

Apunts d'estructures algebriques

ALEIX TORRES I CAMPS

JORDI GUARDIA (JORDI.GUARDIA-RUBIES@UPC.EDU), ANNA RIO I SANTI MOLINA
(MARTÍ OLLER)

Índex

1	Introducció	2
1.1	Estructures algebriques bàsiques	2
2	Anells	2
2.1	Anell de fraccions	8
2.2	Anells factorials	9
3	Cossos	9
4	Grups	9
5	Moduls	9

1 Introducció

Definició 1. Una operació en un conjunt A és una aplicació $\varphi : A \times A \rightarrow A$

Possibles propietats de les operacions

1. (PC) Propietat commutativa (o abeliana) $\forall a, b \in A \varphi(a, b) = \varphi(b, a)$.
2. (PA) Propietat associativa $\forall a, b, c \in A \varphi(a, \varphi(b, c)) = \varphi(\varphi(a, b), c)$.
3. (EN) Element neutre $\exists e \in A$ tal que $\forall a \in A \varphi(e, a) = \varphi(a, e) = a$.

Clarament, l'element neutre és únic. En efecte, si n'existissin 2 elements neutres, e i e' , aleshores $e = \varphi(e, e') = e'$, amb la qual cosa hem arribat a contradicció.

4. (PI) Invers d'un element $a \in A$ és $b \in A$ tal que $\varphi(a, b) = \varphi(b, a) = e$.

Si existeix i és associatiu també és únic. En efecte, si $\exists b, c$ tals que $\varphi(a, b) = \varphi(b, a) = \varphi(a, c) = \varphi(c, a) = e$. En aquest cas, $b = \varphi(b, \varphi(a, c)) = \varphi(\varphi(b, a), c) = c$, per tant, $b = c$ i són el mateix element.

5. (PD) Si tenim dues operacions, que la primera (φ) sigui distributiva respecte la segona (μ) vol dir que $\varphi(a, \mu(b, c)) = \varphi(\mu(a, b), \mu(a, c))$ i que $\varphi(\mu(b, c), a) = \varphi(\mu(b, a), \mu(b, c))$.

1.1 Estructures algebraiques bàsiques

Definició 2. Un Grup $(G, *)$ cal que compleixi EN, PA, PI.

Definició 3. Un Semigrup $(G, *)$ cal que compleixi EN, PA.

Definició 4. Un Grup Abelià és un grup amb PC.

Definició 5. Una Anell $(A, +, *)$ cal que $(A, +)$ sigui un grup abelià, $(A, *)$ un semigrup i la PD respecte la primera.

Definició 6. Un Anell commutatiu (o abelià) és un anell on $(A, *)$ és commutatiu.

Definició 7. Un Cos és un Anell $(A, +, *)$ tal que $(A \setminus \{0\}, *)$ és un grup abelià. On 0 és l'element neutre de $(A, +)$.

Definició 8. Mòdul $(M, +)$ és un mòdul sobre l'Anell A tal que: $(M, +)$ és un grup abelià i $A \times M \rightarrow M$ (multiplicació per escalars) tal que: $a(m_1 + m_2) = am_1 + am_2$, $(a + b)m = am + bm$, $a(bm) = (ab)m$ i $1_A m = m$ ($\forall a, b \in A, \forall m, m_1, m_2 \in M$).

Definició 9. Un espai vectorial és un mòdul sobre un Cos.

2 Anells

Sigui $(A, +, \cdot)$ un Anell (sempre ens referirem a Anells commutatius sense haver de dir-ho cada vegada).

Notació: 0_A és l'element neutre de la suma (+), el "zero". I a l'element neutre del producte (\cdot) és 1_A , l'ü". Denotarem $-a$ l'element invers d'a respecte + (l'"oposat"). a^{-1} l'element invers d'a respecte del producte. $A^* = \{a \in A \text{ tal que } \exists a^{-1}\}$ s'obté un grup abelià.

Proposició 10. *Propietats:*

1. $\forall a, b, c \in A$ si $a + b = a + c$ llavors $b = c$.
2. $\forall a \in A$ es compleix que $0_A \cdot a = 0_A$.
3. $\forall a \in A$ es compleix que $(-1_A) \cdot (-a) = a$.
4. $\forall a \in A$ es compleix que $(-1_A) \cdot (a) = -a$.

