Apunts de matemàtiques

Claudi Lleyda Moltó

Les matemàtiques són un joc de definicions.

Índex

Part I

Introducció

Capítol 1

Coses per fer

Podeu trobar la versió actualitzada d'aquest pdf seguint aquest link.

1.1 Àlgebra lineal

1.1.1 Definicions

Definició 1.1.1.1 (Forma bilineal definida estrictament positiva o negativa)**.** Sigui M una forma bilineal simètrica. Preguntar a en Cedò.

Definició 1.1.1.2 (Norma d'una aplicació lineal)**.**

1.1.2 Proposicions

Proposició 1.1.2.1. *Vectors linealment independents $\Leftrightarrow$ determinant no nul.*

1.1.3 Teoremes

Teorema 1.1.3.1. *Sigui $A = (a_{i,j}) \in M_n(\mathbb{R})$ una matriu simètrica. Aleshores A és definida positiva si i només si*

$$\begin{vmatrix} a_{1,1} & \cdots & a_{1,i} \\ \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,i} \end{vmatrix} > 0$$

per a tot $i \in \{1, \ldots, n\}$.

Demostració. Per inducció sobre n. □

1.2 Funcions de variable real

1.2.1 Definicions

Definició 1.2.1.1 (Funció contínua)**.** Sigui f una funció. Direm que f és contínua en a si

$$\lim_{x \to a} f(x) = f(a).$$

Definició 1.2.1.2 (Partició, poligonal i longitud d'una poligonal)**.** Sigui (a, b) un interval de $\mathbb{R}$. Direm que una partició de (a, b) és un conjunt de escalars $t_0, \ldots, t_n \in [a, b]$ que compleixen $a = t_0 < \cdots < t_n = b$. Direm que $t_0, \ldots, t_n$ són els nodes de la partició.

Sigui $f : (a, b) \to \mathbb{R}^m$ una funció. Definirem la poligonal P_n d'una partició en una funció f com

$$P_n = f(t_0), \ldots, f(t_n).$$

Definim la longitud de la poligonal P_n com

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\|.$$

Definició 1.2.1.3 (Classe de diferenciabilitat d'una funció)**.** Sigui f una funció n-vegades diferenciable amb $f^{(n)}$ contínua. Direm que f és de classe $\mathcal{C}^n$ o que $f \in \mathcal{C}^n$.

Definició 1.2.1.4 (Funció monòtona)**.** Sigui $f : [a, b] \to \mathbb{R}$ una funció. Direm que és f és monòtona si, per a qualsevol $x, y \in [a, b]$, $x > y$ implica $f(x) \geq f(y)$.

Definició 1.2.1.5 (Notació de Landau)**.** $A(h) = \mathrm{o}(B(h)) \ldots$

1.2.2 Proposicions

Proposició 1.2.2.1. *Siguin $I \subseteq \mathbb{R}$ un interval i $f : I \to \mathbb{R}$ una funció. Aleshores, si f és derivable en un punt $a \in I$, f és contínua en a.*

Proposició 1.2.2.2. *Sigui $f : [a, b] \to \mathbb{R}$ una funció acotada i monòtona. Aleshores f és integrable Riemann.*

1.2.3 Teoremes

Teorema 1.2.3.1 (Equivalència entre normes)**.** *Si $q(x)$ és una norma existeixen $m, M \in \mathbb{R}^+$ tals que $m\|x\| \leq q(x) \leq M\|x\|$ per a tot $x \in \mathbb{R}^m$.*

Teorema 1.2.3.2 (Teorema del Valor Mig)**.** hmm trivial

Teorema 1.2.3.3 (Desigualtat de Cauchy-Schwarz)**.**

Teorema 1.2.3.4 (Teorema de Taylor)**.** *Sigui $(a, b) \subseteq \mathbb{R}$ un interval i $f : (a, b) \to \mathbb{R}$ una funció de classe $\mathcal{C}^n$. Aleshores, per a dos punts $x, c \in (a, b)$, amb $x < c$, existeix un punt $x_1 \in (x, c)$ tal que*

$$f(x) = f(c) + \sum_{k=1}^{n-1} \frac{f^{(k)}(c)}{k!}(x - c)^k + \frac{f^{(n)}(x_1)}{n!}(x - c)^n.$$

Teorema 1.2.3.5 (Teorema de Weierstrass)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}$ una funció. Aleshores, donat un compacte $S \subset U$, si f és contínua en S, f té un màxim i un mínim absoluts en S.*

Teorema 1.2.3.6 (Teorema del sandvitx)**.**

Teorema 1.2.3.7 (Teorema de Rolle)**.** *Sigui $f : [a, b] \subset \mathbb{R} \longrightarrow \mathbb{R}$ una funció derivable en (a, b) tal que $f(a) = f(b)$. Aleshores existeix un cert $c \in (a, b)$ tal que $f'(c) = 0$.*

1.3 Trobar lloc per tot això

Definició 1.3.0.1 (Conjunt obert, tancat...)**.**

Definició 1.3.0.2 (Relació d'equivalència)**.**

Definició 1.3.0.3 (Continuïtat uniforme)**.** Siguin $U \subseteq \mathbb{R}^d, V \subseteq \mathbb{R}^m$ dos oberts i $f : U \to V$ una funció. Aleshores direm que f és uniformement contínua en un conjunt $S \subseteq U$ si per a tot $\varepsilon > 0$ existeix un $\delta > 0$ tals que

$$d_U(x, y) < \varepsilon \text{ i } d_V(f(x) - f(y)) < \delta$$

per a tot punt $x, y \in U$.

Teorema 1.3.0.4 (Teorema de Heine)**.** *Siguin $U \subseteq \mathbb{R}^d$ dos oberts, $S \subset U$ un compacte i $f : U \to \mathbb{R}^m$ una funció contínua. Aleshores f és uniformement contínua en S.*

Definició 1.3.0.5 (Funció indicatriu)**.** Siguin X un conjunt i $A \subseteq X$ un subconjunt de X. Definim la funció indicatriu de A com una funció

$$1_A : X \longrightarrow \{0, 1\}$$

tal que

$$1_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A. \end{cases}$$

Teorema 1.3.0.6 (Teorema de la divisió Euclidiana)**.**

Part II

Càlcul en diverses variables i optimització

Capítol 2

Càlcul diferencial

2.1 Introducció

2.1.1 Arcs en múltiples variables

Definició 2.1.1.1 (Arcs a l'espai)**.** Siguin $(a,b) \subseteq \mathbb{R}$ un interval, $f : (a,b) \to \mathbb{R}^m$ una funció i Γ el conjunt definit per

$$\Gamma = \{x \in \mathbb{R}^m : x = f(t) \text{ per a tot } t \in (a,b)\},$$

aleshores direm que Γ és un arc a $\mathbb{R}^m$. També direm que f defineix o recorre aquest arc. Així mateix donem les següents definicions:

1. Direm que Γ és un arc continu si f és contínua en (a,b).
2. Direm que Γ és un arc simple si f és injectiva en (a,b).
3. Si f està definida en $[a,b]$ direm que f va de $f(a)$ a $f(b)$ o que $f(a)$ n'és el punt inicial i $f(b)$ el punt final. Si $f(a) = f(b)$ direm que Γ és un arc tancat.
4. Direm que Γ és un arc regular si f és derivable en (a,b).
5. Direm que Γ és un arc de classe $\mathcal{C}^n$ si $f^{(n)}$ existeix i és contínua en (a,b).

Definició 2.1.1.2 (Longitud d'un arc continu)**.** Sigui Γ un arc continu i f una manera de recórrer Γ donada per

$$f : (a,b) \subseteq \mathbb{R} \longrightarrow \mathbb{R}^m$$

Amb $m \in \mathbb{N}$, $m > 1$.

Considerem la partició $a = t_0 < \cdots < t_n = b$. Observem que els punts donats per $f(t_i)$ per a tot $i \in \{0, \ldots, n\}$ determinen una poligonal, P_n, la longitud de la qual és, per la definició de longitud d'una poligonal (1.2.1.2)

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\|.$$

Aleshores definim la longitud de f com

$$\mathrm{L}(f) = \lim_{n\to\infty} \mathrm{L}(P_n).$$

Direm que els arcs amb recorreguts de longitud finita són arcs rectificables.

Proposició 2.1.1.3. *Sigui Γ un arc de classe $\mathcal{C}^1$. Aleshores Γ és rectificable.*

Demostració. Sigui f una funció que recorre Γ tal que

$$\begin{aligned} f : (a,b) \subseteq \mathbb{R} &\longrightarrow \mathbb{R}^m \\ t &\longmapsto (x_1(t), \dots, x_m(t)). \end{aligned}$$

Donada una partició de (a,b), $a = t_0 < \cdots < t_n = b$ que defineix una poligonal $P_n = f(t_0), \dots, f(t_n)$. Aleshores la longitud de la poligonal és, per la definició de partició (1.2.1.2),

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} \|f(t_{i+1}) - f(t_i)\| = \sum_{i=0}^{n-1} \sqrt{\sum_{j=1}^{m} (x_j(t_{i+1}) - x_j(t_i)))^2}.$$

Per la proposició 1.2.2.1 f és contínua en (a,b), i per tant pel Teorema del Valor Mig (1.2.3.2) tenim

$$x_j(t_{i+1}) - x_j(t_i) = x_j'(\xi_{ij})(t_{i+1} - t_i),$$

amb $t_i < \xi_{ij} < t_{i+1}$, per a tot $i \in \{0, \dots, n-1\}$, $j \in \{1, \dots, m\}$. Per tant

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} (t_{i+1} - t_i) \sqrt{\sum_{j=1}^{m} \left(x_j'(\xi_{ij})\right)^2}. \tag{2.1}$$

Ara volem veure que $\xi_{ij} = \xi_i$ quan n tendeix a infinit. Observem que

$$\lim_{n\to\infty} t_i = \lim_{n\to\infty} t_{i+1}.$$

I com que $t_i < \xi_{ij} < t_{i+1}$ tenim que $\xi_{ij} = \xi_i$ per a tot $j \in \{1, \dots, m\}$. Així veiem que si $n \to \infty$ podem reescriure (2.1) com

$$\mathrm{L}(P_n) = \sum_{i=0}^{n-1} (t_{i+1} - t_i) \|f'(\xi_i)\| = \int_a^b \|f'(t)\| dt.$$

I ja hem acabat. Com que $f \in \mathcal{C}^1$ tenim f' contínua, i $a, b \in \mathbb{R}$, aquesta integral és finita i Γ és rectificable, com volíem veure. □

2.1.2 Oberts connexos

Definició 2.1.2.1 (Conjunt arc-connex o connex)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert. Direm que U és arc-connex si donats dos punts $P, Q \in U$ existeix una funció f que defineix un arc continu tal que $f : [a,b] \longrightarrow U$ amb $P = f(a)$, $Q = f(b)$. Direm que U és connex si el segment que els uneix està tot dins U.

Proposició 2.1.2.2. *Sigui $U \subseteq \mathbb{R}^d$ un obert. Donats dos arc-connexos $U_1, U_2 \subseteq U$ amb $U_1 \cup U_2 = U$, si $U_1 \cap U_2 \neq \emptyset \Longrightarrow U$ és arc-connex.*

Demostració. Siguin P, Q dos punts en U tals que $P \in U_2^{\complement}$ i $Q \in U_1^{\complement}$, i $R \in U_1 \cap U_2$ un altre punt. Com que U_1 i U_2 són arc-connexos, per la definició de conjunt arc-connex (2.1.2.1) existeixen dos arcs continus f, g tals que

$$f : [a, b] \longrightarrow U_1, \quad g : [b, c] \longrightarrow U_2,$$

on $f(a) = P$, $f(b) = g(b) = R$ i $g(c) = Q$. Aleshores definim la funció

$$h(t) = \begin{cases} f(t) & \text{si } a \leq t \leq b \\ g(t) & \text{si } b < t \leq b. \end{cases}$$

Tenim que h defineix un arc continu en U, i per la definició de longitud d'un arc continu (2.1.1.2), U és arc-connex. □

Definició 2.1.2.3 (Distància en un arc-connex)**.** Sigui $U \subseteq \mathbb{R}^d$ un arc-connex, siguin $P, Q \in U$ i F el conjunt de totes les funcions f que defineixen un arc continu en U amb $f(a) = P$, $f(b) = Q$. Definim la distància entre P i Q en U com

$$\mathrm{d}_U(P, Q) = \inf_{f \in F} \mathrm{L}(f).$$

Observació 2.1.2.4. *Notem que si U és connex $\mathrm{d}_U(P, Q) = \|P - Q\|$.*

Proposició 2.1.2.5. *Siguin $U \subseteq \mathbb{R}^d$ un arc-connex i $P, Q, R \in U$ tres punts. Aleshores*

1. $\mathrm{d}_U(P, Q) = \mathrm{d}_U(Q, P) \geq 0$
2. $\mathrm{d}_U(P, Q) = 0 \Longleftrightarrow P = Q$
3. $\mathrm{d}_U(P, Q) \leq \mathrm{d}_U(P, R) + \mathrm{d}_U(R, Q)$ *(desigualtat triangular)*

Demostració. Sigui $f : [a, b] \to U$ una funció contínua amb $f(a) = P$ i $f(b) = Q$, i amb $\mathrm{L}(f) = \inf_{f \in F} \mathrm{L}(f)$, on F és el conjunt de funcions contínues de $[a, b]$ en U que van de P a Q.

Per veure el punt (1) fem

$$\begin{aligned}
\mathrm{d}_U(P, Q) &= \inf_{f \in F} \mathrm{L}(f) \\
&= \inf_{f \in F} \lim_{n \to \infty} \left(\sum_{i=0}^{n-1} (t_{i+1} - t_i) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{ij}) \right)^2} \right) \\
&= \inf_{f \in F} \lim_{n \to \infty} \left(\sum_{i=0}^{n-1} (-1)(t_{n-(i+1)} - t_{n-i}) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{ij}) \right)^2} \right) \\
&= \inf_{f \in F} (-1) \lim_{n \to \infty} \left(\sum_{i=0}^{n-1} (t_{n-(i+1)} - t_{n-i}) \sqrt{\sum_{j=1}^{d} \left(x_j'(\xi_{ij}) \right)^2} \right) \\
&= \inf_{f \in F} (-1) \int_a^b \|f'(t)\| dt \\
&= \inf_{f \in F} \int_b^a \|f'(t)\| dt = \inf_{f \in F} \mathrm{L}(f) = \mathrm{d}_U(Q, P) \geq 0.
\end{aligned}$$

Continuem veient el punt (2). Suposem $P = Q$ i considerem, amb $\varepsilon > 0$, la bola oberta $\mathrm{B}(\varepsilon, P) \subset U$. Aquesta bola és connexa i, pel corol·lari 2.1.2.4, $\mathrm{d}_U(P,Q) = \|P - Q\| = 0 \iff P = Q$.

Acabem veient el punt (3). Sigui F_1 el conjunt de funcions contínues en U que van de P a R i F_2 el conjunt de funcions contínues en U que van de R a Q. Aleshores

$$\mathrm{d}_U(P,Q) = \inf_{f\in F} \mathrm{L}(f) \leq \inf\left(\inf_{F_1} \mathrm{L}(g) + \inf_{F_2} \mathrm{L}(h)\right) = \mathrm{d}_U(P,R) + \mathrm{d}_U(R,Q).$$

Observem que aquestes són les mateixes propietats de una distància. □

2.2 Funcions diferenciables

2.2.1 Diferencial d'una funció en múltiples variables

Definició 2.2.1.1 (Derivada direccional)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert, $t \in \mathbb{R}$ un escalar, $a \in U$ un punt, $\vec{u}$ un vector de $\mathbb{R}^d$ i f una funció definida per

$$\begin{aligned} f : U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a), \ldots, f_m(a)), \end{aligned}$$

i considerem, per a tot $i \in \{1, \ldots, m\}$, els límits

$$D_{\vec{u}} f_i(a) = \lim_{t\to 0} \frac{f_i(a + t\vec{u}) - f_i(a)}{t}.$$

Si tots aquests límits existeixen, direm que la derivada de f en direcció $\vec{u}$ és

$$D_{\vec{u}} f(a) = \left(D_{\vec{u}} f_1(a), \ldots, D_{\vec{u}} f_m(a)\right).$$

Si $\vec{u}$ és l'i-èsim vector de la base canònica utilitzarem la notació $D_i f(a)$.

Proposició 2.2.1.2. *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}^m$ una funció, $D_{\vec{u}} f(a)$ la seva derivada direccional respecte el vector $\vec{u}$ de $\mathbb{R}^d$ i $\lambda \in \mathbb{R}$ un escalar. Aleshores*

$$D_{\lambda\vec{u}} f(a) = \lambda D_{\vec{u}} f(a).$$

Demostració. Tenim que, per a tot $i \in \{1, \ldots, m\}$,

$$\begin{aligned} D_{\lambda\vec{u}} f_i(a) &= \lim_{t\to 0} \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{t} \\ &= \lim_{t\to 0} \lambda \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{\lambda t} \\ &= \lambda \lim_{t\to 0} \frac{f_i(a + \lambda t\vec{u}) - f_i(a)}{\lambda t} = \lambda D_{\vec{u}} f_i(a). \end{aligned}$$

□

Definició 2.2.1.3 (Diferencial d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^m$ una funció i $a \in U$ un punt. Direm que el diferencial de f en a és una aplicació lineal $df(a) : U \to \mathbb{R}^m$ tal que, donat un vector $\vec{h}$ de $\mathbb{R}^d$

$$f(a + \vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

Direm que f és diferenciable en a si existeix aquest $df(a)$.

Observació 2.2.1.4. *Observem que en aquesta definició, si $d = 1$, f és diferenciable en $a \iff f$ és derivable en a, i $df(a)(\vec{h}) = \vec{h}f'(a)$ (Si $d = 1$, multiplicar per un vector de $\mathbb{R}$ és com multiplicar per un escalar).*

Proposició 2.2.1.5. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Aleshores f és contínua en a.*

Demostració. Sigui $df(a)$ el diferencial de f en a. Per la definició de diferencial d'una funció (2.2.1.3) tenim que, per a qualsevol vector $\vec{h}$ de $\mathbb{R}^d$

$$f(a+\vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

Com que $df(a)$ és lineal, $df(a)(\vec{h}) \to (0,\dots,0) \Leftrightarrow \|\vec{h}\| \to 0$. Així veiem que

$$\lim_{\|\vec{h}\|\to 0} f(a+\vec{h}) - f(a) - df(a)(\vec{h}) = \mathrm{o}(\vec{h}).$$

I això compleix la definició de funció contínua (1.2.1.1), per tant f és contínua en el punt a. □

Proposició 2.2.1.6. *Siguin $U \subseteq \mathbb{R}^d$ un obert, $a \in U$ un punt i f una funció tal que*

$$\begin{aligned} f : U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a),\dots,f_m(a)). \end{aligned}$$

Aleshores

$$f \text{ és diferenciable en } a \Leftrightarrow f_i \text{ és diferenciable en } a \ \forall i \in \{1,\dots,m\}.$$

Demostració. Per la definició de diferencial d'una funció (2.2.1.3) tenim que, per a qualsevol vector $\vec{h}$ de $\mathbb{R}^d$

$$f(a+\vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

El que és equivalent a

$$\lim_{\|\vec{h}\|\to 0} \frac{f(a+\vec{h}) - f(a) - df(a)(\vec{h})}{\|\vec{h}\|} = 0.$$

Sabent que $f(a) = (f_1(a),\dots,f_m(a))$ podem entendre aquest límit com el següent, amb un vector al numerador, que descomponem com:

$$\lim_{\|\vec{h}\|\to 0} \frac{(f_1(a+\vec{h}) - f_1(a) - df_1(a)(\vec{h}),\dots,f_m(a+\vec{h}) - f_m(a) - df_m(a)(\vec{h}))}{\|\vec{h}\|} = 0,$$

si i només si

$$\lim_{\|\vec{h}\|\to 0} \frac{f_i(a+\vec{h}) - f_i(a) - df_i(a)(\vec{h})}{\|\vec{h}\|} = 0$$

per a tot $i \in \{1,\dots,m\}$.

Tenint en compte la definició de diferencial d'una funció (2.2.1.3), és equivalent a dir que, per a tot $i \in \{1,\dots,m\}$, f_i és diferenciable en el punt a. □

Proposició 2.2.1.7. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Aleshores tenim que*

1. *Donat un vector $\vec{u}$ de $\mathbb{R}^d$, $D_{\vec{u}}f(a)$ existeix i $df(a)(\vec{u}) = D_{\vec{u}}f(a)$.*
2. *El diferencial de f en a, $df(a)$, és únic.*

Demostració. Sigui $\vec{u}$ un vector de $\mathbb{R}^d$. Tenim que, si $\lambda \in \mathbb{R}$, $\lambda \neq 0$

$$f(a + \lambda\vec{u}) = f(a) + df(a)(\lambda\vec{u}) + \mathrm{o}(\lambda\vec{u})$$

$$f(a + \lambda\vec{u}) - f(a) = \lambda df(a)(\vec{u}) + \mathrm{o}(\lambda\vec{u})$$

$$\frac{f(a + \lambda\vec{u}) - f(a)}{\lambda} = df(a)(\vec{u}) + \frac{\mathrm{o}(\lambda\vec{u})}{\lambda}$$

Per tant, amb $\lambda \to 0$, per la definició de derivada direccional (2.2.1.1) tenim

$$D_{\vec{u}}f(a) = df(a)(\vec{u}).$$

Amb aquesta demostració també es veu la unicitat del diferencial d'una funció en un punt. □

Observació 2.2.1.8. *Com a conseqüència del primer apartat veiem que si f és diferenciable en a existeixen totes les seves derivades direccionals i que aquestes compleixen que, donats dos vectors $\vec{u}, \vec{v}$ i dos escalars λ, μ, $D_{\lambda\vec{u}+\mu\vec{v}}f(a) = \lambda D_{\vec{u}}f(a) + \mu D_{\vec{v}}(a)$.*

Teorema 2.2.1.9 (Condició suficient per a la diferenciabilitat)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}^m$ una funció, $a \in U$ un punt i $\mathrm{B}(a, \varepsilon)$, una bola centrada en a de radi $\varepsilon > 0$. Si les derivades direccionals de f, $D_i f(x)$, existeixen per a tot punt $x \in \mathrm{B}(a, \varepsilon)$, per a tot $i \in \{1, \ldots, d\}$ i són contínues en a, aleshores f és diferenciable en a.*

Demostració. Donat un vector $\vec{h}$ de $\mathbb{R}^d$, considerem la diferencia

$$f(a + \vec{h}) - f(a),$$

amb $a = (a_1, \ldots, a_d)$ i $\vec{h} = (h_1, \ldots, h_d) = \sum_{i=1}^{d} h_i\vec{e}_i$, on $\vec{e}_i$ és l'i-èsim vector de la base canònica, i denotarem $\vec{h}_n = \sum_{i=1}^{n} h_i\vec{e}_i$ per a $1 \leq n \leq d$ i $\vec{h}_0 = (0, \ldots, 0)$. Escrivim la suma telescòpica

$$f(a + \vec{h}) - f(a) = \sum_{i=1}^{d} \left(f(a + \vec{h}_i) - f(a + \vec{h}_{i-1}) \right). \tag{2.2}$$

El primer terme d'aquesta suma telescòpica és $f(a + h_1\vec{e}_1) - f(a)$, i per la definició de derivada direccional (2.2.1.1) això és

$$f(a + h_1\vec{e}_1) - f(a) = h_1 D_1 f(a) + h_1\, \mathrm{o}(\vec{h}),$$

i la resta de termes de (2.2) són

$$f(a + \vec{h}_{k-1} + h_k\vec{e}_k) - f(a + \vec{h}_{k-1}).$$

Veiem que aquestes expressions varien només en $h_k\vec{e}_k$, que correspon a la k-èsima component, i com que les derivades parcials de f existeixen, això vol dir que aquestes expressions són contínues, per tant podem aplicar el Teorema del Valor Mig (1.2.3.2) per a funcions d'una variable i tenim que, per a tot $2 \leq k \leq d$ existeix un escalar ξ_k tal que

$$f(a + \vec{h}_{k-1} + h_k\vec{e}_k) - f(a + \vec{h}_{k-1}) = h_k D_k f(\xi_k)$$

on ξ_k està al segment que uneix $a + \vec{h}_{k-1} + h_k\vec{e}_k$ i $a + \vec{h}_{k-1}$.

Ara notem que quan $\vec{h} \to 0$ tindrem $a + \vec{h}_{k-1} + h_k\vec{e}_k \to a$ i com que, per hipòtesi, les derivades direccionals són contínues

$$h_k D_k f(\xi_k) = h_k D_k f(a) + h_k \, \mathrm{o}(\vec{h})$$

i obtenim

$$\begin{aligned} f(a + \vec{h}) - f(a) &= \sum_{i=1}^{d} h_i D_i f(a) + \sum_{i=1}^{d} h_i \, \mathrm{o}(\vec{h}) \\ &= \sum_{i=1}^{d} D_{h_i\vec{e}_i} f(a) + \sum_{i=1}^{d} h_i \, \mathrm{o}(\vec{h}) \end{aligned}$$

i mentre $a + \vec{h} \in \mathrm{B}(a, \varepsilon)$, el que tenim satisfà la definició de diferencial d'una funció (2.2.1.3) per la proposició 2.2.1.7, i per tant f és diferenciable en a. □

Nota 2.2.1.10. *Notem que en aquesta demostració només hem hagut d'utilitzar la continuïtat de $d-1$ de les derivades parcials de f en a. per tant en veritat tenim prou amb veure que totes les derivades parcials de f existeixen en a i que almenys totes menys una d'aquestes són contínues en a per poder dir que f és diferenciable en a, però a aquest curs només es dona l'enunciat reduït.*

Proposició 2.2.1.11. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f, g : U \to \mathbb{R}^m$ dues funcions diferenciables en un punt $a \in U$ amb diferencials $df(a), dg(a)$, respectivament. Aleshores $f + g$ és diferenciable en a i té per diferencial $df(a) + dg(a)$.*

Demostració. Siguin $\vec{u}$ un vector de $\mathbb{R}^d$ i $D_{\vec{u}}f(a)$, $D_{\vec{u}}g(a)$ les derivades parcials de f i g, respectivament, en el punt a amb direcció $\vec{u}$. La derivada parcial de $f + g$ en a amb direcció $\vec{u}$ és $D_{\vec{u}}(f + g)(a)$. Com que les derivades direccionals es comporten, per definició, com les derivades d'una variable, tenim

$$D_{\vec{u}}f(a) + D_{\vec{u}}g(a) = D_{\vec{u}}(f + g)(a),$$

i per la proposició 2.2.1.7, com que l'argument no depèn de $\vec{u}$, ja hem acabat. □

2.2.2 La Matriu Jacobiana i la regla de la cadena

Definició 2.2.2.1 (Matriu Jacobiana)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Aleshores definim la matriu Jacobiana de f en a com

$$\begin{bmatrix} D_1 f_1(a) & D_2 f_1(a) & \cdots & D_d f_1(a) \\ D_1 f_2(a) & D_2 f_2(a) & \cdots & D_d f_2(a) \\ \vdots & \vdots & & \vdots \\ D_1 f_m(a) & D_2 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix}.$$

Proposició 2.2.2.2. *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$, $df(a)$ el diferencial de f en el punt a i $\vec{h} = (h_1, \ldots, h_d)$ un vector de $\mathbb{R}^d$. Aleshores*

$$df(a)(\vec{h}) = \begin{bmatrix} D_1 f_1(a) & \cdots & D_d f_1(a) \\ \vdots & & \vdots \\ D_1 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix} \begin{bmatrix} h_1 \\ \vdots \\ h_d \end{bmatrix},$$

és a dir, la matriu Jacobiana de f en a és la matriu associada del diferencial de f en el punt a.

Demostració. Observem que aquest enunciat té sentit per la definició de diferencial d'una funció (2.2.1.3) i la definició de matriu Jacobiana (2.2.2.1).

Donada la base canònica de $\mathbb{R}^d$, $(\vec{e_1}, \ldots, \vec{e_d})$, tenim

$$df(a)(\vec{h}) = \sum_{i=1}^{d} h_i df(a)(\vec{e_i}) = \sum_{i=1}^{d} h_i D_i f(a),$$

i si $f(a) = (f_1(a), \ldots, f_m(a))$,

$$D_i f(a) = \begin{bmatrix} D_i f_1(a) \\ \vdots \\ D_i f_m(a) \end{bmatrix}. \tag{2.3}$$

Per tant, podem reescriure aquestes dues igualtats com

$$df(a)(\vec{h}) = \begin{bmatrix} D_1 f(a) & \cdots & D_d f(a) \end{bmatrix} \begin{bmatrix} h_1 \\ \vdots \\ h_d \end{bmatrix}.$$

On, recordant (2.3),

$$\begin{bmatrix} D_1 f(a) & \cdots & D_d f(a) \end{bmatrix} = \begin{bmatrix} D_1 f_1(a) & D_2 f_1(a) & \cdots & D_d f_1(a) \\ D_1 f_2(a) & D_2 f_2(a) & \cdots & D_d f_2(a) \\ \vdots & \vdots & & \vdots \\ D_1 f_m(a) & D_2 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix}.$$

Així que

$$df(a)(\vec{h}) = \begin{bmatrix} D_1 f_1(a) & D_2 f_1(a) & \cdots & D_d f_1(a) \\ D_1 f_2(a) & D_2 f_2(a) & \cdots & D_d f_2(a) \\ \vdots & \vdots & & \vdots \\ D_1 f_m(a) & D_2 f_m(a) & \cdots & D_d f_m(a) \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_d \end{bmatrix}.$$

Així veiem que la matriu Jacobiana de f en a està ben definida com a matriu associada del diferencial de f en a. □

Observació 2.2.2.3. *Suposem $m = 1$. Recordant la definició de diferencial d'una funció (2.2.1.3) i denotant $x = a + \vec{h}$, $a = (a_1, \ldots, a_d)$, $x = (x_1, \ldots, x_d)$*

$$f(x) - f(a) - o(\|x - a\|) = df(a)(x - a)$$

i per la definició de matriu Jacobiana (2.2.2.1) tenim

$$f(x) - f(a) - \mathrm{o}(\|x-a\|) = \begin{bmatrix} D_1 f(a) & \cdots & D_d f(a) \end{bmatrix} \begin{bmatrix} x_1 - a_1 \\ \vdots \\ x_d - a_d \end{bmatrix}.$$

El que, quan $\vec{h} \to 0$*, ens diu que és una aproximació a*

$$(x_1 - a_1)D_1 f(a) + \cdots + (x_d - a_d)D_d f(a) = f(x) - f(a),$$

el que és un espai afí de dimensió $d+1$ *tangent a* f *en el punt* a*.*

Teorema 2.2.2.4 (Regla de la cadena)**.** *Siguin* $U \subseteq \mathbb{R}^d$ *un obert i* $f : U \to \mathbb{R}^m$ *una funció diferenciable en un punt* $a \in U$ *i siguin* $V \subseteq \mathbb{R}^m$ *un obert i* $g : V \to \mathbb{R}^p$ *una funció diferenciable en un punt* $f(a) = b \in V$*. Aleshores* $g(f(x))$ *és diferenciable en* a *amb diferencial* $dg(b)(df(a)(\vec{h}))$*, on* $df(a)$ *i* $dg(b)$ *són els diferencials de* f *i* g *en* a *i* b*, respectivament, i* $\vec{h}$ *és un vector de* $\mathbb{R}$*.*

Demostració. Per la definició de diferencial d'una funció (2.2.1.3), tenim

$$f(a + \vec{h}) = f(a) + df(a)(\vec{h}) + \mathrm{o}(\vec{h}), \quad \|\vec{h}\| \to 0.$$

Reescrivim amb $x = a + \vec{h}$ i $y = b + \vec{h}$

$$f(x) = f(a) + df(a)(x-a) + \mathrm{o}(x-a),$$

$$g(y) = g(b) + dg(b)(y-b) + \mathrm{o}(y-b).$$

Si fem $y = f(x)$ i substituïm en la segona equació obtenim

$$g(f(x)) = g(b) + dg(b)(f(a) + df(a)(x-a) + \mathrm{o}(x-a) - b) + \mathrm{o}(f(x) - b)$$

Si simplifiquem i utilitzem la linealitat del diferencial obtenim

$$g(f(x)) = g(b) + dg(b)(df(x-a)) + dg(b)(\mathrm{o}(x-a)) + \mathrm{o}(f(x) - b)$$

Ara només hem de veure que $dg(b)(\mathrm{o}(x-a))$ i $\mathrm{o}(f(x)-b)$ són $\mathrm{o}(x-a)$. El primer el podem veure amb que

$$\|dg(b)(\mathrm{o}(x-a))\| \leq \|dg(b)\|\,\mathrm{o}(\|x-a\|).$$

I com que quan $x \to a$, $f(a) \to b$ (donat per $\vec{h} \to 0$), ja que f és contínua. Aleshores podem escriure

$$f(x) - b = df(a)(x-a) + \mathrm{o}(x-a),$$

i observant el cas $x \to a$ trobem que $\|f(x) - b\| \leq C\|x-a\|$, on $C \in \mathbb{R}$ és la norma de l'aplicació lineal $dg(b)$. □

2.2.3 Gradient, punts crítics i extrems relatius

Definició 2.2.3.1 (Funció escalar)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}$ una funció. Direm que f és una funció escalar de d variables si f és diferenciable per a tot $x \in U$.

Definició 2.2.3.2 (Conjunts de nivell)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}$ una funció. Aleshores direm que, per a tot $C \in \mathbb{R}$,

$$L_C = \{x \in U : f(x) = C\}$$

és el conjunt de nivell C de la funció f.

Definició 2.2.3.3 (Gradient d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}$ una funció escalar. Definim el gradient de f en un punt $a \in U$ com el vector

$$\nabla f(a) = (D_1 f(a), \dots, D_d f(a)).$$

Proposició 2.2.3.4. *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}$ una funció escalar i $\vec{u} = (u_1, \dots, u_d$ un vector de $\mathbb{R}^d$. Aleshores*

$$\langle \nabla f(a), \vec{u} \rangle = D_{\vec{u}} f(a).$$

Demostració. Ho veiem per la definició de gradient d'una funció (2.2.3.3), la definició de derivada direccional (2.2.1.1) i l'observació 2.2.1.8. Tenim

$$\begin{aligned}
\langle \nabla f(a), \vec{u} \rangle &= u_1 D_1 f(a) + \cdots + u_d D_d f(a) && \text{(gradient d'una funció (2.2.3.3))} \\
&= D_{u_1 \vec{e}_1} f(a) + \cdots + D_{u_d \vec{e}_1} f(a) && \text{(derivada direccional (2.2.1.1))} \\
&= D_{u_1 \vec{e}_1 + \cdots + u_d \vec{e}_1} f(a) && \text{(Observació 2.2.1.8)} \\
&= D_{\vec{u}} f(a),
\end{aligned}$$

com volíem demostrar. □

Observació 2.2.3.5. *El gradient d'una funció en un punt és perpendicular al conjunt de nivell que conté el punt.*

Proposició 2.2.3.6. *Sigui $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}$ una funció escalar i $D_{\vec{u}} f(a)$ la derivada direccional de f en la direcció $\vec{u}$, on $\vec{u}$ és un vector de $\mathbb{R}^d$. Aleshores $D_{\vec{u}} f(a)$ és màxim $\iff$ $\vec{u} = \lambda \nabla f(a)$, amb $\lambda \in \mathbb{R}$.*

Demostració. Pel Teorema de la Desigualtat de Cauchy-Schwarz (1.2.3.3) tenim, amb $\|\vec{u}\| = 1$

$$-\|\nabla f(a)\| \leq \|\langle \nabla f(a), \vec{u} \rangle\| \leq \|\nabla f(a)\|$$
$$-\|\nabla f(a)\| \leq \|D_{\vec{u}}(a)\| \leq \|\nabla f(a)\|,$$

però si prenem $\vec{u} = \frac{\nabla f(a)}{\|\nabla f(a)\|}$ tenim $D_{\vec{u}} f(a) = \nabla f(a)$. Amb això es veu que el gradient d'una funció en un punt ens dona la direcció de màxim creixement de la funció en el punt. □

Observació 2.2.3.7. *Veiem que, donat que $\nabla f(a)$ ens diu la direcció de màxim creixement de f en el punt a, $-\nabla f(a)$ ens dirà la direcció de màxim decreixement de f en a.*

Definició 2.2.3.8 (Extrems relatius i punts crítics)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert, $a \in U$ un punt i $f : U \to \mathbb{R}$ una funció escalar. Direm que el punt a és un extrem relatiu de f si hi ha una bola de radi $r > 0$ centrada en el punt a, $\mathrm{B}(a, r)$, tal que, per a tot $x \in \mathrm{B}(a, r)$, $f(a) \geq f(x)$ (direm que a és un màxim relatiu) o tal que $f(a) \leq f(x)$ (direm que a és un mínim relatiu).

Si $f(a) \geq f(x)$ o $f(a) \leq f(x)$, per a tot $x \in U$, direm que a és un màxim o un mínim absolut de f en U, respectivament.

També direm que a és un punt crític si $\nabla f(a) = \vec{0}$.

