Álgebra II Práctica (clase 22)

Guido Arnone

Universidad de Buenos Aires

14 de Julio de 2020

Prerrequisitos

Para leer estas diapositivas se recomienda haber leído el apunte teórico hasta el Corolario 4.29.

Hacia el teorema de estructura

En esta clase veremos algunas consecuencias del teorema de estructura en el caso de $\mathbb{Z}$ y $k[X]$.

Comenzamos recordando las definiciones relevantes y haciendo algunas observaciones:

Hacia el teorema de estructura

En esta clase veremos algunas consecuencias del teorema de estructura en el caso de $\mathbb{Z}$ y $k[X]$.

Comenzamos recordando las definiciones relevantes y haciendo algunas observaciones:

- Un A-módulo M se dice finitamente generado si tiene un sistema de generadores finito. Esto es equivalente a que existan $n \in \mathbb{N}$ y un epimorfismo $A^n \to M$.

Hacia el teorema de estructura

En esta clase veremos algunas consecuencias del teorema de estructura en el caso de $\mathbb{Z}$ y $k[X]$.

Comenzamos recordando las definiciones relevantes y haciendo algunas observaciones:

- Un A-módulo M se dice finitamente generado si tiene un sistema de generadores finito. Esto es equivalente a que existan $n \in \mathbb{N}$ y un epimorfismo $A^n \to M$.
- Un A-módulo libre L es finitamente generado si y sólo si existe $n \in \mathbb{N}$ tal que $L \simeq A^n$. Decimos en tal caso que L es libre de rango n.

Hacia el teorema de estructura

En esta clase veremos algunas consecuencias del teorema de estructura en el caso de $\mathbb{Z}$ y $k[X]$.

Comenzamos recordando las definiciones relevantes y haciendo algunas observaciones:

- Un A-módulo M se dice finitamente generado si tiene un sistema de generadores finito. Esto es equivalente a que existan $n \in \mathbb{N}$ y un epimorfismo $A^n \to M$.
- Un A-módulo libre L es finitamente generado si y sólo si existe $n \in \mathbb{N}$ tal que $L \simeq A^n$. Decimos en tal caso que L es libre de rango n. Si A es conmutativo, tiene noción de rango, así que n determina a L salvo isomorfismo.

Proposición

Sea A un DIP y L un A-módulo libre de rango n. Todo submódulo de L es libre de rango menor o igual a n.

Anulador y Torsión

Si A es un anillo y M un A-módulo, en anulador de un subconjunto $S \subset M$ es

$$\mathrm{Ann}_A(S) = \{a \in A : a \cdot s = 0 \ (\forall s \in S)\}.$$

Este resulta un ideal a izquierda de A. Notamos $\mathrm{Ann}_A(x) := \mathrm{Ann}_A(\{x\})$ y decimos que x es de torsión si su anulador es distinto de cero.

Anulador y Torsión

Si A es un anillo y M un A-módulo, en anulador de un subconjunto $S \subset M$ es

$$\mathrm{Ann}_A(S) = \{a \in A : a \cdot s = 0 \ (\forall s \in S)\}.$$

Este resulta un ideal a izquierda de A. Notamos $\mathrm{Ann}_A(x) := \mathrm{Ann}_A(\{x\})$ y decimos que x es de torsión si su anulador es distinto de cero.

La torsión de M es el submódulo formado por los elementos de torsión,

$$\tau(M) := \{m \in M : \mathrm{Ann}_A(x) \neq 0\}.$$

Decimos que M es libre de torsión si $\tau(M) = 0$ y de torsión si $\tau(M) = M$.

Anulador y Torsión

Si A es un anillo y M un A-módulo, en anulador de un subconjunto $S \subset M$ es

$$\mathrm{Ann}_A(S) = \{a \in A : a \cdot s = 0 \ (\forall s \in S)\}.$$

Este resulta un ideal a izquierda de A. Notamos $\mathrm{Ann}_A(x) := \mathrm{Ann}_A(\{x\})$ y decimos que x es de torsión si su anulador es distinto de cero.

La torsión de M es el submódulo formado por los elementos de torsión,

$$\tau(M) := \{m \in M : \mathrm{Ann}_A(x) \neq 0\}.$$

Decimos que M es libre de torsión si $\tau(M) = 0$ y de torsión si $\tau(M) = M$.

