Apuntes de Álgebra Conmutativa

Paco Mora

15 de diciembre de 2022

Índice general

CAPÍTULO 1

Tema 1

Ejercicio 1. ***Ejercicio Propuesto***

Sea $A = \mathbb{Z}_n$, con n entero >1 y $\overline{r} \in \mathbb{Z}_n$. Demostrar:

- $\overline{r}$ *cancelable* $\iff$ $\overline{r}$ *invertible* $\iff$ $mcd(r,n) = 1$
- $\overline{r}$ *nilpotente* $\iff$ *todos los divisores primos de* n *dividen a* r.

La siguiente proposición generaliza el ejercicio anterior.

Proposición 1.1. *Sea A un anillo finito y sea $a \in A$. Entonces a es cancelable sii es invertible.*

Demostración

Definimos

$$\lambda_n : A \to A \qquad \lambda_n(x) = ax \ \forall x \in A$$

Es inyectiva, $\lambda_n(x) = \lambda_n(y) \iff ax = ay \implies_{a\ cancel.} x = y$

Por lo tanto, y como A es finito, λ_n es biyectiva y $1 \in Im(\lambda_n) \iff \exists b \in A \mid \lambda_n(b) = 1$

$\square$

Proposición 1.2. *A reducido $\iff$ Nil(A) = $\{$elem nilpotentes de $A\} = \{0\}$*

Demostración

$\implies$

A reducido sii $\forall a \in A$, $a^2 = 0 \implies a = 0$

$\impliedby$

Por reduc. al absurdo, supongamos $b \in Nil(A)\backslash\{0\} \implies \exists n > 0$ (mínimo) con $b^n = 0 \implies b^{n-1} \neq 0$

Pero entonces, $(b^{n-1})^2 = b^{2n-2} = 0$ y $2n-2 \geq n$ para $n \geq 2$, luego llegamos a una contradicción.

$\square$

Ejercicio 2. ***Ejercicio Propuesto***

$\mathbb{Z}_n$ es un anillo reducido $\iff$ n es libre de cuadrados.

Demostración del 1.9(ii)

Demostración

a/b y $a/c \implies \exists b', c' \in D/\ ab' = b,\ ac' = c\ldots$ Sean ahora $r, s \in D$ arbitrarios y veamos que $a/rb + sc$

$$rb + rc = r(ab) + s(ac') = arb' = asc' = a(rb' + sc') \implies a|rb + sc \implies \not{b}1 = \not{b}(dc)$$

$\square$

Ejercicio 3. ***Ejercicio propuesto***

Sean $G_1, G_2 \subset A$. Demostrar que $(G_1)(G_2) = (G_1 \cdot G_2)$. En particular, el producto de ideales principales es un ideal principal.

Observación

$IJ \subset I \cap J$ (estricto en general: $A = \mathbb{Z},\ I = (2),\ J = (4),\ IJ = (8),\ I \cap J = (4)$)

Ejemplo 4. ***Aplicación del teorema de la correspondencia***

Los ideales de $\mathbb{Z}_n$ están en correspondencia con los divisores positivos de n.

$$\mathcal{L}(\mathbb{Z}_n) \to \{d > 0 :\ d/n\}$$

Pero los ideales de $\mathbb{Z}_n$ son isomorfos a $\{I \trianglelefteq \mathbb{Z}\ :\ n\mathbb{Z} \subset I\}$ por el teorema de la correspondencia, entonces:

$$\{I \trianglelefteq \mathbb{Z}\ :\ n\mathbb{Z} \subset I\} = \{d\mathbb{Z} \trianglelefteq \mathbb{Z} :\ n\mathbb{Z} \subset d\mathbb{Z}\} = \{d\mathbb{Z} :\ d|n\} \cong \{d > 0 :\ d/n\}$$

Proposición 1.3. ***Proposición 1.31 extendido*** *(la prueba es la de los apuntes) Sean $A, B_1, ..., B_n$ anillos y sean $g_i : A \to B_i$ homomorf. de anillos.*

1. *$\phi : A \to B_1 \times ... \times B_n$, dado por $\phi(a) = (g_1(a), ..., g_n(a))$ es un homomorf. de anillos con núcleo $\bigcap_{i=1}^n \mathrm{Ker}(g_i)$*
2. *Si los $\mathrm{Ker}(g_i)$ son comaximales dos a dos, entonces se verifica:*
   a) $\mathrm{Im}(\phi) = \mathrm{Im}(g_1) \times ... \times \mathrm{Im}(g_n)$
   b) $\mathrm{Ker}(\phi) = \mathrm{Ker}(g_1) \cdots \mathrm{Ker}(g_n)$
   c) *Se tiene un isom. de anillos:* $\dfrac{A}{\mathrm{Ker}(g_1) \cdots \mathrm{Ker}(g_n)} \cong \mathrm{Im}(g_1) \times ... \times \mathrm{Im}(g_n)$

Demostración

1.

$$\mathrm{Ker}(\phi) = \{a \in A :\ (g_1(a), ..., g_n(a)) = (0, ..., 0)\} = \{a \in A :\ g_i(a) = 0\ \forall i\} = \cap_{i=1}^n \mathrm{Ker}(g_i)$$

2.
2.b

Si los $\mathrm{Ker}(g_i)$ son comaximales dos a dos entonces:

$$\mathrm{Ker}(\phi) = \mathrm{Ker}(g_1) \cdots \mathrm{Ker}(g_n)$$

Con lo que tenemos 2b).
2.a

Si $(b_1, ..., b_n) \in \text{Im}(\phi) \implies (b_1, ..., b_n) = \phi(a) = (g_1(a), ..., g_n(a))$ para algún $a \in A \implies b_i \in \text{Im}(g_i)\ \forall i$. Por tanto, $(b_1, ..., b_n) \in \text{Im}(g_1) \times ... \times \text{Im}(g_n)$

Si probamos ahora que $(0, ..., x_i, 0, ..., 0) \in \text{Im}(\phi)\ \forall x_i \in \text{Im}(g_i)$, entonces toda n-upla $(x_1, ..., x_n) \in \text{Im}(\phi)$ en $\text{Im}(\phi_1) \times ... \times \text{Im}(\phi_n)$. Como los núcleos son comaximales dos a dos.

$$\text{Ker}(g_i) + (\cap_{j \neq i} \text{Ker}(g_j) = A \implies 1 = a + b,\ a \in \text{Ker}(g_i),\ b \in \cap_{j \neq i} \text{Ker}(g_j))$$

Como $x_i \in \text{Im}(g_i) \implies \exists u \in A:\ g_i(u) = x_i$, entonces:

$$x_i = 1 \cdot x_i = (a + b)g_i(u) = g_i((a + b)u)$$

Luego entonces:

$$\phi(bu) = (g_1(bu), ..., g_i(bu), ..., g_n(bu)) = (0, ..., 0, g_i(bu), 0, ..., 0)$$

$$x_i = g_i(u) = g_i(au + bu) = \cancel{g_i(a)g_i(u)} + g_i(bu)$$

Con lo que queda demostrado 2.b.
2.c.

Basta utilizar 2.a), 2.b) y el primer teorema de isomorfía.

□

Definición 1.1. ***Conjunto inductivo***

*Un **conjunto inductivo** es un conjunto ordenado S tal que todo subconjunto totalmente ordenado no vacío tiene una cota superior en S*

Lema 1.4. ***Lema de Zorn***

Todo conjunto inductivo no vacío tiene un elemento maximal.

Demostración

Fijemos $I \trianglelefteq A,\ I \neq A$ ideal propio.

$$S_I = \{J \trianglelefteq A :\ J \text{ ideal propio e } I \subset J\}$$

S_I es inductivo y $\neq \emptyset (I \in S_I)$

Sea Y un subconjunto totalmente ordenado $\neq \emptyset$ de S_I. Tomo $m = \bigcup_{J \in T} J$. Porbemos que m es un ideal propio tal que $I \subset m$. Lo que implica que $m \in S_I$.

Sean $a, b \in m \implies \begin{cases} a \in \bigcup_{J \in T} J \iff \exists J \in T:\ a \in J \\ b \in \bigcup_{J \in T} J \iff \exists J' \in T:\ b \in J' \end{cases}$

Si tomamos por ejemplo que $J \subset J'$, entonces $a, b \in J' \implies a - b \in J' \implies a - b \in m$

Notemos entonces que un elemento maximal de S_I es también un ideal maximal.

□

Ejercicio 5. *$I, P \trianglelefteq A$, siendo P primo. Probar que existe un primo minimal sobre I, pongamos q tal que $q \subset P$*

Lema 1.5. *Lema de Krull*

A anillo, $I \trianglelefteq A$ y $S \subset A$ un subconjunto multiplicativo. Suponemos que $I \cap S = \emptyset$ y consideremos $\mathcal{L}_{I,S} = \{J \trianglelefteq A : \; I \subset J, \; J \cap S = \emptyset\}$. Se verifica:

1. *$\mathcal{L}_{I,S}$ es un conjunto inductivo.*
2. *Cualquier elemento maximal de $\mathcal{L}_{I,S}$ es un ideal primo.*

Demostración

1.

Hemos de probar que si $\mathcal{J} \subset \mathcal{I}_{I,S}$ es un subconjunto totalmente ordenado $\neq \emptyset \implies$ tiene una cota superior en $\mathcal{L}_{I,S}$.

Habría que comprobar que $\widetilde{J} = \bigcup_{J \in \mathcal{J}} J$ es un ideal.

Como tenemos que $I \subset \widetilde{J}$ y $S \cap \widetilde{J} = S \cap (\bigcup J) = \bigcup_{J \in \mathcal{J}} (S \cap J) = \emptyset$

Entonces $\widetilde{J}$ es una cota superior de $\mathcal{J}$ en $\mathcal{L}_{I,S}$.

2.

Sean $a, b \in A$ tales que $ab \in P$. Por reducc. al absurdo, supongamos que $a \notin P$ y $b \notin P$. Entonces:

$$\left\{ \begin{array}{c} P \subsetneq P + (a) \\ P \subsetneq P + (b) \end{array} \right\} \implies P + (a), P + (b) \notin \mathcal{L}_{I,S} \iff \left\{ \begin{array}{c} (P + (a)) \cap S \neq \emptyset \\ (P + (b)) \cap S \neq \emptyset \end{array} \right\}$$

Sean entonces $s \in (P + (a)) \cap S$ y $s' \in (P + (b)) \cap S$. Entonces:

$$\left\{ \begin{array}{l} s = p + ar \\ s' = p' + br' \end{array} \right. \qquad p, p' \in P, \; r, r' \in A$$

$$ss' = (p + ar)(p' + br') = pp' + pbr' + arp' + abrr' \in P \implies P \cap S \neq \emptyset$$

Con lo que llegamos a una contradicción

$\square$

Proposición 1.6. *Sea A un anillo e $I \trianglelefteq A$ un ideal **propio**. Son equivalentes:*

1. *Si $a \in A$ y $a^n \in I$, para algún $n > 0$, entonces $a \in I$*
2. *Śi $a \in A$ y $a^2 \in I$, entonces $a \in I$*
3. *I es una intersección de ideales primos.*
4. *I es la intersección de los ideales primos minimales sobre I.*

Demostración

$1 \implies 2.$

Directa.

$2 \implies 1$

Si $n = 1 \implies a' = a \in I$, podemos suponer que $a \notin I$ y que existe $n > 1$, $a^n \in I$ tal que $a^{n-1} \notin I$. Entonces tenemos:

$$(a^{n-1})^2 = a^{2n-2} = \underbrace{a^n}_{\in I}\underbrace{a^{n-2}}_{\in A} \implies (a^{n-1})^2 \in I \implies a^{n-1} \in I$$

Con lo que tenemos una contradicción y $a \in I$.

$4 \implies 3$.

Directa.

$3 \implies 4$.

Supongamos que $\exists (P_\lambda)_{\lambda\in\Lambda}$ ideales primos tales que $I = \bigcap_{\lambda\in\Lambda} P_\lambda$

$$\forall\lambda \in \Lambda,\ I \subset P_\lambda \implies {}^1\exists Q_\lambda \text{ primo minimal sobre } I \text{ tal que } I \subset Q_\lambda \subset P_\lambda \implies$$
$$\implies I \subset \bigcap_{\lambda\in\Lambda} Q_\lambda \subset \bigcap_{\lambda\in\Lambda} P_\lambda = I \implies I = \cap_{\lambda\in Q_\lambda}$$
$$I \subset \bigcap_{\substack{Q\in\operatorname{Spec}(A)\\ Q\ minimal\ I}} Q \subset \bigcap_{\lambda\in\Lambda} Q_\lambda = I$$

Con lo que tenemos 4.

$3 \implies 2$.

Si $a^2 \in I = \bigcap_{\lambda\in\Lambda} P_\lambda \iff a^2 \in P_\lambda,\ \forall\lambda\in\Lambda \implies a \in P_\lambda,\ \forall\lambda\in\Lambda \iff a \in \bigcap_{\lambda\in\Lambda} P_\lambda = I$

$1 \implies 4$.

Sean $\mathcal{Q} = \{\text{ideales primos minimales sobre } I\}$. Queremos probar que $I = \cap_{Q\in\mathcal{Q}} Q$. La inclusión $\subset$ es directa.

Supongamos ahora que $I \subsetneq \bigcap_{Q\in\mathcal{Q}} Q \implies$ tomamos $x \in \cap_{Q\in\mathcal{Q}} Q$ tal que $x \notin I$.

Como $x \notin I \implies x^n \notin I,\ \forall n \geq 0$. Aplicamos ahora el lema de Krull con I y $S = \{x^n :\ n \geq 0\}$.

Entonces $\mathcal{L}_{I,S} = \{J \trianglelefteq A :\ I \subset J,\ J \cap S = \emptyset\}$ tiene un elemento maximal, pongamos P, que es primo. Entonces:

$$\left\{\begin{array}{l} S \cap P = \emptyset \\ I \subset P \end{array}\right\} \implies {}^2\exists Q \text{ primo minimal sobre } I:\ I \subset Q' \subset P \implies S \cap Q' = \emptyset$$

Con lo que llegamos a una contradicción porque $x \in Q'$

□

Definición 1.2. ***Ideal radical***

Un ideal que cumpla las condiciones de la anterior proposición se dice que es ***radical****.*

Definición 1.3. ***Radical de un ideal***

Sea $I \trianglelefteq A$ *ideal propio,* $\sqrt{I} := \{x \in A :\ x^n \in I, \quad \textit{para algún } n > 0\}$

[1] Por el último ejercicio propuesto.
[2] Por el ejercicio de nuevo.

Proposición 1.7. ***Sustituye al Corolario 1.4.6***

Dado $I \subsetneq A$ ideal propio, el subconjunto $\sqrt{I}$ es un ideal radical de A y puede ser descrito por cada una de las siguientes formas equivalentes:

1. *El menor ideal radical que contiene a I.*
2. *La intersección de todos los ideales radicales que contienen a I.*
3. *La intersección de todos los ideales primos que contienen a I.*
4. *La intersección de todos los ideales primos minimales que contienen a I.*

Demostración

Vemos primero que $\sqrt{I}$ es un ideal radical de A.

Hemos de probar:

$$\begin{cases} \left.\begin{array}{l} a)\ x+y \in \sqrt{I}\ \forall x,y \in \sqrt{I} \\ b)\ ax \in \sqrt{I}\ \forall x \in \sqrt{I},\ a \in A \end{array}\right\} \textit{ideal} \\ c)\ Si\ a^n \in \sqrt{I},\ con\ n > 0 \implies a \in \sqrt{I} \end{cases}$$

Vemos en primer lugar b):

$$(ax)^n = a^n x^n \implies (Como\ x^n \in I,\ a^n x^n \in I) \implies (ax)^n \in I \implies ax \in \sqrt{I}$$

a) se demuestra utilizando el binomio de Newton:

$$y, x \in \sqrt{I} \implies \exists m, n > 0 :\ x^m \in I,\ y^n \in I$$

Sin pérdida de generalidad, supongamos $m = n$

$$(x+y)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} x^i y^{2n-i} \in I \implies x + y \in I$$

Para ver c), sea ahora $a^n \in \sqrt{I} \implies \exists m > 0 :\ (a^n)^m \in I \implies a^{nm} \in I \implies a \in \sqrt{I}$.

Con lo que $\sqrt{I}$ es un ideal radical.

1.

Sea $J \trianglelefteq A$ ideal radical y propio tal que $I \subset J$. Queremos ver que $\sqrt{I} \subset J$.

Sea $x \in \sqrt{I} \implies \exists n > 0 :\ x^n \in I \implies x^n \in J \implies_{J\ radical} x \in J$

2.

Es consecuencia inmediata de 1.

3.

Sea $\mathcal{V}(I) = \{P \in \operatorname{Spec}(A) :\ I \subset P\} \implies ?\sqrt{I} = \bigcap_{P \in \mathcal{V}(I)} P$.

La inclusión $\subset$ es directa con la afirmación 1 y por ser la intersección un ideal radical. Para la otra, sabemos que $\sqrt{I} =$ intersección de los ideales primos minimales sobre $\sqrt{I}$. Entonces:

$$\sqrt{I} = \bigcap_{\substack{Q \in \operatorname{Spec}(A) \\ Q\ minimal/\sqrt{I}}} Q \supseteq \bigcap_{P \in \mathcal{V}(I)} P$$

Luego ya tenemos la igualdad.

4.

Se demuestra aplicando el ejercicio.

□

Ejemplo 6. *Tomamos el caso* $(I) = 0$

$$\sqrt{(0)} = \{x \in A: \ x^n = 0\} = \{\textit{nilpotentes de } A\} =: \operatorname{Nil}(A)$$

1. $\operatorname{Nil}(A)$ *es el menor ideal radical de* A
2. $\operatorname{Nil}(A)$ *es la intersección de todos los ideales radicales de* A.
3. $\operatorname{Nil}(A)$ *es la intersección de todos los ideales primos de* A.
4. $\operatorname{Nil}(A) = \bigcap_{P \in \operatorname{MinSpec}(A)} P$

Ejercicios

Ejercicio 2.

$$x, y \in \mathcal{U}(A) \implies xyy^{-1}x^{-1} = 1 \implies xy \in \mathcal{U}(A)$$

$$xy \in \mathcal{U}(A) \implies \exists w \in A: \ xyw = 1 \implies \begin{cases} x^{-1} = yw \\ y^{-1} = wx \end{cases}$$

Ejercicio 3.

En este ejercicio hay una errata, está por solucionar

Sabemos que en un anillo finito, las unidades y los elementos cancelables son los mismos. Luego $|\mathcal{U}(\mathbb{Z}_n)| = |\{\textit{cancelables}\}|$. *Además sabemos que* $|\{\textit{divisores de cero}\}| = n - |\mathcal{U}(\mathbb{Z}_n)|$. *Además sabemos que:*

$$|\mathcal{U}(\mathbb{Z})_n| = \phi(n) = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1)$$

Entonces,

$$|\{\textit{divisores de cero}\}| = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 \cdots p_r - \prod_{i=1}^{r}(p_i - 1))$$

Vemos entonces el cardinal de $\operatorname{Nil}(\mathbb{Z}_n)$*:*

$$\overline{k} = k + n\mathbb{Z} \in \operatorname{Nil}(\mathbb{Z})_n \iff \textit{todos los } p_i \textit{ dividen a } k$$

$$\overline{k} \in \operatorname{Nil}(\mathbb{Z})_n \iff \exists t > 0: \ \overline{k}^t = \overline{0} \textit{ en } \mathbb{Z}_n \iff \exists t > 0: \ n / k^t \implies \textit{todos los } p_i \textit{ dividen a } k$$

Recíprocamente:

$$k = p_1^{\beta_1} \cdots p_r^{\beta_r}, \textit{ con } 0 < \beta_i \leq \alpha_i \ \forall i = 1, ..., r$$

$$|\operatorname{Nil}(\mathbb{Z})_n| = \alpha_1 \cdots \alpha_r$$

Ejercicio 4.

$$\mathcal{U}(\mathbb{Z}_{24}) = \{\overline{k}: \ \operatorname{mcd}(k, n) = 1\} = \{\textit{cancelables}\} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}\}$$

$$\{divisores\ de\ cero\} = \mathbb{Z}_{24} \setminus \mathcal{U}(\mathbb{Z}_{24})$$

Ejercicio 6.

