Def: un retículo $L \subset \mathbb{R}^N$ es un $\mathbb{Z}$-mod. f.g., digamos

$L = \langle v_1, \dots, v_r \rangle_{\mathbb{Z}}$ t.f. $\{v_1, \dots, v_r\}$ son $\mathbb{R}$-l.i.

$\uparrow$
rango de L.

Existe $\sim \langle 1, \sqrt{2} \rangle_{\mathbb{Z}}$ (no es retículo en $\mathbb{R}$).

Obs: en algunas referencias piden además $r = N$. ⊛

Dado $L \subset \mathbb{R}^N$, $L \otimes_{\mathbb{Z}} \mathbb{R} = \langle v_1, \dots, v_r \rangle_{\mathbb{R}} = V \subset \mathbb{R}^N$

L es retículo ⊛ en V.

Obs: si $L \subset \mathbb{R}^N$ retículo $\Rightarrow$ rango$(L) \leq N$.

Lema 1: si $L \subset \mathbb{R}^N$ $\mathbb{Z}$-módulo t.f. $L \cap U$ es finito para todo $U \subset \mathbb{R}^N$ acotado $\Rightarrow L$ es un retículo.

Demo: sea $\Lambda \subset L$ un retículo de rango máximo.

$\Lambda = \langle v_1, \dots, v_r \rangle_{\mathbb{Z}}$, $\{v_1, \dots, v_r\}$ son $\mathbb{R}$-l.i.

Si $V = \langle v_1, \dots, v_r \rangle_{\mathbb{R}} \subset \mathbb{R}^N$, $L \subset V$; sino, $\exists w \in L \setminus V$

$\Rightarrow \{v_1, \dots, v_r, w\}$ son l.i. ($a_1 v_1 + \dots + a_r v_r = bw$

$\Rightarrow$ $\rightsquigarrow b = 0 \Rightarrow a_i = 0$ pues $\{v_1, \dots, v_r\}$ son l.i.
$\rightsquigarrow b \neq 0 \Rightarrow w \in \langle v_1, \dots, v_r \rangle_{\mathbb{R}} \subset V$ Abs!)

$\Rightarrow$ $\langle v_1, \dots, v_r, w \rangle_{\mathbb{Z}}$ es un retículo de rango mayor que el rango de Λ ¡Abs!.

Cambiando $\mathbb{R}^N$ por V, supongamos que Λ genera todo mi espacio vectorial. Sea Π un dominio fundamental para Λ.

Recordar: si $v \in V$, $\exists\, l \in \Lambda$ t.q. $v - l \in \Pi$. (acotado)

$L/\Lambda \subset \Pi$ (elegimos representantes en Π, son únicos). son elementos en $L \cap \Pi$ = finito. (acotado)

$\rightsquigarrow$ L es f.g. (además es libre) y es un retículo. ($L \subset \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$)

L/Λ es un grupo abeliano finito, si $w \in L$

$\exists\, n \mid n \cdot w \in \Lambda \Rightarrow w \in \frac{\Lambda}{n}$. ∎

Recordar: $\psi : K \longrightarrow \mathbb{R}^{r+2s}$

$$\alpha \to (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \dots)$$

$\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R}) = \{\sigma_1, \dots, \sigma_r\}$, $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_r, \tau_1, \dots, \tau_s, \bar{\tau}_1, \dots, \bar{\tau}_s\}$

$$\log : (\mathbb{R}^X)^{r+2s} \longrightarrow \mathbb{R}^{r+1}$$

$$(x_1, \dots, x_{n+1}) \longrightarrow (\log|x_1|, \dots, \log|x_r|, \log(x_{r+1}^2 + x_{r+1}^2), \dots)$$

Luego ψ

$$\widetilde{\log}: K^\times \longrightarrow \mathbb{R}^{r+1}$$

Miramos la restricción a $\mathcal{O}_K^\times$. $\widetilde{\log}(\mathcal{O}_K^\times) \subset \{x_1 + \dots + x_{r+1} = 0\}$

$N(\widetilde{\log}) = U$ (finito e igual a K_n {raíces de 1})

$V = \widetilde{\log}(\mathcal{O}_K^\times) \Rightarrow \mathcal{O}_K^\times = U \times V$ (V libre de rango $r+1-1$.)

Si $W \subset \mathbb{R}^{r+1}$ acotado $\Rightarrow \widetilde{\log}(\mathcal{O}_K^\times) \cap W$ es finito.

Luego por el Lema, V es un retículo en $H = \{x_1 + \dots + x_{r+1} = 0\}$

con $\text{rango}(V) \leq r+1-1$. Falta ver la otra desigualdad.

Notación: $\alpha \in \mathcal{O}_K^\times$, $\widetilde{\log}(\alpha) = (\widetilde{\log}(\alpha)_1, \dots, \widetilde{\log}(\alpha)_{r+1})$

Lema 2: Fijado $1 \leq k \leq r+1$, dado $\alpha \in \mathcal{O}_K$, $\exists \beta \in \mathcal{O}_K$ t.q.:

- $|N_m(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc}(\mathcal{O}_K)|}$
- $\widetilde{\log}(\beta)_i < \widetilde{\log}(\alpha)_i \quad \forall i \neq k$.

