Groups I

Introduction to Model Theory
(Third hour)

October 9, 2021

Section 1

Groups

Groups

Definition

A *group* is a pair $(G, *)$, where G is a set and $*$ is a binary operation $G \times G \to G$ satisfying the following axioms:

1. The associative law: $x * (y * z) = (x * y) * z$ for $x, y, z \in G$.
2. The identity law: there is an element $e \in G$ such that $x * e = e * x = x$ for all $x \in G$.
3. The inverse law: for any $x \in G$ there is $x' \in G$ such that $x * x' = x' * x = e$, where e is from the identity law.

We say that G is *abelian* if it also satisfies

4. The commutative law: $x * y = y * x$ for any $x, y \in G$.

Example

$(\mathbb{Z}, +)$ is an abelian group, with $e = 0$ and $x' = -x$.

Uniqueness of the identity element

Definition

An *identity element* is an element e such that

$$\forall x \in G : x * e = e * x = x.$$

The identity law says that there is at least one identity element.

Theorem

The identity element is unique (there is only one identity element).

Proof.

If e_1, e_2 are identity elements, then $e_1 = e_1 * e_2 = e_2$. $\square$

So we can talk about "the" identity element.

Uniqueness of inverses

Definition

If $x \in G$, an *inverse* to x is an element y such that $x * y = e = y * x$.

The inverse law says that every element has an inverse.

Theorem

Inverses are unique: x has at most one inverse.

Proof.

Suppose y_1, y_2 are inverses of x. Then
$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2$. □

So we can talk about "the" inverse of x.

The usual notation

- If G is a group, we usually write the group operation as $x \cdot y$, the identity element as 1, and the inverse of x as x^{-1}.
- If G is an abelian group, we often write the group operation as $x + y$, the identity element as 0, and the inverse of x as $-x$. We let $x - y$ denote $x + (-y)$ or $(-y) + x$.

Basic facts

Work in a group $(G, \cdot)$.

- If $xa = ya$, then $x = y$.
- If $ax = ay$, then $x = y$.
- If $ab = 1$, then $a = b^{-1}$ and $b = a^{-1}$.
- $(a^{-1})^{-1} = a$.
- $1^{-1} = 1$.
- $(xy)^{-1} = y^{-1}x^{-1}$.

All of these are easy consequences of the group axioms.

Section 2

Examples of groups

Additive and multiplicative groups

- $(\mathbb{R}, +)$ is a group.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.
- Similarly, these are groups:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{C}, +), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot).$$

All these examples are abelian (commutative).

The general linear group

Let $GL_n(\mathbb{R})$ be the set of $n \times n$ real matrices M with $\det(M) \neq 0$. Then $(GL_n(\mathbb{R}), \cdot)$ is a group, where $M \cdot M'$ is matrix multiplication.

$$\begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} \begin{pmatrix} M'_{11} & M'_{12} \\ M'_{21} & M'_{22} \end{pmatrix} = \begin{pmatrix} M_{11}M'_{11} + M_{12}M'_{21} & M_{11}M'_{12} + M_{12}M'_{22} \\ M_{21}M'_{11} + M_{22}M'_{21} & M_{21}M'_{12} + M_{22}M'_{22} \end{pmatrix}$$

$GL_n(\mathbb{R})$ is called the *general linear group*. It is non-abelian for $n > 1$.

Permutation groups

Let A be a set. Let G be a set of bijections $A \to A$. Suppose G satisfies the following:

- If $f, g \in G$, then $f \circ g \in G$.
- $\mathrm{id}_A \in G$.
- If $f \in G$, then $f^{-1} \in G$.

Then $(G, \circ)$ is a group, usually non-abelian.

The symmetric group

- Let $A = \{1, 2, \dots, n\}$.
- Let G be the set of *all* bijections $A \to A$.
- Then $(G, \circ)$ is called the *nth symmetric group*.
- It has size $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$.
- The symmetric group is non-abelian for $n > 2$.

The group of translations

For $a, b \in \mathbb{R}$, define a function

$$\begin{aligned} T_{a,b} &: \mathbb{R}^2 \to \mathbb{R}^2 \\ (x, y) &\mapsto (x + a, y + b). \end{aligned}$$

Maps of the form $T_{a,b}$ are called *translations*.

Fact

The set of all translations is a permutation group on $\mathbb{R}^2$.

Isometry and homeomorphism groups

Let (M, d) be a metric space.

