Álgebra II Práctica (clase 14)

Iván Sadofschi Costa

Universidad de Buenos Aires

12 de Junio de 2020

Prerrequisitos

Para leer estas diapositivas se recomienda haber leído el apunte teórico hasta 3.9 (inclusive).

Por qué nos interesan los módulos proyectivos?

- Abstraen lo estrictamente necesario para probar propiedades importantes que cumplen los grupos libres (porque libre implica proyectivo).

Por qué nos interesan los módulos proyectivos?

- Abstraen lo estrictamente necesario para probar propiedades importantes que cumplen los grupos libres (porque libre implica proyectivo).
- Tenemos que P es proyectivo si y solo si $\hom(P, -)$ preserva epimorfismos.

Por qué nos interesan los módulos proyectivos?

- Abstraen lo estrictamente necesario para probar propiedades importantes que cumplen los grupos libres (porque libre implica proyectivo).
- Tenemos que P es proyectivo si y solo si $\hom(P, -)$ preserva epimorfismos.
- Equivalentemente son los módulos que cumplen que para toda sucesión exacta
$$0 \to A \to B \to C \to 0$$
la sucesión
$$0 \to \hom(P, A) \to \hom(P, B) \to \hom(P, C) \to 0$$
es también exacta.

Por qué nos interesan los módulos proyectivos?

- Abstraen lo estrictamente necesario para probar propiedades importantes que cumplen los grupos libres (porque libre implica proyectivo).
- Tenemos que P es proyectivo si y solo si $\hom(P, -)$ preserva epimorfismos.
- Equivalentemente son los módulos que cumplen que para toda sucesión exacta
$$0 \to A \to B \to C \to 0$$
la sucesión
$$0 \to \hom(P, A) \to \hom(P, B) \to \hom(P, C) \to 0$$
es también exacta.
- P es proyectivo si y solo sí toda sucesión exacta
$$0 \to N \to M \to P \to 0$$
se parte (esto está dicho de otra forma en Proposición 3.8.4).

Algunos proyectivos que no son libres

- $R = \mathbb{Z}_6$, consideramos los submódulos $P, P' \subseteq R$ de orden 2 y 3. Tenemos que $R = P \oplus P'$ por lo tanto P y P' son proyectivos pero no libres.

Algunos proyectivos que no son libres

- $R = \mathbb{Z}_6$, consideramos los submódulos $P, P' \subseteq R$ de orden 2 y 3. Tenemos que $R = P \oplus P'$ por lo tanto P y P' son proyectivos pero no libres.
- El ejemplo que contó hoy Willie.

Algunos proyectivos que no son libres

- $R = \mathbb{Z}_6$, consideramos los submódulos $P, P' \subseteq R$ de orden 2 y 3. Tenemos que $R = P \oplus P'$ por lo tanto P y P' son proyectivos pero no libres.
- El ejemplo que contó hoy Willie.
- ¿Vimos algún ejemplo más?

Algunos proyectivos que no son libres

- $R = \mathbb{Z}_6$, consideramos los submódulos $P, P' \subseteq R$ de orden 2 y 3. Tenemos que $R = P \oplus P'$ por lo tanto P y P' son proyectivos pero no libres.
- El ejemplo que contó hoy Willie.
- ¿Vimos algún ejemplo más? ¿Qué pasa si miramos los submódulos de $\mathbb{R}[\mathbb{Z}_3]$?

El truco de Eilenberg-Mazur

Recordemos que P se dice proyectivo si existe un módulo Q tal que $P \oplus Q$ es libre. Esta es una de las definiciones usuales que podemos encontrar en los libros.

El truco de Eilenberg-Mazur

Recordemos que P se dice proyectivo si existe un módulo Q tal que $P \oplus Q$ es libre. Esta es una de las definiciones usuales que podemos encontrar en los libros.

Proposición

Si P es proyectivo entonces existe L libre tal que $P \oplus L$ es libre.

El truco de Eilenberg-Mazur

Recordemos que P se dice proyectivo si existe un módulo Q tal que $P \oplus Q$ es libre. Esta es una de las definiciones usuales que podemos encontrar en los libros.

Proposición

Si P es proyectivo entonces existe L libre tal que $P \oplus L$ es libre.

El truco de Eilenberg-Mazur

Recordemos que P se dice proyectivo si existe un módulo Q tal que $P \oplus Q$ es libre. Esta es una de las definiciones usuales que podemos encontrar en los libros.

Proposición

Si P es proyectivo entonces existe L libre tal que $P \oplus L$ es libre.

Sea Q tal que $P \oplus Q$ es libre.

