I: DIP's y DFU's

- (Ecuaciones diofánticas): Se trata de encontrar las soluciones $x, y \in \mathbb{Z}$ tales que $2000x - 266y = -4$, p.ej.

Se usa el Algoritmo de Euclides: si $\begin{matrix} a & \underline{b} \\ \vee & c \end{matrix}$, $mcd(a,b) = mcd(b,r)$. Dividiendo y por recurrencia se haga el mcd, y operando hacia atrás dejando los restos sin operar para despejarlo de la división anterior se encuentre 1 sol particular (multiplicada por un cierto escalar), x_0, y_0. El resto serán los $x, y \in \mathbb{Z}$ tal que $2000(x-x_0) - 266(y-y_0) = 0 \iff 1000(x-x_0) - 133(y-y_0) = 0 \iff \begin{cases} x - x_0 = n \cdot 133 \\ y - y_0 = n \cdot 1000 \end{cases}$.

(primos entre sí)

Definición: Un anillo euclídeo es un anillo íntegro A junto con una aplicación $\delta: A - 0 \longrightarrow \mathbb{N}$ tal que:

i) $\delta(a) \leq \delta(ab)$

ii) (Algoritmo de Euclides) Para cada $a, b \in A-0$, $\exists\, c, r$ (no nec. únicos) tal que $a = b \cdot c + r$, con r bien $r = 0$ bien $\delta(r) \leq \delta(b)$.

Ejemplos: $(\mathbb{Z}, |\cdot|)$, $(K[x], gr)$, $(\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i, \delta(a+bi) = a^2+b^2)$ (¡es multiplicativa!).

¿Cuándo un número entero puede escribirse como suma de dos cuadrados?

Lema I: $p = a^2 + b^2 \iff p \in \mathbb{Z}[i]$ no es irreducible, con p primo.

Lema II: $p \in \mathbb{Z}[i]$ no es irreducible $\iff \exists\, \overline{a} \in \mathbb{Z}/p\mathbb{Z} : \overline{a}^2 = -1$.

Teorema (Caso primo) $p = a^2 + b^2 \iff p = 2$ ó $p \equiv 1 \pmod 4$ (ie, $p = 1 + \hat{4}$).

Teorema (Caso General): Sea $n = p_1^{n_1} \cdots p_r^{n_r} \cdot q_1^{m_1} \cdots q_s^{m_s}$, con $p_i = a_i^2 + b_i^2$ y $q_i \neq c_i^2 + d_i^2$.

$$n = a^2 + b^2 \iff m_i \text{ es par } \forall i.$$

• En los anillos de ints se ha visto que los anills integros son DFU:

Definición: Sea A un anills integro. Se dice que $a \in A$ es propio si no es nulo ni invertible. Se dice que $a \in A$ es irreducible si no es producto de dos propios.

Lema: Sea (A, δ) un anills euclídeo. Si $b, c \in A$ propios $\Rightarrow \delta(b) < \delta(bc)$.

Teorema: (A, δ) euclídeo $\longrightarrow$ A DIP. $\Rightarrow$ A DFU

Definición: Sea A DIP, $a, b \in A$. Se llama $mcd(a,b)$ al generador del ideal $(a,b) = (a) + (b) = (\text{mcd}(a,b))$ (está generado por un dedo por ser A DIP). Es único salvo invertibles. Automáticamente se tiene la identidad de Bezout:

si $d = mcd(a,b)$, $\exists \lambda, \mu \in A$: $\lambda a + \mu b = d$.

• Con si a, b primos entre sí $:=$ no divisores propios comunes, $\exists (1) = (\text{inv}) = A$,

Corolario: Sean $a, b \overset{\in A \text{ DIP}}{\text{primos}}$ entre sí. Entonces $\exists \lambda, \mu \in A$: $\lambda a + \mu b = 1$.

Lema (Euclides): Sea A DIP, $p \in A$ irreducible. Si p divide a ab, divide a algún factor.

Lema (Euclides, General): Sea A DIP, $\exists\ 0 \neq a \in A$. Son equivalentes:

1) $a \in A$ irreducible
2) (a) ideal primo
3) (a) ideal maximal

Es decir, $\text{Spec } A = \{0, (a)\}_{a \text{ irred}}$; $\text{Spec}_{MAX} A = \{(a)\}_{a \text{ irred}}$.

Proposición: Sea A DFU, $\exists\ 0 \neq a \in A$.

$a \in A$ irreducible $\iff$ (a) primo,

es decir, $(\text{Spec } A)_{|\text{principales}} = \{0, (a)\}_{a \text{ irred}}$.

Definición: Un A-módulo M se dice **noetheriano** si todo submódulo es finito-generado. Un anillo A se dice noetheriano cuando sea noetheriano como A-módulo, ie, cuando todo ideal sea finito-generado.

Proposición: Un anillo A es noetheriano $\iff$ cumple la c.c.a.: toda cadena de ideales estabiliza.

Teorema: Sea M un A-módulo, y $N \subseteq M$ submódulo

1) M noeth $\iff$ N, M/N noeth

2) $M = M' \oplus M''$ noeth $\iff$ M', M'' noeth

3) A noeth, M A-módulo fg $\Rightarrow$ M noeth

4) (**Teorema de la Base de Hilbert**) A noeth $\Rightarrow$ $A[x]$ noeth.

5) A noeth $\Rightarrow$ $\dfrac{A[x_1 \dots x_n]}{I}$ noeth.

Proposición: Sea A noetheriano e íntegro. Todo elemento descompone como producto de irreducibles (no necesariamente de modo único).

Definición: Un anillo se dice **local** si solo tiene un ideal maximal.

Lema (Nakayama): Sea $\mathcal{O}$ un anillo local de maximal m, y sea M un $\mathcal{O}$-módulo finito-generado.

$$M = 0 \iff M \otimes_{\mathcal{O}} \mathcal{O}/m = M/mM = 0 \quad (\Leftrightarrow M = mM)$$

$\overset{?}{\Leftrightarrow}$ un $\mathcal{O}/m$-ev.

Corolario: $M = \langle m_1, \dots, m_r \rangle \iff M/mM = \langle \overline{m_1}, \dots, \overline{m_r} \rangle$.

Corolario. $mM = \{ a_1 m_1 + \dots + a_n m_n \}$.

Corolario. M A-módulo, $I \subseteq A$ ideal. M/IM es un A/I-módulo: $\overline{a} \cdot \overline{m} := \overline{am}$. Hipótesis: $I = 0$!!!

Corolario: Sea A anillo. $a \notin A^* \iff a$ está contenido en algún ideal maximal, ie, $\bigcup_{m \text{ max}} m = A - A^*$;

o otra forma,

$$A = \left(\bigcup_{m \text{ max}} m \right) \amalg A^* .$$

Proposición: Sea $\mathcal{O}$ un anillo local noetheriano, de maximal m.

m principal $\iff$ { a) $\mathcal{O}$ DIP (íntegro), en cuyo caso $\dim_{Krull} \mathcal{O} = 1$; o bien
b) $\mathcal{O}$ de ideales principales (no íntegro), en cuyo caso $\dim_{Krull} \mathcal{O} = 0$.

y en tal caso, si $m = (t)$, entonces todo ideal de $\mathcal{O}$ es $I = (t^r)$.

Corolario: Sea $\mathcal{O}$ un anillo local noetheriano de maximal m y $\dim_{Krull} \mathcal{O} > 0$.

$$\mathcal{O} \text{ DIP} \iff \dim_{\mathcal{O}/m} m/m^2 = 1.$$

Proposición: Sea A anillo íntegro noetheriano. Para que A sea DIP es suficiente que los ideales maximales sean principales.

Teorema (Ternas Pitagóricas): Las ternas pitagóricas, ie, las $(x,y,z) \in \mathbb{Z}^3$ tal que $x^2 = y^2 + z^2$ (con $xyz \neq 0$) son:

$$\left.\begin{aligned} x &= c(a^2 - b^2) \\ y &= c(2ab) \\ z &= c(a^2 + b^2) \end{aligned}\right\}$$

II : DOMINIOS DE DEDEKIND

LOCALIZACIÓN

Definición: Sea A un anillo. Un sistema multiplicativo es un subconjunto $S \subseteq A$ tal que

i) $1 \in S$

ii) $s, s' \in S \Rightarrow s \cdot s' \in S$.

Ejemplos: 1) Si A íntegro, $A - 0$ s.t. mlp ; 2) $A - P$, P primo ; 3) $\{a^n\}_{n \geq 0}$.

Definición: Sea A un anillo y $S \subseteq A$ s.t. multipl.. Se llama localización de A por S a

$$A_S := \left\{ \frac{a}{s} \, , \, a \in A, s \in S \, : \, \frac{a}{s} = \frac{a'}{s'} \iff \exists\, t, t' \in S \, : \, \begin{array}{l} ta = t'a' \\ ts = t's' \end{array} \right\}$$

Las operaciones $\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}$; $\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$, que no dependen de los representantes elegidos, dotan

a $(A_S, +, \cdot)$ de estructura de anillo.

Si A íntegro, A_{A-0} es un cuerpo, llamado cuerpo de fracciones de A.

En la localización, los elementos de S se hacen invertibles, y en general algunos más.

Proposición (Propiedades): Sea A un anillo, $S \subseteq A$ s.t. multpl., y A_S la localización.

1) $\frac{a}{s} = 0 \left(= \frac{0}{1} \right) \iff \exists\, t \in S : ta = 0$.

2) $\frac{a}{s} = \frac{a'}{s'} \iff \exists\, t \in S : t(as' - a's) = 0$.

3) $A_S = 0 \iff 0 \in S$

Corolario: Sea A un anillo íntegro.

1) $\frac{a}{s} = 0 \iff a = 0$

2) $\frac{a}{s} = \frac{a'}{s'} \iff as' = a's$.

Definición: Se llama **morfismo de localización** a $j: A \to A_S$, $j(a) = \frac{a}{1}$.

Proposición: Consideremos $\mathcal{C}^\infty(\mathbb{R}^n)$, y dado $\alpha = (\alpha_1 \dots \alpha_n) \in \mathbb{R}^n$, $m_\alpha = \{ f \in \mathcal{C}^\infty(\mathbb{R}^n) : f(\alpha) = 0 \}$ es un ideal maximal.

Pues se cumple que

$$\mathcal{C}^\infty(\mathbb{R}^n)_\alpha \equiv \mathcal{O}_\alpha(\mathbb{R}^n) \equiv \text{anillo de gérmenes de funciones en } \alpha$$

$$\text{div. formal} \hookrightarrow \frac{f}{g} \longrightarrow \left[\frac{f}{g}\right]$$

- $A_x \overset{not}{=} A_{A-p_x}$, $x \in \operatorname{Spec} A$.

