Resource D

Finitely-Generated Abelian Groups

Mordell's Theorem tells us that the rational points on an elliptic curve $\mathcal{E}(\mathbb{Q})$ form a finitely-generated abelian group; while at a simpler level, the points on an elliptic curve $\mathcal{E}(\mathbb{F}_p)$ over a prime field form a finite abelian group.

For these reasons it is important to know the structure of abelian groups, and more generally of finitely-generated abelian groups.

D.1 Finite Abelian Groups

Proposition D.1 $\mathbb{Z}/(m) \oplus \mathbb{Z}/(n) = \mathbb{Z}/(mn)$ *if and only if* $\gcd(m, n) = 1$.

Proof ▶ This is a re-statement of the Chinese Remainder Theorem. If m, n are coprime, then a remainder $r \mod m$ and a remainder $s \mod n$ determin a unique remainder $\mod mn$.

Conversely, if m, n have a common factor $d > 1$ then it is readily verified that there is no element in the sum with order mn; every element has order dividing mn/d. ◀

Cyclic groups are sometimes encountered in multiplicative form C_n, and sometimes in additive form $\mathbb{Z}/(n)$. We assume that results in one form can be translated into the other. For example the Proposition above can equally well be stated in the form

$$C_m \times C_n = C_{mn} \Longleftrightarrow \gcd(m, n) = 1.$$

Thus by the Proposition,

$$C_3 \times C_4 = C_{12},$$

but

$$C_2 \times C_6 \neq C_{12}.$$

Proposition D.2 *Suppose A is an abelian group. For each prime p, the elements of order p^n in A for some $n \in N$ form a subgroup*

$$A_p = \{a \in A : p^n a = 0 \textit{ for some } n \in \mathbb{N}\}.$$

Proof ▶ Suppose $a, b \in A_p$. Then

$$p^m a = 0, \; p^n b = 0,$$

for some m, n. Hence

$$p^{m+n}(a+b) = 0,$$

and so $a + b \in A_p$. ◀

Definition D.1 *We call A_p the* p-component *of A.*

By Lagrange's Theorem A_p vanishes unless p is a factor of $|A|$.

Proposition D.3 *A finite abelian group A is the direct sum of its components A_p:*

$$A = \oplus_{p \textit{ divides } |A|} A_p.$$

Proof ▶ If $a \in A$ then $na = 0$ for some positive integer n. Let

$$n = p_1^{e_1} \cdots p_r^{e_r};$$

and set

$$m_i = n / e_i^{p_i}.$$

Then $\gcd(m_1, \ldots, m_r) = 1$, and so we can find $n_1, \ldots, n_r$ such that

$$m_1 n_1 + \cdots + m_r n_r = 1.$$

Thus

$$a = a_1 + \cdots + a_r,$$

where

$$a_i = m_i n_i a.$$

But

$$p_i^{e_i} a_i = (p_i^{e_i} m_i) n_i a = n n_i a = 0$$

(since $na = 0$). Hence

$$a_i \in A_{p_i}.$$

Thus A is the sum of the subgroups A_p.

To see that this sum is direct, suppose

$$a_1 + \cdots + a_r = 0,$$

where $a_i \in A_{p_i}$, with distinct primes $p_1, \ldots, p_r$. Suppose

$$p_i^{e_i} a_i = 0.$$

Let

$$m_i = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_{i+1}^{e_{i+1}} \cdots p_r^{e_r}.$$

Then

$$m_i a_j = 0 \text{ if } i \neq j.$$

Thus (multiplying the given relation by m_i),

$$m_i a_i = 0.$$

But $\gcd(m_i, p_i^{e_i}) = 1$. Hence we can find m, n such that

$$m m_i + n p_i^{e_i} = 1.$$

But then

$$a_i = m(m_i a_i) + n(p_i^{e_i} a_i) = 0.$$

We conclude that A is the direct sum of its p-components A_p. ◀

Theorem D.1 *Suppose A is a finite abelian p-group (ie each element is of order p^e for some e). Then A can be expressed as a direct sum of cyclic p-groups:*

$$A = \mathbb{Z}/(p^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_r}).$$

Moreover the powers $p^{e_1}, \ldots, p^{e_r}$ are uniquely determined by A.

Proof ▶ We argue by induction on $\|A\| = p^n$. We may assume therefore that the result holds for the subgroup

$$pA = \{pa : a \in A\}.$$

For pA is strictly smaller than A, since

$$pA = A \Longrightarrow p^n A = A,$$

while we know from Lagrange's Theorem that $p^n A = 0$.