Recordemos primero que $p \in A$ es primo sii (p) es un ideal primo.

$f : A \to B$ *homomorf. Si a satisface (P),¿ $f(a)$ cumple (P)?*

Apartado a)

Si $a \in \mathcal{U}(A) \implies \exists a^{-1} \in A : \ a \cdot a^{-1} = 1 \implies f(a)f(a^{-1}) = f(1) = 1 \implies f(a) \in \mathcal{U}(B)$.

Apartado b)

Tomando $\mathbb{Z} \to \dfrac{\mathbb{Z}[X]}{(2x)}$ homomorfismo inyectivo. El 2 es cancelable en $\mathbb{Z}$ pero no lo es en el anillo destino.

Apartado c)

Sea $a \in A$ divisor de 0 $\implies \exists b \in A \setminus \{0\} : \ ab = 0 \implies f(a)f(b) = 0$

Cuando f es inyectiva: sí, porque $f(b) \neq 0$. En otro caso:

Sean $m, n > 1, \ mn\mathbb{Z} \subset n\mathbb{Z} \implies$ tomamos un homomorfismo de anillos suprayectivo:

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \to \mathbb{Z}\frac{\mathbb{Z}}{n\mathbb{Z}}$$

Tomando m, n tales que $\mathrm{mcd}(n, m) = 1$ tenemos que $\overline{m}$ es divisor de cero pero su imagen, $[m] \in \mathcal{U}(\mathbb{Z}_n)$

Apartado d)

Si $a \in A$, existe un exponente $n > 0$ tal que $a^n = 0 \implies f(a)^n = f(a^n) = 0$, entonces $f(a)$ es nilpotente.

Apartado e)

De forma parecida al apartado anterior, vemos que si $e = e^2$ en A, al aplicar f tenemos que $f(e) = f(e)^2 \implies f(e)$ es idempotente.

Apartado f)

Basta tomar la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$ para tener un contraejemplo (no suprayectivo). Para el caso suprayectivo planteamos un ejercicio:

Ejercicio: *Sea $\overline{k} = kp^t\mathbb{Z}$ es irreducible en $\mathbb{Z}_{p^t} \iff \overline{k} = \overline{pu}$, siendo $\overline{u} \in \mathcal{U}(\mathbb{Z}_{p^t})$. Más generalmente: Sea A un anillo y $p \in A$ tales que (p) es el único ideal maximal de A- Entonces los elementos irreducibles de A son los de la forma pu, siendo $u \in \mathcal{U}(A)$ (p es el único irreducible de A salvo asociados)*

Construimos en base a este ejercicio el homomorfismo suprayectivo formado por la proyección $\mathbb{Z} \to \mathbb{Z}_{p^t}$. Dado $q \neq p$ primo, su imagen es $\overline{q} \in \mathcal{U}(\mathbb{Z}_{p^t}) \implies \overline{q}$ no es irreducible.

Apartado g)

Ejercicio: *Sea A un dominio y $p \in A$. Si p es primo entonces es irreducible. Cuando A es un DIP, se verifica también el recíproco.*

Como los contraejemplos del apartado anterior parten de $\mathbb{Z}$ y los irreducibles y los primos son iguales en $\mathbb{Z}$, podemos usar los mismos contraejemplos en este apartado.

Vamos a resolver ahora el primero de los ejercicios planteados:

Ejercicio: *Sea $\overline{k} = kp^t\mathbb{Z}$ es irreducible en $\mathbb{Z}_{p^t} \iff \overline{k} = \overline{pu}$, siendo $\overline{u} \in \mathcal{U}(\mathbb{Z}_{p^t})$. Más generalmente: Sea A un anillo y $p \in A$ tales que (p) es el único ideal maximal de A- Entonces los elementos irreducibles de A son los de la forma pu, siendo $u \in \mathcal{U}(A)$ (p es el único irreducible de A salvo asociados)*

Dado $p = ab$, veamos si p es irreducible. Supongamos que $a \notin \mathcal{U}(A) \implies (a) \trianglelefteq A \implies (a) \subset (p)$ porque (p) es el único ideal maximal. $\implies a = pa'$, siendo $a' \in A$

$$\implies p = ab = pa'b \iff p(1-a'b) = 0 \begin{cases} 1 - a'b \in \mathcal{U}(A) \text{ no, porque implicaría} \\ \quad \text{una contradicción } (p = 0) \\ 1 - a'b \notin \mathcal{U}(A) \end{cases}$$

$1 - a'b \notin \mathcal{U}(A) \implies (1-a'b) \subset (p)$, *pero no puede darse* $(a'b) \subset (p)$, *porque tendríamos*

$$1 = 1 - a'b + a'b \in (p) \implies a'b \in \mathcal{U}(A) \implies b \in \mathcal{U}(A)$$

Sea $q \in A$ irreducible $\implies q \notin \mathcal{U}(A) \iff (q) \ntrianglelefteq A \implies (q) \subset (p) \implies q = pu$, para algún $u \in A$

Vemos ahora los recíprocos.

Apartado a)

La inclusión de $\mathbb{Z}$ a $\mathbb{Q}$ y tomando $a = f(a) = 3$ tenemos un contraejemplo no suprayectivo, para el sobre, tomamos la proyecctión de $\mathbb{Z}$ en $\mathbb{Z}_3$.

Apartados b,c)

Basta aplicar el contrarrecíproco de $f(a)$ cancelable $\implies a$ cancelable y $f(a)$ divisor de $0 \implies a$ divisor de 0

Apartado d)

$f(a)$ *es nilpotente* $\iff f(a)$ *tal que* $\exists n > 0$ *tal que* $f(a)^n = 0 \implies f(a^n) = 0 \iff a^n \in \mathrm{Ker}(f)$.

Si f es inyectiva, sí se cumple la cadena de sii.

Si f es sobre, tomamos el contraejemplo de la proyección de $\mathbb{Z}$ en $\mathbb{Z}_n$ con un producto de primos

Apartado e)

De forma parecida al apartado anterior:

$$f(a) = f(a^2) \iff a - a^2 \in \mathrm{Ker}(f)$$

Si f es inyectiva, sí se cumple.

En el caso sobre, tomamos la proyección de $\mathbb{Z}$ en $\mathbb{Z}_6$, entonces 7 no es idempotente y $f(7) = \overline{1}$ no lo es.

Apartado f)

Para el caso sobre, tomamos la aplicación $\mathbb{Z} \to \mathbb{Z}_{p^t}$ y el elemento $(p^t + 1)p \rightsquigarrow \overline{p}$

La idea para obtener el caso inyectivo es tomar un elemento como $2 \cdot 3$ no irreducible, y llevar uno de sus factores a una unidad. Tomamos la aplicación:

$$\mathbb{Z} \hookrightarrow \mathbb{Z}\left[\frac{1}{2}\right] = \{q \in \mathbb{Q} : \ q = \frac{m}{2^r}, \ m \in \mathbb{Z}, \ r \geq 0\}$$

Dejamos como ejercicio ver que 3 es irreducible en $\mathbb{Z}[1/2]$

Ejercicio 7.

Apartado a)

Si $m < 0 \implies \mathcal{U}(\mathbb{Z}(\sqrt{m}))$ es finito.

$$N(a + b\sqrt{m}) = 1 \iff a^2 - mb^2 = 1 \iff a^2 + b\sqrt{-m}^2 = 1$$

$\implies$ *$(a, b\sqrt{-m})$ está en la circunferencia de centro $(0,0)$ y radio 1 y su 1ª componente a es entera.*

$$\implies \mathcal{U}(Z(\sqrt{m})) \subset \{a + b\sqrt{m} : \ (a, b\sqrt{-m}) \in \{(1,0), (-1,0), (0,1), (0,-1)\}\}$$

Observación

$$a = 0 \iff b\sqrt{-m} = \pm 1 \implies \begin{cases} b = \pm 1 \\ \sqrt{-m} = 1 \end{cases} \implies -m = 1 \implies m = -1$$

Luego $\mathcal{U}(\mathbb{Z}[\sqrt{m}]) = \{-1, 1\}$ salvo cuando $m = -1$ en que $\mathcal{U}(\mathbb{Z}(i)) = \{1, -1, i, -i\}$

Apartado b)

Supongamos que $|\mathcal{U}(\mathbb{Z}[\sqrt{m}])| > 2$ y cojamos $\alpha = a + b\sqrt{m} \neq \pm 1$

Tomamos $X := \{1, \alpha, \alpha^2, ...\}$ = el subgrupo multiplicativo de $\mathcal{U}(\mathbb{Z}[\sqrt{m}])$ generado porα.

Si X es finito $\implies \exists n > 0 : \ \alpha^n = 1$. Elegimos n mínimo con esa propiedad $\implies \alpha$ raíz $n-$ésima (primitiva) de 1.

Como $m > 0 \implies \alpha = a + b\sqrt{m} \in \mathbb{R} \implies \alpha = \pm 1$ (contradice que el que $\alpha \neq \pm 1$)

Apartado c)

Por las conclusiones tomadas en el apartado a). Se tiene que $\mathcal{U}(\mathbb{Z}(\sqrt{-11})) = \{1, -1\}$

Se trata de ver ahora que $x = 1 + \sqrt{-11}$ e $y = 1 - \sqrt{-11}$ son irreducibles. Como son conjugados, bastará con ver que uno solo de ellos es irreducible.

En primer lugar, no es cero ni una unidad. Pongamos $x = (a + b\sqrt{-11})(c + d\sqrt{-11})$. *Tomando normas:*

$$12 = N(x) = N(a + b\sqrt{-11})N(c + d\sqrt{-11})$$

Si ni $a + b\sqrt{-11}$ *ni* $c + d\sqrt{-11}$ *son unidades* $\implies$ *las combinaciones posibles de normas son* $(2, 6), (3, 4), (4, 3), (6, 2)$. *En cualquier caso, la norma de uno de ambos es 2 o 3. Sin pérdida de generalidad, vamos a suponer que la norma de* $(a + b\sqrt{-11})$ *es 2 o 3, en cualquiera de los casos un primo* p.

$$\{2, 3\} \ni p = N(a + b\sqrt{-11}) = a^2 + 11b^2 \implies_{b\ entero} b = 0 \implies a^2 = p$$

Lo cual es imposible porque a *es entero, hemos llegado a una contradicción y* x *es irreducible.*

Ahora tenemos que $xy = (1 + \sqrt{-11})(1 - \sqrt{-11}) = 12 = 2 \cdot 2 \cdot 3$

Basta ver ahora que 2 y 3 son irreducibles en $\mathbb{Z}[\sqrt{-11}]$

$$p = (a + b\sqrt{-11})(c + d\sqrt{-11}) \implies_{tomando\ normas} p^2 = N(a + b\sqrt{-11})N(c + d\sqrt{-11})$$

Supongamos que ninguno de estos dos es 1, tenemos que $N(a + b\sqrt{-11}), N(c + d\sqrt{-11}) = p$ *y aplicando un razonamiento como el anterior, tenemos que es imposible y entonces* p *es irreducible.*

Apartado d)

Nos preguntamos si cuando un primo entero $p > 1$, *¿ es irreducible en* $\mathbb{Z}[\sqrt{-3}]$*?*

Tomamos una factorización $p = (a + b\sqrt{-3})(c + d\sqrt{-3})$ *y tomamos normas:*

$$p^2 = N(a + b\sqrt{-3})N(c + d\sqrt{-3})$$

Entonces tenemos:

$$p \textit{ irreducible} \iff N(a + b\sqrt{-3}) = 1 \text{ ó} N(c + d\sqrt{-3}) = 1$$

$$p \textit{ no es irreducible} \iff N(a + b\sqrt{-3}) = p = N(c + d\sqrt{-3}) \iff {}^{a} N(a + b\sqrt{-3}) = p$$

Como conclusión, tenemos que $\mathbb{Z}$ *es irreducible en* $\mathbb{Z}[\sqrt{-3}]$ *sii la ecuación* $x^2 + 3y^2 = p$ *no tiene solución en* $\mathbb{Z} \times \mathbb{Z}$.

Basta aplicar ahora este resultado a los 4 números a los que nos piden comprobar si son o no irreducibles.

[a] utilizando la ecuación de antes y que $\mathbb{Z}$ es un dominio

Ejercicio 9.

Supongamos que (b, X) *es principal y tenemos* $f \in A[X] :\ (b, X) = (f) \implies$

$$\implies \begin{cases} X = f(X)g(X), \text{ con } g, h \in A[X] \\ b = f(X)h(X) \end{cases} \implies_{X=0} \begin{cases} 0 = f(0)g(0) \\ b = f(0)h(0) \end{cases} \quad \textit{(igualdades en A)}$$

Notemos que b *cancelable* $\implies f(0)$ *cancelable:*

Si fuese $f(0)$ no cancelable (= divisor de 0) $\implies$

$$\exists c \in A \setminus \{0\} : \; f(0)c = 0 \implies \left\{ \begin{array}{c} bc = 0 \\ c \neq 0 \end{array} \right\} \implies b \text{ no es cancelable (contradicción)}$$

$$f(0) \implies g(0) = 0 \implies g(X) = X \cdot g'(X) \implies X = f(X)g(X) = Xf(X)g'(X) \implies$$

$$\implies_{X \text{ cancelable en } A[X]} 1 = f(X)g'(X) \implies f \in \mathcal{U}(A[X]) \implies (b, X) = (f) = A[X]$$

Entonces $1 = br(X) + Xs(X)$ para ciertos $r, s \in A[X] \implies_{X=0} 1 = br(0) \implies b \in \mathcal{U}(A)$, lo cual es una contradicción ya que sabemos que b no es invertible.

Falta ver que (X, Y) no es principal en $A[X, Y]$

$$A[X, Y] \cong (A[Y])[X]$$

Y no es cancelable y no unidad en $A[X]$, basta aplicar ahora el ejercicio.

Ejercicio 10.

Apartado a)

$$IJ_1 = IJ_2 \not\Longrightarrow J_1 = J_2$$

Tomaremos $J_2 = 0$ y $I = J_1 = (\overline{2})$ en $\mathbb{Z}_4$

Apartado b) Enunciado modificado

Todo ideal principal en un dominio cancela (para el producto de ideales)

$I = (y)$ y tenemos que $IJ_1 = IJ_2 \implies ?J_1 = J_2$

Basta con probar que $J_1 \subset J_2$.

Sea $z \in J_1 \implies yz \in IJ_1 = IJ_2 \implies yz = \sum_{i=1}^{t} y_i z_i$

$$y_i \in I = (y) \implies y_i = a_i y \text{ , para algún } a_i \in A \implies yz = \sum_{i=1}^{t} (a_i y) z_i = y \sum_{i=1}^{t} a_i z_i$$

$$\implies z = \sum_{i=1}^{t} a_i z_i \implies z \in J_2$$

Ejercicio 11. *Este ejercicio no está resuelto pero es muy importante.*

Ejercicio 12. ***bis***

Sea $A = A_1 \times ... \times A_m$, donde los A_i son anillos locales (Ej1.21). Probar que los idempotentes de A son las $m-$uplas $(e_1, ..., e_m)$ tales que $e_i \in \{0, 1\}$ $\forall i = 1, ..., m$. Como aplicación, describir un método para calcular todos los elementos idempotentes de $\mathbb{Z}_n$,

para $n > 1$***. Particularizarlo a*** $\mathbb{Z}_{4200}$***.***

Utilizando el ejercicio 5.e), tenemos que $e = (e_1, ..., e_m)$ *es idempotente en* $A \iff e_i$ *es idempotente en* A $\forall i = 1, ..., m$

La primera parte se reduce a probar que si B *es un anillo local, entonces sus únicos idempotentes son 0,1.*

Demostración

Supongamos que $e = e^2 \in B,\ e \notin \{0, 1\} \implies e, 1-e$ *son idempotentes (1.12(b)) y* $e, 1-e \notin \mathcal{U}(B)$ *(1.12(c)). Por tanto* $(e), (1-e)$ *son ideales propios de* $B \implies (e), (1-e) \subset m :=$ *único ideal maximal de* B*. Entonces,* $(e) + (1-e) \subset m \implies 1 = e + (1-e) \in m$

Con lo que tenemos una contradicción porque $m \subsetneq B$

$\square$

Describimos el método: $n = p_1^{\mu_1} \cdots p_t^{\mu_t} \implies$ [a] $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\mu_1}} \times \mathbb{Z}_{p_t^{\mu_t}}$ *que lleva* $\overline{a} \hookrightarrow (\overline{a}, ..., \overline{a})$

Entonces en $\mathbb{Z}_{p^t}$*, el único ideal maximal es* $(\overline{p})$ *(p primo).*

Vemos el caso de $n = 4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$*, tomamos el isomorfismo de anillos:*

$$\mathcal{U} : \mathbb{Z}_{4200} \to \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_7$$

$$\overline{a} \hookrightarrow (a + 8\mathbb{Z}, a + 32\mathbb{Z}, a + 25\mathbb{Z}, a + 7\mathbb{Z})$$

Hay $2^4 = 16$ *idempotentes: Calculamos el idempotente* $\overline{e} \in Z_{4200}$ *tal que* $\phi(\overline{e}) = (\overline{1}, \overline{0}, \overline{1}, \overline{0})$

Luego se nos queda el sistema de congruencias:

$$\begin{cases} e \equiv 1 \ (mod\ 8) \\ e \equiv 0 \ (mod\ 3) \\ e \equiv 1 \ (mod\ 25) \\ e \equiv 0 \ (mod\ 7) \end{cases}$$

Las ecuaciones que son congruentes con 1 se pueden agrupar en $x \equiv \ (mod\ 200 = 8 \cdot 25)$*, de forma análoga nos queda,* $x \equiv \ (mod\ 21)$*.*

$$\begin{cases} x = 1 + 200t \\ x = 21s \end{cases} \implies 1 + 200t = 21s \implies 1 = 21s + 200(-t)$$

Y utilizando la identidad de Bézout y el algoritmo de Euclides obtendremos una solución, en este caso es $(s = -19,\ t = -2)$

[a] Teorema chino de los restos

Ejercicio 12.

Apartado a)

$$a \in (e) \iff a = ea$$

$\implies$

Clara.

$\Longrightarrow$

Sea $a \in (e) \implies a = ex$, *con* $x \in A \implies ea = e^2x = ex = a$

$$\left\{ \begin{array}{c} a = ea \\ b = eb \end{array} \right\} ab = e^2ab = eab$$

Si e *es una unidad, entonces* $e = 1$

$$e =^2 \implies 1 = e$$

Apartado c)

Sea $a \in (e) \cap (f) \implies \left\{ \begin{array}{l} a = ea \implies fa = fea = 0 \\ a = fa \end{array} \right\} \implies a = 0$

Y tenemos que $(e) + (f) = A$ *ya que* $e + f = 1$.