Teorema: Sea A anillo, S s.t. mfp y A_S la loc. Entonces se tiene esta correspondencia que conserva inclusiones:

$$\operatorname{Spec} A_S \equiv \{ x \in \operatorname{Spec} A : \mathcal{P}_x \cap S = \emptyset \}$$

Corolario: Sea $x \in \operatorname{Spec} A$ y consid. A_x. Entonces éste es un anillo local de único ideal maximal $\mathcal{P}_x A_x$:

$$\operatorname{Spec} A_x \equiv \{ y \in \operatorname{Spec} A : \mathcal{P}_y \subseteq \mathcal{P}_x \}$$

$$\begin{array}{ccc} \mathcal{P}_y A_x & \longleftarrow & \mathcal{P}_y \\ \cap & & \cap \\ \mathcal{P}_x A_x & \longleftarrow & \mathcal{P}_x \end{array}$$

Definición: Sea A un anillo, $S \subseteq A$ mult. cerrado y M un A-módulo. Se llama **localización de M por S** a

$$M_S := \left\{ \frac{m}{s}, m \in M, s \in S : \frac{m}{s} = \frac{m'}{s'} \iff \exists t, t' \in S : \begin{array}{l} tm = t'm' \\ ts = t's' \end{array} \right\}.$$

- Las operaciones $\frac{m}{s} + \frac{m'}{s'} := \frac{ms' + m's}{ss'}$ y $\frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}$, se comprueba de los representantes, dotan a $(M_S, +, \cdot)$ de estructura de A_S-módulo.

Teorema: Sean M, N A-módulos, y $S \subseteq A$ mult. cerrado. Dado $f: M \to N$ mf. de A-mód.

$\exists\, f_S : M_S \to N_S$ mf. de A_S-mód que hace el diagrama conmutativo:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle i}\downarrow & \exists f_S & \downarrow \\ M_S & \dashrightarrow & N_S \end{array} \qquad , \quad f_S\left(\frac{m}{s}\right) := \frac{f(m)}{s}.$$

Proposición: $(M \oplus N)_S = M_S \oplus N_S$.

Proposición:

1) $(\ker f)_S = \ker f_S$
2) $(\operatorname{Im} f)_S = \operatorname{Im} f_S$.

Corolario: $(M/N)_S = M_S/N_S$.

Lema: $M = 0 \iff M_x = 0 \quad \forall x \in \operatorname{Spec}_{max} A$ ("ser 0 es una propiedad local").

Teorema: Sea $f: M \to N$ mf de A-mód.

1) f inyectiva $\iff f_x$ inyectiva $\forall x \in \operatorname{Spec}_{max} A$
2) f epiyectiva $\iff f_x$ epiyectiva $\forall x \in \operatorname{Spec}_{max} A$
3) f isomorfismo $\iff f_x$ isomo $\forall x \in \operatorname{Spec}_{max} A$.

Proposición: Sean $N, N' \subseteq M$ submód. $N = N' \iff N_x = N'_x \quad \forall x \in \operatorname{Spec}_{MAX} A$.

DOMINIOS DE DEDEKIND

Definición: Un *dominio de Dedekind* es un anillo íntegro noetheriano tal que A_x es DIP $\forall x \in \operatorname{Spec}_{MAX} A$.

Ej: 1) K cuerpo, 2) A DIP.

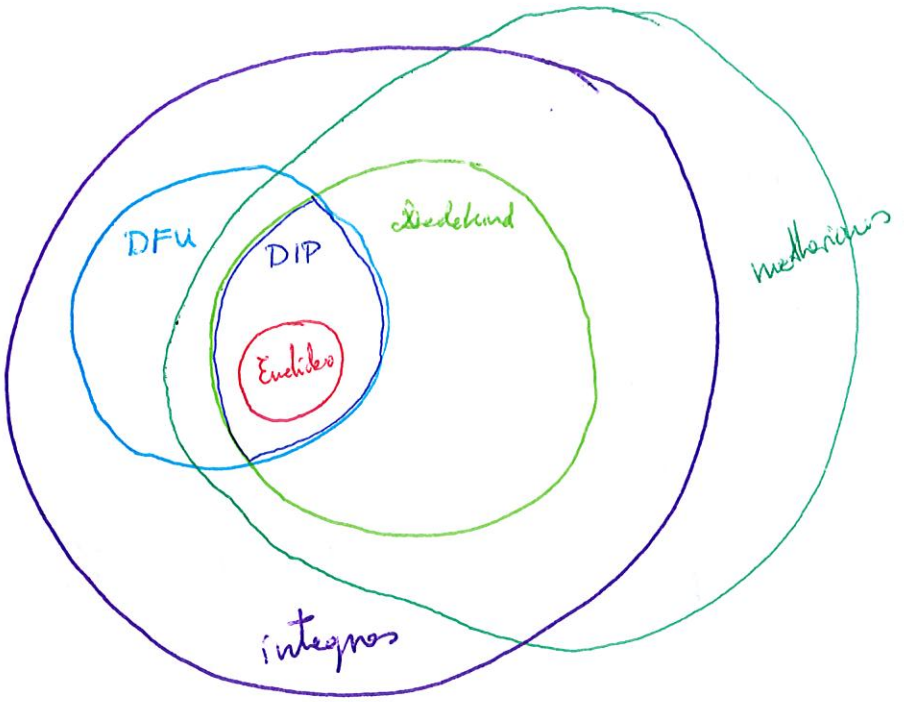
- Todo dominio de Dedekind tiene bien $\dim_{Krull} = 0$ (si es cuerpo) o $\dim_{Krull} = 1$.

Teorema: Sea A un anillo íntegro.

A es dominio de Dedekind $\iff$ todo ideal propio se escribe de modo único como producto de primos,

$$I = \mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}.$$

Corolario: Dedekind + DFU = DIP.



Proposición: Sea A un dominio de Dedekind, y supongamos que $\operatorname{Spec}_{MAX} A = \{x_1, \dots, x_n\}$ un nº finito de ptos.

1) A es DIP
2) A es anillo euclídeo.

- En un dominio de Dedekind A, por tener $\dim_{Krull} = 1$, se cumple que

$$\boxed{\operatorname{Spec} A = \operatorname{Spec}_{MAX} A \amalg \{0\}}$$

PUNTOS SINGULARES

Definición: Sea A un anillo íntegro de $\dim_{Krull} A = 1$. Un punto cerrado $x \in Spec_{max} A$ se dice **no singular** si A_x es DIP (ie, si $\dim_{A/m_x} \frac{m_x}{m_x^2} \leq 1$), y se dice **singular** si A_x no es DIP (ie, si $\dim_{A/m_x} \frac{m_x}{m_x^2} > 1$).

- La equivalencia es el Lema de Nakayama: A_x DIP $\Leftrightarrow m_x A_x = (t) A_x \overset{Nak}{\Leftrightarrow} \frac{m_x}{m_x^2} = \frac{m_x A_x}{m_x^2 A_x} = (\bar{t}) \Leftrightarrow \dim_{A/m_x} \frac{m_x}{m_x^2} \leq 1$.

- Recall: $Spec_{max} \frac{k[x_1 \dots x_n]}{(p(x_1 \dots x_n))} = \{(a_1 \dots a_n) \in k^n : p(a_1 \dots a_n) = 0\}$, si k es alg. cerrado.

- Para anillos de fcns, p.ej. $A = C^\infty(\mathbb{R}^n)$ o $A = k[x_1 \dots x_n]$, dado $a \in \mathbb{R}^n / k^n$, se tiene que $m_a = \{f : f(a) = 0\} = (x_1 - a_1, \dots x_n - a_n)$ es un ideal maximal, y para cada $f \in A$, $f(x) = f(a) + \sum \frac{\partial f}{\partial x_i}(a)(x_i - a_i) + m_a^2$. Quiero llamar **diferencial de f en a** a $d_a f := \overline{f(x) - f(a)} \in \frac{m_a}{m_a^2}$, y tendré que $d_a f = \sum \frac{\partial f}{\partial x_i}(a) \cdot d_a x_i$, y como son L.I.,

Teorema: $\{d_a x_1, \dots, d_a x_n\}$ es base del $A/m_a = \mathbb{R}$-EV $\frac{m_a}{m_a^2}$ (es de dim n).

(ojo, en principio $\frac{m_a}{m_a^2}$ es un A-mod, pero como $\cdot m_a = 0$, también es A/m_a mod.)

Esto lo quiero generalizar a anillos cualesquiera:

Definición:

a) Sea A un anillo y $m_a \subset A$ un ideal (no nec. max.). Dado $f \in m_a$, se llama **diferencial de f en a** a

$$d_a f := \bar{f} \in \frac{m_a}{m_a^2}.$$

b) Sea A una k-álgebra, $m_a \subset A$ un id. maximal con $A/m_a = k$. Dado $f \in A$, se llama **valor de f en a** a $f(a) := \bar{f} \in A/m_a = k$; y la **diferencial de f en a** es $d_a f := \overline{f - f(a)} \in \frac{m_a}{m_a^2}$.

Teorema: Sea A un anillo, $m_\alpha \subset A$ un ideal (no ne. nec.). Sea $I = (f_1, \dots, f_n) \subset m_\alpha$ un ideal f.g incluido en m_α y denotes $\overline{m_\alpha} \subset A/I$. Entonces

$$\frac{\overline{m_\alpha}}{\overline{m_\alpha}^2} = \frac{m_\alpha / m_\alpha^2}{\langle d_\alpha f_1, \dots, d_\alpha f_n \rangle}$$

Corolario: Sea $A = \frac{k[x,y]}{(p(x,y))}$, con k alg cerrado, y sea $(\alpha,\beta) \equiv \overline{m_{(\alpha,\beta)}} \in \operatorname{Spec}_{Max} A$ (ie, $m_{(\alpha,\beta)} = (x-\alpha, y-\beta)$).

