Universidad de la República
Facultad de Ciencias
Centro de Matemática

Módulos finitamente generados sobre un dominio de ideales principales

Notas adaptadas por Mariana Haim para el curso "Anillos y Módulos" 2021.

Este capítulo está dedicado al llamado *Teorema de Estructura* de módulos finitamente generados sobre un DIP, que describe cómo son todos los módulos finitamente generados indescomponibles sobre un DIP y asegura que los demás se construyen a partir de estos tomando sumas directas finitas.

Para acercarnos al resultado, comenzamos con una sección que lista "buenas" propiedades de los módulos sobre un DIP y seguimos con una sección que presenta los módulos de torsión y su también "buen comportamiento" sobre un DIP, fundamentales para entender el Teorema de Estructura. La última sección es una aplicación del Teorema de Estructura que permite obtener la forma de Jordan de una matriz, y una construcción general de ésta para el caso de un cuerpo cualquiera.

0.1. Propiedades hereditarias de los módulos sobre un DIP

Recordamos que un anillo es *noetheriano a izquierda* si sus ideales a izquierda son finitamente generados.

Proposición 0.1.1. *Sean A un anillo noetheriano a izquierda, M un A-módulo y $N \subseteq M$ un submódulo. Si M es finitamente generado, entonces N también lo es.*

Demostración. Haremos inducción en $\mu(M)$.

Si $\mu(M) = 1$, entonces $M = Am \cong \frac{A}{\mathrm{Ann}(m)}$ para algún $m \in M$ y por tanto N es isomorfo a un submódulo de $\frac{A}{\mathrm{Ann}(m)}$. Por el teorema de correspondencia, existe J ideal izquierdo de A tal que $N \cong \frac{J}{\mathrm{Ann}(m)}$. Como J es finitamente generado, N también lo es.

Supongamos que vale el resultado para valores menores o iguales a n y que $\mu(M) = n + 1$. Tomemos $G = \{g_1, \ldots, g_{n+1}\}$ generador de M y definamos $M' = Ag_1 + \cdots + Ag_n$. En la sucesión exacta:

$$0 \to M' \cap N \hookrightarrow N \to \frac{N}{M' \cap N} \to 0$$

el término de la derecha es $\frac{N}{M'\cap N} \cong \frac{M'+N}{M'} \subseteq \frac{M}{M'} = A\overline{g_{n+1}}$ por el segundo teorema de isomorfismo, y el término de la izquierda es un submódulo de M' que verifica $\mu(M') \leqslant n$. Por hipótesis de inducción, ambos términos son finitamente generados, de donde se deduce que el término del medio también lo es (proposición 4.4.3). □

El resultado anterior puede mejorarse para el caso de un DIP, como muestra la siguiente

Proposición 0.1.2. *Sean D un DIP, M un D-módulo y $N \subseteq M$ un submódulo. Si M es finitamente generado, entonces N también lo es y $\mu(N) \leqslant \mu(M)$.*

Demostración. La primera parte de la afirmación es consecuencia directa de la Proposición 0.1.1, ya que todo DIP es noetheriano. Para la segunda parte de la afirmación, recorramos la prueba de la proposición 0.1.1. En el caso base, se tiene que J es generado por un elemento por ser D DIP y por lo tanto N también, de donde $\mu(N) \leqslant 1 = \mu(M)$. En el paso inductivo, se tiene $\mu(M' \cap N) \leqslant \mu(M')$ y $\mu\left(\frac{N}{M'\cap N}\right) \leqslant \mu\left(\frac{M}{M'}\right) = 1$, de donde $\mu(N) \leqslant \mu(M' \cap N) + \mu(\frac{N}{M'\cap N}) \leqslant \mu(M') + 1 \leqslant n + 1 = \mu(M)$. □

Para el caso de submódulos de un módulo libre sobre un DIP, se puede afinar el resultado, a saber:

Proposición 0.1.3. *Sean D un DIP, M un D-módulo y $N \subseteq M$ un submódulo. Si M es libre de rango finito, entonces N también lo es y* $\operatorname{rg}(N) \leqslant \operatorname{rg}(M)$.

Demostración. Otra vez procederemos por inducción, esta vez en $\operatorname{rg}(M)$.

Si $\operatorname{rg}(M) = 1$, entonces $M \cong D$ y por tanto $N \cong J$ siendo J un ideal de D, por lo tanto principal. Se tiene entonces $N \cong (a)$ para cierto $a \in D$. Si $a = 0$, ya está. Si no, como D es un dominio, $\{a\}$ es linealmente independiente y por lo tanto la imagen de $\{a\}$ por el isomorfismo $N \cong (a)$ es base de N, que resulta libre de rango 1.

Supongamos que vale el resultado para módulos de rango menor o igual a n y probémoslo para M de rango $n+1$. Si $B = \{b_1, \ldots, b_{n+1}\}$ es base de M, sea $M' = Ab_1 + \cdots + Ab_n$. Nuevamente, en la sucesión exacta:

$$0 \to M' \cap N \hookrightarrow N \to \frac{N}{M' \cap N} \to 0$$

el término de la derecha es $\frac{N}{M' \cap N} \subseteq \frac{M}{M'} = A\overline{b_{n+1}}$ que es libre de rango 1. En efecto, $\{\overline{b_{n+1}}\}$ es base de $\frac{M}{M'}$: si $a\overline{b_{n+1}} = 0$, entonces $ab_{n+1} \in M'$ y por tanto es combinación lineal del conjunto $\{b_1, \ldots, b_n\}$; como B es linealmente independiente, se obtiene $a = 0$.

Por hipótesis de inducción, se tiene que el término de la derecha es libre y por tanto la sucesión se escinde (corolario 4.4.6), y $N \cong (M' \cap N) \oplus \frac{N}{M' \cap N}$.

Por otra parte, $M' \cap N$ es un submódulo de M' que es libre de rango n. Por hipótesis de inducción, se deduce que N es libre y

$$\operatorname{rg}(N) = \operatorname{rg}(M' \cap N) + \operatorname{rg}\left(\frac{N}{M' \cap N}\right) \leqslant \operatorname{rg}(M') + \operatorname{rg}\left(\frac{M}{M'}\right) = n + 1. \qquad \square$$

Observación 0.1.1. El resultado anterior es válido aunque M no sea finitamente generado. Es decir, sobre un DIP, submódulo de un libre es libre. El lector interesado puede encontrar la prueba del resultado general en el apéndice.