El truco de Eilenberg-Mazur

Recordemos que P se dice proyectivo si existe un módulo Q tal que $P \oplus Q$ es libre. Esta es una de las definiciones usuales que podemos encontrar en los libros.

Proposición

Si P es proyectivo entonces existe L libre tal que $P \oplus L$ es libre.

Sea Q tal que $P \oplus Q$ es libre.

Sea
$$L = (Q \oplus P) \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus \dots$$

El truco de Eilenberg-Mazur

Recordemos que P se dice proyectivo si existe un módulo Q tal que $P \oplus Q$ es libre. Esta es una de las definiciones usuales que podemos encontrar en los libros.

Proposición

Si P es proyectivo entonces existe L libre tal que $P \oplus L$ es libre.

Sea Q tal que $P \oplus Q$ es libre.

Sea

$$L = (Q \oplus P) \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus \dots$$

Claramente L es libre.

El truco de Eilenberg-Mazur

Recordemos que P se dice proyectivo si existe un módulo Q tal que $P \oplus Q$ es libre. Esta es una de las definiciones usuales que podemos encontrar en los libros.

Proposición

Si P es proyectivo entonces existe L libre tal que $P \oplus L$ es libre.

Sea Q tal que $P \oplus Q$ es libre.

Sea

$$L = (Q \oplus P) \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus \dots$$

Claramente L es libre.

Además

$$P \oplus L = (P \oplus Q) \oplus (P \oplus Q) \oplus (P \oplus Q) \oplus \dots$$

es libre.

Bases duales

Ejercicio (Práctica 6, Ejercicio 6)

Sean A un anillo y P un A-módulo a izquierda. Una base dual para P es una familia $\{(x_i, f_i)\}_{i \in I}$ donde $(x_i, f_i) \in P \times P^*$ para cada $i \in I$, que cumple las siguientes condiciones:

(a) para todo $x \in P$ el conjunto $\{i \in I \,:\, f_i(x) \neq 0\}$ es finito, y
(b) para todo $x \in P$ vale la igualdad $x = \sum_{i \in I} f_i(x) x_i$.

Notar que (i) implica que la suma en (ii) tiene sentido.

(i) Mostrar que un A-módulo P es proyectivo si y solo si posee una base dual.
(ii) Mostrar que un A-módulo P es proyectivo y finitamente generado si y solo si posee una base dual finita.

Bases duales

Ejercicio (Práctica 6, Ejercicio 6)

Sean A un anillo y P un A-módulo a izquierda. Una base dual para P es una familia $\{(x_i, f_i)\}_{i \in I}$ donde $(x_i, f_i) \in P \times P^*$ para cada $i \in I$, que cumple las siguientes condiciones:

(a) para todo $x \in P$ el conjunto $\{i \in I \,:\, f_i(x) \neq 0\}$ es finito, y
(b) para todo $x \in P$ vale la igualdad $x = \sum_{i \in I} f_i(x) x_i$.

Notar que (i) implica que la suma en (ii) tiene sentido.

(i) Mostrar que un A-módulo P es proyectivo si y solo si posee una base dual.
(ii) Mostrar que un A-módulo P es proyectivo y finitamente generado si y solo si posee una base dual finita.

Notar que si $\{(x_1, f_1), \ldots, (x_n, f_n)\}$ es una base dual de P entonces el producto de los f_i da un morfismo $s \colon P \to R^n$, los x_i determinan un morfismo $p \colon R^n \to P$ y se tiene $ps = 1_P$.

Hallando bases duales de $\mathbb{Z}[G]$ módulos f.g.

Supongamos que un día termina la cuarentena y vamos caminando por la calle.

Hallando bases duales de $\mathbb{Z}[G]$ módulos f.g.

Supongamos que un día termina la cuarentena y vamos caminando por la calle.

Más aún supongamos que nos encontramos con un $\mathbb{Z}[G]$-módulo P que nos cuenta que es proyectivo.

Hallando bases duales de $\mathbb{Z}[G]$ módulos f.g.

Supongamos que un día termina la cuarentena y vamos caminando por la calle.

Más aún supongamos que nos encontramos con un $\mathbb{Z}[G]$-módulo P que nos cuenta que es proyectivo.

Hallando bases duales de $\mathbb{Z}[G]$ módulos f.g.

Supongamos que un día termina la cuarentena y vamos caminando por la calle.

Más aún supongamos que nos encontramos con un $\mathbb{Z}[G]$-módulo P que nos cuenta que es proyectivo.

Resulta que P nos cuenta que perdió su base dual y nos pide ayuda para volver a encontrarla.