Entonces

$$(\alpha,\beta) \text{ es singular} \iff d_{(\alpha,\beta)} p(x,y) = 0 .$$

Teorema (Fórmula de la fibra): Sea $f: A \to B$ hf. de anills y $\operatorname{Spec} A \xleftarrow{f^*} \operatorname{Spec} B$ el hf inducido. Todos los ideals primos de B se pueden calcular a partir de los de A, a partir de la fibras de sus elems:

dado $y \in \operatorname{Spec} A$,

$$f^{*-1}(y) = \operatorname{Spec} \frac{B_y}{p_y B_y}$$

si y es maximal,

$$f^{*-1}(y) = \operatorname{Spec} \frac{B}{m_y B}$$

y si es minimal,

$$f^{*-1}(y) = \operatorname{Spec} B_y$$

Ej: Ideals primos de $\mathbb{Z}[x]$:

$$\operatorname{Spec} \mathbb{Z}[x] = \left\{ \begin{array}{l} 0 \\ (q(x)) : q(x) \text{ irred. en } \mathbb{Z}[x] \text{ (aquí están los } (p) \text{ tales, } p \text{ primo)} \\ (p, q(x)) : p \text{ primo y } \overline{q(x)} \text{ irred. en } \mathbb{Z}/p\mathbb{Z}[x] \end{array} \right\}$$

↖ maximales

Proposición: Sea $i: A \hookrightarrow B$ un mfs finito, $x \in \operatorname{Spec}_{m_x} A$ y sean $i^{*-1}(x) = \{y_1, \dots, y_n\}$ (sigue n finito en estas condiciones).

1) $\dfrac{B}{m_x B}$ reducido $\Rightarrow$ $m_x B_{y_i} = m_{y_i} B_{y_i}$ $\forall i$

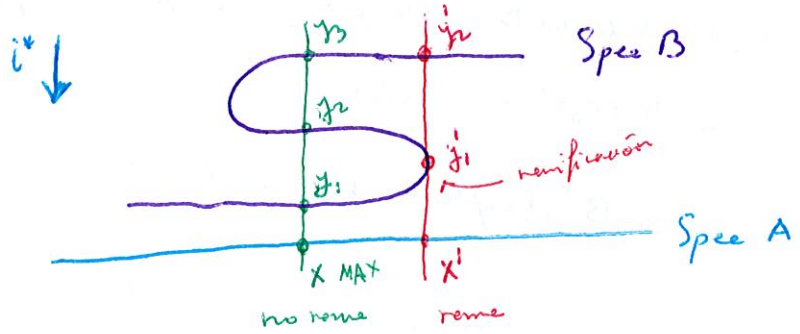
2) $m_x A_x$ principal $\Rightarrow$ $m_{y_i} B_{y_i}$ principales.

Remark. En un mfs finito inyectivo, i^* es epi y $i^{*-1}(\text{maximal}) = \{n \text{ finito de maximales}\}$.

Definición: Sea $i: A \to B$ un mf. finito y $i^*: \operatorname{Spec} B \to \operatorname{Spec} A$. Sea $y \in \operatorname{Spec}_{max} B$ y $x := i^*(y) \in \operatorname{Spec}_{max} A$.

a) Se dice que x es un **punto reme** de i^* si $\dfrac{B}{m_x B}$ no es una A/m_x-álgebra separable. En otro caso se dice que **no es reme**.

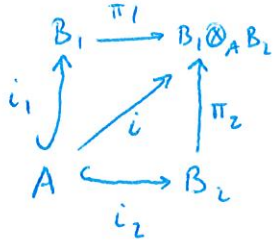
b) Se dice que y es un **punto de ramificación** (o que i^* ramifica en y) si $\dfrac{B_y}{m_x B_y}$ no es una A/m_x-álgebra separable.



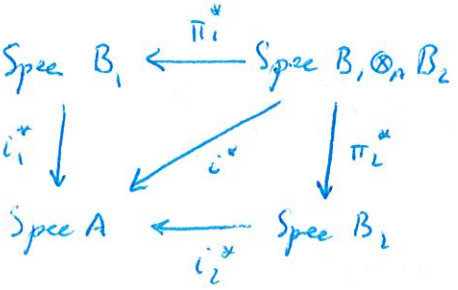
$i^{*-1}(x) = \operatorname{Spec} \dfrac{B}{m_x B} = \{x_1, x_2, x_3\}$

Recall: La k-álgebra $\dfrac{k[x]}{(p(x))}$ es separable $\iff$ $p(x)$ tiene todas sus raíces de multiplicidad 1 (no nec. en k).

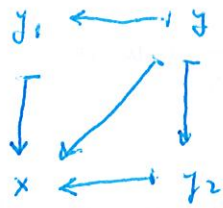
Lema: Sean $i_1: A \hookrightarrow B_1$, $i_2: A \hookrightarrow B_2$ morfismos finitos, y consideremos los morfismos



;



,



Entonces:

1) $\mathfrak{p} \in \operatorname{Spec} A$ no es buena para $i_1^* \iff \mathfrak{p}_2 \in \operatorname{Spec} B_2$ no es buena para π_2^*

2) $\mathfrak{p} \in \operatorname{Spec} A$ no es buena para $i^* \iff \mathfrak{p} \in \operatorname{Spec} A$ no es buena ni de i_1^* ni de i_2^*.

Proposición: $\mathbb{Z}\left[e^{\frac{2\pi i}{n}}\right]$ es un dominio de Dedekind.

ANILLOS NORMALES DE DIM$_{Krull}$ 1

Definición: Sea $A \to B$ mf. de anillos. Un elemento $b \in B$ se dice entero sobre A si $\exists\, p(x) \in A[x]$ mónico tal que $p(b) = 0$, ie, si $\exists\, a_0, \dots, a_{n-1}$: $b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 = 0$.

Definición: Se llama cierre entero de A en B al conjunto de elementos de B enteros sobre A, que forman un subanillo,

$$\overline{A} := \{ b \in B : \exists\, a_0, \dots, a_{n-1} : b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 = 0 \}.$$

Definición: Se dice que un anillo íntegro A es normal o íntegramente cerrado en su cuerpo de fracciones $\Sigma := A_{A-0}$ si cuyle que si $a \in \Sigma$ es entero sobre A (vía $A \hookrightarrow \Sigma$) $\Rightarrow a \in A$. Ie, si $\overline{A} = A \subseteq \Sigma$

Proposición: DFU $\Rightarrow$ normal

Teorema: Sea $\mathcal{O}$ íntegro local noeth y $\dim_{Krull} = 1$. Entonces $\mathcal{O}$ DIP $\iff$ $\mathcal{O}$ normal.

Proposición: "El cierre entero conmuta con los localizados".

Concretamente: Sea $A \to B$ mf de anillos y $S \subset A$ mt. multpl. Sea $\overline{A}$ el cierre entero de A en B y $\overline{A}_S$ el cierre entero de A_S en B_S. Entonces

$$\overline{A_S} = (\overline{A})_S$$

En particular, A normal $\Rightarrow$ loc. normal

Teorema: Sea A anillo noetheriano íntegro de $\dim_{Krull} A = 1$.

$$A \text{ normal} \iff A \text{ Dedekind}.$$

Corolario: Sea A anillo noetheriano íntegro de $\dim_{Krull} A = 1$, Sea Σ su cuerpo de fracciones y $\overline{A}$ el cierre entero de A en Σ (vía $A \hookrightarrow \Sigma$).

$$\mathfrak{p} \in \operatorname{Spec} A \text{ no es singular} \iff A_{\mathfrak{p}} = (\overline{A})_{\mathfrak{p}}.$$

Definición: Sea A anillo noeth íntegro de $\dim_{Krull} A = 1$. Si el cierre entero $\overline{A}$ de A en Σ es noetheriano, $\overline{A}$ es de Dedekind. En tal caso se llama desingularización de $\operatorname{Spec} A$ a $\operatorname{Spec} \overline{A}$. Se dice que $\operatorname{Spec} \overline{A} \to \operatorname{Spec} A$ es el morfismo de desingularización.

ANILLOS DE NÚMEROS ENTEROS

Definición: Un anillo íntegro A se dice que es un anillo de números enteros si existe un morfismo $\mathbb{Z} \hookrightarrow A$ finito e injectivo.

Definición: Dada una ext. finita de cuerpos $\mathbb{Q} \hookrightarrow \Sigma$, se dice que Σ es un cuerpo de números, y que el cierre entero de $\mathbb{Z}$ en Σ, $\overline{\mathbb{Z}} \subset \Sigma$, es el anillo de números enteros de Σ.

Proposición: Sea A un anillo de números enteros, y Σ su cuerpo de fracciones. Entonces $\overline{\mathbb{Z}} = \overline{A} \subseteq \Sigma$.

III : FIBRAS DE UN MORFISMO FINITO

Definición: Un A-módulo $M \neq 0$ se dice **simple** si no contiene submódulos propios, es, si los únicos submódulos que tiene son 0 y M.

- Los K-EV simples son los de dim 1.

Proposición: M simple $\iff M \simeq A/\mathfrak{m}$.

- $\mathbb{Z}$-módulos simples $= \mathbb{Z}/p\mathbb{Z}$.

Definición: Se dice que una cadena de submódulos de M

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_n = M$$

es **irrefinable** si M_i/M_{i-1} es simple $\forall i$. Diremos que tal cadena tiene **longitud** n, Diremos que la **longitud de M** es el mínimo de las longitudes de cadenas irrefinables que existen en 0 y acaban en M.

Teorema: Todas las cadenas irrefinables de un módulo tienen la misma longitud,

- Luego la longitud de un módulo es la longitud de cualquier cadena irrefinable

Proposición: $\boxed{\ell(M/N) = \ell(M) - \ell(N)}$

Proposición: $\boxed{\ell(M_1 \oplus M_2) = \ell(M_1) + \ell(M_2)}$.

Proposición: Si $0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_n = M$ es una cadena de submódulos (no nec. irrefinible), entonces

$$\boxed{\ell(M) = \sum \ell(M_i/M_{i-1})}.$$

Proposición: Sea $\mathcal{O}$ una K-álgebra local de maximal $\mathfrak{m}$, y M un $\mathcal{O}$-módulo. Entonces

$$\boxed{\dim_K M = \ell_{\mathcal{O}}(M) \cdot \dim_K \mathcal{O}/\mathfrak{m}}$$

Proposición: Sea A un anillo integro. Entonces

$$\boxed{\ell\left(\frac{A}{(f \cdot g)}\right) = \ell\left(\frac{A}{(f)}\right) + \ell\left(\frac{A}{(g)}\right)}$$

Proposición: Sea A DIP y $p_1 \dots p_r \in A$ irreducibles. Entonces $\boxed{\ell\left(\frac{A}{(p_1^{n_1} \cdots p_r^{n_r})}\right) = n_1 + \cdots + n_r}$.

Teorema: Sea A un dom. de Dedekind, y $I = \mathfrak{p}_{x_1}^{n_1} \cdots \mathfrak{p}_{x_r}^{n_r}$ un ideal. Entonces

$$\boxed{\ell(A/I) = n_1 + \cdots + n_r}$$

- Recordar de 3º: en un K-álgebra finita A, $\operatorname{Spec} A = \operatorname{Spec}_{\max} A$, y $|\operatorname{Spec} A| \leq \dim_K A < \infty$.

