Lecture 4

Last time:

- notion of a subgroup $H \subset S$
  - closed under multiplication
  - inverses
  - contains e

- every group G is (isomorphic to) a subgroup of S_G

- cyclic subgroups: $x \in S \rightsquigarrow \langle x \rangle_S = \{ x^k \mid k \in \mathbb{Z} \}$
  - want to classify them

- every subgroup S of $(\mathbb{Z}, +)$ is
  - $\{0\}$
  - $\mathbb{Z}a$, a smallest positive in S

main Theorem from last time

* recall idea! *

Corollaries of Thm.

Pick $a, b \in \mathbb{Z}$ nonzero

$$S := \mathbb{Z}a + \mathbb{Z}b = \{ra + sb \mid r, s \in \mathbb{Z}\}$$

S: subgroup of $\mathbb{Z}$ (generated by a, b)

why? *

By Thm., $S = \mathbb{Z}d$ — some positive number

Corollary 1

(a) $d \mid a$, $d \mid b$

(b) if $k \mid a$ and $k \mid b \Rightarrow k \mid d$

(c) $\exists$ integers r, s s.t. $d = ra + sb$

↑ the most important part!

Proof: (c) follows from the equality $S = \mathbb{Z}d$ and the definition of S.

(a) $a, b \in S = \mathbb{Z}d \Rightarrow d \mid a, d \mid b$ ✓

(b) if $k \mid a, k \mid b \Rightarrow k \mid \underbrace{(ra + sb)}_{d}$ ✓

—

Note: number d is nothing else but the $\underline{\gcd(a,b)}$

So, we just proved that $\exists r, s$ such that $\gcd(a,b) = ra + sb$ ← this is a nontrivial statement that we proved using group theory!

Example: $a = 10,\ b = 16 \Rightarrow d = \gcd(10, 16) = 2$

$$\underset{b}{2} \cdot 16 + (-3) \cdot \underset{a}{10} = \underset{d}{2}$$

Corollary 2

Elements a, b are coprime iff $\exists r, s$ such that $ra + sb = 1$

Example: $a = 20,\ b = 3,\ 7 \cdot 3 + (-1) \cdot 20 = 1$

Another subgroup of $\mathbb{Z}$ that one can associate to a pair $a, b \in \mathbb{Z}$ is:

$$S := \mathbb{Z}a \cap \mathbb{Z}b$$

Why subgroup? *

Again we know by Thm that:

$$S = m\mathbb{Z}$$

↖ for some positive integer

<u>Example:</u> take $a = 4$, $b = 6$, then want to describe $4\mathbb{Z} \cap 6\mathbb{Z}$?

Claim: $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$ ← why? *

Question: who is 12? (in terms of a, b) ($a = 4$, $b = 6$) Answer: $12 = \text{l.c.m.}(4,6)$

<u>Lemma/Exercise</u>

$a \mid m \iff \mathbb{Z}m \subset \mathbb{Z}a$

↖ ? *

Corollary 3

Recall that $\underbrace{\mathbb{Z}_a \cap \mathbb{Z}_b}_{\text{"}S\text{"}} = \mathbb{Z}_m$. Then:

(a) $a \mid m$, $b \mid m$

(b) if $a \mid n$, $b \mid n \Rightarrow m \mid n$ ← i.e. $m = l.c.m(a,b)$

use Lemma

proof: (a) $\mathbb{Z}_m \subset \mathbb{Z}_a \Leftrightarrow a \mid m$

Same with b.

(b) $\left.\begin{array}{l} a \mid n \Leftrightarrow \mathbb{Z}_n \subset \mathbb{Z}_a \\ b \mid n \Leftrightarrow \mathbb{Z}_n \subset \mathbb{Z}_b \end{array}\right\} \Rightarrow \mathbb{Z}_n \subset \underbrace{\mathbb{Z}_a \cap \mathbb{Z}_b}_{\| \; \mathbb{Z}_m}$

again Lemma

So $\mathbb{Z}_n \subset \mathbb{Z}_m \Leftrightarrow m \mid n$

Upshot

- every nontrivial subgroup of $\mathbb{Z}$ is $\mathbb{Z}a$
- $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z} \cdot \gcd(a,b)$
- $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z} \cdot \operatorname{lcm}(a,b)$
- $a \mid m \iff \mathbb{Z}m \subset \mathbb{Z}a$
- $\gcd(a,b) = ra + sb$ (for some r, s)
- a, b are coprime $\iff ra + sb = 1$

Cyclic subgroups

We are now ready to classify cyclic subgroups of arbitrary group G

Fix $x \in G$, recall $\langle x \rangle_G = \{ x^k \mid k \in \mathbb{Z} \}$

Idea: from $\langle x \rangle_G$ construct a subgroup $S \subset \mathbb{Z}$

↑ already understand them

How to do that:

$$\langle x \rangle_G \rightsquigarrow S := \{ k \in \mathbb{Z} \mid x^k = e \}$$

Example: $G = (\mathbb{R}^*, \cdot)$; $x = -1 \Rightarrow S = 2\mathbb{Z}$

$G = (\mathbb{Z}, +)$, $x = 2 \Rightarrow S = \{0\}$

$G = (\mathbb{Z}/n\mathbb{Z}, +)$, $x = 1 \Rightarrow S = n\mathbb{Z}$

$G = S_3$, $x = (123) \Rightarrow S = 3\mathbb{Z}$

Lemma

(a) S ← is indeed a subgroup of $\mathbb{Z}$

(b) $x^r = x^s \overset{?}{\Longleftrightarrow} r - s \in S$ *

proof

Take $k, p \in S$, want $k+p \in S$ ✓

$x^k = 1,\ x^p = 1 \Rightarrow \underbrace{x^k \cdot x^p}_{\| \; x^{k+p}} = 1$

If $k \in S \Rightarrow x^k = 1 \Rightarrow (x^k)^{-1} = 1$

$\overset{?}{\|}$

$x^{-k} \Rightarrow -k \in S$ ✓

$x^0 = 1 \Rightarrow 0 \in S$ ✓

(b) If $x^r = x^s$ $\xrightarrow{\text{mult. by } x^{-s}}$ $x^{r-s} = 1$

If $x^{r-s} = 1$ $\xrightarrow{\text{mult. by } x^{s}}$ $x^r = x^s$

Remark: in general $a, b, c \in S$ a group

then $ab = ac \iff b = c$ (cancellation law)

"S controls $\langle x \rangle_G$"

Proposition (classification of cyclic subgroups)

Case 1 S a nontrivial $\parallel$ $\mathbb{Z}n$ then $\langle x \rangle_G = \{1, x, x^2, \dots, x^{n-1}\}$

all of them are distinct

multiplication rule as in $(\mathbb{Z}/n\mathbb{Z}, +)$

Case 2 $S = \{0\}$ then $\langle x \rangle_G = \{x^k \mid k \in \mathbb{Z}\}$ a identifies with the group $(\mathbb{Z}, +)$

proof.

Case 1 $S = n\mathbb{Z}$, so by part (b) of Lemma above $\{1, x, x^2, \ldots, x^{n-1}\}$ distinct

$(x^r = x^s \Rightarrow r - s \in S)$

less than $n!$

Also: $\langle x \rangle_S = \{\ldots, x^{-n}, x^{-n+1}, \ldots, x^{-1}, 1, x, x^2, \ldots, x^{n-1}, x^n, x^{n+1}, x^{n+2}, \ldots\}$

So $\langle x \rangle_S = \{1, x, x^2, \ldots, x^{n-1}\}$

Multiplication as in $\mathbb{Z}/n\mathbb{Z}$

Case 2 ← exercise!