0.2. Teoría de torsión

Definición 0.2.1. Sean A un anillo no trivial y M un A-módulo. Un elemento $m \in M$ se dice *de torsión* si existe $a \in A$ no nulo tal que $am = 0$. Además, se define la *torsión de M* como el subconjunto

$$\operatorname{Tor}(M) = \{m \in M \mid m \text{ es de torsión}\}$$

El módulo M se dice *de torsión* si $\operatorname{Tor}(M) = M$ y se dice *sin torsión* o *libre de torsión* si $\operatorname{Tor}(M) = \{0\}$.

Observación 0.2.1.

- $0 \in M$ siempre es de torsión.
- Si A es conmutativo, considerando A como A-módulo, se tiene $\operatorname{Tor}(A) = \{a \in A \mid a \text{ es divisor de cero}\}$. En particular, si D es un dominio, $\operatorname{Tor}(D) = \{0\}$.

La siguiente proposición muestra que la torsión de M tiene buenas propiedades en el caso en que el anillo es un dominio, por lo que a partir de ahora nos situaremos en ese contexto.

Proposición 0.2.1. *Sea D un dominio y M un D-módulo. Entonces* $\operatorname{Tor}(M) \subseteq M$ *es un submódulo, y* $M/\operatorname{Tor}(M)$ *es sin torsión.*

Demostración. Sean $m, n \in \operatorname{Tor}(M)$. Existen entonces $a, b \in D$ no nulos tales que $am = bn = 0$ y por lo tanto $ab(m+n) = 0$, puesto que D es conmutativo. Como D no tiene divisores de cero, se tiene $ab \neq 0$ y por lo tanto $m + n \in \operatorname{Tor}(M)$.

Por otra parte, si $m \in \operatorname{Tor}(M)$ y $d \in D$, entonces existe $a \in D$ no nulo tal que $am = 0$ y por lo tanto $a(dm) = d(am) = 0$, por lo que $dm \in \operatorname{Tor}(M)$.

Veamos la segunda afirmación. Sea $\overline{x} \in M/\operatorname{Tor}(M)$, $\overline{x} \neq \overline{0}$ (i.e. $x \notin \operatorname{Tor}(M)$). Supongamos que $a\overline{x} = \overline{0}$. Pero entonces $\overline{ax} = \overline{0} \Rightarrow ax \in \operatorname{Tor}(M)$, es decir, existe $b \neq 0$ tal que $bax = 0$. Como $x \notin \operatorname{Tor}(M)$, entonces $ba = 0$. Como $b \neq 0$ y D es un dominio, debe ser $a = 0$. □

Observación 0.2.2.

1. Es sencillo verificar que si $f : M \to N$ es un isomorfismo, se tiene $f(\operatorname{Tor}(M)) = \operatorname{Tor}(N)$, por lo que si D es un dominio y M, N son D-módulos, entonces $M \cong N \Rightarrow \operatorname{Tor}(M) \cong \operatorname{Tor}(N)$.

2. Es un ejercicio verificar que $\operatorname{Tor}(\bigoplus_{i\in I} M_i) \cong \bigoplus_{i\in I} \operatorname{Tor}(M_i)$.

Ejemplos 0.2.1.

1. Si L es libre sobre un dominio, entonces $\operatorname{Tor}(L) = \{0\}$. En efecto, $L \cong \bigoplus_{i\in I} D$ por lo que $\operatorname{Tor}(L) \cong \bigoplus_{i\in I} \operatorname{Tor}(D) = \{0\}$.

2. $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo es de torsión, es decir, $\operatorname{Tor}(\mathbb{Z}_n) = \mathbb{Z}_n$. En efecto $n\overline{x} = 0$, para todo $x \in \mathbb{Z}_n$.

3. Más en general, todo grupo abeliano finito G es de torsión. En efecto, dado $g \in G$ no nulo, consideremos el morfismo de $\mathbb{Z}$-módulos $\varphi_g : \mathbb{Z} \to G$, $\varphi_g(n) = ng$. Si g no es de torsión, entonces $\operatorname{Ker} \varphi = 0$ y por lo tanto G contiene una copia de $\mathbb{Z}$, por lo que es infinito.

En el ejemplo anterior observamos que todo módulo libre sobre un dominio es sin torsión. El recíproco no es cierto, como muestran los siguientes

Ejemplos 0.2.2.

1. $\mathbb{Q}$ es un $\mathbb{Z}$-módulo sin torsión que no es libre.

2. (x, y) es un $\Bbbk[x, y]$-módulo sin torsión que no es libre.

3. $\mathbb{Z}^{\mathbb{N}}$ (el producto directo de infinitas copias de $\mathbb{Z}$) es un $\mathbb{Z}$-módulo sin torsión que no es libre.

Sin embargo, el resultado es positivo para el caso en que D es un DIP y M es finitamente generado, como enuncia la siguiente

Proposición 0.2.2. *Si D es un DIP y M es un D-módulo finitamente generado y sin torsión, entonces M es libre.*

Demostración. Sea $X = \{x_1, \ldots, x_n\}$ un generador de M. Como M es sin torsión, cada uno de los conjuntos $\{x_i\}$ es linealmente independiente, por lo que existe un subconjunto de X linealmente independiente maximal $U = \{u_1, \ldots, u_k\} \subseteq X$. [1]

Supongamos que existe $x_i \in X \backslash U$. Entonces, por maximalidad de U, el conjunto $U \cup \{x_i\}$ es linealmente dependiente, y por lo tanto (como U es linealmente independiente), existe $d_i \in D$ no nulo tal que $d_i x_i = a_1 u_1 + a_2 u_2 + \cdots + a_k u_k$.

Llamemos d al producto de los d_i obtenidos por cada $x_i \in X \backslash U$. Como D es un dominio, debe ser $d \neq 0$. Además, para cada $i \in \{1, \ldots, n\}$, se tiene $dx_i \in \langle u_1, \ldots, u_k\rangle$.

Sea $\varphi : M \to M$, $\varphi(m) = dm$. Es un morfismo de D-módulos. Es inyectivo porque M es sin torsión. Por lo tanto, el primer teorema de isomorfismo nos da $M \simeq \operatorname{Im} \varphi \subset \langle u_1, \ldots, u_k\rangle$ que es libre. Al ser D un DIP, todo submódulo de un D-módulo libre es libre; en particular, $\operatorname{Im} \varphi \simeq M$ es libre. □

[1] Se puede probar, de hecho, que en un módulo finitamente generado sobre un dominio, todo conjunto linealmente independiente tiene $\leqslant$ elementos que un generador.

