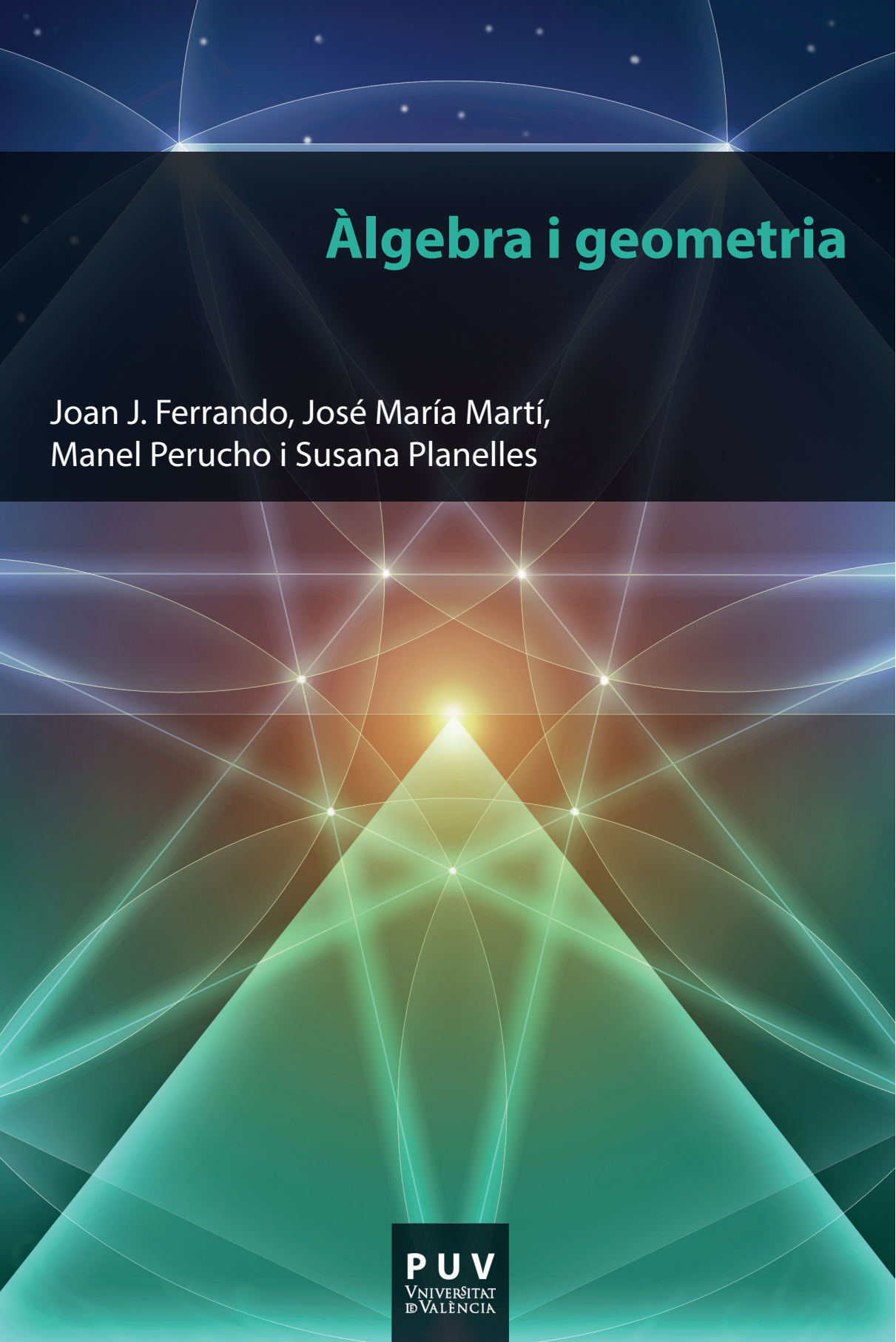
Àlgebra i geometria

Joan J. Ferrando, José María Martí,
Manel Perucho i Susana Planelles



PUV
Universitat de València

ÀLGEBRA I GEOMETRIA

Educació. Materials 121

ÀLGEBRA I GEOMETRIA

Joan J. Ferrando, José María Martí,
Manel Perucho i Susana Planelles

PUV
VNIVERSITAT
DE VALÈNCIA

Col·lecció: Educació. Materials

Coordinació editorial: Juan Pérez
Correcció: Campgràfic Editors S.L.
Maquetació: els autors/es.
Coberta: Inmaculada Mesa

ISBN: 978-84-1118-388-8
ISBN: 978-84-1118-389-5 (ed. digital en PDF)

Edició digital

A les nostres famílies.

Als i les nostres alumnes.

Als nostres professors i professores.

Índex

Pròleg

Divideix 100 barres de pa entre 10 homes, incloent entre ells un barquer, un capatàs i un guàrdia, que reben porcions dobles. Quina quantitat se n'endú cadascun d'ells?

Aquest text, redactat en un papir egipci (papir *Rhind*, Museu Britànic), entorn de l'any 1650 abans de Crist, mostra que la resolució de problemes bàsics relacionats amb l'administració i el comerç, mitjançant una àlgebra senzilla, és tan antiga com les primeres civilitzacions postneolítiques. Sembla que els matemàtics de l'Antiguitat (sumeris, xinesos, egipcis i babilonis) coneixien i resolien sistemes d'equacions lineals.

El primer tractat d'àlgebra conegut, escrit per Diofant d'Alexandria en el segle III després de Crist, recull el saber acumulat anteriorment en els mètodes de resolució d'equacions. En el segle VIII, el matemàtic (possiblement bagdadí) Abu Ja'far Muhammad va escriure el tractat *Ilm al-jabr wa'l-mukabala* o 'La ciència de restaurar el que falta i d'igualar entre semblants', on es troba l'origen etimològic de la paraula *àlgebra*, 'al-jabr', que significa aproximadament 'la reunió de les parts'. Abu Ja'far va ser conegut també com al-Khwarizmi, que és l'origen del terme *algorisme*.