Demostració.

1. $-a + (a + b) = -a + (a + c) \iff (\text{per PA}) (-a + a) + b = (-a + a) + c \iff 0_A + b = 0_A + c \iff b = c$.
2. $0_A \cdot a + 0_A = 0_A \cdot a = ((0_A + 0_A) \cdot a) = [PD] = 0_A \cdot a + 0_A \cdot a \implies 0_A = 0_A \cdot a$.
3. $(-1_A)(-a) = (-1_A)(-a) + (-a) + (a) = [PD] = (1_A - 1_A)(-a) + a = 0_A + a = a$.
4. $-a = [3] = ((-1_A)(-1_A))(-a) = [PA] = (-1_A)((-1_A)(-a)) = [3] = (-1_A)(a)$.

□

Exemple 1. Alguns exemples d'anells.

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. $\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$
3. $M_n(A)$ on A és un Anell
4. $\mathbb{Z}[J] = \{a_0 + a_1J + a_2J^2 + a_3J^3 + a_4J^4 : a_i \in \mathbb{Z}\}$ $J = e^{2\pi i/5}$
5. $\mathbb{Z}/n\mathbb{Z}$ Taules d'operacions per $n = 6, 8$.

Proposició 11. *Sigui A un anell tal que neutre de la suma és el neutre del producte ($0_A = 1_A$) aleshores l'Anell té un sol element ($A = \{0_A\}$).*

Demostració. Suposem que tenim un element $a \in A$ diferent del neutre. Aleshores, $0_A = 0_A \cdot a = 1_A \cdot a = a$. I, per tant, aquest element també és 0_A . □

Definició 12. Sigui A un anell, $n \in \mathbb{Z}$ i $a \in A$. Llavors, si $n > 0$, $n \cdot a := a + \dots + a$, si $n < 0$, $n \cdot a := (-a) + \dots + (-a)$, si $n = 0_{\mathbb{Z}}$, $0_{\mathbb{Z}} \cdot a = 0_A$. De la mateixa manera, si $n > 0$, $a^n := a \cdot \dots \cdot a$, si $n < 0$, $a^n := a^{-1} \cdot \dots \cdot a^{-1}$ i si $n = 0_{\mathbb{Z}}$, $a^n = 1_A$.

Definició 13. Direm que l'anell A té característica n , si n és el menor nombre enter positiu més petit tal que $n \cdot 1_A = 0_A$. En cas que no existeixi ($n \cdot 1_A \neq 0_A \forall n \in \mathbb{Z}^+$), direm que té característica 0.

Observació 14. Està clar que $\text{char}(A) \cdot a = 0_A \forall a \in A$.

Definició 15. Un subanell d'un anell A és un subconjunt S tal que:

1. $1_A \in S$
2. $a, b \in S \implies a - b \in S$
3. $a, b \in S \implies a \cdot b \in S$

Proposició 16. $S \subset A$, llavors S és un subanell $\iff S$ és un anell.

Demostració. \implies Cal veure que $(S, +)$ és un grup (Abelià), (S, \cdot) és un semigrup i que és compleix la PD. De les operacions de A s'hereden automaticament les propietats PA, PC, PD. Ara de la primera característica dels subanells tenim $1_A \in S$. I de la 2a, fent $b = a$, tenim $0_A \in S$ i ara, fent $a = 0_A$, $b = a$, tenim l'invers per la suma. Per tant, S és un anell.

\impliedby Si S és un anell, té el neutre de la multiplicació, té invers de la suma, està tancat per la suma i està tanvat per la multiplicació. Cosa que demostra les característiques 1, 2 i 3, respectivament. \square

Exemple 2. $\mathbb{Z} \subset \mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\} \subset \mathbb{C}$ són anells.

Exemple 3. $2\mathbb{Z} = \{a \in \mathbb{Z} : a \cong 0 \pmod{2}\} = \{2k : k \in \mathbb{Z}\}$ No és un subanell.

Proposició 17. Sigui $J = e^{2\pi i/n}$. $\mathbb{Z}[J] = \{a_0 + a_1J + \dots + a_{n-1}J^{n-1} : a_i \in \mathbb{Z}\}$ Demostreu que és una anell comprovant que és un subanell de \mathbb{C} .

