Àlgebra Commutativa

Claudi Lleyda Moltó

26 de febrer de 2020

1 Anells commutatius

1.1 Anells i ideals

Definició 1.1. Un *anell* és un conjunt A amb dues operacions binàries

$$\begin{aligned} +\colon A \times A &\longrightarrow A \\ (a,b) &\longmapsto a+b \end{aligned} \qquad\qquad \begin{aligned} \cdot\colon A \times A &\longrightarrow A \\ (a,b) &\longmapsto ab \end{aligned}$$

tals que $(A,+)$ és un grup abelià (associativa, element neutre o zero, element simètric o oposat i commutativa), el producte és associatiu i distributiu respecte de la suma.

$$\begin{aligned} \forall a,b \in A \qquad & a+(b+c) = (a+b)+c \\ \exists 0 \in A, \forall a \in A \qquad & a+0 = 0+a = a \\ \forall a \in A, \exists -a \in A \qquad & a+(-a) = (-a)+a = 0 \\ \forall a,b \in A \qquad & a+b = b+a \\ \forall a,b \in A \qquad & a(bc) = (ab)c \\ \forall a,b,c \in A \qquad & a(b+c) = ab+ac \quad \text{i} \quad (b+c)a = ba+ca \end{aligned}$$

Si el producte té element neutre, el denotarem per $1 \in A$ i es diu que A és un *anell amb unitat*.

Si el producte és commutatiu es diu que A és un *anell commutatiu*.

Conveni 1.2. Anell vol dir anell commutatiu amb unitat, a menys que s'especifiqui el contrari.

Exemple 1. *$(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Z}/(n),+,\cdot)$ són anells commutatius.*

Exemple 2. *Si R és un anell, $R[x]$ amb la suma i el producte de polinomis és un anell.*

$R[x_1,\dots,x_n]$ l'anell de polinomis en variables $x_1,\dots,x_n$ sobre R.

Exemple 3. *Si R i S són anells, aleshores*

$$R \times S = \{(r,s) \mid r \in R, s \in S\}$$

amb la suma

$$(r_1,s_1)+(r_2,s_2) = (r_1+r_2, s_1+s_2) \qquad (\forall r_1,r_2 \in R, \forall s_1,s_2 \in S)$$

i el producte

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2) \qquad (\forall r_1, r_2 \in R, \forall s_1, s_2 \in S$$

component a component és un anell.

Exemple 4. $(\{0\}, +, \cdot)$, $0 + 0 = 0$, $0 \cdot 0 = 0$ *és l'*anell zero. *És l'únic anell en que* $0 = 1$.

Definició 1.3. Siguin A, B anells. Un *homeomorfisme d'anells* de A a B és una aplicació $f\colon A \longrightarrow B$ tal que

(i). $f(a_1 + a_2) = f(a_1) + f(a_2)$ per a tot $a_1, a_2 \in A$.

(ii). $f(a_1 a_2) = f(a_1) f(a_2)$ per a tot $a_1, a_2 \in A$.

(iii). $f(1_A) = 1_B$.

Definició 1.4. Un *subanell* d'un anell A és un subconjunt S de A tal que $(S, +)$ és un subgrup de $(A, +)$ i $aa' \in S$ per a tot $a, a' \in S$ i $1_A \in S$.

Definició 1.5. Un *ideal* d'un anell A és un subconjunt I de A tal que $(I, +)$ és un subgrup de $(A, +)$, $aa' \in A$ per a tot $a \in I$ i $a' \in A$.

Definició 1.6. Sigui A un anell i I un ideal de A. Aleshores

$$A/I = \{[a] \mid a \in A\} \qquad \text{on} \qquad [a] = \{a' \in A \mid a - a' \in I\}$$

amb les operacions $[a] + [b] = [a + b]$ i $[a][b] = [ab]$ per a tot $a, b \in A$ és un anell que es diu *anell quocient* de A mòdul I.

Exemple 1. *L'únic subanell de* $\mathbb{Z}$ *és ell mateix. Els ideals de* $\mathbb{Z}$ *són tots de la forma*

$$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} = (n)$$

on n és un enter no negatiu. L'anell $\mathbb{Z}/(n)$ *és l'anell quocient* $\mathbb{Z}$ *mòdul* (n).

Exemple 2. *Si A és un anell i S és un subanell de A. Aleshores l'aplicació inclusió*

$$\begin{aligned} \mathrm{i}\colon S &\longrightarrow S \\ s &\longmapsto s \end{aligned} \qquad (\textit{inclusió natural})$$

és un homeomorfisme injectiu d'anells.

Exemple 3. *Si I és un ideal d'un anell A, aleshores l'aplicació*

$$\begin{aligned} \pi\colon A &\longrightarrow A/I \\ a &\longmapsto [a] \end{aligned} \qquad (\textit{projecció natural})$$

és un homeomorfisme d'anells.