Proposición

Si A es un dominio íntegro, un A-módulo finitamente generado M es de torsión si y sólo si $\mathrm{Ann}_A(M) \neq 0$.

Anulador y Torsión en $\mathbb{Z}$

Fijemos M un $\mathbb{Z}$-módulo, es decir, un grupo abeliano.

Anulador y Torsión en $\mathbb{Z}$

Fijemos M un $\mathbb{Z}$-módulo, es decir, un grupo abeliano.

Si $x \in M$ es un elemento del grupo, como $\mathbb{Z}$ es DIP su anulador

$$\mathrm{Ann}_{\mathbb{Z}}(x) = \{k \in \mathbb{Z} : k \cdot x = 0\}$$

es principal: existe $m \in \mathbb{Z}$ tal que $\mathrm{Ann}_{\mathbb{Z}}(x) = m\mathbb{Z}$.

Anulador y Torsión en $\mathbb{Z}$

Fijemos M un $\mathbb{Z}$-módulo, es decir, un grupo abeliano.

Si $x \in M$ es un elemento del grupo, como $\mathbb{Z}$ es DIP su anulador

$$\mathrm{Ann}_{\mathbb{Z}}(x) = \{k \in \mathbb{Z} : k \cdot x = 0\}$$

es principal: existe $m \in \mathbb{Z}$ tal que $\mathrm{Ann}_{\mathbb{Z}}(x) = m\mathbb{Z}$. El elemento x es de torsión si y sólo si tiene orden finito, y en tal caso su orden es m.

Anulador y Torsión en $\mathbb{Z}$

Fijemos M un $\mathbb{Z}$-módulo, es decir, un grupo abeliano.

Si $x \in M$ es un elemento del grupo, como $\mathbb{Z}$ es DIP su anulador

$$\mathrm{Ann}_{\mathbb{Z}}(x) = \{k \in \mathbb{Z} : k \cdot x = 0\}$$

es principal: existe $m \in \mathbb{Z}$ tal que $\mathrm{Ann}_{\mathbb{Z}}(x) = m\mathbb{Z}$. El elemento x es de torsión si y sólo si tiene orden finito, y en tal caso su orden es m.

Del mismo modo, el $\mathbb{Z}$-módulo M es libre de torsión si *ningún* elemento tiene orden finito y es de torsión si *todo* elemento es de orden finito.

Anulador y Torsión en $\mathbb{Z}$

Fijemos M un $\mathbb{Z}$-módulo, es decir, un grupo abeliano.

Si $x \in M$ es un elemento del grupo, como $\mathbb{Z}$ es DIP su anulador

$$\mathrm{Ann}_{\mathbb{Z}}(x) = \{k \in \mathbb{Z} : k \cdot x = 0\}$$

es principal: existe $m \in \mathbb{Z}$ tal que $\mathrm{Ann}_{\mathbb{Z}}(x) = m\mathbb{Z}$. El elemento x es de torsión si y sólo si tiene orden finito, y en tal caso su orden es m.

Del mismo modo, el $\mathbb{Z}$-módulo M es libre de torsión si *ningún* elemento tiene orden finito y es de torsión si *todo* elemento es de orden finito.

Sabemos que si M es finito entonces es de torsión, así que $\mathrm{Ann}_{\mathbb{Z}}(M) \neq 0$. El generador de este ideal es un concepto conocido: lo habíamos definido como el exponente $\exp(M)$ del grupo.

Anulador y Torsión en $\mathbb{Z}$

Fijemos M un $\mathbb{Z}$-módulo, es decir, un grupo abeliano.

Si $x \in M$ es un elemento del grupo, como $\mathbb{Z}$ es DIP su anulador

$$\mathrm{Ann}_{\mathbb{Z}}(x) = \{k \in \mathbb{Z} : k \cdot x = 0\}$$

es principal: existe $m \in \mathbb{Z}$ tal que $\mathrm{Ann}_{\mathbb{Z}}(x) = m\mathbb{Z}$. El elemento x es de torsión si y sólo si tiene orden finito, y en tal caso su orden es m.

Del mismo modo, el $\mathbb{Z}$-módulo M es libre de torsión si *ningún* elemento tiene orden finito y es de torsión si *todo* elemento es de orden finito.

Sabemos que si M es finito entonces es de torsión, así que $\mathrm{Ann}_{\mathbb{Z}}(M) \neq 0$. El generador de este ideal es un concepto conocido: lo habíamos definido como el exponente $\exp(M)$ del grupo.

