Section 5.2 Finitely generated abelian groups

Recall If $n_1\ n_2\ n_3 \cdots n_k$ are relatively prime, then
$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1 n_2 \cdots n_k}$

Examples $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \quad \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_3 \cong \mathbb{Z}_{150} \quad \mathbb{Z}_2 \times \mathbb{Z}_4 \rightsquigarrow$ can't combine

Theorem (Likely from a previous algebra course)
G is a finite abelian group if and only if
$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \mathbb{Z}_{p_k^{\alpha_k}}$ where the p_i are primes.

Example Find all abelian groups of order $360 = 2^3 \cdot 3^2 \cdot 5$

$$
\begin{aligned}
&\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 && \cong \mathbb{Z}_{360} \\
&(\mathbb{Z}_2 \times \mathbb{Z}_4) \times \mathbb{Z}_9 \times \mathbb{Z}_5 && \cong \mathbb{Z}_{180} \times \mathbb{Z}_2 \\
&(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_9 \times \mathbb{Z}_5 && \cong \mathbb{Z}_{90} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
&\mathbb{Z}_8 \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_5 && \cong \mathbb{Z}_{120} \times \mathbb{Z}_3 \\
&(\mathbb{Z}_2 \times \mathbb{Z}_4) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_5 && \cong \mathbb{Z}_{60} \times \mathbb{Z}_6 \\
&\underbrace{(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_5}_{\text{Elementary divisor decompositions}} && \cong \underbrace{\mathbb{Z}_{30} \times \mathbb{Z}_6 \times \mathbb{Z}_2}_{\text{Invariant factor decompositions}}
\end{aligned}
$$

Definition $\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$ is called the free abelian group of rank r. Recall $\mathbb{Z} = \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$

Definition G is finitely generated if $G = \langle A \rangle$ for a finite set A.

Examples of finitely generated abelian groups:

$\mathbb{Z}^r$ generated by $A = \{(a,1,1,\ldots,1), (1,a,1,\ldots), (1,1,a,\ldots,1) \ldots (1,1,1,\ldots,a)\}$

$\mathbb{Z}^2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ generated by $A = \{(a,1,1,1), (1,a,1,1), (1,1,a,1), (1,1,1,a)\}$

$\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ generated by $A = \{(1,0), (0,1)\}$

Theorem 3 (Fundamental Theo. of finitely generated abelian Groups)
If G is a finitely generated abelian group, then

① $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$ where

ⓐ $r \geq 0$ and $n_i \geq 2 \quad \forall i$

ⓑ $n_{i+1} \mid n_i \quad \forall i, \ 1 \leq i \leq k$

② This expression is unique. If $G = \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_\ell}$ satisfying ⓐ and ⓑ, then $r = t$, $k = \ell$ and $m_i = n_i \ \forall i$.

Definitions r is called the free rank of G

m_i are called invariant factors of G

Decomposition ① is the invariant factor decomposition of G.

Theorem 5 Suppose G is an abelian group of order $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ (prime factorization). Then:

① $G \cong A_1 \times A_2 \times \dots \times A_k$ where $|A_i| = p_i^{\alpha_i}$

② For each $A = A_i$ with $|A| = p^{\alpha}$,

$A \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \dots \times \mathbb{Z}_{p^{\beta_t}}$ (invariant factor decomp)

with $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t$ and $\sum \beta_i = \alpha$

③ Decomposition ①, ② is unique.

Definitions Integers β_i above are called elementary divisors of G.
The decomposition in Theorem 5 is called the elementary divisor decomposition of G.

Elementary Abelian Groups

<u>Definition</u> An abelian group G is called an <u>elementary abelian group</u> if $|G| = p^n$ for some prime p <u>and</u> $a^p = 1$ for all $a \in G$.

By elementary divisor decomposition theorem, such a group must be $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \cong \mathbb{Z}_p^n$.

<u>Notation</u> $G = E_{p^n}$ = elementary abelian group of order p^n.

<u>Example</u> $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 = E_4$

Now lets switch to <u>additive</u> <u>notation</u>.

$E_{p^n} = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^n$

Consider the <u>field</u> $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. If $c \in \mathbb{F}_p$,
and $(x_1, x_2, \ldots x_n) \in E_{p^n}$ then $c(x_1, x_2 \cdots x_n) = (cx_1, cx_2, \ldots cx_n)$

Then E_{p^n} is a <u>vector space</u> over field $\mathbb{F}_p$.

~~Therefore $Aut(E_{p^n}) = GL_n(\mathbb{F}_p)$~~

$$E_{p^n} = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} : x_i \in \mathbb{F}_p \right\}$$

Homomorphisms $\varphi : E_{p^n} \to E_{p^n}$ are the same thing as linear transformations

$$\varphi\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}\right) = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$n \times n$ matrix

φ is automorphism $\Leftrightarrow$ φ invertible $\Leftrightarrow$ A invertible

$$Aut(E_{p^n}) = GL_n(\mathbb{F}_p)$$