Proposició 1.7. *Sigui $f\colon A \longrightarrow B$ un homomorfisme d'anells. Definim el* nucli *de f com*

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0\} \subseteq A$$

i la imatge *de f com*

$$\mathrm{Im}(f) = \{f(a) \in B \mid a \in A\} \subseteq A.$$

Aleshores $\mathrm{Ker}(f)$ *és un ideal de A i* $\mathrm{Im}(f)$ *és un subanell de B.*

Teorema 1.8 (de l'isomorfisme)**.** *Sigui* $f\colon A \longrightarrow B$ *un morfisme d'anells. Aleshores existeix un únic* isomorfisme *(morfisme bijectiu)*

$$\tilde{f}\colon A/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$$

que fa commutatiu el diagrama

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi"] & B \\ A/\mathrm{Ker}(f) \arrow[r, "\tilde{f}"] & \mathrm{Im}(f) \arrow[u, "\mathrm{i}"'] \end{tikzcd} \qquad (f = \mathrm{i} \circ \tilde{f} \circ \pi)$$

on i *i* π *són la inclusió i projecció naturals respectivament.*

Definició 1.9. Sigui A un anell. Direm que un element $a \in A$ és un *divisor de* 0 si existeix $b \in A \setminus \{0\}$ tal que $ab = 0$.

Direm que un element $u \in A$ és una *unitat* o un *element invertible* si existeix un $u' \in A$ tal que $uu' = 1$. Si u' existeix, és únic i es diu que és *l'invers* de u i es denota per u^{-1}.

Direm que un element $a \in A$ és *nilpotent* si existeix un enter positiu n tal que $a^n = 0$.

Direm que un element $e \in A$ és *idempotent* si $e^2 = e$.

Definició 1.10. Un *domini d'integritat* és un anell D sense divisors de zero nuls tal que $0 \neq 1$.

Definició 1.11. Un *cos* és un anell tal que $0 \neq 1$ i tot element no nul és unitat.

Observació 1.12. *Tot cos és domini d'integritat.*

Demostració. Sigui K un cos. Sigui $a \in K \setminus \{0\}$. Sigui $b \in K$ tal que $ab = 0$. Aleshores $b = a^{-1}ab = a^{-1}0 = 0$. □

Exemple 1. $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}[x]$ *són dominis d'integritat i no són cossos.*

Exemple 2. $\mathbb{Z} \times \mathbb{Z}[x]$ *no és un domini d'integritat.*

En un producte finit de dominis d'integritat l'únic nilpotent és el zero.

$$\begin{array}{rl} (1,0)(0,1) = (0,0) & \\ (0,1) \quad i \quad (1,0) & \textit{són divisors de zero} \\ (1,0)(1,0) = (1,0) & \textit{és idempotent} \\ (0,1)(0,1) = (0,1) & \textit{és idempotent} \\ (0,0) & \textit{és l'únic element nilpotent de } \mathbb{Z}\times\mathbb{Z}[x] \end{array}$$

Exemple 3. *Sigui* p *un primer i sigui* n *un enter* $n > 1$.

$$\mathbb{Z}/(p^n) \qquad [p]^n = [p^n] = [0], \qquad [p] \neq [0].$$

$[p]$ *és nilpotent.*

Definició 1.13. Siguin I i J ideals d'un anell A. Definim la seva *suma* com

$I + J$ és l'ideal més petit que conté I i J.

$$I + J = \{a + b \mid a \in I, b \in J\}$$

i el seu *producte* com

$$IJ = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in I, b_i \in J\}.$$

Tant la suma com el producte d'ideals és ideal.

Definició 1.14. Sigui $\{I_\lambda\}_{\lambda\in\Lambda}$ una família no buida d'ideals d'un anell A. Definim la seva *intersecció*

$$\bigcap_{\lambda\in\Lambda} I_\lambda = \{a \in A \mid a \in I_\lambda \text{ per a tot } \lambda \in \Lambda\}.$$

Tenim que $\bigcap_{\lambda\in\Lambda} I_\lambda$ és un ideal de A.

Observació 1.15. *Siguin I i J ideals d'un anell A. Aleshores*

$$IJ \subseteq I \cap J.$$

Aquesta inclusió pot ser estricte. $I = J = 2\mathbb{Z}$

Definició 1.16. Sigui A un anell i sigui S un subconjunt de A. *L'ideal de A general per S* és

$$(S) = \bigcap_{\substack{S\subseteq I\\ I \text{ ideal de } A}} I \qquad (\neq \emptyset \text{ ja que } S \subseteq A,\ A \text{ ideal de } A)$$

(S) és l'ideal de A més petit que conté S.

Direm que un ideal I de A és *finitament generat* si existeixen $a_1, \ldots, a_n \in I$ tal que

$$(a_1, \ldots, a_n) = (\{a_1, \ldots, a_n\}) = I.$$

Observem que $(a_1, \ldots, a_n) = a_1 A + \cdots + a_n A = \{a_1 b_1 + \cdots + a_n b_n \mid b_1, \ldots, b_n \in A\}$.

Definició 1.17. Un *ideal principal* de A és un ideal generat per un element.

Exemple 1. *A $\mathbb{Z}$ tots els ideals són principals.*

Exemple 2. *Si K és un cos, aleshores els ideals de $K[x]$ són principals.*

Definició 1.18. Un *domini d'ideals principals* (DIP) és un domini d'integritat en què tot ideal és principal.