Proposició 2.2.3.9. *Sigui $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}$ una funció escalar diferenciable en a. Aleshores*

$$a \text{ és un màxim o un mínim relatiu de } f \Longrightarrow \nabla f(a) = \vec{0}.$$

Demostració. Si $\vec{u}$ és un vector qualsevol de $\mathbb{R}^d$, la funció $f(a + t\vec{u})$, amb $t \in \mathbb{R}$ té un extrem relatiu en $t = 0$, i per tant la seva derivada ha de ser 0; $D_{\vec{u}} f(a) = 0$, i com això no depèn de $\vec{u}$, per la definició de gradient d'una funció (2.2.3.3), $D_{\vec{u}} = \langle \nabla f(a), \vec{u} \rangle = 0$, el que és equivalent a $\nabla f(a) = \vec{0}$. □

Observació 2.2.3.10. *Amb la definició de extrem relatiu (2.2.3.8) i la proposició 2.2.3.9 tenim que el punt a és un màxim o mínim relatiu de f si a és un punt crític de f.*

Definició 2.2.3.11 (Punt de sella d'una funció)**.** Sigui f una funció i a un punt del seu domini. Si a és un punt crític però no és ni màxim ni mínim local direm que a és un punt de sella de f.

Observem que aquesta definició té sentit per l'observació 2.2.3.10.

2.2.4 Canvis de coordenades diferenciables

Definició 2.2.4.1 (Homeomorfisme i difeomorfisme)**.** Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts i $\Phi : U \longleftrightarrow V$ una aplicació bijectiva tal que Φ, Φ^{-1} siguin contínues. Aleshores direm que Φ és un homeomorfisme. Si pensem Φ com

$$\begin{aligned} \Phi : U &\longleftrightarrow V \\ a &\longmapsto (v_1(a), \ldots, v_d(a)) \end{aligned}$$

aleshores donat un punt $a \in U$, interpretem $v_1(a), \ldots, v_d(a)$ com les noves coordenades del punt a. Amb aquest nou sistema els punts que fan d'eixos de coordenades, que són les famílies de punts definits per

$$\{x \in U : v_i(x) = v_j(a) \Leftrightarrow i \neq j, \forall i, j \in \{1, \ldots, d\}\},$$

que són tots els punts amb totes les coordenades iguals, excepte la j-èsima.

Si Φ, Φ^{-1} són diferenciables direm que és un canvi de coordenades diferenciable o que és un difeomorfisme.

Proposició 2.2.4.2. *Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts i $\Phi : U \longleftrightarrow V$ un difeomorfisme. Aleshores*

$$d(\Phi^{-1}) = (d\Phi)^{-1}.$$

Demostració. Sabem que Φ^{-1} existeix i és diferenciable per la definició de difeomorfisme (2.2.4.1); direm que Φ és diferenciable en un punt a, amb diferencial $d\Phi(a)$ i Φ^{-1} és diferenciable en un punt $b = \Phi(a)$, amb diferencial $d\Phi^{-1}(a)$. Volem veure que $d(\Phi^{-1}) = (d\Phi)^{-1}$.

Considerem la funció $\Phi^{-1}(\Phi)$ i un vector $\vec{h}$ de $\mathbb{R}^d$ fixe. Aleshores el seu diferencial en a aplicat a $\vec{h}$ és, pel Teorema de la regla de la cadena (2.2.2.4)

$$Id_U(a) = d((\Phi^{-1}(\Phi))(a))(\vec{h}) = d((\Phi^{-1})(b))(d\Phi(a)(\vec{h}))$$

i

$$Id_V(b) = d(\Phi((\Phi^{-1}))(b))(\vec{h}) = d(\Phi(a))(d\Phi^{-1}(b)(\vec{h}))$$

Amb això tenim que $d(\Phi^{-1})$ també és la inversa de $d\Phi$ pels dos costats, i per tant $d(\Phi^{-1}) = (d\Phi)^{-1}$, com volíem demostrar. □

Corol·lari 2.2.4.3. *Donada una funció Φ un difeomorfisme diferenciable en un punt a. Aleshores*

$$\det(df(a)) \neq 0.$$

Definició 2.2.4.4 (Derivades parcials d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $a = (a_1, \ldots, a_d)$ un punt de U i f una funció definida per

$$\begin{aligned} f : U &\longrightarrow \mathbb{R}^m \\ a &\longmapsto (f_1(a), \ldots, f_m(a)). \end{aligned}$$

Aleshores, donat un $t \in \mathbb{R}$, direm que la derivada parcial de f respecte la seva i-èsima coordenada és

$$\frac{\partial f}{\partial x_i}(a) = \lim_{t \to 0} \frac{f(a_1, \ldots, a_i + t, \ldots, a_d) - f(a)}{t}.$$

Notem que això és equivalent a derivar respecte la i-èsima variable prenent les altres variables com a constants.

Proposició 2.2.4.5. *Siguin $U, V \subset \mathbb{R}^d$ dos oberts i $\Phi : U \to V$ un difeomorfisme tal que donat un punt $a \in U$, $\Phi(a) = (\Phi_1(a), \ldots, \Phi_d(a)) = (v_1, \ldots, v_d)$. Aleshores, donada una funció $f : U \to V$,*

$$\frac{\partial f}{\partial v_i} = \sum_{j=1}^{d} \frac{\partial f}{\partial x_j} \frac{\partial x_j}{\partial v_i}.$$

Demostració. □

2.3 Teoremes de la funció implícita i inversa

2.3.1 Dependència i independència funcional

Definició 2.3.1.1 (Dependència funcional)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^m$ una funció. Donades $v_1, \ldots, v_k : U \to \mathbb{R}$ k funcions, direm que f depèn funcionalment de $v_1, \ldots, v_k$ si existeix una funció $h : \mathbb{R}^k \to \mathbb{R}^m$ tal que

$$f(x) = h(v_1(x), \ldots, v_k(x)), \ \forall x \in U.$$

Proposició 2.3.1.2. *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}^m$ una funció i $v_1, \dots, v_d$, d funcions escalars sobre U que defineixen un sistema de coordenades que anomenarem $\Phi(x) = (v_1(x), \dots, v_d(x))$. Aleshores, donat un $k < d$ els següents enunciats són equivalents:*

1. *f depèn funcionalment de $v_1, \dots, v_k$ per a tot $x \in U$.*
2. *$\nabla f(x)$ és combinació lineal de $\nabla v_1(x), \dots, \nabla v_k(x)$ per a tot $x \in U$.*
3. *La matriu que té per files $\nabla v_1(x), \dots, \nabla v_k(x)$ i $\nabla f(x)$ té rang k per a tot $x \in U$.*
4. *$\frac{\partial f}{\partial v_{k+1}} = \cdots = \frac{\partial f}{\partial v_d} = 0$*

Teorema 2.3.1.3. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \dots, v_k \in \mathcal{C}^1$ $k < d$ funcions escalars definides en U. Aleshores, donat un punt $a \in U$ i un real $\varepsilon > 0$, les funcions $v_1, \dots, v_k$ formen un sistema de coordenades en $\mathrm{B}(\varepsilon, a) \subset U$ si i només si els seus gradients en a, $\nabla v_1(a), \dots, \nabla v_k(a)$, són linealment independents.*

Demostració. Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \dots, v_k \in \mathcal{C}^1$ k funcions escalars definides en U que formen un sistema de coordenades en $\mathrm{B}(\varepsilon, a) \subset U$. Considerem les $d - k$ funcions escalars definides en U $v_{k+1}, \dots, v_d$ tal que $v_1, \dots, v_d$ formin un sistema de coordenades de U. Per la proposició 2.3.1.2 tenim que aquestes d funcions són funcionalment independents, el que ens diu que el determinant de la matriu composta per els seus gradients en un punt x, $\nabla v_1(x), \dots, \nabla v_d(x)$ té determinant no nul per a tot $x \in U$. Per tant, tenim que $\nabla v_1(x), \dots, \nabla v_d(x)$ són linealment independents per a tot $x \in U$ i, en particular, que $\nabla v_1(a), \dots, \nabla v_k(a)$ són linealment independents. □

2.3.2 Varietats

Definició 2.3.2.1 (Varietat)**.** Siguin, amb $m < d$, $U \subseteq \mathbb{R}^m$, $S \subseteq \mathbb{R}^d$ dos oberts, $M \subseteq \mathbb{R}^d$ un conjunt i $r > 0$ un radi. Aleshores, si per a tot punt $p \in M$, existeix un homeomorfisme $H : U \to S \cap \mathrm{B}(p, r)$ direm que M és una varietat de dimensió m de $\mathbb{R}^d$.

Definició 2.3.2.2 (Varietat regular)**.** Siguin, amb $m < d$, $U \subseteq \mathbb{R}^m$, $S \subseteq \mathbb{R}^d$ dos oberts amb $(0, \dots, 0) = 0 \in U$. Aleshores, donat un conjunt $M \subseteq \mathbb{R}^d$, direm que M és una varietat regular de dimensió m o una varietat diferenciable de classe $\mathcal{C}^1$ i de dimensió m si per a tot punt $p \in M$ existeix un homeomorfisme $H : U \to \mathrm{B}(p, r) \cap S$ tal que $H(0) = p$ i el diferencial de H en $t \in U$, $dH(t)$, tingui rang m per a tot $t \in U$.

Si $m = 1$ tindrem un arc regular, i si $m = 2$ parlarem de superfície regular.

Observació 2.3.2.3. *Un cas particular d'aquesta definició és el dels gràfics. En aquest cas tenim que si*

$$\begin{aligned} H : U &\longleftrightarrow \mathrm{B}(p, r) \cap S \\ t &\longmapsto (h_1(t), \dots, h_d(t)) \end{aligned}$$

aleshores m de les components de H fan de paràmetres; suposem que són els m primers, així H seria de la forma

$$H(t_1, \dots, t_m) = (t_1, \dots, t_m, h_{m+1}(t_1, \dots, t_m), \dots, h_d(t_1, \dots, t_m)).$$

Definició 2.3.2.4 (Espai tangent en un punt)**.** Siguin $U \subseteq \mathbb{R}^m$, $S \subseteq \mathbb{R}^d$ dos oberts i $M \subseteq \mathbb{R}^m$ una varietat regular de dimensió m. Això vol dir que per a tot punt $t \in M$ existeix un homeomorfisme $H : U \to S \cap \mathrm{B}(p, r)$ amb $H(0) = p$. Aleshores definim l'espai tangent a M en p com

$$T_p(M) = \{\vec{h} \text{ un vector de } \mathbb{R}^d : dH(0)(x) = \vec{h}, \text{ per a algun } x \in \mathbb{R}^d\},$$

això és l'imatge de $dH(0)$.

Proposició 2.3.2.5. *Siguin $U \subseteq \mathbb{R}^m$ un obert, M una varietat regular de dimensió m d'un obert $S \subseteq \mathbb{R}^d$, $p \in M$ un punt i*

$$\begin{aligned} H : U &\longleftrightarrow \mathrm{B}(p, r) \cap S \\ t &\longmapsto (h_1(t), \ldots, h_d(t)) \end{aligned}$$

un homeomorfisme tal que $H(0) = p$. Aleshores l'espai tangent a M en un punt $p \in M$, $T_p(M)$, té dimensió m i la seva base és

$$\left(\left(\frac{\partial h_1}{\partial t_1}, \ldots, \frac{\partial h_d}{\partial t_1}\right), \ldots, \left(\frac{\partial h_1}{\partial t_d}, \ldots, \frac{\partial h_d}{\partial t_d}\right)\right).$$

Demostració. Considerem la matriu Jacobiana (2.2.2.1) de H en 0. Per hipòtesi, aquesta té rang m. Aleshores, per la definició d'espai tangent en p tenim

$$T_p(M) = \{\vec{h} \text{ un vector de } \mathbb{R}^d : dH(0)(x) = \vec{h}, \text{ per a algun } x \in \mathbb{R}^d\},$$

per tant, els elements de $T_p(M)$ venen donades pel sistema lineal

$$\begin{bmatrix} D_1h_1(0) & D_2h_1(0) & \cdots & D_mh_1(0) \\ D_1h_2(0) & D_2h_2(0) & \cdots & D_mh_2(0) \\ \vdots & \vdots & & \vdots \\ D_1h_d(0) & D_2h_d(0) & \cdots & D_mh_d(0) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{bmatrix} = \begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_d \end{bmatrix}.$$

Per tant, $T_p(M)$ està generat per les columnes de $dH(0)$, i la seva base és

$$(D_1H(0), \ldots, D_dH(0)),$$

que és equivalent a

$$\left(\left(\frac{\partial h_1}{\partial t_1}, \ldots, \frac{\partial h_d}{\partial t_1}\right), \ldots, \left(\frac{\partial h_1}{\partial t_d}, \ldots, \frac{\partial h_d}{\partial t_d}\right)\right).$$

Amb això també veiem que $T_p(M)$ té dimensió m. □

Proposició 2.3.2.6. *Siguin $U \subseteq \mathbb{R}^d$ un obert, $v_1, \ldots, v_k \in \mathcal{C}^1$ $k < d$ funcions escalars definides en U funcionalment independents en cada punt de U de forma que els conjunts de nivell arc-connexos*

$$M = \{x \in U : v_1(x) = c_1, \ldots, v_k(x) = c_k\}$$

siguin varietats regulars de dimensió $m = d - k$. Aleshores, donada una funció $f : U \to \mathbb{R}^m$ diferenciable depèn funcionalment de $v_1, \ldots, v_k$ si i només si $\nabla f(x)$ és combinació lineal de $\nabla v_1(x), \ldots, \nabla v_k(x)$ per a tot $x \in U$.

Demostració. La implicació cap a la dreta ($\Rightarrow$) està vista a la proposició 2.3.1.2. Fem l'altre implicació ($\Leftarrow$). Per l'observació 2.2.3.5, el subespai generat pels gradients $\nabla v_1(x), \ldots, \nabla v_k(x)$ és ortogonal a l'espai tangent $T_x(M)$. Per tant, per a tot vector $\vec{u}$ de $T_x(M)$ tindrem $D_{\vec{u}} f(x) = 0$, el que significa que $f(x)$ serà constant en M, és a dir, $f(x) = (k_1, \ldots, k_m)$ per a tot $x \in U$ tal que $f(x) \in M$. Aleshores existeix una funció $H : U \to M$ tal que

$$f(x) = H(v_1(x), \ldots, v_k(x)). \qquad \square$$

2.3.3 Teorema de la funció inversa

Proposició 2.3.3.1. *Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts i $f : U \leftrightarrow V$ un homeomorfisme diferenciable en un punt $a \in U$, amb inversa $g = f^{-1}$. Aleshores, g és diferenciable en $f(a)$ si i només si la Jacobiana de f en a té determinant diferent de zero.*

Demostració. Demostrem la implicació cap a la dreta ($\Rightarrow$). En un entorn de a, f es comporta com un difeomorfisme per la definició de difeomorfisme (2.2.4.1). Per tant, amb el corol·lari 2.2.4.3 queda demostrat.

Demostrem ara l'altre implicació ($\Leftarrow$). Denotem $x = a + \vec{h}$, on $\vec{h}$ és un vector de $\mathbb{R}^d$. Per tant tenim, que amb un cert vector $\vec{k}$ de $\mathbb{R}^d$,

$$f(a + \vec{h}) = f(a) + \vec{k},$$

i com que per la definició de homeomorfisme (2.2.4.1) f és un homeomorfisme tenim que $\vec{h} \to 0$ si i només si $\vec{k} \to 0$. Per tant

$$\vec{k} = f(a + \vec{h}) - f(a)$$

i per la definició de diferencial d'una funció (2.2.1.3) quan $\vec{k} \to 0$

$$\vec{k} = f(a + \vec{h}) - f(a) = df(a)(\vec{h}) + \mathrm{o}(\vec{h}).$$

Aplicant $df(a)^{-1}$ als costats de la igualtat tenim

$$df(a)^{-1}(\vec{k}) = df(a)^{-1}(df(a)(\vec{h}) + \mathrm{o}(\vec{h})),$$

i com que $df(a)^{-1}$ és lineal per la definició de diferencial d'una funció (2.2.1.3) tenim que

$$df(a)^{-1}(\vec{k}) = df(a)^{-1}(df(a)(\vec{h})) + df(a)^{-1}(\mathrm{o}(\vec{h})),$$

i aleshores

$$\vec{h} = df(a)^{-1}(\vec{k}) - df(a)^{-1}(\mathrm{o}(\vec{h})),$$

que és equivalent a, amb $b = f(a)$,

$$g(b + \vec{k}) - g(b) = df(a)^{-1}(\vec{k}) - df(a)^{-1}(\mathrm{o}(\vec{h})).$$

Ara en veure que $df(a)^{-1}(\mathrm{o}(\vec{h}))$ és com $\mathrm{o}(\vec{k})$ haurem acabat.

Això ho podem veure fent

$$\|df(a)^{-1}(\vec{k})\| + \|df(a)^{-1}(\mathrm{o}(\vec{h}))\| \leq \|df(a)^{-1}\|\|\vec{k}\| + \|df(a)^{-1}\|\|\mathrm{o}(\vec{h})\|.$$

I per tant, quan $\vec{h} \to 0$ tenim $\mathrm{o}(\vec{h}) \to 0$ i $\vec{k} \to 0$, i veiem que $df(a)^{-1}(\mathrm{o}(\vec{h}))$ ha de ser com $\mathrm{o}(\vec{k})$. $\square$

Lemma 2.3.3.2. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^d$ una funció de classe $\mathcal{C}^1$ amb diferencial de f en un punt $a \in U$ de norma m, $df(a)$, invertible amb inversa $df(a)^{-1}$. Aleshores existeix una bola tancada centrada en a de radi $r > 0$, $\overline{\mathrm{B}}(a, r)$, que, per a tot $x, y \in \overline{\mathrm{B}}(a, r)$ compleix*

1. $\det(df(x)) \neq 0$
2. $\|df(x) - df(a)\| \leq \frac{m}{2}$
3. $\frac{m}{2}\|x - y\| \leq \|f(x) - f(y)\| \leq \frac{3m}{2}\|x - y\|$

Demostració. Observem que el punt (1) és cert ja que si r és prou petita, per la proposició 2.2.1.5, f és contínua.

Per veure el punt (2) tenim que pel Teorema de l'equivalència entre normes (1.2.3.1) existeix $C \in \mathbb{R}$ tal que

$$\|df(x) - df(a)\| \leq C \sum_{i=1}^{n} \sum_{j=1}^{n} \left| \frac{\partial f_i}{\partial x_j}(x) - \frac{\partial f_i}{\partial x_j}(a) \right|,$$

i de nou, per a r prou petita, com que f és contínua, això és arbitràriament petit, i tenim $\|df(x) - df(a)\| \leq \frac{m}{2}$.

Per tant, de moment tenim que, amb r prou petit, existeix una bola tancada $\overline{\mathrm{B}}(a, r)$ que compleix els punts (1) i (2); en veure que *2* $\Rightarrow$ *3* haurem acabat aquesta part.

Considerem l'aplicació $\widehat{f}(x) = f(x) - df(a)(x)$ amb diferencial $d\widehat{f} = d\widehat{f}(x) - d\widehat{f}(a)$. Per el punt (2) i el Teorema del Valor Mig (1.2.3.2) tenim, per a $x, y \in \overline{\mathrm{B}}(a, r)$,

$$\|f(x) - f(y) - df(a)(x - y)\| = \|\hat{f}(x) - \hat{f}(y)\| \leq \frac{m}{2}\|x - y\|.$$

Notem que, per a una funció T amb inversa T^{-1} per la definició de norma d'una aplicació lineal (1.1.1.2) tenim que existeix $K \in \mathbb{R}$ tal que

$$\|T(u)\| \leq K\|u\|,$$

per tant

$$\|T^{-1}(u)\| \leq K\|u\|.$$

Amb això veiem que existeix una m tal que $\|df(a)(x-y)\| \leq m\|x-y\|$, i aleshores

$$\big|\|f(x) - f(y)\| - \|df(a)(x - y)\|\big| \leq \|f(x) - f(y) - df(a)(x - y)\| \leq \\ \leq \frac{m}{2}\|x - y\| \leq \frac{1}{2}\|df(a)(x - y)\|.$$

amb el que obtenim

$$\frac{1}{2}\|df(a)(x - y)\| \leq \|f(x) - f(y)\| \leq \frac{3}{2}\|df(a)(x - y)\|,$$

i per tant

$$\frac{m}{2}\|x - y\| \leq \|f(x) - f(y)\| \leq \frac{3m}{2}\|x - y\|. \qquad \square$$

Teorema 2.3.3.3 (Teorema de la funció inversa)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^d$ una funció de classe $\mathcal{C}^1$ amb diferencial de f en un punt $a \in U$, $df(a)$, invertible. Aleshores existeix un obert $W \subset U$ que conté a tal que, la restricció de f en W sigui un difeomorfisme.*

Demostració. Sigui $df(a)^{-1}$ la inversa del diferencial de f en a, $df(a)$, i $M = \frac{1}{m} = \|df(a)^{-1}\|$ la seva norma. Per la definició de norma d'una aplicació lineal (1.1.1.2) tenim que per a qualsevol vector $\vec{u}$ de $\mathbb{R}^d$,

$$\|df(a)(\vec{u})\| \leq m\|\vec{u}\|.$$

Pel lemma 2.3.3.2 tenim que existeix una bola tancada centrada en a de radi $r > 0$, $\overline{\mathrm{B}}(a, r)$, que, per a tot $x, y \in \overline{\mathrm{B}}(a, r)$ compleix

1. $\det(df(x)) \neq 0$
2. $\|df(x) - df(a)\| \leq \frac{m}{2}$
3. $\frac{m}{2}\|x - y\| \leq \|f(x) - f(y)\| \leq \frac{3m}{2}\|x - y\|$

Considerem S, la frontera de $\overline{\mathrm{B}}(a, r)$, que és compacte. Per tant, el conjunt

$$S' = \{f(x) : \forall x \in S\},$$

que és la imatge de S respecte f també és compacte i no conté $f(a)$, ja que $r > 0$. Aleshores considerem

$$d = \inf_{x \in S'} \|f(a) - x\| > 0$$

com la distància mínima de la imatge de a respecte f al conjunt S', i definim la bola oberta centrada en $f(a)$ de radi $\frac{d}{2}$, $\mathrm{B}\left(f(a), \frac{d}{2}\right)$, i així $\|y - f(a)\| < \|y - f(x)\|$ per a tot $x \in S$. Ara considerem l'obert

$$W = \left\{x \in \overline{\mathrm{B}}(a, r) : f(x) \in \mathrm{B}\left(f(a), \tfrac{d}{2}\right)\right\}.$$

Pel punt (3) veiem que la restricció de f en $\overline{\mathrm{B}}(a, r)$ és injectiva i, per tant, la restricció de f en W també és injectiva. Ara només ens queda veure que la restricció de f en W és exhaustiva i ja haurem acabat. Per a això hem de veure que per a tot $p \in \mathrm{B}\left(f(a), \frac{d}{2}\right)$ existeix un $q \in \overline{\mathrm{B}}(a, r)$ tal que $f(q) = p$.

Si entenem f com $f(a) = (f_1(a), \ldots, f_d(a))$ i un punt $p \in \mathrm{B}\left(f(a), \frac{d}{2}\right)$ com $p = (p_1, \ldots, p_d)$, podem considerar la funció h tal que

$$h(x) = \|p - f(x)\| = \sum_{i=1}^{d} (p_i - f_i(x))^2.$$

Aleshores h té un mínim absolut en el compacte $\overline{\mathrm{B}}(a, r)$, que s'assoleix quan $x = q \in \overline{\mathrm{B}}(a, r)$. Per tant, per la proposició 2.2.3.9, $D_j h(q) = 0$, per a tot $j \in \{1, \ldots, d\}$, que és equivalent a dir

$$\sum_{i=1}^{d} D_j f_i(p)(p_i - f_i(q)) = 0, \quad \forall j \in \{1, \ldots, d\}.$$

Així hem vist que la restricció de f en W és exhaustiva, i per tant bijectiva, i ja teníem que era contínua. Podem veure de nou pel punt (3) del lema 2.3.3.2 que la seva inversa també és contínua. Amb tot això en tenim prou per dir que la restricció de f en W és un homeomorfisme diferenciable en un punt a però, com que, per hipòtesi, tenim $\det(df(a)) \neq 0$, amb la proposició 2.3.3.1 queda demostrat el teorema. □

Corol·lari 2.3.3.4. *Una aplicació $f : U \to \mathbb{R}^d$ de classe $\mathcal{C}^1$ és un difeomorfisme si i només si f és injectiva i $\det(df(a)) \neq 0$ per a tot $x \in U$.*

Proposició 2.3.3.5. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \ldots, v_k \in \mathcal{C}^1$ un sistema de k funcions escalars definides en U. Aleshores, els seus gradients són linealment independents en un punt $a \in U$ si i només si aquest sistema de k funcions escalars formen part d'un sistema de coordenades local en a.*

Demostració. La matriu formada pels gradients de $v_1, \ldots, v_k$ en a té un menor d'ordre k no nul. Per tant, podem expandir aquest sistema de k funcions amb $d-k$ funcions escalars definides en U de classe $\mathcal{C}^1$, $v_{k+1} \ldots, v_d$ amb gradients linealment independents en a, i aquestes d funcions, $v_1, \ldots, v_d$, formen un sistema de coordenades local en a. □

Corol·lari 2.3.3.6. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $v_1, \ldots, v_k \in \mathcal{C}^1$ un sistema de k funcions escalars definides en U. Aleshores una funció f definida en un entorn d'un punt a depèn funcionalment de $v_1, \ldots, v_k$ en un entorn del punt a si i només si $\nabla f(x)$ és combinació lineal de $\nabla v_1(x), \ldots, \nabla v_k(x)$ per a tot x en un entorn del punt a.*

2.3.4 Teorema de la funció implícita

Notació 2.3.4.1. Podem interpretar $\mathbb{R}^d$ com $\mathbb{R}^d = \mathbb{R}^k \times \mathbb{R}^m$, on $d = k + m$. Per tant, denotarem un punt $a = (a_1, \ldots, a_d)$ de $\mathbb{R}^d$ com $a = (a'; a'')$, on a' correspon a $(a_1, \ldots, a_k)$ i a'' a $(a_{k+1}, \ldots, a_d)$.

També entenem que $a' \in \mathbb{R}^k$ i $a'' \in \mathbb{R}^m$.

Teorema 2.3.4.2 (Teorema de la funció implícita)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $a = (a'; a'') \in U$ un punt, $v_1, \ldots, v_k \in \mathcal{C}^1$ un sistema de $k = d - m$ funcions escalars definides en U tals que $v_1(a) = \cdots = v_k(a) = 0$ i els seus gradients en a, $\nabla v_1(a), \ldots, \nabla v_k(a)$ són linealment independents i M un conjunt definit per $M = \{x \in U : v_1(x) = \cdots = v_k(x) = 0\}$. Aleshores hi ha un obert $W \subset \mathbb{R}^d$ que conté a, un obert $U'' \subset \mathbb{R}^m$ que conté a'' i una única funció $h : U'' \to \mathbb{R}^k$ tal que*

$$\begin{aligned} M :&= \{x \in U : v_1(x) = \cdots = v_k(x) = 0\} = \\ &= \{x = (x'; x'') \in W : x' = h(x''), x'' \in U''\}. \end{aligned}$$

Demostració. Per començar definirem un obert $W \subseteq \mathbb{R}^d$, un obert $V \subseteq \mathbb{R}^d$ tal que $(0, \ldots, 0) \in V$ i un difeomorfisme Φ tals que

$$\begin{aligned} \Phi : W &\longleftrightarrow V \\ x = (x_1, \ldots, x_d) &\longmapsto (v_1(x), \ldots, v_k(x), x_{k+1}, \ldots, x_d), \end{aligned}$$

així $(v_1(x), \ldots, v_k(x), x_{k+1}, \ldots, x_d)$ forma un sistema de coordenades en W.

Observem que podem considerar $a = (0, \dots, 0)$ ja que si $(v_1(a), \dots, v_k(a)) = (c_1, \dots, c_k)$ podem treballar amb les funcions $v_1'(x) = v_1(x) - c_1, \dots, v_k'(x) = v_k(x) - c_k$ que compleixen $v_1'(a) = \cdots = v_k'(a) = 0$.

Com que Φ és un difeomorfisme, per la definició de difeomorfisme (2.2.4.1) és bijectiva, prenem la seva inversa

$$\begin{aligned} \Phi^{-1} : V &\longleftrightarrow W \\ y = (y_1, \dots, y_d) &\longmapsto (u_1(y), \dots, u_k(y), y_{k+1}, \dots, y_d), \end{aligned}$$

i, de nou, com que Φ és un difeomorfisme per la definició de difeomorfisme (2.2.4.1) tenim que $u_1, \dots, u_k \in \mathcal{C}^1$.

Aleshores, per a tot $x \in M$ tenim $\Phi(x) = (0'; x'')$. Definim un conjunt

$$U'' = \{y'' \in \mathbb{R}^m : (0; y'') \in V\},$$

i com que Φ és una bijecció, ja que és un difeomorfisme, tenim

$$U'' = \{x'' \in \mathbb{R}^m : \text{Existeix } x' \in \mathbb{R}^k \text{ tal que } (x'; x'') \in M \cap W\}.$$

Aleshores U'' és un obert de $\mathbb{R}^d$ i

$$M = \{(x'; x'') \in W : (u_1(0; x''), \dots, u_k(0; x''); y'') \text{ amb } y'' \in U''\},$$

i la funció que volíem demostrar que existeix és

$$h(x'') = (u_1(0; x''), \dots, u_k(0; x'')). \qquad \square$$

2.4 Extrems relatius

2.4.1 El mètode de multiplicadors de Lagrange

Teorema 2.4.1.1 (Multiplicadors de Lagrange)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, S un conjunt definit per*

$$S = \{x \in U : g(x) = (g_1(x), \dots, g_k(x)) = 0\},$$

on $g_1, \dots, g_k$ són $k < d$ funcions escalars definides en U de classe $\mathcal{C}^1$.

Considerem la funció escalar $f : S \to \mathbb{R}$ tal que $a \in S$ sigui un màxim o un mínim relatiu de f en S i les funcions $g_1, \dots, g_k$ siguin funcionalment independents en a. Aleshores existeixen $\lambda_1, \dots, \lambda_k$ reals tals que

$$D_i f(a) + \sum_{j=1}^{k} \lambda_j D_i g_j(a) = 0, \quad \forall i \in \{1, \dots, d\}.$$

Demostració. Siguin $\lambda_1, \dots, \lambda_k$, aleshores considerem el següent sistema d'equacions lineals

$$\sum_{j=1}^{k} \lambda_j D_i g_j(a) = -D_i f(a) \quad \forall i \in \{1, \dots, k\} \tag{2.4}$$

Com que $g_1, \dots, g_k$ són funcionalment independents en a, la matriu formada pels gradients de $g_1, \dots, g_k$ en a té rang k (proposició 2.3.1.2) el sistema d'equacions

lineals (2.4) té una única solució. Ara només ens cal veure que aquests mateixos reals $\lambda_1, \dots, \lambda_k$ també són solució de les $m = d - k$ equacions restants.

Per fer això ens caldrà el Teorema de la funció implícita (2.3.4.2). Com que $k < d$, amb la notació introduïda a 2.3.4.1, denotem el punt a amb $a = (a'; a'')$, on $a' = (a_1, \dots, a_k)$ i $a'' = (a_{k+1}, \dots, a_d)$ i entenem $a' \in \mathbb{R}^k, a'' \in \mathbb{R}^m$. Aleshores definim una funció $g(x) = (g_1(x), \dots, g_k(x))$, que compleix $g(a', a'') = 0$ i $g \in \mathcal{C}^1$. Això, junt amb que per hipòtesi les funcions $v_1, \dots, v_k$ són funcionalment independents en a i, per la proposició 2.3.1.2, la matriu

$$\begin{bmatrix} D_1 g_1(a) & \cdots & D_k g_1(a) \\ \vdots & & \vdots \\ D_1 g_k(a) & \cdots & D_k g_k(a) \end{bmatrix}$$

té determinant diferent de zero, complim les condicions del Teorema de la funció implícita (2.3.4.2) i l'apliquem. Per tant, existeix un obert $U'' \subset \mathbb{R}^m$ que conté a'' i una única funció $h : U'' \to \mathbb{R}^k$, $h \in \mathcal{C}^1$ amb $h(x) = (h_1(x), \dots, h_k(x))$, tal que $h(a'') = a'$ i que per a tot $y'' \in U''$ compleix $g(h(y''); y'') = 0$. Això significa que el sistema d'equacions

$$g_i(x_1, \dots, x_d) = 0, \quad \forall i \in \{1, \dots, d\},$$

té una única solució de la forma $a' = h(a'')$, per tant definim les funcions, definides en U'',

$$F(y'') = f(h(y''); y'')$$

i, per a tot $i \in \{1, \dots, k\}$

$$G_i(y'') = g_i(h(y''); y'').$$

Degut a que $G_1 = \cdots = G_k = 0$, les seves derivades també són 0. □

2.4.2 Teorema del rang constant

No fer molt cas d'aquesta part. La faré bé quan sàpiga geometria diferencial. La part important d'aquí és l'últim corol·lari que ens diu que els difeomorfismes "conserven" els punts crítics.

Definició 2.4.2.1 (Subvarietat regular)**.** Sigui $U \subseteq \mathbb{R}^d$ un obert i $M \subseteq U$ un conjunt. Direm que M és una subvarietat regular de dimensió m si per a tot punt $p \in M$ existeix una bola centrada en p de radi $r > 0$, $\mathrm{B}(p, r) \subseteq U$, i $k = d - m$ funcions escalars, $v_1, \dots, v_k \in \mathcal{C}^1$, definides en U amb gradients linealment independents tals que

$$M \cap \mathrm{B}(p, r) = \{x \in \mathrm{B}(p, r) : v_1(x) = \cdots = v_k(x) = 0\}.$$

Proposició 2.4.2.2. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $M \subseteq U$ una subvarietat regular de dimensió m de $\mathbb{R}^d$. Aleshores, les afirmacions següents són equivalents:*

1. *Per a tot punt $p \in M$ existeix una bola centrada en p de radi $r > 0$, $\mathrm{B}(p, r) \subseteq U$, i $k = d - m$ funcions escalars, $v_1, \dots, v_k \in \mathcal{C}^1$, definides en U amb gradients linealment independents tals que*

$$M \cap \mathrm{B}(p, r) = \{x \in \mathrm{B}(p, r) : v_1(x) = \cdots = v_k(x) = 0\}.$$

2. *Per a tot punt $p \in M$ existeix un obert $V \subseteq U$ que conté p i un sistema de coordenades $u_1, \dots, u_d$ definit en V tal que*

$$M \cap V = \{x \in V : u_{k+1}(x) = \cdots = u_d(x) = 0\}.$$

3. *Per a tot punt $p \in M$ existeixen un obert $B \subseteq U$ que conté p, un obert $W \subseteq \mathbb{R}^m$ i un homeomorfisme $\Phi : W \to M \cap B$.*

Demostració. no □

Teorema 2.4.2.3 (Teorema del rang constant)**.** *Sigui $U \subseteq \mathbb{R}^m$ un obert i $H : U \to \mathbb{R}^d$ una funció de classe $\mathcal{C}^1$, amb $\operatorname{rang}(dH(t)) = n$ per a tot $t \in U$. Aleshores el conjunt*

$$\{y \in \mathbb{R}^d : y = H(x) \text{ per algun } x \in U\}$$

és una subvarietat de dimensió n.

Demostració. Considerem $H(x) = (h_1(x), \dots, h_d(x))$ i fixem un punt $a \in U$ on es compleixin les condicions de la hipòtesi. Per la proposició 2.3.1.2, hi haurà n components de H tals que els seus gradients siguin linealment independents en a. Existeix una permutació $\sigma \in S_d$ tal que aquestes n components de H siguin $h_{\sigma(1)} \dots, h_{\sigma(n)}$.

