^n = a^{m+n}$$

If $(G, *)$ is abelian, can write $a + b$ instead of $a * b$. Then write

$$-a = a^{-1}, \quad 0a = 0 = e$$

and for n a positive integer

$$na = \overbrace{a + \cdots + a}^{n}, \quad (-n)a = \overbrace{(-a) + \cdots + (-a)}^{n}$$

Good properties of groups

Cancellation laws and linear equations

If $a, b, c \in G$ are such that

$$ab = ac \text{ or } ba = ca$$

then $b = c$.

For $a, b \in G$, the equations

$$ax = b, \quad ya = b \quad x, y \in G$$

have unique solutions $x = a^{-1}b$, $y = ba^{-1}$.

Subgroups

If G is a group, $H \subseteq G$, then H is a **subgroup** if

1. H is closed under multiplication, that is
$$a, b \in H \Rightarrow ab \in H, \text{ and}$$
2. H is a group with the induced binary operation.

Notation: Write $H \leq G$ for "H is a subgroup of G".

Proving H is a subgroup

Given a subset H of a group G, verifying H is a subgroup can be done by checking

1. H closed under multiplication
2. $e \in H$
3. For every $a \in H$, also $a^{-1} \in H$.

Cyclic (sub)-groups

Let G be a group $a \in G$. The **cyclic subgroup generated by** a is

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \leq G.$$

The **order** of a is the order of $\langle a \rangle$.

Theorem

Let G be a group and $a \in G$.

- If there is no $n > 0$ such that $a^n = e$, then all a^i for different $i \in \mathbb{Z}$ are distinct, and $\langle a \rangle \simeq \mathbb{Z}$.
- Otherwise, let n be the smallest positive integer such that $a^n = e$. Then

  $$\langle a \rangle = \{a^0, a^1, \ldots, a^{n-1}\},$$

  where these elements are distinct, and $\langle a \rangle \simeq \mathbb{Z}_n$

Subgroups of cyclic groups

A group G is **cyclic** if there is an $a \in G$ such that $G = \langle a \rangle$.

Theorem: If G is a cyclic group and $H \leq G$, then H is cyclic.

- Any subgroup of $\mathbb{Z}$ is generated by some $k \in \mathbb{Z}$ and is

$$\langle k \rangle = k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$$

- Any subgroup of $\mathbb{Z}_n$ is generated by some $k \in \mathbb{Z}_n$. With $d = \gcd(k, n)$, we have

$$\langle k \rangle = \langle d \rangle = \{0, d, 2d, \ldots n - d\}$$

and $|\langle k \rangle| = \frac{n}{d}$.

Direct products

Given groups $G_1, \ldots, G_n$, define the **direct product group**

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

with multiplication given by

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n').$$

Theorem

Let $n_1, \ldots, n_k \geq 1$. The group

$$G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

is cyclic if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$. If G is cyclic, then $G \simeq \mathbb{Z}_{n_1 \cdots n_k}$.

Generators for a group

Let G be a group, $g_1, \ldots, g_n \in G$. Say the elements $g_1, \ldots, g_n$ **generate** G if every element g can be written on the form

$$g = g_{i_1}^{e_1} g_{i_2}^{e_2} \cdots g_{i_m}^{e_m}$$

with the $i_j \in \{1, \ldots, n\}$, $e_j \in \mathbb{Z}$.
A group G is **finitely generated** if there exists a finite set of elements $g_1, \ldots, g_n$ such that the g_i generate G.

Examples

Every finite group is finitely generated, $\mathbb{Z}$ is finitely generated, $\mathbb{Q}$ is not finitely generated.

Finitely generated abelian groups

Theorem

Let G be a finitely generated abelian group. Then we can write

$$G \simeq \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{b} \times \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}},$$

where the p_i are primes, the e_i are positive integers.
Up to reordering factors, this presentation is unique.

special case

Let G be a *finite* abelian group. Then we can write

$$G \simeq \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}},$$

Permutation groups

Given a set A, a bijection $\sigma\colon A \to A$ is called a **permutation** of A. These form a group

$$S_A = \{\sigma \mid \sigma \text{ is a permutation of } A\}$$

with the binary operation of composition:

$$\sigma_1\sigma_2 = \sigma_1 \circ \sigma_2.$$

For the set $A = \{1, \ldots, n\}$, write $S_n = S_A$.