Definició 1.19. Un ideal P d'un anell A és *primer* si $P \neq A$ i per a tot $a, b \in A \setminus P$, $ab \notin P$.

Definició 1.20. Un ideal M d'un anell A és *maximal* si $M \neq A$ i si I és un ideal de A tal que $M \subseteq I \subseteq A$, aleshores $I = M$ ó $I = A$.

Els ideals maximals són primers en qualsevol anell.
En un DIP els ideals maximals són els primers expte el (0).

Exemple 1. *A $\mathbb{Z}$ els ideals primers són (0) i (p) on p és primer.*

Els ideals maximals de $\mathbb{Z}$ són (p) on p és primer.

Exemple 2. *Si K és un cos. Els ideals primers de $K[x]$ són (0) i $(p(x))$ on $p(x)$ és irreductible de $K[x]$.*

Proposició 1.21. *Sigui A un anell i sigui I un ideal de A. Aleshores*

(i). I és primer si i només si A/I és un domini d'integritat.

(ii). I és maximal si i només si A/I és un cos.

Demostració. Exercici. □

Proposició 1.22. *Sigui A un DIP. Aleshores tot ideal primer no nul de A és maximal.*

Demostració. Sigui P un ideal de A primer no nul. Sigui I un ideal de A tal que $P \subseteq I \subseteq A$. Suposem que $P \neq I$.

Com que A és un DIP, existeixen $a, b \in A$ tals que $P = (a)$ i $I = (b)$.

Com que $P \subseteq I$, existeix $c \in A$ tal que $a = bc \in P$.

Com que P és primer i $b \in I$ tenim que $c \in P$.

Com que $P = (a)$, existeix $d \in A$ tal que $c = da$. Per tant $a = bda$, és a dir, $(bd - 1)a = 0$.

Com que A és domini d'integritat i $a \neq 0$, tenim que $bd = 1 \in I$. Per tant $I = A$, Per tant P es maximal. □

Teorema 1.23. *Tot anell no nul A té almenys un ideal maximal.*

Demostració. Sigui $C = \{I \mid I \text{ ideal de } A, I \neq A\}$. Tenim que $\{0\} \neq A$ i per tant $\{0\} \in C$ i $C \neq \emptyset$.

Ordenem C per inclusió, és a dir, si $I, J \in C$, $I \leq J$ si i només si $I \subseteq J$.

Sigui $\{I_\lambda\}_{\lambda \in \Lambda}$ una cadena no buida d'elements de C, això vol dir que $\forall \alpha, \beta \in \Lambda$, o bé $I_\alpha \subseteq I_\beta$, o bé $U_\beta \subseteq I_\alpha$. Sigui $I = \bigcup_{\lambda \in \Lambda} I_\lambda \neq \emptyset$. Veiem que I és ideal. Siguin $a, b \in I$ i $c \in A$. Existeixen $\alpha, \beta \in \Lambda$ tals que $a \in I_\alpha$ i $b \in I_\beta$.

Podem suposar qe $I_\alpha \subseteq I_\beta$. Aleshores $a, b \in I_\beta$ i com que I_β és un ideal, $a - b \in I_\beta \subseteq I$. Per tant I és un subgrup additiu de A.

Tenim que $ca \in I_\alpha \subseteq I$. Per tant I és un ideal de A.

Sabem que $1 \notin I_\lambda$ per a cap $\lambda \in \Lambda$. Per tant $1 \notin I$. Això demostra que $I \in C$. Per tant $(C, \leq)$ és inductiu.

Pel *lema de Zorn*, C té elements maximals. Anem a veure que els elements maximals són ideals maximals.

Sigui $M \in C$ un element maximal. Sigui J un ideal de A tal que $M \subseteq J \subseteq A$. Suposem que $J \neq A$. Aleshores $J \in C$ i com que $M \leq J$ i M és maximal a C, tenim que $M = J$. Per tant M és un ideal maximal de A. □

Corol·lari 1.24. *Tot ideal propi d'un anell A està contingut a un ideal maximal de A.*

Demostració. Sigui I un ideal propi de A. Considerem l'anell $\bar{A} = A/I$ ($\neq \{0\}$, degut a que $I \neq A$). Pel Teorema anterior, $\bar{A}$ té ideals maximals. Sigui $\bar{M}$ un ideal maximal de $\bar{A}$. Considerem

$$\begin{aligned} \pi \colon A &\longrightarrow \bar{A} = A/I \\ a &\longmapsto [a] \end{aligned}$$

En general, un morfisme exhaustiu entre anells dóna una bijecció entre $\mathcal{A}$ i $\mathcal{B}$ que conserva inclusions.

Sigui $\mathcal{A} = \{J \mid J \text{ ideal de } A \text{ tal que } I \subseteq J\}$ i sigui $\mathcal{B} = \{T \mid T \text{ ideal de } \bar{A}\}$. Definim $\varphi_\pi \colon \mathcal{A} \longleftarrow \mathcal{B}$ per

$$\varphi_\pi(J) = \pi(J).$$

(Exercici: comproveu que $\pi(J)$ és un ideal de $\mathcal{A}$).

