1. Free abelian groups of finite rank and finitely generated abelian groups

<u>Definition</u>: Let $(G,+)$ be an abelian group.

1) A set $X \subseteq G$ is linearly independent if for $a_1,\dots,a_k \in X$ (with $a_i \neq a_j$ for $1 \le i,j \le k$, $i \neq j$) and $n_1,\dots,n_k \in \mathbb{Z}$ we have $\sum_{i=1}^{n} n_i a_i = 0 \implies n_1 = \dots = n_k = 0$,

2) A set $B \subseteq G$ is called a basis (of G) if $\langle B \rangle = G$ and B is linearly independent

<u>Examples</u>: 1) $\{1\}$ and $\{-1\}$ are both bases of $(\mathbb{Z},+)$: $\langle 1 \rangle = \langle -1 \rangle = \mathbb{Z}$ as $n = (\pm n)(\pm 1)\ \forall n \in \mathbb{Z}$ and $n \cdot (\pm 1) = 0 \implies n = 0$

2) Let $m \in \mathbb{N}, m \geq 2$. The group $(\mathbb{Z}_m, +)$ has no basis: Let $X \subseteq \mathbb{Z}_m$ such that $\langle X \rangle = \mathbb{Z}_m$. Then $X \neq \emptyset$ as $\langle \emptyset \rangle = \{\bar{0}\} \subsetneq \mathbb{Z}_m$ and $m \cdot x = \bar{0}\ \forall x \in X$.

3) Let $e_1 = (1,0,\dots,0)$, $e_2 = (0,1,0,\dots,0)$, $\dots$, $e_k = (0,\dots,0,1) \in \mathbb{Z}^k$. Then $\{e_1,\dots,e_k\}$ is a basis of $(\mathbb{Z}^k,+)$: $(n_1,\dots,n_k) = \sum_{i=1}^{k} n_i e_i\ \forall (n_1,\dots,n_k) \in \mathbb{Z}^k$ and $\sum_{i=1}^{k} n_i e_i = 0$

$\implies (n_1,\dots,n_k) = (0,\dots,0) \implies n_1 = \dots = n_k = 0$.

<u>Lemma 1</u> Let G be an abelian group and $a_1,\dots,a_k \in G$ linearly independent. Then every $x \in \langle a_1,\dots,a_k \rangle$ has a unique expression $x = \sum_{i=1}^{k} n_i a_i$ (i.e., $n_1,\dots,n_k \in \mathbb{Z}$ are uniquely determined). If $\{a_1,\dots,a_k\}$ is a basis of G then this holds for every $x \in G$.

<u>Proof</u>: Let $x = \sum_{i=1}^{k} n_i a_i = \sum_{i=1}^{k} m_i a_i$ (with $n_1,\dots,n_k, m_1,\dots,m_k \in \mathbb{Z}$) $\implies \sum_{i=1}^{k} (n_i - m_i) a_i = 0$

$\implies n_i = m_i$ for $1 \le i \le k$.

<u>Theorem 2</u> Let $G (\neq \{0\})$ be an abelian group. The following are equivalent:

(i) G has a finite basis with $k (\geq 1)$ elements,

(ii) $G \cong \mathbb{Z}^k$ (isomorphism of groups).

<u>Proof</u>: (i) $\implies$ (ii) Let $\{a_1,\dots,a_k\}$ be a basis of G. Then $\forall x \in G\ \exists!\, n_1,\dots,n_k \in \mathbb{Z}: x = \sum_{i=1}^{k} n_i a_i$.
The map $\varphi: G \to \mathbb{Z}^k$, $\varphi(x) = (n_1,\dots,n_k)$ is an isomorphism: If $y = \sum_{i=1}^{k} m_i a_i$ then $x + y = \sum_{i=1}^{k} (n_i + m_i) a_i$ and $\varphi(x+y) = (n_1+m_1,\dots,n_k+m_k) = (n_1,\dots,n_k) + (m_1,\dots,m_k) = \varphi(x) + \varphi(y)$, i.e., φ is a homomorphism, $\varphi(x) = (0,\dots,0) \implies (n_1,\dots,n_k) = (0,\dots,0) \implies x = \sum_{i=1}^{k} 0 \cdot a_i = 0$, i.e., φ is injective, and $(n_1,\dots,n_k) = \varphi\left(\sum_{i=1}^{k} n_i a_i\right)\ \forall (n_1,\dots,n_k) \in \mathbb{Z}^k$, i.e., φ is surjective.