Lema: Sea A un K-álgebra finita, y pongamos $\operatorname{Spec} A = \{x_1 \dots x_n\}$. Entonces

$$A \simeq A_{x_1} \times \cdots \times A_{x_n}$$
$$a \longmapsto \left(\frac{a}{1}, \dots, \frac{a}{1}\right).$$

Corolario: En la situación anterior,

$$\boxed{\dim_K A = \sum_{i=1}^{n} \ell_A(A_{x_i}) \cdot \dim_K (A/\mathfrak{m}_{x_i})}$$

Definición: En la misma situación, llamamos

a) número de puntos de $\operatorname{Spec} A$, contando multiplicidades y grados a $\dim_K A$

b) multiplicidad con la que aparece x_i en $\operatorname{Spec} A$ a $\ell_A(A_{x_i})$

c) grado de x_i a $\dim_K (A/\mathfrak{m}_{x_i})$

Así,

$$\begin{pmatrix} \text{nº de ptos de} \\ \operatorname{Spec} A \text{ contando} \\ \text{multipl. y grado} \end{pmatrix} = \sum_{i=1}^{n} \begin{pmatrix} \text{multiplicidad} \\ \text{con la que aparece} \\ x_i \text{ en } \operatorname{Spec} A \end{pmatrix} \cdot (\text{gr } x_i).$$

• (Caso mf. finito): Sea $A \xhookrightarrow{i} B$ un mf finito, y $\operatorname{Spec} B \xrightarrow{i^*} \operatorname{Spec} A$ su mf. inducido.

Si $x \in \operatorname{Spec}_{m_x} A$, $i^{*-1}(x) = \operatorname{Spec} \dfrac{B}{m_x B}$. Además, $\dfrac{B}{m_x B}$ es un $\underbrace{A/m_x}_{K}$-álgebra finita, y la anterior de antes.

Definición: Con las notaciones anteriores, llamemos

a) número de puntos de $i^{*-1}(x)$ contando multipl. y grados a $\dim_{A/m_x} \dfrac{B}{m_x B}$

b) multiplicidad con la que aparece $y \in i^{*-1}(x)$ en $i^{*-1}(x)$ a $\ell_B\left(\left(\dfrac{B}{m_x B}\right)_y\right)$

c) grado de y sobre x a $\dim_{A/m_x} B/m_y$

Teorema: Sea $A \hookrightarrow B$ finita e inyectiva, con A abdedekind y B íntegro.

"El número de ptos de las fibras de i^*, contando multipl. y grados, es constante".

Explicado, para cualquier $x \in \operatorname{Spec} A$,

$$\begin{pmatrix} \text{nº de ptos de } i^{*-1}(x) \\ \text{cont. multpl. y grados} \end{pmatrix} = \dim_{\Sigma_A} \Sigma_B$$

donde $\Sigma_A = A_{A-0}$, $\Sigma_B = B_{B-0}$.

ESPECTRO PRIMO DEL ANILLO DE INVARIANTES

• Sea B un anillo y $G \subseteq \operatorname{Aut}_{alg}(B)$ un subgrupo finito. Cada $g \in G$ da $B \xrightarrow{g} B$, que da $\operatorname{Spec} B \xrightarrow{g^*} \operatorname{Spec} B$. Se denota $g(p) := g^{*-1}(p)$, ó $g(y)$.

• $B^G = \{b : g(b) = b \ \forall g \in G\} = \{b : G \cdot b = b\}$ (existe) son los invariantes de B por G

• $(\operatorname{Spec} B)/G := \{\overline{y}\}$, con $y \in \operatorname{Spec} B$, donde $\overline{y} = \overline{z} \Leftrightarrow \exists g \in G : z = g(y)$. G. Las clases son las órbitas: $\overline{y} = G \cdot y$.

Teorema: $\boxed{\operatorname{Spec}(B^G) = \dfrac{\operatorname{Spec} B}{G}}$.

En particular, si $B^G \xhookrightarrow{i} B$, $\underline{i^{*-1}(x) = G \cdot y}$, con $y \in i^{*-1}(x)$, $x \in \operatorname{Spec} B^G$

Proposición: Sea B una A-álgebra de tipo finito y $G \subseteq \mathrm{Aut}_A B$. Sean $x \in \mathrm{Spec}^{\max.} B^G$, $y \in i^{*-1}(x)$, $y \in \mathrm{Spec}\, B$.

Todos los datos de la fibra de x tienen el mismo grado sobre x y las localizaciones $\frac{B_{y_i}}{m_x B_{y_i}}$ los mismos longitudes. Por tanto, si $D = \{g \in G : g(y) = y\} \subseteq G$, $i^{*-1}(x) = G \cdot y = G/D$ y

$$\begin{pmatrix} \text{nº de ptos de } i^{*-1}(x) \\ \text{cont. mt. y grado} \end{pmatrix} = |G/D| \cdot \ell\left(\frac{B_y}{m_x B_y}\right) \cdot \mathrm{gr}_x y.$$

= "grupo de descomposición de y"

En particular, si y no es de ramificación, ningún pto de la fibra lo es, y $\ell\left(\frac{B_y}{m_x B_y}\right) = 1$ en la fórmula.

Proposición: $D \longrightarrow \mathrm{Aut}_{B^G/m_x} B/m_y$ es epiyectivo $\Leftrightarrow$ si y no de ramifica.

Corolario: Si B íntegro y $\dim_{\text{Krull}} B = 1$, y x no ramifica y y sobre de ramifica, entonces

$$D = \mathrm{Aut}_{B^G/m_x} B/m_y.$$

AUTOMORFISMO DE FROBENIUS

- Si $\mathbb{Z}/p\mathbb{Z} \hookrightarrow k$ ext. finita de cpo, de dim n,

$$k = \{\text{raíces de } x^{p^n} - x \in \mathbb{Z}/p\mathbb{Z}[x]\} = \mathbb{Z}/p\mathbb{Z}[\text{raíces de } x^n - x] =: \mathbb{F}_{p^n},$$

es una extensión de Galois de $\mathbb{Z}/p\mathbb{Z}$ de grado n, luego si G es su grupo de Galois, $|G| = n$.

Teorema: Sea $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$, $F(\lambda) := \lambda^p$ el **automorfismo de Frobenius**. Se cumple

$$\boxed{\langle F \rangle = G}$$

(**Anillos de nº enteros**): Sea $\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \Sigma \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \overline{\mathbb{Z}} \end{array}$ una ext. de cpo de grupo de Galois G.

cumple que $G \subseteq \mathrm{Aut}_{\mathbb{Z}} \overline{\mathbb{Z}}$, y además, $\overline{\mathbb{Z}}^G = \mathbb{Z}$.

Sea $\mathfrak{M}_{\mathfrak{y}} \subset \overline{\mathbb{Z}}$ y $(p) = \mathfrak{M}_{\mathfrak{y}} \cap \mathbb{Z}$. Tenemos la ext. finita de cps (hasta ahora)

$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \overline{\mathbb{Z}}/\mathfrak{M}_{\mathfrak{y}}$. De la Teoría General, $D = \{g \in G : g(\mathfrak{y}) = \mathfrak{y}\}$ (grupo de descomposición de $\mathfrak{y}$).

$D = \mathrm{Aut}_{\mathbb{Z}/p\mathbb{Z}} \overline{\mathbb{Z}}/\mathfrak{M}_{\mathfrak{y}} = \langle F \rangle$.

$g \longleftrightarrow \overline{g}(\overline{b}) = \overline{g(b)}$

Definimos: Llamaremos automorfismo de Frobenius de Σ en p al único F_p que se corresponde con F. Único ya que

$$\boxed{F_p(b) = b^p \pmod{\mathfrak{M}_{\mathfrak{y}}}} \qquad \forall b \in \overline{\mathbb{Z}}. \qquad F_p : \Sigma \longrightarrow \Sigma$$

¿Qué pasa si hubiéramos cogido otro ideal $\mathfrak{M}_{\mathfrak{y}'}$ tal que $\mathfrak{M}_{\mathfrak{y}'} \cap \mathbb{Z} = (p)$?

Proposición: El automorfismo de Frobenius de Σ en p es único, salvo conjugación.

Proposición: Dada $\mathbb{Q} \subset \Sigma' \subset \Sigma$ una $\mathbb{Q}$-subextensión, el mfi de Frobenius de Σ' en p es $F_p|_{\Sigma'}$.

Proposición: Sea $p(x) \in \mathbb{Z}[x]$ un pol separable (i.e., sin raíces múltiples), y sea $p \in \mathbb{Z}$ tal que $\overline{p(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ sea separable. Sean $\alpha_1 \dots \alpha_n$ las raíces de $p(x)$. Si $\mathbb{Z} \xhookrightarrow{i} \mathbb{Z}[\alpha_1 \dots \alpha_n]$, entonces la cpl que $x = (p)$ no es un punto ramificado de i^*.

Definimos: Sea $p(x) \in \mathbb{Z}[x]$ como en la prop. Se llama automorfismo de Frobenius en p de $p(x)$ al automorfismo de Frobenius de $\mathbb{Q}[\alpha_1 \dots \alpha_n]$ cuerpo de descomp. del pol, y lo denotamos como F_p.

"F_p es la permutación de $\alpha_1 \dots \alpha_n$ tal que la congruencia permutación de $\overline{\alpha_1}, \dots \overline{\alpha_n} \in \frac{\mathbb{Z}[\alpha_1 \dots \alpha_n]}{\mathfrak{M}_{\mathfrak{y}}}$ coincide con el mfi elevar a p."

Teorema (Aplicaciones del Teorema de Frobenius):

1) $\mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}[e^{\frac{2\pi i}{n}}]\right) = (\mathbb{Z}/n\mathbb{Z})^*$.

2) Existen pol. con coef enteros irreducibles que no lo son módulo cualquier primo

3) (Ley de reciprocidad cuadrática de Gauss). Dado $q \neq 2$ primo y $n \in \mathbb{Z}$, ¿cuándo $x^2 - n$ tiene raíces mod q (i.e. $\overline{x^2-n} \in \mathbb{F}_q$)?