Hallando bases duales de $\mathbb{Z}[G]$ módulos f.g.

Concretamente supongamos que G es un grupo finito y P es un $\mathbb{Z}[G]$-módulo, que visto como grupo abeliano es $\mathbb{Z}^m$ y con la acción dada como un morfismo $\rho\colon G \to \mathrm{GL}(m, \mathbb{Z})$.

Hallando bases duales de $\mathbb{Z}[G]$ módulos f.g.

Concretamente supongamos que G es un grupo finito y P es un $\mathbb{Z}[G]$-módulo, que visto como grupo abeliano es $\mathbb{Z}^m$ y con la acción dada como un morfismo $\rho\colon G \to \mathrm{GL}(m, \mathbb{Z})$.

O sea nos dan $|G|$ matrices de $m \times m$ con coeficientes enteros que *se comportan como* los elementos de G.

Hallando bases duales de $\mathbb{Z}[G]$ módulos f.g.

Concretamente supongamos que G es un grupo finito y P es un $\mathbb{Z}[G]$-módulo, que visto como grupo abeliano es $\mathbb{Z}^m$ y con la acción dada como un morfismo $\rho\colon G \to \mathrm{GL}(m, \mathbb{Z})$.

O sea nos dan $|G|$ matrices de $m \times m$ con coeficientes enteros que *se comportan como* los elementos de G.

Queremos saber si P es $\mathbb{Z}[G]$-proyectivo y en ese caso poder construir una base dual.

Encontrando la base dual

Supongamos que $\{v_1, \ldots, v_m\}$ es una base de P como $\mathbb{Z}$-módulo.

Encontrando la base dual

Supongamos que $\{v_1, \dots, v_m\}$ es una base de P como $\mathbb{Z}$-módulo.

Consideramos $\mathbb{Z}[G]^m$ (como grupo abeliano podemos pensarlo como $\mathbb{Z}^{m \cdot |G|}$), llamamos e_i al 1 en la i-ésima copia de $\mathbb{Z}[G]$ y consideramos el morfismo de $\mathbb{Z}[G]$ módulos $p \colon \mathbb{Z}[G]^m \to P$ dado por $e_i \mapsto v_i$.

Encontrando la base dual

Supongamos que $\{v_1, \dots, v_m\}$ es una base de P como $\mathbb{Z}$-módulo.

Consideramos $\mathbb{Z}[G]^m$ (como grupo abeliano podemos pensarlo como $\mathbb{Z}^{m\cdot|G|}$), llamamos e_i al 1 en la i-ésima copia de $\mathbb{Z}[G]$ y consideramos el morfismo de $\mathbb{Z}[G]$ módulos $p\colon \mathbb{Z}[G]^m \to P$ dado por $e_i \mapsto v_i$.

Si P es proyectivo p es una retracción y por lo tanto debe existir $s\colon P \to \mathbb{Z}[G]^m$ tal que $ps = 1_P$.

Encontrando la base dual

Supongamos que $\{v_1, \dots, v_m\}$ es una base de P como $\mathbb{Z}$-módulo.

Consideramos $\mathbb{Z}[G]^m$ (como grupo abeliano podemos pensarlo como $\mathbb{Z}^{m\cdot|G|}$), llamamos e_i al 1 en la i-ésima copia de $\mathbb{Z}[G]$ y consideramos el morfismo de $\mathbb{Z}[G]$ módulos $p\colon \mathbb{Z}[G]^m \to P$ dado por $e_i \mapsto v_i$.

Si P es proyectivo p es una retracción y por lo tanto debe existir $s\colon P \to \mathbb{Z}[G]^m$ tal que $ps = 1_P$.

Dar s equivale a dar para cada $i = 1, \dots, m$ un elemento de $\mathbb{Z}[G]^m$, que podemos describir con $m \cdot |G|$ números enteros.

Encontrando la base dual

Supongamos que $\{v_1, \ldots, v_m\}$ es una base de P como $\mathbb{Z}$-módulo.

Consideramos $\mathbb{Z}[G]^m$ (como grupo abeliano podemos pensarlo como $\mathbb{Z}^{m\cdot|G|}$), llamamos e_i al 1 en la i-ésima copia de $\mathbb{Z}[G]$ y consideramos el morfismo de $\mathbb{Z}[G]$ módulos $p\colon \mathbb{Z}[G]^m \to P$ dado por $e_i \mapsto v_i$.

Si P es proyectivo p es una retracción y por lo tanto debe existir $s\colon P \to \mathbb{Z}[G]^m$ tal que $ps = 1_P$.