Per continuïtat, els gradients $\nabla h_{\sigma(1)}(x), \dots, \nabla h_{\sigma(n)}(x)$ són linealment independents per a tot x en un entorn obert de a, que denotarem per $V \subset U$. Per tant, podem expandir-les a un sistema de coordenades de V, $v_1, \dots, v_m$, on $v_i = h_{\sigma(i)}$, $\forall i \in \{1, \dots, n\}$. Com que $\operatorname{rang}(dH(t)) = n$ per a tot $t \in V$, per la proposició 2.3.1.2, els gradients $\nabla h_{\sigma(n+1)}, \dots, \nabla h_{\sigma(d)}$ depenen linealment dels gradients $\nabla v_1, \dots, \nabla v_n$ en V, per tant, pel corol·lari 2.3.3.6, per a cada $i \in \{n+1, \dots, d\}$, existeix una funció φ_i que compleix $h_{\sigma(i)}(x) = \varphi_i(v_1(x), \dots, v_n(x))$ i per tant, si denotem $v(x) = (v_1(x), \dots, v_n(x))$,

$$\begin{aligned} H(x) &= G(v_1(x), \dots, v_n(x)) \\ &= (v_1(x), \dots, v_n(x), \varphi_{n+1}(v(x)), \dots, \varphi_d(v(x))) \end{aligned}$$

i es compleix la definició de subvarietat regular (2.4.2.1) per la proposició 2.4.2.2, ja que, per la definició de homeomorfisme (2.2.4.1), G és un homeomorfisme definit en V. □

Proposició 2.4.2.4. *Siguin $U, V \subseteq \mathbb{R}^d$ dos oberts, $\Phi : U \longleftrightarrow V$ un difeomorfisme de classe $\mathcal{C}^1$ i $M \subseteq U$ una varietat regular de dimensió m de U. Aleshores la imatge de M per Φ és una subvarietat regular de dimensió m de V.*

Demostració. No fer-ne molt cas. Per la definició de varietat regular (2.3.2.2), per a cada punt $p \in M$ existeixen $k = d - m$ equacions escalars, $v_1, \dots, v_k$ definides en U amb gradients linealment independents i una bola de radi $r > 0$ centrada en p, $\mathrm{B}(p, r)$, tals que

$$M \cap \mathrm{B}(p, r) = \{x \in \mathrm{B}(p, r) : v_1(x) = \cdots = v_k(x) = 0\}.$$

Aleshores definim, per a tot $j \in \{1, \dots, k\}$, $u_j(x) = \Phi^{-1}(v_j(x))$. Aleshores tenim que si la imatge de M per Φ és $N \subset V$, per a tot punt $q \in N$ hi ha una bola de radi $r > 0$, $\mathrm{B}(q, r)$, tal que

$$N \cap \mathrm{B}(q, r) = \{y \in \mathrm{B}(q, r) : u_1(x) = \cdots = u_k(x) = 0\},$$

i tenim que $u_1, \dots, u_d$ tenen gradients linealment independents, ja que, pel Teorema de la regla de la cadena (2.2.2.4), $\nabla v_j(x) = (d\Phi(x))^t(\nabla u_j(\Phi(x)))$, i com que Φ defineix un sistema de coordenades, per la proposició 2.3.1.2 els gradients de $u_1, \dots, u_d$ són linealment independents, i això compleix la definició de subvarietat regular (2.4.2.1). □

Corol·lari 2.4.2.5. *$d\Phi(a)(T_a(M)) = T_{\Phi(a)}(\Phi(M))$.*

2.4.3 Derivades d'ordre superior

Fixem-nos en que en derivar una funció f obtenim una altre funció, i que aquesta, sota certes condicions, és derivable. En aquest capítol estudiarem algunes de les propietats d'aquest fet.

Definició 2.4.3.1 (n-èsima derivada d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $\vec{v}_1, \dots, \vec{v}_n$ n vectors de $\mathbb{R}^d$ (no necessàriament diferents) i $f : U \to \mathbb{R}^m$ una funció diferenciable en un punt $a \in U$. Si $\frac{\partial f}{\partial \vec{v}_1}$ és diferenciable en a i prenem la seva derivada respecte $\vec{v}_2$ diem que

$$d^2 f(a)(\vec{v}_2, \vec{v}_1) = \frac{\partial}{\partial \vec{v}_2}\left(\frac{\partial f}{\partial \vec{v}_1}\right)(a) = \frac{\partial^2 f}{\partial \vec{v}_2 \partial \vec{v}_1}(a) = D_{\vec{v}_2,\vec{v}_1} f = D_{\vec{v}_2}(D_{\vec{v}_1} f)(a)$$

és la derivada de segon ordre de f o la segona derivada de f.

Si la segona derivada de f també és derivable podem parlar de la tercera derivada de f, que és la segona derivada de $\frac{\partial f}{\partial \vec{v}_1}$. Si iterem la suposició podem definir la n-èsima derivada de f o una derivada d'ordre n de f. També direm que f és n-vegades diferenciable en a. Ho denotarem amb

$$d^n f(a)(\vec{v}_n \dots \vec{v}_1) = \frac{\partial^n f}{\partial \vec{v}_n \cdots \partial \vec{v}_1} = D_{\vec{v}_n,\dots,\vec{v}_1} f(a).$$

Teorema 2.4.3.2. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}^d$ una funció 2-vegades diferenciable en $a \in U$, aleshores*

$$D_{\vec{v},\vec{u}} f(a) = D_{\vec{u},\vec{v}} f(a).$$

Demostració. Notem que podem dir $f(x) = (f_1(x), \dots, f_m(x))$, on $f_1, \dots, f_m$ són funcions escalars definides en U, i per la proposició 2.2.1.6 només cal que fem la demostració pel cas $m = 1$, ja que implicarà el general. També observem que podem donar un canvi de variables on els vectors $\vec{v}, \vec{u}$ siguin els nous eixos de coordenades, $\vec{e}_1, \vec{e}_2$ respectivament. En aquesta base tindríem que volem demostrar $D_{1,2} f(a) = D_{2,1} f(a)$, i com que això només afecta a una component del punt, podem considerar $d = 2$, i la demostració serà suficient per veure cas general. Per tant, ho demostrem per $m = 1, d = 2$. Aprofitant el canvi de coordenades també suposarem $a = (0, 0)$. Per tant, només hem de demostrar que $D_{2,1} f(0, 0) = D_{1,2} f(0, 0)$.

Considerem, amb un escalar $h > 0$, la següent diferencia:

$$Q(h) = f(h, h) - f(h, 0) - (f(0, h) - f(0, 0)) \tag{2.5}$$

Si fem $A(t) = f(t, h) - f(t, 0)$ tenim $Q(h) = A(h) - A(0)$, i pel Teorema del Valor Mig (1.2.3.2) existeix un escalar $0 < \xi < h$ tal que

$$A(h) - A(0) = hA'(\xi) = h(D_1 f(\xi, h) - D_1 f(\xi, 0)) \tag{2.6}$$

i com que, per hipòtesi, $D_1 f$ és diferenciable en $(0,0)$, per l'observació 2.2.2.3 podem escriure,

$$D_1 f(x,y) = D_1 f(0,0) + xD_{1,1} f(0,0) + yD_{2,1} f(0,0) + \mathrm{o}(\|x,y\|).$$

Ho apliquem a (2.6) i obtenim

$$\begin{aligned} hA'(c) = h\big(&D_1 f(0,0) + \xi D_{1,1} f(0,0) + \\ &+ hD_{2,1} f(0,0) - D_1 f(0,0) - \xi D_{1,1} f(0,0) + \mathrm{o}(|h|)\big) \end{aligned}$$

simplifiquem, i per la definició de $Q(h)$, (2.5),

$$hA'(c) = h^2 D_{2,1} f(0,0) + \mathrm{o}(h^2) = Q(h).$$

i tenim

$$\lim_{h\to 0} \frac{Q(h)}{h^2} = D_{2,1} f(0.0).$$

Repetint el mateix argument amb

$$Q(h) = f(h,h) - f(0,h) - (f(h,0) - f(0,0))$$

obtenim

$$\lim_{h\to 0} \frac{Q(h)}{h^2} = D_{1,2} f(0,0),$$

i per tant

$$D_{2,1} f(0,0) = D_{1,2} f(0,0). \qquad \square$$

Nota 2.4.3.3. *Sospito que una demostració "més general" seria similar a la del Teorema d'una condició suficient per a la diferenciabilitat (2.2.1.9), per si algun valent no ha quedat satisfet.*

Corol·lari 2.4.3.4. *$d^2 f(a)$ és una aplicació bilineal simètrica. De fet, si generalitzem la proposició iterant-la, tenim que $d^n f(a)$ és una aplicació n-lineal simètrica.*

2.4.4 Fórmula de Taylor en múltiples variables

Aquesta secció la farem considerant només funcions escalars (amb $m = 1$ en la notació que hem estat utilitzant). En el cas de voler fer el desenvolupament de Taylor d'una funció f amb $m > 1$ només pensar f com un vector de m funcions escalars, $f(x) = (f_1(x), \ldots, f_m(x))$, i per tant el problema queda reduït a calcular m desenvolupaments de Taylor (donat que es satisfacin certes condicions que estudiarem més endavant) i posar-los en forma de vector.

Notació 2.4.4.1. Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}$ una funció n-vegades diferenciable en un punt $a \in U$ i un altre punt de U, $t = (t_1, \ldots, t_d)$. Introduïm la següent notació:

$$f^{(k)}[a,t] = \sum_{i_k=1}^{d} \cdots \sum_{i_1=1}^{d} D_{i_k,\ldots,i_1} f(a) t_{i_1} \ldots t_{i_k}.$$

Teorema 2.4.4.2 (Fórmula de Taylor en múltiples variables)**.** *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}$ una funció n-vegades diferenciable en un punt $a \in U$ i $b \in U$ un altre punt. Aleshores existeix un punt $z \in U$ tal que, per a algun $0 < \xi < 1$, $z = a + (b - \xi a)$ (això és que el punt z es troba en el segment que uneix els punts a i b) tal que*

$$f(b) - f(a) = \sum_{k=1}^{n-1} \frac{1}{k!} f^{(k)}[a, b-a] + \frac{1}{n} f^{(n)}[z, b-a].$$

Demostració. Com que, per hipòtesi, U és obert, per la definició de conjunt obert (1.3.0.1) sabem que existeix un $\varepsilon > 0$ tal que, per a tot $-\varepsilon < t < 1 + \varepsilon$, tenim que $a + t(b-a) \in S$. Per tant, definim una funció g com

$$\begin{aligned} g : (-\varepsilon, 1+\varepsilon) &\to \mathbb{R} \\ t &\mapsto f(a + t(b-a)) \end{aligned}$$

Aleshores $f(b) - f(a) = g(1) - g(0)$. Aleshores, amb $\xi \in (0,1)$, pel Teorema de Taylor (1.2.3.4) tenim

$$g(1) - g(0) = \sum_{k=1}^{n-1} \frac{1}{k!} g^{(k)}(0) + \frac{1}{m!} g^{(n)}(\xi). \tag{2.7}$$

Si pensem, amb $h(\xi) = a + \xi(b-a)$, que $g(\xi) = f(p(\xi))$, ha de ser $p(\xi) = (p_1(\xi), \ldots, p_d(\xi))$, i si denotem $a = (a_1, \ldots, a_d), b = (b_1, \ldots, b_d)$, tenim, amb $i \in \{1, \ldots, d\}$, que $\frac{\partial p}{\partial x_i}(\xi) = b_i - a_i$. Aplicant el Teorema de la regla de la cadena (2.2.2.4) veiem que g' està definida en $(-\varepsilon, 1+\varepsilon)$ i

$$g'(\xi) = \sum_{i=1}^{d} D_i f(p(\xi))(b_i - a_i) = f^{(1)}[p(\xi), b-a],$$

i aplicant la regla de la cadena una segona vegada,

$$g''(\xi) = \sum_{j=1}^{d} \sum_{i=1}^{d} D_{j,i} f(p(\xi))(b_i - a_i)(b_j - a_j) = f^{(2)}[p(\xi), b-a].$$

Si ho iterem n vegades obtindrem que

$$g^{(n)}(t) = f^{(n)}[p(\xi), b-a],$$

i per tant, recordant (2.7), tenim

$$f(b) - f(a) = \sum_{k=1}^{n-1} \frac{1}{k!} f^{(k)}[a, b-a] + \frac{1}{n} f^{(n)}[z, b-a]$$

amb $z = p(\xi)$. □

2.4.5 Extrems lliures

En aquest apartat utilitzarem el que vam veure a l'observació 2.4.3.4 per classificar els extrems lliures d'una funció.

Això ens servirà per a classificar els punts crítics d'una funció escalar en un conjunt del seu domini, excloent-ne la frontera. Per exemple, en el cas d'utilitzar el Teorema dels multiplicadors de Lagrange (2.4.1.1) per obtenir un conjunt de punts crítics en el domini restringit de la funció. Més tard veurem com classificar els que es troben a la frontera.

Proposició 2.4.5.1. *Siguin $U \subseteq \mathbb{R}^d$ un obert i $f : U \to \mathbb{R}$ una funció 2-vegades diferenciable en un punt $a \in U$ amb segones derivades contínues, i a és un punt crític de f. Aleshores*

1. *$d^2 f(a)$ és definida estrictament positiva $\Rightarrow$ a és un mínim relatiu.*
2. *$d^2 f(a)$ és definida estrictament negativa $\Rightarrow$ a és un màxim relatiu.*
3. *$d^2 f(a)$ és definida positiva $\Leftarrow$ a és un mínim relatiu.*
4. *$d^2 f(a)$ és definida negativa $\Leftarrow$ a és un màxim relatiu.*

Demostració. Comencem demostrant dels punts (1) i (2), que són demostracions anàlogues. Suposem que $d^2 f(a)$ és definida positiva, i considerem el punt $t \in U$, $t = (t_1, \dots, t_d)$ i la funció

$$Q(t) = \tfrac{1}{2} f^{(2)}[a, t] = \sum_{j=0}^{d} \sum_{i=0}^{d} D_{j,i} f(a) t_i t_j.$$

Per hipòtesi, Q és contínua per a tot punt $t \in U$. També tenim, per la definició de n-èsima derivada d'una funció (2.4.3.1), que $Q(t)$ és definida positiva per a tot $t \neq (0, \dots, 0)$.

Definim ara la bola tancada de radi 1 centrada en a, $\overline{\mathrm{B}}(a, 1) \subset U$ i la seva frontera, $S = \mathrm{Fr}(\overline{\mathrm{B}}(a, 1))$. Com que S és compacte, pel Teorema de Weierstrass (1.2.3.5) Q té un mínim relatiu en S, suposem que en aquest punt Q val m. Com que Q és definida estrictament positiva per a tot punt de S, $m > 0$.

Sabent que Q és una forma bilineal simètrica, tenim que, per a tot $c \in \mathbb{R}$, $Q(ct) = c^2 Q(t)$. Si considerem $c = \frac{1}{\|t\|}$, per a $t \neq (0, \dots, 0)$, tenim que $ct \in S$, i per tant $Q(ct) \geq m$, el que significa $Q(t) \geq m\|t\|^2$.

Pel Teorema de la fórmula de Taylor en múltiples variables (2.4.4.2) i la definició de gradient d'una funció (2.2.3.3) tenim

$$f(a + t) - f(a) = \langle \nabla f(a), t \rangle + \tfrac{1}{2} f^{(2)}[z, t],$$

per a algun $z = a + t + (a - \xi(a + t))$, amb $0 < \xi < 1$. Però com que a és un punt crític de f (observació 2.2.3.10), tenim $\nabla f(a) = 0$, i per tant

$$f(a + t) - f(a) = \tfrac{1}{2} f^{(2)}[z, t],$$

i si escrivim $\|t^2\| \, \mathrm{o}(t) = \frac{1}{2} f^{(2)}[z, t] - \frac{1}{2} f^{(2)}[a, t]$ tenim

$$f(a + t) - f(a) = \tfrac{1}{2} f^{(2)}[a, t] + \|t^2\| \, \mathrm{o}(t).$$

Per tant

$$f(a + t) - f(a) = Q(t) + \|t\|^2 \, \mathrm{o}(t) \geq m\|t\|^2 + \|t\|^2 \, \mathrm{o}(t). \tag{2.8}$$

Com que $\mathrm{o}(t) \to 0$ és si i només si $t \to 0$, existeix un $\varepsilon > 0$ tal que, amb $0 < \|t\| < \varepsilon$ tenim $\mathrm{o}(t) < \frac{m}{2}$, i $0 \leq \|t\|^2 \mathrm{o}(t) < \frac{m}{2}\|t\|^2$, i així

$$f(a+t) - f(a) > m\|t\|^2 - \frac{m}{2}\|t\|^2 = \frac{m}{2}\|t\|^2 > 0,$$

i, com que això no depèn de t, per la definició de extrem relatiu (2.2.3.8) tenim que a és un mínim relatiu. Ara només ens queda demostrar (3) i (4), de nou, només ens caldrà demostrar-ne una, ja que l'altre demostració serà anàloga. Suposem doncs que a és un mínim relatiu.

Seguint l'argument sobre la fórmula de Taylor per a múltiples variables que hem fet a la primera meitat d'aquesta demostració arribem a la desigualtat (2.8) i tenim

$$f(a+t) - f(a) \leq m\|t\|^2 + \|t\|^2 \mathrm{o}(t).$$

Aleshores

$$\frac{f(a+t) - f(a)}{\|t\|^2} \leq m + \mathrm{o}(t).$$

Per la definició de extrem relatiu (2.2.3.8) tenim $f(a+t) - f(a) \geq 0$, i per tant, quan $t \to 0$, aleshores $\mathrm{o}(t) \to 0$ i

$$0 \leq \frac{f(a+t) - f(a)}{\|t\|^2} \leq m,$$

i ja hem acabat. □

Capítol 3

Càlcul integral

3.1 Introducció

3.1.1 Funcions integrables Riemann

Definició 3.1.1.1 (Rectangle)**.** Siguin $[a_1, b_1], \ldots, [a_d, b_d] \subset \mathbb{R}$ d intervals tancats. Direm que $\mathfrak{R} = [a_1, b_1] \times \cdots \times [a_d, b_d]$ és un rectangle de $\mathbb{R}^d$.

Definició 3.1.1.2 (Partició d'un rectangle i finor d'una partició)**.** Siguin $\mathfrak{R} = [a_1, b_1] \times \cdots \times [a_d, b_d]$ un rectangle de $\mathbb{R}^d$ i P_i una partició de $[a_i, b_i]$ per a tot $i \in \{1, \ldots, d\}$. Aleshores $P = P_1 \times \cdots \times P_d$ és una partició de $\mathfrak{R}$.

Si $P_i = \{t_{i,0}, \ldots, t_{i,n}\}$, amb $a_i = t_{i,0} < \cdots < t_{i,n} = b_i$, direm que els rectangles definits per $[t_{1,i_1}, t_{1,i_1+1}] \times \cdots \times [t_{d,i_d}, t_{d,i_d+1}] \subset \mathfrak{R}$, amb $0 \leq i_j \leq d-1$ per a tot $j \in \{1, \ldots, d\}$, són subrectangles de $\mathfrak{R}$.

Sigui Q una altre partició de $\mathfrak{R}$. Direm que Q és més fina que P si $P \subset Q$.

Definició 3.1.1.3 (Suma superior i inferior)**.** Sigui $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, P una partició i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Per a cada subrectangle de $\mathfrak{R}$, $\mathfrak{R}_i$, amb $i \in I$, on I és el conjunt d'índexs que denoten els subrectangles de $\mathfrak{R}$ definits per P, definim la suma superior de f per P com

$$\mathrm{S}(f, P) = \sum_{i \in I} \sup_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i|,$$

i la suma inferior de f per P com

$$\mathrm{s}(f, P) = \sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i|.$$

Proposició 3.1.1.4. *Siguin P, Q dues particions d'un rectangle $\mathfrak{R} \subset \mathbb{R}^d$ i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores, si Q és més fina que P,*

$$\mathrm{s}(f, P) \leq \mathrm{s}(f, Q),$$

i

$$\mathrm{S}(f, Q) \leq \mathrm{S}(f, P).$$

Demostració. Demostrarem només la primera desigualtat, ja que la segona té una demostració anàloga. Comencem notant que podem fer la demostració suposant $P = P_1 \times \cdots \times P_d$, on $P_i = t_{i,0} < \cdots < t_{i,n}$ és una partició de $[a_i, b_i]$ i $Q = Q_1 \times \cdots \times Q_d$, on, per a tot $j \in \{1, \ldots, d\} \setminus k$, $P_j = Q_j$, i $Q_k = t_{k,0} < \cdots < t_{k,l} < q < t_{k,l+1} < \cdots < t_{k,n}$, per algun $l \in \{0, \ldots, n-1\}$. Suposarem $l = 0, k = 1$ per simplificar la notació. Aleshores, considerant la definició de suma inferior de f per una partició tenim

$$\mathrm{s}(f, P) = \sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i|,$$

on I és el conjunt d'índexs dels subrectangles de $\mathfrak{R}$ definits per P.

Observem que tots els subrectangles de $\mathfrak{R}$ són els mateixos respecte les particions P i Q, excepte els que s'obtenen fent $\{t_{1,0}, q, t_{1,1}\} \times Q_2 \times \cdots \times Q_d$. Per tant, els únics termes del sumatori que canvien són, amb un nou conjunt d'índexs J, per a tot $j \in J$,

$$\inf_{x \in \mathfrak{R}_j} f(x) |\mathfrak{R}_j|.$$

Ara considerem el conjunt d'índex dels rectangles definits per $\{t_{1,0}, t_{1,1}\} \times Q_2 \times \cdots \times Q_d$, $I' \subset I$, i tenim

$$\sum_{i' \in I'} \inf_{x \in \mathfrak{R}_{i'}} f(x) |\mathfrak{R}_{i'}| \leq \sum_{j \in J} \inf_{x \in \mathfrak{R}_j} f(x) |\mathfrak{R}_j|.$$

I per tant

$$\begin{aligned} \sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| &= \sum_{i \in I \setminus I'} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| + \sum_{i' \in I'} \inf_{x \in \mathfrak{R}_{i'}} f(x) |\mathfrak{R}_{i'}| \leq \\ &\leq \sum_{j \in J} \inf_{x \in \mathfrak{R}_j} f(x) |\mathfrak{R}_j| + \sum_{i \in I \setminus J} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| = \sum_{i \in I \cup J} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i|. \end{aligned}$$

però

$$\sum_{i \in I} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| = \mathrm{s}(f, P)$$

i

$$\sum_{i \in I \cup J} \inf_{x \in \mathfrak{R}_i} f(x) |\mathfrak{R}_i| = \mathrm{s}(f, Q). \qquad \square$$

Proposició 3.1.1.5. *Siguin P, Q dues particions arbitràries d'un rectangle $\mathfrak{R} \subset \mathbb{R}^d$ i $f : \mathfrak{R} \to \mathbb{R}^d$ una funció acotada. Aleshores*

$$\mathrm{s}(f, P) \leq \mathrm{S}(f, Q).$$

Demostració. Considerem la partició definida per $P \cup Q$. Com que $Q \subseteq P \cup Q$ i $Q \subseteq P \cup Q$, $P \cup Q$ és més fina que P i Q. Per tant, per la proposició 3.1.1.4, tenim

$$\mathrm{s}(f, P) \leq \mathrm{s}(f, P \cup Q) \leq \mathrm{S}(f, P \cup Q) \leq \mathrm{S}(f, Q). \qquad \square$$

Definició 3.1.1.6 (Integral superior i inferior)**.** Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$ i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores definim la integral superior de f en $\mathfrak{R}$ com

$$\int^{\mathfrak{R}^+} f = \inf_{P \in \mathcal{P}} \mathrm{S}(f, P)$$

i la integral inferior de f en $\mathfrak{R}$ com

$$\int_{\mathfrak{R}^-} f = \sup_{P\in\mathcal{P}} \mathrm{s}(f,P),$$

on $\mathcal{P}$ és el conjunt de particions de $\mathfrak{R}$.

Proposició 3.1.1.7. *Siguin R un rectangle de $\mathbb{R}^d$ i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores*

$$\int_{\mathfrak{R}^-} f \leq \int^{\mathfrak{R}^+} f.$$

Demostració. Sigui $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$. Com que, per la proposició 3.1.1.5, tenim $\mathrm{s}(f,P) \leq \mathrm{S}(f,Q)$ per a $P, Q \in \mathcal{P}$ arbitraris, ha de ser

$$\int_{\mathfrak{R}^-} f = \sup_{P\in\mathcal{P}} \mathrm{s}(f,P) \leq \inf_{P\in\mathcal{P}} \mathrm{S}(f,P) = \int^{\mathfrak{R}^+} f. \qquad \square$$

Definició 3.1.1.8 (Funció integrable Riemann)**.** Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$ i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Direm que f és integrable Riemann si $\int_{\mathfrak{R}^-} f = \int^{\mathfrak{R}^+} f$.

També direm que $\int_{\mathfrak{R}} f = \int_{\mathfrak{R}^-} f = \int^{\mathfrak{R}^+} f$ és la integral Riemann de f en $\mathfrak{R}$.

Teorema 3.1.1.9 (Criteri d'integrabilitat Riemann)**.** *Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$, $\{\mathfrak{R}_i\}_{i\in I}$ la família de subrectangles de $\mathfrak{R}$ definits per P i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores f és integrable Riemann si i només si per a tot $\varepsilon > 0$ existeix una partició P tal que*

$$\mathrm{S}(f,P) - \mathrm{s}(f,P) = \sum_{i\in I} \left(\sup_{x\in\mathfrak{R}_i} f(x) - \inf_{x\in\mathfrak{R}_i} f(x) \right) |\mathfrak{R}_j| < \varepsilon.$$

Demostració. Comencem demostrant que la condició és necessària ($\Rightarrow$). Sigui $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$. Per la definició de funció integrable Riemann (3.1.1.8) i la definició de integral superior i inferior (3.1.1.6) tenim

$$\sup_{P\in\mathcal{P}} \mathrm{s}(f,P) = \int_{\mathfrak{R}^-} f = \int_{\mathfrak{R}} f = \int^{\mathfrak{R}^+} f = \inf_{P\in\mathcal{P}} \mathrm{S}(f,P),$$

per tant, existeixen un $\varepsilon > 0$ i unes particions $P, Q \in \mathcal{P}$ tals que

$$-\frac{\varepsilon}{2} + \int_{\mathfrak{R}} f < \mathrm{s}(f,P),$$

i

$$\mathrm{S}(f,Q) < \frac{\varepsilon}{2} + \int_{\mathfrak{R}} f.$$

Per la proposició 3.1.1.4 tenim $\mathrm{s}(f,P) \leq \mathrm{s}(f,P\cup Q) \leq \mathrm{S}(f,P\cup Q) \leq \mathrm{S}(f,Q)$, per tant ha de ser $\mathrm{S}(f,P\cup Q) - \mathrm{s}(f,P\cup Q) < \varepsilon$, com calia veure.

Per demostrar que la condició és suficient ($\Leftarrow$) veiem que, per hipòtesi,

$$0 \leq \int^{\mathfrak{R}^+} f - \int_{\mathfrak{R}^-} f \leq \mathrm{S}(f,P) - \mathrm{s}(f,P) < \varepsilon,$$

i quan $\varepsilon \to 0$ ha de ser, per la definició de funció integrable Riemann (3.1.1.8),

$$\int^{\mathfrak{R}^+} f = \int_{\mathfrak{R}^-} f = \int_{\mathfrak{R}} f. \qquad \square$$

Notació 3.1.1.10 (Límit d'una partició)**.** Sigui $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$. Quan vulguem parlar d'una partició de $\mathfrak{R}$ que es fa fina ho denotarem amb

$$\lim_{P \in \mathcal{P}},$$

que es refereix a definir una partició P de $\mathfrak{R}$ tal que

$$\max_{i \in I} \left\{ \max_{x,y \in \mathfrak{R}_i} \|x - y\| \right\} \to 0$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per P.

Corol·lari 3.1.1.11. *Si $\mathcal{P}$ és el conjunt de particions de $\mathfrak{R}$, aleshores f és integrable Riemann si i només si*

$$\lim_{P \in \mathcal{P}} \mathrm{S}(f, P) - \mathrm{s}(f, P) = 0.$$

Teorema 3.1.1.12. *Siguin $\mathfrak{R}$ un rectangle de $\mathbb{R}^d$ i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada i contínua. Aleshores f és integrable Riemann en $\mathfrak{R}$.*

Demostració. Pel Teorema de Heine (1.3.0.4), f és uniformement contínua en $\mathfrak{R}$, per tant, per la definició de continuïtat uniforme (1.3.0.3), donat un $\varepsilon > 0$ hi ha un $\delta > 0$ tal que

$$|f(x) - f(y)| < \frac{\varepsilon}{|\mathfrak{R}|} \text{ si } \|x - y\| < \delta.$$

Sigui $\{\mathfrak{R}_i\}_{i \in I}$ el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició P de $\mathfrak{R}$ tal que

$$\max_{i \in I} \left\{ \max_{x,y \in \mathfrak{R}_i} \|x - y\| \right\} < \delta,$$

això és que els diàmetres dels subrectangles definits per la partició P estiguin fitats per δ.

Considerem

$$\mathrm{S}(f, P) - \mathrm{s}(f, P) = \sum_{i \in I} \left(\sup_{x \in \mathfrak{R}_i} f(x) - \inf_{x \in \mathfrak{R}_i} f(x) \right) |\mathfrak{R}_i|. \tag{3.1}$$

Com que, per hipòtesi, f és contínua en cada $\mathfrak{R}_i$, pel Teorema de Weierstrass (1.2.3.5) tenim que els màxims i mínims de f en cada $\mathfrak{R}_i$ són accessibles. Denotem doncs amb M_i, m_i els punts de $\mathfrak{R}_i$ tals que $f(M_i) = \max_{x \in \mathfrak{R}_i} f(x)$ i $f(m_i) = \min_{x \in \mathfrak{R}_i} f(x)$. Per (3.1) tindrem $\|M_i - m_i\| < \delta$, i com que f és contínuament uniforme en cada $\mathfrak{R}_i$, $f(M_i) - f(m_i) < \frac{\varepsilon}{|\mathfrak{R}|}$, i per tant tenim

$$\mathrm{S}(f, P) - \mathrm{s}(f, P) = \sum_{i \in I} \left(\sup_{x \in \mathfrak{R}_i} f(x) - \inf_{x \in \mathfrak{R}_i} f(x) \right) |\mathfrak{R}_i| \leq \frac{\varepsilon}{|\mathfrak{R}|} \sum_{i \in \mathfrak{R}_i} |\mathfrak{R}_i| = \varepsilon,$$

i això completa la prova. $\square$

3.1.2 La integral com a límit de sumes

Definició 3.1.2.1 (Suma de Riemann)**.** Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada i P una partició de $\mathfrak{R}$. Aleshores definim la suma de Riemann de f associada a P com

$$\Sigma(f, P) = \sum_{i \in I} f(\xi_i)|\mathfrak{R}_i|,$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per P i ξ_i és un punt qualsevol de $\mathfrak{R}_i$, per a tot $i \in I$.

Observació 3.1.2.2.

$$\mathrm{s}(f, P) \leq \Sigma(f, P) \leq \mathrm{S}(f, P).$$

Proposició 3.1.2.3. *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$ i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores f és integrable Riemann si i només si existeix un $L \in \mathbb{R}$ tal que*

$$\lim_{P \in \mathcal{P}} \Sigma(f, P) = L.$$

Demostració. Pel corol·lari 3.1.1.11 tenim

$$\lim_{P \in \mathcal{P}} \mathrm{S}(f, P) = \lim_{P \in \mathcal{P}} \mathrm{s}(f, P),$$

i per l'observació 3.1.2.2 i el Teorema del sandvitx (1.2.3.6) ha de ser

$$\lim_{P \in \mathcal{P}} \mathrm{S}(f, P) = \lim_{P \in \mathcal{P}} \Sigma(f, P) = \lim_{P \in \mathcal{P}} \mathrm{s}(f, P),$$

i amb això es veu que ha de existir un real L tal que $\lim_{P \in \mathcal{P}} \Sigma(f, P) = L$. □

Notació 3.1.2.4. Seguint el resultat de la proposició 3.1.2.3 denotarem

$$\int_{\mathfrak{R}} f(x)dx = \Sigma(f, P_n) = \sum_{i \in I} f(x)|\mathfrak{R}_i| = L.$$

on $\int$ es refereix al sumatori infinit, $f(\xi_i)$ es transforma en $f(x)$ i $|\mathfrak{R}_i|$ s'escriu dx, tot quan fem la partició "infinitament més fina", amb el límit $\lim_{P \in \mathcal{P}} P$.

3.1.3 Propietats de la integral Riemann definida

Proposició 3.1.3.1. *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f, g : \mathfrak{R} \to \mathbb{R}$ dues funcions integrables Riemann. Aleshores són certs els següents enunciats:*

1. *Siguin λ, μ dos escalars. Aleshores*

$$\int_{\mathfrak{R}} (\lambda f + \mu g) = \lambda \int_{\mathfrak{R}} f + \mu \int_{\mathfrak{R}} g.$$

2. *La funció producte fg també és integrable Riemann.*

3. Sigui C un escalar. Si $f(x) \leq Cg(x)$ per a tot $x \in \mathfrak{R}$, aleshores

$$\int_{\mathfrak{R}} f \leq C \int_{\mathfrak{R}} g.$$

Demostració. Sigui $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$.

Comencem demostrant el punt (1), Per la proposició 3.1.2.3 i la definició de suma de Riemann (3.1.2.1) tenim

$$\sum_{i \in I} \left(\lambda f(\xi_i) + \mu g(\xi_i)\right) |\mathfrak{R}_i|,$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició $P \in \mathcal{P}$ i ξ_i és un punt qualsevol de $\mathfrak{R}_i$ per a tot $i \in I$. Això ho podem reescriure com

$$\lambda \sum_{i \in I} f(\xi_i)|\mathfrak{R}_i| + \mu \sum_{i \in I} g(\xi_i)|\mathfrak{R}_i|$$

i per tant

$$\int_{\mathfrak{R}} (\lambda f + \mu g) = \lambda \int_{\mathfrak{R}} f + \mu \int_{\mathfrak{R}} g,$$

com volíem demostrar.

Demostrem ara el punt (2) (En veritat la demostraré quan em doni la gana, i resulta que això no és ara).

Podem veure el punt (3) a partir del punt (1), ja que si $f(x) \leq Cg(x)$ per a tot $x \in \mathfrak{R}$, amb ξ_i qualsevol punt de $\mathfrak{R}_i$ per tot $i \in I$, on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$, tenim

$$\sum_{i \in I} f(\xi_i)|\mathfrak{R}_i| \leq C \sum_{i \in I} g(\xi_i)|\mathfrak{R}_i|,$$

i ja hem acabat. □

Teorema 3.1.3.2. *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $\mathcal{S}$ un conjunt de rectangles disjunts de $\mathfrak{R}$ tals que $\bigcup_{S \in \mathcal{S}} S = \mathfrak{R}$ i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores f és integrable Riemann en $\mathfrak{R}$ si i només si f és integrable Riemann en cada $S \in \mathcal{S}$, i*

$$\int_{\mathfrak{R}} f = \sum_{S \in \mathcal{S}} \int_S f.$$

Demostració. Comencem demostrant la doble implicació ($\Leftrightarrow$). Suposem que f és integrable Riemann en $\mathfrak{R}$. Com que f és integrable Riemann en $\mathfrak{R}$, per la proposició 3.1.2.3 i la definició de suma de Riemann (3.1.2.1). Tenim que, sent $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$, existeix un real L tal que

$$\sum_{i \in I} f(x)|\mathfrak{R}_i| = L,$$

on $\{\mathfrak{R}_i\}_{i \in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició $P \in \mathcal{P}$. Considerem ara el conjunt de particions de S, per a tot $S \in \mathcal{S}$, que denotarem com $\mathcal{P}_S$. Com que $S \subset \mathfrak{R}$ per a tot $S \in \mathcal{S}$, per la definició de partició d'un rectangle (3.1.1.2), tenim que

$$\lim_{P_S \in \mathcal{P}_S} P_S \subset \lim_{P \in \mathcal{P}} P,$$

per a tot $S \in \mathcal{S}$; i com que $\bigcup_{S\in\mathcal{S}} S = \mathfrak{R}$ tenim que

$$\bigcup_{S\in\mathcal{S}} \lim_{P_S\in\mathcal{P}_S} P_S = \lim_{P\in\mathcal{P}} P.$$

Per tant, si I_S és el conjunt d'índexs dels subrectangles $\mathfrak{R}_{S,i}$ de S definits per una partició P_S, per a tot $S \in \mathcal{S}$, com que, per hipòtesi, els rectangles $S \in \mathcal{S}$ són disjunts, tenim

$$\sum_{i\in I} f(x)|\mathfrak{R}_i| = \sum_{S\in\mathcal{S}} \sum_{i\in I_S} f(x)|\mathfrak{R}_{S,i}| = L,$$

i, de nou, per la proposició 3.1.2.3 tenim que f és integrable en cada $S \in \mathcal{S}$, com volíem veure.

Aquesta demostració també ens serveix per veure que

$$\int_{\mathfrak{R}} f = \sum_{S\in\mathcal{S}} \int_S f,$$

per la definició de suma de Riemann (3.1.2.1). □

Teorema 3.1.3.3. *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f : \mathfrak{R} \to \mathbb{R}$ una funció integrable Riemann amb $|f(x)| \leq M$ per a tot $x \in \mathfrak{R}$. Aleshores la funció $|f|$ és integrable Riemann i*

$$\left|\int_{\mathfrak{R}} f\right| \leq \int_{\mathfrak{R}} |f| \leq M|\mathfrak{R}|.$$

Demostració. Sigui $\{\mathfrak{R}_i\}_{i\in I}$ el conjunt de subrectangles definits per una partició de $\mathfrak{R}$. Aleshores

$$\sup_{x\in\mathfrak{R}_i} f(x) - \inf_{x\in\mathfrak{R}_i} f(x) = \sup_{x,y\in\mathfrak{R}_i} |f(x) - f(y)|, \quad \text{per a tot } i \in I,$$

i

$$\sup_{x\in\mathfrak{R}_i} |f(x)| - \inf_{x\in\mathfrak{R}_i} |f(x)| = \sup_{x,y\in\mathfrak{R}'_i} ||f(x)| - |f(y)||, \quad \text{per a tot } i \in I.$$

Per tant, per la definició de suma superior i inferior (3.1.1.3), si P és una partició de $\mathfrak{R}$ tenim

$$\mathrm{S}(|f|, P) - \mathrm{s}(|f|, P) \leq \mathrm{S}(f, P) - \mathrm{s}(f, P)$$

Com que, per hipòtesi, f és integrable Riemann, pel Teorema del criteri d'integrabilitat Riemann (3.1.1.9) tenim que per a tot $\varepsilon > 0$ existeix una partició P de $\mathfrak{R}$ tal que

$$\mathrm{S}(f, P) - \mathrm{s}(f, P) < \varepsilon,$$

el que significa que

$$\mathrm{S}(|f|, P) - \mathrm{s}(|f|, P) \leq \mathrm{S}(f, P) - \mathrm{s}(f, P) < \varepsilon.$$

I pel mateix criteri d'integrabilitat Riemann $|f|$ també és integrable Riemann.

