Tema II.– ESTRUCTURES ALGEBRAIQUES

1.- Llei de composició interna.

(a) Definició i exemples

Nocions prèvies: producte cartesià de dos conjunts, correspondència i aplicació entre dos conjunts, domini i codomini, imatge i antiimatge d'un element, imatge d'una aplicació, aplicació suprajectiva (exhaustiva, epijectiva), aplicació injectiva, aplicació bijectiva, composició d'aplicacions.

Definició de llei de composició interna (l.c.i): donat un conjunt E, anomenem l.c.i definida en E a una aplicació $*$ de $E \times E$ en E,

$$\begin{array}{rccc} * \ : & E \times E & \longrightarrow & E \\ & (x,y) & \longrightarrow & x * y. \end{array}$$

Exemples: la suma i el producte dels conjunts numèrics $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) Propietats notables de les lleis de composició interna

Siga $*$ una l.c.i definida en E. Direm que:

(i) $*$ **és associativa**: si $\forall x, y, z \in E, \quad (x * y) * z = x * (y * z) = x * y * z.$

(ii) $*$ **és commutativa**: si $\forall x, y \in E, \quad x * y = y * x.$

(iii) $*$ **és distributiva respecte de la l.c.i** $\perp$: si $\forall x, y, z \in E$,

$$x * (y \perp z) = x * y \perp x * z \,, \qquad (y \perp z) * x = y * x \perp z * x \,.$$

Exemples: la suma $+$ i el producte $\cdot$ usuals dels conjunts numèrics $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ són l.c.i. associatives i commutatives. A més el producte és distributiu respecte de la suma.

(c) Elements notables de les lleis de composició interna

Elements regulars o simplificables: un element $x \in E$ és regular per l'esquerra (dreta) respecte de la l.c.i $*$ si $\forall a, b \in E$,

$$x * a = x * b \ \ (a * x = b * x) \quad \longrightarrow \quad a = b \,.$$

Direm que un element és regular si ho és a la dreta i a l'esquerra.

Element neutre: un element $e \in E$ direm que és neutre per a la l.c.i. $*$ si $\forall x \in E$,

$$x * e = e * x = x \,.$$

Teorema (unicitat de l'element neutre): donat un conjunt E, i una l.c.i $*$ definida en E, l'element neutre, si existeix, és únic.

Exemples: En els conjunts numèrics la suma i el producte usuals admeten neutre. El 0 és el neutre de la suma i l'1 és el neutre del producte.

Element simètric (o invers): suposem que la l.c.i $*$ admet element neutre $e \in E$, aleshores anomenem simètric d'un element $x \in E$ a l'element $x^{-1} \in E$ tal que,

$$x * x^{-1} = x^{-1} * x = e\,.$$

Si un element $x \in E$ admet simètric direm que és simetritzable.

Teorema (unicitat de l'element simètric): donat un conjunt E, i una l.c.i $*$ associativa definida en E, un element $x \in E$ sols pot tindre un simètric.

Teorema: donat un conjunt E, i una l.c.i $*$ associativa definida en E, tot element simetritzable és regular.

Teorema: donat un conjunt E, i una l.c.i $*$ associativa definida en E, si $x \in E$ és simetritzable aleshores x^{-1} és simetritzable i $(x^{-1})^{-1} = x$.

Exemples:

(i) En $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ el simètric respecte de la suma d'un element x és l'oposat $-x$, $x + (-x) = 0$. En $\mathbb{N}$ no existeix simètric per a la suma.

(ii) En $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ el simètric respecte del producte d'un element $x \neq 0$ és l'invers $1/x$, $x \cdot (1/x) = 1$. El 0 no admet invers respecte del producte. En $\mathbb{N}$ i $\mathbb{Z}$ no existeix simètric per al producte.

2.- Grups

(a) Definició i exemples

Definició: Un grup és una parella $(G, *)$, on G és un conjunt i $*$ és una l.c.i. definida en ell que és associativa, té element neutre $e \in G$, i tot element $a \in G$ admet simètric $a^{-1} \in G$.

Grup abelià: Un grup $(G, *)$ es diu abelià si $*$ és commutativa.

Exemples:

(i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ i $(\mathbb{C}, +)$ són grups abelians.

