Apunts d'estructures algrebraiques

Aleix Torres i Camps

Jordi Guardia (jordi.guardia-rubies@upc.edu), Anna Rio i Santi Molina
(Martí Oller)

1 Introducció

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

Possibles propietats de les operacions

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

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

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

   Si existeix i és associatiu també és únic. En efecte, si $\exists b, c$ tals que $\phi(a, b) = \phi(b, a) = \phi(a, c) = \phi(c, a) = e$. En aquest cas, $b = \phi(b, \phi(a, c)) = \phi(\phi(b, a), c) = c$, 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 $\phi(a, \mu(b, c)) = \phi(\mu(a, b), \mu(a, c))$ i que $\phi(\mu(b, c), a) = \phi(\mu(b, a), \mu(b, c))$.

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 communtatiu (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 $A \times M \to M$ (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'emenent 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. $-a + (a + b) = -a + (a + c) \iff$ *(per PA)* $(-a + a) + b = (-a + a) + c \iff O_A + b = O_A + c \iff b = c$.
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. $-a = [3] = ((-1_A)(-1_A))(-a) = [PA] = (-1_A)((-1_A)(-a)) = [3] = (-1_A)(a)$.

$\square$

Exemple 1. Alguns exemples d'anells.

1. $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$
2. $Z[x] \subset Q[x] \subset R[x] \subset C[x]$
3. $M_n(A)$ on A és un Anell
4. $\mathbf{Z}[J] = \{a_0 + a_1 J + a_2 J^2 + a_3 J^3 + a_4 J^4 : a_i \in \mathbf{Z}\}$ $J = e^{2\pi i/5}$
5. $\mathbf{Z}/n\mathbf{Z}$ 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. $\square$

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

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 $(n \cdot 1_A \neq 0_A \ \forall n \in \mathbf{Z}^+)$, direm que té característica 0.

Observació 14. *Està clar que* $char(A) \cdot a = O_A \ \forall a \in A$.

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

Exemple 3. $2\mathbf{Z} = \{a \in \mathbf{Z} : a \cong 0(\text{mod}2)\} = \{2k : k \in \mathbf{Z}\}$ No és un subanell.

Proposició 17. *Sigui $J = e^{2\pi i/n}$.* $\mathbf{Z}[J] = \{a_0 + a_1 J + \ldots + a_{n-1} J^{n-1} : a_i \in \mathbf{Z}\}$ Demostreu que és una anell comprovant que és un subanell de $\mathbf{C}$.

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

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

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. $m\mathbf{Z} \subset Z$ 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 $a_1, \ldots, a_n \in A$ és $(a_1, a_2, \ldots, a_n) := \{a_1 m_1 + \ldots + a_n m_n : m_i \in A\}$.

4. Per $\alpha \in \mathbf{Q}$, definim $I = \{f(x) \in Q$, llavors $I = \{f(x) \in \mathbf{Q}[x] : f(x) = 0\}$ és un ideal de $\mathbf{Q}[x]$ i coincideix amb el generat per $(x - \alpha) = I$

5. $I = \{f(x, y) \in \mathbf{Q}[x, y] : f(0, 0) = 0\}$ ideal de $\mathbf{Q}[x, y]$. 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, $\alpha_1 u + \alpha_2 v = \alpha_1 \sum_j a_j \cdot b_j + \alpha_2 \sum_i a_i \cdot b_i =$ [PD i PA] $= \sum_j (\alpha_1 a_j) \cdot b_j + \sum_i (\alpha_2 a_i) \cdot b_i = \sum_{k=i,j} (\alpha a_k) b_k \in I \cdot J$, perquè $\alpha_1 a_j, \alpha_2 a_i \in I$.

$\square$

3 Cossos

4 Grups

5 Moduls