LECTURE 23

Subgroups

DEFINITION 23.1. *A subset H of a group G is a* ***subgroup*** *of G if H itself is a group under the group multiplication in G. A subgroup H of a group G is said to be* ***proper*** *if H does not equal $\{e\}$ or G.*

Examples

1. The set $\mathbb{R}^+$ of positive real numbers is a subset of the group $\mathbb{R}^\times$ of non-zero real numbers. $\mathbb{R}^+$ is a proper subgroup of $\mathbb{R}^\times$.

2. If R is any ring and S is any subring of R, then S (considered as an additive group) is a subgroup of R considered as an additive group.

3. The group

$$SL(2) = \{M \in M_2(\mathbb{R}) \mid det\ M = 1\}$$

is a subgroup of the group

$$GL(2) = \{M \in M_2(\mathbb{R}) \mid det\ M \neq 0\} \quad .$$

THEOREM 23.2. *A nonempty subset H of a group G is a subgroup of G provided that ı(i) if $a, b \in H$, then $ab \in H$; and ı(ii) if $a \in H$, then $a^{-1} \in H$.*

Proof. Properties (i) and (ii) are, respectively, the closure and inverse axioms of a group. Associativity holds in H, since it holds already in G. We only need to verify that $e \in H$. But (i) and (ii) together imply that $e = aa^{-1} \in H$. Therefore, H is a group. ∎

THEOREM 23.3. *Let H be a nonempty finite subset of a group G. If H is closed under the group operation in G, then H is a subgroup of G.*

Proof. By Theorem 7.7, we need only verify that the inverse of each element of H is also in H. If $a \in H$, then closure implies that $a^k \in H$ for every positive integer k. Since H is finite, these powers can not all be distinct. So a has finite order n by Corollary 7.6 and $a^n = e$. We then have $a^{n-1} = a^{-1} \in H$. ∎

DEFINITION 23.4. *Let G be a group and let $a \in G$. The* ***cyclic subgroup of*** *G* ***generated by*** *a is the set*

$$\langle a \rangle = \left\{ a^k \mid n \in \mathbb{Z} \right\} \quad .$$

DEFINITION 23.5. *If G is a group and there exists an $a \in G$, such that $\langle a \rangle = G$, we say that G is a* ***cyclic group.***

THEOREM 23.6. *If G is a group and $a \in G$, then the set $\langle a \rangle$ is a subgroup of G.*

Proof. The product of any two elements of $\langle a \rangle$ is in $\langle a \rangle$ since

$$a^i a^j = a^{i+j}$$

by Theorem 7.4. We also have

$$a^i a^{-i} = a^0 \equiv e$$

and so every element of $\langle a \rangle$ has an inverse in $\langle a \rangle$. By Theorem 7.7, $\langle a \rangle$ is a subgroup of G. ∎

THEOREM 23.7. *Let G be a group and let $a \in G$. ı(i) If a has infinite order, then $\langle a \rangle$ is a infinite subgroup of G consisting of the distinct elements a^k, $k \in \mathbb{Z}$. ı(ii) If a has finite order n, then $\langle a \rangle$ is a subgroup of order n and $\langle a \rangle = \left\{ e = a^0, a^1, \ldots, a^{n-1} \right\}$.*

Proof.

THEOREM 23.8. *Every subgroup of a cyclic group is itself cyclic.*

Proof.

THEOREM 23.9. *Let S be a nonempty subset of a group G. Let $\langle S \rangle$ denote the set of all possible products of elements of S and their inverses. Then ı(i) $\langle S \rangle$ is a subgroup of G containing S. ı(ii) If H is a subgroup of G containing the set S, then H contains the entire group $\langle S \rangle$. Thus, $\langle S \rangle$ is the smallest subgroup of G containing the set S.*