12/08/20 § Divisibilidad y factorización (recordatorio de álgebra)

R – dominio

def $\alpha \in R$ es invertible (unidad) si $\exists \beta \in R$ t.q. $\alpha\beta = 1$

$R^\times = \{\alpha \mid \alpha \text{ invertible}\}$ – el gpo de unidades

def $\alpha, \beta \in R$

·) $\alpha \mid \beta \iff \exists \gamma$ t.q. $\beta = \gamma\alpha$.

·) $\alpha \sim \beta$ (asociados) $\iff \alpha \mid \beta$ y $\beta \mid \alpha$

def $(\alpha) = \{\gamma\alpha \mid \gamma \in R\}$ – el ideal generado por α

$$\alpha \mid \beta \iff (\alpha) \supseteq (\beta)$$

$$\alpha \sim \beta \iff (\alpha) = (\beta) \iff \alpha = u\beta \text{ para } u \in R^\times$$

$$\alpha \in R^\times \iff (\alpha) = R$$

def Sea $\pi \in R$, $\pi \neq 0$, $\pi \notin R^\times$

·) π es irreducible $\quad \alpha \mid \pi \Rightarrow \alpha \in R^\times$ ó $\alpha \sim \pi$

·) π es primo $\quad \pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ ó $\pi \mid \beta$

Ejercicio primo $\Rightarrow$ irreducible.

def R es un dominio de factorización única si

1) Todo $\alpha \neq 0$, $\alpha \notin R^\times$ puede ser expresado como
$$\alpha = \pi_1 \cdots \pi_s, \qquad \pi_i \text{ son irreducibles}$$

2) estas expr. son únicas, salvo $\sim$ y permutación

Si $\alpha = \pi_1 \cdots \pi_s = \rho_1 \cdots \rho_t$, entonces $s = t$ y $\pi_i \sim \rho_i$, después de una permutación

Teorema Las siguientes condiciones son equivalentes:

1) R es un DFU

2) R cumple a) toda cadena ascendente de ideales principales se estabiliza.

$$(\alpha_1) \subseteq (\alpha_2) \subseteq (\alpha_3) \subseteq \cdots \Longrightarrow \exists n \text{ t.q. } (\alpha_n) = (\alpha_{n+1}) = \cdots$$

b) todo irreducible es primo

Dem 1) ⇒ 2)] $(\alpha) \subsetneq (\beta)$ $\alpha = \pi_1 \cdots \pi_s$, $\beta = \rho_1 \cdots \rho_t$

entonces $s > t$. No podemos tener una cadena infinita $(\alpha) \subsetneq (\alpha_1) \subsetneq (\alpha_2) \subsetneq \cdots$

Para b), si π es irreducible, $\pi \mid \alpha\beta \Rightarrow \pi \mid \alpha$ ó $\pi \mid \beta$

$\boxed{2) \Rightarrow 1)}$ Usando a), primero ver que todo $\alpha \neq 0$, $\alpha \notin R^\times$ tiene un factor irreducible.

(Si α es reducible $\Rightarrow$ $\alpha = \alpha_1 \beta$, donde $\alpha_1 \in R^\times$, $\alpha_1 \nsim \alpha$.
si α_1 es reducible $\Rightarrow$ repetir el proceso, etc.)

Aplicando la existencia de factor irreducible,

$$\alpha = \pi_1 \cdots \pi_s$$

Falta probar que las factorizaciones son únicas.

$$\pi_1 \cdots \pi_s = \rho_1 \cdots \rho_t, \qquad s \leq t.$$

π_s primo $\Rightarrow$ $\pi_s \mid \rho_i$. Digamos (después de una perm) que $i = t$.

ρ_t irreducible $\Rightarrow$ $\pi_s \sim \rho_t$ $\Leftrightarrow$ $\pi_s = \underbrace{u}_{\in R^\times} \cdot \rho_t$

Cancelando, $\pi_1' \cdots \pi_{s-1}' = \rho_1' \cdots \rho_{t-1}'$

Este es el paso inductivo. ∎

Proposición Si R es un dominio de ideales principales ($\forall$ ideal $I \subseteq R$ $\exists \alpha \in R$ t.q. $I = (\alpha)$), entonces es un DFU.

Dem a) $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \Rightarrow I = \bigcup_{n \geq 1} I_n$

R es un DIP $\Rightarrow$ $\exists \alpha$ t.q. $(\alpha) = I$ $\quad \alpha \in I_n$

$$\Rightarrow (I_n) = (I_{n+1}) = \cdots = I$$

b) Sea $\pi \in R$ irreducible. Supongamos que $\pi \mid \alpha\beta$.

Consideremos $(\pi, \alpha) = \{x\pi + y\alpha \mid x, y \in R\}$

R es un DIP, $\Rightarrow$ $\exists \gamma \in R$ t.q. $(\pi, \alpha) = (\gamma)$

$\gamma | \pi$, $\gamma | \alpha$. Pero π es irreducible.

