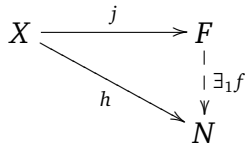
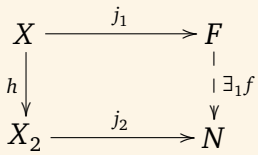
47 Free modules

Let R be a ring, F a right R–module, X a set and $j : X \longrightarrow F$ a map. We say F si **free** over $j : X \longrightarrow F$ if for any right R–module N and any map $h : X \longrightarrow N$ there is a unique module map $f : F \longrightarrow N$ such that $h = f \circ j$, i.e., the following diagram commutes.



Lemma. 47.1.
Let F_i be a free right R–module over $j_i : X_i \longrightarrow F_i$, for $i = 1, 2$. If $h : X_1 \longrightarrow X_2$ is a map, there exists a unique module map $f : F_1 \longrightarrow F_2$ making commutative the following diagram



Lemma. 47.2.
Let F_i be a free right R–module over $j_i : X_i \longrightarrow F_i$, for $i = 1, 2$. If $|X_1| = |X_2|$ then $F_1 \cong F_2$.

If F is a free right R–module over $j : X \longrightarrow F$, then j is a one to one map, hence we may consider that F is free over the subset $\mathrm{Im}(j)$, hence we may restrict to consider free right R–modules over subsets.

PROOF. If j is not injective there are $x, y \in X$ such that $j(x) = j(y)$, we define $h : X \longrightarrow R$ such that $h(y) = 0$ and $h(x) = 1$ for any $x \in X \setminus \{y\}$. There is a module map $f : F \longrightarrow R$ such that $fj = h$, hence $0 = h(y) = fj(y) = fj(x) = 0$, which is a contradiction. □

The subset $\mathrm{Im}(j) \subseteq F$ is called a **basis** of F.

As a consequence, over each set X there is a unique free module F, and two sets with the same cardinality define isomorphic free modules.

2107-01.tex

We can build F as follows. We define $F = \oplus\{R_x \mid x \in X,\ R_x = R, \text{ for any } x \in X\} = R^{(I)}$, and $j : X \longrightarrow F$ as $j(x) = e_x$, where $e_x = (\delta_{x,y})_y$. In this way we may identify X with the subset $\{e_x \mid x \in X\}$.

Proposition. 47.3.
With the above notation F is a free right R–modulo on X.

As a consequence for every free right R–module there is a set X such that $F \cong R^{(X)}$, a direct sum of copies of R.
A very useful property of free modules is the following one.

Theorem. 47.4.
Every right R–module is a quotient of a free right R–module, hence of a direct sum of copies of R.

The bases of free modules can be characterized thought arithmetical properties.
A subset $X \subseteq M$ of a right R–module M is **linearly independent** if for any R–linear combination of elements of X, for instance $\sum_{i=1}^{t} x_i a_i = 0$, we have $a_1 = \cdots = a_t = 0$. A subset that is not linearly independent is called **linearly dependent**. In the example of $R^{(I)}$ the subset $\{e_x \mid x \in X\}$ is a basis.

Lemma. 47.5.
For any right R–module F and any subset $X \subseteq F$, the following statements are equivalent:
(a) X is a basis of M.
(b) X linearly independent system of generators.

PROOF. (a) $\Rightarrow$ (b). It is clear as $F \cong R^{(I)}$ with basis $\{e_x \mid x \in X\}$.
(b) $\Rightarrow$ (a). If $X \subseteq F$ is a linearly independent system of generators, we consider $\oplus_x xR$ and the map $f : \oplus_x xR \longrightarrow F$ defined $f((r_x)_x) = \sum\{xr_x \mid x \in X\}$. Thus f is a surjective module map, as X is a system of generators, and it is injective, as X is linearly independent. □

Corollary. 47.6.
If F is a free right R–module on X, each element of F is written, in a unique way, as an R–linear combination of elements of X.

Exercise. 47.7.
Let M be a right R–module, and $B \subseteq M$ a subset. Show the the following statements are equivalent:
(a) B is a basis of M.
(b) Every element $m \in M$ is written in a unique way as a R–linear combination of elements of B.

We assume that the zero module has basis equal to $\emptyset$. For nonempty bases we have the following properties:

(1) If $B \subseteq M$ is a basis of M and $b \in B$, from the relationship "if $br = 0$ then $r = 0$"; we deduce that $b \neq 0$.
(2) If for $b \in M$ there exists $0 \neq r \in R$ such that $br = 0$, then b is not an element of any basis of M.

Now we can relate bases and independent families of submodules of a right module.

Lemma. 47.8.
Let M be a right R–module and $B \subseteq M$ a nonempty subset, the following statements are equivalent:
(a) B is a basis of M.
(b) $\{b_iR \mid b_i \in B\}$ is an independent family of submodules of M, $\sum_i b_iR = M$, and for any $b \in B$, if $br = 0$ then $r = 0$.
(c) $M = \oplus_i b_iR$ and for any $b \in B$, if $br = 0$ then $r = 0$.

