Remark 6.55 (free modules, R-basis)

R commutative ring, M an R-module.

(1) Recall (Example 6.2 (10)):

By definition

M is free $\iff$ $M \simeq \bigoplus_{i \in I} R$ (denoted as $R^{(I)}$).

$$= \{ (x_i)_{i \in I} \mid x_i \in R \text{ with } x_i \neq 0 \text{ for finitely many } i \in I \}$$

(2) Let M be a module and $\{m_i\}_{i \in I}$ family of elements from M ($m_i \in M$).

- $\{m_i\}_{i \in I}$ is said to be <u>free</u> or <u>linearly independent</u> if

$$\sum_{i \in I} \alpha_i m_i = 0 \implies \alpha_i = 0 \text{ for all } i \in I.$$

$\alpha_i \in R$

- $\{m_i\}_{i \in I}$ is said to be an <u>R-basis</u> of M if the elements $\{m_i\}_{i \in I}$ are lin. independent and generate M

- $\bigoplus_{i \in I} R$ has a basis $\{e_k\}_{k \in I}$, where

Kronecker delta function

$$e_k = (\delta_{ki})_{i \in I} \in \bigoplus_{i \in I} R$$

that is $\delta_{ki} := \begin{cases} 1, & \text{if } i = k \\ 0, & \text{if } i \neq k \end{cases}$

$$e_k = (0, 0, \dots, \underset{k\text{-th coordinate} = 1}{1}, \dots, 0), \text{ others} = 0.$$

$\in \bigoplus_{i \in I} R$

$\forall\, (x_i)_{i \in I} = \sum_{i \in I} x_i e_i$

(3) $\mathrm{Hom}_R\left(\bigoplus_{i\in I} R, M\right) \overset{\text{Universal property}}{\simeq} \prod_{i\in I} \mathrm{Hom}_R(R, M) \overset{(*)}{\simeq} \prod_{i\in I} M$

$f \longmapsto (f_i)_{i\in I} \longmapsto (f(e_i))_{i\in I}$

$R \xrightarrow{i\text{-th component}} \bigoplus_{i\in I} R \xrightarrow{f} M$

f_i

(*) $\mathrm{Hom}_R(R, M) \xrightarrow{\sim} M$

$\varphi \longmapsto \varphi(1) \in M$

Note that φ is uniquely determined by $\varphi(1)$

Indeed, $\varphi(r) = \varphi(r\cdot 1) = r\,\varphi(1)$

(φ is R-linear)

- To define f $\Leftrightarrow$ To define image of the basis $(f(e_i))_{i\in I}$

(4) M admits an R-basis $\{m_i\}_{i\in I}$ $\Rightarrow$ M is free

Indeed,

$\bigoplus_{i\in I} R \longrightarrow M$ is an isomorphism

$e_i \longmapsto m_i$

(• surjective, since $\{m_i\}_{i\in I}$ generate M
• injective, since $\{m_i\}_{i\in I}$ is lin. indep.)

To define an R-linear map $f: M \to N$ $\Leftrightarrow$ To define images of the basis: $\{f(m_i)\}_{i\in I}$

$\forall m \in M$, $m = \sum_{i\in I} \alpha_i m_i$ $\quad f(m) = \sum_{i\in I} \alpha_i f(m_i)$

(5) • If $M \simeq R^n$, we say M is free of rank n and set $\operatorname{rank} M := n$.

Note that $\operatorname{rank} M$ is well-defined, that is $R^n \simeq R^m \Rightarrow n = m$ (next Exercise sheet).

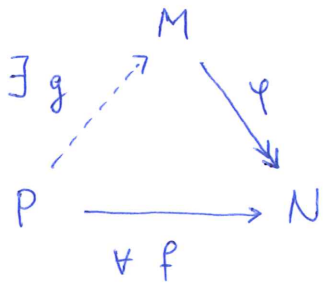
• $\operatorname{rank}(M \oplus N) = \operatorname{rank} M + \operatorname{rank} N$ (M, N free with finite rank)

Next we will prove several properties of projective modules.

