Lecture 8

Groups: Sets equipped with one operation. Rehearse group axioms in the book!

Ex: Examples of groups are

- rings with respect to addition
- $S_n = \{\text{all permutations of } \{1,2,\dots,n\}\}$ w.r.t composition
- $D_n \approx$ "symmetries" of regular polygon with n sides (see book)

Def:
- $|G|$ = number of elements of group G. Is called the <u>order</u> of G.
- If $a \in G$, then $|a|$ = smallest $n \geq 1$ such that $a^n = e$. Is called the <u>order</u> of a.

Last lecture we proved:

$$a \text{ has infinite order} \iff (i \neq j \Rightarrow a^i \neq a^j)$$

Def: Subset $H \neq \emptyset$ of group G is called a <u>subgroup</u> of G if H itself is a group w.r.t <u>same</u> operation as in G.

> **Theorem:** Let $H \neq \emptyset$ be a subset of G. If
>
> (i) $a, b \in H \Rightarrow ab \in H$
>
> (ii) $a \in H \Rightarrow a^{-1} \in H$,
>
> then H is a <u>subgroup</u>.

Proof: Compare axioms for group. Note that $e \in H$, since $a \in H \underset{ii)}{\Rightarrow} a^{-1} \in H \underset{i)}{\Rightarrow} aa^{-1} = e \in H$. □

Ex: S subring of $R \Rightarrow (S,+)$ subgroup of $(R,+)$

Ex: Let $G = S_3$. Then $H = \{f \in S_3 : f(2) = 2\}$ is a subgroup, since

i) $f, g \in H \Rightarrow (f \circ g)(2) = f(g(2)) = f(2) = 2 \Rightarrow f \circ g \in H$

ii) $f \in H \Rightarrow f(2) = 2 \Rightarrow f^{-1}(2) = 2 \Rightarrow f^{-1} \in H$.

> **Theorem:** If $|G|$ is <u>finite</u>, we only need to check condition i) above to have a subgroup.

Proof: ~~Take any $a \in G$. If $a \neq e$,~~ Take any $a \in H$. If $a = e$, then $a^{-1} = e \in H$, and we are done. If $a \neq e$ we note, since $|G|$ is finite, that $a^i = a^j$ for some $i \neq j \Rightarrow a^n = e$ for some $n \geq 2$ $\Rightarrow a \cdot a^{n-1} = a^{n-1} \cdot a = e$, that is $a^{-1} = a^{n-1} \in H$. □

Def (Center): The set

$$Z(G) = \{a \in G;\ ag = ga \text{ for all } g \in G\}$$

is called the <u>center</u> of G, and is a subgroup of G (see book).

Note: $Z(G) = G \iff G$ is abelian

Notation: Let $a \in G$. Then $\langle a \rangle = \{a^i;\ i \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, \underset{e}{\underset{\parallel}{a^0}}, a^1, a^2, \dots\}$.

> **Theorem:** $\langle a \rangle$ is a subgroup.

Proof: i) $a^i \cdot a^j = a^{i+j}$

ii) $(a^i)^{-1} = (a^{-1})^i = a^{-i}$ □

Def: $\langle a \rangle$ is called the <u>cyclic</u> subgroup <u>generated</u> by a. A group G is called <u>cyclic</u> if $G = \langle a \rangle$ for some $a \in G$.

Ex: $G = \{1, -1, i, -i\} = \{i^0, i^2, i^1, i^3\} = \langle i \rangle$ (mult. group)

Ex: $(\mathbb{Z}, +) = \langle 1 \rangle = \{k \cdot 1;\ k \in \mathbb{Z}\}$ (add. group)

Ex: $(\mathbb{Z}_n, +) = \langle 1 \rangle$ (add. group)

Ex: $U_8 = \{\text{units in } \mathbb{Z}_8\} = \{1, 3, 5, 7\}$ is <u>not</u> cyclic. We have $a^2 = 1$ for all $a \in U_8$ (check!) (mult. group)

> **Theorem:** (1) $|a|$ infinite $\Rightarrow |\langle a \rangle|$ infinite, and all a^i distinct.
>
> (2) $|a| = n \Rightarrow |\langle a \rangle| = n$ and $\langle a \rangle = \{a^0, a^1, a^2, \dots, a^{n-1}\}$

Proof: Consequence of the very last theorem of Lecture 7.

> **Theorem:** If G is cyclic, then every subgroup H is cyclic.

Proof: Assume $G = \langle a \rangle$. If $H = \{e\}$, then $H = \langle e \rangle$ and we are done. In case $H \neq \{e\}$, then there exists $a^k \in H$, $k \geq 1$. Let k be the <u>smallest</u> such integer.

Take any $a^m \in H$. Div. alg. $m = q \cdot k + r$, where $0 \leq r < k$, and we get

$$a^m = (a^k)^q \cdot a^r \Rightarrow a^r = \underset{\in H}{a^m} \underset{\in H}{(a^k)^{-q}} \in H.$$

But $a^r \in H$ implies $r = 0$ by the minimality of k.

$\Rightarrow a^m = (a^k)^q \in \langle a^k \rangle$. We conclude that $H = \langle a^k \rangle$. □

Def: Let $S \neq \emptyset$ be a subset of G. The set

$$\langle S \rangle = \{\text{"all finite products of elements and inverses of } S\text{"}\}$$

is the <u>subgroup</u> (check!) <u>generated</u> by <u>S</u>.