Definició 18. Donats A, B anells. el seu anell producte és el conjunt $A \times B$ amb les operacions:

$$\begin{aligned} + : (A \times B) \times (A \times B) &\rightarrow A \times B \\ (a_1, b_1), (a_2, b_2) &\rightarrow (a_1 + a_2, b_1 + b_2) \\ \cdot : (A \times B) \times (A \times B) &\rightarrow A \times B \\ (a_1, b_1), (a_2, b_2) &\rightarrow (a_1 \cdot a_2, b_1 \cdot b_2) \end{aligned}$$

Definició 19. Sigui A un anell. Un subconjunt $I \subset A$ és un ideal si $\forall u, v \in I, \forall \alpha, \beta \in A$.

1. $u \in I, \alpha \in A \implies \alpha \cdot u \in I$
2. $u, v \in I \implies u + v \in I$

I, per tant, només cal comprovar que $\alpha u + \beta v \in I$.

Exemple 4. Alguns ideals:

1. $\{0_A\}$ L'ideal zero. A l'ideal total.
2. $m\mathbb{Z} \subset \mathbb{Z}$ és un ideal.
3. Anell principals o l'anell generat per $a \in A$ és $(a) := \{am : m \in A\}$. Similarment l'ideal finitament generat per $a_1, \dots, a_n \in A$ és $(a_1, a_2, \dots, a_n) := \{a_1m_1 + \dots + a_nm_n : m_i \in A\}$.
4. Per $\alpha \in \mathbb{Q}$, definim $I = \{f(x) \in \mathbb{Q}, \text{ llavors } I = \{f(x) \in \mathbb{Q}[x] : f(x) = 0\}$ és un ideal de $\mathbb{Q}[x]$ i coincideix amb el generat per $(x - \alpha) = I$
5. $I = \{f(x, y) \in \mathbb{Q}[x, y] : f(0, 0) = 0\}$ ideal de $\mathbb{Q}[x, y]$. Coincideix amb $(x, y) = I$.

Proposició 20. $I, J \subset A$ ideals

1. $I + J = \{a + b : a \in I, b \in J\}$ és un ideal i és el menor que conté I i J .
2. $I \cdot J = \{\sum_{j < \infty} a_j b_j : a_j \in I, b_j \in J\}$ és un ideal

Demostració.

1. Primer comprovem que és un ideal. Siguin $a_1, a_2 \in I, b_1, b_2 \in J$ i $u = a_1 + b_1, v = a_2 + b_2 \in I + J$, $\alpha, \beta \in A$, llavors $\alpha u + \beta v = \alpha(a_1 + b_1) + \beta(a_2 + b_2) = (\alpha a_1 + \beta a_2) + (\alpha b_1 + \beta b_2)$ que pertany a $I + J$, ja que $(\alpha a_1 + \beta a_2) \in I$ i $(\alpha b_1 + \beta b_2) \in J$.

I és el menor que conté els I i a J , perquè si un ideal K els conté, com que $\forall a \in I \subset K, \forall b \in J \subset K$ aleshores, com que K ha de ser tancat per la suma, segur que $a + b \in K$.

2. Siguin $a_j, a_i \in I$, $b_j, b_i \in J$ i $u = \sum_j a_j \cdot b_j, v = \sum_i a_i \cdot b_i \in I \cdot J$, $\alpha_1, \alpha_2 \in A$, llavors, $\alpha_1 u + \alpha_2 v = \alpha_1 \sum_j a_j \cdot b_j + \alpha_2 \sum_i a_i \cdot b_i = [\text{PD i P\AA}] = \sum_j (\alpha_1 a_j) \cdot b_j + \sum_i (\alpha_2 a_i) \cdot b_i = \sum_{k=i,j} (\alpha a_k) b_k \in I \cdot J$, perquè $\alpha_1 a_j, \alpha_2 a_i \in I$.

□

Proposició 21. En un anell, $a \in A$, $u \in A^*$, aleshores $(a) = (ua)$, és a dir, l'ideal generat per a i per ua son el mateix.

Demostració.

\subseteq Sigui $b \in (a)$, aleshores $b \in (ua)$ perquè b ha de ser de la forma $b = ax$ llavors, podem escriure b de la forma $b = au(u^{-1}x)$, el qual, clarament és un element de (ua) .