PROOF. First we point out that $\{b_i \mid b \in B\}$ is a system of generators of M.

(a) $\Rightarrow$ (b). Each bR is non–zero and if $b_0R \cap (b_1R + \cdots + b_tR) \neq 0$, there exist $r_0, \ldots, r_T \in R$ such that $0 \neq b_0r_0 = \sum_{i=1}^{t} b_ir_i \in b_0R \cap (b_1R + \cdots + b_tR)$, i.e., $\sum_{i=1}^{t} b_ir_i - b_0r_0 = 0$, hence $r_0 = r_1 = \cdots = r_t = 0$.

(b) $\Rightarrow$ (a). Let us assume that the family $\{b_iR \mid i \in I\}$ is independent, and take $b_1r_1 + \cdots + b_tr_t = 0$. If $t = 1$ then $b_1r_1 = 0$, hence $r_1 = 0$. If $t \geq 1$ and $r_t \neq 0$ then $-b_tr_t = b_1r_1 + \cdots + b_{t-1}r_{t-1} \in b_tR \cap (b_1R + \cdots + b_{t-1}R) = 0$, hence $b_tr_t = 0$, and $r_t = 0$. Applying the same argument to every index we get $r_1 = \cdots = r_t = 0$. □

In general we can not assure for a subset $B \subseteq M$ that if $\{bR \mid b \in B\}$ is an independent family of submodules generating M then B is a basis.

Example. 47.9.
Let $R = \mathbb{Z}$ and $M = \mathbb{Z}_2$; it is clear that $\{M = \langle\overline{1}\rangle\}$ is an independent family of submodules, but $\{\overline{1}\}$ is not a basis as $\overline{1} \cdot 2 = 0$ and $2 \neq 0$.

Modules over division rings

Free modules are useful to characterize some kind of rings; in this case **division rings**, i.e., rings in which every non–zero element has a let an right inverse.

Proposition. 47.10.
If D is a división ring every right D–module is free.

PROOF. it is enough to show that every non–zero right D–module has a basis. Let M be a non–zero right D–module, we define

$$\Gamma = \{\{b_iD \mid i \in I\} \mid \{b_iD \mid i \in I\} \text{ es una familia de submódulos no nulos independiente}\}.$$

We claim $\Gamma \neq \emptyset$. Since $M \neq 0$, there exists $0 \neq m \in M$, and $\{mD\}$ es indpendent.
For any chain in Γ a upper bound is the union; by Zorn's lemma there exists a maximal element in Γ, say $\{b_iD \mid i \in I\} \in \Gamma$. If $\oplus_i b_iD \neq M$, there exists $x \in M \setminus \oplus_i b_iD$. If $xD \cap \oplus_i b_iD \neq 0$, there exists $0 \neq d \in D$ such that $0 \neq xd \in \oplus_i b_iD$, hence $x = xdd^{-1} \in \oplus_i b_iD$, which is a contradiction. Therefore, $M = \oplus_i b_iD$.
By Lemma (47.8.) we know that $\{b_i \mid i \in I\}$ is a basis if $r = 0$ whenever $b_ir = 0$ for any b_i; this is a consequence of D to be a division ring. Thus $\{b_i \mid i \in I\}$ is a basis, and M is a free right D–module. □

the converse of this Proposition also holds.

Theorem. 47.11.
Let R be a ring, if every right R–module is free, then R is a division rings.

PROOF. We show R has no non–zero proper right ideals. Let $\mathfrak{m} \subseteq R$ be a maximal right ideal, then $M = R/\mathfrak{m}$ is a simple right R–module and, by the hypothesis, it is free.
Let B be a basis of M, since M is simple, for any $b \in B$ we have $M = \langle b \rangle = bR$. Hence, for every $c \in B \setminus \{b\}$ there exists $r \in R$ such that $c = br$, which is a contradiction; Thus $B = \{b\}$ is unitary. Therefore, there exists a right module isomorphism $\theta : R \longrightarrow M$, defined $\theta(r) = br$, and R is a simple right R–module derecha, i.e., R has no non–zero proper right ideals.
To show that R is a division ring let $0 \neq r \in R$, since $rR = R$, there exists $s \in R$ such that $rs = 1$, i.e., r has a right inverse. Since $0 \neq r$, the annihilator $\mathrm{Ann}_R^r(r) = \{x \in R \mid rx = 0\} \neq R$ is a proper ideal, hence $\mathrm{Ann}_R^r(r) = 0$. Since $rsr = r$ then $r(sr - 1) = 0$, and $sr = 1$, i.e., r is invertible. □

Exercise. 47.12.
Let R be a ring, show that if every non–zero element of R has a right inverse, then R is a division ring.

SOLUTION. Let $0 \neq a \in R$, there exists $b \in R$ such that $ab = 1$. Therefore, $aba = a$, and $a(ba-1) = 0$. If $ba - 1 = 0$, then $ba = 1$, and a is invertible. If $ba - 1 \neq 0$, there exists a right inverse, and $a = 0$, which is a contradiction. □

48 Módulos libres finitamente generados

Módulos finitamente generados

Dado un R–módulo derecha M dar una **presentación libre** de M es dar un módulo derecha libre F y un submódulo K tal que $F/K \cong M$, o equivalentemente dar un homomorfismo sobreyectivo de un módulo derecha libre a M.