D/ (Minkowski): $E = \{(x_1, \dots, x_n) : |x_1| \leq c_1, \dots, |x_r| \leq c_r,$
$x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \dots, x_{n-1}^2 + x_n^2 \leq c_{r+s}\}$

$n = r+2s$

Donde: $\cdot\ 0 < c_i < e^{\widetilde{\log}(\alpha)_i}$ si $i \neq k$.

$\cdot c_1 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|\mathrm{disc}(K)|}$

$\mathrm{Vol}(E) = 2^r \cdot c_1 \cdots c_r \cdot \pi^s \cdot c_{r+1} \cdots c_{r+s} = 2^{r+s} \sqrt{|\mathrm{disc}(K)|}$

Vimos: $\mathrm{Vol}(\psi(\mathcal{O}_K)) = \mathrm{Vol}\left(\mathbb{R}^n / \psi(\mathcal{O}_K)\right) = \frac{1}{2^s} \cdot \sqrt{|\mathrm{disc}(K)|}$

$\Rightarrow \mathrm{Vol}(E) = 2^n \cdot \mathrm{Vol}(\psi(\mathcal{O}_K))$ (hipótesis de Minkowski)

Como E es compacto, $\exists\, \beta \in \psi(\mathcal{O}_K) \cap E$ no nulo.

Ver que es el buscado ☐

Lema 3: dado $1 \le k \le r+s$, $\exists\, \mu_k \in \mathcal{O}_K^\times$ t.q.

$\tilde{\log}(\mu_k)_i < 0$ si $i \neq k$.

D/ Sea $\alpha_1 \in \mathcal{O}_K$ no nulo cualquiera. Aplicando el lema anterior, $\exists\, \alpha_2$ / $|\mathrm{Nm}(\alpha_2)| \le M$ y $\tilde{\log}(\alpha_2)_i < \tilde{\log}(\alpha_1)_i$ si $i \neq k$

Dado α_2, $\exists\, \alpha_3$ / $|\mathrm{Nm}(\alpha_3)| \le M$ y ....

... $\rightsquigarrow \{\alpha_n\} \subset \mathcal{O}_K$, $|\mathrm{Nm}(\alpha_i)| \le M$.

Luego $(\alpha_1), (\alpha_2), \ldots, (\alpha_n), \ldots$ son ideales de norma $\le M$ todos. Pero hay finitos ideales de norma acotada. $\Rightarrow (\alpha_i) = (\alpha_j)$, algunos $i \neq j$.

$\Rightarrow \exists\, u_\ell$ unidad t.q. $d_i = u_\ell\, d_j$. Pero

$$\widetilde{\log}(d_i)_r = \widetilde{\log}(u_\ell)_r + \widetilde{\log}(d_j)_r < \widetilde{\log}(d_j)_r$$

$$\Rightarrow \widetilde{\log}(u_\ell)_r < 0 \quad \forall r \neq \ell \qquad \square$$

Así, construimos $\{u_1, \dots, u_{r+1}\}$ tales que,

$$\begin{pmatrix} \widetilde{\log}(u_1) & \widetilde{\log}(u_2) & \cdots & \widetilde{\log}(u_{r+1}) \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} = A \in \mathcal{M}_{(r+1)\times(r+1)}(\mathbb{R})$$

que cumple: • $(A_{ij}) < 0$ si $i \neq j$.

• La suma de los elts de cada columna es 0.

Lema 4: A tiene rango $r+1-1$.

D/ Claramente no puede tener rango mayor ($A^t \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow$ tiene núcleo).

Veamos que las primeras $(r+1-1)$-filas son l.i.

Si: $\boxed{\sum_{i=1}^{r+1-1} \lambda_i F_i = \vec{0}}$, $\lambda_i \in \mathbb{R}$. Podemos suponer que $\lambda_i \leq 1$, $\lambda_\ell = 1$ (algún).

Miremos en la combinación lineal, la coordenada k.

$$\textcircled{\downarrow} \quad 0 = \sum_{i=1}^{r+s-1} \lambda_i \overbrace{(\tilde{\log}_p(u_k)_i}^{<0 \text{ si } i \neq k} > \sum_{i=1}^{r+s-1} \tilde{\log}_p(u_k)_i >$$

$$\sum_{i=1}^{r+s} \tilde{\log}_p(u_k)_i = 0 \qquad \underline{\text{Abs!}} \qquad \square$$

$\Rightarrow$ $V = \tilde{\log}_p(U_K)$ es un retículo de rango $r+s-1$

y terminamos la demostración de Dirichlet. $\square$

Números p-ádicos

Sea $p \in \mathbb{N}$ un número primo. Definimos una valuación,

$$v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{Z} \text{ por}$$

$$v_p(a) = \max \{ i \in \mathbb{N} \cup \{0\} : p^i \mid a \}$$

$v_p(a)$ es el exponente de p en la factorización de a.