0.3. Teorema de estructura

Proposición 0.3.1. *Sean D un DIP y M un D-módulo finitamente generado. Entonces existen D-módulos L y T, con L libre y T de torsión, tales que $M \cong T \bigoplus L$. Además, L y T son únicos a menos de isomorfismo.*

Demostración. Alcanza con observar que en la sucesión exacta

$$0 \hookrightarrow \operatorname{Tor}(M) \to M \to \frac{M}{\operatorname{Tor}(M)} \to 0$$

el término de la derecha es sin torsión, y por tanto libre (proposición 0.2.2). Se tiene entonces que la sucesión se escinde, y por consecuencia

$$M \cong \operatorname{Tor}(M) \oplus \frac{M}{\operatorname{Tor}(M)}.$$

Tomando $T = \operatorname{Tor}(M)$ y $L = \frac{M}{\operatorname{Tor}(M)}$ se tiene la descomposición buscada.

Supongamos ahora que $T \oplus L \cong T' \oplus L'$ via un isomorfismo φ. Entonces, por la Observación 0.2.2, se tiene $\varphi(\operatorname{Tor}(T \oplus L)) = \operatorname{Tor}(T' \oplus L')$, i.e. $\varphi(T) = T'$. Tenemos entonces $T \cong T'$ y la prueba termina observando que

$$L \cong \frac{T \oplus L}{T} \cong \frac{\varphi(T \oplus L)}{\varphi(T)} = \frac{T' \oplus L'}{T'} \cong L'. \qquad \square$$

Tenemos entonces descompuesto a un módulo finitamente generado M sobre un DIP de manera única como suma directa de un libre con su torsión $\operatorname{Tor}(M)$. Como ya sabemos, la parte libre es de la forma $\bigoplus_I D$. Ahora investigaremos qué forma tiene la parte de torsión.

Definición 0.3.1. Un módulo $M \neq 0$ se dice **indescomponible** si $M = X \oplus Y$ implica $X = 0$ o $Y = 0$.

Proposición 0.3.2. *Si D es un dip, los D-módulos D y $\frac{D}{(p^\alpha)}$, con p primo y α positivo son indescomponibles y cíclicos.*

Demostración. Sale usando que la intersección de dos ideales de D distintos y no triviales es no trivial, sale la afirmación para D, que está generado por 1.
Para la segunda hay que considerar ideales de D que contienen a (p^α) y sale la afirmación para $\frac{D}{(p^\alpha)}$, que está generado por $\bar{1}$. $\square$

Teorema 0.3.3 (de estructura de módulos finitamente generados de torsión)**.** *Sean D un DIP y M un D-módulo finitamente generado. Existen $p_1, \ldots, p_k \in D$ irreducibles, $n_1, \ldots, n_t \in \mathbb{Z}^+$ y $\alpha_{ij} \in \mathbb{Z}^+, i \in \{1, 2, \ldots, t\}, j \in \{1, 2, \ldots, n_i\}$ tales que*

$$\operatorname{Tor}(M) \cong \frac{D}{(p_1^{\alpha_{11}})} \oplus \cdots \oplus \frac{D}{(p_1^{\alpha_{1n_1}})} \oplus \cdots \oplus \frac{D}{(p_t^{\alpha_{t1}})} \oplus \cdots \oplus \frac{D}{(p_t^{\alpha_{tn_t}})}.$$

Además, los p_i son únicos a menos de asociados y los n_i, α_{ij} son únicos.

Observación 0.3.1.
- Los $p_i^{\alpha_{ij}}$ se dicen *factores invariantes de M*.
- Se trata de una descomposición de $Tor(M)$ en submódulos cíclicos indescomponibles.

- Juntando la segunda afirmación con la proposición 0.3.1, se tiene que todo módulo finitamente generado se descompone en suma directa de submódulos cíclicos indescomponibles (la parte libre aporta sumandos del tipo D, y la parte de torsión sumandos del tipo $\frac{D}{(p^\alpha)}$ con $p \in D$ irreducible y $\alpha \in \mathbb{Z}^+$).

- El conjunto $\{r, t, p_1^{\alpha_{11}}, \ldots, p_t^{\alpha_{tn_t}}\}$ es un *conjunto completo de invariantes*; es decir, si dos D-módulos son isomorfos, entonces tienen los mismos invariantes. Además este conjunto de invariantes es *completo*: es decir, que si dos D-módulos tienen los mismos invariantes entonces son isomorfos.

Demostración. No vamos a demostrar este Teorema en el contexto general; para simplificar, haremos la prueba (en la próxima sección) para el caso $D = \mathbb{Z}$ (esto es, para grupos abelianos). □

0.4. Prueba del Teorema de Estructura de Grupos abelianos finitamente generados

Proposición 0.4.1.
- *Todo grupo abeliano finito se descompone en suma de indescomponibles.*

- *Un grupo abeliano es finitamente generado y de torsıón si y solo si es finito.*

Demostración.
- En efecto, si el grupo es indescomponible, ya está, si no es suma directa de subgrupos de cardinal estrictamente menor. Si ambos son indescomponibles ya está, si no el proceso sigue y para porque el cardinal del grupo original es finito y va bajando estrictamente en cada descomposición no tirival.

- Supongamos que G es finito. Si tiene un elemento sin torsión $x \in G$, el morfismo de grupos $\mathbb{Z} \to G$ que multiplica por x es inyectivo, contradiciendo la finitud de G.
Recíprocamente si X es un generador finito de G, para todo $x \in X$ existe $n \in \mathbb{Z}$ no nulo tal que $n_x x = 0$. Se deduce que todo elemento de G es combinación de los elementos de X con coeficiente en x un entero entre 0 y $n_x - 1$, por lo que hay finitos elementos en G. □

Proposición 0.4.2.
- *Un grupo abeliano es finitamente generado y de torsión si y sólo si es finito.*

- *Si G es un grupo abeliano finito, existe $n \in \mathbb{N}$ tal que $nx = 0, \forall x \in G$.* [2]

Demostración.
- Si G es finito entonces es finitamente generado por el propio G. Además, si tiene un elemento $x \neq 0$ que no es de torsión, se deduce que el morfismo $\mathbb{Z} \to G$ que multiplica por x es inyectivo y por tanto G es infinito.
Recíprocamente, sea X un generador finito de G. Cada elemento $x \in X$ tiene un testigo $n_x \in \mathbb{N}$ de la torsión. Se puede probar a partir de aquíque todo elemento de G es de la forma $\sum_{x \in X} r_x x$, con $0 \leqslant r_x < n_x$, por lo que G tiene a lo sumo $\prod_{x \in X} n_x$ elementos.

