Fonaments de la matemàtica
Resums, exercicis i problemes

Jaume Martí-Farré, Mercè Mora Giné, Miguel C. Muñoz Lecanda

Grau en Matemàtiques
Facultat de Matemàtiques i Estadística
Universitat Politècnica de Catalunya

Setembre 2014

Índex

1
Formalisme matemàtic: enunciats i demostracions

1.1 Resum teòric

Enunciats i demostracions

≡ **Tècniques de demostració** *Implicació, equivalències i inducció.*

1) Demostració de la implicació $P \Rightarrow Q$.
   - *Prova directa.* Deduir Q a partir de P.
   - *Contrarecíproc.* Deduir "*no* P" a partir de "*no* Q".
   - *Reducció a l'absurd.* Suposar que P i "*no* Q" són certes i arribar a una contradicció.
2) Equivalències.
   - Demostrar "$P \Leftrightarrow Q$" és equivalent a demostrar la implicació "$P \Rightarrow Q$" i demostrar la implicació "$Q \Rightarrow P$".
   - Demostrar "$P \Leftrightarrow Q$" és equivalent a demostrar la implicació "$P \Rightarrow Q$" i demostrar la implicació "*no* $P \Rightarrow$ *no* Q".
   - Demostrar la implicació "$P \Rightarrow (Q$ *i* $R)$" és equivalent a demostrar les implicacions "$P \Rightarrow Q$" i "$P \Rightarrow R$".
   - Demostrar la implicació "$P \Rightarrow (Q$ *o* $R)$" és equivalent a demostrar la implicació "$P \Rightarrow Q$" o a demostrar la implicació "$P \Rightarrow R$".
   - Demostrar la implicació "$P \Rightarrow (Q$ *o* $R)$" és equivalent a demostrar R a partir de P i de "*no* Q".
   - Demostrar la implicació "$(P$ *o* $Q) \Rightarrow R$" és equivalent a demostrar les implicacions "$P \Rightarrow R$" i "$Q \Rightarrow R$".

3) Principi d'inducció.

- Considerem una propietat $P(n)$ que depèn de n, on $n \in \mathbb{Z}$. Sigui $n_0 \in \mathbb{Z}$.

  Versió 1. Podem afirmar que $P(n)$ és certa per a tot $n \geq n_0$ si es compleixen les dues condicions següents:
  a) $P(n_0)$ és certa,
  b) per a tot $n \geq n_0$, de $P(n)$ certa, podem deduir que $P(n+1)$ és certa.

  Versió 2. Podem afirmar que $P(n)$ és certa per a tot $n \geq n_0$ si es compleixen les dues condicions següents:
  a) $P(n_0)$ és certa,
  b) per a tot $n > n_0$, de $P(n-1)$ certa, podem deduir que $P(n)$ és certa.

  Versió 3. Podem afirmar que $P(n)$ és certa per a tot $n \geq n_0$ si es compleixen les dues condicions següents:
  a) $P(n_0)$ és certa,
  b) per a tot $n > n_0$, de $P(k)$ certa per a tot k tal que $n_0 \leq k < n$, podem deduir que $P(n)$ és certa.

Proposicions lògiques

≡ **Taules de veritat** *Taules de veritat dels connectius* $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$.

- Siguin P i Q dues proposicions.

P	$\neg P$
1	0
0	1

P	Q	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

≡ **Definició** *Tautologies i contradiccions. Equivalència lògica.*

1) Una tautologia és una forma proposicional que pren sempre el valor de veritat 1.

2) Una contradicció és una forma proposicional que pren sempre el valor de veritat 0.

3) Dues formes proposicionals P i Q són equivalents si prenen sempre el mateix valor de veritat. Ho escriurem $P \equiv Q$.

≡ **Propietats** *Algunes tautologies i equivalències lògiques.*

- Tautologies.

  a) $P \to P \vee Q$

  b) $P \wedge Q \to P$

  c) $((P \to Q) \wedge P) \to Q$

  d) $((P \to Q) \wedge \neg Q) \to \neg P$

  e) $((P \vee Q) \wedge \neg P) \to Q$

  f) $((P \to Q) \wedge (Q \to R)) \to (P \to R)$

- Equivalències lògiques.

  a) $\neg(\neg P) \equiv P$ *(doble negació)*

  b) $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$, $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ *(lleis de De Morgan)*

  c) $P \wedge Q \equiv Q \wedge P$, $P \vee Q \equiv Q \vee P$ *(commutativitat)*

  d) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$, $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ *(associativitat)*

  e) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$, $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ *(distributivitat)*

  f) $P \to Q \equiv \neg P \vee Q$, $\neg(P \to Q) \equiv P \wedge \neg Q$

- Equivalències lògiques corresponents a tècniques de demostració.

  a) $P \to Q \equiv \neg Q \to \neg P$ *(contrarecíproc)*

  b) $P \to (Q \wedge R) \equiv (P \to Q) \wedge (P \to R)$

  c) $P \to (Q \vee R) \equiv (P \to Q) \vee (P \to R)$

  d) $P \to (Q \vee R) \equiv (P \wedge \neg Q) \to R \equiv (P \wedge \neg R) \to Q$

Expressions amb quantificadors

≡ **Notacions** *Predicats i variables. Quantificadors*

- En aquesta secció $P(x)$ denota un *predicat* on x és la seva *variable*. En general, $P(x_1, \ldots, x_n)$ és un predicat que té per variables $x_1, \ldots, x_n$.

- $\forall$: quantificador universal "per a tot".

- $\exists$: quantificador existencial "existeix".

≡ **Propietats** *Negació i commutativitat.*

- Negació.
  a) $\neg\forall x P(x)$ és equivalent a $\exists x \neg P(x)$.
  b) $\neg\exists x P(x)$ és equivalent a $\forall x \neg P(x)$.
  c) $\neg\forall x \forall y P(x,y)$ és equivalent a $\exists x \exists y \neg P(x,y)$.
  d) $\neg\exists x \exists y P(x,y)$ és equivalent a $\forall x \forall y \neg P(x,y)$.
  e) $\neg\forall x \exists y P(x,y)$ és equivalent a $\exists x \forall y \neg P(x,y)$.
  f) $\neg\exists x \forall y P(x,y)$ és equivalent a $\forall x \exists y \neg P(x,y)$.
- Commutativitat.
  a) $\forall x \forall y P(x,y)$ és equivalent a $\forall y \forall x P(x,y)$.
  b) $\exists x \exists y P(x,y)$ és equivalent a $\exists y \exists x P(x,y)$.
  c) En general, l'expressió $\forall x \exists y P(x,y)$ i l'expressió $\exists y \forall x P(x,y)$ no són equivalents. Concretament, sempre es pot deduir que $\forall x \exists y P(x,y)$ a partir de $\exists y \forall x P(x,y)$, però en general no es pot deduir $\exists y \forall x P(x,y)$ a partir de $\forall x \exists y P(x,y)$.

≡ **Tècniques de demostració** *Enunciats amb quantificadors.*

1) Demostració de $\forall x P(x)$.
   - Fer una demostració genèrica de $P(x)$, és a dir, que sigui vàlida per a qualsevol valor de x.
   - Reducció a l'absurd: arribar a contradicció a partir de $\exists x \neg P(x)$.
2) Demostració de $\exists x P(x)$.
   - Trobar un element concret c tal que la proposició $P(c)$ sigui certa.
   - Reducció a l'absurd: arribar a contradicció a partir de $\forall x \neg P(x)$.
3) Demostració de $\neg\forall x P(x)$.
   - És equivalent a demostrar $\exists x \neg P(x)$. En aquest cas, si c és tal que la proposició $\neg P(c)$ és certa, direm que c és un *contraexemple* de $\forall x P(x)$.
4) Demostració de $\neg\exists x P(x)$.
   - És equivalent a demostrar $\forall x \neg P(x)$.

Sumatoris i productoris

≡ **Propietats** *Sumatoris i productoris.*

- Siguin $a_1, \ldots, a_n, b_1, \ldots, b_n, \lambda$ nombres. Aleshores:

$$\sum_{i=1}^{n}(a_i+b_i)=\left(\sum_{i=1}^{n}a_i\right)+\left(\sum_{i=1}^{n}b_i\right). \qquad \prod_{i=1}^{n}(a_ib_i)=\left(\prod_{i=1}^{n}a_i\right)\left(\prod_{i=1}^{n}b_i\right).$$

$$\sum_{i=1}^{n}\lambda a_i=\lambda\sum_{i=1}^{n}a_i. \qquad \prod_{i=1}^{n}\lambda a_i=\lambda^n\prod_{i=1}^{n}a_i.$$

$$\sum_{i=1}^{n}\lambda=n\lambda. \qquad \prod_{i=1}^{n}\lambda=\lambda^n.$$

$$\sum_{i=1}^{n}a_i=\sum_{i=0}^{n-1}a_{i+1}=\sum_{i=2}^{n+1}a_{i-1}. \qquad \prod_{i=1}^{n}a_i=\prod_{i=0}^{n-1}a_{i+1}=\prod_{i=2}^{n+1}a_{i-1}.$$

En general, $\displaystyle\sum_{i=1}^{n}(a_ib_i)\neq\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{i=1}^{n}b_i\right)$, $\displaystyle\prod_{i=1}^{n}(a_i+b_i)\neq\left(\prod_{i=1}^{n}a_i\right)+\left(\prod_{i=1}^{n}b_i\right)$.

- Siguin $a_1,a_2,a_3,a_4,\ldots$ nombres. Aleshores:

  $\displaystyle\sum_{i\geq 1}a_{2i}$ indica la suma dels termes en posició parella, $a_2,a_4,\ldots$.

  $\displaystyle\sum_{i\geq 0}a_{2i+1}$ indica la suma dels termes en posició senar, $a_1,a_3,\ldots$.

  $\displaystyle\prod_{i\geq 1}a_{2i}$ indica el producte dels termes en posició parella, $a_2,a_4,\ldots$.

  $\displaystyle\prod_{i\geq 0}a_{2i+1}$ indica el producte dels termes en posició senar, $a_1,a_3,\ldots$.

≡ **Propietats** *Dobles sumatoris i dobles productoris.*

- Siguin $a_1,\ldots,a_n,b_1,\ldots,b_m,a_{1,1},a_{1,2},\ldots,a_{n,n}$ nombres. Aleshores:

$$\sum_{i=1}^{n}\left(\sum_{j=i}^{n}a_{i,j}\right)=\sum_{j=1}^{n}\left(\sum_{i=1}^{j}a_{i,j}\right)=\sum_{1\leq i\leq j\leq n}a_{i,j}\,.$$

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m}(a_ib_j)\right)=\sum_{j=1}^{m}\left(\sum_{i=1}^{n}(a_ib_j)\right)=\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right).$$

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m}(a_i+b_j)\right)=\sum_{j=1}^{m}\left(\sum_{i=1}^{n}(a_i+b_j)\right)=m\left(\sum_{i=1}^{n}a_i\right)+n\left(\sum_{j=1}^{m}b_j\right).$$

$$\prod_{i=1}^{n}\left(\prod_{j=i}^{n}a_{i,j}\right)=\prod_{j=1}^{n}\left(\prod_{i=1}^{j}a_{i,j}\right)=\prod_{1\leq i\leq j\leq n}a_{i,j}\,.$$

$$\prod_{i=1}^{n}\left(\prod_{j=1}^{m}(a_ib_j)\right)=\prod_{j=1}^{m}\left(\prod_{i=1}^{n}(a_ib_j)\right)=\left(\prod_{i=1}^{n}a_i\right)^m\left(\prod_{j=1}^{m}b_j\right)^n.$$

En general, $\displaystyle\prod_{i=1}^{n}\left(\prod_{j=1}^{m}(a_i+b_j)\right)=\prod_{j=1}^{m}\left(\prod_{i=1}^{n}(a_i+b_j)\right)\neq\left(\prod_{i=1}^{n}a_i\right)+\left(\prod_{j=1}^{m}b_j\right)$.

≡ **Propietats** *Sumatoris de productoris i productoris de sumatoris.*

- Siguin $a_1, \ldots, a_n, b_1, \ldots, b_m$ nombres. Aleshores:

$$\sum_{i=1}^{n}\left(a_i\prod_{j=1}^{m}b_j\right)=\left(\sum_{i=1}^{n}a_i\right)\left(\prod_{j=1}^{m}b_j\right).$$

$$\prod_{j=1}^{m}\left(b_j\sum_{i=1}^{n}a_i\right)=\left(\sum_{i=1}^{n}a_i\right)^m\left(\prod_{j=1}^{m}b_j\right).$$

$$\sum_{i=1}^{n}\left(\prod_{j=1}^{m}(a_ib_j)\right)=\left(\sum_{i=1}^{n}a_i^m\right)\left(\prod_{j=1}^{m}b_j\right).$$

$$\prod_{j=1}^{m}\left(\sum_{i=1}^{n}(a_ib_j)\right)=\left(\sum_{i=1}^{n}a_i\right)^m\left(\prod_{j=1}^{m}b_j\right).$$

$$\sum_{i=1}^{n}\left(a_i+\prod_{j=1}^{m}b_j\right)=\left(\sum_{i=1}^{n}a_i\right)+n\left(\prod_{j=1}^{m}b_j\right).$$

$$\prod_{j=1}^{m}\left(b_j+\sum_{i=1}^{n}a_i\right)=\big(a_1+\cdots+a_n+b_1\big)\cdot\ldots\cdot\big(a_1+\cdots+a_n+b_m\big).$$

$$\sum_{i=1}^{n}\left(\prod_{j=1}^{m}(a_i+b_j)\right)=\Big((a_1+b_1)\cdot\ldots\cdot(a_1+b_m)\Big)+\cdots+\Big((a_n+b_1)\cdot\ldots\cdot(a_n+b_m)\Big).$$

$$\prod_{j=1}^{m}\left(\sum_{i=1}^{n}(a_i+b_j)\right)=\big(a_1+\cdots+a_n+nb_1\big)\cdot\ldots\cdot\big(a_1+\cdots+a_n+nb_m\big)=\prod_{j=1}^{m}\left(n\,b_j+\sum_{i=1}^{n}a_i\right).$$

Alguns sumatoris i productoris

≡ **Progressió aritmètica**

1) Definició.

   Una progressió aritmética és una successió $(a_n)_n$ que satisfà $a_n = a_{n-1} + d$, on d és un valor constant que anomenem *diferència*.

2) Expressió del terme general.

   $a_n = a_k + (n-k)\,d$, per a tot $n \geq k$.

3) Suma de termes consecutius.

$$\sum_{i=1}^{n}a_i=\frac{a_1+a_n}{2}\,n.$$

$$\sum_{i=m}^{n}a_i=\frac{a_m+a_n}{2}(n-m+1).$$

4) Algunes sumes i productes.

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \qquad \prod_{i=1}^{n} i = n!$$

$$\sum_{i=m}^{n} i = \frac{(n-m+1)(m+n)}{2} \qquad \prod_{i=m}^{n} i = \frac{n!}{(m-1)!}, \text{ si } n \geq m$$

$$\sum_{i=1}^{n} i\,a = a\,\frac{n(n+1)}{2} \qquad \prod_{i=1}^{n} i\,a = a^n\,n!$$

≡ Progressió geomètrica

1) Definició.

   Una progressió geomètrica és una successió $(a_n)_n$ que satisfà $a_n = r\,a_{n-1}$, on r és un valor constant que anomenem *raó*.

2) Expressió del terme general.

   $a_n = a_k\,r^{n-k}$, per a tot $n \geq k$.

3) Sumes i productes de termes consecutius.

$$\sum_{i=1}^{n} a_i = \frac{a_n\,r - a_1}{r-1}, \text{ si } r \neq 1 \qquad \prod_{i=1}^{n} a_i = a_1^n\ r^{n(n-1)/2}$$

$$\sum_{i=m}^{n} a_i = \frac{a_n\,r - a_m}{r-1}, \text{ si } r \neq 1 \qquad \prod_{i=m}^{n} a_i = a_m^{n-m+1}\ r^{(n-m+1)(n-m)/2}$$

4) Algunes sumes i productes.

$$\sum_{i=1}^{n} r^i = \frac{r^{n+1} - r}{r-1}, \text{ si } r \neq 1 \qquad \prod_{i=1}^{n} r^i = r^{n(n+1)/2}$$

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r-1}, \text{ si } r \neq 1 \qquad \prod_{i=0}^{n} r^i = r^{n(n+1)/2}$$

$$\sum_{i=m}^{n} r^i = \frac{r^{n+1} - r^m}{r-1}, \text{ si } r \neq 1 \qquad \prod_{i=m}^{n} r^i = r^{(n+m)(n-m+1)/2}$$

≡ Altres sumatoris i productoris

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \qquad \prod_{i=1}^{n} i^k = (n!)^k$$

$$\sum_{i=1}^{n} i^3 = \Big(\sum_{i=1}^{n} i\Big)^2 = \frac{n^2(n+1)^2}{4} \qquad \sum_{j=1}^{m}\left(\sum_{i=1}^{n} i\,j\right) = \frac{nm(n+1)(m+1)}{4}$$

$$\sum_{j=1}^{n} \left(\sum_{i=j}^{n} i\, j \right) = \frac{n(n+1)(n+2)(3n+1)}{24}$$

1.2 Exercicis i problemes. Enunciats

1.1 Feu les taules de veritat de les formes proposicionals següents i determineu quines són tautologies:

1) $P \wedge Q \to P$.

2) $P \vee Q \to P$.

3) $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$.

4) $(P \vee Q \to R) \leftrightarrow ((P \to R) \wedge (Q \to R))$.

5) $(P \vee Q \to R) \leftrightarrow ((P \to R) \vee (Q \to R))$.

1.2 Demostreu les equivalències següents utilitzant cadenes d'equivalències lògiques:

1) $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$.

2) $(P \vee Q \to R) \leftrightarrow ((P \to R) \wedge (Q \to R))$.

1.3 Determineu si les proposicions següents són certes o no:

1) Per a tot enter x existeix un enter y tal que $xy = 0$.

2) Per a tot enter x existeix un únic enter y tal que $xy = 1$.

3) Existeix un enter y tal que per a tot enter x es compleix $xy = 1$.

4) Existeix un enter y tal que per a tot enter x es compleix $xy = x$.

1.4 Negueu els enunciats següents i determineu en cada cas si és cert l'enunciat donat o la seva negació:

1) $\forall x, y \in \mathbb{N}\ (x = y^2)$.

2) $\forall x \in \mathbb{N}\ \exists y \in \mathbb{R}\ (x = y^2)$.

3) $\forall x \in \mathbb{N}\ \exists y \in \mathbb{R}\ x \leq y$.

4) $\forall x, y, z \in \mathbb{R}\ ((x \leq y \text{ i } y \leq z) \Rightarrow x \leq z)$.

5) $\forall x, y \in \mathbb{R}\ (x > 0 \Rightarrow (\exists n \in \mathbb{N}\ y \leq nx))$.

6) $\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R}\ (|x| < \delta \Rightarrow x^2 < \varepsilon)$.

1.5

1) Suposem que les formes proposicionals $P \wedge Q$ i $(P \vee Q) \to R$ són certes. Podem deduir que R és certa?

2) Suposem que les formes proposicionals $P \vee Q \to R$, $S \to P$, $S \vee Q$ i $\neg T \to \neg R$ són certes. Podem deduir que T és certa?

3) Suposem que les formes proposicionals $E \to F$, $\neg G \to \neg F$, $H \to I$ i $E \vee H$ són certes. Podem deduir que $G \vee I$ és certa?

4) Suposem que les formes proposicionals $L \to (P \vee M)$, $(M \vee N) \to (L \to K)$ i $\neg P \wedge L$ són certes. Podem deduir que K és certa?

5) Suposem que les formes proposicionals $\neg A \to (B \to \neg C)$, $C \to \neg A$, $(\neg D \vee A) \to \neg\neg C$ i $\neg D$ són certes. Podem deduir que $\neg B$ és certa?

1.6 Calculeu el valor de cadascuna de les sumes següents:

1) $\sum_{j=1}^{10} 2.$
2) $\sum_{j=1}^{10} j.$
3) $\sum_{j=1}^{10} j^2.$
4) $\sum_{j=1}^{10} 2^j.$
5) $\sum_{n=3}^{6} (n-1).$
6) $\sum_{n=0}^{5} n!.$
7) $\sum_{n=-2}^{2} n^2.$
8) $\sum_{n=-2}^{2} n(n+1).$

1.7 Calculeu el valor de cadascun dels productes següents:

1) $\prod_{m=1}^{5} 3.$
2) $\prod_{m=1}^{5} (m+1).$
3) $\prod_{j=-1}^{4} (j+1).$
4) $\prod_{j=1}^{5} j^2.$
5) $\prod_{j=1}^{5} 2^j.$
6) $\prod_{j=1}^{5} j!.$

1.8 Trobeu el valor de cadascuna de les dobles sumes següents:

1) $\sum_{i=1}^{5}\sum_{j=1}^{6} j.$
2) $\sum_{i=1}^{5}\sum_{j=1}^{6} i.$
3) $\sum_{i=1}^{5}\sum_{j=1}^{6} (i+j).$
4) $\sum_{i=1}^{5}\sum_{j=1}^{6} (i+j+1).$
5) $\sum_{i=1}^{5}\sum_{j=1}^{6} ij.$
6) $\sum_{i=1}^{5}\sum_{j=1}^{6} (i+1)(j+1).$

1.9 Trobeu el valor de cadascun dels dobles productes següents:

1) $\prod_{i=1}^{4}\prod_{j=1}^{3} j.$
2) $\prod_{i=1}^{4}\prod_{j=1}^{3} i.$
3) $\prod_{i=1}^{3}\prod_{j=1}^{3} (i+1).$
4) $\prod_{i=1}^{4}\prod_{j=1}^{3} (i+j).$
5) $\prod_{i=1}^{4}\prod_{j=1}^{3} ij.$
6) $\prod_{i=1}^{4}\prod_{j=1}^{3} (i+1)(j-1).$

1.10 Trobeu el valor de cadascuna de les quantitats següents:

1) $\sum_{i=1}^{3}\prod_{j=1}^{4} ij.$
2) $\prod_{i=1}^{3}\sum_{j=1}^{4} ij.$
3) $\sum_{i=1}^{3}\prod_{j=1}^{4} (i+j).$
4) $\prod_{i=1}^{3}\sum_{j=1}^{4} (i+j).$

1.11 Sigui $S = \sum_{n=1}^{10} a_n$. Expresseu les sumes següents en funció de S:

1) $\sum_{m=1}^{10} a_m$. 2) $\sum_{i=0}^{9} a_{i+1}$. 3) $\sum_{j=1}^{10} a_{j-1}$.

1.12 Siguin m, n enters tals que $m \leq n$. Siguin $A = \sum_{m\leq i\leq n} a_i$ i on $B = \sum_{m\leq i\leq n} b_i$. Expresseu cadascuna de les sumes següents en funció de A i B:

1) $\sum_{m\leq i\leq n} 5a_i$. 2) $\sum_{m\leq i\leq n} (a_i - b_i)$. 3) $\sum_{m\leq i\leq n} (-b_i)$. 4) $\sum_{m\leq i\leq n} (3a_i + 4b_i)$.

1.13

1) Utilitzeu sumatoris per expressar la suma dels n primers nombres naturals parells no nuls i la suma dels n primers nombres naturals senars.
2) Calculeu el valor de l'expressió $\sum_{i=1}^{100}(2i-1) + \sum_{i=0}^{99}(2i+1)$.
3) Calculeu el valor de l'expressió $\sum_{i=1}^{100}(2i)^2 + \sum_{i=0}^{99}(2i+1)^2$. *Indicació*: $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

1.14 Sigui $A = \prod_{i=1}^{n} a_i$. Expresseu els productes següents en funció de A:

1) $\prod_{i=1}^{n} ia_i$. 2) $\prod_{i=1}^{n} a_i^k$.

1.15 Siguin n i m nombres naturals tals que $n \leq m$. Determineu r per tal que $\prod_{i=n}^{m} ka_i = k^r \prod_{i=n}^{m} a_i$.

1.16 Siguin $A = \prod_{i=n}^{m} a_i$ i $B = \prod_{i=n}^{m} b_i$, on $m \geq n$. Expresseu $\prod_{i=n}^{m} a_i b_i$ en funció d'A i B.

1.17 Siguin $A = \prod_{i=1}^{m} a_i$ i $B = \prod_{i=1}^{n} b_i$. Expresseu $\prod_{i=1}^{m}\prod_{j=1}^{n} a_i b_j$ en funció d'A i B.

1.18 Determineu si les expressions següents són iguals en general:

$\prod_{i=1}^{m}(a_i + b_i)$; $\left(\prod_{i=1}^{m} a_i\right) + \left(\prod_{i=1}^{m} b_i\right)$; $\left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{m} b_i\right)$.

1.19 Demostreu per inducció les fórmules següents:

1) $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\forall n \geq 1$. 2) $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\forall n \geq 1$.

3) $\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$, $\forall n \geq 1$.

4) $\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}$, $\forall n \geq 1$.

5) $\sum_{k=1}^{n-1} k \cdot k! = n! - 1$, $\forall n \geq 2$.

6) $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$, $\forall n \geq 0$.

7) $\sum_{k=0}^{n-1} 2\,(-5)^k = \frac{1-(-5)^n}{3}$, $\forall n \geq 1$.

8) $\sum_{k=1}^{n} (-1)^{k-1} k^2 = (-1)^{n-1} \frac{n(n+1)}{2}$, $\forall n \geq 1$.

9) $\sum_{k=1}^{n} k\,2^k = (n-1)2^{n+1} + 2$, $\forall n \geq 1$.

10) $\prod_{k=2}^{n} \left(1 - \frac{1}{k}\right) = \frac{1}{n}$, $\forall n > 1$.

1.20 Considerem la fórmula $\sum_{k=1}^{n} k = \frac{(2n+1)^2}{8}$, on n és enter.

1) Demostreu que, per a tot $n \geq 1$, si la fórmula és certa per a n, també ho és per a $n+1$.

2) Per a quins valors de n és vàlida?

3) Determineu si existeix un nombre real λ tal que $\sum_{k=1}^{n} k = \frac{(2n+1)^2}{8} + \lambda$, per a tot enter $n \geq 1$.

1.21 Demostreu per inducció les desigualtats següents:

1) Si $0 < a \leq b$, aleshores $a^n \leq b^n$, $\forall n \geq 1$.

2) $n^2 - 5n + 6 \geq 0$, $\forall n \geq 0$.

3) $n^2 < 2^n$, $\forall n \geq 5$.

4) $3^n < n!$, $\forall n \geq 7$.

5) $n! < n^n$, $\forall n \geq 2$.

6) $\sum_{k=1}^{n} \frac{1}{k^2} < 2 - \frac{1}{n}$, $\forall n > 1$.

7) $\frac{1}{2n} \leq \prod_{k=1}^{n} \frac{2k-1}{2k}$, $\forall n > 0$.

8) $\sum_{k=0}^{n-1} k^2 < \frac{n^3}{3} < \sum_{k=0}^{n} k^2$, $\forall n \geq 1$.

9) $\sum_{k=1}^{2^n} \frac{1}{k} \leq n + 1$, $\forall n \geq 0$.

1.22 Demostreu que, per a tot natural $n \geq 1$, el nombre $n^3 + (n+1)^3 + (n+2)^3$ és múltiple de 9.

1.23 Considerem un tauler $2^n \times 2^n$ on $n \geq 1$, enter, i triem una casella qualsevol. Demostreu que es pot recobrir tot el tauler excepte la casella triada amb peces formades per 3 caselles en forma de L, sense trencar-les i de forma que no se solapin.

1.24 Siguin x, y nombres reals positius no nuls. Demostreu que si $y > x$, aleshores

$$\frac{x+1}{y+1} > \frac{x}{y}.$$

És cert el recíproc?

1.25 Demostreu la fórmula de resolució de l'equació de segon grau $a\,x^2 + b\,x + c = 0$, on a, b, c són nombres reals tals que $a \neq 0$.

1.26 Demostreu que la suma de dos nombres senars consecutius és múltiple de 4.

1.27 Considerem un enter m i un nombre natural qualsevol n. Demostreu que m^n és senar si, i només si, m és senar.

1.28 Considerem la proposició: "Per a tot $n \in \mathbb{N}$, el nombre $n^2 + 5n + 6$ no és primer".

1) Determineu si són correctes les demostracions següents:

   a) Per a $n = 2$ tenim $n^2 + 5n + 6 = 2^2 + 10 + 6 = 20$, que no és primer. Per tant, la proposició és certa.

   b) Si n és un nombre natural, en particular $n > 0$. Si $n^2 + 5n + 6$ no és primer, aleshores $n^2 + 5n + 6 = pq$ per a alguns nombres naturals p, q tals que $0 < p < n^2 + 5n + 6$ i $0 < q < n^2 + 5n + 6$. Sabem que $n^2 + 5n + 6 = pq$, i els nombres p, q són diferents de 1 i de $n^2 + 5n + 6$. Per tant, $n^2 + 5n + 6$ no és primer, tal com volíem demostrar.

2) Feu una demostració de la proposició si les demostracions anteriors són incorrectes.

1.29 Considerem tres punts qualssevol del pla. Demostreu que els tres punts són d'una mateixa recta o els tres punts són d'una mateixa circumferència.