Recall (Definition 6.27): Let P be an R-module. P is projective (by definition) if for every surjective map of modules $M \xrightarrow{\varphi} N$ the induced map

$$\operatorname{Hom}_R(P, M) \longrightarrow \operatorname{Hom}_R(P, N) \quad \text{is also surjective.}$$
$$g \longmapsto \varphi \circ g$$

That is: $\forall\, f : P \longrightarrow N$ there exists $g : P \longrightarrow M$, s.t. $f = \varphi \circ g$

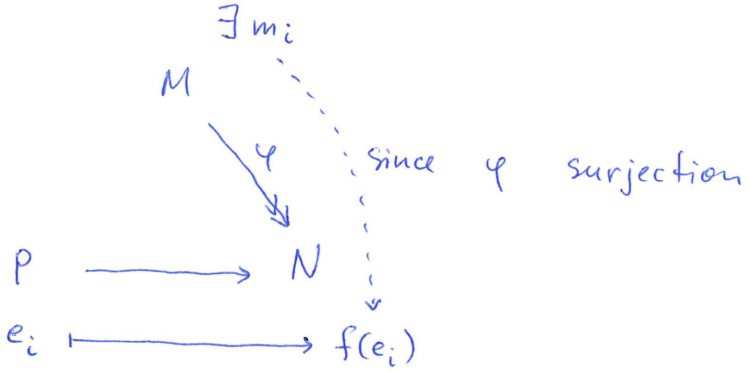


Proposition 6.56 (Example 6.30 (1)).

Free modules are projective.

Proof Let P be a free module with basis $\{e_i\}_{i\in I}$.

Let $\varphi: M \twoheadrightarrow N$ be a surjection & $f: P \longrightarrow N$ a map



Since $\{e_i\}_{i\in I}$ R-basis of P, define $g: P \longrightarrow M$

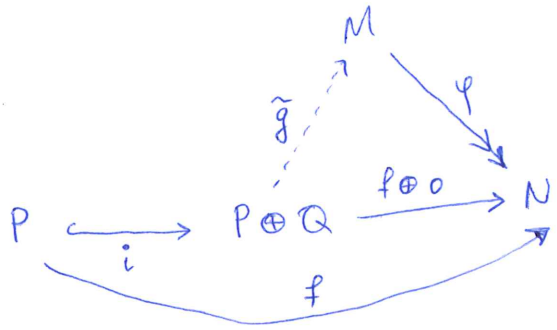
by $g(e_i) := m_i$.

Then $\varphi \circ g\,(e_i) = f(e_i)$ $\forall\, i \in I$ Hence, $\varphi \circ g = f$.

Proposition 6.57 P, Q R-modules. Then

$P \oplus Q$ is projective $\Rightarrow$ P is projective & Q is projective

Proof



Every $f: P \longrightarrow N$ we can write as a composition

$$P \xrightarrow{\ i\ } P \oplus Q \xrightarrow{\ f\oplus 0\ } N$$

$$x \longmapsto (x, 0)$$

Then set $g := \tilde{g} \circ i$

Since $P \oplus Q$ is projective, $\exists\ \tilde{g}: P \oplus Q \longrightarrow M$, such that $\varphi \circ (f \oplus 0) = \tilde{g}$

Definition 6.58

We say that a module M is an ~~dir~~ (internal) direct sum of two submodules $M_1 \subset M$ and $M_2 \subset M$ if the natural map (given by inclusions $M_i \hookrightarrow M$)

$$M_1 \oplus M_2 \xrightarrow{\varphi} M \qquad (m_1, m_2) \longmapsto m_1 + m_2$$

is an iso.

and we write $M = M_1 \oplus M_2$ in this case.

That is
- $M = M_1 + M_2$ ($\Leftrightarrow \varphi$ is surjective)
- $M_1 \cap M_2 = (0)$ ($\Leftrightarrow \varphi$ is injective)

Proposition 6.59 (Retracts in $Mod(R)$ are direct summands)

Exercise on the page 36

Let N, M be two modules and $N \underset{j}{\overset{i}{\rightleftarrows}} M$ two maps, (N is retract of M) such that $j \circ i = id_N$. Then

$$M = \underset{\cong N}{\operatorname{Im} i} \oplus \operatorname{Ker} j$$

- $\forall\, m \in M$ write: $m = i(j(m)) + (m - i(j(m)))$

  $i(j(m)) \in \operatorname{Im} i$, $(m - i(j(m))) \in \operatorname{Ker} j$

  $j(m) - \underbrace{j \circ i \circ j}_{id}(m) = 0$

- Let $m \in \operatorname{Im} i \cap \operatorname{Ker} j$, $m = i(n)$, $0 = j(m) = \underbrace{j \circ i}_{id}(n) = n$

  $\Rightarrow m = i(n) = i(0) = 0$.

Proposition 6.60

P projective module & $\varphi: M \twoheadrightarrow P$ surjection

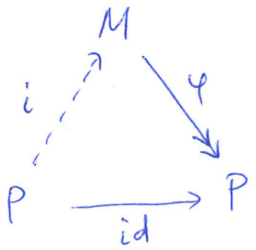
Then $P \oplus \operatorname{Ker}\varphi \simeq M$

In particular, P is a direct summand of M.