- Alcanza con tomar un testigo de la torsión para cada $x \in G$ y multiplicarlos todos entre sí , obteniendo un posible n.

□

[2] Se puede probar, a partir del conocido Teorema de Lagrange para grupos - pero no lo haremos acá- que $\#G$ sirve como un posible n.

Definición 0.4.1. Sea p un natural primo. Un grupo abeliano G es un p-**grupo** si para todo $x \in G$, existe α tal que $p^{\alpha}x = 0$

Observación 0.4.1. Dado un grupo abeliano G y un primo p, se define

$$Tor_p(G) = \{g \in G \mid \exists \alpha \geqslant 1 : p_i^{\alpha} g = 0\}.$$

Es fácil probar que $Tor_p(G)$ es un subgrupo de $Tor(G)$ y que si $G \cong G'$ via φ, entonces $Tor_p(G) \cong Tor_p(G')$ via la correspondiente restricción de φ

Teorema 0.4.3. *Todo grupo abeliano finito se descompone en suma directa de p-grupos.*

Demostración. Sea n como en la Proposición 0.4.2. Para todo $g \in G$, se tiene $ng = 0$. Supongamos $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ con $mcd(p_i, p_j) = 1, \forall i \neq j$ y consideremos para cada $i \in \{1, 2, \cdots, t\}$, el subgrupo

$$G_i = Tor_{p_i}(G) \leqslant G.$$

Veamos primero que $G = \bigoplus_{i=1}^{t} G_i$.
Notar que si $q_i = \frac{n}{p_i^{e_i}}$, se tiene $q_i x \in G_i \forall x \in G$ y $mcd(q_1, q_2, \dots q_t) = 1$, por lo que existen $a_i \in \mathbb{Z}$ tales que $\sum_{i=1}^{k} a_i q_i = 1$. Se deduce, para todo $x \in G$:

$$x = 1 \cdot x = a_1 q_1 x + \cdots a_t q_t x \in \sum_{i=1}^{k} G_i.$$

Además, si $x \in G_i \cap \sum_{j \neq i} G_j$, entonces $p_i^{\alpha} x = 0$ y $x = \sum_{j \neq i} x_j, x_j \in G_j$. Para cada $j \neq i$ sea α_j tal que $p_j^{\alpha_j} x_j = 0$ y $t = \prod_{j \neq i} p_j^{\alpha_j}$. Se deduce $tx = 0$. Pero mcd $(p_i^{\alpha_i}, t) = 1$ de donde $x = 1 \cdot x = 0$.

$\square$

Lema 0.4.4. *Sea G un p-grupo abeliano y $Y = \{y_1, y_2, \cdots, y_t\} \subseteq G$ tal que $< Y >= \bigoplus_{i=1}^{t} < y_i >$.*

1. *Si $pz_i = y_i, \forall i \in \{1, 2, \cdots, t\}$, entonces $< y_1, y_2, \cdots, y_t >= \bigoplus_{i=1}^{t} < y_i >$.*
2. *Si $k_i \in \mathbb{Z}, \forall i \in \{1, 2, \cdots, t\}$, entonces $< k_1 y_1, k_2 y_2, \cdots, k_t y_t >= \bigoplus_{i=1}^{t} < k_i y_i >$.*

Demostración.
1. Supongamos que $\sum_{i=1}^{t} a_i z_i = 0$. Entonces $\sum_{i=1}^{t} a_i y_i = \sum_{i=1}^{t} a_i p z_i = p \sum_{i=1}^{t} a_i z_i = 0$. Usando la hipótesis, se deduce que $a_i y_i = 0, \forall i \in \{1, 2, \cdots, t\}$. Como G es un p-grupo, se deduce que $a_i = pa_i', \forall i$. Se tiene entonces $\sum_{i=1}^{t} a_i' y_i = \sum_{i=1}^{t} a_i' p z_i = 0 = \sum_{i=1}^{t} a_i z_i = 0$ y por tanto $a_i z_i = a_i' p z_i = a_i' y_i = 0, \forall i \in \{1, 2, \cdots, t\}$.
2. Supongamos que $\sum_{i=1}^{t} a_i k_i z_i = 0$ se deduce de la parte anterior que $a_i k_i z_i = 0, \forall i \in \{1, 2, \cdots, t\}$.

$\square$

Teorema 0.4.5. *Todo p-grupo es isomorfo a la suma directa finita de grupos de la forma $\mathbb{Z}_{p^{e_i}}$, con $e_i \in \mathbb{N}, e \geqslant 1$.*

Demostración. Haremos la prueba por inducción en

$$m = min\{\alpha \mid p^{\alpha} x = 0, \forall x \in G\}$$

Si $m = 1$, entonces $px = 0, \forall x \in G$, de lo que se deduce que G es un $\mathbb{Z}_p$-espacio vectorial, y como tal, es suma directa de copias de $\mathbb{Z}_p$ (en particular lo es como grupo abeliano).

Supongamos que el resultado vale hasta m. Lo probaremos para $m+1$. Consideremos $H = pG \leqslant G$. Como $p^m x = 0, \forall x \in H$, se tiene por inducción que $H = \oplus_{i=1}^{t} \mathbb{Z}_{p_i^e}$.
Tomemos $\{pz_1, pz_2, \cdots, pz_t\}$ generador de H tal que pz_i genera $\mathbb{Z}_{p_i^e}$. Por otra parte sea $A_p = \{x \in G \mid px = 0\}$. Para cada z_i en L, si $k_i = min\{n \mid ny_i = 0\}$, entonces $k_i z_i \in A_p$. En efecto $p(k_i z_i) = k_i(pz_i) = ky_i = 0$.
Ahora bien, A_p es un $\mathbb{Z}_p$- espacio vectorial y por lo tanto es suma directa de copias de $\mathbb{Z}_p$. Por el Lema 0.4.4, el conjunto $X = \{k_1 z_1, \cdots k_t z_t\}$ es linealmente independiente (en A_p como $\mathbb{Z}_p$-espacio vectorial), y por tanto se extiende a una base $X \sqcup Y$ de A_p.
Consideremos los subgrupos K Y L generados respectivamente por Y y $\{z_1, z_2, \cdots, z_t\}$. Por un lado, $K \subseteq A_p$, está en las hipotésis de inducción y por lo tanto es suma de (p-) grupos cíclicos. Por otro lado, L es suma directa de los subgrupos generados por los z_i, que son cíclicos (de orden pk_i).
Vamos a probar que $G = K \oplus L$ y con eso tenemos la tesis.
Veamos primero que $K \cap L = 0$: sea $y = \sum_{i=1}^{t} a_i z_i \in < Y > \subseteq A_p$. Se tiene entonces $py = 0$ y por tanto $a_i y_i = pa_i z_i = 0, \forall i = \{1, 2, \cdots, t\}$, de donde $a_i = a_i' k_i$ y se deduce $0 = y - y = \sum_{i=1}^{t} a_i' k_i z_i - y$ y por construcción de Y resulta $y = 0$.
Veamos ahora que $G = K + L$. Para cada $x \in G$, se tiene $px \in H$, por lo que $px = \sum -i = 1^t a_i y_i = \sum_{i=1}^{t} pa_i z_i$, de donde $p(x - \sum_{i=1}^{t} a_i z_i) = 0$. Se deduce que $x - \sum_{i=1}^{t} a_i z_i \in A_p$ y por lo tanto en $K + L$. Finalmente $x \in K + L$ puesto que $\sum_{i=1}^{t} a_i z_i \in L$.