\supseteq Sigui $b \in (ua)$ aleshores b és de la forma $b = uax$ llavors també és de la forma $b = uau^{-1}ux = a(ux)$, per la qual cosa b és un element de (a) . □

Proposició 22. A és un cos \iff els seus únics ideals són 0 i A .

Demostració. \implies Sigui $I \subset A$ un ideal no nul. Sigui $x \in I$, $x \neq 0$, A cos $\implies \exists x^{-1}$, i com $x \in I \implies 1 = xx^{-1} \in I \implies \forall a \in A \ a = a \cdot 1 \in I \implies I = A$.

\impliedby Sigui $x \in A$, $x \neq 0$ si $0 \neq (x) \implies (x) = A \implies 1 \in (x) \implies \exists y \in A$ tal que $1 = xy$ per tant, $y = x^{-1}$. □

Teorema 23. Tots els ideals de l'anell de \mathbb{Z} son principals.

Demostració. Sigui $I \subset \mathbb{Z}$ un ideal. Si $I = (0)$ és principal clarament. Suposem que $\exists x \in I$ amb $x \neq 0$ llavors $x \in I \iff -x \in I$. Per tant, $I^+ = \{x \in I : x > 0\} = I \cap \mathbb{N} \neq \emptyset$. Pel principi de bona ordenació de \mathbb{N} , $\exists m = \min I^+$.

Aleshores, suposem que hi ha un element y que no és de la forma mk . Li fem la divisio euclidiana i escrivim $y = mk + r$ per algun r (el qual pertany a I perquè I és tancat per la suma) entre m i 0 no inclosos. Aleshores, hem arribat a contradicció, perquè abans havíem dit que m era el mínim i ara hem vist que n'existeix un element positiu més petit. □

Proposició 24. Sigui k un cos. Tots els ideals de $k[x]$ són principals.

Demostració. Semblant amb la demostració anterior, només cal canviar el mínim pel polinomi del mínim grau. La contradicció és la mateixa. □

Definició 25. Un anell principal és un anell que tots els seus ideals son principals.

Definició 26. Siguin A, B dos anells. Una aplicació $f : A \rightarrow B$ és un morfisme d'anells si preserva les operacions en A i B .

1. $f(1_A) = 1_B$
2. $\forall x, y \in A \ f(x + y) = f(x) + f(y)$
3. $\forall x, y \in A \ f(xy) = f(x)f(y)$

Anomenarem Monomorfisme al morfisme injectiu, Epimorfisme al morfisme exhaustiu i isomorfisme al morfisme bijectiu.

Observació 27. Sigui A un anell qualsevol. $\varphi : \mathbb{Z} \rightarrow A$ amb $\varphi(m) = m \cdot 1_A$. Aquest morfisme és injectiu si $\text{char}(A) = 0$, i es compleix que $\varphi^{-1}(0) = \text{char}(A)$.

Proposició 28. Propietats bàsiques dels anells . Siguin A i B dos anells i f un morfisme d'anell.

1. $f(a^n) = f(a)^n$
2. $a \in A^* \implies f(a) \in B^*, f(a)^{-1} = f(a^{-1})$
3. Sigui $J \subset B$ un ideal, llavors $f^{-1}(J) \subset A$ és un ideal
4. En general, la imatge d'un ideal d' A no és un ideal de B .
5. Si f és exhaustiva, llavors $I \subset A$ ideal $\implies f(I) \subset B$ també és un ideal.
6. $\ker f := \{a \in A : f(a) = 0\} = f^{-1}((0))$ és un ideal d' A .
7. $\text{Im} f := \{f(a) : a \in A\} \subset B$ subanell de B .
8. f injectiva $\iff \ker f = 0$.
9. A cos $\implies f = 0$ o f injectiu.

Demostració.