(ii) If $\varphi: \mathbb{Z}^k \to G$ is an isomorphism then $\{\varphi(e_1),\dots,\varphi(e_k)\}$ is a basis of G:
If $x \in G$ then $\exists (n_1,\dots,n_k) \in \mathbb{Z}^k: x = \varphi(n_1,\dots,n_k) = \varphi\left(\sum_{i=1}^{k} n_i e_i\right) = \sum_{i=1}^{k} n_i \varphi(e_i)$, i.e., $G = \langle \varphi(e_1),\dots,\varphi(e_k) \rangle$ and $\sum_{i=1}^{k} n_i \varphi(e_i) = 0 \implies \varphi\left(\sum_{i=1}^{k} n_i e_i\right) = 0 \implies \sum_{i=1}^{k} n_i e_i = 0$

$\implies n_1 = \dots = n_k = 0$.

3.10.2022

Theorem 3 Let $G\ (\neq \{0\})$ be an abelian group and B and C two finite bases of G. Then $|B| = |C|$.

Proof: $2G = \{2x \mid x \in G\}$ is a subgroup of G as $2x - 2y = 2(x-y) \in 2G\ \forall x, y \in G$. Let $\varphi: G \to \mathbb{Z}^{|B|}$ be the isomorphism described in the proof of Theorem 2. Then its restriction $\varphi|_{2G}: 2G \to (2\mathbb{Z})^{|B|}$ is also an isomorphism: If $B = \{a_1, \dots, a_k\}$ and $x = \sum_{i=1}^{k} n_i a_i \in G$ then $2x = \sum_{i=1}^{k} (2n_i) a_i$ and $\varphi(2x) = (2n_1, \dots, 2n_k) \in (2\mathbb{Z})^k = (2\mathbb{Z})^{|B|}$, i.e.) $\varphi(2G) \subseteq (2\mathbb{Z})^{|B|}$ and $(2n_1, \dots, 2n_k) = \varphi\left(\sum_{i=1}^{k} (2n_i) a_i\right)\ \forall (n_1, \dots, n_k) \in \mathbb{Z}^k$. Then

$$G/_{2G} \cong \mathbb{Z}^{|B|}/_{(2\mathbb{Z})^{|B|}} \cong (\mathbb{Z}/2\mathbb{Z})^{|B|} \quad \text{and therefore } |G/_{2G}| = 2^{|B|}$$

Analogously $|G/_{2G}| = 2^{|C|}$ which implies $|B| = |C|$.

Definition: An abelian group G with the properties described in Theorem 2 is called a free abelian group of rank k. In addition $\{0\}$ is considered a free abelian group of rank 0 (with basis $\emptyset$).

Remark: A free abelian group of rank 1 is the same as an infinite cyclic group.

Definition: An $n \times n$-matrix $A = (\alpha_{ij})_{1 \le i,j \le n}$ with $\alpha_{ij} \in \mathbb{Z}$ for $1 \le i, j \le n$ is called unimodular if $\det A \in \{1, -1\}$.

Lemma 4 Let F be a free abelian group of rank n, $\{b_1, \dots, b_n\}$ a basis of F, $A = (\alpha_{ij})_{1 \le i,j \le n}$ an $n \times n$-matrix with entries in $\mathbb{Z}$ and $a_i = \sum_{j=1}^{n} \alpha_{ij} b_j$ for $1 \le i \le n$. Then the following are equivalent:

(i) $\{a_1, \dots, a_n\}$ is a basis of F,

(ii) A is unimodular.

Proof: (i) $\Rightarrow$ (ii) If $\{a_1, \dots, a_n\}$ is a basis then there are $\beta_{ij} \in \mathbb{Z}$ (with $1 \le i, j \le n$) such that $b_i = \sum_{j=1}^{n} \beta_{ij} a_j$ for $1 \le i \le n$. Let $B := (\beta_{ij})_{1 \le i,j \le n}$. Then

$$b_i = \sum_{j=1}^{n} \beta_{ij} a_j = \sum_{j=1}^{n} \beta_{ij} \sum_{k=1}^{n} \alpha_{jk} b_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \beta_{ij} \alpha_{jk} \right) b_k \quad \text{for } 1 \le i \le n.$$

As $\{b_1, \dots, b_n\}$ is a basis this implies $\sum_{j=1}^{n} \beta_{ij} \alpha_{jk} = \delta_{ik} = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}$ (with $1 \le i, k \le n$)

This says that $B \cdot A = I_n \left(= \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right)$ and therefore $\det A \cdot \det B = 1$. As $\det A, \det B \in \mathbb{Z}$ we get $\det A = \det B \in \{1, -1\}$.

