Abelian groups

1 Definition

An *Abelian group* is a set A with a binary operation $\circ$ satisfying the following conditions:

(A1) For all $a,b,c \in A$, we have $a\circ(b\circ c) = (a\circ b)\circ c$ (the *associative law*).

(A2) There is an element $e \in A$ such that $a\circ e = a$ for all $a \in A$.

(A3) For any $a \in A$, there exists $b \in A$ such that $a \circ b = e$.

(A4) For all $a,b \in A$, we have $a\circ b = b\circ a$ (the *commutative law*).

The first three axioms are almost identical to the axioms for a group. (In the case of a group,we normally say, for example, $a\circ e = e\circ a = a$ in Axiom (A2); this is obviously not necessary if (A4) holds.) Thus, *an Abelian group is a group satisfying the commutative law*.

Since many important Abelian groups arise as additive structures in various number systems (the integers, real numbers, integers mod m, etc.), it is very common to write the group operation as $+$ instead of $\circ$. With this convention it is natural to write 0 instead of e in (A2), and $-a$ instead of b in (A3). We usually adopt this convention, which we describe as “additive notation”. However, multiplicative structures (the positive rationals, the non-zero complex numbers) also form Abelian groups, and for these we might write ab for $a\circ b$, 1 for e, and a^{-1} for b in (A3); we say that such a group is written with “multiplicative notation”.

A *homomorphism* is a map $\chi : A \to B$ between Abelian groups satisfying $\chi(a_1\circ a_2) = \chi(a_1)\circ\chi(a_2)$. (Sometimes, as common in algebra, we write $a\chi$ instead of $\chi(a)$.) An example we will see below is a *character* of A, which is a homomorphism from A to the multiplicative group of non-zero complex numbers. If A is written additively, a character χ thus satisfies $\chi(a_1+a_2) = \chi(a_1)\chi(a_2)$.

A homomorphism which is one-to-one and onto is called an *isomorphism*. Two Abelian groups are *isomorphic* if there is an isomorphism between them. Isomorphic groups are regarded as “the same” from a structural or group-theoretic point of view, even though their elements might be quite different kinds of object. We write $A \cong B$ to denote “A is isomorphic to B”.

The *order* of a finite group is the number of elements it contains. The *order* of the element a is the smallest positive integer n such that $na = 0$ (assuming that

A is written in additive notation). A connection between these concepts will be seen in the next section. In general, the order of any element of a group divides the order of the group.

2 The Fundamental Theorem of Finite Abelian Groups

The structure of finite Abelian groups can be described completely.

2.1 Cyclic groups

A *cyclic group* is one whose elements are all of the form na for $n \in \mathbb{Z}$, for some fixed element a. (Here, if n is positive, then na means $a + \cdots + a$ with n summands; $0a$ is the group element 0; and $(-m)a = -(ma)$, the inverse of ma, for positive m. The element a is called a *generator* of the group. Any cyclic group is Abelian.

In a finite cyclic group of order n, the generator satisfies $na = 0$, and n is the smallest positive integer with this property. In other words, the order of the generator is equal to the order of the group (though the sense of the word “order” is different).

Any two finite cyclic groups of the same order are isomorphic. We denote the cyclic group of order n by C_n. Two important realisations of C_n are:

- the additive group of integers modulo n (generated by 1);
- the multiplicative group of complex nth roots of unity (generated by $\mathrm{e}^{2\pi\mathrm{i}/n}$).

2.2 Direct sum

The *direct sum* $A \oplus B$ of two Abelian groups A and B is the set of all ordered pairs (a,b), with $a \in A$ and $b \in B$; the operation is given by the rule

$$(a_1,b_1) + (a_2,b_2) = (a_1 + b_1, a_2 + b_2).$$

It is an Abelian group, whose zero is $(0,0)$ (the first 0 being the zero of A and the second that of B), and in which the inverse of (a,b) is $(-a,-b)$.

The definition of direct sum is easily extended to more than two Abelian groups.

If the groups are written in multiplicative notation, we usually speak of *direct product* rather than direct sum, and write it as $A \times B$.

2.3 The Fundamental Theorem

The Fundamental Theorem of Finite Abelian Groups states, in part:

Theorem 1 *Any finite Abelian group is isomorphic to a direct sum of cyclic groups.*

We need more than this, because two different direct sums may be isomorphic. For example, $C_2 \oplus C_3 \cong C_6$. (If a and b are generators of the summands, then $2a = 3b = 0$, and successive multiples of (a,b) are (a,b), $(0,2b)$, $(a,0)$, $(0,b)$, $(a,2b)$, and $(0,0)$.) There are two standard resolutions of this problem.