Como anillos (no ideales), tenemos el isomorfismo de anillos $A \to (e) \times (f)$ *dado por* $a \hookrightarrow (ae, af)$

Apartado d)

$$1 = e + f,\ e \in I,\ f \in J \implies e + f = 1 = 1^2 = (e+f)^2 = e^2 + \underbrace{2ef}_{I \cap J = \{0\}} + f^2 = e^2 + f^2$$

Hemos descompuesto el 1 como suma de elementos de I, J *de dos formas distintas. Como la suma es directa, tenemos entonces que* $e = e^2,\ f = f^2$. *Luego* e *es idempotente,* $f = 1 - e$ *y tenemos* $(e) \subset\ I,\ (1-e) \subset J$. *Falta ver que se da la igualdad:*

$$\text{Sea } x \in I \implies x = x \cdot 1 = x(e+f) = xe + \underbrace{\cancel{xf}}_{\in I \cap J = \{0\}}$$

Ejercicio 14. *Supongamos que* f *es suprayectivo y vamos a probar que si* $P \trianglelefteq B$ *y* $f^{-1}(P)$ *es primo (en A). Entonces* P *es primo en* B.

Usando el primer teorema de isomorfía, $\dfrac{A}{\operatorname{Ker}(f)} \cong B$*:*

$$\operatorname{Spec}(B) \to \operatorname{Spec}\left(\frac{A}{\operatorname{Ker}(f)}\right)$$

$$Q \hookrightarrow \overline{f}^{-1}(q) = \{a \in \frac{A}{\operatorname{Ker}(f)} :\ f(a) \in Q\} = \frac{f^{-1}(q)}{\operatorname{Ker}(f)}$$

Y utilizando 1.38.2 de los apuntes de Alberto tenemos la biyección:

$$\left\{ {}^{\textit{ideales primos que}}_{\textit{contienen a } A} \right\} \to \operatorname{Spec}(\frac{A}{\operatorname{Ker}(f)})$$

Esta biyección lleva $f^{-1}(P) \hookrightarrow \dfrac{f^{-1}(P)}{\mathrm{Ker}(f)} \in \mathrm{Spec}(\dfrac{A}{\mathrm{Ker}(f)})$

Ejercicio 17. ***Consideración previa general.***

Sea $I \lneq A$ *y queremos identificar* $(\overline{a}_{1,\dots,\overline{a}_m}) =$ *ideal de* A/I *generado por* $\{\overline{a}_1, \dots, \overline{a}_m\}$.

$$(\overline{a}_1, \dots, \overline{a}_m) = \frac{J}{I}, \text{ para cierto } J \trianglelefteq A: \; I \subset J$$

Sea ahora $J = (a_1, \dots, a_m) + I$, *tendremos que comprobar si:*

$$(\overline{a}_1, \dots, \overline{a}_m) =? \frac{(a_1, \dots, a_m) + I}{I}$$

La inclusión $\subset$ *es directa porque cada uno de los* $\overline{a}_i$ *se incluye en* $\dfrac{(a_1, \dots, a_m) + I}{I}$.

Para la inclusión $\supset$, *tenemos:*

$$\overline{z} \in \frac{(a_1, \dots, a_m) + I}{I} \implies z + I = b + y + I, \text{ con } b \in (a_1, \dots, a_r), \; y \in I \implies {}_{y \in I} z + I = b + I$$

Por tanto, todos los elementos de $\dfrac{(a_1, \dots, a_m) + I}{I}$ *son de la forma* $b + I = \overline{b}$, *donde* $b \in (a_1, \dots, a_m)$, *pero* $b = r_1 a_1 + \dots + r_m a_m$ *con* $r_i \in A \; \forall i = 1, \dots, m$. *Tomando ahora clases tenemos:*

$$\overline{b} = \overline{r}_1 \overline{a}_1 + \dots + \overline{r}_m \overline{a}_m \implies \overline{b} \in (\overline{a}_1, \dots, \overline{a}_m)$$

Observación:

Llamamos $B = \dfrac{K[X, Y, Z]}{(XY, XZ)}$, $A = K[X, Y, Z]$, $I = (XY, XZ)$.

Apartado a)

$$(\overline{X}, \overline{Y}) = \frac{(X, Y) + (XY, XZ)}{(XY, XZ)} \left({}^{Obs: \; (XY, XZ)}_{\subseteq (X, Y)} \right) = \frac{(X, Y)}{(XY, XZ)}$$

Apartado b)

Razonamiento parecido al apartado anterior:

$$(\overline{X}, \overline{Z}) = \frac{(X, Z)}{(XY, XZ)}$$

Apartado c)

Razonamiento como en a).

$$(\overline{Y}, \overline{Z}) = \frac{(Y, Z)}{(XY, XZ)}$$

Apartado d)

Razonamiento como en a).

$$(\overline{X}) = \frac{(X)}{(XY, XZ)}$$

Apartado e)

$$(\overline{Y}) = \frac{(Y) + (XY, XZ)}{(XY, XZ)} = \left(\substack{Obs:\ (XY) \\ \subseteq (Y)}\right) = \frac{(Y, XZ)}{XY, XZ}$$

Apartado f)

$$(\overline{Z}) = \frac{(Z) + (XY, XZ)}{(XY, XZ)} = \frac{(Z, XY)}{(XY, XZ)}$$

Usaremos ahora que P es primo $\iff$ B/P es dominio, tomaremos $P = J/I$ y $B = A/I$, lo que nos queda:

J/I es primo en A/I $\iff$ $\frac{A/I}{J/I}$ es dominio $\iff$ [a]A/J dominio.

Volvamos ahora a cada caso particular:

Apartado a)

$$\frac{(X, Y)}{(XY, XZ)} \text{ primo } \iff \frac{K[X, Y.Z]}{(X, Y)} \cong K[Z] \text{ dominio}$$

Apartado b,c)

Análogos al a).

Apartado d)

$$\frac{K[X, Y, Z]}{(X) \cong_{ejercicio} K[Y, Z]}$$

Apartado e)

$$\frac{K[X, Y, Z]}{(Y, XZ)} \text{ no es dominio porque } \overline{XZ} = \overline{0} \text{ y } \overline{X} \neq \overline{0} \neq \overline{Z}$$

Apartado f)

Análogo al anterior

[a]Segundo teorema de isomorfía

Ejercicio utilizado en el anterior ejercicio: Sea B anillo y $X_1, ..., X_n$ variables sobre B. Para cada subconjunto $J \subset \mathbb{N}_n = \{1, ..., n\}$ consideremos la composición de homomorfismos de anillos:

$$B[X_i : \ i \in \mathbb{N}_n] \hookrightarrow^i B[X_1, ..., X_n] \xrightarrow{\pi} \frac{B[X_1, ..., X_m]}{(X_j : j \in J)}$$

Probar que $\pi \circ i$ es un isomorfismo de anillos.

Ejercicio 18.

$$I + (x) = \{a + xf : \ a \in I, \ f \in A[X]\} = \{f \in A[X] : \ g(0) \in I\}$$

Se reduce a probar que cada uno es primo si y solo si A/I es dominio si y solo si $A[X]/I[X]$ es dominio si y solo si $A[X]/I + (x)$ es dominio.

Tenemos un homomorfismo de anillos:

$$\phi : \ \frac{A}{I} \to \frac{A[X]}{I + (x)} \ \textit{tal que} \ \overline{a} = a + I \hookrightarrow [a]$$

Claramente está bien definido y es homomorfismo de anillos (conserva suma y multiplicación).

Tenemos:

$$\frac{A[X]}{I + (x)} \ni [f(X)] = [f(0) + Xg(X)] = [f(0)] + \cancel{[Xg(X)]} = \phi(\overline{f(0)})$$

Luego ϕ es suprayectiva. Comprobamos la inyectividad.

$$\mathrm{Ker}(\phi) = \{\overline{a} = a + I : \ [a] = [0]\} = \{\overline{a} \in A/I : \ a \in I + (x)\} = \{\overline{a} \in A/I : \ ainI\} = \{\overline{0}\}$$

Por tanto ϕ es un isomorfismo de anillos. Con esto tenemos el apartado b) y la mitad del apartado a). Veamos ahora la relación entre A/I y $A[X]/I[X]$. Consideremos el homomorfismo:

$$\frac{A}{I} \to \frac{A[X]}{I[X]} \ \textit{dado por} \ \overline{a} \hookrightarrow [a]$$

A partir de este formamos:

$$\psi : \frac{A}{I}[X] \to \frac{A[X]}{I[X]} \ \textit{dado por} \ \psi : \sum_{i=1}^{n} \overline{a}_i X^i \hookrightarrow \sum_{i=1}^{n} [a_i][X]^i = \left[\sum_{i=0}^{n} a_i X^i\right]$$

Es directo ver que ψ es suprayectiva, y tenemos que:

$$\mathrm{Ker}(\psi) = \{\sum \overline{a}_i X^i : \sum_{i=0}^{n} a_i X^i \in I[X]\} \implies \mathrm{Ker}(\psi) = \{\sum_{i=0}^{n} \overline{a}_i X^i : \ a_i \in I \ \forall i = 0, 1, ..., n\} =$$

$$= \{\sum_{i=0}^{n} \overline{a}_i X^i : \overline{a}_i = \overline{0} : \ \forall i = 0, 1, 2, ..., n\} = \{\overline{0}\}$$

Como conclusión llegamos a que $A[X]/I[X] \cong \dfrac{A}{I}[X]$ lo que nos lleva a demostrar c). Porque $\dfrac{A}{I}[X]$ nunca será un cuerpo.

Ejercicio 19. *La última parte se queda como ejercicio planteado.*

$$0 = (-a)^n ?(1-b)^n = \sum_{i=0}^{n} b^i 1^{n-i} = 1 - nb + \binom{n}{2} b^2 + ... + \binom{n}{n-1}(-b)^{n-1} + (-b)^n \implies$$

$$\implies 1 = b(n - \binom{n}{2} b + ... - \binom{n}{n-1}(-b)^{n-2} + (-b)^{n-1})$$

Ejercicio 20. ***Notación modificada.***

Denotamos al radical de Jacobson de A como $J(A)$.

Apartado a)

Demostramos que es un si y solo si.

$\Longleftarrow$

Supongamos que $a \notin J(A)$:

$$\implies \exists M \in \operatorname{MaxSpec}(A) : \; a \notin M \implies M \subsetneq M + (a) \implies M + (a) = A \implies$$

$$1 = m + ra, \; m \in M, \; r \in A \implies m = 1 + (-r)a \in 1 + (a) \implies m \in \mathcal{U}(A) \implies A = (m) \subseteq \; M$$

Con lo que tenemos una contradicción ya que M es propio al ser maximal.

$\Longrightarrow$

Supongamos que $1 + (a) \nsubseteq U(A)$, entonces:

$$\implies \exists r \in A : \; q + ra \notin \mathcal{U}(A) \implies (1 + ra) \subseteq \; M \text{ para algún } M \text{ maximal}$$

$$\implies 1 = \underbrace{1 + ra}_{\in M} + \underbrace{(-r)a}_{\in J(A) \subseteq \; M} \implies 1 \in M$$

Y llegamos de nuevo a la misma contradicción, M es propio, luego no puede contener al 1 (sería el total).

Apartado b)

Sea e idempotente, $e = e^2 \in J(A)$. Por el apartado a). Tenemos que $1 - e \in \mathcal{U}(A)$ y sabemos por el problema 12 que $1 - e$ es idempotente. Además, por este ejercicio también sabemos que al ser unidad e idempotente, $1 - e = 1 \implies e = 0$.

Ejercicio 21. ***Apartado a)***

$\Longrightarrow$

Se trata de probar que $M = A \setminus \mathcal{U}(A)$. La inclusión $\subseteq$ es directa. Basta probar $\supseteq$: Si $a \in A \setminus \mathcal{U}(A) \implies (a)$ es un ideal propio $\implies (a) \subseteq M \implies a \in M$

$\Longleftarrow$

Si $I \subsetneq A$ *es ideal propio,* $I \subseteq \ A \setminus \mathcal{U}(A)$

Apartado b)
(ver ejercicio anterior)

Como $J(A) = M \implies 1 + M \subseteq \mathcal{U}(A)$. *Lo único que tenemos que ver es que sea subgrupo. Que sea cerrado para la multiplicación es trivial. Veamos que existen los inversos.*

Sea $m \in M \implies 1 + m \in 1 + M \subseteq \mathcal{U}(A) \implies$ *escribimos* $(1+m)^{-1} = 1 + m'$, *con* $m' \in A$. *Veamos que* $m' \in A$*:*

$$1 = (1+m)(1+m')$$

Apartado d)

$\overline{1} + m = \overline{1} + (\overline{3})$ *es un subgrupo multiplicativo de* $\mathcal{U}(\mathbb{Z}_{27})$

$$\overline{1} + (\overline{3}) = \{\overline{1+a} : \ a \in 3\mathbb{Z}\} = \{\overline{b} : \ b \equiv 1 \ (mod\ 3)\} = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}, \overline{13}, \overline{16}, \overline{19}, \overline{22}, \overline{25}\}$$

Vemos que lo genera $\overline{4}$*:*

$$< \overline{4} >= \{1, \overline{4}, \overline{16}, \overline{10}, ...\} \ (\textit{tamaño mayor que 4}) \implies \overline{1} + (\overline{3}) =< \overline{4} >$$

Ejercicio 22.

$$\mathbb{Z}_{(p)} = \{q \in \mathbb{Q} : \ q = \frac{a}{b}, \ donde\ p \not| b\}$$

Apartado a)

$$\mathcal{U}(\mathbb{Z}_{(p)}) = \{q \in \mathbb{Z}_{(p)} : \ q = \frac{a}{b}, \ con\ a \notin p\mathbb{Z}\}$$

Apartado b)

$\mathbb{Z}_{(p)}$ *anillo local con* $\mathbb{Z}_{(p)} \setminus \mathcal{U}(\mathbb{Z}_{(p)}) \ = m$ *el único idea maximal que está generado por* $\frac{p}{1} = p$

$$\mathbb{Z}_{(p)} \setminus \mathcal{U}(\mathbb{Z}_{(p)}) = p\mathbb{Z}_{(p)} = \{p\frac{a}{b} : \ \frac{a}{b} \in \mathbb{Z}_{(p)}\}$$

Que se ve (en parte) con el ejercicio 1.21.a

Apartado c)

$$\frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \cong ?\mathbb{Z}_p := \frac{\mathbb{Z}}{p\mathbb{Z}}$$

Definimos el homomorfismo:

$$\mathbb{Z}_p \to \frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \qquad \overline{a} = [a] = a + p\mathbb{Z}_{(p)}$$

$$\text{Ker}(\phi) = \{\overline{a} = a + p\mathbb{Z} : \ a + p\mathbb{Z}_{(p)} = p\mathbb{Z}_{(p)}\}$$

Luego los elementos serán de la forma:

$$\overline{a},\ \text{con } a = p\frac{r}{s},\ \text{con } p \not| s \implies \begin{cases} sa = pr \\ p \not| s \end{cases} \implies p|a \implies \overline{a} = \overline{0} \implies \operatorname{Ker}(\phi) = \{\overline{0}\}$$

Luego ϕ es inyectivo. Sin embargo, esto lo podríamos haber demostrado diciendo simplemente que los homomorfismos que salen de un cuerpo son inyectivos.

Comprobemos ahora que ϕ es sobre. Sea $[a/b] = a/b + p\mathbb{Z}_{(p)} \in \dfrac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}}$. Queremos ver que $[a/b] = [r/1] = \phi(\overline{r})$, para cierto $r \in \mathbb{Z}$

Si $[a/b] = [0]$, no hay nada que probar. Podemos suponer que $[a/b] \neq [0] \iff a/b \notin p\mathbb{Z}_{(p)} = m = \mathbb{Z}_{(p)} \setminus \mathcal{U}(\mathbb{Z}_{(p)})$

$$\implies ab \in \mathcal{U}(\mathbb{Z}_{(p)})\ :\ p \not| a \ (y\ p \not| b)$$

Entonces hacemos:

$$\frac{a}{b} = a \cdot b^{-1} \implies [\frac{a}{b}] = [a][b^{-1}] = [a] \cdot [b]^{-1} = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(\overline{a}\overline{b}^{-1}0)$$

Apartado d)

Hecho en un ejercicio planteado anteriormente de forma más general.

Ejercicio 23. ***Modificado***

Sea $I \precneqq A$ ideal propio tal que $I \subseteq J(A)$. Demostrar:

1. *Para $a \in A$, se verifica:*
$$a \in \mathcal{U}(A) \iff a + I \in \mathcal{U}(A/I)$$
2. *Si A/I no tiene elementos idempotentes no triviales $\implies$ lo mismo pasa con A.*
3. *Si I es maximal, entonces A es local.*

Apartado a)

$\implies$

Trivial ($ab = 1 \implies \overline{a}\overline{b} = \overline{1}$)

$\impliedby$

$$\text{Si } \overline{a} \in \mathcal{U}(\overline{A}) \implies \exists \overline{b} \in \overline{A} : \overline{a}\overline{b} = \overline{1} \implies ab - 1 \in I \subseteq J(A) \implies$$
$$\implies 1 + (ab - 1) \in \mathcal{U}(A) \implies ab \in \mathcal{U}(A) \implies a \in \mathcal{U}(A)$$

Apartado b)

$$\text{Sea } e = e^2 \in A \implies \overline{e} = \overline{e}^2 \implies$$

$$\implies \begin{cases} \overline{e} = \overline{0} \iff e \in I \subseteq J(A) \implies e = 0 \\ \text{ó} \\ \overline{e} = \overline{1} \implies e - 1 \in I \subseteq J(A) \implies 1 + (e-1) \in \mathcal{U}(A) \iff e \in \mathcal{U}(A) \implies e = 1 \end{cases}$$

Ejercicio 24. *Apartado a)*

Tomamos $t = t(n,m) = n + m$ *y hacemos inducción en* $t \geq 2$. *El caso de* $t = 2$ *es claro. Sea* $t > 2$ *y supongamos que es cierto siempre que la suma de los exponentes sea* $<t$.

La hipótesis de inducción nos dice entonces que $I^n,\ J^{m-1}$ *comaximales y* $I^n,\ J$ *comaximales. Ambas propiedades implican entonces que* I^n *es comaximal con* $J^{m-1}J = J$

Apartado b)

$\Longleftarrow$

Tomemos $x = 1,\ y = 0 \implies (1+I)\cap J \neq \emptyset \implies \exists a \in I, b \in J :\ 1+a = b \implies {}_1 = (-a)_{\in I} + b_{\in J}$ $\implies$

Sean $x, y \in A \implies x - y \in A = I + J \implies x - yi + j,$ *con* $i \in I,\ j \in J \implies$

$$x - i = y + j \in (x + I) \cap (y + J)$$

CAPÍTULO 2

Anillos noetherianos

Se han cambiado algunas definiciones respecto a los apuntes de Alberto del Valle.