Def: Dado $q \neq 2$ primo y $n \in \mathbb{Z}$ primo con q, se llama **símbolo de Legendre** a

$$\left(\frac{n}{q}\right) := \begin{cases} 1, & \text{si } n \text{ es un cuadrado (mod } q) \iff n^{\frac{q-1}{2}} = 1 \pmod q \\ -1, & \text{si no} \iff n^{\frac{q-1}{2}} = -1 \pmod q. \end{cases}$$

Propiedades:

1) $\left(\frac{n+bq}{q}\right) = \left(\frac{n}{q}\right)$

2) $\left(\frac{n\cdot m}{q}\right) = \left(\frac{n}{q}\right)\cdot\left(\frac{m}{q}\right)$.

3) $\left(\frac{n}{q}\right) = n^{\frac{q-1}{2}} \pmod q$

La ley dice que, si p primo $< q$,

- $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)$, si $p \neq 2$

- $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$, si $p = 2$.

IV. INVARIANTES DE LOS ANILLOS DE NÚMEROS

Definición: Sea A una K-álgebra finita. Dado un dato $a \in A$, sea $A \xrightarrow{a^\circ} A$, que es una aplicación K-lineal entre K-EV. Si en ciertas bases (a_{ij}) es la matriz de a°, se llama **traza** de $a \in A$ a

$$\operatorname{tr} a := \operatorname{tr}(a^\circ) = \sum_{i=1}^{n} a_{ii}$$

... es bien conocido que no depende de la base.

Definición: Se llama **norma** de $a \in A$ a $N(a) := \det(a^\circ)$. Cumple que $N(ab) = N(a) \cdot N(b)$.

Definición: Se llama **métrica de la traza** a la aplicación K-bilineal

$$\begin{aligned} T_2 : A \times A &\longrightarrow K \\ (a, b) &\longmapsto T_2(a,b) := \operatorname{tr}(ab^\circ) \end{aligned}$$

• Sea A una K-álgebra finita cyclic, y Σ ext. de la que tenía: $A \otimes_K \Sigma = \Sigma \times \overset{n)}{\cdots} \times \Sigma$. De 3º sabemos que $\#\operatorname{Hom}_{K\text{-alg}}(A, \Sigma) = n$, con que sean $\{\sigma_1 \dots \sigma_n\}$. El isomorfismo anterior en cuanto es

$$\boxed{\begin{aligned} A \otimes_K \Sigma &\xrightarrow{\sim} \Sigma \times \cdots \times \Sigma \\ a \otimes \lambda &\longmapsto (\sigma_1(a)\lambda, \dots, \sigma_n(a)\cdot\lambda) \end{aligned}}$$

• Al cambiar el cuerpo base, la matriz de un endo no varía (es una ap. lin. $\mathbb{R}^n \to \mathbb{R}^n$ pensada $\mathbb{C}^n \to \mathbb{C}^n$), de modo que **la traza y la norma son invariantes por cambio de base.** En cuanto, los endomorfismos tienen la misma matriz:

$$\begin{array}{ccc} A & \xrightarrow{a^\circ} & A \\ \downarrow & & \downarrow \\ A \otimes_K \Sigma & \xrightarrow{(a\otimes 1)^\circ} & A \otimes_K \Sigma \\ \| & & \| \\ \Sigma^n & \xrightarrow{(\sigma_1(a), \dots, \sigma_n(a))^\circ} & \Sigma^n \end{array} \qquad \text{de matriz} \quad \begin{pmatrix} \sigma_1(a) & & \\ & \ddots & \\ & & \sigma_n(a) \end{pmatrix}$$

En particular, será

$$\operatorname{tr} a = \sum_{i=1}^{n} \sigma_i(a) \qquad , \qquad N(a) = \prod_{i=1}^{n} \sigma_i(a).$$

Además, T_2 es no singular, pq en la base estándar de $\mathbb{E}^n$ la otra es $T_2 = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$.

Proposición: Sea $A = \mathcal{O}_K$ un anillo de números enteros, $\mathcal{O}_K$ en $\mathbb{Q} \hookrightarrow K$. Se cumple que tr, N de elementos de A son números enteros. En particular, la norma de $a \in \mathbb{Z}$ es de números enteros.

Proposición: Sea A un anillo de números. Entonces $|N(a)| = \left| \frac{A}{aA} \right|$.

Corolario: Sea $(a) = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$. Entonces $N(a) = \left| \frac{A}{\mathfrak{m}_{x_1}} \right|^{n_1} \cdots \left| \frac{A}{\mathfrak{m}_{x_r}} \right|^{n_r}$.

IDEALES CON POT NEGATIVA

Definición: Sea K un cuerpo de números y A el anillo de números enteros de K. Llamaremos **ideales fraccionarios** de K a los A-submódulos finito-generados.

Un anillo de núm A es intgo, noeth, de dim$_{\text{Krull}} = 1$ y normal, así que es Dedekind. Si $\mathfrak{m}_x$ es un ideal maximal, será $\mathfrak{m}_x \mathfrak{b}_x = (t) A_x$, donde necesariamente $(t) = \mathfrak{m}_x \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r}$.

Definición: Dado $n \geq 0$, llamaremos $\mathfrak{m}_x^{-n} := t^{-n} \mathfrak{m}_{x_1}^{n \cdot n_1} \cdots \mathfrak{m}_{x_r}^{n \cdot n_r} \subset K$, y es ideal fraccionario.

Proposición: La anterior definición no depende del generador de (t) elegido.

Teorema: Todo ideal fraccionario factoriza como producto de ideales primos con exponentes enteros, de modo único:

$$I = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r} \qquad , \qquad n_i \in \mathbb{Z}.$$

Prueba: En las pruebas anteriores se ve que si $\mathfrak{m}_x^{-n} = t^{-n} \mathfrak{m}_{x_1}^{n \cdot n_1} \cdots \mathfrak{m}_{x_r}^{n \cdot n_r}$ como antes, entonces localmente

$$(\mathfrak{m}_x^{-n})_y = \begin{cases} A_y & \text{si } y \neq x \\ t^{-n} A_x & \text{para } y = x. \end{cases}$$

Definición: Dado un ideal fraccionario $I = \mathfrak{m}_{x_1}^{n_1} \cdots \mathfrak{m}_{x_r}^{n_r} \subset \mathcal{O}_K$, $n_i \in \mathbb{Z}$, se llama norma de I a

$$N(I) := \left|\frac{A}{\mathfrak{m}_{x_1}}\right|^{n_1} \cdots \left|\frac{A}{\mathfrak{m}_{x_r}}\right|^{n_r}.$$

Proposición: Dado $I \subset A$, $N(I) = |A/I|$, y $N((a)\cdot(b)) = N((a)) \cdot N((b))$.

Proposición: $|N(f)| = N(f \cdot A)$, $f \in K$.

Teorema: Sean $I' \subseteq I$ ideales fraccionarios. Entonces

$$\boxed{\frac{N(I')}{N(I)} = \left|\frac{I}{I'}\right|}$$

DISCRIMINANTE

Definición: Sea K un cuerpo de números y A el anillo de números de K. Sean $\{a_1, \dots, a_n\}$ una base de A como $\mathbb{Z}$-módulo, que también es base de K como $\mathbb{Q}$-ev. La matriz de la métrica de la traza es $T_2 = (\mathrm{tr}(a_i \cdot a_j))$

Se llama **discriminante** de A a $\Delta_A := \det\left(\mathrm{tr}(a_i \cdot a_j)\right)$. No depende de la elección de la base. (Δ es el det de la métrica de la traza).

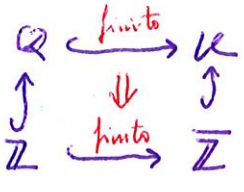
- ¿Cómo varía el discriminante si pasamos a un anillo de números más grande?

Teorema: Sea $A \subset A_1 \subset K$. Entonces

$$\boxed{\Delta_A = \left|\frac{A_1}{A}\right|^2 \cdot \Delta_{A_1}}$$

(i.e. Δ_{A_1} es más pequeño) En particular, $\Delta_A = \Delta_{A'} \iff A = A'$.

Teorema: Sea K un cuerpo de números. El anillo de números enteros de K es un anillo de números enteros.



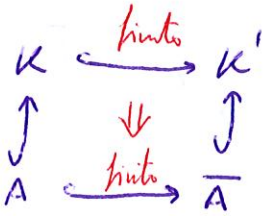
• ¿Cómo calcular el anillo de números de un cuerpo de núm?

Teorema Sea K un cuerpo de números, y $\{a_1, \dots a_n\}$ dentro enteros sobre $\mathbb{Z}$ que sean base de K como $\mathbb{Q}$-ev.

Sea $M = \mathbb{Z}a_1 + \dots + \mathbb{Z}a_n$.

Si M no es el anillo de números enteros de K, $\exists p$ primo : p^2 divide a Δ_M y $\exists\ 0 \le r_1, \dots, r_s < p$ en $\mathbb{N}$ ($s < n$) tal que $a := \frac{1}{p}(r_1 a_1 + \dots + r_s a_s + a_{s+1})$ es entero sobre $\mathbb{Z}$. Notar que $a \notin M$, y que $M_1 := \mathbb{Z}a_1 + \dots + \mathbb{Z}a_s + \mathbb{Z}a + \mathbb{Z}a_{s+2} + \dots + \mathbb{Z}a_n$ cyple que $\Delta_{M_1} = \frac{\Delta_M}{p^2}$.

Proposición Sea $K \hookrightarrow K'$ una ext. finita de cps, con K cpo de núm y A anillo de núm de K. Entonces, si $\overline{A}$ es el cierre entero de A en K', el mapa $A \hookrightarrow \overline{A}$ es finito.



Corolario Sea A un anillo de números. $y \in \mathrm{Spec}_{MAX} A$ ramificado $\Rightarrow y \in (\Delta_A)_0$.

Teorema (Cálculo del discriminante) Sea A un anillo de números de cuerpo de fracciones K.

1) (Caso complejo) Si $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$, entonces

$$\Delta_A = \left| \left(\sigma_i(a_j)\right) \right|^2$$

, $\{a_1, \dots a_n\}$ base

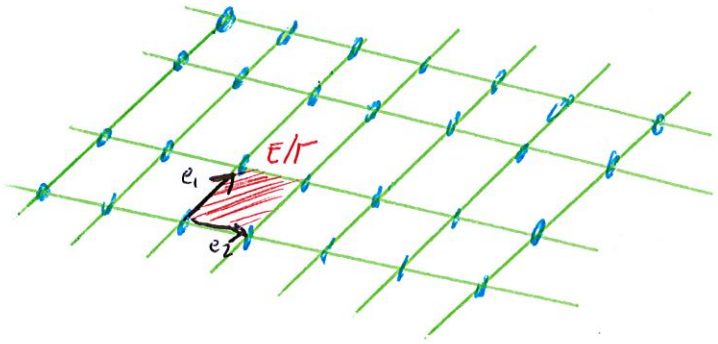
2) (Caso real) Si $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{C}) = \{\sigma_1, \dots \sigma_n\}$, con $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$, entonces

$$\Delta_A = (-4)^s \left| \left(\sigma_i(a_j)\right) \right|^2$$

Corolario: Sea $p(x) \in \mathbb{Z}[x]$ mónico irreducible, y $\alpha_1, \dots, \alpha_n$ las raíces de $p(x)$. Entonces

$$\Delta_{\mathbb{Z}[\alpha_1]} = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix} =: \Delta_{p(x)}$$

Definición: Sea E un K-EV y $\{e_1 \dots e_n\}$ base. Se llama red en E a $\Gamma := \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$; y se llama paralelepípedo asociado a Γ a E/Γ.



