MATH 3311, FALL 2025: LECTURE 38, DECEMBER 3

Video: `https://youtu.be/p_a_4dQblrg`

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

Last time we saw:

Proposition 1. *If p is a prime, the uniqueness part of the fundamental theorem holds for finite p-groups*

We will use this to show the uniqueness in the elementary divisors 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.*

Proof of uniqueness.

Step 1. Reduce to the case where all the elementary divisors are powers of the same prime.

For this, we need the following observations

Observation 1. If G is a finite abelian group, then for any prime p there is a unique Sylow p-subgroup $G_p \leq G$.

Observation 2. If $G = \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{r_n}\mathbb{Z}$, then we have

$$G_p \simeq \prod_{p_k = p} \mathbb{Z}/p^{r_k}\mathbb{Z}.$$

Therefore, the elementary divisors of G that are powers of p are determined completely by the elementary divisors (or invariant factors) of G_p, which is a finite p-group.

Step 2. Prove uniqueness when G is a finite p-group.

This is Proposition 1.

□

Fields

We now move on to a new topic, which we will briefly touch on this semester. We will return to it in much greater detail starting next semester.

Example 1. Consider $\mathbb{Z}/p\mathbb{Z}$: this is an additive abelian group, but it is also equipped with a multiplication operation such that $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ is a *group* under multiplication. This means that one can do linear algebra as one is used to: Row reduction works because we can always 'divide' by non-zero entries.

Let us abstract the properties used for doing linear algebra in the following definition:

Definition 1. A **field** is a 5-tuple $(k, +, 0, \cdot, 1)$ where:

- $(k, +, 0)$ is an additive abelian group;
- $\cdot : k \times k \xrightarrow{(x,y)\mapsto x\cdot y} k$ is a binary operation;
- $1 \in k\backslash\{0\}$ is a non-zero element.

This data is required to satisfy the following properties:

(1) (Commutativity for $\cdot$) For all $x, y \in k$, we have $x \cdot y = y \cdot x$;
(2) (Associativity for $\cdot$) For all $x, y, z \in k$, we have $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
(3) (Identiy for $\cdot$) For all $x \in k$, we have $1 \cdot x = x \cdot 1 = x$;

(4) (Distributivity) For all $x, y, z \in k$, we have

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

(5) (Inverses for $\cdot$) If $x \in k^\times = k \backslash \{0\}$, then there exists $x^{-1} \in k$ such that $xx^{-1} = 1$.

The conditions (1), (2), (3) and (5) together imply that $(k^\times, \cdot, 1)$ is an *abelian* group.