Per veure les desigualtats de l'enunciat, amb $\mathcal{P}$ el conjunt de particions de $\mathfrak{R}$ i $\{\mathfrak{R}_i\}_{i\in I}$ el conjunt de subrectangles definits per una partició $\lim_{P\in\mathcal{P}}$ de $\mathfrak{R}$, tenim

$$\left|\int_{\mathfrak{R}} f\right| = \lim_{P\in\mathcal{P}} \left|\sum_{i\in I} f(x)\,|\mathfrak{R}_i|\right| \leq \lim_{P\in\mathcal{P}} \sum_{i\in I} |f(x)|\,|\mathfrak{R}_i| = \int_{\mathfrak{R}} |f|\,.$$

Com que, per hipòtesi, $|f(x)| \leq M$ per a tot $x \in \mathfrak{R}$, tenim

$$\int_{\mathfrak{R}} |f| \leq \int_{\mathfrak{R}} M = M|\mathfrak{R}|. \qquad \square$$

Corol·lari 3.1.3.4. *Si $f(x) \geq 0$ per a tot $x \in \mathfrak{R}$, $\int_{\mathfrak{R}} f \geq 0$.*

Proposició 3.1.3.5. *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f : \mathfrak{R} \to \mathbb{R}$ una funció contínua i acotada tal que $f(x) \geq 0$ per a tot $x \in \mathfrak{R}$ i $\int_{\mathfrak{R}} f = 0$. Aleshores $f(x) = 0$ per a tot $x \in \mathfrak{R}$.*

Demostració. Observem que la proposició té sentit pel Teorema 3.1.1.12.

Farem aquesta demostració per reducció a l'absurd. Suposem que existeix un punt $c \in \mathfrak{R}$ tal que $f(c) > 0$. Com que, per hipòtesi, f és contínua en un rectangle $\mathfrak{R}$, acotat per la definició de rectangle (3.1.1.1), pel Teorema de Heine (1.3.0.4) f és uniformement contínua en $\mathfrak{R}$, per tant, per la definició de continuïtat uniforme (1.3.0.3), per a tot $\varepsilon > 0$ existeix un $\delta > 0$ tals que

$$\text{si } |x - c| < \delta \text{ aleshores } |f(x) - f(c)| < \varepsilon = \frac{f(c)}{2}.$$

Per tant, si definim un rectangle S inscrit en la bola de radi δ centrada en el punt c, $\mathrm{B}(c, \delta)$, tenim

$$\int_{\mathfrak{R}} f \geq \int_S f \geq \frac{f(x)}{2}|S| > 0,$$

però això contradiu la hipòtesi de que $\int_{\mathfrak{R}} f = 0$, per tant la proposició queda demostrada per reducció a l'absurd. $\square$

3.2 Les funcions integrables Riemann

3.2.1 Caracterització de les funcions integrables Riemann

Definició 3.2.1.1 (Oscil·lació d'una funció en un punt)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $a \in U$ un punt, $\mathrm{B}(a, \delta) \subseteq U$ una bola oberta centrada en a de radi $\delta > 0$ i $f : U \to \mathbb{R}^m$ una funció. Aleshores definim l'aplicació

$$\omega_f(a) = \lim_{\delta \to 0} \sup_{x,y \in B(a,\delta)} \|f(x) - f(y)\|$$

com l'oscil·lació de la funció f en el punt a.

Proposició 3.2.1.2. *Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}^m$ una funció definida en un punt $a \in U$. Aleshores f és contínua en a si i només si $\omega_f(a) = 0$, on $\omega_f(a)$ és la oscil·lació de f en a.*

Demostració. Suposem que $\omega_f(a) = 0$. Observem que quan $\delta \to 0$, per a tot $x, y, \in \mathrm{B}(a, \delta)$ tenim $x \to a$ i $y \to a$, i com que $\omega_f(a) = 0$, podem escriure

$$\begin{aligned} \omega_f(a) &= \lim_{\delta \to 0} \sup_{x,y \in B(a,\delta)} \|f(x) - f(y)\| \\ &= \lim_{x,y \to a} \|f(a) - f(x)\| = 0 \end{aligned}$$

i per tant tenim $\lim_{x\to a} f(x) = \lim_{y\to a} f(y)$, i equivalentment

$$\lim_{x\to a} f(x) = f(a),$$

que és la definició de funció contínua (1.2.1.1). □

Definició 3.2.1.3 (Conjunt de discontinuïtats d'una funció)**.** Siguin $U \subseteq \mathbb{R}^d$ un obert, $f : U \to \mathbb{R}^m$ una funció, τ un escalar positiu i $\omega_f(x)$ l'oscil·lació de f en un punt $x \in U$. Aleshores denotem el conjunt

$$D_\tau = \{x \in U : \omega_f(x) \geq \tau\}$$

com el conjunt de desigualtats majors que τ d'una funció.

Observació 3.2.1.4. *D_τ és compacte.*

Definició 3.2.1.5 (contingut exterior de Jordan)**.** Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle, $A \subseteq \mathfrak{R}$ un conjunt, 1_A la funció indicatriu de A i $\{\mathfrak{R}_i\}_{i\in I}$ el conjunt de subrectangles definits per una partició de $\mathfrak{R}$ amb la condició de que $\mathfrak{R}_i \cap A \neq \emptyset$ per a tot $i \in I$. Aleshores definim

$$c(A) = \sum_{i\in I} \inf_{x\in\mathfrak{R}_i} 1_A(x)|\mathfrak{R}_i|$$

com el contingut exterior de Jordan de A.

Nota 3.2.1.6. *La condició sobre $\mathfrak{R}_i$ pot dir-se com que els $\mathfrak{R}_i$ cobreixen A.*

Observació 3.2.1.7. *Siguin $\{A_i\}_{i\in I}$ un conjunt finit de conjunts amb $c(A_i) = 0$ per a tot $i \in I$ i $A = \bigcup_{i\in I} A_i$. Aleshores $c(A) = 0$.*

Teorema 3.2.1.8. *Siguin $\mathfrak{R} \subset \mathbb{R}^d$ un rectangle i $f : \mathfrak{R} \to \mathbb{R}$ una funció acotada. Aleshores f és integrable Riemann en $\mathfrak{R}$ si i només si el contingut exterior de Jordan del conjunt de desigualtats majors que $\tau > 0$ de f en $\mathfrak{R}$ és cero, és a dir, $c(D_\tau) = 0$ per a tot $\tau > 0$.*

Demostració. Comencem amb la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que $D_\tau = 0$ per a tot $\tau > 0$. Per la definició de contingut exterior de Jordan (3.2.1.5) això és

$$\sum_{i\in I} \inf_{x\in\mathfrak{R}_i} 1_{D_\tau}(x)|\mathfrak{R}_i| = 0$$

on $\{\mathfrak{R}_i\}_{i\in I}$ és el conjunt de subrectangles de $\mathfrak{R}$ definits per una partició del conjunt $\mathcal{P}$ de particions de $\mathfrak{R}$. Considerem el conjunt de subrectangles $\{\mathfrak{R}_j\}_{j\in J}$ tals que $\mathfrak{R}_j \cap D_\tau \neq \emptyset$. Ara bé, per la proposició 3.2.1.2 tenim que f és contínua, i pel Teorema 3.1.1.12 veiem que f és integrable Riemann en $\mathfrak{R}$.

Comprovem ara la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que f és integrable Riemann en R i fixem $\varepsilon > 0$. Pel Teorema del criteri d'integrabilitat Riemann (3.1.1.9) tenim que per a tot $\varepsilon > 0$ existeix una partició P de $\mathfrak{R}$ tal que

$$\sum_{i\in I} \left(\sup_{x\in\mathfrak{R}_i} f(x) - \inf_{x\in\mathfrak{R}_i} f(x) \right) |\mathfrak{R}_j| < \varepsilon$$

on $\{\mathfrak{R}_i\}_{i\in I}$ és el conjunt de subrectangles definits per P. Sigui J el conjunt de subrectangles $\{\mathfrak{R}_j\}_{j\in J}$ tals que $\mathfrak{R}_j \cap D_\tau \neq \emptyset$. Tindrem

$$\sup_{x\in\mathfrak{R}_j} f(x) - \inf_{x\in\mathfrak{R}_j} f(x) \geq \tau$$

per a tot $j \in J$, i per tant, amb $\mathfrak{R}' = \bigcup_{j\in J} \mathfrak{R}_j$, per la definició de contingut exterior de Jordan (3.2.1.5)

$$\begin{aligned}\sum_{j\in J}\left(\sup_{x\in\mathfrak{R}_j} f(x) - \inf_{x\in\mathfrak{R}_j} f(x)\right)|\mathfrak{R}_j| &\geq \sum_{j\in J}\tau|\mathfrak{R}_j| \\ &= \tau\sum_{j\in J}|\mathfrak{R}_j| \\ &\geq \tau\sum_{j\in I}\inf_{x\in\mathfrak{R}_j} 1_{\mathfrak{R}'}(x)|\mathfrak{R}_j| \\ &= \tau c(D_\tau)\end{aligned}$$

Ara bé, com que f és integrable, pel Teorema del criteri d'integrabilitat Riemann (3.1.1.9) tenim que

$$\sum_{j\in J}\left(\sup_{x\in\mathfrak{R}_j} f(x) - \inf_{x\in\mathfrak{R}_j} f(x)\right)|\mathfrak{R}_j| < \varepsilon$$

per a tota $\varepsilon > 0$, i per tant quan $\varepsilon \to 0$ ha de ser $D_\tau = 0$, com volíem veure. □

3.2.2 Integració sobre conjunts generals

Nota 3.2.2.1. *Tota la teoria de l'integració Riemann que hem vist ha estat sobre rectangles. Ara tractem de generalitzar-la desfent-nos d'aquesta limitació.*

Capítol 4

Càlcul vectorial

4.1 Introducció

sona divertit

Part III

Estructures algebraiques

Capítol 5

Teoria de grups

5.1 Introducció

5.1.1 Grups

Definició 5.1.1.1 (Grup)**.** Siguin $G \neq \emptyset$ un conjunt i $* : G \times G \to G$ una operació que satisfà

1. Per a tot $x, y, z \in G$
$$x * (y * z) = (x * y) * z.$$
2. Existeix un $e \in G$ tal que per a tot $x \in G$
$$x * e = e * x = x.$$
3. Per a cada $x \in G$ existeix x' tal que
$$x * x' = x' * x = e.$$

Aleshores $(G, *)$ és un grup. També direm que $*$ és la composició del grup, o que $*$ dota al conjunt G d'estructura de grup.

Proposició 5.1.1.2. *Siguin $(G, *)$ un grup i $e \in G$ tal que $x * e = e * x = x$ per a tot $x \in G$. Aleshores e és únic.*

Demostració. Suposem que existeix un altre element de G amb aquesta propietat, diguem-ne $\hat{e} \in G$. Aleshores hauria de ser
$$e * \hat{e} = e,$$
però per hipòtesi
$$e * \hat{e} = \hat{e}.$$
Per tant, ha de ser $e = \hat{e}$. □

Definició 5.1.1.3 (Element neutre d'un grup)**.** Siguin $(G, *)$ un grup i e un element de G tal que $x * e = e * x = x$ per a tot $x \in G$. Aleshores direm que e és l'element neutre de $(G, *)$.

Observem que aquesta definició té sentit per la proposició 5.1.1.2.

Notació 5.1.1.4. Donat un grup $(G, *)$, aprofitant que la composició $*$ és associativa escriurem

$$(x_1 * x_2) * x_3 = x_1 * x_2 * x_3.$$

També denotarem

$$x^n = x * \overset{n)}{\dots} * x.$$

Si denotem la conjugació del grup per $+$ usarem la notació additiva[1] i escriurem

$$x_1 + \cdots + x_n$$

per referir-nos a la conjugació de $+$ amb si mateix n vegades.

També denotarem

$$nx = x + \overset{n)}{\dots} + x.$$

Proposició 5.1.1.5. *Siguin $(G, *)$ un grup i a, b, c tres elements de $(G, *)$. Aleshores*

1. $a * c = b * c \Rightarrow a = b$.
2. $c * a = c * b \Rightarrow a = b$.

Demostració. Farem només la demostració del punt (1) ja que l'altre és anàloga.

Com que per hipòtesi $(G, *)$ és un grup, per la definició de grup (5.1.1.1) tenim que existeix c' tal que $c * c' = e$, on e és l'element neutre de $(G, *)$, i tenim

$$a * c * c' = b * c * c',$$

el que significa que

$$a * e = b * e,$$

i ens queda $a = b$. □

Proposició 5.1.1.6. *Siguin $(G, *)$ un grup amb element neutre e i a un element de G. Aleshores existeix un únic $a' \in G$ tal que*

$$a * a' = a' * a = e.$$

Demostració. Notem que existeix un $a' \in G$ que satisfà l'equació per la definició de grup (5.1.1.1), i per tant la proposició té sentit.

Suposem doncs que existeix $a'' \in G$ tal que

$$a * a'' = a'' * a = e.$$

Però aleshores tenim

$$a * a'' = e = a * a',$$

i per la proposició 5.1.1.5 ha de ser $a' = a''$, com volíem demostrar. □

Definició 5.1.1.7 (Invers d'un element)**.** Siguin $(G, *)$ un grup amb element neutre e i a un element de G. Per la definició de grup tenim que existeix un $a' \in G$ tal que

$$a * a' = a' * a = e.$$

Aleshores direm que a' és l'invers de a en $(G, *)$, i el denotarem per a^{-1}.

Observem que aquesta definició té sentit per la proposició 5.1.1.6 i la notació introduïda en 5.1.1.4.

[1] En altres textos se sol utilitzar la notació additiva per a grups abelians exclusivament.

Proposició 5.1.1.8. *Sigui $(G, *)$ un grup d'element neutre e. Aleshores*

$$e^{-1} = e.$$

Demostració. Per la definició de grup (5.1.1.1) tenim que

$$e * e^{-1} = e^{-1} * e = e,$$

i per ha de ser $e^{-1} = e$. □

Proposició 5.1.1.9. *Siguin $(G, *)$ un grup amb element neutre e i a un element de G. Aleshores*

$$\left(a^{-1}\right)^{-1} = a.$$

Demostració. Com que $\left(a^{-1}\right)^{-1}$ és l'invers de a^{-1} tenim

$$\left(a^{-1}\right)^{-1} * a^{-1} = e$$

però també tenim que

$$a * a^{-1} = e.$$

Per tant és

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

i per la proposició 5.1.1.5 ha de ser

$$a = \left(a^{-1}\right)^{-1}.$$ □

Proposició 5.1.1.10. *Siguin $(G, *)$ un grup amb element neutre e i a, b dos elements de G. Aleshores*

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

Demostració. Considerem

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

i de manera anàloga trobem

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

Així doncs, per la proposició 5.1.1.6 tenim que $a * b$ és l'inversa de $b^{-1} * a^{-1}$, és a dir

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$ □

Lemma 5.1.1.11. *Siguin $(G, *)$ un grup i a, b dos elements de G. Aleshores existeixen $x, y \in G$ únics tals que*

$$b * x = a \quad i \quad y * b = a.$$

Demostració. Fem només una de les demostracions, ja que l'altre és anàloga. Com que per hipòtesi $(G, *)$ és un grup, per la definició de grup (5.1.1.1) tenim que existeix $b^{-1} \in G$ tal que $b^{-1} * b = e$, on e és l'element neutre de $(G, *)$. Per tant considerem

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

i per la definició de grup (5.1.1.1) tenim que això és equivalent a

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

i de nou per la definició de grup, i per la definició de l'element neutre d'un grup (5.1.1.3),

$$e * x = x = b^{-1} * a;$$

i la unicitat ve donada per la proposició 5.1.1.2. □

Teorema 5.1.1.12. *Siguin G un conjunt i $* : G \times G \to G$ una composició que satisfà $x * (y * z) = (x * y) * z$ per a tot $x, y, z \in G$. Aleshores els següents enunciats són equivalents:*

1. *$(G, *)$ és un grup.*
2. *$G \neq \emptyset$ i per a tot $a, b \in G$ existeix uns únics $x, y \in G$ tals que*

$$b * x = a \quad i \quad y * b = a.$$

3. *Existeix $e \in G$ tal que per a tot $x \in G$ tenim $x * e = x$ i existeix un $x^{-1} \in G$ tal que $x * x^{-1} = e$.*

Demostració. Comencem demostrant (1)⇒(2). Suposem que $(G, *)$ és un grup. Veiem que G no és buit per la segona propietat de la definició de grup (5.1.1.1), ja que tenim que existeix $e \in G$, i la segona part és el lemma 5.1.1.11.

Demostrem ara (2)⇒(3). La primera part es pot veure fixant $x \in G$. Pel punt (2) tenim que per a cada $a \in G$ existeix un únic $b \in G$ tal que

$$a * b = x,$$

i podem fer

$$a * b * e = x * e$$

i substituint ens queda

$$x * e = x.$$

Per veure la segona part notem que pel punt (2) tenim que per a tot $x \in G$ existeix un $a \in G$ tal que

$$x * a = e,$$

i aleshores $a = x^{-1}$.

Ara només ens queda veure (3)⇒(1). Tenim que per a tot $x \in G$ existeix un x^{-1} tal que $x * x^{-1} = e$, i de la mateixa manera, existeix un $y \in G$ tal que $x^{-1} * y = e$. Per tant

$$\begin{aligned} e &= x^{-1} * y \\ &= x^{-1} * e * y \\ &= x^{-1} * x * x^{-1} * y \\ &= x^{-1} * x * e = x^{-1} * x. \end{aligned}$$

Així tenim que per a tot $x \in G$ es compleix $x * x^{-1} = x^{-1} * x = e$, d'on podem veure que $e * x = x * e$, i com que, per hipòtesi, la composició $*$ satisfà $x * (y * z) = (x * y) * z$ per a tot $x, y, z \in G$ es compleix la definició de grup (5.1.1.1) i tenim que $(G, *)$ és un grup.

Així tenim (1)⇒(2)⇒(3)⇒(1), com volíem veure. □

5.1.2 Subgrups i subgrups normals

Definició 5.1.2.1 (Subgrup)**.** Siguin $(G, *)$ un grup i $H \subseteq G$ un subconjunt de G tal que $(H, *)$ sigui un grup. Aleshores diem que $(H, *)$ és un subgrup de $(G, *)$.

També ho denotarem com $(H, *) \leq (G, *)$.

Observació 5.1.2.2. $e \in H$.

Proposició 5.1.2.3. *Siguin $(G, *)$ un grup amb element neutre e i H un subconjunt de G. Aleshores $(H, *)$ és un subgrup de $(G, *)$ si i només si per a tot $x, y \in H$ tenim que $x * y^{-1} \in H$.*

Demostració. Demostrem primer que la condició és necessària (⇒). Això ho podem veure per la definició de grup (5.1.1.1), ja que tenim que y^{-1} existeix i pertany a H, i per tant $x * y^{-1}$ també pertany a H.

Demostrem ara que la condició és suficient (⇐). Tenim que per a tot $x \in H$ es compleix

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

i per tant $e \in H$. També tenim que per a tot $x \in H$ es compleix

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

i per tant $x^{-1} \in H$.

Ara només ens queda veure que $*$ està ben definit en H; és a dir, que per a tot $x, y \in H$ tenim $x * y \in H$. Com que ja hem vist que y^{-1} existeix i pertany a H, per la proposició 5.1.1.9 tenim

$$x * y^{-1} = x * y$$

i per hipòtesi $x * y \in H$.

Per tant, per la definició de grup (5.1.1.1) tenim que $(H, *)$ és un grup, i com que per hipòtesi $H \subseteq G$ per la definició de subgrup (5.1.2.1) tenim que $(H, *)$ és un subgrup de $(G, *)$. □

Proposició 5.1.2.4. *Siguin $(G, *)$ un grup amb element neutre e, $(H_i, *)_{i \in I}$ una família de subgrups de $(G, *)$ i $H = \bigcap_{i \in I} H_i$. Aleshores $(H, *)$ és un subgrup de $(G, *)$.*

Demostració. Ho demostrarem amb la proposició 5.1.2.3. Tenim $H \subseteq G$ i $H \neq \emptyset$, ja que $e \in H$. Comprovem ara que per a tot $x, y \in H$ tenim $x * y^{-1} \in H$. Tenim que si $x, y \in H$, per la definició de H, $x, y \in H_{i \in I}$; i com que $H_{i \in I}$ és un subgrup de $(G, *)$, $x * y^{-1} \in H_{i \in I}$ per la proposició 5.1.2.3, i per tant $x * y^{-1} \in H$, com volíem veure. □

Proposició 5.1.2.5. *Siguin $(G,*)$ un grup amb element neutre e, $S \neq \emptyset$ un subconjunt de G, $(H_i,*)_{i\in I}$ una família de subgrups de $(G,*)$ tals que $S \subseteq H_i$ per a tot $i \in I$ i $H = \bigcap_{i\in I} H_i$. Aleshores $(H,*)$ existeix i és un subgrup de $(G,*)$.*

Demostració. Per veure que $(H,*)$ existeix, és a dir, que $H \neq \emptyset$ tenim prou amb veure que $e \in H$, i per acabar, que $(H,*)$ és un subgrup de $(G,*)$ ho podem veure per la proposició 5.1.2.4. □

Definició 5.1.2.6 (Mínim subgrup generat per un conjunt)**.** Siguin $(G,*)$ un grup, S un subconjunt de G, $(H_i,*)_{i\in I}$ una família de subgrups de $(G,*)$ tals que $S \subseteq H_i$ per a tot $i \in I$ i $H = \bigcap_{i\in I} H_i$. Aleshores direm que el subgrup $(H,*) \leq (G,*)$ és el mínim subgrup generat per S i ho denotarem amb $(\langle S\rangle,*)$.

Observem que aquesta definició té sentit per la proposició 5.1.2.5.

Proposició 5.1.2.7. *Siguin $(G,*)$ un grup i g un element de G. Aleshores $\langle\{g\}\rangle = \{\dots, g^{-3}, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, \dots\}$.*

Demostració. Ho demostrem per doble inclusió.

Comencem veient que $\{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\} \subseteq \langle\{g\}\rangle$. Per la definició de mínim subgrup generat per un conjunt (5.1.2.6) tenim que existeix una família de subconjunts de $(G,*)$ que denotarem per $(H_i,*)_{i\in I}$, amb $\{g\} \subseteq H = \bigcap_{i\in I} H_i$. Com que $(H_i,*)_{i\in I}$ són subgrups de $(G,*)$ tenim que, donat que $g \in H_i$, $g^n \in H_i$ per a tot $i \in I$ i tot $n \in \mathbb{Z}$ per la definició de grup (5.1.1.1), i per tant $g^n \in H$, el que és equivalent a dir que $g^n \in \langle g\rangle$ per a tot $n \in \mathbb{Z}$

Ara veiem que $\langle\{g\}\rangle \subseteq \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}$. Denotarem $H_g = \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}$. Hem de veure que $(H_g,*)$ és un grup. Observem que per a tot $g^i, g^j \in H_g$, $g^i * g^{-j} = g^{i-j} \in H_g$, i per tant $(H_g,*) \leq (G,*)$. Ara bé, com que $\{g\} \subseteq H_g$, tenim que $H_g \in (H_i)_{i\in I}$, és a dir, que H_g pertany a la família de subconjunts de G que contenen $\{g\}$; el que significa que $(\langle\{g\}\rangle,*) \leq (H_g,*)$, i per tant $\langle\{g\}\rangle \subseteq \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}$. □

Definició 5.1.2.8 (Ordre d'un grup)**.** Sigui $(G,*)$ un grup. Direm que $|(G,*)|$ és l'ordre del grup. Si $|(G,*)|$ és finit direm que $(G,*)$ és un grup d'ordre finit, i si $|(G,*)|$ no és finit direm que $(G,*)$ és un grup d'ordre infinit.

Proposició 5.1.2.9. *Siguin $(G,*)$ un grup amb element neutre e i g un element de G. Aleshores*

$$|\langle\{g\}\rangle| = n \iff n = \min\{k \in \mathbb{N} : g^k = e\}.$$

Demostració. Comencem amb la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que $n = \min\{k \in \mathbb{N} : g^k = e\}$. Pel Teorema de la divisió Euclidiana (1.3.0.6) tenim que per a tot $t \in \mathbb{Z}$ existeixen uns únics $Q \in \mathbb{Z}$, $r \in \mathbb{N}$, amb $r < n$ tals que $t = Qn + r$. Per tant

$$\begin{aligned} g^t &= g^{Qm+r} \\ &= g^{Qm} * g^r \\ &= (g^m)^Q * g^r \\ &= e^Q * g^r = g^r. \end{aligned}$$

Per tant, com que $0 \leq r < n$, $|\langle\{g\}\rangle| = n$.

Fem ara la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $|\langle\{g\}\rangle| = n$. Com que el grup és finit per a cada $i \in \mathbb{Z}$ existeix $j \in \mathbb{Z}$ tal que $g^i = g^j$, i com que $(\langle\{g\}\rangle, *)$ és un grup, per la definició de grup (5.1.1.1) existeix $g^{-j} \in \langle\{g\}\rangle$ tal que $g^{i-j} = e$.

Sigui doncs $t \in \mathbb{N}$ tal que $g^t = e$. Aleshores, pel Teorema de la divisió Euclidiana (1.3.0.6) existeixen uns únics $Q, r \in \mathbb{N}$, amb $r < n$ tals que $t = Qn + r$. Per tant

$$\begin{aligned} g^t &= g^{Qn+r} \\ &= g^{Qn} * g^r \\ &= (g^n)^Q * g^r \\ &= e^Q * g^r \\ &= g^r = e. \end{aligned}$$

i per tant $r = 0$, i tenim $t = Qn$, i per tant $n = \min\{k \in \mathbb{N} : g^k = e\}$. □

Definició 5.1.2.10 (Conjugació entre conjunts sobre grups)**.** Siguin $(G, *)$ un grup i H un subconjunt de G. Aleshores definim

$$GH = \{x * h : x \in G, h \in H\}.$$

Definició 5.1.2.11 (Subgrup normal)**.** Siguin $(G, *)$ un grup i $(H, *)$ un subgrup de $(G, *)$. Aleshores direm que $(H, *)$ és un subgrup normal de $(G, *)$ si per a tot $x \in G$ tenim

$$\{x\}H = H\{x\}.$$

Ho denotarem com $(H, *) \trianglelefteq (G, *)$.

Proposició 5.1.2.12. *Siguin $(G, *)$ un grup i $(H, *)$ un subgrup de $(G, *)$. Aleshores són equivalents*

1. *$\{x\}H = H\{x\}$ per a tot $x \in G$.*
2. *$\{x^{-1}\}H\{x\} = H$ per a tot $x \in G$.*
3. *$\{x^{-1}\}H\{x\} \subseteq H$ per a tot $x \in G$.*

Demostració. Comencem demostrant (1)⇒(2). Suposem que $(H, *)$ és un subgrup normal de $(G, *)$, per la definició de subgrup normal (5.1.2.11) tenim $\{x\}H = H\{x\}$ per a tot $x \in G$. Aleshores tenim

$$\begin{aligned} \{x\}H\{x^{-1}\} &= H\{x\}\{x^{-1}\} \\ &= \{h * x * x^{-1} : h \in H\} \\ &= \{h : h \in H\} = H. \end{aligned}$$

Continuem demostrant (2)⇒(3). Suposem que $\{x\}H\{x^{-1}\} = H$. Tenim que $\{x\}H\{x^{-1}\} = H \subseteq H$.

Demostrem ara (3)⇒(1). Suposem doncs que $\{x^{-1}\}H\{x\} \subseteq H$ per a tot $x \in G$. Això significa que per a tot $h \in H$ existeix un $h' \in H$ tal que $x * h * x^{-1} = h'$, i aleshores, per la definició de grup (5.1.1.1), $x * h = h' * x \in H$, i per tant $x * h \in H\{x\}$ per a tot $x \in G$. Així hem vist que $\{x\}H \subseteq H\{x\}$. Per veure l'altre inclusió es pot donar un argument anàleg, i per tant $\{x\}H = H\{x\}$.

I així hem vist que (1)⇒(2)⇒(3)⇒(1) i hem acabat. □

5.1.3 Grups cíclics i grups abelians.

Definició 5.1.3.1 (Grup abelià)**.** Sigui $(G, *)$ un grup tal que per a tot $x, y \in G$ satisfà

$$x * y = y * x.$$

Aleshores direm que $(G, *)$ és un grup abelià.

Proposició 5.1.3.2. *Sigui $(G, *)$ un grup. Aleshores $(G, *)$ és un grup abelià si i només si per a tot $a, b \in G$ es compleix*

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

Demostració. Que la condició és necessària ($\Rightarrow$) ho podem veure amb la definició de grup abelià (5.1.3.1) i la proposició 5.1.1.10.

Demostrem ara que la condició és suficient ($\Leftarrow$). Diem que l'element neutre de $(G, *)$ és e. Per la definició de grup (5.1.1.1) tenim que

$$(a * b) * (a * b)^{-1} = e, \tag{5.1}$$

que és equivalent a

$$(a * b) * (a * b)^{-1} \left((a * b)^{-1}\right)^{-1} = \left((a * b)^{-1}\right)^{-1},$$

i aleshores

$$\begin{aligned} a * b &= \left((a * b)^{-1}\right)^{-1} \\ &= \left(b^{-1} * a^{-1}\right)^{-1} && \text{(Proposició 5.1.1.10)} \\ &= \left((b * a)^{-1}\right)^{-1} && \text{(Hipótesi (5.1))} \\ &= b * a, && \text{(Proposició 5.1.1.9)} \end{aligned}$$

i per la definició de grup abelià (5.1.3.1), $(G, *)$ és un grup abelià. □

Definició 5.1.3.3 (Grup cíclic)**.** Siguin $(G, *)$ un grup i g un element de G. Aleshores diem que el grup $(\langle\{g\}\rangle, *)$ és un grup cíclic i que g és un generador del grup.

Proposició 5.1.3.4. *Sigui $(G, *)$ un grup cíclic. Aleshores $(G, *)$ és abelià.*

Demostració. Com que $(G, *)$ és un grup cíclic, per la definició de grup cíclic (5.1.3.3) tenim que existeix un g tal que $\langle\{g\}\rangle = G$. Siguin a, b dos elements de G, i com que $(G, *)$ és cíclic, ha de ser $a = g^m$ i $b = g^n$ per a certs $m, n \in \mathbb{N}$. Ara bé, tenim que $g^m * g^n = g^m * g^n$, ja que

$$\begin{aligned} g^n * g^m &= g^{n+m} \\ &= g^{m+n} = g^m * g^n \end{aligned}$$

i aleshores $a * b = b * a$, i per la definició de grup abelià (5.1.3.1) hem acabat. □

Proposició 5.1.3.5. *Sigui $(G, *)$ un grup cíclic i $(H, *)$ un subgrup de $(G, *)$. Aleshores $(H, *)$ és cíclic.*

Demostració. Sigui e l'element neutre de $(G, *)$. Per l'observació 5.1.2.2 tenim que $e \in H$. Si $H = \{e\}$ no hi ha res a demostrar. Suposem que $H \neq \{e\}$, aleshores existeix un $g \in G$ tal que $g^n \in H$ per a cert $n \in \mathbb{N}$. Sigui doncs m l'enter més petit tal que $g^m \in H$; volem demostrar que $H = \langle\{g^m\}\rangle$.

Sigui a un element de H. Aleshores com que $a \in H \subseteq G$, $a = g^t$ per a cert $t \in \mathbb{N}$, i pel Teorema de la divisió Euclidiana (1.3.0.6) existeixen $Q, r \in \mathbb{N}$, amb $r < m$ tals que $t = Qm + r$, i per tant $g^t = g^{Qm+r}$. Aleshores tenim

$$g^r = (g^m)^{-Q} * g^t,$$

i ha de ser $g^r \in H$, ja que $g^m \in H$, i per la definició de grup (5.1.1.1) tenim que $(g^m)^{-1} \in H$. Per tant $g^r \in H$. Però ara bé, m era el mínim enter tal que $g^m \in H$, i $r < m$, per tant ha de ser $g^r = e$, és a dir, $r = 0$ i per tant $t = Qm$; el que significa que $H = \{(g^m)^Q : Q \in \mathbb{N}\}$ i per la proposició 5.1.2.7 $H = \langle\{g^m\}\rangle$ i hem acabat. □

5.1.4 Relació d'equivalència entre grups

Proposició 5.1.4.1. *Siguin $(G, *)$ un grup i $(H, *)$ un subgrup de $(G, *)$. Aleshores la relació*

$$x \equiv y \pmod{H} \iff x * y^{-1} \in H \text{ per a tot } x, y \in G$$

és una relació d'equivalència.

Demostració. Sigui e l'element neutre del grup $(G, *)$. Comprovem les propietats de la definició de relació d'equivalència:

1. Reflexiva: Sigui $x \in G$. Aleshores $x * x^{-1} = e$, i tenim l'observació 5.1.2.2.
2. Simètrica: Siguin $x, y \in G$ i suposem que $x \equiv y \pmod{H}$, això significa que $x * y^{-1} \in H$, i per la definició de grup (5.1.1.1) tenim que $(x * y^{-1})^{-1} \in H$, ja que per hipòtesi $(H, *)$ és un grup, i per les proposicions 5.1.1.10 i 5.1.1.9 tenim que
$$(x * y^{-1})^{-1} = y * x^{-1},$$
i això és $y \equiv x \pmod{H}$.
3. Transitiva: Siguin $x, y, z \in G$ i suposem que $x \equiv y \pmod{H}$ i $y \equiv z \pmod{H}$. Per tant tenim que $x * y^{-1} \in H$, i $y * z^{-1} \in H$. Com que per hipòtesi $(H, *)$ és un grup, tenim que $(x * y^{-1}) * (y * z^{-1}) \in H$, que és equivalent a $x * z^{-1} \in H$, i per tant $x \equiv z \pmod{H}$.

I per la definició de relació d'equivalència (1.3.0.2) hem acabat. □

Definició 5.1.4.2 (Relació d'equivalència entre grups)**.** Siguin $(G, *)$ un grup i $(H, *)$ un subgrup de $(G, *)$. Aleshores considerem la següent relació d'equivalència entre grups:

$$x \equiv y \pmod{H} \iff x * y^{-1} \in H$$

Denotarem el conjunt quocient com G/H.

Observem que aquesta definició té sentit per la proposició 5.1.4.1.

Definim també la composició entre classes com l'operació

$$\begin{aligned} * : G \times G &\longrightarrow G \\ [x] * [y] &\longmapsto [x * y]. \end{aligned} \tag{5.2}$$

Lemma 5.1.4.3. *Siguin $(G,*)$ un grup, $(H,*)$ un subgrup de $(G,*)$, x un element de G i*

$$\begin{aligned} f_x : H &\longrightarrow \{x\}H \\ h &\longmapsto x * h \end{aligned}$$

una aplicació. Aleshores f_x és bijectiva.

Demostració. Veiem que aquesta funció és bijectiva trobant la seva inversa:

$$\begin{aligned} f_x^{-1} : \{x\}H &\longrightarrow H \\ y &\longmapsto x^{-1} * y \end{aligned}$$

i comprovant $f_x(f_x^{-1}(h)) = h$ i $f_x^{-1}(f_x(h)) = h$. Per tant f és bijectiva[2]. □

Observació 5.1.4.4. $\{x\}G = G$.

Teorema 5.1.4.5 (Teorema de Lagrange)**.** *Siguin $(G,*)$ un grup d'ordre finit i $(H,*)$ un subgrup de $(G,*)$. Aleshores $|(H,*)|$ divideix $|(G,*)|$.*

Demostració. Fixem $x \in G$ i considerem la funció

$$\begin{aligned} f_x : H &\longrightarrow \{x\}H \\ h &\longmapsto x * h \end{aligned}$$

Pel lemma 5.1.4.3 trobem $|H| = |\{x\}H|$. Tenim que $|(G,*)|$ és el resultat de multiplicar el número de classes d'equivalència pel nombre d'elements d'una de les classes, és a dir

$$|(G,*)| = |(G/H,*)||(H,*)|$$

i per tant $|(H,*)|$ divideix $|(G,*)|$. □

Corol·lari 5.1.4.6. *Tot grup d'ordre primer és cíclic.*

Definició 5.1.4.7 (l'índex d'un subgrup en un grup)**.** Siguin $(G,*)$ un grup i $(H,*)$ un subgrup de $(G,*)$. Aleshores definim

$$[G : H] = \frac{|(G,*)|}{|(H,*)|}$$

com l'índex de $(H,*)$ a $(G,*)$.

5.2 Tres Teoremes d'isomorfisme entre grups

5.2.1 Morfismes entre grups

Definició 5.2.1.1 (Morfisme entre grups)**.** Siguin $(G_1,*)$, $(G_2,\circ)$ dos grups i $f : G_1 \to G_2$ una aplicació que, per a tot $x, y \in G_1$ satisfà

$$f(x * y) = f(x) \circ f(y).$$

Aleshores diem que f és un morfisme entre grups. Definim també

[2] de fet, $f_x^{-1} = f_{x^{-1}}$

1. Si f és injectiva direm que f és un monomorfisme entre grups.
2. Si f és exhaustiva direm que f és un epimorfisme entre grups.
3. Si f és bijectiva direm que f és un isomorfisme entre grups. També escriurem $(G_1, *) \cong (G_2, \circ)$.
4. Si $G_1 = G_2$ direm que f és un endomorfisme entre grups.
5. Si $G_1 = G_2$ i f és bijectiva direm que f és un automorfisme entre grups.