Una presentación libre se llama **finita** cuando tanto F con K son finitamente generados. En este caso si F está generado por $\{f_1,\dots,f_t\}$ y K está generado por $\{k_1,\dots,k_s\}$, siendo $k_j = \sum_i f_i a_i$, representamos el módulo M como $M = \langle f_1,\dots,f_t \mid \sum_i f_i a_i = 0\rangle$.

En particular un R–módulo derecha es finitamente generado si, y sólo si, es un cociente de una suma directa finita de copias de R y advierte que un módulo finitamente generado no tiene que tener una presentación libre finita.

Remark. 48.1.
Puede ser que dos módulos derecha libres F_1, F_2 sobre conjuntos X_1, X_2 sean isomorfos y que X_1 y X_2 no sean biyectivos.

Consideramos un cuerpo K, y V un espacio vectorial sobre K de dimensión numerable. Llamamos $R = \mathrm{End}_K(V)$. Tenemos que R es un anillo no conmutativo. Vamos a ver que $R \cong R \oplus R$, pero R es libre sobre $\{1\}$ y $R \oplus R$ es libre sobre $\{(1,0),(0,1)\}$ no son conjuntos biyectivos.

Basta definir $f : R \to R \oplus R$ mediante $f(\varphi) = (\varphi_1, \varphi_2)$, siendo $\varphi_1 : V \to V$ mediante $\varphi_1(e_i) = \varphi(e_{2i})$ y $\varphi_2 : V \to V$ mediante $\varphi_2(e_i) = \varphi(e_{2i+1})$. La aplicación inversa de f es $g : R \oplus R \to R$ definida por $g(\phi_1, \phi_2) = \phi$ definida por $\phi(e_i) = \begin{cases} \phi_1(e_j) & \text{si } i = 2j \\ \phi_2(e_j) & \text{si } i = 2j+1 \end{cases}$

Un anillo R se dice que tiene un **número de base invariante (IBN)** si $R^r \cong R^t$ entonces $r = t$ para $r, t \in \mathbb{N}$.

Para el caso infinito la situación es más sencilla.

Proposition. 48.2.
Si I es un conjunto infinito, para cualquier conjunto J tal que $R^{(I)} \cong R^{(J)}$ se tiene que $|I| = |J|$.

Ver la demostración en la Proposición (48.11.).

2107-02.tex

Homomorfismos entre módulos libres finitamente generados

Cada R–módulo derecha libre finitamente generado F es isomorfo a una suma directa R^n de copias del anillo R, por lo que el estudio de los homomorfismos entre dos R–módulos derecha libres finitamente generados se reduce al estudio de homomorfismos entre sumas directas finitas de copias de R. Observa que el isomorfismo $F \cong R^n$ se establece fijando una base de F, por lo que tomando bases distintas podemos tener isomorfismos $F \cong R^n$ distintos.

Como cada endomorfismo de R está definido por un elemento $a \in R$, el estudio de los endomorfismos entre módulos libres finitamente generados se reduce al estudio de matrices con coeficientes en R.

Representamos por $M_{n\times m}(R)$ el conjunto de las matrices con coeficientes en R con n filas y m columnas. Por simplicidad el conjunto $M_{n\times n}(R)$ se representa por $M_n(R)$. Un elemento de $M_{n\times m}(R)$ se representa por

$$(a_{ij})_{ij} = \begin{pmatrix} a_{11} \cdots a_{1m} \\ \vdots \ \ddots \ \vdots \\ a_{n1} \cdots a_{nm} \end{pmatrix}$$

El conjunto $M_{n\times m}(R)$ tiene estructura de R–módulo derecha e izquierda y el conjunto $M_n(R)$ tiene estructura de R–álgebra, aunque no conmutativa. Entonces $M_{n\times m}(R)$es un $M_n(R)$–módulo izquierda, y un $M_m(R)$–módulo izquierda.

Al considerar la estructura multiplicativa de $M_n(R)$ aparece de forma natural el **grupo lineal general**, $GL_n(R)$, que es el grupo de las matrices invertibles.

Lemma. 48.3.
Dadas dos matrices X e Y en $M_{n\times m}(R)$ que representan el mismo endomorfismo respecto a distintas bases, existen matrices invertibles $P \in M_n(R)$ y $Q \in M_m(R)$ tales que $X = PYQ$.

Dos matrices X e Y en la situación del lema se llaman matrices **equivalentes**. Es claro que la relación "equivalente a" es una relación de equivalencia en $M_{n\times m}(A)$.

Lemma. 48.4.
Dadas dos matrices X e Y en $M_n(R)$, que representan el mismo endomorfismo respecto a distintas bases, existe una matriz invertible P tal que $Y = PXP^{-1}$.