Definición 2.1. ***Retículo***

*Un conjunto (parcialmente) ordenado $(\mathcal{L}, \leq)$ se dice que es un **retículo** cuando cualquier subconjunto de dos elementos tiene ínfimo y supremo. $(\mathcal{L}, \leq)$ se dice **retículo completo** cuando cualquier subconjunto no vacío tiene ínfimo y supremo.*

Notación

Si $0 \neq S \subseteq \mathcal{L} \implies$

$$\begin{cases} \bigvee_{s \in S} = \sup_{\mathcal{L}}(S) \\ \bigwedge_{s \in S} = \operatorname{ínf}_{\mathcal{L}}(S) \end{cases}$$

Definición 2.2. ***Compacidad y cocompacidad***

*Sea $(\mathcal{L}, \leq)$ un retículo completo. Diremos que $x \in \mathcal{L}$ es **compacto** (resp. **cocompacto**) si dado cualquier subconjunto $\emptyset \neq S \subseteq \mathcal{L}$ tal que $\bigvee_{s \in S} s = x$ (resp. $\bigwedge_{s \in S} s = x$), existe $F \subseteq S$ finito tal que $x = \bigvee_{s \in F} s$ (resp. $x = \bigwedge_{s \in F} s$).*

Ejercicio 1. ***Ejercicio propuesto***

Sea A un anillo. Probar:

1. *$(\mathcal{L}(A), \subseteq)$ es un retículo completo.*
2. *Un ideal $I \trianglelefteq A$ es un elemento compacto de $\mathcal{L}(A)$ sii es un ideal finitamente generado.*

Proposición 2.1. *Sea $(\mathcal{L}, \leq)$ un conjunto ordenado. Las siguientes afirmaciones son equivalentes.*

1. *$(\mathcal{L}, \leq)$ satisface la condición de cadena ascendente (ACC en inglés): Si $s_1 \leq s_2 \leq \ ... \leq \ s_n \leq \ ... \implies m \in \mathbb{Z}^+ : \ s_m = s_{m+1} = ...$*
2. *Todo subconjunto $\emptyset \neq S \subseteq \mathcal{L}$ tiene algún elemento maximal.*

Si además $(\mathcal{L}, \leq)$ es un retículo completo, dichas condiciones son equivalentes a:

3. Todo elemento $x \in \mathcal{L}$ es compacto.

Observación

$(\mathcal{L}, \leq)$ es conj. ordenado (retículo completo) $\iff$ $(\mathcal{L}, \geq)$ es conjunto ordenado (retículo completo).

Luego podemos hacer una proposición equivalente a la anterior cambiando la condición de cadena ascendente por descendente y $\leq$ por $\geq$.

Demostración

$1 \implies 2$

Por reducción al absurdo, supongamos que existe un subconjunto $\emptyset \neq S \subseteq \ \mathcal{L}$ tal que S no tiene elementos maximales.

Sea $s_1 \in S$ arbitrario. Tenemos que s_1 no es maximal, luego $\exists s_2 \in S$ tal que $s_1 < s_2$ con s_2 no maximal, luego podemos tomar s_3. Así construimos una cadena estrictamente ascendente $s_1 < s_2 < ...$, lo que es una contradicción con ACC.

$2 \implies 1$

Sea $s_1 \leq se \leq s_3 \leq ... \leq s_n \leq$ una cadena ascendente $\implies S := \{s_n : n \in \mathbb{Z}^+\}$ tiene un elemento maximal, pongamos $\mu = s_m$ para algún $m \in \mathbb{Z}^+ \implies \mu = s_m \leq s_{m+k} \forall k = 0, 1, ..., \implies S_m = S_{m+k} \ \forall k \geq 0$

En adelante supondremos que $(\mathcal{L}, \leq)$ es un retículo completo.

$3 \implies 1$

Sea $s_1 \leq s_2 \leq ...$ una cadena ascendente en $\mathcal{L}$ y tomamos $x = \bigvee_{n \in \mathbb{Z}^+} s_n \implies x = \bigvee_{k=1}^{r} s_{n_k}$ para cierto subconjunto finito $\{n_1 < ... < n_r\} \subseteq \mathbb{Z}^+ \implies x = s_{n_r}$. Como s_{n_r} es el supremo, $s_{n_r+k} = s_{n_r} \ \forall k > 0$

$2 \implies 3$

Sea $x \in \mathcal{L}$ arbitrario y $\emptyset \neq S \subseteq \mathcal{L}$ tal que $x = \bigvee_{s \in S} s$. Tomamos ahora $x_F = \bigvee_{s \in F} s \ \forall F \subseteq S$ finito, ¿$x = \bigvee_{\substack{F \subseteq S \\ F \ finito}} x_F$?

Pero sabemos que $\Sigma = \{x_F : F \subseteq S \ finito\}$, luego Σ tiene un elemento maximal: $\exists F' \subseteq S$ finito tal que $x_{F'} = \bigvee_{s \in F'} s$ es maximal en Σ.

Se trata de probar que $x = x_{F'}$, sea $s \in S$ arbitrario $\implies$

$$F'' = F' \cup \{s\} \implies x_{F'} = \bigvee_{s \in F'} s \leq x_{F''} = \bigvee_{s \in F''} s \implies x_{F'} \ maximal$$

$$\implies x_{F'} = x_{F''} \implies t \leq x_{F'} \ \forall t \in S \implies x_{F'} \leq x = \bigvee_{s \in S} s \leq x_{F'}$$

□

Definición 2.3. ***Anillo noetheriano***

Un anillo A se dice que es ***noetheriano*** *cuando $(\mathcal{L}(A, \subseteq))$ cumple las tres condiciones equivalentes de la proposición anterior*[a] .

[a] Recordemos que $(\mathcal{L}(A), \subseteq)$ es un retículo completo por el ejercicio propuesto.

Proposición 2.5. *Si A es noetheriano, de cualquier subconjunto $X \subseteq A$ se puede extraer un subconjunto finito (minimal) X_0 tal que $(X) = (X_0)$*

Demostración

$$\Omega = \{I = (X') : \ X' \subseteq X, \ X' \ finito\}$$

$$\mathcal{L}(A) \ noetheriano \implies \exists I_0 = (X_0) \text{ elemento maximal de } \Omega \implies X \subseteq {}^1 I_0 = (X_0)$$

□

Proposición 2.6. *Si D es un dominio noetheriano $\implies$ D es un dominio de factorización (posiblemente no única)*

Demostración

Supongamos que no es así, luego $\exists a \in A \backslash (\mathcal{U}(A) \cup \{0\})$ que no es producto de irreducibles $\implies \Omega \neq \emptyset \implies \exists (b) \in \Omega : \ (b)$ es maximal en $\Omega \implies b$ no es irreducible $\iff_{\mathcal{L}(A) \ noeth} \exists x, y \in A \setminus \mathcal{U}(A) : \ xy = b$. Entonces:

$$\left\{ \begin{array}{c} (b) \subsetneq (x) \\ (b) \subsetneq (y) \end{array} \right\} \implies (x), (y) \notin \Omega \implies$$

$\implies x$ e y son producto finito de irreducibles $\implies b = xy$ también lo es, luego hemos llegado a una contradicción.

□

Proposición 2.7. *Si A es noetheriano, entonces todo ideal contiene un producto finito de ideales principales*

Demostración

Supongamos que no es cierto $\iff \exists I \trianglelefteq A : \ I$ no contiene ningún producto finito de ideales primos.

$$\emptyset \neq \Omega = \{I' \trianglelefteq A : \ I' \text{ no contiene ningún producto finito de ideales primos}\}$$

Como es $\Omega \neq \emptyset$, podemos tomar $I_0 \in \Omega$ maximal $\implies I_0$ no es primo $\iff \exists \ a, b \in A \setminus I_0 : \ ab \in I_0 \implies$

$$\implies \left\{ \begin{array}{c} I_0 \subsetneq I_0 + (a) \\ I_0 \subsetneq I_0 + (b) \end{array} \right\} \implies I_0 + (a), \ I_0 + (b) \notin \Omega \implies \exists P_1, ..., P_r, Q_1, ..., Q_s$$

De forma que P_i, Q_i son ideales primos tales que $P_1 \cdots P_r \subseteq I_0 + (a)$ y $Q_1 \cdots Q_s I_0 + (b) \implies P_1 \cdots P_r Q_1 \cdots Q_s \subseteq (I_0 + (a))(I_0 + (b)) \subseteq I_0$

□

Teorema 2.8. ***De la base de Hilbert***

Sea A un anillo y $n > 0$ un entero. Las siguientes afirmaciones son equivalentes:

1. *A es noetheriano.*
2. *$A[X_1, ..., X_n]$ es noetheriano.*

Demostración

$2 \implies 1$

Observación

[1] Ejercicio

$$I \trianglelefteq A \implies I[X] \trianglelefteq A[X],\ A \cap I[X] = I$$

Sea $I_0 \subseteq I_1 \subseteq ...$ una cadena ascendente de ideales de $A \implies I_0[X] \subseteq I_1[X] \subseteq ...$ es una cadena en $A[X] \implies_{A[X]\ noetheriano} \exists m > 0 :\ I_m[X] = I_{m+k}[X]\ \forall k \geq 0 \implies_{ver\ obs.} A \cap I_m[X] = A \cap I_{m+k}[X]\ \forall k \geq 0$

$1 \implies 2$

Basta probarla cuando $n = 1$, $A[X_1, ..., X_n] \cong A[X_1, ..., X_{n-1}][X_n]$

Vamos a probar que $A[X]$ es noetheriano. Supongamos que no lo es $\implies \exists I \trianglelefteq A[X] :\ I$ no es f.g. $\implies$ elegimos $f_1 \in I \setminus \{0\}$ con grado máximo (n_1) y ponemos b_1 como el coeficiente principal de f_1:

$(0) \subsetneq (f_1) \subsetneq I \implies$ tomo $f_2 \in I \setminus (f_1)$ con grado mínimo $(n_1 \geq n_2)$ y ponemos b_2 el coeficiente prinicpal de f_2. Entonces $(f_1, f_2) \subsetneq I \implies$ tomo $f_3 \in I \setminus (f_1, f_2)$ con grado mínimo $n_3 (\geq n_2 \geq n_1)$ y tomamos b_3 el coeficiente principal de f_3 ...

Probaremos entonces que la cadena $(b_1) \subseteq (b_1, b_2) \subseteq (b_1, b_2, b_3)$ es una cadena **estrictamente** ascendente, lo que nos llevará a una contradicción.

Si $(b_1, ..., b_{k-1}) = (b_1, ..., b_k) \implies b_k = a_1 b_1 + ... + a_{k-1} b_{k-1}$ para ciertos $a_i \in A$, entonces:

$$g := f_k a_1 X^{n_k - n_1} f_1 - ... - a_{k-1} X^{n_k - n_{k-1}} f_k \in I$$

$$0 = b_k - a_1 b_1 - ... - a_{k-1} b_{k-1} \text{ es el coeficiente prinicpal de } X^{n_k} \text{ en } g$$

Si fuese $g \in (f_1, ..., f_{k-1}) \implies f_k = g + \sum_{i=1}^{k-1} a_i X^{n_k - n_i} f_i$

Por tanto $g \notin (f_1, .., f_{k-1})$

b_k es el coeficiente principal de $f_k\ \forall k \geq 1 \implies g \in I \setminus (f_1, ..., f_{k-1})$ y $\mathrm{def}(g) < \deg(f_k)$

□

Teorema 2.12. ***Cohen***

Sea A un anillos. Son equivalentes:

1. *A es noetheriano.*
2. *Todo ideal primo es f.g.*

Notación

Si $I \trianglelefteq A$ y $X \subseteq A \implies (I : X) = \{a \in A :\ aX \subseteq I\}$. Además, $(I : X)$ es un ideal e $I \subseteq (I : X)$

Además, $(I : x) = (I : \{x\})$

Demostración

$2 \implies 1$

Supongamos que A no es noetheriano $\implies I \trianglelefteq A :\ I$ no es f.g. $\implies \Omega = \{I' \trianglelefteq A :\ I'\ \textit{no es f.g.}\} \neq \emptyset$

¿Toda cadena $(I_\lambda)_{\lambda \in \Lambda}$ en Ω tiene una cota superior en Ω?

$$J := \bigcup_{\lambda \in \Lambda} I_\lambda$$

Si $J = (a_1, ..., a_m) \implies \exists \mu \in \Lambda :\ a_1, ..., a_m \in I_\mu \implies (I_{mu} \subseteq) J \subseteq I_\mu \implies J = I_\mu \implies I_\mu$ *f.g. (contradicción)*

Por el lema de Zorn, $\exists P \in \Omega$, elemento maximal. Demostraremos que P es un ideal primo (lo que nos llevará a una contradicción).

Supongamos que P no es primo, sean $a, b \in A \setminus P$ y $ab \in P$

$$\implies \left\{ \begin{array}{l} P \subsetneq P + (a) \\ y \\ b \in (P : (a)) = (P : a) \end{array} \right\} \implies P \subsetneq (P : (a)) \implies$$

$$\implies P + (a), (P : a) \notin \Omega \implies P + (a) = (p_1 + r_1 a, ..., p_s r_s a),\ p_i \in P,\ r_i \in A\ (P : a) = (q_1, ..., q_s)$$

$$\implies ?P = (p_1, ..., p_s, aq_1, ..., aq_s)\ (\implies \text{ contradicción})$$

Sea $p \in P \implies p = b_1(p_1 + r_1 a) + ... + b_s(p_s + r_s a) \implies p = \sum\limits_{i=1}^{s} b_i p_i + a \sum\limits_{i=1}^{s} b_i r_i (*) \implies a \sum\limits_{i=1}^{s} b_i r_i \in P \iff \sum\limits_{i=1}^{s} b_i r_i \in (P : a) = (q_1, ..., q_t) \implies \sum\limits_{i=1}^{s} b_i r_i = \sum\limits_{j=1}^{t} c_j q_j \implies$ (falta el final, consultar apuntes de Alberto del Valle)

$\square$

Teorema 2.13.

Sea A anillo y $n > 0$ un entero. Son equivalentes:

1. *A es noetheriano.*
2. *$A[[X_1, ..., X_n]]$ noetheriano.*

Demostración

$2 \implies 1$

Como en el caso de polinomios (teorema de la base de Hilbert)

$1 \implies 2$

Es la reducción al caso $n = 1$ como en polinomios (Si $n > 1,\ A[[X_1, ..., X_n]] \cong A[[X_1, ..., X_{n-1}]][X_n]$).

Vamos a probar que $A[[X]]$ es noetheriano.

Sea $P \trianglelefteq A[[X]]$ un ideal primo $\implies I_0 = \{a \in A :\ a = f(0),\ \textit{para alguna}\ \subseteq f \in I\} \implies I_0 \trianglelefteq A \implies_{A\ noeth.} I_0 = (b_1, ..., b_n)$.

Como $b_i \in I_0 \implies$ podemos fijar $f_i \in P :\ f_i(0) = b_i\ \forall i = 1, ..., n$

Tenemos entonces dos casos posibles:

1. $X \in P \implies P = (f_1, ..., f_m, X)$. Justificamos esta igualdad:
   El lado $\supseteq$ es directo. Sea ahora $f \in P \implies f = \underbrace{f(0)}_{\in I_0} + Xg(X)$ con $f(0) = a_1 b_1 + ... + a_n b_n$ con los $a_i \in A$. Entonces $f = a_1 b_1 + ... + a_n b_n + Xg(X)$
2. $X \notin P$. Probaremos entonces que $P = (f_{1,...,f_n})$.
3. De nuevo el lado $\supseteq$ es directo. Sea $f \in P \implies f(0) \in I_0 \implies f(0) = a_1^0 b_1 + ... + a_n^0 b_n$. Entonces $g = f - \sum\limits_{i=1}^{n} a_i^0 f_i \implies$ tiene término independiente nulo $\implies g = Xg_1(X) \in P \implies_{X \notin P} g_1 \in P$

Si $g_1(0) = \sum_{i=1}^{n} a_i^1 b_i \implies g_1 - \sum_{i=1}^{n} a_i^1 f_i$ es un polinomio en P con término indep. nulo. $\implies$ $g_1 - \sum_{i=1}^{n} a_i^1 f_i = X g_2 \implies g_1 = \sum_{i=1}^{n} a^1 f_i + g_2$. Con g_2 múltiplo de X, $g_2 = X g_3 \implies g_3 \in P$
Con lo que queda una suma infinita:

$$\sum_{i=0}^{n} a_i^0 f_i + \sum_{i=1}^{n} a_i^1 X f_i + \sum_{i=1}^{n} a_i^2 X^2 f_i + ... = \sum_{i=1}^{n} h_i(X) f_i$$

□

Definición 2.4. ***Dimensión de Krull***

*Sea A un anillo. Se llama **dimensión de Krull** de A al número $n \in \mathbb{N} \cup \{x\}$ tal que:*

$$\dim(A) = \operatorname{Kdim} A = \sup\{n \in \mathbb{N} : \text{ existe una cadena } P_0 \subsetneq P_1 \subsetneq ... \subsetneq P_n \text{ en } \operatorname{Spec}(A)\}$$

Proposición 2.14. *Si A es una anillo artiniano entonces:*

1. $\operatorname{Spec}(A) = \operatorname{MaxSpec}(A)$, *osea todo ideal primo es maximal, o " A tiene dimensión* $\dim(A) = 0$.
2. $\operatorname{Spec}(A) = \operatorname{MaxSpec}(A)$ *es finito.*
3. $J := \operatorname{Jac}(A) = \operatorname{Nil}(A)$ *es **nilpotente***

(no esta copiado entero)

Demostración

1.

$P \in \operatorname{Spec}(A) \implies \dfrac{A}{P}$ dominio artiniano y por el ejemplo 2.4.3 tenemos que A/P es cuerpo $\iff P \in \operatorname{MaxSpec}(A)$

2.

Definimos:

$$\Omega = \{I \trianglelefteq A : \; I = \text{ intersección finita de ideales maximales}\}$$

Tenemos que $\Omega \neq \emptyset$ porque A tiene un ideal maximal $\implies \exists I_0 \in \Omega$ minimal $\implies I_0 = M_1 \cap ... \cap M_r$.

Sea entonces $M \in \operatorname{MaxSpec}(A) \implies I_0 \cap M \in \Omega \implies$

$$\implies \left\{ \begin{array}{c} I_0 \cap M \in \Omega \\ I_0 \cap M \in I_0 \end{array} \right\} \implies_{I_0 \ minimal} I_0 \cap M = I_0 \iff I_0 \subseteq M$$

$$M_1 \cdots M_r \subseteq M_1 \cap ... \cap M_r = I_0 \subseteq M \implies_{M \ primo} \exists j : \; M_j \subseteq M \implies$$
$$\implies_{M_j \ maximal} M_j = M \implies \operatorname{MaxSpec}(A) = \{M_1, ..., M_r\}$$

3.

Como A es artiniano y se tiene la cadena descendente $J \supseteq J^2 \supseteq J^3 \supseteq ... \implies \exists m \in \mathbb{Z}^+$ (minimal) con $J^m = J^{m+k} \; \forall \, k \geq 0$. Definimos $I := J^m$ $(I^2 = I)$.

Supongamos que $I \neq 0 \implies$

$$\emptyset \neq \Omega' := \{K \trianglelefteq A : \; KI \neq 0, \; K \subseteq I\} \ni I$$

$\implies \Omega'$ tiene un elemento minimal K_0 tal que $K_0 I \neq 0 \implies \exists x \in K_0 : \; xI \neq 0 \implies$

$$\left\{ \begin{array}{l} (x)I \neq 0 \implies (x) \in \Omega' \\ (x) \subseteq K_0 \; minimal \end{array} \right\} \implies (x) = K_0$$

Entonces $xI \neq 0 \implies 0 \neq xI = xI^2 = (xI)I \implies xI \in \Omega'$ y se tiene $xI_{\in \Omega'} \subsetneq (x) = K_0 \underset{K_0 \text{ minimal en } \Omega'}{\implies} xI = (x) = K_0$

Entonces $x \in xI \implies x = xy$ para cierto $y \in I$, luego $x = xy = xy^2 = ... = xy^n \; \forall n > 0$ y además $y \in I \subseteq J(A) = \mathrm{Nil}(A) \implies \exists n > 0 : \; y^n = 0$. Entonces $x = 0$, lo que nos lleva a una contradicción.

4.

$J = M_1 \cap ... \cap M_r$, donde $\mathrm{MaxSpec}(A) = \{M_1, ..., M_r\}$. Como cada M_i son maximales, los M_i son comaximales dos a dos. Por tanto, tenemos que:

$$J = M_1 \cap ... M_r = M_1 \cdots M_r \implies 0 = J^m = M_1^m \cdots M_r^m$$

$\square$

Teorema 2.15. ***(Akizuki)***

Sea A un anillo. Son equivalentes:

1. *A es artiniano.*
2. *A es noetheriano y $\dim(A) = 0$.*

Aún no tenemos todos los conceptos necesarios para demostrar este teorema, nos dejaremos algún detalle sin resolver.