Fins al segle XVIII, l'àlgebra podia definir-se com la branca de les matemàtiques dedicada a cercar solucions a equacions (i sistemes d'equacions) polinòmiques de grau arbitrari. Precisament, Girolamo Cardano i Niccolò Fontana Tartaglia (segle XVI) van tractar per primera vegada amb els nombres complexos, com a arrels d'equacions de tercer grau. El teorema fonamental de l'àlgebra (*qualsevol polinomi té solució dins del cos dels nombres complexos*) va ser demostrat en els segles XVIII i XIX de maneres diferents per D'Alembert, Euler, Lagrange i Gauss. Per altra banda, en el segle XVIII es va introduir l'ús dels determinants (per Leibniz a Europa i Seki Kowa al Japó) en la resolució de sistemes d'equacions lineals segons el mètode que més tard s'anomenaria *regla de Cramer*.

En el segle XIX hi va haver un salt fonamental en les aplicacions i el grau d'abstracció de l'àlgebra, amb el desenvolupament dels conceptes de *vector* i *espai vectorial* a partir de les solucions d'un sistema lineal homogeni (Euler, D'Alembert, Lagrange); la generalització matemàtica del terme *vector* (Hamilton, Cayley, Grassman), usat des de feia temps en el camp de la Mecànica; la incorporació dels conceptes d'*independència lineal* i *dimensió d'un espai vectorial* (Grassman); l'àlgebra matricial (Cayley, Sylvester); el teorema de Rouché-Fröbenius; els conceptes d'*equació característica*, *valors propis* i *diagonalització* d'una matriu de representació d'una forma quadràtica (Cauchy), de sistemes

d'equacions diferencials ordinàries (Sturm) o de formes canòniques (matrius de Jordan); la teoria de grups (Galois, Jordan) i l'aplicació d'aquesta teoria a les transformacions continues (Lie); la teoria de les funcions d'operadors lineals (Sylvester); la llei d'inèrcia (Jacobi, Sylvester); el concepte d'*espais mètrics no euclidians* per a espais corbats (Riemann) i per a espais plans (Minkowski).

A les acaballes del segle XIX i principi del segle XX es van recollir i completar treballs previs de Kronecker i Weierstrass per donar forma a l'àlgebra tensorial (Weyl) i es va fixar el concepte d'*ortonormalitat de sistemes de vectors* (Gram, Schmidt). Finalment, Hilbert va desenvolupar la idea dels espais mètrics complets.

Pel que fa a la Geometria, després dels *Elements* d'Euclides i els seus cinc coneguts postulats fonamentals, redactats a Alexandria cap al 300 a. C., diferents autors van dedicar esforços a demostrar el cinquè postulat: *per un punt exterior a una recta, es pot traçar una única paral·lela*. El continu fracàs de la cerca d'aquesta demostració al llarg dels segles XVII i XVIII va portar D'Alembert a parlar de «*l'escàndol de la geometria*», fins que, ja en el segle XIX, Gauss, Bolyai i Lobatxevski van iniciar el camí de les geometries no euclidianes, que va ser culminat per Riemann a mitjan segle XIX, i desenvolupat, entre d'altres, per Ricci-Curbastro, Levi-Civita i Weyl.

En les seues aplicacions físiques, l'Àlgebra i la Geometria són presents en les dues grans teories físiques de començament del segle XX, la Mecánica quàntica i la Relativitat general. A més, ha estat útil per a reformular la Mecànica clàssica, gràcies a la utilització d'un llenguatge matemàtic més compacte i elegant.

El germen d'aquest manual el constitueixen els apunts de l'assignatura de Mètodes matemàtics I de l'antiga llicenciatura de Física extingida el 2010 amb l'última reforma dels plans d'estudi. Els apunts esmentats, elaborats pels professors José Bordes i Vicent Giménez, del departament de Física Teòrica de la Universitat de València, no van ser mai publicats encara que han servit de material d'estudi a nombroses promocions d'alumnes de Física, de la mateixa manera que ens van servir a nosaltres com a base per als cursos d'Àlgebra i Geometria de bon començament. Modificats, completats i ampliats, el nucli d'aquests apunts encara es pot traçar al llarg dels capítols del nostre manual. Volem aprofitar l'ocasió per reconeixer el treball d'aquests dos professors en l'elaboració dels seus apunts i la generositat per compartir-los amb nosaltres.

Les assignatures d'Àlgebra i Geometria I i II s'imparteixen, respectivament, al primer i segon quadrimestre del grau en Física. Tot i això, es tracta de les úniques assignatures del grau sobre aquestes matèries, de manera que els seus continguts sobrepassen el nivell de la resta de les assignatures de primer curs. Salvar amb èxit aquesta dificultat exigeix tenir materials autocontinguts i rigorosos que en faciliten el procés d'aprenentatge de l'alumnat. Aquest manual, com les assignatures a què pretén servir de suport, supera en profunditat les monografies usuals, en general, més elementals. Així, al curs i al manual trobem, per exemple, temes dedicats a l'estudi dels espais prehilbertians (a la base de

la formulació de la Mecànica quàntica), els espais pseudoeuclidians (necessaris per formular la Relativitat general) o l'àlgebra tensorial (utilitzada en diverses teories de camps com l'electromagnetisme o la mateixa Relativitat general), que els estudiants utilitzaran en cursos posteriors. Si volguérem seguir al manual l'estructura de les assignatures d'Àlgebra i Geometria I i II, l'organització seria aproximadament la següent (entre parèntesi, on es poden trobar els continguts dels temes en aquest manual):

– Àlgebra i Geometria I: 1. Nombres complexos (apèndix B); 2. Estructures algebraiques (capítol 1; apèndix C); 3. Espais vectorials (capítol 2); 4. Aplicacions lineals (seccions 1, 2, 3, 4 i 5 del capítol 3); 5. Espais prehilbertians (capítol 4).

