Grupo de clases

Problema: dado K cpo de números, ¿K es DFU? $\Leftrightarrow$ K es DIP.

$\mathcal{O}_K$ anillo de enteros de K, $\mathcal{I} = \{\mathfrak{a} \subset \mathcal{O}_K, \mathfrak{a} \neq 0\}$ (ideal)

En el conjunto $\mathcal{I}$ definimos una relación diciendo que:

$$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists\, \alpha, \beta \in \mathcal{O}_K \text{ t.q. } \alpha\mathfrak{a} = \beta\mathfrak{b}.$$

Lema: $\sim$ es una relación de equivalencia.

D/ Claro. reflexiva y simétrica Transitiva: $\alpha\mathfrak{a} = \beta\mathfrak{b}$, $\gamma\mathfrak{b} = \delta\mathfrak{c}$

$$\overbrace{\alpha\gamma}^{\tilde{\alpha}}\mathfrak{a} = \beta\gamma\mathfrak{b} = \overbrace{\beta\delta}^{\tilde{\beta}}\mathfrak{c}$$ ∎

Def: El grupo de clases de K, denotado $Cl(K)$, es el conjunto

$$\boxed{Cl(K) = \mathcal{I}/\sim}$$

Obs: $\mathcal{O}_K$ es DIP $\Leftrightarrow$ $Cl(K) = \{1\}$.

Prop: $Cl(K)$ es un grupo abeliano.

D/ La operación es el producto de ideales, o sea:

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}.\mathfrak{b}]$$

Es claro que el producto es asociativo, conmutativo, hay neutro $[\mathcal{O}_K]$. Sólo resta ver existencia de inversos.

Si $\mathfrak{a} \in \mathcal{Y} \rightsquigarrow \mathfrak{b} \neq \{0\}$ $\mathfrak{a}\mathfrak{b} = (\alpha) \Rightarrow [\mathfrak{b}] = [\mathfrak{a}]^{-1}$

Si $\alpha \in \mathfrak{a} \setminus \{0\}$, $(\alpha) \subset \mathfrak{a} \iff \mathfrak{a} \mid (\alpha) \iff (\alpha) = \mathfrak{a}\mathfrak{b}$ ∎

Obs: en la práctica, es difícil decidir si dos ideales son equivalentes.

Pregunta: ¿ $\mathrm{Cl}(K)$ es finito? Sí!

Antes, otra visión del grupo de clases. $\mathcal{Y}$ no es un grupo.

Def: un ideal fraccionario es un $\mathcal{O}_K$-módulo de K de la forma $\alpha \cdot \mathfrak{a}$ donde $\mathfrak{a} \subset \mathcal{O}_K$ ideal, $\alpha \in K$.

Propiedades: 1. El producto de ideales fraccionarios es un ideal fraccionario.

ejercicio 2. Si $\mathfrak{a}$ ideal fraccionario no nulo, $\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subset \mathcal{O}_K\}$ es un ideal fraccionario y $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathcal{O}_K$.

(Sugerencia: $\mathfrak{a} \subset \mathcal{O}_K$, $\alpha \in \mathfrak{a}$, $\{\beta \in \mathcal{O}_K : \mathfrak{a}\beta \subset (\alpha)\} = \mathfrak{b}$, $\mathfrak{a}\mathfrak{b} = (\alpha)$)

3. Si $\mathfrak{a}$ es ideal fraccionario, $\mathfrak{a}$ es un $\mathcal{O}_K$-módulo f.g. (noetheriano)

4. Si $\mathfrak{a}$ ideal fraccionario, $\mathfrak{a} \neq 0$, $\mathfrak{a} = \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \text{primos}}} \mathfrak{p}^{a_\mathfrak{p}}$, donde

$a_P \in \mathbb{Z}$ y $a_P = 0$ para todo P salvo finitos, de forma única.

$\mathcal{F} = \{$ ideales fraccionarios no nulos $\}$, $(\mathcal{F}, \cdot)$ es un grupo abeliano. $Cl(K) \simeq \mathcal{F}/\sim$ (sale de la definición). $\mathfrak{a} \sim \mathfrak{b} \iff \exists\, \alpha \in K$ t.f. $\alpha \mathfrak{a} = \mathfrak{b}$.

Teorema: $Cl(K)$ es finito.

Primero probamos finitud y después optimizamos el algoritmo.

Prop: Si K cpo de números, $\exists\, \lambda \in \mathbb{R}$ (depende de K) tal que si $\mathfrak{a} \subset \mathcal{O}_K$ es un ideal no nulo, $\exists\, \alpha \in \mathfrak{a}$, $\alpha \neq 0$, con $|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda \cdot N(\mathfrak{a})$.

Obs: para optimizar, buscamos optimizar λ.

