Thm If $0 \longrightarrow N \xrightarrow{\varphi} M \xrightarrow{\psi} K \longrightarrow 0$ splits from the left

(that is, $\exists\ \tau: M \longrightarrow N$ s.t. $\tau \circ \varphi = id_N$), then

$M \cong N \oplus K$.

Proof Let $K' = \ker(\tau)$. Claim: $K' \cong K$ by ψ and $M = \varphi(N) \oplus K'$

$\psi|_{K'}$ is an isomorphism: if $u \in K'$ & $\psi(u) = 0$ then $\exists\ v \in N$ s.t.

$u = \varphi(v)$. but $\tau(u) = 0$ so $\tau(\varphi(v)) = v = 0$ so $u = 0$, so $\psi|_{K'}$ is injective.

Claim: $K' \cap \varphi(N) = 0$, $K' + \varphi(N) = M$ ($\Rightarrow \psi|_{K'}$ is surjective)

$K' \cap \varphi(N) = K' \cap \ker\psi = \ker \psi|_{K'} = 0$.

why $K' + \varphi(N) = M$? Take $u \in M$. Let $v = \tau(u)$. Let $u_1 = \varphi(\tau(u))$. Then

$u_1 \in \varphi(N)$. Take $u_2 = u - u_1$ so $\tau(u_2) = \tau(u - \varphi(\tau(u))) = \tau(u) - \tau(u) = 0$

So $u_2 \in K'$. So $M = K' + \varphi(N)$, which implies the theorem.

M: R-module a set $S \subseteq M$ is linearly independent if whenever $a_1u_1 + \dots + a_nu_n = 0$

for $a_i \in R$, $u_i \in S$, $a_1 = \dots = a_n = 0$.

Theorem: $B \subseteq M$ is a basis of M iff B is linearly independent & generates M.

Claim: $\exists$ max'l linearly indp. set.

M: module. if $\nexists$ lin indp $\{u\}$, we are done (ϕ is max'l)

. . .

Let $\{u_1\}$ be lin indp if $\nexists u$ s.t. $\{u_1, u\}$ is lin indp, we are done

otherwise pick u_2 s.t. $\{u_1, u_2\}$ is lin indp. et. cetera. (Zorn's Lemma).

ex: torsion module: $\overset{\text{max'l}}{\emptyset}$ doesn't generate

ex: $\mathbb{Q}$ as a $\mathbb{Z}$-module. $u_1 = \frac{m}{n}$, $u_2 = \frac{k}{l}$. Then $(nk)u_1 - (ml)u_2 = 0$

So max'l linearly indep. set is a single element.

but $\{q\}$ does not generate $\mathbb{Q}$. $\mathbb{Q}/\mathbb{Z}\{q\}$ is a torsion module.

(X is a max'l linearly indep set iff M/RX is a torsion module).

Def: a collection $\mathcal{C}$ of subsets of X is a chain (or tower)

if $\forall A, B \in \mathcal{C}$, either $A \subseteq B$ or $B \subseteq A$.

Zorn's Lemma: Let X be a set and let $\mathcal{A}$ be a system of subsets of X.

Assume that for any chain $\mathcal{C} \subseteq \mathcal{A}$, $\bigcup \mathcal{C} = \bigcup_{c \in \mathcal{C}} c \in \mathcal{A}$.

Then $\mathcal{A}$ has a maximal element: $\exists A_0 \in \mathcal{A}$ s.t.

$\nexists B \in \mathcal{A}$ s.t. $A_0 \subsetneq B$.

let $\mathcal{A}$ be the set of all linearly independent subsets of M.

Then $\forall$ chain $\mathcal{C} \subseteq \mathcal{A}$, $\bigcup \mathcal{C}$ is linearly independent. linear independence is a finite property

So $\exists$ max'l chain.

Claim: $\prod_{i=1}^{\infty} \mathbb{Z}$ is not a free $\mathbb{Z}$-module.

Proof Assume it has a basis B. Then B is uncountable (if C is countable, $\mathbb{Z}C$ is countable).

countable $\to$ $\bigoplus_{i=1}^{\infty} \mathbb{Z} \subseteq \prod_{i=1}^{\infty} \mathbb{Z}^{\mathbb{N}}$. $\forall u \in \oplus \mathbb{Z}$, let $B_u \subseteq B$ (finite) s.t. $u \in \mathbb{Z} B_u$. Let $D = \bigcup_{u \in \oplus \mathbb{Z}} B_u$.

D is countable. Let $N = \mathbb{Z}D$. Then N is countable and $\oplus \mathbb{Z} \subseteq N$. Let $M = \prod \mathbb{Z} / N$. - freely generated by $B \setminus D$ (M is free).

But the element $u = (1, 2!, 3!, 4!, \ldots) \bmod N \in M$. Then $\forall k \in \mathbb{Z}$, $\exists v \in M$ so that $kv = u$ (u is divisible by any integer).

But a free $\mathbb{Z}$-module cannot have this property. $\lightning$.