(ii) $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$ i $(\mathbb{C} - \{0\}, \cdot)$ són grups abelians.

(iii) $(\mathbb{Q} - \{0\}, *)$, amb la l.c.i $p * q = \dfrac{pq}{2}$, és grup abelià.

(b) Propietats immediates dels grups

(i) L'element neutre és únic.

(ii) Tots els element admeten un sol simètric.

(iii) $(a * b)^{-1} = a^{-1} * b^{-1}$.

(iv) Tots els elements són regulars.

(v) Les equacions de la forma $a*x = b$ ($x*a = b$), admeten solució i és única, $x = a^{-1}*b$ ($x = b * a^{-1}$).

(c) Subgrups

Definició: Donat un grup $(G,*)$, direm que $H \subset G$ és un subgrup si $*$ és estable (interna) en H i $(H,*)$ és grup.

És a dir, $H \subset G$ és subgrup de $(G,*)$ si:

(i) $\forall a, b \in H, \quad a * b \in H$.

(ii) L'element neutre e de $(G,*)$ està en H, $e \in H$.

(iii) $\forall a \in H, \quad a^{-1} \in H$.

Teorema (caracterització de subgrups): La condició necessària i suficient perquè $H \subset G$ siga un subgrup de $(G,*)$ és que $\forall a, b \in H, \ a * b^{-1} \in H$.

Exemples:

(i) $(\mathbb{Z},+)$ és un subgrup abelià de $(\mathbb{R},+)$.

(ii) $\mathbb{N} \subset \mathbb{Z}$ no és subgrup de $(\mathbb{Z},+)$.

(iii) $(\mathbb{R},+)$ i $(\mathbb{I},+)$ són subgrups de $(\mathbb{C},+)$.

(iv) $(\mathbb{R}-\{0\},\cdot)$ és subgrup de $(\mathbb{C}-\{0\},\cdot)$, però $(\mathbb{I}-\{0\},\cdot)$ no ho és.

(v) $\{e\}$ i G són els subgrups trivials d'un grup $(G,*)$.

Teorema (intersecció de subgrups): Si $H_1, H_2 \subset G$ són subgrups de $(G,*)$, aleshores la seua intersecció $H_1 \cap H_2$ és un subgrup de $(G,*)$.

Nota: La unió $H_1 \cup H_2$ de dos subgrups $H_1, H_2 \subset G$ no és subgrup.

Exemples:

(i) El conjunts $G_n = \{x \ \in \mathbb{Z} \ / \ x = nq, \ q \in \mathbb{Z}\}$ dels múltiples enters d'un nombre natural $n \in \mathbb{N}$ és un subgrup de $(\mathbb{Z},+)$. Aleshores, $G_m \cap G_n = G_{mn}$ és subgrup i $G_m \cup G_n$ no és subgrup $(5 = 2 + 3 \notin G_2 \cup G_3)$.

(ii) $\mathbb{R}$ i $\mathbb{I}$ són subgrups de $(\mathbb{C},+)$. La intersecció $\mathbb{R} \cap \mathbb{I} = \{0\}$ és un subgrup trivial, i la unió $\mathbb{R} \cup \mathbb{I}$ no és un subgrup.

3.- Homomorfismes entre grups

(a) Definició i exemples

Definició: Donats dos grups $(G,*)$ i $(H,\perp)$, direm que una aplicació $f : G \longrightarrow H$ és un homomorfisme de grups si $\forall x, y \in G, \quad f(x * y) = f(x) \perp f(y)$.

Exemples:

(i) Considerem els grups $(\mathbb{Z},+)$ i $(\mathbb{R}-\{0\},\cdot)$. L'aplicació $f : \mathbb{Z} \longrightarrow \mathbb{R} \,; q \longrightarrow e^q$ és un homomorfisme de grups.

(ii) Considerem els grups $(\mathbb{C}-\{0\},\cdot)$ i $(\mathbb{R}-\{0\},\cdot)$. L'aplicació $f(z) = |z|$ és un homomorfisme de grups.

(b) Classificació

Monomorfisme: homomorfisme injectiu, és a dir, $\forall x, y \in G,\ x \neq y \ \rightarrow \ f(x) \neq f(y)$.