Suppose

$$pA = \langle pa_1 \rangle \oplus \cdots \oplus \langle pa_r \rangle.$$

Then the sum

$$\langle a_1 \rangle + \cdots + \langle a_r \rangle = B,$$

say, is direct. For suppose

$$n_1 a_1 + \cdots + n_r a_r = 0.$$

If $p \mid n_1, \ldots, n_r$, say $n_i = pm_i$, then we can write the relation in the form

$$m_1(pa_1) + \cdots + m_r(pa_r) = 0,$$

whence $m_i pa_i = n_i a_i = 0$ for all i.

On the other hand, if p does not divide all the n_i then

$$n_1(pa_1) + \cdots + n_r(pa_r) = 0,$$

and so $pn_i a_i = 0$ for all i. But if $p \nmid n_i$ this implies that $pa_i = 0$. (For the order of a_i is a power of p, say p^e; while $p^e \mid n_i p$ implies that $e \leq 1$.) But this contradicts our choice of pa_i as a generator of a direct summand of pA. Thus the subgroup $B \subset A$ is expressed as a direct sum

$$B = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle.$$

Let

$$K = \{a \in A : pa = 0\}.$$

Then

$$A = B + K.$$

For suppose $a \in A$. Then $pa \in pA$, and so

$$pa = n_1(pa_1) + \cdots + n_r(pa_r)$$

for some $n_1, \ldots, n_r \in \mathbb{Z}$. Thus

$$p(a - n_1 a_1 - \cdots - n_r a_r) = 0,$$

and so

$$a - n_1 a_1 - \cdots - n_r a_r = k \in K.$$

Hence

$$a = (n_1 a_1 + \cdots + n_r a_r) + k \in B + K.$$

If $B = A$ then all is done. If not, then $K \not\subset B$, and so we can find $k_1 \in K, k_1 \notin B$. Now the sum

$$B_1 = B + \langle k_1 \rangle$$

is direct. For $\langle k_1 \rangle$ is a cyclic group of order p, and so has no proper subgroups. Thus

$$B \cap \langle k_1 \rangle = \{0\},$$

and so

$$B_1 = B \oplus \langle k_1 \rangle$$

If now $B_1 = A$ we are done. If not we can repeat the construction, by choosing $k_2 \in K, k_2 \notin B_1$. As before, this gives us a direct sum

$$B_2 = B_1 \oplus \langle k_2 \rangle = B \oplus \langle k_1 \rangle \oplus \langle k_2 \rangle.$$

Continuing in this way, the construction must end after a finite number of steps (since A is finite):

$$\begin{aligned} A = B_s &= B \oplus \langle k_1 \rangle \oplus \cdots \oplus \langle k_s \rangle \\ &= \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle \oplus \langle k_1 \rangle \oplus \cdots \oplus \langle k_s \rangle. \end{aligned}$$

It remains to show that the powers $p^{e_1}, \ldots, p^{e_r}$ are uniquely determined by A. This follows easily by induction. For if A has the form given in the theorem then

$$pA = \mathbb{Z}/(p^{e_1-1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_r-1}).$$

Thus if $e > 1$ then $\mathbb{Z}/(p^e)$ occurs as often in A as $\mathbb{Z}/(p^{e-1})$ does in pA. It only remains to deal with the factors $\mathbb{Z}/(p)$. But the number of these is now determined by the order $\|A\|$ of the group. ◀

Remark: It is important to note that if we think of A as a direct sum of cyclic *subgroups*, then the orders of these subgroups are uniquely determined, by the theorem; but *the actual subgroups themselves are not in general uniquely determined.* In fact the only case in which they are uniquely determined (for a finite p-group A) is if A is itself cyclic,

$$A = \mathbb{Z}/(p^e),$$

in which case of course there is just one summand.

To see this, it is sufficient to consider the case of 2 summands:

$$A = \mathbb{Z}/(p^e) \oplus \mathbb{Z}/(p^f).$$

We may suppose that $e \geq f$. Let a_1, a_2 be the generators of the 2 summands. Then it is easy to see that we could equally well take $a_1' = a_1 + a_2$ in place of a_1:

$$A = \langle a_1 + a_2 \rangle \oplus \langle a_2 \rangle.$$

For certainly these elements $a_1 + a_2, a_2$ generate the group; and the sum must be direct, since otherwise there would not be enough terms $m_1 a_1' + m_2 a_2$ to give all the p^{e+f} elements in A.