1.30 Determineu si és cert o fals: "Si x és irracional, aleshores $\sqrt{x}$ és irracional".

1.31 Suposem que x, y són nombres reals no nuls. Demostreu que $\sqrt{x^2 + y^2} \neq x + y$.

1.32 Demostreu que si $x^2 - 3x + 2 < 0$, aleshores $1 < x < 2$.

1.33 Demostreu que la suma dels angles interiors d'un polígon convex de n vèrtexs és igual a $\pi(n - 2)$.

1.3 Exercicis i problemes. Solucions

1.1

P	Q	$P \wedge Q \to P$	$P \vee Q \to P$	$(P \to Q) \leftrightarrow (\neg Q \to \neg P))$
1	1	1	1	1
1	0	1	1	1
0	1	1	0	1
0	0	1	1	1

P	Q	R	$(P \vee Q \to R) \leftrightarrow ((P \to R) \wedge (Q \to R))$	$(P \vee Q \to R) \leftrightarrow ((P \to R) \vee (Q \to R))$
1	1	1	1	1
1	1	0	1	1
1	0	1	1	1
1	0	0	1	0
0	1	1	1	1
0	1	0	1	0
0	0	1	1	1
0	0	0	1	1

Són tautologies les formes proposicionals dels apartats 1, 3 i 4.

1.3

1) Cert. 2) Fals. 3) Fals. 4) Cert.

1.4

1) $\exists x, y \in \mathbb{N}\ (x \neq y^2)$. L'enunciat és fals.

2) $\exists x \in \mathbb{N}\ \forall y \in \mathbb{R}\ (x \neq y^2)$. L'enunciat és cert.

3) $\exists x \in \mathbb{N}\ \forall y \in \mathbb{R}\ (x > y)$. L'enunciat és cert.

4) $\exists x, y, z \in \mathbb{R}\ (x \leq y \text{ i } y \leq z \text{ i } x > z)$. L'enunciat és cert.

5) $\exists x, y \in \mathbb{R}\ \big(x > 0 \text{ i } \forall n \in \mathbb{N}\ (y > nx)\big)$. L'enunciat és cert.

6) $\exists \varepsilon > 0\ \forall \delta > 0\ \exists x \in \mathbb{R}\ (|x| < \delta \text{ i } x^2 \geq \varepsilon)$. L'enunciat és cert.

1.5

1) Sí. 2) Sí. 3) Sí. 4) Sí. 5) Sí.

1.6

1) 20. 2) 55. 3) 385. 4) 2046. 5) 14. 6) 154. 7) 10. 8) 10.

1.7

1) 243. 2) 720. 3) 0. 4) 14400. 5) 32768. 6) 34560.

1.8

1) 105. 2) 90. 3) 195. 4) 225. 5) 315. 6) 540.

1.9

1) 1296. 2) 13824. 3) 13824. 4) 36288000. 5) 17915904. 6) 0.

1.10

1) 2352. 2) 6000. 3) 1320. 4) 5544.

1.11

1) S. 2) S. 3) $S - a_{10} + a_0$.

1.12

1) $5A$. 2) $A - B$. 3) $-B$. 4) $3A + 4B$.

1.13

1) $\sum_{i=1}^{n}(2i)$, $\sum_{i=1}^{n}(2i-1)$.

2) 20000.

3) És la suma dels quadrats dels primers 200 nombres naturals, $\sum_{i=1}^{200} i^2 = 2686700$.

1.14

1) $n!\,A$. 2) A^k.

1.15 $r = m - n + 1$.

1.18 Les tres expressions són diferents en general.

1.20

1) Per a cap.

2) $\lambda = -\frac{1}{8}$.

2
Conjunts i aplicacions

2.1 Resum teòric

Conjunts

≡ **Definició** *Subconjunt, inclusió i igualtat. Conjunt de les parts.*

1) Inclusió i igualtat.

   - Sigui X un conjunt. Direm que un conjunt Y és un subconjunt del conjunt X, i ho notarem $Y \subseteq X$, si tot element de Y és un element de X.
   - Dos conjunts X_1 i X_2 són iguals si tenen els mateixos elements. Per tant $X_1 = X_2$ si i només si $X_1 \subseteq X_2$ i $X_2 \subseteq X_1$.

2) El conjunt de les parts.

   - El conjunt $\mathcal{P}(X)$ de les parts d'un conjunt X és el conjunt que té com elements tots els subconjunts del conjunt X. És a dir $\mathcal{P}(X) = \{Y : Y \subseteq X\}$.

≡ **Definició** *Operacions entre subconjunts. Operacions entre conjunts.*

1) Unió de subconjunts. Intersecció subconjunts.

   - La unió de dos subconjunts A_1, A_2 d'un conjunt X és el subconjunt $A_1 \cup A_2 = \{x \in X$ tals que $x \in A_1$ o $x \in A_2\}$.
   - La intersecció de dos subconjunts A_1, A_2 d'un conjunt X és el subconjunt $A_1 \cap A_2 = \{x \in X$ tals que $x \in A_1$ i $x \in A_2\}$.

2) Diferència de subconjunts. Complementari d'un subconjunt.

- Si A_1, A_2 són dos subconjunts d'un conjunt X aleshores, es defineix la diferència com el subconjunt $A_1 \setminus A_2 = \{x \in X \text{ tals que } x \in A_1 \text{ i } x \notin A_2\}$. També el denotarem $A_1 - A_2$.
- El complementari d'un subconjunt A d'un conjunt X és el subconjunt $\overline{A} = X - A = \{x \in X \text{ tals que } x \notin A\}$. També el denotarem A^c.

3) Producte cartesià de dos conjunts.

- Siguin X_1 i X_2 dos conjunts. Aleshores, es defineix el producte cartesià $X_1 \times X_2$ dels conjunts X_1 i X_2 com el conjunt $X_1 \times X_2 = \{(x_1, x_2) \text{ amb } x_1 \in X_1 \text{ i } x_2 \in X_2\}$.

≡ Taules de pertinença

Taules de pertinença de les operacions amb subconjunts.

- Siguin A i B subconjuts d'un conjunt X.

A	$\overline{A}$
1	0
0	1

A	B	$A \cap B$	$A \cup B$	$\overline{A} \cup B$	$(\overline{A} \cup B) \cap (A \cup \overline{B})$	$A \setminus B$
1	1	1	1	1	1	0
1	0	0	1	0	0	1
0	1	0	1	1	0	0
0	0	0	0	1	1	0

≡ Propietats

Operacions entre conjunts i subconjunts.

1) Unió i intersecció.

- Si A, B, C són subconjunts d'un conjunt U, aleshores:

$A \cap A = A$	$A \cup A = A$
$A \cap \emptyset = \emptyset$, $A \cap U = A$	$A \cup \emptyset = A$, $A \cup U = U$
$A \cap B = B \cap A$	$A \cup B = B \cup A$
$A \cap (B \cap C) = (A \cap B) \cap C$	$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap B \subseteq A$, $A \cap B \subseteq B$	$A \subseteq A \cup B$, $B \subseteq A \cup B$
$A \subseteq B \Leftrightarrow A = A \cap B$	$A \subseteq B \Leftrightarrow A \cup B = B$

2) Diferència.

- Si A, B són subconjunts d'un conjunt U, aleshores:

$A \setminus B \subseteq A$	$A \setminus B = A \setminus (A \cap B)$	
$A \setminus \emptyset = A$	$A \setminus U = \emptyset$	$A \setminus A = \emptyset$

3) Complementari.

- Si A, B són subconjunts d'un conjunt U, aleshores:

$$\overline{\overline{A}} = A \qquad A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}$$
$$A \cap \overline{A} = \emptyset \qquad A \cup \overline{A} = U$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B} \qquad \overline{A \cup B} = \overline{A} \cap \overline{B}$$

Aplicacions entre conjunts

≡ **Definició** *Correspondència i aplicació.*

1) Correspondència.

- Siguin X, Y dos conjunts. Una correspondència f del conjunt X en el conjunt Y és una terna ordenada $f = (X, Y, F)$ on $F \subseteq X \times Y$.

2) Aplicació.

- Siguin X, Y dos conjunts. Una aplicació f del conjunt X en el conjunt Y és una correspondència $f = (X, Y, F)$ on el conjunt $F \subseteq X \times Y$ verifica que per a tot $x \in X$ existeix un únic $y \in Y$ de manera que $(x, y) \in F$.
- Notarem l'aplicació $f = (X, Y, F)$ per $f : X \to Y$ i per a cada element $x \in X$ notarem per $f(x)$ l'unic element del conjunt Y verificant $(x, f(x)) \in F$.

≡ **Definició** *Imatges i antiimatges per una aplicació.*

1) Imatges i antiimatges d'elements.

- Sigui $f : X \to Y$ una aplicació i sigui $x \in X$ un element. Direm que un element $y \in Y$ és la imatge de x per f si i només si $f(x) = y$. La imatge de x per f existeix i és única.
- Sigui $f : X \to Y$ una aplicació i sigui $y \in Y$ un element. Direm que un element $x \in X$ és una antiimatge de y per f si i només si $f(x) = y$. Un element $y \in Y$ no necessàriament té antiimatge per f i a més, si existeix, no té per què ser única.

2) Imatges i antiimatges de subconjunts.

- Sigui $f : X \to Y$ una aplicació i sigui $A \subseteq X$ un subconjunt. Definim el conjunt imatge de A per f com el conjunt $f(A) = \{y \in Y$ tals que existeix $a \in A$ amb $f(a) = y\}$. Per tant, $f(A) = \{f(a) : a \in A\} \subseteq Y$.
- Sigui $f : X \to Y$ una aplicació i sigui $B \subseteq Y$ un subconjunt. Definim el conjunt antiimatge de B per f com $f^{-1}(B) = \{x \in X$ tals que existeix $b \in B$ amb $f(x) = b\}$. Per tant, $f^{-1}(B) = \{x \in X : f(x) \in B\} \subseteq X$.

≡ **Definició** *Aplicació injectiva, exhaustiva i bijectiva.*

1) Una aplicació $f : X \to Y$ es diu que és injectiva si elements diferents tenen imatges diferents. És a dir, $f : X \to Y$ és injectiva si i només si $f(x_1) \neq f(x_2)$ per a tota parella d'elements diferents $x_1, x_2 \in X$.

2) Una aplicació $f : X \to Y$ es diu que és exhaustiva si tot element del conjunt Y té, com a mínim, una antiimatge per f. És a dir, $f : X \to Y$ és exhaustiva si i només si per a tot $y \in Y$ existeix com a mínim un element $x \in X$ amb $f(x) = y$.

3) Una aplicació $f : X \to Y$ es diu que és bijectiva si és injectiva i exhaustiva. Per tant, $f : X \to Y$ és bijectiva si i només si tot element del conjunt Y té una única antiimatge per f. És a dir, $f : X \to Y$ és bijectiva si i només si per a tot $y \in Y$ existeix un únic element $x \in X$ amb $f(x) = y$.

≡ **Definició** *Composició d'aplicacions.*

- Siguin $f : X \to Y$ i $g : Y' \to Z$ dues aplicacions. Suposem que $f(Y) \subseteq Y'$. En aquesta situació es defineix la composició $g \circ f$ com l'aplicació $g \circ f : X \to Z$ on $(g \circ f)(x) = (g(f(x))$ per a tot $x \in X$.
- Observem que si $Y = Y'$, aleshores sempre té sentit considerar la composició $g \circ f : X \to Z$, que es representa $g \circ f : X \xrightarrow{f} Y \xrightarrow{g} Z$.

≡ **Definició** *Aplicació identitat. Inversa d'una aplicació.*

1) Sigui X un conjunt no buit. La aplicació identitat del conjunt X és l'aplicació $\mathrm{Id}_X : X \to X$ definida per $\mathrm{Id}_X(x) = x$ per a tot $x \in X$.

2) Sigui $f : X \to Y$ una aplicació. Es diu que una aplicació $g : Y \to X$ és la inversa de f si es verifica que $g \circ f = \mathrm{Id}_X$ i que $f \circ g = \mathrm{Id}_Y$. Si existeix l'aplicació inversa de f aleshores aquesta és única i la notarem per f^{-1}.

≡ **Propietats** *Inversa*

1) Si X, Y són dos conjunts, aleshores $X \neq Y \Leftrightarrow \mathrm{Id}_X \neq \mathrm{Id}_Y$.

2) Una aplicació f té inversa si i només si f és bijectiva.

≡ **Propietats** *Composició i tipus d'aplicacions*

Siguin $f : A \longrightarrow B$ i $g : B \longrightarrow C$ dues aplicacions.

1) Si f i g són injectives, aleshores $g \circ f$ és injectiva.

2) Si f i g són exhaustives, aleshores $g \circ f$ és exhaustiva.

3) Si f i g són bijectives, aleshores $g \circ f$ és bijectiva.

4) Si $g \circ f$ és injectiva, aleshores f és injectiva.

5) Si $g \circ f$ és injectiva i f és exhaustiva, aleshores g és injectiva.

6) Si $g \circ f$ és exhaustiva, aleshores g és exhaustiva.

7) Si $g \circ f$ és exhaustiva i g és injectiva, aleshores f és exhaustiva.

8) Si $g \circ f$ és bijectiva, aleshores f és injectiva i g és exhaustiva.

≡ Propietats

Comportament f, f^{-1} respecte contenció, unió, intersecció, diferència

Sigui $f : A \longrightarrow B$ una aplicació.

- Inclusió.

  1) Si $A' \subseteq A'' \subseteq A$, aleshores $f(A') \subseteq f(A'')$.
  2) Si $B' \subseteq B'' \subseteq B$, aleshores $f^{-1}(B') \subseteq f^{-1}(B'')$,

- Unió. Suposem $A_i \subseteq A$, per a tot $i \in I$ i $B_j \subseteq B$, per a tot $j \in J$..

  1) $f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$.
  2) $f^{-1}(\bigcup_{j\in J} B_j) = \bigcup_{j\in J} f^{-1}(B_j)$.

- Intersecció. Suposem $A_i \subseteq A$, per a tot $i \in I$ i $B_j \subseteq B$, per a tot $j \in J$.

  1) $f(\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I} f(A_i)$; si f és injectiva, aleshores $f(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f(A_i)$.
  2) $f^{-1}(\bigcap_{j\in J} B_j) = \bigcap_{j\in J} f^{-1}(B_j)$.

- Diferència. Suposem $A', A'' \subseteq A$ i $B', B'' \subseteq B$.

  1) $f(A') \setminus f(A'') \subseteq f(A' \setminus A'')$; si f és injectiva, aleshores $f(A') \setminus f(A'') = f(A' \setminus A'')$.
  2) $f^{-1}(B') \setminus f^{-1}(B'') = f^{-1}(B' \setminus B'')$.

- Antiimatges d'un conjunt d'imatges. Suposem $A' \subseteq A$.

  1) $A' \subseteq f^{-1}(f(A'))$.
  2) Si f és injectiva, aleshores $f^{-1}(f(A')) = A'$.
  3) f és injectiva si i només si $f^{-1}(f(A')) = A'$, $\forall A' \subseteq A$.

- Imatges d'un conjunt d'antiimatges. Suposem $B' \subseteq B$.

  1) $f(f^{-1}(B')) \subseteq B'$.
  2) Si f és exhaustiva, aleshores $f(f^{-1}(B')) = B'$.
  3) f és exhaustiva si i només si $f(f^{-1}(B')) = B'$, $\forall B' \subseteq B$.

2.2 Exercicis i problemes. Enunciats

2.1 Considerem els subconjunts de nombres enters $A = \{n \in \mathbb{Z} : n \text{ és múltiple de } 12\}$ i $B = \{n \in \mathbb{Z} : n \text{ és múltiple de 2 i de 6}\}$. Determineu si són certes les afirmacions $A \subseteq B$, $B \subseteq A$, $A = B$.

2.2 Considerem el conjunt $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. Decidiu si les expressions següents són certes o falses:

1) $\emptyset \in A$.
2) $\emptyset \subseteq A$.
3) $\{\emptyset\} \in A$.
4) $\{\emptyset\} \subseteq A$.
5) $\{\{\emptyset\}\} \in A$.
6) $\{\{\emptyset\}\} \subseteq A$.
7) $\{\emptyset, \{\emptyset\}\} \in A$.
8) $\{\emptyset, \{\emptyset\}\} \subseteq A$.

2.3 Considerem el conjunts $A = \{\emptyset, 1, 2, \{1\}, \{1, 2\}, \{\{1\}, 2\}, \{1, \{2\}\}\}$. Determineu els elements del conjunt $B = \{x : x \in A \text{ i } x \subseteq A\}$.

2.4 Determineu tots els elements dels conjunts $A \cup B$ i $A \cap B$ per a cadascuna de les parelles de conjunts A i B següents:

1) $A = \{x \in \mathbb{Z} : -1 \leq x \leq 2\}$, $B = \{x \in \mathbb{Z} : -1 \leq x \leq 4\}$.
2) $A = \{x \in \mathbb{Z} : -1 \leq x \leq 5\}$, $B = \{x \in \mathbb{Z} : 0 < x < 10\}$.
3) $A = \{1, 2, 3, 4\}$, $B = \{-4, -3, -2, -1\}$.
4) $A = \{x \in \mathbb{R} : -2 \leq x \leq 1\}$, $B = \{x \in \mathbb{R} : -1 \leq x \leq 2\}$.
5) $A = \{x \in \mathbb{R} : x^2 - 3x + 2 = 0\}$, $B = \{x \in \mathbb{R} : 2x^2 + x - 3 = 0\}$.
6) $A = \{x \in \mathbb{R} : |x| < 2\}$, $B = \{x \in \mathbb{R} : -1 \leq x \leq 4\}$.
7) $A = \{x \in \mathbb{Z} : n \text{ és parell }\}$, $B = \{x \in \mathbb{Z} : n^2 \text{ és senar }\}$.

2.5 Considerem els conjunts $A = \{\emptyset\}$, $B = \{1\}$, $C = \{\{1\}\}$, $D = \{1, 2\}$, $E = \{\{1\}, 2\}$. Determineu els elements de la unió i la intersecció dels conjunts dos a dos.

2.6 Discutiu si els enunciats següents són certs o falsos, on A, B, C són conjunts qualssevol:

1) $A \cup B = \emptyset \Rightarrow A = B = \emptyset$.
2) $A \cap B = \emptyset \Rightarrow A = B = \emptyset$.
3) $A \cup B = A \cup C \Rightarrow B = C$.
4) $A \cap B = A \cap C \Rightarrow B = C$.

2.7 Considerem A, B, C conjunts qualssevol. Demostreu que $A \cup (B \cap C) = (A \cup B) \cap C$ si i només si $A \subseteq C$.

2.8 Donat $A = \{1, 2, 3, 4\}$, decidiu si les afirmacions següents són certes o falses:

1) $\{3\} \in A$.
2) $\{1,2,3,4\} \subseteq A$.
3) $4 \in \mathcal{P}(A)$.
4) $\{\{4\}\} \in \mathcal{P}(A)$.
5) $\{3,4\} \in \mathcal{P}(A)$.
6) $\{\{1\}\} \in \mathcal{P}(\mathcal{P}(A))$.

2.9 Decidiu si per a qualsevol conjunt A les afirmacions següents són certes o falses:

1) $\emptyset \in A$.
2) $\emptyset \in \mathcal{P}(A)$.
3) $\emptyset \subseteq A$.
4) $\emptyset \subseteq \mathcal{P}(A)$.
5) $\{\emptyset\} \subseteq A$.
6) $\{\emptyset\} \subseteq \mathcal{P}(A)$.

2.10 Decidiu si les afirmacions següents són certes o falses:

1) $\{\emptyset\} \subseteq \mathcal{P}(\emptyset)$.
2) $\mathcal{P}(\emptyset) = \{\emptyset, \{\emptyset\}\}$.
3) $\{\{\emptyset\}\} \subseteq \mathcal{P}(\emptyset)$.
4) $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

2.11

1) Calculeu $\mathcal{P}(\emptyset)$, $\mathcal{P}(\{\, a \,\})$, $\mathcal{P}(\{\, a, b \,\})$, $\mathcal{P}(\{\, a, b, c \,\})$ i $\mathcal{P}(\{\, a, b, c, d \,\})$.
2) Demostreu que $\mathcal{P}(A)$ té 2^n elements si A en té n, on $n \geq 0$.

2.12 Doneu, si és possible, un conjunt A de manera que $\mathcal{P}(A)$ sigui:

1) $\emptyset$.
2) $\{\emptyset\}$.
3) $\{\emptyset, \{a\}\}$.
4) $\{\emptyset, \{a\}, \{\emptyset, \{a\}\}\}$.
5) $\{\emptyset, \{a\}, \{\emptyset, \{a\}\}, \{\emptyset, a\}\}$.
6) $\{\emptyset, \{a\}, \{\emptyset\}, \{a, \emptyset\}\}$.

2.13 Demostreu que si A és un conjunt tal que $\mathcal{P}(A \cup \mathcal{P}(A))$ té 8 elements, aleshores A té un sol element. Demostreu que el recíproc és cert si i només si $A \neq \{\emptyset\}$.

2.14 Considerem dos conjunts A, B qualssevol. Demostreu:

1) $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.
2) $A = B \Leftrightarrow \mathcal{P}(A) = \mathcal{P}(B)$.

2.15 Considerem dos conjunts A, B qualssevol.

1) Demostreu $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
2) Demostreu $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$. És cert $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$?
3) Demostreu $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ si i només si $A \subseteq B$ o bé $B \subseteq A$.

2.16 Determineu els elements del complementari del conjunt A en E en els casos següents:

1) $A = \{x \in \mathbb{Z} : x \text{ és parell }\}$, si $E = \mathbb{Z}$.
2) $A = \{x \in \mathbb{Z} : x \geq 5 \text{ o } x < -1\}$, si $E = \mathbb{Z}$.
3) $A = \{x \in \mathbb{R} : |x| > 2\}$, si $E = \mathbb{R}$.
4) $A = \{x \in \mathbb{Z} : x^2 \geq x\}$, si $E = \mathbb{Z}$.

5) $A = \{x \in \mathbb{Z} : x^2 \geq x\}$, si $E = \mathbb{R}$.

6) $A = \{x \in \mathbb{R} : x^2 \geq x\}$, si $E = \mathbb{R}$.

2.17 Determineu els elements del conjunt $A \setminus B$ si $A = \{n \in \mathbb{Z} : -9 \leq n \leq 9\}$ i si B és:

1) $B = \{n \in \mathbb{Z} : n$ és quadrat perfecte$\}$.
2) $B = \{n \in \mathbb{Z} : n$ és múltiple de 2 o de 3$\}$.
3) $B = \{n \in \mathbb{Z} : n$ és múltiple de 2 i de 3$\}$.
4) $B = \{n \in \mathbb{Z} : n < n^2\}$.

2.18 Determineu els elements del conjunt $A \setminus B$ si:

1) $A = \{\emptyset, a\}$, $B = \emptyset$.
2) $A = \{\emptyset, a\}$, $B = \{\emptyset\}$.
3) $A = \emptyset$, $B = \{\emptyset, a\}$.
4) $A = \{\{a\}, b\}$, $B = \{a, b\}$.
5) $A = \{\{a\}, b\}$, $B = \{\{a\}\}$.
6) $A = \{\{a, b\}\}$, $B = \{a, b\}$.

2.19 Demostreu les propietats següents, si són certes, o trobeu-ne un contraexemple:

1) $A \setminus B = A \Leftrightarrow A \cap B = \emptyset \Leftrightarrow B \setminus A = B$.
2) $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow A \setminus B = \emptyset$.
3) $A \subseteq B \subseteq C \Leftrightarrow A \cup B = B \cap C$.
4) $B \subseteq C \Leftrightarrow (A \cup B) \subseteq (A \cup C)$.
5) $B \subseteq C \Leftrightarrow (A \cup B) \subseteq (A \cup C)$ i $(A \cap B) \subseteq (A \cap C)$.

2.20 Expresseu de la manera més simple possible els conjunts següents, on $A, B, C \subseteq E$ i $\overline{A}, \overline{B}$ representa respectivament el complementari de A, B en E:

1) $A \cap (\overline{A} \cup B)$.
2) $(A \cap \overline{B}) \cap (\overline{A} \cap \overline{B})$.
3) $(A \cap B \cap C) \cup ((\overline{A} \cup \overline{B}) \cup \overline{C})$.
4) $(A \cap (\overline{A} \cup B)) \cup (B \cap (B \cup C)) \cup B$.
5) $[(A \cup B) \cap (\overline{\overline{A} \cap B})] \cup [(A \cap B) \cup (\overline{\overline{A} \cup B})]$.

2.21 Siguin A_1, A_2, B_1, B_2 conjunts no buits. Demostreu:

1) $A_1 \times A_2 \subseteq B_1 \times B_2 \Leftrightarrow A_1 \subseteq B_1$ i $A_2 \subseteq B_2$.
2) $(A_1 \cap A_2) \times (B_1 \cap B_2) = (A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \times B_2) \cap (A_2 \times B_1)$.
3) $(A_1 \cup A_2) \times (B_1 \cup B_2) = (A_1 \times B_1) \cup (A_1 \times B_2) \cup (A_2 \times B_1) \cup (A_2 \times B_2)$.
4) $A_1 \times (B_1 \setminus B_2) = (A_1 \times B_1) \setminus (A_1 \times B_2)$.

2.22 Demostreu si és cert o doneu-ne un contraexemple, si és fals: "Si A, B són conjunts no buits i $S \subseteq A \times B$, aleshores existeixen subconjunts C i D de A i B respectivament tals que $S = C \times D$".

2.23 Considerem l'aplicació $f : X \longrightarrow X$ on $f(x) = 2x^2 - 5x$.

1) Suposem que $X = \mathbb{R}$.
   a) Calculeu $f(\{-1, 0, 1, \sqrt{2}\})$ i $f([0, 1))$.
   b) Calculeu $f^{-1}(\{-5, 0, 1\})$ i $f^{-1}([0, 1))$.
   c) Determineu si f és injectiva, exhaustiva i bijectiva.
2) Suposem que $X = \mathbb{Z}$.
   a) Calculeu $f(\{-1, 0, 1, 2\})$.
   b) Calculeu $f^{-1}(\{-1, 0, 3\})$.
   c) Determineu si f és injectiva, exhaustiva i bijectiva.

2.24 Determineu les aplicacions $g \circ f$ i $f \circ g$ si $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ on:

1) $f(x) = x^2 + 1$ i $g(x) = x - 3$ per a tot $x \in \mathbb{R}$.
2) $f(x) = x^2$ i $g(x) = 2^x$ per a tot $x \in \mathbb{R}$.

2.25 Sigui $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida per $f(x - 1) = x^2$. Calculeu $f(x + 1)$.

2.26 Determineu si les aplicacions següents són injectives, exhaustives o bijectives. Calculeu l'aplicació inversa quan siguin bijectives.

1) $f : \mathbb{R} \longrightarrow \mathbb{R}$ on $f(x) = 3x$ per a tot $x \in \mathbb{R}$.
2) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ on $f(x) = 3x$ per a tot $x \in \mathbb{Z}$.
3) $f : \mathbb{R} \longrightarrow \mathbb{R}$ on $f(x) = |x|$ per a tot $x \in \mathbb{R}$.
4) $f : \mathbb{R} \longrightarrow \mathbb{R}$ on $f(x) = x^3 - x$ per a tot $x \in \mathbb{R}$.
5) $f : \mathbb{R} \longrightarrow \mathbb{R}$, on $f(x) = 5x + 3$ per a tot $x \in \mathbb{R}$.
6) $f : \mathbb{R} \longrightarrow \mathbb{R}$, on $f(x) = \begin{cases} 2x - 4, & \text{si } x \leq 3; \\ \frac{1}{2}x^2 - \frac{1}{2}x - 1, & \text{si } x > 3. \end{cases}$
7) $f : \mathbb{R} \setminus \{0\} \longrightarrow \mathbb{R} \setminus \{0\}$, on $f(x) = \dfrac{1}{2x}$ per a tot $x \in \mathbb{R} \setminus \{0\}$.

2.27 Considerem un conjunt qualsevol A. Definim l'aplicació $\phi : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ on $\phi(X)$ és el complementari de X en A. Demostreu que ϕ és bijectiva i determineu ϕ^{-1}.

2.28 Considerem dues aplicacions $f : A \longrightarrow B$ i $g : B \longrightarrow C$.

1) Demostreu:
   a) Si f i g són injectives, aleshores $g \circ f$ és injectiva.
   b) Si f i g són exhaustives, aleshores $g \circ f$ és exhaustiva.
   c) Si f i g són bijectives, aleshores $g \circ f$ és bijectiva.
2) Demostreu que si $g \circ f$ és injectiva, aleshores:
   a) f és injectiva.

b) g no és necessàriament injectiva.

c) Si f és exhaustiva, aleshores g és injectiva.

3) Demostreu que si $g \circ f$ és exhaustiva, aleshores:

a) g és exhaustiva.

b) f no és necessàriament exhaustiva.

c) Si g és injectiva, aleshores f és exhaustiva.

4) Demostreu que si $g \circ f$ és bijectiva, aleshores:

a) f és injectiva i g és exhaustiva.

b) f no és necessàriament exhaustiva, i g no és necessàriament injectiva.

