The Structure Theorem for Finite Abelian Groups

(Saracino, Section 14)

Theorem: Every finite abelian group is isomorphic to a direct product of cyclic groups of orders that are powers of prime numbers. (And of course the product of the powers of orders of these cyclic groups is the order of the original group.) In symbols: If G is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$$

where the p_j's are prime integers, the k_j's are positive integers, and

$$|G| = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_n^{k_n} \ .$$

"Internal" Direct Product

Prop: G group, H, K subgroups. If

(1) $H \cap K = \{e\}$,

(2) $\forall\, h \in H,\ k \in K,\ hk = kh$, and

(3) $HK = G$,

then $H \times K \to G : (h, k) \to hk$ is an isomorphism.

Familiar fact

G abelian group, $m \in \mathbb{N}$:

$$H = \{g \in G : o(g) | m\} \text{ is a subgroup of } G.$$

(Recall: $o(g)|m \iff g^m = e$.)

Sooo . . .

G abelian, $|G| = mn$ where $\gcd(m, n) = 1$,
$H = \{g \in G : o(g)|m\}$, $K = \{g \in G : o(g)|n\}$
$\implies G \cong H \times K$.

Continuing:

$G \cong G(p_1) \times G(p_2) \times \cdots \times G(p_n)$, where
$p_1, p_2, \ldots, p_n$ are the primes dividing $|G|$, and
$G(p_j) = \{g \in G : o(g)$ is a power of $p_j\}$.

Reduce to p-group

So we only need to rewrite each $G(p)$ as a product of $\mathbb{Z}_{p^n}$'s.

So assume every element of G has order a power of a given prime p (i.e., G is a "p-group").

Lemma and corollary

Lemma: If H is a finite abelian group and q is a prime dividing $|H|$, then H has an element of order q.

Proof: Assume BWOC false, and suppose H is the smallest counterexample (for q). Pick $g \in H - \{e\}$ and form $H/\langle g \rangle$. No elt of H has order a multiple of q, so $\gcd(o(g), q) = 1$. But $|H| = o(g)|H/\langle g \rangle|$, so $q||H/\langle g \rangle|$. Because H was the smallest counterexample, $H/\langle g \rangle$ has an element $h\langle g \rangle$ of order q. But then $q|o(h\langle g \rangle)|o(h)$, so h has a power with order q, $\rightarrow\!\!\!\!\leftarrow$

Cor: A finite abelian p-group has order a power of p.

The hard part (1)

The proof now proceeds by proving that, if g in G has the highest order p^n, then there is subgroup H of G for which $G \cong \langle g \rangle \times H$.

Induction again:

- Assume smaller p-groups have the right form.
- Write $G/\langle g \rangle \cong \langle \langle g \rangle x_1 \rangle \times \cdots \times \langle \langle g \rangle x_n \rangle$.
- Argue that we can pick y_i in $\langle g \rangle x_i$ so that $o(y_i)$ in G is equal to $o(\langle g \rangle x_i)$ in $G/\langle g \rangle$. (See next slide.)
- Then argue $G \cong \langle g \rangle \times \langle y_1 \rangle \times \ldots \langle y_n \rangle$. (See slide after that.)

This will complete the proof of the structure theorem.

The hard part (2)

The order p^i of $\langle g \rangle x$ in $G/\langle g \rangle$ divides the order p^j of x in G, but it may be smaller, because x^{p^i} may be in $\langle g \rangle$ without being e. However, we chose g to have largest order p^k in G, so when we write $x^{p^i} = g^{mp^r}$ where $p \nmid m$, then we must have $r \geq i$ so that the orders of these two equal elements of G are the same:

$$o(x^{p^i}) = p^{j-i} \qquad o(g^{mp^r}) = p^{k-r}$$

and $k \geq j$. So $y = xg^{-mp^{r-i}}$ is in $\langle g \rangle x$ and has order p^i.

The hard part (3)

We want to show that if $o(y_i) = o(\langle g \rangle y_i)$ and

$$\begin{aligned}\psi :&\langle \langle g \rangle y_1 \rangle \times \cdots \times \langle \langle g \rangle y_n \rangle \to G/\langle g \rangle : \\ &(\langle g \rangle y_1^{m_1}, \ldots, \langle g \rangle y_n^{m_n}) \mapsto \langle g \rangle y_1^{m_1} \ldots y_m^{m_n}\end{aligned}$$

is an isomorphism, then

$$\begin{aligned}\varphi :&\langle g \rangle \times \langle y_1 \rangle \times \cdots \times \langle y_n \rangle \to G : \\ &(g^m, y_1^{m_1}, \ldots, y_n^{m_n}) \mapsto g^m y_1^{m_1} \ldots y_n^{m_n}\end{aligned}$$

is also an isomorphism.

