Elementary Divisors of Finite Abelian Groups

R. C. Daileda

Here's the fundamental theorem of finite abelian groups, as we're proven it.

Theorem 1. *Let A be a finite abelian group. Then A can be uniquely expressed as a direct sum of abelian p-groups*

$$A = A(p_1) \oplus A(p_2) \oplus \cdots \oplus A(p_k),$$

where the p_i are the distinct prime divisors of $|A|$. Moreover, each $A(p_i)$ is a direct sum of cyclic p_i-groups

$$A(p_i) \cong C_{p_i^{s(i,1)}} \oplus C_{p_i^{s(i,2)}} \oplus \cdots \oplus C_{p_i^{s(i,\ell_i)}}, \tag{1}$$

in which the sequence of exponents

$$s(i,1) \geq s(i,2) \geq \cdots \geq s(i,\ell_i) \geq 1, \tag{2}$$

is unique.

To remind the reader, here

$$A(p) = \{a \in A \,|\, p^k a = 0 \text{ for some } k \in \mathbb{N}_0\},$$

and C_n is a cyclic group of order n. Of course, one could write $\mathbb{Z}/n\mathbb{Z}$ instead, but in our current setting this becomes a bit cumbersome.

There is a somewhat more fruitful way of thinking of the decomposition of Theorem 1, simply by rearranging the summands (we're in an abelian group, so addition is commutative), and applying the Chinese remainder theorem. First, observe that if we insert terminal zeros at the end of every sequence of exponents (2), we lose uniqueness of the sequence, but don't change the isomorphism class of the direct sum (1). So, by inserting zeros if necessary, we may assume $\ell_i = \ell$ for all i.

Now write out the direct summands $A(p_k)$ in rows.

$$\begin{aligned} A(p_1) &\cong C_{p_1^{s(1,1)}} \oplus C_{p_1^{s(1,2)}} \oplus \cdots \oplus C_{p_1^{s(1,\ell)}} \\ A(p_2) &\cong C_{p_2^{s(2,1)}} \oplus C_{p_2^{s(2,2)}} \oplus \cdots \oplus C_{p_2^{s(2,\ell)}} \\ &\vdots \\ A(p_k) &\cong C_{p_k^{s(k,1)}} \oplus C_{p_k^{s(k,2)}} \oplus \cdots \oplus C_{p_k^{s(k,\ell)}} \end{aligned}$$

Now sum down each column and apply the Chinese remainder theorem[1] to obtain

$$C_{p_1^{s(1,j)}} \oplus C_{p_2^{s(2,j)}} \oplus \cdots \oplus C_{p_k^{s(k,j)}} \cong C_{d_j},$$

[1] See the Appendix.

where

$$d_j = p_1^{s(1,j)} p_2^{s(2,j)} \cdots p_k^{s(k,j)}. \tag{3}$$

We therefore have

$$A = A(p_1) \oplus A(p_2) \oplus \cdots A(p_k) \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_\ell}.$$

Because the exponents $s(i,j)$ decrease in j, equation (3) shows that we must have

$$d_\ell | d_{\ell-1} | d_{\ell-2} | \cdots | d_1.$$

Moreover, because the product of the primes powers $p_i^{s(i,j)}$ is equal to the order of A, we also find that

$$|A| = d_1 d_2 \cdots d_\ell.$$

The integers $d_1, d_2, \ldots, d_\ell$ completely classify A and provide us with another, frequently more useful, decomposition of a finite abelian group.

Theorem 2. *Let A be a finite abelian group. There is a unique list $d_1, d_2, \ldots, d_\ell \in \mathbb{N}$ so that*

1. $d_\ell | d_{\ell-1} | \cdots | d_1$
2. $d_1 d_2 \cdots d_\ell = |A|$.
3. $A \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_\ell}$

The integers $d_1, d_2, \ldots, d_\ell$ are called the elementary divisors *of A.*

Proof. We induct on the size of A. If $|A| = 1$, then $d_1 = 1$ is the only elementary divisor of A. Now suppose $|A| > 1$ and the theorem holds for all finite abelian groups of order less than $|A|$. Suppose that $d_1, d_2, \ldots, d_\ell$ is a sequence of elementary divisors for A. Since d_1 is the smallest positive exponent of A, it is uniquely determined by A. Let

$$A_1 = \underbrace{C_{d_1} \oplus 0 \oplus \cdots \oplus 0}_{\ell \text{ summands}}.$$

Then

$$A/A_1 \cong C_{d_2} \oplus \cdots \oplus C_{d_\ell},$$

so that $d_2, \ldots, d_\ell$ are elementary divisors of A/A_1, and are therefore unique by the inductive hypothesis. This completes the proof.

□

We mention a few immediate consequences of (both versions) of the fundamental theorem.

Proposition 1. *Let A be a finite abelian group. For any positive n dividing $|A|$, A has a subgroup of order n.*[2]

[2] Unlike the case in which A is also assumed to be *cyclic*, there is no claim that any such subgroup need to be unique.

Proof. For any prime p dividing n, A must contain a cyclic subgroup of order p (either by the fundamental theorem, or by earlier results). Let A_1 denote the direct sum of these subgroups, $m = |A_1|$, and consider A/A_1. Since n/m divides $|A/A_1| = |A|/m$, we can inductively find a subgroup H' of A/A_1 whose order is n/m. By the correspondence principle, $H' = H/A_1$ for some subgroup H of A. A quick computation shows that

$$\frac{n}{m} = |H'| = \frac{|H|}{|A_1|} = \frac{|H|}{m} \quad \Rightarrow \quad |H| = n,$$

as claimed. □

Although apparently trivial, the following result can be used to yield a quick proof that every finite abelian group occurs as a Galois group over $\mathbb{Q}$.