Note: $\langle S \rangle$ is the smallest subgroup of G that contains S.

Ex: $U_8 = \{1,3,5,7\} = \langle 3,5 \rangle$, since

$$3\cdot 3 = 9 = \underline{1}, \quad 3 = \underline{3}, \quad 5 = \underline{5}, \quad 3\cdot 5 = 15 = \underline{7}.$$

Def (Homomorphism): G, K groups. $f: G \to K$ function.
If
$$f(ab) = f(a)f(b) \quad \text{for all } a,b \in G,$$
then we say that f is a (group) homomorphism.
If, in addition, f is bijective, we say that f is an isomorphism. (An isomorphism $f: G \to G$ is called an automorphism of G.)

Ex: A ring homomorphism/isomorphism $R \to S$ is also a group homomorph./isomorph. $(R,+) \to (S,+)$.

Ex: Let $\mathbb{R}^{**} = \{a \in \mathbb{R};\ a>0\}$. The function $f: (\mathbb{R},+) \to (\mathbb{R}^{**},\cdot)$ defined by $f(x) = 10^x$ is a homomorphism, since
$$f(a+b) = 10^{a+b} = 10^a \cdot 10^b = f(a)\cdot f(b).$$
It is also bijective (check!), which means it is an isomorphism. Conclusion $(\mathbb{R},+) \cong (\mathbb{R}^{**},\cdot)$.

Note that $f^{-1}(x) = {}^{10}\log x$.

Ex: Fix an element $c \in G$ and define $f: G \to G$ by $f(a) = c^{-1}ac$.

f homom.: $f(ab) = c^{-1}abc = (c^{-1}a\underbrace{c)(c^{-1}}_{=e}bc) = f(a)f(b)$

f injective: $f(a) = f(b) \Rightarrow c^{-1}ac = c^{-1}bc \Rightarrow$

$\Rightarrow \underbrace{cc^{-1}}_{=e}a\underbrace{cc^{-1}}_{=e} = \underbrace{cc^{-1}}_{=e}b\underbrace{cc^{-1}}_{=e} \Rightarrow a=b$

f surjective: $a \in G \Rightarrow a = c^{-1}(cac^{-1})c = f(cac^{-1})$

Conclusion: f is an automorphism of G.

Note: f in the example is called the inner automorphism induced by c.

> **Theorem:** Assume G is cyclic, $G = \langle a \rangle$.
> Then ① $|G|$ infinite $\Rightarrow G \cong (\mathbb{Z},+)$
> ② $|G| = n \Rightarrow G \cong (\mathbb{Z}_n,+)$

Proof: ①: We define $f: \mathbb{Z} \to G$ by $f(k) = a^k$.

Homom.: $f(k+l) = a^{k+l} = a^k \cdot a^l = f(k)\cdot f(l)$

Surj. $G \ni a^k = f(k)$ ok.

Inject. $f(k) = f(l) \Rightarrow a^k = a^l \Rightarrow k = l$ lecture 7

Conclusion: $G \cong (\mathbb{Z},+)$

②: We define $f: \mathbb{Z}_n \to G$ by $f([k]) = a^k$.
Is well-defined, since
$[k] = [l] \Leftrightarrow k \equiv l \pmod n \Leftrightarrow a^k = a^l$

A consequence of the final theorem of Lecture 7. Note that $|a| = |G| = n$.

Homom.: $f([k]+[l]) = f([k+l]) = a^{k+l} = a^k \cdot a^l = f([k])\cdot f([l])$

Surj.: $G \ni a^k = f([k])$

Inj. $f([k]) = f([l]) \Rightarrow a^k = a^l \overset{\text{by above}}{\Rightarrow} [k] = [l]$

Conclusion: $G \cong (\mathbb{Z}_n,+)$

> **Theorem:** Let $f: G \to H$ homomorphism.
> Then ① $f(e_G) = e_H$
> ② $f(a^{-1}) = f(a)^{-1}$
> ③ $\operatorname{Im} f = f(G)$ is a subgroup of H

Proof: Imitate proof for rings.

> **Theorem (Cayley's theorem):** Every group G is isomorphic to a group of permutations.

Proof: Let $A(G) = \{$all perm. of the set $G\} = \{$all bijective functions $f: G \to G\}$. $A(G)$ is a group under composition of functions.

For $a \in G$ we define function $\varphi_a: G \to G$ by $\varphi_a(x) = ax$. It follows that φ_a is bijective (check!), i.e. $\varphi_a \in A(G)$.

Define $f: G \to A(G)$ by $f(a) = \varphi_a$.

f homom.: We want to show that
$$f(ab) = \varphi_{ab} \quad \text{and} \quad f(a)\circ f(b) = \varphi_a \circ \varphi_b$$
are equal as functions: For every $x \in G$

- $\varphi_{ab}(x) = (ab)x = \underline{abx}$
- $(\varphi_a \circ \varphi_b)(x) = \varphi_a(\varphi_b(x)) = \varphi_a(bx) = a(bx) = \underline{abx}$ ok!

f injective: $f(a) = f(b) \Leftrightarrow \varphi_a = \varphi_b$ as functions, i.e. for every $x \in G$, $ax = bx$. If we let $x = e$ we get $a\cdot e = b \cdot e \Rightarrow a = b$.

Conclusion: $f: G \to \operatorname{Im} f \subseteq A(G)$ is an isomorphism $\Rightarrow G \cong \operatorname{Im} f$ where $\operatorname{Im} f$ is a group of permutations. □