Group theory notes

Álvaro Romero

December 10, 2023

Contents

1 Basics of groups

Definition 1.1. A Group $(G, \cdot)$ is a group if

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $\exists e \in G$ s.t. $a \cdot e = a = e \cdot a$
3. $\forall a \in G \quad \exists b \in G$ s.t. $ab = e = ba$.

Definition 1.2. The order of

- G is denoted by $|G|$.
- $x \in G : \min\{n | x^n = e, n > 0\} = |\langle x \rangle|$

1.1 Basic group examples

- $\mathbb{Z}/n\mathbb{Z}$ = integers mod n.
- $S_x = \{\tau : X \to X | \, \tau \text{ bijection}\}, \quad S_n = S_{\{1,\dots,n\}}$
- $D_{2n} = \langle r, s | r^n, s^2, srsr \rangle = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

Definition 1.3. $\phi : G \to H$ is called a group *homomorphism* if $\phi(ab) = \phi(a) \cdot \phi(b)$. If ϕ is furthermore a bijection, we call it a group *isomorphism*, and write $G \cong H$

Definition 1.4. $H \leqslant G$ is a *subgroup* if $x, y \in H \implies xy^{-1} \in H$.

Definition 1.5. $N \lhd G$ is a *normal subgroup* if $N \leqslant G$ and if $x \in G$, $n \in N \implies xnx^{-1} \in N$

2 Cyclic groups

Definition 2.1. G is *cyclic* if $\exists x \in G$ s.t. $G = \langle x \rangle = \{x^n | n \in \mathbb{Z}\}$

Theorem 2.1. G is cyclic

$$\implies \begin{array}{ccc} G \cong \mathbb{Z} & \text{or} & G \cong \mathbb{Z}/n\mathbb{Z} \\ x^k \longleftarrow k & & x^k \longleftarrow \bar{k} \end{array}$$

Theorem 2.2. Subgroups of $\mathbb{Z}$ are

- $n\mathbb{Z} = \{nk | \, k \in \mathbb{Z}\}, \; n \geqslant 0$
- $\mathbb{Z}$.

Theorem 2.3. Subgroups of $\mathbb{Z}/n\mathbb{Z} = \langle x \rangle$ are $\langle x^d \rangle$ for d a positive divisor of n.
Moreover

1. $\langle x^l \rangle = \langle x^{(l,n)} \rangle$ where $(l, n) = \gcd(l, n)$
2. $|\langle x^l \rangle| = \frac{n}{(l,n)}$

Recall,

- Subgroups of $\mathbb{Z}/n\mathbb{Z} \leftrightarrow$ subgroups of $\mathbb{Z}$ containing $n\mathbb{Z} \to n\mathbb{Z} \subseteq k\mathbb{Z} \Leftrightarrow k|n$
- $\pi : \mathbb{Z} \to n\mathbb{Z}$ $k\mathbb{Z} \subseteq \mathbb{Z} \implies \pi(k\mathbb{Z}) \leqslant \mathbb{Z}/n\mathbb{Z}$. Applying the inverse image $\pi^{-1}\pi(k\mathbb{Z}) = k\mathbb{Z} + n\mathbb{Z} = (k, n)\mathbb{Z}$ by the Euclidean algorithm.

2.1 Euclidean Algorithm

Theorem 2.4. Let $m, n \in \mathbb{Z}$. Then $\exists a, b \in \mathbb{Z}$ s.t.

$$am + bn = (m, n) := \text{ greatest common divisor of } m \text{ and } n$$

$$\Leftrightarrow \exists 2 \text{ by } 2 \text{ matrix } A \text{ with integer coefficient s.t. } A^{-1} \text{ has integer coeff}$$
$$A \cdot \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} (m, n) \\ 0 \end{pmatrix}.$$

Definition 2.2. $(\mathbb{Z}/n\mathbb{Z})^\times := \{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid (k,n) = 1\}$ and group multiplication is $\bar{k}_1\bar{k}_2 = \overline{k_1 k_2}$

Theorem 2.5. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Where $\mathrm{Aut}(G)$ is the automorphism of G. This is defined, with composition as group multiplication, as

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \mid \phi \text{ group isomorphism}\}.$$

An example of how the above theorem works,

$$\begin{aligned} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) &\cong (\mathbb{Z}/n\mathbb{Z})^\times \\ (\bar{a} \mapsto \bar{k} \cdot \bar{a}) &\longleftarrow \bar{k} \end{aligned}$$

for $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

3 Normal subgroups

Definition 3.1. Let $H \leqslant G$ and $g \in G$,

- $gH := \{gh \mid h \in H\}$ left coset
- $Hg := \{hg \mid h \in H\}$ right coset
- $G/H := \{gH \subseteq G \mid g \in G\}$ left quotient
- $H/G := \{Hg \subseteq G \mid g \in G\}$ right quotient

Notation: $[g] = gH$

Lemma 3.1. $g_1H \cap g_2H = \emptyset \implies g_1H = g_2H \Leftrightarrow g_2^{-1}g_1 \in H$.