Demo: $\mathcal{O}_K = \langle \omega_1, \dots, \omega_n \rangle_{\mathbb{Z}}$ (base de $\mathcal{O}_K$ como $\mathbb{Z}$-mód)

donde $n = [K : \mathbb{Q}]$; sean $\{\sigma_1, \dots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

Como $N(\mathfrak{a}) \in \mathbb{N}$, $\exists\, M \in \mathbb{N}$ t.f.

$$M^n \leq N(\mathfrak{a}) < (M+1)^n$$

Luego, el conjunto $\{\sum_{i=1}^{n} a_i v_i : 0 \le a_i \le M\}$

tiene $(M+1)^n$ elementos, $(M+1)^n > N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$

por el principio del palomar, hay dos elementos congruentes

módulo $\mathfrak{a}$. Su resta $\alpha = \sum_{i=1}^{n} b_i v_i \in \mathfrak{a}$, $-M \le b_i \le M$.

$$|N_{K/\mathbb{Q}}(\alpha)| = \left|\prod_{i=1}^{n} \sigma_i(\alpha)\right| = \left|\prod_{i=1}^{n} \sum_{j=1}^{n} b_j \sigma_i(v_j)\right|$$

$$\le \prod_{i=1}^{n} \sum_{j=1}^{n} \underbrace{|b_j|}_{\le M} \cdot |\sigma_i(v_j)| \le M^n \cdot \underbrace{\left(\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(v_j)|\right)}_{\lambda}$$

$$= \lambda M^n \le \lambda \cdot N(\mathfrak{a}) \qquad \square$$

Demo del Teo: dado $\mathfrak{a} \subset \mathcal{O}_K$ ideal no nulo, por la Proposición, $\exists\, \alpha \in \mathfrak{a}$ t.q. $|N_{K/\mathbb{Q}}(\alpha)| \le \lambda \cdot N(\mathfrak{a})$.

Como $\alpha \in \mathfrak{a}$, $(\alpha) \subset \mathfrak{a} \Rightarrow (\alpha) = \mathfrak{a}\cdot\mathfrak{b} \Rightarrow [\mathfrak{b}] = [\mathfrak{a}]^{-1}$, y

$$N(\mathfrak{b}) = \frac{|N(\alpha)|}{N(\mathfrak{a})} = \frac{|N_{K/\mathbb{Q}}(\alpha)|}{N(\mathfrak{a})} \overset{(*)}{\le} \lambda.$$

Luego toda clase en $Cl(K)$ tiene un representante cuya norma es a lo sumo λ. $\lambda \in \mathbb{R}_{\ge 0}$.

Afirmo: $\{\mathfrak{a} \subset \mathcal{O}_K : N(\mathfrak{a}) \le \lambda\}$ es finito.

Obs: sabemos que todo ideal es producto de ideales

primos. Luego basta ver que $\{\mathfrak{P} \subset \mathcal{O}_K \text{ primos} : N(\mathfrak{P}) \leq \lambda\}$

es finito. ¿Cómo encontramos primos en K? $\mathfrak{P} \cap \mathbb{Z} = p$ primo.

$\Rightarrow$ $\mathfrak{P}$ aparece en la factorización de $p\mathcal{O}_K$.

Hay finitos primos enteros entre 1 y λ, y para c/u de ellos hay finitos primos en $\mathcal{O}_K$ que lo dividen ☺

Algoritmo: dada λ, hallar todos los ideales de norma $\leq \lambda$, y determinar equivalencias entre ellos.

Obs: cuánto más chica es la constante λ, mejor es el algoritmo.

Objetivo: mejorar λ.

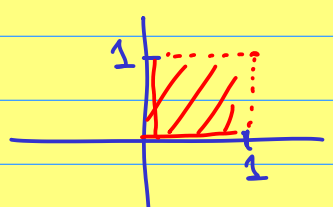
Repasemos algunas definiciones

- Un retículo en $\mathbb{R}^n$ es un $\mathbb{Z}$-módulo L de rango n que genera $\mathbb{R}^n$ (sobre $\mathbb{R}$). Ejemplo: $\mathbb{Z}^n \subset \mathbb{R}^n$

- Si $L \subset \mathbb{R}^n$ es un retículo, $\{v_1, \dots, v_n\}$ base de L como $\mathbb{Z}$-módulo. Un dominio fundamental

$$\Pi = \left\{ \sum_{i=1}^{n} \lambda_i v_i : \lambda_i \in \mathbb{R},\ 0 \leq \lambda_i < 1 \right\}$$

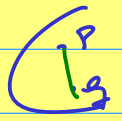
$\mathbb{Z}^2 \subset \mathbb{R}^2$, $\{(1,0),(0,1)\}$



Todo vector en $\mathbb{R}^n$ es equivalente (módulo L) a un único punto en Π.

El volumen de $\mathbb{R}^n/L$ es $\text{vol}(\Pi)$.

- Un conjunto $E \subset \mathbb{R}^n$ se dice convexo si vale que dados dos puntos de E, el segmento que los une está contenido en E. O sea $p, q \in E$, $p \cdot t + (1-t) \cdot q \in E$ $0 \le t \le 1$.



- Un conjunto $E \subset \mathbb{R}^n$ se dice simétrico respecto al $\vec{0}$ si cumple que $p \in E \Leftrightarrow -p \in E$.

