Algebra MATH-310

Lecture 3

Anna Lachowska

September 29, 2025

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures
3. Rings and fields: 5 lectures
4. Review: 1 lecture

Today: Groups: lecture 2

(a) Recall: basic examples of groups

(b) Group homomorphisms and isomorphisms

(c) Presentation of a group in generators and relations

(d) Examples of group homomorphisms

(e) Kernel and image of a group homomorphism

Recall: two groups modulo n

Additive group modulo n

For any $n \in \mathbb{N}, n \geq 2$, the equivalence classes of integers modulo n: $(\mathbb{Z}/n\mathbb{Z}, +, 0) = \{[0], [1], \ldots [n-1]\}$ form an abelian group with respect to addition. $|(\mathbb{Z}/n\mathbb{Z}, +, 0)| = n$.

Multiplicative group modulo n

For any $n \in \mathbb{N}, n \geq 2$, define the group $((\mathbb{Z}/n\mathbb{Z})^*, \cdot, 1) = \{x \in \mathbb{N} : 1 \leq x \leq n,\ \gcd(x, n) = 1\}$. Then $((\mathbb{Z}/n\mathbb{Z},)^* \cdot, 1)$ is an abelian group with respect to multiplication and $|((\mathbb{Z}/n\mathbb{Z})^*, \cdot, 1)| = \varphi(n)$.

Recall: every element of $((\mathbb{Z}/n\mathbb{Z})^*, \cdot, 1)$ has a multiplicative inverse.

$gcd(a,n) = 1 \iff \exists x, y \in \mathbb{Z} : ax + ny = 1$

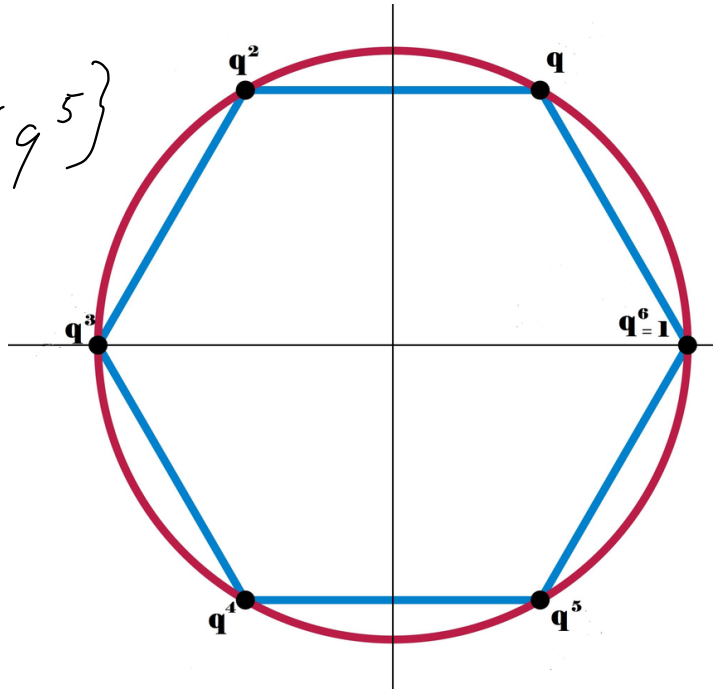
$[a][x] + [0]\cdot[y] = [1] \bmod n \iff [a]\cdot[x] = [1] \Rightarrow [a]^{-1} = [x]$

Group of the roots of unity

Let $n \in \mathbb{N}$, $n \geq 2$ and consider the group $C_n = \{1, q, q^2, \ldots q^{n-1}\}$ where $q = e^{\frac{2\pi i}{n}}$.

Ex. C_6

$\{1, q = e^{\frac{2\pi i}{6}}, q^2, q^3, q^4, q^5\}$



Inverses:

$q \cdot q^5 = 1$

$q^2 \cdot q^4 = 1$

$q^3 \cdot q^3 = 1$

$q^3 \cdot q^5 = q^2$

closed wrt the group operation

$|C_6| = 6$

Intuition: the groups $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ and C_n are "the same"

For any $n \in \mathbb{N}, n \geq 2$,

$(\mathbb{Z}/n\mathbb{Z}, +, 0) = \{[0], [1], \ldots [n-1]\}$ is an abelian group of order n with respect to addition.