2.29 Considerem una aplicació $f : A \longrightarrow B$.

1) Demostreu que f és exhaustiva si i només si existeix una aplicació $g : B \longrightarrow A$ tal que $f \circ g = \mathrm{Id}_B$. Una aplicació g que satisfà aquesta condició s'anomena *secció* de f.

2) Demostreu que f és injectiva si i només si existeix una aplicació $h : B \longrightarrow A$ tal que $h \circ f = \mathrm{Id}_A$. Una aplicació h que satisfà aquesta condició s'anomena *retracció* de f.

3) Definim l'aplicació $f : A \longrightarrow B$, on $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 4\}$, $f(1) = 2$, $f(2) = 3$, $f(3) = 3$ i $f(4) = 4$. Doneu una secció g de f. Té f alguna retracció?

2.30 Considerem una aplicació $f : A \longrightarrow B$ i subconjunts $A', A'' \subseteq A$ i $B', B'' \subseteq B$. Demostreu:

1) Si $A' \subseteq A''$, aleshores $f(A') \subseteq f(A'')$. Demostreu que la igualtat és certa si f és injectiva.

2) Si $B' \subseteq B''$, aleshores $f^{-1}(B') \subseteq f^{-1}(B'')$. Demostreu que la igualtat és certa si f és exhaustiva.

2.31 Considerem una aplicació $f : A \longrightarrow B$. Demostreu:

1) Si $A' \subseteq A$, aleshores $A' \subseteq f^{-1}(f(A'))$.

2) f és injectiva si i només si $A' = f^{-1}(f(A'))$ per a tot subconjunt $A' \subseteq A$.

3) Si $B' \subseteq B$, aleshores $f(f^{-1}(B')) \subseteq B'$.

4) f és exhaustiva si i només si $B' = f(f^{-1}(B'))$ per a tot subconjunt $B' \subseteq B$.

2.32 Considerem una aplicació $f : A \longrightarrow B$. Demostreu:

1) Si $A_i \subseteq A$ per a tot $i \in I$, aleshores $f(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} f(A_i)$.

2) Si $A_i \subseteq A$ per a tot $i \in I$, aleshores $f(\bigcap_{i \in I} A_i) \subseteq \bigcap_{i \in I} f(A_i)$.

3) f és injectiva si i només si $f(\bigcap_{i \in I} A_i) = \bigcap_{i \in I} f(A_i)$ per a subconjunts $A_i \subseteq A$ qualssevol.

4) Si $B_j \subseteq B$ per a tot $j \in J$, aleshores $f^{-1}(\bigcup_{j \in J} B_j) = \bigcup_{j \in J} f^{-1}(B_j)$.

5) Si $B_j \subseteq B$ per a tot $j \in J$, aleshores $f^{-1}(\bigcap_{j\in J} B_j) = \bigcap_{j\in J} f^{-1}(B_j)$.

2.33 Considerem una aplicació $f : A \longrightarrow B$. Demostreu:

1) Si $A', A'' \subseteq A$, aleshores $f(A') \setminus f(A'') \subseteq f(A' \setminus A'')$.

2) f és injectiva si i només si $f(A') \setminus f(A'') = f(A' \setminus A'')$ per a subconjunts $A', A'' \subseteq A$ qualssevol.

3) Si $B', B'' \subseteq B$, aleshores $f^{-1}(B') \setminus f^{-1}(B'') = f^{-1}(B' \setminus B'')$.

2.3 Exercicis i problemes. Solucions

2.1 Només és certa $A \subseteq B$.

2.2

1) Cert. 2) Cert. 3) Cert. 4) Cert. 5) Fals. 6) Cert. 7) Cert. 8) Cert.

2.3 $B = \{\emptyset, \{1\}, \{1,2\}, \{\{1\},2\}\}$.

2.4

1) $A \cup B = \{x \in \mathbb{Z} : -1 \leq x \leq 4\}$, $A \cap B = \{x \in \mathbb{Z} : -1 \leq x \leq 2\}$.
2) $A \cup B = \{x \in \mathbb{Z} : -1 \leq x < 10\}$, $A \cap B = \{x \in \mathbb{Z} : 0 < x \leq 5\}$.
3) $A \cup B = \{-4, -3, -2, -1, 1, 2, 3, 4\}$, $A \cap B = \emptyset$.
4) $A \cup B = \{x \in \mathbb{R} : -2 \leq x \leq 2\}$, $A \cap B = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$.
5) $A \cup B = \{1, 2, -\frac{3}{2}\}$, $A \cap B = \{1\}$.
6) $A \cup B = \{x \in \mathbb{R} : -2 < x \leq 4\}$, $A \cap B = \{x \in \mathbb{R} : -1 \leq x < 2\}$.
7) $A \cup B = \mathbb{Z}$, $A \cap B = \emptyset$.

2.5

$A \cup B = \{\emptyset, 1\}$; $A \cup C = \{\emptyset, \{1\}\}$; $A \cup D = \{\emptyset, 1, 2\}$; $A \cup E = \{\emptyset, \{1\}, 2\}$; $B \cup C = \{1, \{1\}\}$; $B \cup D = \{1, 2\} = D$; $B \cup E = C \cup D = D \cup E = \{1, \{1\}, 2\}$; $C \cup E = \{\{1\}, 2\} = E$.

$B \cap D = \{1\}$; $C \cap E = \{\{1\}\}$; $D \cap E = \{2\}$; la resta d'interseccions són $\emptyset$.

2.6

1) Cert.
2) Fals. P. ex. $A = \{1\}$, $B = \{2\}$.
3) Fals. P. ex. $A = \{1, 2, 3\}$, $B = \{2, 3\}$, $C = \{3\}$.
4) Fals. P. ex. $A = \{1\}$, $B = \{1, 2\}$, $C = \{1, 3\}$.

2.8

1) Fals. 2) Cert. 3) Fals. 4) Fals. 5) Cert. 6) Cert.

2.9

1) Fals. 2) Cert. 3) Cert. 4) Cert. 5) Fals. 6) Cert.

2.10

1) Cert. 2) Fals. 3) Fals. 4) Cert.

2.11

1) $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{\, a \,\}) = \{\emptyset, \{a\}\}$, $\mathcal{P}(\{\, a, b \,\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,
$\mathcal{P}(\{\, a, b, c \,\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$,
$\mathcal{P}(\{\, a, b, c, d \,\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\}$.
2) $|\mathcal{P}(A)| = 2^n$.

2.12

1) No existeix.
2) $A = \emptyset$.
3) $A = \{a\}$.
4) No existeix.
5) No existeix.
6) $A = \{\emptyset, a\}$.

2.15

2) És fals. Per exemple, si $A = \{1\}$ i $B = \{2\}$, $\{1, 2\} \in \mathcal{P}(A \cup B)$ però $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

2.16

1) Són els enters senars.
2) Són els enters x tals que $-1 \leq x \leq 4$.
3) L'interval de nombres reals $[-2, 2]$.
4) $\emptyset$.
5) Els nombres reals que no són enters.
6) L'interval de nombres reals $(0, 1)$.

2.17

1) $\{-9, -8, -7, -6, -5, -4, -3, -2, -1, 2, 3, 5, 6, 7, 8\}$.
2) $\{-7, -5, -1, 1, 5, 7\}$.
3) $\{-9, -8, -7, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 7, 8, 9\}$.
4) $\{0, 1\}$.

2.18

1) $\{\emptyset, a\}$. 2) $\{a\}$. 3) $\emptyset$. 4) $\{\{a\}\}$. 5) $\{b\}$. 6) $\{\{a, b\}\}$.

2.19

1) Cert. 2) Cert. 3) Cert. 4) Fals. 5) Cert.

2.20

1) $A \cap B$. 2) $\emptyset$. 3) E. 4) B. 5) A.

2.22 És fals. P. ex. $A = \{1, 2\}$, $B = \{a, b\}$, $S = \{(1, a), (2, b)\}$.

2.23

1) a) $f(\{-1, 0, 1, \sqrt{2}\}) = \{-3, 0, 4 - 5\sqrt{2}, 7\}$ i $f([0, 1)) = (-3, 0]$.
   b) $f^{-1}(\{-5, 0, 1\}) = \{\frac{5-\sqrt{33}}{4}, 0, \frac{5}{2}, \frac{5+\sqrt{33}}{4}, \}$ i $f^{-1}([0, 1)) = (\frac{5-\sqrt{33}}{4}, 0] \cup [\frac{5}{2}, \frac{5+\sqrt{33}}{4})$.
   c) f no és ni injectiva, ni exhaustiva, ni bijectiva.
2) a) $f(\{-1, 0, 1, 2\}) = \{-3, -2, 0, 7\}$.
   b) $f^{-1}(\{-1, 0, 3\}) = \{0, 3\}$.
   c) f és injectiva, però no és ni exhaustiva, ni bijectiva.

2.24

1) $(g \circ f)(x) = x^2 - 2$; $(f \circ g)(x) = x^2 - 6x + 10$.
2) $(g \circ f)(x) = 2^{x^2}$; $(f \circ g)(x) = 2^{2x}$.

2.25 $f(x + 1) = (x + 2)^2$.

2.26

1) Bijectiva. $f^{-1}(x) = \frac{x}{3}$.
2) Injectiva, no exhaustiva.
3) Ni injectiva, ni exhaustiva.
4) Exhaustiva, no injectiva.
5) Bijectiva. $f^{-1}(x) = (x - 3)/5$ per a tot $x \in \mathbb{R}$.
6) Bijectiva. $f^{-1}(x) = (x + 4)/2$, si $x \leq 2$, i $f^{-1}(x) = (1 + \sqrt{8x + 9})/2$, si $x > 2$.
7) Bijectiva. $f^{-1} = f$.

2.27 $\phi^{-1} = \phi$.

3
Relacions, operacions i estructures

3.1 Resum teòric

Relacions binàries en un conjunt

≡ **Definició** *Relació binària en un conjunt.*

- Sigui A un conjunt. Una relació binària en A és un subconjunt R del producte cartessià $A \times A$. Si $(a, b) \in R$ aleshores direm que l'element a està relacionat amb l'element b i, en aquest cas, notarem aRb.

≡ **Definició** *Propietats de les relacions binàries.*

- Sigui R una relació binària en un conjut A. Direm que la relació R és:

  1) Reflexiva: si per a tot $a \in A$ es té que aRa.
  2) Simètrica: si per a tot $a, b \in A$ amb aRb es té que bRa.
  3) Antisimètrica: si $a, b \in A$ són tals que aRb i bRa aleshores $a = b$.
  4) Transitiva: si per a tot $a, b, c \in A$ amb aRb i amb bRc es té que aRc.
  5) Connexa: si $a, b \in A$ aleshores aRb o bRa.

Relacions d'equivalència

≡ **Definició** *Relació d'equivalència.*

- Sigui A un conjunt. Direm que una relació binària $\sim$ en A és una relació d'equivalència si és reflexiva, simètrica i transitiva.

≡ **Definició** *Classe d'equivalència. Conjunt quocient.*

- Sigui A un conjunt i sigui $\sim$ una relació d'equivalència en A. Aleshores:

  1) La classe d'equivalència d'un element $a \in A$ per la relació d'equivalència $\sim$ és el conjunt $\{b \in A : b \sim a\}$. Notarem $[a]$ la classe d'equivalència de a.
  2) El conjunt quocient $A/_\sim$ de A per la relació d'equivalència $\sim$ és el conjunt que té per elements les classes d'equivalència del elements de A per la relació $\sim$. És a dir $A/_\sim = \{[a] \text{ on } a \in A\}$.

≡ **Propietats** *Propietats de les classes d'equivalència. Conjunt quocient i partició.*

1) Sigui A un conjunt i sigui $\sim$ una relació d'equivalència en A. Aleshores:
   a) Si $a \in A$ aleshores $\emptyset \subsetneq [a] \subseteq A$ i $a \in [a]$.
   b) Si $a \in A$ i si $b \in [a]$ aleshores $[a] = [b]$.
   c) Si $a \in A$ i si $b \notin [a]$ aleshores $[a] \cap [b] = \emptyset$.
   d) Si $a, b \in A$ aleshores les condicions següents són equivalents:
      i) $a \sim b$
      ii) $[a] = [b]$
      iii) $[a] \cap [b] \neq \emptyset$
      iv) existeix $x \in [a]$ i existeix $y \in [b]$ tals que $x \sim y$
      v) per a tot $x \in [a]$ i per a tot $y \in [b]$ es compleix $x \sim y$.
2) Per definició, una *partició* d'un conjunt A és una col·lecció de subconjunts no buits $X_1, \ldots, X_r$ de A tals que $A = X_1 \cup \cdots \cup X_r$ i $X_i \cap X_j = \emptyset$ si $i \neq j$.
3) Es satisfan les propietats següents:
   a) Si A és un conjunt no buit i $\sim$ és una relació d'equivalència en A, aleshores $A/_\sim \subseteq \mathcal{P}(A)$ i els elements del conjunt quocient $A/_\sim$ determinen una partició de A.
   b) Si $\{A_1, \ldots, A_r\}$ és una partició del conjunt A aleshores existeix una única relació d'equivalència $\sim$ en A tal que el seu conjunt quocient és $A/_\sim = \{A_1, \ldots, A_r\}$.

≡ **Teorema** *Descomposició canònica d'una aplicació.*

- Sigui $f : A \to B$ una aplicació, i sigui $\sim_f$ la relació binària en A definida per "$a_1 \sim_f a_2$ si i només si $f(a_1) = f(a_2)$". Aleshores:

  1) La relació binària $\sim_f$ és una relació d'equivalència.
  2) L'aplicació $\Phi_f : A/_{\sim_f} \to \operatorname{Im} f$ on $\Phi_f([a]) = f(a)$, està ben definida i és bijectiva.
  3) Sigui Φ_f l'aplicació bijectiva definida a l'apartat anterior, sigui $i_{\operatorname{Im} f} : \operatorname{Im} f \to B$ l'aplicació injectiva definida per $i_{\operatorname{Im} f}(b) = b$, i sigui $\pi_{\sim_f} : A \to A/_{\sim_f}$ l'aplicació exhaustiva definida per $\pi_{\sim_f}(a) = [a]$. Aleshores $f = i_{\operatorname{Im} f} \circ \Phi_f \circ \pi_{\sim_f}$.

Relacions d'ordre

≡ **Definició** *Preordre, ordre parcial i ordre total.*

- Sigui A un conjunt i sigui $\leq$ una relació binària en A. Aleshores:

  1) Direm que $\leq$ és un preordre si $\leq$ és reflexiva i transitiva. En aquest cas es diu que $(A, \leq)$ és un conjunt preordenat.
  2) Direm que $\leq$ és un ordre parcial si $\leq$ és reflexiva, antisimètrica i transitiva. En aquest cas es diu que $(A, \leq)$ és un conjunt parcialment ordenat.
  3) Direm que $\leq$ és un ordre total si $\leq$ és reflexiva, antisimètrica, transitiva i connexa. En aquest cas es diu que $(A, \leq)$ és un conjunt totalment ordenat.

≡ **Definició** *Elements notables dels conjunts parcialment ordenats.*

- Sigui A un conjunt i sigui $\leq$ un ordre parcial en A. Sigui $X \subseteq A$ un subconjunt arbitrari. Aleshores:

  1) Fites superiors. Fites inferiors.
     a) Direm que un element $a \in A$ és una fita superior de X en $(A, \leq)$ si $x \leq a$ per a tot $x \in X$. Direm que X és un conjunt fitat superiorment en $(A, \leq)$ si existeix com a mínim una fita superior de X en $(A, \leq)$.
     b) Direm que un element $a \in A$ és una fita inferior de X en $(A, \leq)$ si $a \leq x$ per a tot $x \in X$. Direm que X és un conjunt fitat inferiorment en $(A, \leq)$ si existeix com a mínim una fita inferior de X en $(A, \leq)$.
  2) Suprem o extrem superior. Ínfim o extrem inferior.
     a) Direm que un element $a \in A$ és el suprem de X en $(A, \leq)$ si a és una fita superior de X en $(A, \leq)$ i es tal que $a \leq a'$ per a qualsevol fita superior a' de X en $(A, \leq)$. El suprem de X en $(A, \leq)$ si existeix és únic, i s'escriu $\sup X$.

b) Direm que un element $a \in A$ és l'ínfim de X en $(A, \leq)$ si a és una fita inferior de X en $(A, \leq)$ i es tal que $a' \leq a$ per a qualsevol fita inferior a' de X en $(A, \leq)$. L'ínfim de X en $(A, \leq)$ si existeix és únic, i s'escriu $\inf X$.

3) Màxim. Mínim.

a) Direm que un element $a \in A$ és el màxim de X en $(A, \leq)$ si $a = \sup X$ i $a \in X$. El màxim de X en $(A, \leq)$ si existeix és únic, i s'escriu $\max X$.

b) Direm que un element $a \in A$ és el mínim de X en $(A, \leq)$ si $a = \inf X$ i $a \in X$. El mínim de X en $(A, \leq)$ si existeix és únic, i s'escriu $\min X$.

4) Maximal. Minimal.

a) Direm que un element $a \in X$ és un maximal de X en $(A, \leq)$ si no hi ha cap element de X més gran que ell, és a dir, si l'element $a \in X$ satisfà que si $x \in X$ és tal que $a \leq x$ aleshores $a = x$.

b) Direm que un element $a \in X$ és un minimal de X en $(A, \leq)$ si no hi ha cap element de X més petit que ell, és a dir, si l'element $a \in X$ satisfà que si $x \in X$ és tal que $x \leq a$ aleshores $x = a$.

≡ **Definició** *Bon ordre.*

- Un conjunt parcialment ordenat $(A, \leq)$ es diu que és ben ordenat si tot subconjunt no buit $X \subseteq A$ té element mínim per $\leq$.

Estructures algebraiques: grup, anell i cos

≡ **Definició** *Conjunts amb una operació interna. Grup.*

1) Sigui $(A, \perp)$ un conjunt amb una operació interna, (i.e.: A és un conjunt no buit i, si $x, y \in A$, aleshores $x \perp y \in A$). Aleshores:

a) Direm que $\perp$ és associativa si per a tot $x, y, z \in A$ es té que $x \perp (y \perp z) = (x \perp y) \perp z$.

b) Direm que $\perp$ és commutativa si per a tot $x, y \in A$ es té que $x \perp y = y \perp x$.

c) Direm que $\perp$ té element neutre o unitat si existeix $a_0 \in A$ que satisfà $a_0 \perp x = x \perp a_0 = x$ per a tot $x \in A$. En aquest cas direm que a_0 és l'element neutre o la unitat de $(A, \perp)$.

d) Suposem que $(A, \perp)$ té element neutre a_0. Direm que un element $x \in A$ té invers, simètric o oposat respecte $\perp$ si existeix un element $x' \in A$ tal que $x \perp x' = x' \perp x = a_0$. En aquest cas direm que x' és l'invers, el simètric o l'oposat de x en $(A, \perp)$.

2) Grup. Grup commutatiu.

- Direm que un conjunt amb una operació interna $(A, \perp)$ és un grup si $\perp$ és associativa, té element neutre i tot element té invers. Si a més $\perp$ és commutativa, aleshores direm que $(A, \perp)$ és un grup commutatiu.

≡ **Propietats** *Propietats dels conjunts amb una operació interna.*

- Sigui $(A, \perp)$ un conjunt amb una operació interna. Suposem que l'operació $\perp$ és associativa. Aleshores es té que:

  1) L'element neutre, si existeix, és únic.
  2) L'invers d'un element, si existeix, és únic.
  3) Si $a_0 \in A$ és l'element neutre, aleshores existeix $(a_0)'$ i es compleix $(a_0)' = a_0$.
  4) Si existeix x' l'invers de l'element x, aleshores existeix $(x')'$ i es compleix $(x')' = x$.
  5) Si existeixen x', y' els inversos dels elements x, y, aleshores existeix l'invers de $x \perp y$ i es compleix $(x \perp y)' = y' \perp x'$.
  6) Si existeix x' l'invers de l'element x, aleshores es verifiquen les lleis de simplificació:
     a) Si $y, z \in A$ són tals que $x \perp y = x \perp z$, llavors $y = z$.
     b) Si $y, z \in A$ són tals que $y \perp x = z \perp x$, llavors $y = z$.

≡ **Definició** *Conjunts amb dues operacions internes. Anell i cos.*

1) Propietat distributiva.

   - Sigui $(A, \perp, *)$ un conjunt amb dues operacions internes. Direm que $*$ és distributiva respecte $\perp$ si per a tot $x, y, z \in A$ es té que $x * (y \perp z) = (x * y) \perp (x * z)$, i $(y \perp z) * x = (y * x) \perp (z * x)$.

2) Anell. Anell commutatiu.

   - Direm que un conjunt amb dues operacions internes $(A, \perp, *)$ és un anell si $(A, \perp)$ és un grup commutatiu i $*$ és associativa, té element neutre i és distributiva respecte $\perp$. Si a més $*$ és commutativa, aleshores direm que $(A, \perp, *)$ és un anell commutatiu.
   - Sovint en un anell les operacions $\perp$ i $*$ es denoten per $+$ i $\cdot$ respectivament. Amb aquesta notació:
     i) L'element neutre de l'operació $+$ el denotarem 0 i l'element neutre de l'operació $\cdot$ el denotarem 1.
     ii) L'element simètric de $a \in A$ per l'operació $+$ el denotarem $-a$. L'element invers per l'operació $\cdot$, si existeix, el denotarem a^{-1}.
   - Elements invertibles i divisors de zero.
     i) Els elements invertibles de A són els elements que tenen invers per $\cdot$.
     ii) Un element $a \neq 0$ és divisor de zero si $a \cdot b = 0$ per a algun element $b \neq 0$.

3) Cos. Cos commutatiu.

   - Direm que un conjunt amb dues operacions internes $(A, \perp, *)$ és un cos si $(A, \perp, *)$ és un anell i tot element de A diferent de l'element neutre de $\perp$ té invers respecte de $*$. Si a més $*$ és commutativa, aleshores direm que $(A, \perp, *)$ és un cos commutatiu.
   - Sovint en un cos les operacions $\perp$ i $*$ es denoten per $+$ i $\cdot$ respectivament.

≡ **Propietats** *Binomi de Newton.*

- Sigui $(\mathbb{A}, +, \cdot)$ un anell commutatiu. Siguin $x, y \in \mathbb{A}$ i sigui $n \geq 1$ un nombre natural. Aleshores $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$.

≡ **Definició** *Cos ordenat.*

- Sigui $\mathbb{K}$ un conjunt amb dues operacions internes, que notarem suma $+$ i producte $\cdot$, i amb una relació binària entre els seus elements, que notarem $\leq$. Direm que $(\mathbb{K}, +, \cdot, \leq)$ és un cos ordenat si
  1) $(\mathbb{K}, +, \cdot)$ és un cos commutatiu.
  2) $(\mathbb{K}, \leq)$ és un conjunt totalment ordenat.
  3) Si $x, y, z \in \mathbb{K}$ amb $x \leq y$, aleshores $x + z \leq y + z$.
  4) Si $x, y, z \in \mathbb{K}$ amb $x \leq y$ i $0 \leq z$, aleshores $xz \leq yz$.

≡ **Propietats** *Elements positius i elements negatius d'un cos ordenat.*

- Sigui $(\mathbb{K}, +, \cdot, \leq)$ un cos ordenat. Aleshores, podem considerar els conjunts $\mathbb{K}^+$ i $\mathbb{K}^-$ formats pels elements positius i negatius del cos. És a dir els conjunts $\mathbb{K}^+ = \{x \in \mathbb{K} \setminus \{0\} : 0 \leq x\}$ i $\mathbb{K}^- = \{x \in \mathbb{K} \setminus \{0\} : x \leq 0\}$. Així tenim $\mathbb{K} = \mathbb{K}^+ \cup \mathbb{K}^- \cup \{0\}$ i $\mathbb{K}^+ \cap \mathbb{K}^- = \emptyset$. Es té que:
  1) Si $x \leq y$ i si $z \in \mathbb{K}^+$ aleshores $x + z \leq y + z$, $xz \leq yz$.
  2) Si $x \leq y$ i si $z \in \mathbb{K}^-$ aleshores $x + z \leq y + z$, $xz \geq yz$.
  3) Si $x, y \in \mathbb{K}^+$ aleshores $x + y \in \mathbb{K}^+$, $xy \in \mathbb{K}^+$.
  4) Si $x, y \in \mathbb{K}^-$ aleshores $x + y \in \mathbb{K}^-$, $xy \in \mathbb{K}^+$.
  5) Si $x \in \mathbb{K}^+$ i $y \in \mathbb{K}^-$ aleshores $xy \in \mathbb{K}^-$.
  6) Si $x \in \mathbb{K} \setminus \{0\}$, aleshores $x^2 \in \mathbb{K}^+$. En particular $1 \in \mathbb{K}^+$.
  7) Si $x \in \mathbb{K}^+$ aleshores $-x \in \mathbb{K}^-$, $x^{-1} \in \mathbb{K}^+$.
  8) Si $x \in \mathbb{K}^-$ aleshores $-x \in \mathbb{K}^+$, $x^{-1} \in \mathbb{K}^-$.
  9) Si $x, y \in \mathbb{K}$ no nuls amb $x \leq y$, aleshores $-y \leq -x$.
  10) Si $x, y \in \mathbb{K}^+$ o bé $x, y \in \mathbb{K}^-$ amb $x \leq y$, aleshores $y^{-1} \leq x^{-1}$.
  11) Si $x \in \mathbb{K}^-$ i $y \in \mathbb{K}^+$, aleshores $x^{-1} \leq y^{-1}$.

Àlgebra de Boole

≡ **Definició** *Conjunts amb dues operacions internes. Àlgebra de Boole.*

- Sigui $(A, \oplus, \odot)$ un conjunt amb dues operacions internes. Direm que $(A, \oplus, \odot)$ ès una àlgebra de Boole si es verifiquen les següents propietats:

  1) Commutativitat: per a tot $a, b \in A$ es té que $a \oplus b = b \oplus a$, i $a \odot b = b \odot a$.
  2) Distributivitat: per a tot $a, b, c \in A$ es té que $a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c)$, i $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.
  3) Neutres: existeixen elements $0, 1 \in A$ tals que $a \oplus 0 = a$ i $a \odot 1 = a$ per a tot $a \in A$.
  4) Complementari: per a tot $a \in A$ existeix $\overline{a} \in A$ de manera que $a \oplus \overline{a} = 1$ i $a \odot \overline{a} = 0$.

≡ **Propietats** *Propietats de les àlgebres de Boole.*

- Sigui $(A, \oplus, \odot)$ una àlgebra de Boole. Aleshores es verifiquen les següents propietats:

  1) Associativitat: per a tot $a, b, c \in A$ es té que $a \oplus (b \oplus c) = (a \oplus b) \oplus c$, i $a \odot (b \odot c) = (a \odot b) \odot c$.
  2) Idempotència: per a tot $a \in A$ es té que $a \oplus a = a$, i $a \odot a = a$.
  3) Absorció: per a tot $a, b \in A$ es té que $a \oplus (b \odot a) = a$, i $a \odot (b \oplus a) = a$.
  4) Absorció universal: per a tot $a \in A$ es té que $a \oplus 1 = 1$, i $a \odot 0 = 0$.
  5) Complementari dels neutres: $\overline{0} = 1$, i $\overline{1} = 0$.
  6) Doble complementari: per a tot $a \in A$ es té que $\overline{\overline{a}} = a$.
  7) Lleis de De Morgan: per a tot $a, b \in A$ es té que $\overline{a \oplus b} = \overline{a} \odot \overline{b}$, i $\overline{a \odot b} = \overline{a} \oplus \overline{b}$.

≡ **Propietats** *Ordenació en una àlgebra de Boole.*

- Sigui $(A, \oplus, \odot)$ una àlgebra de Boole. Considerem la relació binària $\leq$ definida en el conjunt A per "$a_1 \leq a_2$ si i només si $a_1 \oplus a_2 = a_2$". Aleshores es té que:

  1) $(A, \leq)$ és un conjunt parcialment ordenat.
  2) Si $a_1, a_2 \in A$ aleshores:

  $$a_1 \leq a_2 \Leftrightarrow a_1 \oplus a_2 = a_2 \Leftrightarrow a_1 \odot a_2 = a_1 \Leftrightarrow a_1 \odot \overline{a_2} = 0 \Leftrightarrow \overline{a_1} \oplus a_2 = 1.$$

  3) Per a tot $a \in A$ es té que $0 \leq a \leq 1$.

El grup simètric

≡ **Definició** *Permutació. Grup simètric. Cicles i transposicions.*

1) Sigui X un conjunt. Una permutació del conjunt X és una aplicació bijectiva $\sigma : X \to X$.

2) Notarem $\mathfrak{S}_X$ el conjunt que té com elements totes les permutacions del conjunt X. És a dir, $\mathfrak{S}_X = \{\sigma \text{ on } \sigma : X \to X \text{ és una aplicació bijectiva}\}$. Amb la composició d'aplicacions el conjunt $\mathfrak{S}_X$ té estructura de grup no commutatiu. Direm que $(\mathfrak{S}_X, \circ)$ és el grup simètric.

