

Àlgebra Commutativa

Claudi Lleyda Moltó

17 de febrer de 2020

Capítol 1

Anells commutatius

1.1 Anells i ideals

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

$$\begin{array}{ll} +: A \times A \longrightarrow A & \cdot: A \times A \longrightarrow A \\ (a, b) \longmapsto a + b & (a, b) \longmapsto ab \end{array}$$

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.

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

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

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

i el producte

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

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. Sigui A, B anells. Un *homeomorfisme d'anells* de A a B és una aplicació $f: A \rightarrow B$ 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

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

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

$$\begin{aligned} i: S &\longrightarrow S \\ s &\longmapsto s \end{aligned} \quad (\text{inclusió natural})$$

és un homeomorfisme injectiu d'anells.

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

$$\begin{aligned} \pi: A &\longrightarrow A/I \\ a &\longmapsto [a] \end{aligned} \quad (\text{projecció natural})$$

és un homeomorfisme d'anells.

Proposició 1.7. Sigui $f: A \rightarrow B$ un homomorfisme d'anells. Definim el nucli de f com

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

i la imatge de f com

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

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

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

$$\tilde{f}: A/\text{Ker}(f) \rightarrow \text{Im}(f)$$

que fa commutatiu el diagrama

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \pi & & \uparrow i \\ A/\text{Ker}(f) & \xrightarrow{\tilde{f}} & \text{Im}(f) \end{array} \quad (f = i \circ \tilde{f} \circ \pi)$$

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 $b = a^{-1}ab = a^{-1}0 = 0$. \square

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.

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

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

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

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

$[p]$ és nilpotent.

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

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

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

i el seu *producte* com

$$IJ = \{a_1b_1 + \dots + a_nb_n \mid a_i \in I, b_i \in J\}.$$

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 estricta.

$$I = J = 2\mathbb{Z}$$

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

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

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

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

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

Observem que $(a_1, \dots, a_n) = a_1A + \dots + a_nA = \{a_1b_1 + \dots + a_nb_n \mid b_1, \dots, b_n \in A\}$.

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 $a, b \in A \setminus P$, $ab \notin P$.

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

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 $I = A$.

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 és maximal. \square

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 $I_\beta \subseteq I_\alpha$. Sigui $I = \bigcup_{\lambda \in \Lambda} I_\lambda \neq \emptyset$. Veiem que I és ideal. Sigui $a, b \in I$ i $c \in A$. Existeixen $\alpha, \beta \in \Lambda$ tals que $a \in I_\alpha$ i $b \in I_\beta$.

Podem suposar que $I_\alpha \subseteq I_\beta$. 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 . \square

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 $\bar{A} = A/I (\neq \{0\})$, ja que $I \neq A$. Pel Teorema anterior, \bar{A} té ideals maximals. Sigui \bar{M} un ideal maximal de \bar{A} . Considerem

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

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 $\varphi_\pi: \mathcal{A} \longleftarrow \mathcal{B}$ per

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

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

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

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 $\varphi_\pi^{-1}\varphi_\pi\pi = \text{id}_A$ i $\varphi_\pi\varphi_\pi^{-1} = \text{id}_B$ (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:

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

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 $K[[x]] = \{\sum_{n=0}^{\infty} a_n x^n \mid \text{amb } a_n \in K\}$ 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

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

La suma és finita i té sentit.

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

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

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 .

- (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 el seu únic ideal maximal. \square

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

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

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

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

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

Exercici: Comprovar que aquests són els únics ideals maximals.

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

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

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, $\mathcal{N}(A/\mathcal{N}(A)) = \{0\}$

Demostració. Sabem que $0 \in \mathcal{N}(A)$. Sigui $a, b \in \mathcal{N}(A)$ 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 $x^n x^m = x^{n+m} \in ((a) + M)((b) + M) \subseteq (a)(b) + M \subseteq M$ i arribem a contradicció amb que $M \in C$. \square

Índex alfabètic

- anell, 1
 - amb unitat, 1
 - commutatiu, 1
 - de polinomis, 1
 - de sèries formals, 6
 - local, 6
 - producte, 1
 - quocient, 2
 - \mathbb{Z} mòdul (n) , 2
 - semilocal, 7
 - zero, 2
- cos, 3
 - residual, 6
- divisor de 0, 3
- domini
 - d'ideals principals, 4
 - d'integritat, 3
- element
 - invertible, 3
- homeomorfisme
 - d'anells, 2
- ideal, 2
 - finitament generat, 4
 - generat per un subconjunt, 4
 - maximal, 4
 - primer, 4
 - principal, 4
- idempotent, 3
- imatge, 2
- inclusio natural, 2
- intersecció d'ideals, 4
- invers, 3
- isomorfisme, 3
- lema
 - de Zorn, 5
- nilpotent, 3
- nilradical, 7
- nucli, 2
- producte d'ideals, 4
- projecció natural, 2
- subanell, 2
- suma d'ideals, 3
- Teorema
 - de l'isomorfisme, 3
- unitat, 3