(ii) $\Rightarrow$ (i) As $\det A \in \{1, -1\}$ we know that A^{-1} exists and has entries in $\mathbb{Z}$ (because of Cramer's rule).

Claim: $\{a_1,\dots,a_n\}$ is linearly independent. If $\sum_{i=1}^n m_i a_i = 0$ then

$$0 = \sum_{i=1}^n m_i a_i = \sum_{i=1}^n m_i \sum_{j=1}^n \alpha_{ij} b_j = \sum_{j=1}^n \Big(\sum_{i=1}^n m_i \alpha_{ij}\Big) b_j \implies \sum_{i=1}^n m_i \alpha_{ij} = 0 \text{ for } 1\le j\le n.$$

This says that $(m_1,\dots,m_n)\cdot A = (0,\dots,0)$ and thus $(m_1,\dots,m_n) = (0,\dots,0)\cdot A^{-1} = (0,\dots,0)$.

Claim: $\langle a_1,\dots,a_n\rangle = F$. It suffices to show that $b_1,\dots,b_n \in \langle a_1,\dots,a_n\rangle$.

If $A^{-1} = (\beta_{ij})_{1\le i,j\le n}$ then $A^{-1}\cdot A = I_n \implies \sum_{j=1}^n \beta_{ij}\alpha_{jk} = \delta_{ik}$ (for $1\le i,k\le n$) and

$$b_i = \sum_{k=1}^n \delta_{ik} b_k = \sum_{k=1}^n \Big(\sum_{j=1}^n \beta_{ij}\alpha_{jk}\Big) b_k = \sum_{j=1}^n \beta_{ij} \sum_{k=1}^n \alpha_{jk} b_k = \sum_{j=1}^n \beta_{ij} a_j \quad \text{for } 1\le i\le n.$$

<u>Theorem 5</u> Let F be a free abelian group of rank n and G a subgroup of F. Then G is also a free abelian group of rank $r\le n$. Furthermore, there is a basis $\{b_1,\dots,b_n\}$ of F and positive integers $\alpha_1,\dots,\alpha_r$ such that $\{\alpha_1 b_1,\dots,\alpha_r b_r\}$ is a basis of G and $\alpha_i \mid \alpha_{i+1}$ for $1\le i<r$.

<u>Convention</u>: In these lectures $\mathbb{N}$ will denote the set of positive integers, i.e., $\mathbb{N} = \{1,2,3,\dots\}$.

<u>Proof</u>: We use induction on n.

If $n=1$ then $F = \mathbb{Z}b_1$ for some $b_1\in F$. If $G=\{0\}$ we are done (and $r=0$). If $G\ne\{0\}$ let $S := \{s\in\mathbb{Z} \mid sb_1\in G\}$. As $a\in G \implies -a\in G$ we have $S\cap\mathbb{N}\ne\emptyset$. Let $\alpha_1 := \min(S\cap\mathbb{N})$.
We claim $G = \mathbb{Z}\alpha_1 b_1$: As $\alpha_1 b_1\in G$ we get $\mathbb{Z}\alpha_1 b_1\subseteq G$. If $a\in G$ then $\exists k\in\mathbb{Z}: a = kb_1$.
We use division with remainder: $k = q\alpha_1 + r_0$, $0\le r_0<\alpha_1 \implies r_0 b_1 = kb_1 - q\alpha_1 b_1 = a - q\alpha_1 b_1\in G$.
As α_1 was chosen minimal $r_0 = 0$ and $a = q\alpha_1 b_1\in\mathbb{Z}\alpha_1 b_1$, i.e. $G\subseteq \mathbb{Z}\alpha_1 b_1$.