Por definición $\exp(M)$ es el menor entero positivo m tal que $m \cdot x = 0$ para todo $x \in M$, y Lagrange nos dice que $\exp(G)$ divide a $|G|$

Anulador y Torsión en $k[X]$

Fijemos V un $k[X]$-módulo de dimensión $\dim_k V$ finita, es decir, un k-espacio vectorial de dimensión finita junto con un endomorfismo $T : V \to V$.

Anulador y Torsión en $k[X]$

Fijemos V un $k[X]$-módulo de dimensión $\dim_k V$ finita, es decir, un k-espacio vectorial de dimensión finita junto con un endomorfismo $T : V \to V$.

Si v es un vector de V, su anulador está generado por el polinomio minimal $m_{T,v} \in k[X]$ de v:

$$\mathrm{Ann}_{k[X]}(v) = \{f \in k[X] : f \cdot v = 0\} = \{f \in k[X] : f(T)(v) = 0\} = \langle m_{T,v} \rangle.$$

En particular, todo elemento es de torsión así que un $k[X]$-módulo de dimensión finita sobre k es siempre de torsión.

Anulador y Torsión en $k[X]$

Fijemos V un $k[X]$-módulo de dimensión $\dim_k V$ finita, es decir, un k-espacio vectorial de dimensión finita junto con un endomorfismo $T : V \to V$.

Si v es un vector de V, su anulador está generado por el polinomio minimal $m_{T,v} \in k[X]$ de v:

$$\mathrm{Ann}_{k[X]}(v) = \{f \in k[X] : f \cdot v = 0\} = \{f \in k[X] : f(T)(v) = 0\} = \langle m_{T,v} \rangle.$$

En particular, todo elemento es de torsión así que un $k[X]$-módulo de dimensión finita sobre k es siempre de torsión.

Su anulador está generado por el polinomio minimal m_T de T,

$$\mathrm{Ann}_{k[X]}(V) = \{f \in k[X] : f \cdot v = 0 \ (\forall v \in V)\} = \{f \in k[X] : f(T) \equiv 0\} = \langle m_T \rangle.$$

Anulador y Torsión en $k[X]$

Fijemos V un $k[X]$-módulo de dimensión $\dim_k V$ finita, es decir, un k-espacio vectorial de dimensión finita junto con un endomorfismo $T : V \to V$.

Si v es un vector de V, su anulador está generado por el polinomio minimal $m_{T,v} \in k[X]$ de v:

$$\mathrm{Ann}_{k[X]}(v) = \{f \in k[X] : f \cdot v = 0\} = \{f \in k[X] : f(T)(v) = 0\} = \langle m_{T,v} \rangle.$$

En particular, todo elemento es de torsión así que un $k[X]$-módulo de dimensión finita sobre k es siempre de torsión.

Su anulador está generado por el polinomio minimal m_T de T,

$$\mathrm{Ann}_{k[X]}(V) = \{f \in k[X] : f \cdot v = 0 \ (\forall v \in V)\} = \{f \in k[X] : f(T) \equiv 0\} = \langle m_T \rangle.$$

Como $\mathrm{Ann}_{k[X]}(X) \supset \mathrm{Ann}_{k[X]}(Y)$ si $X \subset Y$, esto nos dice en particular que $m_{v,T}$ divide a m_T para todo $v \in V$.

La descomposición en torsión y parte libre

Si A es un dominio íntegro y M un A-módulo, entonces $M/\tau(M)$ es libre de torsión.

La descomposición en torsión y parte libre

Si A es un dominio íntegro y M un A-módulo, entonces $M/\tau(M)$ es libre de torsión. Por otro lado, si A es DIP, un A-módulo M finitamente generado es libre de torsión si y sólo si es libre.

La descomposición en torsión y parte libre

Si A es un dominio íntegro y M un A-módulo, entonces $M/\tau(M)$ es libre de torsión. Por otro lado, si A es DIP, un A-módulo M finitamente generado es libre de torsión si y sólo si es libre. Esto nos dice que dado M un módulo finitamente generado sobre un DIP la sucesión exacta

$$0 \to \tau(M) \hookrightarrow M \to M/\tau(M) \to 0$$

se parte y $M \simeq \tau(M) \oplus M/\tau(M) \simeq \tau(M) \oplus A^n$ para cierto $n \in \mathbb{N}$.