Corollary 1. *Let A be a finite abelian group. For any positive n dividing $|A|$, A as a subgroup of index n.*

Proof. Apply the Proposition to $|A|/n$. □

The final result we mention is a structure theorem for multiplicative subgroups of $\mathbb{C}^\times$. Although it can be proven directly, the argument we give has two advantages: (i) it avoids the use of the division algorithm; (ii) it applies generally to an arbitrary field. It is essential in understanding the nature of the so-called *roots of unity* in a field, i.e. those solutions to equations of the form $x^n - 1 = 0$.

Proposition 2. *Let $\boldsymbol{\mu}$ be a (multiplicative) subgroup of $\mathbb{C}^\times$. If $\boldsymbol{\mu}$ is finite, then it is cyclic.*

Proof. Because $\boldsymbol{\mu}$ is abelian, we can write

$$\boldsymbol{\mu} \cong C_{d_1} \oplus \cdots \oplus C_{d_\ell}, \tag{4}$$

the isomorphism of course being multiplicative to additive. Because d_1 is an exponent for the direct sum, it must also be an exponent for $\boldsymbol{\mu}$, and hence $z^{d_1} = 1$ for all $z \in \boldsymbol{\mu}$. But the isomorphism also tells us that $|\boldsymbol{\mu}| = d_1 d_2 \cdots d_\ell$. It follows that the degree d_1 polynomial

$$x^{d_1} - 1$$

has $d_1 d_2 \cdots d_\ell$ roots. Since no polynomial over $\mathbb{C}$ can have more roots than its degree, this is a contradiction unless $\ell = 1$. Consequently (4) reduces to

$$\boldsymbol{\mu} \cong C_{d_1},$$

which is what we needed to show. □

Remark 1. Let $\boldsymbol{\mu} < \mathbb{C}^\times$ be finite, of order n. By Lagrange's theorem, every element of $\boldsymbol{\mu}$ must be a root of the degree n polynomial $x^n - 1$, and there can be no other roots. Conversely, it is an easy exercise to show that the roots of $x^n - 1$ in $\mathbb{C}^\times$ do, indeed, form a subgroup $\boldsymbol{\mu}$ of $\mathbb{C}^\times$, and that the the fundamental theorem of algebra guarantees that $|\boldsymbol{\mu}| = n$. That is $\mathbb{C}^\times$ has a unique finite subgroup for every $n \in \mathbb{N}$, consisting precisely of the n roots of the polynomial $x^n - 1$.

The roots of $x^n - 1$ are called *nth roots of unity*, and what we have just shown is that, in every case, they form a subgroup $\boldsymbol{\mu} = \boldsymbol{\mu}_n$ of $\mathbb{C}^\times$ of order n. By Proposition 2, for any n the group $\boldsymbol{\mu}_n$ is cyclic, so there is a $\zeta_n \in \boldsymbol{\mu}_n$, of multiplicative order n, so that $\boldsymbol{\mu}_n = \langle \zeta_n \rangle$. Because every other nth root of unity in $\boldsymbol{\mu}_n$ is a power of ζ_n, we call ζ_n a *primitive root of unity.* Although their existence is useful, primitive nth roots are by no means unique, as they as just unspecified generators of a cyclic group.

Remark 2. If we replace $\mathbb{C}$ with an arbitrary *field* $\mathbb{F}$, (roughly speaking an algebraic structure with addition, subtraction, multiplication and (nonzero) division), Proposition 2 remains valid, by the same proof. The argument of Remark 1 also still works, too, *provided* n is *not* divisible by the *characteristic* of $\mathbb{F}$, when it is positive.[3] The roots of unity in fields of positive characteristic p can still be classified, but there are subtleties tied to the cases in which n is divisible by p. Believe it or not, these are all caused by the apparently trivial identity

$$(x-1)^p \equiv x^p - 1 \pmod{p}.$$

Appendix: The Chinese Remainder Theorem

Theorem 3. *Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers and set $N = m_1 \cdots m_k$. Then*

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

Proof. By mapping onto each coordinate separately, the individual canonical maps $\mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$ together yield a homomorphism

$$h : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

One can show directly that this is surjective, but we prefer a shorter, indirect approach. The kernel of h consists of all those $n \in \mathbb{Z}$ that are simultaneously divisible by every m_i. Because $\gcd(m_i, m_j) = 1$ for all $i \neq j$, this occurs if and only if $m_1 \cdots m_k = N$ divides n. Hence $\ker h = N\mathbb{Z}$, and by the first isomorphism theorem we have

$$\overline{h} : \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

Because the domain and codomain both have order N, the injectivity of $\overline{h}$ implies it is actually a bijection, and therefore an isomorphism. □

Remark. This can also be proven by first treating the case $k = 2$ (by the same method), and then inducting.

[3] Given a (commutative) ring R with (multiplicative) identity, the map $m \mapsto m \cdot 1_R$ is a ring homomorphism $\mathbb{Z} \to R$. Its kernel has the form $k\mathbb{Z}$ for some $k \geq 0$, and via the first isomorphism theorem we get an embedding $\mathbb{Z}/k\mathbb{Z} \hookrightarrow R$. We define the *characteristic* of R to be k. It turns out that if R is a field, either $k = 0$ (e.g. $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}$) or $k = p$, a prime (e.g. $\mathbb{Z}/p\mathbb{Z}$ or any of its extensions).