Hem de veure que aquesta aplicació és bijectiva. De fet

$$\varphi_\pi^{-1}(T) = \pi^{-1}(T) = \{a \in A \mid \pi(a) \in T\}$$

i observem que $\pi^{-1}(0) = I \subseteq \varphi_\pi^{-1}(T)$.

Si agafem $a, b \in \varphi_\pi^{-1}(T)$ i $c \in A$ observem que $\pi(a), \pi(b) \in T$, i així $\pi(a) - \pi(b) = \pi(a-b) \in T$ i $\pi(ca) = \pi(c)\pi(a) \in T$. Per tant φ_π^{-1} està ben definida. Es comprova que $\varphi_\pi^{-1}\varphi_\pi\pi = \mathrm{id}_{\mathcal{A}}$ i $\varphi_\pi\varphi_\pi^{-1} = \mathrm{id}_{\mathcal{B}}$ (exercici).

Si $J_1 \leq J_2$ són ideals de A, clarament

$$\varphi_\pi(J_1) = \pi(J_1) \subseteq \pi(J_2) = \varphi_\pi(J_2).$$

En particular $\pi^{-1}(\bar{M})$ és un ideal maximal de A i $I \subseteq \pi^{-1}(\bar{M})$. □

Definició 1.25. Un *anell local* és un anell amb un únic ideal maximal.

Observem que si A és un anell local i M és el seu ideal maximal, aleshores A/M és un cos. Aleshores cos es diu el *cos residual* de A.

Exemple 1. *Tot cos és un anell local.*

Exemple 2. *Sigui p un primer. Aleshores $\mathbb{Z}/(p^n)$ és un anell local per a tot enter positiu n.*

Els ideals de $\mathbb{Z}/(p^n)$ són els ideals de $\mathbb{Z}$ que contenen p^n: (p^k) amb $0 \leq k < n$. Aleshores estan ordenats:

$$(p^n) \subseteq (p^{n-1}) \subseteq \cdots \subseteq (p) \subseteq (1).$$

Per tant $p\mathbb{Z}/(p^n)$ és l'únic ideal maximal de $\mathbb{Z}/(p^n)$.

El seu cos residual és

$$(\mathbb{Z}/(p^n))/(p\mathbb{Z}/(p^n)) \cong \mathbb{Z}/p\mathbb{Z}.$$

Exemple 3. *Sigui K un cos. L'*anell de sèries formals $K[[x]] = \{\sum_{n=0}^\infty a_n x^n \mid$ *amb* $a_n \in K\}$ *amb la suma*

$$\sum_{n=0}^\infty a_n x^n + \sum_{n=0}^\infty b_n x^n = \sum_{n=0}^\infty (a_n + b_n) x^n$$

i el producte

La suma és finita i té sentit.

$$\left(\sum_{n=0}^\infty a_n x^n\right)\left(\sum_{n=0}^\infty b_n x^n\right) = \sum_{n=0}^\infty c_n x^n \qquad on \qquad c_n = \sum_{i=0}^n a_i b_{n-1}.$$

Exercici: Demostrar que $K[[x]]$ amb aquesta suma i aquest producte és un anell. Demostrar que els elements invertibles en $K[[x]]$ són els que $a_0 \neq 0$. $\mathcal{U}(K[[x]]) = \{\sum_{n=0}^\infty a_n x^n \mid a_0 \neq 0\}$.

Podem identificar

$$x = \sum_{n=0}^\infty a_n^{(x)} x^n, \qquad a_0^{(x)} = 0, a_1^{(x)} = 1, \quad i \quad a_n^{(x)} = 0 \quad \forall n > 1.$$

Aleshores

$$(x) = \left\{ \sum_{n=0}^{\infty} a_n x^n \in K[[x]] \mid a_0 = 0 \right\}$$

és el seu ideal maximal.

Proposició 1.26. *Sigui A un anell i sigui I un ideal propi de A. Aleshores*

(i). Tot $x \in A \setminus I$ és invertible si i només si A és local i I és l'únic ideal maximal de A.

(ii). Si I és maximal i tot element de la forma $1 + x$ amb $x \in I$ és invertible, aleshores A és local i I és l'únic ideal maximal de A.

Demostració. (i). Sigui $x \in A \setminus I$. Si x no és invertible, existeix M ideal maximal de A tal que $x \in M$. Tenim que $M \neq I$.

Si I és l'únic ideal maximal de A, aleshores tot $x \in A \setminus I$ ha de ser invertible.

Suposem que tot $x \in A \setminus I$ és invertible. Aleshores I és ideal maximal de A, a més tot ideal propi de A està contingut a I. Per tant I és l'únic ideal maximal de A.

Si agafem un ideal M de A amb $I \subseteq M$, tenim que M ha de contenir un element invertible i ha de ser $M = A$.

(ii). Suposem que I és ideal maximal de A i tot element de la forma $1 + x$ amb $x \in I$ és invertible.