Def: una valuación discreta, es una función $v : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}$ que cumple:

1. $v(a \cdot b) = v(a) + v(b)$
2. $v(a+b) \geq \min \{v(a), v(b)\}$; vale la igualdad si $v(a) \neq v(b)$

Ejemplos: orden de anulación de $p(x) \in \mathbb{R}[x]$ en 0.

Afirmo: v_p es una valuación.

Propiedad 1 es elemental, y para 2, si $p^r \mid a$ y $p^r \mid b \Rightarrow$ $p^r \mid a+b$. ∎

Podemos extender $v_p: \mathbb{Q}(\{0\}) \to \mathbb{Z}$, por $v_p\left(\frac{a}{b}\right) =$

$= v_p(a) - v_p(b)$.

Ejercicio: la extensión sigue cumpliendo 1) y 2).

Obs: en la bibliografía se suele definir $v_p(0) = +\infty$.

A partir de una valuación, podemos construir un valor absoluto.

$$c = \frac{1}{p}$$

Def: sea $0 < c < 1$, definimos el valor absoluto en $\mathbb{Q}$:

$$|a|_p = \begin{cases} 0 & \text{si } a = 0 \\ c^{v_p(a)} & \text{si } a \neq 0. \end{cases}$$

Lema: $|\ |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ es un valor absoluto. Más aún,

$|a+b|_p \leq \max\{|a|_p, |b|_p\}$. (ultramétrica).

D/ Claramente $|a|_p \geq 0$ y $|a|_p = 0 \Leftrightarrow a = 0$.

$|a+b|_p = c^{v_p(a+b)}$

$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

La función c^x es decreciente pues $0 < c < 1$

$$\Rightarrow c^{v_p(a+b)} \leq c^{\min\{v_p(a), v_p(b)\}} = \max\{c^{v_p(a)}, c^{v_p(b)}\}$$

$$c^{v_p(a\cdot b)} = c^{v_p(a)+v_p(b)} \qquad \max\{|a|_p, |b|_p\}$$

Obs: $|a\cdot b|_p = |a|_p \cdot |b|_p$

Ultramétrica $\Rightarrow$ desigualdad triangular.

Notar que $\{p^n\}_{n\in\mathbb{N}} \longrightarrow 0$ con $|\ |_p$, pues

$$|p^n|_p = \left(\frac{1}{p}\right)^n \xrightarrow[n\to\infty]{} 0 \quad \text{(v.a. chico} \rightsquigarrow \text{muy divisible por } p\text{)}.$$

Obs: $\mathbb{Z} \subset \{x\in\mathbb{Q} : |x|_p \leq 1\}$, $v_p(a) \geq 0 \Rightarrow |a|_p = \left(\frac{1}{p}\right)^{\geq 0} \leq 1$. $\quad a \in \mathbb{Z}\setminus\{0\}$

Los números con v.a. grande (p-ádico) son aquellos cuyo denominador es muy divisible por p.

$$\left|\frac{1}{p^n}\right|_p = \underbrace{\left(|p^n|_p\right)^{-1}}_{\frac{1}{p^n}} = p^n$$

Teniendo un valor absoluto, podemos medir distancias:

$$d_p(a,b) = |a-b|_p$$

Pregunta: ¿cómo se construye $\mathbb{R}$? $\rightsquigarrow$ sucesiones de

Cauchy. $\mathbb{R} = \{\text{Sucesiones } (a_n) \subset \mathbb{Q} \text{ de Cauchy}\}/\sim$

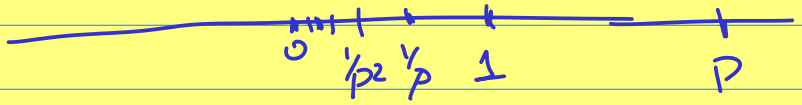
def: $\{a_n\} \sim \{b_n\} \iff \{a_n - b_n\} \to 0$

- es de equivalencia.
- el valor absoluto se extiende a $\mathbb{R}$ y es completo.
- $\mathbb{R}$ es un cuerpo.

Podemos hacer la misma construcción mirando el valor absoluto p-ádico en lugar del usual.

Def: $\mathbb{Q}_p$ = completación de $\mathbb{Q}$ con respecto al valor absoluto p-ádico. Es un cuerpo completo.

Notar que, $|\ |_p : \mathbb{Q} \longrightarrow p^{\mathbb{Z}} \cup \{0\}$



El conjunto de valores del valor absoluto p-ádico tiene al 0 como único punto de acumulación. Luego el valor absoluto en $\mathbb{Q}_p$ también toma los mismos valores.

Ejemplo: $A = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \{x \in \mathbb{Q}_p : |x| < 1.5\}$

bola cerrada ↓ ↓ abierto.

Todos los bolos abiertos son cerrados y viceversa.

$\rightsquigarrow$ $\mathcal{O}_p$ es totalmente disconexo.