The hard part (4)

Because G is abelian, φ is a homomorphism. It is onto G because ψ is onto: The image in $G/\langle g\rangle$ of any element h of G has the form

$$\langle g\rangle h = \langle g\rangle y_1^{m_1}\dots y_n^{m_n}\ , \qquad \text{so} \qquad h = g^m y_1^{m_1}\dots y_n^{m_n}$$

for some m. And φ is 1-1 because $\ker(\varphi)$ is trivial:

$$\begin{aligned}|\langle g\rangle \times \langle y_1\rangle \times \dots \times \langle y_n\rangle| / |\ker(\varphi)| &= |G| = o(g)\cdot |G/\langle g\rangle| \\ &= o(g)\cdot |\langle g\rangle y_1 \times \dots \times \langle g\rangle y_n| \\ &= o(g)\cdot o(\langle g\rangle y_1)\cdot \dots \cdot o(\langle g\rangle y_n) \\ &= o(g)\cdot o(y_1)\cdot \dots \cdot o(y_n) \\ &= |\langle g\rangle \times \langle y_1\rangle \times \dots \times \langle y_n\rangle|\ .\end{aligned}$$

When isomorphic? (1)

Example: $\mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$, by $(a, b, c, d) \mapsto (d, c, a, b)$

In general:

$$\mathbb{Z}_{p^{k(1)}} \times \mathbb{Z}_{p^{k(2)}} \times \cdots \times \mathbb{Z}_{p^{k(n)}} \cong \mathbb{Z}_{p^{j(1)}} \times \mathbb{Z}_{p^{j(2)}} \times \cdots \times \mathbb{Z}_{p^{j(m)}}$$

if $p^{k(1)}, p^{k(2)}, \ldots, p^{k(n)}$ are just $p^{j(1)}, p^{j(2)}, \ldots, p^{j(m)}$, maybe rearranged.
(The isomorphism just rearranges the coordinates.)

When isomorphic? (2)

To see that the converse is true, note that, if finite abelian p-groups G and H are isomorphic, then the isomorphism must take

$$\{g \in G : g^{p^k} = e\} \quad \text{to} \quad \{h \in H : h^{p^k} = e\} .$$

Now we can express in terms of the $k(i)$'s the number of elements in

$$\mathbb{Z}_{p^{k(1)}} \times \mathbb{Z}_{p^{k(2)}} \times \cdots \times \mathbb{Z}_{p^{k(n)}}$$

whose p^k-th power is e. So if they are isomorphic, the lists of $p^{k(i)}$'s must be the same (except for how they are arranged).

An example

Suppose

$$\begin{aligned} G \cong & \quad \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ & \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\ & \times \mathbb{Z}_5 \times \mathbb{Z}_5 . \end{aligned}$$

Take the direct product of the first groups in each row, then the second groups, and so on:

$$\mathbb{Z}_8 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 \qquad \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \qquad \mathbb{Z}_4 \times \mathbb{Z}_3 \qquad \mathbb{Z}_2 \qquad \mathbb{Z}_2$$

The example, ctnd.

The orders in different rows are relatively prime, so these "column direct products" are cyclic:

$$\begin{aligned} \mathbb{Z}_8 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 &\cong \mathbb{Z}_{1080} \\ \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\cong \mathbb{Z}_{120} \\ \mathbb{Z}_4 \times \mathbb{Z}_3 &\cong \mathbb{Z}_{12} \\ \mathbb{Z}_2 &\cong \mathbb{Z}_2 \\ \mathbb{Z}_2 &\cong \mathbb{Z}_2 \end{aligned}$$

Now we have

$$\mathbb{Z}_{1080} \times \mathbb{Z}_{120} \times \mathbb{Z}_{12} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong G$$

and $2|2|12|120|1080$.

Invariants defined

We can do that with any finite abelian group:

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_n}$$

where $d_n | d_{n-1} | \ldots | d_2 | d_1$. The d_i's are called the *invariants* of G.

Two finite abelian groups are isomorphic iff they have the same invariants.