Francesc Bars Cortina

# Uns apunts d'Aritmètica.

Apunts de classe:
Grau en Matemàtiques
UAB, 17 de maig de 2024
Versió preliminar.

# Contingut

# Capítol 1

# Aritmètica en equacions diofantines

## 1.1 Resultats d'Aritmètica clàssica

### 1.1.1 Termes Pitagòriques. Corbes còniques.

Iniciem el curs amb el problema de les termes pitagòriques, és dir busquem $x, y, z \in \mathbb{Z}$ complint

$$x^2 + y^2 = z^2. \tag{1.1}$$

Si $z = 0$: $x^2 + y^2 = 0$ amb $x, y \in \mathbb{Z}$ d'on $x = y = z = 0$, i de ser l'equació homogenea podem pensar en buscar les solucions del conjunt:

$$\{(x, y, z) \in \mathbb{Z}^3 \setminus (0, 0, 0) | mcd(x, y, z) = 1, x^2 + y^2 = z^2\}.$$

Hi ha la bijecció entre $\{(x, y, z) \in \mathbb{Z}^3 \setminus (0, 0, 0) | x^2 + y^2 = z^2, mcd(x, y, z) = 1\}$ i $\{(u, v) \in \mathbb{Q}^2 | u^2 + v^2 = 1\}$ donada per $(x, y, z) \mapsto (\frac{x}{z}, \frac{y}{z})$.

**Lema 1.1.1.** *Hi ha una bijecció entre totes les solucions de $u^2 + v^2 = 1$ amb $(u, v) \in \mathbb{Q}^2 \setminus (-1, 0)$ amb els nombres racionals, a més podem expressar aquestes solucions com:*

$$(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2})$$

*amb $t \in \mathbb{Q}$.*

*Demostració.* Sigui $(\alpha, \beta) \neq (-1, 0)$ un punt racional solució de $u^2 + v^2 = 1$. La pendent de la recta que uneix $(-1, 0)$ i $(\alpha, \beta)$ és $\frac{\beta}{\alpha+1} \in \mathbb{Q}$, per tant això defineix una aplicació injectiva $\varphi$ entre punts racionals de $U^2 + V^2 = 1$ diferents del $(-1, 0)$ a $\mathbb{Q}$, via $(\alpha, \beta) \mapsto \frac{\beta}{\alpha+1}$. Veiem que l'anterior aplicació és exhaustiva.

Triem $t \in \mathbb{Q}$, i considera la recta que passa per $(-1, 0)$ i té pendent $t$: $y = t(x + 1)$ i la intesequem amb $X^2 + Y^2 = 1$.

La intersecció tindrà com a molt dos punts: en substituir var. $Y$ en l'equació de grau dos (corresponent a la recta) tenim una equació de grau 2 en $X$; que correspon a l'equació $X^2 + t^2(X+1)^2 = 1$ que té per solució $x = \frac{-2t^2 \pm \sqrt{4t^4 - 4(t^2+1)(t^2-1)}}{2(t^2+1)}$ (que en principi són elements a la clausura algebraica dels racionals), corresponent a $x = -1$ i $x = \frac{1-t^2}{1+t^2} \in \mathbb{Q}$ (del fet que el discriminant és un quadrat).

En substituir a l'equació de grau 1 de la recta, obtenim que corresponen als punts un és $(-1,0)$ i l'altre $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}) \in \mathbb{Q}^2$, per tant l'aplicació $\varphi$ és bijectiva i obtenim que tot punt correspon a l'expressió demanada. □

Per exemple per $t = \frac{5}{12}$ obtenim $(\frac{119}{169}, \frac{120}{169})$ solució per a $u^2 + v^2 = 1$ i d'aquí la terna Pitagòrica, solució de l'equació (1.6):

$$119^2 + 120^2 = 169^2.$$

**Corol·lari 1.1.2.** *Hi ha una bijecció* $\varphi : \{(x,y) \in \mathbb{Q}^2 \setminus (-1,0) | x^2+y^2 = 1\} \to \mathbb{Q}$ *donada per* $(x,y) \mapsto \frac{y}{x+1}$ *i* $\varphi^{-1}(t) = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$.

Anem a expressar les solucions de l'equació (1.6) parametritzades per enters.

Considera $(\alpha, \beta, \gamma) \in \mathbb{Z}^3$ solució de l'equació (1.6) amb $mcd(\alpha, \beta, \gamma) = 1$, podem pensar $\gamma \neq 0$.

De la igualtat

$$\alpha^2 + \beta^2 \equiv \gamma^2 (mod\ 4)$$

obtenim que si $\alpha$ i $\beta$ senars, s'obtindria que la igualtat anterior mòdul 4 no es satisfaria (els quadrats a $\mathbb{Z}/4$ són 0 i 1), per tant $\alpha$ o $\beta$ són un parell i l'altre senar, (ambdos tampoc poden ser parells per la condició $mcd(\alpha, \beta, \gamma) = 1$).

Escrivim $t = \frac{a}{b} \in \mathbb{Q}$ amb $mcd(a,b) = 1$, obtenim que les solucions a $\mathbb{P}^2(\mathbb{Q})$ [1] de l'equació $X^2 + Y^2 = Z^2$ son donades per

$$(\frac{1 - \frac{a^2}{b^2}}{1 + \frac{a^2}{b^2}} : \frac{2\frac{a}{b}}{1 + \frac{a^2}{b^2}} : 1) = (b^2 - a^2 : 2ab : b^2 + a^2).$$

Observem que l'última expressió té coordenades enteres i

$$mcd(b^2 - a^2, 2ab, b^2 + a^2) = 1 \text{ ó } 2.$$

on 2 correspon a $b$ i $a$ senar.

Per tant hem obtingut quan l'anterior maxim comú divisor és 1,

**Lema 1.1.3.** *Donat* $(\alpha, \beta, \gamma) \in \mathbb{Z}^3 \setminus (0,0,0)$ *amb* $mcd(\alpha, \beta, \gamma) = 1$, *complint que és solució de* $X^2 + Y^2 = Z^2$ *amb* $\alpha \equiv 1(2)$, $\beta \equiv 0(mod\ 2)$ *llavors és de la forma*

$$(b^2 - a^2, 2ab, b^2 + a^2)$$

*amb* $b, a$ *enters coprimers que no són alhora tots dos senars.*

Si el $mcd(b^2 - a^2, 2ab, b^2 + a^2) = 2$, $a, b$ senars i

$$(\frac{b^2 - a^2}{2}, \frac{2ab}{2}, \frac{b^2 + a^2}{2})$$

és solució entera de $X^2 + Y^2 = Z^2$ amb $y$ senar e $x$ parell, permutant $X$ e $Y$, han d'existir $c, d$ enters coprimers que no són alhora senars complint

$$(\frac{b^2 - a^2}{2}, \frac{2ab}{2}, \frac{b^2 + a^2}{2}) = (2cd, c^2 - d^2, c^2 + d^2)$$

pel lema anterior 1.1.3. Per tant obtenim

[1] Recordem que donat $K$ un cos $\mathbb{P}^n(K) = \{(a_1, \ldots, a_n) \in K^n \setminus (0, \ldots, 0) | a_i \in K\} / \sim$ on $(a_1, \ldots, a_n) \sim (b_1, \ldots, b_n)$ si i només si $\exists \lambda \in K^*$ complint que $a_i = \lambda b_i\ \forall i = 1, \ldots n$. Escrivim un element de $\mathbb{P}^n(K)$ via $(\alpha_1 : \ldots : \alpha_n) = \{(\lambda\alpha_1, \ldots, \lambda\alpha_n) \in K^n \setminus (0, \ldots, 0) | \lambda \in K^*\}$.

**Lema 1.1.4.** *Donat* $(\alpha,\beta,\gamma) \in \mathbb{Z}^3 \setminus (0,0,0)$ *amb* $mcd(\alpha,\beta,\gamma) = 1$*, complint que és solució de* $X^2 + Y^2 = Z^2$ *amb* $\alpha \equiv 0(mod\ 2)$*,* $\beta \equiv 1(mod\ 2)$ *llavors és de la forma*

$$(2cd, c^2 - d^2, c^2 + d^2)$$

*amb* $c, d$ *enters coprimers que no són alhora tots dos senars.*

Anem a demostrar el teorema de Fermat per l'equació $X^4 + Y^4 = Z^4$ usant la tècnica anomenada de descens infinit de Fermat.

**Proposició 1.1.5.** *L'equació* $X^4+Y^4 = Z^2$ *no té solucions enteres amb* $xy \neq 0$ *(i no té tampoc solucions racionals amb* $xy \neq 0$*).*

*Demostració.* Sigui $(\alpha,\beta,\gamma)$ una solució entera. Reduïm mòdul 4 i podem pensar sense pèrdua de generalitat que $\alpha \equiv 1(mod\ 2)$, $\beta \equiv 0(mod\ 2)$, $\alpha,\beta,\gamma \geq 0$ amb $mcd(\alpha,\beta) = 1$.

Escrivim $(\alpha^2)^2 + (\beta^2)^2 = \gamma^2$, i tenim una terma Pitagòrica, i del lema 1.1.3 un sistema

$$\begin{cases} \alpha^2 = b^2 - a^2 \\ \beta^2 = 2ab \\ \gamma^2 = b^2 + a^2 \end{cases} \tag{1.2}$$

per certs $a, b$ enters amb $mcd(a,b) = 1$ on $a, b$ un senar i l'altre parell.

De la primera equació en (1.2) $\alpha^2 + a^2 = b^2$ fent mòdul 4, s'obté $a$ ha de ser parell i $b$ senar, ja que $\alpha$ senar. Per tant usant de nou el lema 1.1.3 obtenim el sistema d'equacions

$$\begin{cases} \alpha = p^2 - q^2 \\ a = 2pq \\ b = p^2 + q^2 \end{cases} \tag{1.3}$$

amb $p, q$ coprimers i un parell i l'altre senar.

Fixem-nos que $mcd(p, q, b = p^2 + q^2) = 1$ perquè $mcd(a,b) = 1$.

Ara de l'equació (1.2), (1.3) obtenim

$$\beta^2 = 2ab = 4pq(p^2 + q^2)$$

i de ser coprimers $p, q, p^2 + q^2$, obtenim del teorema de factorització en primers (teorema fonamental de l'aritmètica) que existeixen $r, s, \ell \geq 0$ naturals complint:

$$r^2 = p,\ s^2 = q,\ p^2 + q^2 = \ell^2$$

i per tant obtenim

$$\ell^2 = r^4 + s^4$$

una altra solució entera de $X^4 + Y^4 = Z^2$.

Fixem-nos com $\alpha\beta \neq 0$ tenim $\beta^2 \neq 0$ d'on $pq \neq 0$ i per tant $rs \neq 0$, d'on $(r, s, \ell)$ amb $rs \neq 0$.

Observem a més que

$$\ell^4 = (p^2 + q^2)^2 = b^2 < b^2 + a^2 = \gamma$$

i per tant $\ell < \sqrt[4]{\gamma}$ i $\ell$ un enter positiu per construcció.

Aquesta metodologia la podem iterar obtenint solucions enteres $(\alpha_i, \beta_i, \gamma_i)$ amb $\alpha_i\beta_i \neq 0$ de $X^4+Y^4 = Z^2$ on $\gamma_i > \gamma_{i+1} \geq 1$, i per tant algun moment $\gamma_i = 1$ per cert $i$ però llavors $\beta_i\alpha_i = 0$ en contradicció. Per tant no pot ser possible que hi hagi una solució d'inici com hem suposat. (Aquesta metodologia s'anomena la tècnica de descens infinit de Fermat). □

**Corol·lari 1.1.6.** *L'equació $X^4+Y^4=Z^4$ no té solucions a $\mathbb{Z}$ amb $xyz\neq 0$.*

*Demostració.* Escrivim $w=z^2$ on $x^4+y^4=w^2$ no té solucions amb $xy\neq 0$. □

**Resolució de còniques**

Anem a l'estudi de còniques en $\mathbb{P}^2(\mathbb{Q})$ o més en general sobre un cos arbitrari $K$ enlloc de $\mathbb{Q}$. (Podriem fer la teoria general de formes quadràtiques sobre un cos $K$ per la resolució, però ens restringim al curs a corbes) [2].

Volem resoldre a $\mathbb{P}^2(K)$ l'equació homogènea:

$$aX^2+bY^2+cZ^2+dXY+eYZ+fXZ=0 \tag{1.4}$$

amb $a,b,c,d,e,f\in K$. Suposem $2\in K^*$, és dir $car(K)\neq 2$, tenim que podem escriure l'equació (1.4) en forma matricial,

$$\begin{pmatrix} X & Y & Z \end{pmatrix}\begin{pmatrix} a & d/2 & f/2 \\ d/2 & b & e/2 \\ f/2 & e/2 & c \end{pmatrix}\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}=(0).$$

Escrivim $\mathfrak{X}=\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$ i $A$ per la matriu simètrica $\begin{pmatrix} a & d/2 & f/2 \\ d/2 & b & e/2 \\ f/2 & e/2 & c \end{pmatrix}$ i observeu que un canvi de base $P\in GL_3(K)$ (o de $PGL_3(K)$) transformem la cònica $\mathfrak{X}^tA\mathfrak{X}=(0)$ amb la cònica $\mathfrak{X}'^tP^tAP\mathfrak{X}=(0)$.

**Proposició 1.1.7.** *Si $car(K)\neq 2$ tota equació (1.4) és equivalent a resoldre una equació de la forma*

$$a'X^2+b'Y^2+c'Z^2=0$$

*amb $a',b',c'\in K$, anomenada forma quadràtica diagonal en tres variables.*

*Demostració.* Hem de fer explícit un canvi de variable que ens permet traslladar una equació arbitrària escrita (1.4) a l'expressió de la proposició.

Pensem que $a$,$b$ o $c$ algún d'ells és no-zero de l'equació (1.4). Sense pèrdua de generalitat pensem $a\neq 0$. Fent el canvi $X--->X'=X+\frac{d}{2a}Y$, $Y->Y$, $Z->Z$ eliminem els termes amb $XY$ de l'equació (1.4). Fent el canvi $X'->X''=X'+\frac{f}{2a}Z$, $Y->Y$, $Z->Z$ eliminem els termes amb $XZ$. I per tant fent aquests canvis de base hem arribat a una equació :[3]

$$aX^2+uY^2+vZ^2+hYZ=0,$$

[2] Per saber-ne molt més consulteu el llibre "Introduction to Quadratic forms over fields", de T.Y.Lam, (1973), AMS(2005)

[3] En forma matricial per eliminar $XY$ i $XZ$ hem fet el canvi $\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}=\begin{pmatrix} 1 & -d/(2a) & -f/(2a) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix}$ i fent el producte

$$\begin{pmatrix} 1 & -d/(2a) & -f/(2a) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^t\begin{pmatrix} a & d/2 & f/2 \\ d/2 & b & e/2 \\ f/2 & e/2 & c \end{pmatrix}\begin{pmatrix} 1 & -d/(2a) & -f/(2a) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} a & 0 & 0 \\ 0 & u & h/2 \\ 0 & h/2 & v \end{pmatrix}$$

per certs $u,h,v$ de $K$ provinents del canvi.

amb certs $u, v, h$ de $K$. Si $h = 0$ hem acabat, suposem $h \neq 0$. Ara si $u$ o $v$ és diferent de zero el canvi (pensant $u \neq 0$) $Y -> Y' = Y + \frac{h}{2u}Z$ obtenim la forma diagonal. Si $u$ i $v$ són zero fent $Y -> (Y + Z)$ ens reduïm al cas on $u$ o $v$ no són zero i per tant obtenim una forma diagonal.

Pensem ara que $a = b = c = 0$. Existeix un factor no zero, pensem $XZ$ està a l'equació (és dir $f \neq 0$) sense pèrdua de generalitat. Fent el canvi $Z -> (X+Z)$ $Z -> Z, Y -> Y$ obtenim una equació amb $X^2$ i podem fer l'argument anterior per obtenir una forma diagonal. □

Per tant ens podem restringir a l'estudi de punts en $\mathbb{P}^2(K)$ de còniques de la forma

$$aX^2 + bY^2 = cZ^2. \tag{1.5}$$

**Qüestió 1.1.8.** *Donada una equació (1.5), amb $K = \mathbb{Q}$, podem decidir sempre quant té solució o no? La resposta és si, els casos més complicats usem el criteri de Hasse-Minkowski.*

Per exemple l'equació $aX^2 + bY^2 + cZ^2 = 0$ no té solució a $\mathbb{Q}$ si es té $a > 0$, $b > 0$ i $c > 0$. Si considerem que algún dels $a, b, c$ és negatiu, ja és interessant, per exemple $X^2 + Y^2 - 3Z^2 = 0$ no té solució en $\mathbb{P}^2(\mathbb{Q})$.

**Qüestió 1.1.9.** *Donada una equació (1.5), que té una solució al cos $K$, podem trobar-ne llavors totes les solucions en el cos $K$?*

Anem a respondre aquesta pregunta.

**Lema 1.1.10.** *Considerem la cònica $aX^2 + bY^2 = cZ^2$ amb $a, b, c \in K$, on $K$ un cos amb $car(K) \neq 2$ i $abc \neq 0$. Suposem $(\alpha : \beta : \gamma) \in \mathbb{P}^2(K)$ és una solució, i sense perdua generalitat pensem $\gamma \neq 0$. Llavors hi ha una bijecció entre: $X := \{(x : y : z) \in \mathbb{P}^2(K) | ax^2 + by^2 = cz^2\}$ i $\mathbb{P}^1(K) = \{(a : 1) | a \in K\} \cup \{(1 : 0)\}$.*

*Demostració.* Identifiquem els punts de $X$ de la forma $(x : y : 1)$ amb el conjunt $U = \{(x, y) \in K^2 | ax^2 + by^2 = c\}$, i per formulació tenim $U \neq \emptyset$.

Considerem primer el cas $U = X$ (treballar amb geometría afí dins $K^2$), és dir $-a/b$ no és un quadrat de $K$, i.e. $-a/b \notin (K^*)^2$, i considerem $P = (\alpha, \beta) \in U$ un element de $U$ fixa't.

Podem argumentar de manera similar com Lemma 1.1.1.

Associem a cada punt $Q$ de $U$ amb $Q \neq P$, l'element de $\mathbb{P}^1(K)$ $(t : 1)$ on $t$ és la pendent de la recta que uneix $P$ i $Q$ si la component $X$ de $Q$ no és $\alpha$, i associem $\infty = (1 : 0)$ si la component $X$ de $Q$ és $\alpha$. Si $Q = P$ associem $(t : 1)$ on $t$és la pendent de la recta tangent en aquest punt $P$ a la cònica (on li associem $\infty$ si la recta tangent en $P$ és de la forma $X - \alpha = 0$).

Això defineix una aplicació $\varphi : U \to \mathbb{P}^1(K)$. Clarament és injectiva ja si tenim dos punts $Q_1$, $Q_2$ que defineixen el mateix pendent $t$, com la l'intersecció d'una recta $Y - \beta = t(X - \alpha)$ amb $aX^2 + bY^2 = c$ sol pot tenir dues solucions per $X$'s i per tant dos punts en $U$ arribem a contradicció. (Fixeu-vos que la recta tangent en el punt $P$ és calcula de forma usual de forma implicita via $2bY\frac{dY}{dX} + 2aX = 0$ i per tant $Y'(P) = -\frac{2a\alpha}{2b\beta}$ si $\beta \neq 0$ i per tant la recta tangent és $Y - \beta = -\frac{a\alpha}{b\beta}(X - \alpha)$ i la intersecció amb $aX^2 + bY^2 = c$ és un únic punt $P$; quant $\beta = 0$ la recta tangent en $P$ és $X - \alpha = 0$ i la intersecció amb $aX^2 + bY^2 = c$ és un únic punt).

Veiem que $\varphi$ és exhaustiva. Considerem $t \in \mathbb{P}^1(K)$. Considerem $t \in K$ associat a $(t:1) \in \mathbb{P}^1(K)$. Cal resoldre el sistema

$$\begin{cases} Y - \beta = t(X - \alpha) \\ aX^2 + bY^2 = c \end{cases}$$

Resolent el sistema anterior (substituint la $Y$ de la recta en l'equació de grau 2) arribem a una expressió:

$$aX^2 + b(t(X-\alpha)+\beta)^2 = a\alpha^2 + b\beta^2 = c$$

on com equació de grau 2 en $X$ obtenim que el seu discriminant és

$$\Delta = (2b\beta + 2a\gamma)^2$$

i per tant un quadrat, obtenint dues solucions a $K$ pel valor de $x$ del sistema anterior, un correspon a $x = \alpha$ i substituïnt a l'equació de la recta correspon a $(\alpha, \beta)$. L'altre dóna un punt $Q$ diferent de $P$ si el discriminant $\Delta$ és no zero, i si $\Delta = 0$ tenim $P = Q$ però llavors es comprova que la recta és la recta tangent en el punt $P$. Un argument similar es fa considerant el sistema $X - \alpha = 0$ amb $aX^2 + bY^2 = c$ pel cas $\infty$.

El cas que $-a/b = \delta^2$ és un quadrat en $K$, $\delta \in K$, hem de treballar amb el projectiu $\mathbb{P}^2(K)$, directament ja que en intersecar una equació de grau 2 amb una recta, es tallaran en dos punts en $X$ (dins el projectiu) però no podem treballar en $U$ dins el plà afí $K^2$, ja que el segon punt pot ser en $X$ però no necessàreament en $U$, observeu $X = U \cup (1:\delta:0) \cup (1:-\delta:0)$. Per exemple si $K = \mathbb{Q}$ correspondria el cas d'una hipèrbola on $\pm\delta$ són les pendents de les assímptotes. Exercici. □

En la demostració usem que en $\mathbb{P}^2(K)$ la intersecció d'una recta $eX + bY + cZ = 0$ amb un polinomi homogeni de grau 2 on la recta no estigui continguda es talla en dos punts en la clausura algebraica de $K$ (i que veiem que realment els punts es troben ja definits en el cos $K$), això s'obté de substituir l'equació de la corba en el polinomi homogeni de grau 2. Més en general, tenim un resultat fonamental d'àlgebra commutativa i geometria algebraica següent:

**Teorema 1.1.11** (de Bézout)**.** *Siguin $F$ i $G$ dos polinomis homogenis en $K[X,Y,Z]$, l'anell de polinomis en tres variables a coeficients en un cos $K$, i sigui $n$ el grau de $F$ i $m$ el grau de $G$. Suposem que $F$ i $G$ no tenen cap component comú, és dir que no existeix $H$ homogeni en $K[X,Y,Z]$ complint que $F = H \cdot T$ i $G = H \cdot S$ amb $T, S$ polinomis homogenis en $K[X,Y,Z]$. Podem escriure $V(F) = \{(x:y:z) \in \mathbb{P}^2(\overline{K}) | F(x,y,z) = 0\}$, $V(G) = \{(a:b:c) \in \mathbb{P}^2(\overline{K}) | G(a,b,c) = 0\}$ on $\overline{K}$ denota la clausura algebraica de $K$. Llavors $V(F)$ i $V(G)$ s'intersequen com a molt en $nm$-punts en el projectiu $\mathbb{P}^2(\overline{K})$ (i exactament en $nm$-punts si es compta certa multiplicitat, multiplicitat que no vull entrar a definir en aquests apunts, i que té a veure amb tangències del punt $P \in V(F) \cap V(G)$ respecte les equacions $F$ i $G$).* [4]

[4] Podeu aprofundir i veure la demostració del teorema de Bézout en el llibre W.Fulton "Algebraic Curves", per a una introducció a la geometria algebraica amb poc preliminars d'Àlgebra commutativa.

### 1.1.2 L'equació de Pell

Considerem l'equació $Y^2 - DX^2 = 1$, on $D$ un NATURAL lliure de quadrats i busquem $(x, y) \in \mathbb{Z}^2$ amb $y^2 - Dz^2 = 1$.

Demostrarem en aquesta secció:

**Teorema 1.1.12.** *L'equació $Y^2 - DX^2 = 1$ amb $D$ natural lliure de quadrats té solució a $\mathbb{Z}^2$ diferent de les solucions trivials $(\pm 1, 0)$.*

[5]

**Lema 1.1.13.** *(d'aproximació) Sigui $\theta$ un nombre irracional i $q > 1$ un enters. Llavors existeixen $x, y$ enters complint*

$$|y - x\theta| < \frac{1}{q} (\leq \frac{1}{x})$$

*amb $0 < x \leq q$, on el valor absolut és el valor absolut arquimedià usual en els nombres reals.*

*Demostració.* Fent $x_i \in \{0, \ldots, q\} \subset \mathbb{N}$, per cada $x_i$ triem $y_i$ enter amb $0 \leq y_i - x_i\theta < 1$. Tenim $q + 1$ valors de $Y - X\theta$ en els $q$-intervals

$$[\frac{r}{q}, \frac{r+1}{q}),\ r = 0, \ldots, q - 1.$$

Per tant hi ha dos valors de $y_i - x_i\theta$ dins el mateix interval, sense pèrdua de generalitat podem pensar que els dos valors corresponen a $i = 1, 2$ i per tant,

$$|(y_1 - y_2) - (x_1 - x_2)\theta| < \frac{1}{q} \leq \frac{1}{x_1 - x_2}.$$

□

**Corol·lari 1.1.14.** *Donat $\theta$ un nombre irracional, llavors hi ha una infinitut de solucions a $\mathbb{Z}$ de la inequació*

$$|Y - X\theta| < 1/X.$$

*Demostració.* Pel lema anterior tenim que l'anterior inequació té una solució a $\mathbb{Z}$. Escrivim-la via $|\alpha_1 - \beta_1\theta| < 1/\beta_1$. Triant $q_1 > \frac{1}{|\alpha_1 - \beta_1\theta|}$, usant el lema anterior podem obtenir una solució diferent complint $|\alpha_2 - \beta_2\theta| < 1/q_1 \leq \frac{1}{\beta_2}$, i iterant el procés triant $q_i > \frac{1}{|\alpha_i - \beta_i\theta|}$ construïm solució $(\alpha_{i+1}, \beta_{i+1})$ satsifent la inequació diferent de les anteriors usant el lema anterior, per $i \geq 1$ enter. □

**Lema 1.1.15.** *Existeix $m \in \mathbb{R}$ complint que la inequació*

$$|Y^2 - DX^2| < m$$

*té una infinitud de solucions amb $(x, y) \in \mathbb{Z}^2$.*

[5] Aquest resultat és un corol.lari del teorema de les unitats de Dirichlet, sobre les unitats de l'anell d'enters en el cas concret del cos $\mathbb{Q}(\sqrt{D})$. Potser veurem aquest resultat o almenys l'anell d'enters per extensions finites de $\mathbb{Q}$ a la part final del curs

*Demostració.* Triem $\theta = \sqrt{D}$ en el corol.lari anterior, tenim $x, y$ enters amb $x \neq 0$ complint $|y - x\sqrt{D}| < \frac{1}{|x|}$, i

$$|y + x\sqrt{D}| = |y - x\sqrt{D} + 2x\sqrt{D}| < \frac{1}{|x|} + 2|x|\sqrt{D}$$

i per tant

$$|y^2 - x^2 D| < 2\sqrt{D} + \frac{1}{x^2} \leq 2\sqrt{D} + 1,$$

on podem triar $m = 1 + 2\sqrt{D}$. □

*Demostració.* [Teorema 1.1.12] Pel lema anterior i la seva demostració $\exists k \in \mathbb{Z}$ amb $|k| < 2\sqrt{D}+1$ on $Y^2 - DX^2 = k$ té una infinitud de solucions. Com $(\mathbb{Z}/(k))^2$ és un conjunt finit, podem suposar que hi ha dos solucions $(x_1, y_1), (x_2, y_2)$ diferents de $Y^2 - DX^2 = k$ (amb $x_i$ no zero) complint $x_2 \equiv x_1 (mod\ k)$, $y_2 \equiv y_1 (mod\ k)$ i $(_2, y_2) \neq (-x_1, -y_1)$.

Obtenim llavors de $k = y_1^2 - Dx_1^2 = y_2 - Dx_2^2$ les igualtats:

$$k^2 = (y_1 - Dx_1^2)(y_2 - Dx_2^2) = (y_1 y_2 - Dx_1 x_2)^2 - D(y_1 x_2 - x_1 y_2)^2.$$

Escrivim $y_1 y_2 - Dx_1 x_2 = k\alpha$ i $y_1 x_2 - x_1 y_2 = k\beta$, si veiem que $\alpha, \beta \in \mathbb{Z}$ ja hem obtingut el resultat del fet que $\alpha \neq 0$.

Efectivament $\alpha, \beta \in \mathbb{Z}$ perquè de la elecció triada de les solucions $(x_i, y_i)$ obtenim:

$$y_1 y_2 - Dx_1 x_2 \equiv y_1^2 - Dx_1^2 \equiv 0 (mod\ k)$$
$$y_1 x_2 - x_1 y_2 \equiv x_1(y_1 - y_1) \equiv 0 (mod\ k).$$

□

**Teorema 1.1.16.** *L'equació $Y^2 - DX^2 = 1$ amb $D$ natural lliure de quadrats, té una infinitud de solucions $(x, y) \in \mathbb{Z}^2$.*

*Demostració.* Com l'equació ja hem demostrat que té solució, considerem $(u, t) \in \mathbb{Z}^2$ amb $u > 0$, $t > 0$ on $u$ el valor natural més petit no zero que satisfà l'equació $Y^2 - DX^2 = 1$.

Afirmem que $(x_n, y_n) \in \mathbb{N}^2$ on $y_n + x_n\sqrt{D} := (t + u\sqrt{D})^n \in \mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} | a, b \in \mathbb{Z}\}$ és solució de $Y^2 - DX^2 = 1$ per tot $n \geq 1$ natural. Efectivament,

$$y_n^2 - Dx_n^2 = (y_n + x_n\sqrt{D})(y_n - x_n\sqrt{D}) = (t + u\sqrt{D})^n (t - u\sqrt{D})^n = (t^2 - u^2\sqrt{D})^n = 1$$

on $y_n - x_n\sqrt{D} = \sigma(y_n + x_n\sqrt{D}) = \sigma((t+u\sqrt{D})^n) = (\sigma(t+u\sqrt{D}))^n = (t - u\sqrt{D})^n$
$\sigma \in Gal(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ el generador que envia $\sqrt{D} \mapsto -\sqrt{D}$. □

**Teorema 1.1.17.** *Totes les solucions de l'equació $Y^2 - DX^2 = 1$ amb $D$ natural no quadrat, venen expressades via $y + x\sqrt{D} = \pm(t + u\sqrt{D})^n$ en $\mathbb{Z}[\sqrt{D}]$ per cert $n \in \mathbb{Z}$ on $(u, t) \in \mathbb{N}^2$ amb $u > 0, v > 0$ solució $Y^2 - DX^2 = 1$ amb $X$ mínima.*

*Demostració.* Per $n = 0$ obtenim les solucions trivials $(0, \pm 1)$. La demostració del teorema anterior obtenim:
$x > 0, y > 0$, $y + x\sqrt{D} = (t + u\sqrt{D})^n$ amb $n$ natural són infinites solucions;
$x < 0, y < 0$, $y + x\sqrt{D} = -(t + u\sqrt{D})^n$ amb $n$ natural són infinites solucions;
$x < 0, y > 0$, $y + x\sqrt{D} = (t + u\sqrt{D})^{-n}$ amb $n$ natural són infinites solucions;

$x > 0, y < 0$, $y + x\sqrt{D} = -(t + u\sqrt{D})^{-n}$ amb $n$ natural són infinites solucions.

Sigui $(x, y)$ una altra solució, i sense pèrdua de generalitat pensem $x > 0, y > 0$. De la ordenació dins els reals tenim que existeix $m$ natural complint;

$$(t + u\sqrt{D})^m < y + x\sqrt{D} < (t + u\sqrt{D})^{m+1},$$

i per tant,

$$1 < (y + x\sqrt{D})(t + u\sqrt{D})^{-m} < (t + u\sqrt{D}).$$

Com $(y + x\sqrt{D})(t + u\sqrt{D})^{-m} \in \mathbb{Z}[\sqrt{D}]$ escrivim $a + b\sqrt{D} := (y + x\sqrt{D})(t + u\sqrt{D})^{-m}$ amb $a, b \in \mathbb{Z}$, i es comprova que $(b, a)$ és solució de $X^2 - DY^2 = 1$.

Ara tenim $a + b\sqrt{D} < t + u\sqrt{D}$ i $0 < a - b\sqrt{D} < 1$ (ja que $(a - b\sqrt{D})(a + b\sqrt{D}) = 1$ i $(a + b\sqrt{D}) > 1$) per tant $a > 0$ i $b > 0$, entrant en contradicció amb l'elecció de $(u, t)$ on $u$ és el natural més petit complint $Y^2 - DX^2 = 1$. □

**Conjectura 1.1.18.** *Sigui $p$ primer senar amb $p \equiv 3(mod\ 4)$. Considera l'equació de Pell*

$$Y^2 - pX^2 = 1.$$

*Sigui $u$ com l'anterior teorema on $(u, v)$ solució de l'equació de Pell anterior amb $u > 0, v > 0$ amb $u$ la més petita possible. Llavors $u \not\equiv 0(mod\ p)$.*

**Teorema 1.1.19** (Mordell)**.** *Sigui $p$ primer senar amb $p \equiv 3(mod\ 4)$. Considera l'equació de Pell*

$$Y^2 - pX^2 = 1.$$

*Sigui $u$ com l'anterior teorema on $(u, v)$ solució de l'equació de Pell anterior amb $u > 0, v > 0$ amb $u$ la més petita possible. Llavors:*

$$u \not\equiv 0(mod\ p) \Leftrightarrow E_{\frac{p-3}{4}} \not\equiv 0(mod\ 4),$$

*on $E_n$ denota els nombres d'Euler definits via el desenvolupament $sec(x) = \sum_{n=0}^{\infty} E_n \frac{x^{2n}}{(2n)!}$.*

Per la demostració d'aquest resultat de Mordell podeu consultar: "On a Pellian equation conjecture (II)", Journal London Math. Soc. 36 (1961), 282-288.

### 1.1.3 Perquè els canvis de variable trigonomètrics per fer integració?

Considera $f$ una funció de variable real amb imatge no finita (i domini no un conjunt finit). Denota per $\mathbb{R}[f]$ l'anell generat $\mathbb{R}$ i $f$, on $f^n = f \cdot \ldots \cdot f$ (el producte no la composició).

Observem que $\mathbb{R}[f]$ és un domini: $(a_0 1 + a_1 f + \ldots + a_n f^n)(b_0 1 + \ldots + b_m f^m) = 0$ amb $a_i, b_j \in \mathbb{R}$ tenim que $f(w)$ satisfà un polinomi de cert grau a coeficients reals, per tant $f(w)$ ha de ser les arrels reals d'aquest polinomi, i com $f$ té imatge no finita, això no és pot donar i $\mathbb{R}[f]$ és un domini.

Considerem el morfisme d'anells evaluació en $f$

$$ev_f : \mathbb{R}[X] \to \mathbb{R}[f]$$

$$X \mapsto f$$

evident és exhaustiu, el $ker(ev_f) = (m(x))$, si $m(x)$ és un polinomi no zero $m(f(w)) = 0$ i per l'argument usat per demostrar $\mathbb{R}[f]$-domini arribem que no pot existir, per tant $ker(ev_f) = (0)$.

Considerem $Q(\mathbb{R}[f]) = \mathbb{R}(f) = \{\frac{h}{e} | h, e \in \mathbb{R}[f], e \neq 0\}$ ( el cos de fraccions del domini $\mathbb{R}[t]$), tenim una extensió simple $\mathbb{R}(f)/\mathbb{R}$ i $f$ és transcendent sobre $\mathbb{R}$.

Tornem ara a l'equació de la circumferència

$$X^2 + Y^2 = 1$$

amb $(x, y) \in \mathbb{R}^2$, sabem que $(x, y) = (\cos(\theta), \sin(\theta))$, on pensem $cos(\theta)$, $sin(\theta)$ a partir d'ara amb funcions de variable real amb domini en $(-\frac{\pi}{2}, \frac{\pi}{2})$.

Fixeu-vos que tenim la cadena de cossos:

$$\mathbb{R} \subset \mathbb{R}(cos(\theta)) \subset \mathbb{R}(cos(\theta), sin(\theta))$$

on $\mathbb{R}(cos(\theta))/\mathbb{R}$ és una extensió simple i trascendent sobre $\mathbb{R}$, i $\mathbb{R}(\cos(\theta), \sin(\theta))/\mathbb{R}(cos(\theta))$ és una extensió de grau 2 o 1 (realment 2).

Fent $X := \cos(\theta)$ tenim un isomorfisme de cossos $\mathbb{R}(cos(\theta), \sin(\theta)) \cong \mathbb{R}(X, \mathfrak{Y})$ on $\mathfrak{Y}^2 + X^2 - 1 = 0$ amb $X$ transcendent sobre $\mathbb{R}$, i pel Criteri d'Eisenstein $T^2 + (X - 1)(X + 1)$ és irreductible sobre $\mathbb{R}(X)$ per tant $[\mathbb{R}(cos\theta, sin\theta) : \mathbb{R}(cos\theta)] = 2$.

**Teorema 1.1.20.** *Existeix $u \in \mathbb{R}(\cos(\theta), \sin(\theta)) \cong \mathbb{R}(X, \mathfrak{Y})$ transcendent sobre $\mathbb{R}$ complint que $\mathbb{R}(u) = \mathbb{R}(\cos(x), \sin(x))$.*

*Demostració.* De la parametrització hem vist $(cos(x), sin(x)) = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ on $t$ era la pendent de la recta entre el punt $(-1, 0)$ al punt $(cos(x), sin(x))$, fixeu-vos del dibuix

obtenim $t = \tan(\frac{x}{2})$ i per tant tenim una extensió de cossos

$$\mathbb{R} \subset \mathbb{R}(\cos(x), \sin(x)) = \mathbb{R}(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}) \subseteq \mathbb{R}(t) = \mathbb{R}(\tan(\frac{x}{2})).$$

Veiem que $[\mathbb{R}(t) : \mathbb{R}(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})] = 1$. Denotem $E$ per $\mathbb{R}(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$. Tenim que $\frac{2t}{1+t^2} + 1 = \frac{(1+t)^2}{1+t^2} \in E$, per tant $\frac{1-t^2}{1+t^2} \cdot \frac{1+t^2}{(1+t)^2} = 1 - 2\frac{t}{1+t} \in E$, en particular $\frac{t}{1+t} - 1 = \frac{-1}{t+1} \in K$ d'aquí $1 + t \in E$ i per tant $t \in E$. □

El mateix argument a $X^2 + Y^2 = 1$ en un cos $K$ de $car(K) \neq 2$ demostra

**Teorema 1.1.21.** *Considera $K$ un cos de $car(K) \neq 2$. Considera l'extensió de cossos $K \subset K(X) \subset K(\mathfrak{Y}, X)$ on $X$ és transcendent sobre $K$ i $\mathfrak{Y}^2 + X^2 = 1$. Llavors existeix $u \in K(X, \mathfrak{Y})$ transcendent sobre $K$ complint que $K(u) = K(X, \mathfrak{Y})$.*

6

[6] Un argument similar és pel cos $K(X, \mathfrak{Y})$ on $aX^2 + b\mathfrak{Y}^2 = c$ on $X$ transcendent sobre $K$, $car(K) \neq 2$, sempre i quant l'equació $aX^2 + b\mathfrak{Y}^2 = c$ té una solució en el cos $K$

Més en general podem pensar una corba definida via

$$\mathcal{Y}^m - f(X) = 0$$

amb $f(X) \in K[X]$ no un quadrat, de manera que per Eisentein $T^m - f(X) \in K[X,T]$ és irreductible. Podem considerar l'extensió de cossos:

$$K \subset K(X) \subset K(X,\mathcal{Y}),$$

on $X$ transcendet sobre $X$ i $[K(X,\mathcal{Y}) : K(X)] = m$.

**Qüestió 1.1.22.** *Quant $K(X,\mathcal{Y})/K$ és una extensió simple? És dir quant existeix $u$ transcendet sobre $K$ complint $K(X,\mathcal{Y}) = K(u)$? Si $K$ és algebraicament tancat, això es resolt dient que si i només si el gènere de $Y^m - f(X) = 0$ és zero, equivalent que correspon a una linea projectiva.*

Tenim el següent resultat per extensions simples en grau de trascendencia 1.

**Teorema 1.1.23** (Lüroth)**.** *Suposem $K(t)/K$ és una extensió simple amb $t$ transcendent sobre $K$. Considerem $L$ un cos complint $K \subset L \subset K(t)$. Llavors $L/K$ és una extensió simple.*

Més endavant potser veure'm en aquest curs el següent resultat: considera que $K$ és un cos algebraicament tancat, llavors cossos de trascendencia 1 sobre $K$ correspon (via una bijecció) a corbes llises i projectives sobre el cos $K$. En particular la recta projectiva sobre $K$ correspon al cos $K(t)$ amb $t$ un element transcendent sobre $K$.

### 1.1.4 Congruències. Resolució equacions en cossos finits.

Una tècnica inicial en buscar solucions de $f = 0$ on $f \in R[X_1,\ldots,X_n]$ un polinomi a coeficients en un domini $R$, es estudiar $f \equiv 0(mod\ \mathfrak{p})$ on $\mathfrak{p}$ és un ideal de $R$ (si és primer millor ja que llavors $(R/\mathfrak{p})[X_1,\ldots,X_n]$ és un domini i té millors propietats, i encara millor si l'ideal és maximal).

Anem a repasar algunes propietats quant $R = \mathbb{Z}$ on tot ideal és principal de la forma $(m) = \{ma | a \in \mathbb{Z}\}$ $m \in \mathbb{N}$.

**Lema 1.1.24.** *Considera l'anell $\mathbb{Z}/(m)$. Donat $a \in \mathbb{Z}$ i $[a] \in \mathbb{Z}/(m)$ és un element invertible de $(\mathbb{Z}/(m))^*$ si i només si $mcd(a,m) = 1$. En particular l'anell $\mathbb{Z}/(m)$ és un cos si i només si $m$ és un nombre primer.*

Hi ha el següent resultat:

**Proposició 1.1.25** (teorema de les restes xinès)**.** *Sigui $m$ natural i el factoritzem via $m = n_1 \cdot \ldots \cdot n_s$ amb $n_i \in \mathbb{N}$ complint $mcd(n_i,n_j) = 1$ si $i \neq j$. Llavors hi ha un isomorfisme d'anells:*

$$\rho : \mathbb{Z}/(m) \to \mathbb{Z}/(n_1) \times \ldots \times \mathbb{Z}/(n_s),$$
$$n(mod\ m) \mapsto (n\ mod\ n_i)_{i=1,\ldots,s}.$$

*Demostració.* Exercici al lector comprovar que $\rho$ és morfisme d'anells.
Veiem $\rho$ és injectiva. Si $\rho([b]) = \rho([b'])$ tenim $b - b' \in (n_i)$ per $i = 1,\ldots,s$ per tant

$$b - b' \in \cap_{i=1}^{s}(n_i) = (mcm(n_1,\ldots,n_s)) = (n_1 \cdot \ldots \cdot n_s) = (m)$$

(l'última igualtat de ser coprimers els $n_i$'s), per tant $[b] = [b'] \in \mathbb{Z}/(m)$.
Veiem l'exhaustivitat. Triem $([\alpha_i])_{i=1}^s \in \mathbb{Z}/(n_1) \times \ldots \times \mathbb{Z}/(n_s)$. És suficient trobar $x \in \mathbb{Z}$ complint $x \equiv \alpha_i (mod\ n_i)$ per $i = 1, \ldots, s$. Estudiem primer el cas $s = 2$:

$$\begin{cases} x \equiv \alpha_1 (mod\ n_1) \\ x \equiv \alpha_2 (mod\ n_2) \end{cases}$$

i volem resoldre $x = \alpha_1 + n_1 t = \alpha_2 + n_2 u$ amb $t, u \in \mathbb{Z}$. D'aquí obtenim $n_1 t - n_2 u = (\alpha_2 - \alpha_1)$ i com $mcd(n_1, n_2) = 1$ per Bezout existeixen $\ell_1, \ell_2 \in \mathbb{Z}$ complint $n_1\ell_1 - n_2\ell_2 = 1$ i per tant fent $t = \ell_1(\alpha_2 - \alpha_1) + kn_2$ i $u = \ell_2(\alpha_2 - \alpha_1) - kn_1$ obtenim que $x = \alpha_1 + n_1\ell_1(\alpha_2 - \alpha_1) + n_1 n_2 k$ compleix el sistema de congruències i té una única solució en fer mòdul $n_1 n_2$.

Per a $s \geq 2$ l'argument anterior permet que dues equacions reduir-nos a una augmentant el mòdul, fent aquest procediment obtenim el cas general. □

Denotem la funció $\varphi$ d'Euler a l'aplicació $\varphi : \mathbb{N}_{\geq 1} \to \mathbb{N}$ definida per

$$\varphi(m) = \#\{[a] \in \mathbb{Z}/(m) | [a] \in (\mathbb{Z}/(m))^*\},$$

si $m \geq 2$ i $\varphi(1) = 1$.

**Lema 1.1.26.** *La funció $\varphi$ d'Euler té les següents propietats:*

1. *$\varphi(p) = p - 1$ per tot primer natural $p$ de $\mathbb{Z}$,*
2. *$\varphi(p^n) = p^{n-1}(p-1)$ amb $p$ primer i $n \in \mathbb{N}_{\geq 1}$,*
3. *si $n, m$ naturals coprimers (i.e. $mcd(n, m) = 1$) llavors: $\varphi(nm) = \varphi(n)\varphi(m)$,*
4. *si $n = p_1^{n_1} \cdots p_r^{n_r}$ és la factorització en nombres primers del natural $n$ llavors*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{n_i - 1}(p_i - 1).$$

*Demostració.* La propietat 1,2 són evidents de la definició. La propietat 3 surt del teorem xinès de les restes ja que en particular

$$(\mathbb{Z}/(nm))^* \cong^{\rho} (\mathbb{Z}/(n) \times \mathbb{Z}/(m))^* = (\mathbb{Z}/(n))^* \times (\mathbb{Z}/(m))^*.$$

□

**Corol·lari 1.1.27** (petit Teorema de Fermat)**.** *Donat $a \in \mathbb{Z}$ i $p$ nombre primer, llavors*

$$a^p \equiv a (mod\ p)$$

*o equivalentment $[a]^p = [a]$ en $\mathbb{Z}/(p)$ (i equivalentment a $a^{p-1} \equiv 1 (mod\ p)$ si $a$ és coprimer amb $p$).*

*Demostració.* Tenim $(\mathbb{Z}/(p))^*$ és un grup d'ordre $p - 1$, per tant el subgrup $< [a] >$ (amb $[a] \neq [0]$) té ordre un divisor de $p - 1$ (teorema de Lagrange), i per tant $[a]^{p-1} = [1]$ d'on $[a]^p = [a]$. Si $[a] = [0]$ és clar també $[a]^p = [a]$. □

**Corol·lari 1.1.28.** *Donat $n$ un natural i $a \in \mathbb{Z}$ coprimer amb $n$ llavors*

$$a^{\varphi(n)} \equiv 1 (mod\ n).$$

*Demostració.* Tenim que $(\mathbb{Z}/(n))^*$ és un grup d'ordre $\varphi(n)$. Per $a \in (\mathbb{Z}/(n))^*$ considera $H =< [a] >$ subgrup de $(\mathbb{Z}/(n))^*$, i per Lagrange tenim que $[a]^{\varphi(n)} = [1]$. □

**Lema 1.1.29.** *Donat $n \geq 1$ natural tenim la igualtat*

$$n = \sum_{d|n} \varphi(d).$$

*Demostració.* Si $d|n$ amb $d \neq 1$ es té $(n/d)\mathbb{Z}/(n)$ és l'únic subgroup de $(\mathbb{Z}/(n), +)$ d'ordre $d$ (per ser un grup cíclic), i té exactament $\varphi(d)$ elements com a generador d'aquest subgrup.

Observem que cada $[a] \in (\mathbb{Z}/(n), +)$ no zero té cert ordre, diem-li $\ell$ i per tant és un generador del subgrup cíclic $(n/\ell)\mathbb{Z}/(n)$. Si $[a] = [0]$ correspon al cas extrem $d = 1$ i a $\varphi(1) = 1$. □

**Observació 1.1.30.** *Fixeu-vos que en el grup cìclic $(\mathbb{Z}/(n), +)$, $[a] \in \mathbb{Z}/(n)$ és un generador si $mcd(a, n) = 1$.*
*Fixeu-vos que el grup $(\mathbb{Z}/(n))^*$ no és necessàreament cíclic, per exemple $(\mathbb{Z}/(8))^* = \{1, 3, 5, 7\} \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.*

**Lema 1.1.31.** *Sigui $\mathbb{F}_q$ un cos finit amb $q = p^n$ per cert $p$ primer i $n \geq 1$ natural, en particular té $q$ elements. Llavors $\mathbb{F}_q^*$ és un grup cíclic, en particular $\mathbb{F}_p^* = (\mathbb{Z}/(p))^*$ és un grup cíclic.*

*Demostració.* Sigui $f(X) = X^{q-1} - 1 \in \mathbb{F}_q[X]$ un polinomi que té com a molt $q - 1$ solucions en la clausura algebraica de $\mathbb{F}_q$. Tot $\alpha \in \mathbb{F}_q^*$ compleix $\alpha^{q-1} = 1$ per Lagrange, per tant els zeros de $f(X)$ són elements de $\mathbb{F}_q^*$.

Per cada $d|q-1$ els elements $\beta \in \mathbb{F}_q^*$ d'ordre exactament $d$ (en cas d'existir), són zeros de $X^d - 1$ (en particular n'hi ha $d$ zeros) i per tant el subgrup cíclic d'ordre $d$: $< [\beta] >$ (on tots són solució de $X^d - 1$ i per tant són les $d$ solucions de $X^d - 1$), té exactament $\varphi(d)$ elements generadors (i en particular d'ordre exactament $d$) per la observació anterior, i els altres valors són generadors per divisors estrictes de $d$.

Si per $d = q - 1$ existeix un $\beta$ d'ordre exactament $q - 1$ ja hem finalitzat i és cíclic.

En cas contrari, obtenim que $\sum_{d|q-1, d\neq q-1} \varphi(d) = q - 1$ ja que obtindriem tots els elements $e$ de $\mathbb{F}_q^*$ que són solució cert $d_e|q-1$ and $d_e \neq q-1$ de $X^{d_e} - 1$, però entra en contradicció amb el lemma 1.1.29 ja que $\varphi(q - 1) \geq 1$. □

**Una petita aplicació a criptografia de clau pública**.

Veurem com l'estructura d'anell $(\mathbb{Z}/(m))^*$ ens permet encriptar i desencriptar. El mètode que presentem és usual en Catalunya o Espanya d'enviar informació, on es necessita triar dos nombres primers.

Val a dir que en clau pública els últims anys s'usa Geometria Aritmètica (i Teoria de Nombres) per dissenyar noves formes d'encriptar, on usa les propietats de grup d'una corba el.líptica $Y^2 = aX^3 + bX + c$ sobre un cos finit, veieu l'appendix sobre Tallers del curs per informació preliminar en corbes el.líptiques. El mètode usant corbes el.líptiques s'usa en el passaport alemà, i un grup pioner que utilitza és G.Frey, Univ. Essen (Alemania) colaborant amb Siemens.

Tot seguit presentem de forma molt esquemàtica el mètode més usat encara en clau pública anomenat RSA fonamentat en l'estructura d'anell $(\mathbb{Z}/(p\cdot q))^*$ on $p, q$ són dos primers grans convenientment triats.