Epimorfisme: homomorfisme epijectiu, és a dir, $\forall a \in H,\ \exists\, x \in G \ / \ f(x) = a$.

Isomorfisme: homomorfisme bijectiu.

Endomorfisme: homomorfisme amb $(G, *) = (H, \perp)$.

Automorfisme: endomorfisme bijectiu.

Exemples:

(i) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{R} - \{0\}, \cdot)$; $q \longrightarrow e^q$ és un monomorfisme i no és un epimorfisme.

(ii) El mateix passa si considerem l'extensió de f als reals, $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R} - \{0\}, \cdot)$; $f(x) = e^x$. Però en canvi:

* $f(x) = e^x$ és un isomorfisme entre $(\mathbb{R}, +)$ i el grup $(\mathbb{R}^+, \cdot)$.
* $f(z) = e^z$ és un epimorfisme però no un monomorfisme entre $(\mathbb{C}, +)$ i $(\mathbb{C} - \{0\}, \cdot)$.

(iii) La funció real de variable real $g(x) = x^2$ és un endomorfisme de $(\mathbb{R} - \{0\}, \cdot)$ que no és ni epi- ni mono-.

(iv) La funció real de variable real $h(x) = x^3$ és un automorfisme de $(\mathbb{R} - \{0\}, \cdot)$.

(v) La funció real de variable real $k(x) = \cos x$ no és un endomorfisme, ni de $(\mathbb{R}, +)$ ni de $(\mathbb{R} - \{0\}, \cdot)$.

(c) Propietats immediates dels homomorfismes

Teorema (imatge de l'element neutre): si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, aleshores la imatge de l'element neutre $e_* \in G$ és l'element neutre $e_\perp \in H$, $f(e_*) = e_\perp$.

Teorema (imatge del simètric): si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, aleshores la imatge del simètric, $f(x^{-1})$, d'un element $x \in G$ és el simètric de la imatge de x, $f(x^{-1}) = f(x)^{-1}$.

Definició (imatge d'un homomorfisme): si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, la imatge de f és el conjunt $Im(f) = f(G)$ d'elements de H que tenen anti-imatge,

$$Im(f) = \{a \in H \ / \ \exists\ x \in G,\ f(x) = a\} \subset H\,.$$

Teorema: si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, aleshores la imatge $Im(f)$ de f és un subgrup de $(H, \perp)$.

Definició (nucli d'un homomorfisme): si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, anomenem nucli de f al conjunt $N(f)$ d'elements de G que tenen per imatge el neutre $e_\perp \in H$,

$$N(f) = \{x \in G \ / \ f(x) = e_\perp\} \subset G\,.$$

Teorema: si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, aleshores el nucli $N(f)$ de f és un subgrup de $(G, *)$.

(d) Altres propietats dels homomorfismes

Siga $f : (G, *) \longrightarrow (H, \perp)$ un homomorfisme de grups, aleshores se satisfan les propietats següents:

(i) Si F és un subgrup de $(G, *)$, aleshores $f(F)$ és un subgrup de $(H, \perp)$.

(ii) Si I és un subgrup de $(H, \perp)$, aleshores $f^{-1}(I)$ és un subgrup de $(G, *)$.

(iii) Si $(G, *)$ és commutatiu, aleshores $(f(G), \perp)$ és commutatiu.

(iv) f és epimorfisme sii $Im(f) = H$.

(v) f és monomorfisme sii $N(f) = \{e\}$.

(iv) Si f és un isomorfisme, aleshores f^{-1} existeix i també és un isomorfisme.

(v) La composició $f \circ g$ de dos homomorfismes f i g és un homomorfisme.

4.- Anells i cossos

(a) Anells: definició i exemples

Definició: Un anell és una terna $(A, \perp, *)$ que satisfà les següents condicions:

(i) $(A, \perp)$ és un grup abelià.

(ii) $*$ és una l.c.i. associativa: $\forall a, b, c \in A, \quad a * (b * c) = a * (b * c)$.

(iii) La llei $*$ és distributiva respecte de la llei $\perp$: $\forall a, b, c \in A$,

$$a * (b \perp c) = a * b \perp a * c\,, \qquad (b \perp c) * a = b * a \perp c * a\,.$$

Direm que l'anell és unitari si existeix element neutre per a la l.c.i. $*$.