La descomposición en torsión y parte libre

Si A es un dominio íntegro y M un A-módulo, entonces $M/\tau(M)$ es libre de torsión. Por otro lado, si A es DIP, un A-módulo M finitamente generado es libre de torsión si y sólo si es libre. Esto nos dice que dado M un módulo finitamente generado sobre un DIP la sucesión exacta

$$0 \to \tau(M) \hookrightarrow M \to M/\tau(M) \to 0$$

se parte y $M \simeq \tau(M) \oplus M/\tau(M) \simeq \tau(M) \oplus A^n$ para cierto $n \in \mathbb{N}$.

Además, si $N \simeq \tau(N) \oplus A^n$ y $M \simeq \tau(M) \oplus A^m$ son A-módulos f.g. sobre un DIP, entonces $N \simeq M$ sí y sólo si $n = m$ y $\tau(N) \simeq \tau(M)$.

La descomposición en torsión y parte libre

Si A es un dominio íntegro y M un A-módulo, entonces $M/\tau(M)$ es libre de torsión. Por otro lado, si A es DIP, un A-módulo M finitamente generado es libre de torsión si y sólo si es libre. Esto nos dice que dado M un módulo finitamente generado sobre un DIP la sucesión exacta

$$0 \to \tau(M) \hookrightarrow M \to M/\tau(M) \to 0$$

se parte y $M \simeq \tau(M) \oplus M/\tau(M) \simeq \tau(M) \oplus A^n$ para cierto $n \in \mathbb{N}$.

Además, si $N \simeq \tau(N) \oplus A^n$ y $M \simeq \tau(M) \oplus A^m$ son A-módulos f.g. sobre un DIP, entonces $N \simeq M$ sí y sólo si $n = m$ y $\tau(N) \simeq \tau(M)$.

Esto nos dice que para clasificar los modulos finitamente generados sobre un dominio de ideales principales debemos entender su torsión, o directamente, que debemos entender a los módulos de torsión.

En lo que sigue fijamos A DIP y todo módulo se supondrá finitamente generado.

Descomposición Primaria

Si M es un A-módulo y $f \in A$ irreducible, la f-torsión (o notando $\mathfrak{m} = (f)$, la $\mathfrak{m}$-torsión) de M es el submódulo

$$M[f] := M[\mathfrak{m}] := \{x \in M : \text{existe } n \geq 1 \text{ tal que } f^n \cdot x = 0\}.$$

Si f y g son asociados, entonces $(f) = (g)$ y $M[f] = M[\mathfrak{m}] = M[g]$.

Descomposición Primaria

Si M es un A-módulo y $f \in A$ irreducible, la f-torsión (o notando $\mathfrak{m} = (f)$, la $\mathfrak{m}$-torsión) de M es el submódulo

$$M[f] := M[\mathfrak{m}] := \{x \in M : \text{existe } n \geq 1 \text{ tal que } f^n \cdot x = 0\}.$$

Si f y g son asociados, entonces $(f) = (g)$ y $M[f] = M[\mathfrak{m}] = M[g]$.

El Teorema 4.23 del apunte teórico describe a la torsión en base a la f-torsión,

Teorema

Sea A un DIP. Si M es un A-módulo de torsión finitamente generado, entonces

$$M = \bigoplus_{\mathfrak{m} \in \mathrm{Max}(A)} M[\mathfrak{m}].$$

El Ejemplo 4.24 nos dice además que $M[\mathfrak{m}] \neq 0$ si y sólo si $\mathfrak{m} \supset \mathrm{Ann}_A(M)$.

Descomposición Primaria en $\mathbb{Z}$

Si M es un grupo abeliano finito, el teorema nos dice que

$$M = \bigoplus_{p \geq 1 \text{ primo}} M[p\mathbb{Z}] = \bigoplus_{p \mid |M| \text{ primo}} M[p]$$

y como

$$M[p] = \{x \in M : p^n x = 0 \text{ para algún } n \in \mathbb{N}\}$$

es el p-grupo de M de mayor orden, vemos entonces que un grupo abeliano es la suma directa de sus p-subgrupos de Sylow.

Descomposición Primaria en $k[X]$

Para el caso de (V, T) un $k[X]$-módulo con $\dim_k V < \infty$, recuperamos el teorema de descomposición primaria que se vé en lineal: si la factorización irreducible del polinomio minimal de T es

$$m_T = f_1^{n_1} \cdots f_r^{n_r}$$

entonces tenemos una descomposición de V en subespacios T-invariantes

$$V = V_1 \oplus \cdots \oplus V_r$$

con $V_i = \ker f_i^{n^i}(T) = V[f_i]$.