1. Per inducció, es poden treure potències una per una.
2. Per la propietat del producte dels morfismes i envia l'element neutre a l'element neutre $1_B = f(1_A) = f(aa^{-1}) = f(a)f(a^{-1})$.
3. Siguin $a_1, a_2 \in f^{-1}(J)$ i $\lambda, \mu \in A$, llavors $\lambda a_1 + \mu a_2 \in f^{-1}(J)$? Sí, perquè $f(\lambda a_1 + \mu a_2) = f(\lambda)f(a_1) + f(\mu)f(a_2) \in J$ perquè és combinació d'elements de J . Per tant, és un ideal.
4. Contraexemple, Si $A = \mathbb{Z}$ i $B = \mathbb{Q}$ i f és la inclusió. Un ideal de A és per exemple (2) però $f((2))$ no és un ideal perquè $2\frac{1}{3} \notin f((2))$.
5. Siguin $f(a), f(b) \in f(I)$ i $\lambda, \mu \in B$, llavors $\lambda f(a) + \mu f(b) \in f(I)$, sí, perquè al ser exhaustiva, $\exists x_\lambda, x_\mu$ tal que $f(x_\lambda) = \lambda$ i $f(x_\mu) = \mu$. Per tant, $\lambda f(a) + \mu f(b) = f(x_\lambda)f(a) + f(x_\mu)f(b) = f(x_\lambda a + x_\mu b) \in f(I)$.
6. L'element neutre hi és perquè $f(1_A) = 1_B$, la resta i el producte de dos elements hi són perquè f està tancat per la suma (i resta) i pel producte.
7. Que f sigui injectiva fa que només el 0 pugui anar al 0. Ja que, en qualsevol cas $f(0+0) = f(0) + f(0) \implies f(0) = 0$. I que $\ker f = 0$ implica que si dos elements tiguessin la mateixa imatge $f(a) = f(b) \implies f(a) - f(b) = 0 \implies f(a - b) = 0$ i com que només el 0 va al 0, $a = b$.
8. Suposem que A és un cos i que dos elements diferents tenen la mateixa imatge $f(a) = f(b) \implies f(a - b) = 0$. Aleshores, $f(x) = f(x)f(1) = f(x(a - b)^{-1}(a - b)) = f(x(a - b)^{-1})f(a - b) = 0$. Llavors, f és la funció que va tot a 0. (I sembla que $0_B = 1_B$). Altrament f és injectiva.

□

Definició 29. Anell quocient. Sigui A un anell i $I \subset A$ un ideal. Definim la relació d'equivalència \sim com (per $a, b \in A$) $a \sim b \iff a - b \in I$. El corresponent conjunt quocient l'anotarem com A/I .

En el conjunt quocient A/I definim dues operacions:

1. $\bar{a} + \bar{b} := \overline{a + b}$
2. $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$

Hem de veure que estan ben definides:

Suposem que $a' \in \bar{a}, b' \in \bar{b}$, llavors $a' + b' = \overline{a + b}$ i $a'b' = \overline{ab}$. Aleshores, les seves respectives diferències pertanyen a l'ideal. Llavors $(a + b) - (a' + b') = (a - a') + (b - b') \in I$ perquè cada una de les diferències pertany a l'ideal. I $ab - a'b' = b'(a - a') - a(b - b') \in I$, perquè l'ideal és tancat per la multiplicació.

Exercici: Coproveu que aquestes dues operacions tenen totes les propietats necessàries per a què A/I sigui un anell. En direm anell quocient d' A per I .

Exemple 5.

1. $A = \mathbb{Z}$ i $I = (m)$ i $A/I = \mathbb{Z}/m\mathbb{Z}$
2. $A = K[x]$, $\alpha \in K$ i $I = (x - \alpha)$.

$$\begin{aligned} A/I &= K[x]/(x - \alpha) \rightarrow K \\ p(\bar{x}) &\rightarrow p(\alpha) \end{aligned}$$

Està ben definit, si $q(x) \in p(\bar{x})$, llavors $q(x) - p(x) \in (x - \alpha) \implies q(x) - p(x) = (x - \alpha)h(x) \implies q(\alpha) - p(\alpha) = 0$.

3. $A = \mathbb{R}[x]$ i $I = (x^2 + 1)$ llavors el seu quocient és isomorf a \mathbb{C} . Enviant $p(\bar{x})$ a $p(i)$.

Proposició 30. *L'aplicació natural*

$$\begin{aligned} \pi : A &\rightarrow A/I \\ a &\rightarrow \bar{a} \end{aligned}$$

és un morfisme d'anells.