$\square$

Observación 0.4.2. Notar que los grupos finitos indescomponibles son de la forma $\mathbb{Z}_{p^\alpha}$.

Ejemplo 0.4.1. Hallemos todas las clases de isomorfismo de un grupo abeliano G de cardinal 180. Como $180 = 2^2 \cdot 3^2 \cdot 5$. Por lo tanto G es isomorfo a uno y sólo uno de los siguientes:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5$.

Corolario 0.4.6 (Clasificación de grupos abelianos finitamente generados)**.** *Sea G un grupo abeliano finitamente generado.*
Existe un único $r \in \mathbb{N}$, y únicos (a menos del orden) $p_1, \ldots, p_k \in \mathbb{N}$ primos (no necesariamente diferentes) y $n_1, \cdots, n_k \in \mathbb{N}$ no nulos y $\alpha_{ij} \geqslant 1, \forall i \in \{1, 2, \cdots, k\}, j \in \{1, 2, \cdots n_i\}$, tales que

$$G \cong (\mathbb{Z}_{p_1^{\alpha_{11}}} \oplus \mathbb{Z}_{p_1^{\alpha_{12}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{\alpha_{1n_1}}}) \oplus \cdots \oplus (\mathbb{Z}_{p_k^{\alpha_{k1}}} \oplus \mathbb{Z}_{p_k^{\alpha_{k2}}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{\alpha_{kn_k}}}) \oplus \mathbb{Z}^r$$

Demostración.
Existencia
Como $\mathbb{Z}$ es un DIP, sabemos que todo grupo abeliano G finitamente generado se descompone en suma directa de un subgrupo libre y uno de torsión. La parte libre es de la forma $\mathbb{Z}^r$.
La parte de torsión es finita (porque es finitamente generada) por lo que el resto de la prueba se deduce de los Teoremas 0.4.3 y 0.4.5.
Unicidad Por un lado si $T \oplus L \cong T' \oplus L'$ con T, T' de torsión y L, L' libres, se tiene por la Proposición 0.3.1 que $T \cong T', L \cong L'$. Se deduce que r es único, puesto que D tiene número de base invariante.
Ahora bien, en vista de la Observación 0.4.1, queda probar que si p es primo y

$$\mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_n}} \cong \mathbb{Z}_{p^{\beta_1}} \oplus \mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_k}} \qquad (*)$$

para ciertos $n, k > 0$, $\alpha_i \geqslant \alpha_j \geqslant 1$, $\beta_i \geqslant \beta_j \geqslant 1$ cuando $i > j$, entonces $n = k, \alpha_i = \beta_i, \forall i$.
Lo probaremos por inducción en el cardinal de T. Si es p (es el caso $\mathbb{T} = \mathbb{Z}_p$), la unicidad es clara. Supongamos ahora que la afirmación vale para $\#T < h$ y que

$$\mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_n}} \cong \mathbb{Z}_{p^{\beta_1}} \oplus \mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_k}}$$

con $\alpha_i \geqslant \alpha_j$, $\beta_i \geqslant \beta_j$ cuando $i > j$. Se deduce que

$$p\mathbb{Z}_{p^{\alpha_1}} \oplus p\mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus p\mathbb{Z}_{p^{\alpha_h}} \cong p\mathbb{Z}_{p^{\beta_1}} \oplus p\mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus p\mathbb{Z}_{p^{\beta_k}} \qquad (**)$$

Ahora bien, observemos que

$$p\mathbb{Z}_{p^\gamma} \cong \begin{cases} 0 & \text{si } \gamma = 1 \\ \mathbb{Z}_{p^{\gamma-1}} & \text{si no} \end{cases}$$

(el segundo caso se prueba observando que el morfismo de $\mathbb{Z}_{p^{\gamma-1}} \to \mathbb{Z}_{p^\gamma}$ que multiplica por p está bien definido, es inyectivo y tiene imagen $p\mathbb{Z}_{p^\gamma}$). Si $\alpha_i = 1, \forall i$ entonces queda el grupo trivial a la izquierda, y por lo tanto el grupo trivial a la derecha, lo que implica que $\beta_j = 1 \forall j$ y además, por cardinalidad, que $n = k$.
Si no, se tiene que, en $(**)$, el grupo de torsión involucrado tiene estrictamente al menos p y estrictamente menos de h elementos y

$$\mathbb{Z}_{p^{\alpha_1 - 1}} \oplus \mathbb{Z}_{p^{\alpha_2 - 1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_l - 1}} \cong \mathbb{Z}_{p^{\beta_1 - 1}} \oplus \mathbb{Z}_{p^{\beta_2 - 1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_r - 1}}.$$

donde todos los sumandos son no nulos. Se deduce, aplicando la hipótesis de inducción, que $r = l$, $\alpha_i - 1 = \beta_i - 1, \forall i \leqslant l$.
Además $p\mathbb{Z}_{p^{\alpha_u}} = p\mathbb{Z}_{p^{\beta_u}} = 0, \forall u > l$, de donde $\alpha_u = \beta_u = 1, \forall u > l$. $\square$

0.5. Aplicación: forma de Jordan

En lo que sigue $\Bbbk$ es un cuerpo cualquiera, V un $\Bbbk$-espacio vectorial y $T : V \to V$ una transformación lineal.
Usaremos el Teorema de Estructura para, en el caso en que $\Bbbk = \mathbb{C}$ y V de dimensión finita, obtener una descomposición de V en subespacios T-cíclicos (i.e. generados por un elemento v y sus transformados a través de T y sus iteradas), que da lugar a una base B de V para la cual la matriz asociada ${}_B[T]_B$ es en algún sentido "simple". Dicha matriz es esencialmente única y se llama forma de Jordan de T.