Proposició 5.2.1.2. *Siguin $(G_1, *)$, $(G_2, \circ)$ dos grups amb elements neutres e, e' respectivament i $f : G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. *$f(e) = e'$.*
2. *$f\left(x^{-1}\right) = f(x)^{-1}$ per a tot $x \in G_1$.*

Demostració. Demostrem primer el punt (1). Per la definició de morfisme tenim que per a tot $x \in G_1$

$$\begin{aligned} f(x) \circ f(e) &= f(x * e) && \text{(morfisme entre grups (5.2.1.1))} \\ &= f(x) && \text{(l'element neutre d'un grup (5.1.1.3))} \\ &= f(x) \circ e' \end{aligned}$$

i per la proposició 5.1.1.5 tenim $f(e) = e'$.

Per demostrar el punt (2) en tenim prou en veure que per a tot $x \in G$

$$\begin{aligned} f(x) \circ f(x^{-1}) &= f(x * x^{-1}) && \text{(morfisme entre grups (5.2.1.1))} \\ &= f(e) && \text{(l'invers d'un element d'un grup (5.1.1.7))} \\ &= f(x^{-1} * x) && \text{(morfisme entre grups (5.2.1.1))} \\ &= f(x^{-1}) \circ f(x) \end{aligned}$$

i pel punt (1) d'aquesta proposició $f(x) \circ f(x^{-1}) = f(x^{-1}) \circ f(x) = e'$, i per la proposició 5.1.1.6 tenim que $f(x^{-1}) = f(x)^{-1}$, com volíem. □

Proposició 5.2.1.3. *Siguin $(G, *)$, $(H, \circ)$ i $(K, +)$ tres grups i $f : G \longrightarrow H$ i $g : H \longrightarrow K$ dos morfismes entre grups. Aleshores $g(f) : G \longrightarrow K$ és un morfisme entre grups.*

Demostració. Per la definició de morfisme entre grups (5.2.1.1) tenim que per a tot $g_1, g_2 \in H$ i $h_1, h_2 \in H$ tenim $f(g_1 * g_2) = f(g_1) \circ f(g_2)$ i $g(h_1 \circ h_2) = g(h_1) + g(h_2)$. Per tant

$$g(f(g_1 * g_2)) = g(f(g_1) \circ f(g_2)) = g(f(g_1)) + g(f(g_2)),$$

i per la definició de morfisme entre grups (5.2.1.1) hem acabat. □

Proposició 5.2.1.4. *Siguin $(G_1, *)$ i $(G_2, \circ)$ dos grups isomorfs. Aleshores*

1. *$(G_1, *)$ és abelià si i només si $(G_2, \circ)$ és abelià.*
2. *$(G_1, *)$ és cíclic si i només si $(G_2, \circ)$ és cíclic.*

Demostració. Sigui $f : G_1 \to G_2$ un isomorfisme entre grups.

Comencem demostrant el punt (1). Suposem doncs que $(G_1, *)$ és un grup abelià. Per la definició de grup abelià (5.1.3.1) tenim que per a tot $a, b \in G_1$ es compleix $a * b = b * a$. Aleshores tenim $f(a * b) = f(b * a)$ i per la definició de morfisme entre grups (5.2.1.1) tenim que $f(a) \circ f(b) = f(b) \circ f(a)$, i per tant, com que per la definició de isomorfisme entre grups (5.2.1.1) f és un bijectiu, $(G_2, \circ)$ satisfà la definició de grup abelià (5.1.3.1).

Demostrem ara el punt (2). Suposem doncs que $(G_1, *)$ és cíclic. Per la definició de grup cíclic (5.1.3.3) tenim que $G_1 = \{g^i\}_{i \in \mathbb{Z}}$ per a un cert $g \in G_1$. Per tant, com que f és bijectiva per la definició de isomorfisme entre grups (5.2.1.1) tenim que per a tot $x \in G_2$ es compleix $x = f(g^i)$ per a un cert $i \in \mathbb{Z}$, i per la definició de morfisme entre grups (5.2.1.1) tenim que[3] $f(g^i) = f(g)^i$, i per la definició de grup cíclic (5.1.3.3) $(G_2, \circ)$ és un grup cíclic. □

Definició 5.2.1.5 (Nucli i imatge d'un morfisme entre grups)**.** Siguin $(G_1, *)$, $(G_2, \circ)$ dos grups amb elements neutres e, e' respectivament i $f : G_1 \to G_2$ un morfisme entre grups. Aleshores definim el nucli de f com

$$\ker(f) = \{x \in G_1 : f(x) = e'\},$$

i la imatge de f com

$$\mathrm{Im}(f) = \{f(x) \in G_2 : x \in G_1\}.$$

Observació 5.2.1.6. $\ker(f) \subseteq G_1$, $\mathrm{Im}(f) \subseteq G_2$.

Proposició 5.2.1.7. *Siguin $(G_1, *)$, $(G_2, \circ)$ dos grups amb elements neutres e, e' respectivament, i $f : G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. *$(\ker(f), *)$ és un subgrup normal de $(G_1, *)$.*
2. *$(\mathrm{Im}(f), \circ)$ és un subgrup de $(G_2, \circ)$.*

Demostració. Observem que aquest enunciat té sentit per l'observació 5.2.1.6.

Primer comprovem el punt (1). Comencem veient que $(\ker(f), *)$ és un subgrup de $(G_1, *)$. Per la proposició 5.1.2.3 tenim que ens cal amb veure que si $a, b \in \ker(f)$, aleshores $a * b^{-1} \in \ker(f)$. Això és cert ja que si $a, b \in \ker(f)$ aleshores $f(a) = e'$ i $f(b^{-1}) = e'$, i per tant $a * b^{-1} = e * e^{-1} = e$, el que significa que $f(a * b^{-1}) = e'$, i tenim $a * b^{-1} \in \ker(f)$.

Comprovem ara que el subgrup és normal. Per la proposició 5.1.2.12 en tenim prou en veure que per a tot $x \in \ker(f)$ i $g \in G$, $x * g * x^{-1} \in \ker(f)$. Això ho veiem notant que si $g \in \ker(f)$, $f(g) = e'$, i per tant $f(x * g * x^{-1}) = f(x) \circ e' \circ f(x^{-1})$i això és $f(x * x^{-1}) = e'$, i per tant $x * g * x^{-1} \in \ker(f)$.

Acabem veient el punt (2). De nou per la proposició 5.1.2.3 tenim que si per a tot $f(a), f(b) \in \mathrm{Im}(f)$ tenim $f(a) \circ f(b)^{-1} \in \mathrm{Im}(f)$ aleshores $(\mathrm{Im}(f), \circ)$ és un subgrup de $(G_2, *)$. Això és cert, ja que per la definició de morfisme entre grups (5.2.1.1) i la proposició 5.2.1.2 tenim $f(a) \circ f(b)^{-1} = f(a * b^{-1})$; i per la definició de grup $a * b^{-1} \in G_1$, i per la definició de morfisme entre grups (5.2.1.1) tenim que $f(a) \circ f(b)^{-1} \in \mathrm{Im}(f)$, i per tant $(\mathrm{Im}(f), \circ)$ és un subgrup de $(G_2, \circ)$, com volíem veure. □

[3] el primer és amb la composició $*$ i el segon amb la composició $\circ$.

Proposició 5.2.1.8. *Siguin $(G_1, *), (G_2, \circ)$ dos grups amb elements neutres e i e' respectivament, i $f : G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. *f és un monomorfisme si i només si* $\ker(f) = \{e\}$.
2. *f és un epimorfisme si i només si* $\mathrm{Im}(f) = G_2$.

Demostració. Comencem fent la demostració del punt (1) per la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que f és un monomorfisme, i per tant injectiva. Per la definició de nucli d'un morfisme entre grups (5.2.1.5) tenim que $\ker(f) = \{x \in G_1 : f(x) = e'\}$. Suposem $x \in G_1$, és a dir, $f(x) = e'$. Ara bé, com que f és injectiva per la proposició 5.2.1.2 ha de ser $\ker(f) = \{e\}$.

Demostrem ara la implicació cal a l'esquerra ($\Leftarrow$). Suposem doncs que $\ker(f) = \{e\}$. Siguin $x, y \in G_1$ dos elements que satisfacin $f(x) = f(y)$. Com que, per la proposició 5.2.1.7 $(\ker(f), *)$ és un subgrup de $(G_1, *)$, tenim que $x * y^{-1} \in G_1$, i per tant

$$\begin{aligned} f(x * y^{-1}) &= f(x) \circ f(y^{-1}) && \text{(morfisme entre grups (5.2.1.1))} \\ &= f(x) \circ f(y)^{-1} && \text{(Proposició 5.2.1.2)} \\ &= f(y) \circ f(y)^{-1} = e', \end{aligned}$$

i per tant $x * y^{-1} \in \ker(f)$, però per hipòtesi teníem $\ker(f) = \{e\}$, i per tant ha de ser $x * y^{-1} = e$, el que és equivalent a $x = y$, i per tant f és injectiva.

Demostrem ara el punt (2) començant per la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que f és un epimorfisme, i per tant exhaustiva, i per tant per a cada $y \in G_2$ existeix un $x \in G_1$ tal que $f(x) = y$, i per la definició d'imatge d'un morfisme entre grups (5.2.1.5) tenim que $\mathrm{Im}(f) = G_2$.

Acabem demostrant la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que $\mathrm{Im}(f) = G_2$ i prenem $y \in G_2$. Aleshores per la definició d'imatge d'un morfisme entre grups (5.2.1.5) tenim que existeix un $x \in G_1$ tal que $f(x) = y$, i per tant f és exhaustiva. □

Proposició 5.2.1.9. *Siguin $(G_1, *), (G_2, \circ)$ dos subgrups amb elements neutres e i e' respectivament, i $f : G_1 \to G_2$ un morfisme entre grups. Aleshores*

1. *Si* $(H_1, *) \leq (G_1, *) \Rightarrow (\{f(h) \in G_2 : h \in H_1\}, \circ) \leq (G_2, \circ)$.
2. *Si* $(H_2, \circ) \leq (G_2, \circ) \Rightarrow (\{h \in G_1 : f(h) \in H_2\}, *) \leq (G_1, *)$.
3. *Si* $(H_2, \circ) \trianglelefteq (G_2, \circ) \Rightarrow (\{h \in G_1 : f(h) \in H_2\}, *) \trianglelefteq (G_1, *)$.

Demostració. Comprovem primer el punt (1). Suposem doncs que $(H_1, *)$ és un subgrup de $(G_1, *)$. Denotarem $H = \{f(h) \in G_2 : h \in H_1\}$. Siguin $x, y \in H_1$; per la proposició 5.1.2.3 només ens cal veure que $f(x) \circ f(y)^{-1} \in H$. Això és

$$\begin{aligned} f(x) \circ f(y)^{-1} &= f(x) \circ f(y^{-1}) && \text{(Proposició 5.2.1.2)} \\ &= f(x * y^{-1}). && \text{(morfisme entre grups (5.2.1.1))} \end{aligned}$$

Ara bé, com que $x, y \in H_1$ i $(H_1, *)$ és un subgrup de $(G_1, *)$, per la proposició 5.1.2.3 tenim que $x * y^{-1} \in H_1$, i per tant $f(x * y^{-1}) \in H$, i per la definició de morfisme entre grups (5.2.1.1) i la proposició 5.2.1.2 tenim que $f(x) \circ f(y)^{-1} \in H$, i per tant $(H, \circ)$ és un subgrup de $(G_2, \circ)$, com volíem veure.

Comprovem ara el punt (2). Suposem doncs que $(H_2, \circ)$ és un subgrup de $(G_2, \circ)$ i denotem $H = \{h \in G_1 : f(h) \in H_2\}$. Per la proposició 5.1.2.3 només ens cal veure que per a tot $x, y \in H$ es satisfà $x * y^{-1} \in H$. Si $x, y \in H$ aleshores tenim que $f(x), f(y) \in H_2$, i com que $(H_2, \circ)$ és un grup, aleshores per la definició de grup (5.1.1.1) ha de ser $f(x) \circ f(y^{-1}) \in H_2$ Aleshores, per la definició de morfisme entre grups (5.2.1.1) tenim $f(x) \circ f(y^{-1}) = f(x * y^{-1})$, i per tant $x * y^{-1} \in H$ i així tenim que $(H, *)$ és un subgrup de $(G_1, *)$.

Veiem el punt (3) per acabar. Suposem doncs que $(H_2, \circ)$ és un subgrup normal de $(G_2, \circ)$ i definim $H = \{h \in G_1 : f(h) \in H_2\}$. Per demostrar-ho prenem $g \in G_1$, $h \in H_1$ tal que $f(h) \in H$ i fem

$$\begin{aligned} f(g) \circ f(h) \circ f(g)^{-1} &= f(g) \circ f(h) \circ f(g^{-1}) && \text{(Proposició 5.2.1.2)} \\ &= f(g * h * g^{-1}) && \text{(morfisme entre grups (5.2.1.1))} \end{aligned}$$

Ara bé, com que $(H_2, \circ)$ és un subgrup normal de $(G_2, \circ)$, tenim que, per a tot $g \in G_1$, $f(g * h * g^{-1}) \in H_2$, i per tant $g * h * g^{-1} \in H$, que satisfà la definició de subgrup normal (5.1.2.11) per la proposició 5.1.2.12. □

Teorema 5.2.1.10 (Teorema de representació de Cayley)**.** *Sigui $(G, *)$ un grup. Aleshores $(G, *)$ és isomorf a un subgrup de $(S_G, \circ)$, on S_G és el grup simètric dels elements de G.*

Demostració. Definim

$$\varphi : G \longrightarrow S_G \tag{5.3}$$

$$\begin{aligned} g \longmapsto \sigma_g : G &\longrightarrow G \\ x &\longmapsto g * x \end{aligned} \tag{5.4}$$

Tenim que σ_g és bijectiva ja que és una permutació. Comprovarem que φ és un monomorfisme entre grups. Veiem primer que és un morfisme entre grups. Prenem $g, g' \in G$. Per la definició (5.3) tenim que $\varphi(g * g') = \sigma_{g*g'}$. Per veure que $\sigma_{g*g'} = \sigma_g \circ \sigma_{g'}$ observem que per a tot $x \in G$

$$\begin{aligned} \sigma_{g*g'}(x) &= g * g' * x \\ &= g * \sigma_{g'}(x) \\ &= \sigma_g \circ \sigma_{g'}(x), \end{aligned}$$

i per la definició de morfisme entre grups (5.2.1.1) tenim que φ és un morfisme entre grups. Veiem ara que φ és un monomorfisme. Per la definició de nucli d'un morfisme entre grups (5.2.1.5) tenim que

$$\ker(\varphi) = \{x \in G : f(x) = \mathrm{Id}_G\}.$$

Ara bé, $\sigma_g = \mathrm{Id}$ és, per la definició (5.4), equivalent a dir que $g * x = x$ per a tota $x \in G$, i per la definició de l'element neutre d'un grup (5.1.1.3) això és si i només si $g = e$, i per tant

$$\ker(\varphi) = \{e\},$$

i per la proposició 5.2.1.8 tenim que φ és un monomorfisme, com volíem veure.

Per tant, per la proposició 5.2.1.9 tenim que

$$(G, *) \cong (\mathrm{Im}(\varphi), \circ) \leq (S_G, \circ).$$ □

Corol·lari 5.2.1.11. *Si $(G, *)$ té ordre n aleshores $(G, *) \cong (S_n, \circ)$.*

5.2.2 Teoremes d'isomorfisme entre grups

Teorema 5.2.2.1. *Siguin* $(G_1, *)$, $(G_2, \circ)$ *dos grups i* $f : G_1 \to G_2$ *un morfisme entre grups. Aleshores* $(G_1/\ker(f), *) \cong (\mathrm{Im}(f), \circ)$.

Demostració. Direm que e és l'element neutre de $(G_1, *)$ i e' és l'element neutre de $(G_2, \circ)$. Definim l'aplicació

$$\begin{aligned} \varphi : G_1/\ker(f) &\longleftrightarrow \mathrm{Im}(f) \\ [x] &\longmapsto f(x) \end{aligned} \tag{5.5}$$

Comprovem primer que aquesta aplicació està ben definida:

Suposem que $[x] = [x']$. Això és que $x' \in \{x\}\ker(f)$, i equivalentment $x' = x * h$ per a cert $h \in \ker(f)$. Per tant

$$\begin{aligned} \varphi([x']) &= \varphi([x * h]) && \text{(Definició (5.2))} \\ &= f(x * h) && \text{(Definició (5.5))} \\ &= f(x) \circ f(h) && \text{(morfisme entre grups (5.2.1.1))} \\ &= f(x) \circ e' && \text{(nucli d'un morfisme entre grups (5.2.1.5))} \\ &= f(x) = \varphi([x]) && \text{(Definició (5.5))} \end{aligned}$$

i per tant φ està ben definida. Veiem ara que φ és un morfisme entre grups. Tenim que

$$\begin{aligned} \varphi([x] * [y]) &= \varphi([x * y]) && \text{(Definició (5.2))} \\ &= f(x * y) && \text{(Definició (5.5))} \\ &= f(x) \circ f(y) && \text{(morfisme entre grups (5.2.1.1))} \\ &= \varphi([x]) \circ \varphi([y]), && \text{(Definició (5.5))} \end{aligned}$$

i per la definició de morfisme entre grups (5.2.1.1) φ és un morfisme entre grups. Continuem demostrant que φ és injectiva. Per la definició de nucli d'un morfisme entre grups (5.2.1.5) tenim que $\ker(\varphi) = \{[x] \in G/\ker(f) : \varphi([x]) = e\}$, i per tant $\ker(\varphi) = \ker(f)$, ja que $f(x) = e$ si i només si $x \in \ker(f)$, i per tant $\ker(\varphi) = [e]$ i per la proposició 5.2.1.8 φ és injectiva.

Per veure que φ és exhaustiva veiem que si $[x] \in G_1/\ker(f)$, per la definició de relació d'equivalència entre grups (5.1.4.2) tenim que $x = x' * y$ per a uns certs $x' \in G_2$, $h \in \ker(f)$, i per tant

$$\begin{aligned} \varphi([x]) &= \varphi([x' * h]) \\ &= \varphi([x'] * [h]) && \text{(relació d'equivalència entre grups (5.2))} \\ &= f(x') \circ f(e) && \text{(morfisme entre grups (5.2.1.1))} \\ &= f(x') && \text{(grup (5.1.1.1))} \\ &= f(x * h^{-1}) \\ &= f(x) \circ f(h^{-1}) && \text{(morfisme entre grups (5.2.1.1))} \\ &= f(x) \circ f(h)^{-1} && \text{(Proposició 5.2.1.2)} \\ &= f(x) \circ e^{-1} = f(x). && \text{(Proposició 5.1.1.8)} \end{aligned}$$

Així veiem que $\mathrm{Im}(\varphi) = \mathrm{Im}(f)$. Per tant φ és un isomorfisme, i tenim $(G_1/\ker(f), *) \cong (\mathrm{Im}(f), \circ)$, com volíem veure. □

Teorema 5.2.2.2 (Primer Teorema de l'isomorfisme)**.** *Siguin* $(G_1, *)$, $(G_2, \circ)$ *dos grups i* $f : G_1 \to G_2$ *un epimorfisme entre grups. Aleshores*

1. $(G_1/\ker(f), *) \cong (G_2, \circ)$.
2. *L'aplicació*

$$\begin{aligned} \varphi_1 : \{H : (\ker(f), *) \leq (H, *) \leq (G, *)\} &\longleftrightarrow \{K : (K, \circ) \leq (G_2, \circ)\} \\ H &\longmapsto \{f(h) \in G_2 : h \in H\} \end{aligned} \tag{5.6}$$

   és bijectiva.

3. *L'aplicació*

$$\begin{aligned} \varphi_2 : \{H : (\ker(f), *) \leq (H, *) \trianglelefteq (G, *)\} &\longleftrightarrow \{K : (K, \circ) \trianglelefteq (G_2, \circ)\} \\ H &\longmapsto \{f(h) \in G_2 : h \in H\} \end{aligned} \tag{5.7}$$

   és bijectiva.

Demostració. Direm que e és l'element neutre de $(G_1, *)$ i e' és l'element neutre de $(G_2, \circ)$.

El punt (1) és conseqüència del Teorema 5.2.2.1, ja que si f és exhaustiva, $\mathrm{Im}(f) = G_2$, i per tant $(G_1/\ker(f), *) \cong (G_2, \circ)$.

Per veure el punt (2) comencem demostrant que φ_1 està ben definida. Siguin $H_1 = H_2 \in \{H : (\ker(f), *) \leq (H, *) \leq (G, *)\}$. Aleshores, per la hipòtesi (5.6) tenim $\varphi_1(H_1) = \{f(h) \in G_2 : h \in H_1\}$ i $\varphi_1(H_2) = \{f(h) \in G_2 : h \in H_2\}$, i com que f és una aplicació, i per tant ben definida, $\varphi_1(H_1) = \varphi_1(H_2)$.

Continuem comprovant que φ_1 és bijectiva. Per veure que és injectiva prenem $H_1, H_2 \in \{H : (\ker(f), *) \leq (H, *) \leq (G, *)\}$ tals que $\varphi_1(H_1) = \varphi_1(H_2)$. Això, per la hipòtesi (5.6) és

$$\{f(h) \in G_2 : h \in H_1\} = \{f(h) \in G_2 : h \in H_2\}.$$

Per tant siguin $h_1 \in H_1$, $h_2 \in H_2$ tals que $f(h_1) = f(h_2)$. Equivalentment, per la proposició 5.1.1.6 i la definició de l'invers d'un element d'un grup (5.1.1.7) i la proposició 5.1.1.8 tenim les igualtats $f(h_2^{-1} * h_1) = f(h_1^{-1} * h_2) = e'$, i per la definició de nucli d'un morfisme entre grups (5.2.1.5) tenim $h_2^{-1} * h_1, h_1^{-1} * h_2 \in \ker(f)$, i per la hipòtesi (5.6) això és $h_2^{-1} * h_1 \in \ker(f) \subseteq H_2$ i $h_1^{-1} * h_2 \in \ker(f) \subseteq H_1$. Observem que això és que $h_1 \in \{h_2\}\ker(f)) \subseteq H_2$ i $h_2 \in \{h_1\}\ker(f)) \subseteq H_1$. Això vol dir que $H_1 \subseteq H_2$ i $H_2 \subseteq H_1$, i per doble inclusió això és $H_1 = H_2$, com volíem veure.

Per veure que φ_1 és exhaustiva tenim que per la proposició 5.2.1.9 i per la hipòtesi (5.6) tenim que donat un conjunt K tal que $(K, \circ) \leq (G_2, \circ)$ aleshores el conjunt $H = \{k \in G_1 : f(h) \in K\}$ satisfà $(H, *) \leq (G_1, *)$, i per la definició de nucli d'un morfisme entre grups (5.2.1.5) tenim que es compleix $(\ker(f), *) \leq (H, *) \leq (G_1, *)$, i per tant $\varphi_1(H) = K$, i per tant φ és exhaustiva; i per tant bijectiva.

Es pot demostrar el punt (3) amb el mateix argument que hem donat per demostrar el punt (2). □

Proposició 5.2.2.3. *Siguin* $(G, *)$ *un grup i* $(H, *), (K, *)$ *subgrups de* $(G, *)$. *Aleshores*

1. *Si* $(K,*) \trianglelefteq (G,*)$, *aleshores* $(HK,*) \leq (G,*)$.
2. *Si* $(H,*),(K,*) \trianglelefteq (G,*)$, *aleshores* $(HK,*) \trianglelefteq (G,*)$.

Demostració. Comencem veient el punt (1). Per la proposició 5.1.2.3 només ens cal comprovar que per a tot $x,y \in HK$ es satisfà $x * y^{-1} \in HK$. Siguin doncs $x,y \in HK$, que podem reescriure com $x = h_1 * k_1$ i $y = h_2 * k_2$. Calculem $x * y^{-1}$:

$$\begin{aligned} x * y^{-1} &= h_1 * k_1 * (h_2 * k_2)^{-1} \\ &= h_1 * k_1 * k_2^{-1} * h_2^{-1} && \text{(Proposició 5.1.1.10)} \\ &= h_1 * k_1 * h_2^{-1} * k_2^{-1}, && \text{(subgrup normal (5.1.2.11))} \\ &= h_1 * h_2^{-1} * k_1 * k_2^{-1}, && \text{(subgrup normal (5.1.2.11))} \end{aligned}$$

i com que, per la definició de grup (5.1.1.1) tenim $h_1 * h_2^{-1} \in H$ i $k_1 * k_2^{-1} \in K$, veiem que $x * y^{-1} \in HK$, com volíem demostrar.

La demostració del punt (2) és anàloga a la del punt (1). □

Lemma 5.2.2.4. *Siguin* $(G,*)$ *un grup,* $(H,*)$ *un subgrup de* $(G,*)$ *i* $(K,*)$ *un subgrup normal de* $(G,*)$. *Aleshores* $(H \cap K,*) \trianglelefteq (H,*)$.

Demostració. Prenem $x \in H$ i $y \in H \cap K$. Per la proposició 5.1.2.12 només hem de veure que per a tot $x \in H$ i $y \in H \cap K$, es satisfà $x^{-1} * y * x \in H$. Ara bé, com que $(K,*)$ és un grup normal, per la mateixa proposició 5.1.2.12, com que per hipòtesi $y \in H \cap K$, i en particular $y \in K$, tenim que $x^{-1} * y * x \in K$. Per veure que $x^{-1} * y * x \in H$ tenim prou amb veure que $x,y \in H$, i com que $(H,*)$ és un subgrup de $(G,*)$, i per tant un grup, per la definició de grup (5.1.1.1) tenim que $x^{-1} * y * x \in H$, i per tant $x^{-1} * y * x \in H \cap K$, com volíem veure. □

Teorema 5.2.2.5 (Segon Teorema de l'isomorfisme)**.** *Siguin* $(G,*)$ *un grup,* $(H,*)$ *un subgrup de* $(G,*)$ *i* $(K,*)$ *un subgrup normal de* $(G,*)$. *Aleshores*

$$(HK)/K \cong H/(H \cap K).$$

Demostració. Observem primer que aquest Teorema té sentit per les proposicions 5.1.2.4 i 5.2.2.3.

Definim

$$\begin{aligned} f : HK &\longrightarrow H/(H \cap K) \\ h * k &\longmapsto [h]. \end{aligned} \tag{5.8}$$

Demostrarem que f és un epimorfisme; però primer cal veure que f està ben definida. Prenem doncs $h_1 * k_1, h_2 * k_2 \in HK$ amb $h_1,h_2 \in H$ i $k_1,k_2 \in K$ tals que $h_1 * k_1 = h_2 * k_2$, i per tant $h_2^{-1} * h_1 = k_2 * k_1^{-1}$. Ara bé, com que per hipòtesi i per la definició de l'invers d'un element d'un grup (5.1.1.7) tenim que $h_1, h_2^{-1} \in H$ i a la vegada $k_2, k_1^{-1} \in K$, per la definició de grup (5.1.1.1) tenim $h_2^{-1} * h_1 \in H$ i $k_2 * k_1^{-1} \in K$ i com que $h_2^{-1} * h_1 = k_2 * k_1^{-1}$ tenim que $[h_2^{-1} * h_1] = [k_2^{-1} * k_1] = [e]$, i per la definició de relació d'equivalència entre grups (5.1.4.2) tenim que $[h_1] = [h_2]$ i per tant f està ben definida.

Veiem ara que f és un morfisme entre grups. Prenem $h_1, h_2 \in H$ i $k_1, k_2 \in K$, i per tant $h_1 * k_1, h_2 * k_2 \in HK$, i fem

$$\begin{aligned} f(h_1 * k_1 * h_2 * k_2) &= [h_1 * h_2] && \text{(Definició (5.8))} \\ &= [h_1] * [h_2] && \text{(Definició (5.2))} \\ &= f(h_1 * k_1) * f(h_2 * k_2) && \text{(Definició (5.8))} \end{aligned}$$

i per tant f satisfà la definició de morfisme entre grups (5.2.1.1).

Continuem veient que f és exhaustiva. Prenem $[h] \in H/(H \cap K)$. Per la definició (5.8) tenim que $f(h * k) = [h]$ per a qualsevol $k \in K$, i per tant f és exhaustiva.

Per tant f és un epimorfisme, i per tant, pel Primer Teorema de l'isomorfisme (5.2.2.2) tenim

$$HK/\ker(f) \cong H/(H \cap K).$$

Ara bé, per la definició de nucli d'un morfisme entre grups (5.2.1.5) tenim que $\ker(f) = \{h_1 * k_2 \in HK : f(h_1 * k_1) = [e]\}$, i per tant $\ker(f) = K$ i trobem

$$HK/K \cong H/(H \cap K). \qquad \square$$

Teorema 5.2.2.6 (Tercer Teorema de l'isomorfisme)**.** *Siguin $(G, *)$ un grup i $(H, *), (K, *)$ dos subgrups normals de $(G, *)$ amb $K \subseteq H$. Aleshores*

$$G/H \cong (G/K)/(H/K).$$

Demostració. Definim les aplicacions

$$\begin{aligned} \varphi_1 : G &\longrightarrow G/K \\ g &\longmapsto [g] \end{aligned} \qquad \text{i} \qquad \begin{aligned} \varphi_2 : G/K &\longrightarrow (G/K)/(H/K) \\ [g] &\longmapsto \overline{[g]}. \end{aligned}$$

Veiem que φ_1 i φ_2 són morfismes.

Per la proposició 5.2.1.3 tenim que $\varphi_2(\varphi_1) : G \longrightarrow (G/K)/(H/K)$ és un epimorfisme entre grups, i pel Primer Teorema de l'isomorfisme (5.2.2.2) trobem

$$G/\ker(\varphi_2(\varphi_1)) \cong (G/K)/(H/K).$$

Veiem ara que $\ker(\varphi_2(\varphi_1)) = H$. Per la definició de relació d'equivalència entre grups (5.1.4.2) tenim que $G/K = \{gK : g \in G\}$ i $H/K = \{hK : h \in H\}$, i per tant

$$(G/K)/(H/K) = \{gKhK : g \in G, h \in H\}, \tag{5.9}$$

però com que, per hipòtesi, $(H, *)$ i $(K, *)$ són subgrups normals de $(G, *)$, per la definició de subgrup normal (5.1.2.11) podem reescriure (5.9) com

$$(G/K)/(H/K) = \{ghK : g \in G, h \in H\}. \tag{5.10}$$

Ara bé, com que per hipòtesi $K \subseteq H$ podem reescriure (5.10) com

$$(G/K)/(H/K) = \{gH : g \in G\},$$

i trobem, per la definició de nucli d'un morfisme entre grups (5.2.1.5), que $\ker(\varphi_2(\varphi_1)) = H$, i per tant

$$G/H \cong (G/K)/(H/K). \qquad \square$$

5.3 Tres Teoremes de Sylow

5.3.1 Accions sobre grups

Definició 5.3.1.1 (Acció d'un grup sobre un conjunt)**.** Siguin $(G, *)$ un grup amb element neutre e, X un conjunt no buit i

$$\begin{aligned} \cdot : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

una operació que satisfaci

1. $e \cdot x = x$ per a tot $x \in X$.
2. $(g_1 * g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ per a tot $x \in X$, $g_1, g_2 \in G$.

Aleshores direm que $\cdot$ és una acció de $(G, *)$ sobre X. També direm que X és un G-conjunt amb l'acció $\cdot$.

Proposició 5.3.1.2. *Siguin $(G, *)$ un grup, X un conjunt, $\cdot$ una acció de $(G, *)$ sobre X i $\sim$ una relació sobre X tal que per a tot $x_1, x_2 \in X$ diem que $x_1 \sim x_2$ si i només si existeix un $g \in G$ tal que $x_1 = g \cdot x_2$. Aleshores la relació $\sim$ és una relació d'equivalència.*

Demostració. Sigui e l'element neutre del grup $(G, *)$. Comprovem que $\sim$ satisfà la definició de relació d'equivalència (1.3.0.2):

1. Reflexiva: Sigui $x \in X$. Per la definició de acció d'un grup sobre un conjunt (5.3.1.1) tenim que $x = x \cdot e$, i per tant $x \sim x$.
2. Simètrica: Siguin $x_1, x_2 \in X$ tals que $x_1 \sim x_2$. Per tant existeix $g \in G$ tal que $x_1 = g \cdot x_2$. Per la definició de acció d'un grup sobre un conjunt (5.3.1.1) tenim que $g \cdot x_2 \in X$, i per tant podem prendre $g^{-2} \cdot (g * x_2)$, que és equivalent a $g^{-2} \cdot (g \cdot x_2) = g^{-2} \cdot x_1$, i així $x_2 = g^{-1} \cdot x_1$, i per tant $x_2 \sim x_1$.
3. Transitiva: Siguin $x_1, x_2, x_3 \in X$ tals que $x_1 \sim x_2$ i $x_2 \sim x_3$. Per tant existeixen $g_1, g_2 \in G$ tals que $x_1 = g_1 \cdot x_2$ i $x_2 = g_2 \cdot x_3$, i per tant $x_1 = g_1 \cdot (g_2 \cdot x_3)$, i per la definició de acció d'un grup sobre un conjunt (5.3.1.1) això és $x_1 = (g_1 * g_2) \cdot x_3$, i com que $(G, *)$ és un grup, $g_1 * g_2 \in G$, i tenim que $x_1 \sim x_3$.

per tant $\sim$ és una relació d'equivalència. □

Definició 5.3.1.3 (Òrbita d'un element d'un G-conjunt)**.** Siguin $(G, *)$ un grup, $\cdot$ una acció de $(G, *)$ sobre un conjunt X i $\sim$ una relació d'equivalència sobre X tal que per a tot $x_1, x_2 \in X$ diem que $x_1 \sim x_2$ si i només si existeix un $g \in G$ tal que $x_1 = g \cdot x_2$. Aleshores direm que $\mathcal{O}(x) = [x]$ és l'òrbita de x.

Observem que aquesta definició té sentit per la proposició 5.3.1.2.

Definició 5.3.1.4 (Estabilitzador d'un element per una acció)**.** Siguin $(G, *)$ un grup, X un conjunt i $\cdot$ una acció de $(G, *)$ sobre X. Aleshores direm que el conjunt

$$\mathrm{St}(x) = \{g \in G : g \cdot x = x\}$$

és l'estabilitzador de x per l'acció $\cdot$.

Proposició 5.3.1.5. *Siguin $(G,*)$ un grup, $\cdot$ una acció de $(G,*)$ sobre un conjunt X i $\mathrm{St}(x)$ l'estabilitzador d'un element x de X per l'acció $\cdot$. Aleshores $g \in \mathrm{St}(x)$ si i només si $g^{-1} \in \mathrm{St}(x)$.*

Demostració. Per la definició de l'estabilitzador d'un element per una acció (5.3.1.4) tenim que $g \in \mathrm{St}(x)$ si i només si $g \cdot x = x$. Ara bé, si prenem $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$, i per la definició de acció d'un grup sobre un conjunt (5.3.1.1) tenim que $g^{-1} \cdot (g \cdot x) = (g^{-1} * g) \cdot x$, i per la definició de l'invers d'un element d'un grup (5.1.1.7) tenim que $g^{-1} \cdot x$ i per tant $g^{-1} \in \mathrm{St}(x)$. □

Proposició 5.3.1.6. *Siguin $(G,*)$ un grup, $\cdot$ una acció de $(G,*)$ sobre un conjunt X i $\mathrm{St}(x)$ l'estabilitzador de x per l'acció $\cdot$. Aleshores $(\mathrm{St}(x),*)$ és un subgrup de $(G,*)$.*

Demostració. Per la proposició 5.1.2.3 només ens cal veure que per a tot $g_1, g_2 \in \mathrm{St}(x)$ es compleix $g_1 * g_2^{-1} \in \mathrm{St}(x)$.

Prenem doncs $g_1, g_2 \in \mathrm{St}(x)$. Per la proposició 5.3.1.5 tenim que $g_2^{-1} \in \mathrm{St}(x)$, i per tant, per la definició de l'estabilitzador d'un element per una acció (5.3.1.4) tenim que $(g_1 * g_2^{-1}) \cdot x = x$, i per tant $g_1 * g_2^{-1} \in \mathrm{St}(x)$. □

Proposició 5.3.1.7. *Siguin $(G,*)$ un grup d'ordre finit, X un G-conjunt finit amb una acció $\cdot$ i $\mathrm{St}(x)$ l'estabilitzador d'un element x de X per l'acció $\cdot$. Aleshores*

$$|G/\mathrm{St}(x)| = |\mathcal{O}(x)| = [G : \mathrm{St}(x)].$$

Demostració. Considerem

$$\begin{aligned} f : G/\mathrm{St}(x) &\longrightarrow \mathcal{O}(x) \\ [g] &\longmapsto g \cdot x \end{aligned}$$

Volem veure que f és una aplicació bijectiva, per tant mirem si està ben definida:

Siguin $[g_1], [g_2] \in G/\mathrm{St}(x)$ tals que $[g_1] = [g_2]$. Per tant $g_1 = g_2 * g'$ per a cert $g' \in \mathrm{St}(x)$, i per la definició de l'estabilitzador d'un element per una acció (5.3.1.4) tenim $g_1 \cdot x = x$, $(g_2 * g') \cdot x = x$, i per la definició de acció d'un grup sobre un conjunt (5.3.1.1) això és $g_2 \cdot (g' \cdot x) = x$, i per la proposició 5.3.1.5 $g_2 \cdot x = x$, i per tant f està ben definida.