Demostració. La definició de les operacions A/I ho garanteix. □

Proposició 31. (a) *Segui $J \subset A$ ideal tal que $J \supset I$, llavors $J/I := \pi(J) \subset A/I$ és un ideal. (b) *Segui $U \subset A/I$ ideal, existeix un únic ideal $J \subset A$ tal que $J \supset I$ i $J/I = U$.**

Demostració. (a) L'aplicació π és exhaustiva perquè $\ker \pi = \{a \in A, \bar{a} = \bar{0}\} = \{a \in A : a \in I\} = I$, llavors per una propietat anterior la imatge d'un ideal és un ideal.

(b) Segui $J = \pi^{-1}(U) \subset A$ un ideal (perquè l'antiimatge d'un ideal és un ideal), notem que $\pi(J) = \pi(\pi^{-1}(U)) = [exh] = U$. Aleshores, com que U és ideal, $\bar{0} \in U \implies I = \pi^{-1}(\bar{0}) \subset \pi^{-1}(U) = J$

Suposem que J' també satisfà $\pi(J') = U$ i $J' \supset I$. $\pi(J') = U \implies J' = \pi^{-1}(\pi(J')) \supset \pi^{-1}(U) = J$ i $a \in J' \implies \pi(a) \in U \implies a \in \pi^{-1}(U) = J$. Llavors $J = J'$. □

Proposició 32. *Propietat universal del quocient. Segui $f : A \rightarrow B$ un morfisme d'anells $I \subset A$ ideal tal que $I \subset \ker f$. Existeix un únic morfisme $\varphi : A/I \rightarrow B$ tal que $\varphi \circ \pi = f$*

Demostració. Comencem definint $\varphi(\bar{a}) := f(a)$. Anem a veure que està ben definida i compleix que $\varphi \circ \pi = f$. Que compleix la segona condició està clar perquè $\varphi \circ \pi(a) = \varphi(\bar{a}) = f(a)$. Aleshores, està ben definida perquè si tenim que $\bar{a} = \bar{b}$, vol dir que $a - b \in I$, llavors, per condició de l'enunciat $f(a - b) = 0$ i, per tant, $f(a) = f(b)$, que és el que ens cal perquè $\varphi(\bar{a}) = \varphi(\bar{b})$.

Suposem que existeix una $\varphi' \neq \varphi$ que compleix la mateixa propietat. Aleshores, sigui $x \in A$ un element el qual es compleixi que $\varphi(\bar{x}) \neq \varphi'(\bar{x})$, al ser π exhaustiva, sempre existeix. Però sabem que $\varphi(\bar{x}) = f(x) = \varphi'(\pi(x))$ llavors són la mateixa funció. Per tant, hem acabat, només n'hi ha una. □

Teorema 33. (Teorema d'isomorfisme d'anells) *Segui $f : A \rightarrow B$ un morfisme d'anells. Hi ha un morfisme canònic $\bar{f} : A/\ker f \rightarrow \text{Im} f$.*

Demostració. Definim $\bar{f}(\bar{a}) = f(a)$, aplicant la proposició anterior al morfisme $\tilde{f} : A \rightarrow \text{Im}(f) \subseteq B$ (vam veure que la imatge era un subanell) com a ideal triem $I = \ker f$ (ho vam comprovar en proposicions anteriors). Llavors tenim: $\bar{f} := \varphi$. φ és exhaustiu perquè \tilde{f} ho és i és injectiu perquè $\ker \varphi = \{\bar{a} : \varphi(\bar{a}) = 0\} = \{\bar{a} : \tilde{f}(\bar{a}) = 0\} = \{\bar{a} : f(a) = 0\} = \bar{0}$, perquè els elements a tals que $f(a) = 0$ pertanyen al nucli i, per tant, en aquest cas, en el $\bar{0}$. □

Definició 34. Un divisor de zero en un anell A és un element $a \in A$, $a \neq 0$ tal que $ab = 0$ per algun $b \in A$, $b \neq 0$.

Definició 35. Un anell íntegre és un anell sense divisors de zero.

Definició 36. Un ideal $\mathfrak{p} \subset A$ d'un anell qualsevol s'anomena primer si $ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ o } b \in \mathfrak{p}$.