Tenim un EMISOR i un RECEPTOR, i es vol enviar un missatge de l'EMISOR al RECEPTOR en un canal públic on tothom el pot consultar. L'EMISOR després de redactar el missatge l'encripta i envia el missatge encriptat en el canal públic on tothom el pot consultar. També envia una clau pública de com s'ha encriptat el missatge que es coneguda per EMISOR i RECEPTOR, és una clau que la coneix tothom i tot missatge que s'envia s'encripta en aquesta clau. La idea és que per desxifrar-ho tan sols el RECEPTOR que té una clau privada el poc llegir, tot i que tothom pot enviar missatges encriptats al RECEPTOR.

Anem a explicar breument el $RSA$, considera com clau pública $(N, e)$ on $N = p_1 \cdot p_2$ producte de dos nombres primers grans (on donat $N$ és difícil computacionalment trobar $p_1$ i $p_2$) i sigui $e$ un natural menor que $\varphi(N) = (p_1-1)(p_2-1)$ i coprimer amb $\varphi(N)$ (fixeu-vos que $\varphi(N)$ el coneixà el receptor però és un problema computacional dificil saber-ho a partir de $N$ si no es té la factorització).

Llavors si $M$ és un missatge, el EMISSOR l'encripta amb la clau pública $(N, e)$ fent $M^e \equiv c(mod\ N)$ i envia en el canal públic $c$. El RECEPTOR és l'únic que coneix $\varphi$ i per tant sap $d$ on $de \equiv 1(mod\ \varphi(N))$, i desencripta el missatge, via

$$c^d \equiv (M^e)^d \equiv M^{1+k\varphi(N)} \equiv M(mod\ N)$$

usant el corol.lari 1.1.28, el RECEPTOR obté el missatge original.

Per intentar desxifrar-ho sense la clau pública, un pot enviar missatges encriptats per la clau pública coneguda per tothom, per tant podem conèixer $M$ (el missatge) i $c = M^e\ (mod\ N)$ (el missatge encriptat). I volem resoldre

$$c^X \equiv M(mod\ N),$$

es dir $X$ seria cert logaritme, aquest problema s'anomena el problema del logaritme discret i actualment no es coneix cap algoritme ràpid per poder-lo trobar, fent "segur" el mètode d'encriptació pública RSA si $(N, e)$ són convenientment triats.

### Equacions polinomials sobre cossos finits

Sigui $\mathbb{F}_q$ un cos finit de $q$-elements, $q = p^\ell$, $p$ primer.

**Lema 1.1.32.** *Sigui $n \geq 0$ un enter. Llavors*

$$\mathbb{F}_q \ni \sum_{x\in\mathbb{F}_q} x^n = \begin{cases} -1, & n \geq 1 \text{ i } q-1 \mid n \\ 0, & altrament. \end{cases}$$

*sota el conveni, que si $n = 0$ es té $x^0 = 1$ encara que $x = 0 \in \mathbb{F}_q$.*

*Demostració.* Per $n = 0$ tenim $\sum_{x\in\mathbb{F}_q} = q = 0$, recordem $p = car(\mathbb{F}_q)$.
Si $n \geq 1$ i $q-1|n$ sempre $0^n = 0$ i $x^n = 1$ ja que $\mathbb{F}_q^*$ és un grup cíclic d'ordre $q-1$. per tant $\sum_{x\in\mathbb{F}_q} = q-1 = -1$.
Si $n \geq 1$ i $q-1 \nmid n$, tenim $\exists y \in \mathbb{F}_q^*$ on $y^n \neq 1$ (de ser $\mathbb{F}_q^*$ ciclic ordre $q-1$). Per tant,

$$\sum_{x\in\mathbb{F}_q^*} x^n = \sum_{x\in\mathbb{F}_q^*} y^n(y^{-1}x)^n = \sum_{z\in\mathbb{F}_q^*} y^n z^n = y^n(\sum_{z\in\mathbb{F}_q^*} z^n);$$

d'on $(1-y^n)(\sum_{x\in\mathbb{F}_q^*} x^n) = 0$ obtenint el resultat. □

**Teorema 1.1.33** (Chevalley-Waring)**.** *Siguin $f_\alpha \in \mathbb{F}_q[X_1,\ldots,X_n]$ col.lecció de polinomis en n-variables a coeficients un cos finit $\mathbb{F}_q$, que compleix $\sum_\alpha deg(f_\alpha) < n$ (on $deg(g)$ és el natural que és el valor màxim de la suma dels graus dels monomis associats al polinomi g). Denotem per V al conjunt $\{\beta \in \mathbb{F}_q^n | f_\alpha(\beta) = 0, \forall\alpha\}$. Llavors*

$$\#(V) \equiv 0(mod\ p).$$

*Demostració.* Prenem el polinomi $P := \prod_\alpha (1-f_\alpha^{q-1})$, i sigui $x \in \mathbb{F}_q^n$ un element. Si $x \in V$ llavors $P(x) = \prod_\alpha (1-f_\alpha(x)^{q-1}) = 1$, i si $x \notin V$ existeix un $\alpha$ en la col.lecció on $f_\alpha(x) \neq 0$ i per tant $f_\alpha(x)^{q-1} = 1$ on $P(x) = 0$.
Tenim doncs definida una funció característica:

$$P : \mathbb{F}_q^n \to \{0,1\}$$
$$x \in V \mapsto 1,$$
$$x \notin V \mapsto 0.$$

Considerem per un polinomi en $n$ variables $g \in \mathbb{F}_q[X_1,\ldots,X_n]$ una funció suma $S(g) := \sum_{x\in\mathbb{F}_q^n} g(x)$. Fixeu-vos que

$$S(P) \equiv \#V(mod\ p).$$

Ara del fet que $\sum_\alpha deg(f_\alpha) < n$ tenim que $deg(P) < n(q-1)$, i per tant

$$P = \sum_{(u_1,\ldots,u_n)\in\mathbb{N}^n\cap A,\ A\ finit} a_{(u_1,\ldots,u_n)} X_1^{u_1}\cdot\ldots\cdot X_n^{u_n}$$

amb $a_{(n_1,\ldots,n_n)} \in \mathbb{F}_q$ i complint $\sum_{i=1}^n u_i < n(q-1)$, i de la propietat de la funció suma tenim,

$$S(P) = \sum_{(u_1,\ldots,u_n)\in\mathbb{N}^n\cap A,\ A\ finit} a_{(u_1,\ldots,u_n)} S(X_1^{u_1}\cdot\ldots\cdot X_n^{u_n}).$$

Per com es el conjunt $A$ sempre per algun $i$ $u_i < q-1$. Es suficient demostrar que $S(X_1^{u_1}\cdot\ldots\cdot X_n^{u_n}) = 0$ per concloure. Sense pèrdua de generalitat podem pensar que $u_1 < q-1$, d'on

$$S(X_1^{u_1}\cdot\ldots\cdot X_n^{u_n}) = \sum_{x_1\in\mathbb{F}_q} x_1^{u_1}\Big(\sum_{(x_2,\ldots,x_n)\in\mathbb{F}_q^{n-1}} x_2^{u_2}\cdot\ldots\cdot x_n^{u_n}\Big) = 0$$

on l'última igualtat es segueix del lema 1.1.32.

□

**Corol·lari 1.1.34.** *En la situació del teorema amb $\sum_\alpha deg(f_\alpha) < n$ i demanem que $f_\alpha$ no té terme constant per tot $\alpha$ en la família. Llavors els $f_\alpha$'s tenen un zero comú diferent del trivial $(0,\ldots,0)$.*

*Demostració.* Tenim que $(0,\ldots,0) \in V$, per tant $V \neq \emptyset$, i del teorema de Chevalley-Waring ha d'haver-hi més solucions ja que $\#V \equiv 0(mod\ p)$. □

**Corol·lari 1.1.35.** *Totes les formes quadràtiques en 3 variables sobre $\mathbb{F}_q$ (i.e. expressions de la forma $aX^2+bY^2+cZ^2+dXY+eXZ+fYZ = 0$ amb $a,b,c,d,e,f \in \mathbb{F}_q$ algún d'ells no zero) tenen una solució diferent de la trivial $(0,0,0)$.*

**La llei de reciprocitat quadràtica (Gauss)**

Recordem $\mathbb{F}_q$ és un cos finit amb $q = p^e$ elements. Aquests cossos hi ha el generador del grup de $Gal(\mathbb{F}_q/\mathbb{F}_p)$ donat pel Frobenius $Frob_p(x) = x^p$, que té ordre $e$ en $Gal(\mathbb{F}_q/\mathbb{F}_p)$.

Denotem per $(\mathbb{F}_q^*)^2 := \{x \in \mathbb{F}_q^* | \exists y \in \mathbb{F}_q^* \text{ amb } x = y^2\}$, els elements de $\mathbb{F}_q^*$ que són un quadrat i observeu que és un subgrup de $\mathbb{F}_q^*$.

**Proposició 1.1.36.** *Si $p$ és un primer senar, $(\mathbb{F}_q^*)^2$ és un subgrup d'índex 2 de $\mathbb{F}_q^*$, que és el nucli del morfisme*

$$x \mapsto x^{(q-1)/2}$$

*i en particular tenim una successió exacta*

$$1 \to (\mathbb{F}_q^*)^2 \to \mathbb{F}_q^* \to \{\pm 1\} \to 1.^7$$

*Si $p = 2$ llavors $\mathbb{F}_q^* = (\mathbb{F}_q^*)^2$, tot element és un quadrat.*

*Demostració.* Per $p = 2$, $Frob_2 : \mathbb{F}_q \to \mathbb{F}_q$ és automorfisme de cossos on $Imatge(Frob_2) = (\mathbb{F}_q^*)^2 \cup 0$, per tant per ser epimorfisme $\mathbb{F}_q^* = (\mathbb{F}_q^*)^2$.
Sigui $p$ un primer senar. Denotem per $\overline{\mathbb{F}}_q$ la clausura algebraica de $\mathbb{F}_q$ i pensem totes les extensions finites de $\mathbb{F}_q$ dins aquesta clausura. Considera el morfisme de grups:

$$\pi : \mathbb{F}_q^* \to \mathbb{F}_q^*$$

$$x \mapsto x^{(q-1)/2}.$$

Estudiem la imatge de $\pi$: com $(x^{(q-1)/2})^2 = x^{q-1} = 1$ per $x \in \mathbb{F}_q^*$, són zeros en $\mathbb{F}_q^*$ del polinomi $Y^2 - 1 \in \mathbb{F}_q[Y]$. En $\overline{F}_q$ el polinomi $Y^2 - 1$ té dos arrels, $1, -1 \in \mathbb{F}_q^*$, i $-1$ és en la imatge ja que existeix $u$ generador de $\mathbb{F}_q^*$ i per tant $u^{(q-1)/2} \neq 1$.
Estudiem ara el nucli de $\pi$: sigui $\alpha \in \mathbb{F}_q^*$ amb $\alpha^{(q-1)/2} = 1$. Considera el polinomi $Y^2 - \alpha \in \mathbb{F}_q[Y]$, que és separable i per tant té dos arrels diferents en $\overline{\mathbb{F}}_q^*$, diem $y$ una d'aquestes arrels (l'altra és $-y$). Fixem-nos llavors que

$$y^{q-1} = \alpha^{(q-1)/2} = 1$$

i per tant com $\mathbb{F}_q = \{u \in \overline{\mathbb{F}}_q | u^q = u\}$ tenim $y \in \mathbb{F}_q^*$ i per construcció $\alpha \in (\mathbb{F}_q^*)^2$, i l'inclusió $(\mathbb{F}_q^*)^2 \subset Nucli(\pi)$ és clara del fet $\mathbb{F}_q^*$ és un grup cíclic d'ordre $q-1$. □

**Definició 1.1.37.** *Sigui $p$ un primer senar, $x \in \mathbb{F}_p^*$, definim el simbol de Legendre de $x$ a l'enter $x^{(p-1)/2}$ i l'anotem per $\left(\frac{x}{p}\right)$. Definim $\left(\frac{0}{p}\right) = 0$ i extenem la definició per $n \in \mathbb{Z}$ considerant $[n] \in \mathbb{F}_p$ i definim $\left(\frac{n}{p}\right) = \left(\frac{[n]}{p}\right)$.*

**Lema 1.1.38.** *Donats $x, y \in \mathbb{F}_p$, $p$ primer senar, tenim que*

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right).$$

[7] Una succesió $1 \to A \to^{\alpha} B \to^{\beta} C \to 1$ és diu exacta si $\alpha$ és injectiva, $\beta$ exhaustiva, i $Imatge(\alpha) = Nucli(\beta)$.

*Demostració.* Observeu $\pi : \mathbb{F}_q^* \to \{\pm 1\}$ donat per $\alpha \mapsto \alpha^{(p-1)/2} = \left(\frac{\alpha}{p}\right)$ és morfisme de grups. □

**Lema 1.1.39.** *Sigui p primer senar. Tenim:*

$$\left(\frac{1}{p}\right) = 1,\ \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)},\ \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$$

$$on\ \varepsilon(p) = \begin{cases} 0\ si\ p \equiv 1(mod\ 4) \\ 1\ si\ p \equiv -1(mod\ 4) \end{cases},\ i\ \omega(p) = \begin{cases} 0\ si\ p \equiv \pm 1(mod\ 8) \\ 1\ si\ p \equiv \pm 5(mod\ 8) \end{cases}$$

*Demostració.* Sol cal estudiar l'últim simbol de Lagrange. Sigui $\alpha \in \overline{\mathbb{F}}_q^*$ arrel 8-èssima primitiva de 1 ($Y^8 - 1$ és un polinomi separable en $\mathbb{F}_p[Y]$, $p$ primer senar). Definim $y := \alpha + \alpha^{-1}$, i observem $y^2 = \alpha^2 + \alpha^{-2} + 2$. Com $\alpha^4 = -1$ tenim $\alpha^2 = -\alpha^{-2}$ per tant $y^2 = 1$ i per tant $y$ és una arrel del polinomi $Y^2 - 2 \in \mathbb{F}_p[Y]$ (i l'altra arrel és $-y$ ja que $car(\overline{\mathbb{F}}_p) \neq 2$), per tant $[\mathbb{F}_p(y) : \mathbb{F}_p] \leq 2$.

Fixem-nos que per construcció $\left(\frac{2}{p}\right) = y^{p-1}$.

Anem a estudiar quant $y \in \mathbb{F}_p$ i quant dóna una extensió de grau 2 sobre $\mathbb{F}_p$.
Com tenim característica $p$, tenim $y^p = \alpha^p + \alpha^{-p}$, ara si $p \equiv \pm 1(mod\ 8)$ tenim de ser $\alpha^8 = 1$ la igualtat amb $k$ enter,

$$y^p = \alpha^{1+8k} + \alpha^{-1-8k} = \alpha + \alpha^{-1} = y,$$

on $y \in \mathbb{F}_p^*$ i per tant el simbol de Lagrange té valor 1. Considerem ara $p \equiv \pm 5(mod\ 8)$ tenim llavors de forma similar,

$$y^p = \alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1}) = -y$$

on la segona igualtat prové $\alpha^4(\alpha + \alpha^{-1})$, $\alpha^3 = \alpha^{-5}$ i $\alpha^4 = -1$ de la definició d'$\alpha$. Per tant $y \notin \mathbb{F}_p$ obtenint que el simbol és -1. □

**Corol·lari 1.1.40.** *L'equació $X^2 - pY^m = 2$ amb p primer senar fixat i $m \geq 2$ enter, no té solució als enters si $p \equiv \pm 5(mod\ 8)$.*

*Demostració.* Considerem l'equació en l'anell $\mathbb{Z}/(p)$ i es converteix en

$$X^2 \equiv 2(mod\ p)$$

però $\left(\frac{2}{p}\right) = -1$ i per tant no és un quadrat el 2 en $\mathbb{Z}/(p)$ i per tant l'equació no té solució a $\mathbb{Z}/(p)$ i per tant tampoc a $\mathbb{Z}$. □

**Teorema 1.1.41** (Llei de reciprocitat quadràtica de Gauss)**.** *Siguin $\ell$ i $p$ dos primers senars diferents. Llavors:*

$$\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)(-1)^{\varepsilon(p)\varepsilon(\ell)},$$

*on $\varepsilon(n) \equiv \frac{n-1}{2}(mod\ 2)$ per a n senar.*

*Demostració.* Sigui $\omega \neq 1$ una arrel $\ell$-essima primitiva de 1 en $\overline{\mathbb{F}}_p$. Per cada $n \in \mathbb{Z}$ té sentit $\omega^n \in \overline{\mathbb{F}}_p$ i com $\omega^\ell = 1$ podem considerar $\omega^{[n]} \in \overline{\mathbb{F}}_p$ amb $[n] \in \mathbb{Z}/(\ell) = \mathbb{F}_\ell$. Escrivim:

$$y := \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \omega^x \in \overline{\mathbb{F}}_p.$$

Demostrarem primer:
**A.** Es té la igualtat $y^2 = (-1)^{\varepsilon(\ell)}\ell \in \mathbb{F}_p$.
**B.** $y^{p-1} = \left(\frac{p}{\ell}\right)$.

Demostrem **A.** Tenim les igualtats,

$$y^2 = \sum_{x,z \in \mathbb{F}_\ell} \left(\frac{xz}{\ell}\right) \omega^{x+z} = \sum_{u \in \mathbb{F}_\ell} \omega^u \left(\sum_{t \in \mathbb{F}_\ell} \left(\frac{t(u-t)}{\ell}\right)\right)$$

Si $t = 0$ tenim $\left(\frac{0}{\ell}\right) = 0$, i si $t \neq 0$ obtenim

$$\left(\frac{t(u-t)}{\ell}\right) = \left(\frac{-t^2}{\ell}\right)\left(\frac{1-ut^{-1}}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{1-ut^{-1}}{\ell}\right) = (-1)^{\varepsilon(\ell)}\left(\frac{1-ut^{-1}}{\ell}\right)$$

per tant obtenim

$$(-1)^{\varepsilon(\ell)} y^2 = \sum_{u \in \mathbb{F}_\ell} C_u \omega^u$$

on $C_u = \sum_{t \in \mathbb{F}_\ell^*} \left(\frac{1-ut^{-1}}{\ell}\right)$. Tenim $C_0 = \sum_{t \in \mathbb{F}_\ell^*} \left(\frac{1}{\ell}\right) = \ell - 1$. Per $u \neq 0$ tenim que

$$\{1 - ut^{-1} | t \in \mathbb{F}_\ell^*\} = \{k | k \in \mathbb{F}_\ell \setminus \{1\}\},$$

per tant $C_u = -\left(\frac{1}{\ell}\right) + \left(\sum_{k \in \mathbb{F}_\ell} \left(\frac{k}{\ell}\right)\right) = -\left(\frac{1}{\ell}\right) + \left(\sum_{k \in \mathbb{F}_\ell^*} \left(\frac{k}{\ell}\right)\right) = -\left(\frac{1}{\ell}\right) + 0 = -1$ on en la penúltima igualtat usem que $(\mathbb{F}_\ell^* : (\mathbb{F}_\ell^*)^2) = 2$, per tant

$$(-1)^{\varepsilon(\ell)} y^2 = \ell - 1 - \sum_{u \in \mathbb{F}_\ell^*} \omega^u = \ell,$$

on l'última igualtat prové de ser $\omega \neq 1$ complint $0 = \omega^\ell - 1 = (\omega - 1)(\omega^{\ell-1} + \ldots + \omega + 1)$.

Demostrem **B**. Com estem en característica $p > 0$ i senar: $y^p = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \omega^{xp} = *$ i com $mcd(p, \ell) = 1$ tenim

$$* = \sum_{z \in \mathbb{F}_\ell} \left(\frac{zp^{-1}}{\ell}\right) \omega^z = \left(\frac{p^{-1}}{\ell}\right) y = \left(\frac{p}{\ell}\right) y$$

on en l'última igualtat usem que si $p$ quadrat en $\mathbb{F}_\ell$ si i només si $p^{-1}$ també ho és.

Veiem de les igualtats **A, B** com obtenir la llei de reciprocitat quadràtica de Gauss.

De la propietat **A** obtenim

$$\left(\frac{(-1)^{\varepsilon(\ell)}\ell}{p}\right) = ((-1)^{\varepsilon(\ell)}\ell)^{(p-1)/2} = y^{p-1}$$

i de la propietat **B** $y^{p-1} = \left(\frac{p}{\ell}\right)$ i per tant

$$\left(\frac{(-1)^{\varepsilon(\ell)}}{\ell}\right)\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)$$

ara usant el lema anterior del càlcul dels simbols de Legendre $\left(\frac{\pm 1}{\ell}\right)$ finalitza la demostració. □

**Observació 1.1.42.** *Fixem-nos que tenim per l'anterior llei de reciprocitat:*

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$$

*per tant 29 no és un quadrat en* $\mathbb{Z}/(43) = \mathbb{F}_{43}$*, en particular* $X^2 + 43Y^m = 29$ *no té solució a* $\mathbb{Z}$ *ja que no en té en fer quocient per ideal* $(43)$*.*

## 1.2 Exercicis dels continguts del capítol.

### 1.2.1 Resolució de sistemes lineals sobre un domini d'ideals principals: "PAQ-reducció" en dips?

1. Existeixen solucions enteres de l'equació

   $$a_1x_1 + \ldots + a_nx_n = a$$

   on els $a$'s són enters i $a_1 \cdot \ldots \cdot a_n \neq 0$ si i nomes si el màxim comú divisor de $a_1, \ldots, a_n$ divideix $a$.

2. Existeixen solucions enteres de l'equació

   $$a_1x_1 + \ldots + a_nx_n = a$$

   on els $a$'s són elements en $\mathbb{F}_q[T]$ (anell de polinomis en $T$ en el cos finit $\mathbb{F}_q$ de $q$ elements) i $a_1 \cdot \ldots \cdot a_n \neq 0$ si i nomes si el màxim comú divisor de $a_1, \ldots, a_n$ divideix $a$.

3. Trobeu les solucions enteres (en funció d'una de trobada) de l'equació

   $$a_1x_1 + a_2x_2 = a$$

   on $a, a_1, a_2$ són enters amb $gcd(a_1, a_2)$ dividing $a$. Apliqueu-ho per a trobar les solucions enteres de l'equació:

   $$2012x + 24y = 40.$$

   Sabeu trobar totes les solucions a $\mathbb{F}_{121}[T]$ de l'equació

   $$Tx + (T^2 + 1)x = 10?$$

4. Doneu un argument per a trobar totes les solucions enteres de l'equació

   $$a_1x_1 + \ldots + a_nx_n = a$$

   on els $a$'s són enters i $a_1 \cdot \ldots \cdot a_n \neq 0$ amb $mcd(a_1, \ldots, a_n)|a$. Apliqueu-ho en resoldre a $\mathbb{Z}$ l'equació diofantina lineal:

   $$3x + 2y + 2z + 4t = 0.$$

5. Recordeu ara el teorema de classificació de mòduls sobre DIP's, en particular sobre $\mathbb{Z}$, on donada $A \in M_{m,n}(\mathbb{Z})$ existeix $L \in SL_m(\mathbb{Z}) := \{M \in M_m(\mathbb{Z}) | det(M) \in \{\pm 1\}\}$ i $M \in SL_n(\mathbb{Z})$ complint

$$LAM = D = diag(d_1, \ldots, d_s, 0, \ldots, 0)$$

on $D$ és una matriu diagonal on $d_i > 0$ enters amb $d_i | d_{i+1}$ per $i = 1, \ldots, s-1$.

Considerem el sistema lineal

$$A.x = b \tag{1.6}$$

amb $A \in M_{m,n}(\mathbb{Z})$, $b \in M_{n,1}(\mathbb{Z})$ i busquem de trobar les solucions $x \in M_{n,1}(\mathbb{Z})$.

   (a) Suposem que (1.6) té solució a $\mathbb{Z}^n$, diem-li $\alpha$. Llavors totes les solucions de (1.6) són donades per

$$\alpha + \{x \in \mathbb{Z}^n | Ax = (0)\}$$

   on (0) denota la matriu columna amb $n$ files amb tots els coeficients zero.

   (b) L'equació (1.6) té solució a $\mathbb{Z}^n$ si i només si l'equació lineal amb $y$: $D.y = L.b$ té solució a $\mathbb{Z}^n$.

   (c) (van der Waerden) L'equació (1.6) té solució a $\mathbb{Z}^n$ si i només si es compleix que per qualsevol vector fila $v \in \mathbb{Q}^n$ complint que $v.A \in \mathbb{Z}^n$ es té llavors que $v.b \in \mathbb{Z}$.

   (d) Resoleu el sistema d'equacions a $\mathbb{Z}^n$ amb $A = \begin{pmatrix} 2 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix}$ i $b = \begin{pmatrix} 17 \\ -13 \end{pmatrix}$.

   (e) Resoleu el sistema d'equacions a $\mathbb{Z}^n$ amb $A = \begin{pmatrix} 8 & 3 & 2 & 3 \\ 4 & 3 & 4 & 12 \end{pmatrix}$ i $b = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$.

### 1.2.2 Resolució d'equacions de grau 2, primera part

1. Troba totes les solucions de $x^2 + y^2 = z^2$ amb $(x, y, z) \in \mathbb{F}_q[T]^3$ on $\mathbb{F}_q$ és el cos de $q$-elements amb $q = p^n$ amb $p$ primer senar i $n \geq 1$ natural.

2. Troba totes les solucions de $x^2 + y^2 = z^2$ amb $(x, y, z) \in \mathbb{F}_{2^n}[T]^3$ on $\mathbb{F}_{2^n}$ denota el cos finit amb $2^n$ elements, $n \geq 1$ natural.

3. (**) Considera l'equació en les variables $X, Y$ a $\mathbb{F}_q[T]$: $X^2 - f(T)Y^2 = 1$ on $f(T)$ un polinomi irreductible de $\mathbb{F}_q[T]$. Té solució l'equació a $\mathbb{F}_q[T]$ amb $XY \neq 0$?

4. Considera l'equació en les variables $X, Y$ en $\mathbb{Z}$: $Y^2 - DX^2 = 4$ amb $D > 0$ natural que no és un quadrat. Demostreu que la solució general $(x, y) \in \mathbb{Z}^2$ és de la forma:
$$\frac{y + x\sqrt{D}}{2} = \pm(\frac{t + u\sqrt{D}}{2})^n$$
per $n$ algun enter on $(u, v) \in \mathbb{N}^2$ és solució de $Y^2 - DX^2 = 4$ amb $u > 0, v > 0$ i component en la variable $X$ minimal respecte el valor absolut usual.

5. Considera l'equació $Y^2 - pX^2 = -1$ amb $p$ un primer congruent amb 1 *mod* 4. Demostreu que té infinites solucions a $\mathbb{Z}$.
Indicació: considera $(U, T)$ la solució entera amb $U$ més petit de $Y^2 - pX^2 = 1$, es té $U \equiv 0, T \equiv 1(mod\ 2)$. Escriu $\frac{T+1}{2} \cdot \frac{T-1}{2} = p(\frac{U}{2})^2$.

6. (*) Considera l'equació $x^4 - x^2y^2 + y^4 = z^2$. Les solucions a $\mathbb{Z}$ de l'equació amb $mcd(x, y) = 1$ són $(x, y)$ pertanyen al conjunt
$$\{(1,0), (-1,0), (0,1), (0,-1), (1,1), (1,-1), (-1,1), (-1,-1)\}.$$
Indicació: escriviu l'equació per $(x^2 - y^2)^2 + x^2y^2 = z^2$ i useu la solució de l'equació $x^2 + y^2 = z^2$.

7. Trobeu 3 quadrats en progressió aritmètica en els enters. Demostreu que no hi ha 4 quadrats en progressió aritmètica en els enters.
Indicació: Sigui $x^2, y^2, z^2, w^2$ aquests 4 quadrats, com $x^2 + z^2 = 2y^2$ i $2z^2 = y^2 + w^2$ obtenim $x^2w^2 = x^2(2z^2 - y^2) = w^2(2y^2 - z^2)$ i per tant $2(x^2z^2 - y^2w^2) = x^2y^2 - w^2z^2$. Escriviu $a = xz$, $yw = b$, $2c = xy + wz$, $2d = xy - wz$ i obteniu la igualtat $a^4 - a^2b^2 + b^4 = (c^2 + d^2)^2$.

8. (**) Sigui $car(\mathbb{F}_q[T]) = p$ amb $p \neq 2, 3$. Hi ha 4 quadrats en progressió aritmètica en $\mathbb{F}_q[T] \setminus \mathbb{F}_q$?

9. Àlgebra de quaternions i equacions diofantines:

**Definició 1.2.1.** *Sigui $K$ un cos amb $car(K) \neq 2$ i $a, b \in K^*$. Denotem per $\left(\frac{a,b}{K}\right)$ el $K$-espai vectorial de dimensió 4 amb base $\{e_0, e_1, \ldots, e_3\}$ dotat pel producte definit via:*

*(a) el producte és $K$-bilineal i té per element neutre $e_0 = 1$,*

*(b) el producte és associatiu i $e_1^2 = ae_0 = a, e_2^2 = b$, $e_1e_2 = -e_2e_1 = e_3$.*

*S'anomena $\left(\frac{a,b}{K}\right)$ l'àlgebra de quaternions de paràmetres $a, b$ sobre $K$.* [8]

**Definició 1.2.2.** *Donat un quaternió $q = x_0 + x_1e_1 + x_2e_2 + x_3e_3$ amb $x_i \in K$, el quaternió $\overline{q} = x_0 - x_1e_1 - x_2e_2 - x_3e_3$ s'anomena el conjugat de $q$. La norma de $q$ és l'element de $K$:*
$$N(q) := q\overline{q} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2.$$

[8] Donat $K$ un cos i $(A, +, *)$ un anell, diem que és una $K$-àlgebra, si $(A, +)$ és un $K$-espai vectorial i l'operació $* : A \times A \to A$ és $K$-bilineal, en particular $(k_1 \circ x_1) * (k_2 \circ x_2) = (k_1 \cdot k_2) \circ (x_1 * x_2)$ on $\cdot$ és el producte de $K$ per tot $k_1, k_2 \in K$ i $x_1, x_2 \in A$.

És fàcil verificar que $\overline{q_1+q_2}=\overline{q}_1+\overline{q}_2$, $\overline{q_1q_2}=\overline{q}_2\overline{q}_1$ i $N(q_1q_2)=N(q_1)N(q_2)$.

(a) Demostreu que són equivalents:
   i. $\left(\frac{a,b}{K}\right)$ és un anell de divisió [9]
   ii. l'equació $X^2-aY^2-bZ^2+abW^2=0$ amb $X,Y,Z,W$ incògnites, no té solucions en $K$ diferent a la $X=Y=Z=W=0$,
   iii. l'equació $aX^2+bY^2=Z^2$ no té solucions en $K$ diferent a $X=Y=Z=0$,
   iv. $\left(\frac{a,b}{K}\right)$ no és isomorf a l'àlgebra de les matrius quadrades $2\times 2$ a coeficients en $K$.

(b) Demostreu que donada $\left(\frac{a,b}{K}\right)$ sempre existeix una extensió finita de cossos separable $L/K$ on

$$\left(\frac{a,b}{L}\right)\cong M_2(L)$$

com a $L$-àlgebres, diem llavors que $\left(\frac{a,b}{K}\right)$ és "split" en $L$.

(c) Demostreu que totes les $K$-àlgebres següents són isomorfes a $M_2(K)$:

$$\left(\frac{a,-a}{K}\right),\left(\frac{a,1-a}{K}\right),\left(\frac{a,b^2}{K}\right)\ i\ \left(\frac{a,1}{K}\right)$$

i demostreu que sol hi ha dues $\mathbb{R}$-àlgebres no isomorfes del tipus $\left(\frac{a,b}{\mathbb{R}}\right)$, amb $a,b\in\mathbb{R}^*$, la que no és $M_2(\mathbb{R})$, és la coneguda $\mathbb{R}$-àlgebra dels quaternions de Hamilton.

### 1.2.3 Congruències i equacions sobre cossos finits

1. Resolt el "desafio matemático de Adolfo Quirós" del desembre 2012 que presentava al diari el Pais. Escrivim el planteig del professor Quirós: un número bonito si cumple exactamente una, y solamente una, de estas tres condiciones:
a) es divisible entre 5,
b) da resto 2 al dividirlo entre 7,
c) la suma de sus cifras es divisible entre 9.

   Por ejemplo el 00037 es bonito porque cumple la condición b pero no las otras dos; sin embargo, el 00324 es feo, ya que cumple las condiciones b y c. De igual forma, podríamos decir que el 00041 y el 00450 son horribles. El primero, porque no cumple ninguna de las tres condiciones; y el segundo, porque es un exagerado y cumple las tres.

   El desafío que se propone es decidir cuántos de los números que participan en el sorteo de Lotería de Navidad (recordad, del 00000 al 99999) son bonitos según el criterio expresado anteriormente.

[9] anell de divisió és un anell no commutatiu $A$ on qualsevol $a\in A-\{0\}$ és invertible amb el producte

2. Considera $\mathbb{Z}[x_1, \ldots, x_n]$ l'anell de polinomis en $n$ variables a coeficients a $\mathbb{Z}$ i $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. És clar que si $\exists \alpha \in \mathbb{Z}^n$ complint $F(\alpha) = 0$ llavors $F(x_1, \ldots, x_n) \equiv 0(modn)$ té solució per a tot $n$. Demostreu que el recíproc és fals en general.
   Indicació: Considera $F(x) = (2x + 1)(3x + 1)$.

3. Considerem el sistema lineal $A.x = b$ amb $A \in M_{m,n}(\mathbb{Z})$, $b \in M_{n,1}$. Existeix $x \in M_{n,1}(\mathbb{Z})$ solució del sistema si i només si els corresponents sistemes de congruències $A.x \equiv b(modn)$ tenen solució per a qualsevol enter positiu $n$.

4. Considera l'equació diofantina $k^4 + 4^k$ amb $k$ natural estrictament més gran que 1.

   (a) Suposem que $k$ és coprimer amb 5 si $k$ és senar. Demostreu usant congruències que mai $k^4 + 4^k$ és un nombre primer.

   (b) Demostreu en general que mai $k^4 + 4^k$ és un nombre primer.

5. **Teorema de Sophie Germain.** Sigui $p$ un primer senar i considerem un altre primer senar $q$ que compleixi simultàneament (i), (ii):

   (i) l'equació $X^p + Y^p + Z^p = 0$ $(modq)$ implica que $x$ o $y$ o $z$ tenen residu zero en dividir-los per $q$
   (ii) l'equació $n^p = p$ $(modq)$ no té solució.

   Demostreu llavors que qualsevol solució entera de $X^p + Y^p = Z^p$ té la propietat que un dels $x, y, z$ és divisible per $p$.

6. Un primer $p$ s'anomena de (Sophie) Germain si $2p + 1$ és també primer. [10] Demostreu que si $p$ és un primer de Germain llavors en cas d'existir solucions $(x, y, z)$ amb $mcd(x, y, z) = 1$ de l'equació de Fermat $X^p + Y^p = Z^p$ s'ha de complir que $p$ divideix $xyz$.

7. Sigui $K$ un cos amb $car(K) = p \neq 2$ on $K \cap \overline{\mathbb{F}}_p = \mathbb{F}_p$. Considera l'equació

$$aX^2 + bY^2 = Z^2 \tag{1.7}$$

   amb $a, b \in \mathbb{F}_p^*$ i $X, Y, Z$ variables a valors en el cos $K$ .

   Demostreu que sempre l'equació (1.7) té solucions en $K$ diferent de $X = Y = Z = 0$ i per tant $\left(\frac{a,b}{K}\right)$ és isomorf a la $K$-àlgebra $M_2(K)$.

   Indicació: Demostreu que en un cos finit tot element és suma de dos quadrats.

8. Considera l'equació

$$aX^2 + bY^2 = Z^2 \tag{1.8}$$

   amb $a, b \in \mathbb{Z} - \{0\}$ no quadrats i $X, Y, Z$ variables a valors en el cos $\mathbb{Q}$. Suposa que $-a/b$ no és un quadrat i que tenim un $p$ primer on $p \nmid a$ i $p||b$ i el símbol de Lagrange $\left(\frac{a}{p}\right) = -1$. Demostreu que l'equació (1.8) sol té la solució $X = Y = Z = 0$, en particular la $\mathbb{Q}$-àlgebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ és un anell de divisió.

[10] Hi ha una conjectura que afirma que hi ha una infinitud de primers de Sophie Germain.

9. Sigui $p$ un primer diferent de 2 i 3. Demostreu que -3 és un quadrat en $\mathbb{F}_p$ si i només si $p \equiv 1 (mod\ 3)$.

# Capítol 2

# Valoracions en cossos. Anàlisi no-arquimedià. Principi de Hasse-Minkowski.

## 2.1 Quants valors absoluts i anàlisis hi ha a $\mathbb{Q}$?

**Definició 2.1.1.** *Sigui $K$ un cos. Un valor absolut de $K$ és una aplicació $|| : K \to \mathbb{R}$ on $\forall x, y \in K$ satisfà:*

1. $|x| \geq 0$,
2. $|x| = 0 \Leftrightarrow x = 0$,
3. $|xy| = |x| \cdot |y|$,
4. $|x + y| \leq |x| + |y|$, *ó,* $|x + y| \leq max(|x|, |y|)$.

*Un valor absolut $||$ s'anomena arquimedià si $|x + y| \leq |x| + |y|$, i s'anomena no-arquimedià si $|x + y| \leq max(|x|, |y|)$.*

**Observació 2.1.2.** *Es té $|1| = |1 \cdot 1| = |1| \cdot |1|$ i de $1 \neq 0$ tenim $|1| \neq 0$ d'on $|1| = 1$.*

**Observació 2.1.3.** *Si $K \subset \mathbb{C}$, la restricció a $K$ del valor absolut usual de $\mathbb{C}$ és valor absolut arquimedià de $K$.*

**Exemple 2.1.4.** *Al valor absolut en $K$ on $|x| = 1$ $\forall x \in K^*$ i $|0| = 0$ s'anomena el valor absolut trivial de $K$.*

**Lema 2.1.5.** *Sigui $||$ valor absolut de $K$. Llavors, $||$ és no arquimedià, si i només si $\exists c \in \mathbb{R}$ on $|n| < c$ $\forall c \in \mathbb{N}$.*

*Demostració.* Suposem primer que $|$ és no arquimedià. Llavors $|n| = |1 + \ldots + 1| \leq |1|$ on tenim la fita.

Suposem que existeix $c$ i demostrem que correspon a un valor absolut no-arquimedià. Sigui $x, y \in K$ i $k \geq 1$ natural, usant el binomi de Newton i la desigualtat triangulat obtenim:

$$|x+y|^k \leq \sum_{j=0}^{k} |\begin{pmatrix} k \\ j \end{pmatrix}| |x|^j |y|^{k-j} \leq \sum_{j=0}^{k} |\begin{pmatrix} k \\ j \end{pmatrix}| max(|x|,|y|)^k \leq c(k+1) max(|x|,|y|)^k$$

per tant obtenim

$$|x+y| \leq c^{1/k}(k+1)^{1/k} max(|x|,|y|),$$

i observem el límit quant $k$ tendeix a $\infty$ de $c^{1/k}(k+1)^{1/k}$ és 1, obtenint que $||$ és no-arquimedià. □

**Observació 2.1.6.** *Sigui $K/\mathbb{Q}$ una extensió finita i $\sigma : K \hookrightarrow \mathbb{C}$, definim llavors per $x \in K$ el valor absolut $|x|_\sigma := |\sigma(x)|$ on l'últim és el valor absolut usual a $\mathbb{C}$, on $|x|_\sigma^2 = \sigma(x)\overline{\sigma(x)}$ on $\overline{s}$ denota la conjugació complexa per $s \in \mathbb{C}$. Es té $||_\sigma$ és un valor absolut arquimediana.*

**Definició 2.1.7.** *$K$ un cos i $(\Gamma, +)$ grup abelià totalment ordenat per una relació $\leq$, on $O_\Gamma$ és l'element neutre del grup $(\Gamma, +)$[1]. Una aplicació $v : K^* \to \Gamma$ s'anomena una valoració de $K$ en $\Gamma$ quant $\forall x, y \in K^*$ amb $x + y \neq 0$ tenim,*

1. *$v(xy) = v(x) + v(y)$,*
2. *$v(x + y) \geq min(v(x), v(y))$,*

*i s'entén la valoració a $K$ escrivint $v(0) = +\infty$ (on s'estén $\Gamma$ a un monoid totalment ordenat $\Gamma \cup \{+\infty\}$ via les regles usuals $+\infty > \gamma$, $(+\infty) + (+\infty) = (+\infty)$, $\gamma + (+\infty) = (+\infty)$).*
*La imatge de $v$ s'anomena el grup de valors de $\Gamma$.*

**Exemple 2.1.8.** *$K$ un cos, $v(x) = 0_\Gamma$, $\forall x \in K^*$ és una valoració de $K$ anomenada valoració trivial.*

**Proposició 2.1.9.** *$K$ un cos, $v : K \to \Gamma \cup \{+\infty\}$ valoració no trivial. Denotem per $A_v := \{x \in K : v(x) \geq 0_\Gamma\}$. Llavors $A_v$ és un anell local (és dir un anell amb un sol hi ha un ideal maximal), amb ideal maximal $\mathfrak{B}_v := \{x \in K : v(x) > 0_\Gamma\}$, a més $K$ és el cos de fraccions de $A_v$. L'anell $A_v$ s'anomena l'anell de la valoració $v$, i $\mathfrak{B}_v$ l'ideal associat a la valoració $v$, el cos $A_v/\mathfrak{B}_v$ s'anomena el cos residual associat a la valoració.*

*Demostració.* Per demostrar $A_v$ és local és suficient demostrar que $A_v \setminus \mathfrak{B}_v = \{x \in K : v(x) = 0_\Gamma\} = (A_v)^*$.
Si $u \in (A_v)^*$, tenim $v(u) + v(u^{-1}) = v(1) = 0_\Gamma$ i com $v(u), v(u^{-1}) \geq 0$ ja que $u, u^{-1} \in A_v$ obtenim $v(u) = 0_\Gamma$. Reciprocament, si $a \in A_v$ amb $v(a) = 0_\Gamma$, és clar $a^{-1} \in K$ i compleix $v(a^{-1}) = v(a) + v(a^{-1}) = 0_\Gamma$ on $a^{-1} \in A_v$.

Veiem finalment que $Quot(A_v) = K$. Sigui $x \in K$ amb $x \notin A_v$, en particular $v(x) < 0_\Gamma$ i per tant $v(x^{-1}) > 0_\Gamma$ i per tant $x^{-1} \in A_v$, per tant $x \in Quot(A_v)$. □

[1] És dir $\Gamma$ té una relació totalment ordenada $\leq$ complint que $\forall x, y, z$ amb $x \leq y$ llavors $x + z \leq y + z$

**Proposició 2.1.10.** *Sigui $A$ un domini d'integritat. Llavors, $A$ és un anell de valoració per certa $v$ si i només si $\forall x \in Quot(A)$ $x \neq 0$ es té $x \in A$ o bé $x^{-1} \in A$.*

*Demostració.* Demostrem la impricació no trivial, és dir $\forall x \in Quot(A)$ $x \neq 0$ es té $x \in A$ o bé $x^{-1} \in A$ llavors $A$ és anell de certa valoració $v$.

Denotem la projecció epimorfisme natural de grups $v = proj : K^* \to K^*/A^* = (\Gamma, *)$ via $\alpha \mapsto [\alpha]$. Veiem $\Gamma$ té estructura de grup totalment ordenat via:

$$v(x) \leq v(y) \Leftrightarrow yx^{-1} \in A$$

Exercici: comproveu que $\leq$ no depen dels representats triats i $\leq$ compleix les propietats: reflexiva, transitiva, antisimètrica, i d'ordre (i.e. donats $x, y$ sempre $v(x) \leq v(y)$ ó $v(y) \leq v(x)$).
Observeu que $\leq$ és compatible amb l'estructura de grup, ja que $(yz)(xz)^{-1} = yx^{-1}$ on $v(x) \leq v(y)$ equival a $v(xz) \leq v(xy)$.
Per finalitzar sol falta demostra $v(x+y) \geq min(v(x), v(y)$: és clar si $x + y = 0$, suposem ara $x, y, x+y \in K^*$ i sense pèrdua de generalitat podem pensar $v(x) \leq v(y)$ i equivalentment $yx^{-1} \in A$. Per tant $(x + y)x^{-1} = 1 + yx^{-1} \in A$, d'on $v(x) \leq v(x + y)$. □

**Observació 2.1.11.** *Donat un domini $A$ amb $\mathfrak{p}$ un ideal primer, la localització del domini $A$ a $\mathfrak{p}$ obtenim un anell local amb cos de fraccions el cos $K = Quat(K)$. Per tant tenim la manera de construir molts anells locals. Veieu appèndix per la definició de localització d'un domini, propietats i com la relació d'anell local és molt més dèbil que ser anell de valoració on exigim que $x$ o $x^{-1}$ pertany a l'anell local.*

**Definició 2.1.12.** *Una valoració $v$ s'anomena real quant $\Gamma = Imatge(v)$ és isomorf com a grup ordenat a un subgrup de $(\mathbb{R}, +)$. Una valoració $v$ s'anomena discreta quant $\Gamma = Imatge(v)$ és isomorf com grup ordenat a $(\mathbb{Z}, +)$, i en aquest últim cas $A_v$ s'anomena un anell de valoració discreta.*

**Proposició 2.1.13.** *Sigui $A$ un anell de valoració discreta associat a $v : K = Quot(A) \to \mathbb{Z} \cup \{+\infty\}$. Llavors $A$ és un domini d'ideals principal.*

*Demostració.* Sigui $\mathfrak{a} \subseteq A$ ideal, i triem $a \in \mathfrak{a}$ amb $v(a)$ mínima. Afirmem $\mathfrak{a} = (a)$, per això considera $b \in \mathfrak{a}$, d'on

$$v(ba^{-1}) = v(b) - v(a) \geq 0$$

per tant $ba^{-1} \in A$ i d'aquí $b \in aA = (a)$. □

**Proposició 2.1.14.** *Sigui $K$ un cos arbitrari. Els anells de valoració discreta no-trivials del cos $K$ corresponen als subanells de $K$ que són locals i dominis d'ideals principals i amb cos de fraccions $K$.*

*Demostració.* Ja hem vist que si $A$ és anell de valoració discreta no-trivial de $K$ tenim que $A$ és un anell local amb cos de fraccions $K$ i $A$ és domini d'ideals primers. Veiem el recíproc.

Sigui $A \subset K$ local amb ideal maximal $\mathfrak{m} = (\pi)$. Fixem-nos que $\mathfrak{m}^n = (\pi^n)$ per $n$ natural, i si $x \in \mathfrak{n} \cap \mathfrak{m}^l$ tenim $x = \pi^n a_n = \pi^l a_l$ amb $a_i \in A$ amb $n \leq l$ per

tant $0 = \pi^n(a_n - \pi^{l-n}a_l)$ i per ser domini $a_n = \pi^{l-n}a_l \in (\pi^l)$ on $x \in \mathfrak{m}^l$, per tant $\mathfrak{m}^k \setminus \mathfrak{m}^{k+1} = \{a\pi^k | a \in A \setminus (\pi)\}$ amb $k \geq 0$. Això permet definir

$$v : A \to \mathbb{N}$$

via $v(a) = i$ on $a \in \mathfrak{m}^i \setminus \mathfrak{m}^{i+1}$.

Si $x \notin A$ i com $Quot(A) = K$ podem escriure $x = \frac{a}{b}$ amb $a, b \in A$, amb $b \in \mathfrak{m}$, escrivim $b = \pi^j b'$ amb $b' \in A \setminus (\pi)$, $a = \pi^u a'$ amb $a' \in A \setminus (\pi)$, per ser $A$ domini en $Quot(A)$ tenim que $u < j$ i podem pensar $x = \frac{a'}{b'\pi^{j-u}}$, i per tant $x^{-1} = \frac{b'\pi^{j-u}}{a'}$ ara com $a' \in A \setminus \mathfrak{m} = A^*$ obtenim que $x^{-1} \in A$, d'on $A$ és un anell de valoració. I llavors és fàcil extendre $v$ a una valoració de $K$ discreta. □

**Observació 2.1.15.** *Podem també caracteritar anells de valoració discreta amb la condició de noetherià. Anells noetherians són molt generals i són anells claus en geometria algebraica, i geometria aritmètica. On $A$ és anell noetherià si i només si tot ideal de $A$ és finit generat. Exemple d'anells noetherians són anells de la forma $k[x_1, \ldots, x_n] \subset B$ amb $k$ cos i $x_i \in B$ on $B$ un domini. Quocients d'anells noetherians i localitació d'anells noetherians són anells noetherians.*

**Exemple 2.1.16.** *Considera $K = \mathbb{Q}$. Definim per cada $p$ primer,*

$$v_p : \mathbb{Q}^* \to \mathbb{Z}$$

*on $\frac{a}{b} = p^j \frac{a'}{b'}$ amb $a, b, a', b' \in \mathbb{Z}$ on $p \nmid a'b'$ i $v_p(\frac{a}{b}) = j$ és una valoració discreta de $\mathbb{Q}$.*
*Fixem-nos que $A_{v_p} = \{\frac{a}{b} \in \mathbb{Q} | v_p(\frac{a}{b}) \geq 0\} = \{\frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z},\ mcd(a, b) = 1,\ p \nmid p\}$. Tenim $A_{v_p}$ és un domini d'ideals principals i també s'anota per $\mathbb{Z}_{(p)}$ on aquesta última notació bé de localitzar l'anell $\mathbb{Z}$ en el primer $(p)$, veieu §2.2 per detalls en localització d'un anell per un ideal primer.*

**Exemple 2.1.17.** *Considera $K = F(T)$ el cos de fraccions de l'anell de polinomis $F[T]$ en la variable $T$ sobre un cos $F$. Considera per cada $f(T) \in F[T]$ irreductible,*

$$v_{f(T)} : F(T)^* \to \mathbb{Z}$$

*on $v_{f(T)} = v_{f(T)}(\frac{a}{b} = \frac{f(T)^i a'}{b'}) = i$ és una valoració discreta de $F(T)$ on $a, b, a', b' \in F[T]$ amb $mcd(f(T), a'b') = 1$. Considerem també*

$$v_{1/T} : F(T)^* \to \mathbb{Z}$$

*definit via $v_{1/T}(\frac{a}{b}) = -(deg_T(a) - deg_T(b))$ on $a, b \in F[T]$ amb $mcd(a, b) = 1$, és també una valoració discreta de $F(T)$.*

**Lema 2.1.18.** *Sigui $K$ un cos i $v : K \to \mathbb{R} \cup \{+\infty\}$ una valoració. Per a qualsevol número real $c > 1$ l'aplicació $||_v : K \to \mathbb{R}_{\geq 0}$ definida via $|x|_v := c^{-v(x)}$ defineix un valor absolut no-arquimedià de $K$.*

*Demostració.* Obviament $|x|_v \geq 0$ i $|xy|_v = |x|_v|y|_v$. I observem

$$|x + y|_v = c^{-v(x+y)} \leq c^{-min(v(x),v(y))} = max\{c^{-v(x)}, c^{-v(y)}\} = max\{|x|_v, |y|_v\}.$$

□

**Exemple 2.1.19.** *De l'exemple 2.1.16 per $K = \mathbb{Q}$, el valor absolut $|x|_p = \frac{1}{p^{v_p(x)}}$ s'anomena el valor absolut p-àdic, i en particular $d(x, y) = |y - x|_p$ defineix una distància en $\mathbb{Q}$.*

**Definició 2.1.20.** *Dos valors absoluts de $K$, $||_1$, $||_2$ són equivalents si $\forall x \in K$ és equivalent $|x|_1 < 1$ i $|x|_2 < 1$.*

**Proposició 2.1.21.** *Siguin $||_1$, $||_2$ dos valors absoluts no trivials de $K$ equivalents. Llavors $\exists \beta > 0$ real on $|x|_2 = |x|_1^\beta$ $\forall x \in K$.*

*Demostració.* Com són no-trivials $\exists x_0 \in K$ amb $|x_0|_1 > 1$. Triem $\beta \in \mathbb{R}$ complint $|x_0|_1^\beta = |x_0|_2$, i com $|x_0|_2 > 1$ del fet que ambdos valors absoluts són equivalents tenim que $\beta > 0$.