Dar s equivale a dar para cada $i = 1, \ldots, m$ un elemento de $\mathbb{Z}[G]^m$, que podemos describir con $m \cdot |G|$ números enteros.

Ponemos $m^2 \cdot |G|$ incógnitas $x_{i,j,g}$ con $1 \leq i,j \leq m$ y $g \in G$.

Encontrando la base dual

Supongamos que $\{v_1, \dots, v_m\}$ es una base de P como $\mathbb{Z}$-módulo.

Consideramos $\mathbb{Z}[G]^m$ (como grupo abeliano podemos pensarlo como $\mathbb{Z}^{m\cdot|G|}$), llamamos e_i al 1 en la i-ésima copia de $\mathbb{Z}[G]$ y consideramos el morfismo de $\mathbb{Z}[G]$ módulos $p\colon \mathbb{Z}[G]^m \to P$ dado por $e_i \mapsto v_i$.

Si P es proyectivo p es una retracción y por lo tanto debe existir $s\colon P \to \mathbb{Z}[G]^m$ tal que $ps = 1_P$.

Dar s equivale a dar para cada $i = 1, \dots, m$ un elemento de $\mathbb{Z}[G]^m$, que podemos describir con $m \cdot |G|$ números enteros.

Ponemos $m^2 \cdot |G|$ incógnitas $x_{i,j,g}$ con $1 \leq i, j \leq m$ y $g \in G$.

La idea es ver qué tiene que pasar para que

$$s\left(\sum_{i=1}^{m} \lambda_i v_i\right) = \sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{g\in G} x_{i,j,g}\lambda_i g e_j$$

defina un morfismo $\mathbb{Z}[G]$-lineal y se cumpla $ps = 1_P$.

Encontrando la base dual

Supongamos que $\{v_1, \ldots, v_m\}$ es una base de P como $\mathbb{Z}$-módulo.

Consideramos $\mathbb{Z}[G]^m$ (como grupo abeliano podemos pensarlo como $\mathbb{Z}^{m\cdot|G|}$), llamamos e_i al 1 en la i-ésima copia de $\mathbb{Z}[G]$ y consideramos el morfismo de $\mathbb{Z}[G]$ módulos $p\colon \mathbb{Z}[G]^m \to P$ dado por $e_i \mapsto v_i$.

Si P es proyectivo p es una retracción y por lo tanto debe existir $s\colon P \to \mathbb{Z}[G]^m$ tal que $ps = 1_P$.

Dar s equivale a dar para cada $i = 1, \ldots, m$ un elemento de $\mathbb{Z}[G]^m$, que podemos describir con $m \cdot |G|$ números enteros.

Ponemos $m^2 \cdot |G|$ incógnitas $x_{i,j,g}$ con $1 \leq i, j \leq m$ y $g \in G$.

La idea es ver qué tiene que pasar para que

$$s\left(\sum_{i=1}^{m} \lambda_i v_i\right) = \sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{g\in G} x_{i,j,g}\lambda_i g e_j$$

defina un morfismo $\mathbb{Z}[G]$-lineal y se cumpla $ps = 1_P$. Por construcción es $\mathbb{Z}$-lineal.

Ecuaciones

Recordemos que la acción de G en P está dada por $\rho\colon G \to \mathrm{GL}(m, \mathbb{Z})$. Notamos M^g a la matriz $\rho(g)$.

Ecuaciones

Recordemos que la acción de G en P está dada por $\rho\colon G \to \mathrm{GL}(m, \mathbb{Z})$.
Notamos M^g a la matriz $\rho(g)$.
Queremos que $ps = 1_P$ esto es lo mismo que $v_i = ps(v_i)$ para todo $1 \leq i \leq m$.

Ecuaciones

Recordemos que la acción de G en P está dada por $\rho\colon G \to \mathrm{GL}(m, \mathbb{Z})$.
Notamos M^g a la matriz $\rho(g)$.
Queremos que $ps = 1_P$ esto es lo mismo que $v_i = ps(v_i)$ para todo $1 \leq i \leq m$. Luego queremos que valga

$$\begin{aligned} v_i &= ps(v_i) \\ &= p\left(\sum_{j=1}^{m} \sum_{g \in G} x_{i,j,g}\, g e_j\right) \\ &= \sum_{j=1}^{m} \sum_{g \in G} x_{i,j,g}\, g v_j \\ &= \sum_{j=1}^{m} \sum_{g \in G} \sum_{k=1}^{m} x_{i,j,g} M^g_{k,j} v_k \end{aligned}$$