Cayley's theorem: Every group G is isomorphic to a subgroup of S_G.

More on symmetric groups

In S_n, write

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

A **cycle** in S_A is an element of the form

$$\sigma = (a_1\ a_2\ \cdots\ a_l),$$

meaning

$$\sigma(a_i) = a_{i+1} \text{ for } 1 \leq i \leq l-1$$
$$\sigma(a_l) = a_1$$
$$\sigma(b) = b \text{ if } b \notin \{a_1, \ldots, a_l\}$$

Even more on symmetric groups

Two cycles

$$(a_1 \cdots a_l) \text{ and } (b_1 \cdots b_m)$$

are **disjoint** if $a_i \neq b_j$ for all i, j. In S_n, every element σ can be written as

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$$

where the σ_i are pairwise disjoint cycles.

Example

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4).$$

Transpositions and the alternating groups

A cycle of length two, $\tau = (a_1\ a_2)$ is called a **transposition**.

Theorem

Every $\sigma \in S_n$ can be written as

$$\sigma = \tau_1 \tau_2 \cdots \tau_l,$$

If σ is a product as above with l even/odd, say that σ is even/odd. Define the **alternating group** on n letters

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\} \leq S_n$$

Subgroups and cosets

Let G be a group, $H \leq G$. The **left coset of** H containing a is

$$aH = \{ah \mid h \in H\} \subseteq G,$$

the **right coset of** H containing a is

$$Ha = \{ha \mid h \in H\} \subseteq G.$$

Every element of G lies in a unique left[1] coset of H. We have

$$aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH.$$

Write

$$G/H = \{\text{left cosets of } H\}.$$

The **index** of H in G is

$$(G : H) = |G/H|.$$

[1] All statements about left cosets have equivalent versions for right cosets – we omit those here.

Size of cosets

Let $H \leq G$, and $a \in G$. Then

$$|aH| = |H|$$

If G is finite, since we can partition G into $(G : H)$ cosets of H, all of the same size $|H|$, we get

$$|G| = |H|(G : H),$$

which gives

Lagrange's theorem

If $H \leq G$ and G is finite, then $|H|$ divides $|G|$.

Images and inverses images

Let $\varphi\colon A \to A'$ be a map of sets, let $S \subset A$ and $S' \subset A'$. Then the **image of S under φ** is

$$\varphi[S] = \{\varphi(s) \mid s \in S\}.$$

The **inverse image of S' under φ** is

$$\varphi^{-1}[S'] = \{a \in A \mid \varphi(a) \in S'\}$$

Homomorphisms

Let G, G' be groups. A map $\varphi\colon G \to G'$ is a **homomorphism** if

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \forall a, b \in G.$$

Theorem

Let $\varphi\colon G \to G'$ be a homomorphism, let $a \in G$, let $H \leq G$, $K' \leq G'$. Then

1. $\varphi(e) = e'$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$
3. $\varphi[H]$ is a subgroup of G'
4. $\varphi^{-1}[K']$ is a subgroup of G

Kernels

Let $\varphi\colon G \to G'$ be a homomorphism of groups. The **kernel** of φ is

$$\operatorname{Ker}\varphi = \varphi^{-1}[\{e'\}] = \{g \in G \mid \varphi(g) = e'\}.$$

Cosets of $\operatorname{Ker}\varphi$

Write $H = \operatorname{Ker}\varphi$. For each $a \in G$, we have

$$\varphi^{-1}[\{\varphi(a)\}] = \{g \in G \mid \varphi(g) = \varphi(a)\} = aH = Ha$$

Corollary: A homomorphism of groups $\varphi\colon G \to G'$ is injective if and only if $\operatorname{Ker}\varphi = \{e\}$.

Normal subgroups

Let G be a group, $H \leq G$. Then H is **normal** if for every $a \in G$, we have

$$aH = Ha.$$

Equivalent characterisations

Let H be a subgroup of G. The following are equivalent

1. H is normal.
2. For each $g \in G$, $gHg^{-1} = H$.
3. For each $g \in G$, $h \in H$, we have $ghg^{-1} \in H$
4. There exists a homomorphism $\varphi\colon G \to G'$ such that $H = \operatorname{Ker}\varphi$.