$C_n = \{1, q, q^2, \ldots q^{n-1}\}$ where $q = e^{\frac{2\pi i}{n}}$ is an abelian group of order n with respect to multiplication.

$|(\mathbb{Z}/n\mathbb{Z}, +, 0)| = n \quad ; \quad |C_n| = n$

$+ \qquad \cdot$

$0 \longrightarrow 1$

$1 \longrightarrow q = e^{\frac{2\pi i}{n}}$

$k \longrightarrow q^k$

The map respects the group operation

How to tell if two groups are "the same"?

Example: $|G_1| = |G_2|$

$G_1 = \{1, a, b, ab = ba \,|\, a^2 = b^2 = 1\}$.

$abab = aabb = a^2b^2 = 1 \cdot 1 = 1 \Rightarrow (ab)^2 = 1$

$\underbrace{ab}_{ab}\underbrace{ab}_{ba}a = ba^2 = b \cdot 1 = b$; $b\underbrace{ab}_{ba} = b^2a = a$

$|G_1| = 4$

$G_2 = \{1, q, q^2, q^3 \,|\, q^4 = 1\}$. $= C_4 = \{1, i, -1, -i\}$

$|G_2| = 4$

$q \in G_2 : \; q^4 = 1$ and $q^2 \neq 1$

But in G_1, there is no such element: $a^2 = b^2 = (ab)^2 = 1$

Groups G_1 and G_2 have different structure.

Conclusion:

$|G_1| = |G_2|$ does not imply that the groups have the same structure.

Group homomorphisms

Definition

A map $\phi : G \to H$ between two groups is a group homomorphism if

$$\phi(x \cdot_G y) = \phi(x) \cdot_H \phi(y) \qquad \forall x, y \in G.$$

Proposition

If $\phi : G \to H$ is a group homomorphism, then $\phi(1_G) = 1_H$ and $\phi(x^{-1}) = (\phi(x))^{-1}$ for any $x \in G$.

Proof: Let $x, y \in G \Rightarrow \varphi(x \cdot \underbrace{y^{-1} \cdot y}_{1_G}) = \varphi(xy^{-1}) \cdot \varphi(y) = \varphi(x) \quad \forall x, y \in G$

$\Rightarrow \varphi(xy^{-1}) = \varphi(x)(\varphi(y))^{-1}$

$\Rightarrow$ Take $y = x \Rightarrow \underbrace{\varphi(x \cdot x^{-1})}_{\varphi(1_G)} = \varphi(x) \cdot (\varphi(x))^{-1} = 1_H \Rightarrow \varphi(1_G) = 1_H$

Group homomorphisms

$\Rightarrow$ Take $x = 1_G$ $\Rightarrow \varphi(xy^{-1}) = \varphi(y^{-1}) = \underbrace{\varphi(1_G)}_{1_H} \cdot (\varphi(y))^{-1} = (\varphi(y))^{-1}$ $\forall y \in G$

$\Rightarrow \varphi(y^{-1}) = (\varphi(y))^{-1} \quad \forall y \in G$ ▨

Definition

A group homomorphism that is invertible is called an isomorphism:

$$\phi : G \to H, \quad \psi : H \to G : \qquad \phi \circ \psi = \mathrm{Id}_H, \quad \psi \circ \phi = \mathrm{Id}_G.$$

Then $G \simeq H$ are isomorphic groups.
A group automorphism is an isomorphism of a group to itself $\phi : G \to G$.