Sigui $x \in K \setminus \{0\}$ un element arbitrari de $K$. Tenim que $|x|_1 = |x_0|_1^s$ per cert $s \in \mathbb{R}$. Elegim una successió d'enters $\{m_i\}$, $\{n_i\}$ amb $n_i > 0$ amb $s = \lim_{i\to\infty} \frac{m_i}{n_i}$ amb $\frac{m_i}{n_i} > s$ $\forall i$, per tant $|x|_1 = |x_0|_1^s < |x_0|_1^{m_i/n_i}$ perquè $|x_0| > 1$. D'on obtenim,

$$|x^{n_i}/x_0^{m_i}|_1 < 1, \text{ d'on } |x^{n_i}/x_0^{m_i}|_2 < 1, \text{ per tant } |x|_2 < |x_0|_2^{m_i/n_i}, \text{ d'on } |x|_2 \leq |x_0|_2^s.$$

Argumentant però amb $\{m_i'\}$, $\{n_i'\}$ successió d'enters amb $n_i' > 0$ amb $\frac{m_i'}{n_i'} < s$ $\forall i$, obtenim que $|x|_2 \geq |x_0|^s$. Per tant obtenim

$$|x|_2 = |x_0|_2^s = |x_0|_1^{\beta s} = |x|_1^\beta.$$

□

**Corol·lari 2.1.22.** *Dos valors absoluts $||_1$ i $||_2$ de $K$ són equivalents si i només si defineixen la mateixa topologia.*

*Demostració.* Suposem que $|x|_1 = |x|_2^r$ per cert $r \in \mathbb{R}_{>0}$. Denotem per $B_\epsilon(y)_i$ la bola oberta en la topología $i$ del valor absolut $||_i$ centrada en $y$ amb radi $\epsilon$. Llavors tenim

$$B_\epsilon(y)_1 = B_{\epsilon^{1/r}}(y)_2;$$

per tot $\epsilon > 0$ i $y \in K$, per tant tenim les mateixes boles obertes en les dos topologies.

Suposem ara que els dos valors defineixen la mateixa topología, veiem que ambdos valors són equivalents. Considera la bola oberta $B_1(0)_1$, existeix una bola $B_\epsilon(0)_2 \subseteq B_1(0)_1$, e inversament existeix una bola oberta $B_{\epsilon'}(0)_1 \subseteq B_1(0)_2$. En particular per la elecció de $\epsilon, \epsilon'$ tenim $|y|_2 < \epsilon \Rightarrow |y|_1 < 1$, i $|z|_1 < \epsilon' \Rightarrow |z|_2 < 1$. Per tant veiem la relació amb les boles de radi unitat; sigui $y$ amb $|y|_2 < 1$, llavors existeix $n$ natural amb $|y^n|_2 < \epsilon$ i per tant $|y^n|_1 < 1$ d'on $|y|_1 < 1$ i similarment obtenim que si $|z|_1 < 1$ s'obté que $|z|_2 < 1$ obtenint que ambdos valors absoluts són equivalents. □

**Lema 2.1.23.** *Els valors absoluts no-trivials de $\mathbb{Q}$ $||_p$ amb $p$ primer i $|| = ||_\infty$ el valor absolut arquimedià usual, són dos a dos no-equivalents.*

*Demostració.* Sigui $p$, $\ell$ dos primers diferents és clar que són no equivalents ja que $|p|_p = 1/p < 1$ i $|p|_\ell = 1$. □

**Observació 2.1.24.** *Pel cos $K = \mathbb{F}_q(T)$, cos de fraccions de l'anell de polinomis en una variable $\mathbb{F}_q[T]$ on $\mathbb{F}_q$ un cos finit tenim les següents valoracions no-equivalents (demostreu-ho pel lector interessat): $|*|_\infty = q^{-v_{1/T}(*)}$, i per cada $f \in \mathbb{F}_q[T]$ irreductible $|*|_f := q^{-v_f(*)}$.*

**Teorema 2.1.25.** *Tot valor absolut arquimedià a $\mathbb{Q}$ és equivalent a $||_\infty$. Tot valor absolut no-trivial i no-arquimedià de $\mathbb{Q}$ és equivalent a $||_p$ (valor absolut p-àdic) per cert p primer.*

*Demostració.* Sigui $||$ un valor absolut de $\mathbb{Q}$.
Considera $m, n \in \mathbb{N}$ i escrivim $m$ en la base $n$:

$$m = \sum_{i=0}^{t} a_i n^i$$

amb $a_i \in \{0, \dots, n-1\}$ amb $a_t \neq 0$. Obtenim:

$$|m| \leq \sum_{i=0}^{t} |a_i||n|^i \leq \sum_{i=0}^{t} |a_i| max(1, |n|)^i \leq \sum_{i=0}^{t} |a_i| max(1, |n|)^t,$$

i de $|a_i| \leq a_i|1| < n$, d'on obtenim:

$$|m| \leq (t+1)n \cdot max(1, |n|)^t \leq (1 + \frac{logm}{logn})n \cdot max(1, |n|)^{\log(m)/\log(n)}, \quad (2.1)$$

del fet que $t \leq \frac{\log(m)}{\log(n)}$. Canviem $m$ per $m^k$ amb $k > 0$ i elevant a $1/k$ l'expressió (2.1) obtenim

$$|m| \leq (1 + \frac{k\log(m)}{\log(n)})^{1/k} n^{1/k} max(1, |n|)^{\log(m)/\log(n)},$$

i fent $k \to +\infty$ obtenim

$$|m| \leq max(1, |n|)^{\log(m)/\log(n)} \quad (2.2)$$

$\forall m, n > 1$ naturals.

**Cas A:** per tot natural $n > 1$ compleix $|n| > 1$:
tenim llavors que l'equació (2.2) es reescriu via $|m|^{1/\log(m)} \leq |n|^{1/\log(n)}$ e intercanviant els paper de $n$ i $m$ obtenim

$$|m|^{1/\log(m)} = |n|^{1/\log(n)} = c$$

no depen del natural i per tant $|n| = c^{\log(n)}$ per a tot natural $> 0$.

Donat ara $\frac{n}{m} \in \mathbb{Q}$ tenim $|\frac{n}{m}| = c^{\log(n/m)}$ i si escrivim $c = e^a > 1$ per cert $a > 0$ real, obtenim que $|x| = |x|_\infty^a$ i per tant $||$ és equivalent a $||_\infty$.

**Cas B:** existeix un natural $n > 1$ tal que $|n| \leq 1$:
Fixem aquest $n$, on $max(1, |n|) = 1$ i de l'equació (2.2) obtenim $|m| \leq 1$ per tot enter positiu, per tant pel lema 2.1.5 $||$ és no-arquimedià.

Denotem $A := \{x \in \mathbb{Q} : |x| \leq 1\}$ i $\mathfrak{b} := \{x \in \mathbb{Q} : |x| < 1\}$, i com $|x + y| \leq max(|x|, |y|)$ tenim que $A$ és un anell, i és fàcil demostrar que $\mathfrak{b}$ és l'únic ideal maximal de $A$, ja que $A^* = A \setminus \mathfrak{b}$. A més tenim $\mathbb{Z} \subset A$.

Considerem $\mathfrak{b} \cap \mathbb{Z}$ un ideal de $\mathbb{Z}$ (que és principal de ser $\mathbb{Z}$ un domini ideals primer). Si $\forall p$ primer de $\mathbb{Z}$ complís $|p| = 1$ llavors pel teorema principal de l'aritmètica i la propietat multiplicativa del valor absolut obtenim $|n| = 1$ per tot natural $n$ i obtenim $|\frac{n}{m}| = 1$ i és el valor absolut trivial.

Per tant existeix $p$ primer amb $|p| < 1$, d'on $(p) \subset \mathfrak{b} \cap \mathbb{Z}$. Si existís un altre primer $p_2$ complint $|p_2| < 1$ obtenim $1 \in \mathbb{Z} = (p, p_1) \subset \mathfrak{b} \cap \mathbb{Z}$, d'on $\mathfrak{b} = A$ cosa que no pot ser. Com $(p)$ és ideal maximal de $\mathbb{Z}$ ha de complir $(p) = \mathfrak{b} \cap \mathbb{Z}$.

Considera $m \in \mathbb{Z} \setminus p\mathbb{Z}$, tenim $m \notin \mathfrak{b}$ on $|m| = 1$ i $|\frac{m}{m}p^f| = |p|^f$ amb $f \in \mathbb{Z}$, $(m, n) = 1 = (mn, p)$. □

Observem en $\mathbb{Q}$ que $|x|_\infty = max\{x, -x\}$ i $|p|_p := \frac{1}{p}$, i per un anell commutatiu $A$ denotem

$$Spec_{max}(A) := \{ideals\ maximals\ de\ A\}.$$

**Corol·lari 2.1.26** (Fórmula del producte)**.** *Per $x \in \mathbb{Q}\setminus\{0\}$, els $\ell \in Spec_{max}(\mathbb{Z})$ on $|x|_\ell \neq 1$ és finit i es compleix*

$$\prod_{\ell \in Spec_{max}(\mathbb{Z}) \cup \{\infty\}} |x|_\ell = 1.$$

## 2.2 Completació d'un cos amb ||

Denotem per $(K, ||)$ un cos $K$ amb un valor absolut $||$.

Una successió $\{a_n\}_{n\geq 0}$ una successió d'elements en $K$, diem que és de Cauchy si $\forall \epsilon > 0$, $\exists n_0(\epsilon)$ on $\forall m \geq n \geq n_0(\epsilon)$ es té $|a_m - a_n| < \epsilon$.

Una successió es diu que és convergent de límit $a \in K$ si $\forall \epsilon > 0$ $\exists n_0(\epsilon)$ on $\forall n \geq n_0(\epsilon)$ es satisfà $|a_n - a| < \epsilon$.

(És fàcil observat que tota successió convergent és de Cauchy, i que tota successió de Cauchy és fitada).

**Definició 2.2.1.** *Un cos $(K, ||)$ és complet quant tota succesió de Cauchy d'elements de $K$ convergeix a un element de $K$.*

**Observació 2.2.2.** *Un domini $A$ amb $A \subset K$ tancat en $(K, ||)$ podem fer un anàleg dels conceptes anteriors, en particular de successions de Cauchy en $A$, on $(A, ||)$ s'anomena complet si tota successió de Cauchy en $A$ té límit en $A$.*

**Teorema 2.2.3.** *Donat $(K, ||_K)$. Existiex un cos $\hat{K}$ i un valor absolut $||_{\hat{K}}$ complint,*

1. *$(\hat{K}, ||_{\hat{K}})$ és un cos complex amb $||_{\hat{K}}$,*
2. *$K \subset \hat{K}$ i $||_{\hat{K}} : K \to \mathbb{R}_{>0}$ coincideix amb $||_K$,*
3. *$K$ és dens en $\hat{K}$.*
4. *Si $(\hat{K}_1, ||_1)$, $(\hat{K}_2, ||_2)$ són dos cossos que satisfan les propietats anteriors, aleshores existeix un morfisme de cossos únics $\varphi : \hat{K}_1 \to \hat{K}_2$ amb $\varphi_{|_K} = id$ amb $|\varphi(x)|_2 = |x|_1$.*

*La parella $(\hat{K}, ||_{\hat{K}})$ s'anomena una completació de $(K, ||)$ i és única llevat isometria de cossos per l'última propietat.*

*Demostració.* Considera $\mathcal{C}(K)$ el conjunt de successions de Cauchy en el cos $K$. Observem donats $(a_n)_n, (b_n)_n \in \mathcal{C}(K)$, tenim definides les operacions:

$$(a_n)_n + (b_n)_n := (a_n + b_n)_n \in \mathcal{C}(K),$$

$$(a_n)_n * (b_n)_n := (a_n b_n)_n \in \mathcal{C}(K),$$

que doten $\mathcal{C}(K)$ de domini.

Fixem-nos que $K \subset \mathcal{C}(K)$ via donat $k \mapsto (k)_n$ a la successió de Cauchy(i convergent) constant igual a $k$ per tot $n \in \mathbb{N}$.

Denotem per $\mathfrak{M}$ el conjunt de les successions convergents de límit $0 \in K$. Clarament $\mathfrak{M}$ és un ideal de $\mathcal{C}(K)$ (la suma de dos successions convergents a zero és convergent a zero, i el producte d'una successió de Cauchy amb una convergent a zero és una successió convergent a zero). Fixem-nos que $\mathfrak{M}$ és un ideal maximal de $\mathcal{C}(K)$ ja que si $c = (c_n)_n \in \mathcal{C}(K) \setminus \mathfrak{M}$, fixem-nos llavors que per $n \geq n_0$ un natural fix $c_n \neq 0$ (ja que no és convergent a zero) i la successió $(\frac{1}{c_n})_{n \geq n_0}$ és fàcil veure que és una successió de Cauchy i per tant $(c_n)_n \in \mathcal{C}(K)^*$.

Escrivim $\hat{K} := \mathcal{C}(K)/\mathfrak{M}$ el cos que per construcció $K \subset \hat{K}$ on $k \mapsto [(k)_n]$, que és injectiva.

Definim $||_{\hat{K}}$, donat $(x_n)_n \in \mathcal{C}(K)$, via

$$|(x_n)_n|_{\hat{K}} := \lim_{n \to \infty} |x_n|_K \in \mathbb{R},$$

on observem que té sentit ja que la successió de nombres reals $(|x_n|)_n$ és de Cauchy i per tant convergent (efectivament, com $(x_n)_n$ de Cauchy en $K$, tenim $\forall \epsilon > 0\ \exists n_0(\epsilon)$ complint $|x_m - x_{n_0(\epsilon)}| < \epsilon$, on $|x_m| \leq |x_m - x_{n_0(\epsilon)}| + |x_{n_0(\epsilon)}| < \epsilon + |x_{n_0(\epsilon)}|$, d'aquí $|x_m| - |x_{n_0(\epsilon)}| < \epsilon$).

Llavors la tupla $(\hat{K}, ||_{\hat{K}})$ és el cos complet que satisfà les condicions demanades. Exercici al lector.

Demostrem tan sols aquí que $\hat{K}$ és complet amb $||_{\hat{K}}$.

Considerem $(d_n)_n \in \mathcal{C}(\hat{K})$ una successió de Cauchy en $(\hat{K}, ||_{\hat{K}})$. Escrivim $d_m = [(a_{i,m})_i] \in \mathcal{C}(K)$. Fixem-nos que $\forall \epsilon > 0$ i $\forall n, m \geq n_0(\epsilon)$ tenim

$$|d_n - d_m|_{\hat{K}} = \lim_{i \to \infty} |a_{i,n} - a_{i,m}| < \epsilon.$$

Triem $\alpha = [(\alpha_i)_i]$ la successió definida per $\alpha_i := a_{i,n_0(1/10^i)}$ pensant que triem successió creixent de naturals amb $n_0(1/10^i) < n_0(1/10^{i+1})$ (amb límit $+\infty$). És fàcil demostrar que $\alpha \in \hat{K}$. Observeu finalment que donat $\epsilon' > 0$ existeix $i$ on $\epsilon' > \frac{1}{10^i}$ i per tant per $n \geq n_0(1/10^i)$ tenim que $|d_n - \alpha|_{\hat{K}} = \lim_{i \to \infty} |a_{i,n} - a_{i,n_0(1/10^i)}| < \frac{1}{10^i} < \epsilon'\ \forall n \geq n_0(1/10^i)$ obtenint $(d_n)_n$ convergeix en $\alpha \in \hat{K}$. $\square$

Tenim el següent resultat que no demostrarem en aquest curs,

**Teorema 2.2.4** (Ostrowski)**.** *Sigui $K$ cos complet respecte d'un valor absolut arquimedià $||$. Llavors $(K, ||)$ és isomorf (una isometria) a $(\mathbb{R}, ||_\infty)$ ó $(\mathbb{C}, ||_\infty)$.*

Anem a estudiar l'extensió a la completació dels valors absoluts no-arquimediants.

**Proposició 2.2.5.** *Sigui $(K, ||_v)$ on $||_v$ prové d'una valoració $v : K^* \to \mathbb{R}$, és dir $|x|_v = c^{-v(x)}$ amb $c > 1$ un real. Denotem $\hat{K}$ completació de $K$ respecte $||_v$. Llavors existeix una única valoració $\hat{v} : \hat{K}^* \to \mathbb{R}$ que estén $K$ i compleix que la imatge de $\hat{v}$ coincideix amb $\hat{v}$ i $|x|_{\hat{K}} = c^{-\hat{v}(x)}$.*

*Demostració.* Per la noció de valors absoluts equivalents pensem $|*|_v = e^{-v(*)}$ d'on $v(x) = -\log(|x|)$. Considerem la tupla $(\hat{K}, ||_{\hat{K}})$ construïda en teorema 2.2.3 i definim $\hat{v}(\alpha) := \log(|\alpha|_{\hat{K}})$ per $\alpha \in \hat{K}$, on per construcció $\hat{v}$ satisfà les propietats d'aplicació de valoració (de ser valors absoluts no-arquimedians) i per definició $|*|_{\hat{K}} = |*|_{\hat{v}} = e^{-\hat{v}(*)}$. Demostrem ara que $Im(\hat{v}) = Im(v)$ les imatges de les valoracions coincideixen.

Sigui $\alpha \in \hat{K}^*$, $\alpha = [(a_n)_n]$ on $(a_n)_n$ una successió de Cauchy en $K$, (en particular vam demostrar en la demostració del teorema 2.2.3 que $(|a_n|)_n$ és una successió de Cauchy en $\mathbb{R}$ i per tant convergent), on $|\alpha|_{\hat{K}} = \lim_{n\to\infty} |a_n|$. Del fet que ser imatge d'una valoraci'o un grup tenim $\hat{v}(\alpha) \in Im(\hat{v}) \Leftrightarrow \hat{v}(\alpha^{-1}) \in Im(\hat{v})$ podem suposar (canviant $\alpha$ per $\alpha^{-1}$ si cal) que $(|a_n|)_n$ és una successió de nombres reals decreixent.

Veiem que aquesta successió és constant a partir d'un $n$. Si no, agafem-ne una subsuccessió de $(|a_n|)_n$ que sigui estrictament decreixent, és dir $(|a'_n|)_n$ amb $|a'_{n+1}| < |a'_n|$. Fixem-nos de ser un valor absolut no-arquimedià, tenim llavors que $|x+y| = max(|x|, |y|)$ si $|x| \neq |y|$, i per tant,

$$|a'_n - a'_{n+1}|_K = |a'_n|_K$$

prenent limit l'anterior igualtat obtenim: $0 = |\alpha|_{\hat{K}}$ en contradicció. Per tant la successió real $(|a_n|)_n$ és constant a partir d'un $n' \geq n_0$, per tant

$$|\alpha|_{\hat{K}} = |a_{n'}|_K.$$

□

**Corol·lari 2.2.6.** *Sigui $(K, ||_v)$ on $||_v$ prové d'una valoració $v : K^* \to \mathbb{Z}$ discreta. Denotem $(\hat{K}, ||_{\hat{v}})$ completació de $K$ respecte $||_v$. Llavors $\hat{v}$ és una valoració discreta de $\hat{K}$.*

**Definició 2.2.7.** *Considerem $(\mathbb{Q}, ||_p)$. Llavors la completació de $\mathbb{Q}$ respecte el valor absolut p-adic, s'anomena el cos dels nombres p-àdics i escriurem la tupla via $(\mathbb{Q}_p, ||_p)$.*

**Proposició 2.2.8.** *Sigui $A$ un anell de valoració discreta $v$ amb ideal maximal $\mathfrak{p} = \pi A$, i $K = Quot(A)$. Sigui $\hat{K}$ la completació de $K$ respecte la valoració associada a $\mathfrak{p}$. Escrivim:*

$$\hat{A} := \{x \in \hat{K} : |x|_{\hat{v}} \leq 1\},$$

$$\hat{\mathfrak{p}} := \{x \in \hat{A} : |x| < 1\}.$$

*Llavors tenim:*

1. *$\hat{A}$ és un anell de valoració discreta amb ideal maximal $\hat{\mathfrak{p}}$,*
2. *$\forall n \geq 0$ enter tenim $\hat{\mathfrak{p}}^n = \pi^n \hat{A}$,*
3. *$\forall n \geq 1$ tenim un isomorfisme natural $A/\mathfrak{p}^n \cong \hat{A}/\hat{\mathfrak{p}}^n$,*
4. *$\hat{A}$ és complet respecte $||_{\hat{v}}$.*

*Demostració.* Pel corol.lari anterior $\hat{v}$ defineix una valoració discreta de $\hat{K}$ per tant $\hat{A} = \{x \in \hat{K} | v(x) \geq 0\}$ és un anell de valoració discreta amb maximal $\hat{\mathfrak{p}}$.

Pel corol.lari anterior tenim que $\hat{v}(\pi^n) = v(\pi^n)$ per tant per la demostració dels ideals en anells de valoració discretes tenim que $\hat{\mathfrak{p}}^n = \pi^n \hat{A}$.

Què $\hat{A}$ és complet, prové de ser un tancat de l'espai topològic complet $\hat{K}$.

Anem finalment a demostrar $A/\mathfrak{p}^n \cong \hat{A}/\hat{\mathfrak{p}}^n$.

Considerem el morfisme natural $\varphi_1 : A \to \hat{A} \to \hat{A}/\hat{\mathfrak{p}} = k_{\hat{v}}$ de $A$ al cos residual $k_{\hat{v}}$ de la valoració discreta $\hat{v}$. Veiem primer que $\varphi_1$ és epimorfisme. Efectivament, triem $\alpha \in \hat{A} \setminus \mathfrak{p}$, $\alpha = [(a_n)_n] \in \hat{A}$ amb $a_n \in A$, i com $v$ discreta $\exists n \geq n_0$ on $|a_n| = 1$ per $n \geq n_0$ i com $(a_n)_n$ és de Cauchy tenim que $a_{n+1} - a_n \in \pi A$ per $n$ suficientment gran $n \geq n_1$, per tant per $n \geq n_1$ definim $b_n := a_{n_1} + (a_n - a_{n_1})$ on $(a_n - a_{n_1})_n$ és una successió de Cauchy d'elements en $\mathfrak{p}$, per tant pertany a $\hat{\mathfrak{p}}$. D'on la exhaustivitat. Observem que $\mathfrak{p}$ està al nucli de $\varphi_1$ d'on obtenim un epimorfisme

$$A/\mathfrak{p} \to \hat{A}/\hat{\mathfrak{p}}$$

i com són cossos el morfisme anterior és injectiu, per tant isomorfisme.

Suposem $n \geq 2$ i demostrem ara $A/\mathfrak{p}^n \cong \hat{A}/\hat{\mathfrak{p}}^n$. De la demostració per $n = 1$ hem observat que $\hat{A} = A + \hat{\mathfrak{p}}$ on $\hat{\mathfrak{p}} = \pi\hat{A} = \pi A + \pi\hat{\mathfrak{p}} = \pi A + \hat{\mathfrak{p}}^2$.

Similarment $\hat{A} = A + (\pi A + \hat{\mathfrak{p}}^2) = A + \hat{\mathfrak{p}}^2$ i recursivament obtenim que $\hat{A} = A + \hat{\mathfrak{p}}^n$, i mirant els valors en la valoració obtenim que $A \cap \hat{\mathfrak{p}}^n = \mathfrak{p}^n$ d'on el morfisme projecció $\varphi_n : A \to \hat{A}/\hat{\mathfrak{p}}^n$ és epimorfisme amb nucli $\mathfrak{p}^n$. □

**Definició 2.2.9.** *Considerem $\{X_n\}_{n\in\mathbb{N}}$ una col.lecció de conjunts (grups, anells, grups topològics) i aplicacions $\pi_n^{n+1} : X_{n+1} \to X_n$ (respectivament morfisme de grups, anells, ...) es defineix el limit projectiu $(X_n, \pi_n^{n+1})_n$ al conjunt (respectivament grup, anell,grups topològics)*

$$\{(x_i)_i \in \prod_{i\in\mathbb{N}} X_i | \pi_n^{n+1}(x_{n+1}) = x_n \ \forall n \geq 0\} \subset \prod_{i\in\mathbb{N}} X_i,$$

*(amb la topologia induïda per la topologia producte dels $X_i$'s en cas de tenir topologia els $X_i$'s).*

**Proposició 2.2.10.** *Sigui $(K, ||_v)$ un cos amb valor no-arquimedià $v$, valoració discreta. Considera $(\hat{K}, ||_{\hat{v}})$ la completació, i denotem per $\hat{A} := \{x \in \hat{K} | |x|_{\tilde{v}} \leq 1\}$ l'anell de valoració discreta de $\hat{K}$ definit per $\hat{v}$.*

*Llavors:*

1. *$\hat{A}$ coincideix amb el limit projectiu $(A/\mathfrak{p}^n, \pi_n^{n+1})$ on $\pi_n^{n+1}$ és la projecció natural,*

2. *si fixem un subconjunt $R \subset A$ que és un sistema de representants del cos residual $k_v = A/\mathfrak{p}$ i $\pi$ on $\mathfrak{p} = (\pi)$, tot $x \in \hat{K}^*$ es pot escriure de manera única com una serie de Laurent, és dir denotem $n_x := \hat{v}(x) \in \mathbb{Z}$ tenim*

$$x = \sum_{n \geq n_x} r_n \pi^n,$$

*amb $r_n \in \mathbb{R}$ i $r_{n_x} \neq 0$.*

*Demostració.* Del primer apartat, tan sols demostrarem en aquests apunts que $\hat{A} = \lim(A/\mathfrak{p}^n, \pi_n^{n+1})$ com a conjunt.

Sigui $[(a_i)_i] \in \hat{A}$, com $\forall \epsilon = c^{-k} > 0$ amb $k$ enter (on pensem que $|*|_v = c^{-v(*)}$), tenim $|a_i - a_{i_0(\epsilon)}|\epsilon$ i per tant $(a_i - a_{i_0(\epsilon)}) \in \pi^k A$ d'on la successió $(a_i)_i$ és constant per $i \geq i_0(\epsilon)$ en l'anell $A/\mathfrak{p}^k$, i no depen de la classe triada en $\hat{A}$, diem aquest element $\xi_k \in A/\mathfrak{p}^k$, així definim una aplicació:

$$\hat{A} \to A/\mathfrak{p}^n$$

$$[(a_i)_i] \mapsto \xi_k.$$

Per construcció tenim $\pi_k^{k+1}(\xi_{k+1}) = \xi_k$, això defineix

$$\psi : \hat{A} \to \lim(A/\mathfrak{p}^n, \pi_n^{n+1})$$

$$[(a_i)_i] \mapsto (\xi_k)_k.$$

Veiem que tot $(\delta_k)_k \in \lim(A/\mathfrak{p}^n, \pi_n^{n+1})$ construïm una successió de Cauchy en $A$.

Per cada $n$ triem $a_n \in \varphi_n(\delta_n) \subset A$ del epimorfisme $\varphi_n : A \to A/\mathfrak{p}^n$. Fixem-nos que per $m \geq n$ tenim $|a_m - a_n| \leq c^{-n}$ i per tant $(a_n)_n$ és una successió de Cauchy, provant $\psi$ és exhaustiva. Per veure que $\psi$ és injectiva, observem si $\psi([(a_n)_n]) = \psi([(b_n)_n])$ obtenim $\varphi_n(a_m - b_m) = 0$ per $m$ suficientment gran, és dir $|a_m - b_m| \leq c^{-n}$ per $m \geq n_0(n)$ demostrant que en $\hat{A}$ tenim $[(a_n)_n] = [(b_n)_n]$.

Demostrem la segona part de la proposició, és dir que tot element de $\hat{K}^*$ s'escriu com una sèrie de Laurent.

Seguint la notació de l'enunciat tenim $\pi^{-n_0(x)}x \in \hat{A}$ on $\psi(\pi^{-n_0(x)}x) = (\xi_k)_k$.

Com $\hat{A}$ és el límit projectiu de $A/\mathfrak{p}^n$ amb els morfisme projecció natural (i $A/\pi^n = \{\sum_{i=0}^{n-1} s_i\pi^i | s_i \in R\}$) i podem construir una successió d'elements en $A$ via:

$$\{S_0 := r_0, S_1 := r_0 + r_1\pi, \ldots, S_n := r_0 + r_1\pi + \ldots + r_n\pi^n, \ldots\}$$

on $\varphi_{n+1}(S_n) = \delta_{n+1} \in A/\mathfrak{p}^{n+1}$ que és de Cauchy equivalent en $\hat{K}$ amb $\pi^{-n_0(x)}x$, i com $\hat{A}$ complet podem considerar que té límit els $S_n$ s'anota usualment per

$$\pi^{-n_0(x)}x = \sum_{i=0}^{\infty} r_i\pi^i \in \hat{A},$$

d'on el resultat, llevat d'unicitat. Exercici al lector provar-ne la unicitat de la sèrie de Laurent associada a $x$. □

**Observació 2.2.11.** *Observeu que $\mathbb{Z}$ és dip, i per cada ideal primer $(p)$, denotem per $\mathbb{Z}_{(p)}$ la localització de l'anell $\mathbb{Z}$ amb l'ideal primer, en particular tenim del resultat A.0.7 tenim un isomorfisme natural*

$$\{[0], \ldots, [p-1]\} = \mathbb{Z}/p \to^{\cong} \mathbb{Z}_{(p)}/(p).$$

*A més per la valoració p-adica en $\mathbb{Q}$ $v_p$, és dir $(\mathbb{Q}, ||_p)$, tenim que l'anell de valoració de $v_p$ és $A_{v_p} = \mathbb{Z}_{(p)} \subset \mathbb{Q}$ (en la nostra situació), i per tant obtenim d'un resultat anterior en aquesta secció que*

$$A_{v_p}/pA_{v_p} \cong \hat{A_{v_p}}/p\hat{A_{v_p}},$$

*i en el resultat anterior podem agafar el conjunt $R$ com representants els elements de $\mathbb{Z}$ $\{0, \ldots, p-1\}$ per expressar l'anell $\hat{A_{v_p}}$ en sèrie respecte potències de p amb coeficients entre 0 i p-1.*

**Definició 2.2.12.** *Per $(\mathbb{Q}, |*|_p)$ tenim que $\hat{\mathbb{Q}} = \mathbb{Q}_p$ s'anomena el cos p-àdic, $\hat{A}$ els enters p-àdics que denotarem per $\mathbb{Z}_p$, i observem de la proposició anterior que*

$$\mathbb{Q}_p = \{\sum_{i \geq n_0} a_i p^i | 0 \leq a_i \leq p-1, \text{ amb } a_i \in \mathbb{N}, \ n_0 \in \mathbb{Z}\},$$

$$\mathbb{Z}_p = \{\sum_{i \geq 0} a_i p^i | 0 \leq a_i \leq p-1, \text{ amb } a_i \in \mathbb{N}\}.$$

**Observació 2.2.13.** *Sabem $\mathbb{Z} \subset \hat{A}$ sempre i quant el cos de fraccions de $\hat{A}$ és de característica zero. Com $\mathbb{Q}_p$ té característica zero, fixem-nos que descrivim $\mathbb{Z}$ dins $\mathbb{Z}_p$ de manera fàcil si pensem $\mathbb{Z}_p$ com límit projectiu de $\mathbb{Z}/p^n$. Per exemple facilment $-\mathbb{N} \subset \mathbb{Z}_p$ ja que*

$$-1 = (p-1) + (p-1)p + \ldots + (p-1)p^n + \ldots \in \mathbb{Z}_p$$

*on aquesta sèrie la construim mirant el limit projectiu ja que $[-1] = [p^m - 1] \in \mathbb{Z}/p^m$ i $p^m - 1 = (p-1)(1 + p + \ldots + p^{m-1})$.*

## 2.3 Principi local-global: Teorema de Hasse-Minkowski per equacions de grau 2.

Tornem al tema central del curs en resoldre equacions diofantines en un cos $K$, considerem $F(X_1, \ldots, X_n) = 0$ una equació polinomial en un cos $K$, i és clar que si té solució en $K^n$ en té en $(\hat{K}, ||_{\hat{K}})$ per tota completació del cos $K$ pels diferents valors absoluts possibles en el cos $K$.

**Definició 2.3.1.** *Diem que una equació $F(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ amb K cos, satisfà el principi de Hasse: si tenir l'equació $F(X_1, \ldots, X_n) = 0$ solució en tots els completats $(\hat{K}, |*|_{\hat{K}})$ del cos K variant-ne tots els valors absoluts implica que $F(X_1, \ldots, X_n) = 0$ té solución en K.*

En els cursos de càlcul i de mètodes matemàtics heu vist diferents tècniques per donat $F(X_1, \ldots, X_n) = 0$ trobar-ne solucions als nombres reals i calcular-les (potser de forma aproximada). Intentem introduir alguna tècnica per respondre la pregunta amb els nombres $p$-àdics, almenys en el cas d'un polinomi.

**Lema 2.3.2** (de Hensel)**.** *Donat $f \in \mathbb{Z}[X]$ un polinomi en una variable a coeficients enters. Suposem existeixen $k, n \in \mathbb{Z}$ amb $0 \leq 2k < n$ i $x \in \mathbb{Z}$ complint les condicions següents:*

1. $f(x) \equiv 0 (mod\ p^n)$,
2. $f'(x) \equiv 0 (mod\ p^k)$,
3. $f'(x) \not\equiv 0 (mod\ p^{k+1})$.

*Llavors existeix $y \in \mathbb{Z}$ complint les següents condicions:*

1. $y \equiv x (mod\ p^{n-k})$,
2. $f(y) \equiv 0 (mod\ p^{n+1})$,

3. $f'(y) \equiv 0(mod\ p^k)$

4. $f'(y) \not\equiv 0(mod\ p^{k+1})$.

*En particular si $k = 0$, donat $x \in \mathbb{Z}$ i $n \in \mathbb{Z}_{\geq 0}$ on $f(x) \equiv 0(mod\ p^n)$ tenim que $f(y) \equiv 0(mod\ p^{n+1})$ on $y \equiv x(mo\ p^n)$ i $f'(y) \not\equiv 0(mod\ p)$.*

*Demostració.* Escrivim $y := x + zp^{n-k}$, $z$ a trobar-se en $\mathbb{Z}$.

Del teorema de Taylor en polinonomis obtenim:

$$f(y) \equiv f(x) + f'(x)zp^{n-k}(mod\ p^{2n-2k}),$$

ii com $2n - 2k \geq 2n - (n-1) = n - 1$ obtenim llavors que

$$f(y) \equiv f(x) + f'(x)zp^{n-k}(mod\ p^{n+1}). \tag{2.3}$$

Ara usant que $f(x) \equiv 0(mod\ p^n)$, i $f'(x) \equiv 0(mod\ p^k)$ amb $f'(x) \not\equiv 0(mod\ p^{k+1})$ podem escriure (2.3) mitjançant:

$$f(y) \equiv bp^n + ap^k zp^{n-k} \equiv (az + b)p^n(mod\ p^{n+1}),$$

amb $b \not\equiv 0(mod\ p)$ (ja que sino $y = x$ ja estariem) i $a \not\equiv 0(mod\ p)$. Triem $z \in \mathbb{Z}$ complint $z = -a^{-1}b(mod\ p)$, directament tenim $f(y) \equiv 0(mod\ p^{n+1})$.

Usant de nou el teorema de Taylor obtenim:

$$f'(y) \equiv f'(x) + f''(x)zp^{n-k}(mod\ p^{2n-2k}),$$

i com $2n - 2k > n - k \geq 2k + 1 - k = k + 1$ obtenim $f'(y) \equiv f'(x)(mod\ p^{k+1})$, en particular $f'(y) \equiv f'(x) \equiv 0(mod\ p^k)$ i $f'(y) \equiv f'(x) \not\equiv 0(mod\ p^{k+1})$. □

**Corol·lari 2.3.3.** *Sigui $F(X) \in \mathbb{Z}[X]$ amb el màxim comú divisor dels coeficients igual a 1. Suposem que $F(X)$ té una arrel simple fent mòdul $p$ amb $p$ un nombre primer. Llavors $F(X)$ té una arrel simple en $\mathbb{Z}_p$ (en particular en $\mathbb{Q}_p$).*

*Demostració.* Aplicant el lema de Hensel anterior tenim una successió $\alpha_n \in \mathbb{Z}$ complint que $F(\alpha_n) \equiv 0(mod\ p^n)$, $F'(\alpha_n) \not\equiv 0(mod\ p)$ amb $\alpha_{n+1} \equiv \alpha_n(mod\ p^n)$. Per tant existeix

$$\alpha \in \lim(\mathbb{Z}/p^n, proj) \cong \mathbb{Z}_p$$

on $F(\alpha) \equiv F(\alpha_n) \equiv 0(mod\ p^n)$ per tot $n$ natural per tant $F(\alpha) = 0 \in \mathbb{Z}_p$.

Tenim que $F'(\alpha) \in \mathbb{Z}_p$, ara com $F'(\alpha) \equiv F'(\alpha_n) \not\equiv 0(mod\ p^n)$ obtenim $F'(\alpha) \neq 0 \in \mathbb{Z}_p$ i per tant una arrel simple. □

El lema de Hensel té un enunciat més general, que en aquest curs tan sols enunciarem

**Lema 2.3.4** (Hensel)**.** *Sigui $A$ un anell de valoració discreta $v$, $K = Quot(A)$, and $\mathfrak{p}$ ideal maximal de $A$, $\kappa = A/\mathfrak{p}$ cos residual de la valoració i suposem que $K$ és complet amb la valoració $v$. Sigui $F(X) \in A[X]$ un polinomi mònic on*

$$[F(X)] = g(X)h(X) \in \kappa[X]$$

*amb $g, h$ polinomis primers entre si en $\kappa[X]$. Llavors $\exists G(X), H(X) \in A[X]$ amb $[G(X)] = g(X)$, $[H(X)] = h(X)$ en $\kappa[X]$ complint*

$$F(X) = G(X)H(X).$$

**Observació 2.3.5.** Als dominis locals $A$ amb maximal $\mathfrak{p}$ que safisfan: que donat $F(X) \in A[X]$ un polinomi mònic on

$$[F(X)] = g(X)h(X) \in A/\mathfrak{p}[X]$$

amb $g, h$ polinomis primers entre si en $\kappa[X]$, es compleix que $\exists G(X), H(X) \in A[X]$ amb $[G(X)] = g(X)$, $[H(X)] = h(X)$ en $\kappa[X]$ complint

$$F(X) = G(X)H(X),$$

es diu que $A$ és un anell henselià. En particular els anells de valoració discreta són exemples d'anells henselians.

Enunciem el teorema de Hasse-Minkowski general per polinomis de grau 2.

**Teorema 2.3.6** (Hasse-Minkowski)**.** *Considerem una forma quadràtica a coeficients racionals, és dir considerem*

$$f(X_1, \ldots, X_n) := \sum_{i \leq j} a_{i,j} X_i X_j \in \mathbb{Q}[X_1, \ldots, X_n].$$

*Considerem l'equació homogènia $f(X_1, \ldots, X_n) = 0$. Llavors tenim: $f(X_1, \ldots, X_n) = 0$ té solució en $\mathbb{P}^{n-1}(\mathbb{Q})$ si i només si $f(X_1, \ldots, X_n) = 0$ té solució en $\mathbb{P}^{n-1}(\mathbb{R})$ i per cada primer $p$, $f(X_1, \ldots, X_n) = 0$ té solució en $\mathbb{P}^{n-1}(\mathbb{Q}_p)$.*

*És a dir $f(X_1, \ldots, X_n) = 0$ satisfà el principi de Hasse.*

En aquest curs nosaltres tan sols demostrarem el teorema de Hasse-Minkowski pel cas concret:

$$a'X^2 + b'Y^2 = cZ^2$$

amb $a', b', c \in \mathbb{Z}$ complint $a'b'c \neq 0$. Per tenir solució en $(x : y : z) \in \mathbb{P}^2(\mathbb{Q})$ amb $xyz = 0$ és necessari i suficient que $\frac{c}{a'}$, $\frac{c}{b'}$ o bé $\frac{-b'}{a'}$ sigui un quadrat en $\mathbb{Q}$.

Per a estudiar l'equació sobre $\mathbb{Q}$ anterior ens podem restringim a estudiar les solucions sobre $\mathbb{Q}$ de

$$aX^2 + bY^2 = 1$$

on $a = \frac{a'}{c}$ i $b = \frac{b'}{c}$.

**Definició 2.3.7.** *Sigui $p$ un primer i $a, b \in \mathbb{Q}^*$ [2] definim el símbol de Hilbert $(a, b)_p$ com segueix. Escrivim*

$$a = p^i u, \quad b = p^j v, \quad (i, j \in \mathbb{Z}, \quad u, v \in (\mathbb{Z}_{(p)})^*),$$

*i escrivim*

$$r := (-1)^{ij} a^j b^{-i} = (-1)^{ij} u^j v^{-i} \in (\mathbb{Z}_{(p)})^*.$$

*Si $p \neq 2$, definim*

$$(a, b)_p = \left( \frac{r \bmod p}{p} \right),$$

*on el símbol de la dreta és el símbol de Lagrange.*
*Si $p = 2$ definim*

$$(a, b)_2 := (-1)^{\frac{r^2-1}{8}} (-1)^{\frac{u-1}{2} \cdot \frac{v-1}{2}},$$

[2] Recordem que $\mathbb{Z}_{p)} = \{ \frac{a}{b} \in \mathbb{Q} | a, b \in \mathbb{Z} \ p \nmid b \} \subset \mathbb{Q}$ que correspon a localitzar l'anell $\mathbb{Z}$ amb l'ideal primer $(p)$

*on els exponents de $-1$ són elements de $\mathbb{Z}_{(2)}$ però els pensem via el morfisme $\mathbb{Z}_{(2)} \to \mathbb{Z}/2\mathbb{Z}$.*

*Definim el simbol de Hilbert per la part arquimediana $p = \infty$ via*

$$(a,b)_\infty = \begin{cases} 1 \text{ si } a > 0 \text{ o } b > 0 \\ -1 \text{ si } a < 0 \text{ i } b < 0 \end{cases}$$

El símbol de Hilbert té les següents propietats que deixem com a exercici,

**Lema 2.3.8.** *Denotem per $v$ un $p$ primer qualsevol, $a, b \in \mathbb{Q}$. Llavors:*

1. $(a,b)_v = (b,a)_v$,
2. $(a,bc)_v = (a,b)_v(a,c)_v$,
3. $(a,-a)_v = 1$. *Si $a \neq 1$ llavors $(a,1-a)_v = 1$.*
4. *si $v$ és senar i $a, b \in (\mathbb{Z}_{(p)})^*$ llavors*
   (a) $(a,b)_p = 1$,
   (b) $(a,pb)_p = \left(\frac{a \bmod p}{p}\right)$.
5. *si $a, b \in \mathbb{Z}^*_{(2)}$ tenim:*
   (a) $(a,b)_2 = 1$ *si $a \equiv 1 \ mod 4$ o $b \equiv 1 (mod\ 4)$, altrament -1.*
   (b) $(a,2b)_2 = 1$ *si $a \equiv 1\ (mod\ 8)$ o $a \equiv 1 - 2b (mod\ 8)$, i -1 altrament.*
6. *Veieu que podeu extendre $(-,-)_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \{\pm 1\}$ i que compleix totes les propietats anteriors substituint $\mathbb{Z}_{(p)}$ per l'anell $\mathbb{Z}_p$.*

**Proposició 2.3.9.** *Per $a, b \in \mathbb{Q}_p^*$ són equivalents:*

1. $(a,b)_p = 1$,
2. $\exists x, y \in \mathbb{Q}_p$ *complint* $ax^2 + by^2 = 1$.

*El cas $p = \infty$ (pensant $\mathbb{Q}_\infty = \mathbb{R}$) també és veritat el resultat.*

*Demostració.* El cas $p = \infty$ és obvi. Per $p$ primers, sol demostrarem quant $p \neq 2$ (el cas $p = 2$ veieu un exercici de la llista de problemes).

Suposem primer: $\exists x, y \in \mathbb{Q}_p$ complint $ax^2 + by^2 = 1$. Si $x = 0$ tenim $b \in (\mathbb{Q}_p^*)^2$, ó si $y = 0$ tenim $a \in (\mathbb{Q}_p^*)^2$ i de les propietats del símbol de Hilbert en el lema anterior obtenim $(a,b)_v = (a_1^2, b)_v = (a_1, b)_v(a_1, b)_v = 1$ si $a = a_1^2 \in \mathbb{Q}_p^*$, similarment quan $x = 0$.

Suposem ara $xy \neq 0$. Llavors de les propietats del símbol de Hilbert del lema anterior obtenim:

$$1 = (ax^2, 1 - ax^2)_p = (ax^2, by^2)_p = (a, by^2)_p(x^2, by^2)_p =$$

$$(a, by^2)_p(x, by^2)_p(x, by^2)_p = (a, by^2)_p = (a,b)_p(a,y)_p(a,y)_p = (a,b)_p.$$

Suposem ara que $(a,b)_p = 1$.
Fixem-nos primer que ambdues condicions de la proposició tan sols depén de la imatge de $a, b \in \mathbb{Q}_p^*$ en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, i podem suposar que $a, b \in \mathbb{Z}_p^* \cup p\mathbb{Z}_p^*$ (és dir elements de $\mathbb{Q}_p$ amb valoració zero o valoració 1).

Estudiem primer que $a, b \in p\mathbb{Z}_p^*$. En aquest cas l'enunciat (i) i (ii) de la proposició podem canviar $a$ per $-ab^{-1} \in \mathbb{Z}_p^*$: efectivament,

$$(-ab^{-1}, b)_p = (-ab^{-1}, b)_p (b,b)_p (b,b)_p = (-a,b)_p (b,b)_p = (-ab,b)_p =$$

$$= (a,b)_p (-b,b)_p = (a,b)_p.$$

Fixem-nos que $\exists x, y \in \mathbb{Q}_p$ amb $xy \neq 0$ complint $-ab^{-1}x^2 + by^2 = 1$ si i només si $-ab^{-1}x^2 + by^2 = z^2$ amb $xyz \neq 0$, si i només si $(by)^2 = ax^2 + bz^2$ amb $xyz \neq 0$ si i només si $\exists x, y \in \mathbb{Q}_p$ complint $ax^2 + by^2 = 1$ amb $xy \neq 0$. I hem vist en el capítol 1 que si $\tilde{a}X^2 + \tilde{b}Y^2 = 1$ amb $\tilde{a}, \tilde{b} \in K$ un cos, té solució en el cos $K$ (de característica diferent de 2) llavors té una infinitat de solucions, i per tant alguna amb $xy \neq 0$. Per tant, $(car(\mathbb{Q}_p) = 0)$ obtenim doncs que $\exists x, y \in \mathbb{Q}_p$ complint $-ab^{-1}x^2 + by^2 = 1$ si i només $\exists x, y \in \mathbb{Q}_p$ complint $ax^2 + by^2 = 1$.

Per tant ens reduïm a les situacions:
cas **A**: $a \in \mathbb{Z}_p^*$ i $b \in p\mathbb{Z}_p^*$;
cas **B**: $a, b \in \mathbb{Z}_p^*$.

Demostració pel cas **A**: tenim de ser $1 = (a,b)_p = \left(\frac{a}{p}\right)$ que $a$ és un quadrat en $\mathbb{F}_p^*$, i pel lema de Hensel $\exists t \in \mathbb{Q}_p^*$ complint $t^2 = a$ i per tant

$$a(\frac{1}{t})^2 + b0^2 = 1$$

és una solució de $aX^2 + bY^2 = 1$.

Demostració pel cas **B**: sota les condicions de $a$, $b$ sempre tenim $(a,b)_p = 1$, hem de construir una solució aquí en $\mathbb{Q}_p$ de $aX^2 + bY^2 = 1$.

Considera $[a], [b] \in \mathbb{F}_p$ les classes de $a, b \in \mathbb{Z}_p$ via el morfisme $proj : \mathbb{Z}_p \to \mathbb{Z}_p/p \cong \mathbb{Z}/p = \mathbb{F}_p$. Considera els subconjunts de $\mathbb{F}_p$ següents $C := \{[a]u^2 | u \in \mathbb{F}_p\}$ i $D := \{1 - [b]v^2 | v \in \mathbb{F}_p\}$. Fixem-nos que $|C| = |D| = (p+1)/2$, i per tant tenen intersecció no buida, sigui doncs $x, y \in \mathbb{Z}_p$ complint

$$ax^2 \equiv 1 - by^2 (mod\ p\mathbb{Z}_p).$$

Si $x \not\equiv 0 (mod\ p\mathbb{Z}_p)$ el polinomi $T^2 - (\frac{1-by^2}{a}) \in \mathbb{Z}_p[T]$ és separable $(p \neq 2)$ i té arrels simples en $\mathbb{F}_p[T]$, per tant pel lema de Hensel, $\exists t \in \mathbb{Z}_p^*$ satisfent

$$at^2 - (1 - by^2) = 0$$

i per tant el resultat.

Si $x \equiv 0 (mod\ p\mathbb{Z}_p)$, tenim $1 \equiv by^2 (mod\ p\mathbb{Z}_p)$, i raonant també via el lema de Hensel, $\exists t \in \mathbb{Q}_p^*$ complint que $t^2 = b^{-1} \in \mathbb{Z}_p$ i obtenim la solució

$$a0 + bt^2 = 1.$$

□

**Teorema 2.3.10** (Hasse-Minkowski)**.** *Sigui $a, b \in \mathbb{Q}^*$ fixats. Existeix $(x, y) \in \mathbb{Q}^2$ satisfent $ax^2 + by^2 = 1$, si i només si $(a, b)_\infty$ i $(a, b)_p = 1$ per tot $p$ primer.*

*Demostració.* Evidentment si té solució a $\mathbb{Q}$ l'equació $aX^2 + bY^2 = 1$, en té a $\mathbb{R}$ i a $\mathbb{Q}_p$ i per la proposició anterior obtenim que $(a, b)_\infty$ i $(a, b)_p = 1$ per tot $p$ primer.

Suposem ara que $(a, b)_\infty$ i $(a, b)_p = 1$ per tot $p$ primer. Sense pèrdua de generalitat podem suposar que $a, b$ són lliure de quadrats i enters. Demostrarem que $aX^2 + bY^2 = 1$ té solució als racional per inducció respecte $max(|a|, |b|)$.

Observeu si $a$ o $b$ és 1 evidentment $aX^2 + bY^2 = 1$ té solució a $\mathbb{Q}$. Si $max(|a|, |b|) = 1$ tenim $a > 0$ o $b > 0$ ja que $(a, b)_\infty = 1$ per tant $aX^2 + bY^2 = 1$ té solució a $\mathbb{Q}$.

Suposem que $max(|a|, |b|) > 1$, sense pèrdua de generalitat de com és l'equació podem suposar $|a| \leq |b| = p_1 \cdots p_k$ amb $p_i$'s primers diferents (de ser lliure de quadrats).

Demostrem primer que $a(mod|b|)$ és un quadrat en $\mathbb{Z}/(b)$.