Dos matrices X e Y en la situación del lema se llaman matrices **semejantes**. Es claro que la relación "semejante a" es una relación de equivalencia en $M_n(R)$.

Anillos IBN

Un anillo R es **IBN** (derecha), tiene número base invariante, si para cada $n, m \in \mathbb{N}$ si $R^n \cong R^m$, como módulos derecha, se tiene $n = m$. Esto es, todas las bases de un R–módulo derecha finitamente generado tienen el mismo cardinal.

Lemma. 48.5.
Sea R un anillo, y $n, m \in \mathbb{N}$. Son equivalentes:
(a) $R^n \cong R^m$.
(b) Existen matrices $A \in M_{n\times m}(R)$, $B \in M_{m\times n}(R)$ tales que $AB = id_n$ y $BA = id_m$.

PROOF. Un homomorfismo $\theta : R^n \longrightarrow R^m$ está determinado por una matriz $B \in M_{m\times n}(R)$, y uno $\eta : R^m \longrightarrow R^n$ por una matriz $A \in M_{n\times m}(R)$. El resultado es claro. □

Proposition. 48.6.
Tenemos entonces que para cada anillo R los siguientes resultados son equivalentes:
(a) R no es IBN.
(b) Existen $n, m \in \mathbb{N}$ tales que $n \neq m$ y $R^n \cong R^m$.
(c) Existen $n, m \in \mathbb{N}$ tales que $n \neq m$ y matrices $A \in M_{n\times m}(R)$, $B \in M_{m\times n}(R)$ tales que $AB = id_n$ y $BA = id_m$.

El siguiente resultado también es inmediato.

Corollary. 48.7.
Sea R un anillo, se verifica:
(1) Si R es IBN, entonces $M_n(R)$ es un anillo IBN.
(2) Si R no es IBN y $f : R \longrightarrow S$ es un homomorfismo de anillos, entonces S no es IBN.
(3) Ningún cociente de un anillo que no es IBN es IBN.

Corollary. 48.8.
Todo anillo conmutativo es IBN.

PROOF. Como todo cuerpo es IBN, y como todo anillo conmutativo tiene un cociente que es un cuerpo, resulta que todo anillo conmutativo es IBN. □

No todo anillo es IBN como el siguiente ejemplo prueba.

Example. 48.9.
Sea K un cuerpo y V un espacio vectorial de dimensión infinita, por ejemplo $V = K^{(\mathbb{N})}$. Llamamos $R = \mathrm{End}_K(V)$; vamos a ver que R no es IBN. Basta ver que $R \cong R^2$. Tomamos $\{e_n \mid n \in \mathbb{N}\}$ una base de V. Se define $\eta : R^2 \longrightarrow R$ mediante

$$\eta(f_0, f_1)(e_n) = \begin{cases} f_0(e_{n/2}) & \text{si } n \text{ es par.} \\ f_1(e_{(n-1)/2}) & \text{si } n \text{ es impar.} \end{cases}$$

Es claro que η es un homomorfismo de R–módulos inyectivo. Por otro lado, dado $f \in R$, se definen

$$g_0(e_n) = f(e_{2n}).$$
$$g_1(e_n) = f(e_{2n+1}).$$

Se tiene

$$\eta(g_0, g_1)(e_n) = \begin{cases} g_0(e_{n/2}) = f(e_n) & \text{si } n \text{ es par.} \\ g_1(e_{(n-1)/2}) = f(e_{2\frac{n-1}{2}+1}) = f(e_n) & \text{si } n \text{ es impar.} \end{cases}$$

También podemos definir $\theta : R \longrightarrow R^2$ mediante $\theta(f) = (g_0, g_1)$, y comprobar $\eta\theta = \mathrm{id}$ y $\theta\eta = \mathrm{id}$.

Proposition. 48.10.
Todo anillo de división es IBN.

PROOF. Sean $n, m \in \mathbb{N}$ tales que $D^n \cong D^m$. Supongamos que $n < m$, y sean $x_1, \ldots, x_n$ y $y_1, \ldots, y_m$ bases. Existe una combinación $y_1 = x_1 d_{1,1} + \cdots + x_n d_{n,1}$, con algún $d_{j,1} \neq 0$, entonces podemos sustituir x_j por y_1 y tenemos un sistema de generadores $\{x_1, \ldots, \widehat{x_j}, \ldots, x_n\} \cup \{y_1\}$. Existe una combinación $y_2 = x_1 d_{1,2} + \cdots + \widehat{x_j d_{j,2}} + \cdots + x_n d_{n,2} + y_1 d_{n+1,2}$, en la que algún $d_{h,2}$ es no nulo, ya que no existe una combinación lineal no trivial de los y_i. En este caso sustituimos x_h por y_2, y seguimos teniendo un sistema de generadores. Repitiendo este proceso llegamos a que basta con n de los y_i para generar D^m, lo que es una contradicción. Por tanto $n \geq m$, y del mismo modo $m \geq n$, por lo que se tiene $n = m$. □

El problema de la cardinalidad surge solamente en el caso finitamente generado, ya que para módulos no finitamente generados se tiene:

Proposition. 48.11.
Si R es un anillo y F es un R–módulo derecha libre con una base infinita, entonces cada dos bases de F tienen el mismo cardinal.

