Free Abelian Groups

"linear algebra with groups"

Def: Let G be an abelian group w/ binary operation $+$. We say G is a free abelian group if there is a subset $X \subseteq G$ such that every $a \in G$ has a unique expression of the form

$$\boxed{a = n_1 x_1 + n_2 x_2 + \dots + n_r x_r}$$

where $n_j \in \mathbb{Z}$, $x_j \in X$

We call X a basis for G.

Ex: $G = \mathbb{Z} \oplus \mathbb{Z}$ is a free abelian group w/ basis $X = \{(1,0), (0,1)\}$

"Proof": $a \in G$ $\quad a = (m,n)$

$$a = \underline{m}(1,0) + \underline{n}(0,1)$$

Ex: $G = \mathbb{Z} \oplus \mathbb{Z}$ also has basis $X = \{(1,0), (1,1)\}$

$$(m,n) = \underline{c}\,(1,0) + \underline{d}\,(1,1)$$

$$\left.\begin{array}{l} m = c + d \\ n = d \end{array}\right\} \qquad d = n, \quad c = m - d = m - n$$

$$(m,n) = (m-n)(1,0) + n(1,1)$$

(still need to show this is unique)

Ex: $G = \mathbb{Z} \oplus \mathbb{Z}$. The set $X = \{(2,0), (0,2)\}$ is not a basis!

$$c(2,0) + d(0,2) = (2c, 2d)$$

Only getting pairs of even integers!!!

Not all groups are free abelian groups :(

Ex: $G = \mathbb{Z}_2 \oplus \mathbb{Z}$ Claim G is not a free abelian group

Proof of claim: Assume X is a basis for G.

$$\boxed{(1,0) = n_1x_1 + n_2x_2 + \dots + n_rx_r}$$

for some $n_j \in \mathbb{Z}$ and $x_j \in X$.

violates uniqueness!

But

$$3(1,0) = (3,0) = (1,0)$$

$$(1,0) = 3(1,0) = 3(n_1x_1 + n_2x_2 + \dots + n_rx_r)$$

$$\boxed{(1,0) = 3n_1x_1 + 3n_2x_2 + \dots + 3n_rx_r}$$

Couldn't have been a basis ...

Thus this is a contradiction and there <u>is</u> no basis!

<u>Theorem</u>: If G is a free abelian group w/ basis X (finite) $|X| = r$, then $G \cong \mathbb{Z}^r$

<u>Proof</u>:

Write $X = \{x_1, x_2, \dots, x_r\}$.

Define a map

$$\varphi: \mathbb{Z}^r \longrightarrow G$$

$$(n_1, n_2, \dots, n_r) \longmapsto \sum_{j=1}^{r} n_j x_j$$

<u>Claim</u>: This is an isomorphism!

$$(n_1, n_2, \dots, n_r) + (m_1, m_2, \dots, m_r) = (n_1+m_1, n_2+m_2, \dots, n_r+m_r)$$

$$\downarrow \varphi \qquad\qquad \downarrow \varphi \qquad\qquad \downarrow \varphi$$

$$\underbrace{\sum_{j=1}^{r} n_j x_j + \sum_{j=1}^{r} m_j x_j}_{\sum_{j=1}^{r} n_j x_j + m_j x_j} = \sum_{j=1}^{r} (n_j + m_j) x_j$$

Thus φ is a homomorphism

Surjectivity:

$$\varphi(n_1, \dots, n_r) = \sum_{j=1}^{r} n_j x_j$$

Since X is a basis, everything in G is of this form. Thus φ is surjective.

Injectivity: Suffices to show that

$$\ker(\varphi) = \{(0,0,\dots,0)\}$$

S'pose $\varphi(n_1, \dots, n_r) = \boxed{\sum_{j=1}^{r} n_j x_j = e} \in G$

Since φ is a homomorphism

$$e = \varphi(0,0,\dots,0) = \boxed{\sum_{j=1}^{r} 0\, x_j}$$

By uniqueness:

$$n_j = 0 \quad \forall j$$

Hence $(n_1, \dots, n_r) = (0,0,\dots,0)$

This proves $\ker(\varphi) = \{(0,0,\dots,0)\}$

$\square$

Assume G has a finite basis!

Theorem: Any two bases for a free abelian group G have the same cardinality.

Proof:

Let X be a basis for G.