Sigui $y \in A \setminus I$. Com que I és ideal maximal $I + (y) = A$. Per tant existeix $x \in I$ i $a \in A$ tals que $1 = x + ay$. Així $ay = 1 - x$ és invertible. Per tant y és invertible. Per (i), A és local i I és le seu únic ideal maximal. □

Definició 1.27. Un anell és *semilocal* si té un nombre finit d'ideals maximals.

Exemple 1. *Un producte finit de cossos $K_1 \times K_2 \times \cdots \times K_n$ és semilocal.*

Els ideals maximals de $K_1 \times K_2 \times \ldots K_n$ són

$$M_i = K_1 \times \cdots \times K_{i-1} \times \{0\} \times K_{i+1} \times \cdots \times K_n.$$

Exercici: Comprovar que aquests són els únics ideals maximals.

Definició 1.28. Sigui A un anell. El *nilradical* de A és

$$\mathcal{N}(A) = \{a \in A \mid a \text{ és nilpotent}\}.$$

És diferent del buit perquè $0 \in \mathcal{N}(A)$

Proposició 1.29. *Sigui A un anell. Aleshores $\mathcal{N}(A)$ és un ideal de A i si $A \neq \{0\}$, aleshores $\mathcal{N}(A)$ és la intersecció de tots els ideals primers de A. A més $A/\mathcal{N}(A)$ no té elements nilpotents no nuls.*

És a dir, $\mathcal{N}(A/\mathcal{N}(A))$ és nul

Demostració. Sabem que $0 \in \mathcal{N}(A)$. Siguin $a, b \in \mathcal{N}(A)$ i $c \in A$. Existeixen enters positius n i m tals que $a^n = b^m = 0$. Per tant

$$(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i}. = 0$$

Per tant $a + b \in \mathcal{N}(A)$. També tenim que $(ac)^n = a^n c^n = 0$. Per tant $ac \in \mathcal{N}(A)$ i això demostra que $\mathcal{N}(A)$ és un ideal de A.

Com a i b commuten podem utilitzar el binomi de Newton.

Sigui $[x] \in A/\mathcal{N}(A)$ nilpotent (amb $x \in A$). Existeix un enter positiu l tal que $[x]^l = [0]$. Per tant $x^l \in \mathcal{N}(A)$. Per tant existeix un enter positiu k tal que $(x^l)^k = 0$. Així $x \in \mathcal{N}(A)$ i $[x] = [0]$.

Suposem que $A \neq \{0\}$. Sigui P un ideal primer de A. Sigui $a \in \mathcal{N}(A)$. Existeix un enter positiu n tal que

$$a^n = 0 \in P.$$

Aleshores $a \in P$ ó $a^{n-1} \in P$, i per inducció sobre n veiem que $a \in P$. Per tant $\mathcal{N}(A) \subseteq P$.

Sigui $x \in A \setminus \mathcal{N}(A)$. Sigui

$$C = \{I \mid I \text{ ideal de } A \text{ tal que } x^n \notin I \text{ per a tot enter positiu } n\}.$$

Tenim que $\{0\} \in C$. Ordenem C per inclusió. Sigui $\{I_\lambda\}_{\lambda \in \Lambda}$ una cadena no buida d'elements de C. Considerem $I = \bigcup_{\lambda \in \Lambda} I_\lambda$. Clarament $I \in C$, i així C és inductiu no buit. Pel lema de Zorn C té maximals.

Sigui $M \in C$ maximal. Veiem que M és primer. Siguin $a, b \in A$ tals que $ab \in M$. Suposem que $a \notin M$. Aleshores tenim que $(a) + M \in C$. Suposem que $b \notin M$. Tenim que $(b) + M \notin C$. Existeixen n, m enters positius tals que $x^n \in (a) + M$ i $x^m \in (b) + M$.

Fixem-nos que $x^n x^m = x^{n+m} \in \big((a) + M\big)\big((b) + M\big) \subseteq (a)(b) + M \subseteq M$ i arribem a contradicció amb que $M \in C$. ◻

Exemple 1. *Considerem* $\mathcal{N}(\mathrm{M}_2(\mathbb{R})) = \{\left(\begin{smallmatrix} a & b \\ c & b \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{R}) \mid \left(\begin{smallmatrix} a & b \\ c & b \end{smallmatrix}\right)$ *és nilpotent*$\}$. *Observem que* $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in \mathcal{N}(\mathrm{M}_2(\mathbb{R}))$, *però* $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \notin \mathcal{N}(\mathrm{M}_2(\mathbb{R}))$. *Per tant* $\mathcal{N}(A)$ *no és in ideal.*

Conjectura 1.30 (Conjectura de Köthe (1931))**.** *Sigui I un ideal nil (tot element de I és nilpotent). Aleshores* $\mathrm{M}_2(I)$ *és nil.*

Definició 1.31. Sigui A un anell. El seu *radical de Jacobson* és

$$\mathrm{J}(A) = \bigcap_{\substack{M \text{ ideal} \\ \text{maximal} \\ \text{de } A}} M$$

Observació 1.32. $\mathcal{N}(A) \subseteq \mathrm{J}(A)$ *per a tot anell* $A \neq \{0\}$.

