Algebra MATH-310

Lecture 2

Anna Lachowska

September 23, 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-1

(a) Definition and first examples

(b) Subgroups

(c) Cosets and Lagrange's theorem

(d) Application: Euler's and Fermat's theorems

(e) Application: RSA

Fermat's theorem

Poll: The following statement is NOT a Fermat's theorem:

√ A: There are no nonzero integers a, b, c such that $a^3 + b^3 = c^3$

√ B: $a^3 + b^3 \neq c^3$ for any positive integers a, b, c

√ C: $a^n + b^n \neq c^n$ for natural $n \geq 3$ and any positive integers a, b, c

the last Fermat's theorem

D: There exist nonzero integers a, b, c such that $a^n + b^n = c^n$ for some, but not all natural $n \geq 3$ False

√ F: For $a \in \mathbb{Z}_+$ and p a prime that does not divide a, we have $a^{p-1} \equiv 1 \pmod{p}$. little Fermat's theorem

Groups: definition

Definition

A group is a set G with a binary operation $\cdot : G \times G \to G$ satisfying the axioms:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in G$.
2. Neutral element: $\exists\, 1 \in G$ such that $1 \cdot a = a \cdot 1 = a$ for any $a \in G$
3. Inverse: For any $a \in G$ $\exists\, a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} a = 1$.

Definition

A group G is called finite if $|G| < \infty$. In this case $|G| \in \mathbb{N}$ is called the order of the group.

Definition

A group G is called abelian if $a \cdot b = b \cdot a$ for any $a, b \in G$.

Groups: first examples

abelian infinite

1. The real numbers $(\mathbb{R}, +, 0)$ form an abelian group with respect to addition. The integers $(\mathbb{Z}, +, 0)$ form an abelian group with respect to addition.

abelian finite

2. For any $n \in \mathbb{N}, n \geq 2$, the equivalence classes of integers modulo n:
   $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots [n-1]\}$ $\quad n = 6$
   form an abelian group with respect to addition. In $\mathbb{Z}/6Z$, we have $[2] + [5] = [1]$ etc. The order $|\mathbb{Z}/n\mathbb{Z}| = n$.
   $[0]$ is neutral; $[2]+[4]=[0] \Rightarrow [4]$ is the inverse of $[2]$ in $\mathbb{Z}/6\mathbb{Z}$.

3. The group of real invertible $n \times n$ matrices $GL(n, \mathbb{R})$ is a non-abelian infinite group with respect to the matrix multiplication.

infinite non-abelian

$$A \cdot B \neq B \cdot A; \quad \forall\, A \ \exists\ \underline{A^{-1}} \in GL(n\mathbb{R}).$$

$$\mathrm{Id} = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}$$

Groups: further examples

Euler's totient function

Multiplicative group modulo n

Let $n \in \mathbb{Z}_{\geq 2}$, $K = \{x \in \mathbb{N} : 1 \leq x \leq n, \gcd(x, n) = 1\}$. Then K is a group with respect to multiplication modulo n, and $\boxed{|K| = \varphi(n)}$.
Notation: $(\mathbb{Z}/n\mathbb{Z}, \cdot)^*$.

$\{1 \leq x \leq n : \gcd(x,n) = 1\} \iff \exists a, b \in \mathbb{Z} : ax + bn = 1 \iff$
$ax \equiv 1 \pmod{n} \iff [a]\cdot[x] = [1]$
$\Rightarrow [x]$ is invertible.

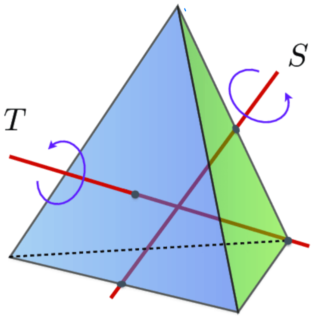
Let $n = 5$. Then $K = \{[1], [2], [3], [4]\}$

$[1]\cdot[1] = [1]$, $[2]\cdot[3] = [1]$, $[4]\cdot[4] = [1] \Rightarrow$

$[2]^{-1} = [3]$, $[3]^{-1} = [2]$, $[4]^{-1} = [4]$,

$[1]$ is the neutral element in K.