– Àlgebra i Geometria II: 1. Matrius, determinants i equacions lineals (apèndix D); 2. Operadors lineals (seccions 6, 7 i 8 del capítol 3; capítol 5); 3. Teoria espectral (capítol 6); 4. Tensors. Teoria algebraica (capítol 7); 5. Espai afí (seccions 1, 2, 3 i 4 del capítol 8); 6. Geometria analítica a l'espai (capítol 9).

A banda dels continguts inclosos en aquestes assignatures, el manual conté materials adicionals. L'apèndix B recull conceptes bàsics de la teoria de conjunts necessaris en diverses parts del curs. L'espaitemps de Galileu i la geometria Lorentziana (referida breument en diverses parts del curs) es presenten amb detall a la secció 8.5 i al capítol 10, respectivament, d'aquest manual.

Al llarg del manual s'han escrit en negreta els conceptes a l'hora de ser definits i en cursiva aquells que, tot i tenir una definició específica, no s'hi defineixen. La bibliografia utilitzada s'indica al llarg del manual quan cal.

1. Estructures algebraiques

La suma i el producte definits en els conjunts numèrics són els exemples més senzills d'operacions binàries, o lleis de composició internes. Aquestes operacions satisfan algunes propietats que ens són familiars, com per exemple, les propietats associativa o commutativa. Tanmateix, hi ha conjunts matemàtics, com ara els formats per funcions, que satisfan algunes de les propietats de l'aritmètica ordinària i que tenen interés per desenvolupar algunes de les teories físiques fonamentals. Quan en matemàtiques tenim un conjunt en el qual hem definit una o dues operacions que satisfan unes propietats específiques es diu que tenim una estructura algebraica.

El concepte de grup és fonamental en Física i defineix una de les estructures algebraiques més bàsiques. Històricament apareix com una necessitat en la teoria de nombres, en la teoria de les equacions algebraiques i en geometria. Els grups permeten definir les estructures d'anell i de cos, i formalitzar algebraicament els conjunts numèrics. El terme grup va ser introduït per Galois (1811-1832), que amb Abel (1802-1829), va estudiar la resolució per radicals de les equacions algebraiques. Cayley (1821-1895) va estudiar les permutacions com a grup de transformacions, i Noether (1888-1935) va mostrar que els grups d'isometries tenen associades magnituds conservades.

Les estructures d'anell i de cos estan definides per dues operacions amb determinades propietats que, a més, estan conectades per la propietat distributiva.

Per a la comprensió del capítol són necessaris alguns conceptes elementals de la teoria de conjunts. Podem trobar una introducció bàsica a aquesta teoria a l'apèndix A.

1.1. Llei de composició interna

Donat un conjunt E, s'anomena **llei de composició interna** (l.c.i.) definida en E a una aplicació $*$:

$$* : E \times E \longrightarrow E; \quad (x, y) \longrightarrow x * y.$$

EXEMPLE 1.1.1. La suma i el producte usuals són lleis de composició internes en els conjunts numèrics $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$.

Propietats notables d'una llei de composició interna

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

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

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

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

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

Noteu que el fet que la llei siga associativa permet eliminar els parèntesis i escriure la composició de tres elements $x, y, z \in E$ com $x * y * z$ sense ambigüitat.

EXEMPLE 1.1.2. La suma i el producte 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.

Elements notables d'una llei de composició interna

Un element $x \in E$ és **regular per l'esquerra (dreta)** respecte de la l.c.i. $*$ si donats $a, b \in E$ tals que $x * a = x * b$ $(a * x = b * x)$, aleshores $a = b$. Direm que un element és **regular** si ho és per la dreta i per l'esquerra. Els elements regulars també s'anomenen **simplificables**.

EXEMPLE 1.1.3. Tots els elements dels conjunts numèrics $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ són simplificables respecte de la suma usual, i tots excepte el 0 ho són respecte del producte.

Un element $e \in E$ és **neutre** per a la l.c.i. $*$ si $\forall x \in E$, $x * e = e * x = x$.

Teorema 1.1.1. *Unicitat de l'element neutre*
Donat un conjunt E i una l.c.i. $*$ definida en ell, l'element neutre, si existeix, és únic.

Prova. Siguen e' i e'' dos elements neutres de E respecte de la l.c.i. $*$. Tindrem, per tant, que

$$x * e' = e' * x = x, \qquad x * e'' = e'' * x = x,$$

per a un element $x \in E$ arbitrari. Aleshores, si fem $x = e''$ en la primera expressió i $x = e'$ en la segona, i igualem les expressions resultants, trobem que $e' = e''$. □

EXEMPLE 1.1.4. 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.

Suposem ara 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 1.1.2. *Unicitat de l'element simètric*
Siga $*$ una l.c.i. associativa definida en E. Aleshores, un element $x \in E$ sols pot tenir un simètric.

Prova. Siguen $x', x'' \in E$ simètrics de l'element $x \in E$, i $e \in E$ el neutre respecte de la llei $*$. Aleshores tenim que si la llei és associativa,

$$x' = x' * e = x' * (x * x'') = x' * x * x'' = (x' * x) * x'' = e * x'' = x'',$$

Per tant, $x' = x''$, i el simètric de x és únic. □

Teorema 1.1.3. Donat un conjunt E, i una l.c.i. $*$ associativa definida en aquest, tot element simetritzable és regular.

Prova. Siga $x \in E$ simetritzable i $x^{-1} \in E$ el seu simètric. Siguen ara $a, b \in E$ tals que $x * a = x * b$. Aleshores resulta:

$$\begin{aligned} a = e * a = (x^{-1} * x) * a = x^{-1} * (x * a) = \\ = x^{-1} * (x * b) = (x^{-1} * x) * b = e * b = b. \end{aligned}$$

Així hem provat que x es regular per l'esquerra. D'una manera semblant es demostra que x és regular a la dreta. □

Teorema 1.1.4. Donat un conjunt E, i una l.c.i. $*$ associativa definida en aquest, si $x \in E$ és simetritzable aleshores el seu simètric x^{-1} és simetritzable i $(x^{-1})^{-1} = x$.