Ecuaciones

Recordemos que la acción de G en P está dada por $\rho\colon G \to \mathrm{GL}(m, \mathbb{Z})$.
Notamos M^g a la matriz $\rho(g)$.
Queremos que $ps = 1_P$ esto es lo mismo que $v_i = ps(v_i)$ para todo $1 \leq i \leq m$. Luego queremos que valga

$$\begin{aligned} v_i &= ps(v_i) \\ &= p\left(\sum_{j=1}^{m}\sum_{g\in G} x_{i,j,g}\, g e_j\right) \\ &= \sum_{j=1}^{m}\sum_{g\in G} x_{i,j,g}\, g v_j \\ &= \sum_{j=1}^{m}\sum_{g\in G}\sum_{k=1}^{m} x_{i,j,g} M^g_{k,j} v_k \end{aligned}$$

Luego para $1 \leq i, k \leq m$ debe valer

$$\delta_{i,k} = \sum_{j=1}\sum_{g\in G} x_{i,j,g} M^g_{j,k}.$$

Más ecuaciones

Para cada $h \in G$ y para cada $1 \leq i \leq m$ tiene que valer $s(h \cdot v_i) = h \cdot s(v_i)$.

Más ecuaciones

Para cada $h \in G$ y para cada $1 \leq i \leq m$ tiene que valer $s(h \cdot v_i) = h \cdot s(v_i)$. Entonces por como definimos s,

$$s\left(\sum_{j=1}^{m} M_{j,i}^{h} v_j\right) = h \cdot \sum_{j=1}^{m} \sum_{g \in G} x_{i,j,g} g e_j$$

Más ecuaciones

Para cada $h \in G$ y para cada $1 \leq i \leq m$ tiene que valer $s(h \cdot v_i) = h \cdot s(v_i)$. Entonces por como definimos s,

$$s\left(\sum_{j=1}^{m} M^h_{j,i} v_j\right) = h \cdot \sum_{j=1}^{m} \sum_{g \in G} x_{i,j,g} g e_j$$

$$\sum_{j=1}^{m} \sum_{k=1}^{m} \sum_{g \in G} x_{j,k,g} M^h_{j,i} g e_k = \sum_{k=1}^{m} \sum_{g \in G} x_{i,k,g} h g e_k$$

Más ecuaciones

Para cada $h \in G$ y para cada $1 \leq i \leq m$ tiene que valer $s(h \cdot v_i) = h \cdot s(v_i)$. Entonces por como definimos s,

$$s\left(\sum_{j=1}^{m} M^h_{j,i} v_j\right) = h \cdot \sum_{j=1}^{m} \sum_{g \in G} x_{i,j,g}\, g e_j$$

$$\sum_{j=1}^{m} \sum_{k=1}^{m} \sum_{g \in G} x_{j,k,g} M^h_{j,i}\, g e_k = \sum_{k=1}^{m} \sum_{g \in G} x_{i,k,g}\, h g e_k$$

Entonces para cada $1 \leq i, k \leq m$ y cada $h \in G$ se tiene

$$\sum_{j=1}^{m} \sum_{g \in G} x_{j,k,g} M^h_{j,i}\, g = \sum_{g \in G} x_{i,k,g}\, h g$$

Más ecuaciones (cont.)

Entonces para cada $1 \leq i, k \leq m$ y cada $h \in G$ se tiene

$$\sum_{j=1}^{m} \sum_{g \in G} x_{j,k,g} M^{h}_{j,i} g = \sum_{g \in G} x_{i,k,g} hg$$

Más ecuaciones (cont.)

Entonces para cada $1 \leq i, k \leq m$ y cada $h \in G$ se tiene

$$\sum_{j=1}^{m} \sum_{g \in G} x_{j,k,g} M_{j,i}^{h} g = \sum_{g \in G} x_{i,k,g} hg$$

Entonces para cada $1 \leq i, k \leq m$ y cada $h, g \in G$ se tiene

$$\sum_{j=1}^{m} x_{j,k,g} M_{j,i}^{h} = x_{i,k,h^{-1}g}$$

El sistema

Pasando en limpio, P es proyectivo si y solo si el sistema de ecuaciones lineales

- $\displaystyle\sum_{j=1}^{m} x_{j,k,g} M^{h}_{j,i} = x_{i,k,h^{-1}g}$, con $1 \leq i, k \leq m$ y $h, g \in G$
- $\displaystyle\delta_{i,k} = \sum_{j=1} \sum_{g \in G} x_{i,j,g} M^{g}_{j,k}$, con $1 \leq i, k \leq m$

admite una solución entera. La solución en ese caso nos da una base dual.