Veiem ara que f és injectiva. Prenem $g \cdot x, g' \cdot x \in \mathcal{O}(x)$ tals que $g \cdot x = g' \cdot x$. Això, per la definició de acció d'un grup sobre un conjunt (5.3.1.1), és equivalent a dir $x = (g^{-1} * g') \cdot x$, i per la definició de l'estabilitzador d'un element per una acció (5.3.1.4) tenim que $g^{-1} * g \in \mathrm{St}(x)$. Per tant, per la definició de relació d'equivalència entre grups (5.1.4.2) tenim que $[g] = [g']$, i per tant f és injectiva.

Per veure que f és exhaustiva veiem que per a qualsevol $g \cdot x \in \mathcal{O}(x)$, $f([g]) = g \cdot x$, i per tant f és exhaustiva i tenim que $|\mathrm{St}(x)| = |\mathcal{O}(x)|$, ja que f és una bijecció. □

5.3.2 Teoremes de Sylow

Definició 5.3.2.1 (p-subgrup de Sylow)**.** Siguin $(G,*)$ un grup tal que $|G| = p^n m$ amb p primer que no divideix m i $(P,*)$ un subgrup de $(G,*)$ amb $|P| = p^n$. Aleshores direm que $(P,*)$ és un p-subgrup de Sylow de $(G,*)$.

Lemma 5.3.2.2. *Siguin p un primer i m un enter positiu tal que p no divideixi m. Aleshores per a tot n natural tenim que*

$$\binom{p^n m}{p^n} \tag{5.11}$$

no és divisible per p.

Demostració. Tenim que

$$\binom{p^n m}{p^n} = \frac{p^n m(p^n m-1)\cdots(p^n m-p^n+1)}{p^n(p^n-1)\cdots(p^n-p^n+1)} = \prod_{i=0}^{p^n-1} \frac{p^n m-i}{p^n-i}. \tag{5.12}$$

Com que, per hipòtesi, p és primer aquesta expressió només serà divisible per p si ho són els elements del numerador. Fixem doncs $i \in \{0,\dots,p^n+1\}$ i estudiem l'i-èsim terme del producte de (5.12). Notem primer que si $i=0$ aquest terme no és divisible per p. Imposem ara també que $i \neq 0$. Si el denominador, $p^n m-i$, és divisible per p tindrem que $p^n m-i = p^k m'$, on m' no és divisible per p, i per tant k serà l'exponent més gran que satisfaci la igualtat. Si aïllem i obtindrem $i = p^k(p^{n-k}m-m')$. Ara bé, tenim doncs que $p^n-i = p^n-p^k(p^{n-k}m-m')$, i això és $p^n-p^k(p^{n-k}m-m') = p^k(p^{n-k}(1-m)-m')$, i per tant tindrem que l'i-èsim terme del producte de (5.12) serà de la forma

$$\frac{p^n m-i}{p^n-i} = \frac{p^k m'}{p^k(p^{n-k}(1-m)-m')} = \frac{m'}{p^{n-k}(1-m)-m'},$$

i així veiem que aquest i-èsim terme del producte no serà divisible per p; i com que això és cert per a qualsevol $i \in \{0,\dots,p^n+1\}$ tenim que (5.11) tampoc ho serà, com volíem veure. □

Teorema 5.3.2.3 (Primer Teorema de Sylow)**.** *Siguin $(G,*)$ un grup tal que $|G| = p^n m$ amb p primer que no divideix m. Aleshores existeix un subconjunt $P \subseteq G$ tal que $(P,*)$ sigui un p-subgrup de Sylow de $(G,*)$.*

Demostració. Sigui $\mathcal{P}_{p^n}(G) = \{H \subseteq G : |H| = p^n\} = \{H_1,\dots,H_k\}$ el conjunt de subconjunts d'ordre p^n de G. Aleshores tenim que

$$k = |\mathcal{P}_{p^n}(G)| = \binom{p^n m}{p^n},$$

i pel lemma 5.3.2.2 tenim que p no divideix k.

Sigui e l'element neutre de $(G,*)$. Definim

$$\begin{aligned} \cdot : G \times \mathcal{P}_{p^n}(G) &\longrightarrow \mathcal{P}_{p^n}(G) \\ (g,X) &\longmapsto \{g\}X. \end{aligned} \tag{5.13}$$

Veurem que $\cdot$ és una acció de $(G,*)$ sobre $\mathcal{P}_{p^n}(G)$. Primer hem de veure que, efectivament, $\cdot$ està ben definida. Prenem $g_1,g_2 \in G$ i $X_1,X_2 \in \mathcal{P}_{p^n}(G)$ tals que $g_1 = g_2$ i $X_1 = X_2$. Per tant tenim $g_1 \cdot X_1 = g_2 \cdot X_2$ ja que $\{g_1\}X_1 = \{g_2\}X_2$. Per veure que $g_1 \cdot X_1 \in \mathcal{P}_{p^n}(G)$ en tenim prou amb veure que, per a tot $X \in \mathcal{P}_{p^n}(G)$, si fixem $g \in G$ l'aplicació $g \cdot X$ té inversa, que per la definició de l'invers d'un element d'un grup (5.1.1.7) és $x^{-1} \cdot X$, i per tant $X \in \mathcal{P}_{p^n}(G)$.

Comprovem que $\cdot$ satisfà la definició de acció d'un grup sobre un conjunt (5.3.1.1). Tenim que $e \cdot X = X$ per a tot $X \in \mathcal{P}_{p^n}(G)$ ja que, per la definició de conjugació entre conjunts sobre grups (5.1.2.10), $eX = X$.

De nou per la definició de conjugació entre conjunts sobre grups (5.1.2.10) veiem que per a tot $g_1, g_2 \in G$ i $X \in \mathcal{P}_{p^n}(G)$ tenim que

$$\begin{aligned}(g_1 * g_2) \cdot X &= \{g_1 * g_2\}X \\ &= \{g_1\}\{g_2\}X \\ &= \{g_1\}(\{g_2\}X) = g_1 \cdot (g_2 \cdot X).\end{aligned}$$

i per tant $\cdot$ satisfà la definició de acció d'un grup sobre un conjunt (5.3.1.1).

Veiem ara que existeix almenys un element $X \in \mathcal{P}_{p^n}(G)$ tal que la seva òrbita, $\mathcal{O}(X)$, tingui ordre no divisible per p. Per veure això observem que per la definició de l'òrbita d'un element d'un G-conjunt (5.3.1.3) veiem que $\mathcal{O}(X)$ és un classe d'equivalència, i per tant l'ordre del conjunt $\mathcal{P}_{p^n}$ és la suma dels ordres de les òrbites dels seus elements, $\mathcal{O}(X)$, i si p dividís l'ordre de $\mathcal{O}(X)$ per a tot $X \in \mathcal{P}_{p^n}$ tindríem que p també divideix k, però ja hem vist que això no pot ser. Per tant existeix almenys un element $X \in \mathcal{P}_{p^n}$ tal que $|\mathcal{O}(X)|$ no és divisible per p. Fixem aquest conjunt X.

Prenem l'estabilitzador de X, $\mathrm{St}(X)$. Per la proposició 5.3.1.7 tenim que $|\mathrm{St}(x)|$ divideix p^n. Prenem també $x_o \in X$ i $g \in \mathrm{St}(X)$. Per la definició de l'estabilitzador d'un element per una acció (5.3.1.4) tenim que $\{g\}X = X$, i per tant $g * x_0 \in X$, i equivalentment $g \in X\{x_0^{-1}\}$. Així veiem que $\mathrm{St}(X) \subseteq X\{x_0^{-1}\}$, i per tant tenim que $|\mathrm{St}(X)| \leq |X\{x_0\}|$. Observem que $X\{x_0\} \in \mathcal{P}_{p^n}(G)$ i per tant $|X\{x_0\}| = p^n$. Ara bé, l'ordre de $\mathrm{St}(X)$ divideix p^n, però acabem de veure que $|\mathrm{St}(X)| \leq p^n$. Per tant ha de ser $|\mathrm{St}(X)| = p^n$, i per tant, per la proposició 5.3.1.6 tenim que $(\mathrm{St}(X), *) \leq (G, *)$, i per tant, per la definició de p-subgrup de Sylow (5.3.2.1), $(\mathrm{St}(X), *)$ és un p-subgrup de Sylow. □

Corol·lari 5.3.2.4 (Teorema de Cauchy per grups)**.** *Siguin $(G, *)$ un grup d'ordre finit i p un primer que divideix l'ordre de $(G, *)$. Aleshores existeix un element $g \in G$ tal que l'ordre de g sigui p.*

Demostració. Direm que e és l'element neutre de $(G, *)$. Pel Primer Teorema de Sylow (5.3.2.3) tenim que existeix un p-subgrup de Sylow $(P, *)$ de $(G, *)$, que per la definició de p-subgrup de Sylow (5.3.2.1) té ordre p^n per a cert $n \in \mathbb{N}$. Ara bé, pel Teorema de Lagrange (5.1.4.5) tenim que per a tot $x \in P$ diferent del neutre el grup cíclic general per x ha de tenir ordre p^t amb $t \in \{2, \ldots, n\}$, i per tant l'element $x^{p^{t-1}}$ té ordre p, ja que

$$\left(x^{p^{t-1}}\right)^p = x^{p^t} = e.$$ □

Lemma 5.3.2.5. *Siguin $(G, *)$ un grup d'ordre p^n on p és un primer, X un G-conjunt d'ordre finit amb una acció $\cdot$ i $X_G = \{x \in X : g \cdot x = x \text{ per a tot } g \in G\}$ un conjunt. Aleshores*

$$|X_G| \equiv |X| \pmod{p}.$$

Demostració. Siguin $\mathcal{O}(x_1), \ldots, \mathcal{O}(x_r)$ les òrbites dels elements de X. Aleshores, com que per la definició de l'òrbita d'un element d'un G-conjunt (5.3.1.3) aquestes

són classes d'equivalència, tenim que

$$X = \bigcup_{i=1}^{r} \mathcal{O}(x_i),$$

i com que aquestes òrbites són disjuntes per ser classes d'equivalència

$$|X| = \sum_{i=0}^{r} |\mathcal{O}(x_i)|. \tag{5.14}$$

Ara bé, per les proposicions 5.3.1.7 i 5.3.1.6 i el Teorema de Lagrange (5.1.4.5) tenim que l'ordre $\mathcal{O}(x_i)$ divideix l'ordre de X, i per tant els únics elements amb òrbites que tinguin un ordre que no sigui divisible per p són els elements del conjunt X_G; i com que les òrbites d'aquests elements tenen un únic element tenim que

$$|X_G| = \sum_{x \in X_G} |\mathcal{O}(x)|,$$

i per tant, recordant que totes les altres òrbites tenen ordre divisible per p, trobem, amb (5.14), que

$$|X_G| \equiv |X| \pmod{p}. \qquad \square$$

Teorema 5.3.2.6 (Segon Teorema de Sylow)**.** *Siguin $(G, *)$ un grup d'ordre finit, p un primer que divideixi l'ordre de $(G, *)$ i $(P_1, *), (P_2, *)$ dos p-subgrups de Sylow de $(G, *)$. Aleshores existeix $g \in G$ tal que*

$$\{g\}P_1\{g^{-1}\} = P_2.$$

Demostració. Primer observem que aquest enunciat té sentit pel Primer Teorema de Sylow (5.3.2.3).

Definim el conjunt $X = \{\{x\}P_1 : x \in G\}$ i

$$\begin{aligned} \cdot : P_2 \times X &\longrightarrow X \\ (y, \{x\}P_1) &\longmapsto \{y\}\{x\}P_1. \end{aligned} \tag{5.15}$$

Primer veurem que $\cdot$ és una acció. Per veure que $\cdot$ està ben definida prenem $\{x\}P_1, \{x'\}P_1 \in X$ tals que $\{x\}P_1 = \{x'\}P_1$. Aleshores per a tot $y \in P_2$ tindrem $y \cdot \{x\}P_1 = \{y\}\{x\}P_1$ i $y \cdot \{x'\}P_1 = \{y\}\{x'\}P_1$, i com que per hipòtesi $\{x\}P_1 = \{x'\}P_1$, ha de ser $\{y\}\{x\}P_1 = \{y\}\{x'\}P_1$.

Comprovem que $\cdot$ satisfà la definició de acció d'un grup sobre un conjunt (5.3.1.1). Veiem que per a tot $y \in P_2$, $\{x\}P_1 \in X$ es compleix que $y \cdot \{x\}P_1 \in X$. Per la definició (5.15) tenim $y \cdot \{x\}P_1 \in X = \{y\}\{x\}P_1 = \{y * x\}P_1$, i com que per hipòtesi $(G, *)$ és un grup i $x, y \in G$, per la definició de grup (5.1.1.1) tenim que $y * x \in G$, i per tant $y \cdot \{x\}P_1 \in X$.

Sigui e l'element neutre de $(G, *)$. Tenim que

$$\begin{aligned} e \cdot \{x\}P_1 &= \{e\}\{x\}P_1 \\ &= \{e * x\}P_1 = \{x\}P_1. \qquad \text{(l'element neutre d'un grup (5.1.1.3))} \end{aligned}$$

i per últim veiem que per a tot $y, y' \in G$ tenim $(y * y') \cdot P_1 = y \cdot (y' \cdot P_1)$. Això és

$$\begin{aligned}(y * y') \cdot P_1 &= \{y * y'\}P_1 \\ &= \{y\}\{y'\}P_1 \\ &= \{y\}(\{y'\}P_1) = y \cdot (y' \cdot P_1). \qquad \text{(Definició (5.15))}\end{aligned}$$

i per la definició de acció d'un grup sobre un conjunt (5.3.1.1) tenim que X és un G-conjunt.

Definim el conjunt

$$X_{P_2} = \{\{x\}P_1 \in X : y \cdot \{x\}P_1 = \{x\}P_1 \text{ per a tot } y \in P_2\}. \tag{5.16}$$

Aleshores pel lemma 5.3.2.5 tenim que

$$|X_{P_2}| \equiv |X| \pmod{p}.$$

Ara bé, per la definició de l'índex d'un subgrup en un grup (5.1.4.7) i (5.15) tenim que $|X| = [G : P_1]$, i per hipòtesi tenim que $|X| = \frac{p^n m}{p^n} = m$, en particular $|X_{P_2}| \neq 0$. Així veiem que existeix almenys un element que satisfà la definició de X_{P_2}, (5.16); és a dir, existeix almenys un $\{x\}P_1$ tal que $y \cdot \{x\}P_1 = \{x\}P_1$ per a tot $y \in P_2$, i per tant tenim que $\{y\}\{x\}P_1 = \{x\}P_1$, i per tant $\{x^{-1}\}\{y\}\{x\}P_1 \in \{x^{-1}\}\{x\}P_1$, i equivalentment $x^{-1} * y * x \in P_1$ per a tot $y \in P_2$, i per tant $\{x^{-1}\}P_2\{x\} \subseteq P_1$, però, per hipòtesi, al ser els dos p-subgrups de Sylow, per la definició de p-subgrup de Sylow (5.3.2.1) trobem $|P_1| = |P_2| = |\{x^{-1}\}P_2\{x\}|$ i tenim que $\{x\}P_1\{x^{-1}\} = P_2$. □

Corol·lari 5.3.2.7. *$(G, *)$ té un únic p-subgrup de Sylow si i només si aquest és un subgrup normal.*

Teorema 5.3.2.8 (Tercer Teorema de Sylow)**.** *Siguin $(G, *)$ un grup d'ordre $p^n m$ on p és un primer que no divideix m i n_p el número de p-subgrups de Sylow de $(G, *)$. Aleshores $n_p \equiv 1 \pmod{p}$ i n_p divideix l'ordre de $(G, *)$.*

Demostració. Definim el conjunt

$$X = \{T \subseteq G : (T, *) \text{ és un } p\text{-subgrup de Sylow de } (G, *)\}.$$

Pel Primer Teorema de Sylow (5.3.2.3) tenim que X és no buit[4] i fixem $P \in X$.

Definim

$$\begin{aligned}\cdot : P \times X &\longrightarrow X \\ (g, T) &\longmapsto \{g\}T\{g^{-1}\}.\end{aligned} \tag{5.17}$$

Anem a veure que $\cdot$ és una acció. Veiem que $\cdot$ està ben definida, ja que si $T \in X$, aleshores per a tot $x \in G$, i en particular per a tot $x \in P$ ja que $(P, *) \leq (G, *)$, tenim $|\{x\}T\{x^{-1}\}| = |T|$, i per tant $|\{x\}T\{x^{-1}\}| \in X$ per la definició de p-subgrup de Sylow (5.3.2.1). Veiem ara que $\cdot$ satisfà les condicions de la definició de acció d'un grup sobre un conjunt (5.3.1.1). Sigui e l'element neutre de $(G, *)$. Tenim que per a tot $T \in X$

$$\begin{aligned}e \cdot T &= \{e\}T\{e^{-1}\} \qquad \text{(Definició (5.17))} \\ &= T\end{aligned}$$

[4] Tindrem que $|X| = n_p$.

i per a tot $g_1, g_2 \in P$ i $T \in X$

$$\begin{aligned}
(g_1 * g_2) \cdot T &= \{g_1 * g_2\} T \{g_1 * {g_2}^{-1}\} && \text{(Definició (5.17))} \\
&= \{g_1 * g_2\} T \{g_2^{-1} * g_1^{-1}\} && \text{(Proposició 5.1.1.10)} \\
&= \{g_1\}\{g_2\} T \{g_2^{-1}\}\{g_1^{-1}\} \\
&= \{g_1\}(g_2 \cdot T)\{g_1^{-1}\} && \text{(Definició (5.17))} \\
&= g_1 \cdot (g_2 \cdot T) && \text{(Definició (5.17))}
\end{aligned}$$

i per tant, per la definició de acció d'un grup sobre un conjunt (5.3.1.1) X és un P-conjunt amb l'acció $\cdot$.

Definim el conjunt

$$X_P = \{T \in X : g \cdot T = T \text{ per a tot } g \in P\},$$

i per la definició (5.17) tenim que si $T \in X_P$ aleshores per a tot $g \in G$ es compleix $\{g\}T\{g^{-1}\} = T$. Ara bé, això és que $T = P$ per a tot $T \in X_P$, i per tant $|X_P| = 1$. Aleshores pel lemma 5.3.2.5 tenim que

$$|X| \equiv |X_p| \pmod{p},$$

o equivalentment

$$|X| \equiv 1 \pmod{p}.$$

Per veure que $|X|$ divideix l'ordre de $(G, *)$ prenem $P \in X$ i tenim, pel Segon Teorema de Sylow (5.3.2.6) i la definició de l'òrbita d'un element d'un G-conjunt (5.3.1.3), que

$$\mathcal{O}(P) = X,$$

on $\mathcal{O}(P)$ és l'òrbita de P, i per tant

$$|\mathcal{O}(P)| = |X|,$$

i per les proposicions 5.3.1.6 i 5.3.1.7 i el Teorema de Lagrange (5.1.4.5) tenim que $|X|$ divideix l'ordre de $(G, *)$. □

Corol·lari 5.3.2.9. *Si $(G, *)$ té ordre $p^n q^m$ on p, q són primers amb $p < q$ aleshores $n_q = 1$, i pel corol·lari 5.3.2.7, aquest és normal en $(G, *)$.*

Capítol 6

Teoria d'anells

6.1 Introducció

6.1.1 Anells

Definició 6.1.1.1 (Anell)**.** Sigui R un conjunt no buit i

$$+ : R \times R \longrightarrow R \qquad \cdot : R \times R \longrightarrow R$$

dues operacions que satisfan

- $(R, +)$ és un grup abelià.
- Per a tot $x, y, z \in R$ tenim

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

- Per a tot $x, y, z \in R$ tenim

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{i} \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Aleshores direm que $(R, +, \cdot)$ és un anell.

Si per a tot $x, y \in R$ tenim $x \cdot y = y \cdot x$ direm que $(R, +, \cdot)$ és un anell commutatiu, i si existeix un element e' tal que $x \cdot e' = e' \cdot x = x$ per a tot $x \in A$ direm que $(R, +, \cdot)$ és un anell amb element neutre pel producte.

També anomenarem a l'operació $+$ suma i a l'operació $\cdot$ producte.

Proposició 6.1.1.2. *Sigui $(R, +, \cdot)$ un anell amb element neutre pel producte e'. Aleshores el neutre pel producte e' de $(R, +, \cdot)$ és únic.*

Demostració. Suposem que existeix un altre $e'' \neq e'$ tal que $x \cdot e'' = e'' \cdot x = x$ per a tot $x \in R$. Aleshores tindríem

$$e' \cdot e'' = e'' \cdot e' = e'$$

a la vegada que

$$e' \cdot e'' = e'' \cdot e' = e''$$

i per tant ha de ser $e' = e''$, que contradiu la hipòtesi que existeix un altre element neutre pel producte a $(R, +, \cdot)$, i en conseqüència aquest és únic. □

Definició 6.1.1.3 (Elements neutres d'un anell)**.** Sigui $(R,+,\cdot)$ un anell amb element neutre pel producte 1_R on l'element neutre del grup $(R,+)$ és 0_R. Aleshores direm que 0_R és l'element neutre de l'anell $(R,+,\cdot)$ per la suma i 1_R és l'element neutre de l'anell $(R,+,\cdot)$ pel producte i els denotarem per 0_R i 1_R, respectivament.

Observem que aquesta definició té sentit per les proposicions 5.1.1.2 i 6.1.1.2.

Notació 6.1.1.4. Donat un anell $(R,+,\cdot)$, aprofitant que el producte $\cdot$ és associatiu escriurem

$$(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot x_2 \cdot x_3.$$

També, si el context ho permet (quan treballem amb un únic anell R), denotarem $1_R = 1$ i $0_R = 0$.

Proposició 6.1.1.5. *Sigui $(R,+,\cdot)$ un anell. Aleshores per a tot $a,b,c \in R$ tenim*

1. $0 \cdot a = a \cdot 0 = 0$.
2. $(-1) \cdot a = a \cdot (-1) = -a$.
3. $(-a) \cdot (-b) = a \cdot b$.
4. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

Demostració. Comprovem el punt (1). Només veurem que $0 \cdot a = 0$ ja que l'altre demostració és anàloga. Com que $0 = 0 + 0$ per la definició de l'element neutre d'un anell per la suma (6.1.1.3), per la definició d'anell (6.1.1.1) tenim que

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a \\ &= 0 \cdot a + 0 \cdot a \end{aligned}$$

i per tant, per la definició de grup (5.1.1.1)

$$0 \cdot a - (0 \cdot a) = 0 \cdot a + 0 \cdot a - (0 \cdot a)$$

d'on veiem

$$0 \cdot a = 0,$$

com volíem veure.

Veiem ara el punt (2). Per la definició d'anell (6.1.1.1) tenim

$$1 \cdot a + (-1) \cdot a = (1-1) \cdot a \quad \text{i} \quad (-1) \cdot a + 1 \cdot a = (-1+1) \cdot a$$

i per tant, com que $1 - 1 = -1 + 1 = 0$ per la definició de l'element neutre d'un anell per la suma (6.1.1.3), tenim que $a + (-1) \cdot a = (-1) \cdot a + a = 0$, però per la proposició 5.1.1.6 tenim que $(-1) \cdot a = -a$. L'altre igualtat és anàloga.

Continuem veient el punt (3). Pel punt (2) tenim que

$$(-a) \cdot (-b) = a \cdot (-1) \cdot (-1) \cdot b.$$

Ara bé, pel punt (2) de nou tenim que $(-1) \cdot (-1) = -(-1)$, i per la proposició 5.1.1.9 tenim que $-(-1) = 1$ i per tant

$$(-a) \cdot (-b) = a \cdot b.$$

Per veure el punt (4) només veurem que $(-a)\cdot b = -(a\cdot b)$ ja que l'altre demostració és anàloga. Pel punt (2) tenim que

$$-(a\cdot b) = (-1)\cdot(a\cdot b) \quad \text{i} \quad (-a)\cdot b = (-1)\cdot a\cdot b.$$

Ara bé, per la definició d'anell (6.1.1.1)

$$(-1)\cdot a\cdot b - (-1)\cdot(a\cdot b) = (-1-(-1))\cdot(a\cdot b),$$

i per la proposició 5.1.1.9 tenim que $-(-1) = 1$ i per tant, per la definició de grup (5.1.1.1) tenim $-1+1=0$ i trobem

$$(-1)\cdot a\cdot b - (-1)\cdot(a\cdot b) = 0\cdot(a\cdot b) = 0,$$

i podem veure també que

$$(-1)\cdot(a\cdot b) - (-1)\cdot a\cdot b = 0$$

de manera anàloga. Aleshores, per la proposició 5.1.1.6 tenim que

$$(-a)\cdot b = -(a\cdot b),$$

com volíem veure. □

Proposició 6.1.1.6. *Siguin $(R,+,\cdot)$ un anell i a un element invertible de R, tal que existeixi $b\in R$ que satisfaci*

$$a\cdot b = b\cdot a = 1.$$

Aleshores b és únic.

Demostració. Suposem que existeix un altre element $b'\in R$ tal que

$$a\cdot b' = b'\cdot a = 1.$$

Aleshores tenim

$$a\cdot b = a\cdot b'$$

i per tant

$$b\cdot a\cdot b = b\cdot a\cdot b'$$

i com que per hipòtesi $b\cdot a = 1$ per la definició de l'element neutre d'un anell pel producte (6.1.1.3) trobem

$$b = b'.$$ □

Definició 6.1.1.7 (Element invertible)**.** Siguin $(R,+,\cdot)$ un anell i x un element de R tal que existeixi $x'\in R$ tals que

$$x\cdot x' = x'\cdot x = 1.$$

Aleshores direm que x és invertible o que x és un element invertible de R.

Definició 6.1.1.8 (L'invers d'un element)**.** Siguin $(R,+,\cdot)$ un anell i x un element invertible de R. Aleshores denotarem per x^{-1} l'element de R tal que

$$x\cdot x^{-1} = x^{-1}\cdot x = 1.$$

Direm que x^{-1} és l'invers de x.

Observem que aquesta definició té sentit per la proposició 6.1.1.6.

Definició 6.1.1.9 (Subanell)**.** Siguin $(R,+,\cdot)$ un anell i $S\subseteq R$ un subconjunt amb $1\in S$ tal que per a tot $a,b\in S$ tenim $a\cdot b, a+b\in S$ i $(S,+,\cdot)$ és un anell. Aleshores direm que $(S,+,\cdot)$ és un subanell de $(R,+,\cdot)$

Ho denotarem amb $(S,+,\cdot)\subseteq(R,+,\cdot)$.

6.1.2 Ideals i ideals principals

Definició 6.1.2.1 (Ideal)**.** Siguin $(R,+,\cdot)$ un anell commutatiu amb $1 \neq 0$ i I un subconjunt no buit de R tal que $(I,+)$ sigui un subgrup de $(R,+)$ i tal que per a tot $x \in I$, $r \in R$ tenim $r \cdot x \in I$. Aleshores direm que I és un ideal de $(R,+,\cdot)$.

Observació 6.1.2.2. $0 \in I$.

Notació 6.1.2.3. Si I és un ideal d'un anell $(R,+,\cdot)$ denotarem $I \triangleleft (R,+,\cdot)$.

Proposició 6.1.2.4. *Siguin $(R,+,\cdot)$ un anell commutatiu amb $1 \neq 0$ i I un subconjunt no buit de R. Aleshores tenim que I és un ideal de $(R,+,\cdot)$ si i només si*

1. *Per a tot $x,y \in I$ tenim $x-y \in I$.*
2. *Per a tot $r \in R$, $x \in I$ tenim $r \cdot x \in I$.*

Demostració. Veiem que la condició és suficient ($\Rightarrow$). Suposem que I és un ideal de $(R,+,\cdot)$. Hem de veure que per a tot $x,y \in I$, $r \in R$ tenim $x-y \in I$ i $r \cdot x \in I$. Per la definició de grup (5.1.1.1) tenim que $x-y \in I$, ja que, per la definició d'ideal d'un anell (6.1.2.1) $(I,+)$ és un grup. També trobem $r \cdot x \in I$ per la definició d'ideal d'un anell (6.1.2.1).

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem que per a tot $x,y \in I$, $r \in R$ tenim $x-y \in I$ i $r \cdot x \in I$. Per la proposició 5.1.2.3 tenim que $(I,+)$ és un subgrup de $(R,+)$, i per la definició d'ideal d'un anell (6.1.2.1) tenim que I és un ideal de $(R,+,\cdot)$. □

Notació 6.1.2.5. Si (a) és un ideal principal d'un anell $(R,+,\cdot)$ denotarem $(a) \trianglelefteq (R,+,\cdot)$.

Proposició 6.1.2.6. *Siguin I,J dos ideals d'un anell $(R,+,\cdot)$. Aleshores els conjunts*

1. *$I+J = \{x+y : x \in I, y \in J\}$.*
2. *$I \cap J$.*
3. *$IJ = \{x_1 \cdot y_1 + \ldots x_n \cdot y_n : x_1,\ldots,x_n \in I, y_1,\ldots,y_n \in J, n \in \mathbb{N}\}$.*

són ideals de $(R,+,\cdot)$.

Demostració. Comencem demostrant el punt (1). Per la proposició 6.1.2.4 només ens cal veure que per a tot $a,b \in I+J$, $r \in R$ tenim $a-b \in I+J$ i $r \cdot a \in I+J$. Prenem doncs $a,b \in I+J$. Aleshores tenim $a = a_1+a_2$ i $b = b_1+b_2$ per a certs $a_1,b_1 \in I$ i $a_2,b_2 \in J$. Volem veure que $a-b \in I+J$. Això és

$$\begin{aligned} a_1+a_2-(b_1+b_2) &= a_1+a_2-b_1-b_2 && (6.1.1.5)\\ &= (a_1-b_1)+(a_2-b_2) && (\text{grup abelià } (5.1.3.1)) \end{aligned}$$

i com que, per hipòtesi, I,J són ideals de $(R,+,\cdot)$ per la proposició 6.1.2.4 tenim que $a_1-b_1 \in I$ i $a_2-b_2 \in J$, i per tant $a-b = (a_1-b_1)+(a_2-b_2) \in I+J$.

Veiem ara que per a tot $r \in R$ es satisfà $r \cdot a \in I + J$. Tenim

$$\begin{aligned} r \cdot a &= r \cdot (a_1 + a_2) && \text{(anell (6.1.1.1))} \\ &= r \cdot a_1 + r \cdot a_2 && \text{(anell (6.1.1.1))} \end{aligned}$$

i per la proposició 6.1.2.4 tenim que $r \cdot a_1 \in I$ i $r \cdot a_2 \in J$, i per tant $r \cdot a = r \cdot a_1 + r \cdot a_2 \in I + J$. Aleshores per la proposició 6.1.2.4 tenim que $I + J$ és un ideal de $(R, +, \cdot)$.

Veiem ara el punt (2). Per la proposició 6.1.2.4 només ens cal veure que per a tot $a, b \in I \cap J$, $r \in R$ tenim $a - b \in I \cap J$ i $r \cdot a \in I \cap J$. Prenem doncs $a, b \in I \cap J$, i per tant $a, b \in I$ i $a, b \in J$, i per la proposició 6.1.2.4 tenim que $a - b \in I$ i $a - b \in J$, i tenim que $a - b \in I \cap J$.

Per veure que $r \cdot a \in I \cap J$ per a tot $r \in R$ tenim per la definició d'ideal d'un anell (6.1.2.1) que $r \cdot a \in I$ i $r \cdot a \in J$, i per tant $r \cdot a \in I \cap J$ i per la proposició 6.1.2.4 $I \cap J$ és un ideal de $(R, +, \cdot)$.

Acabem veient el punt (3). Per la proposició 6.1.2.4 només ens cal veure que per a tot $a, b \in IJ$, $r \in R$ tenim $a - b \in IJ$ i $r \cdot a \in IJ$. Prenem doncs $a, b \in IJ$, i tenim que $a = x_1 \cdot y_1 + \cdots + x_n \cdot y_n$, $b = x'_1 \cdot y'_1 + \cdots + x'_m \cdot y'_m$ per a certs $x_1, \ldots, x_n, x'_1, \ldots, x'_m \in I$, $y_1, \ldots, y_n, y'_1, \ldots, y'_m \in J$. Per veure que $a - b \in IJ$ fem, per la proposició 6.1.1.5,

$$\begin{aligned} a - b = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - (x'_1 \cdot y'_1 + \cdots + x'_m \cdot y'_m) = \\ = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - x'_1 \cdot y'_1 - \cdots - x'_m \cdot y'_m \end{aligned}$$

i com que I és, per hipòtesi, un anell, per les proposicions 6.1.1.5 i 6.1.2.4 tenim que $-x'_1, \ldots, -x'_m \in I$ i $a - b = x_1 \cdot y_1 + \cdots + x_n \cdot y_n - x'_1 \cdot y'_1 - \cdots - x'_m \cdot y'_m \in IJ$.

Veiem ara que per a tot $r \in R$ es satisfà $r \cdot a \in I$. Això és

$$\begin{aligned} r \cdot a &= r \cdot (x_1 \cdot y_1 + \cdots + x_n \cdot y_n) \\ &= r \cdot x_1 \cdot y_1 + \cdots + r \cdot x_n \cdot y_n && (6.1.1.5) \end{aligned}$$

i com que I és, per hipòtesi, un anell, per les proposicions 6.1.1.5 i 6.1.2.4 tenim que $r \cdot x_1, \ldots, r \cdot x_n \in I$, i per tant $r \cdot a = r \cdot x_1 \cdot y_1 + \cdots + r \cdot x_n \cdot y_n \in IJ$ i per la proposició 6.1.2.4 tenim que IJ és un ideal de $(R, +, \cdot)$. □

Definició 6.1.2.7 (Ideal principal)**.** Sigui I un ideal de $(R, +, \cdot)$ tal que $I = \{a\}R = R\{a\} = \{r \cdot a : r \in R\}$ per a cert $a \in I$. Aleshores direm que I és un anell principal de $(R, +, \cdot)$. Ho denotarem amb $I = (a)$.

6.1.3 Cossos i l'anell quocient

Definició 6.1.3.1 (Cos)**.** Sigui $(R, +, \cdot)$ un anell commutatiu amb $1 \neq 0$ tal que $(R \setminus \{0\}, \cdot)$ sigui un grup abelià. Aleshores direm que $(R, +, \cdot)$ és un cos.

Proposició 6.1.3.2. *Sigui $(R, +, \cdot)$ un anell commutatiu amb $1 \neq 0$. Aleshores $(R, +, \cdot)$ és un cos si i només si els únics ideals de $(R, +, \cdot)$ són (0) i R.*

Demostració. Comencem comprovant que la condició és suficient ($\Rightarrow$). Suposem doncs que $(R, +, \cdot)$ és un cos i que I és un ideal de $(R, +, \cdot)$ amb $I \neq (0)$, i per tant existeix $a \in R$, $a \neq 0$ tal que $a \in I$. Com que, per hipòtesi, $(R \setminus \{0\}, \cdot)$ és un grup i $a \neq 0$ per la definició de l'invers d'un element d'un grup (5.1.1.7)

existeix $a^{-1} \in R$ tal que $a \cdot a^{-1} = 1$, i per la definició d'ideal d'un anell (6.1.2.1) trobem que $1 \in I$, i per tant per la proposició 6.1.2.4 tenim que per a tot $x \in R$ tenim $x \cdot 1 = x \in I$, i per tant $I = R$.

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem que els únics ideals de R són (0) i R. Prenem un element $a \in R$, $a \neq 0$ i considerem l'ideal principal (a), que per hipòtesi ha de ser $(a) = (1) = R$, i per la definició d'ideal principal (6.1.2.7) tenim que existeix $a' \in (1)$ tal que $a \cdot a' = 1$, i per tant, per la definició de grup (5.1.1.1) tenim que $(R \setminus \{0\}, \cdot)$ és un grup i per la definició de cos (6.1.3.1) tenim que $(R, +, \cdot)$ és un cos. □

Proposició 6.1.3.3. *Sigui I un ideal principal d'un anell $(R, +, \cdot)$. Aleshores la relació*

$$x \sim y \iff x - y \in I \quad \textit{per a tot } x, y \in R$$

és una relació d'equivalència.

Demostració. Comprovem que $\sim$ satisfà la definició de relació d'equivalència (1.3.0.2):

1. Reflexiva: Prenem $x \in R$. Per l'observació 6.1.2.2 tenim que $0 \in I$, i per tant $x - x = 0 \in I$ i veiem que $x \sim x$.

2. Simètrica: Siguin $x_1, x_2 \in I$ tals que $x_1 \sim x_2$. Això és que $x_1 - x_2 \in I$, és a dir, si $I = (a)$ tenim $x_1 - x_2 = r \cdot a$ per a cert $r \in R$. Ara bé, també tenim que $x_2 - x_1 = -r \cdot a$, i com que per la definició d'anell (6.1.1.1) tenim que $-r \in R$, tenim, per la definició d'ideal principal (6.1.2.7), $-r \cdot a \in I$ i per tant $x_2 \sim x_1$.