Proof P projective $\Rightarrow$ $\operatorname{Hom}_R(P,M) \twoheadrightarrow \operatorname{Hom}_R(P,P)$ surjective (identity $\in \operatorname{Hom}_R(P,P)$)

$g \longmapsto \varphi \circ g$

There is a preimage of id_P:



$\exists\, i \in \operatorname{Hom}_R(P,M)$, s.t. $\varphi \circ i = id$

Note that i is injective

By Proposition 6.59: $M = \underset{\simeq P}{\operatorname{Im} i} \oplus \operatorname{Ker}\varphi \simeq P \oplus \operatorname{Ker}\varphi$

Remark 6.61

P projective module.

For an exact sequence: $0 \longrightarrow Q \xrightarrow{\alpha} M \xrightarrow{\varphi} P \longrightarrow 0$ (*)

we have: $M \simeq P \oplus Q$

Indeed by Prop 6.60 $M \simeq P \oplus \underset{\operatorname{Im}\alpha}{\operatorname{Ker}\varphi} = P \oplus \operatorname{Im}\alpha \simeq P \oplus Q$.

We say that the sequence (*) is split

(See Tutorium 6, Ex. 3)

Proposition 6.62 Let P be a module.

The following two conditions are equivalent

(1) P is projective

(2) $\exists$ module Q, such that $P \oplus Q$ is free

(P is a direct summand of a free module).

Proof: (2) $\Rightarrow$ (1)

follows from Prop 6.56 (free $\Rightarrow$ projective) + Proposition 6.57 ($P \oplus Q$ projective $\Rightarrow$ P projective)

Let us prove (1) $\Rightarrow$ (2)

By Proposition 6.60 it is enough to find a free module M with surjection $\varphi: M \twoheadrightarrow P$

Let $\{x_i\}_{i \in I}$ be a family of generators of P

Take $M = \bigoplus_{i \in I} R$ and define $\varphi: \bigoplus_{i \in I} R \longrightarrow P$

$e_i \longrightarrow m_i$

Clearly φ is surjective (since $\{m_i\}_{i \in I}$ generate P) ∎

Remark 6.63 We know that "free" $\Rightarrow$ "projective"

The converse is not true in general.

Take $R = R_1 \times R_2$, where $R_1 \neq 0$, $R_2 \neq 0$ two rings.

Denote $e_1 = (1,0)$, $e_2 = (0,1)$ and consider principal ideals $I_1 = (e_1)$ & $I_2 = (e_2)$

$1 = e_1 + e_2$ & $e_i^2 = e_i$ & $e_1 e_2 = 0$

Then

$R = I_1 \oplus I_2 \Rightarrow I_1$ projective, but $e_2 I_1 = 0$ (so I_1 can not be free)

Later: "free" $\underset{R \text{ is PID}}{<}$ "projective"

Modules: free $\xrightarrow[\text{Prop 6.56}]{\Longrightarrow}$ projective $\xrightarrow[\text{Ex 1 Sheet 6}]{\Longrightarrow}$ flat

Proposition 6.64 (Ideal Criterion for flatness)

R commutative ring, M R-module.

Then M is flat over R if and only if for every finitely gen. ideal I the inclusion $I \xrightarrow{i} R$ induces an injection

$$I \otimes_R M \xrightarrow{i \otimes id} R \otimes_R M \simeq M$$

$$i \otimes m \longmapsto i \otimes m = im$$

Proof "$\Rightarrow$" is clear.

Assume for every fin. gen. ideal I

$$(*) \quad I \otimes M \longrightarrow R \otimes M \quad \text{is injective.}$$

Observations:

(1) $(*)$ also holds for any ideal $I \subset R$.

Let $x \in \ker i \otimes id$

$$I \otimes M \xrightarrow{i \otimes id} M$$

$$x = \sum_{\ell=1}^{k} i_\ell \otimes m_\ell \longmapsto 0$$

$$\uparrow$$

$$x' = \sum_{\ell=1}^{k} i_\ell \otimes m_\ell$$

$$I' \otimes M \quad (i_1, \dots, i_k)$$

$\uparrow$ finitely generated

$j \circ (i \otimes id)$ is injective $\Rightarrow$ $x' = 0$ $\Rightarrow$ $x = 0$ $\Rightarrow$ $i \otimes id$ injective

We have to show:

$$(**) \quad \underbrace{(N' \hookrightarrow N)}_{\text{injective}} \Rightarrow \underbrace{(N' \otimes M \longrightarrow N \otimes M)}_{\text{injective}}$$

- We can assume $N' \xrightarrow{f} N$ a submodule of N.
- We can assume N/N' is finitely generated as R-module (see Corollary 2.13, Atiyah Macdonald book)

That is $N = N' + (n_1, \dots, n_k)$, $n_i \in N$

- By induction on k we can assume $k = 1$.

