CHAPTER 2

Further Properties of Groups

2.1. Order

Definition. Suppose that a group G has a finite number of elements. Then we say that G is a finite group, and the number of elements G, denoted by $|G|$, is called the order of the group G. Also, we say that G is an infinite group if the number of elements of G is infinite.

Examples. (1) If $G = \mathbb{Z}_8$, with addition modulo 8, then $|G| = 8$.
(2) The group $(\mathbb{Z}, +)$ is infinite.

Definition. Suppose that G is a group, and that $a \in G$. Suppose further that $\langle a \rangle$ is finite. Then we say that the order of a is $|\langle a \rangle|$. On the other hand, if $\langle a \rangle$ is infinite, then we say that a is of infinite order.

Remark. If $\langle a \rangle$ is finite, then it can be shown that the order of a is the smallest natural number $n \in \mathbb{N}$ such that $a^n = e$.

Examples. (1) In $(\mathbb{Z}_8, +)$, the elements $1, 3, 5$ and 7 are all of order 8, the elements 2 and 6 have order 4, the element 4 has order 2 and the element 0 has order 1.
(2) Is there an element of finite order in $(\mathbb{Z}, +)$?

Note that in Example (1) above, the order of each element of $(\mathbb{Z}_8, +)$ is a divisor of the order of $(\mathbb{Z}_8, +)$. This turns out to be true whenever the group in question is finite.

2.2. Lagrange's Theorem

Theorem 2.1 (Lagrange). *Suppose that G is a finite group, and that H is a subgroup of G. Then $|H|$ divides $|G|$.*

Proof. The proof is a little lengthy, but can essentially be divided into three parts. We shall (i) use the subgroup H to construct an equivalence relation on the group G; (ii) show that H is one of the equivalence classes; and finally (iii) show that all the equivalence classes have the same number of elements.

(i) Define a relation $\mathcal{R}$ on G in the following way: For every $x, y \in G$, we say that $x\mathcal{R}y$ if $x' * y \in H$. Clearly, for every $x \in G$, we have $x\mathcal{R}x$, for $x' * x = e \in H$. Hence $\mathcal{R}$ is reflexive. On the other hand, if $x, y \in G$ and $x\mathcal{R}y$, then $x' * y \in H$, so that $y' * x = (x' * y)' \in H$, whence $y\mathcal{R}x$. Hence $\mathcal{R}$ is symmetric. Furthermore, if $x, y, z \in G$ and $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x' * y \in H$ and $y' * z \in H$, so that $x' * z = (x' * y) * (y' * z) \in H$, whence $x\mathcal{R}z$. Hence $\mathcal{R}$ is transitive. It follows that $\mathcal{R}$ is an equivalence relation on G.

(ii) It now follows that $\mathcal{R}$ partitions G into a finite disjoint union of equivalence classes. Note now that the equivalence class of G containing the identity element e is

$$\{y \in G : e\mathcal{R}y\} = \{y \in G : e' * y \in H\} = H.$$

(iii) Suppose now that K is one of the equivalence classes. Let $a \in K$. Then for every $x \in H$, $a' * (a * x) = x \in H$, so that $a\mathcal{R}(a * x)$, whence $a * x \in K$. We now define $\phi : H \to K$ by writing

$\phi(x) = a * x \in K$ for every $x \in H$. It is easy to see that ϕ is one-to-one, for if $x, y \in H$ and $\phi(x) = \phi(y)$, then $x = y$ in view of left cancellation. On the other hand, ϕ is onto, for if $u \in K$, then $a\mathcal{R}u$, so that $a' * u \in H$. Let $x \in H$ such that $a' * u = x$. Then clearly $u = a * x$, so that $u = \phi(x)$.

It now follows that $|H|$ divides $|G|$. ○

COROLLARY 2.2. *Suppose that G is a finite group, and that $a \in G$. Then the order of a divides $|G|$.*

PROOF. Simply note that the order of a is the order of $\langle a \rangle$. On the other hand, $\langle a \rangle$ is a subgroup of G by Theorem 1.6. The result now follows from Theorem 2.1. ○

2.3. Cyclic Groups

DEFINITION. A group G is said to be cyclic if there exists $a \in G$ such that $G = \langle a \rangle$.

