Lecture 13

Subgroups

Def: Let $(G,*)$ be a group. A subset $H \subseteq G$ is called a subgroup of G if

(1) $H \neq \emptyset$

(2) $x, y \in H \Rightarrow x*y \in H$, $\forall x,y \in H$ — closed under the operation of G

(3) $x \in H \Rightarrow x^{-1} \in H$, $\forall x \in H$ — closed under inverses

If H is a proper subset of G (i.e. $H \subseteq G$ and $H \neq G$), then H is called a proper subgroup of G.

Notation: $H \leq G$ — H is a subgroup of G or $H < G$ — H is a proper subgroup of G

Examples:

1) Trivial subgroups: $\{e\}$ and G.

2) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ and $\mathbb{Q}\setminus\{0\} < \mathbb{R}\setminus\{0\} < \mathbb{C}\setminus\{0\}$.

3) $(\mathbb{Q}\setminus\{0\}, \cdot) \nleq (\mathbb{R}, +)$

4) Let $n \in \mathbb{Z}$, then $n\mathbb{Z} \leq \mathbb{Z}$, i.e. the set of multiples of n is a subgroup of $\mathbb{Z}$.

5) $\mathbb{Q}[\sqrt{2}] < \mathbb{R}\setminus\{0\}$

6) Let $n \in \mathbb{N}\setminus\{0,1\}$, then $\mu_n < \mathbb{C}\setminus\{0\}$

7) Let $\mathbb{I} := \mathbb{R}\setminus\mathbb{Q}$ be the set of irrational numbers.

$(\mathbb{I}, +) \nleq (\mathbb{R}, +)$ because $\sqrt{2} - \sqrt{2} \notin \mathbb{I}$.

8) $\{1, r, r^2, \ldots, r^{n-1}\}$ is a subgroup of D_{2n}.

9) Let $a \in G$. If $|a| = m$, then $\langle a \rangle := \{e, a, a^2, \ldots, a^{m-1}\} \leq G$

If $|a| = \infty$, then $\langle a \rangle := \{a^n : n \in \mathbb{Z}\} \leq G$

Prove it!

$\langle a \rangle$ is called the cyclic subgroup generated by a.

10) $SL(n, \mathbb{C}) = \{A \in GL(n, \mathbb{C}) : \det A = 1\}$ is a subgroup of $GL(n, \mathbb{C})$ called the Special Linear Group of Degree n over $\mathbb{C}$.

11) $Tor(G) \leq G$.

12) If $A, B \subseteq G$, then

Intersection: $A \cap B$ is a subgroup of G. Prove it!

Union: $A \cup B$ is not a subgroup of G. Disprove it!

Remarks:

1. A subgroup of $(G, *)$ are just subsets of G which are themselves groups wrt $*$.
2. $H \leqslant G$ means we consider H with the operation of G.
3. It is possible that $H \subset G$ has the group structure wrt some operation other than the one in G. But in that case H is not a subgroup of G because "being a subgroup" means H is considered with the operation in G.
4. If $H \leqslant G$, then the identity for H is the same as the one for G, and the inverse of x in H is the same as the inverse of x in G. Prove it!

Subgroup Tests

Theorem 16: Let $(G, *)$ be a group and $H \subseteq G$.

H is a subgroup of G $\iff$ (1) $H \neq \emptyset$

(2) For all $a, b \in H$, $a * b^{-1} \in H$.

Multiplicative Notation: $ab^{-1} \in H$

Additive Notation: $a - b \in H$

Proof:

($\Rightarrow$) ✓

($\Leftarrow$)

- $H \neq \emptyset$ by hypothesis (1).
- Let $x \in H$, then $e = x * x^{-1} \in H$. Thus $x^{-1} = e * x^{-1} \in H$. By hyp (2).
- Let $x, y \in H$. Then $x * y = x * (y^{-1})^{-1} \in H$. By hyp (2) and previous step.

∎

Theorem 17: Let $(G, *)$ be finite group and $H \subseteq G$.

H is a subgroup of G $\iff$ (1) $H \neq \phi$

(2) For all $a, b \in H$, $a * b \in H$.

Proof:

($\Rightarrow$) ✓

($\Leftarrow$)
- $H \neq \phi$ by hypothesis (1).
- H is closed under $*$ by hypothesis (2).
- Let $x \in H$. Since G is finite, H is finite. Then there are only finitely many distinct elements $x, x^2, x^3, \ldots$ in H, i.e. $x^a = x^b$ for some $a, b \in \mathbb{Z}^+$, $a > b$. Thus, $e = x^{b-a} \in H$ by hyp (2). Furthermore, $x^{-1} = x^{b-a-1} \in H$.

■

Centralizer, Center, and Normalizer

Def: Let G be a group. Let $A \subseteq G$ be a subset.

(1) The centralizer of A in G is

$$C_G(A) := \{ g \in G \mid ga = ag \text{ for all } a \in A \}$$

set of elements in G that commute with every element of A

If $A = \{a\}$, we write $C_G(a)$.