To show $(**)$ it is enough to consider the case $N = N' + (n)$, where $N' \subset N$ and $n \in N$.

$$I := \{a \in R \mid an \in N'\} = \ker\left(R \xrightarrow{g} N \xrightarrow{\pi} N/N'\right)$$
$$1 \longmapsto n$$

$$\begin{array}{ccccccc}
0 & \to & I & \xrightarrow{i} & R & \longrightarrow & R/I \xrightarrow{1} 0 \\
 & & \downarrow \tilde{g} & & \downarrow g & & \downarrow \wr \quad \downarrow \\
0 & \to & N' & \xrightarrow[f]{} & N & \longrightarrow & N/N' \to 0 \\
 & & & & & & n+N'
\end{array}$$

The following sequence is exact

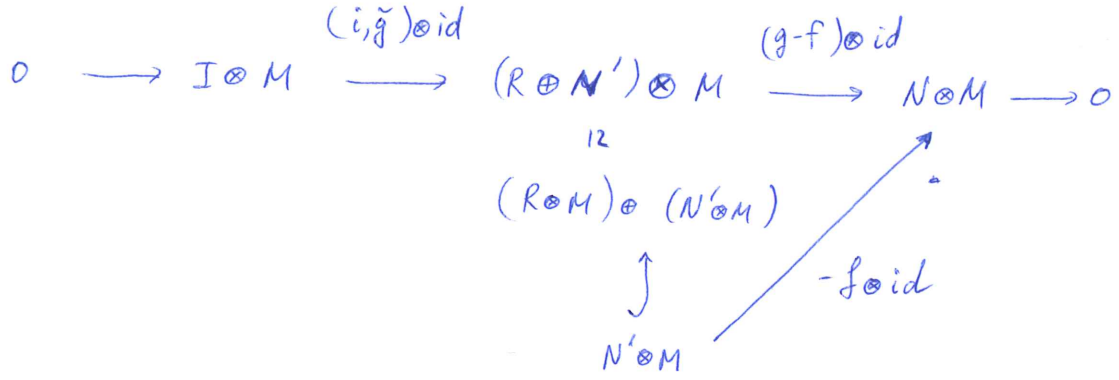
$$(a, n') \longmapsto an - n'$$

$$(ES) \quad 0 \longrightarrow I \xrightarrow{(i, \tilde{g})} R \oplus N' \xrightarrow{g-f} N \to 0$$

$$a \longmapsto (a, an)$$

Applying $-\otimes_R M$ to (ES) we get

($-\otimes_R M$ is right exact by ~~Prop~~ Lemma 6.26)



Let $y \in \ker f\otimes id$, then

$0\otimes y \in \ker (g-f)\otimes id = \operatorname{Im}(i,\tilde{g})\otimes id$

$\exists\, x \in I\otimes M$, s.t. $(i\otimes id)(x) = 0$ & $(\tilde{g}\otimes id)(x) = y$

↑

since $i\otimes id$ is injective

by our assumption, it follows $x=0 \Rightarrow y = 0$ $(\tilde{g}\otimes id)(\underset{0}{x}) = 0$

$\Rightarrow \ker(f\otimes id) = 0 \Rightarrow f\otimes id$ is injective ∎

(Finitely generated) modules over PIDs.

Let R be a PID (integral + every ideal is principal)

Definition 6.65 R PID and M R-module. Define

$$\mathrm{Tors}(M) = \{ m \in M \mid \exists\, r \in R \setminus \{0\} \text{ s.t. } rm = 0 \}$$

an R-submodule of M called the submodule of torsion elements. An R-module is called torsion if $\mathrm{Tors}(M) = M$ and torsion-free if $\mathrm{Tors}(M) = 0$

Example: $\mathrm{Tors}(R) = 0$ & $\mathrm{Tors}(R/I) = R/I$

Remark 6.66 For a general ring, R

$$\mathrm{Tors}(M) := \{ m \in M \mid \exists\, r \in R \text{ not zero divisor, s.t. } rm = 0 \}$$

Prop. 6.67 R PID, M R-module

Then M is flat $\Leftrightarrow$ M is torsion free.