D.2 Finitely-generated abelian groups

Definition D.2 *The abelian group A is said to be finitely-generated if there exist elements $a_1, \ldots, a_n$ such that each $a \in A$ is expressible in the form*

$$a = n_1 a_1 + \cdots + n_r a_r,$$

with $n_i \in \mathbb{Z}$.

We write $A = \langle a_1, \ldots, a_n \rangle$.

Proposition D.4 *The elements of finite order in an abelian group A form a subgroup T.*

Definition D.3 *We call this subgroup the torsion subgroup T of A; and we call $t \in T$ a torsion element.*

Proposition D.5 *The torsion subgroup T of a finitely-generated abelian group A is finite.*

Proof ► We argue by induction on the minimal number n of generators of A. Suppose $A = \langle a_1, \ldots, a_n \rangle$.

Each element $t \in T$ can be written in the form

$$t = n_1 a_1 + \cdots + n_r a_r.$$

If every $t \in T$ has $n_1 = 0$ then $T \subset \langle a_2, \ldots, a_n \rangle$, and the result follows by induction.

Otherwise choose $t_1 \in T$ with smallest $n_1 > 0$, say m_1 Then the coefficient n_1 of each $t \in T$ is a multiple of m_1, say $n_1 = rm_1$. It follows that

$$t = rt_1 + u,$$

Where $u \in \langle a_2, \ldots, a_n \rangle$, and again the result follows by induction. ◄

We say that an abelian group A is *torsion-free* if $T = 0$, ie A has no elements of finite order except 0.

Proposition D.6 *If A is an abelian group with torsion subgroup T then A/T is torsion-free.*

Proposition D.7 *A torsion-free finitely-generated abelian group A is isomorphic to the direct sum of a number of copies of $\mathbb{Z}$;*

$$A = \mathbb{Z}^r = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

Proof ► To each abelian group A we can associate a vector space V over $\mathbb{Q}$ as follows. The elements of V are the expressions λa, where $\lambda \in \mathbb{Q}$, $a \in A$. We set $\lambda a = \mu b$ in V if $(d\lambda)a = (d\mu)b$ in A for some non-zero integer d for which $d\lambda$, $d\mu \in \mathbb{Z}$. (In other words, V is the tensor product $A \otimes \mathbb{Q}$.)

There is a natural abelian group homomorphism $\phi : A \to V$ under which $a \mapsto 1 \cdot a$. It is easy to see that $\ker \phi = T$. In particular, if A is torsion-free then we can identify A with an abelian subgroup of V:

$$A \subset V.$$

If now $A = \langle a_1, \ldots, a_n \rangle$ then these elements span V. Hence we can choose a basis for V from among them. After re-ordering we may suppose the $a_1, \ldots, a_r$ form a basis for V.

We derive a $\mathbb{Z}$-basis $b_1, \ldots, b_r$ for A as follows. Choose b_1 to be the smallest positive multiple of a_1 in A:

$$b_1 = \lambda_1 a_1 \in A.$$

(It is easy to see that $\lambda_1 = 1/d$ for some $d \in \mathbb{N}$.)

Now choose b_2 to be an element of A in the vector subspace $\langle a_1, a_2 \rangle$ with smallest positive second coefficient

$$b_2 = \mu_1 a_1 + \lambda_2 a_2 \in A.$$

(Again, it is easy to see that $\lambda_2 = 1/m_2$ for some $m \in \mathbb{N}$.)

Continuing in this way, choose b_i to be an element of A in the vector subspace $\langle a_1, \ldots, a_i \rangle$ with smallest positive ith coefficient

$$b_i = \mu_1 a_1 + \cdots + \mu_{i-1} a_{i-1} + \lambda_i a_i \in A.$$

(Once again, it is easy to see that $\lambda_i = 1/m_i$ for some $m \in \mathbb{N}$.)

Finally, we choose b_r to be an element of A with smallest positive last coefficient

$$b_r = \mu_1 a_1 + \cdots + \mu_{r-1} a_{i-1} + \lambda_r a_i \in A.$$

We assert that $b_1, \ldots, b_r$ forms a $\mathbb{Z}$-basis for A. For suppose $a \in A$. Let

$$a = \rho_{r,1} a_1 + \cdots + \rho_{r,r} a_r,$$

where $\rho_1, \ldots, \rho_r \in \mathbb{Q}$. The last coefficient $\rho_{r,r}$ must be an integral multiple of λ_r,

$$\rho_{r,r} = n_r \lambda_r.$$

For otherwise we could find a combination $ma + nb_r$ with last coefficient positive but smaller than λ_r.