Example of a group isomorphism: $(\mathbb{Z}/n\mathbb{Z}, +, 0) \simeq C_n$

$C_n = \{1, g, g^2 \dots g^{n-1}\}$

φ : $1 \to [0]$, $g \to [1]$, $g^2 \to [2]$, $\dots$, $g^{n-1} \to [n-1]$ is a bijection

$\varphi(g^i g^j) = \varphi(g^{i+j}) = [i+j]$

$\varphi(g^i) \cdot \varphi(g^j) = [i] + [j]$ mod n

$\varphi(1) = \varphi(\underbrace{g \cdot g \cdots g}_{n}) = \underbrace{\varphi(g) \cdots \varphi(g)}_{n} = \underbrace{[1] + [1] + \dots + [1]}_{n} = [n] = [0]$

$\Rightarrow \varphi : C_n \to \mathbb{Z}/n\mathbb{Z}$ is a group isomorphism

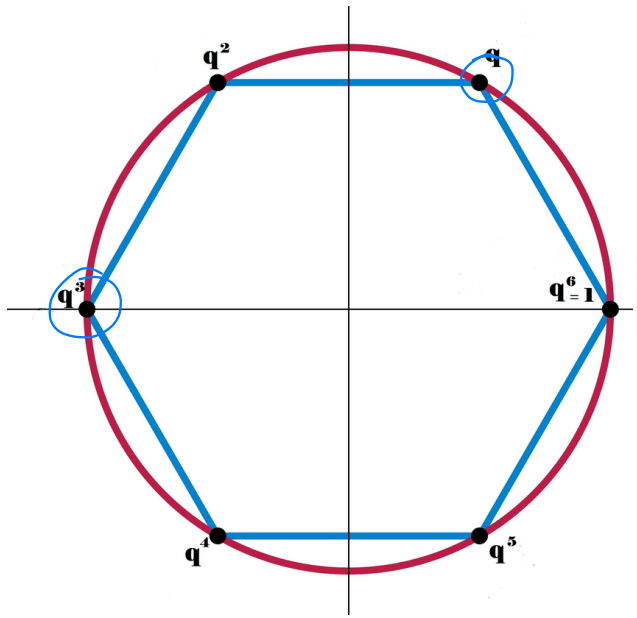
$C_n \simeq \mathbb{Z}/n\mathbb{Z}$ isomorphic groups

Conclusions

1. A group homomorphism is a map between two groups that respects the multiplication.
2. Two isomorphic groups may have different descriptions but they admit a bijective map (an isomorphism) that respects the group operation. In particular, it sends the product to product and inverse to inverse.

$\mathbb{Z}/6\mathbb{Z}$, $n = 6$ $\simeq$ C_n, $n = 6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4



Presentation of a group in generators and relations

Definition

Generators of a group is a minimal set of elements of G such that any element of G can be written as a product of the generators and their inverses.

Example

$C_n = \{1, q, q^2, \dots q^{n-1}\}$ has a generator q.

Can it have any other generators?

Yes! $q^{n-1} = q^{-1}$ for example.

In general, q^k is a generator of $C_n \iff \gcd(k,n) = 1$

If $\gcd(k,n) = d \Rightarrow n = ds,\ k = dt \Rightarrow (q^k)^s = q^{dst} = (q^n)^t = 1$

$\Rightarrow q^k$ only generates a subgroup of order $s = \frac{n}{\gcd(k,n)}$

If $\gcd(k,n) = 1 \Rightarrow \exists\, a, b \in \mathbb{Z}: ak + bn = 1 \Rightarrow (q^k)^a = q \Rightarrow$ it generates C_n.

Generators: example

Let $\mathbb{Q}_+^*$ denote the set of positive rational numbers. Then $\mathbb{Q}_+^*$ is a group with respect to multiplication.

Poll: What are the generators of the group $\mathbb{Q}_+^*$?

A: All squares of prime numbers and 1 cannot get 2 ; only 2^{2k-2m}

B: All positive natural numbers $\mathbb{N}_+$ too many: $6 = 2 \cdot 3$

C: All odd positive integers and 2 too many: $9 = 3 \cdot 3$

D: All odd prime numbers and $\frac{1}{2}$ ✓ $n = p_1^{m_1} \cdots p_n^{m_n} \Rightarrow$ all $\mathbb{N}_+$ $\frac{1}{p_1^{m_1}} \cdots \frac{1}{p_n^{m_n}}$ all natural $\frac{1}{2} \leftrightarrow 2$

E: All numbers of the form $\frac{1}{n}$ where $n \in \mathbb{N}_+$ too many: $\frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2}$

Bonus question: what are the generators of the multiplicative group of nonzero rational numbers $\mathbb{Q}^*$? {all primes and -1}

Relations in a group

Definition

Any equation satisfied by the products of generators is called a relation in a group.