Groups: further examples



vertex to midface:
2×4 nontrivial rotations
by $\frac{2\pi}{3}$, $\frac{4\pi}{3}$

mid-edge to mid-edge:
1×3 nontrivial rotations
by π

1 trivial element

12 rotations at least.

Poll: The order of the group of rotational symmetries of the regular tetrahedron is:

A: 6

B: 8

C: 9

D: 12

Conclusions

1. There are groups with respect to addition, multiplication, or another binary operation satisfying the axioms.
2. Important example: additive and multiplicative groups of integers modulo n: $(\mathbb{Z}/n\mathbb{Z}, +) \neq (\mathbb{Z}/n\mathbb{Z}, \cdot)^*$.
In particular, $|(\mathbb{Z}/n\mathbb{Z}, +)| = n$ and $|(\mathbb{Z}/n\mathbb{Z}, \cdot)^*| = \varphi(n)$.

see Appendix B groups_Math310_2023.pdf for more examples of unusual groups (Appendix A and B are not a part of the exam).

Subgroups

Definition

A subgroup $H \subset G$ is a subset in G such that $1 \in H$ and H is closed with respect to the multiplication and taking inverses.

Example: $\{0, \pm 3, \pm 6, \pm 9, \dots\} \subset (\mathbb{Z}, +, 0)$ is a subgroup of integers with respect to addition.

$$3n + 3k = 3(n+k) \in \{0, \pm 3, \pm 6, \dots\}$$

$$3n + (3(-n)) = 0 \quad \text{inverse element}$$

Subgroup generated by a single element

Suppose $g \in G$. Consider the subset $\langle g \rangle = \{1, g^{\pm 1}, g^{\pm 2}, g^{\pm 3}, \dots\} \subset G$. Then $g^i \cdot g^k = g^{i+k} \in \langle g \rangle$, and for each g^i the inverse $g^{-i} \in \langle g \rangle$. Therefore $\langle g \rangle \subset G$ is a subgroup by construction. It is called the subgroup in G generated by the element g. It is the smallest subgroup of G containing g.

Example: $(\mathbb{Z}, +, 0) = G$, $g = 3 \Rightarrow \langle g \rangle = \{0, \pm 3, \pm 6, \pm 9 \dots\} = 3\mathbb{Z}$

$3\mathbb{Z} \subset \mathbb{Z}$ is a subgroup with respect to addition, generated by $3 \in \mathbb{Z}$.

Definition

If there exists $n \in \mathbb{N}_+$ minimal such that $g^n = 1$ in G, then n is called the order of element g. In this case $\langle g \rangle = \{1, g, g^2, \dots g^{n-1}\}$ and $|\langle g \rangle| = n$.

Inverse: $g \cdot g^{n-1} = 1$

Cosets

Definition

Let $H \subset G$ be a subgroup and $g \in G$ an element. The left coset gH is the set of group elements of the form $gH = \{gh,\ h \in H\}$.

Proposition

1. *Two cosets xH and yH are either equal or disjoint: $xH = yH$ or $xH \cap yH = \emptyset$.*
2. *Any element $g \in G$ belongs to a left H-coset*
3. *If H is finite, then $|xH| = |H|$ for any $x \in G$.*

Proof: (1) $xH \cap yH \neq \emptyset \Rightarrow \exists h_1 h_2 \in H : xh_1 = yh_2 \Rightarrow x = yh_2h_1^{-1} = yh_3 \in yH$

Then $\forall h \in H \Rightarrow xh = y\underbrace{h_3 h}_{\in H} \in yH \Rightarrow xH \subset yH$, similarly $yH \subset xH \Rightarrow xH = yH$.

(2) Take the coset of g : $gH = \{g, gh_1, gh_2 \dots\}_{h_1, h_2 \in H}$

(3) Let $f: H \to xH$, $f(h) = xh$ $\forall h \in H$: f is surjective: $xH = \{xh\}_{h \in H}$

f is injective: if $xh_1 = xh_2 \Rightarrow x^{-1}xh_1 = x^{-1}xh_2 \Rightarrow h_1 = h_2$