EXAMPLES. (1) $(\mathbb{Z}_8, +) = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$.
(2) $(\{\pm 1\}, \cdot) = \langle -1 \rangle$.
(3) $(\mathbb{Z}, +) = \langle 1 \rangle$.
(4) $(\mathbb{R} \setminus \{0\}, \cdot)$ is not cyclic. To show this, take any $a \in \mathbb{R} \setminus \{0\}$. Then clearly $|a|^{1/2} \in \mathbb{R} \setminus \{0\}$ but $|a|^{1/2} \notin \langle a \rangle$. It follows that $(\mathbb{R} \setminus \{0\}, \cdot) \neq \langle a \rangle$ for any $a \in \mathbb{R}$.

PROPOSITION 2.3. *Suppose that G is a group of order p, where p is a prime. Then G is cyclic.*

PROOF. Let $a \in G$ such that $a \neq e$. Then $\langle a \rangle \neq \{e\}$, so that $|\langle a \rangle| \neq 1$. On the other hand, $\langle a \rangle$ is a subgroup of G by Theorem 1.6, and so $|\langle a \rangle|$ divides p by Theorem 2.1. It follows that $\langle a \rangle = G$. ○

PROPOSITION 2.4. *A finite group G is cyclic if and only if G contains an element of order $|G|$.*

PROOF. Let $a \in G$ be of order $|G| = n$. Then $a, a^2, \ldots, a^n \in G$ are distinct, so that

$$G = \{a, a^2, \ldots, a^n\} \subseteq \langle a \rangle.$$

It follows that $G = \langle a \rangle$. On the other hand, if G does not contain any element of order $|G|$, then for every $x \in G$, $\langle x \rangle = \{x, x^2, \ldots, x^m\}$ for some $m \in \mathbb{N}$ where m is a proper divisor of $|G|$ by Corollary 2.2, so that $m < |G|$. It follows that $\langle x \rangle \neq G$. Hence G is not cyclic. ○

PROPOSITION 2.5. *Suppose that G is a cyclic group. Then G is abelian.*

PROOF. Let $a \in G$ such that $G = \langle a \rangle$. Then for every $x, y \in G$, there exist $m, n \in \mathbb{Z}$ such that $x = a^m$ and $y = a^n$. It follows that $x * y = a^m a^n = a^{m+n} = a^n a^m = y * x$. Hence G is abelian. ○

PROPOSITION 2.6. *Suppose that G is a cyclic group, and that H is a subgroup of G. Then H is cyclic.*

PROOF. Let $G = \langle a \rangle$, where $a \in G$. If $H = \{e\}$, then clearly H is cyclic. Suppose now that $H \neq \{e\}$. Then there exists $n \in \mathbb{Z} \setminus \{0\}$ such that $a^n, a^{-n} \in H$. Let $m = \min\{n \in \mathbb{N} : a^n \in H\}$. We shall show that $H = \langle a^m \rangle$. Since $a^m \in H$ and H is a group, we must have $\langle a^m \rangle \subseteq H$. It therefore suffices to show that $H \subseteq \langle a^m \rangle$. Suppose on the contrary that $x \in H$ and $x \notin \langle a^m \rangle$. Since $x \in G = \langle a \rangle$, there exists $n \in \mathbb{Z}$ such that $x = a^n$. Let $q, r \in \mathbb{Z}$ such that $n = mq + r$ and $0 \leqslant r < m$. Since $x \notin \langle a^m \rangle$, we must have $r \neq 0$. Note now that $a^r = a^{n-mq} = a^n(a^{-m})^q \in H$. But $r < m$, contradicting the minimality of m. ○

Problems for Chapter 2

1. Suppose that $(G, *)$ is an abelian group, and that $x, y, z \in G$. Suppose further that the orders of x, y, z are $3, 4, 6$ respectively. What are the orders of the elements $x * x$, $y * y$, $z * z$, $x * y$, $x * z$ and $y * z$? Justify your assertions.

2. Suppose that G is a finite group of order n and with identity element e. Determine which elements $x \in G$ satisfy $x^n = e$, and justify your assertion.

3. Suppose that G is an abelian group.
   (i) Suppose further that $H = \{x \in G : x \text{ is of finite order}\}$. Prove that H is a subgroup of G.
   (ii) Let $n \in \mathbb{N}$ be fixed. Is $K = \{x \in G : x \text{ is of order } n\}$ a subgroup of G? Justify your assertion.

4. Suppose that $(G, *)$ is a group with identity element e. Suppose further that $x * x = e$ for every $x \in G$. Prove that G is abelian.

5. Prove that $(\mathbb{Q}, +)$ is a group, and that it is not cyclic.