Proof: "$\Rightarrow$" holds for an arbitrary R

(see Tutorium 6, Ex 2): (M flat, $a \in R$ not a zero-divisor

Then $am = 0 \Rightarrow m = 0$ $\forall m \in M$)

"$\Leftarrow$" By Prop 6.64 it is enough to

show that $I \otimes M \xrightarrow{\varphi} M$ is injective $\forall$ ideal $I \hookrightarrow R$

$i \otimes m \longmapsto im$

$I=(a)$ for some $a \in R$ (since R is PID)

Every element in $(a) \otimes M$ can be written as

$a \otimes m$

(Indeed, $\sum x_i a \otimes m_i = \sum a \otimes x_i m_i = a \otimes \sum x_i m_i$)

If $0 = \varphi(a \otimes m) = am$ (and $a \neq 0$), then $m = 0$ (since M torsion free)

Hence, $a \otimes m = 0$ and φ is injective.

Example 6.68

- $\mathbb{Q}$ is a flat $\mathbb{Z}$-module (since $\mathbb{Q}$ is torsion free)
- $\mathbb{Q}$ is not projective over $\mathbb{Z}$ (Exercise)

Remark 6.69 R commutative Ring.

Let

$$(*) \quad 0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$$

be an exact sequence of R-modules

Let $N \subset M$ submodule.

Then the induced sequence

$$(**) \quad 0 \longrightarrow i^{-1}(N) \xrightarrow{i} N \xrightarrow{p} p(N) \longrightarrow 0$$

is also exact.

Proof Exactness of $(**)$ follows from the construction (we take preimage $i^{-1}(N)$ & image $p(N)$ of N) and the exactness of $(*)$

Proposition 6.70 R PID. Let M be a submodule of a free module F of finite Rank n (that is $F \simeq R^n$)
Then M is free and ~~rk~~ rank $(N) \leq n$.

Proof Induction on rank $F = n$.

- $n = 1$ N is a submodule of R
  $\Rightarrow$ $N \subset R$ an ideal $\Rightarrow$ (R is PID) $N = (x)$ for some $x \in R$
  - $x = 0 \Rightarrow N = (0)$ free of rank 0.
  - $x \neq 0$ ($\varphi_x : R \longrightarrow R$, $a \longmapsto ax$ injective $\Rightarrow R \simeq \operatorname{Im} \varphi_x = N$)
    N is free of rank 1.

In general, assume $N \subseteq F = R^n$

and consider the exact sequence

$$0 \longrightarrow R^{n-1} \xrightarrow{i} R^n \xrightarrow{p} R \longrightarrow 0$$

where

$$(x_1, \dots, x_{n-1}) \xmapsto{i} (x_1, \dots, x_{n-1}, 0)$$

and p is the projection on the last coordinate

$$R^n \ni (x_1, \dots, x_n) \xmapsto{p} x_n \in R$$

By Remark 6.69 we get the induced exact sequence (below)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^{n-1} & \xrightarrow{i} & R^n & \xrightarrow{p} & R & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & i^{-1}(N) & \xrightarrow{\tilde{i}} & N & \xrightarrow{\tilde{p}} & p(N) & \longrightarrow & 0 \end{array}$$

$\tilde{i}$ and $\tilde{p}$ are respectively restrictions of i and p on $i^{-1}(N)$ and N. (respectively)

- $p(N) \subset R$
  - $p(N) = 0$, then $N \subseteq R^{n-1}$ and by induction hypothesis N is free of rank $\leq n-1$.
  - $p(N) \neq 0$ then $p(N) \simeq R$ (in particular, $p(N)$ is projective)

Hence the sequence $0 \longrightarrow i^{-1}(N) \xrightarrow{\tilde{i}} N \xrightarrow{\tilde{p}} p(N) \longrightarrow 0$

split by Remark 6.61 (since $p(N) \simeq R$ is projective)

We get $N \simeq \underbrace{p(N)}_{\substack{\text{free} \\ \text{case } n=1}} \oplus \underbrace{i^{-1}(N)}_{\substack{\text{free by induction hypothesis} \\ (\text{since } i^{-1}(N) \subseteq R^{n-1})}}$

Therefore N is free and rank $N \leq 1 + (n-1) = n$. ∎

Corollary 6.71 . Finitely generated projective modules over PID are free

Proof By Prop 6.61 a finitely generated proj. module P is a submodule of a free module of finite rank (since P is fin. gen.)

Then the statement follows from Proposition 6.70.

Remark 6.72 Proposition 6.70 holds for any free module F.
(but a bit more difficult to prove, one needs some set theory)

Thus, ~~over PID~~ for modules over PID we have:

projective $\Rightarrow$ free.