Example

In $C_n = \{1, q, q^2, \dots q^{n-1}\}$ we have a generator q that satisfy the relation $q^n = 1$.
$q^{n+3} = q^3$ is another relation.

Generators and relations in a group are not unique in general!

Group defined by generators and relations

Definition

A presentation of G in terms of generators and relations is an expression $\langle S \mid R \rangle$, where S is a set of generators and R is a minimal set of relations in G, such that any other relation in G follows from these.

Example

$C_n = \langle q \mid q^n = 1 \rangle$. This is the cyclic group of order n.

Example: The Klein group: $K = \langle a, b \mid a^2 = 1,\ b^2 = 1,\ ab = ba \rangle$

$(ab)^2 = a\underbrace{ba}_{ab}b = a^2b^2 = 1$

Another possible def. of the same group $K = \langle a, b \mid a^2 = 1,\ b^2 = 1,\ (ab)^2 = 1 \rangle$

$b = b^{-1}$

$abab = 1 \Rightarrow bab = a^{-1} = a \Rightarrow \underline{ba = ab^{-1} = ab}$

What are they useful for?

Defining group homomorphism in terms of generators and relations

Proposition

Let $G = \langle S \,|R_1, R_2, \ldots R_k\rangle$ be a group defined by generators and relations, and H another group. Define $\phi : G \to H$ as follows

(a) *Define $\phi(s_i)$ for each generator $s_i \in S$* and $\varphi(1_G) = 1_H$

(b) *Set $\phi(x_1 \cdot x_2) = \phi(x_1) \cdot \phi(x_2)$ for any $x_1, x_2 \in G$* , $\varphi(x^{-1}) = (\varphi(x))^{-1} \; \forall x \in G$

(c) *Then $\phi : G \to H$ is a group homomorphism if any only if the defining relations $R_1, \ldots R_k$ in G are satisfied by the images of the generators $\phi(S_i)$ in H.*

Idea: If R_2 is not satisfied by $\varphi(s_i)$ $\Rightarrow$ $\varphi(\underbrace{s_1 \ldots s_k}_{=1\ R_2}) = \varphi(1_G)$

But $\varphi(s_1)\varphi(s_2)\ldots\varphi(s_k) \neq 1_H$ $\not\Rightarrow$

φ is not a group homomorphism

Defining group homomorphism in terms of generators and relations

If $\varphi(S_1) \dots \varphi(S_n)$ satisfy all relations $R_1, R_2 \dots R_k$

$\Rightarrow$ Any equation $S_{j_1} S_{j_2} \dots S_{j_p} = 1$ in G follows from these.

$\Rightarrow$ Then $\varphi(S_{j_1} S_{j_2} \dots S_{j_p}) = \underbrace{\varphi(S_{j_1}) \dots \varphi(S_{j_p}) = 1}_{\text{satisfied in } H}$

$\Rightarrow$ we get a well defined group homomorphism $\varphi: G \to H$.

Examples of group homomorphisms

Let $C_8 = \langle q \mid q^8 = 1 \rangle$, $C_4 = \langle t \mid t^4 = 1 \rangle$.

Let $\phi : C_8 \to C_4$ be a group homomorphism. Need to define $\varphi(q) \in C_4$

$\Rightarrow \varphi(q) = t^k$ Needs to satisfy: $(\varphi(q))^8 = 1$ $\because \varphi(q^8) = (\varphi(q))^8 = 1$

$\varphi(q) = t^k$

$\varphi(q^8) = 1$, $(\varphi(q))^8 = t^{8k}$

$\Rightarrow t^{8k} = 1$, true for all possible k since $t^{8k} = (t^4)^{2k} = 1^{2k} = 1$

		1	q	q^2	q^3	q^4	q^5	q^6	q^7
φ_0	$k=0$	1	1	1	1	1	1	1	1
φ_1	$k=1$	1	t	t^2	t^3	1	t	t^2	t^3
φ_2	$k=2$	1	t^2	1	t^2	1	t^2	1	t^2
φ_3	$k=3$	1	t^3	t^2	t	1	t^3	t^2	t

Examples of group homomorphisms

Let $C_8 = \langle q \mid q^8 = 1 \rangle$, $C_4 = \langle t \mid t^4 = 1 \rangle$.
Let $f : C_4 \to C_8$ be a group homomorphism.