(a) An Abelian group is in *Smith canonical form* if it is written as

$$C_{n_1} \oplus \cdots \oplus C_{n_r},$$

where $n_1, \ldots, n_r$ are integers greater than 1 and n_i divides n_{i+1} for $1 \leq i \leq r-1$.

(b) An Abelian group is in *prime-power canonical form* if it is written as

$$C_{q_1} \oplus \cdots \oplus C_{q_r},$$

where $q_1, \ldots, q_r$ are prime powers greater than 1.

Theorem 2 *(a) Any finite Abelian group can be written in Smith canonical form.. If two groups in Smith canonical form are isomorphic, then the multisets of orders of the cyclic factors are equal.*

(b) The same holds with "prime-power" in place of "Smith".

To convert Smith into prime-power and *vice versa*, use the fact that if $n = q_1 \cdots q_m$, where $q_1, \ldots, q_m$ are powers of distinct prime numbers, then

$$C_n \cong C_{q_1} \oplus \cdots \oplus C_{q_m}.$$

Thus, from Smith to prime-power, simply factorise the orders of the cyclic factors. From prime-power to Smith, gather up the largest power of each prime and multiply them; then repeat until nothing remains.

For example, the group $C_4 \oplus C_{12} \oplus C_{36}$ is in Smith canonical form; the group $C_4 \oplus C_4 \oplus C_4 \oplus C_3 \oplus C_9$ is in prime-power canonical form; and these two groups are isomorphic.

2.4 A consequence

It follows from the Fundamental Theorem that, if m is the least common multiple of the orders of the elements of the Abelian group A, then there is an element of order m in A. (The number m with this property is the order of the largest cyclic factor in the Smith canonical form of A.)

This is not true in arbitrary (non-Abelian) groups.

3 Characters

As defined earlier, a *character* of A is a homomorphism from A to the multiplicative group of non-zero complex numbers. The characters of A themselves form a multiplicative Abelian group, where $(\chi\psi)(a) = (\chi(a))(\psi(a))$. The group of characters of A is the *dual group* of A, denoted by A^*.

Theorem 3 *The dual group of a finite Abelian group A is isomorphic to A.*

This is easily seen for cyclic groups. If $A = C_n$, generated by a, then the characters of A all have the form

$$\chi_j(ka) = \mathrm{e}^{2\pi\mathrm{i}jk/n}$$

where j belongs to the integers mod n; thus χ_1 generates A^*. Now the theorem is extended to all finite Abelian groups by using the Fundamental Theorem.

4 Groups of units

Let$\mathbb{Z}/n$ denote the integers modulo n. The additive group of $\mathbb{Z}/n$ is a cyclic group of order n, as we have seen. The multiplicative structure is more intricate.

First, we must select which elements to use. An element a of $\mathbb{Z}/n$ is a *unit* if there exists b such that $ab = 1$ in $\mathbb{Z}/n$ (that is, $ab \equiv 1 \pmod{n}$). Using Euclid's Algorithm, we see that a is a unit if and only if a is coprime to n, that is, $\gcd(a,n) = 1$.) Moreover, the set of units is a multiplicative group, called the *group of units* modulo n and denoted by $U(n)$. The order of this group is *Euler's function* $\phi(n)$. The next theorem gives its structure.

Theorem 4 *(a) If $n = q_1 \cdots q_r$, where $q_1, \ldots, q_r$ are powers of distinct primes, then*

$$U(n) \cong U(q_1) \times \cdots \times U(q_r).$$

(b) If p is an odd prime and $m > 0$, then $U(p^m)$ is cyclic of order $p^{m-1}(p-1)$.

(c)

$$U(2^m) \cong \begin{cases} 1 & \textit{if } m = 1; \\ C_2 & \textit{if } m = 2; \\ C_2 \times C_{2^{m-2}} & \textit{if } m \geq 3. \end{cases}.$$

Note that the decomposition given by the theorem is not usually in canonical form. For example,

$$U(35) \cong U(5) \times U(7) \cong C_4 \times C_6.$$

The Smith canonical form of this group is $C_2 \times C_{12}$, while the prime-power canonical form is $C_2 \times C_4 \times C_3$.

It follows from the above theorem that $U(n)$ is cyclic if and only if $n = p^a$, $n = 2p^a$, or $n = 4$, where p^a is an odd prime power. In these cases, a generator of $U(n)$ is called a *primitive root* of n. For example, $U(9)$ is cyclic of order 6, and 2 is a primitive root of 9.

In general, the maximum order of an element of $U(n)$ (which is the least common multiple of the orders of all elements) is $\lambda(n)$, where λ is *Carmichael's lambda-function*. An element of order $\lambda(n)$ is called a *primitive lambda-root* of n. For example, $\lambda(35) = 12$, and 2 is a primitive lambda-root of 35.

Peter J. Cameron
September 13, 2004