a) Seja M um $\mathbb{Z}$-módulo finitamente gerado tal que $am \neq 0$ para todo $a \in \mathbb{Z}^*$ e $m \in M^*$. Mostrar que M é um $\mathbb{Z}$-módulo livre.

Como M é finitamente gerado, então existe um $X \subseteq M$ finito tal que $M = AX$. Este X é um A-gerador de M. Assim temos que M é um A-módulo livre, se e somente se, admite pelo menos uma base.

Como temos $a \in \mathbb{Z}^*$, ou seja, $\mathbb{Z}$ sem o zero, e M^*, ou seja é um conjunto sem o zero. Então $am \neq 0$, para todo $a \in \mathbb{Z}^*$ e $m \in M^*$.

Como $\mathbb{Z}^*$ é um anel, então como todo anel é um módulo sobre si mesmo, tomamos a soma direta de $\mathbb{Z}^*$ com ele mesmo "$|I|$ vezes". Se $I = \{1, \dots, n\}$ então:

$$\mathbb{Z}^{*I} = \mathbb{Z}^{*(I)} = \underbrace{\mathbb{Z}^* \dots \mathbb{Z}^*}_{n \text{ vezes}} = \mathbb{Z}^{*N}$$

<u>Teorema</u>: Seja M um A-módulo, então M é livre, se e somente se, admite pelo menos uma A-base.

i) Por hipótese existe um conjunto $I \neq \emptyset$ tal que $M \cong \mathbb{Z}^{(I)}$, então existe um isomorfismo de $\mathbb{Z}$-módulo:

$$\varphi : \mathbb{Z}^{(I)} \longrightarrow M$$

Se tomarmos a proposição:

$\varphi: M \to N$ isomorfismo de A-módulo, S é A-base de M então $\varphi(S)$ é uma A-base de N.

Continuando se tomarmos: $S = \{e_i \mid i \in I\}$ é uma base de $\mathbb{Z}^{(I)}$ então $\varphi(S)$ é uma A-base de M.

ii) Supondo agora que M admite uma A-base S, considere: $S = \{v_i\}_{i \in S}$ e considere a função:

$$\varphi: \mathbb{Z}^{(I)} \longrightarrow M$$
$$(x_i)_{i \in I} \longrightarrow \sum_{i \in I} x_i v_i = \sum_{i \in \text{suport}(x)} x_i v_i$$

φ é um morfismo de $\mathbb{Z}$-modulos, e sejam $x = (x_i)_{i \in I}$, $y = (y_i)_{i \in I} \in \mathbb{Z}$ e $a \in A$. Então:

$$\varphi(ax+y) = \varphi\left((ax_i+y_i)_{i \in I}\right) =$$

$$\sum_{i \in I} (ax_i + y_i) v_i = a \sum_{i \in I} x_i v_i + \sum_{i \in I} y_i v_i =$$
$$a\varphi(x) + \varphi(y)$$

1) φ é injetiva, então seja $x = (x_i)_{i \in I} \in \ker \varphi$, seja $i \in I$ qualquer se $i \notin \text{suporte}(x)$ então $x_i = 0_{\mathbb{Z}}$.

Supondo que $i \in$ suporte(x), logo:

$$0_M = \varphi(x) = \sum_{l \in \text{suporte}(x)} x_l v_l$$

e como S é li, então $x_l = 0_{\mathbb{Z}}$ $\forall i \in I \Rightarrow$ $x = 0_{\mathbb{Z}^{(I)}}$.

2) φ é sobrejetiva, seja $v \in M$ e como S é um $\mathbb{Z}$-gerador de M, então:

$v = \alpha_1 v_1 + \dots + \alpha_N v_N$, com: $\alpha_1, \dots, \alpha_N \in \mathbb{Z}$ e $i_1, \dots, i_N \in I$.

Defini-se $x = (x_i)_{i \in I}$ dado por:

$$x_i = \begin{cases} \alpha_l, \text{ se } i = i_l, \text{ para algum } l \in \{1, \dots, N\} \\ 0_{\mathbb{Z}}, \text{ se } i \neq i_l \ \forall l \in \{1, \dots, N\} \end{cases}$$

Logo: $\varphi(x) = \sum_{i \in I} x_i v_i = 0$ para todos os índices fora de l, e portanto se tomarmos elementos em $\mathbb{Z}^*$ e M^* podemos desconsiderar este caso. Então temos somente o outro caso.

$$\sum_{l=1}^{N} x_{i_l} v_{i_l} = \sum_{l=1}^{N} \alpha_l v_{i_l} = v$$

Portanto, $\varphi: A^{(I)} \to M$ é um isomorfismo de $\mathbb{Z}$-módulos, e M é um $\mathbb{Z}$-módulo livre, possui uma base.

b) Mostrar com um exemplo, que na parte a) que a conclusão pode ser falsa se M não satisfaz a condição de que $am \neq 0$ para todo $a \in \mathbb{Z}^*$ e $m \in M^*$.

Tomamos um $\mathbb{Z}_{10}$.

$$10 \cdot m = \underbrace{m + m + \ldots\ldots + m}_{10 \text{ vezes}} = \bar{0}$$

Onde $10 \in \mathbb{Z}$ e $\mathbb{Z}_{10} \in M$

Então $\mathbb{Z}_{10}$ não é $\mathbb{Z}$-módulo livre.

Outro exemplo: $A = \dfrac{\mathbb{Z}}{4\mathbb{Z}}$, então $A^2 = A \oplus A$ é um A-módulo livre. Assim:

- $\bar{2} \in A$, $\bar{2} \neq \bar{0} = 0_A$
- $V = (\bar{2}, \bar{2}) \in A^2$, e $V \neq 0_{A^2}$

Porém: $\bar{2} \cdot V = (\bar{2} \cdot \bar{2}, \bar{2} \cdot \bar{2}) = (\bar{0}, \bar{0}) = 0_{A^2}$

c) Mostre com um exemplo, que na parte a) que a conclusão pode ser falsa se M não for finitamente gerado.

Tomamos o $\mathbb{Z}_p$, onde $\mathbb{Z}_p$-módulo.

Temos que $1 \in$ base de $\mathbb{Z}_p$, então:

$\bar{a}.\bar{1} = 0 \hookrightarrow \bar{a} = 0$, mas $a \in \mathbb{Z}^*$ e $m \in \mathbb{Z}^*$

Então $\mathbb{Z}_p$-módulo com p sendo primo deve ser finitamente gerado.