PROOF. Supongamos que $\mathscr{B} = \{x_h \mid h \in H\} \subseteq F$ es una base infinita de F.
Si $\mathscr{D} = \{y_1, \ldots, y_t\}$ es una base finita, para cada y_k existe $\mathscr{B}_k \subseteq \mathscr{B}$, finito, tal que $y_k \in \langle \mathscr{B}_k \rangle$, por tanto $\cup_k \mathscr{B}_k$ es un sistema de generadores, y es finito, lo que es una contradicción.
Si $\mathscr{D} = \{y_k \mid k \in K\}$ es una base infinita, para cada y_k consideramos $\mathscr{B}_k \subseteq \mathscr{B}$, finito, tal que $y_k \in \langle \mathscr{B}_k \rangle$. Tenemos así una aplicación $\nu : \mathscr{D} \longrightarrow \mathscr{P}_F(\mathscr{B})$, el conjunto de las partes finitas de $\mathscr{B}$. Del mismo modo podemos construir una aplicación $\theta : \mathscr{B} \longrightarrow \mathscr{P}_F(\mathscr{D})$.
Para cada $S \in \mathscr{P}_F(\mathscr{B})$ el conjunto $\nu^{-1}(S) \subseteq \mathscr{D}$ es finito. En efecto, se tiene $\langle \nu^{-1}(S) \rangle \subseteq \langle S \rangle$. Por otro lado, $\langle S \rangle \subseteq \langle \theta(S) \rangle$, y juntando estas inclusiones tenemos:

$$\langle \nu^{-1}(S) \rangle \subseteq \langle S \rangle \subseteq \langle \theta(S) \rangle.$$

En consecuencia $\nu^{-1}(S) \subseteq \theta(S)$ y es un conjunto finito.
Consideramos en $\mathscr{D}$ la relación de equivalencia dada por $y_k \sim y_{k'}$ si $\nu(y_k) = \nu(y_{k'})$, como cada clase de equivalencia tiene un número finito de elementos, resulta que $\operatorname{card}(\mathscr{D}) = \operatorname{card}\left(\frac{\mathscr{D}}{\sim}\right)$. Por otro lado, existe una aplicación inyectiva $\frac{\mathscr{D}}{\sim} \xrightarrow{\nu} \mathscr{P}_F(\mathscr{B})$, y por tanto $\operatorname{card}(\mathscr{D}) = \operatorname{card}\left(\frac{\mathscr{D}}{\sim}\right) \leq \operatorname{card}(\mathscr{P}_F(\mathscr{B})) = \operatorname{card}(\mathscr{B})$. Del mismo modo tendríamos $\operatorname{card}(\mathscr{B}) \leq \operatorname{card}(\mathscr{D})$, y los dos cardinales coinciden. □

Exercise. 48.12.
Sea F un R–módulo derecha libre con base X de cardinal infinito $|X|$. Prueba que cada subconjunto $Y \subseteq F$, de cardinal $|Y| < |X|$, está contenido en un sumando directo propio de F.

SOLUTION. Dado $y \in Y$, existe una expresión (única) $y = \sum_x x r_x$, con $x \in X$ y $r_x \in R$. Definimos entonces $A(y) = \{x \in X \mid r_x \neq 0\}$, que por construcción es un conjunto finito, por tanto $Z = \cup\{A(y) \mid y \in Y\}$ es un conjunto de cardinal $|Y| < |X|$. Tenemos entonces la siguiente descomposición de F:

$$F = (\oplus\{R \mid x \in Z\}) \oplus (\oplus\{R \mid x \in X \setminus Z\}),$$

y tenemos $Y \subseteq \oplus\{R \mid x \in Z\}$. □

Ya que el concepto IBN es un concepto definido para un lado, en este caso la derecha, cabe preguntarse si es o no un concepto bilátero.

Exercise. 48.13.
Sea R un anillo, prueba que son equivalentes:
(a) R es un anillo IBN derecha.
(b) R es un anillo IBN izquierda.

SOLUTION. Sea M un R–módulo derecha libre finitamente generado con base $\{e_1,\dots,e_t\}$, entonces $\{e_1^*,\dots,e_t^*\} \in M^* = \mathrm{Hom}_R(M,R)$ es una base del R–módulo izquierda M^*, (aquí se tiene $e_i^*(e_j) = \delta_{i,j}$). En efecto, si $\sum_i r_i e_i^* = 0$, para cada e_j se tiene

$$0 = \left(\sum_i r_i e_i^*\right)(e_j) = \sum_i \left(r_i e_i^*\right)(e_j) = \sum_i r_i \delta_{i,j} = r_j,$$

y es un sistema de generadores, pues dado $f \in M^*$, se tiene $f = \sum_i f(e_i) e_i^*$, ya que