Theorem 3.2. $N \lhd G$ normal. Then $G/N = N/G$ and G/N is a group s.t.

$$\begin{aligned} \pi : G &\to G/N \\ g &\mapsto [g] \end{aligned}$$

is a group homomorphism. Moreover, $\ker(\pi) == N$, where $\ker(\pi) = \{x \in G \mid \pi(x) = e\}$.

Theorem 3.3. To give a group homomorphism $G/N \to H$ is the same as giving group hom $\varphi :\ G{-}{>}H$ s.t. $\varphi(N) = e \Leftrightarrow N \leqslant \ker(\varphi)$

Theorem 3.4. $H \leqslant G/N \quad \mapsto \quad \pi^{-1}(H)$ have a 1 to 1 correspondence between normal subgroups of G/N and normal subgroups containing N.

3.1 Three isomorphism theorems

Theorem 3.5 (First)**.** $\phi :\ G \to H$ group hom. $\implies \mathrm{im}(\phi) \cong G/\ker(\phi)$
Also $\mathrm{im}(\phi) \leqslant H$ and $\ker(\phi) \lhd G$.

Theorem 3.6 (Second)**.** $A, B \leqslant G$. Assume $A \leqslant N_G(B) := \{g \in G \mid gBg^{-1} = B\}$, then

$$\frac{AB}{B} \cong \frac{A}{A \cap B},$$

where $AB = \{a \cdot b \,|\, a \in A,\, b \in B\}$. In particular,

- $AB \leqslant G$
- $B \lhd AB$
- $A \cap B \lhd A$

Theorem 3.7 (Third). $H, K \lhd G$. Then,

$$(G/H)/(K/H) \cong G/K,$$

in particular, $K/H \lhd G/H$.

4 Group Actions

Definition 4.1. A group action $G \circlearrowright X$ is a group homorphism $G \to S_X$ that is equivalent to a map

$$\rho : \; G \times X \to X,$$

written as $\rho(g, x) = g \cdot x$ satisfying

- $g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x,\ \forall\, g_1, g_2 \in G$ and $x \in X$,
- $e \cdot x = x,\ \forall\, x \in X$

Group acting on itself

A group can act on itself ($G \circlearrowright G$) in three different ways.

$$(g, x) \longmapsto g \cdot x, \quad \textbf{left-regular action}$$
$$(g, x) \longmapsto x \cdot g^{-1}, \quad \textbf{right-regular action}$$
$$(g, x) \longmapsto gx \cdot g^{-1}, \quad \textbf{adjoint action}$$

4.1 Orbits

Definition 4.2. $G \cdot x = \{g \cdot x \,|\, g \in G\} \subseteq X$ is the orbit through $x \in X$. Furthermore, $X/G = \{G \cdot x \,|\, x \in X\}$ is the set of orbits or the quotient.

Theorem 4.1. $G \circlearrowright X$. Then X is the disjoint union of orbits,

$$X = \bigcup_{[x] \in X/G} G \cdot x$$

ie

$$Gx_1 \cap Gx_2 \neq \emptyset \iff Gx_1 = Gx_2 \iff \exists g \in G \text{ st } gx_1 = x_2.$$

Theorem 4.2 (Lagrange's). Let $H \leqslant G$, then $|H|$ divides $|G|$. In particular

$$|G/H| = \frac{|G|}{|H|},$$

where $|G/H|$ is called the **index**.

Corollary 4.3. $|G| = p$, p prime, $\implies G \cong \mathbb{Z}/p\mathbb{Z}$, the cyclic group.

Note.

Let $H \leqslant G$. Then $G \circlearrowright G/H$, where G/H might be a set if H is not normal; by $(g, V) \mapsto gV$, for $(g, V) \in G \times G/H$, $gV \in G/H$.

Theorem 4.4. Let $G \circlearrowright X$ and $\{x_1, x_2, \dots\}$ representative of G orbits. Then

$$X \cong G/\mathrm{Stab}_G(x_1) \cup G/\mathrm{Stab}_G(x_2) \cup \dots,$$

where $Stab_G(x_i) = \{g \in G \mid gx_i = x_i\}$, ie all the elements in G that fix a given x_i.

Corollary 4.5 (Orbit-Stabilizer formula)**.** Let $G \circlearrowright X$ and $x \in X$. Then $G \cdot x \cong G/\mathrm{Stab}_G(x)$

$$\implies |G \cdot x| = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

From this we can also conclude that $|G \cdot x|$ divides $|G|$.

Corollary 4.6 (Class equation)**.** Let $G \circlearrowright X$,

$$|X| = |\mathrm{Fix}_G(x)| + \sum_{i=1}^{l} \frac{|G|}{|\mathrm{Stab}_G(x_i)|},$$

where $\mathrm{Fix}_G(x) = \{x \in X \mid gx = x \ \forall g \in G\} \iff |G \cdot x| = 1$, the points where the index is 1, and where $x_1, \dots x_l$ are the representatives of all the orbits not in $\mathrm{Fix}_G(x)$.