Antes de enunciar el primer resultado, conviene recordar algunas definiciones. Decimos que un subespacio W de V es T-*invariante* si $T(W) \subseteq W$, y que es T-*cíclico* si para cierto $w \in W$, se tiene que el conjunto $\{w, T(w), T^2(w), \dots, T^n(w), \dots\}$ es un generador de W. En este último caso, notamos $W = Z(T, w)$.

Recordemos además que un A-módulo M se dice *cíclico* si $M = Am = \{am \mid a \in A\}$ para cierto $m \in M$.

La siguiente proposición permite poner nuestra situación en contexto de módulos sobre $\Bbbk[x]$.

Proposición 0.5.1. *Sean $\Bbbk$ un cuerpo, V un $\Bbbk$-espacio vectorial y $T : V \to V$ una transformación lineal. Entonces:*

1. *Definiendo $p\dot{v} = p(T)(v)$ para todo $v \in V, p \in \Bbbk[x]$, se obtiene que V es un $\Bbbk[x]$-módulo.*

2. *Si $W \subseteq V$ es un subespacio vectorial, entonces se tiene que:*

   a) *W es T-invariante si y sólo si W es un $\Bbbk[x]$-submódulo de V,*

   b) *W es T-cíclico si y sólo si W es un $\Bbbk[x]$-módulo cíclico.*

Demostración. 1. La estructura aditiva de V como $\Bbbk[x]$-módulo es la de V como $\Bbbk$-módulo. Por otra parte es claro que la operación $\cdot : \Bbbk[x] \times V \to V$ es distributiva con respecto a la suma en $\Bbbk[x]$ y con respecto a la suma en V. Observemos además que $1\dot{v} = \mathrm{Id}(v) = v$ para todo $v \in V$. Falta entonces verificar que

$$\dot{p(q\dot{v})} = (pq)\dot{v} \quad \forall p, q \in \Bbbk[x], v \in V$$

Para esto, es claro que alcanza con verificarlo para p y q monomios de $\Bbbk[x]$. En efecto, basta con observar que si $p = \sum_{i=0}^{k} a_i x^i$, entonces

$$p \cdot v = \sum_{i=0}^{k} a_i \left(x^i \cdot v\right) \tag{1}$$

Tomemos entonces $p = ax^i, q = bx^j$. Tenemos que $q = (bT^j)(v) = bT^j(v)$. Entonces

$$\dot{p(q\dot{v})} = \dot{p(bT^j(v))} = (aT^i)\left(bT^j(v)\right) = aT^i\left(bT^j(v)\right) = abT^i\left(T^j(v)\right) = abT^{i+j}(v)$$

Como $pq = abx^{i+j}$, se deduce la tesis.

2. Tomemos ahora $W \subseteq V$ subespacio.

   a) W es T-invariante si y sólo si $T(w) \in W$ para todo $w \in W$, si y sólo si $x \cdot w \in W$ para todo $w \in W$. Es claro por (1) que esto último equivale a $p \cdot w \in W$ para todo $w \in W, p \in \Bbbk[x]$, es decir, a que W sea un $\Bbbk[x]$-submódulo de V.

   b) $W = Z(T, w)$ si y sólo si W es generado como $\Bbbk$-espacio vectorial por $\{T^i(w) \mid i \in \mathbb{N}\}$, si y sólo si W es generado como $\Bbbk[x]$-módulo por w (puesto que $T^n(w) = x^n \cdot w$). $\square$

Observación 0.5.1. 1. Considerando $\Bbbk \subseteq \Bbbk[x]$, la acción de $\Bbbk[x]$ en V definida arriba extiende a la acción original de $\Bbbk$ en V. En efecto, $\lambda \cdot v = (\lambda\,\mathrm{Id})(v) = \lambda v$ para todo $\lambda \in \Bbbk, v \in V$.

2. A partir de la Observación 0.5.1.1, se deduce que un generador de V como $\Bbbk$-espacio vectorial también es generador de V como $\Bbbk[x]$-módulo.

3. Es claro que si V es de dimensión finita $Z(T, w)$ también lo es, y por lo tanto existe $k \in \mathbb{N}$ tal que el conjunto $\{w, T(w), T^2(w), \dots, T^{k-1}(w)\}$ es generador de $Z(T, w)$. Más adelante, veremos que se puede optimizar dicho k para obtener una base.

4. Si $f \in \Bbbk[x]$, se tiene que $\frac{\Bbbk[x]}{(f)}$ es un espacio vectorial de dimensión $\mathrm{gr}\,(f)$. En efecto, es fácil verificar que el conjunto $\{\bar{1}, \bar{x}, \dots, \bar{x}^{\mathrm{gr}\,(f)-1}\}$ es una base.

Polinomios característico y minimal Consideremos la inclusión $\iota : \Bbbk \to \mathrm{End}(V)$, definida por $\iota(\lambda) = \lambda\,\mathrm{Id}$. Es claro que es un morfismo de anillos y por tanto se extiende de manera única a un morfismo de anillos $\varepsilon_T : \Bbbk[x] \to \mathrm{End}(V)$ tal que $\varepsilon_T(x) = T$. Explícitamente, se tiene $\varepsilon_T(p) = p(T)$.

Si V tiene dimensión finita, podemos considerar el polinomio $\chi_T = \det(T - x\,\mathrm{Id})$. Dicho polinomio se llama *polinomio característico de* T, es de grado $\dim(V)$ y por tanto no nulo. El Teorema de Cayley-Hamilton asegura que $\chi_T(T) = 0$.

Se deduce que $\ker(\varepsilon_T)$ es un ideal de $\Bbbk[x]$ no nulo, y por tanto generado por un polinomio no nulo $m_T \in \Bbbk[x]$ que se elige mónico y se llama *polinomio minimal de* T. (Notar que al elegir m_T mónico, forzamos que sea único).

Es claro entonces que $m_T(T) = 0$, que $m_T \mid \chi_T$ y que m_T es el polinomio mónico de menor grado entre los que anulan a T.

La siguiente proposición permite poner a V, en el caso en que tenga dimensión finita, en el contexto del Teorema de Estructura.

Proposición 0.5.2. *Sean $\Bbbk$, V y T como antes. Supongamos además que V es de dimensión finita. Entonces V es un $\Bbbk[x]$-módulo finitamente generado y de torsión.*

Demostración. Por la Observación 0.5.1.2 es claro que V es finitamente generado, puesto que es de dimensión finita.