Direm que l'anell és abelià si la l.c.i. $*$ és commutativa.

Exemples: els conjunts numèrics $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ amb la suma i el producte usuals són anells commutatius i unitaris.

Notació: denotem per 0 l'element neutre de la llei $\perp$. Denotem $-a$ el simètric (o oposat) d'un element a respecte d'eixa llei.

Si l'anell és unitari, denotem per 1 l'element neutre de la llei $*$. Si un element a admet simètric a^{-1} respecte d'eixa llei, l'anomenarem també invers.

Regles dels signes. Si $(A, \perp, *)$ és un anell, se satisfan les propietats següents:

(i) $a * 0 = 0 * a = 0 \quad \forall\, a \in A$.

(ii) $(-a) * b = a * (-b) = -(a * b) \quad \forall\, a, b \in A$.

(iii) $(-a) * (-b) = a * b \quad \forall\, a, b \in A$.

(b) Cossos: definició i exemples

Definició: Un cos és una terna $(K, \perp, *)$ que satisfà les següents condicions:

(i) $(K, \perp)$ és un grup abelià.

(ii) $(K - \{0\}, *)$ és un grup abelià.

(iii) la llei $*$ és distributiva respecte de la llei $\perp$.

Exemples: els conjunts numèrics $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ amb la suma i el producte usuals són cossos.

Propietat. Si $(K, \perp, *)$ és un cos, $\quad a * b = 0 \quad \longleftrightarrow \quad a = 0 \quad o \quad b = 0.$

5.- Grup de permutacions

(a) Definició de permutació

S'anomena permutació de n elements a la reordenació de n objectes diferents. Si numerem els objectes de 1 a n, una permutació és una reordenació del n primers nombres naturals. Tenim la següent definició matemàtica formal.

Definició: Una permutació d'un conjunt E_n de n elements és una bijecció $\sigma : E_n \to E_n$.

Si $E_n = \{1, 2, ..., n\}$, donar la permutació és donar les imatges $\sigma(k),\ k = 1, ..., n$. Escriurem:

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

Denotarem S_n el conjunt de les permutacions d'un conjunt de n elements E_n.

S'anomena cardinal d'un conjunt al número d'elements del conjunt. Tenim: $\mathrm{card}(E_n) = n$.

Exemple: les permutacions de $E_3 = \{1, 2, 3\}$ són les bijeccions

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Propietat: el nombre de permutacions d'un conjunt de n elements és $n!$, $\mathrm{card}(S_n) = n!$

(b) Composició de permutacions i estructura de grup

Com que una permutació és una aplicació, podem fer la composició de dues permutacions. I com la composició de dues bijeccions és una bijecció tenim:

Propietat: La composició d'aplicacions $\circ$ és una l.c.i en el conjunt de les permutacions S_n, és a dir, si $\alpha, \beta \in S_n$, aleshores $\alpha \circ \beta \in S_n$.

Exemple: en les permutacions de E_3, $\sigma_4 \circ \sigma_2 = \sigma_3$.

Teorema: $(S_n, \circ)$ és un grup (*grup de les permutacions*),

(i) La composició és associativa.

(ii) L'element neutre és l'aplicació identitat $I \in S_n$.

(iii) El simètric de $\sigma \in S_n$ és l'aplicació inversa $\sigma^{-1} \in S_n$.

En general, $(S_n, \circ)$ no és abelià. Per exemple, en S_3, $\sigma_3 \circ \sigma_6 = \sigma_5 \neq \sigma_4 = \sigma_6 \circ \sigma_3$.

Exemples: en les permutacions de E_3, $\sigma_1 = I$, $\sigma_1^{-1} = \sigma_1$, $\sigma_2^{-1} = \sigma_2$, $\sigma_3^{-1} = \sigma_3$, $\sigma_4^{-1} = \sigma_5$, $\sigma_6^{-1} = \sigma_6$.