Prova. De la definició d'element simètric es veu que si x^{-1} és simètric de l'element x, aleshores x és simètric de x^{-1}, com ho és $(x^{-1})^{-1}$. Per altra banda, hem vist que si la llei és associativa, els simètrics són únics (teorema 1.1.2), i per tant, $x = (x^{-1})^{-1}$. □

EXEMPLE 1.1.5. 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.

EXEMPLE 1.1.6. 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.

1.2. Grups i subgrups

Un **grup** és una parella $(G, *)$, on G és un conjunt i $*$ és una l.c.i. definida en aquest amb les propietats següents:

(i) És associativa.

(ii) Té element neutre $e \in G$.

(iii) Tot element $a \in G$ admet simètric $a^{-1} \in G$.

Un grup $(G, *)$ es diu **abelià** o **commutatiu** si $*$ és commutativa.

EXEMPLE 1.2.1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ i $(\mathbb{C}, +)$ són grups abelians.

EXEMPLE 1.2.2. $(\mathbb{Q} - \{0\}, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$ i $(\mathbb{C} - \{0\}, \cdot)$ són grups abelians.

EXEMPLE 1.2.3. $(\mathbb{Q} - \{0\}, *)$, amb la l.c.i. $p * q = \dfrac{pq}{2}$, és un grup abelià.

Propietats immediates dels grups

Proposició 1.2.1. En un grup $(G, *)$ es verifiquen les propietats següents:

(i) L'element neutre és únic.

(ii) Tots els elements admeten un sol simètric.

(iii) Tots els elements són regulars.

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

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

Prova. Les tres primeres propietats es deriven directament dels resultats provats en la secció anterior. Per a demostrar-ne la quarta, haurem de provar que $b^{-1} * a^{-1}$ és el simètric de l'element $a * b$ tenint en compte l'associativitat de la llei de composició

$$(a * b) * (b^{-1} * a^{-1}) = a * b * b^{-1} * a^{-1} = a * e * a^{-1} = a * a^{-1} = e,$$

on e representa el neutre respecte de $*$. La cinquena propietat es demostra per substitució directa de la solució proposada en l'equació corresponent i tenint en compte de nou l'associativitat de $*$. La unicitat de la solució és conseqüència de la unicitat dels elements simètrics i del fet que $*$ és una aplicació. □

Subgrups

Donat un grup $(G, *)$, direm que $H \subset G$ és **subgrup** de $(G, *)$ si $(H, *)$ és grup. És a dir, $H \subset G$ és subgrup de $(G, *)$ si:

(i) $*$ és estable (interna) en H: $\forall a, b \in H,\ \ a * b \in H$.

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

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

Noteu que l'associativitat de $*$ i l'existència de l'element neutre i dels simètrics dels elements de H està garantida per ser $(G, *)$ grup i no caldrà tornar a provar-les. Per altra banda, si un grup és abelià, tots els seus subgrups també ho seran.

Teorema 1.2.2. *Caracterització de subgrups*
La condició necessària i suficient perquè $H \subset G$ siga un subgrup de $(G, *)$ és que $\forall a, b \in H,\ \ a * b^{-1} \in H$.

Prova. Per a veure que és una condició necessària, considerem dos elements arbitraris $a, b \in H$. Com que $(H, *)$ és un subgrup de $(G, *)$, $b^{-1} \in H$ (per la condició (iii) de la definició de subgrup) i $a * b^{-1} \in H$ (per la condició (i)), tal com volíem demostrar.

Per a provar la condició suficient partim del fet que en $H \subset G$ es verifica que $a * b^{-1} \in H, \forall a, b \in H$. Ara, prenent $b = a$, tenim que $a * a^{-1} = e \in H$, el que prova la condició (ii) de la definició de subgrup. Per a provar la condició (iii), prenem $a = e (\in H)$ i $b \in H$ arbitrari. Tenim, doncs, que $e * b^{-1} = b^{-1} \in H$. Finalment, provarem la condició (i). Siguen $a, b \in H$ arbitraris. Per (iii), sabem que $b^{-1} \in H$ i, per la hipòtesi, $a * (b^{-1})^{-1} \in H$. Ara bé, com que $*$ és associativa, $(b^{-1})^{-1} = b$ (teorema 1.1.4), i en conseqüència $a * b \in H$. □

EXEMPLE 1.2.4. $(\mathbb{Z}, +)$ és un subgrup abelià de $(\mathbb{R}, +)$.

EXEMPLE 1.2.5. $\mathbb{N} \subset \mathbb{Z}$ no és un subgrup de $(\mathbb{Z}, +)$.

EXEMPLE 1.2.6. $(\mathbb{R}, +)$ i $(\mathbb{I}, +)$ són subgrups de $(\mathbb{C}, +)$ (amb $\mathbb{I}$ el conjunt dels imaginaris purs).

EXEMPLE 1.2.7. $(\mathbb{R} - \{0\}, \cdot)$ és un subgrup de $(\mathbb{C} - \{0\}, \cdot)$, però $(\mathbb{I} - \{0\}, \cdot)$ no ho és.

EXEMPLE 1.2.8. $\{e\}$ i G són els subgrups trivials d'un grup $(G, *)$.

EXEMPLE 1.2.9. Si G és un grup, el centre del grup, $Z(G) = \{z \in G \mid z * a = a * z, \forall a \in G\}$, és un subgrup abelià de G. Si G és abelià, aleshores $Z(G) = G$.

Teorema 1.2.3. *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 $(G, *)$.

