MTHM024/MTH714U **Group Theory**

Notes 1 **Autumn 2011**

---

1 The Fundamental Theorem of Finite Abelian Groups

We can't describe all the groups of order n, but at least we can describe the abelian groups:

Theorem 1.1 *Any finite abelian group G can be written in the form*

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r},$$

where $1 < n_1 \mid n_2 \mid \cdots \mid n_r$. *Moreover, if also*

$$G \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_s},$$

where $1 < m_1 \mid m_2 \mid \cdots \mid m_s$, *then* $r = s$ *and* $n_i = m_i$ *for* $i = 1, 2, \dots, r$.

Remark 1 We need the divisibility condition in order to get the uniqueness part of the theorem. For example,

$$C_2 \times C_6 \cong C_2 \times C_2 \times C_3;$$

the first expression, but not the second, satisfies this condition.

Remark 2 The proof given below is a kludge. There is an elegant proof of the theorem, which you should meet if you study Rings and Modules, or which you can read in a good algebra book. An abelian group can be regarded as a module over the ring $\mathbb{Z}$, and the Fundamental Theorem above is a special case of a structure theorem for finitely-generated modules over principal ideal domains.

We need a couple of preliminaries before embarking on the proof. The *exponent* of a group G is the smallest positive integer n such that $g^n = 1$ for all $g \in G$. Equivalently, it is the least common multiple of the orders of the elements of G. Note that the exponent of any subgroup or factor group of G divides the exponent of G; and, by Lagrange's Theorem, the exponent of a group divides its order.

For example, the symmetric group S_3 contains elements of orders 2 and 3, so its exponent is 6. However, it doesn't contain an element of order 6.

Lemma 1.2 *If G is abelian with exponent n, then G contains an element of order n.*

Proof Write $n = p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes. Since n is the l.c.m. of orders of elements, there is an element with order divisible by $p_i^{a_i}$, and hence some power of it (say g_i) has order exactly $p_i^{a_i}$. Now in an abelian group, if two (or more) elements have pairwise coprime orders, then the order of their product is the product of their orders. So $g_1 \cdots g_r$ is the required element.

Proof of the Theorem We will prove the existence, but not the uniqueness. We use induction on $|G|$; so we suppose the theorem is true for abelian groups of smaller order than G.

Let n be the exponent of G; take a to be an element of order n, and let $A = \langle a \rangle$, so $A \cong C_n$. Let B be a subgroup of G of largest order subject to the condition that $A \cap B = \{1\}$. We *claim* that

$$AB = G.$$

Suppose this is proved. Since A and B are normal subgroups, it follows that $G = A \times B$. By induction, B can be expressed as a direct product of cyclic groups satisfying the divisibility condition; and the order of the largest one divides n, since n is the exponent of G. So we have the required decomposition of G.

Thus it remains to prove the claim. Suppose, for a contradiction, that $AB \neq G$. Then G/AB contains an element of prime order p dividing n; so an element x in this coset satisfies $x \notin AB$, $x^p \in AB$. Let $x^p = a^k b$ where $b \in B$.

Case 1: $p \mid k$. Let $k = pl$, and let $y = xa^{-l}$. Then $y \notin B$ (for if it were, then $x = ya^l \in AB$, contrary to assumption.) Now $B' = \langle B, y \rangle$ is a subgroup p times as large as B with $A \cap B' = \{1\}$, contradicting the definition of B. (If $A \cap B' \neq 1$, then $xa^{-l}b \in A$ for some $b \in B$, whence $x \in AB$.)

Case 2: If p does not divide k, then the order of x is divisible by a higher power of p than the order of a, contradicting the fact that the order of a is the exponent of G.

In either case we have a contradiction to the assumption that $AB \neq G$. So our claim is proved.

Using the uniqueness part of the theorem (which we didn't prove), we can in principle count the abelian groups of order n; we simply have to list all expressions for n as a product of factors each dividing the next. For example, let $n = 72$. The expressions are:

$$72$$
$$2 \cdot 36$$
$$2 \cdot 2 \cdot 18$$
$$3 \cdot 24$$
$$6 \cdot 12$$
$$2 \cdot 6 \cdot 6$$

So there are six abelian groups of order 72, up to isomorphism.

Exercise Let $A(n)$ be the number of abelian groups of order n.

(a) Let p be a prime and a a positive integer. Prove that $A(p^a)$ is the number of *partitions* of a, that is, the number of expressions for a as a sum of positive integers, where order is not important).

(b) Show that $A(p^a) \leq 2^{a-1}$ for $a \geq 1$ and p prime. [*Hint:* the number of expressions for a as a sum of positive integers, where order is important, is 2^{a-1}.]

(c) Let $n = p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r$ are positive integers. Show that

$$A(n) = A(p_1^{a_1}) \cdots A(p_r^{a_r}).$$

(d) Deduce that $A(n) \leq n/2$ for all $n > 1$.