$$\left(\sum_i f(e_i) e_i^*\right)(e_j) = f(e_j).$$

Análogamente tendremos que $\{e_1^{**},\dots,e_t^{**}\}$ es una base de M^{**}.
Existe un isomorfismo $\nu : M \longrightarrow M^{**}$, definido $\nu(m)(e_j^*) = e_j(m)$, para cada $m \in M$. Por tanto $\nu(e_i)(e_j^*) = e_j(e_i) = \delta_{j,i}$; esto es, $\nu(e_i) = e_i^{**}$ para caa índice i, y resulta que ν es un isomorfismo de R–módulo derecha, ya que lleva una base de M a un abase de M^{**}.
Se considera ahora dos R–módulos izquierda N_1 y N_2 libres y finitamente generados con bases formadas por d_1 y d_2 elementos, respectivamente. Tenemos que N_1^* y N_2^* son R–módulos derecha libres con bases formadas por d_1 y d_2 elementos, respectivamente. Si $N_1 \cong N_2$, entonces $N_1^* \cong N_2^*$, y $d_1 = d_2$; por lo tanto R es un anillo IBN izquierda. □

Exercise. 48.14.
Sea R un anillo verificando una condición de cadena (ascendente o descendente), prueba que R es un anillo IBN.

SOLUTION. Supongamos que R es un anillo artiniano derecha y que $R^n \overset{\nu}{\cong} R^m$, para $n,m \in \mathbb{N}$. Si $n < m$, entonces $R^n \overset{\alpha}{\cong} N_1 \subsetneqq R^m$. Como $N_1 \overset{\alpha^{-1}}{\cong} R^n \overset{\nu}{\cong} R^m$, podemos repetir el proceso, y encontrar un submódulo $N_2 \subsetneqq N_1$ definido por la relación:

$$R^n \overset{\alpha}{\cong} N_2 \subsetneqq R^m \overset{\nu^{-1}}{\cong} R^n \overset{\alpha}{\cong} N_1.$$

Este proceso podemos iterarlo tantas veces como sea necesario para obtener una cadena estrictamente descendente de submódulos de R^m, que es artiniano ya que R lo es, lo que es una contradicción.
Supongamos que R es un anillo noetheriano derecha y que $R^n \overset{\nu}{\cong} R^m$, para $n,m \in \mathbb{N}$. Si $n < m$, existe un submódulo propio $N_1 \subsetneqq R^m$ tal que $R^m/N_1 \overset{\alpha}{\cong} R^n \overset{\nu}{\cong} R^m$. Reiterando el proceso, encontramos $N_2 \supsetneqq N_1$ verificando

$$\frac{R^m}{N_2} \cong \frac{R^m/N_1}{N_2/N_1} \cong \frac{R^m}{N_1} \cong R^m.$$

Tenemos de este modo una cadena estrictamente ascendente de submódulos de R^m, lo que es una contradicción, pues R^m es noetheriano. □

Miscelánea

Sea X un conjunto y $\mathscr{F} \subseteq \mathscr{P}(X)$, una familia de subconjuntos de X. Una subfamilia $\mathscr{N} \subseteq \mathscr{F}$ se llama un **encaje** si para cualesquiera $A, B \in \mathscr{N}$, se tiene $A \subseteq B$ ó $B \subseteq A$.
Un encaje $\mathscr{N} \subseteq \mathscr{F}$ se llama **maximal** si

- $\mathscr{N} \neq \mathscr{F}$, y
- para cualquier otro encaje $\mathscr{N}'$ tal que $\mathscr{N} \subsetneq \mathscr{N}' \subseteq \mathscr{F}$, se tiene $\mathscr{N}' = \mathscr{F}$.

La siguiente propiedad la imponemos como axioma de nuestra teoría: *Para cada conjunto X, y cada familia de subconjuntos $\mathscr{F}$, existe al menos un encaje maximal contenido en $\mathscr{F}$.*

Un subconjunto $X \subseteq M$ de un R–módulo derecha M se llama **independiente** si la familia de submódulos $\{xR \mid x \in X\}$ es independiente.
Un subconjunto $X \subseteq M$ de un R–módulo derecha M se llama **uniformemente independiente** si

- es independiente, y
- para cada $x \in X$, el submódulo xR es uniforme.

Y se llama **simplemente independiente** si

- es independiente, y
- para cada $x \in X$, el submódulo xR es simple.

Lemma. 48.15.
Sea $\mathscr{F} \subseteq \mathscr{P}(X)$ un encaje de un R–módulo derecha M. Se verifica:

(1) Si cada elemento de $\mathscr{F}$ es un conjunto independiente, entonces $\cup\mathscr{F}$ es independiente.
(2) Si cada elemento de $\mathscr{F}$ es un conjunto uniformemente independiente, entonces $\cup\mathscr{F}$ es uniformemente independiente.
(3) Si cada elemento de $\mathscr{F}$ es un conjunto simplemente independiente, entonces $\cup\mathscr{F}$ es simplemente independiente.