Exemple 1. *Si A és un anell local i M és el seu ideal maximal,* $\mathrm{J}(A) = M$.

Exemple 2. $\mathrm{J}(K[[x]]) = xK[[x]]$ *amb K cos.* $\mathcal{N}(K[[x]]) = \{0\}$.

Exemple 3. $\mathrm{J}(\mathbb{Z}) = \bigcap_{p \text{ primer}}(p)$, $\mathcal{N}(\mathbb{Z}) = \{0\}$.

Proposició 1.33. *Sigui A un anell. Aleshores*

$$\mathrm{J}(A) = \{x \in A \mid 1 + xy \text{ és invertible per a tot } y \in A\}.$$

Demostració. Sigui $x \in \mathrm{J}(A)$ i sigui $y \in A$. Suposem que $1 + xy$ no és invertible. Existeix un ideal maximal M tal que $1 + xy \in M$. Però $x \in M$. Per tant $1 = 1 + xy - xy \in M$, una contradicció. Per tant $1 + xy$ és invertible.

Sigui $x \in A$ tal que $1 + xy$ és invertible per a tot $y \in A$. Suposem que $x \notin M$ per algun ideal maximal M de A. Tenim que $(x) + M = A$. Per tant existeixen $y \in A$ i $z \in M$ tals que $xy + z = 1$ i així $z = 1 - xy = 1 + x(-y)$ és invertible. Però un ideal maximal no pot contenir elements invertibles. Per tant $x \in \mathrm{J}(A)$ i això demostra la igualtat. ◻

1.1.1 Algunes propietats de la suma, producte i intersecció d'ideals

Aquestes tres operacions són associatives i commutatives. També tenim que el producte és distributiva respecta la suma:

$$I_1(I_2 + I_3) = I_1 I_2 + I_1 I_3 \qquad \text{per a ideals } I_1, I_2, I_3 \text{ d'un anell } A.$$

Exercici: Buscar un exemple d'ideals d'un anell tals que la intersecció no sigui distributiva respecte la suma.

Proposició 1.34. *Si I_1, I_2, I_3 són ideals d'un anell A i $I_2 \subseteq I_1$, aleshores*

$$I_1 \cap (I_2 + I_3) = I_2 + (I_1 \cap I_3). \qquad \text{(llei modular)}$$

Demostració. Observem que $I_2 \subseteq I_1$ i $I_1 \cap I_3 \subseteq I_1$. Per tant $I_2 + (I_1 \cap I_3) \subseteq I_1$. Per tant és clar que $I_2 + (I_1 \cap I_3) \subseteq I_1 \cap (I_1 + I_3)$.

Sigui $x \in I_1 \cap (I_2 + I_3)$. Existeixen $y \in I_2$ i $z \in I_3$ tals que $x = y + z$. Tenim que

$$z = x - y$$

i $y \in I_2 \subseteq I_1$. Per tant $z \in I_1$. Per tant $I_1 \cap (I_2 + I_3) = I_2 + (I_1 \cap I_3)$. □

Vam veure que si I_1 i I_2 són ideals d'un anell A, aleshores $I_1 I_2 \subseteq I_1 \cap I_2$. Observem que

$$(I_1 + I_2)(I_1 \cap I_2) = I_1(I_1 \cap I_2) + I_2(I_1 \cap I_2) \subseteq I_1 I_2.$$

Si $I_1 + I_2 = A$, aleshores $I_1 \cap I_2 = I_1 I_2$.

Definició 1.35. Direm que dos ideals I_1, I_2 d'un anell A són *primers entre ells* o *comaximals* si $I_1 + I_2 = A$.

Proposició 1.36. *Sigui A un anell i siguin $I_1, \dots, I_n$ ideals de A tals que I_i i I_j són comaximals per a tot $i \neq j$. Aleshores*

$$\bigcap_{i=1}^{n} I_i = I_1 \cdots I_n.$$

Demostració. Ho demostrarem per inducció sobre n. Per a $n = 2$ ja ho sabem. Suposem que $n > 2$ i que el resultat és cert per a $n - 1$.

Per hipòtesi d'inducció tenim que

$$I = I_1 \cdots I_{n-1} = \bigcap_{i=1}^{n-1} I_i.$$

Com que $I_i + I_n = A$ per a tot $i = 1, \dots, n-1$, existeixen $x_i \in I_n$ i $y_i \in I_i$ tals que $x_i + y_i = 1$. Ara

$$y_1 \cdots y_{n-1} = (1 - x_1) \cdots (1 - x_{n-1}) = 1 + y$$

per a un cert $y \in I_n$, i $y_1 \cdots y_{n-1} \in I$.

Per tant $1 = y_1 \cdots y_{n-1} - y \in I + I_n$, i això ens demostra que I i I_n són comaximals. Per tant $I \cap I_n = I I_n$ pel cas $n = 2$. Observem que $I \cap I_n = \bigcap_{i=1}^{n} I_i$ i $I I_n = I_1 \cdots I_n$ i el resultat segueix per inducció. □

De vegades convé estudiar un anell a través dels seus anells quocients.