Además si V es de dimensión finita, podemos considerar el polinomio característico de T. Como $\chi_T(T) = 0$, tenemos $\chi_T \cdot v = 0$ para todo $v \in V$. Se deduce que todo $v \in V$ es de torsión. □

Estamos entonces en condiciones de aplicar el Teorema de Estructura al $\Bbbk[x]$-módulo V, y eso es lo que nos permitirá demostrar el siguiente resultado.

Teorema 0.5.3. *Sea V un espacio vectorial de dimensión $n < \infty$ y $T \in \operatorname{End}(V)$. Sea además $m_T = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$ la descomposición en irreducibles mónicos no asociados dos a dos del polinomio minimal. Entonces existen $k_1, \ldots, k_r \in \mathbb{Z}^+$ y subespacios $V_{ij}, i \in \{1, \ldots, r\}, j \in \{1, \ldots, k_i\}$ de V, tales que*

1. $V = \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{k_i} V_{ij}$,
2. *para todo par (i, j), el subespacio V_{ij} es T-cíclico,*
3. *para todo par (i, j), existe $n_{ij} \in \mathbb{Z}^+$ tal que* $V_{ij} \cong \frac{\Bbbk[x]}{(q_i^{n_{ij}})}$,
4. *para todo i, se tiene* $n_i = \max\{n_{ij} \mid j \in \{1, \ldots, k_i\}\}$,
5. $n = \sum_{ij} \operatorname{gr}(q_i) n_{ij}$.

Más aún, los V_{ij} son únicos a menos de isomorfismos y de reordenaciones.

Demostración. Como V es de torsión y finitamente generado sobre el dominio de ideales principales $\Bbbk[x]$, el Teorema de Estructura nos da una descomposición de V en submódulos cíclicos indescomponibles:

$$V \cong \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{s_i} \frac{\Bbbk[x]}{(p_i^{n_{ij}})},$$

para ciertos $p_i \in \Bbbk[x]$ irreducibles no asociados dos a dos y ciertos $n_{ij} \in \mathbb{Z}^+$ no nulos. Es claro que los p_i pueden elegirse mónicos, y eso hacemos.

Llamemos $\varphi : \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{s_i} \frac{\Bbbk[x]}{(p_i^{n_{ij}})} \to V$ al isomorfismo involucrado y definamos entonces, para cada $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s_i\}$,

$$V_{ij} := \varphi\left(\frac{\Bbbk[x]}{(p_i^{n_{ij}})}\right).$$

Es claro que $V = \bigoplus_{i=1}^{t}\bigoplus_{j=1}^{s_i} V_{ij}$, que $\mathrm{Ann}(V_{ij}) = (p_i^{n_{ij}})$. Además, para cada $i \in \{1, \dots, t\}$, podemos reordenar los $j \in \{1, \dots, s_i\}$ para que $n_{i1} \geqslant \cdots \geqslant n_{is_i}$.

Veamos ahora que:

- $r = t$,
- podemos reordernar los $i \in \{1, \dots, r = t\}$ para que $p_i = q_i$ y $s_i = k_i$, para todo $i \in \{1, \dots, r = t\}$,
- $n_i = n_{i1}$, para todo $i \in \{1, \dots, r = t\}$.

Como $\Bbbk[x]$ es un dominio factorial, m_T se descompone de manera única (a menos de reordenaciones) en producto de irreducibles mónicos, por lo que alcanza con ver que

$$m_T = p_1^{n_{11}} p_2^{n_{21}} \cdots p_t^{n_{t1}} \tag{2}$$

para deducir las tres afirmaciones de arriba. Llamemos p al polinomio del lado derecho de (2). Como $p_i^{n_{ij}}$ anula a cada V_{ij}, se tiene que $p_i^{n_{i1}}$ anula a cada V_{ij}, y por tanto p anula a V. Se deduce que p es múltiplo de m_T.

Recíprocamente, observar que el polinomio minimal de $T_{|V_{ij}}$ es $p_i^{n_{ij}}$; como m_T anula a V_{ij} se tiene que m_T es múltiplo de cada $p_i^{n_{ij}}$. Como p es el el mínimo común múltiplo de los $p_i^{n_{ij}}$, se obtiene que m_T es múltiplo de p.

Al ser m_T y p asociados y mónicos, se deduce que son iguales.

Finalmente, notar que por la observación 0.5.1.4, tenemos $\dim(V_{ij}) = \mathrm{gr}\,(p_i)n_{ij} = \mathrm{gr}\,(q_i)n_{ij}$ de donde deducimos que la dimensión de V es $n = \sum_{ij} \mathrm{gr}\,(q_i)n_{ij}$.

La unicidad se deduce de la unicidad en el Teorema de Estructura. □

Lema 0.5.4. *Para cualquier $\lambda \in \Bbbk$, se tiene $Z(T, v) = Z(T + \lambda id_V, v)$.*

Demostración. Es claro que alcanza con probar una inclusión (la otra se deduce tomando $-\lambda$ en lugar de λ). Para cada $w \in Z(T, v)$, existe $p \in \Bbbk[x]$ tal que $w = p(T)(v)$. Sea $q(x) := p(x - \lambda)$. Si $S = T + \lambda id_V$, se tiene $q(S) = p(S - \lambda id_V) = p(T)$, por lo que $w = q(S)(v) \in Z(S, v)$. □

Corolario 0.5.5 (Forma canónica de Jordan)**.** *Sean $\Bbbk$ un cuerpo y $A \in M_n(\Bbbk)$ tal que el polinomio minimal es producto de polinomios de grado 1 con coeficientes en $\Bbbk$. Entonces A es semejante a una matriz de la forma*

$$J = \begin{pmatrix} \begin{matrix} J_{11} & 0 & \cdots & 0 \\ 0 & J_{12} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{1k_1} \end{matrix} & 0 & & 0 \\ 0 & \begin{matrix} J_{21} & 0 & \cdots & 0 \\ 0 & J_{22} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{2k_2} \end{matrix} & & 0 \\ & & \ddots & \\ 0 & 0 & & \begin{matrix} J_{t1} & 0 & \cdots & 0 \\ 0 & J_{t2} & & 0 \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{tk_t} \end{matrix} \end{pmatrix},$$

donde para cada $i \in \{1, \ldots, t\}, j \in \{1, \ldots, k_i\}$, se tiene que

$$J_{ij} = \begin{pmatrix} \lambda_i & 0 & \cdots & \cdots & 0 \\ 1 & \lambda_i & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda_i & 0 \\ 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix},$$

para cierto $\lambda_i \in \Bbbk$.

