MATH 3311, FALL 2025: LECTURE 37, DECEMBER 1

Video: `https://youtu.be/KnWNwfHrFqs`

The uniqueness part of the fundamental theorem for finitely generated abelian groups

What we have to show: If we have

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z} \times \mathbb{Z}^r$$

and

$$G \simeq \mathbb{Z}/d_1'\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{m'}'\mathbb{Z} \times \mathbb{Z}^{r'}$$

with $2 \leq d_1 \mid \cdots \mid d_m$ and $2 \leq d_1' \mid \cdots \mid d_m'$ then in fact $m' = m$ and $r' = r$.

Last time we saw:

Proposition 1. *In the above situation, we have $r' = r$.*

Proof. In Homework 11, we saw: If $f : G \xrightarrow{\simeq} H$ is an isomorphism, then we obtain isomorphisms

$$G^{\mathrm{tors}} \xrightarrow{\simeq} H^{\mathrm{tors}} \; ; \; G^{\mathrm{tf}} \xrightarrow{\simeq} H^{\mathrm{tf}}.$$

Moreover, it is not difficult to see that, if

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z} \times \mathbb{Z}^r$$

then $G^{\mathrm{tf}} \simeq \mathbb{Z}^r$. Therefore, applying this to the two different presentations of G, we find that $\mathbb{Z}^r \simeq \mathbb{Z}^{r'}$. This can only happen if $r = r'$: see problem 3 on Homework 12. □

So we can focus now on the *torsion* parts, which are *finite* abelian groups. We begin by focusing even more specifically at the situation of finite abelian p-groups for a fixed prime p.

Observation 1. If G is a finite abelian p-group, and

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}$$

with $2 \leq d_1 \mid \cdots \mid d_m$, then $d_i = p^{k_i}$ with

$$1 \leq k_1 \leq \cdots \leq k_m$$

Therefore, uniqueness in this case is telling us that the integers $k_1 \leq \cdots \leq k_m$ are determined *uniquely* by G. An equivalent formulation: For each positive integer k, let m_k be the number of times k shows up in the list $k_1, \ldots, k_m$.

Example 1. If $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$, then we have

$$m_1 = 2, m_2 = 0, m_3 = 1, m_4 = 1$$

and $m_k = 0$ for all $k \geq 5$.

Uniqueness is now implied by:

Proposition 2. *The integers $\{m_k : \ k \geq 1\}$ are determined uniquely by the finite abelian p-group G.*

To see this, we must somehow extract this numerical information in an *intrinsic* way; that is, *without* using any particular product representation.

Definition 1. If G is an abelian group (with the operation written additively), then for any $n \in \mathbb{Z}$, we set:

$$nG = \{n \cdot a : \ a \in G\}.$$

This is a *subgroup* of G and normal, because G is abelian.

Fact 1. If $G = \mathbb{Z}/m\mathbb{Z}$, then $nG \leq G$ is the subgroup generated by $n \pmod m$. Moreover, nG is isomorphic to $\gcd(n,m)\mathbb{Z}/n\mathbb{Z}$. In particular, if $G = \mathbb{Z}/p^k\mathbb{Z}$, we have

$$p^\ell G \simeq \begin{cases} p^k\mathbb{Z}/p^\ell\mathbb{Z} & \text{if } k > \ell \\ 0 & \text{if } k < \ell. \end{cases}$$

Proof. This was shown in problem 5 of Homework 6, but the point is that multiples of both m and n are dead in G/nG, and so is any linear combination of them, which means that $\gcd(n,m)$ must die in G/nG. □

Consequence 1. Suppose that

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \cdots \times (\mathbb{Z}/p^r\mathbb{Z})^{m_r}.$$

Then

$$p^\ell G \simeq \prod_{k>\ell} (p^\ell\mathbb{Z}/p^k\mathbb{Z})^{m_k}.$$

Proof. This is a consequence of the previous fact and the folllowing observations about direct products of abelian groups: If G_1, G_2 are abelian groups, then $n(G_1 \times G_2) = nG_1 \times nG_2$. □

Proof of Proposition 1. By the consequence above, if we have

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \times \cdots \times (\mathbb{Z}/p^r\mathbb{Z})^{m_r},$$

then we get

$$|p^\ell G| = p^{m_{\ell+1}} \cdot p^{2m_{\ell+2}} \cdots p^{(r-\ell)m_r}$$

which we can rewrite as

$$\log_p |p^\ell G| = m_{\ell+1} + 2m_{\ell+2} + \cdots + (r-\ell)m_r.$$

The left hand side is an intrinsic quantity attached to G and is independent of the product decomposition chosen for G. As ℓ ranges between 1 and r, this gives us r equations in the 'unknowns' $m_1, \ldots, m_r$. This is a linear system of equations governed by the matrix of coefficients

$$A = \begin{bmatrix} 1 & 2 & 3 & \cdots & r \\ 0 & 1 & 2 & \cdots & r-1 \\ 0 & 0 & 1 & \cdots & r-2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

This matrix is always invertible as an *integer* matrix, since its determinant is 1. This implies that the integers $m_1, \ldots, m_r$ are *uniquely* determined by these equations, and are therefore intrinsic to G. More precisely, if A^{-1} is the inverse matrix, then we have

$$\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} = A^{-1} \begin{pmatrix} \log_p |G| \\ \log_p |pG| \\ \cdots \\ \log_p |p^{r-1}G| \end{pmatrix}$$

□

Example 2. If $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$, then we go up to $r = 4$, and the column matrix on the right is

$$\begin{pmatrix} \log_p |G| \\ \log_p |pG| \\ \cdots \\ \log_p |p^{r-1}G| \end{pmatrix} = \begin{pmatrix} 9 \\ 5 \\ 3 \\ 1 \end{pmatrix}$$

Example 3. If $G' = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^4\mathbb{Z}$, then we have

$$\begin{pmatrix} \log_p |G'| \\ \log_p |pG'| \\ \cdots \\ \log_p |p^{r-1}G'| \end{pmatrix} = \begin{pmatrix} 9 \\ 5 \\ 2 \\ 1 \end{pmatrix}$$

To go from uniqueness of abelian p-groups to all finite abelian groups, we need an alternate formulation of the Fundamental Theorem:

Theorem 1. *Let G be a finite abelian group. There exists a canonical list of prime powers $p_1^{r_1}, \dots, p_m^{r_m}$ unique up to permutation such that*

$$G \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_m^{r_m}\mathbb{Z}.$$

*The prime powers $p_1^{r_1}, \dots, p_m^{r_m}$ are called the **elementary divisors** of G.*

As you will verify on Homework 12, to establish uniqueness of invariant factors, it is sufficient to do so for elementary divisors.

Example 4. Consider $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$: this is given in terms of invariant factors. We will use the Chinese Remainder Theorem (Homework 10, problem 8) to rewrite this (up to isomorphism) as the product

$$\mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}$$

This gives the list of elmentary divisors.