Prova. Farem ús del teorema de caracterització de subgrups (teorema 1.2.2). Siguen $a, b \in H_1 \cap H_2$. Aleshores, $a, b \in H_1$ i $a, b \in H_2$, i com que H_1 i H_2 són subgrups, per l'esmentat teorema de caracterització, $a * b^{-1} \in H_1$, $a * b^{-1} \in H_2$ i, en conseqüència, $a * b^{-1} \in H_1 \cap H_2$. Sent a i b dos elements arbitraris de $H_1 \cap H_2$, el resultat anterior ens permet concloure que $H_1 \cap H_2$ és subgrup, per l'aplicació de nou del teorema de caracterització. □

Cal notar que la unió $H_1 \cup H_2$ de dos subgrups $H_1, H_2 \subset G$ no és un subgrup. De fet, es pot demostrar la proposició següent:

Proposició 1.2.4. Donats dos subgrups $H_1, H_2 \subset G$ d'un grup $(G, *)$, la unió $H_1 \cup H_2$ és un subgrup si, i sols si, $H_1 \subset H_2$ o $H_2 \subset H_1$.

Prova. Serà suficient demostrar que si $H_1 \not\subset H_2$ aleshores $H_2 \subset H_1$. Suposem que $\exists y \in H_1$ tal que $y \notin H_2$. Considerem $x \in H_2$ i demostrarem que $x \in H_1$. Tenim que $x, y \in H_1 \cup H_2$, i per ser subgrup, $z = x * y^{-1} \in H_1 \cup H_2$. Aleshores, si $z \in H_2$ resulta $y^{-1} = x^{-1} * z \in H_2$, és a dir, $y \in H_2$, en contra del que havíem suposat. Per tant, $z \in H_1$ i, en conseqüència, $x = z * y \in H_1$. □

EXEMPLE 1.2.10. El conjunt $G_n = \{x \in \mathbb{Z} \mid x = nq,\ q \in \mathbb{Z}\}$ dels múltiples enters d'un nombre natural $n \in \mathbb{N}$ és un subgrup de $(\mathbb{Z}, +)$. Aleshores, resulta que $G_m \cap G_n = G_p$, on p és el mínim comú múltiple de m i n, és un subgrup, i $G_m \cup G_n$ no ho és.

EXEMPLE 1.2.11. $\mathbb{R}$ 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.

1.3. Homomorfismes de grups

Donats dos grups $(G, *)$ i $(H, \perp)$, direm que una aplicació $f : G \longrightarrow H$ és un **homomorfisme de grups** si

$$\forall x, y \in G,\ \ f(x * y) = f(x) \perp f(y).$$

EXEMPLE 1.3.1. L'aplicació $f : \mathbb{Z} \longrightarrow \mathbb{R}\ ; q \longrightarrow e^q$ és un homomorfisme entre els grups $(\mathbb{Z}, +)$ i $(\mathbb{R} - \{0\}, \cdot)$.

EXEMPLE 1.3.2. L'aplicació $f(z) = |z|$ és un homomorfisme entre els grups $(\mathbb{C} - \{0\}, \cdot)$ i $(\mathbb{R} - \{0\}, \cdot)$.

EXEMPLE 1.3.3. La funció real de variable real $k(x) = \cos x$ no és un homomorfisme entre les estructures usuals de grup que tenim definides en $\mathbb{R}$ (el grup additiu $(\mathbb{R}, +)$ i el grup multiplicatiu $(\mathbb{R} - \{0\}, \cdot)$).

Classificació d'homomorfismes

Existeixen diferents tipus d'homomorfismes, depenent del tipus d'aplicació subjacent en cada cas:

(i) *Monomorfismes*: homomorfismes injectius, és a dir, aquells homomorfismes que satisfan $\forall x, y \in G,\ x \neq y \ \Rightarrow\ f(x) \neq f(y)$.

(ii) *Epimorfismes*: homomorfismes epijectius, és a dir, aquells homomorfismes que satisfan $\forall a \in H,\ \exists\, x \in G$ tal que $f(x) = a$.

(iii) *Isomorfismes*: homomorfismes bijectius.

(iv) *Endomorfismes*: homomorfismes amb $(H, \perp) = (G, *)$.

(v) *Automorfismes*: endomorfismes bijectius.

Direm que $(G, *)$ i $(H, \perp)$ són **grups isomorfs** si existeix un isomorfisme entre ells.

EXEMPLE 1.3.4. *Aplicació nul·la*: $\mathcal{O}(a) = e_\perp$, $\forall\ a \in (G, *)$, $e_\perp$ neutre de $(H, \perp)$ és un homomorfisme. No és ni epimorfisme ni monomorfisme.

EXEMPLE 1.3.5. *Aplicació identitat*: $\mathcal{I}(a) = a$, $\forall\ a \in G$, és un automorfisme del grup $(G, *)$.

EXEMPLE 1.3.6. La funció $f(x) = e^x$ és un monomorfisme entre els grups $(\mathbb{Z}, +)$ i $(\mathbb{R} - \{0\}, \cdot)$, o entre els grups $(\mathbb{R}, +)$ i $(\mathbb{R} - \{0\}, \cdot)$, però no és epimorfisme. En canvi, és un isomorfisme entre $(\mathbb{R}, +)$ i el grup $(\mathbb{R}^+, \cdot)$, i un epimorfisme (però no un monomorfisme) entre els grups $(\mathbb{C}, +)$ i $(\mathbb{C} - \{0\}, \cdot)$.

EXEMPLE 1.3.7. La funció real de variable real $g(x) = x^2$ és un endomorfisme de $(\mathbb{R} - \{0\}, \cdot)$ que no és ni epimorfisme ni monomorfisme.

EXEMPLE 1.3.8. La funció real de variable real $h(x) = x^3$ és un automorfisme de $(\mathbb{R} - \{0\}, \cdot)$.

Propietats immediates dels homomorfismes

Teorema 1.3.1. *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 $e_\perp \in H$, és a dir, $f(e_*) = e_\perp$.

Prova. Siga a un element arbitrari de G. Si $e_* \in G$ i $e_\perp \in H$ són respectivament els neutres de $*$ i $\perp$, aleshores per definició de neutre i per ser f un homomorfisme,

$$f(a) \perp e_\perp = f(a) = f(a * e_*) = f(a) \perp f(e_*).$$

Finalment, simplificant $f(a)$, arribem al resultat desitjat. □

Teorema 1.3.2. *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 l'element x, és a dir, $f(x^{-1}) = f(x)^{-1}$.