3. Transitiva: Siguin $x_1, x_2, x_3 \in R$ tals que $x_1 \sim x_2$ i $x_2 \sim x_3$. Això és que, si $I = (a)$, existeixen $r_1, r_2 \in R$ tals que

   $$x_1 - x_2 = r_1 \cdot a \quad \text{i} \quad x_2 - x_3 = r_2 \cdot a,$$

   i per tant

   $$\begin{aligned} x_1 - x_3 &= x_1 - x_2 + x_2 - x_3 \\ &= r_1 \cdot a + r_2 \cdot a \\ &= (r_1 + r_2) \cdot a. \end{aligned} \tag{6.1.1.5}$$

   Ara bé, per la definició d'anell (6.1.1.1) tenim que $r_1 + r_2 \in R$, i per tant, per la definició d'ideal principal (6.1.2.7), trobem $(r_1 + r_2) \cdot a \in I$ i tenim que $x_1 \sim x_3$.

Per tant $\sim$ és una relació d'equivalència. □

Proposició 6.1.3.4. *Sigui I un ideal principal d'un anell $(R, +, \cdot)$. Aleshores $(R/I, +, \cdot)$ amb el producte $[x] \cdot [y] = [x \cdot y]$ és un anell.*

Demostració. Observem que aquest enunciat té sentit per la proposició 6.1.3.3.

Per la proposició 5.1.4.1 tenim que $(R/I, +)$ és un grup, i com que

$$\begin{aligned} [x] + [y] &= [x + y] \\ &= [y + x] && \text{(grup abelià (5.1.3.1))} \\ &= [y] + [x] \end{aligned}$$

tenim que $(R/I, +)$ és un grup abelià. Veiem ara que per a tot $x, y, z \in R/I$ tenim $[x] \cdot ([y] \cdot [z]) = ([x] \cdot [y]) \cdot [z]$ i $[x] \cdot ([y] + [z]) = [x] \cdot [y] + [x] \cdot [z]$. Tenim

$$\begin{aligned}[x] \cdot ([y] \cdot [z]) &= [x] \cdot [y \cdot z] \\ &= [x \cdot (y \cdot z)] \\ &= [(x \cdot y) \cdot z] \\ &= [x \cdot y] \cdot [z] = ([x] \cdot [y]) \cdot [z]\end{aligned}$$

i

$$\begin{aligned}[x] \cdot ([y] + [z]) &= [x] \cdot [y + z] \\ &= [x \cdot (y + z)] \\ &= [x \cdot y + x \cdot z] = [x] \cdot [y] + [x] \cdot [z]\end{aligned}$$

i per la definició d'anell (6.1.1.1) tenim que $(R/I, +, \cdot)$ és un anell. □

Definició 6.1.3.5 (Anell quocient)**.** Siguin $(R, +, \cdot)$ un anell commutatiu amb $1 \neq 0$ i I un ideal principal de $(R, +, \cdot)$. Aleshores direm que $(R/I, +, \cdot)$ és un anell quocient.

Observem que aquesta definició té sentit per la proposició 6.1.3.4.

6.2 Tres Teoremes d'isomorfisme entre anells

6.2.1 Morfismes entre anells

Definició 6.2.1.1 (Morfisme entre anells)**.** Siguin $(R, +, \cdot)$, $(S, \oplus, *)$ dos anells commutatius amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f : R \longrightarrow S$ una aplicació tal que

1. $f(x + y) = f(x) \oplus f(y)$ per a tot $x, y \in R$.
2. $f(x \cdot y) = f(x) * f(y)$ per a tot $x, y \in R$.
3. $f(1_R) = 1_S$.

Aleshores diem que f és un morfisme entre anells. Definim també

1. Si f és injectiva direm que f és un monomorfisme entre anells.
2. Si f és exhaustiva direm que f és un epimorfisme entre anells.
3. Si f és bijectiva direm que f és un isomorfisme entre anells. També escriurem $(R, +, \cdot) \cong (S, \oplus, *)$.
4. Si $R = S$ direm que f és un endomorfisme entre anells.
5. Si $R = S$ i f és bijectiva direm que f és un automorfisme entre anells.

Proposició 6.2.1.2. *Siguin $(R, +, \cdot)$, $(S, \oplus, *)$ dos anells commutatius amb $1_R \neq 0_R$ i $1_S \neq 0_S$ i $f : R \longrightarrow S$ un morfisme entre anells. Aleshores*

1. *$f(0_R) = 0_S$.*
2. *$f(-x) = -f(x)$ per a tot $x \in R$.*

Demostració. Per la definició de morfisme entre grups (5.2.1.1) tenim que f és un morfisme entre els grups $(R,+)$ i $(S,\oplus)$, i per la proposició 5.2.1.2 tenim que $f(0_R)=0_S$ i $f(-x)=-f(x)$ per a tot $x\in R$. □

Definició 6.2.1.3 (Nucli i imatge d'un morfisme entre anells)**.** Siguin $(R,+,\cdot)$, $(S,\oplus,*)$ dos anells commutatius amb $1_R\neq 0_R$ i $1_S\neq 0_S$ i $f:R\longrightarrow S$ un morfisme entre anells. Aleshores definim

$$\ker(f)=\{x\in R: f(x)=0_S\}$$

com el nucli de f, i

$$\mathrm{Im}(f)=\{y\in S: f(x)=y \text{ per a cert } x\in R\}$$

com la imatge de f.

Observació 6.2.1.4. $\ker(f)\subseteq R$, $\mathrm{Im}(f)\subseteq S$.

Proposició 6.2.1.5. *Siguin $(R,+,\cdot)$, $(S,\oplus,*)$ dos anells commutatius amb $1_R\neq 0_R$ i $1_S\neq 0_S$ i $f:R\longrightarrow S$ un morfisme entre anells. Aleshores*

1. $\ker(f)\triangleleft(R,+,\cdot)$.
2. $(\mathrm{Im}(f),\oplus,*)\subseteq(S,\oplus,*)$.

Demostració. Observem que aquest enunciat té sentit per l'observació 6.2.1.5

Comencem veient el punt (1). Com que, per la proposició 6.2.1.2, tenim que $f(0_R)=0_S$ veiem, per la definició de nucli d'un morfisme entre anells (6.2.1.3), que $\ker(f)\neq\emptyset$. Prenem doncs $a\in\ker(f)$. Observem que, per la definició de morfisme entre anells (6.2.1.1), tenim que $f(r\cdot a)=f(r)*f(a)$ per a tot $r\in R$, i per tant, com que per la definició de nucli d'un morfisme entre anells (6.2.1.3) es compleix $f(a)=0_S$ tenim que

$$f(r\cdot a)=f(r)*f(a)=f(r)*0_S=0_S$$

i per tant $r\cdot a\in\ker(f)$ per a tot $r\in R$, $a\in\ker(f)$. Ara bé per la definició de ideal d'un anell (6.1.2.1) tenim que $\ker(f)$ és un ideal de $(R,+,\cdot)$.

Veiem ara el punt (2). Veiem que per a tot $x,y\in\mathrm{Im}(f)$ tenim $x*y\in\mathrm{Im}(f)$. Per la definició d'imatge d'un morfisme entre anells (6.2.1.3) tenim que existeixen $a,b\in R$ tals que $f(a)=x$ i $f(b)=y$. Ara bé, per la definició d'anell (6.1.1.1) tenim que $a\cdot b=c\in R$, i per tant per la definició d'imatge d'un morfisme entre anells (6.2.1.3) tenim que $f(c)=x*y\in\mathrm{Im}(f)$. Veiem ara que $(\mathrm{Im}(f),\oplus,*)$ és un anell. Com que, per la definició de morfisme entre grups (5.2.1.1) tenim que f és un morfisme entre grups per la proposició 5.2.1.7 tenim que $\mathrm{Im}(f),\oplus)$ és un subgrup de $(S,\oplus)$; i per la definició d'anell (6.1.1.1) tenim que per a tot $x,y,z\in R$ es satisfà

$$x\cdot(y\cdot z)=(x\cdot y)\cdot z \quad \text{i} \quad x\cdot(y+z)=x\cdot y+x\cdot z,$$

i per la definició de subanell (6.1.1.9) tenim que $(\mathrm{Im}(f),\oplus,*)$ és un subanell de $(S,\oplus,*)$, com volíem veure. □

Proposició 6.2.1.6. *Siguin $(R,+,\cdot)$, $(S,\oplus,*)$ dos anells commutatius amb $1_R\neq 0_R$ i $1_S\neq 0_S$, I un ideal de $(R,+,\cdot)$, J un ideal de $(S,\oplus,*)$ i $f:R\longrightarrow S$ un morfisme entre anells. Aleshores*

1. $\{x \in R : f(x) \in J\}$ *és un ideal de* $(R, +, \cdot)$.

2. *Si* f *és exhaustiva,* $\{f(x) \in S : x \in J\}$ *és un ideal de* $(S, \oplus, *)$.

Demostració. Comencem veient el punt (1). Volem veure que per a tot $x \in R$, $r \in \{x \in R : f(x) \in J\}$ tenim $x \cdot r \in \{x \in R : f(x) \in J\}$. □

Proposició 6.2.1.7. *Siguin* $(R, +, \cdot)$, $(S, \oplus, *)$ *dos anells commutatius amb* $1_R \neq 0_R$ *i* $1_S \neq 0_S$, $(R', +, \cdot)$ *un subanell de* $(R, +, \cdot)$, $(S', \oplus, *)$ *un subanell de* $(S, \oplus, *)$ *i* $f : R \longrightarrow S$ *un morfisme entre anells. Aleshores*

1. $(\{f(x) \in S : x \in R\}, \oplus, *)$ *és un subanell de* $(S, \oplus, *)$.

2. $(\{x \in R : f(x) \in S\}, +, \cdot)$ *és un subanell de* $(R, +, \cdot)$.

Demostració. □

6.2.2 Teoremes d'isomorfisme entre anells

6.2.3 Característica d'un anell

Definició 6.2.3.1 (Característica)**.** Sigui $(R, +, \cdot)$ un anell. Direm que $(R, +, \cdot)$ té característica $n > 0$ si $n = \min_{n \in \mathbb{N}}\{n \cdot 1 = 0\}$. Ho denotarem amb $\mathrm{ch}(R) = n$. Si aquest n no existeix diem que R té característica 0 i $\mathrm{ch}(R) = 0$.

Proposició 6.2.3.2. *Siguin* $(R, +, \cdot)$ *un anell i*

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n \cdot 1 = 1 + \overset{n)}{\dots} + 1 \end{aligned}$$

una aplicació. Aleshores f *és un morfisme entre anells i* $\ker(f) = (\mathrm{ch}(R))$.

Demostració. Observem que aquest enunciat té sentit per la proposició 6.2.1.5.

Comencem veient que f és un morfisme entre anells. Veiem que f és un morfisme entre els grup. Tenim que per a tot $n, m \in \mathbb{Z}$

$$\begin{aligned} f(n+m) &= 1 + \overset{n+m)}{\dots} + 1 \\ &= (1 + \overset{n)}{\dots} + 1) + (1 + \overset{m)}{\dots} + 1) \\ &= f(n) + f(m) \end{aligned}$$

i per la definició de morfisme entre grups (5.2.1.1) tenim que f és un morfisme entre grups. Veiem ara que $f(1) = 1_R$. Tenim que $f(1) = 1 \cdot 1 = 1$ i per tant per la definició de morfisme entre anells (6.2.1.1) tenim que f és un morfisme entre anells.

Veiem ara que $\ker(f) = (\mathrm{ch}(n))$. Per la definició de nucli d'un morfisme entre anells (6.2.1.3) tenim que $\ker(f) = \{x \in \mathbb{N} : f(n) = 0_R\}$. Per tant

$$\ker(f) = \{n \in \mathbb{N} : n \cdot 1 = 0_R\}$$

i per la definició de característica d'un anell (6.2.3.1) tenim que $n = \mathrm{ch}(R)$, i per tant $\ker(f) = \{k \cdot n : k \in \mathbb{N}\}$. Ara bé, per la definició de ideal d'un anell (6.1.2.1) tenim que $\ker(f) = (n)$, com volíem veure. □

Corol·lari 6.2.3.3. *Si* $\mathrm{ch}(R) = 0$ *aleshores existeix un subanell* $(S, +, \cdot)$ *de* $(R, +, \cdot)$ *tal que* $S \cong \mathbb{Z}$.

Si $\mathrm{ch}(R) = n$ *aleshores existeix un subanell* $(S, +, \cdot)$ *de* $(R, +, \cdot)$ *tal que* $S \cong \mathbb{Z}/(n)$.

6.3 Dominis

6.3.1 Dominis d'integritat, ideals primers i maximals

Definició 6.3.1.1 (Divisor de 0)**.** Siguin $(R,+,\cdot)$ un anell commutatiu amb $1 \neq 0$ i $a, b \neq 0$ dos elements de R tals que $a \cdot b = 0$. Aleshores diem que a és un divisor de 0 en l'anell $(R,+,\cdot)$.

Definició 6.3.1.2 (Dominis d'integritat)**.** Sigui $(D,+,\cdot)$ un anell commutatiu amb $1 \neq 0$. Diem que $(D,+,\cdot)$ és un domini d'integritat si no existeix cap $a \in D$ tal que a sigui un divisor de 0 en $(D,+,\cdot)$.

Proposició 6.3.1.3. *Siguin $(D,+,\cdot)$ un domini d'integritat i $a \neq 0$ un element de D. Aleshores*

$$a \cdot x = a \cdot y \Longrightarrow x = y.$$

Demostració. Tenim

$$a \cdot x - a \cdot y = 0$$

i per la proposició 6.1.1.5 tenim que

$$(x - y) \cdot a = 0.$$

Ara bé, com que, per hipòtesi, $(D,+,\cdot)$ és un domini d'integritat i $a \neq 0$ tenim que ha de ser $x - y = 0$, i per tant trobem $x = y$. □

Definició 6.3.1.4 (Ideal primer)**.** Sigui I un ideal d'un anell $(R,+,\cdot)$ amb $I \neq R$ tal que si $a \cdot b \in I$ tenim $a \in I$ o $b \in I$. Aleshores direm que I és un ideal primer de $(R,+,\cdot)$.

Proposició 6.3.1.5. *Sigui I un ideal d'un anell $(R,+,\cdot)$ amb $I \neq R$. Aleshores*

$$(R/I,+,\cdot) \text{ és un domini d'integritat} \Longleftrightarrow I \text{ és un ideal primer de } (R,+,\cdot).$$

Demostració. Comencem demostrant que la condició és suficient ($\Rightarrow$). Suposem doncs que $(R/I,+,\cdot)$ és un domini d'integritat i prenem $[a],[b] \in R/I$ tals que $[a] \cdot [b] = [0]$. Aleshores per la definició de anell quocient (6.1.3.5) tenim que $a \cdot b \in I$. Ara bé, com que per hipòtesi $(R/I,+,\cdot)$ és un domini d'integritat tenim que ha de ser $[a] = [0]$ ó $[b] = [0]$, i per tant trobem que ha de ser $a \in I$ o $b \in I$, i per la definició d'ideal primer (6.3.1.4) trobem que I és un ideal primer de $(R,+,\cdot)$.

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem doncs que I és un ideal primer de $(R,+,\cdot)$. Per la proposició 6.1.3.4 tenim que $(R/I,+,\cdot)$ és un anell commutatiu amb $1 \neq 0$. Prenem doncs $a \in R$, $a \notin I$ i suposem que existeix $b \in R$ tal que $[a] \cdot [b] = [0]$. Això és que $a \cdot b \in I$, i com que per hipòtesi I és un ideal primer, per la definició d'ideal primer (6.3.1.4) trobem que ha de ser $b \in I$, i per tant $[b] = [0]$ i per la definició de domini d'integritat (6.3.1.2) tenim que $(R/I,+,\cdot)$ és un domini d'integritat. □

Corol·lari 6.3.1.6. *$(R,+,\cdot)$ és un domini d'integritat si i només si (0) és un ideal primer.*

Definició 6.3.1.7 (Ideal maximal)**.** Sigui M un ideal d'un anell $(R,+,\cdot)$ amb $M \neq R$ tal que per a tot ideal I de $(R,+,\cdot)$ amb $M \subseteq I \subseteq R$ ha de ser $I = M$ o $I = R$. Aleshores direm que M és un ideal maximal de $(R,+,\cdot)$.

Proposició 6.3.1.8. *Sigui M un ideal d'un anell $(R,+,\cdot)$ amb $I \neq R$. Aleshores*

$$(R/M,+,\cdot) \text{ és un cos} \iff M \text{ és un ideal maximal de } (R,+,\cdot).$$

Demostració. Observem que aquest enunciat té sentit per la proposició 6.1.3.4.

Comencem veient la implicació cap a la dreta ($\Rightarrow$). Suposem doncs que $(R/M,+,\cdot)$ és un cos i prenem un ideal I/M de $(R/M,+,\cdot)$. Aleshores ha de ser $M \subseteq I \subseteq R$. Per la proposició 6.1.3.2 tenim que els únics ideals de $(R/M,+,\cdot)$ són $([0])$ i R/M, i per tant ha de ser $I = M$ o $I = R$, i per la definició d'ideal maximal (6.3.1.7) tenim que M és un ideal maximal de $(R,+,\cdot)$.

Veiem ara la implicació cap a l'esquerra ($\Leftarrow$). Suposem doncs que M és un ideal maximal de l'anell $(R,+,\cdot)$ i considerem, per la proposició 6.1.3.4, l'anell $(R/M,+,\cdot)$. Per la proposició 6.1.3.2 tenim que només hem de veure que els únics ideals de $(R/M,+,\cdot)$ són (0) i R. Prenem un ideal I/M de $(R/M,+,\cdot)$. Aquest ha de ser tal que $M \subseteq I \subseteq R$, i per la definició d'ideal maximal (6.3.1.7) tenim que ha de ser $I = M$ o $I = R$, i per tant I/M ha de ser $([0])$ o R/M i per la proposició 6.1.3.4 tenim que $(R/M,+,\cdot)$ és un cos. □

Corol·lari 6.3.1.9. *M és maximal $\Longrightarrow$ M és primer.*

Proposició 6.3.1.10. *Sigui $I \neq (0)$ un ideal primer d'un domini d'integritat $(D,+,\cdot)$. Aleshores I és maximal.*

Demostració. Posem $I = (a)$. Per hipòtesi tenim que $a \neq 0$ i que I és un ideal primer. Sigui $b \in D$ tal que $(a) \subseteq (b)$. Aleshores tenim que $a \in (b)$, i per la definició d'ideal principal (6.1.2.7) tenim que $a = a' \cdot b$ per a cert $a' \in D$. Aleshores, per la definició d'ideal primer (6.3.1.4), tenim que $a' \in (a)$ o $b \in (a)$.

Suposem que $a' \in (a)$. Aleshores tenim que $a' = a \cdot \beta$ per a cert $\beta \in D$, i per tant $a = a \cdot \beta \cdot b$, i per la proposició 6.3.1.3 tenim que $1 = \beta \cdot b$, i per tant $1 \in (b)$, d'on trobem $(b) = R$. Suposem ara que $b \in I$. Aleshores $(a) = (b)$, i per la definició de ideal maximal (6.3.1.7) tenim que $I = (a)$ és un ideal maximal de $(D,+,\cdot)$. □

6.3.2 Lemma de Zorn

Definició 6.3.2.1 (Relació d'ordre)**.** Sigui A un conjunt no buit i $\leq$ una relació binària en A que satisfaci

1. Reflexiva: $a \leq a$ per a tot $a \in A$.
2. Antisimètrica: $a \leq b$ i $b \leq a$ impliquen $a = b$ per a tot $a, b \in A$.
3. Transitiva: Si $a \leq b$ i $b \leq c$, aleshores $a \leq c$ per a tot $a, b, c \in A$.

Definició 6.3.2.2 (Cadena)**.** Siguin $\mathcal{C}$ un conjunt i $\leq$ una relació d'ordre en A tal que per a tot $a, b \in A$ es satisfà $a \leq b$ ó $b \leq a$. Aleshores direm que $(\mathcal{C}, \leq)$ és una cadena.

Proposició 6.3.2.3. *Siguin Y i $\mathcal{X} \subseteq \mathcal{P}(Y)$ dos conjunts tals que per a tot $A, B \in X$ tenim $A \subseteq B$ o $B \subseteq A$. Aleshores $(\mathcal{X}, \subseteq)$ és una cadena.*

Demostració. Comprovem que $\subseteq$ satisfà les condicions de la definició de relació d'ordre (6.3.2.1):

1. Reflexiva: Si $A \in \mathcal{X}$ tenim $A = A$, i en particular $A \subseteq A$.
2. Antisimètrica: Si $A, B \in \mathcal{X}$ tals que $A \subseteq B$ i $B \subseteq A$ tenim, per doble inclusió, que $A = B$.
3. Transitiva: Si $A, B, C \in \mathcal{X}$ tals que $A \subseteq B$ i $B \subseteq C$ aleshores $A \subseteq C$.

per tant, per les definicions de relació d'ordre (6.3.2.1) i cadena (6.3.2.2) tenim que $(\mathcal{X}, \subseteq)$ és una cadena. □

Definició 6.3.2.4 (Cota superior d'una cadena)**.** Siguin $(\mathcal{C}, \leq)$ una cadena, a un element de $\mathcal{C}$ i B un subconjunt de $\mathcal{C}$ tal que per a tot $b \in B$ es compleix $b \leq A$. Aleshores direm que a és una cota superior de B.

Si $a \leq b$ implica $b = a$ per a tot $b \in B$ direm que a és maximal per B.

Axioma 6.3.2.5 (Lemma de Zorn)**.** *Sigui $(\mathcal{A}, \leq)$ una cadena tal que per a tot subconjunt $\mathcal{C} \subseteq \mathcal{A}$ la cadena $(\mathcal{C}, \leq)$ té alguna cota superior. Aleshores $(\mathcal{A}, \leq)$ té algun element maximal.*

Teorema 6.3.2.6. *Sigui $(R, +, \cdot)$ un anell commutatiu amb $1 \neq 0$. Aleshores existeix $M \subseteq R$ tal que M sigui un ideal maximal de $(R, +, \cdot)$.*

Demostració. Definim el conjunt

$$A = \{I \lhd R : I \neq R\}.$$

i amb un subconjunt $\mathcal{C} \subseteq A$ considerem, per la proposició 6.3.2.3, la cadena $(\mathcal{C}, \subseteq)$. Considerem ara el conjunt

$$J = \bigcup_{I \in \mathcal{C}} I$$

i veiem que J és un ideal de R, ja que si $x, y \in J$ tenim $x \in J_1$ i $y \in J_2$ per a certs $J_1, J_2 \in \mathcal{C}$. Ara bé, si $J_2 \subseteq J_1$ tenim que $x - y \in J_1$, i per tant $x - y \in J$, i si $J_1 \subseteq J_2$ tenim que $x - y \in J_2$, i per tant $x - y \in J$. Si prenem $x \in J$ i $r \in R$ aleshores $r \cdot x \in J$, ja que tenim $x \in J_1$ per a cert $J_1 \in \mathcal{C}$, i per tant $r \cdot x \in J_1$, i en particular $r \cdot x \in J$. Per tant per la definició d'ideal d'un anell (6.1.2.1) tenim que J és un ideal de R. Per veure que $J \in A$ hem de comprovar que $J \neq R$. Ho fem per contradicció. Suposem que $J = R$. Aleshores $1 \in J$, i per tant $1 \in I$ per a cert $I \in A$, però això no pot ser ja que si $I \in A$ s'ha de complir $I \neq A$, i per tant $1 \notin I$. Per tant $J \neq R$ i tenim que $J \in A$.

Ara bé, pel Lemma de Zorn (6.3.2.5) tenim que existeix $M \in \mathcal{C}$ tal que per a tot $I \in \mathcal{C}$ tenim $I \subseteq M$ i per la definició d'ideal maximal (6.3.1.7) tenim que M és un ideal maximal de $(R, +, \cdot)$. □

6.3.3 Divisibilitat

Definició 6.3.3.1 (Divisors i múltiples)**.** Siguin $(D, +, \cdot)$ un domini d'integritat i $a, b \in D$ tals que existeix $c \in D$ tal que $b = a \cdot c$. Aleshores direm que a divideix b o que b és múltiple de a. Ho denotarem amb $a|b$.

Observació 6.3.3.2. $b|a \Leftrightarrow (a) \subseteq (b)$.

Proposició 6.3.3.3. *Siguin $(D,+,\cdot)$ un domini d'integritat i a,b,c,c' quatre elements, amb $a\neq 0$, $b\neq 0$, tals que $a|b$ i $b|a$, i $a=c\cdot b$ i $b=c'\cdot a$. Aleshores $c'=c^{-1}$.*

Demostració. Tenim que $b=c'\cdot c\cdot b$, i per la proposició 6.3.1.3 tenim que $1=c'\cdot c$, i per la definició d'element invertible (6.1.1.7) tenim que $c'=c^{-1}$. □

Proposició 6.3.3.4. *Sigui $(R,+,\cdot)$ un anell commutatiu amb $1\neq 0$ i $\sim$ una relació binària tal que per a tot $x,y\in R$ tenim*

$$x\sim y \Longrightarrow x=u\cdot y \text{ per a algun } u\in R \text{ invertible.}$$

Aleshores $\sim$ és una relació d'equivalència.

Demostració. Comprovem les condicions de la definició de relació d'equivalència (1.3.0.2):

1. Simètrica: Per a tot $x\in R$ tenim $x=1\cdot x$.
2. Reflexiva: Siguin $x,y\in R$ tals que $x\sim y$. Aleshores tenim que existeix $u\in R$ invertible tal que $x=u\cdot y$. Ara bé, com que u és invertible tenim per la definició de element invertible (6.1.1.7) que $y=u^{-1}\cdot x$, i per tant $y\sim x$.
3. Transitiva: Siguin $x,y,z\in R$ tals que $x\sim y$ i $y\sim z$. Aleshores tenim que $x=u\cdot y$ i $y=u'\cdot z$ per a certs $u,u'\in R$ invertibles, i per tant $x=u\cdot u'\cdot z$, i com que $1=u\cdot u'\cdot u'^{-1}\cdot u^{-1}$ per la definició de element invertible (6.1.1.7) tenim que $x\sim z$.

i per la definició de relació d'equivalència (1.3.0.2) tenim que $\sim$ és una relació d'equivalència. □

Definició 6.3.3.5 (Elements associats)**.** Siguin $(R,+,\cdot)$ un anell commutatiu amb $1\neq 0$ i $a,b\in R$ dos elements tals que existeix un element invertible $u\in R$ tal que $a=u\cdot b$. Aleshores direm que a i b són associats i escriurem $a\sim b$.

Observem que aquesta definició té sentit per la proposició 6.3.3.4.

Proposició 6.3.3.6. *Siguin $(D,+,\cdot)$ un domini d'integritat, a,b dos elements de D i $X\subseteq D$ un conjunt tal que per a tot $d\in X$ tenim $d|a$, $d|b$ i per a tot $c\in D$ tal que $c|a$, $c|b$ es compleix $c|d$. Aleshores tenim que per a tot $d'\in X$ si i només si $d\sim d'$.*

Demostració. Comencem amb la implicació cap a la dreta ($\Rightarrow$). Suposem que $d'\in X$. Hem de veure que $d\sim d'$. Tenim $d|d'$ i $d'|d$ i per la definició de divisor (6.3.3.1) trobem que $d\sim d'$.

Fem ara la implicació cap a l'esquerra ($\Leftarrow$). Suposem que $d'\sim d$. Hem de veure que $d'\in X$. Per hipòtesi tenim que $d|a$ i $d|b$. Per tant existeixen $\alpha,\beta\in D$ tals que $a=\alpha d$ i $b=\beta d$, i per la proposició 6.3.3.3 tenim que si $d'=d\cdot u$ amb $u\in D$ invertible aleshores $d=d'\cdot u^{-1}$. Per tant

$$a=\alpha\cdot d'\cdot u^{-1} \quad \text{i} \quad b=\beta\cdot d'\cdot u^{-1}$$

i per tant $d'|a$ i $d'|b$. Ara bé, com que per hipòtesi $d\sim d'$, per la definició d'elements associats (6.3.3.5) tenim que $d'\in X$. □

Definició 6.3.3.7 (Màxim comú divisor)**.** Siguin $(D,+,\cdot)$ un domini d'integritat i $a,b,d \in D$ tres elements tals que $d|a$ i $d|b$ i tals que per a tot $c \in D$ que satisfaci $c|a$ i $c|b$ tenim $c|d$. Aleshores direm que d és el màxim comú divisor de a i b. Direm que d és un màxim comú divisor de a i b o que $d \sim \text{mcd}(a,b)$.

Observem que aquesta definició té sentit per la proposició 6.3.3.6.

Proposició 6.3.3.8. *Siguin $(D,+,\cdot)$ un domini d'integritat, a,b dos elements de D i $X \subseteq D$ un conjunt tal que per a tot $m \in X$ tenim $a|m$, $b|m$ i per a tot $c \in D$ tal que $a|c$, $b|c$ es compleix $m|c$. Aleshores tenim que per a tot $m' \in X$ si i només si $m \sim m'$.*

Demostració. Comencem amb la implicació cap a la dreta ($\Rightarrow$). Suposem que $m' \in X$. Hem de veure que $m \sim m'$. Tenim $m'|m$ i $m|m'$ i per la definició de múltiple (6.3.3.1) trobem que $m \sim m'$.

Fem ara la implicació cap a l'esquerra ($\Leftarrow$). Suposem que $m' \sim m$. Hem de veure que $m' \in X$. Per hipòtesi tenim que $a|m$ i $b|m$. Per tant existeixen $\alpha,\beta \in D$ tals que $m = \alpha \cdot a$ i $m = \beta \cdot b$, i per la proposició 6.3.3.3 tenim que si $m' = u \cdot m$ amb $u \in D$ invertible aleshores $m = m' \cdot u^{-1}$. Per tant

$$m' = \alpha \cdot a \cdot u^{-1} \quad \text{i} \quad m' = \beta \cdot b \cdot {u'}^{-1}$$

i per tant $m'|a$ i $m'|b$. Ara bé, com que per hipòtesi $m \sim m'$, per la definició d'elements associats (6.3.3.5) tenim que $m' \in X$. □

Definició 6.3.3.9 (Mínim comú múltiple)**.** Siguin $(D,+,\cdot)$ un domini d'integritat i $a,b,m \in D$ tres elements tals que $a|m$ i $b|m$ i tals que per a tot $c \in D$ que satisfaci $a|c$ i $b|c$ tenim $m|c$. Aleshores direm que m és el mínim comú múltiple de a i b. Direm que m és un mínim comú múltiple de a i b o que $m \sim \text{mcm}(a,b)$. Entendrem que $\text{mcd}(a,b)$ i $\text{mcm}(a,b)$ són elements de D.

Observem que aquesta definició té sentit per la proposició 6.3.3.8.

Proposició 6.3.3.10. *Siguin $(a),(b)$ dos ideals principals d'un domini d'integritat $(D,+,\cdot)$. Aleshores tenim les igualtats*

1. $(a)+(b) = (\text{mcd}(a,b))$.
2. $(a) \cap (b) = (\text{mcm}(a,b))$.
3. $(a)(b) = (a \cdot b)$.

Demostració. Comencem veient el punt (1). Per la proposició 6.1.2.6 tenim que $(a)+(b) = \{x+y : x \in (a), y \in (b)\}$, i per la definició d'ideal principal (6.1.2.7) això és

$$(a)+(b) = \{r_1 \cdot a + r_2 \cdot b : r_1, r_2 \in R\},$$

que podem reescriure com

$$(a)+(b) = \{x : \text{existeixen } m,n \in R \text{ tals que } x = n \cdot m + b \cdot n\}$$

i per tant $(a)+(b) = (\text{mcd}(a,b))$ és un ideal principal de $(R,+,\cdot)$.

Continuem veient el punt (2). Per la proposició 6.1.2.6 tenim que

$$(a) \cap (b) = \{x : x \in (a), x \in (b)\},$$

que, per la definició d'ideal principal (6.1.2.7), podem reescriure com

$$(a) \cap (b) = \{x : x \text{ divideix } a \text{ i } b\}$$

i per tant $(a) \cap (b) = (\text{mcm}(a, b))$ és un ideal principal de $(R, +, \cdot)$.

Acabem veient el punt (3). Per la proposició 6.1.2.6 tenim que

$$(a)(b) = \{x_1 \cdot y_1 + \cdots + x_n \cdot y_n : x_1, \ldots, x_n \in (a), y_1, \ldots, y_n \in (b)\},$$

que, per la definició d'ideal principal (6.1.2.7) i la proposició 6.1.1.5, podem reescriure com

$$\begin{aligned}(a)(b) &= \{(r_1 \cdot a)(r_1' \cdot b) + \cdots + (r_n \cdot a)(r_n' \cdot b) : r_1, \ldots, r_n, r_1', \ldots, r_n' \in R\} \\ &= \{(r_1 \cdot r_1' + \cdots + r_n \cdot r_n') \cdot (a \cdot b) : r_1, \ldots, r_n, r_1', \ldots, r_n' \in R\},\end{aligned}$$

i si fixem $r_2 = \ldots r_n = 0$ i $r_1' = 1$ tenim, amb $r_1 = r$ que

$$(a)(b) = \{r \cdot (a \cdot b) : r \in R\},$$

i per la definició d'ideal principal (6.1.2.7) tenim que $(a)(b)$ és un ideal principal de $(R, +, \cdot)$ amb

$$(a)(b) = (a \cdot b). \qquad \square$$

Definició 6.3.3.11 (Primer)**.** Siguin $(D, +, \cdot$ un domini d'integritat, $p \neq 0$ un element de D tal que per a tot a, b dos elements de D que satisfacin $p|a \cdot b$ tenim $p|a$ ó $p|b$. Aleshores direm que p és primer.

Observació 6.3.3.12. *(a) és un ideal primer si i només si a és primer.*

Definició 6.3.3.13 (Element irreductible)**.** Siguin $(D, +, \cdot)$ un domini d'integritat, $a \neq 0$ un element no invertible de D i b, c dos elements de D tals que $a = b \cdot c$. Aleshores direm que a és irreductible si b ó c són invertibles.

Proposició 6.3.3.14. *Siguin $(D, +, \cdot)$ un domini d'integritat i p un element primer de D. Aleshores p és irreductible.*

Demostració. Suposem que a, b són dos elements de D tals que $p = a \cdot b$. Per la definició de primer (6.3.3.11) tenim que ha de ser $p|a$ ó $p|b$. Si $p|a$ tenim que $a = \alpha \cdot p$ per a cert $\alpha \in D$. Ara bé, per hipòtesi, tenim que $p = a \cdot b$. Per tant $a = \alpha \cdot a \cdot b$, i per la proposició 6.3.1.3 tenim que $1 = \alpha \cdot b$, i per la definició d'element invertible (6.1.1.7) tenim que b és invertible i per la definició d'irreductible (6.3.3.13) tenim que p és irreductible.

El cas $p|b$ és anàleg. $\square$

6.3.4 Dominis de factorització única

Definició 6.3.4.1 (Domini de factorització única)**.** Sigui $(D, +, \cdot)$ un domini d'integritat tal que per a tot element no invertible $a \neq 0$ de D

1. Existeixen $p_1, \ldots, p_n$ elements irreductibles de D tals que

$$a = p_1 \cdot \ldots \cdot p_n.$$

2. Si existeixen $p_1, \ldots, p_r$ i $q_1, \ldots, q_s$ elements irreductibles de D tals que

$$a = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

aleshores $r = s$ i existeix $\sigma \in S_r$ tal que

$$p_1 \cdot \ldots \cdot p_r = q_{\sigma(1)} \cdot \ldots \cdot q_{\sigma(r)},$$

amb $p_i \sim q_{\sigma(i)}$ per a tot $i \in \{1, \ldots, r\}$.

Teorema 6.3.4.2. *Sigui $(D, +, \cdot)$ un domini d'integritat. Aleshores $(D, +, \cdot)$ és un domini de factorització única si i només si tenim*

1. *Per a tot a element no invertible de D existeixen $p_1, \ldots, p_r$ elements irreductibles de D tals que*

$$a = p_1 \cdot \ldots \cdot p_r$$

2. *Si a és in element irreductible de D aleshores a és primer.*

Demostració. Comencem demostrant que la condició és suficient ($\Rightarrow$). Suposem doncs que $(D, +, \cdot)$ és un domini de factorització única. El punt (1) és conseqüència de la definició de domini de factorització única (6.3.4.1). Per tant només ens queda veure que tot element irreductible és primer. Siguin p un element irreductible de D i a, b dos elements irreductibles de D tals que $p|a \cdot b$. Per la definició de domini de factorització única (6.3.4.1) tenim que existeixen $p_1, \ldots, p_r, q_1, \ldots, q_s$ elements irreductibles de D tals que

$$a = p_1 \cdot \ldots \cdot p_r \quad \text{i} \quad b = q_1 \cdot \ldots \cdot q_s$$

i per tant

$$a \cdot b = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$$

i com que, per hipòtesi, $p|a \cdot b$ i la definició de domini de factorització única (6.3.4.1) tenim que

$$a \cdot b = p \cdot \alpha_1 \cdot \ldots \cdot \alpha_t$$

per a certs $\alpha_1, \cdots, \alpha_t$ elements irreductibles de D. Per tant tenim

$$a \cdot b = p \cdot \alpha_1 \cdot \ldots \cdot \alpha_t = p_1 \cdot \ldots \cdot p_r \cdot q_1 \cdot \ldots \cdot q_s$$

i, de nou, per la definició de domini de factorització única (6.3.4.1) tenim que $p \sim p_i$ ó $p \sim q_j$ per a certs $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s\}$, i per tant $p|a$ ó $p|b$, i per la definició de primer (6.3.3.11) tenim que p és primer.