Proposició 1.37. *Sigui A un anell i siguin $I_1, \ldots, I_n$ ideals de A. Sigui $\Phi\colon A \longrightarrow \prod_{i=1}^n (A/I_i)$ l'aplicació definida per $\Phi(x) = ([x]_1, \ldots, [x]_n)$ on $[x]_i$ és la classe de x mòdul I_i. Aleshores*

(i). *Φ és exhaustiva si i només is I_1 i I_j són comaximals per a tot $i \neq j$.*

(ii). *Φ és injectiva si i només si $\bigcap_{i=1}^n I_i = \{0\}$.*

Demostració. *(ii)* és una simple observació.

(i) Sigui $e_i = (0, \ldots, 0, \overset{i)}{1}, 0, \ldots, 0) \in \prod_{j=1}^n (A/I_j)$. Sigui $1 \leq i \leq n$, amb $j \neq i$. Existeix $x \in A$ tal que $\Phi(x) = e_i$. Tenim que $x \in I_i$ i $1 - x \in I_i$. Per tant,

$$1 = 1 - x + x \in I_i + I_j.$$

Per tant, $I_i + I_j = A$.

Veiem que $e_i \in \mathrm{Im}(\Phi)$ per a tot $i = 1, \ldots, n$. Per a cada $i \neq j$, tenim $x_i \in I_i$ i $y_j \in I_j$ tals que $x_i + y_j = 1$. Aleshores

$$(1 - y_1) \cdots (1 - y_{i-1})(1 - y_{i+1}) \cdots (1 - y_n) = x_1 \cdots x_{i-1} x_{i+1} \cdots x_n$$

i

$$(1 - y_1) \cdots (1 - y_{i-1})(1 - y_{i+1}) \cdots (1 - y_n) = 1 + y$$

per a un cert $y \in I_i$. Per tant

$$\Phi(x_1 \cdots x_{i-1} x_{i+1} \cdots x_n) = (0, \ldots, 0, 1, 0, \ldots, 0) = e_i. \qquad \square$$

Proposició 1.38. *(i).* *Siguin $P_1, \ldots, P_n$ ideals primers i sigui I un ideal d'un anell A. Si $I \subseteq \bigcup_{i=1}^n P_i$, aleshores $I \subseteq P_j$ per algun j.*

(ii). *Siguin $I_1, \ldots, I_n$ ideals i P un ideal primer d'un anell A. Si $P \supseteq \bigcap_{i=1}^n I_i$, aleshores $P \supseteq I_j$ per algun j. Si $P = \bigcap_{i=1}^n I_i$, aleshores $P = I_j$ per algun j.*

Demostració. (i). Suposem que $I \nsubseteq P_i$ per a cert i. Demostrarem que $I \nsubseteq \bigcup_{i=1}^n P_i$ per inducció sobre n. Si $n = 1$ és obvi. Suposem que $n > 1$ i que el resultat és cert per $n - 1$. Per a cada i, existeix $x_i \in I$ tal que $x_i \notin P_j$ per a tot $j \neq i$. Per hipòtesi d'inducció podem suposar que $x_i \neq P_i$ per a tot i. Sigui

$$y = \sum_{i=1}^n x_1 \cdots x_{i-1} x_{i+1} \cdots x_n \in I,$$

aleshores $x_1 \ldots x_{i-1} x_{i+1} \cdots x_n \notin P_i$, ja que $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \notin P_i$ i P_i és primer. Per tant $y \notin P_i$ per cap i. Així tenim que $y \in I \setminus \bigcup_{i=1}^n P_i$ i això vol dir que $I \nsubseteq \bigcup_{i=1}^n P_i$.

(ii). Suposem que $P \nsupseteq I_i$ per cap i. Aleshores existeixen $x_i \in I_i$ tals que $x_i \notin P$. Per tant $x_1, \ldots, x_n \notin P$, ja que P és primer, però

$$x_1 \cdots x_n \in I_1 \cdots I_n \subseteq \bigcap_{i=1}^n I_i \subseteq P$$

i arribem a contradicció. Per tant, existeix i tal que $I_i \subseteq P$.

Si $P = \bigcap_{i=1}^{n} I_i \subseteq I_j \subseteq P$ per algun j. $\square$

Definició 1.39. Siguin I, J ideals d'un anell A. El seu *ideal quocient* és

$$(I : J) = \{x \in A \mid xJ \subset I\}$$

i és un ideal de A.

En particular, $(0 : J)$ es diu que és l'*anul·lador* de J i es denota per $\mathrm{Ann}(J)$.

Si $J = (x)$, escriurem $(I : x)$, en comptes de $(I : (x))$.

Definició 1.40. Sigui I un ideal d'un anell A. El *radical* de I en A és

$$\sqrt{I} = \{x \in A \mid x^m \in I \text{ per algun enter } m \text{ positiu}\}$$

i és ideal de A.

Observació 1.41. *Si* $\pi \colon A \longleftarrow A/I$ *és la projecció natural, aleshores*

- $(I : J) = \pi^{-1}(\mathrm{Ann}((I + J)/I)$.
- $\sqrt{I} = \pi^{-1}(\mathcal{N}(A/I))$.