But now

$$a - n_r b_r \in \langle a_1, \ldots, a_{r-1} \rangle,$$

say

$$a - n_r b_r = \rho_{r-1,1} a_1 + \cdots + \rho_{r-1,r-1} a_{r-1}.$$

By the same argument, the last coefficient $\rho_{r-1,r-1}$ is an integral multiple of λ_{r-1}.

$$\rho_{r-1,r-1} = n_{r-1} \lambda_{r-1},$$

and so

$$a - n_r b_r - n_{r-1} b_{r-1} \in \langle a_1, \ldots, a_{r-2} \rangle.$$

Continuing in this fashion, we find finally that

$$a = n_r b_r + n_{r-1} b_{r-1} + n_1 b_1,$$

with $n_r, \ldots, n_1 \in \mathbb{Z}$. Thus $b_1, \ldots, b_r$ forms a $\mathbb{Z}$-basis for A, and

$$A = \mathbb{Z} b_1 \oplus \cdots \oplus \mathbb{Z} b_r \equiv \mathbb{Z}^r.$$

◄

Theorem D.2 *Every finitely-generated abelian group A is expessible as a direct sum*

$$A = T \oplus \mathbb{Z}^r.$$

Proof ► We know that $A/T = \mathbb{Z}^n = \langle e_1, \ldots, e_n \rangle$. For each e_i choose an element $a_i \in A$ which maps onto e_i.

Suppose $a \in A$. Let its image in $\mathbb{Z}^n$ be $c_1 e_1 + \cdots c_n e_n$. Then

$$c_1 a_1 + \cdots c_n a_n \mapsto c_1 e_1 + \cdots c_n e_n.$$

It follows that

$$a - (c_1 a_1 + \cdots c_n a_n) \mapsto 0,$$

ie

$$t = a - (c_1 a_1 + \cdots c_n a_n) \in T,$$

and so

$$a = t + c_1 a_1 + \cdots c_n a_n,$$

as required. ◄

Theorem D.3 *Every finitely-generated abelian group A is expressible as a direct sum of cyclic groups (including $\mathbb{Z}$):*

$$A = \mathbb{Z}/(p^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_s}) \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

Moreover the prime-powers $p_1^{e_1}, \ldots, p_s^{e_s}$ and the number of copies of $\mathbb{Z}$ are uniquely determined by A.

Proof ► We have seen that the expression for the torsion subgroup is unique, while $r = \dim V$, where V is the associated vector space over $\mathbb{Q}$. ◄

Definition D.4 *The* rank *of the abelian group A is the number of copies of $\mathbb{Z}$.*

Exercises 3 Finitely-Generated Abelian Groups

In exercises 1–6 determine the number of abelian groups of the given order.

* 1. 5

** 2. 6

** 3. 16

** 4. 96

** 5. 175

In exercises 6–10 determine the number of elements of the given order in the given abelian group

** 6. order 4 in $\mathbb{Z}/(12)$

** 7. order 2 in $C_2 \times C_4$

** 8. order 3 in $(\mathbb{Z}/21)^{\times}$

** 9. order 4 in $\mathbb{Z}/(6) \oplus \mathbb{Z}/(8)$

** 10. order 3 in $(\mathbb{Z}/21)^{\times}$

** 11. Show that a finite abelian group A is cyclic if and only if each component A_p is cyclic.

** 12. Show that every subgroup of a cyclic group is cyclic.

** 13. Show that C_n has just one subgroup of each order $m \mid n$.

** 14. Is $\mathbb{Q}$ finitely-generated as an abelian group?

** 15. Show that the Vier-Gruppe $D_2 = \{1, a, b, c\}$ can be expressed as a product $C_2 \times C_2$ in 3 ways.

In exercises 16–20 determine the abelian group on the given elliptic curve:

*** 16. $\mathcal{E}(F_3)\ y^2 = x^3 + x + 1$

*** 17. $\mathcal{E}(F_3)\ y^2 = x^3 + x$

*** 18. $\mathcal{E}(F_5)\ y^2 = x^3 + 1$

*** 19. $\mathcal{E}(F_5)\ y^2 = x^3 - 1$

*** 20. $\mathcal{E}(F_5)\ y^2 = x^3 + x + 1$