Corollary 4.7. $\sigma \in S_n$ has a cycle decomposition $\sigma = (a_{1k_1})(a_{k_1+1} \dots) \dots (a_{k_{l-1}+1} \dots a_{k_l})$

$$\text{where } (a_1 \dots a_l) : \begin{cases} a_i \mapsto a_{i+1} \\ a_l \mapsto a_1 \\ x \mapsto x \end{cases}.$$

5 Sylow theorems

Definition 5.1. We define

- The center of G, $Z(G) = \mathrm{Fix}_G^{\mathrm{ad}}(G) \lhd G$ for $G \circlearrowright G$ the adjoint action
- The **centralizer** $C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \mathrm{Stab}_G^{\mathrm{ad}}(x)$.
- Two elements are called **conjugate** if they belong to the same orbit, ie for some $x, y \in G$, $G \cdot_{\mathrm{adj}} x = G \cdot_{\mathrm{adj}} y$
- The adjoint orbits $(G \cdot_{\mathrm{adj}} x)$ are called **conjugacy classes**.

From this we get a modification of the class equation,

Theorem 5.1 (Class equation).

$$|G| = |Z(G)| + \sum_{i=1}^{l} \frac{|G|}{|C_G(g_i)|},$$

where $g_1, \dots, g_l$ are the set of representatives of conjugacy classes not contained in $Z(G)$, the center. A special thing about this is that thanks to $Z(G) \lhd G$, $|Z(G)|$ also divides $|G|$, which is not true for all actions.

Theorem 5.2. $|G| = p^\alpha \implies Z(G) \neq \{e\}$, it can't be the trivial group.

Corollary 5.3. $|G| = p^2$ then G is Abelian $\implies G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by finetely generated Abelian groups theorem.

Theorem 5.4 (Sylow). $|G| = p^\alpha m$ and $p \nmid m$,

1. G has a subgroup P of order p^α, **Sylow p-subgroup**
2. Let Q be a group of order p^k (a p-subgroup), then $\exists g \in G$ s.t. $Q \leqslant pPg^{-1}$
3. $n_p =$ number of Sylow p-subgroups $= |G/N_G(P)| \equiv 1 (\text{mod } p)$ and also $n_p \mid m$

Theorem 5.5 (Cauchy). $p \mid |G| \implies G$ contains elements of order p.

5.1 Classification of small groups

We use the Sylow theorems to find (ideally) normal subgroups ($n_p = 1 \iff p$ is normal). A strategy would be that if n_{p1}, n_{p2} are large, then we could obtain too many elements. Eg if we have to groups P, Q normal and $PQ = G$, $P \cap Q = \{e\} \implies G \cong P \times Q$. And then study elements more carefully. You also have the case when only one is normal, take (Q), but $PQ = G$, $P \cap Q = \{e\}$ still. Then we would have the following action

$$\begin{aligned} \phi : \; & Q \to Aut(P) \\ & q \mapsto \text{ad}_q = qxq^{-1}, \text{ the adjoint action} \end{aligned}$$

$$\implies G \cong P \rtimes_\phi Q.$$

From here we need to know what is P, what is Q and what that homomorphism is. This helps us noting that a lot of them are isom. to the cyclic groups.

Definition 5.2. G is simple if $\{e\}$ and G are the only normal subgroups.

Theorem 5.6. $\mathbb{Z}/p\mathbb{Z}$ is simple.

6 Alternating groups

Definition 6.1 (Alternating groups). We define

- The group homomorphism $\epsilon : S_n \to \{\pm 1\}$, such that $\epsilon(\sigma) = (-1)^k$ if σ is a composition of k transpositions (2-cycles)

- The alternating group $A_n = \ker(\epsilon)$

Structure of A_n

- S_n is generated by 2-cycles
- A_n is generated by 3-cycles

Theorem 6.1. A_n, $n \geqslant 5$ is a simple group. If it's smaller we could understand it in terms of what we know.

7 Finitely generated Abelian groups

Definition 7.1. An abelian group A is finetely generated by a finite set $s_1, \ldots, s_l$ if $\forall a \in A$, $\exists n_i \in \mathbb{Z}$ s.t. $a = \sum_{i=1}^{l} n_i s_i$, a linear combination of the spanning set.

Theorem 7.1. A fin. generated Abelian group. Then we can express it in **invariant factor decomposition**

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/k_1\mathbb{Z} \times \ldots \times \mathbb{Z}/k_l\mathbb{Z},$$

or **primary component decomposition**

$$A \cong \mathbb{Z}^r \times A_{p_1} \times \ldots \times A_{p_r},$$

where the numbers $(r, k_1, \ldots, k_l)$ are uniquely determined by A.

1. $r \geqslant 0$ is called the **rank** and $k_1, \ldots, k_l$ the **invariant factors**
2. $k_i \geqslant 2$ $\forall i$, and $k_i \mid k_{i+1}$ for $1 \leqslant i \leqslant s-1$
3. $A_p := \{a \in A \mid p^k a = 0 \text{ for some } k \geqslant 0\ \}$

Theorem 7.2 (Chinese Reminder)**.** $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$ if $(m, n) = 1$.

From this also follows that you can't have $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \ncong \mathbb{Z}/p^2\mathbb{Z}$