Veiem ara que la condició és necessària ($\Leftarrow$). Suposem doncs que

1. Per a tot a element no invertible de D existeixen $p_1, \ldots, p_r$ elements irreductibles de D tals que

$$a = p_1 \cdot \ldots \cdot p_r$$

2. Si a és in element irreductible de D aleshores a és primer.

Sigui a un element no invertible de D. Pel punt (1) tenim que existeixen $p_1, \ldots, p_r$ elements irreductibles de D tals que

$$a = p_1 \cdot \ldots \cdot p_r.$$

Suposem que existeixen també $q_1, \ldots, q_s$ elements irreductibles de D tals que

$$a = q_1, \ldots, q_s.$$

Aleshores volem veure que $r = s$ i que existeix $\sigma \in S_r$ tal que

$$p_1 \cdot \ldots \cdot p_r = q_{\sigma(1)} \cdot \ldots \cdot q_{\sigma(r)},$$

amb $p_i \sim q_{\sigma(i)}$ per a tot $i \in \{1, \ldots, r\}$.

Tenim que $p_1 | a$, i com que pel punt (2) tenim que p_1 és primer, per la definició de primer (6.3.3.11) tenim que $p_1 | q_j$ per a cert $j \in \{1, \ldots, s\}$, i per la definició de irreductible (6.3.3.13) i la definició d'elements associats (6.3.3.5) tenim que $p_1 \sim q_j$. Sigui doncs $\sigma \in S_s$ tal que $p_1 | q_{\sigma(1)}$. Aleshores tenim

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = u_1 \cdot q_{\sigma(1)} \cdot \ldots \cdot q_s$$

per a cert u_1 element invertible de D. Podem iterar aquest argument per a $p_2, \ldots, p_t$, on $t = \min(r, s)$ per obtenir

$$p_1 \cdot \ldots \cdot p_t \cdot p_{t+1} \cdot \ldots \cdot p_r = (u_1 \cdot q_1) \cdot \ldots \cdot (u_t \cdot q_t) \cdot p_{t+1} \cdot \ldots \cdot p_s$$

per a certs $u_1, \ldots, u_t$ elements invertibles de D. Ara bé, tenim que $r = s$, ja que si $r > s$ tindríem que $p_{s+1}, \ldots, p_r$ són invertibles, i si $s > r$ tindríem que $q_{r+1}, \ldots, q_s$ són invertibles, però per la definició d'irreductible (6.3.3.13) i la definició de element invertible (6.1.1.7) tenim que això no pot ser, i per tant $r = s$ i per la definició de domini de factorització única (6.3.4.1) tenim que $(D, +, \cdot)$ és un domini de factorització única, com volíem veure. □

Proposició 6.3.4.3. *Siguin $(D, +, \cdot)$ un domini de factorització única i a, b dos elements no invertibles i no nuls de D tals que existeixen $p_1, \ldots, p_r$ tals que*

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \quad i \quad b = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$$

per a certs $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r \in \mathbb{N}$. Aleshores

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

Demostració. Denotem $d = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$ i $m = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$.

Prenem c un element de D tal que $c | a$ i $c | b$. Aleshores tenim que

$$c = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$$

per a certs $\gamma_i \leq \min(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$. Ara bé, com que $\gamma_i \leq \min(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$, i per tant $d | c$, i per la definició de màxim comú divisor (6.3.3.7) tenim que $d \sim \mathrm{mcd}(a, b)$.

Prenem ara c un element de D tal que $a | c$ i $b | c$. Aleshores tenim que

$$c = q \cdot p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$$

per a cert q element de D i certs $\gamma_i \geq \max(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$. Ara bé, com que $\gamma_i \geq \max(\alpha_i, \beta_i)$ per a tot $i \in \{1, \ldots, r\}$, i per tant $m | c$, i per la definició de mínim comú múltiple (6.3.3.9) tenim que $m \sim \mathrm{mcm}(a, b)$. □

6.3.5 Anells Noetherians

Definició 6.3.5.1 (Anell Noetherià)**.** Sigui $(N, +, \cdot)$ un anell commutatiu amb $1 \neq 0$ tal que si

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

són ideals de $(N, +, \cdot)$ existeix n_0 tal que per a tot $i \leq n_0$ tenim $I_i = I_{i+1}$. Aleshores diem que $(N, +, \cdot)$ és Noetherià.

Observació 6.3.5.2. *$(\{I_1, I_2, I_3 \dots\}, \subseteq)$ és una cadena.*

Lemma 6.3.5.3. *Siguin $(N, +, \cdot)$ un domini d'integritat Noetherià i $a \neq 0$ un element no invertible de N. Aleshores existeixen $p_1, \dots, p_n$ elements irreductibles de N tals que*

$$a = p_1 \cdot \dots \cdot p_n.$$

Demostració. Ho farem per reducció a l'absurd. Definim el conjunt

$$X = \{a \in N \text{ invertible} : a \neq p_1 \cdot \dots \cdot p_n \text{ per a } p_1, \dots, p_n \in N \text{ irreductibles}\}.$$

Volem veure que $X = \emptyset$. Suposem doncs que $X \neq \emptyset$ i prenem $a_1 \in X$. Per la definició d'irreductible (6.3.3.13) tenim que a_1 no és irreductible, i per tant existeixen $b_1, c_1 \in N$ no invertibles tals que

$$a_1 = b_1 \cdot c_1$$

i ha de ser $b_1 \in X$ o $c_1 \in X$.

Suposem que $b_1 \in X$, la demostració de l'altre opció és anàloga. Aleshores tenim, per l'observació 6.3.3.2, que $(a) \subset (b)$. Ara bé, també tindríem que $b_1 = b_2 \cdot c_2$ per a certs b_2, c_2 elements no invertibles de N amb $b_2 \in X$ o $c_2 \in X$, i podem iterar aquest argument per construir

$$(a_1) \subset (b_1) \subset (b_2) \subset (b_3) \subset \dots$$

però això entra en contradicció amb la definició de anell Noetherià (6.3.5.1), i per tant $X = \emptyset$, com volíem veure. □

6.3.6 Dominis d'ideals principals

Definició 6.3.6.1 (Domini d'ideals principals)**.** Sigui $(D, +, \cdot)$ un domini d'integritat tal que tot ideal de $(D, +, \cdot)$ és un ideal principal. Aleshores direm que $(D, +, \cdot)$ és un domini d'ideals principals.

Proposició 6.3.6.2. *Sigui $(D, +, \cdot)$ i un anell d'ideals principals. Aleshores un element $a \in D$ és irreductible si i només si (a) és un ideal maximal.*

Demostració. Comencem veient que la condició és suficient ($\Leftarrow$). Suposem doncs que a és un element irreductible de D i prenem $b \in D$ tal que $(a) \subseteq (b) \neq D$. Aleshores, per l'observació 6.3.3.2 tenim que $a|b$, és a dir, existeix $r \in D$ tal que $a = b \cdot r$, i per la definició d'irreductible (6.3.3.13) tenim que r ó b són invertibles. Ara bé, com que, per hipòtesi, $(b) \neq D$ tenim que b no és invertible, per tant ha de ser r invertible per la definició d'element invertible (6.1.1.7) tenim que $a \cdot r^{-1} = b$, per l'observació 6.3.3.2 tenim que $(a) = (b)$, i per la definició d'ideal maximal (6.3.1.7) tenim que (a) és un ideal maximal. □

Proposició 6.3.6.3. *Siguin $(D,+,\cdot)$ un domini d'ideals principals i a un element irreductible de D. Aleshores a és primer.*

Demostració. Per la proposició 6.3.6.2 tenim que (a) és maximal, pel corol·lari 6.3.1.9 veiem que (a) és primer, i per l'observació 6.3.3.12 trobem que a és primer, com volíem veure. □

Teorema 6.3.6.4. *Sigui $(D,+,\cdot)$ un domini d'ideals principals. Aleshores $(D,+,\cdot)$ és Noetherià.*

Demostració. Siguin $I_1,\ldots,I_i,\ldots$ ideals de $(D,+,\cdot)$ tals que

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

i

$$\mathcal{I} = \bigcup_{i=1}^{\infty} I_i.$$

Aleshores tenim que $\mathcal{I}$ és un ideal. També veiem que si $x \in \mathcal{I}$ existeix n tal que $x \in I_n$, i per la definició d'ideal d'un anell (6.1.2.1) tenim que si $y \in D$ aleshores $x \cdot y \in I_n$.

Ara bé, com que per hipòtesi $(D,+,\cdot)$ és un domini d'ideals principals tenim, per la definició de domini d'ideals principals (6.3.6.1) que existeix $a \in D$ tal que $\mathcal{I} = (a)$, i per tant existeix n tal que $a \in I_n$, i trobem que

$$\mathcal{I} = (a) \subseteq I_n \subseteq I_{n+k} \subseteq \mathcal{I}$$

per a tot $k \in \mathbb{N}$, i per tant $I_n = I_{n+k}$ per a tot $k \in \mathbb{N}$, i per la definició de anell Noetherià (6.3.5.1) trobem que $(D,+,\cdot)$ és un anell Noetherià. □

Teorema 6.3.6.5. *Sigui $(D,+,\cdot)$ un domini d'ideals principals. Aleshores $(D,+,\cdot)$ és un domini de factorització única.*

Demostració. Pel Teorema 6.3.6.4 tenim que $(D,+,\cdot)$ és un anell Noetherià, i pel lemma 6.3.5.3 tenim que per a tot element no irreductible a de D existeixen $p_1,\ldots,p_n$ elements irreductibles de N tals que

$$a = p_1 \cdot \ldots \cdot p_n.$$

També tenim, per la proposició 6.3.6.3 que si a és un element irreductible de D aleshores a és primer.

Per acabar, pel Teorema 6.3.4.2 tenim que $(D,+,\cdot)$ és un domini de factorització única. □

6.3.7 Dominis Euclidians

Definició 6.3.7.1 (Domini Euclidià)**.** Siguin $(D,+,\cdot)$ un domini de integritat i $U : D \setminus \{0\} \longrightarrow \mathbb{N}$ una aplicació tal que

1. $U(x) \leq U(x \cdot y)$ per a tot $x, y \in D \setminus \{0\}$.
2. Per a tot $x, y \in D$, $y \neq 0$ existeixen $Q, r \in D$ tals que $x = Q \cdot y + r$, amb $r = 0$ ó $U(r) < U(y)$.

Aleshores direm que $(D, +, \cdot)$ és un domini Euclidià amb la norma U.

Proposició 6.3.7.2. *Sigui $(D, +, \cdot)$ un domini Euclidià amb la norma U. Aleshores*

$$U(1) \leq U(x) \quad \textit{per a tot } x \in D \setminus \{0\}.$$

Demostració. Per la definició de domini Euclidià (6.3.7.1) tenim que $U(x) \leq U(x \cdot y)$ per a tot $x, y \in D \setminus \{0\}$. Per tant

$$U(1) \leq U(1 \cdot x) = U(x) \quad \text{per a tot } x \in D \setminus \{0\}. \qquad \square$$

Proposició 6.3.7.3. *Sigui $(D, +, \cdot)$ un domini Euclidià amb la norma U. Aleshores*

$$U(u) = U(1) \iff u \textit{ és un element invertible de } D.$$

Demostració. Comencem veient l'implicació cap a la dreta ($\Rightarrow$). Suposem doncs que u és un element invertible de D.

Per la proposició 6.3.7.2 tenim que $U(1) \leq U(u)$ i que $U(u) \leq U(u \cdot u^{-1})$. Ara bé, per la definició de l'invers d'un element invertible (6.1.1.8) tenim que $u \cdot u^{-1} = 1$, i per tant

$$U(1) \leq U(u) \leq U(u \cdot u^{-1}) = U(1),$$

i trobem $U(u) = U(1)$.

Veiem ara l'implicació cap a l'esquerra ($\Leftarrow$). Suposem que $U(u) = U(1)$.

Per la definició de domini Euclidià (6.3.7.1) tenim que existeixen Q, r elements de D tals que

$$1 = Q \cdot u + r$$

amb $r = 0$ ó $U(r) < U(u)$. Ara bé, per hipòtesi $U(u) = U(1)$, i per la proposició 6.3.7.2 trobem que ha de ser $r = 0$. Per tant tenim

$$1 = Q \cdot u$$

i per la definició d'element invertible (6.1.1.7) trobem que u és invertible. $\square$

Teorema 6.3.7.4. *Sigui $(D, +, \cdot)$ un domini Euclidià. Aleshores $(D, +, \cdot)$ és un domini d'ideals principals.*

Demostració. Siguin U una norma de $(D, +, \cdot)$ i I un ideal de $(D, +, \cdot)$. Si $I = \{0\}$ aleshores $I = (0)$. Suposem doncs que $I \neq (0)$ i prenem $b \in I$ tal que $U(b) \leq U(x)$ per a tot $x \in I$, $x \neq 0$.

Prenem ara $a \in I$. Per la definició de domini Euclidià (6.3.7.1) tenim que existeixen $Q, r \in D$ tals que

$$a = Q \cdot b + r$$

amb $r = 0$ ó $U(r) < U(b)$. I com que, per la definició de anell (6.1.1.1) tenim que $(D, +)$ és un grup tenim

$$r = a - Q \cdot b,$$

i per la proposició 6.1.2.4 tenim que

$$r = a - Q \cdot b \in I$$

i per tant, $r \in I$ amb $r = 0$ ó $U(r) < U(b)$. Ara bé, per hipòtesi tenim que $U(r) \geq U(b)$, per tant ha de ser $r = 0$ i tenim que

$$a = Q \cdot b,$$

d'on trobem que I és un ideal principal, i per la definició de domini d'ideals principals (6.3.6.1) tenim que $(D, +, \cdot)$ és un domini d'ideals principals. □

Teorema 6.3.7.5. *Sigui* $(K, +, \cdot)$ *un cos. Aleshores* $(K, +, \cdot)$ *és un domini Euclidià.*

Demostració. content... □

Capítol 7

Cossos finits

7.1 Introducció

Part IV

Mètodes Numèrics

Capítol 8

Interpolació

Sovint podem mesurar un procés físic com un número de punts (per exemple, la temperatura d'una habitació en diferents instants de temps), però no tenim una expressió analítica per aquest procés que ens permeti calcular el seu valor en un punt arbitrari. L'interpolació ens proporciona un mètode simple per estimar aquesta expressió analítica en el rang dels punts mesurats[1].

8.1 Introducció

8.1.1 Problema d'interpolació

Definició 8.1.1.1 (Problema d'interpolació)**.** Siguin

$$\Phi(x; a_1, \ldots, a_n) : \mathbb{R} \longrightarrow \mathbb{R}$$

una família de funcions que depenen dels paràmetres reals $a_0, \ldots, a_n$, una família $\{(x_i, y_i)\}_{i=0}^n$ de n punts. Direm que el problema d'interpolació de $\{(x_i, y_i)\}_{i=0}^n$ per $\Phi(x; a_0, \ldots, a_n)$ consisteix a determinar $a_0, \ldots, a_n$ tals que

$$\Phi(x_i; a_0, \ldots, a_n) = y_i \quad \text{per a tot } i \in \{1, \ldots, n\}.$$

També direm que $\{(x_i, y_i)\}_{i=0}^n$ són els punts de suport, $\{x_i\}_{i=0}^n$ són les abscisses de suport i $\{y_i\}_{i=0}^n$ les ordenades de suport.

Direm que un problema d'interpolació de $\{(x_i, y_i)\}_{i=0}^n$ per $\Phi(x; a_0, \ldots, a_n)$ és un problema d'interpolació lineal si existeixen $\Phi_0, \ldots, \Phi_n : \mathbb{R} \longrightarrow \mathbb{R}$ tals que

$$\Phi(x; a_0, \ldots, a_n) = a_0\Phi_0(x) + \cdots + a_n\Phi_n(x).$$

Exemple 8.1.1.2. *Exemples de problemes d'interpolació lineal són problemes com la interpolació polinòmica:*

$$\Phi(x; a_0, \ldots, a_n) = a_0 + a_1 x + \cdots + a_n x^n;$$

o la interpolació trigonomètrica:

$$\Phi(x; a_0, \ldots, a_n) = a_0 + a_1 e^{xi} + \cdots + a_n e^{nxi}.$$

[1] Si el punt que avaluem es troba fora del rang aquest problema s'anomena extrapolació i sol ser menys precís que la interpolació.

Mentre que exemples de problemes d'interpolació no lineals són problemes com la interpolació racional:

$$\Phi(x; a_0, \ldots, a_n, b_0, \ldots, b_m) = \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m};$$

o la interpolació exponencial:

$$\Phi(x; a_0, \ldots, a_n, \lambda_0, \ldots, \lambda_n) = a_0 e^{\lambda_0 x} + \cdots + a_n e^{\lambda_n x}.$$

La interpolació trigonomètrica es fa servir en l'anàlisi numèric de les sèries de Fourier, la interpolació exponencial és útil en l'anàlisi de desintegració radioactiva.

8.2 Polinomis interpoladors de Lagrange

8.2.1 Interpolació de Lagrange

Definició 8.2.1.1 (Problema d'interpolació de Lagrange)**.** Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació per $P(x; a_0, \ldots, a_n) \in \mathbb{R}_n[x]$ tal que $x_i \neq x_j$ per a tot $i, j \in \{0, \ldots, n-1\}$, amb $i \neq j$. Aleshores direm que el problema d'interpolació és un problema d'interpolació de Lagrange.

Definició 8.2.1.2 (Polinomis bàsics de Lagrange)**.** Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x; a_0, \ldots, a_n)$ on, per a cert $k \in \{0, \ldots, n\}$ fix tenim que $y_k = 1$ i per a tot $i \in I = \{0, \ldots, k-1, k+1, \ldots, n\}$ tenim $y_i = 0$. Aleshores direm que els polinomis

$$L_k(x) = \prod_{i \in I} \frac{x - x_i}{x_k - x_i} = \frac{(x - x_0) \cdots (x - x_{k-1})(x - x_{k+1}) \cdots (x - x_n)}{(x_k - x_0) \cdots (x_k - x_{k-1})(x_k - x_{k+1}) \cdots (x_k - x_n)}$$

són polinomis bàsics de Lagrange.

Observació 8.2.1.3.

$$L_k(x_i) = \begin{cases} 1 & \text{si } i = k, \\ 0 & \text{si } i \neq k. \end{cases}$$

Proposició 8.2.1.4. *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x)$. Aleshores la funció $P(x)$ que satisfà*

$$P(x_i) = y_i$$

per a tot $i \in \{0, \ldots, n\}$ és única.

Demostració. Per l'observació 8.2.1.3 veiem que una solució a aquest problema d'interpolació és

$$P(x) = y_0 L_0(x) + y_1 L_1(x) + \cdots + y_n L_n(x).$$

Per veure'n la unicitat suposem que existeix un altre $Q(x) \in \mathbb{R}_{n+1}[x]$ tal que

$$P(x_i) = Q(x_i) = y_i$$

per a tot $i \in \{0, \dots, n\}$. Això és equivalent a que

$$P(x_i) - Q(x_i) = 0$$

per a tot $i \in \{0, \dots, n\}$. Ara bé, tenim que $x_0, \dots, x_n$ són arrels diferents de $P(x) - Q(x)$ per la definició de problema d'interpolació de Lagrange (8.2.1.1). Com que $P(x) - Q(x) \in \mathbb{R}_{n+1}[x]$, aquests són els seus únics zeros, i pel Teorema Fonamental de l'Àlgebra tenim que ha de ser $P(x) = Q(x)$. □

Proposició 8.2.1.5. *Siguin $\{(x_i, y_i)\}_{i=0}^n$ un conjunt de punts de suport, $I = \{i_0, \dots, i_k\} \subseteq \{1, \dots, n\}$ un conjunt i $\{(x_i, y_i)\}_{i \in I}$ un problema d'interpolació per $P_{i_0,\dots,i_k} \in \mathbb{R}_k[x]$, on*

$$P_{i_0,\dots,i_k}\left(x_{i_j}\right) = y_{i_j} \quad \text{per a tot } j \in \{0, \dots, k\}.$$

Aleshores

$$P_i(x) = y_i$$

i

$$P_{i_0,\dots,i_k}(x) = \frac{(x - x_{i_0})\, P_{i_1,\dots,i_k}(x) - (x - x_{i_k})\, P_{i_0,\dots,i_{k-1}}(x)}{x_{i_k} - x_{i_0}}.$$

Demostració. Fixem $k = 1$. Aleshores tenim

$$P_i(x) = y_i.$$

Veiem la segona part. Definim $G(x) = \frac{(x-x_{i_0})P_{i_1,\dots,i_k}(x) - (x-x_{i_k})P_{i_0,\dots,i_{k-1}}(x)}{x_{i_k} - x_{i_0}}$ tenim $G = P_{i_0,\dots,i_k}$ per la proposició 8.2.1.4, i per tant

$$G(x_{i_0}) = P_{i_0,\dots,i_{k-1}}(x_{i_0}) = y_{i_0}$$

i

$$G(x_{i_k}) = P_{i_1,\dots,i_k}(x_{i_k}) = y_{i_k},$$

i per tant

$$G(x_{i_j}) = \frac{(x_{i_j} - x_{i_0})y_{i_j} - (x_{i_j} - x_{i_k})y_{i_j}}{x_{i_k} - x_{i_0}} = y_{i_j}$$

per a tot $j \in \{1, \dots, k-1\}$, com volíem veure. □

Observació 8.2.1.6 (Algorisme de Neville)**.** *Aquest mètode recurrent es pot organitzar en una taula com*

	$k=0$	$k=1$	$k=2$
x_0	$y_0 = P_0(x)$		
		$P_{0,1}(x)$	
x_1	$y_1 = P_1(x)$		$P_{0,1,2}(x)$
		$P_{1,2}(x)$	
x_2	$y_2 = P_2(x)$		
$\vdots$	$\vdots$		

que s'omple de columna a columna de dreta a esquerra. Es coneix com a algorisme de Neville.

Exemple 8.2.1.7. *Sigui* $\{(0,1),(1,3),(3,2)\}$ *un problema d'interpolació per* $P_{0,1,2}(x) \in \mathbb{R}_2[x]$. *Volem avaluar el polinomi interpolador de Lagrange en* $x = 2$, *és a dir, volem trobar* $P_{0,1,2}(2)$.

Solució. La taula de l'algoritme de Neville plantejada en l'observació algorisme de Neville (8.2.1.6) per aquest problema és

	$k=0$	$k=1$	$k=2$
$x_0 = 0$	$y_0 = P_0(2) = 1$		
		$P_{0,1}(2) = 5$	
$x_1 = 1$	$y_1 = P_1(2) = 3$		$P_{0,1,2}(2) = \frac{10}{3}$
		$P_{1,2}(2) = \frac{5}{2}$	
$x_2 = 3$	$y_2 = P_2(2) = 2$		

i per tant trobem $P_{0,1,2}(2) = \frac{10}{3}$. ◊

8.2.2 Mètode de les diferències dividides de Newton

El mètode de Neville és útil per avaluar un polinomi interpolador en un punt una vegada, però si es vol obtenir l'expressió general del polinomi interpolador per poder avaluar-lo múltiples vegades en diferents punts s'hauran d'emparar altres solucions.

Definició 8.2.2.1 (Diferències dividides)**.** Sigui $P(x; a_0, \ldots, a_n)$ el polinomi interpolador de Lagrange amb els punts de suport $\{(x_i, y_i)\}_{i=0}^n$. Aleshores direm que

$$[x_0, \ldots, x_k] = a_k$$

és la diferència dividida d'ordre n del problema d'interpolació de Lagrange de $\{(x_i, y_i)\}_{i=0}^k$ per $P(x; a_0, \ldots, a_k)$.

Observem que aquesta definició té sentit per la proposició 8.2.1.4.

Proposició 8.2.2.2. *Sigui* $\{(x_i, y_i)\}_{i=0}^n$ *un problema d'interpolació de Lagrange per* $P(x)$. *Aleshores*

$$P(x) = [x_0] + [x_0, x_1](x - x_0) + [x_0, x_1, x_2](x - x_0)(x - x_1) + \cdots$$
$$\cdots + [x_0, \ldots, x_n](x - x_0) \cdots (x - x_{n-1}) = \sum_{i=0}^{n} \left([x_0, \ldots, x_i] \prod_{j=0}^{i-1} (x - x_j) \right).$$

Demostració. Denotem per $P_{1,\ldots,k} \in \mathbb{K}_{k+1}[x]$ el polinomi que satisfà

$$P_{0,\ldots,k}(x_j) = y_j \quad \text{per a tot } j \in \{0, \ldots, k\}.$$

Aleshores tenim que el polinomi

$$G_k(x) = P_{0,\ldots,k}(x) - P_{0,\ldots,k-1}(x)$$

té com arrels $x_0, \ldots, x_{k-1}$, i per tant existeix una única constant C_k tal que

$$G_k(x) = C_k(x - x_0) \cdots (x - x_{k-1})$$

i per tant, si fem

$$G_k(x) = a_0 + a_1 x + \cdots + a_k x^k$$

tenim que $C_k = a_k$. Aleshores per la definició de diferències dividides (8.2.2.1) tenim que

$$G_k(x) = [x_0, \dots, x_k](x - x_0) \cdots (x - x_{k-1})$$

i per la proposició 8.2.1.4 tenim

$$P(x) = P_n$$

i per tant trobem recursivament

$$\begin{aligned}
P_n(x) =& P_{n-1}(x) + [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1}) \\
=& P_{n-2}(x) + [x_0, \dots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
&+ [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1}) \\
&\vdots \\
=& P_{n-r}(x) + \sum_{i=0}^{n-r+1} \left([x_0, \dots, x_{n-l+1}] \prod_{j=0}^{n-r} (x - x_j) \right) \qquad \text{(r>0)} \\
&\vdots \\
=& P_1(x) + [x_0, x_1](x - x_0) + [x_0, x_1, x_2](x - x_0)(x - x_1) + \cdots \\
&\cdots + [x_0, \dots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
&+ [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1})
\end{aligned}$$

i per la definició de diferències dividides (8.2.2.1) tenim que $P_1(x) = [x_0]$

$$\begin{aligned}
=& [x_0] + [x_0, x_1](x - x_0) + \cdots + [x_0, \dots, x_{n-1}](x - x_0) \cdots (x - x_{n-2}) + \\
&+ [x_0, \dots, x_n](x - x_0) \cdots (x - x_{n-1}) = P(x).
\end{aligned}$$

□

Observació 8.2.2.3. *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange. Aleshores per a tot $\sigma \in S_4$ tenim*

$$[x_0, \dots, x_n] = [x_{\sigma 0}, \dots, x_{\sigma(n)}].$$

Demostració. Per la proposició 8.2.1.4. □

Proposició 8.2.2.4. *Sigui $\{(x_i, y_i)\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x)$. Aleshores*

$$[x_i] = y_i \quad \textit{per a tot } i \in \{0, \dots, n\} \tag{8.1}$$

i

$$[x_0, \dots, x_n] = \frac{[x_1, \dots, x_n] - [x_0, \dots, x_{n-1}]}{x_n - x_0}. \tag{8.2}$$

Demostració. Per veure (8.1) tenim prou en veure que per a un problema d'interpolació de $\{(x, y)\}$ per $P(x)$ tenim que $P(x) \in \mathbb{R}_0[x]$, i per tant és una constant i per la definició de diferències dividides (8.2.2.1) trobem $[x] = y$.

Per veure (8.2) tenim, per la proposició 8.2.1.5

$$P_{0,\dots,n}(x) = \frac{(x - x_0)\, P_{1,\dots,n}(x) - (x - x_n)\, P_{0,\dots,n-1}(x)}{x_n - x_0},$$

on $P_{i_1,\dots,i_k}(x)$ és el polinomi interpolador de Lagrange del problema interpolador del problema $\{(x_i, y_i)\}_{i\in\{i_1,\dots,i_k\}}$. Per tant per la proposició 8.2.2.2 trobem

$$[x_0,\dots,x_n] = \frac{[x_1,\dots,x_n] - [x_0,\dots,x_{n-1}]}{x_n - x_0},$$

com volíem veure. □

8.2.3 Error en la interpolació de Lagrange

Teorema 8.2.3.1. *Siguin $f : [a,b] \longrightarrow \mathbb{R}$ una funció de classe de diferenciabilitat $\mathcal{C}^{n+1}$ i $\{(x_i, f(x_i))\}_{i=0}^n$ un problema d'interpolació de Lagrange per $P(x)$ amb abscisses de suport que satisfan $\{x_i\}_{i=0}^n \subset [a,b]$. Aleshores per a tot $x \in [a,b]$ tenim*

$$f(x) - P(x) = \frac{f^{(n+1)}(\xi(x))}{(n+1)!}\omega(x),$$

on $\omega(x) = (x-x_0)\cdots(x-x_n)$, per a una certa funció $\xi(x) : [a,b] \longrightarrow [c,d]$ amb $c = \min\left\{\min_{i\in[0,n]}\{x_i\}, x\right\}$ i $d = \max\left\{\max_{i\in[0,n]}\{x_i\}, x\right\}$.

Demostració. Fixem $x \in [a,b]$. Tenim $f(x_i) - P(x_i) = 0$ per a tot $i \in \{0,\dots,n\}$. Si imposem $x \notin \{x_0,\dots,x_n\}$ i definim la funció

$$F(z) = f(z) - P(z) - \omega(z)S(x)$$

on

$$S(x) = \frac{f(x) - P(x)}{\omega(x)}. \tag{8.3}$$

Observem que $S(x)$ està ben definida pel Teorema Fonamental de l'Àlgebra.

Observem també que

$$F(x_i) = f(x_i) - P(x_i) - \omega(x_i)S(x) = 0$$

i

$$F(x) = f(x) - P(x) - \omega(x)\frac{f(x) - P(x)}{\omega(x)} = 0$$

és a dir, $F(z)$ existeixen $\xi_{0,0},\dots,\xi_{0,n+1} \in [a,b]$ tals que $F(\xi_{0,i}) = 0$ per a tot $i \in \{0,\dots,n+1\}$ amb $\xi_{0,i+1} > \xi_{0,i}$ per a tot $i \in \{0,\dots,n\}$.

Aplicant el Teorema de Rolle (1.2.3.7) trobem que per a tot $i \in \{1,\dots,n+1\}$ existeixen $\{\xi_{1,i}\}_{i=1}^{n+1}$ tals que $F'(\xi_{1,i}) = 0$ amb $\xi_{1,i} \in (\xi_{0,i-1}, \xi_{0,i})$. Iterant aquest argument trobem que per a $k \in \{0,\dots,n+1\}$ tenim que per a tot $i \in \{k,\dots,n+1\}$ existeixen $\{\xi_{k,i}\}_{i=k}^{n+1}$ tals que $F^k(\xi_{k,i}) = 0$ amb $\xi_{k,i} \in (\xi_{k-1,i-1}, \xi_{k-1,i})$; i per tant quan $k = n+1$ tenim que existeix $\xi_{n+1,n+1} \in (\xi_{n,n}, \xi_{n,n+1})$ tal que $F^{(n+1)}(\xi_{n+1,n+1}) = 0$ i trobem

$$F^{(n+1)}(\xi_{n+1,n+1}) = f^{(n+1)}(\xi_{n+1,n+1}) - (n+1)!S(x)$$

i per tant, recordant (8.3), tenim

$$\frac{f^{(n+1)}(\xi_{n+1,n+1})}{(n+1)!} = \frac{f(x) - P(x)}{\omega(x)}$$

i per tant

$$f(x) - P(x) = \frac{f^{(n+1)}(\xi_{n+1,n+1})}{(n+1)!}\omega(x),$$

com volíem veure. □

Observació 8.2.3.2.

$$f(x) - P(x) = [x_0, \ldots, x_n, x]\omega(x)$$

Corol·lari 8.2.3.3. *Sigui $\{(x_i, f(x_i))\}_{i=0}^n$ un problema d'interpolació de Lagrange. Aleshores existeix un cert $\xi \in [x_0, x_n]$ tal que*

$$[x_0, \ldots, x_n] = \frac{f^{(n)}(\xi)}{n!}.$$

Exemple 8.2.3.4. *Considerem el següent problema d'interpolació*

i	0	1	2	4
x_i	100	101	102	103
$\log(x_i)$	$\log(100)$	$\log(101)$	$\log(102)$	$\log(103)$

per $P(x)$. Volem estimar l'error comés en calcular el valor de $P(102.5)$.

Solució. Per la definició de problema d'interpolació de Lagrange (8.2.1.1) tenim que aquest problema d'interpolació és de Lagrange. Aleshores, pel Teorema 8.2.3.1 tenim que

$$f(x) - P(x) = \frac{f^{(4)}(\xi(x))}{4!}\omega(x)$$

i per tant, amb $f(x) = \log(x)$,

$$\log(x) - P(x) = \frac{-1}{\xi^4(x)4}(x-100)(x-101)(x-102)(x-103)$$

i si prenem $x = 102.5$ tenim

$$\log(102.5) - P(102.5) = \frac{-1}{\xi^4(102.5)4}\frac{5}{2}\frac{3}{2}\frac{1}{2}\frac{-1}{2}$$

amb $\xi(102.5) \in [100, 103]$, i per tant $\frac{1}{103} \leq \frac{1}{\xi(102.5)} \leq \frac{1}{100}$. Aleshores tenim

$$|\log(102.5) - P(x)| = \frac{3 \cdot 5}{2^4 \cdot \xi^4(102.5)} \leq \frac{15}{64}\frac{1}{100^4} \approx 2.34 \cdot 10^{-9}. \qquad \Diamond$$

8.2.4 Interpolació en nodes equiespaiats

Definició 8.2.4.1 (Nodes equiespaiats)**.** Sigui $\{x_i\}_{i=0}^n$ abscisses de suport que satisfacin

$$x_i = x_0 + ih$$

amb $h = \frac{x_n - x_0}{n}$ per a tot $i \in \{0, \ldots, n\}$. Aleshores direm que les abscisses de suport $\{x_i\}_{i=0}^n$ són equiespaiades o que un problema d'interpolació $\{(x_i, y_i)\}_{i=0}^n$ és un problema d'interpolació amb nodes equiespaiats.

També denotarem

$$\Delta f(x) = f(x+h) - f(x) \quad \text{i} \quad \Delta^{n+1} f(x) = \Delta(\Delta^n f(x)).$$

Teorema 8.2.4.2. *Sigui $\{(x_i, f(x_i))\}_{i=0}^n$ un problema d'interpolació de Lagrange amb nodes equiespaiats. Aleshores, si $h = \frac{x_n - x_0}{n}$ tenim*

$$[x_0, \dots, x_n] = \frac{\Delta^n f(x_0)}{n! h^n}.$$

Demostració. Ho farem per inducció sobre n. El cas $n = 1$ és cert, ja que

$$\begin{aligned}
\Delta f(x_0) &= f(x_0 + h) - f(x_0) && \text{(nodes equiespaiats (8.2.4.1))} \\
&= f(x_1) - f(x_0) \\
&= h \frac{f(x_1) - f(x_0)}{x_1 - x_0} \\
&= h[x_0, x_n] && \text{(diferències dividides (8.2.2.1))}
\end{aligned}$$

i per tant

$$[x_0, x_n] = \frac{\Delta f(x_0)}{h}. \tag{8.4}$$

Suposem ara que l'enunciat és cert per a k fix i demostrem-ho pel cas $k+1$. Tenim que

$$\begin{aligned}
\Delta^{k+1} f(x_0) &= \Delta(\Delta^k(f(x_0)) && \text{(nodes equiespaiats (8.2.4.1))} \\
&= \Delta^k f(x_1) - \Delta^k f(x_0) && \text{(nodes equiespaiats (8.2.4.1))} \\
&= k! h^k \left([x_1, \dots, x_{k+1}] - [x_0, \dots, x_k]\right) && \text{(8.4)} \\
&= k! h^k (k+1) h \frac{[x_1, \dots, x_{k+1}] - [x_0, \dots, x_k]}{x_{k+1} - x_0} \\
&= (k+1)! h^{k+1} [x_0, \dots, x_{k+1}], && \text{(diferències dividides (8.2.2.1))}
\end{aligned}$$

i per tant tenim

$$[x_0, \dots, x_{k+1}] = \frac{\Delta^{k+1} f(x_0)}{(k+1)! h^{k+1}},$$

com volíem veure. □

8.3 Polinomis interpoladors per splines

8.3.1 Interpolació per splines

Definició 8.3.1.1. Siguin $\Delta = \{x_i\}_{i=0}^n$ una partició d'un interval $[a, b] \subset \mathbb{R}$ i $s : [a, b] \longrightarrow \mathbb{R}$ una funció a trossos de classe $\mathcal{C}^{p-1}$ de la forma

$$s(x) = \begin{cases} s_1(x) & \text{si } x \in [x_0, x_1] \\ \vdots & \\ s_{k+1}(x) & \text{si } x \in [x_k, x_{k+1}] \\ \vdots & \\ s_n(x) & \text{si } x \in [x_{n-1}, x_n] \end{cases}$$

amb $s_i \in \mathbb{R}_p[x]$ per a tot $i \in \{1, \dots, n\}$. Aleshores direm que s és un spline de grau p associat a Δ.

Denotarem

$$S_p(\Delta) = \{s : s \text{ és un spline de grau } p \text{ associat a } \Delta\}.$$

Nota 8.3.1.2. *Només treballarem amb splines cúbics, és a dir, amb* $p = 3$*, que són els més emparats.*

ai haig de córrer