By the previous theorem, there exists an isomorphism $\varphi : G \xrightarrow{\cong} \mathbb{Z}^r$

Because φ is a homomorphism,

$$\varphi(2g) = 2\varphi(g) \in 2\mathbb{Z}^r \quad \forall g \in G$$

$$\therefore \quad \varphi(2G) \subseteq 2\mathbb{Z}^r = 2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}$$

$\varphi(2G) = 2\mathbb{Z}^r$ because φ iso!

$$G \to \mathbb{Z}^r \to \mathbb{Z}^r / 2\mathbb{Z}^r$$

1st isomorphism theorem $\quad G/2G \cong \mathbb{Z}^r/2\mathbb{Z}^r$.

$$\mathbb{Z}^r/2\mathbb{Z}^r = \frac{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}{2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}} \cong \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{\substack{r\text{-many copies} \\ 2^r \text{ many elements}}}$$

$$2^r = |G/2G|$$

Summary: If X is a basis and $|X| = r$, then

- $|G/2G| = 2^r$

If Y is another basis and $|Y| = s$, then

- $|G/2G| = 2^s$

$$2^s = 2^r \Rightarrow s = r$$

$\square$

<u>Definition</u>: The <u>rank</u> of a free group G is the number of elements in a basis.

<u>Theorem</u>: Let G be a free abelian group with basis X. and H be another abelian group.
Then any function $f_0 : X \to H$ extends uniquely to a group homomorphism

$$f : G \to H.$$

ie $f(x) = f_0(x)$ for $x \in X$.

<u>Proof</u>: (Sketch)

Any element $a \in G$ must be of the form

$a = n_1 x_1 + n_2 x_2 + \dots + n_r x_r$ for some $x_1, \dots, x_r \in X$ and $n_1, \dots, n_r \in \mathbb{Z}$

$$\begin{aligned} f(a) &= f(n_1 x_1 + n_2 x_2 + \dots + n_r x_r) \\ &= f(n_1 x_1) + f(n_2 x_2) + \dots + f(n_r x_r) \\ &= n_1 f(x_1) + n_2 f(x_2) + \dots + n_r f(x_r) \end{aligned}$$

$$\boxed{f(a) = n_1 f_0(x_1) + n_2 f_0(x_2) + \dots + n_r f_0(x_r)}$$

Try this at home: prove that f is well-defined and a homomorphism.

Quick note on well-defined: make sure if $a \in G$ then $\exists!\, b \in H$ with $f(a) = b$.

<u>Corollary</u>: Any finitely generated abelian group G is a quotient of a free group.

<u>Proof</u>:

Let $\{g_1, g_2, \dots, g_r\}$ to be a set of generators of G. Define a homomorphism

$$\boxed{\begin{aligned} f: \mathbb{Z}^r &\to G \\ e_i &\mapsto g_i \end{aligned}}$$

where
$e_1 = (1, 0, 0, \dots, 0)$
$e_2 = (0, 1, 0, \dots, 0)$
$\vdots$
$e_r = (0, 0, 0, \dots, 1)$

Canonical basis for $\mathbb{Z}^n$

$$\begin{aligned} \operatorname{img}(f) &= \{ f(n_1, \dots, n_r) \mid (n_1, \dots, n_r) \in \mathbb{Z}^r \} \\ &= \{ \sum_{j=1}^{r} n_j g_i \mid n_1, \dots, n_r \in \mathbb{Z} \} \\ &= \langle \{ g_1, \dots, g_r \} \rangle = G \end{aligned}$$

!! surjective

1^{st} Iso. theorem $\Rightarrow$

$$\boxed{\frac{\mathbb{Z}^r}{\ker(f)} \cong G}$$

$\square$

<u>Theorem</u>: If $H < G$ and G is a free group then H is also a free group. Furthermore we can find a basis $\{x_1, \dots, x_r\}$ of G such that there are integers $a_1, a_2, \dots, a_s$ $(s < r)$ w/ $a_1 | a_2 | a_3 | \cdots | a_s$ satisfying

$\{a_1 x_1, \dots, a_s x_s\}$ is a basis of H.

<u>Ex</u>: $G = \mathbb{Z}_1$ $\quad H = 3\mathbb{Z}_1$

Basis for G is $\{1\}$

Basis for H is $\{3 \cdot 1\}$. $\square$