Prova. Siguen $e_* \in G$ i $e_\perp \in H$ els neutres de $*$ i $\perp$, respectivament, Si considerem que f és homomorfisme i tenim en compte el resultat establert en el teorema anterior, aleshores, per a cada $x \in G$,

$$f(x^{-1}) \perp f(x) = f(x^{-1} * x) = f(e_*) = e_\perp.$$

$$f(x) \perp f(x^{-1}) = f(x * x^{-1}) = f(e_*) = e_\perp.$$

Les igualtats anteriors proven que $f(x^{-1})$ és el simètric de $f(x)$. □

Imatge i nucli 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 definit per,

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

Teorema 1.3.3. *Imatge d'un homomorfisme*
Si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, aleshores la imatge $Im(f)$ de f és un subgrup de $(H, \perp)$.

Prova. Ens basarem en el teorema de caracterització de subgrups (teorema 1.2.2) i provarem que donats $a, b \in Im(f)$, $a \perp b^{-1} \in Im(f)$. Siguen $a, b \in Im(f)$. Aleshores, $\exists\, x, y \in G$ tals que $a = f(x), b = f(y)$. Calculem ara $a \perp b^{-1} = f(x) \perp f(y)^{-1} = f(x) \perp f(y^{-1}) = f(x * y^{-1})$, on hem fet ús del teorema anterior. Per tant $a \perp b^{-1}$ és la imatge de l'element $x * y^{-1} \in G$. □

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

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

Teorema 1.3.4. *Nucli d'un homomorfisme*
Si $f : (G, *) \longrightarrow (H, \perp)$ és un homomorfisme de grups, aleshores el nucli $N(f)$ de f és un subgrup de $(G, *)$.

Prova. Novament, farem ús del teorema de caracterització de subgrups (teorema 1.2.2) i reduïrem la demostració a veure que si $x, y \in N(f)$ arbitraris, aleshores $x * y^{-1} \in N(f)$. Si tenim en compte el teorema 1.3.2 i el fet que $f(x) = e_\perp, f(y) = e_\perp$, resulta

$$f(x * y^{-1}) = f(x) \perp f(y^{-1}) = f(x) \perp f(y)^{-1} = e_\perp \perp e_\perp^{-1} = e_\perp.$$

Per tant, $x * y^{-1}$ està en el nucli de l'homomorfisme f. □

EXEMPLE 1.3.9. La imatge i el nucli de l'homomorfisme entre els grups $(\mathbb{Z}, +)$ i $(\mathbb{R} - \{0\}, \cdot)$, $f(q) = e^q$ són $Im(f) = \{e^q, q \in \mathbb{Z}\}$ i $N(f) = \{0\}$.

EXEMPLE 1.3.10. La imatge i el nucli de l'homomorfisme $f(z) = |z|$ entre els grups $(\mathbb{C} - \{0\}, \cdot)$ i $(\mathbb{R} - \{0\}, \cdot)$ són $Im(f) = \mathbb{R}^+ \cup \{0\}$, $N(f) = \{e^{i\theta}, \theta \in \mathbb{R}\}$.

Altres propietats dels homomorfismes

Proposició 1.3.5. 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 si i sols si $Im(f) = H$.

(v) f és monomorfisme si i sols si $N(f) = \{e_*\}$, on e_* és el neutre de $*$.

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

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

Prova. (i) La demostració d'aquesta propietat segueix l'argumentació de la prova del teorema 1.3.3, ara aplicada al grup $(F, *)$.

(ii) En aquest cas, cal aclarir que $f^{-1}(I)$ es refereix al conjunt de les antiimatges del conjunt I. La demostració es basa en el teorema de caracterització de subgrups (teorema 1.2.2). Siguen x, y dos elements arbitraris de $f^{-1}(I)$. Aleshores, existeixen dos elements $a, b \in I$ tals que $f(x) = a$, $f(y) = b$. Basant-nos ara en el teorema 1.3.2 i en el fet que I és subgrup provem, finalment, que $f(x * y^{-1}) \in I$ i, per tant, que $x * y^{-1} \in f^{-1}(I)$.

(iii) La demostració en aquest cas és molt senzilla i, a més, es pot estendre a qualsevol subgrup commutatiu de $(G, *)$ i la seua imatge.

(iv) És la definició d'homomorfisme epijectiu.

(v) Es tracta d'una caracterització molt útil dels monomorfismes. Provarem primer la condició necessària. Siga $x \in N(f)$. Aleshores, $f(x) = e_\perp$, on $e_\perp$ és el neutre de $\perp$. Ara bé, pel teorema 1.3.1, sabem que $f(e_*) = e_\perp$, i com que f és injectiva, resulta $x = e_*$ i $N(f) = \{e_*\}$. Per a demostrar la condició suficient, prenem $x, y \in G$ tals que $f(x) = f(y)$ i provarem que $x = y$. Tenim:

$$f(x * y^{-1}) = f(x) \perp f(y^{-1}) = f(x) \perp f(y)^{-1} = e_\perp,$$

on hem fet ús del teorema 1.3.2 i del fet que $f(x) = f(y)$. Tenim aleshores que $x * y^{-1} \in N(f) (= \{e_*\})$, d'on es conclou que $x = y$.

(vi) Com que f és bijectiva, f^{-1} és una aplicació (bijectiva). Provarem que és, a més, homomorfisme, és a dir, que $f^{-1}(a \perp b) = f^{-1}(a) * f^{-1}(b),\ \forall a, b \in H$.

Siguen $a, b \in H$. Aleshores, $\exists!\ x, y \in G$ tals que $f(x) = a, f(y) = b$. Ara,

$$\begin{aligned} f^{-1}(a) * f^{-1}(b) &= f^{-1}(f(x)) * f^{-1}(f(y)) = (f^{-1} \circ f)(x) * (f^{-1} \circ f)(y) = \\ &= x * y = (f^{-1} \circ f)(x * y) = f^{-1}(f(x * y)) = \\ &= f^{-1}(f(x) \perp f(y)) = f^{-1}(a \perp b), \end{aligned}$$

on hem fet ús del fet que $f^{-1} \circ f$ és l'aplicació identitat.