3) Sigui $\sigma \in \mathfrak{S}_X$.

   a) L'ordre d'un element $x \in X$ respecte de σ és l'enter $k \geq 1$ més petit tal que $\sigma^k(x) = x$. Els elements d'ordre 1 són els punts fixos de σ.

   b) L'ordre de la permutació σ és l'enter $k \geq 1$ més petit tal que $\sigma^k = \mathrm{Id}_X$.

4) Si $X = \{1, \ldots, n\}$ per a cert natural $n \geq 1$, aleshores notarem $\mathfrak{S}_n = \mathfrak{S}_X$ i direm que $(\mathfrak{S}_n, \circ)$ és el grup simètric de n elements. En aquest cas, els elements de $\mathfrak{S}_n$ són les permutacions de n elements i les escriurem

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix} \in \mathfrak{S}_n.$$

5) Sigui $r \geq 2$ un natural. Un cicle d'ordre r és una permutació $\sigma \in \mathfrak{S}_n$ per a la qual existeix $i \in \{1, \ldots, n\}$ de manera que $i, \sigma(i), \ldots, \sigma^{r-1}(i)$ són r elements diferents, que $\sigma^r(i) = i$, i que $\sigma(j) = j$ si $j \in \{1, \ldots, n\} \setminus \{i, \sigma(i), \ldots, \sigma^{r-1}(i)\}$. En aquest cas notarem

$$\sigma = \big(i, \sigma(i), \ldots, \sigma^{r-1}(i)\big).$$

   Observem que:

   a) Els cicles d'ordre r són permutacions d'ordre r.

   b) Els elements $i, \sigma(i), \ldots, \sigma^{r-1}(i)$ tenen ordre r respecte de σ i la resta, tenen ordre 1.

6) Una transposició és un cicle d'ordre 2. Equivalentment, una permutació $\tau \in \mathfrak{S}_n$ és una transposició si i només si existeixen $i_1, i_2 \in \{1, \ldots, n\}$ diferents de manera que $\tau(i_1) = i_2$, $\sigma(i_2) = i_1$ i $\tau(i) = i$ si $i \in \{1, \ldots, n\} \setminus \{i_1, i_2\}$. En aquest cas notarem

$$\tau = (\, i_1, i_2 \,).$$

≡ **Propietats** *Descomposició en cicles i en transposicions. Ordre i signe d'una permutació.*

1) El conjunt $\mathfrak{S}_n$ té $n!$ elements.

2) Descomposicions en cicles i en transposicions:

   a) Tota permutació $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{Id}\}$ es pot descompondre en producte de cicles. Aquesta descomposició no és única.

   b) Tota permutació $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{Id}\}$ es pot descompondre en producte de cicles disjunts. Aquesta descomposició és única llevat de l'ordre dels factors.

   c) Si $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ és una descomposició en cicles disjunts de la permutació $\sigma \in \mathfrak{S}_n$, aleshores l'ordre de σ és el mínim comú múltiple dels ordres de $\sigma_1, \ldots, \sigma_r$.

   d) Tot cicle es pot descompondre en producte de transposicions. Aquesta descomposició no és única.

   e) Tota permutació $\sigma \in \mathfrak{S}_n$ es pot descompondre en producte de transposicions. Aquesta descomposició no és única.

   f) La identitat descompon en un nombre parell de transposicions.

g) Si una permutació $\sigma \in \mathfrak{S}_n$ admet una descomposició en un nombre parell de transposicions, aleshores qualsevol descomposició de σ en transposicions també té un nombre parell de factors.

3) Signe d'una permutació.

a) Definim el signe de la permutació $\sigma \in \mathfrak{S}_n$ com $\varepsilon(\sigma) = 1$ si σ té una descomposició en un nombre parell de transposicions, i $\varepsilon(\sigma) = -1$ si σ té una descomposició en un nombre senar de transposicions.

b) Una permutació $\sigma \in \mathfrak{S}_n$ es diu que és parella si $\varepsilon(\sigma) = 1$, i es diu que és senar si $\varepsilon(\sigma) = -1$.

c) Notarem $\mathfrak{A}_n$ el conjunt format per les permutacions parells. Amb la composició $(\mathfrak{A}_n, \circ)$ és un grup. Es diu que $\mathfrak{A}_n$ és el grup alternat.

4) El conjunt $\mathfrak{A}_n$ té $n!/2$ elements.

3.2 Exercicis i problemes. Enunciats

3.1 Sigui $A = \{2, 3, 4, 5, 7, 9, 16, 18\}$. Doneu la descripció de les relacions binàries següents com a subconjunt del producte cartesià $A \times A$. Comproveu si són reflexives, simètriques o transitives.

1) $xRy \Leftrightarrow x$ és divisor de y.
2) $xRy \Leftrightarrow x$ és el quadrat de y.
3) $xRy \Leftrightarrow y - x = 2$.
4) $xRy \Leftrightarrow x + y = 20$.
5) $xRy \Leftrightarrow x + y = 30$.

3.2

1) Considereu el raonament següent, segons el qual tota relació R simètrica i transitiva és també reflexiva: com que la relació és simètrica, aleshores sempre que xRy també es té yRx; aleshores, com que la relació és transitiva, es té xRx. És correcta aquesta demostració? Perquè?
2) Suposem que R és una relació simètrica i transitiva definida en un conjunt A. Suposem que per a tot $x \in A$, existeix un element $y_x \in A$ tal que xRy_x. Demostreu que R és una relació d'equivalència en A.
3) Doneu un exemple de relació simètrica i transitiva que no sigui reflexiva.

3.3 Considereu un nombre enter fixat n. Demostreu que la relació $xRy \Leftrightarrow n \mid y - x$ és d'equivalència. Determineu les classes d'equivalència i el conjunt quocient.

3.4 Demostreu que la relació $(a, b)R_1(c, d) \Leftrightarrow a + d = b + c$ és d'equivalència a $\mathbb{N} \times \mathbb{N}$ i que la relació $(a, b)R_2(c, d) \Leftrightarrow ad = bc$ ho és a $\mathbb{Z} \times \mathbb{Z}$. ¿Quines són les classes d'equivalència en cada cas? Interpreteu els conjunts quocients.

3.5 Es defineix en $\mathbb{R}$ la relació:

$$x \, R \, y \Leftrightarrow x - y \in \mathbb{Z}.$$

Demostreu que R és una relació d'equivalència en $\mathbb{R}$. Descriviu les classes d'equivalència i el conjunt quocient $\mathbb{R}/R$.

3.6 Sigui $\mathbb{Z} \times \mathbb{Z}$ el subconjunt del pla dels punts amb coordenades enteres. En aquest conjunt es defineix la relació

$$(a, b)R(c, d) \Leftrightarrow a - c = \dot{2} \quad \text{i} \quad b - d = \dot{3}.$$

Proveu que és d'equivalència. Calculeu el nombre de classes d'equivalència i doneu un representant de cada classe a distància mínima de l'origen.

3.7 Considerem el conjunt $\mathcal{P}$ de punts del pla i un punt qualsevol $\mathcal{O}$ de $\mathcal{P}$. Per a qualsevol punt $X \in \mathcal{P}$, denotem per $d(X, \mathcal{O})$ la distància del punt X al punt $\mathcal{O}$. Definim la relació en $\mathcal{P}$:

$$A \, R \, B \Leftrightarrow d(A, \mathcal{O}) = d(B, \mathcal{O}).$$

Demostreu que R és una relació d'equivalència en $\mathcal{P}$. Descriviu les classes d'equivalència i el conjunt quocient $\mathcal{P}/R$.

3.8 Demostreu que, dins el conjunt de les rectes del pla, la relació de paral·lelisme és d'equivalència i la de perpendicularitat no ho és. Quin és, en el primer cas, el conjunt quocient?

3.9 Considerem el conjunt $\mathcal{P}$ de punts del pla i un punt qualsevol $\mathcal{O}$ de $\mathcal{P}$. Definim la relació en $\mathcal{P}^* = \mathcal{P} \setminus \{\mathcal{O}\}$:

$$A \sim B \Leftrightarrow \text{ A, B i } \mathcal{O} \text{ estan alineats.}$$

Demostreu que $\sim$ és una relació d'equivalència en $\mathcal{P}^*$. Descriviu les classes d'equivalència i el conjunt quocient $\mathcal{P}^*/\sim$.

3.10 Definim en $\mathbb{Z}$ la relació:

$$a\,R\,b \Leftrightarrow a^2 + a = b^2 + b.$$

Demostreu que R és una relació d'equivalència en $\mathbb{Z}$. Descriviu les classes d'equivalència i el conjunt quocient $\mathbb{Z}/R$.

3.11 Direm que dues relacions d'equivaléncia definides en un conjunt A són iguals si determinen les mateixes classes d'equivalència. Calculeu quantes relacions d'equivaléncia diferents es poden definir en un conjunt amb 1, 2, 3 i 4 elements respectivament.

3.12 Determineu la descomposició canònica de l'aplicació $f : \mathbb{R} \longrightarrow \mathbb{R}^2$ on $f(x) = (\cos x, \sin x)$.

3.13 Considerem el conjunt $X = \{1, 2, 3, 4\}$. Determineu la descomposició canònica de l'aplicació $f : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$ on $f(A) = A \cap \{1, 2\}$ per a $A \in \mathcal{P}(X)$ qualsevol.

3.14 Demostreu que, donat un conjunt A qualsevol, la relació $XRY \Leftrightarrow X \subseteq Y$, on $X, Y \in \mathcal{P}(A)$, és una relació d'ordre dins $\mathcal{P}(A)$. Com ha de ser el conjunt A per tal que l'ordre sigui total?

3.15 Al conjunt dels segments del pla, es defineix la relació següent: *dos segments estan relacionats quan pertanyen a una mateixa recta.* Estudieu aquesta relació.

3.16 Al conjunt $\mathbb{R}^2$ dels punts del pla es defineix la relació

$$(a, b) \preceq (c, d) \;\Leftrightarrow\; a < c \text{ o bé } (a = c \text{ i } b \leq d).$$

Proveu que és un ordre. És total? (Aquest ordre s'anomena *ordre lexicogràfic.*)

3.17 Demostreu que, al conjunt dels nombre naturals, la relació definida per $xRy \Leftrightarrow x \mid y$ és d'ordre, i que es tracta d'un ordre parcial. Expliciteu un conjunt que no tingui mínim.

3.18 Considereu els subconjunts següents de $\mathbb{N}$, ordenat per divisibilitat. Tenen fites inferiors, fites superiors, ínfim, suprem, mínim, màxim, elements maximals i/o elements minimals? En cas afirmatiu, indiqueu quin o quins.

1) $A = \{2, 3, 4, 6, 9, 12\}$.

2) $A = \{2, 4, 5, 6, 12\}$.

3.19 Construcció d'un ordre a partir d'un preordre.

1) Si R és un *preordre* dins el conjunt A (una relació reflexiva i transitiva), definim la relació binària $\equiv$ en A:
$$a \equiv b \;\Leftrightarrow\; aRb \text{ i } bRa.$$
Proveu que $\equiv$ és una relació d'equivalència (direm que és la relació d'equivalència induïda per R). Demostreu que la relació R indueix sobre el conjunt quocient $A/\!\equiv$ una relació d'ordre.

2) Demostreu que la relació binària:
$$\forall x, y \in \mathbb{Z}, \quad xRy \;\Leftrightarrow\; x \mid y$$
és un preordre en $\mathbb{Z}$ i determineu l'ordre associat a aquest preordre.

3.20 Sigui $f : A \longrightarrow B$ una aplicació bijectiva.

1) Considerem una relació binària R_B en B i definim en A la relació R_A on $a_1\, R_A\, a_2$ si i només si $f(a_1)\, R_B\, f(a_2)$. Demostreu que si R_B és relació d'equivalència en B (resp. d'ordre), aleshores R_A és relació d'equivalència A (resp. d'ordre).

2) Considerem una relació binària S_A en A i definim en B la relació S_B on $b_1\, S_B\, b_2$ si i només si $f^{-1}(b_1)\, S_A\, f^{-1}(b_2)$. Demostreu que si S_A és relació d'equivalència en A (resp. d'ordre), aleshores S_B és relació d'equivalència en B (resp. d'ordre).

3.21 Doneu totes les possibles taules d'un grup amb exactament tres elements.

3.22 Un element a és idempotent per una operació $*$ si $a * a = a$. Demostreu que un grup té exactament un element idempotent. És cert si no és grup?

3.23 Definim $a * b = a + b + ab$ per a $a, b \in \mathbb{R}$ qualssevol. Sigui $S = \mathbb{R} \setminus \{-1\}$.

1) Demostreu que $*$ és una operació binària interna en S.

2) Demostreu que $(S, *)$ té estructura de grup commutatiu.

3) Resoleu l'equació $2 * x * 3 = 7$ en $(S, *)$.

3.24 Estudieu si $(\mathbb{R}, *)$, on $x * y = \sqrt[3]{x^3 + y^3}$ per a $x, y \in \mathbb{R}$, té estructura de grup commutatiu.

3.25

1) Considerem dos grups $(G, \oplus)$ i $(H, \odot)$ i definim en el producte cartesià $G \times H$ l'operació $*$ tal que per a tot $(g, h), (g', h') \in G \times H$,
$$(g, h) * (g', h') = (g \oplus g', h \odot h').$$
Demostreu que $(G \times H, *)$ és un grup. Demostreu que $(G \times H, *)$ és un grup abelià si, i només si, G i H són grups abelians.

2) Sigui $\mathbb{Q}_0$ el conjunt dels nombres racionals diferents de zero. Definim $(a, b) \cdot (c, d) = (ac, bc + d)$ per a $(a, b), (c, d) \in \mathbb{Q}_0 \times \mathbb{Q}$ qualssevol. Comproveu que $(\mathbb{Q}_0 \times \mathbb{Q}, \cdot)$ té estructura de grup no abelià.

3.26 Determineu l'estructura dels conjunts de nombres reals $A_{\mathbb{Z}} = \{ x + y\sqrt{3} \,:\, x, y \in \mathbb{Z} \}$ i $A_{\mathbb{Q}} = \{ x + y\sqrt{3} \,:\, x, y \in \mathbb{Q} \}$ amb la suma i producte usuals.

3.27 Considerem l'anell unitari no commutatiu $(\mathcal{M}_2(\mathbb{R}), +, \cdot)$ de les matrius quadrades 2×2 amb coeficients reals.

1) Justifiqueu que no és un cos, i demostreu que si $A \in \mathcal{M}_2(\mathbb{R})$ aleshores existeix una matriu $B \in \mathcal{M}_2(\mathbb{R})$ tal que o bé $AB = \mathrm{Id}_2$ o bé $AB = 0$.

2) Estudieu si les operacions suma i producte usuals de $\mathcal{M}_2(\mathbb{R})$ són tancades en el conjunt $\mathcal{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,:\, a, b \in \mathbb{R} \right\}$. Quina estructura té $(\mathcal{C}, +, \cdot)$?

3.28 Considerem en el conjunt $\mathbb{Z}$ les operacions

$$a \oplus b = a + b - 6$$
$$a \odot b = ab + \alpha(a + b) + 42$$

on $\alpha \in \mathbb{Z}$.

1) Comproveu que $(\mathbb{Z}, \oplus)$ és un grup commutatiu.

2) Demostreu que l'operació $\odot$ és associativa si, i només si, $\alpha = -6$ o $\alpha = 7$.

3) Demostreu que l'operació $\odot$ té element neutre si, i només si, $\alpha = -6$ o $\alpha = 7$.

4) Per a quins valors de α és $(\mathbb{Z}, \oplus, \odot)$ un anell?

3.29 Sigui $f : A \longrightarrow B$ una aplicació bijectiva.

1) Si $(A, +)$ és un grup, definim en B l'operació $b_1 \oplus b_2 = f(f^{-1}(b_1) + f^{-1}(b_2))$. Demostreu que $(B, \oplus)$ és un grup.

2) Si $(B, \times)$ és un grup, definim en A l'operació $a_1 \otimes a_2 = f^{-1}(f(a_1) \times f(a_2))$. Demostreu que $(A, \otimes)$ és un grup.

3.30 Donat un conjunt Ω qualsevol, en el conjunt $\mathcal{P}(\Omega)$ de les parts d'Ω definim l'operació *diferència simètrica* o *suma disjuntiva* per

$$A \oplus B = (A \cup B) \setminus (A \cap B).$$

1) Demostreu que, per a tot $A, B \in \mathcal{P}(\Omega)$, es compleix $A \oplus B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$.

2) Demostreu que $(\mathcal{P}(\Omega), \cup, \cap)$ és àlgebra de Boole i que $(\mathcal{P}(\Omega), \oplus, \cap)$ és un anell commutatiu.

3.31 Considerem una permutació $\sigma \in \mathfrak{S}_n$. Demostreu que si n és senar, aleshores el producte $(\sigma(1) - 1)(\sigma(2) - 2) \cdot \cdots \cdot (\sigma(n) - n)$ és parell. (Indicació: considereu sumes.)

3.32 Feu les taules dels grups $(\mathfrak{S}_2, \circ)$ i $(\mathfrak{S}_3, \circ)$.

3.33 Considereu la permutació de $\mathfrak{S}_8$ següent: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 8 & 2 & 7 & 5 \end{pmatrix}$.

1) Descomponeu σ en producte de cicles.

2) Trobeu l'ordre de σ.

3) Calculeu σ^{250}.

4) Descomponeu σ en producte de transposicions.

5) Calculeu la signatura de σ.

3.34 Descomponeu en producte de transposicions les permutacions següents,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}.$$

3.35 Calculeu $(1,2)(5,6)(2,3)(4,5)(4,1)(4,6)$ i descomponeu la permutació resultant en un nombre de transposicions més petit.

3.36 Considereu les permutacions de $\mathfrak{S}_5$ següents:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}.$$

1) Descomponeu les tres permutacions en producte de cicles.

2) Calculeu $\sigma\tau\rho$ i $\sigma\rho^2$.

3) Trobeu la signatura de τ i de ρ^{-1}.

3.37 Determineu quines de les permutacions següents són cicles. Si no són cicles ni la permutació identitat, expresseu-les com a producte de cicles disjunts.

1) $(1,2,3,5,7)(2,4,7,6)$.

2) $(1,2)(1,3)(1,4)$.

3) $(1,2,3,4,5)(1,2,3,4,6)(1,2,3,4,7)$.

4) $(1,2,3)(1,3,2)$.

5) $(1,2,3,4,5)^3$.

3.38 Considerem el grup simètric $\mathfrak{S}_n$, $n \geq 2$.

1) Calculeu $(1,j)(1,i)(1,j)$, on $i \neq j$.

2) Demostreu que tota permutació de $\mathfrak{S}_n$ es pot expressar com a producte de permutacions del conjunt $\{(1,2),(1,3),(1,4),\ldots,(1,n)\}$.

3.39 Demostreu que si τ_1 i τ_2 són dues transposicions diferents, aleshores $\tau_2\tau_1$ és d'ordre 2 o 3.

3.40 Sigui $\sigma = (a_1,\ldots,a_k)$ un cicle de $\mathfrak{S}_n$. Escriviu σ^{-1} en forma de cicle.

3.41

1) Demostreu que si $(i_1, i_2, \ldots, i_r)$ és un cicle de $\mathfrak{S}_n$ i $\sigma \in \mathfrak{S}_n$, aleshores $\sigma \circ (i_1, i_2, \ldots, i_r) \circ \sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_r))$.

2) Expresseu la permutació $(1,2,3)(3,5,7,9)(1,2,3)^{-1}$ com un cicle.

3) Trobeu una permutació σ tal que $\sigma(1,2)\sigma^{-1} = (1,3)$.

4) Demostreu que no existeix cap permutació σ tal que $\sigma(1,2,3)\sigma^{-1} = (1,2,4)(5,6,7)$.

3.3 Exercicis i problemes. Solucions

3.1

1) $R = \{(2,2),(3,3),(4,4),(5,5),(7,7),(9,9),(16,16),(18,18),(2,4),(2,16),(2,18),(3,9),(3,18),(4,16),(9,18)\}$. No és simètrica, però és reflexiva i transitiva.

2) $R = \{(4,2),(9,3),(16,4)\}$. No és ni reflexiva, ni simètrica, ni transitiva.

3) $R = \{(2,4),(3,5),(5,7),(7,9),(16,18)\}$. No és ni reflexiva, ni simètrica, ni transitiva.

4) $R = \{(2,18),(4,16),(16,4),(18,2)\}$. No és ni reflexiva ni transitiva, però és simètrica.

5) $R = \emptyset$. No és reflexiva, però és simètrica i transitiva.

3.2

1) No és correcta.

3.3 $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$.

3.4 $\mathbb{N}\times\mathbb{N}/R_1 = \mathbb{Z}$, $\mathbb{Z}\times\mathbb{Z}/R_2 = \mathbb{Q}$.

3.5 La classe de $x \in \mathbb{R}$ és el conjunt $\{x+n : n \in \mathbb{Z}\}$. El conjunt quocient $\mathbb{R}/R$ té tants elements com nombres reals de l'interval $[0,1)$.

3.6 Les classes són 6 i els seus representants a distància mínima de l'origen són $(0,0)$, $(0,1)$, $(0,-1)$, $(1,0)$, $(1,1)$ i $(1,-1)$.

3.7 La classe d'equivalència del punt A és el conjunt de punts de la circumferència de centre $\mathcal{O}$ que conté el punt A. El conjunt quocient $\mathcal{P}/R$ té tants elements com punts d'un semirecta amb origen en $\mathcal{O}$.

3.8 Fixat un punt P qualsevol, cada element del conjunt quocient es pot identificar amb una recta que passa per P.

3.9 La classe d'equivalència del punt A és el conjunt de punts $\mathcal{P}^*$ que són de la recta que passa per $\mathcal{O}$ i A (és a dir, els punts de la recta determinada per $\mathcal{O}$ i A, excepte $\mathcal{O}$). El conjunt quocient $\mathcal{P}^*/\sim$ té tants elements com rectes del pla que passen pel punt $\mathcal{O}$.

3.10 La classe de $a \in \mathbb{Z}$ és el conjunt $\{a,-1-a\}$. El conjunt quocient $\mathbb{Z}/R$ té tants elements com nombres enters no negatius.

3.11 Si el conjunt té 1, 2, 3 i 4 elements es poden definir respectivament 1, 2, 5 i 15 relacions d'equivaléncia.

3.14 L'ordre és total si A té exactament un element.

3.15 Es tracta d'una relació d'equivalència. Hi ha una classe per cada recta.

3.16 Sí.

3.17 Cal demostrar que és reflexiva, antisimètrica i transitiva, i que existeixen al menys dos nombres naturals que no estan relacionats. Qualsevol conjunt que no contingui un nombre que sigui divisor de tots els altres serveix com exemple.

3.18

1) El conjunt de fites superiors està format pels múltiples de 36. El conjunt no té màxim, es seu suprem és 36 i els seus elements maximals són 9 i 12. L'única fita inferior és 1, que és alhora l'ínfim. El conjunt no té mínim, però sí dos elements minimals: 2 i 3.

2) El conjunt de fites superiors està format pels múltiples de 60. El conjunt no té màxim, es seu suprem és 60 i els seus elements maximals són 5 i 12. L'única fita inferior és 1, que és alhora l'ínfim. El conjunt no té mínim, però sí dos elements minimals: 2 i 5.

3.19

1)

2) $\mathbb{Z}/R = \mathbb{N}$.

3.21 Si els 3 elements diferents del grup són e, a i b, on e és l'element neutre, aleshores:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

3.22 Si no és grup, no és pot afirmar.

3.23

3) $x = -1/3$.

3.24 $(\mathbb{R}, *)$ és grup commutatiu.

3.26 $(A_{\mathbb{Z}}, +, \cdot)$ és anell commutatiu unitari. $(A_{\mathbb{Q}}, +, \cdot)$ és cos commutatiu.

3.27

1) No és un cos ja que, per exemple, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ no té element invers.

2) $(\mathcal{C}, +, \cdot)$ és cos.

3.28

4) $\alpha = -6$.

3.32 Si $\mathfrak{S}_2 = \{\mathrm{Id}, \tau\}$, on $\tau = (1,2)$, aleshores:

	Id	τ
Id	Id	τ
τ	τ	Id

Si $\mathfrak{S}_3 = \{\mathrm{Id}, c_1, c_2, \tau_1, \tau_2, \tau_3\}$, on $c_1 = (1,2,3)$, $c_2 = (1,3,2)$, $\tau_1 = (1,2)$, $\tau_2 = (2,3)$, $\tau_3 = (1,3)$, aleshores:

	Id	c_1	c_2	τ_1	τ_2	τ_3
Id	Id	c_1	c_2	τ_1	τ_2	τ_3
c_1	c_1	c_2	Id	τ_3	τ_1	τ_2
c_2	c_2	Id	c_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	Id	c_1	c_2
τ_2	τ_2	τ_3	τ_1	c_2	Id	c_1
τ_3	τ_3	τ_1	τ_2	c_1	c_2	Id

3.33

1) $\sigma = (3,1)(4,6,2)(8,5)$.

2) 6.

3) $\sigma^{250} = \sigma^4 = (4,6,2)$.

4) $\sigma = (3,1)(4,2)(4,6)(8,5)$.

5) 1.

3.34 $\sigma = (2,4,3,5,1) = (2,4)(3,4)(3,5)(1,5)$, $\tau = (2,3,1)(5,6,4) = (2,3)(1,3)(5,6)(4,6)$.

3.35 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} = (1,6,2,3)(4,5) = (6,1)(6,3)(6,2)(5,4)$.

3.36

1) $\sigma = (3,4,1)(5,2)$, $\tau = (5,1)(3,4,2)$, $\rho = (3,4,5,1)(2)$.

2) $\sigma\tau\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$, $\sigma\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}$.

3) La signatura de τ és -1 i la de ρ^{-1} també.

3.37

1) $(2,4,1)(5,7,6,3)$.

2) $(1,4,3,2)$.

3) $(1,4,7,3,6,2,5)$.

4) Identitat.

5) $(1,4,2,5,3)$.

3.38

1) (i, j).

3.39 És d'ordre 2 si són disjunts i 3 altrament.

3.40 $\sigma^{-1} = (a_k, \ldots, a_1)$.

3.41

1)

2) $(1, 5, 7, 9)$.

3) $\sigma = (2, 3)$ o bé $\sigma = (1, 3, 2)$. Si $n = 3$, σ ha de ser una de les dues anteriors; si $n \geq 4$, hi ha més permutacions que ho satisfan.

4) No existeix, ja que $\sigma(1, 2, 3)\sigma^{-1}$ és un cicle.

4
Conjunts de nombres. Numerabilitat

4.1 Resum teòric

Conjunts finits. Cardinal

≡ **Conjunts equipotents**

- Dos conjunts no buits A i B són *equipotents* si existeix una aplicació bijectiva $f : A \longrightarrow B$. Si A i B són equipotents, escriurem $A \simeq B$.

- La relació $A \simeq B$ és d'equivalència.

≡ **Definició** *Conjunt finit i infinits. Cardinal.*

- Un conjunt A és *finit* si és buit o és equipotent a C_n per a algun enter positiu n, on $C_n = \{1, 2, \ldots, n\}$.

- Direm que el conjunt buit té *cardinal* 0 i un conjunt finit A no buit té *cardinal* n si és equipotent a C_n. Notació: $|A|$ o bé $\#A$ o bé $\text{card}(A)$ representa el cardinal de A.

- Un conjunt és *infinit* si no és finit.

≡ **Propietats**

1) Siguin A i B conjunts tals que $A \simeq B$. Si $|A| = n$, aleshores $|B| = n$.

2) Sigui A un conjunt finit tal que $|A| = n$.

   - Si $x \in A$, aleshores $|A - \{x\}| = n - 1$.
   - Si $y \notin A$, aleshores $|A \cup \{y\}| = n + 1$.

3) C_n i C_m són equipotents si i només si $n = m$.

4) Si A és un conjunt tal que $A \simeq C_n$ i $A \simeq C_m$, aleshores $n = m$.

5) Si A és un conjunt finit i $B \subseteq A$, aleshores:

   - B és finit i $|B| \leq |A|$.
   - $|B| = |A|$ si i només si $B = A$.

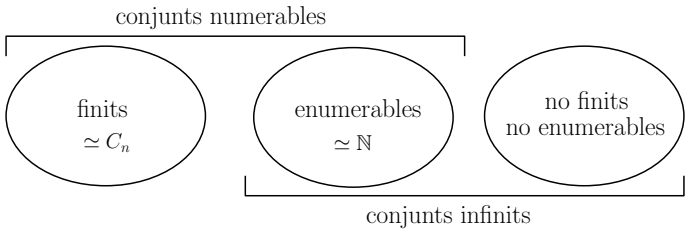
6) Si A i B són conjunts finits, aleshores $A \times B$, $A \cup B$ i $A \cap B$ són finits i a més

$$|A \times B| = |A| \cdot |B|$$
$$|A \cup B| = |A - B| + |B - A| + |A \cap B| = |A| + |B| - |A \cap B|$$

Conjunts numerables i enumerables

≡ **Definició** *Conjunts enumerables i numerables.*

- Un conjunt A és *enumerable* si és equipotent al conjunt dels nombres naturals $\mathbb{N}$, és a dir, si existeix una bijecció $f : A \longrightarrow \mathbb{N}$.
- Un conjunt és *numerable* si és finit o enumerable.



≡ **Propietats** *Conjunts enumerables.*

1) Sigui A un conjunt enumerable.