(2) The centralizer of G in G is called the center of G

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

set of commuting elements of G

(3) If $g \in G$, let $gAg^{-1} := \{ gag^{-1} \mid a \in A \}$. The normalizer of A in G is

$$N_G(A) := \{ g \in G \mid gAg^{-1} = A \}$$

Proposition 18: Let G be a group and $A \subseteq G$.

(1) $C_G(A) \leq N_G(A) \leq G$

(2) If G is abelian, then $Z(G) = G$ and $C_G(A) = N_G(A)$.

Proof: Exercise.

Ex: Prove the statements below.

1) In D_8.
   - $Z(D_8) = \{1, r^2\}$
   - If $A = \{1, r, r^2, r^3\}$, then $C_{D_8}(A) = A$ and $N_{D_8}(A) = D_8$.

2) $Z(S_3) = \{1\}$

3) $Z(GL(n, \mathbb{C})) = \{\lambda I_n : \lambda \in \mathbb{C} \setminus \{0\}\}$ scalar matrices

4) $Z(SL(n, \mathbb{C})) = \{\lambda I_n : \lambda \in \mu_n\}$

Cyclic Groups

Def: A group $(G, *)$ is cyclic if there exists $x \in G$ such that

$$G = \{ x^n : n \in \mathbb{Z} \}.$$

Notation: $G = \langle x \rangle$

G is generated by x and x is a generator of G.

Multiplicative Notation:	$\{ x^n : n \in \mathbb{Z} \} = \{ \dots, x^{-2}, x^{-1}, 1, x, x^2, \dots \}$	$x \cdot x \cdot \dots \cdot x$
Additive Notation:	$\{ nx : n \in \mathbb{Z} \} = \{ \dots, -2x, -x, 0, x, 2x, \dots \}$	$x + x + \dots + x$

Ex:

1. $(\mathbb{Z}, +)$ is cyclic $\quad \mathbb{Z} = \{ \dots, -2(1), -1, 0, 1, 2(1), \dots \} = \{ n(1) : n \in \mathbb{Z} \}$

   $\mathbb{Z} = \langle 1 \rangle$. Also, $\mathbb{Z} = \langle -1 \rangle$.

2. If $G = \langle x \rangle$, then x^{-1} is also a generator of G.

3) $(\mathbb{Z}/n, +)$ is cyclic $\quad \mathbb{Z}/n = \{[0], [1], 2[1], 3[1], \ldots, (n-1)[1]\} = \langle [1] \rangle$

Also $\mathbb{Z}/n = \langle -[1] \rangle = \langle [n-1] \rangle$

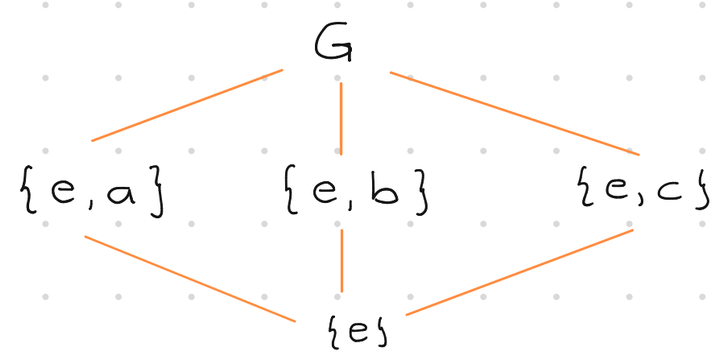
4) $(\mathbb{Z}/8, +) = \langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle$.

$\mathbb{Z}/8 \neq \langle [2] \rangle = \{[0], [2], [4], [6]\}$

5) Let $G = \{e, a, b, c\}$ be the group from Q8, P55. This group is called the Klein group.

G is abelian, $a^2 = b^2 = c^2 = e$, $ab = c$, $ac = b$ and $bc = a$

The Klein group is not cyclic. All its subgroups (except G) are proper.



Proposition 19: Every cyclic group is abelian.

Proof: Exercise.

Proposition 20: Let $G = \langle x \rangle$, then $|G| = |x|$. More specifically,

(1) If $|G| = n$, then $x^n = e$ and $e, x, x^2, \dots, x^{n-1}$ are all distinct.

(2) If G is infinite, then $x^n \neq e$ for all $n \in \mathbb{Z} \setminus \{0\}$ and

$$x^a \neq x^b \quad \text{for all} \quad a \neq b \quad \text{in} \quad \mathbb{Z}.$$

Multiplicative Notation	Additive Notation
(1) $x^n = 1$ and $1, x, x^2, \dots, x^{n-1}$	(1) $nx = 0$ and $0, x, 2x, \dots, (n-1)x$
(2) $x^n \neq 1$ and $x^a \neq x^b$	(2) $nx \neq 0$ and $ax \neq bx$

Proof: Exercise.

Theorem 21: Let $G = \langle x \rangle$.

(1) Let $|x| = n$. $G = \langle x^a \rangle$ iff $\gcd(a, n) = 1$.

(2) Let $|x|$ be infinite. $G = \langle x^a \rangle$ iff $a = \pm 1$.

Proof: Exercise.