(vii) La demostració consisteix a provar que $f \circ g$ verifica la definició d'homomorfisme recolzant-se en la definició de composició d'aplicacions i el fet que f i g són homomorfismes. □

Grups d'homomorfismes

Si $(G,*)$ i $(H,+)$ són dos grups abelians, denotem per $Hom(G,H)$ el conjunt de tots els homomorfismes de G en H. En el conjunt $Hom(G,H)$ podem definir la *suma d'homomorfismes*:

$$(f+g)(a) = f(a) + g(a), \quad \forall a \in G.$$

Teorema 1.3.6. *El grup $Hom(G,H)$*
El conjunt dels homomorfismes entre els grups abelians $(G,*)$ i $(H,+)$, té estructura de grup abelià amb l'operació suma.

Prova. És fàcil provar que $f+g$ és homomorfisme si f i g ho són. La propietat associativa és conseqüència de l'associativa en $(H,+)$. L'element neutre és l'aplicació nul·la $\mathcal{O}$, $\mathcal{O}(a) = 0\ \forall a \in G$, on 0 és el neutre del grup H. El simètric de f és l'aplicació $-f$ definida com $(-f)(a) = -f(a)$. □

Teorema 1.3.7. *El grup d'automorfismes, $Aut(G)$*
El conjunt dels automorfismes d'un grup $(G,*)$, $Aut(G)$, té estructura de grup no commutatiu amb la composició d'aplicacions.

Prova. La composició d'aplicacions és associativa i la composició de dues bijeccions és una bijecció. L'aplicació identitat és l'element neutre. Les propietats (vi) i (vii) de la proposició 1.3.5 impliquen la resta de propietats. □

EXEMPLE 1.3.11. Els automorfismes del grup additiu dels reals, $(\mathbb{R},+)$, són les funcions reals de variable real de la forma $f(x) = \alpha x$, $\alpha \in \mathbb{R}$, $\alpha \neq 0$. És un grup isomorf al grup multiplicatiu dels reals, $Aut(\mathbb{R},+) \approx (\mathbb{R} - \{0\}, \cdot)$.

EXEMPLE 1.3.12. Els automorfismes del grup $(\mathbb{Z},+)$ són les funcions $\mathcal{I}$ (identitat) i $-\mathcal{I}$. És un grup isomorf al grup multiplicatiu $(\{1,-1\},\cdot)$.

1.4. Grup simètric i grup de permutacions

El grup simètric i els seus subgrups, els grups de transformacions, tenen un paper important en la teoria abstracta de grups i en les aplicacions a la Física teòrica. El grup lineal general i els grups d'isometries són grups de transformacions que permeten definir les lleis d'invariància d'una teoria física.

Si X és un conjunt arbitrari, anomenem **transformació del conjunt** X a qualsevol aplicació bijectiva de X en X. El conjunt de les transformacions es denota S_X. Amb un raonament semblant al que s'ha fet a la prova del teorema 1.3.7 es demostra el teorema següent:

Teorema 1.4.1. *Grup simètric*
El conjunt S_X de les transformacions d'un conjunt X té estructura de grup amb la composició d'aplicacions.

El grup S_X s'anomena **grup simètric**. Els subgrups del grup simètric s'anomenen **grups de transformacions**. Si el conjunt és un grup G, aleshores $Aut(G)$ és un grup de transformacions: $Aut(G) \subset S_G$.

Una **acció a l'esquerra** del grup $(G, *)$ sobre el conjunt X és un homomorfisme $\phi : G \longrightarrow S_X$. Per a $x \in X$ i $g \in G$, escriurem $\phi(g)(x) = gx$. L'**òrbita del punt** $x \in X$ **per l'acció del grup** G és el subconjunt de X:

$$Gx = \{gx \mid g \in G\}.$$

Es diu que l'acció del grup G sobre X és **transitiva** si $\forall x, y \in X$, $\exists g \in G$ tal que $y = gx$, és a dir, $X = Gx$ per a tot $x \in X$.

Proposició 1.4.2. *Grup d'isotropia*
El conjunt $G_x = \{g \mid gx = x\}$ és un subgrup de G que s'anomena **grup d'isotropia**.

Prova. Per ser l'acció ϕ un homomorfisme, $\phi(g)^{-1} = \phi(g^{-1})$. Per tant, si $gx = x$ aleshores $g^{-1}x = x$, és a dir, $g^{-1} \in G_x$ si $g \in G_x$. Si $a, b \in G_x$, aleshores $a * b \in G_x$ ja que $(a * b)x = a(bx) = ax = x$. □

Si $(G, *)$ és un grup, es defineix la **translació a l'esquerra** per l'element $g \in G$ com l'aplicació $L_g : G \longrightarrow G$, $L_g(a) = g * a$.

Proposició 1.4.3. El conjunt L_G de les translacions a l'esquerra d'un grup $(G, *)$ és un subgrup del grup simètric S_G.

Prova. Una translació L_g admet inversa i està donada per $L_g^{-1} = L_{g^{-1}}$. Per tant, $L_G \subset S_G$. A més, $L_g \circ L_h^{-1} = L_g \circ L_{h^{-1}} = L_{g*h^{-1}} \in L_G$. □

Teorema 1.4.4. L'aplicació $\phi : G \longrightarrow S_G$, $\phi(g) = L_g$ defineix una acció del grup $(G, *)$ sobre ell mateix.

Prova. Caldrà demostrar que ϕ és un homomorfisme, és a dir, se satisfà que $\phi(g * h) = \phi(g) \circ \phi(h)$. En efecte,

$$\phi(g*h)(a) = (g*h)*a = g*(h*a) = \phi(g)[\phi(h)(a)] = [\phi(g) \circ \phi(h)](a). \quad \square$$

Corol·lari 1.4.5. *Teorema de Cayley*
Tot grup $(G, *)$ és isomorf a un grup de transformacions, en concret al grup de les translacions a l'esquerra L_G.