- Let $\mathrm{Isom}(M)$ be the set of *isometries* of M, bijections $f : M \to M$ such that
$$d(x, y) = d(f(x), f(y)).$$
- Then $(\mathrm{Isom}(M), \circ)$ is a group.

Let X be a topological space.

- Let G be the set of homeomorphisms $X \to X$.
- Then $(G, \circ)$ is a group.

In general, the "symmetries" of a mathematical structure are usually a group.

Section 3

Subgroups

Subgroups

Let $(H, \cdot)$ and $(G, \cdot)$ be groups.

Definition

$(H, \cdot)$ is a *subgroup* of $(G, \cdot)$ if $H \subseteq G$ and $\cdot$ is the restriction of $\cdot$ to H.

Examples:

- $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is *not* a subgroup of $(\mathbb{R}, +)$.

Subgroups as subsets

Let $(G, \cdot)$ be a group.

Fact

Let $H \subseteq G$ be a subset with the following properties:

- *H is closed under $\cdot$: if $x, y \in H$, then $x \cdot y \in H$.*
- *H contains 1_G.*
- *H is closed under inverses: if $x \in H$, then $x^{-1} \in H$.*

Then $(H, \cdot)$ is a subgroup of $(G, \cdot)$.
All subgroups arise this way.

- $\mathbb{Z}$ is a subgroup of $(\mathbb{R}, +)$.
- $\mathbb{N} = \{0, 1, 2, \ldots\}$ is not a subgroup of $(\mathbb{R}, +)$, because $\mathbb{N}$ is not closed under negation.

Permutation groups as subgroups

- G is a permutation group on $\{1, 2, \ldots, n\} \iff G$ is a subgroup of the nth symmetric group.
- More generally, a permutation group on A is the same thing as a subgroup of the group of bijections $A \to A$.

Generation, abstractly

Let G be a group, and $S \subseteq G$ be a subset.

Definition

The subgroup of G *generated by* S, written $\langle S \rangle$, is the smallest subgroup of G containing S.
Equivalently, $\langle S \rangle$ is the intersection of all subgroups of G containing S.

Example

The subgroup of $(\mathbb{R}, +)$ generated by 1 is $(\mathbb{Z}, +)$.

Generation, concretely

Let G be a group and S be a subset.

Fact

Let $S^{-1} = \{g^{-1} : g \in S\}$. Then $\langle S \rangle$ is precisely the set of things of the form $a_1 \cdot a_2 \cdot a_3 \cdots a_n$, where $n \geq 0$ and $a_1, a_2, \ldots, a_n \in S \cup S^{-1}$.

If $n = 0$, then $a_1 \cdot a_2 \cdots a_n$ means 1_G.

Generators

S is a set of *generators* for G, or S *generates* G, if $\langle S \rangle = G$.

Example

1 is a generator of $(\mathbb{Z}, +)$.

Definition

G is *finitely generated* if G is generated by a finite set.

Finite groups are finitely generated, and finitely generated groups are countable.

Generators of the symmetric group

The symmetric group S_n is the set of bijections ($=$ permutations) on $\{1, \ldots, n\}$.
If $a, b \leq n$ and $a \neq b$, then $(a\ b)$ denotes the permutation swapping a and b:

$$x \mapsto \begin{cases} b & \text{if } x = a \\ a & \text{if } x = b \\ x & \text{otherwise.} \end{cases}$$

Such permutations are called *transpositions*.

Fact

S_n is generated by the set of transpositions.

Section 4

Homomorphisms

Homomorphisms

Let $(G, \cdot)$ and $(H, \cdot)$ be groups.

Definition

A *homomorphism* from G to H is a map $f : G \to H$ preserving the group operation:

$$f(x \cdot y) = f(x) \cdot f(y).$$

Example

$f(x) = -3x$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}, +)$, because

$$-3(x + y) = (-3x) + (-3y).$$

Example

$\exp(-)$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R} \setminus \{0\}, \cdot)$, because

$$\exp(x + y) = \exp(x) \cdot \exp(y).$$

Homomorphisms: basic facts

- If $f : G \to H$ is a homomorphism, then f preserves identity and inverses:

$$f(1_G) = 1_H$$
$$f(x^{-1}) = f(x)^{-1}.$$

- If $f : G \to H$ and $g : H \to K$ are homomorphisms, then the composition $g \circ f : G \to K$ is a homomorphism.
- id_G is a homomorphism from G to G.
- If G, H are groups, the constant function $f(x) = 1_H$ is a homomorphism from G to H.