El teorema de estructura

De estudiar la f-torsión obtenemos el teorema de estructura, pues un módulo de f-torsión finitamente generado es isomorfismo a uno de la forma

$$A/(f^{\alpha_1}) \oplus \cdots \oplus A/(f^{\alpha_r})$$

con $\alpha_1 \geq \cdots \geq \alpha_r$.

Veamos versiones equivalentes del teorema:

El teorema de estructura

De estudiar la f-torsión obtenemos el teorema de estructura, pues un módulo de f-torsión finitamente generado es isomorfismo a uno de la forma

$$A/(f^{\alpha_1}) \oplus \cdots \oplus A/(f^{\alpha_r})$$

con $\alpha_1 \geq \cdots \geq \alpha_r$.

Veamos versiones equivalentes del teorema:

Teorema (de estructura para módulos f.g. sobre un DIP)

Sea A un DIP y M un A-módulo finitamente generado. Existen únicos número $n, r \geq 0$ e ideales propios $0 \neq I_1 \subset \cdots \subset I_r \subsetneq A$ tales que

$$M \simeq A^n \oplus \bigoplus_{j=1}^{r} A/I_j.$$

El teorema de estructura

Teorema (de estructura para módulos f.g. sobre un DIP)

Sea A un DIP y M un A-módulo finitamente generado. Existen únicos números $n, r \geq 0$ e ideales propios $0 \neq I_1 \subset \cdots \subset I_r \subsetneq A$ tales que

$$M \simeq A^n \oplus \bigoplus_{j=1}^{r} A/I_j.$$

Teorema (de estructura para módulos f.g. sobre un DIP)

Sea A un DIP y M un A-módulo finitamente generado. Existen únicos números $n, r \geq 0$ y elementos únicos salvo asociados $d_1 \mid \cdots \mid d_r$, no nulos ni unidades, tales que

$$M \simeq A^n \oplus \bigoplus_{j=1}^{r} A/(d_j).$$

El teorema de estructura

Teorema (de estructura para módulos f.g. sobre un DIP)

Sea A un DIP y M un A-módulo finitamente generado. Existen únicos números $n, r \geq 0$, ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, $s \geq 1$ y vectores $n_i = (n_{i,1}, \ldots, n_{i,r}) \in \mathbb{N}_0^r$ tales que para cada i, j es $n_{i,j} \geq n_{i+1,j}$ y

$$M \simeq A^n \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s} A/\mathfrak{m}^{n_{i,j}}.$$

El teorema de estructura

Teorema (de estructura para módulos f.g. sobre un DIP)

Sea A un DIP y M un A-módulo finitamente generado. Existen únicos números $n, r \geq 0$, ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, $s \geq 1$ y vectores $n_i = (n_{i,1}, \ldots, n_{i,r}) \in \mathbb{N}_0^r$ tales que para cada i, j es $n_{i,j} \geq n_{i+1,j}$ y

$$M \simeq A^n \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s} A/\mathfrak{m}^{n_{i,j}}.$$

Teorema (de estructura para módulos f.g. sobre un DIP)

Sea A un DIP y M un A-módulo finitamente generado. Existen únicos números $n, r \geq 0$, elementos irreducibles únicos salvo asociados $f_1, \ldots, f_r$, $s \geq 1$ y $n_i = (n_{i,1}, \ldots, n_{i,r}) \in \mathbb{N}_0^r$ tales que para cada i, j es $n_{i,j} \geq n_{i+1,j}$ y

$$M \simeq A^n \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s} A/(f_i^{n_{i,j}}).$$

El teorema de estructura en $\mathbb{Z}$

Esto clasifica todos los grupos abelianos finitamente generados,

Teorema (de estructura para grupos abelianos finitamente generados)

Sea G un grupo abeliano finitamente generado. Existen únicos números $n, r \geq 0$ y primos $p_1, \ldots, p_r \geq 1$, $s \geq 1$ y $n_i = (n_{i,1}, \ldots, n_{i,r}) \in \mathbb{N}_0^r$ tales que para cada i, j es $n_{i,j} \geq n_{i+1,j}$ y

$$G \simeq \mathbb{Z}^n \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{s} \mathbb{Z}_{p_i^{n_{i,j}}}.$$