Factor groups

Let G be a group, $H \leq G$. Write

$$G/H = \{\text{left cosets of } H\}.$$

If (and only if) H is normal, we can define a binary operation on G/H by

$$(aH)(bH) = abH, \quad a, b \in G$$

and this makes G/H a group, called the **factor group/quotient group** of G by H.

Example

Let $n \in \mathbb{Z}^+$. Then

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\},$$

and $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

Homomorphisms and factor groups

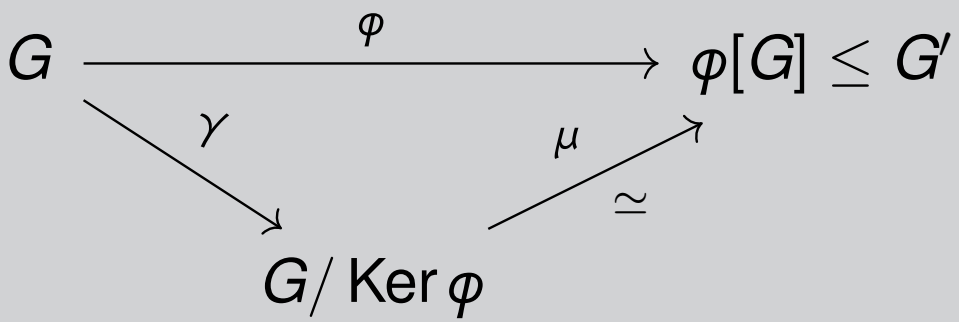
Let G be a group, $H \leq G$ a normal subgroup. There is a surjective homomorphism $\gamma\colon G \to G/H$ given by

$$\gamma(a) = aH,$$

with $\operatorname{Ker}\gamma = H$.

The fundamental theorem of homomorphisms

Let $\varphi\colon G \to G'$ be a group homomorphism. Then we can write $\varphi = \mu \circ \gamma$, with $\mu\colon G/\operatorname{Ker}\varphi \to \varphi[G]$ an isomorphism of groups.



Simple groups

A group G is **simple** if $G \neq \{e\}$ and its only normal subgroups are $\{e\}$ and G.

- An abelian group G is simple if and only if $G \simeq \mathbb{Z}_p$ with p a prime.
- If $n \geq 5$, then A_n is simple.

Group actions

Let G be a group and X a set. An **action** of G on X is a map $*\colon G \times X \to X$, written $*(g, x) = gx$, satisfying

1. $ex = x \quad \forall x \in X$
2. $g_1(g_2x) = (g_1g_2)x \quad \forall g_1, g_2 \in G, x \in X$

A set X with an action of G is called a G**-set**.

Actions as homomorphisms to S_X

An action of G on X gives us a homomorphism $\varphi\colon G \to S_X$ by

$$\varphi(g)(x) = gx.$$

Conversely, a homomorphism $\varphi\colon G \to S_X$ induces an action of G on X by setting

$$gx = \varphi(g)(x).$$

Fix point sets and isotropy groups

Let X be a G-set.

- For $g \in G$, define

$$X_g = \{x \in X \mid gx = x\},$$

  the **fix point set** of g.

- For $x \in X$, define

$$G_x = \{g \in G \mid gx = x\},$$

  the **isotropy group** of x, a subgroup of G.

Orbits of a G-action

Let X be a G-set, $x \in X$. The **orbit** of x is

$$Gx = \{gx \mid g \in G\}.$$

Every element of X lies in precisely one orbit, so X is partitioned into orbits.

Orbits versus isotropy groups

We have a bijection

$$Gx \leftrightarrow G/G_x.$$

If G and X are finite, then

$$|G| = |Gx||G_x|.$$

Counting orbits

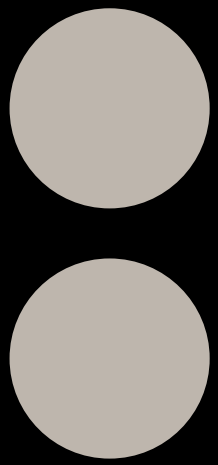
Let G be a finite group and X a finite G-set.

Burnside's formula

Let r be the number of G-orbits in X. Then

$$r = \frac{\sum_{g \in G} |X_g|}{|G|}.$$

UiO : Department of Mathematics
University of Oslo



MAT2200 Spring 2023

Revision on groups