Now let $n\ge 2$ and assume that the assertion has been proved for all free abelian groups of rank $<n$. If $G=\{0\}$ we are done. Assume $G\ne\{0\}$. Let

$$S := \{s\in\mathbb{Z} \mid \exists \text{ basis } \{c_1,\dots,c_n\} \text{ of } F \text{ and } \exists k_2,\dots,k_n\in\mathbb{Z}: sc_1 + k_2c_2+\dots+k_nc_n\in G\}.$$

Just as in the case $n=1$ we have $S\cap\mathbb{N}\ne\emptyset$. Let $\alpha_1 := \min(S\cap\mathbb{N})$. Then there is an $a\in G$, a basis $\{c_1,\dots,c_n\}$ of F and $k_2,\dots,k_n\in\mathbb{Z}$ such that $a = \alpha_1c_1 + k_2c_2+\dots+c_nk_n\in G$.
We use division with remainder: Let $k_i = \alpha_1 q_i + r_i$ with $0\le r_i<\alpha_1$ for $2\le i\le n$. Then

$$a = \alpha_1 c_1 + (\alpha_1 q_2 + r_2)c_2 + \dots + (\alpha_1 q_n + r_n)c_n = \alpha_1(c_1 + q_2c_2+\dots+q_nc_n) + r_2c_2+\dots+r_nc_n.$$

Let $b_1 := c_1 + q_2c_2+\dots+q_nc_n$. By Lemma 4 $\{b_1,c_2,\dots,c_n\}$ is also a basis of F.
As $a\in G$ and $r_i<\alpha_1$ for $2\le i\le n$ the definition of S implies $r_2=\dots=r_n=0$, i.e., $a = \alpha_1 b_1\in G$.
Let $H := \langle c_2,\dots,c_n\rangle = \mathbb{Z}c_2+\dots+\mathbb{Z}c_n$. Then H is a free abelian group of rank $n-1$

5.10.2022

and $F = \mathbb{Z}b_1 \oplus H$. We claim that $G = \mathbb{Z}\alpha_1 b_1 \oplus (G\cap H)$. We have

$\{0\} \subseteq (\mathbb{Z}\alpha_1 b_1) \cap (G\cap H) \subseteq \mathbb{Z}b_1 \cap H = \{0\}$ and therefore $(\mathbb{Z}\alpha_1 b_1)\cap(G\cap H) = \{0\}$.

We now check that $(\mathbb{Z}\alpha_1 b_1) + (G\cap H) = G$. As $\alpha_1 b_1 \in G$ clearly $(\mathbb{Z}\alpha_1 b_1) + (G\cap H) \subseteq G$.

Let $x\in G$. Then $\exists\, t_1,\dots,t_n \in \mathbb{Z} : x = t_1 b_1 + t_2 c_2 + \dots + t_n c_n \in G$. Use division with remainder:

$t_1 = \alpha_1 q_1 + r_1$ with $0 \le r_1 < \alpha_1 \Rightarrow x - \alpha_1 q_1 b_1 = r_1 b_1 + t_2 c_2 + \dots + t_n c_n \in G$. As α_1 was minimal we get $r_1 = 0$ and therefore $x = q_1\cdot\alpha_1 b_1 + \underbrace{t_2c_2 + \dots + t_n c_n}_{\in G\cap H} \in \mathbb{Z}\alpha_1 b_1 + (G\cap H)$.

If $G\cap H = \{0\}$ then $G = \mathbb{Z}\alpha_1 b_1$ and we are done (with $r=1$).

If $G\cap H \neq \{0\}$ the induction hypothesis implies that there is a basis $\{b_2,\dots,b_n\}$ of H, $r\in\{2,\dots,n\}$ and $\alpha_2,\dots,\alpha_r \in \mathbb{N}$ such that $G\cap H$ is a free abelian group with basis $\{\alpha_2 b_2,\dots,\alpha_r b_r\}$ where $\alpha_i \mid \alpha_{i+1}$ (for $2\le i<r$). Therefore $\{b_1,\dots,b_n\}$ is a basis of F and $\{\alpha_1 b_1, \alpha_2 b_2,\dots,\alpha_r b_r\}$ is a basis of G with $\alpha_i\mid\alpha_{i+1}$ for $2\le i<r$.

We still have to show $\alpha_1 \mid \alpha_2$: Let $\alpha_2 = q\alpha_1 + r_2$ with $0\le r_2 < \alpha_1$. By Lemma 4 $\{b_2, b_1 + qb_2, b_3,\dots,b_n\}$ is also a basis of F. We have $r_2 b_2 + \alpha_1(b_1 + q b_2) = \alpha_1 b_1 + \alpha_2 b_2 \in G$. As α_1 was minimal we get $r_2 = 0$ and therefore $\alpha_1\mid\alpha_2$

<u>Corollary 6</u> Let F be a free abelian group of rank r and G a subgroup of F. Then F/G is finite if and only if $\operatorname{rank} G = r$. If this is the case and $\{b_1,\dots,b_r\}$ and $\{c_1,\dots,c_r\}$ are bases of F and G with $c_i = \sum_{j=1}^{r} \gamma_{ij} b_j$ and $A = (\gamma_{ij})_{1\le i,j\le r}$ (a matrix with entries $\gamma_{ij}\in\mathbb{Z}$ for $1\le i,j\le r$) then $|F/G| = |\det A|$.