(c) Cicles i transposicions

Definició: un cicle de longitud p és una permutació $\sigma \in S_n$ en la que per a p elements $i_1, ..., i_p$ se satisfà $\sigma(i_k) = i_{k+1}$, $k = 1...p-1$, $\sigma(i_p) = i_1$, i els $n-p$ elements restant queden inalterats. Escriurem $\sigma = (i_1 \dots i_p)$.

Exemples: en les permutacions de E_3, σ_4 i σ_5 són cicles de longitud 3, $\sigma_4 = (1\,2\,3)$ i $\sigma_5 = (1\,3\,2)$; i σ_2, σ_3 i σ_6 són cicles de longitud 2, $\sigma_2 = (2\,3)$, $\sigma_3 = (1\,2)$ i $\sigma_6 = (1\,3)$.

Definició: una transposició és un cicle de longitud 2, és a dir, la transposició consisteix a intercanviar dos elements.

Propietat: un cicle γ de longitud p satisfà $\gamma^p = I$.

En particular, si τ és una transposició tindrem: $\tau^2 = I$, $\tau^{-1} = \tau$.

Definició: dues permutacions direm que són disjuntes si cada element que és alterat per una queda inalterat per l'altra.

Teorema: Tota permutació pot descompondre's en producte de cicles disjunts.

Teorema: Tot cicle de longitud p pot escriure's com producte de $p - 1$ transposicions.

Una forma de fer aquesta descomposició és la següent:

$$(i_1\ i_2\ \dots\ i_p) = (i_1\ i_p)(i_1\ i_{p-1})\dots(i_1\ i_2)$$

Conseqüència: Tota permutació pot descompondre's en producte de transposicions.

Teorema: La descomposició d'una permutació en transposicions no és única però el número de transposicions és sempre parell o sempre senar.

Exemple: en les permutacions de E_4,

$$(1\ 3)(3\ 2)(4\ 1)(4\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (1\ 4\ 2)(3) = (1\ 2)(1\ 4)$$

(d) Signatura d'una permutació i símbol de Levi-Civita

Definició: anomenem signatura d'una permutació $\sigma \in S_n$ a

$$\text{sign}(\sigma) \equiv (-1)^{n_t} = \begin{cases} +1 & \texttt{si } n_t \texttt{ és parell} \\ -1 & \texttt{si } n_t \texttt{ és senar} \end{cases}$$

on n_t és el nombre de transposicions en que es descompon la permutació σ.

Direm que σ és una permutació parella (senar) si $\text{sign}(\sigma) = +1$ (-1).

Propietat: tot cicle σ de longitud p té signatura $\text{sign}(\sigma) = (-1)^{p-1}$.

Les transposicions τ tenen signatura $\text{sign}(\tau) = -1$. La identitat té signatura $\text{sign}(I) = 1$.

Exemples: en les permutacions de E_3, σ_1, σ_4 i σ_5 són permutacions parelles, i σ_2, σ_3 i σ_6 són permutacions senars, és a dir, $\text{sign}(\sigma_1) = \text{sign}(\sigma_4) = \text{sign}(\sigma_5) = +1$, $\text{sign}(\sigma_2) = \text{sign}(\sigma_3) = \text{sign}(\sigma_6) = -1$.

Teorema: La signatura del producte de dues permutacions σ_1, σ_2 és igual al producte de les signatures,

$$\text{sign}(\sigma_1 \circ \sigma_2) = \text{sign}(\sigma_1)\,\text{sign}(\sigma_2).$$

Aquest teorema ens diu que la signatura sign és un homeomorfisme entre el grup de permutacions $(S_n, \circ)$ i el grup multiplicatiu $(\{+1. -1\}, \cdot)$.

Símbol de Levi-Civita: una manera de representar la signatura d'una permutació és usant el símbol de Levi-Civita $\epsilon_{i_1\, i_2\, \dots\, i_n}$, $i_k = 1....n$,

$$\epsilon_{i_1\, i_2\, \dots\, i_n} \equiv \begin{cases} 0 \ \texttt{si hi ha algun índex repetit} \\ \text{sign} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \end{cases}$$

Exemple: $\epsilon_{341625} = \text{sign} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix} = \text{sign}\{(1\ 3)(2\ 4\ 6\ 5)\} = (-1)^3(-1) = +1.$

Aplicacions: càlcul vectorial i determinants.