Proposition 6.73 Let R be a PID,
M finitely generated torsion-free module over R.
Then M is a free module of finite rank.

Proof Let $\{m_1, \dots, m_n\}$ be the set of generators of M.
Let r be the maximal number of lin. independent elements in the set $\{m_1, \dots, m_n\}$

Up to reordering assume that $m_1, \dots, m_r$ are linearly independent.
and set $N = (m_1, \dots, m_r) \subseteq M$

Note that N is free of rank r.

$\forall\, j = r+1, \dots, n$ there exist $a_j \in R$, $a_j \neq 0$, such that $a_j m_j \in N$
(otherwise $\{m_1, \dots, m_r, m_j$ are linearly independent which contradicts the choice of r).

Take $a = a_{r+1} \cdot \dots \cdot a_n \neq 0$

Consider the R-linear map

$$\varphi_a : M \longrightarrow M \qquad m \longmapsto am$$

injective, since $a \neq 0$ & M is torsion free.

Note that $am_i \in N \quad \forall\, i = 1, \dots, n$

Hence, we have $M \simeq \operatorname{Im} \varphi_a \subseteq N$ (φ_a injective; N free finitely generated) $\overset{\text{Prop. 6.70}}{\Longrightarrow}$ M is free of finite rank.

Corollary 6.74 Every finitely generated flat module over PID is free.

Proof: Follows from Proposition 6.67 and the above Proposition.

(over PID: flat $\Leftrightarrow$ torsion free)

Remark: In general, not every flat module over PID is free.
Counterexample: $\mathbb{Q}$ as $\mathbb{Z}$-module. ($\mathbb{Q}$ is even not projective)

Exercise: Deduce from Prop 6.73 that for any finitely generated R-module M (R is PID) we have:

$$M \simeq M' \oplus \operatorname{Tors} M,$$

for some free module M'.

Theorem 6.75

R PID

Let M be a free R-module of finite rank n.
and let N be a submodule of M

Then there exist a basis $w_1, w_2, \dots, w_n$ of M
such that $a_1 w_1, \dots, a_m w_m$ is an R-basis of N
for some $m \le n$ and $a_i \in R$, $a_i \neq 0$ with $a_1 | a_2 | \dots | a_m$

Proof: ~~Assume $N \neq 0$. Suppose~~
Induction on $\operatorname{rk} M = n$

Consider the set of ideals in R

$$S := \{ \underbrace{\varphi(N)}_{(a_\varphi)} \mid \varphi : M \longrightarrow R \quad R\text{-linear} \}$$

$S \neq \emptyset$, since $(0) \in S$.

If $N = 0$ we take $m = 0$, assume $N \neq 0$

R is Noetherian (since PID $\Rightarrow$ Noetherian)

Hence, S has a maximal element (a_u) (with respect to inclusion) for some $u : M \longrightarrow R$

We denote $a_1 := a_u$ and $w \in N$, s.t. $u(w) = a_1$

Note that $a_1 \neq 0$ (since $N \neq 0$)

Take $0 \neq n = \alpha_1 e_1 + \dots + \alpha_n e_n \in N$, where $\{e_i\}$ basis of M

Then at least one $\alpha_i \neq 0$

Then $e_i^*(N) \neq 0$ and $e_i^*(N) \in S$

where $e_i^* : M \longrightarrow R$

$e_j \longmapsto \delta_{ij}$

Claim: $\forall\ \varphi : M \longrightarrow R$ R-linear we have $\varphi(\omega) \in (a_1)$

(that is $a_1 \mid \varphi(\omega)$)

Consider the ideal $(\varphi(\omega), a_1) = (d)$ for some $d \in R$

$$d = r_1\varphi(\omega) + r_2 a_1 = r_1\varphi(\omega) + r_2 v(\omega) = \underbrace{(r_1\varphi + r_2 v)}(\omega)$$

R-linear map: $M \to R$

$$\Rightarrow \quad d \in (r_1\varphi + r_2 v)(N) \in S$$

We have $(a_1) \subseteq (d) \subseteq (r_1\varphi + r_2 v)(N) \in S$

By maximality of (a_1) we must have equalities in both inclusions above $\Rightarrow$ $(a_1) = (d) = (\varphi(\omega), a_1)$

$\Rightarrow$ $\varphi(\omega) \in (a_1)$ $\Rightarrow$ $a_1 \mid \varphi(\omega)$.