De l'isomorfisme d'anells

$$\varphi : \mathbb{Z}/(b) \to \mathbb{Z}/(p_1) \times \cdots \times \mathbb{Z}/(p_k)$$

$$a(mod\ |b|) \mapsto (a(modp_i))_{i=1,\ldots,k}$$

tenim que si $[a]$ no és un quadrat en $\mathbb{Z}/(b)$ tenim que existeix $i$ on $(a(modp_i))$ no és un quadrat en $\mathbb{Z}/(p_i)$ on $p_i|b$. Fixeu-vos que $p_i \neq 2$ ja que com en $\mathbb{Z}/(2)$ tot element és un quadrat. Ara fixem-nos com $p_i|b$ i $p_i^2|b$ i $p_i \nmid a$ de les propietats del símbol de Hilbert on $p_i$ un primer senar tenim que

$$(a, b)_{p_i} = \left(\frac{a}{p_i}\right)$$

i el símbol de Lagrange és -1 ja que $(a(mod\ p_i))$ no és un quadrat. Llavors, per la proposició anterior l'equació $aX^2 + bY^2 = 1$ no té solució en $\mathbb{Q}_{p_i}$ en contra hipòtesi.

Per tant tenim que $a(mod\ b)$ és un quadrat en $\mathbb{Z}/(b)$. Obtenim llavors que $\exists r \in \mathbb{Z}$ complint $r^2 \equiv a(mod\ b)$ i podem triar en $\mathbb{Z}$ representant tots els elements de $\mathbb{Z}/(b)$ en l'interval $-\frac{|b|}{2} \leq n \leq \frac{|b|}{2}$ i per tant podem triar $0 \leq r \leq \frac{|b|}{2}$. Escrivim

$$r^2 - a = bc$$

amb $c \in \mathbb{Z}$. Si $c = 0$ ja estem, $a(1/r)^2 + b0^2 = 1$ solució a $\mathbb{Q}$. Si $c \neq 0$ tenim,

$$|c| = |\frac{r^2 - a}{b}| \leq |\frac{r^2}{b}| + |\frac{a}{b}| \leq \frac{|b|}{4} + 1 < |b|$$

on en l'última desigualtat usem $|b| \geq 2$.

Fixem-nos ara que donat $K$ un cos amb $a, b, c \in K^*$ i $r \in K$ complint que $r^2 - a = bc$, hi ha una bijecció entre els conjunts $E$, $F$:

$$E := \{(x, y, z) \in K^3 | ax^2 + by^2 = z^2,\ (x, y, z) \neq (0, 0, 0)\}$$

$$F := \{(x, y, z) \in K^3 | ax^2 + cy^2 = z^2,\ (x, y, z) \neq (0, 0, 0)\},$$

via $(x, y, z) \mapsto (rx + z, by, ax + rz)$ i $(x, y, z) \mapsto (rx - z, cy, -ax + rz)$.

Per tant retornant a la demostració, si $|a| < |b|$ usant la hipòtesi d'inducció finalitzem ja que $|c| < |b|$. Si $|a| = |b|$ ens reduïm al cas $|a| < |b|$ ja que $|c| < |b|$. □

## 2.4 Sobre extensions algebraiques de $\mathbb{Q}_p$

Fixeu-vos que qualsevol extensió algebraica de $\mathbb{Q}_p$ és separable. El cas anàleg de la completació de $\mathbb{Q}$ pel valor usual arquimedià és els nombres reals $\mathbb{R}$, i extensions algebraiques de $\mathbb{R}$ sol n'hi ha una i és els complexos. El cas dels $p$-àdics la situació és molt diferent, i anem a fer-ne un esboç en aquesta secció.

**Definició 2.4.1.** *Donat un conjunt $X$ de punts de $\mathbb{R}^2$ l'envolvent convexa inferior per a $X$ es defineix com el conjunt convex més petit que conté $X$ i les semirectes $L_{(x,y)}$ per cada punt $(x,y) \in X$ on $L_{(x,y} = \{(x,t)|t \geq y\}$.*

**Definició 2.4.2.** *Donat un polinomi $f(X) = \sum_{i=0}^{N} a_i X^i \in K[X]$ on $K$ és un cos complet amb $||$ no arquimedià i discret (pensem aquí $K = \mathbb{Q}_p$ per exemple), i $v$ valoració del cos $K$ amb $v : K^* \to \mathbb{Z}$ on $v(\pi) = 1$ (on $\pi$ uniformitzant de l'ideal maximal associat, podeu pensar $\pi = p$ ideal maximal de $\mathbb{Z}_p$, en el cas dels nombres p-àdics). Suposem $a_0 a_N \neq 0$. Denotem el conjunt $X = \{(i, v(a_i)) \in \mathbb{R}^2 | 0 \leq i \leq N\}$. Prenem l'envolvent convexa inferior de $X$ i ens quedem amb els segments inferiors d'aquesta envolvent que van del punt $(0, v(a_0))$ fins $(N, v(a_N))$, i els anomenem el polígon de Newton associat a $f(X)$*

**Fet 2.4.3.** *Sigui $f(X) = \sum_{i=0}^{N} a_i X^i \in \mathbb{Q}_p[X]$ amb $a_0 a_N \neq 0$. I suposem que el polígon de Newton té exactament $s$ segments i el segment $i$ del polígon de Newton uneix els punts $(r_i, v_p(a_{r_i}))$ amb $(r_{i+1}, v_p(a_{r_{i+1}}))$ amb $i = 0, \ldots, s$ i de pendent $-m_i$. Llavors en $\mathbb{Q}_p[X]$ tenim*

$$f(X) = f_1(X) \ldots f_s(X)$$

*on el grau de cada $f_i(X) \in \mathbb{Q}_p[X]$ és $r_{i+1} - r_i$, a més si $L$ és el cos de descomposició de $f$ sobre $\mathbb{Q}_p$, i per $\alpha \in L$ definim $\omega(\alpha) = \frac{1}{[L:\mathbb{Q}_p]} v_p(Norm_{L/\mathbb{Q}_p}(\alpha))$, tenim que les arrels $\beta$ de $f_i$ compleixen que $w(\beta) = m_i$.*

**Fet 2.4.4.** *Sigui $f(X) \in \mathbb{Z}_p[X]$ on el seu polígon de Newton és un únic segment unint $(0, v_p(a_0))$ amb $(grau(f), v_p(a_{grau(f)}))$, i a més aquest segment no tingui cap altre punt $(n, m) \in \mathbb{Z}^2$ dins el segment, llavors $f(X)$ és irreductible en $\mathbb{Q}_p[X]$.*

*En particular (tenim criteri Eisenstein) si $f(X) = \sum_{i=0}^{N} a_i X^i$ amb $a_N a_0 \neq 0$ i $v_p(a_N) = 1$, $v_p(a_0) = 1$ i $v_p(a_i) \geq 1$ per a $1 \leq i \leq N-1$, llavors $f(X)$ és irreductible en $\mathbb{Q}_p[X]$*

**Observació 2.4.5.** Magma permet facilment treballar amb els $p$-àdics i en particular en la factorització. Per exemple:

```
R:=padicRing(5);
P<x>:=Polynomial(R);
f:=X^5+x^4+x^3+x^2+x+1;
Factorization(f);
```

obtenim la factorització a $\mathbb{Q}_5[X]$.

## 2.5 Exercicis dels continguts del capítol

### 2.5.1 Anàlisi no-arquimdedià. Completació d'un cos. Els $p$-àdics.

1. Sigui $K$ un cos complet amb una valoració discreta no trivial $v$. Sigui $\overline{K}$ una clausura algebraica de $K$.

   (a) (**) Donada $L/K$ extensió finita de cossos, existeix una valoració $w$ en $L$ on $w(x) = v(x)\ \forall x \in K$ i $L$ és complet amb la valoració $w$.

   (b) (**) Demostreu que existeix una valoració $\overline{v}$ en $\overline{K}$ que estén $v$, és dir $\overline{v}(x) = v(x)\ \forall x \in \overline{K}$.

   (c) (**) Demostreu que $\overline{K}$ amb $\overline{v}$ no és necessareament un cos complet.

   (d) Considera $\hat{\overline{K}}$ la completació de $\overline{K}$ amb la valoració $\overline{v}$. Demostreu que $\hat{\overline{K}}$ és algebraicament tancat.

2. Considera una successió $a_n$ d'elements d'un cos $K$ complet amb una valor absolut $||$ no arquimedià i no trivial donat per una valoració $v$, i suposem que $K$ és complet amb aquest valor absolut. Demostreu que la sèrie $\sum_{n\geq 0} a_n$ convergeix en $K$ si i només si existeix el limit de $a_n$ i aquest limit és zero.

3. Una sèrie de potencies $f(x) = \sum_{n\geq 0} a_n x^n$ amb $a_i \in K$ on $K$ és un cos complet amb un valor absolut no-arquimedià donat per una valoració real $v$. Definit l'ordre de convergència de $f(x)$ mitjançant:

$$\rho(f) := -\lim_{j\to\infty} v(a_j)/j.$$

   Demostreu que $f(x)$ convergeix en $\alpha \in K$ si $v(\alpha) > \rho(f)$ i divergeix si $v(\alpha) < \rho(f)$.

4. **El polígon de Newton.** Sigui $f(x) = \sum_{j=0}^{\infty} a_j x^j \in K[[x]]$ una sèrie de potencies amb $K$ un cos complet amb un valor absolut no-arquimedià no trivial donat per una valoració real $v$. Considera el conjunt $S = \{(j, v(a_j))|j \in \mathbb{N}, a_j \neq 0\} \subset \mathbb{R}^2$. El polígon de Newton de $f(x)$ és "the lower convex hull of $S$",és dir la envolvent convexa inferior del conjunt $S$.

   Siguin $\{m_i\}$ la sequència de pendents del polígon de Newton de $f(x)$. Llavors $\{m_i\}$ és monòtona creixent i $-lim_{i\to\infty} m_i = \rho(f)$.

5. Sigui $K$ amb una valoració discreta $v$ (amb $Imatge(v) = \mathbb{Z}$) complint que el cos residual $A_v/\mathcal{B}_v$ és un cos finit de $q$ elements. Denotem per $U^{(1)} := \{x \in A_v | v(1-x) \geq 1\}$. Demostreu, usant el Lemma de Hensel, que tenim una descomposició de la forma:

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)}$$

   on $\pi \in \mathcal{B}_v$ amb $val(\pi) = 1$ (anomenat un uniformitzant de $v$), $\mu_{q-1}$ el grup multiplicatiu cíclic d'ordre $q-1$ corresponent a arrels $q-1$-èssimes de 1.

6. Sigui $A$ un anell commutatiu. $A$ és un anell de valoració discreta si i només si $A$ és anell local, noetherià i el seu ideal maximal està generat per un element no nilpotent. [3]

7. Sigui $A$ un domini, amb $A$ anell noetherià. $A$ és un anell de valoració discreta si i només si $A$ té un unic ideal primer no zero i $A$ és integrament tancat [4].

8. Sigui $A$ un anell de valoració discreta, amb valoració $v$. Siguin $a, b \in A$ amb $v(a) > v(b)$. Demostreu llavors que $v(a+b) = min(v(a), v(b)) = v(b)$. Observeu amb un exemple que quant $v(a) = v(b)$ llavors la desigualtat $v(a+b) \geq min(v(a), v(b))$ pot ser estricta.

9. Demostreu que qualsevol valor absolut en un cos $K$ amb $car(K) = p > 0$ és no arquimedià.

10. Considera el cos de fraccions de l'anell de polinomis en una variable $T$ sobre un cos finit $\mathbb{F}_q$, denotem-lo per $\mathbb{F}_q(T) = Q(\mathbb{F}_q[T])$. Recordem que donat $p(x) \in \mathbb{F}_q[T]$ irreductible definim la valoració discreta

$$v_{p(x)} : \mathbb{F}_q(T)^* \to \mathbb{Z}$$

via $v(a/b) = j$ on $\frac{a}{b} = p(x)^j \frac{a'}{b'}$ on $(mcd(p(x), a'b')) = (1)$. Definim també

$$v_\infty : \mathbb{F}_q(T)^* \to \mathbb{Z}$$

via $v(a/b) := -(grau(a) - grau(b))$.

Definim el valor absolut associat a aquestes valoracions $v_u$ via $|x|_u = \ell^{-v_u(x)}$ on $\ell$ és el nombre d'elements del cos finit $\mathbb{F}_q[T]/f(T)$ si $u = f(T)$ i el nombre d'elements del cos finit $\mathbb{F}_q[1/T]/(1/T)$ si $u = \infty$.

Demostreu que tot valor absolut de $\mathbb{F}_q(T)$ és equivalent a un dels anteriors.

11. Considera $K[[x]]$ les series formals $\sum_{i\geq 0} a_i x^i$ amb la variable $x$ amb $a_i \in K$. $K[[x]]$ és un domini amb la suma i multiplicació usual. Demostreu que $K[[x]]^*$ són les series formals amb $a_0 \in K^*$. Considera l'anell de les series de Laurent en $K$, és dir expressions formal $\sum_{i\geq n_0} a_i x^i$ amb $a_i \in K$ i $n_0 \in \mathbb{Z}$. Demostreu que el cos de fraccions de $K[[x]]$ que denotem per $K((x))$ coincideix amb l'anell de les series de Laurent en $K$.

12. Demostreu que la completació d'un valor absolut $||$ de $\mathbb{F}_q(T)$ és isomorf a $\mathbb{F}_\ell((U))$ on $\ell = q^a$ i on $\mathbb{F}_q((U))$ denota el cos de fraccions de $K[[U]]$ amb $U$ una certa variable.

13. Fixem $p$ primer. Demostreu que donat $c \in \mathbb{Q}$ amb $val_p(c) \geq 1$ compleix que $\sum_{i=0}^{\infty} c^i = \frac{1}{1-c}$ en $\mathbb{Q}_p$.

[3] Un anell $A$ s'anomena noetherià si tota successió creixent d'ideals de $A$ estaciona, o equivalentment que tot ideal de $A$ és finitament generat.

[4] Un element $x$ d'un anell que conté $A$ és diu integre sobre $A$ si satisfà una equció polinomial mónica:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

amb $a_i \in A$. Diem que $A$ és integrament tancat en un anell $B$ amb $A \subset B$ si tot element de $B$ que és integre sobre $A$ pertant a $A$. Diem que un domini $A$ és integrament tancat si és integrament tancat dins el seu cos de fraccions $Q(A)$.

14. Demostreu que existeix l'arrel quadrada de $-1$ en $\mathbb{Q}_p$ si i només si $p \equiv 1$ *mod* 4.

15. Fix $p$, demostreu que hi ha una finitud d'extensions de grau 2 de $\mathbb{Q}_p$ diferents, en particular hi ha exactament tres extensions de grau 2 de $\mathbb{Q}_p$ si $p$‘ $\neq 2$ i exactament cinc extensions de grau 2 de $\mathbb{Q}_2$. Determineu les tres extensions de grau 2 de $\mathbb{Q}_5$.

16. Per qualsevol enter $n \geq 0$ i $p$ un primer demostreu que

$$v_p(n!) = \sum_{i=1}^{\infty} \left[ \frac{n}{p^i} \right]$$

on $[x]$ denota l'enter més gran possible complint que $[x] \leq x$.

17. Sigui $c$ un nombre real fix. Demostreu que:

    (a) la condició $nc - v_p(n!) \to \infty$ quant $n$ tendeix a $\infty$ és equivalent a $c > \frac{1}{p-1}$,

    (b) la condició $nc - v_p(n) \to \infty$ quant $n$ tendeix a $\infty$ és equivalent a $c > 0$,

    (c) si $c > \frac{1}{p-1}$, llavors per qualsevol $n \geq 1$ tenim $nc - v_p(n!) \geq c$.

18. **Funció exponencial i logaritme en $\mathbb{Q}_p$.**
Considera les series formals

$$exp(x) := \sum_{n \geq 0} \frac{x^n}{n!} \in \mathbb{Q}_p[[x]]$$

$$i\ log(t) := \sum_{n \geq p} \frac{(-1)^{n-1}}{n} (t-1)^n \in \mathbb{Q}_p[[t]].$$

I evaluem-es amb elements de $\mathbb{Q}_p$. Demostreu:

    (a) $exp(x)$ convergeix en $\mathbb{Q}_p$ si i només si $v_p(x) \geq 1$ en el cas que $p \neq 2$ i si $p = 2$ ha de complir $v_2(x) \geq 2$, i.e. la exponencial no convergeix en tot $\mathbb{Q}_p$.

    (b) $log(t)$ convergeix si i nomes si $v(t-1) \geq 1$.

    (c) si $x_1, x_2$ estan en el domini de convergencia de $exp(x)$, i $t_1, t_2$ estan en el domini de convergencia de $log(t)$ llavors tenim:

$$exp(x_1 + x_2) = exp(x_1)exp(x_2) \in \mathbb{Q}_p; \quad log(t_1 t_2) = log(t_1)log(t_2).$$

    (d) Sigui $m \geq 1$ si $p \neq 2$ o $m \geq 2$ si $p = 2$. Demostreu que $exp$ i $log$ donen l'isomorfisme de grups entre: el grup additiu $p^m\mathbb{Z}_p$ amb el grup multiplicatiu $1 + p^m\mathbb{Z}_p = U^{(m)} = \{1 + p^m a | a \in \mathbb{Z}_p\}$.

19. Calculeu $v_3(4^n - 1)$ amb $n \in \mathbb{Z}$.

20. Trobeu una successió de nombres racionals que convegeixi a 1 en els reals i que convergeixi a zero en $\mathbb{Q}_2$. Trobem un exemple d'una altra successió de nombres racionals que convergeixi a 1 en $\mathbb{Q}_5$ i a zero a $\mathbb{Q}_2$.

21. Considera l'anell $\mathbb{Z}_p$. Demostreu que no és un conjunt numerable.

22. $\mathbb{Z}_p$ és tancat i obert en $\mathbb{Q}_p$. $\mathbb{Z}$ és dens en $\mathbb{Z}_p$.

23. (*) Considera l'anell $\mathbb{Z}[\frac{1}{p}] := \{\frac{a}{p^n} | a \in \mathbb{Z}, n \geq 0\}$. Observa $\mathbb{Z}$ no és un ideal d'aquest anell però si un subgrup amb la suma, per tant obtenim el grup abelià quocient $G := \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ amb l'operació suma. Demostra que tot element de $G$ és de torsió i l'ordre de qualsevol element és una potència de $p$.

    Denota per $Hom(G, G)$ els morfismes de grup de $G$ en $G$, té estructura d'anell on el producte ve donat per la composició.

    Demostreu que
    $$\mathbb{Z}_p \cong Hom(G, G)$$
    com a anells.

24. **Estructura de $\mathbb{Q}_p^*$ i quadrats en $\mathbb{Q}_p^*$.**

    (a) Demostreu que hi ha un isomorfisme de grups abelians entre
    $$\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p^*$$
    a més tenim un isomorfisme de grup entre
    $$\mathbb{Z}_p^* \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$$
    i un altre isomorfisme de grups entre $1 + p\mathbb{Z}_p$ a $(\mathbb{Z}_p, +)$ si $p \neq 2$ o entre $1 + 4\mathbb{Z}_2$ amb $(\mathbb{Z}_2, +)$ per $p = 2$.

    (b) Escrivim $a \in \mathbb{Q}_p^*$ via $a = p^n u$ amb $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^*$. Llavors $a$ és un quadrat en $\mathbb{Q}_p^*$ si i només si es compleixen les dues condicions següents:

    i. $n$ és parell,

    ii. si $p \neq 2$ i $u(mod\ p\mathbb{Z}_p)$ és un quadrat en $\mathbb{F}_p^*$; si $p = 2$ $u \equiv 1(mod\ 8\mathbb{Z}_2)$.

    (c) Demostreu que si $p \neq 2$ $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ com grups abelians. Si $p = 2$ demostreu que tenim l'isomorfisme com grups abelians $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

25. (*) **Estructura de $\mathbb{F}_q((T))^*$** Recordem que $\mathbb{F}_q((T))$ és en particular el cos complet de $\mathbb{F}_q(T)$ per la valoració $v_T$. Demostreu que com a grups abelians tenim un isomorfisme
    $$\mathbb{F}_q((T))^* \cong (\mathbb{Z}, +) \times (\mathbb{Z}/(q-1), +) \times ((1 + T\mathbb{F}_q[[T]]), \cdot)$$
    i
    $$(1 + T\mathbb{F}_q[[T]]), \cdot) \cong \mathbb{Z}_p^{\mathbb{N}}.$$

26. (*) Sigui $F/K$ una extensió separable i normal, és a dir Galois. Considerem $G := Gal(F/K)$ el grup dels automorfismes de cossos de $F$ que deixen fix $K$. Per cada subextensió $E$ amb $K \subseteq E \subseteq F$ amb $E/K$ Galois i FINITA,

escrivim $G_E = Gal(E/K)$ i tenim el morfisme restricció $\pi_E^F : G \to G_E$ i per donades dos subextensions $E_1, E_2$ finites sobre $K$ com abans on $K \subseteq E_1 \subseteq E_2 \subseteq F$ escrivim $\pi_{E_1}^{E_2} : G_{E_2} \to G_{E_2}$ el morfismes restricció. Denotem per $\varprojlim_E G_E$ el subgrup de $\prod_{E\subset F;E/K finita\ i\ Galois} G_E$ definit per

$\varprojlim_E G_E := \{(a_E)_E \in \prod_{E\subset F;E/K finita\ i\ Galois} G_E | \pi_{E_1}^{E_2}(a_{E_2}) = a_{E_1}\ si\ E_2 \subset E_1, \}$.

Demostreu que com a grups tenim

$$Gal(F/K) \cong \varprojlim_E G_E.$$

5

## 2.5.2 Equacions de grau 2, segona part:Hasse-Minkowski

1. **El símbol de Hilbert.** Sigui $p$ un primer i $a, b \in \mathbb{Q}^*$ definim el símbol de Hilbert $(a, b)_p$ com segueix. Escrivim

$$a = p^i u, \quad b = p^j v, \quad (i, j \in \mathbb{Z}, \quad u, v \in (\mathbb{Z}_{(p)})^*),$$

i escrivim

$$r := (-1)^{ij} a^j b^{-i} = (-1)^{ij} u^j v^{-i} \in (\mathbb{Z}_{(p)})^*.$$

Si $p \neq 2$, definim

$$(a, b)_p = \left(\frac{r\ mod\ p}{p}\right),$$

on el símbol de la dreta és el símbol de Lagrange.
Si $p = 2$ definim

$$(a, b)_2 := (-1)^{\frac{r^2-1}{8}} (-1)^{\frac{u-1}{2}\cdot\frac{v-1}{2}},$$

on els exponents de $-1$ són elements de $\mathbb{Z}_{(2)}$ però els pensem via el morfisme $\mathbb{Z}_{(2)} \to \mathbb{Z}/2\mathbb{Z}$.

Denotem per $v$ un $p$ primer qualsevol. Demostreu:

(a) $(a, b)_v = (b, a)_v$,

(b) $(a, bc)_v = (a, b)_v (a, c)_v$,

(c) $(a, -a)_v = 1$. Si $a \neq 1$ llavors $(a, 1 - a)_v = 1$.

(d) si $v$ és senar i $a, b \in (\mathbb{Z}_{(p)})^*$ llavors

  i. $(a, b)_p = 1$,

  ii. $(a, pb)_p = \left(\frac{a\ mod\ p}{p}\right)$.

(e) si $a, b \in \mathbb{Z}_{(2)}^*$ tenim:

[5] Dotant $G_E$ amb la topologia discreta, llavors via la topologia producte tenim una topologia natural en $\prod_{E\subset F;E/K finita\ i\ Galois} G_E$, i la topologia induïda en aquest producte dona una topologia natural a $\varprojlim_E G_E$ i en particular al grup de Galois $Gal(F/K)$. Aquesta topologia és clau per la correspondencia bijectiva de Galois quant l'extensió Galois $F/K$ no és finita.

i. $(a,b)_2 = 1$ si $a \equiv 1\ mod 4$ o $b \equiv 1 (mod\ 4)$, altrament -1.

ii. $(a,2b)_2 = 1$ si $a \equiv 1\ (mod\ 8)$ o $a \equiv 1 - 2b (mod\ 8)$, i -1 altrament.

(f) Veieu que podeu extendre $(-,-)_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \{\pm 1\}$ i que compleix totes les propietats anteriors substituint $\mathbb{Z}_{(p)}$ per l'anell $\mathbb{Z}_p$.

2. Siguin $a, b \in \mathbb{Z}_2^*$ amb $(a,b)_2 = 1$, demostreu que $\exists x, y \in \mathbb{Q}_2$ que compleix l'equació $aX^2 + bY^2 = 1$.

3. Sigui $p$ un nombre primer. Demostreu els següents enunciats:

(a) $X^2 + 2 = 0$ té solució en $\mathbb{Q}_p$ si i només si $p \equiv 1, 3 (mod\ 8)$,

(b) $X^2 + Y^2 = -2$ té solució en $\mathbb{Q}_p$ si només si $p \neq 2$,

(c) $X^2 + Y^2 + Z^2 = -2$ té solució en $\mathbb{Q}_p$ per qualsevol $p$,

(d) $15X^2 - 36 = Y^2$ no té solució en $\mathbb{Q}$.

4. (**) L'equació $3X^3 + 4Y^3 + 5Z^3 = 0$ amb $(x,y,z) \in \mathbb{P}^2(\mathbb{Q})$ no té solucions, en canvi té solucions en $\mathbb{P}^2(\mathbb{Q}_p)$ per tot primer $p$ i també té solucions en $\mathbb{P}^2(\mathbb{R})$. Per tant diem que el principi de Hasse falla per aquesta equació.

5. (**) Considera l'equació $aX^2 + bY^2 = c$ amb $a, b, c \in \mathbb{F}_q[T]$. Obtén condició/ons per tal que l'equació tingui solució en la completació de $\mathbb{F}_q[T]$ en la valoració $v_{f(T)}$ amb $f(T)$ irreductible de $\mathbb{F}_q[T]$. Decidiu si l'equació compleix el principi de Hasse o no.

## 2.6 Exercici dirigit: Exemple no complint el principi de Hasse-Minkowski

Considerem l'equació diofantina

$$aX^4 + bY^4 = cZ^2$$

amb $a, b, c \in \mathbb{Z}$ enters coprimers i no zero. Denotem per

$$V_K := \{(x,y,z) \in K^3 - \{(0,0,0)\} | ax^4 + by^4 = cz^2\},$$

on $K$ denota un anell o cos (i pensem $\mathbb{Z}$ dins $K$ via el morfisme $\iota : \mathbb{Z} \to K$ $\iota(n) = n$).

1. Demostreu que si $V_{\mathbb{Q}} \neq \emptyset$ llavors existeix $(x,y,z) \in \mathbb{Z}^3 - \{(0,0,0)\} \in V_{\mathbb{Q}}$. Demostreu que si $V_{\mathbb{Q}} \neq \emptyset$ llavors $V_{\mathbb{R}} \neq \emptyset$ i $V_{\mathbb{Q}_\ell} \neq \emptyset$ per tot primer $\ell$.

   I observeu que $V_{\mathbb{R}} = \emptyset$ si i només si $ab > 0$ i $ac < 0$.

2. Sigui $p$ primer senar amb $p \nmid abc$. Demostreu que $V_{\mathbb{F}_p} \neq \emptyset$.

   Indicació: podem reduir-nos a trobar una solució no trivial de $a'X^4 + b'Y^4 = Z^2$ en $\mathbb{F}_p$ i seguir les següents pautes:

   (a) Considera l'equació $a'(X')^2 + b'(Y')^2 = Z^2$. Demostreu que l'equació $a'(X')^2 + b'(Y')^2 = 1$ té solució en $\mathbb{F}_p$ i escrivim per $(x_0, y_0) \in \mathbb{F}_p^2$ una solució.

(b) Com sabem resoldre $a'(X')^2+b'(Y')^2=Z^2$ en $\mathbb{F}_p[T]$ (on $T$ una variable) (recordeu són certs anàlegs del cas de les termes Pitagòriques), proveu que una solució en $\mathbb{F}_p[T]^3$ de $a'(X')^2+b'(Y')^2=Z^2$ és:

$$(\alpha(T),\beta(T),\gamma(T)):=$$

$$(b'x_0T^2-2b'y_0T-a'x_0,-b'y_0T^2-2a'x_0T+a'y_0,b'T^2+a').$$

i comproveu que els polinomis $\alpha(T),\beta(T),\gamma(T)$ són dos a dos coprimers.

(c) Demostreu: siguin $f,g\in\mathbb{F}_p[T]-\mathbb{F}_p$ amb grau com a molt dos i que compleixen que els símbols de Lagrange següents satisfan:

$$\left(\frac{f(t)}{p}\right)=-\left(\frac{g(t)}{p}\right)$$

per a tot $t\in\mathbb{F}_p$ llavors el $mcd(f,g)\neq 1$.

(d) Trobeu ara una solució no trivial de $a'X^4+b'Y^4=Z^2$ en $\mathbb{F}_p$ via triar $t\in\mathbb{F}_p$ on

$$\left(\frac{\alpha(t)}{p}\right)\neq-\left(\frac{\beta(t)}{p}\right)$$

on en particular $\alpha(t)\beta(t)$ és un quadrat en $\mathbb{F}_p$.

3. Sigui $p$ primer senar amb $p\nmid abc$ i $k\geq 1$ un natural. Demostreu que $V_{\mathbb{Z}/p^k}\neq\emptyset$.

Indicació: Podeu demostrar-ho seguint les pautes següents:

(a) Si $N$ i $s>0$ enters on $p\nmid sN$ demostreu per inducció: si $N=c^s(mod\ p)$ llavors per tot $n\geq 1$ enter es té que existeix un enter $d_n$ complint $N=d_n^s(mod\ p^n)$.

(b) Com $mcd(p^k,c)=1$ en $\mathbb{Z}/p^k$ existeix $c^{-1}\in\mathbb{Z}/p^k$ i considereu l'equació en $\mathbb{Z}/p^k$:

$$c^{-1}aX^4+c^{-1}bY^4=Z^2.$$

Sabem que té solució no trivial $([u_0],[v_0],[w_0])\in\mathbb{F}_p^3$ (de $V_{\mathbb{F}_p}\neq\emptyset$). Fixeu-vos llavors que si $w_0\not\equiv 0(mod\ p)$ tenim $N:=c^{-1}(au_0^4+bv_0^4)$ és un quadrat $(mod\ p)$ i per tant un quadrat fent modulo $p^k$, i escrivint $N\equiv m^2(mod\ p^k)$ obteniu que $(u_0,v_0,m)\in(\mathbb{Z}/p^k)^3$ ens proporcionarà una solució.

4. Demostreu que per $p$ primer senar amb $p\nmid abc$ tenim $V_{\mathbb{Z}_p}\neq\emptyset$ i en particular $V_{\mathbb{Q}_p}\neq\emptyset$.

5. Considera $a=1$, $b=-97$ i $c=2$, és dir l'equació diofantina

$$X^4-97Y^4=2Z^2.$$

(a) Demostreu que té solució no trivial en $\mathbb{Q}_\ell$ per tot $\ell$ primer.
Indicació: per $\ell\nmid 2\cdot 97$ ja ho hem demostrat per l'argument dels apartats anteriors. Per demostrar-ho per $\ell=97$ podeu usar el lema de Hensel resolent l'equació a $\mathbb{F}_{97}$. Per $p=2$, demostreu que si $N\equiv 1(mod 16)$ llavors $N$ és una potència quarta mòdul $2^n$ per a tot $n\geq 1$.

(b) Demostreu que les solucions a $\mathbb{Q}$ de $X^4 - 97Y^4 = 2Z^2$ tant sols és la solució $(0, 0, 0)$.

Indicació: suposem que tingués una solució no trivial i observem que poder triar-ne una amb $(x, y, z) \in \mathbb{Z}^3 - \{(0, 0, 0\}$ i amb $mcd(x, y, z) = 1$. Preneu $q$ primer que divideix $z$. Demostreu que el símbol de Lagrange $\left(\frac{q}{97}\right)$ sempre és 1 i per tant $z \equiv z_0^2 (mod\ 97)$. Observeu després que 2 no és una potència quarta en $\mathbb{F}_{97}$.

# Capítol 3

# Unes primeres nocions de Corbes el.líptiques

Pel lector interessat, recomanem la lectura del llibre [Silverman] de la bibliografia d'aquest tema.

## 3.1 Corbes algebraiques i primeres definicions

Recomdem primer conceptes de teoria de cossos.

**Definició 3.1.1.** *Un conjunt $S = \{v_1, \ldots, v_n\}$ on $v_i \in L$ amb $L$ un cos on $L/K$ una extensió de cossos. Diem que $S$ és algebraicament independent sobre $K$ si el morfime d'anells evaluació $ev_{v_1,\ldots,v_n} : K[X_1, \ldots, X_n] \to K[v_1, \ldots, v_n] \subseteq L$ satisfà que el nucli és trivial igual al ideal zero.*

**Teorema 3.1.2.** *Sigui $L/K$ una extensió finit generada, i per tant escrivim $L = K(a_1, \ldots, a_n)$. Denotem per $\mathfrak{S} := \{a_1, \ldots, a_n\}$.*

1. *Tot subconjunt $S$ de $\mathfrak{S}$ algebraicament independent sobre $K$ maximal respecte inclusió defineix una extensió $M = K(S)$ on $L/M$ finita i $M$ isomorf al cos de fraccions de l'anell de polinomis en $\#S$-variables.*

2. *Tot subconjunt d'elements de $L$ algebraicament independent sobre $K$ maximal respecte inclusió és un subconjunt finit i tots aquests subconjunts tenen el mateix nombre d'elements, aquest nombre s'anomena el grau de* **trascendència** *de $L/K$ i s'anota $deg.tras_K(L)$.*

*Demostració.* 1. Pensem $S = \{a_1, \ldots, a_k\}$ maximal respecte inclusió algebraicament independent sobre $K$. Tenim $L = K(S)(a_{k+1}, \ldots, a_n)$ per la maximalitat de $S$ tenim $S \cup \{a_j\}$ no és algebraicament independent per $j > k$ i per tant existeix $f_j(X_1, \ldots, X_k, X_{k+1}) \in K[X_1, \ldots, X_{k+1}]$ no constant on $g_j(X_{k+1}) := f(a_1, \ldots, a_k, X_{k+1}) \in K(S)[X_{k+1}]$ no constant i $g(a_j) = 0$, per tant $a_j$ és algebraic sobre $K(S)$ i per tant $L$ és algebraic sobre $K(S)$. Considera ara el morfisme evaluació

$$ev_{a_1,\ldots,a_k} : K[X_1, \ldots, X_k] \to K(S)$$

definit per $ev_{a_1,\ldots,a_k}(p(X_1,\ldots,X_k)) := p(a_1,\ldots,a_n)$, i de ser $S$ algebraicament independent tenim $Ker(ev_{a_1,\ldots,a_k}) = (0)$ i per tant facilment podem demostrar que $Quot(K[X_1,\ldots,X_k]) \cong K(S)$, per la propietat universal del cos quocient.

2. Fixem el conjunt $S = \{a_1,\ldots,a_k\}$ maximal algebraicament independent via inclusió de l'apartat anterior. Sigui $\{b_j\}_j \in J$ un altre conjunt maximal alg. independent sobre $K$ via inclusió dins el cos $L$.

   Fixem-nos que $b_1 \in L$ i $b_1$ algebraic sobre $K(S)$, per tant $S \cup \{b_1\}$ no és algebraicament independent sobre $K$, per tant existeix un $a_i \in S$ on $S' := S \cup \{b_1\} \setminus \{a_i\}$ és algebraicament independent sobre $K$ i $a_i$ algebraic sobre $L(S')$ d'on $L/K(S')$ algebraic, aquest procés podem anar iterant perquè els $b's$ son algebraicament independent sobre $K$ i per tant arribem que $\#J \leq k$.

□

**Definició 3.1.3.** *Una corba algebraica completa (llissa i projectiva) sobre un cos $K$ és un cos $L$ extensió de $K$ amb $deg.tras_K(L) = 1$ i complint que $\overline{K} \cap L = K$ on $\overline{K}$ denota la clausura algebraica de $K$. A partir d'ara corba algebraica voldrà dir corba algebraica completa.*

Un morfisme sobre $K$ de corbes algebraiques $L_1, L_2$ sobre $K$ és una injecció de cossos entre $L_1$ a $L_2$ on la restricció a $K$ és la identitat.

**Exemple 3.1.4.** *Observem $Y^2 + (X-1)(X+1) \in K(X)[Y]$ és irreductible usant lema de Gauss i Eisenstein, per tant $L = K(X)[y]/(y^2 + (x^2 - 1)$ és una corba algebraica sobre cos $K$, tenim $K \subset K(X) \subset L$ on $L/K(X)$ té grau 2, i ho relacionem amb la corba $Y^2 + X^2 - 1 = 0$ ja treballada al capítol 1 del curs. Es pot veure $\overline{K} \cap L = K$.*

**Definició 3.1.5** (Extensió escalars)**.** *Si $F/K$ és una extensió algebraica i separable de $K$, i $L$ una corba algebraica sobre $K$ i pensem que $L = K(X)[y]/f(X,y)$. La corba algebraica sobre $F$ de la forma $F(X)[y]/(f(X,y)$ s'anomena l'extensió d'escalars de la corba $L$ al cos $F$ i s'anota $L_F$ o bé $L \otimes_K F$, on $L_F$ és una corba algebraica sobre el cos $F$. Si $F$ denota la clausura algebraica separable de $K$, denotem per $L_F$ per $L^{alg}$.*

**Definició 3.1.6.** *Diem que una corba algebraica $L$ sobre $K$ és diu que és de gènere zero si $L^{alg} = K^{alg}(t)$ per cert element transcendent $t$ sobre $K^{alg}$.*

**Exemple 3.1.7.** *Considerem $L = \mathbb{Q}(X)[y]/(y^2 + (X^2 - 1)$. Hem vist qué té un punt i per tant $L = \mathbb{Q}(t)$ on $t$ s'ha calculat explicit en el tema 1 del curs. Per tant és una corba algebraica sobre $\mathbb{Q}$ de gènere 0.*

**Exemple 3.1.8.** *Considerem $L = \mathbb{Q}(X)[y]/(y^2 + (X^2 - 3)$. Hem vist que $X^2 + Y^2 = 3$ no té cap punt racional, però a $\mathbb{Q}[\sqrt{3}]$ en té i per tant podem fer argument de la pendents $t$ per a obtenir que $L_{\mathbb{Q}(\sqrt{3})}$ és $\mathbb{Q}(\sqrt{3})(t)$ per a cert $t$ i per tant $L$ és també una corba algebraica de gènere 0.*

A partir d'ara endavant $K$ serà un cos de característica zero.
**D'ara en endavant** $car(K) = 0$.

**Definició 3.1.9.** *Una expressió $f(X,Y)=0$ on $f(X,Y)\in K[X,Y]$ s'anomena corba hiperel.líptica sobre $K$ si $L=K(X)[y]/(f(X,y))$ és una corba algebraica sobre $K$ i a més existeix $u(X',Y)=Y^2-h(X')$ amb $h\in K[X']$ i $gcd(h,h')=1$ on $L=K(X')[y]/u(X',y)$ i en particular $L$ és una extensió de grau 2 sobre el cos $K(X')$ i diem que $u(X,Y)=Y^2-h(X)$ és un model de la corba hiperel.líptica $L$ sobre $K$ on denotem el grau de $h$ amb $2g+1$ o $2g+2$ si el grau és senar o parell, on $g$ denotarà el gènere d'aquesta corba hiperel.líptica (i es pot demostrar que el gènere no depèn del model $u(X,Y)=0$ hiperel.líptic triat). En particular una corba hiperel.líptica amb gènere 1 on $h$ és de grau 3 s'anomena corba el.líptica.*

**Observació 3.1.10.** *Si tenim una equació $f(X,Y)=Y^2-h(X)=0$ on $m(X)=gcd(h,h')\neq 1$ amb $f\in K[X,Y]$ observem que en l'extensió escalars a $K^{alg}$ tenim que podem escriure $h(X)=(X-\alpha)^2h_1(X)$ per cert $\alpha\in K^{alg}$ i per tant fent el canvi $Z=\frac{Y}{(X-\alpha)}$ s'obté un isomorfisme de cossos sobre $K^{alg}$ entre $K^{alg}(X)[y]/(y^2-h(X))$ i $K^{alg}(X)[z]/(z^2-h_1(X))$ on la diferencia del grau entre $h$ i $h_1$ és dos, (el concepte de gènere de la corba es un invariant del cos de la corba algebraica $L$ sobre $K$ quan fem extensió d'escalars a $K^{alg}$, i per tant que $h$ no té arrels repetides), i en la definició anterior ja assumim que treballem amb corbes on aquesta situació ja succeeix al cos base $K$ en definir-hi l'equació.*

**Definició 3.1.11.** *Diem que dues corbes algebraiques completes $C_1,C_2$ sobre un cos $K$, són isomorfes sobre $K$ si existeix un isomorfisme entre $K(C_1)$ a $K(C_2)$ fixant $K$, on $K(C_i)$ denota el cos corresponent (que és una extensió de trascendència 1 sobre $K$).*

**Observació 3.1.12.** *Un isomorfisme entre dues corbes algebraiques completes ha de preservar el concepte de gènere, no obstant una definició de gènere associat a una corba completa i que l'isomorfisme manté aquest invariant està fora del contingut del curs. Per a les persones interesades podeu consultar chapter IX en [Lorenzini, Chapter IX].*

**Definició 3.1.13.** *(Twist de corbes) Dues corbes algebraiques completes sobre $K$: $C_1,C_2$ és diuen que una és un Twist de l'altra si existeix un isomorfisme de cossos entre $K^{alg}(C_1)$ amb $K^{alg}(C_2)$ fixant el cos $K^{alg}$.*

**Exemple 3.1.14.** *Considerem la corba algebraica sobre $\mathbb{Q}$ amb $t\in\mathbb{Q}$ donada per:*

$$tY^2-X^3-cX-d=F_t(X,Y)$$

*on $F_1(X,Y)$ correspon a una corba el.líptica $L_1:=\mathbb{Q}(X)[y]/F_t(X,y)$ i fixem-ho que el canvi $\sqrt{t}Y\leftrightarrow Y$ obté que $L_t:=\mathbb{Q}(X)[y]/F_t(X,y)$ s'obté $L_t\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{t})=L_1\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{t})$ i per tant tenim que $L_t$ amb $t\in\mathbb{Q}$ són totes twistats una de les altres, anomenats twist quadratics de la corba el.líptica $L_1$.*

*Si pensem en una equació definidora de $L_t$ com a corba el.líptica sobre $\mathbb{Q}$, observem el següent: $t\cdot Y^2=X^3+cX+d$, multipliquem per $t^3$ d'on $t^4Y^2=t^3X+ct^2tX+t^3d$ i fem el canvi de variables $(X,Y)\leftrightarrow(tX,t^2Y)$ i per tant*

$$L_t=\mathbb{Q}(X)[y]/(y^2-X^3-ct^2X-dt^3)$$

*on un model de la corba algebraica $L_t$ és la corba el.líptica $Y^2-X^3-ct^2X-dt^3$.*

### 3.1.1 Diferents models per a corbes el.líptiques

Pensem $L$ sobre $K$ una corba el.líptica, un model per a $L$ sobre $K$ és una expressió $f(X,Y)=0$ on $f(X,Y)\in K[X,Y]$ on $L=K(X)[y]/f(X,y)$ i fent un abús de notació direm $E$ corba el.líptica sobre $K$ denotant tant el cos $L$ con $E$ l'expressió $f(X,Y)=0$.

**Model de Weierstrass sobre** $K$ correspon a una expressió de la forma:

$$E: Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6 \tag{3.1}$$

amb un punt distingit $O$ corresponent a $(0,1,0)\in\mathbb{P}^2(K)$ amb $a_i\in K$. [1]

A l'expressió (3.1) fem el canvi $Y\leftrightarrow\frac{1}{2}(Y-a_1X-a_3)$ i obtenim un model isomorf a $E$ sobre $K$ de la forma:

$$E: Y^2=4X^3+b_2X^2+2b_4X+b_6 \tag{3.2}$$

on $b_2=a_1^2+4a_2$, $b_4=2a_4+a_1a_3$, $b_6=a_3^2+4a_6$ i denotem el discriminant pel polinomi en $X$ per saber si té arrels repetides o no, que escrivim per $\Delta$ i s'obté que $\Delta=-b_2^6b_6-8b_4^3-27b_6^2+9b_2b_4b_6$.

Si volem eliminar el terme en $X^2$ podem fer el canvi $(X,Y)\leftrightarrow(\frac{X-3b_2}{36},\frac{Y}{108})$ obtenim una altra equació per a $E$ sobre $K$ de la forma

$$E: Y^2=X^3-27c_4X-56c_6 \tag{3.3}$$

on $c_4=b_2^2-24b_4$, $c_6=-b_2^3+36b_2b_4-216b_6$ i el discriminant s'escriu ara per $\Delta=\frac{c_4^3-c_6^2}{1728}$.

**Definició 3.1.15.** *Donada $E$ una corba el.líptica sobre un cos $K$, amb un model (3.3) es defineix el $j$-invariant de $E$ que s'anota per $j(E)$ al valor en $K$ donat per $c_4^3/\Delta$ sempre que $\Delta\neq 0$. Fixem-nos que una corba el.líptica com hem definit té un model sobre $K$ de la forma (3.3).*

**Definició 3.1.16.** *Donada $F(X,Y)=0$ amb $F(X,Y)\in K[X,Y]$. Un punt $(x,y)\in\overline{K}^2$ s'anomena un punt singular de l'expressió $C: F(X,Y)=0$ si compleix les tres condicions següents:*

- *$F(x,y)=0$, i.e. $(x,y)$ satisfan l'equació que defineix l'expressió $C$,*
- *$\partial F/\partial X(x,y)=0$ anul.la la derivada parcial en la variable $X$,*
- *$\partial F/\partial Y(x,y)=0$ anul.la la derivada parcial en la variable $Y$.*

**Exemple 3.1.17.** *Considerem $Y^2-X^2(X+1)=F(X,Y)$. Fixeu-vos que el punt $(0,0)$ és un punt singular de l'expressió $C: F(X,Y)=0$, si fem el dibuix real s'obté que en el punt $(0,0)$ hi ha un loop, i.e. dos rectes tangents. Observem aquí $\mathbb{Q}(X)[y]/(y^2-X^2(X+1))=\mathbb{Q}(X)[u]/(u^2-(X+1))=\mathbb{Q}(u)$ on $u=y/X$ i per tant aquest cos correspon a una corba hiperel.líptica de gènere 0 i no a una corba el.líptica, on ara en l'equació del cos hem tret la singularitat del model d'equació inicial donada per l'expressió $F(X,Y)=0$.*

[1] El punt $O$ correspon a l'únic punt amb $X=0$ en la equació projectiva de la corba el.líptica $E$ i sempre està definit en el cos $K$ indiferentment que l'expressió afí (3.1) tingui alguna solució a $K^2$ o no.

*Un altre exemple però amb una cúspide seria considerear* $Y^2-X^3 = F(X,Y)$ *amb* $(0,0)$ *com a punt singular de la corba.*[2]

**Lema 3.1.18.** *Considerem* $F(X,Y) = Y^2 - X^3 - AX - B$ *amb* $A, B \in K$*, on* $h(X) = X^3 + AX + B$*. Llavors* $F(X,Y) = 0$ *té un punt singular si i només si* $\Delta = 0$ *si i només si* $gcd(h(X), h'(X)) = 1$*.*

*Demostració.* Demostrem primer que si $Y^2 - X^3 - AX - B$ té un punt singular llavors $\Delta = 0$ i $gcd(h, h') = 1$. Efectivament de $\partial F/\partial Y = 0$ s'obté $y = 0$ i de $\partial F/\partial X(x,y) = F(x,y) = 0$ tenim que $x$ és zero del polinomi $m(x) = gcd(h, h')$ i per tant el resultat, i respecte $\Delta$ sol cal observar que $\partial F/\partial X = -3X^2 - A$ d'on $3x^2+A = 0$ i $F(x,y) = 0$ tenim que $x^3+Ax+B = 0$ d'on sobté que $x = -\frac{3B}{4A}$ i per tant de $3x^2 + A = 0$ s'obté que $4A^3+27B^2 = 0$ i per tant $\Delta = -16(4A^3+27B^2)$ és zero. Deixem al lector els detalls de les altres implicacions. □

**Observació 3.1.19.** *Observem que una corba el.líptica* $E$ *sobre* $K$ *en aquest curs és un cos* $K(E)$ *ó* $L_E$ *de grau de trascendència 1 sobre* $K$ *amb un model de Weierstrass sobre* $K$ *o un model (3.2) o (3.3) sempre amb* $\Delta \neq 0$*.*

**Teorema 3.1.20.** *Dues corbes el.líptiques amb models* $F_1, F_2$ *de tipus (3.3) fixats respectivament sobre un cos* $K$*, i denotem el seu cos associat per* $K(E_1)$ *i* $K(E_2)$ *respectivament. Llavors les corbes el.líptiques són isomorfes en* $\overline{K}$ *(i.e. els cossos* $K^{alg}(C_1) \cong K^{alg}(E_2)$ *via un isomorfisme de cossos* $K^{alg}$*-linear) si i només si ambdues tenen el mateix* $j$*-invariant.*

Per fer la demostració concreta faltaria explicitat tots els possibles isomorfismes entre dos cossos obtinguts amb un model $F$ tipus (3.3) cosa que es pot demostrar usant per exemple resultats de divisors amb la teoria de Riemann de corbes algebraiques que està fora del curs en principi, per aquest motiu farem sol la demostració d'una implicació i l'altra comentarem com seria la prova si podem usar aquest resultat d'automorfismes.

*Demostració.* $\Leftarrow$ Escrivim $E_1 : Y^2 = X^3+A_1X+B_1$ i $E_2 : Y^2 = X^3+A_2X+B_2$. De tenir el mateix $j$-invariant obtenim la igualtat

$$\frac{1}{1+((27B_1^2)/(4A_1^3))} = \frac{(4A_1)^3}{(4A_1^3+27B_1^2)} = \frac{(4A_2)^3}{(4A_2^3+27B_2^2)} = \frac{1}{1+((27B_2^2)/(4A_2^3))},$$

d'aquí s'obté que $A_1^3B_2^2 = A_2^3B_1^2$. Pensem ara un $K$-isomorfisme de la forma $(x,y) = (u^2x', u^3y')$ per a portar el cos $K^{alg}(E_1)$ a $K^{alg}(E_2)$ on component $X$ o $X'$ seria la variable trascendent per a l'extensió per exemple.

Considerem tres situacions:

- $A_1 = 0$ (corresponent a $j = 0$) tenim com $\Delta \neq 0$ que $B_1 \neq 0$ i per tant $A_2 = 0$ i triem l'isomorfisme amb $u = (B_1/B_2)^{1/6} \in K^{alg}$.
- $B_1 = 0$ (correspon a $j = 1728$) de $\Delta \neq 0$ s'obté $B_2 = 0$ i prenem $u = (A_1/A_2)^{1/4} \in K^{alg}$ i d'aquí el resultat del mateix $j$-invariant

[2]Donada una corba amb una expressió $C : F(X,Y) = 0$ amb singularitats, és vol resoldre les singularitats donant una nova expressió, i aquest és un tema molt interessant en geometria algebraica i aritmètica i ben entès pel cas de corbes, però d'interés encara en superficies. Per a aprofundir en resolució de singularitats podeu consultar [Spivakovsky].

- Si $A_1B_1 \neq 0$, tenim $A_2B_2 \neq 0$ i es tria $u = (A_1/A_2)^{1/4} = (B_1/B_2)^{1/6} \in K^{alg}$ donant l'isomorfisme buscat.