$\Gamma \equiv$ nodos.

Si A es un anillo de números, $A = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_n \hookrightarrow K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^{r+2s}$, así que puede ver como una red en $\mathbb{R}^{r+2s}$.

Definición: Si T es una métrica simétrica en E, el volumen de un paralelepípedo E/Γ, con $\Gamma = \bigoplus \mathbb{Z}e_i$, es

$$\mathrm{Vol}(E/\Gamma) := \sqrt{|\Delta_\Gamma|} = \sqrt{\left|\det(T(e_i, e_j))\right|}$$

y si $A \subset K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^n$ es un anillo de números,

$$\mathrm{Vol}(\mathbb{R}^n/A) = 2^s \left|\det(\sigma_i(a_j))\right| = 2^s \sqrt{|\Delta_A|}$$

Definición: Si $I \subset K$ es un ideal fraccionario, se define

$$\mathrm{Vol}\left(\frac{K \otimes_{\mathbb{Q}} \mathbb{R}}{I}\right) := \sqrt{|\Delta_I|}$$

Teorema: Sea $I \subset \mathcal{O}_K$ un ideal fraccionario. Entonces

$$N(I) = \frac{\sqrt{|\Delta_I|}}{\sqrt{|\Delta_{\mathcal{O}_K}|}} = \frac{\mathrm{Vol}\left(\frac{K \otimes_{\mathbb{Q}} \mathbb{R}}{I}\right)}{\sqrt{|\Delta_{\mathcal{O}_K}|}}.$$

V: VALORACIONES Y VALORES ABSOLUTOS

Defin: Sea Σ un cuerpo. Una **valoración real** es una aplicación $v: \Sigma - 0 \longrightarrow \mathbb{R}$ que verifica:

i) $v(f \cdot g) = v(f) + v(g)$

ii) $v(f+g) \geq \min\{v(f), v(g)\}$.

Se dice que la valoración v es **discreta** si $\operatorname{Im} v = \mathbb{Z}$, y **trivial** si $\operatorname{Im} v = 0$.

Lema: $v: (\Sigma^*, \cdot) \longrightarrow (\mathbb{R}, +)$ es un morfismo de grupos.

Proposición: Sea $\mathcal{O}$ un anillo íntegro local de maximal $\mathfrak{m}$ y cuerpo de fracciones Σ, con la siguiente propiedad:

$$\left.\begin{array}{l} f \in \mathfrak{m}^n - \mathfrak{m}^{n+1} \\ g \in \mathfrak{m}^m - \mathfrak{m}^{m+1} \end{array}\right\} \Rightarrow fg \in \mathfrak{m}^{n+m} - \mathfrak{m}^{n+m+1}$$

Entonces la aplicación

$$\begin{array}{rcl} v_{\mathfrak{m}}: \Sigma - 0 & \longrightarrow & \mathbb{Z} \subset \mathbb{R} \\ \frac{f}{g} & \xmapsto{\text{DEF}} & n - m \end{array}$$

es una valoración discreta, llamada valoración **$\mathfrak{m}$-ádica**.

Teorema: Sea $v: \Sigma - 0 \longrightarrow \mathbb{R}$ una valoración. El conjunto

$$\mathcal{O}_v := \{ f \in \Sigma : v(f) \geq 0 \}$$

es un anillo local de maximal

$$\mathfrak{R}_v := \{ f \in \Sigma : v(f) > 0 \},$$

de cuerpo de fracciones Σ, y de invertibles

$$\mathcal{O}_v^* = \{ f \in \Sigma : v(f) = 0 \}.$$

Más aún, si v es discreta, $\mathcal{O}_v$ es DIP y v es la valoración $\mathcal{P}_v$-ádica, $v = v_{\mathcal{P}_v}$.

Teorema: Existe una correspondencia biunívoca

$$\left\{ \begin{array}{c} \text{valoraciones discretas} \\ \text{de } \Sigma \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subanillos de } \Sigma \\ \text{locales, DIP, y de cuerpo de fracc. } \Sigma \end{array} \right\}.$$

$$v \longmapsto \mathcal{O}_v$$

$$v_m \longleftarrow (\mathcal{O}, m)$$

Definición: Dada una valoración $v : \Sigma^* \longrightarrow \mathbb{R}$, se dice que $\mathcal{O}_v$ es un anillo de valoración de Σ, y si v es discreta se dice que $\mathcal{O}_v$ es un anillo de valoración discreta.

Definición: Dos valoraciones $v, v' : \Sigma^* \longrightarrow \mathbb{R}$ se dicen equivalentes si existe $\alpha > 0$: $v' = \alpha \cdot v$.

Teorema: $v \equiv v' \iff \mathcal{O}_v = \mathcal{O}_{v'}$.

ANILLOS DE VALORACIÓN Y CIERRE ENTERO

Proposición: Todo anillo de valoración $\mathcal{O}_v$ es normal.

Proposición: "$\mathcal{O}_v$ no puede estar dominado por nadie":

Si $\mathcal{O}'$ es un subanillo local de Σ de maximal m', y

$\mathcal{O}_v \subset \mathcal{O}' \subset \Sigma$
$\cup \qquad \cup$
$\mathcal{P}_v \subset m'$

$\mathcal{O}_v \cap m' = \mathcal{P}_v$), entonces $\mathcal{O}_v = \mathcal{O}'$.

* **Teorema**: Sea K un cuerpo de números de anillo de números A. Se tiene la siguiente correspondencia:

$$\left\{ \begin{array}{c} \text{anillos de valoración} \\ \text{en } K \end{array} \right\} = \operatorname{Spec} A \quad \left(= \left\{ \begin{array}{c} \text{valoraciones reales} \\ \text{de } K \end{array} \right\} / \sim \right)$$

$$A_X \longleftarrow X \longrightarrow V_{m_X}$$

$$\mathcal{O}_{V_{m_X}} \longleftarrow X$$

Lema: Sea A un anillo íntegro de cuerpo de fracciones Σ. Entonces

$$A = \bigcap_{X \in \operatorname{Spec}_{pm} A} A_X .$$

Teorema: El anillo de números A de un cuerpo de números K es

$$A = \bigcap_{\substack{V \\ \text{valoración}}} \mathcal{O}_V .$$

Proposición: Sea $A = \dfrac{K[x_1, \dots x_n]}{I}$ un anillo de funciones algebraicas de una curva íntegra. Entonces

1) $$\left\{ \begin{array}{c} \text{anillos de valoración} \\ \text{de } \Sigma = A_{A \cdot 0} \end{array} \right\} = \operatorname{Spec} \overline{K[x]} \cup \operatorname{Spec} \overline{K\left[\tfrac{1}{x}\right]} .$$

2) $$\overline{A} = \bigcap_{\substack{A \subseteq \mathcal{O}_V \\ \text{anillo de valoración}}} \mathcal{O}_V .$$

VARIEDADES PROYECTIVAS

- Recordar $\mathbb{P}_n := \mathbb{P}(\Phi)$, y tiene coordenadas homogéneas $(x_0, x_1, \dots x_n)$. Además, elegido un hiperplano H, $\mathbb{P} - H = A = \mathbb{C}^n$. Si los H son los hiperplanos $\{x_i = 0\}$, $i = 0, \dots n$, y denotamos $\mathbb{C}^n_i = \mathbb{P}_n - \{x_i = 0\}$, (vía $\mathbb{C}^n_i \hookrightarrow \mathbb{P}_n$, $(a_1 \dots a_n) \longmapsto (a_1, \dots, \overset{i)}{1}, a_i, \dots a_n)$), pues se ve que $\mathbb{P}_n = \bigcup_{i=0}^{n} \mathbb{C}^n_i$.

- Para ver de dónde sale lo siguiente $\quad \mathbb{C}^n_0 \hookrightarrow \mathbb{P}_n \hookleftarrow \mathbb{C}^n_1$

$$(a_1 \dots a_n) \longmapsto (1, a_1 \dots a_n) \longmapsto \left(\frac{1}{a_1}, \frac{a_2}{a_1}, \dots, \frac{a_n}{a_1}\right)$$
$$\| \quad \left(\frac{1}{a_1}, 1, \frac{a_2}{a_1} \dots \frac{a_n}{a_1}\right)$$

- Si $A = \dfrac{k[x,y]}{(xy-1)} = k[\bar{x}, \bar{y}] \subset \Sigma = k(\bar{x}, \bar{y})$, otro "abierto afín" es $A' = k\left[\frac{1}{\bar{x}}, \frac{\bar{y}}{\bar{x}}\right]$, pues

y se ve que $A_{\bar{x}} = A'_{\frac{1}{\bar{x}}}$, luego $\quad \begin{matrix} \operatorname{Spec} A_{\bar{x}} \\ \| \\ \operatorname{Spec} A_{\frac{1}{\bar{x}}} \end{matrix} \subset \operatorname{Spec} A$.

La <u>variedad proyectiva</u> asociada a $\operatorname{Spec} k[x,y]$ será

$$X := \operatorname{Spec} k[\bar{x}, \bar{y}) \cup \operatorname{Spec} k\left[\frac{1}{\bar{x}}, \frac{\bar{y}}{\bar{x}}\right] \cup \operatorname{Spec} k\left[\frac{\bar{x}}{\bar{y}}, \frac{1}{\bar{y}}\right].$$

En general:

<u>Definición</u>: Sea $A = k[\xi_1 \dots \xi_n]$ una k-álgebra de tipo finito íntegra, y $\Sigma = k(\xi_1 \dots \xi_n)$ su cuerpo de fracciones. Si denotamos con $A_i := k\left[\frac{\xi_1}{\xi_i}, \dots, \frac{1}{\xi_i}, \dots, \frac{\xi_n}{\xi_i}\right]$, y $A_{ij} := (A_i)_{\xi_i/\xi_j} = (A_j)_{\xi_j/\xi_i}$, ($A = A_0$)

llamaremos <u>variedad proyectiva asociada a $\operatorname{Spec} A$</u> a

$$X := \bigcup_{i=0}^{n} \operatorname{Spec} A_i.$$

(la unión se entiende unión disjunta pero identificando ptos vía $\operatorname{Spec} A_{ij}$).