Let $e_1, \dots, e_n$ be an R-basis of M

Consider $e_i^* : M \longrightarrow R$

$$e_j \longmapsto \delta_{ji} = \begin{cases} 1, & \text{if } j = i \\ 0, & \text{if } j \neq i \end{cases}$$

Then $e_i^* (\alpha_1 e_1 + \dots + \alpha_n e_n) = \alpha_i$

Write $w = \alpha_1 e_1 + \dots + \alpha_n e_n$

Then $e_i^*(w) = \alpha_i$ and by Claim $a_1 \mid \alpha_i \quad \forall i = 1, \dots, n$,

that is $\alpha_i = a_1 \beta_i$ for some $\beta_i, i = 1, \dots n$.

We have $w = \alpha_1 e_1 + \dots + \alpha_n e_n = a_1 \beta_1 e_1 + \dots + a_1 \beta_n e_n = a_1 \underbrace{(\beta_1 e_1 + \dots + \beta_n e_n)}_{\text{denote by } w_1}$

Since $u(w) = a_1$, we get $a_1 = u(w) = u(a_1 w_1) = a_1 u(w_1)$

$\Rightarrow u(w_1) = 1$ (Indeed, $a_1 (1 - u(w_1)) = 0 \Longrightarrow u(w_1) = 1$) (R is PID)

Now we can reduce to the case $rk = n-1$.

We have

$$M \underset{\exists\, i \ R\text{-linear with } i(1) = w_1}{\overset{u}{\rightleftarrows}} R \qquad w_1 \longmapsto 1$$

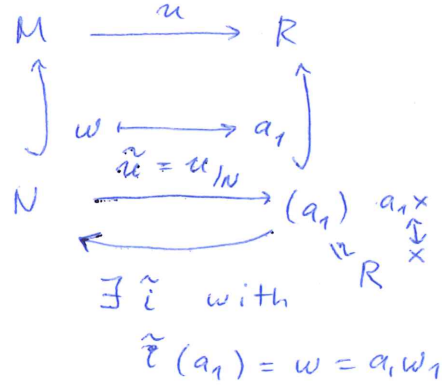
, then $u \circ i = id_R$ (so we know that R is a direct summand of M)

More precisely,

By Proposition 6.59 : $M = \underset{\cong R}{\operatorname{Im} i} \oplus \operatorname{Ker} u = R w_1 \oplus \operatorname{Ker} u$

$rk(\operatorname{Ker} u) = n-1$

Similarly :



$\Rightarrow \quad \tilde{u} \circ \tilde{i} = id$

Once again by Prop 6.59 we have:

$$N = \underset{\cong R}{\operatorname{Im} \tilde{i}} \oplus \operatorname{Ker} \tilde{u} = R(aw_1) \oplus \underbrace{(\operatorname{Ker} u \cap N)}_{N'}$$

Now $\operatorname{rk}(\operatorname{Ker} u) = n-1$ and $N' \subset \operatorname{Ker} u$,

so by Induction hypothesis

$\exists$ R-basis $w_2, \dots, w_n$ of $\operatorname{Ker} u$

such that $a_2 w_2, \dots, a_m w_m$ is an R-basis of N'

for some $m \leq n$ & $a_i \in R$, $a_i \neq 0$ with $a_2 | a_3 | \dots | a_m$

Then we take $w_1, w_2, \dots, w_n$ for an R-basis of M.

It ~~remains to show that~~ $a_1 | a_2$

and $a_1 w_1, \dots, a_n w_n$ is an R-basis of N.

It remains to show that $a_1 | a_2$.

Consider $(w_1^* + w_2^*) : M \longrightarrow R$ R-linear.

We have $(w_1^* + w_2^*)(\underset{= a_1 w_1}{w}) = a_1 \in (w_1^* + w_2^*)(N)$

$\Rightarrow (a_1) \subseteq (w_1^* + w_2^*)(N) \xrightarrow[\text{of } (a_1) \text{ in } S]{\text{By maximality}} (a_1) = (w_1^* + w_2^*)(N)$

Then $a_2 = (w_1^* + w_2^*)(\underbrace{a_2 w_2}_{\in N}) \in (a_1) \Longrightarrow a_2 \in (a_1) \Rightarrow a_1 | a_2$

Corollary 6.76 (Structure Theorem for finitely generated modules over PID)

R PID, M a finitely generated module over R

Then $$M \simeq \bigoplus_{i=1}^{r} R \oplus \bigoplus_{i=1}^{m} R/(a_i)$$ where a_i are non-zero not units & $a_1 | a_2 | \dots | a_m$ $(m \leq n)$

Moreover, r, m and ideals (a_i) are uniquely determined.