Per a l'altra implicació, si tenim dues corbes el.liptiques $E_1$ i $E_2$ i cadascuna té associat un model de Weierstrass assumint que projectivitzant el model de Weierstrass correspon al punt $(0:1:0) \in mathbbP^2$ (on $f(X,Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$ per a $E_1$ i $f(X1,Y1) = Y1^2 + b_1X1Y1 + b_3Y1 - X1^3 - b_2X1^2 - b4X1 - b_6$ per a $E_2$) els únics isomorfismes possibles per $K(E_1)$ i $K(E_2)$ corresponen a $X = u^2X1 + r$ i $Y = u^3Y1 + u^2sX1 + t$ per a certs $u, r, s, t \in K^{alg}$ i d'aquí el resultat del mateix $j$-invariant [Silverman, p.49]. □

**Exemple 3.1.21.** *Recordem que els twists quadràtics $E_t : Y^2 - X^3 - ct^2X - dt^3$ amb $t$ racional i $c, d$ racionals fixats tots tenen el mateix $j$-Invariant i per tant totes elles son isomorfes en $\overline{Q}$ no obstant no necessariament sobre $\mathbb{Q}$ i les propietats aritmètiques sobre $\mathbb{Q}$ són diferents, veieu Observació 3.2.9.*

### 3.1.2 Corbes el.líptiques sobre els nombres complexos

Veurem aquí que corbes el.líptiques sobre $K = \mathbb{C}$ corresponen a un tor complex.

En aquesta secció necessitem molts preliminars que potser no tenim afiançats però que trobo útil escriure-ho en forma d'esboç per veure la interelació entre anàlisi, topologia, geometria i àlgebra.

Fixem-nos que amb el que hem introduït fins ara una corba el.líptica sobre $\mathbb{C}$ és un cos de trascendència 1 sobre els complexos de la forma: $\mathbb{C}(X)[y]/(f(X,y))$ on $f(X,Y) = 0$ pot ser un model de Weierstrass (3.1) o una expressió com (3.2) o (3.3).

**Definició 3.1.22.** *Una xarxa $\Lambda$ en $\mathbb{C}$ correspon a $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ amb $\omega_1 \in \mathbb{C}$ complint que $\omega_1\mathbb{R} + \omega_2\mathbb{R} = \mathbb{C}$.*

**Definició 3.1.23.** *Una funció el.líptica sobre una xarxa $\Lambda$ és una funció meromorfa $f(z)$ en $\mathbb{C}$ complint que $f(z + \omega) = f(z)$ per a tot $w \in \mathbb{C}$ i tot $\omega \in \Lambda$.*

**Definició 3.1.24** (Cos funcions el.líptiques)**.** *Denotem per $\mathbb{C}(\Lambda)$ el conjunt de totes les funcions el.líptiques en una xarxa fixada $\Lambda$, i es comprova que $\mathbb{C}(\Lambda)$ és un cos, extensió dels nombres complexos.*

**Lema 3.1.25.** *Una funció el.líptica sense pols (o zeros) és constant, és dir un element del cos $\mathbb{C}$.*

*Demostració.* Si $f(z) \in \mathbb{C}(\Lambda)$ holomorfa (sense pols) com $f(z + \lambda) = f(z)$ per tot $\lambda \in \Lambda$ tenim que

$$sup_{z\in\mathbb{C}}|f(z)| = sup_{z\in\overline{D}}|f(z)|$$

on $D$ és un paralelogram fonamental per $\Lambda$ definit per $D_a := \{a + r_1\omega_1 + r_2\omega_2 | 0 \leq r_i < 1\}$ amb $a \in \mathbb{C}$ i $\overline{D}_a$ el compacte més petit dins $\mathbb{C}$. Com $f$ contínua i $\overline{D}_a$ compacte obtenim que $|f(z)|$ és acotat en aquest paral.lelogram fonamental, d'on $f$ acotada a tot $\mathbb{C}$, i per tant pel curs d'Anàlisi Complexa $f$ és una constant.

Si $f$ no té zeros, $1/f$ és holomorfa i fem l'argument anterior. □

Anem a construir funcions el.líptiques no constants.

**Definició 3.1.26.** *Sigui $\Lambda \subset \mathbb{C}$ una xarxa. La funció $\wp$ de Weierstrass (relativa a $\Lambda$) es defineix per:*

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda\in\Lambda,\lambda\neq 0} (\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}).$$

*La sèrie d'Eisenstein de pes $2k$ amb $k > 1$ natural positiu per a $\Lambda$ per a la sèrie:*

$$G_{2k}(\Lambda) := \sum_{\lambda\in\Lambda\setminus 0} \lambda^{-2k}.$$

**Lema 3.1.27.** *$G_{2k}(\Lambda)$ per a $k > 1$ és absolutament convergent i defineix un nombre complex.*

*Demostració.* Es deixa al lector comprovar que existeix una constant $c = c(\Lambda)$ complint que $\forall N \geq 1$ tenim

$$\#\{\lambda \in \Lambda | N \leq |\lambda| < N+1\} < c \cdot N.$$

Llavors tenim:

$$\sum_{\lambda\in\Lambda,|\lambda|\geq 1} \frac{1}{|\lambda|^{2k}} \leq \sum_{N=1}^{\infty} \frac{\#\{\lambda \in \Lambda | N \leq |\lambda| < N+1\}}{N^{2k}} < \sum_{N=1}^{\infty} \frac{c}{N^{2k-1}} < \infty.$$

□

**Teorema 3.1.28.** *La funció $\wp_\Lambda(z)$ convergeix absolutament i defineix una funció meromorfa amb un pol doble amb residu 0 en cada punt de la xarxa $\Lambda$ i no té altres pols. A més $\wp_\Lambda(z) \in \mathbb{C}(\Lambda)$ i és parell, (és a dir $\wp_\Lambda(-z) = \wp_\Lambda(z)$), i $\wp'_\Lambda(z) \in \mathbb{C}(\Lambda)$ i és una funció senar.*

*Demostració.* Observem que per $z \in \mathbb{C} \setminus \Lambda$ que fixem tenim llavors

$$|\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}| = |\frac{z(2\lambda - z)}{\lambda^2(z-\lambda)^2}| \leq \frac{10|z|}{|\lambda|^3},$$

on en l'última desigualtat usem que es compleix $|\lambda| > 2|z|$ per a la major part del sumatori de la $\wp$-Weierstrass llevat d'un nombre finit de summands de $\lambda \in \Lambda$. Ara de la demostració del Lemma 3.1.27 per a sèries d'Eisenstein anterior, obtenim que $\wp_\Lambda(z)$ convergeix absolutament per a $z \in \mathbb{C} \setminus \Lambda$ fixat. Per construcció $\wp_\Lambda$ té un pol doble amb residu 0 per a cada $\lambda \in \Lambda$ i $\wp_\Lambda(z) = \wp_\Lambda(-z)$.

Veiem tot seguit que $\wp_\Lambda \in \mathbb{C}(\Lambda)$.

Considerem ara la derivada de $\wp_\Lambda(z)$, i per la convergència absoluta podem derivar terme a terme obtenim

$$\wp'_\Lambda(z) = -2\sum_{\lambda\in\Lambda} \frac{1}{(z-\lambda)^3}$$

i clarament per la seva expressió $\wp'_\Lambda(z) \in \mathbb{C}(\Lambda)$ i per tant integrant-la s'obté

$$\wp_\Lambda(z+\lambda) = \wp_\Lambda(z) + constant(\lambda)$$

per a tot $z \in \mathbb{C} \setminus \Lambda$. Triant $z = -\lambda/2$ obtenim que $quec(\lambda) = 0$ i per tant $\wp_\Lambda(z) \in \mathbb{C}(\Lambda)$. □

Necessitem ara introduir alguns resultats d'Anàlisi complexa per a demostrar que cos $\mathbb{C}(\Lambda)$ està generat per les funcions el.líptiques $\wp_\Lambda$ i $\wp'_\Lambda$.[3]

**Definició 3.1.29.** *Donada $f \in \mathbb{C}(\Lambda)$ i $w \in \mathbb{C}$ definim per*

- *$ord_w(f)$ ordre d'anul.lació de la funció $f$ en $w$,*
- *$res_w(f)$ el residu de la funció $f$ en $w$.*

**Proposició 3.1.30.** *Donada $f \in \mathbb{C}(\Lambda)$ llavors:*

1. $\sum_{w\in\mathbb{C}/\Lambda} res_w(f) = 0$,
2. $\sum_{w\in\mathbb{C}/\Lambda} ord_w(f) = 0$,
3. $\sum_{w\in\mathbb{C}/\Lambda} ord_w(f)\cdot w \in \Lambda \subset \mathbb{C}$.

*Demostració.* Pensem que podem pensar la funció $f$ en el tor $\mathbb{C}/\Lambda$. Triem un paral.lelogram fonamental $D_a$ per a $\Lambda$ on $f(z)$ no tingui zeros ni pols en la frontera de $D_a$. Apliquem ara el teorema del residu a la funció $f$ obtenim

$$\sum_{w\in\mathbb{C}/\Lambda} res_w(f) = \frac{1}{2\pi i}\int_{\partial D_a} f(z)dz.$$

Ara com $f$ és periodica en elements de $\Lambda$ la integral a traves de costats oposats del paral.lelogram $D_a$ es cancel.len i per tant la integral a la vora de $D_a$ és zero obtenim el primer punt de la proposició.

Observem que com $f$ és períodica, també s'obté que la seva derivada compleix $f'(z) \in \mathbb{C}(\Lambda)$. Aplicant el teorema del residu a $f(z)/f'(z)$ obtenim

$$\sum_{w\in\mathbb{C}/\Lambda} ord_w(f) = \int_{\partial D_{a'}} \frac{f'(z)}{f(z)}dz$$

on l'integral és zero de ser el.líptica la funció.

Apliquem, per a demostrar l'últim punt de la proposició, el teorema del residu a la funció $zf'(z)/f(z)$. S'obté

$$\sum_{w\in\mathbb{C}/\Lambda} ord_w(f)w = \frac{1}{2\pi i}\int_{D_a} zf'(z)/f(z)dz.$$

Trenquem la integral en 4 integrals recorrent la vora del paral.lelogram $D_a$ que elegim que no té zerons ni pols en aquesta frontera, aquests 4 intervals corresponen a: $[a, a+\omega_1]$, $[a+\omega_1, a+\omega_1+\omega_2]$, $[a+\omega_1+\omega_2, a+\omega_2]$ i $[a+\omega_2, a]$. En el segon i tercera integral corresponent al segon i tercer interval fem el canvi de variables $z \to z-\omega_1$ (respectivament $z \to z-\omega_2$) i per la periodicitat de $f'/f$ obtenim

$$\sum_{w\in\mathbb{C}/\Lambda} ord_w(f)w = -\frac{\omega_2}{2\pi i}\int_a^{a+\omega_1} \frac{f'(z)}{f(z)}dz + \frac{\omega_1}{2\pi i}\int_a^{a+\omega_2} \frac{f'(z)}{f(z)}dz.$$

Un resultat de funcions meromorfes $g(z)$ d'anàlisi complexa afirma que la integral $\frac{1}{2\pi i}\int_a^b \frac{g'(z)}{g(z)}dz$ és el número de voltes al voltant del zero del camí $[0,1] \to \mathbb{C}$: $t \mapsto g((1-t)a+tb)$, i si $g(a) = g(b)$ l'integral és un enter, per la periodicitat de $f'/f$ s'obé el resultat. □

[3] La funció $\zeta_\Lambda$ i $\zeta'_\Lambda$ són un anàleg del que són les funcions sin i cos per a la corba de gènere 0 $\mathbb{C}(X)[y]/(y^2 - X^2 - 1)$ en l'inici del curs.

**Definició 3.1.31.** *L'ordre d'una funció el.líptica és el seu nombre de pols (comptats amb multiplicitat) en qualsevol parel.lelogram fonamental.*

**Corol·lari 3.1.32.** *Una funció el.líptica no constant té ordre almenys 2.*

*Demostració.* Si $f(z)$ fos holomorfa seria constant. Assumim que tingués sol un pol simple, llavors el residu al pol únic no podria ser zero però pel lema anterior no és possible ja que la suma de tots els residus de tots els pols és igual a zero. □

**Definició 3.1.33.** *El grup de divisors de $\mathbb{C}/\Lambda$ consisteix amb el grup abelià lliure generat per $[w]$ amb $[w] \in \mathbb{C}/\Lambda$, és a dir els elements corresponen a $\sum_{[w]\in\mathbb{C}/\Lambda} n_{[w]}[w]$ amb $n_{[w]}$ enters on $n_{[w]} = 0$ per tot $[w]$ llevat d'un nombre finit. És defineix el grau d'un divisor $D = \sum_{[w]\in\mathbb{C}/\Lambda} n_{[w],D}[w]$ a l'enter $\sum n_{[w],D}$ i s'anota $deg(D)$.*

Donada $f \in \mathbb{C}(\Lambda)^* = \mathbb{C}(\Lambda) \setminus \{0\}$ definim el divisor de la funció $f$ i s'anotarà per $div(f)$ al divisor

$$div(f) := \sum_{[w]\in\mathbb{C}/\Lambda} ord_{[w]}(f)([w]) \in Div(\mathbb{C}/\Lambda),$$

on pel lemma anterior $\sum_{[w]} n_{[w]} = 0$ i sol un numero finit de $n_{[w]}$ són no zeros, i per tant

$$div(f) \in Div^0(\mathbb{C}/\Lambda) := \{D \in Div(\mathbb{C}/\Lambda) | deg(D) = 0\}.$$

Escrivim $C(\mathbb{C}) := \mathbb{C}/\Lambda$ i considerem $div : \mathbb{C}(\Lambda)^* \to Div^0(C(\mathbb{C}))$ donada per $f \mapsto div(f)$ i el morfisme $Add : Div^0(C(\mathbb{C})) \to C(\mathbb{C})$ via $\sum n_{[w]}[w] \mapsto \sum n_{[w]} w \ mod \ \Lambda$.

**Corol·lari 3.1.34.** *La successió de grups commutatius*

$$1 \to \mathbb{C}^* \to \mathbb{C}(\Lambda)^* \to^{div} Div^0(C(\mathbb{C})) \to^{Add} C(\mathbb{C}) \to 0$$

*és exacta.*[4]

*Demostració.* Es clar que el nucli de $div$ són les funcions el.líptiques constants. Que la imatge de $div$ és dins el nucli de $Add$ prové del tercer punt en la Proposició 3.1.30. Ara sobre l'epimorfisme de $Add$ prové de $Add([w] - [0]) = w$. Falta demostrar tan sols que $Ker(Add) \subseteq Im(div)$, ho provem en la Proposició 3.1.35. □

Per a demostrar aquest resultat necessitem resultats d'Anàlisi complexa de funcions donades per productes infinits, veieu qualsevol llibre d'Anàlisi complexa com a referència.

**Proposició 3.1.35.** *Siguin $m_1, \ldots, m_k \in \mathbb{Z}$ i nombres complexos $z_1, \ldots, z_k \in \mathbb{C}$ complint que $\sum_{i=1}^k m_i = 0$ i $\sum_i m_i z_i \in \Lambda$. Llavors existeix una funció el.líptica $f \in \mathbb{C}(\Lambda)$ complint $div(f) = \sum_{i=1}^k m_i[z_i]$ i per tant $Ker(Add) = Im(div)$.*

[4]El grup $Div^0(\mathbb{C}/\Lambda)/Im(div)$ s'anomena grup de Picard. Donat un cos $L$ de trascendència 1 sobre $\mathbb{C}$ o un cos algebraicament tantat li podem associar aquest grup de divisors i de Picard i obtenim molta informació de la corba algebraica $L$, veieu [Lorenzini, chp X].

*Demostració.* Considerem primer fa funció $\sigma$ de Weierstrass definida per

$$\sigma_\Lambda(z) := z \prod_{w \in \Lambda \setminus 0} \left(1 - \frac{z}{w}\right) e^{\frac{(z/w)+(z/w)^2}{2}},$$

i és pot demostrar (veieu una prova a [Silverman, Lemma 3.3] ) que és holomorfa a tot $\mathbb{C}$ amb zeros simples per a cada $\lambda \in \Lambda$ i no té més zeros (per tant es prova que $div(\sigma_\Lambda(z-u)) = [u] - [t]$ per cert $t$ independent de $u$), compleix $\frac{d^2}{dz^2} \log \sigma_\Lambda(z) = -\wp_\Lambda(z)$ $\forall z \in \mathbb{C} \setminus \Lambda$ i per a qualsevol $\lambda \in \Lambda$ existeixen constants $a, b \in \mathbb{C}$ complint

$$\sigma_\Lambda(z+\lambda) = e^{az+b}\sigma_\Lambda(z)$$

per a tot $z \in \mathbb{C}$.

Ara ja podem demostrar la proposició.

Escrivim $\sum m_i z_i =: \lambda \in \Lambda$, i considerem $D = \sum_{i=1}^k m_i[z_i] - [\lambda] + [0] \in Div^0(\mathbb{C}/\Lambda)$, i considerem la funció

$$f(z) := (\prod_{i=1}^k \sigma_\Lambda(z-z_i)^{m_i}) \cdot \sigma_\Lambda(z-\lambda)^{-1}\sigma_\Lambda(z)$$

on per construcció tenim que $div(f) = D$.

Observem tot seguit que $f(z+\lambda)/f(z) =$

$$e^{a(z-\lambda)+b}e^{az+b}\prod_{i=1}^k e^{(a(z-z_i)+b)n_i} = e^{(az+b)(\sum m_i+1-1)}e^{-a(0-\lambda+\sum m_i z_i)} = 1$$

i per tant $f \in \mathbb{C}(\Lambda)$. □

Veiem la relació de la definició de corba el.líptica com a cos de trascendència 1 sobre els complexos amb el cos de les funcions el.líptiques.

**Teorema 3.1.36.** *El cos $\mathbb{C}(\Lambda)$ és un cos de trascendència 1 sobre els complexos i compleix les següents condicions*

1. $\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda(z), \wp'_\Lambda(z))$,
2. *La serie de Laurent al voltant de $z = 0$ és $\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{k=1}^\infty (2+1)G_{2k+2}(\Lambda)z^{2k}$*
3. $\forall z \in \mathbb{C} \setminus \Lambda$, *tenim*

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - 60G_4(\Lambda)\wp_\Lambda(z) - 140G_6(\Lambda).$$

*Demostració.* • Considerem $f(z) \in \mathbb{C}(\Lambda)$ i podem escriure $f(z) = \frac{1}{2}(f(z) + f(-z)) + \frac{1}{2}(f(z) - f(-z))$ i per tant es suficient demostrar per a funcions parelles i funcions senars que pertanyin a $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$.

Si $f$ és senar llavors $\wp'_\Lambda(z)f(z)$ és parell, per tant podem reduir-nos a suposar $f \in \mathbb{C}(\Lambda)$ parell. Tenim llavors la igualtat en la derivada $i$-èssima: $f^{(i)}(z) = (-1)^i f^{(i)}(-z)$ i $ord_z(f) = ord_{-z}(f)$. Ara si $2w \in Lambda$ s'obté $f^{(i)}(w) = 0$ per a $i$ senar i per tant $ord_w(f)$ és parell. Considerem

un paral.lelogram fonamental $D_a$ i pensem en la meitat d'ell, via la paritat amb $\pm 1$, diem-li $H$ on $(H+\Lambda)\cup(-H+\Lambda)=\mathbb{C}$, llavors podem escriure

$$div(f)=\sum_{w\in H} m_w([w]+[-w]).$$

Considerem la funció $g(z):=\prod_{w\in H\setminus 0}(\wp_\Lambda(z)-\wp_\Lambda(w))^{m_w}$ on $div(\wp_\Lambda(z)-\wp_\Lambda(w))=[w]+[-w]-2[0]$ i per tant de com controlem els pols i zeros que $\frac{f(z)}{g(z)}$ és una funció el.líptica holomorfa sense zeros ni pols, i per tant constant d'aquí obtenim que $f(z)\in\mathbb{C}(\wp_\Lambda,\wp'_\Lambda)$.

- Anem a estudiar el desenvolupament de Laurent de $\wp_\Lambda$ al voltant de $z=0$. Si $|z|<|\lambda$ podem escriure:

$$(z-\lambda)^{-2}-\lambda^{-2}=\lambda^{-2}((1-(z/\lambda))^{-2}-1)=\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\lambda^{n+2}},$$

D'aquí obtenim

$$\wp_\Lambda(z)=\frac{1}{z^2}+\sum_{\lambda\in\Lambda\setminus 0}(\sum_{n=1}^{\infty}\frac{(n+1)z^n}{\lambda^{n+2}})=$$

$$z^{-2}+\sum_{n=1}^{\infty}(n+1)z^n(\sum_{\lambda\in\Lambda\setminus 0}\frac{1}{\lambda^{n+2}}),$$

que és l'expressió buscada, ja que observem que si $n+2$ és senar $\sum_{\lambda\in\Lambda\setminus 0}\frac{1}{\lambda^{n+2}}=0$ ja que com és absolutament convergent, podem reordenar i $-\lambda\in\Lambda$ per tot $\lambda\in\Lambda$.

- Observem que tenim les següents expressions de Laurent al voltant de $z=0$:

$$\wp_\Lambda(z)=z^{-2}+3G_4(\Lambda)z^2+\dots$$

$$\wp_\Lambda(z)^3=z^{-6}+9G_4(\Lambda)z^{-2}+15G_6(\Lambda)+\dots$$

$$\wp'_\Lambda(z)^2=4z^{-6}-24G_4(\Lambda)z^{-2}-80G_6(\Lambda)+\dots$$

d'on la funció el.líptica $f(z)=\wp'_\Lambda(z)^2-4\wp_\Lambda(z)^3+60G_4(\Lambda)\wp_\Lambda(z)+140G_6(\Lambda)$ s'anul.la en $z=0$ per construcció i és una funció holomorfa al voltant de $z=0$ i per tant és constant. Com $f(0)=0$ obtenim el resultat que $f(z)$ és la funció constant zero.

□

**Observació 3.1.37.** Podem pensar la $\wp_\Lambda$ anàleg de les funcions sin i cos per $x^2+y^2=1$ ara per corba el.líptica $y^2=x^3+G_4(\Lambda)x+G_6(\lambda)$, que dóna una parametrització de la corba el.líptica per funcions analítiques.

**Corol·lari 3.1.38.** *Donada $\Lambda$ una xarxa en $\mathbb{C}$ obtenim que $\mathbb{C}(\Lambda)$ és una corba el.líptica sobre $\mathbb{C}$.*

*Demostració.* Sol cal demostrar que $P(X) = 4X^3 - 60G_4(\Lambda)X - 140G_6(\Lambda)$ no té arrels repetides, o equivalentment que el discriminant és no zero, aquest valor correspon a $\Delta(\Lambda) := \Delta(Y^2 - (P(X))) = (60G_4(\Lambda))^3 - 27(140G_6(\Lambda))^2$. Recordem que escrivim $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ i denotem per $\omega_3 := \omega_1 + \omega_2$, i com $\wp'_\Lambda(z)$ és una funció el.líptica senar obtenim que $\wp'_\Lambda(\omega_i/2) = 0$ i per tant $P(x)$ s'anul.la en $x = \wp_\Lambda(\omega_i/2)$ per $i = 1, 2, 3$. Veiem són aquests tres valors diferents.

Considerem la funció $\wp_\Lambda(z) - \wp_\Lambda(w_i/2)$ amb $i$ fixat. És una funció parell, per tant té un zero doble en $z = w_i/2$, però $\wp_\Lambda$ sol té un pol ordre 2 i com el grau del divisor de la funció és zero no pot haver-hi altre zero per tant els tres valors són diferents on obtenim que $\mathbb{C}(\Lambda)$ és una corba el.líptica sobre $\mathbb{C}$. □

**Teorema 3.1.39** (Teorema d'Uniformització)**.** *Tota corba el.líptica sobre $\mathbb{C}$ correspon a $\mathbb{C}(\Lambda)$ per a certa xarxa $\Lambda$ i per a cada xarxa $\Lambda$ li correspon una corba el.líptica sobre $\mathbb{C}$.*

Per a una demostració cosulteu [Serre, VII Prop 5], [Shimura, §4.2].

**Definició 3.1.40** ($K$-punts)**.** *Considerem una corba el.líptica $L$ sobre $K$ amb $L = K(X)[y]/y^2 - h(X)$ on $h(X)$ polinomi de grau 3 en variable $X$ a coeficients al cos $K$ amb $gcd(h, h') = 1$. Els $K$-punts de la corba el.líptica denota el conjunt que denotarem per $E_L(K)$ i que correspon a*

$$E_L(K) := \{(x, t) \in K^2 | t^2 = h(x)\} \cup \{O = (0 : 1 : 0)\}$$

*que corresponen als zeros dins $\mathbb{P}^2(K)$ de projectivitzar l'equació $T^2 - h(X)$ em a l'anell de polinomis en les variables $T, X$ a coeficients al cos $K$.*

**Observació 3.1.41.** *Hi ha una bijecció entre els ideals maximals $\mathfrak{m}$ de l'anell $A = K[X][y]/(y^2 - h(X)) \subset L$ on $A/\mathfrak{m} \cong K$ amb $E_L(K) \setminus 0$, o equivalentment entre morfismes d'anells que van de $A$ al cos $K$. En particular si $K = \mathbb{C}$ els ideals maximals de $A$ están amb bijecció amb $E_L(\mathbb{C}) \setminus 0$ ja que en general $A/\mathfrak{m}$ sempre és una extensió finita de $K$ per a tot ideal maximal del domini $A$ (per aprofundir-ho consulteu [Lorenzini, Chapter X]).*

**Proposició 3.1.42.** *Tenim una bijecció*

$$UnifMap : \mathbb{C}/\Lambda \to E_L(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$$

*donada per $[z] \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z) : 1)$ quan $[z] \neq [0]$ i $[0] \mapsto 0 = (0 : 1 : 0)$.*[5]

*Demostració.* Tenim que està ben definida per un teorema anterior. Provem primer que $UnifMap$ és exhaustiva, i considerem $(x, y) \in E_L(\mathbb{C}) \setminus 0$. Observem que $g(z) := \wp_\Lambda(z) - x$ és una funció el.líptica no constant, per tant té un zero (el grau del divisor $deg(g)$ és zero i $g$ té pol en $z = 0$), on $g(z) = 0$ amb $a \in \mathbb{C} \setminus \Lambda$, per tant de ser $(x, y) \in E_L(\mathbb{C})$ obtenim que $y^2 = \wp'_\Lambda(a)$, canviant $a$ per $-a$ si fos necessari, s'obté que $y = \wp'_\Lambda(a)$ i per tant l'exhaustivitat.

Suposem ara que $UnifMap([z_1]) = UnifMap([z_2])$. Suposem primer que $2z_1 \notin \Lambda$. Llavors podem observar que la funció $m(z) := \wp_\Lambda(z) - \wp_\Lambda(z_1)$ té ordre 2 i zeros en $[z_1]$, $[-z_1]$, $[z_2]$ i per tant $z_2 \equiv \pm z_1 \ mod\ \Lambda$ i com $\wp'_\Lambda(z_1) = \wp'_\Lambda(z_2) = \wp'_\Lambda(\pm z_1) = \pm\wp'_\Lambda(z_1)$ de ser funció senar s'obté que $[z_1] = [z_2]$ (ja que de la prova de ser $(h, h') = 1$ corba el.líptica es prova que $\wp'_\Lambda(z_1) \neq 0$). Suposem ara $2z_1 \in \Lambda$, tenim $n(z) := \wp_\Lambda(z) - \wp_\Lambda(z_1)$ té un zero doble en $z_1$ i s'anul.la en $z_2$ concloent altre cop que $[z_1] = [z_2] \in \mathbb{C}/\Lambda$. □

[5] Fixeu-vos que $\mathbb{C}/\Lambda$ és un grup abelià, i aquest morfisme d'uniformització podem traslladar a una suma en $E_L(\mathbb{C})$. Les varietats algebraiques on els $\mathbb{C}$-punts tenen una operació suma s'anomenen varietats abelianes, podeu aprofundir-hi en aquestes en [Shimura2, Chp I].

## 3.2 Estructura de grup abelià per a $E_L(K)$, $L$ corba el.líptica

Considerem $L$ una corba el.líptica sobre $K$ de la forma $L = K(X)[y]/(y^2 - X^3 - cX - d)$ amb $c, d \in K$, tenim definit els $K$-punts via $E_L(K)$, i anem a traslladar la suma de $\mathbb{C}/\Lambda$ de lúltim resultat de l'apartat anterior a $E_L(K)$ però vàlida per a tot cos $K$ (de car. zero per simplificar, recordeu).

1. $O = (0 : 1 : 0)$ és l'element neutre de $E_L(K)$.

2. si $P, Q \in E_L(K)$ i $P = (x_1, y_1) \neq 0$ i $Q = (x_2, y_2) \neq 0$ amb $P \neq Q$ denotem per $R = (x_3, y_3) \in E_F(K)$ el tercer punt de la intersecció de $Y^2 - X^3 - cX - d = 0$ amb la recta que passe pels punts $P$, i $Q$, i observem que $(x_3, -y_3) \in E_F(K)$ i definim $P + Q := (x_3, -y_3)$.
   Anem-ho a expressar-ho amb equacions per veure que l'assignació anterior té sentit:
   La recta que passe pels dos punts, si $x_1 \neq x_2$ correspon a:
   $$Y = \frac{y_2 - y_1}{x_2 - x_1}(X - x_1) + y_1$$
   i substituint-ho a $Y^2 = X^3 + cX + d$ obtenim $M(X) = X^3 + rX^2 + sX + t$ amb $r, s, t \in K$, on $M(x_1) = M(x_2) = 0$ i per tant en $K[X]$ tenim $M(X) = (X - x_1)(X - x_2)(X - x_3)$ amb $x_3 \in K$, concretament el tercer punt de tall és:
   $$(x_3, y_3) = (\frac{(y_2 - y_1)^2}{(x_2 - x_1)^2} - x_1 - x_2, \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) + y_1),$$
   per tant $P + Q \in E_L(K)$.

3. Si suposem que $x_1 = x_2$ i $P \neq Q$, tenim $y_1 = -y_2$ definim llavors $P + Q = O$.

4. si $P, Q \in E_L(K)$ i $P = (x_1, y_1) \neq 0$ i $Q = (x_2, y_2) \neq 0$ amb $P = Q$ denotem per $R = (x_3, y_3) \in E_F(K)$ el tercer punt de la intersecció de $M(X, Y) := Y^2 - X^3 - cX - d = 0$ amb la recta tangent de $M(X, Y)$ que passe pels punt $P = Q$ , i observem que $(x_3, -y_3) \in E_F(K)$ i definim $P + Q := (x_3, -y_3)$.
   Anem-ho a detallar. La recta tangent a $Y^2 = X^3 + cX + d$ pel punt $P = Q = (x_1, y_1)$ correspon a:
   $$Y = \frac{3x_1^2 + c}{2y_1}(X - x_1) + y_1$$
   i sustituint la $Y$ a $Y^2 = X^3 + cX + d$ obtenim $qX^3 + rX^2 + sX + t = 0$ amb $q, r, s, t \in K$ amb $q \neq 0$ i com $X = x_1$ és una solució doble, tenim $qX^3 + rX^2 + sX + t = q(X - x_1)^2(X - x_3) \in K[X]$, i per tant $x_3 \in K$, donant $(x_3, y_4)$ un punt de tall de la recta tangent de la corba, definim llavors $P + Q = P + P = 2P$ pel punt $(x_3, y_3) \in E_L(K)$ següent
   $$2P = P + P =$$
   $$(\frac{1}{4y_1^2}(x_1^4 - 2cx_1^2 - 8dx_1 + c^2), \frac{1}{8y_1^3}(x_1^6 + 5cx_1^4 + 20a^2dx_1^3 - 5c^2x_1^2 - 4cdx_1 - 8d^2 - c^3)).$$

**Teorema 3.2.1.** *Donada $L/K$ una corba el.líptica, tenim $(E_L(K), +)$ és un grup abelià.*

Podeu consultat una prova a [Silverman, Chapter III,§2] i el cas $(E_L(\mathbb{C}), +) \cong (\mathbb{C}/\Lambda, +)$ una referència en [Shimura, §4], [Serre, VII].

**Lema 3.2.2.** *Si $L$ una corba el.líptica sobre $\mathbb{C}$, llavors $E_L(\mathbb{C})$ és un grup abelià no finit generat.*

*Demostració.* Aquest grup abelià correspon a $\mathbb{C}/\Lambda$ amb la suma usual dels nombres complexos i com a conjunt correspon bijectivament a $D_a$ per cert $a \in \mathbb{C}$ fixat, per tant no numerable, en particular no pot ser finit generat. □

No obstant tenim el següent resultat

**Teorema 3.2.3** (Mordel)**.** *Sigui $K/\mathbb{Q}$ una extensió finita i $L$ una corba el.líptica sobre $K$ llavors el grup abelià $E_L(K)$ és finit generat, i denotem el seu rank per $rank_K E_L$ i la seva torsió per $E_L(K)_{tors}$.*

La demostració del teorema no la farem, per una referència de la prova, consulteu una demostració per a $K = \mathbb{Q}$ en [Silverman, VIII,§4].

Hi ha algoritmes per $c, d$ enters no molt grans per a calcular el rank i la torsió de corbes el.líptiques $L = \mathbb{Q}(X)[y]/(y^2 - X^3 - cX - d)$ sobre $\mathbb{Q}$

Per exemple amb Magma calculator online

```
http://magma.maths.usyd.edu.au/calc/
```

podem fer molts càlculs per a corbes el.líptiques i hiperel.líptiques consulteu CHAPTER 10 del manual de MAGMA, en particular per corbes el.líptiques sobre $\mathbb{Q}$ podem introduir el codi següent per a calcular-ne el rank sobre $\mathbb{Q}$ dels $\mathbb{Q}$-punts i el grup de torsió dels $\mathbb{Q}$-punts per a $Y^2 = X^3 + cX + d$:

```
c:= 2;
d:=1;
P<x>:=PolynomialRing(RationalField());
if Discriminant(x^3+c*x+d) ne 0 then
E:=EllipticCurve([c,d]);
print E;
Rank(E);
TorsionSubgroup(E);
P:=Points(E: Bound:=100);
P;
Generators(E);
end if;
```

On $Points(E : Bound := 100)$ dóna un conjunt de punts racionals de la corba on tinguin altura menor que 100, i $Gerenators(E)$ dón generadors de la part lliure de torsió i de la torsió per a $E_L(\mathbb{Q})$. La idea d'altura, és clau per Magma per calcular punts en corbes de gènere arbitrari, però heuristicament per genere $\geq 2$ tots els punts tindran altura petita, en canvi per a gènere 1 pot succeir obtenir generadors de la part lliure de torsió amb altura molt i molt gran, per aprofundir en altures en corbes el.líptiques podeu consultat [Silverman, Chapter VIII,§6].

Canviant $c$ i $d$ obtenim diferents corbes el.líptiques sobre els racionals que Magma es surt de calcular, on calculem primer el discriminant per no haver-hi arrels repetides i correspongui a una corba completa i més concretament una corba el.líptica.

Hi ha els següents resultats fora dels continguts del curs (consulteu per exemple [Herrerias]):

**Teorema 3.2.4** (Mazur, 1977)**.** *Donada L una corba el.líptica sobre $\mathbb{Q}$, llavors $E_L(\mathbb{Q})_{tors}$ sol pot ser un de la llista finita següent:*

1. $\mathbb{Z}/n$ *on* $1 \leq n \leq 10$ *o* $n = 12$
2. $\mathbb{Z}/n \oplus \mathbb{Z}/2$ *on* $n = 2, 4, 6$ *ó 8.*

*A més fixat G un dels grups finits anteriors, llavors existeix una corba el.líptica sobre $\mathbb{Q}$ amb $E_L(\mathbb{Q})_{tors} = G$.*

**Conjectura 3.2.5** (del Rang)**.** *Donat $r \in \mathbb{N} > 0$, llavors existeix $L_r$ corba el.líptica sobre $\mathbb{Q}$ complint que $rank_{\mathbb{Q}} E_{L_r}(\mathbb{Q}) > r$.*

**Observació 3.2.6.** *En el moment actual el rècord d'un rank per una corba el.líptica sobre $\mathbb{Q}$ és rank almenys 28 trobada per Noam Elkies l'any 2006, donada per*

$$y^2 2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x +$$

$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9.$$

*i fins l'any 2021 és la que té rank màxim (as far as I know!). Consulteu [Elkies-Klagsbrun] per a aprofundir-hi.*

**Observació 3.2.7.** *Generalitzant el teorema de Mordel, hi ha el teorema de Mordel-Lang que afirma si $M/k$ és una extensió de cossos finit generada i L una corba el.líptica sobre k llavors $E_L(M)$ és un grup abelià finit generat.*

**Observació 3.2.8.** *Una corba el.líptica sobre $\mathbb{C}$ "correspon" a $\mathbb{C}/\Lambda$. Aquest concepte es pot generalitzar i no restringir-ho a corbes, parlant de varietats abelianes que sobre $\mathbb{C}$ correspondria a $\mathbb{C}^d/\tilde{\Lambda}$ en una xarxa discreta de $\mathbb{Z}$-rang $2d$ amb un aparellament bilineal concret. El resultat de Mordel per corbes el.líptiques també té un anàleg en varietats abelianes que no anem a detallar en aquest apunts, veieu [Shimura].*

**Observació 3.2.9.** *Hem parlat abans que les corbes el.líptiques*

$$E_t : Y^2 = X^3 + t^2 cX + t^3 d$$

*amb $c, d \in \mathbb{Q}$ fixats i variant $t \in \mathbb{Q}$ donen corbes el.líptiques (suposant $h(X) = X^3 + t^2 cX + t^3 d$ no té arrels repetides) amb el mateix $j$ invariant per tant son isomorfes en la clausura algebraica sobre $\mathbb{Q}$. No obstant no són isomorfes sobre el cos $\mathbb{Q}$ moltes d'elles, per exemple usant Magma online podem calcular $rank_{\mathbb{Q}} L_{E_t}(\mathbb{Q})$ i si no són iguals es pot demostrar que no són isomorfes sobre els racionals les corbes el.líptiques corresponents (amb una mica més de teoria del que hem fet fins ara):*

```
c:=2; d:=1;
d:=1;
P<x>:=PolynomialRing(RationalField());
for t in [-10..10] do
if Discriminant(x^3+t^2*c*x+t^3*d) ne 0 then
E:=EllipticCurve([c*t^2,d*t^3]);
print E;
Rank(E);
end if;
end for;
```

*S'obté per exemple* $rank_{\mathbb{Q}}(L_{E_{-2}}) = 2$, $rank_{\mathbb{Q}}(L_{E_{-1}}) = 0$ *i* $rank_{\mathbb{Q}}(L_{E_1}) = 0$, *on totes* $jInvariant(E) = \frac{55296}{59}$, *i per tant són isomorfes en la clausura sobre* $\mathbb{Q}$ *però* $L_{E_{-2}}$, $L_{E_{-1}}$ *i* $L_{E_1}$ *no són corbes el.líptiques isomorfes una a l'altra sobre els racionals.*

**Observació 3.2.10.** *Les corbes de la forma* $Y^2 = f(X)$ *amb* $f(X)$ *de grau 4 amb* $mcd(f, f') = 1$ *obtenim que* $L = K(X)[y]/(y^2 - f(X))$ *forma una corba hiperel.líptica de gènere 1, però si* $K$ *no és algebraicament tancat no necessàriament* $L$ *és una corba el.líptica sobre* $K$*, i l'estudi aritmètic de corbes de gènere 1 que no són corbes el.líptiques sobre un cos* $K$ *fix tenen molt interés aritmètic, consulteu per exemple [Silverman, ChpII,Ex.2.5.1].*

## 3.3 Exercici dirigit: corbes el.líptiques.

**Definició 3.3.1.** *Una corba el.líptica sobre un cos* $K$ *amb* $car(K) \neq 2, 3$ *es donada per l'equació polinomial:*

$$E : Y^2Z = aX^3 + bX^2Z + cXZ^2 + dZ^3$$

*amb* $a, b, c, d \in K$, $a \neq 0$ *i* $mcd(aX^3 + bX^2 + cX + d, 3aX^2 + 2bX + c) = 1$.

Per a tota extensió finita de cossos $L/K$ escrivim $E(L)$ els punts $(x : y : z) \in \mathbb{P}^2(L)$ complint $y^2z = ax^3 + bx^2z + cxz^2 + dz^3$. Fixeu-vos que sempre tenim el punt $O := (0 : 1 : 0) \in E(K)$ fent $Z = 0$ a l'equació de $E$.

Podem pensar $E(L)$ com la solucions $(x, y) \in L^2$ complint $Y^2 = aX^3 + bx^2 + cX + d$ (corresponent als punts $(x : y : 1) \in \mathbb{P}^2(L)$ solució de $Y^2Z = aX^3 + bX^2Z + cXZ^2 + dZ^3$) unió el punt que diem de l'infinit $O$ (corresponent a $(0 : 1 : 0)$).

El fet crucial i singular de les corbes $E$ és que $E(L)$ té estructura de grup abelià, amb operació suma donada de la forma següent:

i) el punt $O$ és l'element identitat o zero (en notació aditiva),
ii) l'oposat d'un punt $P = (x : y : 1) \in E(L) - O$ és $(x : -y : 1)$,
iii) Per definir la suma de dos punts es suficient definir-la per a $P = (x_1 : y_1 : 1)$ i $Q = (x_2 : y_2 : 1)$ d'$E(L)$. Sigui $S$ el tercer punt que talla la recta que passe pel punts $P$ i $Q$ amb l'equació $E$, si $R = (a : b : 1)$ llavors definim $P + Q = (a : -b : 1)$ (on si $P = Q$ es pren la recta tangent pel punt $P$ i que talla en un altre punt amb $E$, que diem $R$). En el cas que $R = O$ es defineix $P + Q = O$.

ecs.png

Dibuix que reprodueix la suma de punts on dibuixem tan sols els punts reals de la corba $E$ concreta que especifica.

**Proposició 3.3.2.** *$E(L)$ amb l'anterior operació $+$ té estructura de grup abelià* [6].

Tenim el següent resultat molt important en la teoria de corbes el.líptiques.

**Teorema 3.3.3** (Mordell)**.** *Fixat $L$ i $E$, el grup $E(L)$ és un grup abelià finitament generat, és a dir hi ha un isomorfisme de grups*

$$E(L) \cong E(L)_{tors} \oplus \mathbb{Z}^{n(E,L)}$$

*amb $n(E,L)$ un natural, que s'anomena el rang del grup abelià $E(L)$ i $E(L)_{tors}$ és el subgrup abelià finit format pels elements de torsió de $E(L)$ que corresponen als punts $P \in E(L)$ on existeix un natural $n_P$ on $n_P \cdot P = P + \overbrace{\ldots}^{n_P} + P = 0$.*

**Exercici 3.3.4.** *Doneu un exemple d'un grup abelià no finit generat $(G,+)$ on $(G/2G,+)$ és finit.*
*Demostreu que $\mathbb{Q}/\mathbb{Z}$ amb la suma no és un grup abelià finit generat.*
*És el cos $\mathbb{Q}$ amb la suma un grup abelià finit generat? Justifica la resposta.*

D'ara en endavant pensem $K = L = \mathbb{Q}$.

Per a demostrar el teorema de Mordell usualment s'usen dos resultats claus que presentem a continuació:

**Teorema 3.3.5** (Mordell dèbil)**.** *El grup abelià quocient $E(\mathbb{Q})/2E(\mathbb{Q})$ és finit.*

Observeu que per l'*Exercici 1*, no podem afirmar a partir del teorema dèbil de Mordell anterior que $E(\mathbb{Q})$ és un grup abelià finit generat.

**Definició 3.3.6.** *Els punts $E(\mathbb{Q})$ li associem una funció $H_E : E(\mathbb{Q}) \to \mathbb{N}$ anomenada funció altura definida per si $P = (x : y : 1) \in E(\mathbb{Q})$ i escrivim $x = \frac{m}{n}$ amb $m, n$ enters coprimers, llavors $H_E(P) = max(|m|, |n|)$ i $H_E((0 : 1 : 0)) = 1$. El valor $H_E(P)$ s'anomena l'altura del punt $P$.*

Evidentment, per a qualsevol nombre real positiu $C$ el conjunt $\{P \in E(\mathbb{Q}) | H(P) \leq C\}$ és finit. És pot demostrar

**Teorema 3.3.7.** *Donada $E$ una corba el.líptica sobre $\mathbb{Q}$ llavors existeix un nombre real positiu $C$ complint les dues condicions següents per a qualsevol $P, Q \in E(\mathbb{Q})$:*

$$C \cdot H_E(2P) \geq H_E(P)^4$$

$$C \cdot H_E(P) H_E(Q) \geq min(H_E(P+Q), H_E(P-Q)).$$

[6] Demostrar la propietat associativa és laboriosa, pels qui esteu interessats podeu trobar-ne una demostració en Fulton "Algebraic Curves". La propietat de dotar d'estructura de grup els $L$-punts de la solució d'una equació polinòmica en dues variables és particular de les equacions cúbiques (o de grau quatre).

**Exercici 3.3.8.** *Considera $E$ una corba el.líptica sobre $\mathbb{Q}$. A partir del teorema dèbil de Mordell (teorema 3.3.5) i el teorema d'altures (teorema 3.3.7) demostreu el teorema 3.3.3 de Mordell.*
*Indicació: Siguin $Q_1, \ldots, Q_n \in E(\mathbb{Q})$ certs representants dels elements del conjunt finit $E(\mathbb{Q})/2E(\mathbb{Q})$, és dir $\{Q_i \ mod 2E(\mathbb{Q}) | i = 1, \ldots, n\} = E(\mathbb{Q})/2E(\mathbb{Q})$. Sigui $C$ un real positiu que satisfà el teorema 3.3.7 i $M := max\{C, H(Q_1), \ldots, H(Q_n)\}$. Demostreu que $E(\mathbb{Q})$ com a grup abelià està generat pel conjunt finit*

$$\{P \in E(\mathbb{Q}) | H(P) \leq M\}.$$

**Exercici 3.3.9.** *Donada la corba el.líptica sobre $\mathbb{Q}$ $E_1 : y^2 = x^3 - x$ demostreu que $E_1(\mathbb{Q})$ són els punts $(0,0), (\pm 1, 0)$ i $O$ i que $E_1(\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ com a grup abelià.*
*Demostreu-ho fent els següents pasos intermedis:*
*considereu $P = (x_0, y_0)$ solució amb $y_0 \neq 0$ (en particular $x_0 \neq 0$) i la triem amb $H(P)$ mínim.*

1. *Podem triar-la de manera que $x_0 > 1$.*
   *Indicació: observeu $(x, y) \in E_1(\mathbb{Q})$ llavors $(-1/x, y/x^2) \in E_1(\mathbb{Q})$ i tenen la mateixa altura. Si $x_0 > 0$ de la igualtat $y_0^2 = x_0(x_0-1)(x_0+1)$ concloeu.*

2. *Demostreu que cada $x_0$, $x_0 - 1$ i $x_0 + 1$ és el quadrat d'un nombre racional.*
   *Indicació: $x_0 = m/n$, $m, n$ naturals coprimers. Veieu que $m, n$ no poden ser alhora senars, ja que $x_0' := \frac{x_0+1}{x_0-1}$ definiria la coordenada $x$ d'un punt solució de $E_1(\mathbb{Q})$ d'altura més petita que $H(P)$.*
   *I observeu després que $(x_0 - 1)x_0(x_0 + 1) = \frac{mn(m-n)(m+n)}{n^4}$.*

3. *Demostreu que $[2] : E_1(\mathbb{Q}) \to E_1(\mathbb{Q})$ definit per $[2](Q) = Q + Q$ per $Q \in E_1(\mathbb{Q})$ té per imatge el $O$ i els elements $(v, t) \in E_1(\mathbb{Q})$ amb $v, v - 1, v + 1$ quadrats en $\mathbb{Q}$.*

4. *Construïu un punt $(x_1 : y_1 : 1) \in E_1(\mathbb{Q})$ amb $[2](x_1 : y_1 : 1) = (x_0 : y_0 : 1)$ amb $x_1 y_1 \neq 0$ i $x_1 > 0$ d'altura més petita que $P$ i per l'argument de descens infinit concloeu que $E_1(\mathbb{Q})$ és un grup abelià format per quatre elements.*

5. *Calculeu finalment el grup abelià de torsió de $E_1(\mathbb{Q})$*

Deixeu-m'he escriure un parell de fets molt importants referent a aquest grup abelià finit generat $E(\mathbb{Q})$ per a corbes el.líptiques sobre els racionals.

**Teorema 3.3.10** (Mazur, 1976)**.** *Donada $E$ una corba el.líptica sobre $\mathbb{Q}$. Llavors hi ha una llista concreta i FINITA dels grups finits que apareixen com a grup de torsió $E(\mathbb{Q})_{tor}$. (En particular un d'aquests grups és $\mathbb{Z}/2 \times \mathbb{Z}/2$)* [7].

**Conjectura 3.3.11** (del Rang)**.** *Hi ha corbes el.líptiques $E$ sobre $\mathbb{Q}$ on el seu rang és tan gran com es vulgui, és dir, els nombres naturals $n(E, \mathbb{Q})$ no estan acotats quan $E$ recorre totes les corbes el.líptiques sobre $\mathbb{Q}$.*

Fins ara la corba el.líptica sobre $\mathbb{Q}$ amb rang més gran que es coneix és amb rang 28 per Elkies l'any 2006, veieu http://web.math.pmf.unizg.hr/∼duje/tors/rk28.html .

[7] La llista finita són els grups de torsió: els grups cíclics $\mathbb{Z}/m$ amb $1 \leq m \leq 10$, $m = 12$, i els grups de la forma $\mathbb{Z}/2j \oplus \mathbb{Z}/2$ amb $1 \leq j \leq 4$

**Exercici 3.3.12.** *Considereu la corba $E_1$. Demostreu que existeixen punts $U = (c, d) \in \mathbb{C}^2$ amb $cd \neq 0$ que satisfan l'equació $E_1$ i compleixen que $U$ té ordre 3, és dir $3U = O$. Per tant existeix un subgrup abelià d'ordre 3 en $E_1(\mathbb{C})$ generat per qualsevol d'aquests $U$. És algun d'aquests punts en $E_1(\mathbb{Q})$? En cas negatiu trobeu l'extensió $L$ més petita de cossos de $\mathbb{Q}$ dins de $\mathbb{C}$ on tots aquests punts $U$ pertanyin a $E(L)$.*

**Exercici 3.3.13.** *Usant l'exercici 3, demostreu que no hi solucions enteres de $X^4 + Y^4 = Z^4$ amb $XYZ \neq 0$.*
*Indicació: Escriviu $x^4 = z^4 - y^4$ i multipliqueu per $z^2/y^6$.*

**Exercici 3.3.14.** *Usant l'exercici 3 demostreu que no existeix un triangle rectangle on els tres costats són nombres racionals i la seva àrea és 1.*

*Indicació: Demostreu que hi ha una bijecció entre els conjunts $A = \{(x, y, z) \in \mathbb{Q}^3 | x^2 + y^2 = z^2,\ \frac{1}{2}xy = 1\}$, $B = \{(u, v, w) \in \mathbb{Q}^3 | u^2 + 1 = v^2, v^2 + 1 = w^2\}$, $C = \{(x, y) \in \mathbb{Q}^2 | y^2 = x^3 - x, y \neq 0\}$, podeu pensar en aplicacions de la forma $(x, y, z) \mapsto ((y - x)/2, z/2, (x + y)/2)$ per $A$ a $B$ i $h(u, v, w) = (u^2 + 1, uvw)$ entre $B$ i $C$.*

# Capítol 4

# Idees de Kummer per atacar equació de Fermat. Dominis de Dedekind.

## 4.1 Motivació

Considerem l'equació $X^p + Y^p = Z^p$ amb $p$ un primer senar i ens preguntem a buscar $x, y, z \in \mathbb{Z}$ i fixem-nos que podem pensar que busquem solucions a $\mathbb{Z}[\zeta_p]$ on $\zeta_p = e^{2\pi i/p}$ de la forma

$$\prod_{j=1}^{p}(x + \zeta_p y) = z^p$$

Ens interessa estudiar propietats de l'anell $\mathbb{Z}[\zeta_p]$. S'observa que $\mathbb{Z}[\zeta] = \{\alpha \in \mathbb{Q}[\zeta_p] | Irr(\alpha, \mathbb{Q}) \in \mathbb{Z}[X]\}$ i per tant podem pensar que correspon a fer una teoria de Galois en anells iniciant per l'anell d'enters.