- Si $x \in A$, aleshores $A - \{x\}$ és enumerable.
- Si $y \notin A$, aleshores $|A \cup \{y\}|$ és enumerable.

2) Els subconjunts de $\mathbb{N}$ són numerables.

3) Els subconjunts d'un conjunt enumerable són numerables.

4) Si A i B són enumerables, aleshores $A \times B$, $A \cup B$ i $A \cap B$ són enumerables.

≡ **Propietats** *Conjunts infinits.*

1) Si A és un conjunt infinit, aleshores conté un subconjunt propi enumerable.

2) Un conjunt A és infinit si i només si és equipotent a un subconjunt propi.

Conjunts de nombres

≡ **Construcció** *Naturals, enters, racionals.*

1) Els nombres naturals.

- El conjunt $\mathbb{N}$ dels nombres naturals satisfà els *Axiomes de Peano*:
  1) Existeix un element en $\mathbb{N}$ que anomenarem 0.
  2) Existeix una aplicació $\varphi : \mathbb{N} \to \mathbb{N}$ que anomenem "aplicació següent".
  3) El 0 no té cap antiimatge per l'aplicació següent, és a dir, $0 \notin \varphi(\mathbb{N})$.
  4) L'aplicació següent és injectiva.
  5) Si $A \subseteq \mathbb{N}$, aleshores:

$$\left.\begin{array}{l} 0 \in A \\ (\forall n \in \mathbb{N})(n \in A \Rightarrow \varphi(n) \in A) \end{array}\right\} \Rightarrow A = \mathbb{N}.$$

2) Els nombres enters.

- El conjunt $\mathbb{Z}$ dels nombres enters és el conjunt quocient $\mathbb{N} \times \mathbb{N}/\sim$, on $\sim$ és la relació d'equivalència en $\mathbb{N} \times \mathbb{N}$:

$$(a, b) \sim (c, d) \;\Leftrightarrow\; a + d = b + c$$

- La classe d'equivalència de (a, b) s'identifica amb el nombre enter $a - b$.

3) Els nombres racionals.

- El conjunt $\mathbb{Q}$ dels nombres racionals és el conjunt quocient $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim$, on $\sim$ és la relació d'equivalència en $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

$$(a, b) \sim (c, d) \;\Leftrightarrow\; a\,d = b\,c$$

- La classe d'equivalència de (a, b) s'identifica amb el nombre racional a/b.

≡ **Propietats** *Numerabilitat.*

1) Els conjunts dels nombres naturals, enters i racionals són infinits i numerables (i per tant, són enumerables).

2) Els conjunts dels nombres irracionals i reals són infinits i no numerables (i per tant, no són enumerables).

4.2 Exercicis i problemes. Enunciats

4.1 Demostreu que si A, B, C són conjunts finits qualssevol, aleshores:

1) $|A \setminus B| = |A| - |A \cap B|$.
2) $|A \cup B| = |A| + |B| - |A \cap B|$.
3) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

4.2 Sigui Ω un conjunt finit. En el conjunt $\mathcal{P}(\Omega)$ definim la relació binària $\preceq$, on $A \preceq B$ si i només si $|A| \leq |B|$. Estudieu si la relació binària $\preceq$ és d'ordre. Donats dos subconjunts A, B de Ω, quina relació hi ha entre $A \preceq B$ i $A \subseteq B$?

4.3 Considerem nombres reals a, b, c, d tals que $a < b$ i $c < d$. Demostreu que els intervals $[a, b]$ i $[c, d]$ són equipotents.

4.4 Demostreu que el conjunt d'enters múltiples de 3 és equipotent al conjunt d'enters senars.

4.5 Ordeneu de forma creixent els nombres enters següents: $100!$, 100^{100}, 2^{100}, $(50!)^2$. Per a cadascun d'aquests nombres doneu un conjunt que el tingui per cardinal.

4.6 Sigui $f : X \longrightarrow X$ una aplicació, on X és un conjunt finit. Demostreu que:

$$f \text{ és bijectiva } \Leftrightarrow f \text{ és injectiva } \Leftrightarrow f \text{ és exhaustiva.}$$

4.7 Considerem dos conjunts finits X, Y. Demostreu que:

1) $|X| = |Y| \Leftrightarrow$ existeix una aplicació $f : X \longrightarrow Y$ bijectiva.
2) $|X| \leq |Y| \Leftrightarrow$ existeix una aplicació $f : X \longrightarrow Y$ injectiva.
3) $|Y| \leq |X| \Leftrightarrow$ existeix una aplicació $f : X \longrightarrow Y$ exhaustiva.

4.8 Considerem dos conjunts finits X, Y.

1) Sigui $f : X \longrightarrow Y$ una aplicació. Demostreu que:
   a) $\forall A \subseteq X$, $|f(A)| \leq |A|$.
   b) f és injectiva $\Leftrightarrow \forall A \subseteq X$, $|f(A)| = |A|$.
   c) f és exhaustiva $\Leftrightarrow \forall B \subseteq Y$, $|f^{-1}(B)| \geq |B|$.
2) Doneu exemples d'aplicacions $f : X \longrightarrow Y$ i subconjunts $A \subseteq X$, $B \subseteq Y$ tals que:
   a) $|f(A)| < |A|$.
   b) $|f(A)| = |A|$.
   c) $|f^{-1}(B)| < |B|$.

d) $|f^{-1}(B)| = |B|$.

e) $|f^{-1}(B)| > |B|$.

4.9 Demostreu que un conjunt X és numerable si i només si existeix una aplicació injectiva $f : X \to \mathbb{N}$

4.10

1) Considerem el conjunt $\mathcal{M}_{m\times n}(\mathbb{K})$ de matrius amb m files i n columnes amb coeficients en el cos $\mathbb{K}$, on $\mathbb{K}$ és $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Decidiu si $\mathcal{M}_{m\times n}(\mathbb{K})$ és o no és enumerable.

2) Sigui E un $\mathbb{K}$-espai vectorial de dimensió finita $n \geq 1$, on $\mathbb{K}$ és $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Decidiu si E és o no és enumerable.

4.11

1) Considerem una col·lecció de subconjunts $\{A_n : n \in \mathbb{N}\}$. Suposem que per a tot $n \in \mathbb{N}$ existeix una aplicació injectiva $\varphi_n : A_n \longrightarrow \mathbb{N}$. Per a tot $x \in \bigcup_{n\in\mathbb{N}} A_n$ definim:

$$i_x = \min\{ n \in \mathbb{N} : x \in A_n\}.$$

Demostreu que l'aplicació

$$\phi : \bigcup_{n\in\mathbb{N}} A_n \longrightarrow \mathbb{N} \times \mathbb{N}$$

definida per $\phi(x) = (i_x, \varphi_{i_x}(x))$ és injectiva.

2) Demostreu que si I és un conjunt numerable i per a tot $i \in I$, A_i és un conjunt numerable, aleshores el conjunt $\bigcup_{i\in I} A_i$ és numerable (és a dir, la unió numerable de conjunts numerables és numerable).

3) Demostreu que el conjunt de polinomis amb coeficients enters és enumerable.

4.3 Exercicis i problemes. Solucions

4.2 La relació binària $\preceq$ és reflexiva i transitiva, però no és antisimètrica. Es compleix la implicació $A \subseteq B \Rightarrow A \preceq B$, peró en general no és cert el recíproc. Per exemple, si $\Omega = \{1, 2, 3\}$, $A = \{1\}$ i $B = \{2, 3\}$, aleshores $A \preceq B$ però $A \nsubseteq B$.

4.3 Una possible bijecció de $[a, b]$ a $[c, d]$ és l'aplicació f tal que $f(x) = \dfrac{d-c}{b-a}(x-a) + c$.

4.4 Una possible bijecció del conjunt d'enters múltiples de 3 al conjunt d'enters senars és l'aplicació f tal que $f(x) = 1 + 2x/3$.

4.5 $2^{100} < (50!)^2 < 100! < 100^{100}$. Els conjunts $\mathcal{S}_{100}$, $\overbrace{C_{100} \times \cdots \times C_{100}}^{100)}$, $\mathcal{P}(C_{100})$, $\mathcal{S}_{50} \times \mathcal{S}_{50}$ tenen cardinal 100!, 100^{100}, 2^{100}, $(50!)^2$ respectivament.

4.8

2) $f : \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$, tal que $f(1) = f(2) = 1$, $f(3) = 3$, i:
   a) $A = \{1, 2\}$.
   b) $A = \{1\}$.
   c) $B = \{2\}$ o $B = \{1, 3\}$.
   d) $B = \{3\}$.
   e) $B = \{1\}$.

4.10

1) És enumerable si i només si $\mathbb{K} = \mathbb{Q}$.
2) És enumerable si i només si $\mathbb{K} = \mathbb{Q}$.

5
El cos dels nombres complexos

5.1 Resum teòric

≡ **Definició** *El cos dels nombres complexos.*

- Definim el cos $\mathbb{C}$ dels nombres complexos com el cos commutatiu $(\mathbb{C}, +, \cdot) = (\mathbb{R}^2, +, \cdot)$ on les operacions internes suma i producte són:
  - Suma: $(a, b) + (c, d) = (a + c, b + d)$.
  - Producte: $(a, b)(c, d) = (ac - bd, ad + bc)$.

≡ **Observacions** *Observacions i propietats dels nombres complexos.*

1) Com a conjunt, $\mathbb{C}$ és $\mathbb{R}^2$. Per tant els nombres complexos són parells ordenats de nombres reals. És a dir, els elements de $\mathbb{C}$ són del tipus $z = (a, b)$ amb $a, b \in \mathbb{R}$.

2) Igualtat de nombres complexos.
   - Dos nombres complexos són iguals si i només si són iguals com a parells ordenats de nombres reals. És a dir, si $z_1 = (a_1, b_1)$ i si $z_2 = (a_2, b_2)$ són dos nombres complexos, aleshores $z_1 = z_2$ si i només si $a_1 = a_2$ i $b_1 = b_2$.

3) Element neutre i invers en el cos dels nombres complexos.
   - L'element neutre de la suma és $(0, 0)$, i l'oposat de (a, b) és $-(a, b) = (-a, -b)$.
   - L'element neutre del producte és $(1, 0)$, i si $(a, b) \neq (0, 0)$ aleshores el seu invers és $(a, b)^{-1} = (a/(a^2 + b^2), -b/(a^2 + b^2))$.

4) El cos dels nombres complexos és una extensió del cos dels nombres reals. És a dir, es té que $\mathbb{R} \subseteq \mathbb{C}$ identificant el nombre real $\lambda \in \mathbb{R}$ amb el nombre complex $(\lambda, 0) \in \mathbb{C}$ i, a més, aquesta inclusió conserva les operacions:

- Si $\lambda_1, \lambda_2 \in \mathbb{R}$ aleshores en $\mathbb{C}$ es té que $(\lambda_1, 0) + (\lambda_2, 0) = (\lambda_1 + \lambda_2, 0)$.
- Si $\lambda_1, \lambda_2 \in \mathbb{R}$ aleshores en $\mathbb{C}$ es té que $(\lambda_1, 0)(\lambda_2, 0) = (\lambda_1\lambda_2, 0)$.

5) Podem operar nombres reals amb nombres complexos. És a dir, si $\lambda \in \mathbb{R}$ és un real i si $z \in \mathbb{C}$ és un complex, aleshores es té que $\lambda + z \in \mathbb{C}$ i a més $\lambda z \in \mathbb{C}$, concretament:

- Si $\lambda \in \mathbb{R}$ i si $z = (a, b) \in \mathbb{C}$, aleshores $\lambda + z = (\lambda, 0) + (a, b) = (\lambda + a, b) \in \mathbb{C}$.
- Si $\lambda \in \mathbb{R}$ i si $z = (a, b) \in \mathbb{C}$, aleshores $\lambda z = (\lambda, 0)(a, b) = (\lambda a, \lambda b) \in \mathbb{C}$.

6) Fent servir les operacions entre nombres reals i nombres complexos, es tenen les següents igualtats:

- Si $z \in \mathbb{C}$ és un nombre complex aleshores $-z = (-1)z$.
- Si $z = (a, b) \in \mathbb{C}$ és un complex no nul, aleshores $(a^2 + b^2)^{-1}$ és un nombre real i es té que $z^{-1} = (a, b)^{-1} = (a^2 + b^2)^{-1}(a, -b)$.
- Si $z = (a, b) \in \mathbb{C}$ és un nombre complex, aleshores podem escriure $z = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a(1, 0) + b(0, 1)$.

≡ **Definició** *Part real i part imaginària. La unitat imaginària.*

1) Si $z = (a, b) \in \mathbb{C}$ és un nombre complex, aleshores direm que a és la seva part real i que b és la seva part imaginària. Notarem $\mathrm{Re}(z) = a$, $\mathrm{Im}(z) = b$.

2) Direm que un nombre complex z és real si i només si $\mathrm{Im}(z) = 0$. Direm que z és imaginari (o imaginari pur) si i només si $\mathrm{Re}(z) = 0$.

3) Definim la unitat imaginària i com el nombre complex $i = (0, 1) \in \mathbb{C}$.

≡ **Propietats** *Propietats de la unitat imaginària.*

1) La unitat imaginària i satisfà $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$.

2) Per tant, la unitat imaginària i és una solució de l'equació $x^2 + 1 = 0$.

3) Si $n \geq 0$ és un nombre natural, aleshores: $i^{4n} = 1$, $i^{4n+1} = i$, $i^{4n+2} = -1$, $i^{4n+3} = -i$.

≡ **Definició** *Parell ordenat i forma binòmica d'un nombre complex.*

- Si $z = (a, b) \in \mathbb{C}$ és un nombre complex, aleshores podem escriure $z = (a, b) = a(1, 0) + b(0, 1) = a + bi$. Direm que (a, b) és l'expressió de z com parell ordenat i direm que $a + bi$ és l'expressió binòmica del nombre complex z.

≡ **Propietats** *Operacions en forma binòmica. El conjugat. Propietats del conjugat.*

1) La suma i el producte de nombres complexos expressats en forma binòmica es realitza operant formalment els binomis.

2) Observem que:

$$(a+bi)(a-bi) = a^2+b^2$$
$$(a+bi)^{-1} = \frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$$

3) El conjugat d'un nombre complex.

   - Definim el conjugat $\overline{z}$ d'un nombre complex $z=(a,b)$ com el complex $\overline{z}=(a,-b)$.
   - És a dir, si $z=a+bi$ aleshores $\overline{z}=a-bi$.

4) El conjugat satisfà les propietats següents:

   - $\mathrm{Re}(\overline{z}) = \mathrm{Re}(z)$.
   - $\mathrm{Im}(\overline{z}) = -\mathrm{Im}(z)$.
   - Un nombre complex z és real si i només si $z=\overline{z}$.
   - Un nombre complex z és imaginari si i només si $z=-\overline{z}$.
   - $z+\overline{z} = 2\,\mathrm{Re}(z)$.
   - $z-\overline{z} = 2i\,\mathrm{Im}(z)$.
   - $z\overline{z} = \mathrm{Re}(z)^2+\mathrm{Im}(z)^2$.
   - Si $z=(a,b)$ és un complex no nul, aleshores $z^{-1} = \overline{z}/(z\,\overline{z}) = \overline{z}/(a^2+b^2)$.

5) Conjugació i operacions:

   - Suma: $\overline{z_1+z_2} = \overline{z_1}+\overline{z_2}$.
   - Producte: $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.
   - Invers: $\overline{z^{-1}} = (\overline{z})^{-1}$.
   - Conjugat: $\overline{\overline{z}} = z$.

≡ **Observació** *Mòdul i argument d'un nombre complex.*

- Sigui $z=(a,b)\in\mathbb{C}$ un nombre complex. Com a punt del pla podem considerar el seu mòdul (que és un nombre real més gran o igual que zero) i, en cas que $z\neq 0$, aleshores podem considerar el seu argument (que està definit mòdul 2π). És a dir:

- $\begin{cases} a = r\cos\theta \\ b = r\sin\theta \end{cases}$ on: $\begin{cases} r=\sqrt{a^2+b^2} \text{ és el mòdul de } z. \text{ Notarem } |z|=r. \\ \theta \text{ és l'argument de } z. \text{ Notarem } \arg(z)=\theta. \end{cases}$

≡ **Definició** *Expressió trigonomètrica i expressió polar d'un nombre complex.*

- Amb les notacions de l'observació anterior, donat un nombre complex z direm que r_θ és l'expressió polar de z i que $r(\cos\theta + i\sin\theta)$ és l'expressió trigonomètrica de z.

≡ **Propietats** *Propietats del mòdul i de l'argument. Operacions en forma polar.*

1) El mòdul d'un nombre real és el seu valor absolut, i el seu argument és 0 (si el nombre real és positiu) o π (si el nombre real és negatiu).
2) $z\overline{z} = |z|^2$, $z^{-1} = \overline{z}/|z|^2$, $z/\overline{z} = 1_{2\arg(z)}$.
3) Mòdul, argument i operacions de nombres complexos.
   - Suma: $|z_1 + z_2| \leq |z_1| + |z_2|$.
   - Producte: $|z_1 z_2| = |z_1||z_2|$, $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$.
   - Invers: $|z^{-1}| = |z|^{-1}$, $\arg(z^{-1}) = -\arg(z)$.
   - Conjugat: $|\overline{z}| = |z|$, $\arg(\overline{z}) = -\arg(z)$.
4) Operacions de nombres complexos en forma polar.
   - Producte: $(r_1)_{\theta_1}(r_2)_{\theta_2} = (r_1 r_2)_{\theta_1+\theta_2}$.
   - Invers: $(r_\theta)^{-1} = (r^{-1})_{-\theta}$.
   - Conjugat: $\overline{r_\theta} = r_{-\theta}$.
   - Potències: $(r_\theta)^n = (r^n)_{n\,\theta}$, per a tot n enter.

≡ **Propietats** *Potències i arrels d'un nombre complex.*

1) Fórmula de De Moivre.
   - Si $n \geq 1$ és un nombre natural, aleshores $(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$.
2) Arrels n-èsimes d'un nombre complex.
   - Un nombre complex no nul té exactament n arrels n-èsimes diferents.
   - Concretament, si $n \geq 1$ és un nombre natural i si $z = r_\theta$ és l'expressió polar del nombre complex no nul z aleshores $\sqrt[n]{z} = \{(\sqrt[n]{r})_{(\theta+2k\pi)/n} : k = 0, \ldots, n-1\}$, on $\sqrt[n]{r}$ és l'arrel real positiva n-èsima del nombre real positiu r.

≡ **Definició** *Exponencial d'un nombre complex.*

- Definim l'exponencial complexa e^z d'un nombre complex $z = (a, b) \in \mathbb{C}$ com el nombre complex $e^z = e^a e^{bi}$, on $e^{bi} = \cos b + i\sin b$.

- La darrera igualtat s'anomena la fórmula d'Euler.

≡ **Propietats** *Propietats de l'exponencial complexa.*

1) L'exponencial complexa és una extensió de l'exponencial real.
2) Relacions bàsiques: $e^{\pi i}+1=0$, $e^{2\pi i}=1$, $e^{\pi i/2}=i$, $e^{3\pi i/2}=-i$.
3) Mòdul: $|e^z|=e^{\mathrm{Re}(z)}$.
4) Argument: $\arg(e^z)=\mathrm{Im}(z)$.
5) Part real: $\mathrm{Re}(e^z)=e^{\mathrm{Re}(z)}\cos\mathrm{Im}(z)$.
6) Part imaginaria: $\mathrm{Im}(e^z)=e^{\mathrm{Re}(z)}\sin\mathrm{Im}(z)$.
7) Exponencial i cosinus: $\cos\theta=\mathrm{Re}(e^{\theta i})=(e^{\theta i}+e^{-\theta i})/2$.
8) Exponencial i sinus: $\sin\theta=\mathrm{Im}(e^{\theta i})=(e^{\theta i}-e^{-\theta i})/2i$.
9) Periodicitat: $e^{z+2k\pi i}=e^z$ per a tot $k\in\mathbb{Z}$.
10) Igualtat: $e^{z_1}=e^{z_2}$ si i només si $z_2=z_1+2k\pi i$ amb $k\in\mathbb{Z}$.

≡ **Propietats** *Operacions amb l'exponencial complexa. Logaritme.*

1) Producte: $e^{z_1}e^{z_2}=e^{z_1+z_2}$.
2) Potències: $(e^z)^n=e^{nz}$ per a tot natural $n\geq 0$.
3) Invers: $(e^z)^{-1}=e^{-z}$.
4) Conjugat: $\overline{e^z}=e^{\overline{z}}$.
5) Logaritme: Si $z=r_\theta$ és l'expressió polar del complex no nul z, aleshores els complexos $w\in\mathbb{C}$ que satisfan $e^w=z$ són del tipus $w=\ln r+(\theta+2k\pi)i$ amb $k\in\mathbb{Z}$.

≡ **Definició** *Expressió exponencial d'un nombre complex.*

- Si $z\in\mathbb{C}$ és un nombre complex, aleshores podem escriure $z=|z|e^{\arg(z)\,i}$. Direm que aquesta expressió és l'expressió exponencial del nombre complex z.

≡ **Definició** *Expressió matricial d'un nombre complex.*

- La representació matricial d'un nombre complex $z = (a, b) \in \mathbb{C}$ és la matriu quadrada d'ordre dos amb coeficients reals $M(z) = \begin{pmatrix} \mathrm{Re}(z) & -\mathrm{Im}(z) \\ \mathrm{Im}(z) & \mathrm{Re}(z) \end{pmatrix}$.
- Per tant,
  a) si $z = (a, b) = a + bi$, aleshores $M(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$;
  b) si $z = r_\theta = r(\cos\theta + i\sin\theta) = re^{i\theta}$, aleshores $M(z) = r\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

≡ **Propietats** *Propietats de la representació matricial.*

1) Un complex z és un nombre real si i només si existeix un real λ tal que $M(z) = \lambda\,\mathrm{Id}_2$. En aquest cas, $z = \lambda$.
2) Suma: $M(z_1 + z_2) = M(z_1) + M(z_2)$ per a tot $z_1, z_2 \in \mathbb{C}$.
3) Producte: $M(z_1 z_2) = M(z_1)M(z_2)$ per a tot $z_1, z_2 \in \mathbb{C}$.
4) Producte per un real: $M(\lambda z) = \lambda M(z)$ per a tot $z \in \mathbb{C}$ i per a tot $\lambda \in \mathbb{R}$.
5) Conjugació i transposició: $M(\overline{z}) = M(z)^T$ per a tot $z \in \mathbb{C}$.
6) Mòdul i determinant: $|z|^2 = \det(M(z))$ per a tot $z \in \mathbb{C}$.
7) Invers: $M(z^{-1}) = M(z)^{-1}$ per a tot $z \in \mathbb{C}$ no nul.

5.2 Exercicis i problemes. Enunciats

5.1 Expresseu els següents nombres complexos en forma binòmica:

1) $(1+i)^2$
2) $(2+3i)(3-4i)$
3) $\dfrac{1}{i}$
4) $\dfrac{1}{1+i}$
5) $\dfrac{1}{1+i}+\dfrac{1}{1-i}$
6) $\dfrac{1+i}{1-2i}$
7) $\dfrac{(1+i)^4}{(1-i)^3}+\dfrac{(1-i)^4}{(1+i)^3}$
8) i^5+i^{16}
9) $1+i+i^2+i^3$
10) $\dfrac{1}{2}(1+i)(1+i^{-8})$

5.2 Calculeu el mòdul dels següents nombres complexos:

1) $1+i$
2) $3+4i$
3) $\dfrac{1+i}{1-i}$
4) $1+i+i^2$
5) i^7+i^{10}
6) $2(1-i)+3(2+i)$

5.3 Calculeu el mòdul i l'argument dels nombres complexos següents:

1) $2i$
2) $-3i$
3) -1
4) 1
5) $-3+\sqrt{3}\,i$
6) $\dfrac{1+i}{\sqrt{2}}$
7) $(-1+i)^3$
8) $(-1-i)^3$
9) $\dfrac{1}{1+i}$
10) $\dfrac{1}{(1+i)^2}$

5.4 Expresseu els següents nombres complexos en forma binòmica:

1) $e^{\pi i/2}$
2) $2e^{-\pi i/2}$
3) $3e^{\pi i}$
4) $-e^{-\pi i}$
5) $i+e^{2\pi i}$
6) $e^{\pi i/4}$
7) $e^{\pi i/4}-e^{-\pi i/4}$
8) $\dfrac{1-e^{\pi i/2}}{1+e^{\pi i/2}}$
9) $e^{5\pi i/6}+e^{-\pi i/6}$
10) $e^{2\pi i/3}$

5.5 Sigui z el nombre complex donat per $z=(1,-1)$.

1) Expresseu z, $-z$, z^{-1} i $\overline{z}$ en forma binòmica, polar, trigonomètrica, i exponencial complexa.
2) Determineu per a quins nombres naturals n el complex z^n és un nombre real.
3) Sigui $z_1 \in \mathbb{C}$ un nombre complex no nul. Sigui $z_2 = z^n z_1$, on n és un nombre natural. Determineu la diferència entre els arguments de z_1 i de z_2 en funció de n.

5.6 Calculeu les arrels que s'indiquen:

1) Les arrels cúbiques de i.
2) Les arrels quartes de -1.
3) Les arrels cúbiques de $-2+2i$.
4) Les arrels sisenes de -8.

5.7 Trobeu els nombres complexos $w \in \mathbb{C}$ solució de l'equació $e^w = z$ on:

1) $z = 1$
2) $z = i$
3) $z = -\sqrt{3} - i$

5.8 Calculeu $\displaystyle\sum_{k=1}^{2435} i^k$.

5.9 Calculeu el determinant de les matrius següents:

1) $\begin{pmatrix} 1 & z^2 & z \\ z & 1 & z^2 \\ z^2 & z & 1 \end{pmatrix}$, on $z \in \mathbb{C}$ és una arrel cúbica de la unitat.

2) $\begin{pmatrix} z & 1 & z \\ 1 & z & 1 \\ 1 & 1 & z^2 \end{pmatrix}$, on $z = \cos\dfrac{\pi}{4} + i \sin\dfrac{\pi}{4}$.

5.10 Descriviu geomètricament el conjunt de nombres complexos z que satisfan les equacions:

1) $0 < |z| \leq 3$
2) $|z - i| = 1$.
3) $|z + i| \leq 3$.
4) $z(\overline{z} + 2) = 3$.
5) $\mathrm{Re}(\overline{z} - i) = 2$.
6) $\mathrm{Im}(z^2) = 4$.

5.11 Sigui z un complex no nul, i sigui z' el complex que resulta de multiplicar z per i. Determineu la diferència entre els arguments de z i z'.

5.12 Determineu els nombres complexos que coincideixen amb la cinquena potència del seu conjugat.

5.13 Trobeu els nombres complexos no nuls tals que el seu cub és igual al quadrat del seu conjugat.

5.14 Sigui z un nombre complex. Suposem que existeix una arrel quarta w de z de manera que el complex $(1+i)w$ és un nombre real. Determineu l'argument de z.

5.15 Demostreu les fórmules següents:

1) $\cos(3\alpha) = \cos^3\alpha - 3\sin^2\alpha\,\cos\alpha$.
2) $\sin(3\alpha) = -\sin^3\alpha + 3\,\cos^2\alpha\,\sin\alpha$.
3) $\cos^3(\alpha) = \frac{1}{4}(3\cos\alpha + \cos(3\alpha))$.
4) $\sin^3(\alpha) = \frac{1}{4}(3\sin\alpha - \sin(3\alpha))$.

5.16 Estudieu si les operacions suma i producte són tancades en els següents conjunts de nombres complexos i en quins casos determinen estructura de grup:

1) $A = \{z \in \mathbb{C} \text{ tals que } |\,z\,| = 1\}$.

2) $B = \{z \in \mathbb{C} \text{ tals que } \arg(z) = \pi/4\}$.

3) $R_n = \{z \in \mathbb{C} \text{ tals que } z^n = 1\}$, on $n \geq 1$ és un natural.

5.17 Considerem el conjunt $G = \{1, -1, z, -z, z^2, -z^2\}$, on z és un nombre complex tal que $z \neq \pm 1$ i $z^3 = 1$. Feu la taula del producte i comproveu si G amb el producte és un grup commutatiu.

5.3 Exercicis i problemes. Solucions

5.1 La forma binòmica és:

1) $2i$ 3) $-i$ 5) 1 7) 2 9) 0

2) $18+i$ 4) $1/2-(1/2)i$ 6) $-1/5+(3/5)i$ 8) $1+i$ 10) $1+i$

5.2 Els seus mòduls són:

1) $\sqrt{2}$ 2) 5 3) 1 4) 1 5) $\sqrt{2}$ 6) $\sqrt{65}$

5.3

1) El mòdul de $2i$ és 2, i el seu argument és $\pi/2$.
2) El mòdul de $-3i$ és 3, i el seu argument és $-\pi/2$.
3) El mòdul de -1 és 1, i el seu argument és π.
4) El mòdul de 1 és 1, i el seu argument és 0.
5) El mòdul de $-3+\sqrt{3}\,i$ és $2\sqrt{3}$, i el seu argument és $(5\pi)/6$.
6) El mòdul de $(1+i)/\sqrt{2}$ és 1, i el seu argument és $\pi/4$.
7) El mòdul de $(-1+i)^3$ és $2\sqrt{2}$, i el seu argument és $\pi/4$.
8) El mòdul de $(-1-i)^3$ és $2\sqrt{2}$, i el seu argument és $-\pi/4$.
9) El mòdul de $1/(1+i)$ és $\sqrt{2}/2$, i el seu argument és $-\pi/4$.
10) El mòdul de $1/(1+i)^2$ és $1/2$, i el seu argument és $-\pi/2$.