Demostración

$1 \implies 2$

Ya hemos visto que $\dim(A) = 0$. Queda pendiente probar que A es noetheriano.

$2 \implies 1$

Sabemos que $\implies \mathrm{MaxSpec}(A) = \mathrm{Spec}(A) = \mathrm{MinSpec}(A) \implies$ [2] este conjunto es finito.

Si tomamos $\mathrm{Spec}(A) = \{M_1, ..., M_r\}$ tenemos que $J := J(A) = \mathrm{Nil}(A) = M_1 \cap ... \cap M_r = M_1 \cdots M_r$ (ya que los elementos son maximales dos a dos).

Por ser A noetheriano, J es f.g y como también es nil (todos sus elementos son nipotentes), tenemos que J es nilpotente (ejercicio 2.4) $\iff \exists m > 0$ (minimal) tal que $J^m = 0 \implies 0 = M_1^m \cdots M_r^m$

Utilizando ahora el teorema chino de los restos (la versión general de esta asignatura), tenemos que

$$\begin{aligned} \phi : A \; &\to \frac{A}{M_1^m} \times ... \times \frac{A}{M_r^m} \\ a \; &\hookrightarrow (\overline{a}, ..., \overline{a}) \end{aligned}$$

es un isomorfismo de anillos.

Entonces A es artiniano $\iff \dfrac{A}{M_i^m}$ es artiniano $\forall i = 1, ..., r$

[2] Ejercicio 2.7

Afirmamos ahora que A/M_i^m es un anillo local (noetheriano) con M_i/M_i^m como único ideal maximal (= primo).

Basta con ver que es el único ya que usando el teorema de correspondencia podremos ver que es maximal.

Sea M/M_i^m un ideal maximal de $A/M_i^m(\implies M \in \text{MaxSpec}(A)) \implies M_i^m \subseteq M \implies_{M\ primo} M_i \subseteq M \implies_{M_i\ maximal} M_i = M$

La prueba entonces queda reducida a probar que si A es un anillo noetheriano local con $\dim(A) = 0$ (y M como único ideal maximal), entonces A es artiniano.

Observación

M es nilpotente $\iff \exists q > 0$ $(minimal)$ tal que $M^q = 0$

Observación

M es f.g. $\implies$ fijo $\{x_1, ..., x_d\}$ conjunto de generadores de $M \implies_{ejerc.} M^t = (x_{i_1}, ..., x_{i_t} : i_1, ..., i_t \in \{1, 2, ..., d\})$

Crucial: Cada cociente M^t/M^{t+1} (en particular $M^{q-1} = M^{q-1}/M^q$) es un A/M-esp. vectorial con $\{\overline{x_{i_1}, ..., x_{i_t}}\}$ como conjunto de generadores. Definimos entonces:

$$\begin{array}{rcl} \dfrac{A}{M} \times \dfrac{M^t}{M^{t+1}} \to & & \dfrac{M^t}{M^{t+1}} \\ (a+m, y+m^{t+1}) \hookrightarrow & & ay + m^{t+1} \end{array}$$

Probad que está bien definida y transforma M^t/M^{t+1} es un A/M-esp. vectorial.

Además, si $y \in M^t \implies y = \sum a_i x_{i_1} \cdots x_{i_t} \implies y + M^{t+1} = \sum a_i + m(x_{i_1 \cdots x_{i_t}} {}_{M^{t+1}}) \implies M^{t/M^{t+1}}$ está generado como A/M-esp. vectorial por $\{\overline{x_{i_1} \cdots x_{i_t}}\}$

Entonces cada M^t/M^{t+1} es un $\dfrac{A}{M}$-esp. vectorial de dimensión finita.

Entonces $M^q = 0 \neq M^{q-1}$. Probaremos por inducción en $q \geq 1$ que A es artiniano.

Si $q = 1 \implies M = 0 \implies A = A/M$ es un cuerpo y terminamos.

Sea $q > 1$ y lo suponemos cierto para $q - 1 \implies A/M^{q-1}$ es artiniano.

Sea $I_0 \supseteq I_1 \supseteq ... \supseteq I_n \supseteq ...$ una cadena descendente de ideales de A. Entonces:

$$\left\{ \begin{array}{ll} \dfrac{I_0 + M^{q-1}}{m^{q-1}} \supseteq \dfrac{I_1 +^{q-1}}{m^{q-1}} \supseteq ... & \text{se estaciona por ser } A/M^{q-1} \text{ artiniano} \\ I_0 \cap M^{q-1} \supseteq I_1 \cap M^{q-1} \supseteq ... & \text{se estaciona por ser } M^{q-1} \text{ un } A/M\text{-esp. vectorial de dimensión finita} \end{array} \right.$$

Entonces $\exists s > 0$ tal que:

$$\left\{ \begin{array}{l} I_s + M^{q-1} = I_{s+k} + M^{q-1} \\ I_s \cap M^{q-1} = I_{s+k} \cap M^{q-1} \end{array} \right\} \forall k \geq 0$$

Se trata ahora de probar que si $I, J \trianglelefteq A :\ I \supseteq J$ y se tiene

$$\left\{ \begin{array}{l} I + M^{q-1} = J + M^{q-1} \\ I \cap M^{q-1} = J \cap M^{q-1} \end{array} \right. \implies ?I = J$$

Sea $y \in I \subseteq I + M^{q-1} = J + M^{q-1} \implies y = z + h$ donde $h \in M^{q-1},\ z \in J \implies h = \underbrace{y}_{\in I} - \underbrace{z}_{\in J \subseteq I} \implies h \in I \cap M^{q-1} = J \cap M^{q-1} \implies h \in J \implies y = z + h \in J$

$\square$

Ejercicios

Ejercicio 1.

Apartado c)

$$X \subseteq (X) \implies_{2,1.b)} (I : (X)) \subseteq (I : X)$$

Probamos que $(I : X) \subseteq (I : (X))$.

Sea $a \in (I : X) \iff ax \in I\ \forall x \in X$.

Quiero probar que si $z \in (X) \implies az \in I$*:*

$$z \in (X) \iff z = \sum_{i=1}^{n} b_i x_i\ (b_i \in A, x_i \in X) \implies az = \sum_{i=1}^{n} b_i ax \implies az \in I$$

Apartado e)

1.

Sea $a \in A$*:*

$$a \in ((I : X) : Z) \iff aZ \subseteq (I : X) \iff az \in (I : X)\ \forall z \in Z \iff (az)X \subseteq I\ \forall z \in Z$$

$$(az)x = a(zx) \in I\ \forall z \in Z,\ \forall x \in X \iff aw \in I\ \forall w \in X \cdot Z = Z \cdot X \iff a \in (I : X \cdot Z)$$

Apartado f)

Sea $a \in A$*:*

$$a \in (I : \bigcup_t X_t) \iff az \in I\ \forall z \in \bigcup_t X_t \iff az \in I\ \forall z \in X_t \text{ con } t \in T \text{ arbitrario}$$

$$\iff a \in (I : X_t)\ \forall t \in T \iff a \in \bigcap_{t \in T} (I : X_t)$$

2.

Sabemos que $\sum_{t \in T} J_t = \left(\bigcup_{t \in T} J_t\right)$ *y aplicando el apartado c) y el caso anterior:*

$$\left(I : \sum_{t \in T} J_t\right) = \left(I : (\bigcup_{t \in T} J_t)\right) = \left(I : \bigcup_{t \in T} J_t\right)) \bigcap_{t \in T} (I : J_t)$$

Ejercicio 2. *Hay una errata en el tercer caso del a). El enunciado correcto es:*

$$\left(\frac{J}{I}\right)\left(\frac{J'}{I}\right) = \frac{JJ'+I}{I}$$

Ejercicio 3.

$\supseteq$

Directa. Basta con ver que el conjunto de generadores de $(X \cdot Y)$ *está contenido en* $(X)(Y)$*, que es directo.*

$\subseteq$

$(X)(Y) = ((X)\cdot(Y)) \implies$ *sus elementos son las sumas* $\sum_{i=1}^{n} z_i w_i$ *donde* $z_i \in (X),\ w_i \in (Y)$*. Entonces* $z_i \in (X) \implies z_i = \sum_{j=1}^{m_i} a_{ij}x_j$ *donde* $a_{ij} \in A,\ x_j \in X$ *y* $w_j \in (Y) \implies w_i = \sum_{k=1}^{q_i} b_{ik}y_k$*, donde* $b_{ik} \in A,\ y_k \in Y \implies z_i w_i = \sum_{j,k} a_{ij}b_{ik}x_j y_k \in (X \cdot Y)$

Ejercicio 4.

Tenemos que $I = (b_1, ..., b_n)$*. Hacemos inducción en* $n \geq 1$*.*

Para $n = 1$, $I = (b_1)$*. Como* b_1 *es nilpotente,* $\exists m >$: $b_1^m = 0 \implies I^m = 0$

Sea $n > 1$ *y cierto para ideales nil generados por menos de* n *elementos. Si tomamos* $I' = (b_1, ..., b_{n-1})$, I' *es nil* ($I' \subseteq I$)*. La hipótesis de inducción nos da además un* $p > 0$ *entero tal que* $I'^p = 0$.

Por otra parte, $(b_n)^q = 0$ *para un cierto entero* $q > 0$*. Observamos además que* $I = I' + (b_n)$*. ¿Existe entonces* m *tal que* $I^m = 0$*? Esto ocurre si y solo si* $\forall y_1, ..., y_m \in I$ *se tiene que* $y_1 \cdots y_m = 0$

Ahora, podemos poner $y_i = y_i' + z_i$ *con* $y_i' \in I'$ *y* $z_i \in (b_n)$*. Si tomamos* $m = p + q$ *entonces* $(y_i + z_i)^m = 0\ \forall i$*. Luego* I *es nilpotente.*

Ejercicio 5.

Tomamos el cociente $\frac{A}{I}$*, tenemos que* $\mathrm{Nil}\left(\frac{A}{I}\right) = \frac{\sqrt{I}}{I}$ *es nil y f.g. Utilizando ahora el ejercicio anterior, tenemos que* $\exists m$ *tal que* $\left(\frac{\sqrt{I}}{I}\right)^m$*. Entonces:*

$$0 = \left(\frac{\sqrt{I}}{I}\right)^m = \frac{(\sqrt{I})^m + I}{I} \implies (\sqrt{I})^m \subseteq I$$

Ejercicio 6.

Si $x \in \bigcap_{n>0}(b^n) \implies \forall n > 0,\ \exists x_n \in A$ *tal que* $x = b^n x_n \implies \forall n > 0$ *se tiene:*

$$\cancel{b^n} x_n = x = b^{\cancel{n}+1} x_{n+1} \implies x_n = b x_{n+1}$$

$$\implies (x_1) \subseteq (x_2) \subseteq ... \subseteq (x_n) \subseteq ...$$

Luego tenemos una cadena ascendente en $\mathcal{L}(A)$*, pero como* A *es noetheriano, la cadena se estaciona, es decir,* $\exists m > 0$ *tal que* $(x_m) = (x_{m+1})\ \forall k \geq 0$

En particular, tenemos que:

$$x_{m+1} \in (x_m) \implies \exists c \in A:\ x_{m+1} = c x_m \implies x_m = b x_{m+1} = bc x_m$$

Tenemos ahora dos casos:

Si x *es cancelable,* x_m *es cancelable (siguiente línea)* $\implies bc = 1 \implies b \in \mathcal{U}(A)$ *(contradicción).*

Si x_n *no fuese cancelable, entonces existe* $y_n \in A \setminus \{0\}$ *tal que* $x_n y_n = 0 \implies x y_n = 0$ *(contradicción ya que* x *es cancelable)*

Si x *no fuera cancelable, ¿podríamos tomar* $x_n = x_{n+1}\ \forall n > 0$*? Le llamamos* y *a ese elemento.* $x = by = b^2 y = ... \implies_{b\ cancelable} y = by$

Si probamos que $\overline{y} \neq \overline{0}$ *y que* $\overline{z}$ *es cancelable en* A*, entonces* $0 \neq \overline{y} \in \bigcap_{n>0}(\overline{z}^n)$

Veamos primero que $\overline{y} \neq \overline{0}$*. Supongamos que* $\overline{y} = \overline{0} \implies y \in (y(1-z)) \implies y = y(1-z)f(y,z)$ *con* $f \in \mathrm{K}[y,z]$*. COmo* y *es cancelable,* $(1-z)f(y,z) = 1 \implies 1 - z \in \mathcal{U}(\mathrm{K}[y,z])$*. Lo cual es una contradicción, las unidades de un anillo de polinomios son las unidades del "anillo origen".*

Supongamos ahora que $\overline{z}$ *no es cancelable. Lo que es equivalente a que* $\overline{z}$ *sea divisor de cero en* A*. Entonces* $\exists g \in \mathrm{K}[y,z]$ *tal que* $\overline{z} \cdot \overline{g} = \overline{0},\ \overline{g} \neq 0 \iff$

$$\iff zg(y,z) \in (y(1-z)) \iff \exists h = h(y,z):\ zg(y,z) = y(1-z)h(y,z)\ (*)$$

Entonces $zg(y,z) \in (y),\ z \notin (y)$*. Luego* $g(y,z) \in (y) \implies g(y,z) = y\widetilde{g}(y,z) \implies (*) z\widetilde{g}(y,z) = (1-z)h(y,z)\ (**)$

$$\left\{ \begin{array}{l} (1-z)h(y,z) \in (z) \\ 1 - z \notin (z) \end{array} \right\} \implies h(y,z) \in (z) \iff h(y,z) = z\widetilde{h}(y,z) \text{ para algún } \widetilde{h} \in \mathrm{K}[y,z] \implies$$

$$\implies (**) \widetilde{g}(y,z) = (1-z)\widetilde{h}(y,z)$$

Entonces tenemos:

$$g(y,z) = y\widetilde{g}(y,z) = y(1-z)\widetilde{h}(y,z) \implies g(y,z) \in (y(1-z)) \iff \overline{g} = \overline{0} \text{ (contradicción)}$$

Ejercicio 7.

Si aplicamos la proposición 2.7, tenemos que $(0) = P_1 \cdots P_r$*, donde los* P_i *son primos (quizá algunos repetidos). Sea* $P \in \mathrm{MinSpec}(A) \implies (0) = P_1 \cdots P_r \subseteq P$*. Pero como* P *es primo,* $\exists j$ *tal* *que* $P_j \subseteq P$ *y como* P *es minimal en* $\mathrm{Spec}(A)$*,* $P_j = P \implies P \in \{P_1, ..., P_r\}$*. Entonces el número de primos minimales es finito (hay hasta* r*)*

Para la segunda parte, tomamos $I \subsetneq\!\!\trianglelefteq A$ *y usamos el teorema de la correspondencia para ideales primos:*

$$\begin{array}{ccc} \{P \in \mathrm{Spec}(A) :\ I \subseteq P\} \xrightarrow{biyección} & & \mathrm{Spec}(\frac{A}{I}) \\ P \longmapsto & & \frac{P}{I} \\ \left\{ \begin{matrix} \scriptstyle primos\ minimales \\ sobre\ I \end{matrix} \right\} \leftrightarrow & & \mathrm{MinSpec}\left(\frac{A}{I}\right)\ (finito) \end{array}$$

Ejercicio 8.

Visto en la prueba del teorema de Akizuki.

Ejercicio 9.

Si $a \in \mathcal{U}(A) \implies a = u = up^0$

Si $0 \neq a \notin \mathcal{U}(A)$*:*

$$\implies (a) \subsetneq A \implies (a) \subseteq J = (p) \implies a = pa_1 \implies a \in (p) \setminus \bigcap_{n\in\mathbb{N}} (p^n) \implies$$

$$\implies \{n \in \mathbb{N} :\ a \in (p^n)\} \implies \exists m \text{ maximal con } a \in (p^m)$$

Entonces $a = p^m u$ *y basta probar que* $u \in \mathcal{U}(A)$*.*

Si $u \notin \mathcal{U}(A) \implies (u) \subseteq J = (p) \implies u = pv$*, con* $v \in A \implies a = p^m u = p^m(pv) = p^{m+1}v \implies a \in (p^{m+1})$ *lo cual es una contradicción.*

Observación

Hemos probado que todo ideal principal de A *es 0 o de la forma* (p^n) *con* $n \in \mathbb{N}$

Entonces tenemos:

$$A = (p^0) \supsetneq (p^1) \supsetneq ... \supsetneq (p^n) \supsetneq ...$$

Sea ahora $I \trianglelefteq A$ *f.g.* $\implies I = (x_1, ..., x_n) = \sum_{i=1}^{n} (x_i)$

Si suponemos que $(x_i) = (p^{m_i})$ *y suponemos* $m_1 \geq m_2 \geq ... \geq m_n$*, entonces* $\sum_{i=1}^{n} (x_i) = \sum_{i=1}^{n} (p^{m_i}) = (p^{m_n})$

Supongamos que $I \subsetneq\!\!\trianglelefteq A$ *que no es finitamente generado.*

Tomamos $y_1 \in I \setminus \{0\}$ *arbitrario, entonces* $(y_1) \subsetneq I \implies \exists y_2 \in I \setminus (y_1) \implies (y_1, y_2) \subsetneq I$ *.... Construimos así una cadena ascendente:*

$$\begin{array}{cccccc} 0 \neq & (y_1) \subsetneq & (y_1, y_2) \subsetneq & ... \subsetneq & (y_1, ..., y_n) \subsetneq ... \\ & (p^{m_1}) \subsetneq & (p^{m_2}) \subsetneq & ... \subsetneq & (p^{m_n}) \subsetneq ... \end{array}$$

CAPÍTULO 4

Módulos

Está haciendo la introducción bastante rápido, quedan apuntados los conceptos que introduce. Los ha visto conforme a los apuntes de Alberto.

Definición 4.1. ***Módulo***

Definición 4.2. ***Submódulo***

Notación

Al conjunto de submódulos del $A-$módulo M lo denotamos por $\mathcal{L}(_AM)$

Proposición 4.1. ***Extraída de los ejemplos 4.9***

Un A-módulo M es cíclico sii es isomorfo a $\dfrac{A}{I}$, para un ideal I de A.

Demostración

Si $\dfrac{A}{I}$ es cíclico generado por $\overline{1} = 1 + I$ ya que $a + I = a(1 + I)$

Si M es cíclico, entonces $M = (x) = Ax = \{ax : \ a \in A\}$. Si defino $f :_a A \to M = Ax$ de forma que $a \mapsto f(a) = ax$ tenemos un epimorfismo de A-módulos.

Por el teorema de isomorfía, tenemos que $\dfrac{A}{\mathrm{Ker}(f)} \cong M$. Siendo $\mathrm{Ker}(f)$ un ideal de A.

Observación

$$\mathrm{Ker}(f) = \{a \in A : \ ax = 0\} = ann_A(x) \overset{M \ cicl.}{=} ann_A(M)$$

Para $\subseteq$ en la última igualdad necesitamos probar que si $\underbrace{ax = 0}_{a \in ann_A(x)} \implies \underbrace{a(bx) = 0}_{a \in ann_A(M)}$ $\forall b \in A$

$\square$

Proposición 4.10. ***Proposición-Definición***

Sea $(M_i)_{i\in I}$ una familia de submódulos del A-módulo M. Decimos que es una familia independiente (de submódulos) cuando satisface cualquiera de las siguientes condiciones equivalentes:

1. *La expresión de un $x \in \sum\limits_{i\in I} M_i$ como $x = \sum\limits_{i\in I} x_i$ (**suma finita**) con $x_i \in M_i$ $\forall i \in I$, es única.*
2. *Si 0 $= \sum\limits_{i=I}^{x_i}$ (**suma finita**) con $x_i \in M_i$ $\forall i \in I$, entonces $x_i = 0 \forall i \in I$.*
3. *$\forall j \in I$, se tiene que $M_j \cap \left(\sum\limits_{i\neq j} M_i\right) = 0$*

Demostración

$1 \implies 2.$

Trivial.