Proof ~~Take E a free R-module~~

M is generated by $m_1, \dots, m_n \in M$

Take E a free R-module with R-basis $\{e_1, \dots, e_n\}$

Consider R-linear map: $\varphi : E \twoheadrightarrow M$, $e_i \mapsto m_i$

φ surjective, since $m_1, \dots, m_n$ generate M. Set $N = \ker \varphi$

By Isomorphic sat z $$M \simeq E/\ker\varphi = E/N$$

We apply Theorem 6.75 to $N \subset E$: (E free of rank n.)

$\exists$ R-basis $w_1, w_2, \dots, w_n$ of E, such that

$a_1 w_1, a_2 w_2, \dots, a_m w_m$ is an R-basis of N

for some $m \leq n$ and $a_1 | a_2 | \dots | a_m$ $(a_i \neq 0)$

Set $a_{m+1} = \dots = a_n = 0$

Then

$$\begin{array}{ccc} E & \xrightarrow{\alpha_1 w_1 + \dots + \alpha_n w_n \;\mapsto\; (\bar\alpha_1, \dots, \bar\alpha_n)} & \\ \downarrow \pi & \searrow^{\psi} & \\ E/N & \xrightarrow[\tilde\psi]{\sim} & R/(a_1) \oplus \dots \oplus R/(a_m) \oplus \underbrace{R/(a_{m+1}) \oplus \dots \oplus R/(a_n)}_{\cong\, R^r} \end{array}$$

$$\bar x = \overline{\alpha_1 w_1 + \dots + \alpha_n w_n} \xmapsto{\tilde\psi} (\bar\alpha_1, \dots, \bar\alpha_n) \in \bigoplus_{i=1}^{n} R/(a_i)$$

Clearly, $N \subset \operatorname{Ker}\psi$ ⇝ we get $\tilde\psi : E/N \to \bigoplus_{i=1}^{n} R/(a_i)$

- $\tilde\psi$ is surjective (since α_i can take any value in R)
- $\tilde\psi$ is injective. Indeed, if $(\bar\alpha_1, \dots, \bar\alpha_n) = 0$ then $\alpha_i \in (a_i) \Rightarrow \alpha_i = a_i \beta_i$ for some β_i

$\Rightarrow \alpha_i w_i \in N \quad \forall i = 1, \dots, r \Rightarrow x \in N \Rightarrow \bar x = 0$

It follows that $\tilde\psi$ is an isomorphism and

$$M \simeq \bigoplus_{i=1}^{r} R \oplus \bigoplus_{i=1}^{n} R/(a_i)$$

$$M \simeq R/(a_1) \oplus R/(a_2) \oplus \dots \oplus \underbrace{R/(a_{m+1}) \oplus \dots \oplus R/(a_n)}_{\cong R^r,\ r = n-m}$$

$R/(a_i)$ can be 0, if a_i is a unit in R.

In this case we just skip this summand from the direct sum.

Uniqueness

$K = Q(R)$ quotient field of R, $Q(R) = \{\frac{a}{b} \mid a \in R, b \in R, b \neq 0\}$

$r = \dim_K (\underbrace{K \otimes_R M}_{K\text{-vector space}})$ (Indeed, $Q(R) \otimes_R R \simeq Q(R)$, $Q(R) \otimes_R R/(a_i) = 0$)

Exercise: Show the uniqueness of (a_i) & m. ∎

Remark 6.77

- $\operatorname{Tors} M \simeq \bigoplus_{i=1}^{m} R/(a_i)$
- $a_1, \ldots, a_m$ are called invariant factors of M
- Using Chinese Remainder Theorem

$$a_i = \prod_{j=1}^{k} p_j^{e_j} \quad \text{with } p_j \text{ primes}$$

$$R/(a_i) \simeq \bigoplus_{j=1}^{k} R/(p_j^{e_j})$$

We get the following variant of the above Structure Theorem

$$M \simeq R^r \oplus \bigoplus_{(p) \in \operatorname{Spec} R} \bigoplus_{i=1}^{n(p)} R/(p^{e_i})$$

with $1 \leq e_1 \leq \ldots \leq e_{n(p)}$,

where $n(p), e_i$ are uniquely determined (p^{e_i} are called elementary divisors of M)

Remark 6.78 (Applications of Structure Theorem)

- Exercise: Let K be a field.
  Then any finite subgroup of K^* is cyclic
  (K^*: multiplicative group of K.)

- Exercise: K algebraically closed
  V finite dim. K-vector space
  $\varphi : V \longrightarrow V$ K-endomorphism

Consider V as $K[X]$-module
(via $X.v = \varphi(v)$ for $v \in V$)

and deduce from Corollary 6.76 the existence of the Jordan normal form of φ.