Algebra MATH-310

Lecture 3

Anna Lachowska

September ~~29~~ 30, 2024

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) 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 group homomorphisms

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: $(\mathbb{Z}/n\mathbb{Z}, +, 0) = \{[0], [1], \dots [n-1]\}$ 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.

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

$[a] \cdot [x] = [1] \mod n \implies [a]^{-1} = [x]$.

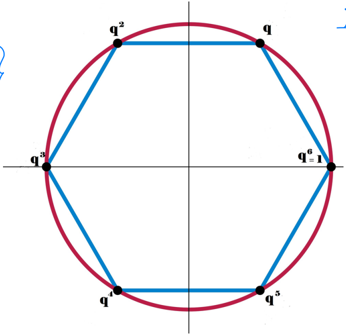
Group of the n-th roots of unity

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

Ex C_6

$\{1, q, q^2, q^3, q^4, q^5\}$

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



Inverses: $q \cdot q^5 = 1$

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

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

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.

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

$$\begin{array}{ccc} + & & \cdot \\ 0 & \longrightarrow & 1 \\ 1 & \longrightarrow & q = e^{\frac{2\pi i}{n}} \end{array}$$

How can we tell when the two groups are "the same"?

Example: $|G_1| = |G_2|$

$G_1 = \{1, a, b, ab = ba \,|a^2 = b^2 = 1\}$. $\quad |G_1| = 4$

$(ab)(ba) = (ab)(ab) = 1 \Rightarrow (ab)^{-1} = (ab)$

$a \cdot ab = a \cdot ba = b$;

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

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

But in G_1 : $a^2 = 1$, $b^2 = 1$, $(ab)^2 = 1 \Rightarrow (\text{any element})^2 = 1$.

Groups G_1 and G_2 have different structure.

Conclusion:

$|G_1| = |G_2|$ does <u>not</u> 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

$$\phi(x \underset{G}{\cdot} y) = \phi(x) \underset{H}{\cdot} \phi(y) \qquad \forall x, y \in G.$$

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

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

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

Group homomorphisms

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

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

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

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

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

$\varphi: \quad 1 \mapsto [0], \quad g \mapsto [1], \quad g^2 \mapsto [2], \quad \dots \quad g^{n-1} \mapsto [n-1]$ is a bijection

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

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

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

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

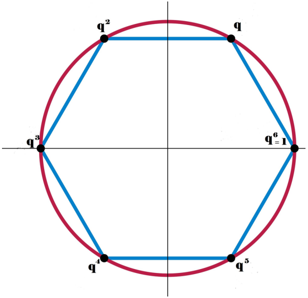
$C_n \simeq \mathbb{Z}/n\mathbb{Z}$ isomorphic groups

Conclusions

1. A group homomorphism is a map between two groups that respects the multiplication.
2. Two isomorphic groups can have a different description but they admit a bijective map (an isomorphism) that sends product to product and inverse to inverse.

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

$C_n = \{1, q, q^2, \ldots q^{n-1}\}$ has a generator q.
Can it have any other generators?

Yes! $q^{n-1} = q^{-1}$

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

If $\gcd(k,n)=d \Rightarrow q^k = q^{dt} \Rightarrow (q^k)^s = 1 \Rightarrow q^k$ generates only a gp of $s = \frac{n}{d}$ elts.
$n = ds$

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 elements of $\mathbb{Q}_+^*$

B: All positive natural numbers $\mathbb{N}_+$

C: All prime numbers

D: All odd positive integers and 2

E: All numbers of the form $\frac{1}{n}$ where $n \in \mathbb{N}_+$

$n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r} \Rightarrow$ get all natural positive numbers

$\frac{1}{p_1^{n_1}} \frac{1}{p_2^{n_2}} \dots \frac{1}{p_r^{n_r}} \Rightarrow$ get all positive rational numbers.

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 equality 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.

$q^{n+3} = q^3$ it follows from the relation $q^n = 1$ by multiplication by q^3: $q^n = 1 \Rightarrow q^{n+3} = q^3$.

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

What are they useful for?

Defining group homomorphism in terms of generators and relations

Proposition

Let $G = \langle S \,|R_1, R_2, \dots R_k\rangle$ 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 $s_i \in S$*

(b) *Set $\phi(x_1 \cdot x_2) = \phi(x_1) \cdot \phi(x_2)$ for any $x_1, x_2 \in G$*

(c) *Then $\phi : G \to H$ is a group homomorphism if any only if all the relations $R_1, \dots R_k$ are satisfied in H for $\phi(S_i)$.*

Idea:

If R_2 is not satisfied by $\varphi(s_i) \Rightarrow \varphi(s_1 \dots s_k) = \varphi(1)$

$R_2 : \; s_1 \dots s_k = 1$

$\varphi(s_1)\varphi(s_2) \cdot \varphi(s_k) \neq 1_H$

$\Rightarrow \varphi$ fails to be a group homomorphism

Defining group homomorphism in terms of generators and relations

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

$\Rightarrow$ Any equation $S_{j_1} S_{j_2} \ldots S_{j_p} = 1$ in G follows from the relations $R_1, R_2 \ldots R_k$ $\Rightarrow$

Then $\varphi(S_{j_1} S_{j_2} \ldots S_{j_p}) = \varphi(S_{j_1}) \varphi(S_{j_2}) \ldots \varphi(S_{j_p}) = 1_H$

is satisfied by the images of the generators

$\Rightarrow$ 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:* $\underbrace{\varphi(q^8)}_{=1} = \varphi(1) = \underbrace{(\varphi(q))^8}_{=t^{8k}}$

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

$\Rightarrow$ *Get* 4 *homomorphisms* $\varphi_1, \varphi_2, \varphi_3, \varphi_4 : C_8 \to C_4$

		1	q	q^2	q^3	q^4	q^5	q^6	q^7
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
φ_0	$k = 0$	1	1	1	1	1	1	1	1

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 is: $f(t^4) = f(1) = (f(t))^4$

$\underset{1}{\overset{\|}{}} = \underset{q^{4k}}{\overset{\|}{}}$

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

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

Definition

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

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

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

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.

<u>Proof</u> (a) $\varphi(1)=1 \Rightarrow 1 \in \ker\varphi$; if $\varphi(a)=1$ and $\varphi(b)=1$
$\Rightarrow \varphi(ab) = \varphi(a)\cdot\varphi(b) = 1\cdot 1 = 1 \Rightarrow \ker\varphi$ is closed wrt products
$a \in \ker\varphi \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1} = 1^{-1} \Rightarrow a^{-1} \in \ker\varphi$

$\Big\}$ $\ker\varphi \subset G$ is a subgroup.

(b) $\varphi(1)=1_H \Rightarrow 1_H \in \mathrm{Im}\,\varphi$; if $a_1 = \varphi(g_1)$, $a_2 = \varphi(g_2)$
$a_1 a_2 = \varphi(g_1)\cdot\varphi(g_2) = \varphi(\underbrace{g_1 g_2}_{\in G}) \Rightarrow a_1 a_2 \in \mathrm{Im}\,\varphi$
If $a = \varphi(g) \Rightarrow a^{-1} = (\varphi(g))^{-1} = \varphi(g^{-1}) \Rightarrow a^{-1} \in \mathrm{Im}\,\varphi$

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

$\blacksquare$

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: $H \trianglelefteq G$. normal subgroup in 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: $ghg^{-1} \in \ker\varphi$

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

$h \in \ker\varphi \Rightarrow$

homomorphism

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