Isomorphisms

Let G, H be groups.

Definition

An *isomorphism* from G to H is a homomorphism $f : G \to H$ that is a bijection. G and H are *isomorphic* if there is at least one isomorphism between them.

Example

Let $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\} = (0, +\infty)$. Then $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}_{>0}, \cdot)$ via the isomorphism $\exp : \mathbb{R} \to \mathbb{R}_{>0}$.

Isomorphisms

1. $\mathrm{id}_G : G \to G$ is an isomorphism.
2. If $f : G \to H$ is an isomorphism, then $f^{-1} : H \to G$ is an isomorphism.
3. If $f : G \to H$ and $g : H \to K$ are isomorphisms, then $(g \circ f) : G \to K$ is an isomorphism.
4. The relation $G \cong H$ is an equivalence relation on the class of groups.
5. If G, H are isomorphic, then we regard G and H as being fundamentally "the same" group, with different labelings.

Groups and permutation groups

Fact (Part of the Cayley representation theorem)

Every group is isomorphic to a permutation group.

Corollary

A structure $(G, \cdot)$ is a group if and only if $(G, \cdot)$ is isomorphic to a permutation group.

Endomorphisms

Definition

An *endomorphism* of G is a homomorphism from G to G.

- The map $f(x) = -3x$ is an endomorphism of $(\mathbb{R}, +)$.
- In an abelian group G, the maps x^2 and x^{-1} are endomorphisms:

$$(xy)^2 = xyxy = xxyy = x^2y^2$$
$$(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}.$$

Automorphisms

Definition

An *automorphism* of G is an isomorphism from G to G, i.e., a bijective endomorphism.

- In any group G, id_G is an automorphism.
- In an abelian group, $x \mapsto x^{-1}$ is an automorphism.
- In $GL_n(\mathbb{R})$, the map $M \mapsto (M^{-1})^T$ is an automorphism, because

$$((M \cdot N)^{-1})^T = (N^{-1} \cdot M^{-1})^T = (M^{-1})^T \cdot (N^{-1})^T.$$

The set of automorphisms of G is denoted $\mathrm{Aut}(G)$.

The automorphism group

- If G is a group, then $(\mathrm{Aut}(G), \circ)$ is a group, the *automorphism group* of G.
- This is analogous to the isometry group of a metric space, or the homeomorphism group of a topological space.

Section 5

Group actions

Group actions

Let G be a group and A be a set. A *(left) action* of G on A is a map

$$(\cdot) : G \times A \to A$$

satisfying the following axioms for $g, h \in G$ and $x \in A$:

$$(g \cdot h) \cdot x = g \cdot (h \cdot x).$$
$$1 \cdot x = x.$$

We say that "G acts on A" if there is a natural action of G on A.
A *G-set* is a set A with an action of G on A.

Matrix action on vector spaces

$GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ via matrix multiplication: if $M_1, M_2 \in GL_n(\mathbb{R})$ and $v \in \mathbb{R}^n$, then

$$M_1(M_2 v) = (M_1 M_2)v$$
$$I_n v = v.$$

Permutation groups and actions

Let G be a permutation group on A. Define

$$(\cdot) : G \times A \to A$$
$$f \cdot x = f(x).$$

This gives an action of G on A, since

$$(f \circ g)(x) = f(g(x))$$
$$\mathrm{id}_A(x) = x.$$

Permutation groups and actions

- Let G be a group acting on a set A.
- Let $\mathrm{Bij}(A)$ be the group of bijections $A \to A$.
- For $g \in G$, define $\phi_g : A \to A$ to be $\phi_g(x) = g \cdot x$.
- Then $g \mapsto \phi_g$ is a homomorphism from G to $\mathrm{Bij}(A)$.

Fact

There is a one-to-one correspondence between

- *Actions of G on A.*
- *Homomorphisms $G \to \mathrm{Bij}(A)$.*

Orbits

Suppose G acts on A.