Teorema (de estructura para grupos abelianos finitamente generados)

Sea A un DIP y G un grupo abeliano finitamente generado. Existen únicos números $n, r \geq 0$ y enteros positivos $d_1 \mid \cdots \mid d_r$ tales que

$$M \simeq \mathbb{Z}^n \oplus \bigoplus_{j=1}^{r} \mathbb{Z}_{d_j}.$$

El teorema de estructura en $\mathbb{Z}$

Veamos un ejemplo explícito de como se dan ambas escrituras para

$$G = \mathbb{Z}_9 \oplus \mathbb{Z}_{33} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_4.$$

El teorema de estructura en $\mathbb{Z}$

Veamos un ejemplo explícito de como se dan ambas escrituras para

$$G = \mathbb{Z}_9 \oplus \mathbb{Z}_{33} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_4.$$

Usando que la p-torsión separa sumas,

El teorema de estructura en $\mathbb{Z}$

Veamos un ejemplo explícito de como se dan ambas escrituras para

$$G = \mathbb{Z}_9 \oplus \mathbb{Z}_{33} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_4.$$

Usando que la p-torsión separa sumas,

- la 2-torsión es $\mathbb{Z}_4 \oplus \mathbb{Z}_8$,

El teorema de estructura en $\mathbb{Z}$

Veamos un ejemplo explícito de como se dan ambas escrituras para

$$G = \mathbb{Z}_9 \oplus \mathbb{Z}_{33} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_4.$$

Usando que la p-torsión separa sumas,

- la 2-torsión es $\mathbb{Z}_4 \oplus \mathbb{Z}_8$,
- la 3-torsión es $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, y

El teorema de estructura en $\mathbb{Z}$

Veamos un ejemplo explícito de como se dan ambas escrituras para

$$G = \mathbb{Z}_9 \oplus \mathbb{Z}_{33} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_4.$$

Usando que la p-torsión separa sumas,

- la 2-torsión es $\mathbb{Z}_4 \oplus \mathbb{Z}_8$,
- la 3-torsión es $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, y
- la 11-torsión es $\mathbb{Z}_{11}$.

El teorema de estructura en $\mathbb{Z}$

Veamos un ejemplo explícito de como se dan ambas escrituras para

$$G = \mathbb{Z}_9 \oplus \mathbb{Z}_{33} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_4.$$

Usando que la p-torsión separa sumas,

- la 2-torsión es $\mathbb{Z}_4 \oplus \mathbb{Z}_8$,
- la 3-torsión es $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, y
- la 11-torsión es $\mathbb{Z}_{11}$.

Ordenando las potencias de cada torsión crecientemente conseguimos los factores invariantes:

G	$\mathbb{Z}_{792}$	$\mathbb{Z}_{12}$	$\mathbb{Z}_3$
$G[2]$	$\mathbb{Z}_8$	$\mathbb{Z}_4$	0
$G[3]$	$\mathbb{Z}_9$	$\mathbb{Z}_3$	$\mathbb{Z}_3$
$G[11]$	$\mathbb{Z}_{11}$	0	0

obtenemos la descomposición de $G = \mathbb{Z}_3 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{792}$. Recíprocamente, podemos volver a la descomposición en torsión aplicando el teorema chino del resto en cada caso.

El teorema de estructura en $k[X]$

Supongamos que k es un cuerpo algebraicamente cerrado y sea (V, T) un $k[X]$-módulo con $\dim_k V < \infty$. Sea $m_T = (X - \lambda_1)^{n_1} \cdots (X - \lambda_r)^{n_r}$ la factorización irreducible del polinomio minimal de T. .

El teorema de estructura en $k[X]$

Supongamos que k es un cuerpo algebraicamente cerrado y sea (V, T) un $k[X]$-módulo con $\dim_k V < \infty$. Sea $m_T = (X - \lambda_1)^{n_1} \cdots (X - \lambda_r)^{n_r}$ la factorización irreducible del polinomio minimal de T. .

Vimos que el teorema de descomposición primaria nos daba una descomposición en subespacios T-invariantes

$$V = V_1 \oplus \cdots \oplus V_r$$

con V_i la $(X - \lambda_i)$-torsión de V.

El teorema de estructura en $k[X]$

Supongamos que k es un cuerpo algebraicamente cerrado y sea (V, T) un $k[X]$-módulo con $\dim_k V < \infty$. Sea $m_T = (X - \lambda_1)^{n_1} \cdots (X - \lambda_r)^{n_r}$ la factorización irreducible del polinomio minimal de T. .