Más aún, la matriz J es única a menos de reordenaciones de los bloques J_{ij}.

Demostración. Consideremos los V_{ij} de la descomposición del Teorema 0.5.3 y para cada par (i, j), sea $T_{ij} = T_{|V_{ij}}$. Sabemos, por el dicho Teorema, que el polinomio minimal de T_{ij} es de la forma $q_i^{n_{ij}}$, para cierto $q_i \in \Bbbk[x]$ mónico e irreducible. Pero por hipótesis, dicho irreducible debe ser de grado 1 y por tanto de la forma $x - \lambda_i$, para cierto $\lambda_i \in \Bbbk$.

Consideremos entonces $S_{ij} : V_{ij} \to V_{ij}$ definida por $S_{ij} = T_{ij} - \lambda_i \operatorname{Id}_{V_{ij}}$. Por el Lema 0.4.5, se tiene que V_{ij} es S_{ij}-cíclico, y por lo tanto admite una base $C_{ij} = \{v_{ij}, S_{ij}(v_{ij}), S_{ij}^2(v_{ij}), \ldots, S_{ij}^{n_{ij}-1}(v_{ij})\}$. Como además $S_{ij}^{n_{ij}} = 0$, tenemos que la matriz asociada a S_{ij} en dicha base es

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Como $T_{ij} = S_{ij} + \lambda_i \operatorname{Id}_{V_{ij}}$, la matriz asociada a T_{ij} en la base C_{ij} es

$$\begin{pmatrix} \lambda_i & 0 & \cdots & \cdots & 0 \\ 1 & \lambda_i & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda_i & 0 \\ 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix}$$

Tomando la base $C = \bigcup_{i,j} C_{ij}$ (ordenando los pares (i, j) según el orden lexicográfico), se obtiene que la matriz asociada a T en la base C es la buscada.

La unicidad se deduce de la unicidad en el Teorema 0.5.3. □

Definición 0.5.1. La matriz R del Corolario 0.5.5 se dice *forma canónica de Jordan* de la matriz A en el cuerpo $\Bbbk$.

Observaciones 0.5.1.

1. La forma de Jordan sobre un cuerpo $\Bbbk$ no siempre está definida.
2. Si A es diagonalizable semejante a D, la forma canónica de Jordan de A está definida y es D (puesto que el polinomio minimal es el producto de los polinomios $x - d_i$, variando d_i en todas las entradas distintas de la diagonal de D).
3. Si A es nilpotente, la forma canónica de Jordan de A está definida (puesto que su polinomio minimal es de la forma X^n y por tanto se descompone en producto de polinomios irreducibles de grado 1).

Ejemplos 0.5.1. 1. Sean $\Bbbk$ un cuerpo y $T : \Bbbk^5 \to \Bbbk^5$ definida por $T(a, b, c, d, e) = (2b, -2a, a+5c, a+b+c-2d, 5e)$. Hallemos, si corresponde, la forma de Jordan de T en los casos $\Bbbk = \mathbb{R}$ y $\Bbbk = \mathbb{C}$.

La matriz asociada a T en la base canónica es

$$A = \begin{pmatrix} 0 & -2 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 5 & 1 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

y por tanto el polinomio característico de T es $\chi_T = (x^2 + 4)(5 - x)^2(-2 - x)$. Calculemos el polinomio minimal m_T. Tenemos dos posibilidades

$$m_T = \chi_T \text{ o } m_T = (x^2 + 4)(5 - x)(-2 - x).$$

Ahora bien se tiene $(A^2 + 4Id)(5Id - A)(-2Id - A) = 0$, por lo que $m_T = (x^2 + 4)(5 - x)(-2 - x)$. En el caso $\Bbbk = \mathbb{C}$, como A es diagonalizable, su forma de Jordan es

$$J_{\mathbb{C}} = \begin{pmatrix} 2i & 0 & 0 & 0 & 0 \\ 0 & -2i & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}.$$

.

2. Supongamos ahora que $T : \Bbbk^5 \to \Bbbk^5$ es tal que $\chi_T = (x - 2)^3(x + 5)^2 = m_T$. Tanto en el caso $\Bbbk = \mathbb{C}$ como en el caso $\Bbbk = \mathbb{R}$ se tiene que la matriz de Jordan es

$$J = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -5 & 0 \\ 0 & 0 & 0 & 1 & -5 \end{pmatrix}.$$

Supongamos que $B = \{v_1, v_2, v_3, v_4, v_5\}$ es una base para R. Esto es $T(v_1) = v_2, T(v_2) = v_3, T(v_3) = 8v_1 - 12v_2 + 6v_3, T(v_4) = v_5, T(v_5) = -25v_4 - 10v_5$. Hallemos una base para J.

Es fácil ver que $w_3 = 4v_1 - 4v_2 + v_3$ y $w_5 = 5v_4 + v_5$ son vectores propios asociados respectivamente a 2 y -5 (para hallarlos se impuso la condición de vector propio a combinaciones lineales de v_1, v_2 y v_3 y a de v_4 y v_5 respectivamente). Para completar la base, buscamos w_1 y w_2 combinaciones lineales de v_1, v_2 y v_3 tales que $T(w_1) = 2w_1 + w_2$ y $T(w_2) = 2w_2 + w_3$ y además $w_4 = \lambda v_4 + \mu v_5$ tal que $T(w_4) = -5w_4 + w_5$.

Hallemos primero w_4. La condición para su transformado implica $\lambda v_5 + \mu(-25v_4 - 10v_5) = -5\lambda v_4 - 5\lambda v_5 + 5v_4 + v_5$, lo que implica

$$-25\mu = -5\lambda + 5, \quad \lambda - 10\mu = -5\lambda + 1,$$

esto es $\lambda - 5\mu = 1, \quad 6\lambda - 10\mu = 1$ y por lo tanto $\lambda = \frac{1}{4}, \mu = \frac{-3}{20}$. Se obtuvo $w_4 = \frac{1}{4}v_4 - \frac{3}{20}v_5$.
Análogamente, se tiene $w_2 = 2v_1 - 3v_2 + v_3$ y $w_1 = 3v_1 - 3v_2 + v_3$.
Así, si la base original B es la base canónica de $\mathbb{C}^5$, la base de Jordan es

$$\{(3, -3, 1, 0, 0), (2, -3, 1, 0, 0), (4, -4, 1, 0, 0), (0, 0, 0, 5, 1), (0, 0, 0, \frac{1}{4}, \frac{3}{20})\}.$$