Michel Waldschmidt Update: *12/11/2013*

SEAMS School 2013 ITB
Number theory

Structure of finite abelian groups

Recall that a direct (or Cartesian) product of abelian groups is an abelian group. We first study the simplest abelian groups, namely the cyclic groups, next we decompose any finite abelian group into a direct product of cyclic groups.

1 Cyclic groups

Two cyclic groups of the same order are isomorphic. For n a positive integer, we denote by C_n the cyclic group of order a. Examples are the additive group $\mathbf{Z}/n\mathbf{Z}$, generated by the class of 1 modulo n, and the multiplicative group of n-th roots of unity in $\mathbf{C}^\times$, generated by $e^{2i\pi/n}$.

Let G be a cyclic group of order n generated by t. If we write G additively, then an element x of G is a generator of G if and only if $x = kt$ with $k \in \mathbf{Z}$ satisfying $\gcd(k,n) = 1$. If we write G multiplicatively, then an element x of G is a generator of G if and only if $x = t^k$ with $k \in \mathbf{Z}$ satisfying $\gcd(k,n) = 1$. It follows that the number of generators of G is $\varphi(n)$, where φ is Euler function. Recall that $\varphi(n)$ is the number of integers m in the range $1 \le m \le n$ which are prime to n.

Any subgroup of a cyclic group G is cyclic, its order divides the order of G. Conversely, if G is cyclic of order n and if d divides n, then G has a unique subgroup of order d. If G is generated by t and if $n = dd'$, then the unique subgroup of G of order d is the subgroup generated by $d't$ if G is written additively, by $t^{d'}$ if G is written multiplicatively. As a consequence, a direct product $C_a \times C_b$ of two cyclic groups of orders a and b respectively is cyclic if and only if a and b are relatively prime.

Any quotient of a cyclic group is cyclic. If G' is a subgroup of G and if t is a generator of G, then G/G' is generated by the class of t modulo G'.

Example. If G is a finite group of order p where p is prime, then any element other than the unity in G is a generator of G. Conversely, if any element other than the unity in a group G is a generator, then the order of G is either 1 or a prime number.

2 Exponent of a finite abelian group

The exponent e of a finite abelian group G is the least common multiple of the orders of its elements. From this definition, it follows that e is the gcd of the positive integers n such that $nx = 0$ for any $x \in G$, when G is written additively, such that $x^n = 1$ for any $x \in G$, when G is written multiplicatively.

Proposition 1. *Let G be a finite abelian group of exponent e. Then there exists $x \in G$ of order e.*

Proof. Let us write G additively. Let $x \in G$ be an element of order a and $y \in G$ be an element of order b. Let $m = \mathrm{ppcm}(a, b)$. From the Fundamental Theorem of Arithmetic (unique decomposition of an integer into prime factors), it follows that there exist divisors a' and b' of a and b respectively, with $\gcd(a', b') = 1$, such that $m = a'b'$. Then $x' = (a/a')x$ has order a', $y' = (b/b')y$ has order b', and $x'y'$ has order m.

By induction on n, it follows that for any finite set $x_1, \ldots, x_n$ of elements of G of orders $a_1, \ldots, a_n$, there exists an element of G of order $\mathrm{ppcm}(a_1, \ldots, a_n)$. This completes the proof of Proposition 1.

$\square$

We have seen that a direct product $C_a \times C_b$ of two cyclic groups is cyclic if and only if their orders a and b are relatively prime. Let us show that any abelian group is a direct product of cyclic groups. The example $C_6 = C_2 \times C_3$ shows that there is no unicity of such a decomposition, unless one adds a condition, as follows.

Theorem 1. *Let G be a finite abelian group of order > 1. There exists a unique integer $s \geq 1$ and a unique finite sequence of integers $a_1, \ldots, a_s$, all > 1, satisfying the following properties.*
(i) For $i = 1, \ldots, s - 1$, a_i divides a_{i+1}.
(ii) The group G is isomorphic to the direct product $C_{a_1} \times \cdots \times C_{a_s}$.

Definition. The integers $a_1, \ldots, a_s$ are called the *invariants* of the group G.

Proof. We prove the existence of $a_1, \ldots, a_s$ by induction on the order of G. If G is cyclic, then the result is true with $s = 1$ and a_1 the order of G. In particular the result is true for a group G with 2 elements, with $s = 1$ and $a_1 = 2$,

Denote by a the exponent of G and by x an element of order a in G. Let G' be the quotient of G by the subgroup generated by x. If G' is the trivial group with 1 element, then G is cyclic and the result is true. Assume G' has more than one element. By the induction hypothesis, there exist integers $a_1, \ldots, a_{s-1}$ with a_i dividing a_{i+1} for $1 \leq i < s-1$ and there exist elements $x'_1, \ldots, x'_{s-1}$ of orders $a_1, \ldots, a_{s-1}$ respectively, such that G' is the direct product of the cyclic groups generated by $x'_1, \ldots, x'_{s-1}$. Since a_{s-1} is the exponent of G', it follows that a_{s-1} divides the exponent a of G. We set $a_s = a$ and $x_s = x$.

We claim that for $i = 1, \ldots, s-1$, there exists an element x_i in G of order a_i, the image of which in G' is x'_i. Indeed, let y_i be an element in G, the class of which in G' is x'_i. Then $a_i y_i$ is in the subgroup of G generated by x_s: there exists an integer b_i such that $a_i y_i = b_i x_s$. We have

$$0 = a_s y_1 = \frac{a_s}{a_i} a_i y_i = \frac{a_s}{a_i} b_i x_s,$$

hence a_s divides $(a_s/a_i)b_i$, which means that a_i divides b_i. Now define

$$x_i = y_i - \frac{b_i}{a_i} x_s.$$

We have

$$a_i x_i = 0,$$

hence the order of x_i divides a_i. Since the image x'_i of x_i in G' has order a_i, we deduce that the order of x_i is a_i.

Let H be the subgroup of G which is the direct product of the subgroups generated by $x_1, \ldots, x_{s-1}$. The intersection of H with the subgroup generated by x_s is $\{0\}$. It follows that G is the direct product of H with the subgroup generated by x_s.

It remains to prove the unicity of $a_1, \ldots, a_s$. The unicity of a_s is clear: it is the exponent of G. However we start by the unicity of a_1 and of s.

For any integer d, define

$$\Phi(d) = \mathrm{Card}\left\{x \in G \mid dx = 0\right\}.$$

We have

$$\Phi(d) = \prod_{i=1}^{s} \gcd(d, a_i) \leq d^s.$$

The integer s is the least integer k such that $\Phi(d) \leq d^k$ for all $d \geq 1$, hence s depends only on G. Also a_1 is the greatest integer $d \geq 1$ such that $\Phi(d) \leq d^s$, hence a_1 depends only on G.

We complete the proof of Theorem 1 by induction on the order of G. Let $G[a_1]$ be the subgroup of G containing the elements having an order which divides a_1. For $i \geq 1$, $(\mathbf{Z}/a_i\mathbf{Z})[a_1] = (a_i/a_1)\mathbf{Z}/a_i\mathbf{Z}$, hence $G/G[a_i]$ has invariant factors $a_2/a_1, \ldots, a_s/a_1$. By the induction hypothesis, these factors depend only on G. Hence the same is true for $a_2, \ldots, a_s$.

□

http://www.math.jussieu.fr/~miw/