<u>Proof</u>: Let G have rank $s\,(\le r)$ and let $\{\bar b_1,\dots,\bar b_r\}$ and $\{\bar c_1,\dots,\bar c_s\}$ be bases of F and G as in Theorem 5, i.e., $\bar c_i = \alpha_i \bar b_i$ for some $\alpha_i\in\mathbb{N}$ (with $1\le i\le s$). Then

$$F/G \cong \underbrace{(\mathbb{Z}\oplus\dots\oplus\mathbb{Z})}_{r \text{ times}} \Big/ \big(\alpha_1\mathbb{Z}\oplus\dots\oplus\alpha_s\mathbb{Z}\oplus\underbrace{\{0\}\oplus\dots\oplus\{0\}}_{r-s \text{ times}}\big)$$

$$\cong (\mathbb{Z}/\alpha_1\mathbb{Z})\oplus\dots\oplus(\mathbb{Z}/\alpha_s\mathbb{Z})\oplus\underbrace{\mathbb{Z}\oplus\dots\oplus\mathbb{Z}}_{r-s \text{ times}}.$$

Clearly F/G is finite if and only if $r=s$. If this is the case then $|F/G| = \alpha_1\cdots\alpha_r$.

One can express $\bar b_i = \sum_{j=1}^{r}\beta_{ij} b_j$ $(1\le i\le r)$ and $c_i = \sum_{j=1}^{r}\mu_{ij}\bar c_j$ $(1\le i\le r)$ and therefore

$$\sum_{k=1}^{r}\gamma_{ik} b_k = c_i = \sum_{j=1}^{r}\mu_{ij}\bar c_j = \sum_{j=1}^{r}\mu_{ij}\alpha_j \bar b_j = \sum_{j=1}^{r}\mu_{ij}\alpha_j\sum_{k=1}^{r}\beta_{jk} b_k$$

$$= \sum_{k=1}^{r}\Big(\sum_{j=1}^{r}\mu_{ij}\alpha_j\beta_{jk}\Big) b_k$$

As $\{b_1,\dots,b_r\}$ is a basis this implies $\gamma_{ik} = \sum_{j=1}^{r} \mu_{ij}\alpha_j\beta_{jk}$ for $1\le i,k\le r$. $(\ast)$

We set $M := (\mu_{ij})_{1\le i,j\le r}$ and $B = (\beta_{jk})_{1\le j,k\le r}$. Then M and B are unimodular because of Lemma 4 and $(\ast)$ can be written as $A = M\cdot\begin{pmatrix}\alpha_1 & & 0\\ & \ddots & \\ 0 & & \alpha_r\end{pmatrix}\cdot B$. Taking determinants shows $|\det A| = \underbrace{|\det M|}_{=1}\cdot\underbrace{(\alpha_1\cdots\alpha_r)}_{=|F/G|}\cdot\underbrace{|\det B|}_{=1} = |F/G|$.

Lemma 7: Let G be a finitely generated abelian group with $\langle X\rangle = G$ where $X(\subseteq G)$ is finite. Then there is an epimorphism $\varphi: \mathbb{Z}^{|X|}\to G$.

Proof: If $X=\{a_1,\dots,a_n\}$ let $\varphi:\mathbb{Z}^{|X|}\to G$, $\varphi(k_1,\dots,k_n) = \sum_{i=1}^{n} k_ia_i$. Then φ is an epimorphism.

Theorem 8: Let G be a finitely generated abelian group generated by n of its elements. Then there are $s,t\in\mathbb{Z}$ (with $0\le s,t\le n$) and $m_1,\dots,m_t\in\mathbb{N}$ (with $m_1>1$ and $m_i|m_{i+1}$ for $1\le i<t$) such that $G\cong \mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_t\mathbb{Z}\oplus\mathbb{Z}^s$.