En el caso de curvas algebraicas, diremos que X es una <u>variedad de Riemann</u>.

Proposición: Sea $\mathcal{O}_v$ un anillo de valoración de Σ que contiene a K. Entonces $\mathcal{O}_v$ contiene algún A_i.

Como cada $A_i \subseteq \mathcal{O}_v \Rightarrow \overline{A_i}_x = \mathcal{O}_v$, y entonces

Definición: Se dice que $\overline{X} := \bigcup \operatorname{Spec} \overline{A_i}$ es la desingularización de X.

Teorema:

$$\left\{ \begin{array}{l} \text{anillos de valoración de } \Sigma \\ (\text{que contienen a } K) \end{array} \right\} = \overline{X}$$

$$\overline{A}_{i_x} \longleftrightarrow x = \overline{x}_i \in \operatorname{Spec} \overline{A_i} \, .$$

Definición: Sea $K = k(\xi_1 \dots \xi_n)$ una k-extensión de grado de trascendencia 1 (i.e. hay un cierto algebraicamente independiente, pero no dos). Dado $f \in K$ trascendente, $k(f) \hookrightarrow K$ es una ext. finita y se llama variedad de Riemann de K a $\left\{ \begin{array}{l} \text{anillos de val} \\ (\text{que contienen a } k \end{array} \right\}$.

Propuesta: La variedad de Riemann de K es $\operatorname{Spec} \overline{k(f)} \cup \operatorname{Spec} \overline{k\left(\frac{1}{f}\right)}$.

Definición: Sea X una variedad de Riemann. Se dice que $x \in X$ es un cero de $f \in K$ si $v_x(f) > 0$, y que $x \in X$ es un polo de f si $v_x(f) < 0$.

Definición: Llamamos grado de una valoración v a $\operatorname{gr} v := \dim \mathcal{O}_v / \mathcal{P}_v$.

Teorema: "El número de ceros de $f \in K$ es igual al número de polos".

Comprensión, sea K una k-extensión de tipo finito de grado de trascendencia 1, y X la variedad de Riemann asociada a K. Si $f \in K$, entonces

$$\boxed{\sum_{x \in X} v_x(f) \cdot \operatorname{gr} x = 0}$$

Teorema (Bézout): Dos curvas proyectivas planas de grados n y m, sin componentes comunes, se cortan en $n \cdot m$ puntos (contando grados y multiplicidades).

VALORES ABSOLUTOS

Definición: Un valor absoluto sobre un anillo A es una aplicación $|\cdot| : A \to \mathbb{R}$ tal que

i) $|a| \geq 0$, y $|a| = 0 \iff a = 0$.

ii) $|a \cdot b| = |a| \cdot |b|$

iii) $|a+b| \leq |a| + |b|$.

- En cuanto, $|1| = |-1| = 1$, y $|-a| = |a|$. Además, ii) dice que de haber un valor absoluto en A, debe ser íntegro.
- Todo valor absoluto se extiende a su cuerpo de fracciones de modo único: $\left|\frac{a}{b}\right| := \frac{|a|}{|b|}$.

Ejemplos: 1) En $\mathbb{Q}$, $|\cdot|_\infty$ es el valor absoluto usual.

2) En $\mathbb{Q}$: dado $p \in \mathbb{Z}$ primo, $\left|\frac{a}{b}\right|_p := e^{-v_p\left(\frac{a}{b}\right)}$.

3) En general: si v es una valoración sobre K, $|f|_v := e^{-v(f)}$.

Definición: Un valor absoluto se dice ultramétrico si cumple que $|f+g| \leq \max\{|f|, |g|\}$.

5) (hoja 2) son ultramétricos.

Definición: Sean A un anillo. Dos valores absolutos $|\cdot|$, $|\cdot|'$ se dicen equivalentes si existe $\alpha > 0$ tal que $|\cdot|' = |\cdot|^\alpha$.

Todo valor absoluto en A define una estructura de espacio métrico: $d(a,b) := |a-b|$.

Teorema: $|\cdot| \equiv |\cdot|' \iff$ definen la misma topología.

Teorema: Se tiene la siguiente correspondencia:

$$\left\{ \begin{array}{c} \text{valores absolutos} \\ \text{ultramétricos} \end{array} \right\}/\sim \quad \longleftrightarrow \quad \left\{ \begin{array}{c} \text{valoraciones} \\ \text{reales} \end{array} \right\}/\sim$$

$$|\cdot| := e^{-v(\cdot)} \longleftarrow v$$

$$|\cdot| \longmapsto v(\cdot) := -\ln|\cdot| .$$

Definición: Se dice que un valor absoluto $|\cdot| : A \to \mathbb{R}$ es arquimediano si $\{|n|\}_{n \in \mathbb{N}}$ no está acotado. En caso contrario diremos que es no arquimediano.

Teorema: Sea $|\cdot|$ un valor absoluto.

$$|\cdot| \text{ ultramétrico} \iff |\cdot| \text{ no arquimediano.}$$

Teorema: Sea $|\cdot|$ un valor absoluto.

$$|\cdot| \text{ arquimediano} \iff |n| > 1 \quad \forall n \in \mathbb{N},\ n > 1.$$

Teorema (Primer teorema de Ostrowski): Todo valor absoluto arquimediano sobre $\mathbb{Q}$ es equivalente al valor absoluto usual.

VALORES ABSOLUTOS EN LA TEORÍA DE NÚMEROS

Teorema: Sea K un cuerpo de números.

$$\left\{ \begin{array}{c} \text{valores absolutos arquimedianos} \\ \text{sobre } K \end{array} \right\} / \sim \quad \longrightarrow \quad \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{C}) \,/\, \text{conjugación}$$

$$|\cdot|_\sigma \longleftarrow [\sigma]$$

con $|a|_\sigma := |\sigma(a)| = |\lambda + \mu i| = \sqrt{\lambda^2 + \mu^2}$.

Corolario: Sea K un cuerpo de números, de orden de unos n.

$$\left\{ \begin{array}{c} \text{valores absolutos} \\ \text{de } K \end{array} \right\} / \sim \quad = \quad \left\{ \begin{array}{c} \text{valores absolutos} \\ \text{arquimedianos sobre} \\ K \end{array} \right\} / \sim \quad \amalg \quad \left\{ \begin{array}{c} \text{valores absolutos} \\ \text{no arquimedianos} \\ \text{sobre } K \end{array} \right\} / \sim$$

$$\| \qquad\qquad\qquad\qquad\qquad\qquad \| \qquad\qquad\qquad\qquad\qquad\qquad \|$$

$$\mathrm{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R}) \qquad\qquad\qquad\qquad\qquad\qquad \mathrm{Spec}\, A$$

luego

$$\overline{X} = X_\infty \amalg X$$

PRODUCTO DE VALORES ABSOLUTOS

Propos. Sea $\overline{X}$ una variedad de Riemann de cuerpo de funciones K, y $f \in K$. Entonces

$$\prod_{x \in \overline{X}} |f|_x^{gr\, x} = 1$$

· Esto también pasa en cuerpos de números:

Teorema: Sea K un cuerpo de números y $f \in K$.

$$\prod_{x \in \overline{X}} |f|_x^{gr\, x} = 1$$

y además: $\overline{X} = \{ \text{val. abs. de } K \} / \sim \; = X_\infty \amalg \operatorname{Spec} A$, donde aquí,

$x \in \operatorname{Spec} A$, $gr\, x := \ln \left| \frac{A}{m_x} \right|$,

$x \in X_\infty$, $gr\, x := \dim_{\mathbb{R}} \frac{K \otimes_K \mathbb{R}}{m_x}$ $(= 1 \text{ ó } 2)$.

VI. TEOREMAS DE LA TEORÍA DE NÚMEROS

• En adelante A será un dominio de Dedekind al menos.

Definición: Se llama *divisor afín* de $\operatorname{Spec} A$ a una suma formal $D = n_1 x_1 + \cdots + n_r x_r$, con $n_i \in \mathbb{Z}$ y $x_i \in \operatorname{Spec}_{max} A$.

Definición: Sea $K = A_{A-0}$, y $f \in K$. Se llama *divisor principal asociado a* f a

$$D(f) := \sum_{x \in \operatorname{Spec}_{max} A} v_x(f) \cdot x$$

• Los divisores se pueden sumar, $D + D' = \sum (n_i + n_i') x$, y para los principales $D(f \cdot g) = D(f) + D(g)$.

• Denotaremos como $\operatorname{Div}(A)$ al conjunto de divisores formales, es, al conjunto de sumas formales finitas y por haber,

$$\operatorname{Div}(A) = \bigoplus_{x \in \operatorname{Spec}_{max} A} \mathbb{Z} \cdot x$$

y por $\operatorname{DivPrinc}(A)$ al subgrupo formado por los divisores principales.

Definición. Se llama *grupo de Picard* al cociente

$$\operatorname{Pic}(A) := \frac{\operatorname{Div}(A)}{\operatorname{Div Princ}(A)},$$

es, $[D] = [D'] \iff D' = D + D(f)$ para cierto $f \in K$.

Definición: Dados $D = \sum n_i x_i$, $D' = \sum n_i' x_i$, diremos que $D \geq D'$ si $n_i \geq n_i'$ $\forall i$. Diremos que D es un *divisor efectivo* si $D \geq 0$, es, si $n_i \geq 0$ $\forall i$.

Proposición: Se tiene la siguiente correspondencia biunívoca:

$$\left\{\text{divisores efectivos}\right\} \longleftrightarrow \left\{\text{ideales de } A\right\}$$

$$\cap \qquad\qquad\qquad \cap$$

$$\mathrm{Div}(A) \longleftrightarrow \left\{\text{ideales fracionarios de } A\right\}$$

$$D = \sum n_i x_i \longmapsto I_D = \prod \mathfrak{m}_{x_i}^{n_i}.$$

Lema: dos ideales fracionarios I, I' son isomorfos (como A-módulos) $\Leftrightarrow$ el isomorfismo es $I \xrightarrow{f\cdot} I'$, con $f \in K$.

Teorema: Se cumple que $\mathrm{Pic}(A) \longleftrightarrow \left\{\text{ideales fraccionarios de } A\right\}/\text{isomorfismo}$.