Prova. L'homomorfisme ϕ que defineix l'acció del teorema anterior és injectiu ja que si L_g és l'aplicació identitat aleshores $g = e$, és a dir, $N(\phi) = \{e\}$, on e és el neutre de G. A més $Im(\phi) = L_G$, on L_G és el conjunt de les translacions a l'esquerra. El corol·lari queda demostrat si tenim en compte que una aplicació injectiva és bijectiva sobre el conjunt imatge. □

Grup de permutacions

Una **permutació** de n elements és una reordenació d'aquests elements. Matemàticament podem definir les permutacions com bijeccions del conjunt de n elements, X_n, en ell mateix. Per tant el conjunt de les permutacions és el grup simètric d'un conjunt finit. El denotarem S_n. El seu cardinal és $\mathrm{card}\,(S_n) = n!$.

Els subgrups de S_n s'anomenen **grups de permutacions** (grups de transformacions per al cas finit). Els grups de permutacions no són en general abelians.

Una **transposició** és una permutació en què tan sols dos elements intercanvien la seua posició. Pot veure's fàcilment que tota permutació pot ser descomposta en un conjunt de transposicions, i que el nombre de transposicions en què es pot descompondre una permutació donada, encara que no és únic, és sempre parell o senar. Aquest resultat ens permet introduir el concepte de signatura d'una permutació. Si $\sigma \in S_n$ és una permutació del conjunt de les permutacions de n elements, es defineix la **signatura** de σ, $\operatorname{sign}(\sigma)$, com

$$\operatorname{sign}(\sigma) \equiv (-1)^{n_t} = \begin{cases} +1, & \text{per } n_t \text{ parell} \\ -1, & \text{per } n_t \text{ senar,} \end{cases}$$

on n_t és el nombre de transposicions en què es descompon la permutació σ. Direm que σ és una permutació parella (senar) si $\operatorname{sign}(\sigma) = +1$ (-1). La permutació identitat es considera parella.

Acabem amb un teorema i dues conseqüències interessants.

Teorema 1.4.6. La signatura del producte de dues permutacions σ_1, σ_2 és igual al producte de les signatures,

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

Prova. La demostració es basa en l'associativitat de la composició de permutacions. □

Corol·lari 1.4.7. La signatura sign és un homomorfisme entre el grup de permutacions $(S_n, \circ)$ i el grup multiplicatiu $(\{+1, -1\}, \cdot)$.

Prova. La prova és l'enunciat del teorema anterior. □

Corol·lari 1.4.8. S_n^+, el subconjunt de S_n de les permutacions de n elements amb signatura parella, és un subgrup del grup $(S_n, \circ)$.

Prova. Utilitzarem el teorema de caracterització de subgrups, teorema 1.2.2, el teorema 1.3.2 per a homomorfismes de grups, i el teorema i corol·lari anteriors. Siguen $\sigma_1, \sigma_2 \in S_n^+$. Aleshores tenim $\operatorname{sign}(\sigma_1 \circ \sigma_2^{-1}) = \operatorname{sign}(\sigma_1) \operatorname{sign}(\sigma_2^{-1}) = \operatorname{sign}(\sigma_1) \operatorname{sign}(\sigma_2)^{-1} = (+1)(+1) = +1$, el que prova el corol·lari. □

A l'apèndix C s'estudien algunes propietats més del grup de permutacions.

1.5. Anells i cossos

Anells

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

(i) $(A, \perp)$ és un grup abelià.

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

(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 un neutre per a la l.c.i. $*$. Per altra banda, direm que l'anell és **abelià** si la l.c.i. $*$ és commutativa.

EXEMPLE 1.5.1. Els conjunts numèrics $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ amb la suma i el producte usuals són anells commutatius i unitaris.

Denotem per 0 l'element neutre de la llei $\perp$ (que anomenem *llei additiva*). Denotem $-a$ el simètric (o oposat) d'un element a respecte d'aquesta llei. Si l'anell és unitari, denotem per 1 l'element neutre de la llei $*$ (*llei multiplicativa*). Si un element a admet simètric a^{-1} respecte d'aquesta llei, l'anomenarem també invers.

Si $(G, +)$ és un grup abelià, denotem $End(G)$ el conjunt de tots els endomorfismes de G. En $End(G)$ tenim definida la suma i la composició d'aplicacions.

Teorema 1.5.1. *L'anell $End(G)$*
El conjunt dels endomorfismes d'un grup $(G, +)$ té estructura d'anell unitari no commutatiu amb la suma i la composició d'aplicacions.

Prova. El teorema 1.3.6 ens diu que $End(G)$ és un grup abelià amb l'operació suma, i ja hem vist (proposició 1.3.5(vii)) que la composició és l.c.i. que, a més, és associativa. L'element neutre de la composició és l'aplicació identitat. Finalment, la propietat distributiva, $f \circ (g + h) = f \circ g + f \circ h$, se satisfà com a conseqüència de la definició de suma d'aplicacions i per ser f un homomorfisme. □

Proposició 1.5.2. Si $(A, \perp, *)$ és un anell, se satisfan les *regles dels signes* 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) $(-a) * (-b) = a * b \quad \forall\, a, b \in A.$

Prova. (i) Provarem que $a * 0 = 0$ basant-nos en la propietat distributiva de la llei multiplicativa respecte de l'additiva

$$a * a = a * (a \perp 0) = (a * a) \perp (a * 0) \implies a * 0 = 0.$$

(ii) Provarem que $(-a) * b$ és l'oposat de $(a * b)$ utilitzant de nou la distributiva de la llei multiplicativa respecte de l'additiva i la regla (i)

$$(a * b) \perp ((-a) * b) = (a \perp (-a)) * b = 0 * b = 0.$$