Example of cosets $(\mathbb{Z}, +, 0) = G$; $3\mathbb{Z} = H \subset \mathbb{Z}$

Coset 0 wrt $3\mathbb{Z}$ in $\mathbb{Z}$

$$\{0 + 3k\}_{k \in \mathbb{Z}} = 3\mathbb{Z} = H$$

Coset of 1 wrt $3\mathbb{Z}$ in $\mathbb{Z}$

$$\{1 + 3k\}_{k \in \mathbb{Z}} = \{1, 4, 7, -2, -5 \dots \}$$

Coset of 10 $= \{10 + 3k\}_{k \in \mathbb{Z}} = \{1, 4, 7, -2, -5 .. 10 \dots \} = \{1 + 3k\}_{k \in \mathbb{Z}}$

Coset of 2 $= \{2 + 3k\}_{k \in \mathbb{Z}} = \{2, 5, -1, -4, \dots \}$

Note that $\mathbb{Z} = \{0 + 3k\}_{k \in \mathbb{Z}} \cup \{1 + 3k\}_{k \in \mathbb{Z}} \cup \{2 + 3k\}_{k \in \mathbb{Z}}$

Lagrange's theorem

Theorem

Let G be a finite group and $H \subset G$ a subgroup. Then $|H|$ divides $|G|$.

Proof: Each $g \in G$ belongs to a left H-coset, and $xH = yH$, or $xH \cap yH = \emptyset$

$\Rightarrow G = \bigcup_{i=1}^{r} x_i H$ disjoint union of left H-cosets, finitely many

$\Rightarrow |G| = \sum_{i=1}^{r} |x_i H|$, but $|x_i H| = |H| \quad \forall x_i$

$\Rightarrow |G| = \sum_{i=1}^{r} |H| = r \cdot |H| \Rightarrow |H|$ divides $|G|$. ▨

Definition

The number of left H-cosets in G is called the index of H in G. Notation: $[G : H] = \frac{|G|}{|H|} \in \mathbb{N}_+$.

Order of an element divides order of the group

Corollary

1. *Let G be a finite group, and $g \in G$. Then the order of g divides $|G|$.*
2. $g^{|G|} = 1$.

Proof: (1) Let $H = \langle g \rangle = \{1, g, g^2 \dots g^{k-1}\}$ where k is the order of g in G.

$\Rightarrow \langle g \rangle = H < G$ subgroup $\Rightarrow$ by Lagrange $\Rightarrow |\langle g \rangle| = k$ divides $|G|$.

(2) We have $g^k = 1 \Rightarrow g^{|G|} = g^{k \cdot t} = (g^k)^t = 1^t = 1$

$|G| = kt, \quad t \in \mathbb{N}$

Applications of Lagrange's theorem

Theorem

(Euler's theorem)
Let $a, n \in \mathbb{Z}_+$ such that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof: Let $G = (\mathbb{Z}/_n\mathbb{Z}, \cdot, 1)^*$, then $|G| = \varphi(n)$

if $\gcd(a,n) = 1 \Rightarrow [a] \in G \Rightarrow$ by Corollary $[a]^{\varphi(n)} = [1] \in G$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$\blacksquare$

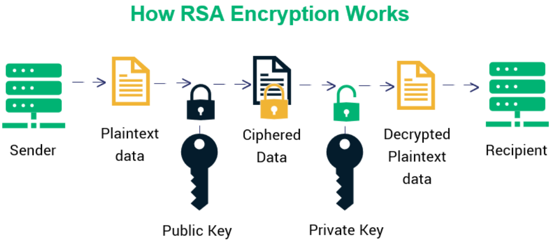
Theorem

(Fermat's little theorem)
Let $a \in \mathbb{Z}_+$ and p a prime that does not divide a. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: $\gcd(a,p) = 1$, $\varphi(p) = p-1 \Rightarrow$ by Euler's thm $\Rightarrow a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p}$ $\blacksquare$

Conclusions

1. If G is a finite group, and $H \subset G$ a subgroup, then $|H|$ divides $|G|$.
2. If G is a finite group, and $g \in G$, then the order of the element g divides $|G|$.
3. Let $a, n \in \mathbb{Z}_+$ such that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.
Why do we care?



RSA encryption system

Setting

1. Choose two large distinct primes p, q.
2. Let $m = pq$. Then $\varphi(m) = (p-1)(q-1)$.
3. Choose $1 < e < m$ such that $\gcd(e, \varphi(m)) = 1$.
4. Use the Euclidean algorithm to find $d \in \mathbb{Z}$ such that $ed - k\varphi(m) = 1$ for some $k \in \mathbb{Z}$.
5. Publish the encryption key (m, e).
6. Keep secret the decryption key (m, d).