$2 \implies 1.$

$$\left\{\begin{array}{l} x = \sum x_i \\ x = \sum x_i' \end{array}\right\} \overset{Suma\ finita}{\implies} 0 = \sum_{i=I}(x_i - x_i') \implies x_i - x_i' = 0$$

$3 \implies 2.$

Si $0 = \sum x_i \implies \forall j \in I$ tenemos que $x_j = \sum\limits_{i\neq j}(-x_i) \implies x_j \in M \cap \left(\sum\limits_{i\neq j} M_i\right) \overset{3)}{=} 0 \implies x_j = 0\ \forall j \in I$

$1, 2 \implies 3.$

Sea $x \in M_j \cap \left(\sum\limits_{i\neq j} M_i\right) \implies x = \sum\limits_{i\neq j} x_i$, con $x_i \in M_i$ $\forall i \in I \setminus \{j\} \implies 0 = \sum\limits_{i\neq j} x_i + (-x) \overset{2)}{\implies} -x = 0 \iff x = 0$

□

Cuando $(M_i)_{i\in I}$ es una familia independiente de submódulos de M, la suma $\sum\limits_{i\in I} M_i$ suele denotarse por $\bigoplus\limits_{i\in I}^{int} M_i =$ suma directa interna de los M_i.

Recordemos que se tiene la suma directa externa $\bigoplus\limits_{i\in I}^{ext} M_i = \{(x_i) \in \prod_{i\in I} M_i : \ x_i = 0\ \forall i \in I\}$.

En general, si $(M_i)_{i\in I}$ es una familia de submódulos de M, se tiene un homomorfismo inducido:

$$\begin{aligned} \phi : \bigoplus_{i\in I}^{ext} M_i &\to M \\ (x_i) &\mapsto \sum x_i \end{aligned}$$

Cuya imagen es $\sum\limits_{i\in I} M_i$, es decir $\mathrm{Im}(\phi) = \sum\limits_{i\in I} M_i$

Se tiene que ϕ es un monomorfismo $\iff$ $(M_i)_{i\in I}$ es una familia independiente. En tal caso induce un isomorfismo entre la suma externa y la interna. Por tanto, obviaremos el superíndice ext o int.

Proposición 4.12. *Sea $(M_i)_{i\in I}$ una familia independiente de submódulos de M tal que $M = \bigoplus_{i\in I} M_i$. Para cada $j \in I$, se tiene:*

1. $M_j \cong \dfrac{\bigoplus M_i}{\bigoplus\limits_{i\neq j}}$
2. $\bigoplus\limits_{i\neq j} M_i \cong \dfrac{M}{M_j}$

Como caso particular, se tiene que si $M = N \oplus N'$, entonces:

$$\frac{M}{N'} \cong N \qquad\qquad \frac{M}{N} \cong N'$$

Demostración

1.

Utilizamos la proyección de M a M_j que tiene por núcleo $\bigoplus\limits_{i\neq j} M_i$

2.

De nuevo, tomamos la proyecctión de M a $\bigoplus\limits_{i\neq j} M_i$ cuyo núcleo es M_j

□

Vemos ahora una proposición que no está incluida en los apuntes de Alberto del Valle

Observación previa

Si M es un A-módulo, entonces $\mathrm{End}_A(M)$ es un anillo no conmutativo en general (con la composición como producto).

Proposición 4.13. *M es indescomponible sii los únicos idempotentes de $\mathrm{End}_A(M)$ son 0 y 1_M*

Demostración

$\Longrightarrow$

Sea $\varepsilon \in \mathrm{End}_A(M)$ idempotente ($\Longrightarrow$ $1_M - \varepsilon$ también lo es) $\overset{?}{\Longrightarrow}$ $M = Im(\varepsilon) \oplus Im(1_M - \varepsilon)$

Si eso está probado, entonces al ser M indescomponible $Im(\varepsilon) = 0$ o $Im(1_M - \varepsilon) = 0 \iff \varepsilon = 0$ o $1_M - \varepsilon = 0$

$$M = Im(\varepsilon) + Im(1-\varepsilon) : \; x = \varepsilon(x) + (1_M - \varepsilon)(x)$$

$$x \in Im(\varepsilon) \cap Im(1-\varepsilon) \Longrightarrow \begin{cases} x = \varepsilon(y) & \Longrightarrow (1_M - \varepsilon)(x) = \underbrace{[(1_M - \varepsilon)\cdot \varepsilon]}_{0}(x) \\ y & \\ x = (1_M - \varepsilon)(z) & \Longrightarrow \varepsilon(x) = 0 \end{cases}$$

$\Longleftarrow$

Si $M = N \oplus N'$ (suma directa interna), entonces:

$$\begin{array}{rlll} \varepsilon_N : M = & N \oplus N' \to & N \hookrightarrow & M \\ & v + v' \mapsto & \mapsto v + 0 & \end{array}$$

Entonces ε_N es idempotente, luego $\varepsilon_N = 0$ ($\iff N = 0$) o bien $\varepsilon_N = 1_M$ ($\iff N = M$)

□

Lema 4.14. *Sea $0 \neq M$ un A-módulo cíclico, entonces M es indescomponible sii los únicos idempotentes del anillo $\dfrac{A}{ann_A(M)}$ son $\overline{0}, \overline{1}$.*

Si tenemos entonces un isomorfismo en ${}_A Mod$: $\dfrac{A}{ann_A(M)} \cong M$, entonces $\mathrm{End}_A(M) \cong \mathrm{End}_A\left(\dfrac{A}{ann_A(M)}\right)$

Ejercicio 1. *Si $I \subsetneq A$, entonces la aplicación $\dfrac{A}{I} \xrightarrow{\mu} \mathrm{End}_A(A/I)$ ($\mu_{\overline{a}}\overline{b} \mapsto \overline{ab} = \overline{a} \cdot \overline{b}$) es un isomorfismo de anillos.*

Que sea un homomorfismo es directo, vemos que:

$$\mathrm{Ker}(\mu) = \{\overline{a} : \mu_{\overline{a}} \equiv 0\} = \{\overline{a} \in \frac{A}{I} : \ \overline{ab} = \overline{0} \ \forall \overline{b} \in \frac{A}{I} \ (\implies \overline{a} = \overline{a}\overline{1} = \overline{0})\} \implies$$

$$\mathrm{Ker}(\mu) = 0 \implies \mu \text{ inyectiva}$$

Vemos que μ es suprayectivo. Sea $f \in \mathrm{End}_A\left(\dfrac{A}{I}\right)$ de forma que $f(\overline{1}) = \overline{a}$. Entonces tenemos que $\overline{b} = b\overline{1} \mapsto bf(\overline{1}) = b\overline{a} = \overline{b}\overline{a} \implies f = \mu_{\overline{a}}$. Luego μ es sobre.

Ejercicio 2. ***Ejercicio planteado***

Sea $M \in \mathrm{MaxSpec}(A)$ y $n > 0$ un entero. Probar que el A-módulo A/M^n es indescomponible.

Ejercicio 3. ***Ejercicio planteado***

Sea $a \in A \setminus (\mathcal{U}(A) \cup \{0\})$, donde A es un DIP. Probar:

$$\frac{A}{(a)} \text{ indescomponible } \iff a \text{ es asociado a } p^t, \text{ para algún } p \in A \text{ irreducible y algún } t > 0$$

Definición previa a la proposición 4.26

Definición 4.3. ***Sucesión exacta corta***

*Se dice que una sucesión de A-módulos y $A-$-homomorfismos $0 \to L \to M \to N \to 0$ es una **sucesión exacta corta** si el núcleo de cada morfismo es la imagen del que la precede. Esto es equivalente a:*

$$\begin{cases} g & epimorfismo \\ f & monomorfismo \\ \mathrm{Im}(f) = \mathrm{Ker}(g) & \end{cases}$$

Ejercicio 4.

Toda sucesión exacta corta con término central M es isomorfa a una del estilo:

$$0 \to K \hookleftarrow M \xrightarrow{\pi} M/K \to 0$$

Donde $\hookleftarrow$ es la inclusión desde un submódulo y π es la proyección sobre el cociente.

Corolario 4.27. $\bigoplus_{i=1}^{n} M_i$ *es noeth. (resp. artiniano) si y solo si todos los M_i son noeth. (resp. artinianos)*

Demostración

Se reduce trivialmente al caso $n = 2$. Vemos que $N_1 \oplus N_2$ noeth $\iff$ $N_1, \; N_2$ lo son. Sabemos que:

$$N_2 \cong \frac{N_1 \oplus N_2}{N_1}$$

Lo cual da la prueba de forma directa.

□

Corolario 4.28. ***Apartado a)***

Sea A anillo. Son equivalentes:

1. *A anillo noeth. (resp. artiniano)*
2. *Para algún (resp. todo) entero $n > 0$, el A-módulo libre A^n es noeth. (resp. artiniano).*
3. *Todo A-módulo fin. generado es noeth. (resp. artiniano)*

Observación previa a la prueba

Como en los dos casos de este corolario hay una parte fuerte y una débil en 2), para probar esto hay que hacer el caso fuerte para $1 \implies 2$ y el débil para $2 \implies 3$

Demostración

$1 \implies 2.$

Hay que probar que $\forall n > 0_A A^n$ es noeth (sale por el corolario anterior).

$2 \implies 1.$

Suponemos que $\exists n > 0$ tal que ${}_AA^n$ noeth. $\implies$ ${}_AA$ noeth.

$(1, 2) \implies 3.$

$\exists$ epimorfismo $\pi :_A A^n \to M$ y ${}_AA^n$ noeth. $\implies$ M noeth.

$3 \implies 1.$

Trivial

□

Corolario 4.28. ***Apartado b)***

Sea A un anillo noeth. (resp. artiniano) y sea $f : A \to B$ un homomorfismo de anillos tal que B es f.g. como A-módulo (con la restricción de escalones). Entonces B es anillo noeth. (resp. artiniano)

Demostración

$$\mathcal{L}({}_BB) \subseteq \mathcal{L}({}_AB)$$

El apartado a) nos dice que ${}_AB$ es noeth. (resp. artiniano). Entonces sale ”directamente” la prueba.

□

Ejercicio 5.

Sea $A = A_1 \times ... \times A_n$ producto finito de anillos. Probar que todo A-módulo es isomorfos aun producto $M_1 \times ...M_n$, donde cada M_i es un A_i-módulo. En particular:

$$\mathcal{L}({}_AM) \cong \mathcal{L}({}_{A_1}M_1) \times ... \times \mathcal{L}({}_{A_n}M_n)$$

Lema 4.29. ***Lema de Artin***

Demostración

Sean $0 = m_1^{n_1} \cdots m_r^{n_r}$, donde los m_i son maximales distintos y los $n_i > 0$. Aplicamos entonces el teorema chino de los restos.

$$A \cong \frac{A}{m_1^{n_1}} \times ... \times \frac{A}{m_r^{n_r}}$$

Entonces si A es un anillo y $m \in \text{MaxSpec}(A) \implies \dfrac{A}{M^n}$ es un anillo local (con un único ideal maximal $\dfrac{m}{m^n}$)

La prueba se reduce ahora al caso en que A es un anillo local y su ideal maximal M satisface $m^n = 0$, para algún $n > 0$. Usamos inducción en n.

Si $n = 1$, entonces A es un cuerpo (sus únicos ideales son 0 y A)

Si $n > 1$ y se cumple para $n - 1$. Consideramos la sucesión exacta corta:

$$0 \to m^{n-1}M \to M \to \frac{M}{m^{n-1}M} \to 0$$

Donde $\dfrac{M}{m^{n-1}M}$ es un $\dfrac{A}{m^{n-1}}$-módulo. Y además, $m^{n-1}M$ es un $\dfrac{A}{m}$-esp. vectorial

□

Con esto podemos completar la demostración del teorema de Akizuki.

Demostración

$$A \text{ artiniano} \iff {}_AA \textit{ artiniano} \implies_{lem.\ Art}\ {}_AA \textit{ noeth.} \iff A \textit{ anillo noeth.}$$

□

Definición 4.4. *Un A-módulo M se dice de longitud finita si es noeth. y artiniano.*

Corolario 4.31. *Un anillo A es artiniano sii todo A-módulo f.g. es de longitud finita.*

Demostración

Akizuki $\implies$ A es noeth. $\implies$ todo $A-$módulo y f.g es noeth. y artiniano.

$\square$

Ejercicios

Ejercicio 1.

$$\mu(a+b)(x) = (a+b)(x) = ax + b = \mu(a)(x) + \mu(b)(x) \implies \mu(a+b) = \mu(a) + \mu(b)$$

$$\mu(ab)(x) = (ab)(x) = a(bx) = \mu(a)(\mu(b)(x)) = (\mu(a) \circ \mu(b))(x) \implies \mu(ab) = \mu(a) \circ \mu(b)$$

$$\mu(1)(x) = 1x = x \forall x \in M \implies \mu(1) = 1_M$$

Sea (M, f) un par formado donde M es un grupo abeliano y $f : A \to End_{\mathbb{Z}}(M)$ es un homomorfismo de anillos. Entonces M adquiere una estructura de A-módulo donde el producto es $A \times M \to M$ que viene definido por $(a, x) \mapsto ax := f(a)(x)$. Hay que probar varias propiedades:

$$a(x+y) = f(a)(x+y) = {}^{a}f(a)(x) + f(a)(y) = ax + ay$$

El resto de propiedades, como este, son rutinarias.

[a] f es un homomorfismo de grupos abelianos

Ejercicio 2.

"Pura rutina"

Ejercicio 3.

Apartado a)

$$X = \{x_j : j \in J\}$$

$$m, m' \in IX \implies \begin{cases} m = \sum_{j \in J} a_j x_j, \text{ con } a_i \in I, \forall i \in I \text{ y } a_i = 0 \ \forall i \in J \\ m' = \sum_{j \in J} a'_j x_j, \ \ldots \end{cases}$$

$$m + m' = \sum (a_j + a'_j) x_j \in IX$$

$$b \in A \ bm = b\sum_{j\in J} a_j x_j = \sum_{j\in J}(ba_j)x_j \in IX$$

Apartado b)

Tomamos $SN = \{m \in M : \ m = \sum_{j\in J} s_j x_j, \ con \ s_j \in S, \ x_j \in N\}$ *que es un* $A-$*submódulo de* M*. El resto es parecido al a).*

Ejercicio 4. *"Rutinario"*

Ejercicio 5.

Tendremos que probar que ϕ *conserva la suma y la multiplicación por elementos de* $K[X]$*.*

$$\phi\left[\left(\sum_{i=0}^{n}\lambda_i X^i\right)v\right] \stackrel{?}{=} \left(\sum_{i=0}^{n}\lambda_i X^i\right)\phi(v) \qquad \forall v \in V_1 \ \forall \sum_{i=0}^{n}\lambda_i X^i \in K[X]$$

Tenemos

$$\phi\left[\left(\sum_{i=0}^{n}\lambda_i X^i\right)v\right] = \phi\left(\sum_{i=0}^{n}\lambda_i f_1^i(v)\right) =_{\phi \ K-lineal} \sum_{i=0}^{n}\lambda_i\phi\left(f_1^i(v)\right) = \sum_{i=0}^{n}\lambda_i(\phi\circ f_1^i)(v)$$

$$= \sum_{i=0}^{n}\lambda_i(f_2^i\circ\phi)(v) = \sum_{i=0}^{n}\lambda_i f_2^i(\phi(v)) = \left(\sum_{i=0}^{n}\lambda_i X^i\right)\phi(v)$$

Ejercicio 6.

$\Longleftarrow$

Sea $f : \dfrac{A}{I} \to \dfrac{A}{J}$ *un A-homomorfismo.*

¿Cómo son los A-homomorfismos $f : \dfrac{A}{I} \to N$*, donde* $N \in_{A\,\mathrm{Mod}}$ *?*

Vienen unívocamente determinados por la imagen del $\overline{1}$*,* $f(\overline{1}) \in \{y \in N : Iy = 0\}$

Tenemos entonces una aplicación inducida:

$$\begin{aligned} \psi : \mathrm{Hom}_A\left(\frac{A}{I}, N\right) &\to \{y \in N : Iy = 0\} \\ f \qquad\qquad &\mapsto f(\overline{1}) \end{aligned}$$

Vemos que esta aplicación tiene inversa: dado $y \in \{y \in N : \ Iy = 0\}$*, podemos tomar* $\mu_y : \dfrac{A}{I} \to N$ *determinada por* $\mu_y(\overline{1}) = y$*. Se deja como ejercicio probar que esta asignación define la inversa.*

Volviendo al inicio, y denotando con $\bar{\cdot}$ *a las clases de* $\dfrac{A}{I}$ *y con* $[]$ *a las de* $\dfrac{A}{J}$ *sabemos que*

$f = \mu_{[b]} : \overline{a} \mapsto [ab]$ *donde* $[b] \in \{[c] \in \frac{A}{J} : \ I[c] = [0]\} = \{c + J : \ Ic \subseteq J\} = \frac{(J:I)}{J}$.

Como conlusión, llegamos a que $f = \mu_{[b]}$*, donde* $[b] \in \frac{(J:I)}{J} (\iff b \in (J:I))$

Vemos cuando es este $\mu_{[b]}$ *inyectivo. Lo será cuando*

$$\begin{array}{rcl} \mu_{[b]} = (\overline{a}) = [0] & \Longrightarrow & \overline{a} = \overline{0} \\ [ab] = [0] & \Longrightarrow & \overline{a} = \overline{0} \\ \Updownarrow & & \Updownarrow \\ ab \in J & \Longrightarrow & a \in I \\ a \in (J:b) & \Longrightarrow & a \in I \iff (J:b) \subseteq I \end{array}$$

En conclusión, $\mu_{[b]}$ *intectivo sii* $(J:b) \subseteq I$

Comprobarmos ahora cuando es $\mu_{[b]}$ *suprayectivo.*

$$\operatorname{Im}(\mu_{[b]}) = \{[ab] : \ \overline{a} \in \frac{A}{I}\} = \{ab + J : \ a \in A\} = \frac{Ab + J}{J}$$

Luego $\mu_{[b]}$ *es sobre* $\iff \frac{Ab+J}{J} = \frac{A}{J} \iff Ab + J = A \Longrightarrow I(Ab+J) = I \Longrightarrow I = Ib + IJ \subseteq J + IJ = J$

Ejercicio 7. ***Apartado a)***

Basta con ver que L *es cíclico de orden 3, luego* $((0,6)) \cong \mathbb{Z}_3$

$$\frac{M}{K} = \frac{\mathbb{Z}_3 \oplus \mathbb{Z}_9}{\mathbb{Z}_3 \oplus 0} \cong \frac{\mathbb{Z}_3}{\mathbb{Z}_3} \oplus \frac{\mathbb{Z}_9}{0} \cong \mathbb{Z}_9$$
$$\frac{M}{L} = \frac{\mathbb{Z}_3 \oplus \mathbb{Z}_9}{0 \oplus (6)} \cong \mathbb{Z}_3 \oplus \frac{\mathbb{Z}_9}{(6)} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

No son isomorfos porque uno es cíclio y el otro no.