Definition

The *orbit* of an element $x \in A$ is the set

$$G \cdot x = \{g \cdot x : g \in G\}.$$

Fact

The collection of orbits is a partition of A. The orbits are the equivalence classes of the relation $x \sim y$ defined by

$$x \sim y \iff (\exists g \in G : g \cdot x = y).$$

Orbits

Let G be the group of rotations in $\mathbb{R}^2$ around the origin

$$(x, y) \mapsto (\cos(\theta)x - \sin(\theta)y, \sin(\theta)x + \cos(\theta)y).$$

- G acts on $\mathbb{R}^2$.
- Two points (x, y) and (x', y') are in the same orbit if and only if $x^2 + y^2 = (x')^2 + (y')^2$.
- The orbits of G are the circles

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$$

for $r \geq 0$.

Orbits

- Consider $\mathbb{R}^2$ as a metric space with respect to the usual metric.
- $\mathrm{Isom}(\mathbb{R}^2)$ is the group of plane isometries (translations, reflections, rotations, and glide reflections).
- Let $\mathcal{T}$ be the set of "triangles."
- $\mathrm{Isom}(\mathbb{R}^2)$ acts naturally on $\mathcal{T}$.
- Two triangles ΔABC and ΔDEF are in the same orbit iff they are congruent (in the sense of high school geometry)

$$\Delta ABC \cong \Delta DEF.$$

Stabilizers and orbits

Suppose G acts on A.

Definition

The *stabilizer* of $x \in A$ is the subset

$$\mathrm{Stab}(x) = \{g \in G : g \cdot x = x\}.$$

The stabilizer is always a subgroup of G.

Fact (Orbit-stabilizer theorem)

If $x \in A$ has orbit Gx, then

$$|G| = |\mathrm{Stab}(x)| \cdot |Gx|,$$

where $|S|$ denotes the size of a set S.

Types of group actions

An action of G on A is...

- ...*transitive* if there is only one orbit.
  - Equivalently, for any $x, y \in A$ there is $g \in G$ with $gx = y$.
- ...*faithful* if the homomorphism $G \to \mathrm{Bij}(A)$ is injective.
  - Equivalently, if $g, h \in G$ and $g \neq h$, then there is at least one $x \in A$ with $gx \neq hx$.

Cayley representation theorem

Definition

The *left regular* action of G on G is the action given by the group operation: $g \cdot h = gh$.

Fact

- *The left regular action is faithful and transitive.*
- *The associated homomorphism* $G \to \mathrm{Bij}(G)$ *gives an isomorphism from* G *to a permutation group on* G*.*
- G *is isomorphic to a permutation group.*

Section 6

Conjugation

Conjugation

Define $\phi_g(h)$ to be ghg^{-1}.

- $\phi_g(h)$ is also denoted ${}^g h$; there is no consensus on the notation.
- $\phi_1(x) = x$, and $\phi_{gh}(x) = \phi_g(\phi_h(x))$. Therefore, conjugation defines an action of G on G.
- Orbits are called *conjugacy classes*.

Remark

In an abelian group, $\phi_g(x) = x$, and so the conjugacy class of x is $\{x\}$.

Intuition for conjugation

Suppose $\sigma, \tau \in \mathrm{Isom}(\mathbb{R}^2)$, the group of plane isometries.

- If τ is a rotation by angle θ around a point $p \in \mathbb{R}^2$, then the conjugate $\phi_\sigma(\tau)$ is a rotation by $\pm\theta$ around $\sigma(p)$.
- If τ is a reflection over a line ℓ, then $\phi_\sigma(\tau)$ is the reflection over the line $\sigma(\ell)$.
  - The class of reflections is a single conjugacy class.
- If τ is a translation $x \mapsto x + v$, then $\phi_\sigma(\tau)$ is also a translation $x \mapsto x + v'$ for some v' related to v in a certain way.

Intuition for conjugation

Work in the symmetric group $S_n = \mathrm{Bij}(\{1, 2, \ldots, n\})$. Recall that $(a\ b)$ is the transposition swapping a and b.

Fact

If $\sigma \in S_n$ and $\tau = (a\ b)$, then the conjugate $\phi_\sigma(\tau)$ is $(a'\ b')$, where $a' = \sigma(a)$ and $b' = \sigma(b)$.
The class of transpositions is one conjugacy class in S_n.

Inner automorphisms

Work in a group G.

- $\phi_g(hk) = \phi_g(h)\phi_g(k)$.
- Therefore $\phi_g \in \mathrm{Aut}(G)$ for $g \in G$.
- An *inner automorphism* is an automorphism of the form ϕ_g.
- The inner automorphisms of G form a subgroup of $\mathrm{Aut}(G)$.