Send a message

1. A publishes the encryption key (m, e).
2. B wants to send message x, $0 < x < m$ to A. Then B computes $y \equiv x^e \pmod{m}$ and sends y publicly to A.
3. A computes $y^d = x^{ed} \overset{!!!}{\equiv} x \pmod{m}$.

RSA encryption system

Why does it work?

Proposition

Let p, q be two distinct primes and $m = pq$. Let $1 < e < m$ be such that $\gcd(e, \varphi(m)) = 1$, and $d \in \mathbb{Z}$ such that $ed - k\varphi(m) = 1$ for some $k \in \mathbb{Z}$. Then for any $0 < x < m$, $x^{ed} \equiv x \pmod{m}$.

<u>Proof:</u> (1) If $x = pt \Rightarrow x^{ed} \equiv 0 \pmod{p} \Rightarrow (x^{ed} - x) \equiv 0 \pmod{p}$

(2) If x is not divisible by $p \Rightarrow$ Fermat's thm $x^{p-1} \equiv 1 \pmod{p}$

$$x^{ed} = x^{k\varphi(m)+1} = x^{k(p-1)(q-1)+1} = \underbrace{(x^{p-1})}_{\equiv 1 \pmod{p}}{}^{k(q-1)} x \equiv 1 \cdot x \pmod{p}$$

$$\Rightarrow (x^{ed} - x) \equiv 0 \pmod{p}.$$

The same argument works for $q \Rightarrow (x^{ed} - x)$ divisible by p and q

$$\Rightarrow x^{ed} \equiv x \pmod{\underbrace{pq}_{= m}}$$

RSA encryption system

Why does it work?

Proposition

Let p, q be two distinct primes and $m = pq$. Let $1 < e < m$ be such that $\gcd(e, \varphi(m)) = 1$, and $d \in \mathbb{Z}$ such that $ed - k\varphi(m) = 1$ for some $k \in \mathbb{Z}$. Then for any $0 < x < m$, $x^{ed} \equiv x \pmod{m}$.

Example $p = 3$, $q = 11 \Rightarrow m = pq = 33$, $\varphi(m) = (p-1)(q-1) = 20$

Let $e = 7 \Rightarrow \gcd(7, 20) = 1$. Compute d: $ed - k\varphi(m) = 1$

$$\underbrace{7}_{e} \cdot \underbrace{3}_{d} - \underbrace{20}_{\varphi(m)} \cdot \underbrace{1}_{k} = 1 \Rightarrow d = 3$$

$(m, e) = (33, 7)$ encoding key

$(m, d) = (33, 3)$ decoding key.

Suppose we want to send $x = 20$. Encoding: compute $x^e \pmod{m}$

$$20^7 \pmod{33} = 2^{14} \cdot 5^7 \pmod{33} = (2^5)^2 \cdot 2^4 \cdot 5^7 \pmod{33} = 2^4 (-8)^3 \cdot 5 \pmod{33}$$

$$= -2^{13} \cdot 5 \pmod{33} = -(2^5)^2 \cdot 8 \cdot 5 \pmod{33} = -7 \pmod{33} \equiv 26 \pmod{33}$$

RSA encryption system

Why does it work?

Proposition

Let p, q be two distinct primes and $m = pq$. Let $1 < e < m$ be such that $\gcd(e, \varphi(m)) = 1$, and $d \in \mathbb{Z}$ such that $ed - k\varphi(m) = 1$ for some $k \in \mathbb{Z}$. Then for any $0 < x < m$, $x^{ed} \equiv x \pmod{m}$.

$\Rightarrow$ send $\underline{y = 26}$

To decode: $y^d \pmod{m} \equiv 26^3 \pmod{33} \equiv (-7)^3 \pmod{33}$

$\equiv -49 \cdot 7 \pmod{33} \equiv -16 \cdot 7 \pmod{33} \equiv -13 \pmod{33} \equiv 20 \pmod{33}$

$\Rightarrow y^d \equiv x = 20 \pmod{33}$.

:)