Apartado b)

$$\frac{M}{K+L} = \frac{\mathbb{Z}_3 \oplus \mathbb{Z}_9}{\mathbb{Z}_3 \oplus (6)} = 0 \oplus \frac{\mathbb{Z}_9}{(6)} \cong \mathbb{Z}_3$$
$$\frac{M}{N} = \frac{\mathbb{Z}_3 \oplus \mathbb{Z}_9}{0 \oplus \mathbb{Z}_9} = \cong \mathbb{Z}_3$$

$$K + L = \mathbb{Z}_3 \oplus (6) \cong \mathbb{Z}_3\mathbb{Z}_3$$
$$N \cong \mathbb{Z}_9$$

Ejercicio 10.

Pongamos que $N = (x_1, ..., x_s)$ *y* $\dfrac{M}{N}(\overline{y}_1, ..., \overline{y}_t)$.

Parece razonable comprobar que $M = (x_1, ..., x_s, y_1, ..., y_t)$, *donde los* y_i *son representantes arbitrarios de las clases* $\overline{y}_i$.

Sea $m \in M \implies \overline{m} = m + N = \sum_{j=1}^{t} b_j \overline{y}_j$ *donde los* $b_j \in A$

Pero $\sum_{j=1}^{t} b_j \overline{y}_j = \overline{\sum b_j y_j} = m$. *Por lo tanto:*

$$m - \sum_{j=1}^{t} b_j y_j \in N \implies m - \sum_{j=1}^{t} b_j y_j = \sum_{i=1}^{s} a_i x_i$$

Con $a_i \in A$. *Por lo tanto:*

$m = \sum_{i=1}^{s} a_i x_i + \sum_{j=1}^{t} b_j y_j$

Ejercicio 12.

Si $\mathbb{Z}[\frac{1}{q}] = \{\frac{m}{q^t} : \ m \in Z, \ t \geq 0\}$ *fuera finitamente generado, tomamos denominadores comunes y podemos expresar* $\mathbb{Z}[\frac{1}{q}]$ *como:*

$$Z[\frac{1}{q}] = \left(\frac{m_1}{q^t}, ..., \frac{m_n}{q^t}\right)$$

Pero entonces $\dfrac{1}{q^{t+1}}$ *no se puede generar (o algo así era).*

Ejercicio 14.

Probamos primero que $\mathrm{Ker}(f) \cap \mathrm{Im}(f) = 0$

Sea $x \in \mathrm{Ker}(f) \cap \mathrm{Im}(f) \implies$

$$\left\{ \begin{array}{l} f(x) = 0 \\ y \\ x = f(z), \ z \in M \end{array} \right\} \implies f(f(z)) = 0 \iff f^2(z) = 0 \implies_{f^2 = f} \implies f(z) = 0 \implies x = 0$$

Luego la intersección es nula.

La segunda parte será probar que $M = \mathrm{Ker}(f) + \mathrm{Im}(f)$.

Sea $x \in M$, *podemos expresarlo como* $(x - f(x)) + f(x)$ *y tendríamos que probar que* $(x - f(x)) \in \mathrm{Ker}(f)$

$$f(x - f(x)) = f(x) - f^2(x) = f(x) - f(x) = 0$$

Ejercicio 15.

Tenemos las bases de los módulos libres:

$$K = ((1,0,-1),(0,1,-1)) \qquad L_1 = ((1,0,1),(0,0,1)) \qquad L_2 = ((1,2,3))$$

$$L_3 = ((1,1,1)) \qquad L_4 = ((0,0,1))$$

¿Cuándo es $K \oplus L_i = \mathbb{Z}^3$? Vemos primero cuándo tienen intersección nula: "a ojo" se ve que se da para L_2, L_3, L_4 pero no para L_1.

Para $i = 2,3,4$ se tiene que $K \oplus L_i$ es libre con base $\{(1,0,-1),(0,1,-1),v_i\} = \mathcal{B}_i$ con cada v_i el elemento de la base de L_i.

Entonces $K \oplus L_i = \mathbb{Z}^3$ será cierta sii $\mathcal{B}_i$ es un conjunto generador de $\mathbb{Z}^3$.

Vemos algún caso, si $i = 2$: ¿$\forall (a,b,c) \in \mathbb{Z}^3,\ \exists x,y,z \in \mathbb{Z}$ tal que

$$x(1,0,-1) + y(0,1,-1) + z(1,2,3) = (a,b,c)?$$

$$\begin{cases} \begin{array}{rrrr} x & & +z & = a \\ & y & +2z & = b \\ -x & -y & +3z & = c \end{array} \end{cases}$$

Se tendría que resolver como cualquier sistema lineal haciendo transformaciones elementales. Sin embargo, solo se pueden multiplicar filas (columnas) por unidades de $\mathbb{Z}$, es decir, ± 1. Queda finalmente:

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & a \\ 0 & 1 & 2 & b \\ -1 & -1 & 3 & c \end{array}\right) \leftrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & a \\ 0 & 1 & 2 & b \\ 0 & 0 & 6 & a+b+c \end{array}\right)$$

Y queda $6z = a+b+c$ y no tenemos solución.

Con $i = 4$ sí tenemos solución. Haciendo un razonamiento parecido llegamos a:

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ -1 & -1 & 1 & c \end{array}\right) \leftrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & a+b+c \end{array}\right)$$

Ejercicio 16.

Lo primero que tenemos que probar es que si q es primo, entonces:

$$\mathbb{Z}_{q^\infty} \cap \left(\sum_{p \neq q} \mathbb{Z}_{p^\infty} \right) = 0$$

Si no fuera así, tendríamos:

$$\left[\frac{m}{q^t}\right] = \left[\frac{m_1}{p^{s_1}}\right] + ... + \left[\frac{m_r}{p_r^{s_r}}\right] \qquad s_i > 0$$

Podemos suponer que tenemos la misma potencia para los primos p_i, s, sin pérdida de generalidad. Entonces tendríamos:

$$\left[\frac{m}{q^t}\right] = \left[\frac{m_1'}{p_1^s \cdots p_r^s} + ... + \frac{m_r'}{p_1^s \cdots p_r^s}\right] \implies$$

$$\implies \frac{m}{q^t} - \frac{m_1' + ... + m_r'}{(p_1 \cdots p_r)^s} \in \mathbb{Z} \implies (p_1 \cdots p_r)^s m - (m_1' + ... + m_r')q^t = q^t (p_1 \cdots p_r)^s z, \; z \in \mathbb{Z}$$

$$\implies q^t | (p_1 \cdots p_r)^s m \implies q^t | m \implies \left[\frac{m}{q^t}\right] = [0]$$

Lo segundo que tenemos que ver es que $\frac{\mathbb{Q}}{\mathbb{Z}} \subseteq \bigoplus_{p\ primo} \mathbb{Z}_{p^\infty}$

Dado un elemento $[a/b] \in \mathbb{Q}/\mathbb{Z}$*, podemos expresarlo como a* $\left[\frac{1}{b}\right]$*. Hemos de probar entonces que:*

$$\left[\frac{1}{b}\right] \in \bigoplus_{p\ primo} \mathbb{Z}_{p^\infty} \;\; \forall b \in \mathbb{N} \setminus \{0\}$$

Suponemos $b > 1 \implies b = p_1^{\mu_1} \cdots p_r^{\mu_r}$*, con los* $p_i > 0$ *distintos y los* $\mu_i > 0$*.*

Lo haremos por inducción en r*.*

Si $r = 1,\; b = p_1^{\mu_1} \implies \left[\frac{1}{b}\right] = \left[\frac{1}{p_1^{\mu_1}}\right] \in \mathbb{Z}_{p_1^\infty}$

Sea ahora $r > 1$*, lo que haremos será separar* $p_1^{\mu_1}$ *del resto. Entonces* $p_1^{\mu_1},\; p_2^{\mu_2} \cdots p_r^{\mu_r}$ *son coprimos y aplicando Bézout:*

$$\exists u, v \in \mathbb{Z} : \;\; p_1^{\mu_1} u + p_2^{\mu_2} \cdots p_r^{\mu_r} = 1$$

$$\frac{1}{b} = \frac{1}{p_1^{\mu_1} \cdots p_r^{\mu_r}} = \frac{u}{p_2^{\mu_r} \cdots p_r^{\mu_r}} + \frac{v}{p_1^{\mu_1}}$$

Y tomando módulos:

$$\left[\frac{1}{b}\right] = \left[\frac{u}{p_2^{\mu_r} \cdots p_r^{\mu_r}}\right] + \left[\frac{v}{p_1^{\mu_1}}\right]$$

Aplicando ahora la hipótesis de inducción, terminamos el ejercicio.

Ejercicio 17.

$1 \implies 2.$

Si B es una base de $F \leq_Z \mathbb{Q} \implies |B| \leq 1 \implies F$ es cíclio.

$2 \implies 1.$

Sea $F = \left(\frac{a}{b}\right)$, $\frac{a}{b} \neq 0$ (si fuera = 0, lo tendríamos directamente). Podemos crear un homomorfismo:

$$\begin{aligned} \mathbb{Z} \to & \quad F \\ m \mapsto & \quad m\frac{a}{b} = \frac{ma}{b} \end{aligned}$$

Es directo ver que es inyectivo, luego es un isomorfismo y el anillo es libre.

$2 \iff 3.$

$$F = \left(\frac{a_1}{b_1}, ..., \frac{a_n}{b_n}\right) \text{ con } \frac{a_i}{b_i} \neq 0 \ \forall i = 1, ..., n$$

Se pueden reducir las fracciones a común denominador:

$$F = \left(\frac{a_1'}{b}, ..., \frac{a_n'}{b}\right) \subseteq \left(\frac{1}{b}\right)$$

Pero este último es ismorfo a $\mathbb{Z}$ por el apartado anterior.

CAPÍTULO 5

Módulos sobre DIP

Ejercicios

Ejercicio 2.

Apartado c)

Es un caso particular de b). Utilizando que $\bigcap_{i\in I}(b_i) = (mcm_{i\in I}(b_i))$

Ejercicio 3.

Tomemos $k < n$ *y sea* $\overline{a} \in M$ *tal que* $\overline{a} \in ann_M(p^k)$*:*

$$\iff p^k\overline{a} = \overline{0} \iff \overline{p^k a} = \overline{0} \iff p^n | p^k a \iff p^{n-k} | a \iff a \in (p^{n-k}) \iff {}^{a}\overline{a} \in \frac{(p^{n-k})}{(p^n)}$$

Si $k \geq n$*, entonces :*

$$p^n M = 0 \implies p^k M = 0 \ \forall k \geq n \iff ann_M(p^k) = M \ \forall k \geq n$$

Probamos ahora que:

$$ann_M(p) = \frac{(p^{n-1})}{(p^n)}$$

Sabemos que $\dim V = 1 \iff \exists f : K \to V$ *lineal y biyectiva con* $\dim K = 1$.

Entonces buscamos una aplicación lineal y biyectiva $f : \dfrac{A}{(p)} \to \dfrac{(p^{n-1})}{(p^n)}$*. Basta tomar la aplicación* $f(\overline{a}) = \overline{p^{n-1}a}$*. Para ver que es biyectiva, basta ver que es sobre al ser homomorfismo de módulos y que el espacio de salida es de dimensión 1.*

[a] Teorema de la correspondencia

Ejercicio 4. *Para hacer este ejercicio hace falta resolver el ejercicio 6.*

Tenemos que en $\frac{Q}{A}$, *cualquier elemento* $\left[\frac{a}{b}\right]$ *es anulado por* $b : b\left[\frac{a}{b}\right] = [a] = [0] \implies \frac{Q}{A} \in \mathcal{T}$.

Volviendo al caso general, se tiene $N \cap A \subseteq N \subseteq Q$

Observación

Tenemos un epimorfismo de $A-$*módulos:*

$$\begin{aligned} \pi : \frac{Q}{N \cap A} &\to \frac{Q}{N} \\ [q] &\mapsto \overline{q} \end{aligned}$$

Basta entonces probar que si $N' \leq_A A(\iff N'$ *ideal de* $A)$, *entonces* $\frac{Q}{N'} \in \mathcal{T}$.

Sea $\overline{q} = q + N'$, *quiero probar que existe* $a \in A \setminus \{0\} :\ a\overline{q} = \overline{0}$

Sabemos que $[q] := q + A$ *es un elemento de torsión en* $\frac{Q}{A} \implies \exists b \in A \setminus \{0\}$ *tal que* $b[q] = [0] \iff [bq] = [0]$ *en* $\frac{Q}{A}$:

$$\implies \exists b \in A \setminus \{0\} :\ b[q] = [0] \iff [bq] = [0] \text{ en } \frac{Q}{A} \implies bq \in A$$

Entonces: $N' \trianglelefteq A \implies_{A\ DIP} N' = (r) \implies \frac{A}{N'} = \frac{A}{(r)} \in \mathcal{T} \implies r(bq) \in N' \iff rb\overline{q} = \overline{0}$ *en* $\frac{Q}{N'}$

Ejercicio 6.

Apartado a)

Supongamos $N, \frac{M}{N} \in \mathcal{T}$, *vemos que* $M \in \mathcal{T}$, *es decir, que* $\forall x \in M,\ \exists a \in A \setminus \{0\} :\ ax = 0$.

Sea $x \in M \implies \overline{x} := x + N$ *es de torsión en* $\frac{M}{N} \implies$

$$\implies \exists a \in A \setminus \{0\} :\ a\overline{x} = \overline{0} \iff \overline{ax} = \overline{0} \iff ax \in N \implies_{N \text{ de torsión}}$$

$$\implies \exists b \in A \setminus \{0\} :\ b(ax) = 0 \implies ba \neq 0 \text{ y } (ba)x = 0$$

Por lo tanto, $M \in \mathcal{T}$

Recordemos que $M \in \mathcal{F} \iff t(M) = 0 \iff \forall x \in M \setminus \{0\}$ *se tiene:*

Comprobamos que $N, \frac{M}{N} \in \mathcal{F} \implies M \in \mathcal{F}$

Sea $x \in M \setminus \{0\}$ *y supongmos que* $\exists a \in A \setminus \{0\} :\ ax = 0 \implies$

$$\implies \overline{ax} = \overline{0} \iff \overline{ax} = \overline{0} \implies_{M/N \in \mathcal{F}} \overline{x} = \overline{0} \iff x \in N$$

$\implies x \in N \setminus \{0\}$ *y* $ax = 0$ *con* $a \neq 0$, *luego tenemos una contradicción con* $N \in \mathcal{F}$

Apartado b)

Los casos $M \in \mathcal{T} \implies N, \dfrac{M}{N} \in \mathcal{T}$ *y* $M \in \mathcal{F} \implies N \in \mathcal{F}$ *quedan como ejercicio planteado.*

El caso $M \in \mathcal{F} \implies \dfrac{M}{N} \in \mathcal{F}$ *no se cumple, basta tomar* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$

Apartado c)

Este ejercicio es una consecuencia directa de la parte planteada en el apartado anterior.

Apartado d)

Tomamos la proyección, que es homomorfismo suprayectivo $K \oplus N \xrightarrow{\pi} K + N$. *Entonces* $K + N \cong \dfrac{K \oplus N}{\operatorname{Ker}(\pi)}$

Vemos que $K \oplus N \in \mathcal{T}$, *sabemos que* $\dfrac{K \oplus N}{K \oplus 0} \cong N$, *entonces:*

$$\left\{ \begin{array}{l} \dfrac{K \oplus N}{K \oplus 0} \in \mathcal{T} \\ K \oplus 0 \cong K \in \mathcal{T} \end{array} \right. \implies_{\textit{Apartado a)}} K \oplus N \in \mathcal{T}$$

Podemos ver que el otro caso falla, sea $M = \mathbb{Z} \oplus \mathbb{Z}_2$ *y tomemos* $K = \mathbb{Z}(m, \overline{1})$ *libre de torsión y* $\mathbb{Z}(m, \overline{0}) = N$ *libre de torsión* ($m \neq 0$). *Entonces* $(m, \overline{1}) - (m, \overline{0}) \in K + F$ *es un elemento de torsión.*

Más generalmente, si $F \neq 0, T \neq 0$ *son un módulo libre de torsión y de torsión respectivamnte no nulos, entonces* $\exists K, N \leq_A M := F \times T :\ K, N \in \mathcal{F}$ *pero* $K + N \notin \mathcal{F}$, *(siendo* A *un DIP).*

Ejercicio 7.

Sea $(x_p)_{p \in \mathcal{P}} \in t\left(\prod_{p \in \mathcal{P}} \mathbb{Z}_p\right) \implies$

$$\exists a \in \mathbb{Z} \setminus \{0\} :\ a(\overline{x})_{p \in \mathcal{P}} = 0 = (\overline{0}_p)_{p \in \mathcal{P}} \iff a\overline{x}_p = \overline{0} \text{ en } \mathbb{Z}_p\ \forall p \in \mathcal{P} \iff p | a x_p\ \forall p \in \mathcal{P} \iff$$

$$\iff \overline{x}_p = \overline{0}\ \forall p \in \mathcal{P} \text{ que no sea divisor de } a \implies t\left(\prod_{p \in \mathcal{P}} \mathbb{Z}_p\right) \subseteq \bigoplus_{p \in \mathcal{P}} \mathbb{Z}_p$$

La otra inclusión es más directa.

Ejercicio 8.

Se hace utilizando transformaciones elementales hasta llegar a la forma normal, primero las filas y luego las columnas. Recordando la demostración vista en clase, en este caos tenemos que tomar $\delta = |\cdot| : \mathbb{Z} \to \mathbb{N}$. *Las transformaciones son:*

- $F_1 \leftrightarrow F_3$
- $F_2 + 2F_1, F_3 - 7F_1$
- $C_2 + 2C_1,\ C_3 - 7C_1,\ C_4 + C_1$

- $C_2 \leftrightarrow C_4$
- $C_3 + 12C_1,\ C_4 + 6C_1$

Y se llega a la matriz:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -132 & -30 \end{pmatrix}$$

Hay que hacer la división euclídea para la siguiente transformación $-132 - 4 * (-30) = -12$, $C_3 - 4C_4$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -12 & -30 \end{pmatrix}$$

De nuevo son división euclídea: $-30 - 2(-12) = -6$, $C_4 - 2C_3$*:*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -12 & -6 \end{pmatrix}$$

Haciendo $C_3 \leftrightarrow C_4$*:*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -6 & -12 \end{pmatrix} \xrightarrow{C_4 - 2C_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -6 & 0 \end{pmatrix} \xrightarrow{(-1)F_2} \begin{pmatrix} diag(1,1,-6) & 0 \\ 0 & 0 \end{pmatrix}$$

Ejercicio 9. *Descomponemos primero cada componente:*

$$\mathbb{Z}_{24}:\ 24 = 2^3 \cdot 3 \to (2^3, 3)$$

$$\mathbb{Z}_{30}:\ 30 = 2 \cdot 3 \cdot 5 \to (2, 3, 5)$$

$$\mathbb{Z}_{75}:\ 75 = 3 \cdot 5^2 \to (3, 5^2)$$

Entonces por el teorema chino de los resto, los divisores elementales son: $2, 2^3, 3, 3, 3, 5, 5^2$.