Definició 1.42. Sigui $f \colon A \longleftarrow B$ un morfisme d'anells. Siguin I un ideal de A i J un ideal de B. Definim l'*extensió* de I per f com

$$f(I)B = I^{\mathrm{e}} \qquad \text{(ideal generat per } f(I))$$

Definim la *contracció* de J per f com

$$f^{-1}(J) = J^{\mathrm{c}}.$$

2 Mòduls

Definició 2.1. Sigui A un anell. Un A-*mòdul* (o mòdul sobre A) és un grup abelià M (amb $+$) junt amb una operació externa

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, m) &\longmapsto am \end{aligned}$$

tal que

(i). $a(m_1 + m_2) = am_1 + am_2$

(ii). $(a + b)m = am + bm$

(iii). $a(bm) = (ab)m$

(iv). $1m = m$

per a tot $m, m_1, m_2 \in M$ i tot $a, b \in A$.

Exemple 1. *Si* $\mathbb{K}$ *és un cos, els* $\mathbb{K}$*-mòduls són els* $\mathbb{K}$-espais vectorials.

Exemple 2. *Tot ideal* I *d'un anell* A *és un* A*-mòdul.*

Exemple 3. *Els $\mathbb{Z}$-mòduls són els grups abelians. Sigui $(G,+)$ un grup abelià. El producte d'elements de $\mathbb{Z}$ per elements de G és*

$$zg = \begin{cases} g + \overset{z}{\cdots} + g & si\ z > 0 \\ 0 & si\ z = 0 \\ -g - \overset{|z|}{\cdots} - g & si\ z < 0 \end{cases}$$

per a tot $g \in G$ i $z \in \mathbb{Z}$.

Definició 2.2. Siguin M_1, M_2 A-mòduls. Una aplicació $f\colon M_1 \longrightarrow M_2$ és un *homeomorfisme* o *morfisme de mòduls* si $f(m+m') = f(m) + f(m')$ i $f(am) = af(m)$ per a tot $m, m' \in M$ i $a \in A$.

Els homeomorfismes entre $\mathbb{K}$-mòduls amb $\mathbb{K}$ cos són les aplicacions lineals sobre $\mathbb{K}$.

Definició 2.3. Siguin M_1, M_2 A-mòduls.

$$\mathrm{Hom}_A(M_1, M_2) = \{f\colon M_1 \longrightarrow M_2 \mid f \text{ és un homeomorfisme de } A\text{-mòduls}\}.$$

Definim

$$(f+g)(m) = f(m) + g(m)$$
$$(af)(m) = af(m)$$

per a tot $f, g \in \mathrm{Hom}_A(M_1, M_2)$ i tot $a \in A$ i tot $m \in M_1$.

Exercici: Veure que $\mathrm{Hom}_A(M_1, M_2)$ és un A-mòdul.

Definició 2.4. Siguin M M', N, N' A-mòduls i $f\colon M' \longrightarrow M$ i $g\colon N \longleftarrow N'$ morfismes de A-mòduls. Definim

$$\begin{aligned} \overline{f}\colon \mathrm{Hom}_A(M,N) &\longrightarrow \mathrm{Hom}_A(M',N) \\ h &\longmapsto h \circ f \\ \overline{g}\colon \mathrm{Hom}_A(M,N) &\longrightarrow \mathrm{Hom}_A(M,N') \\ h &\longmapsto g \circ h \end{aligned}$$

Aleshores $\overline{f}$ i $\overline{g}$ són morfismes de A-mòduls i es diu que són els *morfismes induïts* per f i g respectivament.

Definició 2.5. Un *submòdul* d'un A-mòdul M és un subgrup M' de M tal que $am' \in M'$ per a tot $a \in A$ i tot $m' \in M'$.

Definició 2.6. Sigui N un submòdul d'un A-mòdul M. Al grup quocient M/N definim $a[m] = [am]$ per a tot $a \in A$ i tot $m \in M$, on

$$[m] = \{x \in M \mid m - x \in M\}.$$

Aleshores M/N és un A-mòdul que es diu que és el *mòdul quocient* de M per N.

Observació 2.7. *Si N és un submòdul d'un A-mòdul M, aleshores*

$$\begin{aligned} \mathrm{i}\colon N &\longrightarrow M \\ m &\longmapsto m \end{aligned} \qquad i \qquad \begin{aligned} \pi\colon M &\longrightarrow M/N \\ m &\longmapsto [m] \end{aligned}$$

són morfismes de A-mòduls.

Teorema 2.8 (de l'isomorfisme)**.** *Sigui* $f\colon M \longrightarrow M'$ *un morfisme de A-mòduls. Aleshores existeix un únic isomorfisme* $\widehat{f}\colon M/\mathrm{Ker}(f) \longleftarrow \mathrm{Im}(f)$ *tal que el diagrama*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & M' \\ M/\mathrm{Ker}(f) \arrow[r, "\widehat{f}"] & \mathrm{Im}(f) \arrow[u, "\mathrm{i}"'] \end{tikzcd}$$

és commutatiu, és a dir $f = \mathrm{i} \circ \widehat{f} \circ \pi$.

Índex alfabètic