5.4 La seva forma binòmica és:

1) i 3) -3 5) $1+i$ 7) $\sqrt{2}\,i$ 9) 0

2) $-2i$ 4) 1 6) $(1+i)/\sqrt{2}$ 8) $-i$ 10) $-1/2+\sqrt{3}\,i/2$

5.5

1) $z=(1,-1)=1-i=(\sqrt{2})_{7\pi/4}=\sqrt{2}(\cos(7\pi/4)+i\sin(7\pi/4))=\sqrt{2}e^{7\pi i/4}$.
$-z=(-1,1)=-1+i=(\sqrt{2})_{3\pi/4}=\sqrt{2}(\cos(3\pi/4)+i\sin(3\pi/4))=\sqrt{2}e^{3\pi i/4}$.
$z^{-1}=(1/2,1/2)=1/2+i/2=(1/\sqrt{2})_{\pi/4}=(1/\sqrt{2})(\cos(\pi/4)+i\sin(\pi/4))=(1/\sqrt{2})e^{\pi i/4}$.
2) Per a n múltiple de 4.
3) $7\pi n/4$.

5.6

1) $(\sqrt{3}+i)/2$, $(-\sqrt{3}+i)/2$, $-i$.
2) $(1+i)/\sqrt{2}$, $(-1+i)/\sqrt{2}$, $(-1-i)/\sqrt{2}$, $(1-i)/\sqrt{2}$.
3) $1+i$, $(-\sqrt{3}-1)/2+(\sqrt{3}-1)i/2$, $(\sqrt{3}-1)/2-(\sqrt{3}+1)i/2$.
4) $(\sqrt{6}+\sqrt{2}i)/2$, $\sqrt{2}i$,$(-\sqrt{6}+\sqrt{2}i)/2$, $(-\sqrt{6}-\sqrt{2}i)/2$, $-\sqrt{2}i$, $(\sqrt{6}-\sqrt{2}i)/2$.

5.7

1) $2k\pi i$, on $k \in \mathbb{Z}$.
2) $(\pi/2+2k\pi)i$, on $k \in \mathbb{Z}$.
3) $\ln(2)+(-5\pi/6+2k\pi)i$, on $k \in \mathbb{Z}$.

5.8 -1.

5.9

1) 0.
2) $-2i$.

5.10

1) Cercle de centre l'origen i radi 3, excepte l'origen.
2) Circumferència de centre $(0,1)$ i radi 1.
3) Cercle de centre $(0,-1)$ i radi 3.
4) Els punts $(1,0)$ i $(-3,0)$.
5) Recta d'equació $x=2$.
6) Hipèrbola d'equació $xy=2$.

5.11 $\pi/2$.

5.12 $z=0$, i $z=e^{k\pi i/3}$ on $k \in \{0,1,2,3,4,5\}$.

5.13 Són les arrels cinquenes de la unitat.

5.14 π.

5.16

1) La suma no és tancada, el producte sí. Amb el producte és grup.
2) La suma és tancada, el producte no. No és grup ni amb la suma ni amb el producte.
3) La suma no és tancada, el producte sí. És grup amb el producte.

5.17 G amb el producte és un grup commutatiu.

6
Aritmètica

6.1 Resum teòric

Divisibilitat a l'anell $\mathbb{Z}$

≡ **L'anell dels nombres enters** *Elements invertibles. Divisors de zero. Divisors.*

1) Elements invertibles. Divisors de zero.

   - El conjunt dels nombres enters amb la suma i el producte, $(\mathbb{Z}, +, \cdot)$, és un anell commutatiu sense divisors de zero i on els únics elements invertibles són 1 i -1.

2) Divisors.

   - Si $a, b \in \mathbb{Z}$, direm que a divideix b (o bé a és divisor de b, o bé b és múltiple de a) si existeix un enter $c \in Z$ tal que $b = a\,c$.
   - Si a divideix b, escriurem $a|b$.

≡ **Propietats** *Relació de divisibilitat.*

- Si a, b, c, r, s són enters qualssevol, aleshores:

1) $a|a$
2) $a|b\ ,\ b|c \Rightarrow a|c$
3) $a|b\ ,\ b|a \Rightarrow b = \pm a$
4) $a|b\ ,\ a|c \Rightarrow a|(b+c)$
5) $a|b \Rightarrow a|bc$
6) $a|b\ ,\ a|c \Rightarrow a|(br+cs)$
7) $a|b \Rightarrow \pm a| \pm b$
8) $a|b, b \neq 0 \Rightarrow |a| \leq |b|$

- Si n, d són enters ≥ 1, el nombre de múltiples de d entre 1 i n és la part entera inferior de $\frac{n}{d}$.

≡ **Teorema** *Teorema de la divisió euclidiana.*

- Si a, b són enters i $b \neq 0$, aleshores existeixen enters q i r únics tals que $a = bq + r$ amb $0 \leq r < |b|$. Els nombres q, r s'anomenen respectivament quocient i residu de la divisió entera de a entre b.

≡ **Observació** *Divisors i divisió.*

- Si a i b són enters i $b \neq 0$, aleshores $b|a$ si i només si el residu de fer la divisió entera de a entre b és 0.

Màxim comú divisor

≡ **Definicions** *Màxim comú divisor. Enters relativament primers.*

- Si a, b son enters, direm que un enter $d \geq 0$ és el màxim comú divisor de a i b si compleix les dues condicions següents:

  i) $d|a$, $d|b$.

  ii) si $d' \in \mathbb{Z}$ satisfà $d'|a$ i $d'|b$, aleshores $d'|d$.

- El màxim comú divisor de a i b es denota $\text{mcd}(a, b)$.

- Dos enters a, b són relativament primers si $\text{mcd}(a, b) = 1$.

≡ **Observació** *Definició equivalent de màxim comú divisor.*

1) Si $a = b = 0$, aleshores el màxim comú divisor de a i b és 0.

2) Si a, b son enters, no tots dos nuls, el màxim comú divisor de a i b és el més gran de tots els divisors comuns de a i b. És a dir, d és el màxim comú divisor de a i b si es compleixen les dues condicions següents:

   i) $d|a$, $d|b$.

   ii) si $d' \in \mathbb{Z}$ satisfà $d'|a$ i $d'|b$, aleshores $d' \leq d$.

≡ Propietats

Màxim comú divisor.

- Si a, b, r són enters, aleshores

  a) $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,a)$.

  b) $\mathrm{mcd}(a,b) = \mathrm{mcd}(\pm a, \pm b) = \mathrm{mcd}(|a|,|b|)$.

  c) $a|b \Leftrightarrow \mathrm{mcd}(a,b) = |a|$.

  d) $\mathrm{mcd}(a,b) = \mathrm{mcd}(a, b+ar)$, per a tot enter r.

  e) $\mathrm{mcd}(a,b) = \mathrm{mcd}(a,b+a) = \mathrm{mcd}(a,b-a) = \mathrm{mcd}(a,a-b)$.

≡ Identitat de Bézout i algorisme d'Euclides

1) Identitat de Bézout.

   - Si $\mathrm{mcd}(a,b) = d$, aleshores existeixen enters s, t tals que $as + bt = d$.
   - Els enters r, s de la identitat de Bézout no són únics.

2) Algorisme d'Euclides.

   - Considerem a, b enters tals que $a \geq b > 0$ i b no divideix a. Si fem successivament les divisions enteres següents fins obtenir residu 0:

$$\begin{aligned} a &= bq + r_0 \\ b &= r_0 q_0 + r_1 \\ r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\cdots\cdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n + 0, \end{aligned}$$

   aleshores $\mathrm{mcd}(a,b) = r_n$.

3) Càlcul del mcd i dels coeficients de la Identitat de Bézout.

   - Si a, b són enters tals que $a > b > 0$ i b no divideix a, considerem les divisions successives obtingudes a l'algorisme d'Euclides:

1	0	s_0	$-s_1$	$\cdots$	$(-1)^{n-2}s_{n-2}$	$(-1)^{n-1}s_{n-1}$	$(-1)^n s_n$
0	1	$-t_0$	t_1	$\cdots$	$(-1)^{n-1}t_{n-2}$	$(-1)^n t_{n-1}$	$(-1)^{n+1}t_n$
	q	q_0	q_1	$\cdots$	q_{n-2}	q_{n-1}	q_n
a	b	r_0	r_1	$\cdots$	r_{n-2}	r_{n-1}	r_n
r_0	r_1	r_2	r_3	$\cdots$	r_n	0	

   on:

$$\begin{aligned} &s_0 = 1 && t_0 = q \\ &s_1 = s_0\, q_0 = q_0 && t_1 = t_0\, q_0 + 1 = q\, q_0 + 1 \\ &s_i = s_{i-1}\, q_{i-1} + s_{i-2}, \text{ si } i \geq 2 && t_i = t_{i-1}\, q_{i-1} + t_{i-2}, \text{ si } i \geq 2 \end{aligned}$$

Aleshores,

$$\mathrm{mcd}(a,b) = r_n = a\,(-1)^n s_n + b\,(-1)^{n+1} t_n,$$

i en general, per a tot $i \geq 0$,

$$r_i = a\,(-1)^i s_i + b\,(-1)^{i+1} t_i\,.$$

≡ Propietats

Conseqüències de la Identitat de Bézout.

- Si a, b, r, s, $t \in \mathbb{Z}$, aleshores:

  a) $r|a, r|b \Rightarrow r|\,\mathrm{mcd}(a,b)$.

  b) $as + bt = 1 \Rightarrow \mathrm{mcd}(a,b) = 1$.

  c) $\mathrm{mcd}(a,b) = d \Rightarrow \mathrm{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

  d) $r > 0 \Rightarrow \mathrm{mcd}(ra, rb) = r\ \mathrm{mcd}(a,b)$.

  e) $a|bc$ i $\mathrm{mcd}(a,b) = 1 \Rightarrow a|c$.

≡ Equacions diofàntiques

Existència de solució i resolució.

1) Equacions diofàntiques.

   - Una equació diofàntica és una equació amb coeficients enters per a la qual només es permeten solucions enteres.

2) L'equació diofàntica $ax + by = c$, on $a, b, c \in \mathbb{Z}$.

   a) Existència de solucions.

      - L'equació diofàntica $ax + by = c$ té solució si, i només si, $\mathrm{mcd}(a,b)|c$.

   b) Càlcul d'una solució.

      - Sigui $d = \mathrm{mcd}(a,b)$ i suposem que $d|c$. Si s, t són enters tals que $d = as + bt$, llavors una solució de l'equació diofàntica $ax + by = c$ és (x_0, y_0), on:

$$x_0 = \frac{sc}{d} \quad , \quad y_0 = \frac{tc}{d}$$

   c) Càlcul de totes les solucions.

      - Sigui $d = \mathrm{mcd}(a,b)$ i suposem que $d|c$. Si (x_0, y_0) és una solució de l'equació diofàntica $ax + by = c$, aleshores totes les solucions de l'equació són (x, y) on:

$$x = x_0 + \frac{b}{d}\,\alpha \quad , \quad y = y_0 - \frac{a}{d}\,\alpha \quad , \quad \text{amb } \alpha \in \mathbb{Z}.$$

Factorització en nombres primers

≡ **Definició** *Nombre primer.*

- Un enter $p \geq 2$ és primer si els únics divisors positius de p són 1 i p.

≡ **Propietats** *Nombres primers.*

- Si p és primer i $a, b, a_1, \ldots, a_n \in \mathbb{Z}$, aleshores:

  a) $p|ab \Rightarrow p|a$ ó $p|b$.

  b) $p\Big|\prod_{i=1}^{n} a_i \Rightarrow \exists j,\ 1 \leq j \leq n$, tal que $p|a_j$.

  c) $p|a^n,\ n \geq 1 \Rightarrow p|a$ i $p^n|a^n$.

≡ **Teorema** *Teorema Fonamental de l'Aritmètica.*

- Tot enter $m \geq 2$ es pot expressar com a producte de nombres primers de forma única llevat de l'ordre dels factors. Per tant, es pot expressar de forma única com

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}$$

on $p_1 < p_2 < \cdots < p_k$ són primers i α_i enter positiu per a tot i.

≡ **Propietats** *Nombres primers.*

1) Hi ha infinits nombres primers.

2) Tot enter $n \geq 2$ no primer té almenys un factor primer $p \leq \sqrt{n}$.

3) El Garbell d'Eratóstenes permet generar la llista de nombres primers més petits que un nombre natural donat.

4) Hi ha 25 nombres primers més petits que 100 i són: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

5) El nombre primer més gran conegut a gener de 2013 és $2^{57885161} - 1$, que té 17425170 dígits decimals.

Mínim comú múltiple

≡ **Definició** *Mínim comú múltiple.*

- Si a, b son enters, direm que un enter $m \geq 0$ és el mínim comú múltiple de a i b si compleix les dues condicions següents:

  i) $a|m$, $b|m$.

  ii) si $m' \in \mathbb{Z}$ satisfà $a|m'$ i $b|m'$, aleshores $m|m'$.

- El mínim comú múltiple de a i b es denota $\text{mcm}(a, b)$.

≡ **Observació** *Definició equivalent de mínim comú múltiple.*

1) Si $a = 0$ o $b = 0$, aleshores el mínim comú múltiple de a i b és 0.

2) Si a, b son enters no nuls, el mínim comú múltiple de a i b és el menor de tots els múltiples positius comuns de a i b. És a dir, $m \geq 1$ és el mínim comú múltiple de a i b si es compleixen les dues condicions següents:

   i) $a|m$, $b|m$.

   ii) si $m' \geq 1$ és un enter que satisfà $a|m'$ i $b|m'$, aleshores $m \leq m'$.

≡ **Propietats** *Mínim comú múltiple.*

1) Si a, b són enters positius, $\text{mcd}(a, b) \cdot \text{mcm}(a, b) = a \cdot b$.

2) $a|r$, $b|r \Rightarrow \text{mcm}(a, b)|r$.

≡ **Proposició** *Màxim comú divisor, mínim comú múltiple i factorització en primers.*

1) Si $a = \prod_{i=1}^{k} p_i^{\alpha_i}$, on $p_1, \ldots, p_k$ són primers diferents dos a dos i α_i enter positiu per a tot $i \in \{1, \ldots, k\}$, aleshores:

   a) els divisors positius de a són de la forma $\prod_{i=1}^{k} p_i^{\beta_i}$, on $0 \leq \beta_i \leq \alpha_i$ per a tot $i \in \{1, \ldots, k\}$.

   b) a té exactament $\prod_{i=1}^{k} (\alpha_i + 1)$ divisors positius.

2) Si $a, b \geq 2$ són enters, aleshores podem escriure

$$a = \prod_{i=1}^{k} p_i^{\alpha_i} \ , \qquad b = \prod_{i=1}^{k} p_i^{\beta_i}$$

on $p_1, p_2, \ldots, p_k$ són els factors primers de a o de b, i per tant $\alpha_i \geq 0$, $\beta_i \geq 0$ per a tot $i \in \{1, 2, \ldots, k\}$ (és a dir, si un nombre primer no és factor de a o de b apareix amb exponent 0). Amb aquesta notació:

$$\mathrm{mcd}(a, b) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i\}} \ , \qquad \mathrm{mcm}(a, b) = \prod_{i=1}^{k} p_i^{\max\{\alpha_i, \beta_i\}}.$$

Congruències

≡ **Definició** *Relació de congruència.*

- Sigui $m > 0$ enter. Si $a, b \in \mathbb{Z}$, direm que a és congruent a b mòdul m si i només si $m|(b - a)$.
- Si a és congruent a b mòdul m escriurem $a \equiv b \pmod{m}$.

≡ **Propietats** *Relació de congruència.*

1) Les condicions següents són equivalents:
   - i) $m|(b - a)$.
   - ii) La divisió entera de a entre m i de b entre m dóna el mateix residu.
   - iii) $\{\, a + m\,k \,|\, k \in \mathbb{Z} \,\} = \{\, b + m\,k \,|\, k \in \mathbb{Z} \,\}$.
2) La relació de congruència mòdul m és relació d'equivalència. És a dir, si $a, b, c \in \mathbb{Z}$ aleshores:
   - a) $a \equiv a \pmod{m}$.
   - b) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.
   - c) $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.
3) La relació de congruència mòdul m és compatible amb la suma i producte. És a dir, si $a, a', b, b' \in \mathbb{Z}$ aleshores:
   - a) $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m} \Rightarrow a + a' \equiv b + b' \pmod{m}$.
   - b) $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m} \Rightarrow a\,a' \equiv b\,b' \pmod{m}$.
4) Siguin $r, s > 0$ enters. Si $a, b \in \mathbb{Z}$, aleshores:
   - a) $a \equiv b \pmod{m}$ i $r|m \Rightarrow a \equiv b \pmod{r}$.
   - b) $a \equiv b \pmod{r}$ i $a \equiv b \pmod{s} \Rightarrow a \equiv b \pmod{\mathrm{mcm}(a, b)}$.

c) $ra \equiv rb \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{\mathrm{mcd}(m,r)}}$.

≡ **Equacions amb congruències** *Existència de solucions i resolució.*

1) L'equació $a + x \equiv b \pmod{m}$ sempre té solució, i la solució és $x \equiv b - a \pmod{m}$.

2) L'equació $ax \equiv b \pmod{m}$.

   a) Existència de solució.

      - L'equació $ax \equiv b \pmod{m}$ té solució si i només si $\mathrm{mcd}(a,m)|b$.

   b) Càlcul d'una solució.

      - Sigui $d = \mathrm{mcd}(a,m)$ i $s,t \in \mathbb{Z}$ tals que $d = a\,s + m\,t$. Suposem que $d|b$. Una solució de l 'equació $ax \equiv b \pmod{m}$ és $x_0 = \frac{s\,b}{d}$

   c) Càlcul de totes les solucions.

      - Sigui $d = \mathrm{mcd}(a,m)$ i $s,t \in \mathbb{Z}$ tals que $d = a\,s + m\,t$. Suposem que $d|b$ i que x_0 és una solució de l'equació $ax \equiv b \pmod{m}$. Aleshores, el conjunt de totes les solucions de l'equació està format pels enters x tals que $x \equiv x_0 \pmod{\frac{m}{d}}$.

L'anell d'enters modulars

≡ **Definició** *L'anell* $(\mathbb{Z}_m, +, \cdot)$.

- Sigui $m \geq 2$ un enter.

1) El conjunt $\mathbb{Z}_m$ és el quocient de $\mathbb{Z}$ per la relació d'equivalència defiida per la congruència mòdul m. Per tant, $\mathbb{Z}_m$ té exactament m elements:

$$\mathbb{Z}_m = \{[a]_m : a \in \mathbb{Z}\} = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$$

   on $[a]_m$ és la classe de congruència de a mòdul m, és a dir:

$$[a]_m = \{b : b \equiv a \pmod{m}\} = \{a + km : k \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

2) La suma i el producte de $[a]_m, [b]_m \in \mathbb{Z}_m$ es defineixen de la forma següent:

$$[a]_m + [b]_m = [a+b]_m$$

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

3) Amb aquestes operacions, $(\mathbb{Z}_m, +, \cdot)$ és un anell commutatiu.

≡ **Proposició** *Elements invertibles i divisors de zero. Els cossos $\mathbb{Z}_p$.*

1) Un element $[a]_m \in \mathbb{Z}_m$ és invertible si i només si $\text{mcd}(a, m) = 1$.

2) Un element $[a]_m \in \mathbb{Z}_m$, $[a]_m \neq [0]_m$, és divisor de zero si i només si $\text{mcd}(a, m) \neq 1$.

3) Sigui $[a]_m \in \mathbb{Z}_m$, aleshores:

   a) Si $\text{mcd}(a, m) = m$, llavors $[a]_m = [0]_m$ no és ni invertible ni divisor de zero.

   b) Si $\text{mcd}(a, m) = 1$, llavors $[a]_m$ és invertible.

   c) Si $\text{mcd}(a, m) \neq 1, m$, llavors $[a]_m$ és divisor de zero.

4) L'anell $(\mathbb{Z}_m, +, \cdot)$ és un cos si i només si m és primer.

6.2 Exercicis i problemes. Enunciats

6.1 Doneu el quocient q i el residu r de la divisió entera de a entre b en els casos següents:

1) $a = 4073$, $b = 60$.
2) $a = 4073$, $b = -60$.
3) $a = -4073$, $b = 60$.
4) $a = -4073$, $b = -60$.
5) $a = 60$, $b = 4073$.
6) $a = 60$, $b = -4073$.
7) $a = -60$, $b = 4073$.
8) $a = -60$, $b = -4073$.

6.2 Calculeu el màxim comú divisor i la identitat de Bézout dels nombres enters a i b en els casos següents:

1) $a = 78$, $b = 32$.
2) $a = 273$, $b = -962$.
3) $a = 2097$, $b = 320$.
4) $a = -3399$, $b = -829$.
5) $a = 442$, $b = 3510$.
6) $a = -5935$, $b = 2105$.
7) $a = 243$, $b = 36936$.
8) $a = -152$, $b = 36936$.

6.3 Siguin a, b enters.

1) Demostreu que si $b|a$ aleshores $\mathrm{mcd}(a, b) = |b|$.
2) Calculeu:
   a) $\mathrm{mcd}(a, 1)$.
   b) $\mathrm{mcd}(a, ma)$, on $m \in \mathbb{Z}$.
   c) $\mathrm{mcd}(a, a^n)$, on $n \geq 1$.
   d) $\mathrm{mcd}(a, p)$, on p és un nombre primer.
   e) $\mathrm{mcd}(a + b, a^2 - b^2)$.
   f) $\mathrm{mcd}(a^2 - b^2, a^4 - b^4)$.

6.4 Descomponeu en producte de primers els nombres següents:

1) 167706000. 2) 382836861. 3) 5767. 4) 29947.

6.5 Calculeu el màxim comú divisor i el mínim comú múltiple dels nombres enters a i b en els casos següents:

1) $a = 2013^{2013}$, $b = 2013$. 2) $a = 2426806849$, $b = 120$. 3) $a = 2^4\, 3^{50}\, 11^{20}$, $b = 123453$.

6.6 Resolució d'*equacions diofàntiques*.

1) Siguin $a, b, c \in \mathbb{Z}$. Considerem l'equació $a\,x + b\,y = c$, on $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.
   a) Demostreu que l'equació té solució si i només si $\mathrm{mcd}(a, b)|c$.

b) Utilitzeu la identitat de Bézout per calcular una solució si $\mathrm{mcd}(a,b)|c$.

c) Demostreu que si (x_0, y_0) és una solució, aleshores el conjunt de totes les solucions és:

$$\left\{\left(x_0 + \frac{b}{d}\,t, y_0 - \frac{a}{d}\,t\right) : t \in \mathbb{Z}\right\}$$

on $d = \mathrm{mcd}(a,b)$.

2) Calculeu totes les solucions enteres de les equacions següents:

a) $2013x + 2014y = 1$.

b) $1915x + 2177y = -11$.

c) $390x - 462y = 6$.

d) $5935x - 2105y = 15$.

e) $1526x - 1071y = 10$.

6.7 Descomponeu de totes les maneres possibles el nombre racional $230/247$ com a suma de dues fraccions positives de denominadors 19 i 13.

6.8 Considerem nombres enters a, b, r, s, d qualssevol amb $d > 0$.

1) Demostreu que si $ar + bs = 1$, aleshores $\mathrm{mcd}(a,b) = \mathrm{mcd}(a,s) = \mathrm{mcd}(r,s) = \mathrm{mcd}(r,b) = 1$.

2) Suposem que $ar + bs = d$. Podem deduir que $\mathrm{mcd}(a,b)|d$? Podem deduir que $\mathrm{mcd}(a,b) = d$?

3) Suposem que $ar + bs = d$. Podem deduir que $\mathrm{mcd}(a,b) = \mathrm{mcd}(a,s) = \mathrm{mcd}(r,s) = \mathrm{mcd}(r,b)$? Podem deduir que algun d'aquests quatre màxims comuns divisors és d? És possible que els quatre valors siguin diferents i a més diferents de d?

4) Suposem que $ar + bs = d$. Demostreu que si $\mathrm{mcd}(a,b) = d$, aleshores $\mathrm{mcd}(r,s) = 1$. És cert el recíproc?

6.9

1) Demostreu que per a enters a, b, m qualssevol, $\mathrm{mcd}(a,b) = \mathrm{mcd}(a, b + am)$.

2) Calculeu el màxim comú divisor dels parells d'enters següents:

a) $\mathrm{mcd}(a, a+1)$, per a tot enter a.

b) $\mathrm{mcd}(a, a+2)$, per a tot enter a.

c) $\mathrm{mcd}(a, a+p)$, per a tot enter a, on p és un nombre primer.

d) $\mathrm{mcd}(2a+5, 3a+7)$, per a tot enter a.

e) $\mathrm{mcd}(F_n, F_{n+1})$, per a tot enter $n \geq 1$, on F_n és el terme general de la successió de Fibonacci $(F_n)_{n\geq 1}$ definida recursivament com la successió tal que $F_1 = 1$, $F_2 = 1$ i $F_n = F_{n-1} + F_{n-2}$ si $n \geq 3$.

3) Demostreu que per a tot nombre enter n, la fracció $\dfrac{2n+3}{4n+5}$ és irreductible.

4) Calculeu el màxim comú divisor i el mínim comú múltiple de $a = 2426806849$ i $b = 2426806841$.

6.10 Determineu tots els parells de nombres enters positius a, b tals que $a + b = 57$ i $\mathrm{mcm}(a,b) = 680$.

6.11

1) Calculeu el nombre de divisors positius de 675.
2) Doneu una fórmula per calcular el nombre de divisors positius d'un nombre a partir de la seva descomposició en factors primers.
3) Quin és el menor nombre natural tal que té exactament 10 divisors positius?

6.12 Demostreu que si $m \geq 2$, $n \geq 1$ i $p_1, p_2, \ldots, p_n$ són nombres primers diferents, aleshores el nombre $\sqrt[m]{\prod_{i=1}^{n} p_i}$ no és racional.

6.13 Un nombre és perfecte si és igual a la suma de tots els seus divisors excepte ell mateix.

1) Comproveu que 6 i 28 són perfectes.
2) Demostreu que $2^n - 1$ és primer si i només si $2^{n-1}(2^n - 1)$ és un nombre perfecte.

6.14

1) Demostreu que si $2^n - 1$ és primer, aleshores n és primer. És cert el recíproc?
2) Demostreu que si $2^n + 1$ és primer, aleshores n és potència de 2. És cert el recíproc?

6.15

1) Demostreu que si $a_1, a_2, \ldots, a_n$ són nombres naturals més grans que 1, aleshores per a tot $i \in \{1, 2, \ldots, n\}$ el nombre $\left(\prod_{k=1}^{n} a_k\right) + a_i$ no és primer.
2) Demostreu que per a tot nombre natural n, $n \geq 1$, existeixen n nombres consecutius no primers.

6.16 Determineu si es compleixen les congruències següents:

1) $153 \equiv 123 \pmod{10}$.
2) $153 \equiv 123 \pmod{5}$.
3) $153 \equiv 123 \pmod{2}$.
4) $153 \equiv -123 \pmod{10}$.
5) $153 \equiv -123 \pmod{5}$.
6) $153 \equiv -123 \pmod{2}$.

6.17 Calculeu tots els nombres naturals m tals que $91 \equiv 217 \pmod{m}$.

6.18

1) Doneu tots els elements invertibles i tots els divisors de zero de $\mathbb{Z}_{15}$.
2) Doneu tots els elements invertibles i tots els divisors de zero de $\mathbb{Z}_{19}$.

6.19 Doneu les solucions de les equacions següents:

1) $42x - 13 \equiv 0 \pmod{73}$.
2) $17x + 12 \equiv 0 \pmod{23}$.
3) $44x - 9 \equiv 0 \pmod{72}$.
4) $44x - 8 \equiv 0 \pmod{72}$.

6.20

1) Demostreu que $7^n \equiv 7^r \pmod{10}$ si i només si $n \equiv r \pmod{4}$.
2) Determineu el darrer dígit de la representació decimal de 7^{94}.

6.21

1) Demostreu que $2^n \equiv 2^r \pmod{7}$ si i només si $n \equiv r \pmod{3}$.
2) Calculeu $1 + 2^n + 2^{2n}$ mòdul 7, on n és un nombre natural qualsevol.

6.22 Doneu i demostreu criteris de divisibilitat per 2, 3, 4, 5, 8, 9, 10 i 11.

6.23

1) Calculeu els quadrats dels elements de $\mathbb{Z}_4$ i de $\mathbb{Z}_8$.
2) Calculeu les arrels quadrades de 1 i 3 en $\mathbb{Z}_8$.
3) Demostreu:
   a) Si $m \equiv 7 \pmod{8}$, aleshores m no pot ser suma de tres quadrats.
   b) La suma de 4 nombres naturals consecutius no pot ser quadrat perfecte. Es pot obtenir un quadrat perfecte al sumar dos o tres nombres naturals consecutius?
   c) La suma dels quadrats de 5 nombres naturals consecutius no pot ser quadrat perfecte.