Proof: By Lemma 7 there is a free abelian group F of rank n and an epimorphism $\varphi: F\to G$. If φ is an is an isomorphism then $G\cong F\cong\mathbb{Z}^n$ and the theorem is proved (with $t=0$ and $s=n$). If φ is not an isomorphism then $\ker\varphi\neq\{0\}$ and by Theorem 5 there is a basis $\{b_1,\dots,b_n\}$ of F and $\alpha_1,\dots,\alpha_r\in\mathbb{N}$ with $\alpha_i|\alpha_{i+1}$ (for $1\le i<r$) such that $\{\alpha_1b_1,\dots,\alpha_rb_r\}$ is a basis of $\ker\varphi$.

Set $\alpha_i:=0$ for $r<i\le n$. Then $F=\mathbb{Z}b_1\oplus\cdots\oplus\mathbb{Z}b_n$ and $\ker\varphi = \mathbb{Z}\alpha_1b_1\oplus\cdots\oplus\mathbb{Z}\alpha_nb_n$.

Then

$$G\cong F/\ker\varphi = (\mathbb{Z}b_1\oplus\cdots\oplus\mathbb{Z}b_n)/(\mathbb{Z}\alpha_1b_1\oplus\cdots\oplus\mathbb{Z}\alpha_nb_n)$$
$$\cong(\mathbb{Z}b_1/\mathbb{Z}\alpha_1b_1)\oplus\cdots\oplus(\mathbb{Z}b_n/\mathbb{Z}\alpha_nb_n)\cong(\mathbb{Z}/\alpha_1\mathbb{Z})\oplus\cdots\oplus(\mathbb{Z}/\alpha_n\mathbb{Z}).$$

It holds that $\mathbb{Z}/\alpha_i\mathbb{Z}=\{0\}$ if $\alpha_i=1$ and $\mathbb{Z}/\alpha_i\mathbb{Z}=\mathbb{Z}$ if $\alpha_i=0$. So let $t:=|\{i\mid 1\le i\le n,\ \alpha_i\notin\{0,1\}\}|$, $s:=|\{i\mid 1\le i\le n,\ \alpha_i=0\}|$ and $m_1,\dots,m_t$ those α_i which are $\notin\{0,1\}$ (in the same order). Then $G\cong(\mathbb{Z}/m_1\mathbb{Z})\oplus\cdots\oplus(\mathbb{Z}/m_t\mathbb{Z})\oplus\mathbb{Z}^s$ where $m_1>1$ and $m_i|m_{i+1}$ for $1\le i<t$.

Remarks: 1) One can show that the integers s and $m_1,\dots,m_t$ in Theorem 8 are uniquely determined. The integers $m_1,\dots,m_t$ are called the invariant factors of the group G. Note that $m_1,\dots,m_t$ are not necessarily distinct.

2) Theorem 8 can be generalized to finitely generated modules over principal ideal domains.

Corollary 9 Let G be finitely generated abelian group. Then there are integers $s, \nu \geq 0$ and (not necessarily distinct) prime powers $p_1^{\beta_1}, \dots, p_\nu^{\beta_\nu}$ such that

$$G \cong (\mathbb{Z}/p_1^{\beta_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_\nu^{\beta_\nu}\mathbb{Z}) \oplus \mathbb{Z}^s.$$

Proof: This follows immediately from Theorem 8 and the following fact. If $m \in \mathbb{N}$ (with $m \geq 2$) has prime factorization $m = q_1^{\gamma_1} \cdots q_e^{\gamma_e}$ then

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/q_1^{\gamma_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/q_e^{\gamma_e}\mathbb{Z}).$$

Corollary 10 Let G be a finitely generated abelian group and H a subgroup of G. Then H is finitely generated too.

Proof: By Lemma 7 there is a free abelian group F and an epimorphism $\varphi: F \to G$. Then $\varphi^{-1}(H)$ is a subgroup of F and by Theorem 5 $\varphi^{-1}(H)$ is a free abelian group. If B is a (necessarily finite) basis of $\varphi^{-1}(H)$ then $\langle \varphi(B) \rangle = H$.

Remarks: 1) One can show that the prime powers in Corollary 9 are uniquely determined (except for their order). They are called elementary divisors of G.

2) Corollary 9 can also be generalized to finitely generated modules over principal ideal domains.

3) The subgroup $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z} \oplus \{0\}$ (which is the same as the subgroup $\mathbb{Z}/p_1^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_\nu^{\beta_\nu}\mathbb{Z} \oplus \{0\}$) is called the torsion subgroup of G. It contains exactly those elements of G which are of finite order.

10.10.2022