$f(t) = q^k$, the condition to satisfy: $f(t^4) = f(1) = (f(t))^4 = 1$

$1 = q^{4k}$

$\Rightarrow$ k has to be even $\Rightarrow$ 4 homomorphisms

		1	t	t^2	t^3
f_0	$k = 0$	1	1	1	1
f_2	$k = 2$	1	q^2	q^4	q^6
f_4	$k = 4$	1	q^4	1	q^4
f_6	$k = 6$	1	q^6	q^4	q^2

Kernel and image of a group homomorphism

Definition

The kernel of a group homomorphism $\phi : G \to H$ is the set of elements $g \in G$ such that $\phi(g) = 1 \in H$.

Example: $f_4 : C_4 \to C_8 \Rightarrow \ker f_4 = \{1, t^2\}$

$\varphi_1 : C_8 \to C_4 \Rightarrow \ker \varphi_1 = \{1, g^4\}$

Definition

Let $\phi : G \to H$ be a group homomorphism. Then $\phi(G) \subset H$ is called the image of ϕ.

Example: $f_4 : C_4 \to C_8 \Rightarrow \operatorname{Im} f_4 = \{1, g^4\}$

$\varphi_1 : C_8 \to C_4 \Rightarrow \operatorname{Im} \varphi_1 = \{1, t, t^2, t^3\} = C_4$

Properties of the kernel and the image

Proposition

Let $\phi : G \to H$ be a group homomorphism.
Then $\ker\phi \subset G$ is a subgroup in G, and $\mathrm{Im}\phi \subset H$ is a subgroup in H.

Proof: (a) $\varphi(1)=1 \Rightarrow 1 \in \ker\varphi$; if $\varphi(a)=1$ and $\varphi(b)=1$
$\Rightarrow \varphi(ab)=\varphi(a)\cdot\varphi(b)=1\cdot 1 \Rightarrow \ker\varphi$ is closed wrt $\cdot_G$
$a \in \ker\varphi \Rightarrow \varphi(a^{-1})=(\varphi(a))^{-1}=1 \Rightarrow a^{-1}\in\ker\varphi$

$\ker\varphi \subset G$ is a subgroup

(b) $\varphi(1_G)=1_H \Rightarrow 1_H \in \mathrm{Im}\,\varphi$, if $a=\varphi(g_1), b=\varphi(g_2)$
$\Rightarrow ab=\varphi(g_1)\varphi(g_2)=\varphi(g_1g_2) \Rightarrow ab \in \mathrm{Im}\,\varphi$

If $a=\varphi(g) \Rightarrow a^{-1}=(\varphi(g))^{-1}=\varphi(g^{-1}) \in \mathrm{Im}\,\varphi$

$\mathrm{Im}\,\varphi \subset H$ is a subgroup.

Normal subgroup

Definition

Let G be a group. A subgroup $H \subset G$ is a normal subgroup if for any $h \in H$, $g \in G$ we have

$$ghg^{-1} \in H.$$

Notation: $H \trianglelefteq G$.

Proposition

Let $\phi : G \to H$ be a group homomorphism. Then $\ker\phi \trianglelefteq G$ is a normal subgroup in G.

Proof: Let $h \in \ker\varphi$, $g \in G$. Need to show: $ghg^{-1} \in \ker\varphi = H$

$$\varphi(ghg^{-1}) = \varphi(g)\underbrace{\varphi(h)}_{\text{"}1\text{"}}\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1$$

$h \in \ker\varphi$ $\quad 1$

homomorphism

$$\Rightarrow ghg^{-1} \in \ker\varphi$$