Definició 37. L'espectre de A $\text{Spec}(A) = \{\mathfrak{p} \subset A; \mathfrak{p} \text{ primer}\}$

Proposició 38. Sigui $\mathfrak{p} \subset A$ un ideal. Llavors \mathfrak{p} primer $\iff A/\mathfrak{p}$ és un anell íntegre.

Demostració. \implies Siguin $\bar{a}, \bar{b} \in A/\mathfrak{p}$ tal que $\bar{a}, \bar{b} \neq 0$. Suposem que $\bar{a}\bar{b} = \bar{0} \implies \bar{a}\bar{b} = \bar{0} \implies ab \in \bar{0} = \mathfrak{p} \implies a \in \mathfrak{p} \text{ o } b \in \mathfrak{p}$. Però això voldria dir que o a o b pertanyen a la classe del 0, contradicció amb el que hem suposat.

\Leftarrow Suposem que $ab \in \mathfrak{p}$ si $ab \in \mathfrak{p} \implies \bar{a}\bar{b} = \bar{a}\bar{b} = 0 \implies$ per ser A/\mathfrak{p} íntegre, o a o b són de la classe del 0, per tant, o un o l'altre pertanyen a \mathfrak{p} . \square

Definició 39. Un ideal $m \subset A$ s'anomena maximal si no està contingut en cap altre ideal propi d' A .

Proposició 40. $m \subset A$ és un ideal. Llavors, m maximal $\iff A/m$ és un cos.

Demostració. \Leftarrow Suposem $m \subsetneq J$ ideal, per tant, $\exists x \in J \setminus m$ per tant, $x \notin m \implies \bar{x} \neq 0 \implies \exists \bar{y} \neq 0$ tal que $\bar{x}\bar{y} = 1 \implies u = 1 - xy \in J$, llavors $1 = u + xy$, com és suma de dos elements de J , $1 \in J \implies A = J$.

\implies Els ideals de A/m són de la forma J/m amb $m \subset J$ ideal d' A . Com que m és maximal, o $J = m$ o bé, $J = A$, en el primer cas $J/m = (J)$ i, en el segon, $J/m = A/m$. Per tant, els únics ideals de A/m són el zero i el total $\implies A/m$ és un cos (propietat dels cossos que vam veure). \square

Corol·lari 41. m maximal $\implies m$ primer.

2.1 Anell de fraccions

Sigui A un anell íntegre, $F = A \times (A \setminus \{0\}) = \{(a, s) : a, s \in A, s \neq 0\}$. Definim en F una relació \sim amb $(a, b) \sim (c, t) \iff at - bs = 0$ i és una relació d'equivalència (**exercici**).

Definició 42. Sigui $Fr(A) =$ conjunt de classes d'equivalència segons aquesta relació i l'anomenarem *fraccions* d' A . $\frac{a}{s} := (a, s)$. En $Fr(A)$ definim dues operacions:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} - \frac{b}{t} = \frac{at - bs}{st}$$

Cal demostrar que estan ben definides.

Aquestes operacions compleixen totes les propietats necessàries per tal que $Fr(A)$ sigui un anell. On el $0_{Fr(A)} = \frac{0}{1}$ i $1_{Fr(A)} = \frac{1}{1}$.

En aquest anell, tot element no nul té invers. Si $\frac{a}{s} = \frac{0}{1}$, llavors $a1 = 0s = 0 \implies a = 0$. Llavors si $\frac{a}{s} \neq \frac{0}{1} \implies a \neq 0$, el seu element invers és $\frac{s}{a}$ ja que $\frac{a}{s} \frac{s}{a} = \frac{1}{1}$, per tant $Fr(A)$ és un cos.

Tenim un morfisme natural

$$i : A \longrightarrow Fr(A)$$

$$a \mapsto i(a) = \frac{a}{1}$$

Aquesta aplicació és un morfisme d'anells i és injectiva. **Cal demostració.**

Exemple 6. $Q := Fr(\mathbb{Z})$ o $Q(x) := Fr(\mathbb{Z}[x])$ o també $Q(x) = Fr(\mathbb{Z}[x])$

Proposició 43. (*propietat universal del cos de fraccions*) Sigui A un anell íntegre. (a) Si $f : A \rightarrow B$ és un morfisme d'anells tal que $f(A \setminus \{0\}) \subset B^*$ llavors existeix un únic morfisme $\varphi : Fr(A) \rightarrow B$ tal que $\varphi \circ i = f$.
(b) Si $i : A \rightarrow F$ és una injecció d' A en un altre cos F' que satisfà (a) llavors $F' \simeq Fr(A)$.