PROOF. (1). Supongamos que $\mathscr{F} = \{X_i \mid i \in I\}$ es un encaje y que cada X_i es un conjunto independiente; llamamos $X = \cup_i X_i$, vamos a ver que X es independiente. Dados $x_0, \ldots, x_t \in X$, existe un índice j tal que $x_0, \ldots, x_t \in X_j$, luego $\{x_0, \ldots, x_t\}$ es un conjunto independiente.
(2) y (3). Son inmediatos. □

Theorem. 48.16.
Para cada R–módulo derecha M se tiene que:

(1) existe un subconjunto independiente maximal.
(2) existe un subconjunto uniformemente independiente maximal.
(3) existe un subconjunto simplemente independiente maximal.

PROOF. (1). Consideramos $\mathscr{F}$ la familia de todos los subconjuntos de M que son independientes; esta familia es no vacía, ya que el conjunto vacío es independiente, y es inductive. Aplicando el lema de Zorn tiene al menos un elemento maximal. Éste es el elemento que andamos buscando.

Un método alternativo consiste en utilizar la propiedad anterior sobre existencia de encajes maximales; por él existe en $\mathscr{F}$ un encaje maximal, y la unión de sus elementos es el subconjunto buscado.

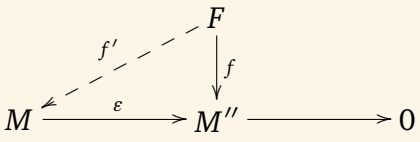
(2) y (3). Son inmediatos. □

Un posible nuevo invariante de un R–módulo M es el cardinal de estos subconjuntos.

49 Projective modules

Let F be a free right R–module, in order to give properties similar to freeness inner to the category of modules we prove the following result.

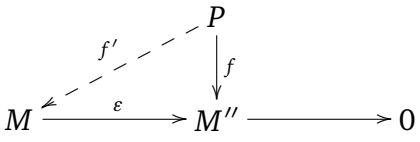
Proposition. 49.1.
Let F be a free right R–module, for any epimorphism $\varepsilon : M \longrightarrow M''$ and any module map $f : F \longrightarrow M''$ there is a module map $f' : F \longrightarrow M$ such that $f = \varepsilon f'$.



PROOF. Let $B \subseteq F$ be a basis, for any $b \in B$ we take $m \in M$ such that $\varepsilon m) = f(b)$, and define f' such that $f'(b) = m$. □

Now, using this property, we introduce a new notion for modules.

A right R–module P is **projective** if for every epimorphism $M \xrightarrow{\varepsilon} M'' \to 0$ and every module map $f : P \to M$" there is a module map $f' : P \to M$ such that $f = \varepsilon \circ f'$.



Proposition. 49.2.
For any ring R and any right R–module P the following statements are equivalent:
(a) P is projective.
(b) The functor $\mathrm{Hom}_R(P,-)$ is exact.
(c) Every epimorphism $X \to P \to 0$ splits.
(d) P is a direct summand of a free right R–module.

As a consequence we have:

2107-03.tex

Proposition. 49.3.
For any ring R and any family of right R–modules $\{P_i \mid i \in I\}$ the following statements are equivalent:
(a) $\oplus_i P_i$ *is projective.*
(b) Every P_i *is projective.*

In particular we have the following:

Corollary. 49.4.
For any ring R the following statements are equivalent:
(a) Every short exact sequence of right R–modules splits.
(b) Every right R–module is projective.

Observe that conditions in Corollary (49.4.) are equivalent conditions for R to be (artinian) semisimple ring.

Rings characterized by projective modules

As we have seen before division rings are characterized as those all whose right R–modules are free, due to the fact that free module is not a categorical notion, we are interested in determining all rings such that its category of right modules is equivalent to the category of right modules over a división ring. In this way first we observe that projective module is a categorical notion and that it extends, in some sense, the notion of free module, hence we will characterize those rings R such that all modules in **Mod**–R are projective. We will show that these rings are direct product of matrices rings with coefficients in división rings.
Our first result assures that simple module are everywhere.

Lemma. 49.5.
Let R be a ring such that every right R–module is projective, then every non–zero module contains a simple submodule.

PROOF. If $M \neq 0$ we take $0 \neq m \in M$, then mR contains a maximal submodule, say $L \subseteq mR$, hence $mR \cong L \oplus \frac{mR}{L}$. Since $\frac{mR}{L}$ is simple, we have the result. □

We will collect all simple submodules of a given right module M, thus we define $\mathrm{Soc}(M) = \sum\{H \subseteq M \mid H \text{ simple}\}$. A right R–module M is **semisimple** if $M = \mathrm{Soc}(M)$.

Lemma. 49.6.
Let R be a ring such that every right R–module is projective, then for every right R–module M we have:

(1) every submodule of M is a direct summand.
(2) M is semisimple.

PROOF. (1). By the hypothesis every short exact sequence splits.
(2). By the hypothesis we have that $\mathrm{Soc}(M) \subseteq M$ is a direct summand, and since every non–zero module contains a simple submodule, then $\mathrm{Soc}(M) = M$. □

As a consequence we have:

Theorem. 49.7.
Let R be a ring, the following statements are equivalent:

(a) Every right R–module is projective.
(b) Every right R–module is semisimple.
(c) For every right R–module M every submodule is a direct summand.
(d) Every short exact sequence splits

In order to characterize these kind of rings we need to study more in detail semisimple right R–modules.