Para los factores invariantes usamos la prueba del teorema 5.3:

$$\begin{cases} d_{t-2} = 3d_{t-1} = 2 \cdot 3 \cdot 5 = 30 \\ d_t = 2^3 \cdot 3 \cdot 5 = 600 \end{cases}$$

Se construye de abajo a arriba. Para d_t *tomamos cada primo de los divisores elementales elevado al mayor exponente con el que aparece. Seguimos con* d_{t-1} *con el segundo mayor exponente etc.*

Ejercicio 10.

$$M = \langle a, b, c | 4a + 4b + 2c, 2a - 4b + 3c \rangle = M(C)$$

$$C = \begin{pmatrix} 4 & 2 \\ 4 & -4 \\ 2 & 3 \end{pmatrix}$$

$$\begin{aligned} \mathbb{Z}^2 \to & \qquad\qquad\qquad \mathbb{Z}a \oplus \mathbb{Z}b \oplus \mathbb{Z}c \\ e_1 \mapsto & \; 4a + 4b + 2c \\ e_2 \mapsto & \; 2a - 4b + 3c \end{aligned}$$

Y haremos transformaciones elementales para llegar a la forma normal:

- $C_1 \leftrightarrow C_2$
- $F_3 - F_1$
- $F_1 \leftrightarrow F_3$
- $F_2 + 4F_1, \;\; F_3 - 2F_1$
- $C_2 + 2C_1$
- $F_3 + 2F_2$

Y nos queda:

$$C' = \begin{pmatrix} 1 & 0 \\ 0 & -4 \\ 0 & 0 \end{pmatrix} = PCQ^{-1}$$

$$\left\{ \begin{array}{c} s = 1 \\ t = 1 \\ m = 3 \end{array} \right\} \Longrightarrow \textit{ el rango libre de torsión es 1}$$

Factores invariantes: 4, luego el único divisor elemental es 2^2, $M \cong \mathbb{Z}_4 \oplus \mathbb{Z}$

Vamos a calcular una descomposición interna (aunque no la pida el ejercicio):

Queremos ahora encontrar una descomposición en suma directa interna $M = M_1 \oplus M_2$ *con* $M_1 \cong \mathbb{Z}_4$ *y* $M_2 \cong \mathbb{Z}$

Para esto necesitamos P^{-1}*. Para calcular esta matriz hay que hacer las transformaciones que hemos hecho anteriormente en orden inverso a la matriz identidad. El resultado es:*

$$P^{-1} = \begin{pmatrix} 2 & -2 & 1 \\ -4 & 1 & 0 \\ 3 & -2 & 1 \end{pmatrix}$$

$$M(C) = \frac{\mathbb{Z}}{(1)} \oplus \frac{\mathbb{Z}}{(4)} \oplus \frac{\mathbb{Z}}{(0)} \to M = M(C)$$

Tomando $\{a, b, c\}$ *como base de* $\mathbb{Z}a \oplus \mathbb{Z}b \oplus \mathbb{Z}c$*, vemos las imágenes que han de tener* $\{e_1, e_2, e_3\}$

$$\overline{e_1} = \overline{0} \mapsto 0$$
$$\overline{e_2} \mapsto \overline{P^{-1}e_2} = \overline{-2a + b - 2c}$$
$$\overline{e_3} \mapsto \overline{P^{-1}e_3} = \overline{a + c}$$

Entonces, $M = (\overline{-2a + b - 2c}) \oplus (\overline{a + c})$

Ejercicio 11.

Hacemos solo el de 324 $= 2^2 \cdot 3^4$*. Sabemos que:*

$$M = \left(\bigoplus_{j=1}^{r_1} \frac{\mathbb{Z}}{(2^{n_{1j}})} \right) \oplus \left(\bigoplus_{j=1}^{r_2} \frac{\mathbb{Z}}{(3^{n_{2j}})} \right) \tag{5.1}$$

Con $0 < n_{i_1} \leq n_{i_2} \leq ... \leq n_{i_1 r_1}$

$$2^2 3^4 = \left(\prod_{j=1}^{r_1} 2^{n_{1j}} \right) \left(\prod_{j=1}^{r_2} 3^{n_{2j}} \right) = 2^{\sum_{j=1}^{r_1} n_{1j}} \cdot 3^{\sum_{j=1}^{r_2} n_{2j}}$$

Entonces igualando exponentes:

$$\sum_{j=1}^{r_1} n_{1j} = 2 \qquad \sum_{j=1}^{r_2} n_{2j} = 4$$

Tomando entonces los posibles valores de n_{ij} *para que se den esas igualdades, tenemos los posibles grupos pedidos sustituyendo en* (5.1)*. Estos posibles valores son:*

$$(2, 2, 3^4), (2, 2, 3, 3^3), (2, 2, 3^2, 3^2), (2, 2, 3, 3, 3^2), (2, 2, 3, 3, 3, 3),$$
$$(2^2, 3^4), (2^2, 3, 3^3), (2^2, 3^2, 3^2), (2^2, 3, 3, 3^2), (2^2, 3, 3, 3, 3)$$

Ejercicio 12.

Apartado a)

Por el ejercicio 11 de la teoría sabemos que $g = f_C$ *para una única* $C \in M_{n\times n}(\mathbb{Z})$

$$M = \frac{\mathbb{Z}^n}{\mathrm{Im}(g)} = \frac{\mathbb{Z}^n}{\mathrm{Im}(f_C)} = M(C)$$

Entonces $M = M(C)$ *es finito* $\iff$ $M(C')$ *es finito, siendo* C' *la forma normal de* C.

Recordemos que:

$$C = \left(\begin{array}{c|c} diag(1, ..., 1, d_1, ..., d_t) & 0 \\ \hline 0 & 0 \end{array} \right) \tag{5.2}$$

$M(C')$ *es finito* $\iff n - s - t^a = 0 \iff C' = \mathrm{diag}(1, ..., 1, d_1, ..., d_t)$

Como A *es un DIP y* $C' = PCQ$ *con* $C, C' \in M_{n\times n}(A),\ P, Q \in GL_n(A) \implies$

$$\det(C') = \underbrace{\det(P)\det(Q)}_{\in \mathcal{U}(A} \det(C) \implies$$

Se tiene que $\det(C')$ *y* $\det(C)$ *son asociados en* A*. Hasta ahora tenemos:*

M finito $\overset{?}{\iff} \det(C) \neq 0 \iff \det(C') \neq 0 \iff d_1 \cdots d_t \neq 0$

Para comprobar la equivalencia que no tenemos, vemos que M finito $\iff d_1 \cdots d_t \neq 0$

En el caso en el que no haya d_i*, tenemos que* $M = 0$*. Vamos con el caso general:*

$\Longleftarrow$

$$M \cong \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_t} \implies |M| = |d_1 \cdots d_t| = |\det(C)| = |\det(g)|$$

$\Longrightarrow$

Directo.

Apartado b)

Lo hemos visto al hacer $\Longleftarrow$ *en el apartado anterior.*

[a]Tamaño de la matriz de ceros en la parte inferior derecha de C'

Ejercicio 13.

a) $\Longrightarrow$ *b)*

$$p(f) = 0 \iff p(f)(v) = 0 \ \forall v \in V \iff {}^{a}p(x)v = 0 \ \forall v \in M = V \iff p(x)M = 0$$

Donde para la última implicación se ha usado que: "A−módulo" = "A-módulo anulado por I" $(I \trianglelefteq A)$*, entonces* M *es un* $\dfrac{K[X]}{(p(x))}$*−esp. vectorial.*

$K' = \dfrac{K[X]}{(p(x))}$ *y sea* $\{v_1, ..., v_t\}$*, es* K'*−base de* M *sii se tiene una descomposición en suma directa interna de* K'*-subesp. vect.* $M = K'v_1 \oplus ... \oplus K'v_t$ *sii* $M = K[x]v_1 \oplus ... \oplus K[x]v_t$*, como* $K[X]$*-submódulo.*

Observación

$K[x]v_j = K$*−subesp. vectorial de* V *generado por* $\{f^k(v_j) : \ k \in \mathbb{N}\}$*. Ya que se tiene que:*

$$K[x]v_j = \{\left(\sum_{k=0}^{s} \lambda_k x^k\right) v_j : \ \sum \lambda_k x^k \in K[X]\} = \{\sum_{k=0}^{s} \lambda_k f^k(v_j) : \ \lambda_k \in K \ \forall k \in \mathbb{N}\} =$$

$$= \langle f^k(v_j) : \ k = 0, 1, ... \rangle$$

Fin de la observación

Como se tiene que:

$$p(x) = x^d + \lambda_{d-1} x^{d-1} + ... + \lambda_1 x + \lambda_0$$

Llegamos a:

$$0 = p(f)(v_j) = f^d(v_j) + \lambda_{d-1} f^{d-1}(v_j) + ... + \lambda_1 f(v_j) + \lambda_0 1_v(v_j) \implies f^d(v_j) =$$

$$= -\sum_{i=0}^{d-1} \lambda_k f^k(v_j) \implies f^d(v_j) \in \langle v_j, f(v_j), ..., f^{d-1}(v_j) \rangle$$

Luego $\{v_j, f(v_j), ..., f^{d-1}(v_j)\}$ *es conjunto generador, vemos que es base (es LI). Supongamos:*

$$\sum_{k=0}^{d-1} \mu_k f^k(v_j) = 0, \ \mu_k \in K \ \forall k$$

Si algún μ_k *es no nulo, entonces* $G := \sum_{k=0}^{d-1 \mu_k x^k}$ *y se tiene que* $G(x)v_j = 0$. *Entonces* $p(x)$ *y* $G(x)$ *son coprimos y por la identidad de Bézout* $\exists F(x), H(x) \in K[X]$ *tales que* $F(x)p(x) + H(x)G(x) = 1$, *luego se tiene:*

$$v_j = 1v_j = \Big(F(x) + p(x) + H(x)G(x)\Big)v_j = F(f)(\underbrace{p(f)(v_j)}_{=0}) + H(f)(\underbrace{G(f)(v_j)}_{=0}) = 0$$

Lo que es una contradicción.

Como conclusión, si se tiene (V, f) *arbitrario y* $v \in V \setminus \{0\}$, *entonces* $K[X]v = \langle f^k(v) : \ k \in N \rangle$ *y una base suya es* $\{v, f(v), ..., f^{d-1}(v)\}$ *donde* $d = \deg(F)$ *para* $(F) = ann_A(M)$

b) $\implies$ *a)*

Sea $\bigcup_{j=1}^{t} \{v_j, f(v_j), ..., f^{d-1}(v_j)\}$ *base de* V

Observación

$$\langle v_j, f(v_j), ..., f^{d-1}(v_j) \rangle = K[X]v_j$$

Entonces:

$$\begin{array}{lllll} \textit{Como esp. vectorial:} & V & = \bigoplus_{j=1}^{t} & \langle v_j, f(v_j), ..., f^{d-1}(v_j) \rangle & \\ \textit{Como módulos} & M & = \bigoplus_{j=1}^{t} & K[X]v_j & = {}^{b} \bigoplus_{j=1}^{t} \dfrac{K[X]}{(p(x))} v_j \end{array}$$

[a] Viendo como módulo
[b] Ya que $p(x)M = 0$

Ejercicio 17.

$$\phi_C(x) = (x^2 - x + 1)^2$$

$$C' = \bigoplus_{j=1}^{t} C_{n_j}(x^2 - x + 1)$$

$$\phi_C(x) = \phi_{C'}(x) = \prod_j (x^2 - x + 1)^{n_j}$$

$$\begin{cases} C_2(x^2 - x + 1) \to pmin = (x^2 - x + 1) \\ C_1(x^2 - x + 1) \oplus C_1(x^2 - x + 1) \to pmines x^2 - x + 1 \end{cases}$$

El segundo caso se da sii $C^2 - C + I = 0$. *Sí se cumple, así que* $C' = C_1(x^2 - x + 1) \oplus C_1(x^2 - x + 1)$.

Por el teorema 6.9, tenemos que $F = F_1$ *y* $|F_1| = 2$.

Necesitoamos entonces $v_1, v_2 \in F_1$ *tales que* $v_1, v_2 \in \mathrm{Ker}(C^2 - C + I)$ *induzcan una base en* $\frac{\mathrm{Ker}(C^2 - C + I)}{\mathrm{Ker}(C^2 - C + I)} = \frac{\mathbb{R}^4}{0}$ *como* $\frac{K[X]}{(x^2 - x + 1)}$*-esp. vectorial.*

En este caso queremos $v_1, v_2 \in \mathbb{R}^2 = M_{(V, f_c)}$ *sean una base como* $\frac{K[X]}{(x^2 - x + 1)}$*-esp. vectorial.*

Necesito $v_1, v_2 \in \mathbb{R}^4$ *tales que* $\{v_1, f(v_1), v_2, f(v_2)\}$ *base de* V *como* $\mathbb{R}-$*esp. vectorial. Tomamos* $v_1 = e_1$ *y* $v_2 = e_4$ *nos queda:*

$$\{e_1, e_1 + e_2 + e_3 + e_4, e_4, -e_3\}$$

Ejercicio 18. ***Ejercicio planteado***

Dado M*,* $A-$*módulo siendo* A *un DIP. Se tiene* $v_g(p_i)$ *la multiplicidad geométrica de cada* p_i *en la descomposición de* M*. Demostrar entonces que:*

$$v_g(p_i) = \dim_{A/(p)} ann_M(p_i)$$

Tendremos entonces el caso particular $f : V \to V$ un K-endomorfismo y $\dim V < \infty$, entonces $M_B(f) \sim C' = \bigoplus_{i=1}^{k} \left(\bigoplus_{j=1}^{r} C_{nij}(p_i) \right)$

$$v_g(p_i) = r_i = \dim_{K[X]/(p_i(x))} \mathrm{Ker}(p_i(f)) = \frac{\dim_K \mathrm{Ker}(p_i(f))}{\deg(p_i)} = \frac{\dim V - \mathrm{rang}(p_i(f))}{\deg(p_i)}$$

Y otro caso aún más particular:

$p_i(x) = x - \lambda_i$ para λ_i valor propio de f.

$$v_g(\lambda_i) := v_g(x - \lambda_i) = \mathrm{V} - \mathrm{rang}(p_i(f)) = \text{nº bloques de Jordan que aparecen en } C'$$

Utilizaremos esto en otros ejercicios.

Ejercicio 28.

Apartado b)

Tenemos $\dim V = 6$*,* $d_f(x) = (x+3)^2(x+1)^2$

$$u_f(x) = (x+3)^{m_1}(x+1)^{m_2}$$

Donde se tiene que $2 \leq m_i$ *y* $m_1 + m_2 = 6$

Por lo tanto, las combinaciones posibles de m_1, m_2 *son* $\{(2,4), (3,3), (4,2)\}$*. Vemos cada caso:*

El polinomio cada característico en cada caso es $(x+3)^2(x+1)^4$, $(x+3)^3(x+1)^3$ *y* $(x+3)^4(x+1)^2$.

Los divisores elementales en cada caso son:

- $(x+3)^2, (x+1)^2, (x+1)^2$ *o* $(x+3)^2, (x+1), (x+1), (x+1)^2$
- $x+3, (x+3)^2, x+1, (x+1)^2$

- $(x+3)^2, (x+3)^2, (x+1)^2$ *o* $x+3, x+3, (x+3)^2, (x+1)^2$

El método para ver los factores invariantes lo hemos estudiado en otros ejercicios ya.

Vamos con la multiplicidad en cada caso. Usamos el ejercicio propuesto y su caso particular. Lo vemos para cada caso.

- *(1,2) o (1,3)*
- *(2,2)*
- *(2,1) o (3,1)*

Por último, esto son las posibles formas de Jordan:

- $J_2(-3) \oplus J_2(-1) \oplus J_2(-1)$ *o* $J_2(-3) \oplus J_1(-1) \oplus J_1(-1) \oplus J_2(-1)$
- $J_1(-3) \oplus J_2(-3) \oplus J_1(-1) \oplus J_2(-1)$

Ejercicio 29.

$$n(-1) = \min\{s > 0 : \operatorname{rang}(C+I)^s = \operatorname{rang}(C+I)^{s+1}\} \implies M(x+1) = \operatorname{Ker}(((C+I)^{n(-1)})) =$$

$$= \{v \in V : \ (C+I)^t v = 0 \textit{ para algún } t > 0\} = \bigcup_{t>0} \operatorname{Ker}(((C+I))^t)$$

Apartado c)

Nos pude una base $\mathcal{B}'$ *de* $\operatorname{Ker}(((C+I))^{n(-1)})$ *tal que* $M_{\mathcal{B}'}(f|_{\operatorname{Ker}(((C+I)^{n(-1)}))}) =$ *suma diagonal de los bloques* $J_h(-1)$

Tenemos que ver cómo lidiar con esta matriz tan grande sin hacer una gran cantidad de cálculos. Recordemos que dada una matriz $D \in M_{n\times n}(\mathbb{K})$, *entonces* $\operatorname{rang}(\mathrm{D}) = \dim \operatorname{Im}(f_D)$ *con* $\operatorname{Im}(f_D) = \langle De_1, De_2, ..., De_n\rangle$

Vemos que $\operatorname{rang}((C+I)^3) = 4$ *y además* $\operatorname{Im}((C+I)^3) = \langle e_1, e_6, e_7, e_8\rangle$

$\operatorname{Im}((C+I)^4) = (C+I)(\operatorname{Im}((C+I)^3)) = \langle (C+I)e_1, (C+I)e_6, (C+I)e_7, (C+I)e_8\rangle = \langle e_6, -e_1, e_7, e_8\rangle$

Parece razonable pensar que:

$$\operatorname{rang}(C+I)^s = \operatorname{rang}((C+I)^3) \ \forall s \geq 3 \implies n(-1) \leq 3$$

Vamos a hacer un esquema de cada imagen de los vectores de la base:

e_1	$(C+I)e_i$	$(C+I)^2 e_i$
e_1	e_6	$-e_1$
e_2	$-e_7$	$-e_7$
e_3	e_8	e_8
e_4	$-e_3$	$-e_8$
e_5	e_2	$-e_7$
e_6	$-e_1$	$-e_6$
e_7	e_7	e_7
e_8	e_8	e_8

Entonces $\operatorname{rang}(C+I) = 6$ *y* $\operatorname{rang}(C+I)^2 = 4$

$n(-1) = 2 \implies$ existe al menos un bloque de Jordan $J_2(-1)$ y ninguno más grande.

$$v_g(-1) = \dim \operatorname{Ker}(C+I) = 8 - \operatorname{rang}(C+I) = 2$$

Luego hay dos bloques de la forma $J_h(-1)$

$$\mu_1 := \mu_1(x+1) = \operatorname{rang}(C+I)^0 + \operatorname{rang}(C+I)^2 - 2\operatorname{rang}(C+I) = 8 + 4 - 2 \cdot 6 = 0 \implies$$

$J_2(-1) \oplus J_2(-1)$ es la suma de bloques de Jordan asociados a $\lambda = -1$

Apartado c)

Conocer diversas e importantes aplicaciones de los resultados fundamentales estudiados en este tema tales como la existencia de límites de Banach, extensión de operadores positivos en espacios vectoriales reticulados, existencia de funciones continuas con series de Fourier puntualmente

Necesitamos vectores $v_1, v_2 \in \operatorname{Ker}((C+I)^2)$ que induzcan una base de $\dfrac{\operatorname{Ker}((C+I)^2)}{\operatorname{Ker}((C+I))}$. Cuando tengamos eso, susaremos la proposición 7.4 para tener

$$\operatorname{Ker}((C+I)^2) = M(x+1) = \mathbb{R}[x]v_1 \oplus \mathbb{R}[x]v_2$$

Donde $\operatorname{Ker}((C+I)^2) = W(v_1) \oplus W(v_2)$ con $W(v_1)$ está formada por la base $\{(C+I)v_1, v_1\}$, $\{(C+I)v_2, v_2\}$ y $W(v_2)$ por $\{(C+I)v_2, v_2\}$. Luego la base de Jordan que se nos queda es $\mathcal{B}' = \{(C+I)v_1, v_1, (C+I)v_2, v_2\}$

Podemos tomar $v_1 = e_4 + e_8$ y $v_2 = e_5 + e_7$