

Math 4032 Prof. Pennance – Summary of Lecture on Subgroups

1. Let (G, \odot) be a group. A subset $H \subseteq G$ is a *subgroup* of G , written $H \leq G$ if H is a group under the operation \odot restricted to H .

2. Examples:

- (a) Trivial subgroup. $e_G \leq G$
- (b) Let $K = \{e, a, b, c\}$ be the Klein group. Then $\{e, a\} \leq K$ and $\{e, a, b\} \not\leq K$.
- (c) $2\mathbb{Z} \leq \mathbb{Z}$

3. Let G, H be groups. If $H \leq G$ then:

- (a) $e_H = e_G$.
- (b) If $h \in H$ then h has the same inverse in both H and G .

4. Subgroup criterion: Let (G, \odot) be a group. A subset $H \subseteq G$ is a subgroup of G if and only if the following are true:

- (a) $H \neq \emptyset$
- (b) If $h, h' \in H$ then $h \odot h' \in H$
- (c) If $h \in H$ then $h^{-1} \in H$


5. Finite subgroup criterion (Exercise): Let (G, \odot) be a finite group. A subset $H \subseteq G$ is a subgroup of G if and only if the following are true:

- (a) $H \neq \emptyset$
- (b) If $h, h' \in H$ then $h \odot h' \in H$

6. Examples

- (a) $(\mathbb{R}^+, \cdot) \leq (\mathbb{R} - 0, \cdot)$
- (b) $(\{2^n : n \in \mathbb{Z}\}, \cdot) \leq (\mathbb{R} - 0, \cdot)$
- (c) $(\{z \in \mathbb{C} : z^n = 1\}, \cdot) \leq (\mathbb{C} - 0, \cdot)$
- (d) Let G be a group and $a \in G$. Let $C(a) = \{g \in G : ga = ag\}$ Then $C(a)$ is a subgroup of G .

7. Let (G, \odot) be a group and $a \in G$ then $\langle a \rangle = \{a^n : n \in \mathbb{Z}\} \leq G$. The subgroup $\langle a \rangle$ is called the *cyclic subgroup generated by a*.

8. Let $r \in S_4$ be the permutation  ,

$$\text{then } \langle r \rangle = \left\{ \begin{array}{c} \begin{array}{cc} \circlearrowleft & \circlearrowright \\ \bullet & \bullet \end{array} \\ \begin{array}{cc} \circlearrowleft & \circlearrowright \\ \bullet & \bullet \end{array} \end{array} , \begin{array}{c} \begin{array}{cc} \circlearrowleft & \circlearrowright \\ \bullet & \bullet \end{array} \\ \begin{array}{cc} \circlearrowright & \circlearrowleft \\ \bullet & \bullet \end{array} \end{array} , \begin{array}{c} \begin{array}{cc} \circlearrowleft & \circlearrowright \\ \bullet & \bullet \end{array} \\ \begin{array}{cc} \circlearrowright & \circlearrowleft \\ \bullet & \bullet \end{array} \end{array} , \begin{array}{c} \begin{array}{cc} \circlearrowleft & \circlearrowright \\ \bullet & \bullet \end{array} \\ \begin{array}{cc} \circlearrowleft & \circlearrowright \\ \bullet & \bullet \end{array} \end{array} \right\}$$

9. Multiplicative versus additive notation:

Multiplicative	Additive
ab	$a + b$
e_G	0_G
a^{-1}	$-a$
ab^{-1}	$a - b$
a^n	na
a^{-n}	$-na$

In additive notation

$$\langle a \rangle = \{na : n \in \mathbb{Z}\}$$

Example: $\langle 2 \rangle = \{2n : n \in \mathbb{Z}\}$ denotes the cyclic subgroup of \mathbb{Z} generated by 2. This group is usually denoted $2\mathbb{Z}$.

10. Let (G, \odot) be a group and $a \in G$. Then $\langle a \rangle$ is infinite if and only if $n \mapsto a^n$, $n \in \mathbb{Z}$ is injective.

11. if $\langle a \rangle$ is finite then there exists a positive integer n such that $a^n = e_G$. In this case we define the *order* of a , denoted $o(a)$ to be the least such integer. Otherwise we say that a has infinite order.

12. If $\langle a \rangle$ is finite, $\langle a \rangle = \{a^0, a^1, \dots, a^{n-1}\}$ where $n = o(a)$ and so $|\langle a \rangle| = o(a)$.

13. Let (G, \odot) be a group and $a \in G$ an element of order $o(a)$. If $a^n = e_G$ then n is a multiple of $o(a)$.

14. A finite group G is cyclic if and only if there exists an element $a \in G$ with $o(a) = |G|$.