Maximal submodules

Let M be a right R–module, a **maximal submodule** N of M is a proper submodule $N \subsetneqq M$ such that for any submodule $N \subseteq H \subsetneqq M$ we have $N = H$.
It is well known that

Lemma. 49.8.
Every non–zero free right R–module contains a maximal submodule.

PROOF. Let $M = R^{(I)}$ be a non–zero free right R–module with basis $\{e_i \mid ; i \in I\}$If we fix $i_0 \in I$, we may consider the epimorphism $p : R^{(I)} \longrightarrow R$ defined $p(e_i) = 0$, if $i \neq i_0$, and $p(e_{i_0}) = 1$, hence, since R contains a maximal submodule, $\mathrm{Ker}(p)$ is contained in a maximal submodule. □

Our interest now is to show that every non–zero projective right R–module contains a maximal submodule.

Example. 49.9.
Observe that, in general, not any proper submodule of a free module is contained in a maximal submodule. Consider a free presentation of $\mathbb{Q}$ as abelian group: $\mathbb{Z}^{(I)} \xrightarrow{p} \mathbb{Q}$; the proper submodule $\mathrm{Ker}(p)$ is not contained in any maximal submodule, whenever $\mathbb{Q}$ has not simple quotients.

The Jacobson radical of any right R–module satisfies.

Lemma. 49.10.
For any right R–module M we have $M\,\mathrm{Jac}(R) \subseteq \mathrm{Jac}(M)$

PROOF. Since $\mathrm{Jac}(M)$ is the intersection of all maximal submodules of M, then $M/\mathrm{Jac}(M)$ is a submodule of a direct product of simple modules, hence $(M/\mathrm{Jac}(M))\,\mathrm{Jac}(R) = 0$, hence $M\,\mathrm{Jac}(R) \subseteq \mathrm{Jac}(M)$. □

The reverse inclusion does not hold in general. In the particular case of projective modules we have.

Lemma. 49.11.
For any projective right R–module M we have $\mathrm{Jac}(M) = M\,\mathrm{Jac}(R)$.

PROOF. We may assume there exist H and I such that $M + H \cong R^{(I)}$. Therefore,

$$\begin{aligned}\mathrm{Jac}(M) \oplus \mathrm{Jac}(H) = \mathrm{Jac}(M+H) = \mathrm{Jac}(R^{(I)}) = \mathrm{Jac}(R)^{(I)} = R^{(I)}\,\mathrm{Jac}(R)\\ = (M \oplus H)\,\mathrm{Jac}(R) = (M\,\mathrm{Jac}(R)) \oplus (H\,\mathrm{Jac}(R)).\end{aligned}$$

On the other hand, since $M\,\mathrm{Jac}(R) \subseteq \mathrm{Jac}(M)$, and $H\,\mathrm{Jac}(R) \subseteq \mathrm{Jac}(H)$, then $M\,\mathrm{Jac}(R) = \mathrm{Jac}(M)$.

□

Proposition. 49.12.
Every non–zero projective right R–module contains a maximal submodule.

PROOF. We only need to show that $\mathrm{Jac}(M) \neq M$, or equivalently, $M\,\mathrm{Jac}(R) \neq M$. If M is finitely generated, this is a consequence of Nakayama's lemma. In the general case we proceed as follows.

Let us assume $M \oplus H \cong R^{(I)}$, and let $\{e_i \mid i \in I\}$ be a basis of $R^{(I)}$. For any element $x \in M$ there is a linear combination $x = \sum_{i=1}^{n} e_i a_i$, for some $a_i \in R$.
If $M\,\mathrm{Jac}(M) = M$, let $p : R^{(I)} \longrightarrow M$ the projection, hence for any e_i we have $p(e_i) \in M$, and can be written as $p(e_i) = \sum_j e_j a_{ij}$ for some $a_{ij} \in \mathrm{Jac}(R)$, hence

$$x = p(x) = p(\sum_i e_i a_i) = \sum_i p(e_i) a_i = \sum_i \sum_j e_j a_{ij} a_i = \sum_j e_j \left(\sum_i a_{ij} a_i \right).$$

Since $\{e_i \ i \in I\}$ is a basis, then $a_j = \sum_i a_{ij} a_i$ for any j. We can write the latest expression as $\sum_i \delta_{ij} a_i = \sum_i a_{ij} a_i$, which written in matricial form is

$$\left(I - (a_{ij})_{ij}\right)(a_i)_i = 0.$$

Since $a_{ij} \in \mathrm{Jac}(R)$, then $(a_{ij})_{ij} \in M_n(\mathrm{Jac}(R)) = \mathrm{Jac}(M_n(R))$, and $I - (a_{ij})_{ij}$ is invertible. As a consequence $(a_i)_i = 0$, and $x = 0$. This means that $M = 0$, which is a contradiction. □