Teo (Minkowski): Si $L \subset \mathbb{R}^n$ retículo y $E \subset \mathbb{R}^n$ es un conjunto convexo, simétrico respecto a $\vec{0}$ y medible t.q.

$$\text{vol}(E) \boxed{\geq} 2^n \text{vol}(\mathbb{R}^n/L)$$

entonces E contiene un punto no nulo de L. Si además, E es compacto, podemos cambiar $>$ por $\geq$.

Demo: Π un dominio fundamental.

$$\mathbb{R}^n = \bigcup_{x \in L} (\Pi + x)$$

$E \neq \emptyset$ y simétrico y convexo $\Rightarrow 0 \in E$. Dado $t \in \mathbb{R}$

podemos dilatar/contraer al conjunto E, mirando $t \cdot E$

$\{t \cdot p : p \in E\} \subset E$ si $t \leq 1$

para todo $t \in \mathbb{R}$ $(t < 1)$

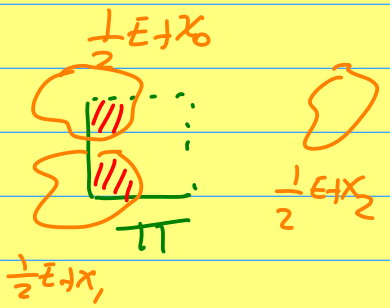
A la vez, tE cumple las mismas hipótesis.

$$\frac{1}{2}E = \frac{1}{2}E \cap \mathbb{R}^n = \bigcup_{x \in L} \left(\left(\frac{1}{2}E\right) \cap (\Pi + x) \right)$$

$$\text{vol}(\Pi) < \frac{\text{vol}(E)}{2^n} = \text{vol}\left(\frac{1}{2}E\right) = \sum_{x \in L} \text{vol}\left(\left(\frac{1}{2}E\right) \cap (\Pi + x) \right)$$

$$= \sum_{x \in L} \text{vol}\left(\left(\frac{1}{2}E + x\right) \cap \Pi \right)$$

↑ volumen es invariante por traslación.



Como la desigualdad es estricta, dos trasladados se tienen que intersecar. O sea, $\exists\, x_0, x_1 \in L$ distintos t.q.

$$\left(\frac{1}{2}E + x_0\right) \cap \left(\frac{1}{2}E + x_1\right) \neq \emptyset \qquad (\in E,\ \in E)$$

$$\Rightarrow \frac{1}{2}p + x_0 = \frac{1}{2}q + x_1, \quad p, q \in E. \Rightarrow \underbrace{x_1 - x_0}_{\in L} = \frac{1}{2}p + \frac{1}{2}(-q)$$

$\Rightarrow$ ¡$x_1 - x_0 \in L \cap E$. (listo 1° caso).

Si E es compacto, para cada $m \in \mathbb{N}$, $E_m = \left(1 + \frac{1}{m}\right)E$

cumple las mismas hipótesis que E, $\text{vol}(E_m) > \text{vol}(\mathbb{R}^n/L)$

cerrado. 2^n cpcto.

Por el caso anterior, $\exists\, x_m \in L \cap E_m \subset \underbrace{L \cap E_1}$.

compacto y discreto ptos cerrados. $\Rightarrow$ finito.

Luego existe $x_0 \in L \cap E_m$ para infinitos valores de m.

$\Rightarrow x_0 \in L \cap \overline{E} = L \cap E$ ∎

med., conv., sim.

Cono: Si E es como antes y cpcto, $\text{vol}(E) > 0$, supongamos además, $f: \mathbb{R}^n \to \mathbb{R}$ t.q. $f(tx) = t^n \cdot f(x)$, y

$E \subset \{ x \in \mathbb{R}^n : f(x) \leq 1 \}$

entonces todo reticulo $L \subset \mathbb{R}^n$ contiene un $x_0 \neq 0$ que cumple

$$f(x_0) \leq \frac{2^n}{\mathrm{vol}(E)} \cdot \mathrm{vol}(\mathbb{R}^n/L)$$

$(L \hookrightarrow \mathcal{Q}, \quad x_0 \hookrightarrow \alpha, \quad \lambda = \uparrow)$

Demo: $t = \sqrt[n]{\frac{2^n}{\mathrm{vol}(E)} \cdot \mathrm{vol}(\mathbb{R}^n/L)}$, $\tilde{E} = t \cdot E$

$$\mathrm{vol}(\tilde{E}) = t^n \cdot \mathrm{vol}(E) = 2^n \cdot \mathrm{vol}(\mathbb{R}^n/L)$$

$\Rightarrow \tilde{E}$ está en las hip. del Teo $\Rightarrow \exists\, x_0 \in \tilde{E} \cap L \Rightarrow x_0 \in L$

$$f(x_0) = f(t \cdot \underbrace{\frac{x_0}{t}}_{\in E}) = t^n \cdot f\left(\frac{x_0}{t}\right) \leq t^n = \frac{2^n}{\mathrm{vol}(E)} \cdot \mathrm{vol}(\mathbb{R}^n/L)$$

□

Veremos: $\lambda = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathcal{Q}_K)|}$