Teorema: Para generar $\mathrm{Pic}(A)$ basta elegir los ideales de A, i.e., los divisores efectivos.

$$\mathrm{Pic}(A) \longleftrightarrow \left\{\text{divisores efectivos}\right\}/\sim \longleftrightarrow \left\{\text{ideales de } A\right\}/\sim$$

Definición: Se llama **grado** al mapa de grupos $\mathrm{gr} : \mathrm{Div}(A) \longrightarrow \mathbb{R}$, $\mathrm{gr}(D = \sum n_i x_i) := \sum n_i \,\mathrm{gr}\, x_i$.

El grado, si vemos $\mathrm{Div}A$ como ideales fracs, es la norma (cont):

$$\begin{array}{ccc} \mathrm{Div}(A) & \xrightarrow{\mathrm{gr}} & \mathbb{R} \\ \| & & \| e^x \\ \text{id. fracs} & \xrightarrow{N} & \mathbb{R}^+ \end{array}$$

DIVISORES EN LA TEORÍA DE NÚMEROSSSS

• Sea K un cuerpo de números de anillo de números A, y $X := \mathrm{Spec}_{mx} A$, la parte finita, y

$X_\infty := \mathrm{Spec}\,(K \otimes_{\mathbb{Q}} \mathbb{R})$ la parte del infinito y $\overline{X} := X \amalg X_\infty$.

Defini: Se llama divisor completo a los sumas formales finitas

$$\overline{D} = \overbrace{\sum_{x \in X} n_x\, x}^{\overline{D}_{|X}} + \overbrace{\sum_{y \in X_\infty} \lambda_y\, y}^{\overline{D}_\infty}, \qquad n_x \in \mathbb{Z},\ \lambda_y \in \mathbb{R},$$

parte afín — parte del infinito

y llamamos $\mathrm{Div}(\overline{X})$ al conjunto de div. completos, que con la suma es grupo abeliano.

Defini: Diremos que $\overline{D} \geq \overline{D}'$ si $n_x \geq n_x'$ y $\lambda_y \geq \lambda_y'$.

Defini: Se llama divisor principal completo asociado a $f \in K^\times$

$$\overline{D}(f) := \sum_{x \in X} v_x(f) \cdot x + \sum_{y \in X_\infty} v_y(f) \cdot y,$$

donde se entiende $v_y(f) := -\log |f|_y$ (pues X_∞ son v.a. arquimedianas).

• $\overline{D}(fg) = \overline{D}(f) + \overline{D}(g)$, y $\overline{D}(f^{-1}) = -\overline{D}(f)$.

• Análogamente llamamos $\mathrm{DivPrinc}(\overline{X}) \subseteq \mathrm{Div}(\overline{X})$ a los div. princ. completos, y

Defini: Se llama grupo de Picard completo a

$$\mathrm{Pic}(\overline{X}) = \frac{\mathrm{Div}(\overline{X})}{\mathrm{DivPrinc}(\overline{X})}.$$

Defini: Se llama grado de $\overline{D} = \sum_{x \in X} n_x\, x + \sum_{y \in X_\infty} \lambda_y\, y$ a $\mathrm{gr}\,\overline{D} := \sum n_x \,\mathrm{gr}\, x + \sum \lambda_y \,\mathrm{gr}\, y$.

Proposición: $\mathrm{gr}\,\overline{D}(f) = 0$.

TEOREMA DE RIEMANN-ROCH DÉBIL

Definición: Fijemos $\overline{D} \in \mathrm{Div}(\overline{X})$. Llamamos $\overline{I}_{\overline{D}} := \{f \in K : \overline{D}(f) \geq \overline{D}\}$.

- Si $\overline{D} = \sum n_x x + \sum \lambda_y y$, etc. $\quad \overline{I}_{\overline{D}} = \left(\prod M_{x_i}^{n_i}\right) \cap \left\{ (\mu_1 \dots \mu_{r+s}) \in \mathbb{R}^{*r} \times \mathbb{C}^s : \begin{array}{l} \\ |\mu_i| \leq e^{\lambda_{y_i}} \end{array} \right\}$,

que son unos cuantos puntos de una red.

Proposición (Propiedades):

1) $\overline{D}' = \overline{D} + \overline{D}(g) \Rightarrow \overline{I}_{\overline{D}'} = g \cdot \overline{I}_{\overline{D}} \overset{\delta}{\simeq} \overline{I}_{\overline{D}}$.

2) $|\overline{I}_{\overline{D}}| < \infty$

3) $\overline{I}_0 = \mu_K = \{$raíces n-ésimas de la unidad contenidas en $K\}$

4) $\left(\overline{I}_{-\overline{D}} - 0\right) / \mu_K := \{$Divisores completos efectivos equivalentes a $\overline{D}\}$.

5) $\mathrm{gr}\,\overline{D} < 0 \Rightarrow \overline{I}_{-\overline{D}} = 0$.

6) $\mathrm{gr}\,\overline{D} = 0$, $\overline{I}_{-\overline{D}} \neq 0 \Rightarrow \exists f \in K : \overline{D} = \overline{D}(f)$.

Teorema (del punto de la red de Minkowski): Sea E un $\mathbb{R}$-EV de dim d, y T_2 una métrica no singular. Sea $\Gamma \subset E$ una red y C un compacto convexo simétrico resp. al origen. Entonces

$$\mathrm{Vol}(C) \geq 2^d \mathrm{Vol}(E/\Gamma) \Rightarrow \exists\, 0 \neq e \in \Gamma : e \in C.$$

Teorema (Riemann-Roch débil): Sea $\overline{D}$ un divisor completo y $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$, K cuerpo de números. Si

$$\mathrm{gr}\,\overline{D} \geq \ln \sqrt{|\Delta_K|} - s \cdot \ln \frac{\pi}{2},$$

entonces $\overline{D}$ es equivalente a un divisor completo efectivo.

Corolario: Todo divisor afín es infinito equivalente a un divisor afín efectivo de grado $\leq \ln \sqrt{|\Delta_K|}$.

Proposición: Sea K un cuerpo de números de anillo de enteros A. Si todo ideal primo $\mathfrak{p} \neq (0)$ de A tal que $|A/\mathfrak{p}| \leq \sqrt{|\Delta_K|}$ es principal, $\Rightarrow A$ es DIP.

Defini: Sea K un cuerpo de núms de anillo de núms A, y $\mathfrak{P}_x \subset A$ un ideal prim. Se llama grado de $\mathfrak{P}_x$ sobre $\mathbb{Z}$ a

$$gr_{\mathbb{Z}}\, x := l_{\mathbb{Z}}\left(A/\mathfrak{P}_x\right) = l_{\mathbb{Z}/p\mathbb{Z}}\left(A/\mathfrak{P}_x\right) = \dim_{\mathbb{Z}/p\mathbb{Z}}\left(A/\mathfrak{P}_x\right).$$

donde $p : (p) = \mathfrak{P}_x \cap A$ núm

$gr_{\mathbb{Z}}\, x = 1 \Leftrightarrow A/\mathfrak{P}_x = \mathbb{Z}/p\mathbb{Z}$.

Definición: Dadas dos funs $f, g : (1,\infty) \longrightarrow \mathbb{R}$ continuas, establecen la siguiente rel. de eq.:

$$f \sim g :\Leftrightarrow \lim_{x\to 1} \frac{f(x)}{g(x)} = cte \neq 0.$$

$\zeta_K \sim \frac{1}{x-1}$, pues $\lim_{x\to 1} (x-1)\cdot\zeta(x) = V$.

Teorema:

$$\boxed{\zeta_K(x) \sim \prod_{gr_{\mathbb{Z}}\, \mathfrak{P} = 1} \left(1 - \frac{1}{N(\mathfrak{P})^x}\right)^{-1}}$$

Teorema: El núms de ideales prims de grado 1 sobre $\mathbb{Z}$ de un cuerpo de números es infinito. (not: en su anillo de núms)

Corolario: Dado $n \in \mathbb{N}$ fijo, en $\{1 + m\cdot n\}_{m\in\mathbb{N}}$ hay infinitos primos.

Proposición: Sea $p(x) \in \mathbb{Z}[x]$. Existen infinitos primos p tales que $\overline{p(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ tiene todas las raíces en $\mathbb{Z}/p\mathbb{Z}$.

Lema: Sea

$$\left.\begin{aligned} p_1(x_1 \dots x_n) &= 0 \\ &\vdots \\ p_r(x_1 \dots x_n) &= 0 \end{aligned}\right\} (*) \text{ un sistema de ecuaciones algebraicas diofánticas.}$$

El sistema tiene alguna real. compleja $\Longleftrightarrow$ tiene alguna solución $\mathbb{Q}$-algebraica.

Teorema: El sistema $(*)$ tiene alguna solución compleja $\Leftrightarrow$ tiene soluciones modulares (ie, en $\mathbb{Z}/p\mathbb{Z}$) para infinitos primos p.

Teorema: $\{$ valoraciones discretas de Σ $\}$ $=$ $\{$ subanillos de Σ locales DIP de cuerpo de fracc. Σ $\}$

$$v \longmapsto \mathcal{O}_v$$
$$v_m \longleftarrow (\mathcal{O}, m)$$

Teorema: En un cuerpo de núm., mod eq., todas las valoraciones son las m-ádicas:

$\{$ anillos de enteros en K $\}$ $=$ $\operatorname{Spec} A$ $=$ $\{$ valoraciones reales de K $\}/\sim$

$$A_x \longleftarrow x \longrightarrow v_x$$

Teorema: $\{$ v.a. ultramétricas $\}/\sim$ $=$ $\{$ valoraciones reales $\}/\sim$

$$|\cdot| \longmapsto v = -\ln|\cdot|$$
$$e^{-v(\cdot)} \longleftarrow v$$

Teorema: Sea K un cuerpo de núm. de anillo de enteros A.

$\{$ valores absolutos de K $\}/\sim$ $=$ $\{$ val. abs. arquimedianas $\}/\sim$ $\amalg$ $\{$ val. abs. no arq. $\}/\sim$

$\{$ val. abs. arquimedianas $\}/\sim$ $=$ $\operatorname{Spec}(K \otimes_{\mathbb{Q}} \mathbb{R})$

$\{$ val. abs. no arq. $\}/\sim$ $=$ $\{$ v.a. ultrametricas $\}/\sim$ $=$ $\{$ valoraciones reales $\}/\sim$ $=$ $\{$ anillos de valoración $\}$ $=$ $\operatorname{Spec} A$.

$$\overline{X} = X_\infty \amalg X$$