Vimos que el teorema de descomposición primaria nos daba una descomposición en subespacios T-invariantes

$$V = V_1 \oplus \cdots \oplus V_r$$

con V_i la $(X - \lambda_i)$-torsión de V. Para cada $i \in [\![r]\!]$, el teorema de estructura nos dice que existen $n_{i,1} \cdots n_{i,s}$ tales que

$$V_i \simeq \frac{k[X]}{\langle (X - \lambda_i)^{n_{i,1}} \rangle} \oplus \cdots \oplus \frac{k[X]}{\langle (X - \lambda_i)^{n_{i,s}} \rangle}.$$

El teorema de estructura en $k[X]$

El $k[X]$-módulo $k[X]/\langle (X-\lambda_i)^{n_{i,j}} \rangle$ tiene dimensión $n_{i,j}$ con base

$$B = \{1, X-\lambda, \cdots, (X-\lambda)^{n_{i,j}-1}\}$$

y en esta base la multiplicación por X tiene como matriz un bloque de Jordan

$$J(\lambda, n) = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

El teorema de estructura en $k[X]$

El $k[X]$-módulo $k[X]/\langle (X-\lambda_i)^{n_{i,j}} \rangle$ tiene dimensión $n_{i,j}$ con base

$$B = \{1, X-\lambda, \cdots, (X-\lambda)^{n_{i,j}-1}\}$$

y en esta base la multiplicación por X tiene como matriz un bloque de Jordan

$$J(\lambda, n) = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & \lambda & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

Vemos así que el teorema de estructura recupera en particular el teorema de Jordan que se ve en álgebra lineal. Los detalles están en el Ejemplo 4.30 del apunte teórico.

Un Ejercicio y una Aplicación

Ejercicio

Probar que un grupo abeliano finito G es cíclico si y sólo si $\exp(G) = |G|$.

Un Ejercicio y una Aplicación

Ejercicio

Probar que un grupo abeliano finito G es cíclico si y sólo si $\exp(G) = |G|$.

Teorema (del elemento primitivo)

Si k es un cuerpo, todo subgrupo finito $G \leq k^\times$ es cíclico.

Un Ejercicio y una Aplicación

Ejercicio

Probar que un grupo abeliano finito G es cíclico si y sólo si $\exp(G) = |G|$.

Teorema (del elemento primitivo)

Si k es un cuerpo, todo subgrupo finito $G \leq k^\times$ es cíclico.

Demostración.

Sea $e = \exp(G)$ y veamos que $e = |G|$.

Un Ejercicio y una Aplicación

Ejercicio

Probar que un grupo abeliano finito G es cíclico si y sólo si $\exp(G) = |G|$.

Teorema (del elemento primitivo)

Si k es un cuerpo, todo subgrupo finito $G \leq k^\times$ es cíclico.

Demostración.

Sea $e = \exp(G)$ y veamos que $e = |G|$. Por definición, se tiene que $x^e = 1$ para todo $x \in G$.

Un Ejercicio y una Aplicación

Ejercicio

Probar que un grupo abeliano finito G es cíclico si y sólo si $\exp(G) = |G|$.

Teorema (del elemento primitivo)

Si k es un cuerpo, todo subgrupo finito $G \leq k^\times$ es cíclico.

Demostración.

Sea $e = \exp(G)$ y veamos que $e = |G|$. Por definición, se tiene que $x^e = 1$ para todo $x \in G$. Dicho de otra forma, el polinomio $p = X^e - 1 \in k[X]$ tiene por raíz a todo elemento de G.

Un Ejercicio y una Aplicación

Ejercicio

Probar que un grupo abeliano finito G es cíclico si y sólo si $\exp(G) = |G|$.

Teorema (del elemento primitivo)

Si k es un cuerpo, todo subgrupo finito $G \leq k^\times$ es cíclico.

Demostración.

Sea $e = \exp(G)$ y veamos que $e = |G|$. Por definición, se tiene que $x^e = 1$ para todo $x \in G$. Dicho de otra forma, el polinomio $p = X^e - 1 \in k[X]$ tiene por raíz a todo elemento de G. Como p no puede tener más de e raíces distintas, necesariamente $|G| \leq e$. La otra desigualdad vale siempre. □