Kummer l'any 1840 va observar que $\mathbb{Z}[\zeta_p]$ no és domini de factorització única.

Desconeixent aquest resultat, Lammé l'any 1880 afirmava que havia demostrat el teorema de Fermat, el que havia demostrat és: si $\mathbb{Z}[\zeta_p]$ és domini de factorització única llavors $X^p + Y^p = Z^p$ sol té solucions enteres i compleixen $xyz = 0$.

## 4.2 Elements enters

**Definició 4.2.1.** *Sigui $A$ un domini dins un cos $L$. Diem que $\alpha \in L$ és enter sobre $A$ si $\alpha$ és l'arrel d'un polinomi mònic en $A[X]$. Quan $A = \mathbb{Z}$ es diu que $\alpha$ és un enter algebraic.*

**Observació 4.2.2.** *A domini, i $K = Quot(A)$ el seu cos de fraccions. Considerem $L/K$ una extensió finita de cossos, donat $\alpha \in L$ on $Irr(\alpha, K)[X] \in A[X]$ llavors tenim que $\alpha$ és enter sobre $A$.*

*Què succeeix en l'enunciat invers? S*

*Suposem $\alpha \in L$ i $\alpha$ enter sobre $A$, on tenim $f(X) \in A[X]$ monic amb $f(\alpha) = 0$ obtenim que $Irr(\alpha, K)[X] | f(X)$ en $K[X]$. Si tenim que $A$ és DFU (domini de factorització única) usant el lema de Gauss amb $f(X) = g(X)Irr(\alpha, K)[X]$ de ser $f(X) \in A[X]$ monic tenim en particular $Irr(\alpha, K)[X] \in A[X]$.*

**Lema 4.2.3.** *Sigui $d \in \mathbb{Z}$ lliure de quadrats amb $d \neq 0, 1$, i sigui $L = \mathbb{Q}[\sqrt{d}]$. Els enters de $L$ sobre $A = \mathbb{Z}$ corresponen al conjunt $B$ on*

$$B = \begin{cases} \mathbb{Z}[\sqrt{d}] & si\ d \equiv 2, 3 (mod\ 4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & si\ d \equiv 1 (mod\ 4) \end{cases} .$$

*Demostració.* Escrivim $\alpha = m + n\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$ amb $n, m \in \mathbb{Q}$ és enter algebraic, si $n = 0$ i de ser enter sobre $\mathbb{Z}$ tenim que $\alpha \in \mathbb{Z}$. Si $n \neq 0$ tenim $Irr(\alpha, \mathbb{Q})[X]$ no és de grau 1 i per l'observació anterior

$$X^2 - 2mX + (m^2 - n^2 d) = Irr(\alpha, \mathbb{Q})[X] \in \mathbb{Z}[X]$$

i per tant $2m \in \mathbb{Z}$ i $m^2 - n^2 d \in \mathbb{Z}$, i treballant modul 4 obtenim el resultat. □

**Definició 4.2.4.** *Sigui $A$ un domini, diem que $M$ és un $A$-mòdul si $(M, +)$ és un grup abelià i té un producte*

$$A \times M \to M; (a, m) \mapsto a \cdot m$$

*complint les propietats següents:*

1. $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$
2. $(a + b) \cdot m = a \cdot m + b \cdot m$
3. $(ab) \cdot m = a \cdot (b \cdot m)$
4. $1 \cdot m = m$.

**Definició 4.2.5.** *Diem $M$ un $A$-mòdul finit generat, si existeixen $m_1, \ldots, m_k \in M$ on $M = Am_1 + \ldots + Am_k$.*

**Exemple 4.2.6.** *Si $A = K$ un cos noció $A$-mòduls correspon a la noció de $K$-espai vectorial. La noció de $K$-mòduls finit generats correspon a la noció de $K$-espais vectorials de dimensió finita.*

**Proposició 4.2.7.** *Sigui $A$ un domini dins un cos $L$, i $\alpha \in L$. Són equivalents:*

1. *$\alpha$ és enter sobre $A$,*
2. *$A[\alpha] \subset L$ és un $A$-modul finit generat.*
3. *existeix $M$ un $A$-mòdul finit generat amb $M \subset L$ i complint $\alpha M \subset M$.*

*Demostració. i) $\Rightarrow$ ii)* si $\alpha$ enter tenim

$$\alpha^N + a_{N-1}\alpha^{N-1} + \ldots + a_0 = 0$$

amb $a_i \in A$, tenim que $A[\alpha] = A1 + A\alpha + \ldots A\alpha^{N-1}$ i per tant finit generat, efectivament donat $\beta \in A[\alpha]$, usant que $\alpha^N \in A1 + A\alpha + \ldots A\alpha^{N-1}$, obtenim iterant $\alpha^{N+k} \in A1 + A\alpha + \ldots A\alpha^{N-1}$, i per tant el resultat.

Per *ii*) $\Rightarrow$ *iii*) prenem $M = A[\alpha]$
Per *iii*) $\Rightarrow$ *i*), escrivim $M = Am_1 + \dots Am_s$ l'$A$-modul finit generat. Tenim

$$\alpha m_i = \sum_{j=1}^{s} b_{i,j} m_j$$

amb $b_{i,j} \in A$. Escrivim-ho matricialment per $B = (b_{i,j})_{1 \leq i,j \leq s} \in M_s(A)$ i $E = (m_j)_{1 \leq j \leq s} \in M_{s,1}(M)$ obtenim

$$\alpha \cdot E = B \cdot E, \ d'on \ (\alpha I_s - B) \cdot E = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Fixem-nos que tant $m_i$ com coeficients $(\alpha I_s - B) \in M_s(L)$ i té solució no trivial per tant tenim

$$det(\alpha I_s - B) = 0 = \alpha^s + \sum_{i=0}^{s-1} a_i \alpha^i \in A[X]$$

i per tant obtenim que $\alpha$ és enter sobre $A$. □

**Corol·lari 4.2.8.** *Sigui $A$ un domini dins un cos $L$. Denotem per $B_A := \{\alpha \in L | \alpha$ enter sobre $A\} \subset L$. Llavors $B_A$ és un domini.*

*Demostració.* Observem que tot $a \in A$ és enter sobre $A$ ja que és arrel de $X - a \in A[X]$, d'on $A \subseteq B_A$. Per demostrar-ho és suficient demostrar que donats $\alpha, \beta \in B_A$ llavors $\alpha + \beta$ i $\alpha\beta \in B_A$.

Escrivim $A[\alpha] = Am_1 + \ldots + Am_s$ i $A[\beta] = An_1 + \ldots + An_l$ d'on observem que $A[\alpha, \beta]$ és un $A$-mòdul finit generat usant la família $n_i m_j{}_{1 \leq i \leq s, 1 \leq j \leq l}$, i observem que com $\alpha + \beta \in A[\alpha, \beta]$ i $\alpha\beta \in A[\alpha, \beta]$ obtenim que

$$(\alpha + \beta) A[\alpha, \beta] \subseteq A[\alpha, \beta]$$

$$\alpha\beta A[\alpha, \beta] \subseteq A[\alpha, \beta]$$

i usant proposició anterior obtenim el resultat ja que $A[\alpha, \beta]$ és un $A$-submodul de $L$ finit generat. □

**Definició 4.2.9.** *Sigui $A$ un domini dins un cos $L$. La clausura entera $B$ de $A$ en $L$ és els elements de $L$ que son enters sobre $A$ (aquest conjunt $B$ és un domini per un resultat anterior dins aquesta secció). Quan $L/\mathbb{Q}$ és una extensió finita de cossos i $A = \mathbb{Z}$ aquesta clausura entera s'anomena* **anell d'enters del cos** *$L$ i s'anota per $\mathcal{O}_L$.*

**Definició 4.2.10.** *Un domini $A$ s'anomena integrament tancat si és igual a la clausura entera en $L = Quot(A)$ el cos de fraccions de $A$.*

**Exemple 4.2.11.** *Els dominis $\mathbb{Z}$ i $K[X]$ amb $K$ cos són integrament tancats.*

Més en general es té el següent resultat:

**Lema 4.2.12.** *Si $A$ és un domini de factorització única llavors $A$ és integrament tancat.*

*Demostració.* Escrivim $K = Quot(A)$, donat $z = \frac{b}{c}$ amb $b, c \in A$ coprimers, i suposem $z$ enter sobre $A$, tenim llavors:

$$(\frac{b}{c})^N + a_{N-1}(\frac{b}{c})^{N-1} + \ldots + a_0 = 0$$

amb $a_i \in A$, d'on s'obté:

$$-b^N = c(a_{N-1}b^{N-1} + \ldots + a_1bc^{N-2} + a_0c^{N-1})$$

com $A$ és DFU, qualsevol factor irreductible de $c$ divideix $b$ i com $b, c$ coprimers obtenim que $c$ és una unitat, per tant $z \in A$. □

**Lema 4.2.13.** *Sigui $A$ un domini integrament tancat i denotem per $K = Quot(A)$. Sigui $\alpha \in \overline{K}$ un element algebraic sobre $K$. Llavors:*

$$\alpha \text{ enter sobre } A \Leftrightarrow Irr(\alpha, K)[X] \in A[X].$$

*Demostració.* Suposem $\alpha$ enter sobre $A$, i $f(X) \in A[X]$ monic on $f(\alpha) = 0$. Denotem per $L$ cos de descomposició per $Irr(\alpha, K)[X]$ sobre $K$ i escrivim $Irr(\alpha, K)[X] = \prod_{i=1}^{\ell}(X - \alpha_i) \in L[X]$. Sabem que $Irr(\alpha, K)[X] | f(X)$ en $K[X]$ on els $\alpha_i$'s són també enters sobre $A$. Escrivim $B = A[\alpha_1 = \alpha, \ldots, \alpha_\ell]$. Observem que els coeficients de $Irr(\alpha, K)[X]$ son funcions simètriques a coeficients enters en les arrels $\alpha_1, \ldots, \alpha_n$ i per tant són enters sobre $A$ i que pertanyen a $K$, i com $A$ és integrament tancat aquest coeficients són de $A$ i per tant $Irr(\alpha, K)[X] \in A[X]$. L'altra implicació és obvia. □

Anem a estudiar la propietat de ser entera via torres de dominis. Donats dos dominis $A \subset B$, diem $B$ és enter sobre $A$ si tot element $b \in B$ és enter sobre $A$.

**Lema 4.2.14.** *Siguin $A, B, C$ dominis complint $A \subseteq B \subseteq C$. Llavors tenim:*

$$C \text{ enter sobre } A \Leftrightarrow C \text{ enter sobre } B \text{ i } B \text{ és enter sobre } A.$$

*Demostració.* $\Rightarrow$ obvi.
$\Leftarrow$ Sigui $c \in C$ enter sobre $B$, on $h(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0 \in B[X]$ on $h(c) = 0$. Escrivim $B' = A[b_{n-1}, \ldots, b_0]$ és un $A$-modul finit generat ja que cada $b_i$ enters sobre $A$ (demostreu és finit generat amb inducció sobre $n-1$ per exemple), per tant $B'[\alpha]$ és un $A$-mòdul finit generat complint $\alpha B'[\alpha] \subseteq B'[\alpha]$ i per tant $\alpha$ és enter sobre $A$ gracies a una proposició anterior. □

**Proposició 4.2.15.** *Sigui $A$ un domini i $K = Quot(A)$. Sigui $L/K$ una extensió finita de cossos. Denotem per $B$ la clausura entera de $A$ en $L$. Tenim:*

1. *$\alpha \in L$ llavors $\exists b \in B$ i $a \in A$ on $\alpha = b/a$, (en particular $L = Quot(B)$).*
2. *El domini $B$ és integrament tancat.*
3. *Si $A$ és integrament tancat llavors $B \cap K = A$.*
4. *Si $L/K$ és Galois amb $G = Gal(L/K)$ llavors $\sigma(B) = B$ $\forall \sigma \in G$. Si a més $A$ és integrament tancat llavors $A = B^G$.*

*Demostració.* 1. sigui $\ell \in L$, $g(X) = Irr(\ell, K)[X] = X^n + \frac{c_{n-1}}{d_{n-1}}X^{n-1} + \ldots + \frac{c_0}{d_0}$ amb $c_i, d_i \in A$, $K = Quot(A)$, pensant $d_i \neq 0$ per tot $i$, tenim $d := \prod_{i=0}^{n-1} d_i \in A$ d'on

$$0 = d^n g(\ell) = (d\ell)^n + d\frac{c_{n-1}}{d_{n-1}}(d\ell)^{n-1} + \ldots + d^n\frac{c_0}{d_0}$$

d'on s'obté que $d\ell$ és enter sobre $A$ per tant $d\ell \in B$ i d'aquí $\ell = \frac{b}{d}$ amb $b \in B$ i $d \in A$.

2. De l'apartat anterior $Quot(B) = L$ i de la proposició anterior la clausura entera de $B$ en $L$ correspon a $B^{cl}$ és enter sobre $A$ i per tant $B = B^{cl}$.

3. Per definició $A \subseteq B \cap K$. Per $\alpha \in K$ i enter sobre $A$ tenim $\alpha \in A$ si $A$ integrament tancat.

4. Agafem $b \in B$ on $g(b) = 0$ amb $g(X) \in A[X]$ monic. Tenim llavors

$$0 = \tau(g(b)))g(\tau(b))$$

i per tant $\tau(b) \in B$ on $\tau(B) \subset B$ i de ser $\tau$ iso, tenim la igualtat. De ser Galois $K = L^G$ d'on $B^G = B \cap K$ i si $A$ integrament tancat de l'apartat anterior $A = B \cap K = B^G$.

□

**Corol·lari 4.2.16.** *Sigui $A$ un domini i $K = Quot(A)$, i considerem $L/K$ finita de grau $n$. Denotem per $B$ la clausura entera de $A$ en $L$. Llavors $\exists$ $e_1, \ldots, e_n \in B$ on $(e_1, \ldots, e_n)$ és una base de $L$ com $K$-espai vectorial.*

*Demostració.* sigui $(f_1, \ldots, f_n)$ una $K$-base, escrivim $f_i = \frac{b_i}{c_i}$ amb $b_i \in B$ i $c_i \in A$, obtenim $(b_1, \ldots, b_n)$ és una $K$-base de $L$ amb $b_i \in B$. □

## 4.3 Nocions d'anells noetherians

Un ideal $I$ d'un anell commutatiu $A$ s'anomena finit generat si ho és com $A$-mòdul, és a dir, si existeixen $i_1, \ldots, i_n \in I$ on

$$I = i_1A + \ldots + i_nA$$

**Definició 4.3.1.** *$M$ un $A$-mòdul, s'anomena noetherià si donada qualsevol cadena*

$$M_1 \subset M_2 \subset \ldots$$

*amb $M_i$ submòduls de $M$ (i.e. suma i producte per $A$ en $M$ restringeixen en $M_i$ complint totes les propietats de $A$-mòdul) llavors existeix $k \in \mathbb{N}$ on $M_{k+j} = M_k$ $\forall j \in \mathbb{Z}$.*

**Proposició 4.3.2.** *$M$ és un $A$-mòdul noetherià si i només si per cada $A$-submòdul de $M$ és un $A$-mòdul finit generat.*

*Demostració.* $\Rightarrow$ Sigui $N$ un $A$-submòdul de $M$. Denotem per

$$\Sigma := \{tots\ els\ submoduls\ de\ N; finit\ generats\}.$$

$\Sigma \neq \emptyset$ perquè $\{0\} \in \Sigma$, on $\Sigma$ té un element maximal del fet que $M$ és noetherià, diem $N_0$ aquest element maximal. Si $N_0 \neq N$ obtenim $N_0 + xA$ amb $x \in N \setminus N_0$ però finit generat en contradicció i per tant $N_0 = N$ i $N$ és finit generat.

$\Leftarrow$) Considerem una cadena de $A$-submòduls de $M$ $M_1 \subseteq M_2 \subseteq \ldots$, i considerem $N := \cup_i M_i$ és un $A$-submòdul de $M$ i per tant finit generat, escrivim doncs $N = m_1 A + \ldots + m_s A$ i com $M_i$'s creixent, $\exists k$ on $m_i \in M_k$ per tot $i$, ja que és un conjunt finit, per tant $M_{k+j} = M_k$ per a tot natural $j$. □

**Definició 4.3.3.** *Un anell commutatiu $A$ s'anomena noetherià si $A$ com $A$-mòdul és noetherià.*

Observeu si $A$ és DIP llavors és noetherià. En particular si $A = K$ cos també.

**Lema 4.3.4.** *Si $A$ és noetherià llavors $A/I$ és noetherià per a $I$ un ideal de $A$.*

*Demostració.* Si $R$ un anell noetherià, tot submodul correspon als ideals de l'anell. Sigui $\overline{J}$ un ideal de $A/I$, i considera $\pi : A \to A/I$ la projecció, considerem l'ideal $J = \pi^{-1}(\overline{J})$ de $A$ on $J = (j_1, \ldots, j_k)$ de ser noetheriá i per tant $\overline{J} = (\pi(j_1), \ldots, \pi(j_k))$. □

Recordem el següent resultat clau, que es demostra en un curs d'Àlgebra Commutativa però que no farem amb aquest curs, consulteu les persones interessades [Atiyah-Macdonald].

**Fet 4.3.5.** *Sigui $A$ un anell noetherià. Llavors, tot submòdul d'un $A$-mòdul finit generat és finit generat.*

**Lema 4.3.6.** *Sigui $A \subseteq B$ dos anells commutatius. Si $A$ és noetherià i $B$ un $A$-mòdul finit generat llavors $B$ és noetherià.*

*Demostració.* Sigui $I_B$ un ideal de $B$, que en particular és un $A$-submòdul del $A$-mòdul $B$ finit generat, per tant tenim que és finit generat com $A$-mòdul per ser $A$ noetherià, en particular finit generat com $B$-mòdul, per tant el resultat. □

Amb la idea del curs d'estendre teoria de Galois però ara de dominis $B$ enters sobre $A$, estudiem si la propietat de noetherià puja en la torre d'anells.

**Teorema 4.3.7.** *Sigui $A$ un domini integrament tancat, i $K = Quot(A)$. Sigui $L/K$ una extensió separable de grau $n$ i $\{e_1, \ldots, e_n\} \subset B$ amb $B$ la clausura entera de $A$ en $L$, on $(e_1, \ldots, e_n)$ és una $K$-base de $L$. Llavors existeix $d \in A$ complint*

$$Ae_1 \oplus \ldots Ae_n \subseteq B \subseteq A\frac{e_1}{d} \oplus \ldots \oplus A\frac{e_n}{d} \subseteq L.$$

Ens interessa destacar abans de ferne la demostració el següent corol.lari: com $A\frac{e_1}{d} \oplus \ldots \oplus A\frac{e_n}{d}$ és un $A$-mòdul finit generat, de la Proposició 4.3.5 tenim que $B$ és un $A$-mòdul finit generat i pel Lema 4.3.6 tenim $B$ noetherià:

**Corol·lari 4.3.8.** *Si $A$ domini noetherià e integrament tancat, $B$ la clausura entera de $A$ en $L$ on $L/Quot(A) = K$ és una extensió finita i separable de cossos. Llavors $B$ és un $A$-mòdul finit generat i en particular $B$ és noetherià.*

*Demostració.* [Teorema 4.3.7] Hem vist anteriorment que sense perdua de generalitat podem triar $(e_1, \ldots, e_n)$ una base de $L$ com a $K$-espai vectorial amb $e_i \in B$.

Sigui $\beta \in L = Quot(B)$ i escrivim-lo per: $\beta = x_1e_1 + \ldots + x_ne_n$ amb $x_i \in K$. Volem construir $d \in A \setminus \{0\}$ on $\beta = dx_1\frac{e_1}{d} + \ldots + dx_n\frac{e_n}{d}$ compleixi $dx_i \in A$ sempre que $\beta \in B$.

Suposem d'ara en endavant $\beta \in B$.

Fixem $\overline{K}$ una clausura separable de $K$ (és com la clausura algebraica però introduint-hi totes les arrels de polinomis separables a coeficients en el cos $K$), com $L/K$ separable finita de grau $n$ podem triar del curs de teoria de Galois $L = K(\alpha)$ amb $\alpha \in L$ i amb resultats vist anteriorment amb $\alpha \in B$. Escrivim $Irr(\alpha, K)[X] = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n) \in \overline{K}[X]$ on $\alpha = \alpha_1$, on tenim $n$ inmersions a $\overline{K}$ corresponents a $\sigma_i(\alpha) = \alpha_i$ amb $\sigma_i : K(\alpha) \hookrightarrow \overline{K}$.

Considerem la matriu $M := (\sigma_i(e_j))_{1\leq i,j\leq n} \in M_n(K)$ i tenim la igualtat matricial següent:

$$\begin{pmatrix} \sigma_1(\beta) \\ \vdots \\ \sigma_n(\beta) \end{pmatrix} = M \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix};\ i\ obtenim$$

$$(M^{ad})^t \begin{pmatrix} \sigma_1(\beta) \\ \vdots \\ \sigma_n(\beta) \end{pmatrix} = (M^{ad})^t M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} (detM)x_1 \\ \vdots \\ (detM)x_n \end{pmatrix}.$$

Com tenim que $\sigma_i(e_j)$ i $\sigma_i(\beta)$ són enters sobre $A$, obtenim que $detM$ i $detMx_i$ són enters sobre $A$. (Observeu si $detM \in K$ ja hauriem finalitzat).

Observem $\forall \eta \in Aut_K(\overline{K})$ tenim $\eta_{|L} = \sigma_i$ per algun $i$, triem per cada $\sigma_i$ un $\eta_i$ que en restringir a $L$ correspongui a $\sigma_i$. Observem que $\eta_i$ permuta les columnes de la matriu $M$ i per les propietats de matrius tenim

$$\eta_i(det(M)) = \pm\eta_i(det(M)),$$

i per tant $d = (det(M))^2$ és fix $\forall \eta \in Aut_K(\overline{K})$ i tot l'argumentari anterior podem canviar $\overline{K}$ per $N$ on $N$ és el cos de descomposició de $Irr(\alpha, K)[X]$ on $L = K(\alpha)$, i per tant $d$ és fix per $Gal(N/K)$ i per tant $d \in K$, ara bé com $det(M)$ és enter sobre $A$ i $A$ integrament tancat obtenim que $d \in A$ i per tant obtenim

$$dx_i = (detM)(detM)x_i$$

d'on com $det(M)$ i $det(M)x_i$ enters sobre $A$, obtenim $dx_i$ enter sobre $A$ i $dx_i \in K$ per tant de ser integrament tancat $dx_i \in A$ obtenint que aquest $d$ és el que buscàvem. □

## 4.4 Un esboç de dimensió de Krull igual a 1

**Definició 4.4.1.** *Sigui $A$ un anell commutatiu. Una cadena d'ideals primers de longitud $n$ en $A$ és un conjunt de $n+1$ ideals primers diferents: $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ de $A$ on*

$$\mathfrak{p}_n \subset \ldots \subset \mathfrak{p}_1 \subset \mathfrak{p}_0.$$

*L'altura d'un ideal primer $\mathcal{P}$ de $A$, denotat per $ht(\mathcal{P})$ és el suprem de les longituds de totes les cadenes d'ideals primers en $A$ amb $\mathfrak{p}_0 = \mathcal{P}$.*

*La dimensió de Krull de $A$ es defineix per:*

$$dim_{Krull}(A) := suprem\{ht(\mathcal{P}) | \mathcal{P} \text{ ideal primer de } A\}.$$

**Exemple 4.4.2.** *Observeu que si $K$ és un cos llavors $dim_{Krull}(K) = 0$.*

*També fàcilment obtenim que $dim_{Krull}(\mathbb{Z}) = 1$ i $dim_{Krull}(K[X]) = 1$ en l'anell de polinomis.*

*I és obvi que $dim_{Krull}(K[X_1, \ldots, X_n]) \geq n$ de la cadena ideals primers*

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \ldots \subset (X_1, \ldots, X_n)$$

*i que $dim_{Krull}(\mathbb{Z}[X]) \geq 2$ en consider la cadena d'ideals primers*

$$(0) \subset (p) \subset (p, X).$$

**Lema 4.4.3.** *Sigui $A$ un domini i $P_1 = (p_1)$ i $P_2 = (p_2)$ dos ideals primers diferents de $A$ que són principals amb $P_i \neq (0)$ (i en particular $P_i \neq A$) per $i \in \{1, 2\}$. Llavors $P_1 \not\subset P_2$ en particular si $A$ és un domini d'ideals principals que no és un cos tenim $dim_{Krull}(A) = 1$.*

*Demostració.* Suposem $P_1 \subset P_2$, per tant $p_1 = ap_2$, i de ser $P_1$ ideal primer obtenim que $p_2 \in P_1$ i d'aquí $P_1 = P_2$, o bé que $a \in P_1$ i podem escriure $a = bp_1$ per cert $b \in A$, i s'obté $p_1(1 - bp_2) = 0$ i com $A$ és domini i $P_1 \neq (0)$ s'obté que $1 - bp_2 = 0$ d'on $p_2$ una unitat de $A$ i s'obté $P_2 = (A)$ que tampoc pot complir-se. Per tant si $P_1 \subset P_2$ amb $P_i \neq (0)$ i $P_i \neq (A)$ no és satisfà. □

**Exercici 4.4.4.** *Si $A$ és un domini de factorització única $P \neq (0)$ un ideal primer, llavors tenim:*

$$ht_A(P) = 1 \Leftrightarrow P \text{ és ideal principal.}$$

*I proveu que si a més $dim_{Krull}(A) = 1$, llavors $A$ és un domini d'ideals principals.*

**Proposició 4.4.5.** *Sigui $A$ un domini amb $dim_{Krull}(A) = 1$. Sigui $A \subset B$ inclusió de dominis on per a tot $b \in B$ és enter sobre $A$. Llavors $dim_{Krull}(B) = 1$.*

*Demostració.* Sigui $\mathfrak{P}$ ideal primer de $B$ diferent del (0), i es té que $\mathfrak{P} \cap A = P$ és un ideal primer de $A$ perqué si considerem el morfisme projecció $proj : A \to B/\mathfrak{P}$ de ser $B/\mathfrak{P}$ domini, obtenim que $ker(proj) = \mathfrak{P} \cap A$ és un ideal primer de $A$.

Observem primer que $P \neq (0)$: si $\beta \in \mathfrak{P} \setminus \{0\}$ obtenim

$$g(\beta) = \beta^N + a_{N-1}\beta^{N-1} + \ldots + a_1\beta + a_0 = 0$$

amb $a_i \in A$ i agafem $g(X) \in A[X]$ amb $g(\beta) = 0$ mònic de grau mínim, i per tant tenim de grau mínim que $a_0 \neq 0$ i en particular

$$a_0 = -\beta^N - a_{N-1}\beta^{N-1} - \ldots - a_1\beta \in \mathfrak{P} \cap A$$

d'aquí $P \neq (0)$.

Ara de ser $P$ primer i $dim_{Krull}(A) = 1$ obtenim $P$ és un ideal maximal de $A$. Provem tot seguit que $\mathfrak{P}$ també és un ideal maximal de $B$ i per tant el resultat (provem que $B/\mathfrak{P}$ és un cos).

Clarament tot $[b] \in B/\mathfrak{P}$ és enter sobre $A/P$ de ser $B$ enter sobre $A$. Triem $[b] \neq [0]$, i obtenim

$$[b]^k + c_{k-1}[b]^{k-1} + \ldots + c_0 = 0$$

amb $c_i \in k := A/P$ cos, i $\ell(X) = X^k + c_{k-1}X^{k-1} + \ldots + c_0 \in k[X]$ de grau mínim que anul.la $[b]$, on per aquesta minimalitat és fàcil demostrar que $c_0 \neq 0$ i per tant tenim

$$[b] \cdot (-c_0^{-1}[b]^{k-1} - \ldots - c_0^{-1}c_1) = 1 \in B/\mathfrak{P}$$

per tant $[b]$ és invertible. □

**Corol·lari 4.4.6.** *Sigui $A$ un domini amb $dim_{Krull}(A) = 1$ i $L/Quot(A)$ una extensió finita de cossos. Sigui $B$ la clausura entera de $A$ en $L$. Llavors $dim_{Krull}(B) = 1$.*

## 4.5 Dominis de Dedekind

**Definició 4.5.1.** *$A$ un domini, s'anomena de Dedekind si compleix les tres propietats següents:*

- *$A$ és noetherià,*
- *$A$ té $dim_{Krull}(A) = 1$,*
- *$A$ és integrament tancat.*

Dels resultats en les seccions anteriors obtenim

**Corol·lari 4.5.2.** *Sigui $A$ un domini de Dedekind i $L/Quot(A)$ una extensió finita i separable de cossos, llavors $B$ la clausura entera de $A$ en $L$ és també un domini de Dedekind.*

**Definició 4.5.3.** *Considerem $A = \mathbb{Z}$ i $L/\mathbb{Q}$ una extensió finita, la clausura entera de $\mathbb{Z}$ en $L$ s'anomena l'anell d'enters del cos $L$ i s'anota per $\mathcal{O}_L$, i pel corol.lari anterior és un domini de Dedekind.*

Un altre exemple bàsic de domini de Dedekind és la clausura entera de l'anell de polinomis $K[X]$ en un cos $L$ on $L/Quot(K[X])$ és finita i separable, diem aquests dominis de Dedekind, **dominis de corbes de Dedekind**.

Hi ha el següent resultat per a buscar de forma explícita dominis de corbes de Dedekind que és molt útil, per una demostració podeu consultar [Lorenzini, Chap 2].

**Teorema-Fact 4.5.4.** *Sigui $f \in \overline{K}[X,Y]$ on és irreductible en $Quot(\overline{K}[X])[Y]$ llavors el domini $Quot(\overline{K}[X])[Y]/(f(X,Y))$ és integrament tancat si i només si $f$ no té cap punt singular en $\overline{K}^2$.*

I podem trobar efectivament dominis de corbes de Dedekind:

**Exemple 4.5.5.** *Considerem una corba hiperel.líptica* $y^2 = h(x)$ *on* $Y^2 - h(X) \in \mathbb{Q}[X,Y]$ *és un polinomi irreductible en* $\overline{\mathbb{Q}}(X)[Y]$*, llavors la clausura entera de* $\overline{\mathbb{Q}}[X]$ *en* $L := \overline{\mathbb{Q}}(X)[Y]/(Y^2-h(X))$ *és l'anell* $B = \overline{\mathbb{Q}}[X,Y]/(Y^2-h(X))$*, en particular* $B$ *és un domini de Dedekind dins el cos* $L$*.*

*Efectivament, fixem-nos que* $B$ *és integrament tancat ja que* $h(X)$ *no tenia arrels repetides i per tant compleix la condició de no-singular i per tant és integrament tancat. Com tot element de* $B$ *és enter sobre* $A = \overline{\mathbb{Q}}[X]$ *per construcció s'obté que* $dim_{Krull}(B) = 1$*. Per noetherià suficient observar que* $B = \overline{\mathbb{Q}}[X] + [y]\overline{\mathbb{Q}}[X]$ *i per tant és un* $A$*-mòdul finit generat amb* $A$ *noetherià i per tant* $B$ *noetherià.*

**Observació 4.5.6.** *Es pot demostrar, veieu [Lorenzini, Chp.IX] que si* $f(X,Y) \in K[X,Y]$ *irreductible en* $\overline{K}(X)[Y]$ *i no-singular en* $\overline{K}[X,Y]$*, llavors el domini* $B = K[X,Y]/f(X,Y)$ *és un domini (de corbes) de Dedekind i que correspon a la clausura entera de* $K[X]$ *en el cos* $L = Quot(K[X])[Y]/f(X,Y)$ *amb* $K$ *un cos de característica zero.*

## 4.6 Factorització única per a ideals primers

**Proposició 4.6.1.** *Sigui* $A$ *un domini noetherià. Sigui* $I \neq (0)$ *un ideal de* $A$*,* $I \neq A$*. Llavors existeix un número finit de ideals primers de* $A$*:* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ *i naturals:* $a_1, \ldots, a_s$ *complint que*

$$\mathfrak{p}_1^{a_1} \cdot \ldots \cdot \mathfrak{p}_s^{a_s} \subseteq I \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s.$$

*Demostració.* Denotem per $\Sigma$ el conjunt d'ideals de $A$ que no satisfan la proposició a demostrar i suposem que $\Sigma \neq \emptyset$. Del fet que $A$ és un domini noetherià, tota cadena en $\Sigma$ tindrà maximal i per tant $\Sigma$ conté un ideal maximal, diem-li $I$. Observem que $I$ no pot ser un ideal primer de $A$ (ja que $\Sigma$ no conté els ideals primers!). Com $I$ no és un ideal primer, existeixen $x, y \in A$ complint $xy \in I$ i $x, y \notin I$. Denotem els ideals de $A$: $I_x := (x, I)$, $I_y := (y, I)$, i observem que

$$(I^2, Ix, Iy, Ixy) = I_x \cdot I_y \subseteq I \subseteq I_x \cap I_y$$

(on la primera inclusió correspon a que $I_x, I_y$ contenen estrictament $I$ i no-trivials). Ara com $I$ és maximal en $\Sigma$ podem escriure:

$$\mathfrak{p}_1^{a_1} \cdot \ldots \cdot \mathfrak{p}_s^{a_s} \subseteq I_x \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$$

$$\mathfrak{q}_1^{b_1} \ldots \mathfrak{q}_t^{b_t} \subseteq I_y \subseteq \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_t$$

amb $\mathfrak{q}_i$ ideals primers de $A$. D'aquestes inclusions obtenim:

$$\mathfrak{p}_1^{a_1} \cdot \ldots \cdot \mathfrak{p}_2^{a_2} \cdot \mathfrak{q}_1^{b_1} \cdot \ldots \cdot \mathfrak{q}_t^{b_t} \subseteq I_x I_y \subseteq I$$

$$I \subseteq I_x \cap I_y \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s \cap \mathfrak{q}_1 \cap \ldots \mathfrak{q}_t$$

que contradiu que $I$ maximal amb $I \in \Sigma$, per tant $\Sigma = \emptyset$. □

Ara volem caracteritzar els dominis que tenen factorització única però enlloc d'elements amb ideals primers.

**Definició 4.6.2.** *Un domini $A$ s'anomena domini de factorització única per ideals si per a tot $I \subseteq A$ ideal de $A$ no-trivial s'escriu*

$$I = \mathfrak{p}_1 \dots \mathfrak{p}_s$$

*amb $\mathfrak{p}_i$ ideals primers de $A$ (no necessariament diferents) i aquesta descomposició és única llevat d'ordre.*

Anem doncs a aprofundir amb producte d'ideals i la interrelació amb la intersecció d'ideals. Un cop fet intentarem caracteritzar aquests dominis.

**Lema 4.6.3.** *Sigui $\mathfrak{p}$ un ideal primer de $A$, un anell commutatiu, i $I$,$J$ dos ideals de $A$ complint que $IJ \subseteq \mathfrak{p}$. Llavors $I \subseteq \mathfrak{p}$ ó $J \subseteq \mathfrak{p}$.*

*Demostració.* Si $I \not\subseteq \mathfrak{p}$ i $J \not\subseteq \mathfrak{p}$ llavors $\exists x \in I \setminus \mathfrak{p}$ i $y \in I \setminus \mathfrak{p}$ on $xy \in IJ \subseteq \mathfrak{p}$ obtenint contradicció amb el fet que $\mathfrak{p}$ és un ideal primer. □

**Lema 4.6.4.** *Sigui $A$ anell commutatiu i $I_1, \dots, I_n$ $n$ ideals de $A$ amb $I_i, I_j$ coprimers si $i \neq j$ (és a dir $I_i + I_j = A$ si $i \neq j$)- Llavors:*

1. *$I_1 \cdot \ldots \cdot I_s$ coprimer amb $I_{s+1}$ per a $s = 1, \dots, n-1$,*
2. *$I_1 \cdot \ldots \cdot I_n = I_1 \cap \ldots \cap I_n$.*

*Demostració.* 1. per cada $1 \leq j \leq s$ triem $x_j \in I_{s+1}$ i $y_j \in I_j$ on $x_j + y_j = 1$. Tenim doncs

$$1 = \prod_{j=1}^{s} (x_j + y_j) \in (x_1, \dots, x_s, y_1 \cdot \ldots \cdot y_s) \subseteq I_{s+1} + (I_1 \cdot \ldots \cdot I_s).$$

2. Per inducció en $n$. Per a $n = 2$: $x \in I_1$, $y \in I_2$, $z \in I_1 \cap I_2$ tenim

$$z \cdot 1 = zx + zy \in I_1 I_2$$

per tant $I_1 \cap I_2 \subseteq I_1 I_2$, i clarament $I_1 I_2 \subset I_1 \cap I_2$. Suposem ara cert per a $n = s$, tenim que $I_1 \cdot \ldots \cdot I_s$ i $I_{s+1}$ són coprimers, per tant del cas 2 i hipòtesi inducció obtenim

$$(I_1 \cap \ldots \cap I_s) \cap I_{s+1} =^{H.I.} (I_1 \cdot \ldots \cdot I_s) \cap I_{s+1} =^{n=2} I_1 \cdot \ldots \cdot I_{s+1}.$$

□

**Corol·lari 4.6.5.** *Sigui $A$ domini commutatiu noetherià amb $dim_{Krull}(A) = 1$, sigui $I$ un ideal de $A$ amb $I \neq (0)$ i $I \neq A$. Llavors el conjunt $U$ d'ideals maximals de $A$ que contenen $I$ és un conjunt finit i a més existeixen $a_i \in \mathbb{N}_{\geq 1}$ complint:*

$$M_1^{a_1} \cdot \ldots \cdot M_s^{a_s} \subseteq I \subseteq M_1 \cdot \ldots \cdot M_s$$

*on $U = \{M_1, \dots, M_s\}$.*

*Demostració.* Per la proposició 4.6.1 tenim ideals maximals $M_i$ de $A$ i $a_i \geq 1$ naturals complint

$$M_1^{a_1} \cdot \ldots \cdot M_s^{a_s} \subseteq I \subseteq M_1 \cap \ldots \cap M_s.$$

Si $M$ és un ideal maximal de $A$ que conté $I$ tenim $M_1^{a_1} \cdot \ldots \cdot M_s^{a_s} \subseteq M$ i pel Lemma 4.6.3 existeix $i$ on $M_i \subseteq M$ i com ara ambdos són ideals maximals tenim $M = M_i$, i per tant $\{M_1, \dots, M_s\} = U$. Ara pel Lemma 4.6.4 obtenim que $M_1 \cap \ldots \cap M_s = M_1 \cdot \ldots \cdot M_s$. □

**Proposició 4.6.6.** *Sigui $A$ un domini noetherià amb $dim_{Krull}(A) = 1$ i local, és a dir amb un únic ideal maximal $M$. Són equivalents:*

1. *$A$ és domini de factorització única per ideals,*
2. *$A$ és un domini d'ideals principals,*
3. *$A$ és integrament tancat.*

*Demostració.* Sigui $A$ DFUideals, triem $x \in M \setminus M^2$, tenim $(x) = M^a$ de la proposició 4.6.1 amb $a \neq 2$, per tant $(x) = M$ i per tant $M$ és un ideal principal, llavors per exercici 9 llista, tenim que $A$ is DIP.

Si $A$ DIP clarament és DFUideals. També si $A$ DIP és integrament tancat.

Suposem $A$ integrament tancat, triem $x \in M$ amb $x \neq 0$, si $M = (x)$ per l'exercici 9 ja estem.

Doncs suposem que $(x) \neq M$, tenim llavors que $M^n \subseteq (x)$ i $M^{n-1} \subseteq (x)$, i triem $y \in M^{n-1} \setminus (x)$. Tenim llavors $y/x \in Quot(A)$, $y/x \notin A$ del fet que $(y) \not\subseteq (x)$. Pel fet de ser $A$ integrament tancat tenim que $y/x$ no és enter sobre $A$. Ara tenim de ser $A$ noetherià que $M$ és un $A$-mòdul finit generat i tenim $(y/x)M \not\subseteq M$ de ser $y/x$ no enter sobre $A$. Observem que per construcció $yM \subseteq M^n \subseteq (x)$ i per tant $(y/x)M \subseteq A$ i per tant $(y/x)M$ és un ideal de $A$ no contingut en l'únic ideal maximal de $A$ per tant $(y/x)M = A$ i d'aquí $M = (x/y)A$ és un ideal principal, usant l'exercici 9 de la llista d'exercicis d'aquest tema. □

**Teorema 4.6.7.** *Sigui $A$ un domini noetherià on $dim_{Krull}(A) = 1$ són equivalents:*

1. *$A$ és Dedekind,*
2. *$A$ és DFUideals.*

Abans de fer-ne la demostració, la idea és anar d'un domini a un domini local i usar la Proposició 4.6.6, això és usual la idea en anell fent servir les operacions elementals en Àlgebra Commutativa que descrivim en la subsecció següent.

### 4.6.1 Operacions elementals en dominis commutatius

Recomanem al lector interessat consultar el llibre [Atiyah-Macdonald] per a aprofundir coneixements de dominis commutatius.

Sigui $A$ un domini commutatius i $\mathfrak{p}$ un ideal primer de $A$, hi ha operacions usuals que són de gran utilitat per Geometria i Àlgebra i que usualment es donen en un curs bàsic d'Estructures algebraiques en un segon curs de Grau en Matemàtiques.

#### Fer quocient

Considerem el morfisme $proj : A \to A/\mathfrak{p}$ definit per $\pi(a) = a \ mod \ \mathfrak{p}$.

- Els ideals primers de $A/\mathfrak{p}$ estan en bijecció amb els ideals primers de $A$ que contenen $\mathfrak{p}$.
- $A$ noetherià llavors $A/\mathfrak{p}$ és noetherià.

**Localització en $S = A \setminus \mathfrak{p}$**

Tenim el morfisme $\pi : A \to S^{-1}A = A_{(\mathfrak{p})} = \{\frac{a}{b} | b \in S, a \in A\} \subseteq Quot(A)$ i compleix les propietats següents:

1. Els ideals primers del domini $S^{-1}A$ estan en bijecció amb els ideals primers de $A$ entre (0) i $\mathfrak{p}$.
2. $A$ noetherià llavors $A_{(\mathfrak{p})}$ és noetherià,
3. $A$ integrament tancat, llavors $A_{(\mathfrak{p})}$ és integrament tancat.
4. $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$ per a $I, J$ ideals de $A$, (on $S^{-1}I = \pi(I)A_{(\mathfrak{p})}$ ideal de $A_{(\mathfrak{p})}$)
5. si $J \subseteq I$ ideals de $A$ tenim: $I = J \Leftrightarrow S^{-1}J = S^{-1}I \ \forall S = A \setminus \mathfrak{M}$ amb $\mathfrak{M}$ ideal maximals de $A$.
6. Tenim la desigualtat

$$dim_{Krull}A_{(\mathfrak{p})} + dim_{Krull}(A/\mathfrak{p}) \leq dim_{Krull}(A).$$

**Completació de $A$ en $\mathfrak{p}$**

Observem que tenim la filtració

$$(0) \subseteq \ldots \subseteq (\mathfrak{p}^{n+k}) \subseteq \ldots \subseteq (\mathfrak{p}^n) \subseteq \ldots \subseteq (\mathfrak{p}) \subseteq A$$

i definim una successió de Cauchy $(a_n)_n$ en $A$ sota l'ideal $\mathfrak{p}$ si compleix $\forall \epsilon > 0$ $\exists n_0(\epsilon)$ on $a_m - a_0 \in \mathfrak{p}^{k(\epsilon)}$ $\forall m, n \geq n_0(\epsilon)$ on $k(\epsilon)$ és un natural cada cop més gran sempre que $\epsilon$ va a zero, i si $\epsilon \to 0$ llavors $k(\epsilon) \mapsto +\infty$. D'aquesta manera es defineix $A_{\mathfrak{p}}$ (compte en ,Àlgebra Commutativa alguns llibres $A_{\mathfrak{p}}$ denota $S^{-1}A$) com el domini (suposem $\cap_{n\in\mathbb{N}}\mathfrak{p}^n = (0)$) que consisteix de les successions de Cauchy en $A$ mòdulo les convergents a zero, i que és isomorf al limit projectiu $A/\mathfrak{p}^n$ variant $n$ respecte morfismes projecció, similarment com els nombres enters $p$-àdics vist al capítol 1 del curs.

Tenim el morfisme natural $hat : A \to A_{\mathfrak{p}}$ Tenim les següents propietats:

- Si $A$ noetherià llavors $A_{\mathfrak{p}}$ és noetherià.
- Si $A$ és noetherià amb $\mathfrak{p}$ l'únic ideal maximal, llavors $A_{\mathfrak{p}}$ és noetheria i únic ideal maximal $hat(\mathfrak{p})A_{\mathfrak{p}}$.
- Si $A$ noetherià tenim $dim_{Krull}(A_{\mathfrak{p}}) \leq dim_{Krull}(A)$ amb igualtat si i només si $\mathfrak{p} \subseteq rad(A) := \cap_{M\in Spec_{max}(A)}M$.

### 4.6.2 Algunes idees per a demostrar el teorema 4.6.7.

Fem un esquetx del Teorema 4.6.7 ja que caldria precisar més els conceptes d'àlgebra commutativa, però que donem per coneguts.

*Demostració.* Observem que si $A$ és Dedekind tenim que $A$ és integrament tancat per tant per les propietats de localització obtenim $A_{(\mathfrak{p})}$ és un domini integrament tancat i anell local amb únic ideal maximal $\pi(\mathfrak{p})A_{(\mathfrak{p})}$ per a tot ideal maximal $\mathfrak{p}$ de $A$ (recordem $dim_{Krull}(A) = 1$), i per tant de la Proposició 4.6.6

la condició intergrament tancat és equivalent a que $A_{(\mathfrak{p})}$ és un DFUideals per a tot ideal maximal $\mathfrak{p}$ de $A$.

Ara usant exercici 11, que afirma $A = \cap A_{(M)}$ on $M$ recorre tots ideals maximals de $A$ on $Quot(A) = Quot(A_{(M)}) = K$, podem demostrar que si $A_{(\mathfrak{p})}$ és integrament tancat per tot $\mathfrak{p}$ ideal maximal de $A$ llavors $A$ és integrament tancat.

Per tant per finalitzar la demostració del teorema és equivalent a poder demostrar: $A_{(\mathfrak{p})}$ DFUideals per a tot $\mathfrak{p}$ ideal maximal de $A \Leftrightarrow A$ és DFUideals.

En aquests apunts sol demostrarem una implicació: $\Rightarrow$

Considera $I$ un ideal de $A$ amb $I \neq (0)$. De la proposició 4.3.5 tenim

$$M_1^{b_1} \cdot \ldots \cdot M_s^{b_s} \subseteq I \subseteq M_1 \cdot \ldots \cdot M_s$$

amb $b_i \geq 1$ naturals on els ideals maximals de $A$ que contenen $I$ corresponen al conjunt $\{M_1, \ldots, M_s\}$. Considerem els morfismes de localització $\pi_i : A \to A_{(M_i)}$ per $i = 1, \ldots, s$ on $A_{(M_i)}$ són anells locals noetherians amb únic ideal maximal $M_i A_{(M_i)}$, i per tant $\pi_i(I) = (M_i A_{(M_i)})^{a_i}$ per un únic natural $a_i > 0$. Demostrarem que $I = M_1^{a_1} \cdot \ldots \cdot M_s^{a_s}$.

Per construcció:

$$I \subseteq \pi_1^{-1}((M_1 A_{(M_1)})^{a_1}) \cap \ldots \cap \pi_s^{-1}((M_s A_{(M_s)})^{a_s})$$

com $M_i^{a_i} \subseteq \pi_i^{-1}((M_i A_{(M_i)})^{a_i})$ i $M_i$ únic ideal primer de $A$ que conté $M_i^{a_i}$ tenim de les propietats de localització que $M_i^a = \pi_i^{-1}((M_i A_{(M_i)})^{a_i})$, ara de ser $M_i^{a_i}$ i $M_j^{a_j}$ coprimers per $i \neq j$ del lema 4.6.4 $M_1^{a_1} \cap \ldots \cap M_s^{a_s} = M_1^{a_1} \cdot \ldots \cdot M_s^{a_s}$ obtenim que

$$I \subseteq M_1^{a_1} \cdot \ldots \cdot M_s^{a_s}$$

i obtenim

$$\pi_i(I) = M_i^{a_i} A_{(M_i)} \subseteq \prod_{j=1}^{s} \pi_i(M_j^{a_j}) = \pi_i(M_i)^{a_i} = M_i^{a_i} A_{(M_i)}$$

per a tot ideal $M_i$ maximal per tant per la propietat de localitzacions obtenim que $I = M_1^{a_1} \cdot \ldots \cdot M_s^{a_s}$. □

## 4.7 Grup de classes d'ideals d'un domini Dedekind

Donat $A$ un domini, denotem

$$\mathcal{M}(A) := \{I \neq (0) \textit{ ideals de } A\}$$

amb $I \star J := I \cdot J$, és un monoid amb unitat (i.e. $\star$ és commutatiu, distribuitiu i amb element neurtre $I = A$)

**Definició 4.7.1.** *Donats $I, J \in \mathcal{M}(A)$. Diem $I \sim J$ si i només si $\exists \alpha, \beta \in A \backslash (0)$ on $(\alpha) \cdot I = (\beta) \cdot J$.*

**Lema 4.7.2.** *Es té que $\sim$ és una relació equivalència on a més es comporta bé amb l'operació $\star$, és a dir si $I \sim I'$ i $J \sim J'$ llavors tenim $I \star J \sim I' \star J'$.*

*Demostració.* Exercici pel lector. □

**Corol·lari 4.7.3.** *Suposem $A$ és un domini de Dedekind. Llavors $\mathcal{M}(A)/\sim$ amb $\star$ és un grup abelià.*

*Demostració.* Del Lema 4.7.2 tenim que $\mathcal{A}/\sim$ amb $\star$ és un monoid commutatiu amb unitat. Considerem $I \in \mathcal{M}(A)$ amb $I \neq (0)$, i podem escriure

$$I = \mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_s^{n_s}$$

amb $\mathfrak{p}_j$ ideals maximals de $A$ diferents i $n_j \geq 1$ enters. Triem $i \in I \setminus \{0\}$, i tenim

$$(i) \subseteq I \subseteq \mathfrak{p}_j$$

per $1 \leq j \leq s$, per tant podem escriure

$$(i) = \mathfrak{p}_1^{a_1} \cdot \ldots \mathfrak{p}_s^{a_s} \cdot \mathfrak{q}_1^{b_1} \cdot \ldots \cdot \mathfrak{q}_t^{b_t}$$

de ser DFUideals, ara localitzant en $A_{(\mathfrak{p}_i)}$ tenim que

$$(i)A_{(\mathfrak{p}_j)} = \mathfrak{p}_j^{a_j} A_{(\mathfrak{p}_j)} \subset IA_{(\mathfrak{p}_j)} = \mathfrak{p}_j^{n_j} A_{(\mathfrak{p}_j)}$$

per tant $n_j \leq a_j$ i escrivint

$$J = \mathfrak{p}_1^{a_1 - n_1} \cdot \ldots \mathfrak{p}_s^{a_s - n_s} \cdot \mathfrak{q}_1^{b_1} \cdot \ldots \cdot \mathfrak{q}_t^{b_t}$$

obtenim que $I \cdot J = (i)$, i per tant $I \cdot J \sim (1)$ d'on $[I] \in \mathcal{M}(A)/\sim$ té invers. □

**Definició 4.7.4.** *Donat $A$ un domini de Dedekind al grup abelià $\mathcal{M}(A)/\sim$ s'anomena el grup de classes ideals de $A$ o grup de Picard de $A$ i s'anota per $C\ell(A)$.*

Enunciem un teorema que no demostrarem aquest curs, per una demostració podeu consultar [Lorenzini, Chp.V,Theorem 3.10].