6.24

1) Demostreu que si $n > 4$ és un nombre natural no primer, aleshores $(n-1)! \equiv 0 \pmod{n}$.
2) Demostreu que si $n > 1$ és un nombre natural, aleshores $(n-1)! \equiv -1 \pmod{n}$ si i només si n és primer. (Teorema de Wilson).

6.25 Suposem que a, b són nombres enters qualssevol.

1) Demostreu que si p és primer, aleshores en $\mathbb{Z}_p$ es satisfan les igualtats següents:
   a) $\binom{p}{k} = 0$, si $k = 1, \ldots, p-1$.
   b) $(a+b)^p = a^p + b^p$.
   c) $a^p = a$. (Petit Teorema de Fermat).
2) Són certs els resultats anteriors si p no és primer?

6.26 Calculeu el residu de la divisió de 2012^{2012} entre 23.

6.27 Demostreu que si $a, b, m \in \mathbb{Z}$ i $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ és la descomposició en factors primers d'un nombre natural $n \geq 2$, aleshores:

1) $a \equiv b \pmod{\text{mcm}(m,n)} \iff \begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases}$

2) $a \equiv b \pmod{n} \iff \begin{cases} a \equiv b \pmod{p_1^{\alpha_1}} \\ a \equiv b \pmod{p_2^{\alpha_2}} \\ \cdots\cdots\cdots \\ a \equiv b \pmod{p_k^{\alpha_k}} \end{cases}$

6.28 Calculeu el mínim nombre enter positiu a tal que $1001x + 770y = 10^{360} + a$ tingui solució.

6.29 Demostreu que si n és senar i no divisible per 3, aleshores $n^2 \equiv 1 \pmod{24}$.

6.30 Determineu tots els nombres enters n tals que $n^{13} \equiv n \pmod{1365}$.

6.31 Siguin $a, b, m, n \in \mathbb{Z}$. Considerem el sistema:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

1) Demostreu que té solució en $\mathbb{Z}$ si i només si $a \equiv b \pmod{d}$, on $d = \text{mcd}(m,n)$.

2) Demostreu que si té solució, aleshores és única mòdul $\text{mcm}(m,n)$.

3) Justifiqueu que si m i n són relativament primers, aleshores el sistema sempre té solució en $\mathbb{Z}$ i és única mòdul mn. (Teorema xinès de la resta.)

6.32 Resoleu els sistemes de congruències següents:

1) $\begin{cases} x \equiv 3 \pmod{10} \\ x \equiv 4 \pmod{21} \end{cases}$

2) $\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 3 \pmod{6} \end{cases}$

3) $\begin{cases} x \equiv 4 \pmod{10} \\ x \equiv 3 \pmod{6} \end{cases}$

4) $\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{6} \\ x \equiv 1 \pmod{5} \end{cases}$

6.33 Discutiu si els sistemes d'equacions lineals següents tenen solució en $\mathbb{Z}$, $\mathbb{Z}_3$ i $\mathbb{Z}_5$:

1) $\begin{cases} 2x - y = 1 \\ x + y = 1 \end{cases}$

2) $\begin{cases} x + z = 2 \\ x + y + 2z = 2 \\ 2x + y = 1 \end{cases}$

3) $\begin{cases} x + z = 1 \\ x + y = 1 \\ 2x + y + z = 2 \end{cases}$

6.3 Exercicis i problemes. Solucions

6.1

1) $q = 67$, $r = 53$.
2) $q = -67$, $r = 53$.
3) $q = -68$, $r = 7$.
4) $q = 68$, $r = 7$.
5) $q = 0$, $r = 60$.
6) $q = 0$, $r = 60$.
7) $q = -1$, $r = 4013$.
8) $q = 1$, $r = 4013$.

6.2

1) $\mathrm{mcd}(a, b) = 2 = 7a + (-17)b$.
2) $\mathrm{mcd}(a, b) = 13 = (-7)a + (-2)b$.
3) $\mathrm{mcd}(a, b) = 1 = (-47)a + 308b$.
4) $\mathrm{mcd}(a, b) = 1 = (-10)a + 41b$.
5) $\mathrm{mcd}(a, b) = 26 = 8a + (-1)b$.
6) $\mathrm{mcd}(a, b) = 5 = (-72)a + (-203)b$.
7) $\mathrm{mcd}(a, b) = 243 = a + 0 \cdot b$.
8) $\mathrm{mcd}(a, b) = 152 = (-1)a + 0 \cdot b$.

6.3

2) a) 1.
   b) $|a|$.
   c) $|a|$.
   d) p, si a és múltiple de p; 1, altrament.
   e) $|a + b|$.
   f) $|a^2 - b^2|$.

6.4

1) $2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11^3$.
2) $3^4 \cdot 11^3 \cdot 53 \cdot 67$.
3) $73 \cdot 79$.
4) 29947.

6.5

1) $\mathrm{mcd}(a, b) = b = 2013$, $\mathrm{mcm}(a, b) = a$.
2) $\mathrm{mcd}(a, b) = 1$, $\mathrm{mcm}(a, b) = ab$.
3) $\mathrm{mcd}(a, b) = 99$, $\mathrm{mcm}(a, b) = ab/99$.

6.6

2) Les solucions de les equacions són els parells $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ de la forma:
   a) $(x, y) = (-1 + 2014\,t, 1 - 2013\,t)$, on $t \in \mathbb{Z}$.

b) $(x, y) = (-5027 + 2177\,t, 4422 - 1915\,t)$, on $t \in \mathbb{Z}$.

c) $(x, y) = (32 + 77\,t, 27 + 65\,t)$, on $t \in \mathbb{Z}$.

d) $(x, y) = (216 + 421\,t, 609 + 1187\,t)$, on $t \in \mathbb{Z}$.

e) No té solucions enteres.

6.7 Només hi ha una solució: $\dfrac{230}{247} = \dfrac{6}{19} + \dfrac{8}{13}$.

6.8

2) Sí. No. 3) No. No. Sí. 4) −. No.

6.9

2) a) 1.

b) 1, si a és senar; 2, si a és parell.

c) p, si a és múltiple de p; 1, altrament.

d) 1.

e) 1.

4) $\mathrm{mcd}(a, b) = 1$, $\mathrm{mcm}(a, b) = ab$.

6.10 $\{a, b\} = \{17, 40\}$.

6.11

1) 675 té 12 divisors positius.

2) Si $N = \prod_{i=1}^{r} p_i^{\alpha_i}$, on $p_1, \ldots, p_r$ són primers diferents i $\alpha_1, \ldots, \alpha_r \geq 1$, aleshores N té exactament $\prod_{i=1}^{r} (\alpha_i + 1)$ divisors positius.

3) 48.

6.14

1) Indicació: utilitzeu la identitat $x^m - 1 = (x - 1)(1 + x + x^2 + x^3 + \cdots + x^{m-1})$. El recíproc no és cert.

2) Indicació: utilitzeu la identitat $x^m + 1 = (x + 1)(1 - x + x^2 - x^3 + x^4 - \cdots + x^{m-1})$, si m és senar. El recíproc no és cert.

6.16

1) Sí. 2) Sí. 3) Sí. 4) No. 5) No. 6) Sí.

6.17 1, 2, 3, 6, 7, 9, 14, 18, 21, 42, 63, 126.

6.18

1) Les classes de 1, 2, 4, 7, 8, 11, 13, 14 són invertibles. Les classes de 3, 5, 6, 9, 10, 12 són divisors de zero.

2) Tots els elements no nuls són invertibles. No té divisors de zero.

6.19

1) $x \equiv 9 \pmod{73}$.

2) $x \equiv 2 \pmod{23}$.

3) No té solució.

4) $x \equiv 10 \pmod{18}$, o bé $x \equiv 10, 28, 46, 64 \pmod{72}$.

6.20

2) 9.

6.21

2) 3, si n és múltiple de 3; 0, si n no és múltiple de 3.

6.22 Un enter és divisible per:

2, si l'última xifra és parella;

3, si la suma de les xifres és múltiple de 3;

4, si el nombre format per les dues últimes xifres és múltiple de 4;

5, si l'última xifra és 0 o 5;

8, si el nombre format per les tres últimes xifres és múltiple de 8; o bé la suma de la xifra de les unitats, més dues vegades la de les desenes, més quatre vegades la de les centenes és múltiple de 8.

9, si la suma de les xifres és múltiple de 9;

10, si l'última xifra és 0;

11, si la suma de les xifres que ocupen un lloc senar menys la suma de les xifres que ocupen un lloc parell, és múltiple de 11.

6.23

1) Els quadrats dels elements de $\mathbb{Z}_4$ són 0 i 1; els de $\mathbb{Z}_8$ són 0, 1 i 4.

2) Les arrels quadrades de 1 són 1, 3, 5 i 7. La classe de 3 no té cap arrel quadrada.

6.26 2.

6.28 76.

6.30 Tots els enters satisfan la congruència.

6.32

1) $x \equiv 193 \pmod{210}$.

2) $x \equiv 27 \pmod{30}$.

3) No té solució.

4) $x \equiv 101 \pmod{210}$.

6.33

1) El sistema és incompatible en $\mathbb{Z}_3$. En $\mathbb{Z}_5$ el sistema compatible determinat i la solució és $x = 4$, $y = 2$.

2) En $\mathbb{Z}_3$ el sistema és compatible indeterminat i la solució és $x = 2 + 2t$, $y = 2t$, $z = t$, on $t \in \mathbb{Z}_3$. En $\mathbb{Z}_5$ el sistema és compatible determinat i la solució és $x = 1$, $y = 4$, $z = 1$.

3) En $\mathbb{Z}_3$ el sistema és compatible indeterminat i la solució és $x = 1 + 2t$, $y = t$, $z = t$, on $t \in \mathbb{Z}_3$. En $\mathbb{Z}_5$ el sistema és compatible indeterminat i la solució és $x = 1 + 4t$, $y = t$, $z = t$, on $t \in \mathbb{Z}_5$.

7
Polinomis

7.1 Resum teòric

Definicions i operacions

– **Comentari**

- Els polinomis es poden considerar amb coeficients en un anell commutatiu o en un cos commutatiu. En aquest capítol, si no es diu el contrari, es consideren polinomis sobre un cos commutatiu $\mathbb{K}$.

≡ **Definició** *Polinomi amb una indeterminada.*

- Sigui $(\mathbb{K}, +, \cdot)$ un cos commutatiu. Definim el conjunt $\mathbb{K}[x]$ dels polinomis amb coeficients en el cos $\mathbb{K}$ i amb indeterminada x com el conjunt que té com elements expressions formals del tipus $p = \sum_{i \geq 0} a_i x^i$ verificant:
  - Per a tot natural $i \geq 0$ es té que $a_i \in \mathbb{K}$.
  - Existeix un natural $n \geq 0$ tal que $a_i = 0$ si $i > n$.
- Si $p = \sum_{i \geq 0} a_i x^i \in \mathbb{K}[x]$ és un polinomi amb coeficients en el cos $\mathbb{K}$ i amb indeterminada x aleshores:
  - Direm que a_i és el coeficient del terme de grau i del polinomi p. El coeficient del terme de grau zero s'anomena el terme independent del polinomi p.

- Direm que p és un polinomi no nul si existeix $i \geq 0$ de manera que $a_i \neq 0$.
- Direm que p és un polinomi constant si $a_i = 0$ per a tot $i > 0$.
- Si p és no nul, aleshores definim el grau de p com $\deg(p) = \max\{i \geq 0 \text{ tals que } a_i \neq 0\}$. És a dir, $\deg(p) = n$ si i només si $p = \sum_{i=0}^{n} a_i x^i$ amb $a_n \neq 0$. En aquest cas direm que a_n és el coeficient dominant del polinomi p.
- Direm que p és un polinomi mònic si és no nul i el seu coeficient dominant és 1.

≡ **Observació** *Igualtat de polinomis.*

- Dos polinomis $p, q \in \mathbb{K}[x]$ són iguals si i només si tenen el mateixos coeficients. És a dir, si $p = \sum_{i\geq 0} a_i x^i$ i si $q = \sum_{i\geq 0} b_i x^i$, aleshores $p = q$ si i només si $a_i = b_i$ per a tot $i \geq 0$.

≡ **Definició** *Suma i producte de polinomis.*

- Definim la suma $p + q$ de dos polinomis $p = \sum_{i\geq 0} a_i x^i \in \mathbb{K}[x]$ i $q = \sum_{i\geq 0} b_i x^i \in \mathbb{K}[x]$ com el polinomi $p + q = \sum_{i\geq 0}(a_i + b_i)x^i \in \mathbb{K}[x]$.
- Definim el producte pq de dos polinomis $p = \sum_{i\geq 0} a_i x^i \in \mathbb{K}[x]$ i $q = \sum_{i\geq 0} b_i x^i \in \mathbb{K}[x]$ com el polinomi $pq = \sum_{i\geq 0} c_i x^i \in \mathbb{K}[x]$ on $c_i = \sum_{k=0}^{i} a_k b_{i-k}$ per a tot $i \geq 0$.

≡ **Propietats** *Propietats de les operacions. Estructura algebraica.*

1) La suma i el producte de polinomis són operacions internes en $\mathbb{K}[x]$.
2) Comportament del grau.
   - Si $p, q \in \mathbb{K}[x]$ aleshores $\deg(p + q) \leq \max\{\deg(p), \deg(q)\}$.
   - Si $p, q \in \mathbb{K}[x]$ aleshores $\deg(pq) = \deg(p) + \deg(q)$.
3) Amb aquestes operacions es té que $(\mathbb{K}[x], +, \cdot)$ és un anell commutatiu però no és cos.
   - L'element neutre de la suma de $\mathbb{K}[x]$ és el 0, i l'element neutre del poducte és 1.
   - Si $p = \sum_{i\geq 0} a_i x^i \in \mathbb{K}[x]$ és un polinomi, aleshores $-p = \sum_{i\geq 0}(-a_i)x^i \in \mathbb{K}[x]$.
   - Si $p = \sum_{i\geq 0} a_i x^i \in \mathbb{K}[x]$ és un polinomi, aleshores p té invers respecte del producte si i només si $a_0 \neq 0$ i $a_i = 0$ per a $i > 0$. En aquest cas, $p^{-1} = a_0^{-1}$.
4) L'anell dels polinomis $\mathbb{K}[x]$ és una extensió del cos $\mathbb{K}$.
   - Concretament es té que $\mathbb{K} \subseteq \mathbb{K}[x]$ identificant un element λ del cos $\mathbb{K}$ amb el polinomi constant $\lambda \in \mathbb{K}[x]$.
   - Amb aquesta identificació es té que si $p = \sum_{i\geq 0} a_i x^i \in \mathbb{K}[x]$ i si $\lambda \in \mathbb{K}$ aleshores podem considerar el polinomi $\lambda + p \in \mathbb{K}[x]$ on $\lambda + p = (a_0 + \lambda) + \sum_{i\geq 1} a_i x^i \in \mathbb{K}[x]$, i també podem considerar el polinomi $\lambda p \in \mathbb{K}[x]$ on $\lambda p = \sum_{i\geq 0}(\lambda a_i)x^i \in \mathbb{K}[x]$.
   - Un polinomi $p \in \mathbb{K}[x]$ té invers respecte del producte si i només si $p \in \mathbb{K} - \{0\}$.

Divisió euclidiana i factorització

≡ **Teorema** *Teorema de la divisió euclidiana.*

- Siguin $p, q \in \mathbb{K}[x]$ dos polinomis. Suposem que q és no nul. Aleshores existeixen uns únics polinomis $c, r \in \mathbb{K}[x]$ de manera que $p = cq + r$ amb $r = 0$ o $0 \leq \deg(r) < \deg(q)$. Direm que c és el quocient de la divisió de p per q i que r és la resta de la divisió de p per q.

≡ **Definició** *Divisors d'un polinomi. Polinomis primers o irreductibles. Polinomis associats.*

- Siguin $p, q \in \mathbb{K}[x]$ dos polinomis. Direm que el polinomi q és un divisor del polinomi p, (o que q divideix p, o que p és un múltiple de q), si i només si existeix un polinomi $c \in \mathbb{K}[x]$ tal que $p = cq$. Notarem $q|p$.
- Sigui $p \in \mathbb{K}[x]$ un polinomi no nul i no constant. Direm que p és un polinomi primer o irreductible en $\mathbb{K}[x]$ si no té més divisors que els trivials. És a dir, si i només si els únics divisors que té p són els polinomis $q \in \mathbb{K}[x]$ del tipus $q = \lambda$ o $q = \lambda p$ amb $\lambda \in \mathbb{K} - \{0\}$.
- Siguin $p, q \in \mathbb{K}[x]$. Direm que els polinomis p, q són associats si existeix $\mu \in \mathbb{K} - \{0\}$ tal que $q = \mu\, p$.

≡ **Observacions** *Propietats dels polinomis primers.*

1) Els polinomis de grau 1 són polinomis primers. És a dir, si $\alpha, \beta \in \mathbb{K}$ amb $\alpha \neq 0$, aleshores el polinomi $\alpha x - \beta \in \mathbb{K}[x]$ és un polinomi primer de $\mathbb{K}[x]$.
2) Si $p \in \mathbb{K}[x]$ és un polinomi primer en $\mathbb{K}[x]$, aleshores per a tot $\mu \in \mathbb{K} - \{0\}$ es té que el polinomi μp també és un polinomi primer en $\mathbb{K}[x]$.
3) En particular, si $p \in \mathbb{K}[x]$ és un polinomi no nul i no constant, aleshores p és un polinomi primer de $\mathbb{K}[x]$ si i només si ho és el seu normalitzat. És a dir, p és primer si i només si ho és el polinomi $a_n^{-1} p$, on a_n és el coeficient dominant de p.

≡ **Teorema** *Teorema de descomposició factorial.*

- Sigui $p \in \mathbb{K}[x]$ un polinomi no nul i no constant. Aleshores podem factoritzar p de manera única llevat de l'ordre dels factors:

$$p = a p_1^{m_1} \cdot \ldots \cdot p_r^{m_r},$$

on $a \in \mathbb{K} - \{0\}$, i $p_1, \ldots, p_r \in \mathbb{K}[x]$ són polinomis primers, mònics i diferents dos a dos, amb $m_1, \ldots, m_r \geq 1$ naturals. Direm que $a p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$ és la descomposició factorial de p en $\mathbb{K}[x]$, que els polinomis $p_1, \ldots, p_r$ són els factors primers de p en $\mathbb{K}[x]$, i que el natural m_i és la multiplicitat del factor primer p_i.

≡ **Observacions** *Propietats de la descomposició factorial i dels factors primers.*

1) Sigui $p \in \mathbb{K}[x]$ un polinomi no nul i no constant. Si $p = ap_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$ és la descomposició factorial de p en $\mathbb{K}[x]$ aleshores, $\deg(p) = \sum_{i=1}^{r} m_i \deg(p_i)$ i a és el coeficient dominant de p.

2) Si q és un polinomi primer mònic de $\mathbb{K}[x]$ aleshores, q és un factor primer del polinomi p en $\mathbb{K}[x]$ si i només si $q|p$.

3) Si q és un polinomi primer mònic de $\mathbb{K}[x]$ aleshores, q és un factor primer del polinomi p en $\mathbb{K}[x]$ de multiplicitat m si i només si $q^m | \, p$ i $q^{m+1} \not| \, p$.

≡ **Definició** *Màxim comú divisor.*

- Siguin $p, q, d \in \mathbb{K}[x]$. Direm que el polinomi d és un màxim comú divisor dels polinomis p i q si i només si $d|p$, $d|q$ i si $d' \in \mathbb{K}[x]$ és un polinomi tal que $d'|p$, $d'|q$, aleshores $d'|d$.

- Denotarem amb $\mathrm{mcd}(p, q)$ qualsevol màxim comú divisor de p i q.

≡ **Observacions** *Màxim comú divisor.*

1) Si d és un màxim comú divisor dels polinomis p i q, aleshores un polinomi d' també és un màxim comú divisor de p i q si i només si existeix $\lambda \in \mathbb{K} - \{0\}$ tal que $d' = \lambda\, d$.

2) Si $p \neq 0$ o $q \neq 0$, aleshores existeix un únic polinomi mònic que és màxim comú divisor dels polinomis p i q.

3) Siguin $p, q, d \in \mathbb{K}[x]$. Si $p \neq 0$ o $q \neq 0$, el polinomi d és un màxim comú divisor dels polinomis p i q si i només si $d|p$, $d|q$ i si $d' \in \mathbb{K}[x]$ és un polinomi tal que $d'|p$, $d'|q$, aleshores $\deg(d') \leq \deg(d)$.

4) Si $p = q = 0$, aleshores el màxim comú divisor de p i q és el polinomi 0.

≡ **Propietats** *Algorisme d'Euclides i identitat de Bézout.*

1) Identitat de Bézout.

   - Si d és un màxim comú divisor de $p, q \in \mathbb{K}[x]$, aleshores existeixen polinomis $s, t \in \mathbb{K}[x]$ tals que $ps + qt = d$.
   - Els polinomis $s, t \in \mathbb{K}[x]$ de la identitat de Bézout no són únics.

2) Algorisme d'Euclides.

- Siguin $p, q \in \mathbb{K}[x]$ dos polinomis no nuls. Fem les divisions euclidianes successives fins obtenir residu 0:

$$\begin{aligned} p &= qc + r_0 \\ q &= r_0c_0 + r_1 \\ r_0 &= r_1c_1 + r_2 \\ r_1 &= r_2c_2 + r_3 \\ &\cdots\cdots \\ r_{n-2} &= r_{n-1}c_{n-1} + r_n \\ r_{n-1} &= r_nc_n + 0, \end{aligned}$$

on $\deg(r_n) < \deg(r_{n-1}) < \cdots < \deg(r_2) < \deg(r_1) < \deg(r_0) < \deg(q)$. Aleshores, $\mathrm{mcd}(p, q) = r_n$.

3) Càlcul dels coeficients de la identitat de Bézout.

- Es poden obtenir amb el mateix mètode que hem descrit per a obtenir la Identitat de Bézout per a nombres enters.

Funcions polinomials i arrels

≡ **Definició** *Funció polinomial.*

- Donat un polinomi $p = \sum_{i\geq 0} a_i x^i \in \mathbb{K}[x]$, podem considerar la seva funció polinomial associada $p : \mathbb{K} \to \mathbb{K}$ definida per $p(\alpha) = \sum_{i\geq 0} a_i \alpha^i$ si $\alpha \in \mathbb{K}$.

≡ **Propietats** *Propietats de la funció polinomial.*

1) Funció polinomial i elements neutres.

- Si $p \in \mathbb{K}[x]$ és un polinomi aleshores $p(0)$ és el terme independent del polinomi p, i $p(1)$ és la suma dels coeficients del polinomi p.

2) Funció polinomial i operacions de polinomis.

- Si $p, q \in \mathbb{K}[x]$ i si $\alpha \in \mathbb{K}$ aleshores: $(p + q)(\alpha) = p(\alpha) + q(\alpha)$, $(pq)(\alpha) = p(\alpha)q(\alpha)$.

3) Funció polinomial i igualtat de polinomis.

- Si $\mathbb{K}$ és un cos infinit, aleshores dos polinomis $p, q \in \mathbb{K}[x]$ són iguals si i només si defineixen la mateixa funció polinòmica. És a dir, $p = q$ si i només si $p(\alpha) = q(\alpha)$ per a tot $\alpha \in \mathbb{K}$.

4) Funció polinomial i divisió euclidiana.

   - Si $p \in \mathbb{K}[x]$ és un polinomi i $\alpha \in \mathbb{K}$ és un element del cos, aleshores la resta de la divisió de p per $x - \alpha$ és $p(\alpha)$.
   - En particular, si $\alpha \in \mathbb{K}$ aleshores $p(\alpha) = 0$ si i només si existeix un polinomi $q \in \mathbb{K}[x]$ tal que $p = (x - \alpha)q$.

≡ **Definició** *Arrel d'un polinomi. Arrel simple i múltiple. Multiplicitat d'una arrel.*

- Sigui $p \in \mathbb{K}[x]$ un polinomi. Direm que un element $\alpha \in \mathbb{K}$ és un zero o una arrel del polinomi p si $p(\alpha) = 0$. Per tant, $\alpha \in \mathbb{K}$ és una arrel del polinomi $p \in \mathbb{K}[x]$ si i només si existeix un polinomi $q \in \mathbb{K}[x]$ tal que $p = (x - \alpha)q$.
- Direm que α és una arrel simple del polinomi p si $p = (x - \alpha)q$ amb $q(\alpha) \neq 0$. Direm que α és una arrel múltiple del polinomi p si $p = (x - \alpha)q$ amb $q(\alpha) = 0$.
- Direm que α és una arrel de p de multiplicitat m si $p = (x - \alpha)^m q$ amb $q(\alpha) \neq 0$.

≡ **Observacions** *Arrels d'un polinomi.*

1) Si $p \in \mathbb{K}[x]$ és un polinomi de grau $n \geq 1$ aleshores p té, com a màxim n arrels.
2) La suma de les multiplicitats de les arrels de p és menor o igual que el grau del polinomi.
3) Si $\alpha \in \mathbb{K}$ aleshores, $x - \alpha$ és un factor primer del polinomi p en $\mathbb{K}[x]$ si i només si $p(\alpha) = 0$. És a dir, si i només si α és una arrel o zero de p.
4) Sigui $\alpha \in \mathbb{K}$. Aleshores, $x - \alpha$ és un factor primer del polinomi p en $\mathbb{K}[x]$ de multiplicitat m si i només si $p = (x - \alpha)^m q$ amb $q \in \mathbb{K}[x]$ tal que $q(\alpha) \neq 0$. És a dir, si i només si α és una arrel o zero de p de multiplicitat m.

≡ **Observacions** *Arrels i polinomis primers.*

1) Si un polinomi $p \in \mathbb{K}[x]$ de grau $n \geq 2$ té una arrel, aleshores p no és primer.
2) El recíproc del resultat anterior és fals en general. És a dir, hi ha polinomis no primers de grau $n \geq 2$ que no tenen arrels.
3) Si $p \in \mathbb{K}[x]$ és un polinomi de grau 2 o 3, aleshores p és primer si i només si p no té arrels.
4) Si $p \in \mathbb{K}[x]$ és un polinomi de grau ≥ 4 primer, aleshores p no té arrels.
5) El recíproc de la propietat anterior no és cert: existeixen polinomis de grau ≥ 4 que no tenen arrels i no són primers.

Polinomis amb coeficients reals i complexos

≡ **Proposició** *Propietats dels polinomis amb coeficients reals.*

1) Sigui $p \in \mathbb{R}[x]$ un polinomi no nul i no constant amb coeficients en $\mathbb{R}$ i sigui $\alpha \in \mathbb{C}$ un nombre complex no real. Aleshores:

   - La funció polinomial commuta amb la conjugació. És a dir, $p(\overline{\alpha}) = \overline{p(\alpha)}$.
   - Si α és una arrel del polinomi p de multiplicitat m, aleshores el conjugat $\overline{\alpha} \in \mathbb{C}$ també és arrel de p de multiplicitat m.

2) Sigui $\alpha \in \mathbb{C}$ un nombre complex no real. Aleshores:

   - El polinomi $(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}$ és un polinomi amb coeficients reals i no té arrels reals.

3) Sigui $p \in \mathbb{R}[x]$ un polinomi no nul i no constant i sigui $\alpha \in \mathbb{C}$ un nombre complex no real.

   - Si α és una arrel de p de multiplicitat m, aleshores existeix un polinomi $q \in \mathbb{R}[x]$ de manera que $p = (x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha})^m q$ amb $q(\alpha) \neq 0$.

4) Polinomis amb coeficients reals de grau senar.

   - Si $p \in \mathbb{R}[x]$ és un polinomi de grau senar aleshores p té, com a mínim, una arrel en $\mathbb{R}$.

5) Polinomis amb coeficients reals de grau parell.

   - Un polinomi de grau dos $p = ax^2 + bx + c$ amb coeficients reals té com a mínim una arrel real si i només si $b^2 \geq 4ac$.
   - Per a tot nombre natural parell $n \geq 2$ existeixen polinomis amb coeficients reals $p \in \mathbb{R}[x]$ de grau n sense arrels reals.

≡ **Teorema** *Teorema Fonamental de l'Àlgebra. Teorema de D'Alembert-Gauss.*

- Sigui $p \in \mathbb{C}[x]$ un polinomi no nul i no constant amb coeficients en $\mathbb{C}$. Aleshores p té, com a mínim, una arrel en $\mathbb{C}$.

≡ **Corol.lari** *Polinomis primers amb coeficients complexos, reals o racionals.*

1) Els polinomis primers de $\mathbb{C}[x]$ són els polinomis de grau 1.

2) Els polinomis primers de $\mathbb{R}[x]$ són els polinomis de grau 1 i els polinomis de grau 2 del tipus $ax^2 + bx + c$ amb $a, b, c \in \mathbb{R}$ verificant $b^2 < 4ac$.

3) En $\mathbb{Q}[x]$ existeixen polinomis primers de grau n per a tot $n \geq 1$.