Demostració. (a) Anem a deduir què ha de ser φ : $\varphi(\frac{a}{b}) = \varphi(\frac{a}{1} \frac{1}{b}) = \varphi(\frac{a}{1})\varphi(\frac{1}{b}) = \varphi(i(a))\varphi(i(b)^{-1}) = f(a)f(b)^{-1}$. Llavors definim $\varphi(\frac{a}{s}) := f(a)f(s)^{-1}$. Cal veure que φ està ben definida, que φ és un morfisme i unicitat. **DEMOSTRACIÓ.**

(b) Combinant les dues propietats provinents d'(a) tenim que existeixen unes úniques funcions $\varphi : Fr(A) \rightarrow F$ i $\psi : F \rightarrow Fr(A)$ tal que $\varphi \circ i = i'$ i al revés, $\psi \circ i' = i$. Llavors, fixem-nos que $\psi \circ \varphi \circ i = i$ (substituint). Però fixem-nos també que la propietat universal també la podem aplicar amb el mateix conjunt $Fr(A)$ i la inclusió, aleshores, la funció $\psi \circ \varphi$ és l'única que compleix la propietat universal, però trivialment la identitat també, així que són la mateixa funció. Similarment escollint F dues vegades, tenim que $\varphi \circ \psi = i'$. Amb això i sabent que composició de morfismes és morfisme tenim que $Fr(A) \simeq F$. \square

2.2 Anells factorials

La motivació d'aquest capítol és la de veure en quins anell tenim un teorema fonamental de l'aritmètica com tenim en els enter. El teorema fonamental de l'aritmètica diu el següent: tot nombre enter $m \in \mathbb{Z}$ té una única factorització com a producte de factors primers. $m = \pm p_1^{e_1} \cdots p_r^{e_r}$ amb p_i primers $p_i > 0$.

Definició 44. Un element $a \neq 0 \in A$ és irreductible si

- (1) a no és una unitat ($a \notin A^*$).
- (2) Si podem escriure $a = bc$ llavors b o c son unitats ($\in A^*$)

Definició 45. Un element $a \in A$ és primer si (a) és un ideal primer.

Proposició 46. A íntegre a primer $\implies a$ irreductible.

Demostració. Suposem que $a = bc$ llavors $bc \in (a)$ llavors, per ser (a) un ideal primer, o bé b , o bé c pertanyen a (a) . Sense pèrdua de generalitat, suposem $b \in (a)$, llavors existeix $d \in A$ tal que $b = ad$, llavors $a = adc$, per tant, $a(1 - dc) = 0 \implies dc = 1$, llavors $c \in A^*$. \square

Exemple 7. Considerem l'anell $A = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. En aquest anell 2 és irreductible. Suposem que $2 = (\alpha + \beta\sqrt{-5})(\gamma + \delta\sqrt{-5})$, llavors $2 = (\alpha - \beta\sqrt{-5})(\gamma - \delta\sqrt{-5})$, per tant, $4 = (\alpha^2 + 5\beta^2)(\gamma^2 + 5\delta^2)$, que és una igualtat entre enters positius llavors els divisors son 1, 2 o 4. $\alpha^2 + 5\beta^2 \leq 5 \implies \beta = 0$, per tant, com que 2 no és un quadrat, $\alpha^2 = 1$ (per tant, $\alpha = 1, -1$), així que $\alpha + \beta\sqrt{-5} = \alpha \in \mathbb{Z}[\sqrt{-5}]^*$ és una unitat, per tant 2 és irreductible. En canvi, 2 no és primer, perquè $2|6$ però com $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, però 2 no divideix a cap dels dos perquè 2 no divideix a 1.

Definició 47. Un anell factorial (o domini de factorització única - DFU, UFD) és un anell íntegre en el qual cada element no nul admet una factorització 'única' (*) en producte d'elements irreductibles. (*) llevat d'ordre i de producte per unitats.

Definició 48. Dos elements $a, b \in A$ són associats si $\exists n \in A^*$ tal que $a = nb$.

3 Cossos

4 Grups

5 Moduls