**Fet 4.7.5.** *Considerem $A = \mathbb{Z}$ o $\mathbb{F}_q[T]$, i $B$ la clausura entera de $A$ en $L$ on $L$ és una extensió finita i separable de $Quot(A)$. Llavors $C\ell(B)$ és un grup abelià finit.*

**Definició 4.7.6.** *Una extensió finita $K$ de $\mathbb{Q}$ o bé de $Quot(\mathbb{F}_q[T])$ s'anomena $K$* **un cos global***, i en cas de ser una extensió de $\mathbb{Q}$ s'anomena també que és un cos de nombres.*

**Definició 4.7.7.** *Sigui $K$ un cos de nombres, tenim l'anell d'enters $\mathcal{O}_K$ que correspon a la clausura entera de $\mathbb{Z}$ en el cos $K$, pel teorema 4.7.5 tenim que $C\ell(\mathcal{O}_K)$ és un grup abelià finit. En aquest cas també s'anota per $C\ell(K)$ i es parla del grup de classes d'ideals del cos $K$, i $|C\ell(\mathcal{O}_K)| = |C\ell(K)|$ s'anomena el nombre de classes d'ideals de $K$ (o $\mathcal{O}_K$) i s'anota per $h_K := |C\ell(K)|$.*

**Observació 4.7.8.** *Quan $K$ és un cos de nombres, tenim realment un domini de Dedekind "minimal", que tot domini de Dedekind el conté que correspon a l'anell d'enters, en canvi quan $K$ és un cos global de característica positiva en tenim dos de forma natural: un corresponent a la clausura entera de $\mathbb{F}_q[T]$ en $K$, i la clausura entera de $\mathbb{F}_q[1/T]$ en $K$.*

Hi ha un exercici que si $B$ és un domini de Dedekind tenim $C\ell(B) = \{1\}$ si i només si $B$ és domini de factorització única, si i només si $B$ és un domini d'ideals principals.

Anem a donar un resultat que ens ajuda a determinar $h_K$ quan $K$ és un cos de nombres. Per a una demostració d'aquest resultat podeu consultar [Lorenzini, Chp.V,§4].

**Teorema 4.7.9.** *Considerem $K$ un cos global (on $K \cap \overline{\mathbb{F}}_p = \mathbb{F}_q$, si $car(K) = p > 0$), i $B$ la clausura entera de $\mathbb{Z}$ ó $\mathbb{F}_q[T]$. Llavors existeix $\lambda_B \in \mathbb{R}^+$ on $\forall I$ ideal de $B$ amb $I \neq (0)$ es té que existeix $J \sim I$ en $C\ell(B)$ complint que $||J||_B := |B/J| \leq \lambda_B$.*

*Quan $K$ és un cos de nombres, $B$ correspon a l'anell d'enters s'obté que podem agafar*

$$\lambda_B = \prod_{i=1}^{n}(\sum_{j=1}^{n} |\sigma_i(\alpha_j)|_{\mathbb{C}})$$

*on $[L : K] = n$, $(\alpha_1, \ldots, \alpha_n)$ és una $A$-base de $B$ i $\sigma_j$ són les inmersions $\sigma_i : L \hookrightarrow \mathbb{C}$ definides de la següent manera: del curs de teoria de Galois $K = \mathbb{Q}(\alpha)$ cert $\alpha \in K$, i $Irr(\alpha, \mathbb{Q})[X]$ és un polinomi mònic de grau $n$ amb $n$ arrels diferents dins $\mathbb{C}$: $\gamma_1, \ldots, \gamma_n$, per tant escrivint $L = \mathbb{Q}[X]/Irr(\alpha, \mathbb{Q})[X]$ $\sigma_i([X]) := \gamma_i$ són les $n$ inmersions del cos $L$ dins els complexos.*

Anem a aplicar el Teorema 4.7.9 per donar exemples d'anells que no són dominis de factorització única però si són dominis de Dedekind.

**Exemple 4.7.10.** *Considerem $K = \mathbb{Q}(\sqrt{m})$ amb $m$ lliure de quadrats, enter i complint $m \equiv 2, 3 (mod\ 4)$, en aquest cas l'anell d'enters $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$. Llavor la $\lambda_B$ del teorema 4.7.9 correspon a:*

$$\lambda_{\mathbb{Z}[\sqrt{m}]} = \prod_{i=1}^{2}(\sum_{j=1}^{2} |\sigma_i(\alpha_j)|) = (1 + \sqrt{|m|})(1 + |-\sqrt{m}|) = (1 + \sqrt{|m|})^2$$

*amb $A$-base $\{1, \sqrt{m}\}$. Considerem cas $m = 2$ i veiem que $C\ell(\mathbb{Z}[\sqrt{2}]) = (1)$ i per tant $\mathbb{Z}[\sqrt{2}]$ és un DIP. Efectivament, sol cal considerar ideals $I \neq (0)$ de $\mathbb{Z}[\sqrt{2}]$ amb $||I|| \leq (1 + \sqrt{2})^2 < 6$ i com $I$ és producte d'ideals primers fàcil veure del que si $I = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_s^{e_s}$ tenim $||I|| = \prod_{i=1}^{s} ||\mathfrak{p}_i||^{e_i}$ i per tant ens podem restrigir a ideals primers ja que $||I||$ sempre serà un natural no zero (recordeu $|B/I| = ||I||_B$ on aquí no escrivim explícitament però és l'anell enters del cos involucrat).*

*Observem que si $P$ ideal maximal de $\mathcal{O}_K$ tenim $P \cap \mathbb{Z} = (p)$ per a cert primer $p$ i per tant $p||\mathcal{O}_K/P| = ||P||_{\mathcal{O}_K}$ (ja que $\mathbb{Z}/p \subseteq \mathcal{O}_K/P$). Per tant sol cal estudiar que succeeix amb $p = 2$ i $p = 3$.*

*Fixem-nos $2\mathbb{Z}[\sqrt{2}] = (\sqrt{2})^2$ i per tant fixeu-vos $(\sqrt{2})$ és ideal maximal de $\mathbb{Z}[\sqrt{2}]$ perquè $\mathbb{Z}[\sqrt{2}]/(\sqrt{2}) \cong \mathbb{Z}[X]/(X^2-2, X) \cong \mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/(2)[X]/(X) \cong \mathbb{Z}/(2)$ és un cos.*

*Observem també que $3\mathbb{Z}[\sqrt{2}]$ i $5\mathbb{Z}[\sqrt{2}]$ són ideals principals i primers de $\mathbb{Z}[\sqrt{2}]$. Comprovem-ho per a l'ideal $3\mathbb{Z}[\sqrt{2}]$, (el ideal 5 exercici al lector). Observem que $\mathbb{Z}[\sqrt{2}]/(3)$ és isomorf a $\mathbb{Z}/(3)[X]/(X^2-2)$ i com $X^2-2$ irreductible a $\mathbb{F}_3[X]$ tenim que és un cos i per tant és id. maximal, en particular ideal primer.*

*Per tant com tot ideal $I$ amb $||I|| < 6$ és principal tenim que $\mathbb{Z}[\sqrt{2}]$ és un Domini de Dedekind que és DIP. (Aquí per concloure hem de saber que com $p|||I||$ implica que $I \cap \mathbb{Z} \subseteq (p)$ i la factorització ideals primers de $I$ han de ser dins els primers d'enters de $K$ que pujen l'ideal $p$, en la secció següent treballarem més aquest punt).*

Abans de fer un exemple d'un domini de Dedekind que no sigui DIP (o DFU), es convenient mirar la secció següent i enunciem el següent lema, que deixem com exercici al lector.

**Lema 4.7.11.** *Considerem $K = \mathbb{Q}[\sqrt{d}]$ amb $d$ lliure de quadrats, enter i $d \equiv 2, 3 (mod\ 4)$, on l'anell d'enters correspon a $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Llavors es té:*

- *si $p|d$ llavors $p\mathcal{O}_K = (p, \sqrt{d})^2$ on $(p, \sqrt{d})$ és un ideal maximal,*
- *si $2 \nmid d$ llavors $2\mathcal{O}_K = (2, 1 + \sqrt{d})^2$ on $(2, 1 + \sqrt{d})$ és un ideal maximal*
- *si $p \nmid d$ amb $p$ senar llavors tenim:*

$$p\mathcal{O}_K = \begin{cases} p\mathcal{O}_K \text{ ideal primer si } (\frac{d}{p}) = -1 \\ (p, \sqrt{d} + n)(p, \sqrt{d} - n) \text{ si } (\frac{d}{p}) = 1 \end{cases}$$

*on si $d$ és un quadrat mòdul $p$ escrivim $n^2 \equiv d (mod\ p)$.*

**Exemple 4.7.12.** *Considerem ara el cas $m = -5$ i calculem $h_{\mathbb{Q}[\sqrt{-5}]}$ i veurem que no és 1 i per tant $\mathbb{Z}[\sqrt{-5}]$ és Dedekind però no DFU amb elements.*

*Efectivament, del teorema 4.7.9 tenim que*

$$\lambda_{\mathbb{Z}[\sqrt{-5}]} = (1 + \sqrt{5})^2 < 11$$

*i del Lema 4.7.11 obtenim la següent factorització en ideals primers dels ideals $i\mathbb{Z}[\sqrt{-5}]$ per a $i = 2, 3, 5, 7$:*

$$(2) = (2, 1 + \sqrt{-5})^2 = P^2$$
$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = P_1 \cdot P_2$$
$$(5) = (\sqrt{-5})^2 = P_3^2$$
$$(7) = (7, 3 + \sqrt{-5})(7, 3 - \sqrt{5}) = P_4 \cdot P_5$$

*on es pot demostrar que $P, P_1, P_2, P_3, P_4, P_5$ són ideals primers diferents i no són ideals principals llevat de $P_3$ i per tant $C\ell(\mathbb{Z}[\sqrt{-5}])$ no és el grup abelià trivial i per tant $|h_{\mathbb{Q}[\sqrt{-5}]}| \neq 1$.*

*Fàcilment podem demostrar que tenim les següents relacions entre els ideals primers de norma menor que 11 com ideals de $\mathbb{Z}[\sqrt{-5}]$:*

$$(2)(3, 1 \pm \sqrt{-5}) = (1 \pm \sqrt{-5})P$$
$$(2)(3 \pm \sqrt{-5}) = (3 \pm \sqrt{-5})P$$

*per tant en $C\ell(\mathbb{Z}[\sqrt{-5}])$ tot ideal de norma menor que 11 és principal o bé equivalent a $P$ i tenim $P^2 = (2)$ ideal principal per tant s'obté*

$$C\ell(\mathbb{Z}[\sqrt{-5}]) = \{(1), P\}$$

*i $C\ell(\mathbb{Z}[\sqrt{-5}]) \cong \mathbb{Z}/(2)$ amb $h_{\mathbb{Q}[\sqrt{-5}]} = 2$.*

## 4.8 Relació entre els ideals primers en clausures enteres d'una extensió de cossos

En aquesta secció pensarem sempre amb la següent notació i situació, tenim $A$ un domini de Dedekind, i $K = Quot(A)$, considerem $L/K$ una extensió finita i i separable de cossos sobre el cos $K$, i $B$ la clausura entera de $A$ en $L$, per resultats anteriors sabem que $B$ també és un domini de Dedekind, per tant tant $A$ com $B$ són DFUideals.

**Lema 4.8.1.** *En la situació d'aquesta secció, donat $P$ ideal primer de $A$ llavors $PB \neq B$.*

*Demostració.* Si $P = (\ell)$ és un ideal principal de $A$ i $PB = B$ existeix $b \in B$ on $\ell b = 1$ i $b \notin A$ ja que $P \neq A$, com $B$ és enter sobre $A$, existeix $f(X) \in A[X]$ mònic de grau mínim on $f(b) = 0$, escrivim $f(X) = X^N + a_{N-1}X^{N-1} + \ldots + a_0 \in A[X]$ i usant que $fb = 1$ obtenim

$$0 = \ell f(b) = b^{N-1} + a_{N-1}b^{N-2} + \ldots + a_1 + \ell \cdot a_0$$

d'on obtenim una $A$-relació de $b$ de grau $< N$, per la minimalitat de $f(X)$ obtenim que $b$ no existeix i per tant $PB \neq B$.

Suposem ara $P$ és ideal maximal de $A$ però que no es principal. Considerem $A_{(P)}$ anell localitzat que per les propietats de localització és un domini de Dedekind amb un únic ideal maximal, i per exercici 14 de les llistes tenim que $A_{(P)}$ és un domini d'ideals principals. D'aquì $PA_{(P)} = \pi A_{(P)}$, si ara $PB = B$ s'obté amb $S = A \setminus P$ que $S^{-1}PS^{-1}B = S^{-1}B$ però entra contradicció en el cas vist anteriorment. □

Per tant donat $P$ ideal maximal de $A$ podem escriure gràcies al Teorema 4.6.7 i el lemma 4.8.1

$$PB = M_1^{e_1} \cdot \ldots \cdot M_s^{e_s}$$

on $M_i$ són els ideals maximals de $B$ complint que $M_i \cap A = P$, el natural $e_i \geq 1$ s'anomena l'índex de $M_i$ sobre $P$ i s'anomena l'ındex de **ramificació** de $M_i$ sobre $P$ i també s'anota aquest valor per $e_{M_i/P}$.

Com $M_i \cap A = P$ tenim una inclussió de cossos $A/P \hookrightarrow B/M_i$ per a $i = 1, \ldots, s$ i com $B$ és un $A$-mòdul finit generat i tenim que $(B/M_i)/(A/P)$ és una extensió finita de cossos i $f_{M_i/P} := [B/M_i : A/P]$ s'anomena el **grau residual de $M_i$ sobre $P$.**

**Exemple 4.8.2.** *Sigui $A = \mathbb{Z}$ $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$ i $B = \mathbb{Z}[i]$. Considerem $P = 2\mathbb{Z}$ i com $2 = i(i-1)^2$ i com $i$ és una unitat obtenim*

$$PB = ((i-1)B)^2$$

*on $(i-1)B$ és un ideal maximal (i primer) de $B$ ja que $\mathbb{Z}[i]/(i-1) \cong \mathbb{Z}[Y]/(Y^2+1, Y-1) \cong \mathbb{Z}[Y]/(2, Y-1) \cong (\mathbb{Z}/(2))[Y]/(Y-1) \cong \mathbb{Z}/(2)$, i per tant $f_{(i-1)B/P} = 1$ i $e_{(i-1)B/P} = 2$.*

**Teorema 4.8.3.** *En la situació d'aquest capítol on $P$ ideal maximal de $A$ llavors*

$$[L : K] = \sum_{\mathfrak{M}|PB} e_{\mathfrak{M}/P} f_{\mathfrak{M}/P}$$

*on $\mathfrak{M}$ recorre tots els ideals maximals de $B$ que divideixen $PB$ o equivalentment que apareixen en la descomposició amb ideals primers de $PB$ en el domini de Dedekind $B$.*

**Definició 4.8.4.** *Donada la situació d'aquesta secció els ideals maximals de $A$ $P$ on existeix un $M_i$ ideal maximal de $B$ on $e_{M_i/P} > 1$ diem que l'extensió $L/K$ ramifica en l'ideal $P$ o en l'ideal $M_i$ (observem que $M_i \cap A = P$). Una extensió $L/K$ de cossos de nombres és diu no ramificada si no existeix cap $P$ que ramifica entre $B/A$. Diem que un primer $P$ de $A$ explita completament si $f_{M_i/P} = 1$ per tot ideal maximal $M_i$ de $B$ sobre $P$ i $e_{M_i/P} = 1$ (per ideals primers $M$ de $B$ diem splita en $B/A$ si l'ideal primer $P = M \cap A$ esplita completament en $B/A$).*

*Demostració.* [Teorema 4.8.3] Escrivim $PB = \prod_{i=1}^{s} M_i^{e_i}$ amb $M_i^{e_i}$ coprimers dos a dos. Per l'exercici 12 de la llista d'exercicis d'aquest tema obteni un isomorfime d'anells (en particular de $A/P$-espais vectorials):

$$B/PB \to^{\cong} \prod_{i=1}^{s} B/M_i^{e_i}.$$

El resultat s'obté de demostrar els dos ítems següents:

- $dim_{A/P}(B/PB) = [L : K]$,
- per $i = 1, \ldots, s$ es té $dim_{A/P}(B/M_i^{e_i}) = e_{M_i/P} f_{M_i/P}$.

Primer provarem els dos ítems anteriors suposant que $A$ i $B$ son dominis d'ideals principals.[1]

Observem que $B$ és un $A$-mòdul lliure de torsió, i com hem vist $\exists d \in A \setminus \{0\}$ on $e_1 A + \ldots + e_N A \subset B \subseteq \frac{e_1}{d} A + \ldots + \frac{e_N}{d} A$ on $N = [L : K]$ i de ser DIP tenim $P = \pi A$ amb $\pi \in A$ d'on

$$B/\pi B \cong (\oplus_{i=1}^{N} A)/\pi(\oplus_{i=1}^{N} A) \cong (A/(\pi))^N.$$

Pel segon punt a demostrar com $P \subset M^e$ tenim $B/M^e$ és un $A/P$-espai vectorial, i demostrem per inducció en $e$ que

$$dim_{A/P}(B/M^e) = e dim_{A/P}(B/M).$$

El cas $e = 1$ és obvi. Suposem cert per $e - 1$ i considerem la successió exacta de $A/P$-mòduls:

$$0 \to M^{e-1}/M^e \to B/M^e \to B/M^{e-1} \to 0$$

i per tant com son espais vectorials tenim

$$dim_{A/P}(B/M^e) = dim_{A/P}(B/M^{e-1}) + dim_{A/P}(M^{e-1}/M^e) =$$

$$(e-1) dim_{A/P}(B/M) + dim_{A/P}(M^{e-1}/M^e).$$

[1] En el pla d'estudis a Estructures Algebraiques haurien d'haver vist el teorema de classificació de grups abelians que afirma que tot grup abelià finit generat és $\mathbb{Z}^n \oplus \mathbb{Z}/(d_1) \oplus \ldots \mathbb{Z}/(d_s)$ on $d_1 | \ldots | d_s$ i és única amb aquesta propietat, on $n$ és el rang del grup abelià. Fixem-nos que un grup abelià finit generat és un $\mathbb{Z}$-modul finti generat. En cas de $A$-mòduls finit generats amb $A$ un DIP hi ha un teorema de classificació similar sustituint $\mathbb{Z}$ per $A$ i $d_i$'s per elements d'$A$, i si és un $A$-mòdul lliure de torsió tenim és de la forma $A^n$

Ara $M = mB$ de ser $B$ DIP, i considerem $\vee : B \to M^{e-1}/M^e$ via $\vee(1) = m^{e-1}(mod\ M^e)$ és epimorfisme de $A/P$-espais vectorials i $\vee(ab) = \vee(a) \vee (b)$ amb $M \subseteq Ker(\vee)$ d'on podem pensar $\vee : B/M \to M^{e-1}/M^e$ pero com $B/M$ és un cos i la propietat amb el producte tenim que és injectiu morfisme $\vee$. Això finalita el cas $A$ i $B$ son DIPs.

Considerem $A$ i $B$ dos dominis de Dedekind qualsevols.

Considerem el conjunt multiplicativament tancat $S = A \setminus P$, i tenim $S^{-1}A = A_{(P)}$ és un domini de Dedekind amb un únic ideal maximal, i per l'exercici 14 tenim que $A_{(P)}$ és DIP, fixem-nos llavors $S^{-1}B$ és també un Domini de Dedekind amb un número finit d'ideals maximals que corresponen a $S^{-1}M_i$ i per l'exercici 14 d'aquest tema tenim que $S^{-1}B$ també és un DIP.

Ara de les propietats de localització d'anells tenim que l'ideals tenim

$$(S^{-1}P)(S^{-1}B) = \prod_{i=1}^{s}(S^{-1}M)^{e_i}$$

i usant el que hem demostrat per Dominis de Dedekind que són DFU obtenim que

$$[L : K] = \sum_{i=1}^{s} e_i \tilde{f}_i$$

on $\tilde{f}_i := dim_{S^{-1}A/S^{-1}P}(S^{-1}B/S^{-1}M_i)$ i de propietats localització d'Àlgebra Commutativa l'anterior dimensió coincideix amb $dim_{A/P}(B/M_i)$ ja que en localitzar per $S$ no afect la dimensió, amb això finalitzaria la demostració del teorema. □

**Observació 4.8.5.** Si en el Teorema 4.8.3 assumim que $L/K$ és una extensió de Galois, on $P$ és un primer de $K$. Llavors es té que tots els $e_{\mathfrak{M}/P}$ són iguals a cert natural $e$ per a tot $\mathfrak{M}|PB$, i tots els graus residuals $f_{\mathfrak{M}/P}$ són igual a cert natural $f$ per a tot $\mathfrak{M}|PB$, i per tant

$$[L : K] = efs$$

on $s$ son els primers diferents de $B$ en que descomposa $PB$ com producte d'ideals primers en el domini de Dedekind B.

**Exemple 4.8.6.** *L'ideal $(1-\zeta)\mathbb{Z}[\zeta]$ és un ideal primer de $\mathbb{Z}[\zeta]$ on $\zeta = e^{2\pi i/p}$ amb $p$ primer senar, on assumim que $\mathbb{Z}[\zeta]$ és l'anell d'enters del cos $\mathbb{Q}(\zeta_p)$, i a més $p\mathbb{Z}[\zeta] = (1-\zeta)^{p-1}$ i per tant $(p)$ ramifica en $\mathbb{Q}[\zeta]/\mathbb{Q}$.*

*Efectivament, de $X^{p-1} + \ldots + X + 1 = \prod_{j=1}^{p-1}(X - \zeta^j)$, i fent $X = 1$ obtenim $p = \prod_{j=1}^{p-1}(1-\zeta^j)$ i per tant*

$$p\mathbb{Z}[\zeta] = \prod_{j=1}^{p-1}((1-\zeta^j)\mathbb{Z}[\zeta]).$$

*Ara per finalitzar demostrarem que $(1-\zeta)\mathbb{Z}[\zeta] = (1-\zeta^j)\mathbb{Z}[\zeta]$ per a $j = 2, \ldots, p-1$. Triem $\ell$ on $1 \equiv j\ell(mod\ p)$, i tenim:*

$$\frac{1-\zeta}{1-\zeta^j} = \frac{\zeta - 1}{\zeta^j - 1} = \frac{\zeta^{j\ell} - 1}{\zeta^j - 1} = 1 + \zeta^j + \ldots + \zeta^{j(\ell-1)} \in \mathbb{Z}[\zeta]$$

*i similarment* $\frac{1-\zeta^j}{1-\zeta} \in \mathbb{Z}[\zeta]$ *i per tant* $\frac{1-\zeta}{1-\zeta^j} \in \mathbb{Z}[\zeta]^*$ *i per tant*

$$(1-\zeta)\mathbb{Z}[\zeta] = (1-\zeta^j)\mathbb{Z}[\zeta]$$

*i per tant* $p\mathbb{Z}[\zeta] = ((1-\zeta)\mathbb{Z}[\zeta])^{p-1}$.

## 4.9 Atacant l'equació de Fermat $X^p + Y^p = Z^p$.

**En aquesta secció volem demostrar el primer cas de l'equació de Fermat donada per Kummer.**

**Teorema 4.9.1** (Kummer)**.** *Sigui* $p \geq 5$ *un primer i suposem que* $p \nmid C\ell(\mathbb{Q}(e^{2\pi i/p}))$ *llavors no hi ha* $x, y, z$ *enters amb* $xyz \neq 0$ *i* $p \nmid xyz$ *complint:*

$$x^p + y^p = z^p.$$

### 4.9.1 Reducció dins el domini de Dedeking $\mathbb{Z}[e^{2\pi i/p}]$ a elements

**Suposem que existeixen aquests** $x, y, z \in \mathbb{Z}$ **satisfent l'equació de Fermat i canviant** $y$ **per** $-y$ **podem pensar que** $x^p - y^p = z^p$**, i recordem l'anell d'enters de** $\mathbb{Q}[e^{2\pi i/p}]$ **és** $B = \mathbb{Z}[e^{2\pi i/p}]$**, sense perdua de generalitat podem suposar que** $mcd(x, y, z) = 1$**, escrivim** $\xi = e^{2\pi i/p}$**. Tenim la factorització en aquest any via:**

$$z^p = \prod_{i=0}^{p-1}(x - \xi^i y)$$

**Com** $B$ **és Dedekind l'ideal principal** $t_i := (x - \xi^i y)$ **té una factorització amb ideals primers de** $B$**, observem que** $t_i$ **i** $t_j$ **son coprimers 2 a 2 com ideals. Suposem que existeix un ideal prime** $\mathfrak{p}$ **complint** $\mathfrak{p}|(x - \xi^i y)$ **i** $\mathfrak{p}|(x - \xi^j y)$ **amb** $i \neq j$**. Per tant:**

$$x - \xi^i y - (x - \xi^j y) = (\xi^j - \xi^i)y = \xi^j(1 - \xi^{i-j})y \in \mathfrak{p}$$

$$\xi^j x - \xi^{i+j} y - (\xi^i x - \xi^{j+1} y) = (\xi^j - \xi^i)x \in \mathfrak{p}$$

**d'aquí obtenim** $\xi^j(1 - \xi^{i-j})(x, y) \subseteq \mathfrak{p}$**, on observem que** $mcd(x, y) = 1$ **(de ser** $mcd(x, y, z) = 1$ **i satisfer l'equació de Fermat), i per tant** $(x, y) = (1)$ **d'on obtenim que** $(1 - \xi^k) \subseteq \mathfrak{p}$**, i per l'exemple 4.8.6 sabem que** $(1 - \xi^k) = (1 - \xi)$ **és un ideal primer de** $B$ **d'on** $\mathfrak{p} = (1 - \xi)$**.**

**De complir l'equació de Fermat obtenim doncs** $z^p \in \mathfrak{p}$ **i de ser ideal primer obtenim** $z \in \mathfrak{p} \cap \mathbb{Z} = (p)$ **on** $p|x$ **en contra de la hipòtesi que** $p \nmid xyz$**. Per tant** $(t_0), \ldots, (t_{p-1})$ **són ideals principals de** $B$ **coprimers dos a dos.**

**Tenim la igualtat ideals en** $B$**:** $(t_0) \cdot \ldots \cdot (t_{p-1}) = (z)^p$ **i obtenim una factorització única amb ideals primers i de ser els** $(t_i)'s$ **coprimers obtenim que**

$$(t_i) = \mathfrak{A}_i^p$$

**on $\mathfrak{A}_i$ un ideal de $B$. Ara com $p \nmid C\ell(B)$ obtenim que $\mathfrak{A}_i = (a_i)$ és un ideal principal de $B$ i per tant**

$$t_i = u_i a_i^p$$

**on $u_i \in B^*$ per $i = 0, \ldots, p-1$.**

### 4.9.2 Treballant amb propietats d'elements per l'anell $\mathbb{Z}[\xi]$

**Un cop reduït a treballar amb elements en anell $\mathbb{Z}[\xi]$ ja es sabia que el teorema de Fermat es compleix, amb un estudi de propietats d'elements de l'anell $B = \mathbb{Z}[\xi]$, anem a detallar un procediment.**

**Lema 4.9.2.** *Si $a \in \mathbb{Z}[\xi]$ llavors $a^p$ és congru modul $p\mathbb{Z}[\xi]$ a un enter.*

*Demostració.* Recordem que $(1-\xi)^p = (p)$ com ideals de $\mathbb{Z}[\xi]$ i $(1-\xi) \cap \mathbb{Z} = (p)$, i tenim que $\mathbb{Z}[\xi]/(1-\xi) = \mathbb{Z}/p$ per la propietat de Dominis de Dedekind e extensió d'ideals en torres de dominis de Dedekind. Prenem doncs ara l'element $a = a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}$ amb $a_i \in \mathbb{Z}$ obtenim fent mòdul ideal $(p)$ la congruència:

$$a^p \equiv a_0^p + (a_1\xi)^p + \ldots + (a_{p-2}\xi^{p-2})^p \equiv \sum_{i=0}^{p-2} a_i^p.$$

□

**Lema 4.9.3.** *Escrivim $a = b_0 + b_1\xi + \ldots b_{p-1}\xi^{p-1} \in \mathbb{Z}[\xi]$ amb $b_i \in \mathbb{Z}$ (or recordem que $\xi^{p-1} = -\sum_{i=0}^{p-2} \xi^i$). i suposem que algun dels $b_i = 0$ per cert $i$. Si $n \in \mathbb{Z}$ divideix $a$, llavors $n$ divideix cada $b_j$.*

*Demostració.* Fixem-nos que a $\mathbb{Z}[\xi]$ és un $\mathbb{Z}$-module finit generat lliure sense torsió (=grup abelià finit generat) per un subconjunt qualsevol de $p-1$ elements en el conjunt de $p$ elements $S := \{1, \xi, \ldots, \xi^{p-1}\}$, i per tant si algun $b_i = 0$ triem els generadors per aquest grup $S \setminus \{\xi^i\}$ d'on obtenim el resultat. □

**Lema 4.9.4.** *Sigui $u$ una unitat de $\mathbb{Z}[e^{2\pi i/p}]$ (recordem que aquest domini és l'anell d'enters de $\mathbb{Q}[e^{2\pi i/p}]$). Llavors existeix $\varepsilon \in \mathbb{Z}[\xi + \xi^{-1}]$ on*

$$u = \xi^r \varepsilon$$

*per algun $r$ natural.*

*Demostració.* Escrivim $\beta = \frac{\overline{u}}{u}$ on $\overline{x}$ denota la conjugació complexa del nombre $x$, com $u \in \mathbb{Z}[\xi]^*$ tenim que $\beta \in \mathbb{Z}[\xi]$. Fixem-nos que per tot $\sigma \in Aut_{\mathbb{Q}}(\mathbb{C})$ commute amb conjugació complexa i per tant

$$|\sigma(\beta)| = |\frac{\overline{\sigma(u)}}{\sigma(u)}| = 1$$

Per tant $|\sigma(\beta)| = 1$ per a tot $\sigma$. Veiem ara que $\sigma = \xi^r$ per a cert $r$, (observem que les arrels unitats dins $\mathbb{Q}[\xi]$ són tant sols potències de $\xi$). Suposem doncs que $\beta$ no fos una potencia de $\xi$ i $\pm 1$, per tant $\beta^n$ son diferents per tot $n$, pero $\beta^n \in \mathbb{Z}[\xi]$ i per tant $Irr(\beta^n, \mathbb{Q})[X] = \sum_{i=0}^{m_n} a_i(n) X^i \in \mathbb{Z}[\xi]$ i els coeficients amb

valor absolut estan acotats, per exemple $|a_0(n)| = 1$ i $|a_1(n)| = |suma\ arrels| \leq 1+\ldots+1 = m_n \leq [\mathbb{Q}[\xi] : \mathbb{Q}]$ i per cada coeficient, per tant sol tenim un numero finit de polinomis, i per tant no poden ser infinits $\beta^n$'s amb $n$ natural diferents, per tant $\beta = \xi^k$ per a cert $k$.

Per tant tenim $u = \pm\xi^t\overline{u}$. Escrivim $u = c_0 + c_1\xi + \ldots + c_{p-2}\xi^{p-2}$ amb $c_i \in \mathbb{Z}$ tenim fent mòdul per l'ideal $(1-\xi)$ tenim que $u \equiv c_0+c_1+\ldots+c_{p-2}\ (mod(1-\xi))$ (on iguals en el cos $\mathbb{Z}[\xi]/(1-\xi)$), i com $\overline{u} = c_0+c_1\xi^{-1}+\ldots+c_{p-2}\xi^{2-p}$ fent modul $(1-\xi)$ otenim $u \equiv \overline{u}(mod\ (1-\xi))$. Ara si $u = -\xi^t\cdot\overline{u}$ obtenim $u \equiv -u(mod\ (1-\xi))$ d'on $2u \equiv 0(mod\ \xi-1)$ però $2 \nmid (\xi-1)$ (recordem que $(\xi-1)$ es sobre ideal de $\mathbb{Z}$ $(p)$ disjunt amb 2) i $u$ tampoc ja que és una unitat, per tant no pot ser.

D'aquí obtenim que

$$u = +\xi^t\overline{u}.$$

Triam $r$ on $2r \equiv t(mod\ p)$ i escrivim $\varepsilon := \xi^{-r}u$, fixem-nos que $\overline{\varepsilon} = \xi^r\overline{u} = \xi^{-r}u = \varepsilon$ per tant hem construït

$$u = \xi^r\varepsilon$$

amb $\varepsilon \in \mathbb{Z}[\xi] \cap \mathbb{R} \subseteq \mathbb{Z}[\xi+\xi^{-1}]$. □

### 4.9.3 Demostració primer cas del Teorema de Fermat

**Farem tot seguit una demostració del Teorema 4.9.1.**

*Demostració.* Si $x, y, z$ enters amb $xyz \neq 0$ i $p \nmid xyz$ i $p \nmid C\ell(\mathbb{Q}(\xi))$ on $x^p - y^p = z^p$ tenim que podem escriure

$$x - \xi y = \xi^r\varepsilon_1\delta^p$$

amb $\varepsilon_1$ de $\mathbb{Z}[\xi+\xi^{-1}]$ i $\delta \in \mathbb{Z}[\xi]$, per cert enter $r$.

Usem ara que $\delta^p \equiv a$ modul $p$ per un lema de la subsecció anterior amb $a$ un enter d'aquí:

$$x - \xi y = \xi^r\varepsilon_1\delta^p \equiv \xi^r\varepsilon_1 a(mod\ (p))$$

$$x - \xi^{-1}y = \xi^{-r}\varepsilon_1\overline{\delta}^p \equiv \xi^{-r}\varepsilon_1\overline{a}(mod\ (\overline{p}))$$

on la barra denota aquí la conjugació complexa, i observem que $\overline{a} = a$ i $(p) = (\overline{p})$, per tant obtenim

$$\xi^{-r}(x - \xi y) \equiv \xi^r(x - \xi^{-1}y)(mod\ p)$$

o equivalentment:

$$x - \xi y - \xi^{2r}x + \xi^{2r-1}y \equiv 0(mod\ (p)). \tag{4.1}$$

Ara si $1, \xi, \xi^{2r}, \xi^{2r-1}$ són tots diferents, llavors ($p \geq 5$) tenim pel Lemma 4.9.3 obtenim que $p$ divideix $x$ i $y$, en contradicció amb les hipòtesis.

Suposem ara que dos dels nombres $1, \xi, \xi^{2r}, \xi^{2r-1}$ són iguals, considerant tots les situacions possibles.

- Suposem $1 = \xi^{2r}$. De l'equació (4.1) obtenim

  $$-\xi y + \xi^{-1}y \equiv 0(mod\ p)$$

  d'on pel Lemma 4.9.3 obtenim $p|y$ en contra la hipòtesi que $p \nmid xyz$.

- Suposem $\xi = \xi^{2r-1}$. De l'equació (4.1) obtenim

$$x - \xi^2 x \equiv 0(mod\ p)$$

  i pel Lemma 4.9.3 obtenim $p|x$ en contra la hipòtesi que $p \nmid xyz$.

- Falta per finalitzar estudiar el cas $1 = \xi^{2r-1}$. De l'equació (4.1) obtenim:

$$(x+y) + (x+y)\xi \equiv 0(mod\ p).$$

  Del Lemma (4.1) obtenim que $x + y \equiv 0(mod\ p)$ i per tant sempre

$$x \equiv -y(mod\ p),$$

  on $x^p - y^p = z^p$ amb $x, y, z$ enters d'on fent modul $p$ tenim $z \equiv z^p \equiv x^p - y^p \equiv x - y \equiv\equiv -2y \equiv y \equiv 0(mod\ p)$ en contra hipòtesi que $p \nmid xyz$.

Per tant obtenim el resultat Teorema 4.9.1.

□

### 4.9.4 Sobre condició $p \nmid |C\ell(\mathbb{Z}[\xi])|$.

**Definició 4.9.5.** *Diem que un primer p enter és regular si* $p \nmid h_{\mathbb{Q}[\xi]} = |C\ell(\mathbb{Z}[\xi])|$.

**Considerem ara el desenvolupament al voltant del zero de**

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

**on** $B_i \in \mathbb{Q}$ **s'on els nombres de Bernouilli que compleixen diverses propietats com** $B_{2k+3} = 0$**, per** $k \geq 0$ **i per exemple:**

$$B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_4 = -1/30 = B_8,$$

$$B_6 = 1/42, B_{10} = 5/66, B_{12} = -691/2730, \ldots$$

**Fet 4.9.6** (Kummer)**.** *$p|h_{\mathbb{Q}(e^{2\pi i/p})}$ si i només si p divideix el numerador d'algun nombre de Bernouilli $B_{2k}$, amb $k = 2, 4, \ldots, p-3$.*

**Inspirat amb aquest resultat es va intentar estudiar molt aquests números. I en particular, Kummer va demostra de forma analítica el que s'anomena actualment congruències de Kummer:**

**Fet 4.9.7** (Kummer)**.** *Suposem $m \equiv n \not\equiv 0(mod\ p-1)$ amb $m, n$ enters parells positius. Llavors:*

$$\frac{B_m}{m} \equiv \frac{B_n}{n}(mod\ p)$$

**i va demostrar que**

**Fet 4.9.8.** *Hi ha una infinitut de primers irregulars.*

**Observació 4.9.9.** *Els vuit primers irregulars corresponen a:*

$$37, 59, 67, 101, 103, 131, 149 \text{ } i \text{ } 157.$$

**Referent als denominadors que poden aparèixer als nombres de Bernoulli, ja era conegut en el temps del Kummer i era el resultat següent:**

**Fet 4.9.10** (von Staudt-Clausen)**.** *Sigui $n$ un enter positiu i parell. Llavors*

$$B_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z}$$

*on la suma es sobre els nombres primers $p$ on $p-1$ divideix $n$.*

**Podeu llegir una demostració dels Fets d'aquesta secció en [Washington, Chapter 5].**

## 4.10 Exercicis del Tema.

1. **Trobeu l'anell d'enters del cos $\mathbb{Q}(e^{2\pi i/N})$ amb $N$ un natural.**

2. **Considera $k(X)$ el cos de fraccions en l'anell de polinomis en la variable $X$ a coeficients en un cos $k$ algebraicament tancat. Sigui $f(X,Y) \in k[X,Y]$ amb $X,Y$ variables irreductible. Estudieu quan $k[C_f] := k[X,Y]/f(X,Y)$ és noetherià. Estudieu quan $k[C_f]$ té dimensió de Krull 1.**

3. **Considera $k[C_f]$ amb $f(X,Y) = Y^2 - X^3$. Proveu que $k[C_f]$ no és integrament tancat. Qui seria la clausura entera de $k[X]$ dins el cos de fraccions de $k[C_f]$?**

4. **Considera $k[C_f]$ amb $f(X,Y) = Y^2 - X^3 - X^2$. Proveu que $f(X,Y) \in k[X,Y]$ és irreductible i trobeu la clausura entera de $k[X]$ dins el cos de fraccions de $k[C_f]$.**

5. **Considera $k[C_f]$ on $f = Y^2 - X^3 - aX - b \in k[X,Y]$ on defineix una corba el.líptica. Demostreu que $k[C_f]$ és un domini de Dedekind.**

6. **Penseu els tres exercicis anteriors amb $k$ no algebraicament tancat.**

7. **Trobeu qui són tots els ideals maximals de $k[X,Y]$ amb $k$ algebraicament tancat on $k[X,Y]$ és anell en dues variables $X,Y$ a coeficients en el cos $k$ algebraicament tancat.**

8. **Trobeu tots els ideals maximals de $k[C_f]$ quan $f(X,Y) \in k[X,Y]$ irreductible amb $k$ algebraicament tancat.**

9. **Sigui $A$ un anell commutatiu. Son equivalents: (1) tot ideal de $A$ és principal, (2) tot ideal primer de $A$ és principal.**

10. **Sigui $A$ un domini llavors**

    $$A = \cap_{P \in Spec(A)} A_{(P)} = \cap_{M \in Spec_M(A)} A_{(M)}$$

    **on $Spec(A)$ són tots els ideals primers del domini $A$ i $A_{(P)}$ és la localització de l'anell $A$ amb l'ideal primer $P$.**

11. **Considera $f(X,Y) = Y^2 - X^3(1-X)$ i observem que $k[C_f]$ és un domini però no integrament tancat. Trobeu la clausura entera dins el cos de fraccions de $k[C_f]$.**

12. **Sigui $A$ un anell commutatiu. Siguin $I_1, \ldots, I_n$ $n$ ideals de $A$. Suposem que $I_i$ i $I_j$ son coprimers si $i \neq j$. Siguin donats $y_1, \ldots, y_n \in A$. Llavors existeix $y \in A$ complint que per a tot $i = 1, \ldots, n$ amb $y - y_i \in I_i$.**

13. **Sigui $A$ un domini de Dedekind. Demostreu que tot ideal de $A$ es pot generar amb dos elements de $A$.**

14. **Si $A$ un domini de Dedekind on té un número finit d'ideals maximals, llavors $A$ és un domini d'ideals principals.**

**15. Proveu que el nombre de classes de $\mathbb{Q}(\sqrt{-11})$ és 1.**

**16. Sigui $d = p_1 \cdot \ldots \cdot p_n$ un enter lliure de quadrats amb $p_i$ primers diferents. Sigui $L = \mathbb{Q}(\sqrt{-d})$. Proveu que el grup de classes de l'anell d'enters de $L$ conté un subgrup isomorf a $(\mathbb{Z}/(2))^{n-1}$.**

**17. Sigui $K = \mathbb{Q}(\sqrt{m})$ amb $K/\mathbb{Q}$ de grau 2, $G = Gal(K/\mathbb{Q}) = \{\sigma, id\}$. Sigui $\alpha \in K^*$ on $\sigma(\alpha)\alpha = 1$. Demostreu existeix $\gamma \in \mathcal{O}_K$, l'anell d'enters de $K$, complint $\alpha = \sigma(\gamma)/\gamma$.**

**18. Demostreu que el nombre de classes de $\mathbb{Q}(\sqrt{-p})$ és senar si $p \equiv 3(mod\ 4)$.**

**19. Demostreu que el nombre de classes de $\mathbb{Q}(\sqrt{-p})$ és parell si $p \equiv 1(mod\ 4)$.**

**20. Sigui $k$ un cos de $char(k) \neq 2$. Sigui $d(X) \in k[X]$ un polinomi lliure de quadrats.**

- **Proveu que $B := k[x][\sqrt{-d(X)}]$ és un domini de Dedekind.**
- **Si $d(x) = \prod_{i=1}^{N}(X - b_i)$ amb $b_i \in k$ amb $N$ senar o que $-1$ no és un quadrat en el cos $k$. Demostreu que $C\ell(B)$ conté un subgrup isomorf a $(\mathbb{Z}/(2))^{N-1}$.**
- **Si $k$ finit $C\ell(B)$ és un grup finit, però no es veritat per $k$ no finit. Doneu un exemple per tal que $C\ell(B)$ no és finit.**
- **Si $d(X) = \alpha X^6 + 3X^4 + 3X^2 + 1$ amb $\alpha$ convenientment triat, demostreu que llavors $C\ell(B)$ conté un element d'ordre 3.**

**21. Calculeu la ramificació de l'extensió $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ amb $d$ enter lliure de quadrats.**

**22. Calculeu la ramificació de l'extensió $\mathbb{Q}(e^{2\pi i/p})/\mathbb{Q}$ amb $p$ primer. Quina extensió $L := \mathbb{Q}(\sqrt{d})$ quadràtica es troba dins de $\mathbb{Q}(e^{2\pi i/p})$?**

**23. Sigui $L/K$ una extensió finita i separable. Sigui $A$ un domini de Dedekind amb cos de fraccions $K$, i $B$ la clausura entera de $A$ en $L$. Sigui $P$ un ideal maximal de $A$. Construïu $L/K$ de grau 3 i $P$ complint $PB = Q(Q')^2$ amb $Q, Q'$ ideals maximals de $B$.**

**24. Sigui $A$ un domini de Dedekind amb cos de fraccions $K$. Sigui $P$ un ideal maximal de $A$, i sigui $f(Y) \in A[X]$ $P$-Eisenstein. Sigui $\beta$ una arrel de $f(Y)$ i escrivim $L = K(\beta)$. Sigui $B$ la clausura de $A$ en $L$. Proveu que $PB = M^{deg(f)}$ amb $M$ ideal maximal de $B$.**

**25. Sigui $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ i $K = \mathbb{Q}(\sqrt{-5})$. Proveu que l'extensió entre els anells d'enters de $L$ i $K$ és no-ramificada.**

**26. Denotem ara $K = \mathbb{Q}(\sqrt{-14})$ i $L = K(\gamma)$ amb $\gamma = \sqrt{2\sqrt{2} - 1}$. Demostreu que cap primer de l'anell d'enters de $K$ ramifica en l'anell d'enters de $L$.**

**27. Sigui $f(X,Y) \in \mathbb{Z}[X,Y]$ un polinomi irreductible no-constant. Sigui $p$ un primer i denotem per $f_p(X,Y) \in \mathbb{F}_p[X,Y]$ la reducció modul $p$ del polinomi. Tenim una aplicació natural $\varphi_p : \mathbb{Z}[X,Y]/(f) \to \mathbb{F}_p[X,Y]/(f_p)$ que indueix una aplicació entre ideals maximals. Demostreu que els ideals maximals de $\mathbb{Z}[X,Y]/(f)$ estan amb bijecció amb la unió disjunta variant $p$ dels ideals maximals de $\mathbb{F}_p[X,Y]/(f_p)$ via el morfisme $\varphi_p$.**

## 4.11 Tema 3. Exercicis de treball comú.

**1. Sigui $A$ un domini Dedekind, i $K = Quot(A)$. Considera per $IdEnter(A)$ el monoid amb la multiplicació d'ideals generat pels ideals maximals de $A$, i considerem $(1) = A$ com element neutre en $IdEnter(A)$.**

**(a) Definim $IdFrac(A)$ pels ideals fraccionaris de $A$, on $J \in IdFrac(A)$ si $J \subset K$ és un $A$-mòdul i existeix $\beta \in A$ on $\beta \cdot J \subset A$ (en particular $\beta J$ és un ideal de $A$). Proveu primer que tot $A$-submòdul de $K$ ($M \subset K$) finit generat és un ideal fraccionari de $A$. Considerem $IdFrac(A)$ amb l'operació multiplicació de $A$-mòduls, veieu que dóna a $IdFrac(A)$ una estructura de monoïd.**

**Tot seguit demostreu que si $I \in IdFrac(A)$ llavors $I(A : I) = A$ on**

$$(I : A) = \{k \in K | kI \subset A\}.$$

**i proveu que $IdFrac(A)$ és un grup abelià lliure generat pels ideals primers de $A$ i tot ideal fraccionari de $A$ és un $A$-mòdul finit generat.**

**(b) Diem que un ideal fraccionari és principal si es de la forma $\alpha A$ per cert $\alpha \in K^*$. Diem dos ideals fraccionaris $I_1 \equiv I_2$ si $I_1 I_2^{-1}$ és un ideal fraccionari principal dins $IdFrac(A)$. Veieu $\equiv$ és una relació d'equivalència i $IdFrac(A)/\equiv$ és un grup abelià.**

**(c) Demostreu un isomorfisme de grups entre $C\ell(A)$ i $IdFrac(A)/\equiv$.**

**(d) Demostreu que tot ideal en un domini de Dedekind $A$ està generat com a molt per 2 elements.**

**2. Considera $K$ un cos algebraicament tancat de $car(K) > d$ i $L = K(X)[y]/f(y,X)$ on $f(Y,X) = Y^2 - f(X)$ amb $f(X) \in K[X]$ un polinomi mònic de grau $d \geq 3$ sense arrels repetides. Considereu $K[X]$ l'anell de polinomis en la variable $X$, i sigui $B = K[X,y]/f(y,X)$.**

**(a) Observeu que $L$ és un cos i proveu que $B$ és la clausura entera de $K[X]$ en $L$, en particular justifiqueu que $B$ és un domini de Dedekind.**

**(b) Trobeu la descomposició en ideals primers en $B$ de $(X-\alpha)B$ amb $\alpha \in K$. Explicitant quins ideals $(X-\alpha)K[X]$ ramifiquen en $B$ i quins espliten completament en $B$.**

(c) **Trobeu $B'$ la clausura entera de $K[1/X]$ en el cos $L$ i estudieu la descomposició dels ideals primers de $K[1/X]$ en $B'$.**

(d) **Si $K$ no és algebraicament tancat, imposem que $f(X)$ factoritza en $K[X]$ en polinomis de grau 1 coprimers dos a dos. Quins arguments dels apartats a),b)c) anteriors són vàlids encara en aquesta situació?**

3. **Sigui $A$ un domini integrament tancat, i $K = Quot(A)$. Sigui $L/K$ una extensió finita i separable de cossos i escrivim $L = K(\alpha)$. Sigui $B$ la clausura entera de $A$ en $L$, on sempre podem pensar $\alpha \in B$. Considera $Irr(\alpha, K)[]X] \in A[X]$ observa que $B \subseteq f'(\alpha)'A[\alpha]$.**

   (a) **(Lemma de Nakayama) Si $B'$ és un subanell de $B$ contenint $A$ i satisfent les dues condicions següents:**

   - **$L$ és generat per $B'$ com a $K$-espai vectorial,**
   - **$B' + \mathfrak{m}B = B$ per a tot ideal primer no zero $\mathfrak{m}$ de $A$.**

   **Demostreu llavors que $B' = B$.**

   (b) **Suposem $Irr(\alpha, K)[X] = \sum_{i=0}^{d} a_i X^i \in A[X]$ on existeix un ideal primer $\mathfrak{m}$ de $A$ on $a_i \in \mathfrak{m}$ per $i = 0, \ldots, a_{d-1}$, $a_d = 1$ i $a_0 \notin \mathfrak{m}^2$ (diem $Irr(\alpha, K)[X]$ es un polinomi $\mathfrak{m}$-Eisenstein). Demostreu llavors $\mathfrak{m}B$ té en la seva factorització en ideals primers en $B$ un únic ideal maximal, i es té $A[\alpha] + \mathfrak{m}B = B$.**

   (c) **Sigui $B'$ un subanell de $B$ contenint $A$, on $B'$ genera $L$ com $K$-espai vectorial i $Irr(\alpha, K)[X]$ is $\mathfrak{m}$-Eisenstein per un ideal maximal de $A$ amb $\alpha \in B' \subset B$ i $L = K(\alpha)$. Demostreu en aquesta situació que $B' = B$.**

   (d) **Proveu que $\mathbb{Z}[\sqrt[3]{3}]$ és integrament tancat.**

4. **Sigui $K = \mathbb{Q}[\sqrt{m}]$ amb $m$ un enter lliure de quadrats.**

   (a) **Trobeu $\mathcal{O}_K$ l'anell d'enters de $K$, i expliciteu per cada primer $p$ com és $p\mathcal{O}_K$ com ideals primers de $K$, és dir si és el producte d'un ideal primer, de dos ideals primers diferents o bé dos ideals primers però iguals.**

   (b) **Suposa que $m \equiv 2, 3 (mod\ 4)$ fixat i suposem $C\ell(\mathbb{Q}[\sqrt{m}]) = 1$ en aquest apartat. Quines condicions hem d'imposar en $\mathbb{Z}[\sqrt{m}]$ i l'ideal primer $p\mathbb{Z}$ senar, per a que existeixen $x$,$y$ enters on $x^2 - my^2 = (x - \sqrt{m}y)(x + \sqrt{m}y) = p$?**

   (c) **(*) existeixen $x, y \in \mathbb{Z}$ complint $p = x^2 + 6y^2$ amb $p$ primer, si i només si $p \equiv 1, 7$ mòdul 24.**