Polinomis amb coeficients en cossos finits

≡ **Propietats** *Polinomis primers amb coeficients de $\mathbb{Z}_p$, p primer.*

1) Per a tot $n \geq 1$, hi ha polinomis primers de $\mathbb{Z}_p[x]$ de grau n.

2) Polinomis diferents de $\mathbb{Z}_p[x]$ poden donar lloc a la mateixa funció polinòmica.

3) Si $p \neq 2$ i $a \neq 0$, aleshores el polinomi $ax^2 + bx + c \in \mathbb{Z}_p[x]$ és primer si i només si $b^2 - 4ac$ no és quadrat perfecte en $\mathbb{Z}_p$.

Fraccions racionals

≡ **Definició** *Fracció racional.*

- Sigui $(\mathbb{K}, +, \cdot)$ un cos commutatiu. Definim el conjunt $\mathbb{K}(x)$ de les fraccions racionals amb coeficients en el cos $\mathbb{K}$ i amb indeterminada x com el conjunt que té com elements expressions formals del tipus $\dfrac{p}{q}$ on $p, q \in \mathbb{K}[x]$ són polinomis amb coeficients en el cos $\mathbb{K}$ amb q no nul.

- Direm que dos fraccions racionals $\dfrac{p_1}{q_1}$ i $\dfrac{p_2}{q_2}$ són iguals si i només si $p_1 q_2 = p_2 q_1$ en $\mathbb{K}[x]$.

≡ **Definició** *Operacions. Suma i producte de fraccions racionals.*

- Donades dos fraccions racionals $\dfrac{p_1}{q_1}$ i $\dfrac{p_2}{q_2}$ definim la seva suma $\dfrac{p_1}{q_1} + \dfrac{p_2}{q_2}$ com la fracció racional $\dfrac{p_1}{q_1} + \dfrac{p_2}{q_2} = \dfrac{p_1 q_2 + p_2 q_1}{q_1 q_2}$, i definim el seu producte $\dfrac{p_1}{q_1} \cdot \dfrac{p_2}{q_2}$ com la fracció racional $\dfrac{p_1}{q_1} \cdot \dfrac{p_2}{q_2} = \dfrac{p_1 p_2}{q_1 q_2}$.

≡ **Propietats** *Estructura algebraica.*

1) La suma i el producte de fraccions racionals són operacions internes en $\mathbb{K}(x)$. Amb aquestes operacions es té que $(\mathbb{K}(x), +, \cdot)$ és un cos commutatiu.

2) El cos de les fraccions racionals $\mathbb{K}(x)$ és una extensió de l'anell dels polinomis $\mathbb{K}[x]$. Concretament es té que $\mathbb{K}[x] \subseteq \mathbb{K}(x)$ identificant un polinomi p amb la fracció racional $\dfrac{p}{1}$.

≡ **Definició** *Fracció racional pròpia. Fracció racional impròpia.*

- Direm que una fracció racional $\frac{p}{q}$ és impròpia si $\deg p \geq \deg q$. Si $\deg p < \deg q$ direm que la fracció racional és pròpia.

≡ **Propietats** *Divisió euclidiana i reducció a fraccions pròpies.*

- Tota fracció racional es pot escriure, de manera única, com suma d'un polinomi i d'una fracció racional pròpia. És a dir, si $\frac{p}{q} \in \mathbb{K}(x)$ aleshores existeix un únic polinomi $c \in \mathbb{K}[x]$ i existeix una única fracció racional pròpia $\frac{p_1}{q_1} \in \mathbb{K}(x)$ de manera que $\frac{p}{q} = c + \frac{p_1}{q_1}$.

≡ **Definició** *Fraccions simples complexes. Fraccions simples reals.*

1) Les fraccions simples complexes són les fraccions racionals del tipus $\frac{A}{(x-\alpha)^n}$ on $A, \alpha \in \mathbb{C}$ i on $n \geq 1$ és un natural.

2) Les fraccions simples reals són les fraccions del tipus $\frac{A}{(x-\alpha)^n}$ on $A, \alpha \in \mathbb{R}$ i on $n \geq 1$ és un natural, o del tipus $\frac{Ax+B}{(x^2+ax+b)^n}$ on $A, B, a, b \in \mathbb{R}$ amb $a^2 < 4b$ i on $n \geq 1$ és un natural.

≡ **Teorema** *Descomposició de fraccions racionals complexes en fraccions simples.*

- Sigui $p \in \mathbb{C}[x]$ un polinomi amb coeficients complexos i sigui $q \in \mathbb{C}[x]$ el polinomi

$$q = (x-\alpha_1)^{n_1} \cdot \ldots \cdot (x-\alpha_r)^{n_r}$$

on $\alpha_1, \ldots, \alpha_r$ són nombres complexos diferents dos a dos i on $n_1, \ldots, n_r \geq 1$ són nombres naturals. Aleshores, existeix un únic polinomi $c \in \mathbb{C}[x]$ i existeixen uns únics nombres complexos $A_{1,1}, \ldots, A_{1,n_1}, \ldots, A_{r,1}, \ldots, A_{r,n_r} \in \mathbb{C}$ de manera que

$$\frac{p}{q} = c + \sum_{j=1}^{r} \sum_{k=1}^{n_j} \frac{A_{j,k}}{(x-\alpha_j)^k}.$$

- Per tant, tota fracció racional complexa es pot descompondre, de manera única, com suma d'un polinomi amb coeficients complexos i de fraccions simples complexes.

≡ **Teorema** *Descomposició de fraccions racionals reals en fraccions simples.*

- Sigui $p \in \mathbb{R}[x]$ un polinomi amb coeficients reals i sigui $q \in \mathbb{R}[x]$ el polinomi

$$q = (x-\alpha_1)^{n_1} \cdot \ldots \cdot (x-\alpha_r)^{n_r} \cdot (x^2+a_1x+b_1)^{m_1} \cdot \ldots \cdot (x^2+a_sx+b_s)^{m_s}$$

on $\alpha_1, \ldots, \alpha_r$ són nombres reals diferents dos a dos, on $x^2+a_1x+b_1, \ldots, x^2+a_sx+b_s$ són polinomis diferents dos a dos i que no tenen arrels reals, i on $n_1, \ldots, n_r, m_1, \ldots, m_s \geq 1$ són nombres naturals. Aleshores, existeix un únic polinomi $c \in \mathbb{R}[x]$ amb coeficients reals i existeixen uns únics nombres reals $A_{i,j}, M_{k,l}, N_{k,l} \in \mathbb{R}$ de manera que

$$\frac{p}{q} = c + \sum_{i=1}^{r} \sum_{j=1}^{n_i} \frac{A_{i,j}}{(x-\alpha_i)^j} + \sum_{k=1}^{s} \sum_{l=1}^{m_k} \frac{M_{k,l}x+N_{k,l}}{(x^2+a_kx+b_k)^l}.$$

- Per tant, tota fracció racional real es pot descompondre, de manera única, com suma d'un polinomi amb coeficients reals i de fraccions simples reals.

7.2 Exercicis i problemes. Enunciats

7.1 Estudieu si les operacions suma i producte són tancades en els següents conjunts de polinomis i en quins casos determinen estructura de grup:

1) $A_{\leq n} = \{\, p \in \mathbb{R}[x] : \deg(p) \leq n \,\} \cup \{0\}$.

2) $A_{\geq n} = \{\, p \in \mathbb{R}[x] : \deg(p) \geq n \,\}$.

3) $A_n = \{\, p \in \mathbb{R}[x] : \deg(p) = n \,\}$.

4) $B_\alpha = \{\, p \in \mathbb{R}[x] : p(\alpha) = 0 \,\}$, $\alpha \in \mathbb{R}$ fix.

5) $C_\alpha = \{\, p \in \mathbb{R}[x] : p(\alpha) = 1 \,\}$, $\alpha \in \mathbb{R}$ fix.

7.2 Trobeu les arrels dels polinomis següents en $\mathbb{Q}$, en $\mathbb{R}$ i en $\mathbb{C}$:

1) $x^3 + 2x^2 - 3x - 6$.

2) $x^6 - 8$.

3) $x^6 + 6x^4 + 9x^2 + 4$.

4) $x^4 - x^2 + 1$.

7.3 Determineu en cada cas el polinomi que satisfà les condicions que s'indiquen.

1) El polinomi real mònic de grau mínim p que satisfà $p(2i) = p(3) = p(1 + 2i) = 0$.

2) El polinomi real p de la forma $p = x^4 + ax^2 + b$ que tingui com arrel el nombre complex $1 + i$.

3) El polinomi de la forma $x^2 - (ia)x + b$, amb a, b reals no nuls, que tingui una arrel doble de mòdul 1.

4) El polinomi amb coeficients complexos $x^n + w$ que tingui $1 + i$ com arrel.

7.4

1) a) Determineu els coeficients del polinomi $(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$.

   b) Demostreu que el terme independent del polinomi $\prod_{i=1}^{n}(x - \alpha_i)$ és $(-1)^n \prod_{i=1}^{n} \alpha_i$ i que el coeficient del terme de grau $n - 1$ és $-\sum_{i=1}^{n} \alpha_i$.

2) a) Determineu λ per tal que el polinomi $x^3 - 7x^2 - 42x + \lambda \in \mathbb{R}[x]$ tingui les arrels en progressió geomètrica.

   b) Determineu λ per tal que el polinomi $2x^3 - x^2 - 7x + \lambda \in \mathbb{R}[x]$ tingui dues arrels que sumin 1.

   c) Sigui $\mathbb{K}$ un cos. Determineu $a, b, c \in \mathbb{K}$ per tal que $x^3 - ax^2 + bx - c \in \mathbb{K}[x]$ tingui per arrels a, b i c.

7.5

1) Demostreu que α és una arrel de multiplicitat $r \geq 1$ del polinomi p si i només si α és arrel dels polinomis $p, p', \ldots, p^{(r-1)}$ i no és arrel del polinomi $p^{(r)}$, on $p^{(i)}$ representa el polinomi derivada i-èsima de p.

2) Sigui $n \geq 1$. Demostreu:

   a) El polinomi $\displaystyle\sum_{i=0}^{n} \frac{1}{i!}\, x^i = \frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + \frac{x^2}{2!} + x + 1 \in \mathbb{R}[x]$ no té arrels múltiples.

   b) El polinomi $nx^{n+2} - (n+2)x^{n+1} + (n+2)x - n \in \mathbb{R}[x]$ té una arrel de multiplicitat com a mínim 3.

   c) El polinomi $(x+1)^{6n+1} - x^{6n+1} - 1$ és divisible per $(x^2 + x + 1)^2$ a $\mathbb{C}[x]$.

7.6

1) Considerem el polinomi $p = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}[x]$. Demostreu que si $a/b \in \mathbb{Q}$ és arrel de p, on a, b són enters relativament primers, aleshores $a|c_0$ i $b|c_n$. Deduïu que les arrels enteres de p són divisors del terme independent.

2) Trobeu les arrels racionals dels polinomis següents:

   a) $6x^3 + 3x - 18$. b) $5x^3 + x^2 + x - 4$. c) $3x^3 - 7x - 5$.

7.7

1) Demostreu que si $p \in \mathbb{Z}[x]$ i si α, β, m són enters tals que $\alpha \equiv \beta \pmod{m}$, aleshores $p(\alpha) \equiv p(\beta) \pmod{m}$.

2) Sigui $p \in \mathbb{Z}[x]$. Demostreu que si $p(1)$ o $p(-1)$ és senar, aleshores $p(1)$ i $p(-1)$ són senars i p no té arrels enteres senars.

7.8

1) Sigui $\mathbb{K}$ un cos, $\alpha \in \mathbb{K}$ un escalar, i $p \in \mathbb{K}[x]$ un polinomi amb coeficients en el cos $\mathbb{K}$. Demostreu que la resta de dividir p per $x - \alpha$ és $p(\alpha)$.

2) a) Sigui $p \in \mathbb{R}[x]$ un polinomi tal que en dividir-lo per $x+1$ la resta és -2 i en dividir-lo per $x-2$ la resta és 4. Quina és la resta en dividir p per $x^2 - x - 2$?

   b) Sigui $p \in \mathbb{R}[x]$ un polinomi tal que en dividir-lo per $x-1$ la resta és 3, en dividir-lo per x la resta és també 3 i en dividir-lo per $x+1$ la resta és 1. Quina és la resta en dividir p per $x^3 - x$?

   c) Sigui $p \in \mathbb{C}[x]$ un polinomi tal que en dividir-lo per $x-1$ la resta és 3 i en dividir-lo per $x - i$ la resta és $2i$. Quina és la resta en dividir p per $x^2 - (1+i)x + i$?

7.9 Determineu a per tal que el polinomi $x^2 - ax + 1$ sigui divisor de $x^4 - x + a$ a $\mathbb{R}[x]$.

7.10 Demostreu que si $n, m \geq 1$, aleshores $1 + x + \cdots + x^{n-1}$ divideix $(1 + x + \cdots + x^n)^m - x^n$ en $\mathbb{Q}[x]$.

7.11 Determineu quantes arrels comunes sobre $\mathbb{R}$ i sobre $\mathbb{C}$ tenen els polinomis p i q, i calculeu el màxim comú divisor, on:

1) $p = x^3 - 2$, $q = x^2 + x + 2$.

2) $p = x^4 - 1$, $q = x^3 - 3x - 2$.

3) $p = x^4 - 2x^2 + 1$, $q = x^4 + 3x^2 + 2$.

4) $p = x^3 + 7x + 6$, $q = x^2 - 1$.

5) $p = x^5 - 6x^3 + 6x^2 + 7x + 6$, $q = x^2 + 3x + 2$.

6) $p = x^3 + x$, $q = x^3 + ix^2 + x + i$.

7) $p = x^4 + 2$, $q = x^8 - 4$.

7.12 Considerem els polinomis $p = x^2 - (2a-1)x + a(a-1)$ i $q = x^4 - (2a-1)x^2 - a^2(a-1)^2 + b$ on $a, b \in \mathbb{R}$.

1) Determineu a, b per tal que p i q tinguin dues arrels comunes i per tal que p i q tinguin exactament una arrel comuna.

2) Calculeu el màxim comú divisor de p i q en funció dels paràmetres a i b.

7.13 Calculeu un màxim comú divisor dels polinomis $p = x^2 - x + 4$ i $q = x^3 + 2x^2 + 3x + 2$ i doneu la identitat de Bézout en els anells $\mathbb{R}[x]$ i $\mathbb{Z}_3[x]$.

7.14 Doneu en cada cas polinomis $p, q \in \mathbb{R}[x]$ tals que:

1) $(x^2 - 3x + 2)\,p + (x^2 + x + 1)\,q = 1$.

2) $(2x^3 - 7x^2 + 7x - 2)\,p + (2x^3 + x^2 + x - 1)\,q = 2x - 1$.

7.15

1) Donats dos polinomis q_1, q_2, demostreu que existeix un polinomi p tal que p sigui divisible per q_1 i $p - 1$ sigui divisible per q_2 si i només si $\mathrm{mcd}(q_1, q_2) = 1$.

2) Determineu un polinomi $p \in \mathbb{R}[x]$ de grau mínim que sigui divisible per $x^2 + 1$ i tal que el polinomi $p - 1$ sigui divisible per $x^3 + 1$.

7.16 Factoritzeu com a producte de polinomis irreductibles en els anells $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_3[x]$ i $\mathbb{Z}_5[x]$ els polinomis:

1) $x^2 + x + 1$.

2) $x^3 + x + 2$.

3) $x^4 + x^3 + x + 1$.

4) $x^2 + 1$.

5) $x^4 - x^2 + 1$.

6) $x^9 - x$.

7.17 Factoritzeu com a producte de polinomis irreductibles a $\mathbb{Z}_3[x]$ i a $\mathbb{Z}_5[x]$:

1) $3x^3 + 4x^2 + 3$.

2) $x^3 + x - 1$.

7.18 Factoritzeu el polinomi $x^4 + x^3 + x - 1$ com a producte de polinomis irreductibles a $\mathbb{Z}_3[x]$.

7.19 Sigui $a \neq 0$ enter.

1) Quantes arrels pot tenir el polinomi $x^2 - a$ en $\mathbb{Z}_p$, si p és primer senar?

2) Quantes arrels pot tenir el polinomi $x^2 - a$ en $\mathbb{Z}_8$?

7.20

1) Sigui $m \geq 2$. És possible que un polinomi $p \in \mathbb{Z}_m[x]$ de grau n tingui més de n arrels en $\mathbb{Z}_m$?

2) Quantes arrels té el polinomi $x^{13} - x$ en $\mathbb{Z}_{1365}$?

7.21 Expresseu les fraccions racionals reals següents com suma d'un polinomi i una fracció racional pròpia:

1) $\dfrac{2x^3 - 3x^2 - 12x + 19}{x^2 - x - 6}$.

2) $\dfrac{x^5 + 4x^4 + 2x^3 - 5x^2 + 5x + 17}{x^2 + 4x + 4}$.

7.22 Expresseu les fraccions racionals complexes següents com suma d'un polinomi i una fracció racional pròpia:

1) $\dfrac{x^4}{ix^2 - 1}$.

2) $\dfrac{x^3 + 3x + 1}{x^2 + ix + 1}$.

7.23 Descomponeu les fraccions racionals reals següents en fraccions simples:

1) $\dfrac{-x + 13}{x^2 - x - 6}$.

2) $\dfrac{x + 5}{x^2 + 4x + 4}$.

3) $\dfrac{x^4 - x^3 + 2}{x^5}$.

4) $\dfrac{x^2 - 6x + 7}{x^3 - 9x^2 + 27x - 27}$.

5) $\dfrac{-10x}{x^3 + 2x^2 + x + 2}$.

6) $\dfrac{3x^2 + 2x + 5}{x^3 + x^2 - 2}$.

7) $\dfrac{x^3 + 2x^2 + 2x + 3}{(x^2 + x + 1)^2}$.

7.24 Descomponeu les fraccions racionals complexes següents en fraccions simples:

1) $\dfrac{-10x}{x^3 + 2x^2 + x + 2}$.

2) $\dfrac{3x^2 + 2x + 5}{x^3 + x^2 - 2}$.

3) $\dfrac{x + 4 + i}{(x - i)(x + 2)}$.

4) $\dfrac{4x}{(x^2 + 2x + 2)^2}$.

7.25 Considerem el polinomi q de $\mathbb{C}[x]$, $q = x^3 - (5 + 3i)x^2 + (5 + 8i)x - 1 - 5i$.

1) Trobeu totes les arrels reals de q.

2) Determineu totes les arrels complexes de q. (Podeu utilitzar que les arrels quadrades de $3+4\,i$ són $\pm(2 + i)$.) Comproveu que $(2 + i)^2 = 3 + 4i$.

3) Descomponeu en fraccions simples complexes la fracció racional $\dfrac{x + 1}{q}$.

7.26 Demostreu que $\dfrac{1}{1 - x} = \displaystyle\sum_{k=0}^{n-1} x^k + \frac{x^n}{1 - x}$, $\forall n \geq 1$.

7.3 Exercicis i problemes. Solucions

7.1

1) Amb la suma és grup. El producte no és una operació tancada.

2) La suma no és tancada. El producte és tancat. No és grup amb el producte.

3) Ni la suma ni el producte són operacions tancades.

4) Les dues operacions són tancades. Amb la suma és grup, però no amb el producte.

5) La suma no és tancada. El producte és tancat. No és grup amb cap de les dues operacions.

7.2

1) -2 en $\mathbb{Q}$.
-2, $\sqrt{3}$, $-\sqrt{3}$ en $\mathbb{R}$ i en $\mathbb{C}$.

2) No té arrels en $\mathbb{Q}$.
$\sqrt{2}$, $-\sqrt{2}$ en $\mathbb{R}$.
$\sqrt{2}$, $-\sqrt{2}$, α, $-\alpha$, $\overline{\alpha}$, $-\overline{\alpha}$, on $\alpha = (\sqrt{2} + i\sqrt{6})/2$, en $\mathbb{C}$.

3) No té arrels ni en $\mathbb{Q}$ ni en $\mathbb{R}$.
i, $-i$, $2i$, $-2i$ en $\mathbb{C}$.

4) No té arrels ni en $\mathbb{Q}$ ni en $\mathbb{R}$.
$(\sqrt{3}+i)/2$, $(\sqrt{3}-i)/2$, $-(\sqrt{3}+i)/2$, $-(\sqrt{3}-i)/2$ en $\mathbb{C}$.

7.3

1) $p = x^5 - 5x^4 + 15x^3 - 35x^2 + 44x - 60$.

2) $a = 0$, $b = 4$.

3) $a = \pm 2$, $b = -1$.

4) $w = -(\sqrt{2})^n e^{n\pi i/4}$.

7.4

1) a) $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = x^3 - (\alpha_1+\alpha_2+\alpha_3)x^2 + (\alpha_1\,\alpha_2 + \alpha_2\,\alpha_3 + \alpha_3\,\alpha_1)x - \alpha_1\,\alpha_2\,\alpha_3$.

2) a) $\lambda = 216$.
b) $\lambda = -3$.
c) $b = c = 0$ i a qualsevol, o bé $a = b = -1$ i $c = 1$.

7.6

2) a) No té cap arrel racional.

b) $4/5$.

c) No té cap arrel racional.

7.8

2) a) $2x$.

b) $-x^2+x+3$.

c) $\dfrac{5+i}{2}x+\dfrac{1-i}{2}$.

7.9 $a=\dfrac{1\pm\sqrt{5}}{2}$.

7.10 Observeu que $(1+x+\cdots+x^n)^m=(1+x(1+x+\cdots+x^{n-1}))^m$ i apliqueu el binomi de Newton.

7.11

1) No tenen arrels en comú ni en $\mathbb{R}$ ni en $\mathbb{C}$, $\operatorname{mcd}(p,q)=1$ en $\mathbb{R}[x]$ i en $\mathbb{C}[x]$.

2) Tenen una arrel en comú en $\mathbb{R}$ i en $\mathbb{C}$, $\operatorname{mcd}(p,q)=x+1$ en $\mathbb{R}[x]$ i en $\mathbb{C}[x]$.

3) No tenen arrels en comú ni en $\mathbb{R}$ ni en $\mathbb{C}$, $\operatorname{mcd}(p,q)=1$ en $\mathbb{R}[x]$ i en $\mathbb{C}[x]$.

4) No tenen arrels en comú ni en $\mathbb{R}$ ni en $\mathbb{C}$, $\operatorname{mcd}(p,q)=1$ en $\mathbb{R}[x]$ i en $\mathbb{C}[x]$.

5) No tenen arrels en comú ni en $\mathbb{R}$ ni en $\mathbb{C}$, $\operatorname{mcd}(p,q)=1$ en $\mathbb{R}[x]$ i en $\mathbb{C}[x]$.

6) No tenen arrels en comú en $\mathbb{R}$, però tenen dues arrels en comú en $\mathbb{C}$. El màxim comú divisor és $\operatorname{mcd}(p,q)=x^2+1$ en $\mathbb{C}[x]$. No té sentit calcular el màxim comú divisor en $\mathbb{R}[x]$, ja que q no és de $\mathbb{R}[x]$.

7) No tenen arrels en comú en $\mathbb{R}$, però tenen quatre arrels en comú en $\mathbb{C}$, $\operatorname{mcd}(p,q)=x^4+2$ en $\mathbb{R}[x]$ i en $\mathbb{C}[x]$.

7.12

1) Tenen dues arrels comunes si $a\in\{1/2,1\}$ i $b=0$.

Tenen una arrel comuna si $a\notin\{1/2,1\}$ i $b\in\{0,2(2a-1)(a-1)^2\}$.

2) $\operatorname{mcd}(p,q)=\begin{cases} p, & \text{si } a\in\{1/2,1\} \text{ i } b=0;\\ x-a, & \text{si } a\notin\{1/2,1\} \text{ i } b=0;\\ x-(a-1), & \text{si } a\notin\{1/2,1\} \text{ i } b=2(2a-1)(a-1)^2;\\ 1, & \text{altrament.}\end{cases}$

7.13

$$1 = \left(\frac{1}{48}x^2 + \frac{7}{48}x + \frac{7}{24}\right) p + \left(-\frac{1}{48}\,x - \frac{1}{12}\right) q \text{ en } \mathbb{R}[x].$$

$x + 1 = x\,p + 2\,q$ en $\mathbb{Z}_3[x]$.

7.14

1) $p = \dfrac{1}{21}\big(4x + 5\big)$ i $q = \dfrac{1}{21}\,\big(-4\,x + 11\big)$.

2) $p = \dfrac{1}{21}\big(4x + 5\big)$ i $q = \dfrac{1}{21}\,\big(-4\,x + 11\big)$.

7.15

2) $p = \dfrac{1}{2}\big(-x^4 - x^3 - x + 1\big)$.

7.16 La descomposició en $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_3[x]$ i $\mathbb{Z}_5[x]$ és respectivament:

1) $(x + \frac{1}{2} + \frac{\sqrt{3}}{2}\,i)(x + \frac{1}{2} - \frac{\sqrt{3}}{2}\,i)$;
   $x^2 + x + 1$;
   $(x + 2)^2$;
   $x^2 + x + 1$.

2) $(x + 1)(x - \frac{1}{2} - \frac{\sqrt{7}}{2}\,i)(x - \frac{1}{2} - \frac{\sqrt{7}}{2}\,i)$;
   $(x + 1)(x^2 - x + 2)$;
   $(x + 1)(x^2 + 2x + 2)$;
   $(x + 1)(x^2 + 4x + 2)$.

3) $(x + 1)^2(x - \frac{1}{2} + \frac{\sqrt{3}}{2}\,i)(x - \frac{1}{2} - \frac{\sqrt{3}}{2}\,i)$;
   $(x + 1)^2(x^2 - x + 1)$;
   $(x + 1)^4$;
   $(x + 1)^2(x^2 + 4x + 1)$.

4) $(x - i)(x + i)$;
   $x^2 + 1$;
   $x^2 + 1$;
   $(x + 3)(x + 2)$.

5) $\Big(x - (\frac{\sqrt{3}}{2} + \frac{1}{2}\,i)\Big)\Big(x - (\frac{\sqrt{3}}{2} - \frac{1}{2}\,i)\Big)\Big(x - (-\frac{\sqrt{3}}{2} + \frac{1}{2}\,i)\Big)\Big(x - (-\frac{\sqrt{3}}{2} - \frac{1}{2}\,i)\Big)$;
   $(x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1)$;
   $(x^2 + 1)^2$;
   $(x^2 + 2x + 4)(x^2 + 3x + 4)$.

6) $x\prod_{i=0}^{7}(x-e^{\frac{\pi k}{4}i}) = x(x-1)(x+1)(x-i)(x+i)(x-\alpha)(x-\overline{\alpha})(x-\beta)(x-\overline{\beta})$
on $\alpha = (1+i)/\sqrt{2}$ i on $\beta = (-1+i)/\sqrt{2}$;
$x(x-1)(x+1)(x^2+1)(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$;
$x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$;
$x(x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3)$.

7.17

1) x^2 a $\mathbb{Z}_3[x]$; $3(x+4)(x+2)^2$ a $\mathbb{Z}_5[x]$.

2) $(x+1)(x^2+2x+2)$ a $\mathbb{Z}_3[x]$; és irreductible a $\mathbb{Z}_5[x]$.

7.18 $x^4+x^3+x-1 = (x^2+1)(x^2+x+2)$

7.19

1) 0 o 2.

2) 0, 2 o 4.

7.20

1) Sí.

2) 1365.

7.21

1) $2x-1+\dfrac{-x+13}{x^2-x-6}$.

2) $x^3-2x+3+\dfrac{x+5}{x^2+4x+4}$.

7.22

1) $-ix^2-1+\dfrac{-1}{ix^2-1}$.

2) $x-i+\dfrac{x+i+1}{x^2+ix+1}$.

7.23

1) $\dfrac{2}{x-3}+\dfrac{-3}{x+2}$.

2) $\dfrac{1}{x+2}+\dfrac{3}{(x+2)^2}$.

3) $\dfrac{1}{x}+\dfrac{-1}{x^2}+\dfrac{2}{x^5}$.

4) $\dfrac{1}{x-3}+\dfrac{-2}{(x-3)^3}$.

5) $\dfrac{4}{x+2}+\dfrac{-4x-2}{x^2+1}$.

6) $\dfrac{2}{x-1}+\dfrac{x-1}{x^2+2x+2}$.

7) $\dfrac{x+1}{x^2+x+1}+\dfrac{2}{(x^2+x+1)^2}$.

7.24

1) $\dfrac{4}{x+2}+\dfrac{-2-i}{x+i}+\dfrac{-2+i}{x-i}$.

2) $\dfrac{2}{x-1}+\dfrac{1/2-i}{x+i+1}+\dfrac{1/2+i}{x-i+1}$.

3) $\dfrac{2}{x-i}+\dfrac{-1}{x+2}$.

4) $\dfrac{-i}{x+i+1}+\dfrac{1+i}{(x+i+1)^2}+\dfrac{i}{x-i+1}+\dfrac{1-i}{(x-i+1)^2}$.

7.25

1) 1.

2) $1,\ 3+2\,i,\ 1+i$.

3) $\dfrac{x+1}{q}=\dfrac{-1/2-i/2}{x-1}+\dfrac{i}{x-1-i}+\dfrac{1/2-i/2}{x-3-2\,i}$.