   (d) **De teoria de Galois sabem que hi ha exactament un cos $K$ (per cert $m$) entre $\mathbb{Q}[e^{2\pi i/p}]$ i $\mathbb{Q}$ on $p$ és un primer senar. Pensant en la ramificació d'ideals entre $\mathbb{Q}[e^{2\pi i/p}]/\mathbb{Q}$ i que $K$ és un cos intermig podeu dir alguna cosa respecte qui pot ser aquest valor de $m$?**

### 4.11.1 Alguns resultats a conèixer

**Per fer els exercicis anteriors podeu usar sense demostrar els següents resultats, en cas d'utilitat.**

**Sempre en el que segueix $A$ és un domini de Dedekind, amb $K = Quot(A)$ i $L/K$ una extensió finita separable de cossos on $B$ la clausura entera de $A$ en $L$. Podem pensar $L$ com $K$-espai vectorial i donat $\beta \in L$ tenim $\beta : L \to L$ on $\beta(l) := \beta l$ és un morfisme de $K$-espai vectorials, i es defineix la $Tr_{L/K}(\beta)$ la traça de la matriu associada a l'aplicació $K$-lineal $\beta$ en una $K$-base fixada de $L$ (on és pot demostrar que aquest valor no depén de la $K$-base triada). És defineix l'ideal fraccionari de $L$:**

$$\mathcal{D}(B/A)^{-1} := \{\alpha \in L | Tr_{L/K}(\alpha B) \subseteq A\}$$

**i es demostra que $B \subseteq \mathcal{D}(B/A)^{-1}$ i la different correspon a l'ideal de $B$:**

$$\mathcal{D}(B/A) = \{b \in B | b \cdot \mathcal{D}(B/A)^{-1} \subseteq B\}.$$

**Fet 4.11.1.** *Un ideal primer $\mathfrak{m}$ de $B$ és ramificat sobre $A$ si i només si $\mathfrak{m} | \mathcal{D}(B/A)$.*

**Fet 4.11.2.** *Suposa $\alpha \in B$ i $B = A[\alpha]$ Si $Irr(\alpha, K)[X] \in A[X]$ llavors*

$$\mathcal{D}(B/A) = (f'(\alpha))$$

*com ideals de $B$ on $f'$ denota la derivada de $f$.*

[2]

**Fet 4.11.3.** *Si $L = K(\alpha)$ i $Irr(\alpha, K)[X] \in A[X]$. Llavors*

$$\mathcal{D}(B/A)^{-1} \subseteq f'(\alpha)^{-1} A[\alpha].$$

*En particular, tenim $f'(\alpha)B \subset \mathcal{D}(B/A)$, i un ideal primer $\mathfrak{m}$ de $B$ on $f'(\alpha) \notin \mathfrak{m}$ és no-ramificat en $L$.*

**Fet 4.11.4.** *Sigui $\alpha \in B$ i $L = K(\alpha)$. I sigui $f(X) = Irr(\alpha, K)[X] \in A[X]$. Sigui $\mathfrak{p}$ un ideal primer de $A$ no-zero i pensem*

$$\mathfrak{p}B = \beta_1^{e_1} \dots \beta_s^{e_s}$$

*amb $\beta_i$ ideals primers de $B$ diferents, i $e_j$ naturals $\geq 1$.*

*Suposem a més que $f'(\alpha) \notin \beta_i$, d'on s'obté que $e_i = 1$.*

*Amb aquestes hipòtesis, tenim:*

1. *Factoritzem $f(x)$ modul $\mathfrak{p}$ en $A/\mathfrak{p}[X]$ en producte de polinomis irreductibles en $A/\mathfrak{p}[X] =: \kappa[X]$:*

   $$f(X) = f_1(X) \cdot \dots \cdot f_h(X) \in \kappa[X].$$

   *Llavors, $s = h$, a més per a cada $1 \leq i \leq g$ (fent una reordenació si cal) tenim $\beta_i = \mathfrak{p}B + \tilde{f}_i(\alpha)B$ on $\tilde{f}_i \in A[X]$ monic on $\tilde{f}_i = f_i (mod\ \mathfrak{p})$. A més per cada $i$ entre 1 i $g$ tenim:*

   $$\kappa[X]/(f_i(X)) \cong B/\beta_i;\ X \mapsto \alpha\ mod\ \beta_i$$

   *i per tant el grau residual de $\beta_i$ sobre $\mathfrak{p}$ és igual al grau del polinomi $f_i(X) \in \kappa[X]$.*

[2] No sempre la clausura entera de $A$ en $L$ és de la forma $A[\alpha]$ on $L = K(\alpha)$

2. *Suposem que $L/K$ és una extensió Galois, llavors tots els graus dels $f_i$'s són iguals i en particular:* $\mathfrak{p}$ *descomposa totalment en $L$ si i només si $f$ té una arrel en $\kappa[X]$, si i només si $f(X)$ factoritza en polinomis de grau 1 en $\kappa[X]$.*

# Capítol 5

# Una invitació a Geometria Aritmètica, presentant el Teorema de Faltings

**En aquest capítol sol farem un overview de geometría aritmètica, per aprofundir-hi recomanem el llibre [Lorenzini] de la bibliografia per exemple.**

## 5.1 Anells locals dins cossos

**Definició 5.1.1.** *Sigui $L$ un cos. Una valoració de $L$ és una aplicació $v : L^* \to \Gamma$ on $\Gamma$ és un grup abelià totalment ordenat, complint les propietats següents:*

1. *$v(xy) = v(x) + v(y)$ per a tot $x, y \in L^*$*
2. *$v(x + y) \geq min(v(x), v(y))$.*

*S'extén a $L$ definint $v(0) := +\infty$.*

*En el cas que $v(L^*) \subset (\mathbb{Z}, +)$ diem que vés una valoració discreta de $L$.*

**Exemple 5.1.2.** *Sigui $A$ un domini de Dedekind, i escrivim $K = Q(A)$. Sigui $\mathfrak{p}$ un ideal primer no zero de $A$. Dona $a \in A$ tenim que podem escriure com producte ideals primers de $A$*

$$(a) = \mathfrak{p}^{n_a} \beta_1^{n_{1,a}} \dots \beta_k^{n_{k,a}}$$

*on $n_a > 0$ si $a \in \mathfrak{p}$, i definim l'aplicació*

$$v_\mathfrak{p} : A^* \to \mathbb{Z}$$

$$a \mapsto n_a$$

*i l'extenem a $K^*$ via $x = \frac{a}{b}$ amb $a, b \in A$ i definim $v_\mathfrak{p}(x) := v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$.*

*És exercici al lector que $v_\mathfrak{p}$ és una valoració discreta del cos $K$. Fixe-mos que aquesta valoració $v_\mathfrak{p}$ ens dóna un valor absolut natural si $A/\mathfrak{p}$ és un cos finit via:*

$$||_\mathfrak{p} : K \to \mathbb{R}_{>0}$$

$$x \mapsto |x|_{\mathfrak{p}} := |A/\mathfrak{p}|^{-v_{\mathfrak{p}}(x)}.$$

*Considerem ara $L/K$ una extensió finita i separable de $K$, i diem $B$ la clausura entera de $A$ en el cos $L$, on $B$ és Dedekind i per cada ideal prime $\mathfrak{f}$ de $B$ tenim definida una valoració i un valor absolut no arquimedia. Fent $\mathfrak{f} \cap A = \mathfrak{p}$ per cert ideal $\mathfrak{p}$ de $A$, tenim llavors*

$$\mathfrak{p}B = \mathfrak{f}^{e_{\mathfrak{f}/\mathfrak{p}}} \cdot I$$

*amb $I$ ideal coprimer amb $\mathfrak{f}$ i es pot demostrar fàcilment:*

$$v_{\mathfrak{f}}(x) = e_{\mathfrak{f}/\mathfrak{p}} v_{\mathfrak{p}}(x)$$

*per a $x \in K^*$.*

*Referent als valors absoluts no arquimedians, observeu que podem definir*

$$||x||_{\mathfrak{f}} := |B/\mathfrak{f}|^{-v_{\mathfrak{f}}(x)}$$

*per a $x \in L$, però si $x \in K$ aquest valor absolut no coincideix amb $|x|_{\mathfrak{p}}$, per tant que coincideixi en restringir cossos inferiors, definim el valor absolut en $B$ associat a $v_{\mathfrak{f}}$ per:*

$$|x|_{\mathfrak{f}} := |A/(\mathfrak{f} \cap A)|^{-[B/\mathfrak{f}:A/\mathfrak{p}]v_{\mathfrak{f}}(x)}$$

*on recordem que $[B/\mathfrak{f} : A/\mathfrak{p}] = f_{\mathfrak{f}/\mathfrak{p}}$ és el grau residual de $\mathfrak{f}|\mathfrak{p}$ en l'extensió $L/K$.*

**Introduim la següent notació per a una valoració d'un cos $K$ via**

$$v : K^* \to (\Gamma, +, \geq)$$

$$\mathcal{O}_v := \{\alpha \in K^* | v(\alpha) \geq 0\} \cup \{0\}$$

$$\mathcal{M}_v := \{\alpha \in K^* | v(\alpha) > 0\} \cup \{0\}.$$

**Lema 5.1.3.** *Tenim que $\mathcal{O}_v$ és un anell local amb ideal maximal $\mathcal{M}_v$.*

*Demostració.* Per la propietat de valoracions i subconjunt d'un cos, clarament $\mathcal{O}_v$ és un domini i $\mathcal{M}_v$ és un ideal de $\mathcal{O}_v$.

Per veure és local, és suficient veure que $\mathcal{M}_v$ és ideal maximal i tot ideal $I$ de $\mathcal{O}_v$ no el total està dins de $\mathcal{M}_v$.

És suficient demostrar que per a tot $\beta \in \mathcal{O}_v \setminus \mathcal{M}_v$ és una unitat de $\mathcal{O}_v$. Observem que $v(\beta) = 0$ com $\beta \in K^*$ té invers en $K^*$ diem-li $\beta^{-1}$ però observem que

$$0 = v(1) = v(\beta \cdot \beta^{-1}) = v(\beta) + v(\beta^{-1})$$

per tant $v(\beta^{-1}) = 0$ on $\beta^{-1} \in \mathcal{O}_v$ on $\beta$ una unitat de $\mathcal{O}_v$. □

**Proposició 5.1.4.** *Sigui $v : K^* \hookrightarrow (\mathbb{Z}, +, \geq)$ una valoració discreta del cos $K$. Llavors $\mathcal{O}_v$ és un domini d'ideals principals. A més, l'aplicació:*

$$\varphi : v \mapsto \mathcal{O}_v$$

*dóna una bijecció entre valoracions discretes de $K$ amb $A$ dominis locals d'ideals principals continguts en el cos $K$ amb $Q(A) = K$.*

*Demostració.* Provem que $\mathcal{O}_v$ és un DIP, ja sabem que és local. Triem $\pi \in \mathcal{O}_v$ amb $v(\pi) = 1$, i observem que de la demostració lema anterior sabem que $u \in \mathcal{O}_v^*$ si i només si $v(u) = 0$.

Si $\alpha \in \mathcal{M}_v$ (no és una unitat) tenim $v(\alpha) = k > 0$, i observem $v(\alpha\pi^{-k}) = 0$, doncs $\alpha\pi^{-k} \in \mathcal{O}_v^*$ una unitat, per tant tot element s'escriu com $\pi^k \cdot unitat$ per cert natural $k$ i $\mathcal{M}_v = (\pi)$ principal, i per un exercici llista del tema 3 obtenim que $\mathcal{O}_v$ és DIP.

Veiem ara $\varphi$ dóna una bijecció.

*$\varphi$ és injectiva*:

Si $\mathcal{O}_{v_1} = \mathcal{O}_{v_2} \subseteq K$ DIP i anells locals, tenim que l'ideal maximal principal coincideix $\mathfrak{M}_{v_1} = \mathfrak{M}_{v_2} = \pi\mathcal{O}_{v_i}$ per a $i = 1, 2$, en particular $v_i(\pi) = 1$ i tot element d'aquells anells locals s'escriu com $unitat \cdot \pi^k$, per tant les dues valoracions discretes eren la mateixa.

*$\varphi$ és exhaustiva*:

Sigui $A \subset K$ un DIP dins un cos on $Q(A) = K$ amb únic ideal maxima $\mathfrak{m} = \pi A$ on $\pi \in A \subseteq K$, tot $a \in A$ s'escriu per $a = u\pi^k$ amb $k$ natural i $u$ una unitat de $A$, per tant per $x \in K^*$ s'escriu com $x = u'\pi^k$ amb $k$ enter i $u'$ una unitat de $A$ i clarament definint $v : K^* \to \mathbb{Z}$ via $v(x) = k$ defineix una valoració discreta de $K$ on $\mathcal{O}_v = A$. □

**Tenim el següent resultat que sol demostrarem parcialment en aquest curs.**

**Fet 5.1.5.** *Sigui $A$ un domini amb $dim_{Krull}(A) = 1$, i escrivim $K = Q(A)$. Podem definirm una aplicació $\Phi$ entre valoracions exhaustives discretes $v : K^* \to \mathbb{Z}$ amb $v(A) \geq 0$ e ideals maximals, definida per*

$$\Phi(v) := \mathcal{M}_v \cap A.$$

*Si a més $A$ és un domini de Dedekind llavors $\Phi$ és una bijecció.*

*Demostració.* Veiem tant sols que $\Phi$ està ben definida.

Com $v(A) \geq 0$ tenim $A \subseteq \mathcal{O}_v$ i $\mathfrak{m} = \mathcal{M}_v \cap A$ és un ideal primer de $A$ i com tot $u \in A \setminus \mathfrak{m}$ és una unitat en $\mathcal{O}_v$ per propietats de localització obtenim que

$$A_{(\mathfrak{m})} \subseteq \mathcal{O}_v$$

ara com la $dim_{Krull}(A) = 1$ tenim si $\mathfrak{m} = 0$ $K \subseteq \mathcal{O}_v$ cosa que no pot ser, per tant $\mathfrak{m}$ és ideal maximal i $\Phi$ definida. □

## 5.2 Corbes algebraiques completes no-singulars

**Definició 5.2.1.** *Donada una valoració d'un cos $L$, $v : L^* \to (\Gamma, +, \geq)$ i sigui $k \subset L$ un subcos de $L$. Diem que $v$ és trivial sobre el cos $k$ si $v|_{k^*} = 0$.*

*Denotem per $\mathcal{V}(L/k)$ el conjunt de valoracions discretes trivials en $k$.*

**Definició 5.2.2.** *Sigui $k$ un cos. Una corba completa no-singular $X/k$ sobre el cos $k$ és una parella $(X, k(X)/k)$ on $k(X)/k$ és un cos de trascendència 1 sobre $k$ i $X$ s'identifica amb $\mathcal{V}(k(X)/k)$.*

**Lema 5.2.3.** *Sigui $t$ un element trascendent sobre $k$, llavors $\mathcal{V}(k(t)/k)$ corresponen a les valoracions donats pels ideals primers de $k[t]$ amb la valoració que correspon a l'ideal primer $(1/t)$ en el domini $k[1/t]$.*

*Demostració.* [esboç] Considerem $v : k(t)^* \to \mathbb{Z}$ epi, clarament existeix un polinomi en $t$: $h \in k[t]$ on $v(h) \neq 0$ de ser $v$ epi. Si $v(h) > 0$ llavors existeix un factor $f$ irreductible en $k[t]$ de $h$ i $v = v_f$ definit de ser $k[t]$ un Domini de Dedekind. Suposem que $v(h) < 0$, llavors es pot veure que $v = v_\infty$ on $v_\infty(polinomi)$ és igual a - el grau en $t$ del polinomi. □

**Definició 5.2.4.** *Sigui $X/k$ una corba algebraica completa no-singular sobre el cos $k$ que correspon a la parella $(k(X)/k, \mathcal{V}(k(X)/k))$.*

*Un element $P \in \mathcal{V}(k(X)/k)$ s'anomena un punt de $X$, i $k(X)$ el cos racional de les funcions racionals de $X$. A cada punt $P$, tenim associat l'anell local $\mathcal{O}_P$ amb ideal maximal $\mathcal{M}_P$. Diem $\mathcal{O}_P$ l'anell de les funcions racionals en $P$, i $f \in \mathcal{O}_P$ s'anomena funció de $X$ definida en el punt $P$. Una funció $\alpha \in \mathcal{O}_P$ s'anul.la en $P$ o té un zero en $P$ si $\alpha \in \mathcal{M}_P$. Les funcions $\alpha \in k(X) \setminus \mathcal{O}_P$ es diuen tenen un pol en $P$, l'enter $|v_P(\alpha)|$ és l'ordre del pol.*

*Donat $\alpha \in k(X)$, el domini d'$\alpha$ és el conjunt de punts $P \in X$ on $v_P(\alpha) \geq 0$.*

*Si $U \subset X$ (identificant $X$ amb $\mathcal{V}(k(X)/k)$), escriurem $\mathcal{O}_X(U) := \cap_{P \in U} \mathcal{O}_P$ anell de les funcions definides en tot $U$. I posem a $X$ la topologia de Zariski, on $C \subseteq X$ és tancat si i només si $C = \emptyset$, $X$, o un número finit de punts $P$ de $X$.*

**Exemple 5.2.5.** *Fixem-nos que $k(X)[y]/(f(X,y))$ on $f(X,Y) \in k[X,Y]$ un polinomi irreductible en $k(X)[Y]$ és un cos de trascendència 1 sobre $k$, i per tant $(k(X)[y]/(f(X,y)), \mathcal{V}(k(X)[y]/(f(X,y)))/k)$ és una corba algebraica completa sobre $k$ que usualment també diem la corba algebraica associada a $f(X,Y) = 0$. No obstant per controlar millor $\mathcal{V}(k(X)[y]/(f(X,y)))$ demanem que $f(X,Y)$ sigui no-singular llavors tenim que $B = k[X][y]/(f(X,y))$ és un domini de Dedekind i els elements de $\mathcal{V}(k(X)[y]/(f(X,y)))/k)$ corresponen a les valoracions dels ideals maximals de $B$ on cal afegir les valoracions d'ideals primers que surten en fer $(1/X)C$ on $C$ és la clausura entera de $K[1/X]$ en el cos $L = k(X)[y]/(f(X,y))$, que són un número finit de punts.*

**Definició 5.2.6.** *Donada $X$ una corba algebraica completa no-singular, un conjunt obert $U$ de $X$ s'anomena afí si $\mathcal{O}_X(U)$ és una $k$-àlgebra finit generada (és dir isomorfa a $k[X_1, \ldots, X_N]/I$ amb $I$ un ideal) i Dedekind i a més l'aplicació:*

$$U \to Spec_{Max}(\mathcal{O}_X(U))$$

$$P \mapsto \mathcal{M}_{v_P} \cap \mathcal{O}_X(U)$$

*és una bijecció.*

**Lema 5.2.7.** *Sigui $X/k$ una corba no-singular completa, i sigui $x \in k(X) \setminus k$. Denotem per $U$ el domini de $x$ i per $U'$ el domini de $x^{-1}$. Llavors $X = U \cup U'$.*

*Demostració.* Sigui $P \in X$, considerem ideal local principal $\mathcal{O}_P$ on $Q(\mathcal{O}_P) = k(X)$ tenim que $v_P(x) \geq 0$ o bé $v_P(x^{-1}) \geq 0$, per tant $P \in U$ o bé $P \in U'$ respectivament. □

**Teorema 5.2.8.** *Sigui $X/k$ una corba no-singular completa sobre $k$. Triem $x \in k(X)/k$ on $k(X)/k(x)$ una extensió finita separable. Sigui $U$ el domini de $x \in X$. Llavors $U$ és un subconjunt afí de $X$, $\mathcal{O}_X(U)$ és la clausura entera de $k[x]$ en $k(X)$. El complement de $U$ en $X$ son els punts $P$ on $k[1/x]_{(1/x)} \subset \mathcal{O}_P$.*

*Demostració.* [esboç] Per a $P \in U$, tenim llavors que $x \in \mathcal{O}_P$, d'on tenim $k[x] \subseteq \mathcal{O}_P$. Observem que $x$ no és algebraic sobre $k$ ja que $k(X)/k(x)$ és una extensió finita. Sigui $B$ la clausura entera de $k[x]$ en $L = k(X)$. Com $\mathcal{O}_P$ DIP llavors és integrament tancat en $L$ i per tant $B \subseteq \mathcal{O}_P$, per a tot $P \in U$. Fixem-nos de ser $L/k(x)$ finita separable, tenim que $B$ és un $k[x]$-mòdul finit generat, i tenim una bijecció entre ideals maximals de $B$ i valoracions discretes amb $v(B) \geq 0$ amb $Q(B) = L$, per tant $\mathcal{O}_X(U) = B$.

Veiem $U$ és obert, prenem $P \in X \setminus U$ per tant $v_P(x^{-1}) > 0$ i per tant $k[1/x]_{(1/x)} \subseteq \mathcal{O}_P$ i la clausura entera de $k[1/x]_{(1/x)}$ en $L$ sol té un número finit d'ideals maximals, per tant sol un número finit de valoracions discretes. □

**Corol·lari 5.2.9.** *Donada una corba $X/k$ no-singular completa sobre cos $k$, llavors és unió de dos oberts afins.*

## 5.3 Grup de Picard per a $X/k$

**Definició 5.3.1.** *Sigui $B$ un domini Dedekind on $L = Q(B)$. Escrivim $\mathcal{V}(L)$ valoracions discretes no valoració zero. Es defineix el grup de divisors de $B$ al grup abelià lliure generat pels elements de $\mathcal{V}(L)$, és a dir:*

$$Div(B) := \oplus_{v \in \mathcal{V}(L), v(B) \geq 0} \mathbb{Z} x_v.$$

**Fet 5.3.2.** *Donat $B$ un domini de Dedekind, hi ha un epimorfisme de grups:*

$$c\ell : Div(B) \to C\ell(B)$$

$$x_v \mapsto [\mathcal{M}_v \cap B]$$

*i el $ker(c\ell)$ correspon als divisors dels elements $L^*$, corresponent a $div_B(L^*) = \{\sum_{v \in \mathcal{V}(L), v(B) \geq 0} v(f) x_v | f \in L\}$.*[1]

**Definició 5.3.3.** *Sigui $L/k$ una extensió de grau de trascendència 1 i $\mathcal{V}(L/k)$ el conjunt de valoracions discretes no-trivials de $L$ trivials en $k$, i suposem que aquest conjunt és no buit. Es defineix el grup de divisors com el grup abelià lliure generat per aquestes valoracions discretes:*

$$Div(L/k) := \oplus_{v \in \mathcal{V}(L/k)} \mathbb{Z} x_v.$$

*Es defineix $div_L : L^* \to Div^0(L/k) := \{\sum n_v x_v \in Div(L/k) | \sum n_v = 0\}$ via $div_L(f) = \sum_{v \in \mathcal{V}(L/k)} v(f) x_v$ on és pot demostrar que és ben definida $v(f) \neq 0$ per un número finit de valoracions i usualment s'anota $(f)_0 - (f)_\infty$ correspon als zeros menys els pols de la funció $f$.*

*Finalment el grup de Picard de $L/k$ i denotat per $Pic(L/k)$ és el grup abelià $Div(L/k)/div_L(L^*)$.*

**Fet 5.3.4.** *Sigui $L/k$ una extensió de cossos de grau de trascendència 1. Tenim la successió exacta següent:*

$$(1) \to \cap_{v \in \mathcal{V}(L/k)} \mathcal{O}_v^* \to L^* \to^{div_L} Div(L/k) \to^{c\ell} Pic(L/k) \to 0$$

*i quan $L = k(X)$ on $X/k$ corba completa no singular, parlarem de grup de divisors i grup de Picard de la corba $X$ enlloc de l'extensió de cossos $k(X)/k$.*

[1] Observo que es pot demostrar donat $f \in L^*$ sol hi ha un número finit de $v$'s on $v(f) \neq 0$, és a dir un número finit de zeros i pols la funció $f$ on $v$ recorre totes les valoracions discretes de $L$

## 5.4 Una definició (no-geomètrica) del gènere de $X/k$

**Pensem $X/k$ una corba completa no-singular sobre $k$ on pensem $k = \overline{k}$ és un cos algebraicament tancat.**

**Definició 5.4.1.** *Donat $D = \sum_{i=1}^{s} a_i P_i \in Div(X/k)$ on $P_i$ denotem punts de $X/k$, s'anomena que $D$ és efectiu o positiu sempre que $a_i \geq 0$ per a tot $1 \leq i \leq s$.*

*Això permet definir un ordre en $Div(X/k)$ via*

$$D' \geq D \Leftrightarrow D' - D \text{ és un divisor positiu.}$$

**Recordem que si $f \in k(X)^*$ tenim $div_X(f) = \sum_{P_i \in \mathbb{V}(k(X)/k)} v_{P_i}(f) P_i \in Div^0(X/k)$.**

**Podem definir el morfisme grau, $deg : Div(X/k) \to \mathbb{Z}$ via $\sum_i a_i P_i \mapsto \sum_i a_i$ on $ker(deg)$ s'anota $Div^0(X/k)$ i és pot demostrar que $deg(div_X(f)) = 0$ per tot $f \in k(X)^*$.**

**Definició 5.4.2.** *Considerem $D \in Div(X/k)$, llavors definim*

$$H^0(D) := \{f \in k(X)^* | div_X(f) + D \geq 0\}$$

**Observem que $H^0(D)$ és un $k$-espai vectorial perque si $f \in H^0(D)$ tenim $div_X(af) = div_X(f)$ per tot $a \in k$ ja que no aporten ni pols ni zero (recordem que les valoracions són trivials en el cos $k$).**

**Fet 5.4.3.** *Sigui $D \in Div(X/k)$ un divisor effectiu. Lavors*

$$dim_k(H^0(D)) \leq deg(D) + 1.$$

*Demostració.* [esboç] Escrivim $D = a_1 P_1 + \ldots + a_s P_s$ amb $a_i > 0$. Ara si $f \in k(X)$ i $f \in H^0(D)$ i escrivim $div_X(f) = (f)_0 - (f)_\infty$ i com $D + div_X(f) \geq 0$ tenim que els pols de $f$ (corresponent a $(f)_\infty$) han de trobar-se en els $P_i$'s, per tant de ser d'$H^0(D)$ tenim $-a_i \leq v_{P_i}(f) = -k \leq -1$ i pensant que $\mathcal{M}_{P_i} = \pi_i \mathcal{O}_{P_i} \subset \mathcal{O}_{P_i} \subset k(X)$ podem escriure $f$ com una sèrie de Laurent en potències de $\pi_i$ via: $f = \sum_{j=-k}^{-1} b_{i,j,f} \pi_i^j + f'$ on $f' \in \mathcal{O}_{P_i}$ on $b_{i,j,f} \in \mathcal{O}_{P_i}/\mathcal{M}_{P_i} = k$ i extenent-ho per zeros obtenim una tupla

$$(b_{i,-a_i,f}, \ldots, a_{i,-1,f}) \in k^{a_i}$$

fent-ho per a cada $P_i$ on es troba el divisor, podem definir un morfisme:

$$\theta : H^0(D) \to \oplus_{i=1}^{s} (k)^{a_i}$$

$$f \mapsto \oplus_{i=1}^{s} (b_{i,-a_i,f}, \ldots, a_{i,-1,f})$$

que es pot comprovar que és un morfisme de $k$-espais vectorial i clarament $k \subseteq Ker(\theta)$, per tant

$$dim_k(H^0(D)) \leq dim_k(ker(\theta)) + dim_k(Im(\theta)) \leq 1 + deg(D).$$

□

**Definim per $P \in X$ i $D = \sum_{i=1}^{s} a_i P_i \in Div(X/k)$ el $k$-espai vectorial:**

$$\mathcal{L}(D)_P := \{f \in k(X) | v_P(f) \geq -a_P\},$$

**on $a_P = 0$ si $P \notin \{P_1, \ldots, P_s\}$.**

**Denotem per $H$ al $k$-espai vectorial $\oplus_{P \in X}(k(X)/\mathcal{L}(D)_P)$ i definim un morfisme de $k$-espai vectorials següent:**

$$\varphi_D : k(X) \to H$$

$$f \mapsto \oplus_{P \in X}(f \ mod \ \mathcal{L}(D)_P).$$

**És fàcil demostrar que $ker(\varphi_D) = H^0(D)$ i definim**

$$H^1(D) = coker(\varphi_D) = H/Im(\varphi_D).$$

**Fet 5.4.4.** *Donat $D \in Div(X/k)$ tenim que $H^1(D)$ és un $k$-espai vectorial de dimensió finita.*

**Definició 5.4.5.** *Donada $X/k$ una corba completa no-singular, amb $k = \overline{k}$. Definim el gènere de $X/k$ i s'anota $g(X)$ a la dimensió com $k$-espai vectorial de $H^1(0)$ on el divisor $0 \in Div(X/k)$ correspon a $0 = \sum_{P \in \mathcal{V}(k(X)/k)} 0 \cdot P$.*

**Observació 5.4.6.** *Si $k = \mathbb{C}$ i $k(X) = k(X)[y]/(f(X,y))$ on $f(X,y) \in k[X,Y]$ un polinomi irreductible, llavors els punts de $(\alpha, \beta) \in \mathbb{C}^2$ complint $f(\alpha, \beta) = 0$, són una superfície de Riemann amb $g(X)$-forats, en particular si el gènere és zero correspon a una esfera, si és 1 a un tor complex.*

**Fet 5.4.7** (Teorema de Rieman)**.** *Sigui $X/k$ una corba completa no-singular sobre $k = \overline{k}$, i sigui $D \in Div(X/k)$ amb $D$ efectiu. Llavors el valor enter*

$$dim_k H^0(D) - dim_k H^1(D) - deg(D)$$

*és independent del divisor efectiu $D$. Més concretament es compleix:*

$$dim_k H^0(D) = deg(D) + 1 - g(X) + dim_k H^1(D).$$

*Si $deg(D) \geq 2g(X) + 1$ llavors $dim_k H^0(D) = deg(D) + 1 - g(X)$.*

## 5.5 El Teorema de Faltings, idees heurístiques per a trobar tots els punts

.

**Sigui $X/k$ una corba no-singular completa sobre un cos $k$ on $k$ no necessariament algebraicament tancat.**

**I suposem que $k(X) \cap \overline{k} = k$. Per aquesta secció pensarem que $k(X) = k(X)[y]/(f(y,X))$ on $f(X,Y) \in k[X,Y]$ és un polinomi irreductible en $\overline{k}[X,Y]$, i suposem a més que $f(X,Y)$ és no singular, veieu-ne la definició en el Tema 3 dels apunts.**

**Definim llavors $C_f(L) := \{(\alpha, \beta) \in L^2 | f(\alpha, \beta) = 0\}$ amb $L$ un cos extensió de $k$ i dins la clausura algebraica de $k$: $\overline{k}$.**

**Considerem l'extensió d'escalar a $\overline{k}$ de la corba $X/k$ donat per $\overline{k}(X) := \overline{k}(X)[y]/f(y,X)$ definint una corba no-singular completa sobre $\overline{k}$ que denotem per $X/k \otimes_k \overline{k}$.**

**En els Temes 1 i 2 del curs hem vist que si $g(X/k \otimes_k \overline{k}) = 0$ llavors si $C_f(L) \neq \emptyset$ llavors hi ha una infinitut de punts i es poden parametritzar aquests punts.**

**En el tema 3 del curs hem descrit que si $g(X/k \otimes_k \overline{k}) = 1$ amb $k = \mathbb{Q}$ (o una extensió finita de $\mathbb{Q}$) i $C_f(L)$ té almenys un punt i $L$ una extensió finita de $\mathbb{Q}$ llavors $C_f(L)$ té estructura de grup abelià finit generat i potser finit o no, i dependrà fortament del polinomi $f(X,Y)$.**

**Fet 5.5.1** (Gerd Faltings, 1983). *Sigui $k$ una extensió finita dels racionals, i $X/k$ una corba algebraica sobre $k$ i suposem $g(X/k \otimes_k \overline{k}) \geq 2$ i per simplificar restringim-nos a $k(X) = k(X)[y]/f(X,y)$ amb $f(X,Y) \in k[X,Y]$ irreductible en $\overline{k}[X,Y]$ i no-singular. Llavors*

$$|C_f(L)| < \infty$$

*on $L$ és una extensió finita i fixada de $k$.*

**Per tant per gènere almenys 2, sol podem esperar de trobar un número finit de punts definits en un cos fixat (extensió finita dels racionals) que satisfacin una equació en 2 variables $f(X,Y) = 0$. Com trobar aquestes possible conjunt finit de solucions en un cos de nombres?**

**Heurísticament Magma o SageMath permet calcular els possibles punts solucions, la dificultat radica a demostrar teòricament que aquests punts efectivament son tots, actualment hi ha metodologies basades en fer el teorema de Faltings efectiu, anomenats mètode de Chabouty i derivats, però no sempre és pot concloure teoricament.**

```
P<x,y,z>:=ProjectiveSpace(Rationals(),2);
f:=x^(37)+y^(37)-z^(37);
C:=Curve(P,f);
Genus(C);
RationalPoints(C:Bound:=1000);
```

**i ens dona:**

```
630
{@ (0 : 1 : 1), (1 : 0 : 1), (-1 : 1 : 0) @}
```

**Fixem-nos que introduïm amb Magma aquest codi, introduim la corba $f(x,y)$ sobre els racionals en forma projectiva $f(x,y,z)$ on el grau de cada monomi és el mateix i calculem els punts projectius de la projectivització de $f(x,y)$ via acotant 'per 1000 (una altura de punts) busca els punts racionals. Fixem-nos que el gènere és 630 i la corba Fermat amb $p = 37$, no podem usar el resultat de Kummer ja que és un primer irregular. Fixeu-vos que ens dóna els punts els esperats per l'equació de Fermat amb $p = 37$.**

**Heurísticament aquest codi per $f$ arbitrari amb gènere $\geq 2$ ens donaran tots els punts racionals de la corba $C_f(\mathbb{Q})$, però demostrar que el que ens dóna el programa Magma són exactament tots és molt difícil.**

# Appendix A

# Ideals primers, Localitació d'un domini versus anells de valoració

**Sigui $A$ un domini qualsevol i $K$ el cos de fraccions de l'anell $A$. Denotem per $Spec(A) := \{ideals\ primers\ de\ A\}$, pensem $(0) \in Spec(A)$ de ser $A$ domini.**

**Definició A.0.1.** *L'altura d'un ideal primer $\mathfrak{p}$ is el suprem de tots els enters $n$ on hi ha una cadena*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

*d'ideals primers de $A$. La dimensió de Krull de l'anell $A$ és el suprem de totes les altures de tots els ideals primers.*

**Exemple A.0.2.** *La dimensió de Krull de $\mathbb{Z}$ o de $K[X]$ amb $K$ un cos és 1. La dimensió de Krull de $\mathbb{Z}[X]$ és com a mínim 2 ja que tenim la cadena,*

$$(0) \subset (p) \subset (p, X).$$

*La dimensió de Krull d'un cos és zero.*

**Hi ha el següent resultat útil pel càlcul de dimensió de Krull,**

**Teorema A.0.3.** *Sigui $K$ un cos, i $B$ un domini que és una $K$-algebra finitament generada, llavors:*

1. *la dimensió de Krull de $B$ és igual al grau de trascendencia dels cos de fraccions de $B$, $Quot(B)$ sobre $K$,*
2. *per cada ideal $\mathfrak{p} \in Spec(B)$ es té:*

$$altura(\mathfrak{p}) + dim_{Krull} B/\mathfrak{p} = dim_{Krull} B.$$

**Definició A.0.4.** *Considera $S$ un conjunt multiplicativament tancat de $A$ amb $1 \in S$. Definim*

$$S^{-1}A := A \times S/\sim$$

*on $(a, s) \sim (b, t)$ si i només si $(at - bs) = 0$. $S^{-1}A$ té estructura d'anell i compleix la propietat universal...*

**Quant $S = A \setminus \mathfrak{p}$ amb $\mathfrak{p} \in Spec(A)$ denotem per $S^{-1}A$ per $A_{\mathfrak{p}}$, quant $S = A - \{0\}$ tenim $S^{-1}A = Quot(A)$ el cos de fraccions de $A$.**

**Lema A.0.5.** *Per a qualsevol $\mathfrak{p} \in Spec(A)$, el cos de fraccions de $A_{\mathfrak{p}}$ correspon al cos de fraccions $Quot(A)$ del domini $A$.*

*Demostració.* Denotem per $K = Quot(A)$ i per construcció

$$A \subset A_{\mathfrak{p}} \subset K.$$

Evidentment tot element $k \in K$ és $\frac{a}{b}$ amb $a, b \in A$ amb $b \neq 0$ i per tant $a, b \in A_{\mathfrak{p}}$, d'on $K \subset Quot(A_{\mathfrak{p}})$, però el cos de quocients és el cos més petit que conté el domini, per tant $K = Quot(A_{\mathfrak{p}})$. □

**Els segons dos resultats són fàcils de demostrar que deixem al lector interessat.**

**Lema A.0.6.** *Donat $A$ un domini i $\mathfrak{p} \in Spec(A) \setminus (0)$ tenim que l'anell $A_{\mathfrak{p}}$ és un anell local. Més generalment hi ha una bijecció entre $Spec(S^{-1}A)$ i $\{\mathfrak{p} \in Spec(A) | \mathfrak{p} \cap A = \emptyset\}$. En particular $dim_{Krull} A_{\mathfrak{p}} \leq dim_{Krull} A$.*

**Proposició A.0.7.** *Sigui $A$ un domini i $\mathfrak{p}$ un ideal primer de $A$. Llavors per tot $n \in \mathbb{N}$ hi ha un isomorfisme natural*

$$A/\mathfrak{p}^n \to A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}.$$

**Quant de lluny és la condició sobre un domini $A$ on els anells locals $A_{\mathfrak{p}}$ son anells de valoració?**

**Podeu llegir literatura respecte: Prüfer domain, Bezout domain, Krull domains,...**

**Definició A.0.8.** *Un anell commutatiu $R$ s'anomena noetherià si tota cadena ascendent d'ideals via inclusió és estacionaria.*

**Tenim la següent caracterització d'anell noetherià.**

**Lema A.0.9.** *Un anell $R$ és noetherià si i només si tot ideal de $A$ és finit generat.*

**Lema A.0.10.** *Sigui $A$ un domini noetherià, i $S$ un conjunt multiplicativament tancat. Llavors $S^{-1}A$ és noetherià.*

**Teorema A.0.11** (Hilbert)**.** *Sigui $K[X_1, \ldots, X_n]$ anell de polinomis en $n$-variables sobre un cos $K$. Llavors $K[X_1, \ldots, X_n]$ és un anell noetherià.*

**Anem a caracteritzar anells de valoració discreta amb la condició d'anells noetherians.**

**Proposició A.0.12.** *Sigui $R$ un anell commutatiu (no necessàrement domini). Tenim que $R$ és un anell de valoració discreta si i només si és un anell local que és noetherià i que l'ideal maximal es generat per un element no-nilpotent.*

**Tenim la següent caracterització en dominis noetherians.**

**Proposició A.0.13.** *Sigui $A$ un domini que és un anell Noetherià. Llavors $A$ és un anell de valoració discreta si i nomes si $A$ té un únic ideal primer no-zero i $A$ és integrament tancat (on $A$ és integrament tancat, si per tot $x \in Quot(A)$ que és arrel d'un polinomi mònic en $A[x]$ es té que $x \in A$).*

**Per més detalls [?, Chp, 1].**

# Appendix B

# Completacions i limits projectius

**Sigui $(G,+)$ un grup abelià topològic, és dir $G$ un grup abelià amb una topologia tal que les aplicacions $G\times G\to G$ $(g_1,g_2)\mapsto g_1+g_2$ i $G\to G$ $g\mapsto -g$ són contínues.**

**Observació B.0.1.** *Fixem-nos que $\{0\}$ és tancat en $G$ llavors tenim que la diagonal de $G$,*

$$\Delta_G := \{(x,y)\in G\times G | x=y\}$$

*és tancat en $G\times G$ perquè $\Delta_G = h^{-1}(\{0\})$ on $h$ és la composició de les aplicacions contínues $G\times G\to G\times G$ $(x,y)\mapsto(x,-y)$ i la suma $G\times G\to G$.*
*És un fet conegut general de topología que $\Delta_G$ és tancat en $G\times G$ si i només si $G$ és Hausdorff.*

**Podem considerar l'aplicació bijectiva:**

$$T_a : G\to G$$

$$x\mapsto x+a$$

**que és contínua (ja que $G\to G\times G$ $x\mapsto(x,a)$ és continua i després composem amb l'operació suma), i per tant $T_a$ és un homeomofisme.**

**En particular si $U$ és un entorn de 0 de $G$, tenim $U+a$ és un entorn de $a$, i per tant la topología de $G$ està determinada pels entorns al voltant de l'element neutre de $G$.**

**Lema B.0.2.** *Sigui $H$ la intersecció de tots els entorns de 0 de $G$. Llavors:*

1. *$H$ és un subgrup de $G$.*
2. *$H$ és l'adherència del zero, és dir $H=\overline{\{0\}}$.*
3. *$G/H$ amb la topologia quocient és Hausdorff.*
4. *$G$ és Hausdorff si i només si $H=\{0\}$.*

*Demostració.* 1. si $U$ entorn, $-U$ també (del fet que aplicació invers és contínua), per tant si $x \in \cap_{entorns\ del\ 0} = H$ tenim $-x \in H$. Igualment donats $x, y \in H$ i si $x + y \notin V$ on $V$ un entorn del zero tenim $x + y \in V^c$ on $0 \notin V^c$ però l'antiimatge de $V$ per l'apliació continua suma és $U_1 \times U_2$ amb $U_1, U_2$ entorn oberts de 0, i en particular $x \in U_1$ i $y \in U_2$, arriban a contradicció que $x + y \notin V$.

2. $x \in H \Leftrightarrow x - U\ entorn\ de\ 0 \Leftrightarrow x \in \overline{\{0\}}$ [1]

3. De ser $H$ tancat i $T_a$ contínua, les classes laterals $g + H$ són tancats de $G$ per $g \in G$, per tant en la topologia quocient de $G/H$ (del morfisme $proj : G \to G/H$), els punts de $G/H$ són tancats. [2] Però si $[x_1], [x_2] \in G/H$ tenim que $x_1 + U, x_2 + U$ són oberts de $x_1, x_2$ respectivament on $U \subset V$ on $V$ entorn del zero, per tant $[x_i] = proj(x_i + U)$ són oberts en $G/H$, per tant $G/H$ Hausdorff.

4. Si $H = \{0\} = \overline{\{0\}}$ tenim $G$ és Hausdorff per l'apartat anterior. Ara si $G$ Haussdorf, llavors $H$ ha de ser trivial ja que si $x \in H$ i $0 \in H$ no entorns que els pogués separar.

□

**Ara observem donat $G$ un grup topològic amb un sistema fonamental d'entorns al voltant del zero, podem definir successions de Cauchy en $G$ via $\{(x_n)_n\}$ amb $x_n \in G$ on $\forall U$ entorn del zero $\exists n(U) \in \mathbb{N}$ complint que $x_n - x_m \in U\ \forall n, m \geq n(U)$. Per tant podem definir el completat $\tilde{G}$ de $G$ com hem fet en el capítol 2 via $\mathcal{C}(G)$ successions de Cauchy en $G$ modul l'ideal de les successions convegents a zero, és dir via la relació d'equivalència:**

$$(x_n)_n \sim (y_n)_n \Leftrightarrow x_n - y_n \to^n 0\ en\ G,$$

**traslladant l'operació aditiva de $G$ en $\hat{G}$ via $[(x_n)_n] + [(y_n)_n] = [(x_n + y_n)_n]$ i podem dotar $\hat{G}$ de grup topològic via els entorns $U$ de $G$ on $x = [(x_n)_n] \in \hat{U}$ on $\hat{U}$ entorn de $\hat{G}$ si $\exists n_x$ on $x_n \in U\ \forall n \geq n_x$. Tenim un morfisme de grups abelians natural i continu**

$$\phi : G \to \hat{G}$$

$$x \mapsto [(x)_n]$$

**que s'aplica a la successió constant $x$. Observeu que $ker(\phi) = \cap U$ on $U$ recorre els entorns del zero. On tenim,**

**Lema B.0.3.** *Donat $G$ un grup abelià topològic i $N = \cap U$ respecte tots els entorns del zero. Llavors:*
*$\phi : G \to \hat{G}$ és injectiu si i només si $G$ és Hausdorff.*

**Es pot demostrar el següent resultat,**

[1] On recordem Lema 2.7 del llibre Kosniowski d'un primer curs en Topologia Algebraica:
$x \in \overline{Y} \Leftrightarrow U\ obert\ amb$
$x \in U\ \ U \cap Y \neq \emptyset$.

[2] Recordem del curs de topologia, o consulteu Kosniowski, que un espai $X$ és $T_1$ si i només si tot punt de $X$ és tancat. Recordem també que Hausdorff és la propietat $T_2$ i sempre la propietat $T_2$ implica $T_1$.

**Lema B.0.4.** *Donat $f : G \to G'$ i $g : G' \to G''$ morfismes continus de grups abelians topològics. Llavors és té morfismes de grups naturals i continus $\hat{f} : \hat{G} \to \hat{G'}$ i $\hat{g} : \hat{G'} \to \hat{G''}$ complint $g \hat{\circ} f = \hat{g} \circ \hat{f}$.*

**Definició B.0.5.** *Diem $(G, +)$ és complet si $\phi : G \to \hat{G}$ és una bijecció.*

**Observació B.0.6.** *Aquesta definició coincideix per $K$ cos amb $(K, +)$ com a grup abelià quan afirmem que $K$ és complet. Realment si $\phi$ és una bijecció, és té que és un homeomorfisme.*

**Observació B.0.7.** *Es pot demostrar que $\hat{G}$ és sempre complet, és dir que $\phi : \hat{G} \to \hat{\hat{G}}$ és sempre una bijecció (realment isomorfisme de grups que és homemorfisme).*

**Ens interessa per $(G, +)$ un grup abelià topològic el següent cas, considera**

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n \supseteq 0 \tag{B.1}$$

**amb $G_i$ subgrups de $G$, on $U \subset G$ és un entorn del zero de $G$ si i només si conté algún $G_n$.**

**Observació B.0.8.** *En l'anterior situació els $G_n$ són oberts i tancats en la topología de $G$:*
*- si $g \in G_n$ tenim $g + G_n$ entorn de $g$ i com $g + G_n \subset G_n$ tenim $G_n$ és obert;*
*-tenim que $\cup_{h \notin G_n}(h + G_n)$ és obert i coincideix amb $G \setminus G_n$ per tant $G_n$ és tancat.*

**En la situació que els entorns són via subgrups com en l'expressió (B.1), el grup $\hat{G}$ és equivalent a la següent formulació con a conjunt: $(x_n)_n \in \hat{G}$, per cada $n$ tenim que $[x_m] \in G/G_n$ és constant per $m \geq n(G_n)$, escrivim $\xi_n \in G/G_n$ aquest valor. Per definició i construcció obtenim**

$$\pi_n^{n+1} = projecció : G/G_{n+1} \to G/G_n$$

$$\xi_{n+1} \mapsto \xi_n.$$

**Lema B.0.9.** *Un grup $(G, +)$ abelià topològic amb una filtració d'entorns del zero per subgroups $G_n$, llavors hi ha un isomorfisme de grups entre $\hat{G}$ i $\varprojlim_n G/G_n$, el límit projectiu de $G/G_n$ via $\pi_n^{n+1}$* [3].

*Demostració.* Demostrem tan sols la bijecció com a conjunts. Per això sol falta demostrar que donat $(\xi_n)_n \in \varprojlim_n G/G_n$ construir una successió de Cauchy en $G$. Prenem $x_n \in G$ qualsevol element complint $[x_n] = \xi_n \in G/G_n$ on $x_{n+1} - x_n \in G_n$, i facilment es comprova que $(x_n)_n$ és una successió de Cauchy de $G$. És una comprovació que aquesta bijecció manté l'operació de grups abelians. □

**Donat un domini commutatiu $A$ i $\mathfrak{a}$ un ideal de $A$ observem que $\mathfrak{a}^n A$ defineix una filtració amb la suma, i en particular dota a l'anell $A$ d'una topología anomenada topològia $\mathfrak{a}$-àdica.**

**Escrivim per $\hat{A}^{\mathfrak{a}}$ la completació $\mathfrak{a}$-àdica de $A$ (com a grup topològic amb la suma) i és fàcil demostrar que té estructura d'anell, de ser $A$ un anell.**

[3] Aquest isomorfisme és de grups topològics (és dir és també un homeomorfisme) si en $G/G_n$ hi possem la topologia quocient i en el limit projectiu la topologia induïda de la topologia producte en $\prod_n G/G_n$

**Corol·lari B.0.10.** *Sigui $A$ un anell de valoració discreta donada per una valoració $v : K := Quot(A) \to \mathbb{Z} \cup \{\infty\}$, i escrivim $(\pi) = \mathfrak{p}$ l'ideal maximal de $A$ on $v(\pi) = 1$. Llavors la filtració*

$$A \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots$$

*defineix la topología $\mathfrak{p}$-àdica en $A$ que coincideix amb la donada pel valor absolut $||_v$ i a més*

$$\hat{A}^{\mathfrak{p}} = \hat{A} = \{x \in \hat{K} | |x|_{\hat{v}} \leq 1\}.$$

*Demostració.* Fixem-nos que $v^{-1}(n\mathbb{N}) = \mathfrak{p}^n$ i per tant la topologia de la filtració coincideix amb la donada pel valor absolut. Ambdues completacions $\hat{A}$ i $\hat{A}^{\mathfrak{p}}$ coincideixen amb el mateix limit projectiu, i per tant coincideixen les successions de Cauchy a partir d'elements de $A$ mòdul equivalència. □

# Bibliografia


[Atiyah-Macdonald] M.F. Atiyah, I.G.Macdonald: "Introduction to Commutative Algebra". Addison-Wesley Publish, 1969. Versió espanyola per Griselda Pacual Xufré en editorial Reverté, 1989.

[Herrerias] Marta Herrerias: Elliptic Curves and Mazur's theorem. Master thesis UPC, 2020, supervisat per Joan Carles Lario.

[Elkies-Klagsbrun] N. D. Elkies and Z. Klagsbrun: New rank records for elliptic curves faving rational torsion. Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Mathematical Sciences Publishers, Berkeley, 2020, pp. 233-250.

[Lorenzini] Dino Lorenzini: An invitation to Arithmetic Geometry. GTM vol.9. American Math.Society, 1996, ISBN 10: 0821802674.

[Milne] J.S. Milne: Elliptic Curves. 2006, 978-1419652578. See his personal web page for interesting books on Arithmetic Geometry.

[Serre] J.P.Serre: A course in Arithmetic. Springer Verlag, 1973, ISBN:978-0387900407.

[Serre-LF] J.P.Serre: Local Fields.Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[Spivakovsky] Mark Spivakovsky: Resolution of Singularities: an Introduction. Handbook of Geometry and Topology of Singularities I, Springer, pp.183-242, 2020, 978-3-030-53060-0.

[Silverman] Joseph J. Silverman: The arithmetic of elliptic curves. GTM106, 2nd edition 2009, ISBN: 978-0-387-09493-9.

[Silverman2] Joseph J. Silverman: Advanced topics of elliptic curves. Springer, GTM 151, 1994. ISBN: 978-0387943282.

[Shimura] G.Shimura: An introduction to the Arithmetic Theory of Automorphic Functions. Princeton Univ.Press, 1971.

[Shimura2] G.Shimura: Abelian varieties with complex multiplication and modular functions. Princeton Univer.Press, 1998.

[Washington] L.C. Washington: Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997. xiv+487 pp. ISBN: 0-387-94762-0.