- $\gamma \sim \pi \Rightarrow \pi | \alpha$
- $\gamma \in R^*$ $\Rightarrow \pi | \beta$ $\blacksquare$

Def R es euclidiano si existe $\delta : R \setminus \{0\} \to \mathbb{N}$.
t.q. $\forall \alpha, \beta \in R$, $\beta \neq 0$ $\exists q, r \in R$ t.q.
$\alpha = q\beta + r$, donde $r = 0$ ó $\delta(r) < \delta(\beta)$,

Ejemplos:
- $\mathbb{Z}$ es euclidiano respecto a $\delta(n) = |n|$
- $k[x]$, donde k es un campo, es euclidiano respecto a $\delta(f) = \deg f$.
(la división con resto de polinomios)

Teorema Todo dominio euclidiano es un DIP
(y en particular DFU)

Dem. Sea $I \subseteq R$ un ideal. Si $I = (0)$, es principal.
Si $I \neq (0)$, sea $\alpha \in I$ un elto no nulo con
la mínima posible $\delta(\alpha)$. (es decir, si $r \in I$, $\delta(r) < \delta(\alpha)$
$\Rightarrow r = 0$)
Por la elección de α, todo $\beta \in I$ está en (α). $\blacksquare$

$$\text{Euclidiano} \underset{\not\Leftarrow}{\Rightarrow} \text{DIP} \underset{\not\Leftarrow}{\Rightarrow} \text{DFU}.$$

§ **Enteros de Gauss** $\mathbb{Z}[i] \subset \mathbb{Q}(i)$

Tenemos $\sigma : \alpha = a + bi \mapsto \bar{\alpha} = a - bi$.

Definamos para $\alpha \in \mathbb{Q}(i)$, $\alpha = a + bi$: $N(\alpha) := \alpha \cdot \sigma(\alpha) = a^2 + b^2$

$N : \mathbb{Q}(i) \to \mathbb{Q}$ es la norma de $\mathbb{Q}(i)/\mathbb{Q}$

Se restringe $N : \mathbb{Z}[i] \to \mathbb{N}$. Es multiplicativa:
$N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.

Lema 1) $\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\}$

2) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{$las raíces cuartas de $1\}$

3) Si $N(\pi) = p$ es primo $\Rightarrow$ π es irreducible.

4) Si $N(\pi) = n$, y $\forall\, d \mid n$, $d \neq 1, n$ no hay eltos de $N = d$

$\Rightarrow$ π es irreducible.

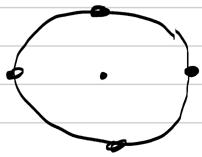
Dem 1) $u \in \mathbb{Z}[i]^\times \Rightarrow u \cdot u^{-1} = 1 \Rightarrow N(u) \cdot N(u^{-1}) = 1$

$\Rightarrow N(u) = N(u^{-1}) = 1$

Viceversa, $N(u) = 1 \Rightarrow u \cdot \bar{u} = 1 \Rightarrow u^{-1} = \bar{u}$

2) $N(a + bi) = a^2 + b^2 = 1$

$\Rightarrow (a, b) = (\pm 1, 0)$ ó $(0, \pm 1)$



3) Si $N(\pi) = p$, y $\pi = \alpha\beta$. $\Rightarrow \underset{p}{\underset{\|}{N(\pi)}} = N(\alpha) \cdot N(\beta)$

$N(\alpha) = p$, $N(\beta) = 1$

$\Rightarrow \pi \sim \alpha$, $\beta \in \mathbb{Z}[i]^\times$.

$N(\alpha) = 1$, $N(\beta) = p$

$\Rightarrow \alpha \in \mathbb{Z}[i]^\times$, $p \sim \pi$

4) Similar. ∎

Lema $\mathbb{Z}[i]$ es euclidiano respecto a $\delta(a + bi) = N(a + bi) = a^2 + b^2$.

Dem $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$.

$\frac{\alpha}{\beta} = x + yi$, donde $x, y \in \mathbb{Q}$
en $\mathbb{Q}(i)$

Existen $a, b \in \mathbb{Z}$ t.q.

$N((x-a) + (y-b)i) = (x-a)^2 + (y-b)^2 < 1$

Pongamos $q = a + bi$. $r = \alpha - q\beta$.

$= \beta \cdot ((x-a) + (y-b)i)$

$N(r) = N(\beta) \cdot \underbrace{N((x-a) + (y-b)i)}_{< 1} < N(\beta)$. ∎

$\mathbb{Z}[i]$ euclidiano $\Rightarrow$ $\mathbb{Z}[i]$ DFU.

¿Cómo se ven los primos (= irreducibles)?

$\pi \in \mathbb{Z}[i]$ primo $\Rightarrow$ $N(\pi) = \pi \cdot \overline{\pi}$
$$\underset{p_1 \cdots p_s}{\|} \Rightarrow \pi \mid p_i$$

def Los primos $p \in \mathbb{Z}$, se llaman los primos racionales

Teorema Sea $p \in \mathbb{Z}$, un primo racional.

1) Si $p = 2$ $\Rightarrow$ $2 = -i(1+i)^2$, donde $1+i$ "se ramifica" en $\mathbb{Z}[i]$ es primo.

2) Si $p \equiv 3\ (4)$ $\Rightarrow$ p es primo en $\mathbb{Z}[i]$ "es inerte"

3) Si $p \equiv 1\ (4)$ $\Rightarrow$ $p = \pi\overline{\pi}$, donde $\pi, \overline{\pi}$ "se escinde" (split) son primos en $\mathbb{Z}[i]$, no asociados entre sí.

Dem. 1) $N(1+i) = 2 \Rightarrow 1+i$ es primo.

2) Si $p \equiv 3\ (4)$, notamos que $a^2 + b^2 \not\equiv 3\ (4)$

No hay elementos de norma p, $N(p) = p^2$

$\Rightarrow$ p es irreducible $\Rightarrow$ es primo.

3) Si $p \equiv 1\ (4)$, entonces $\left(\frac{-1}{p}\right) = +1$,

es decir $\exists\, a \in \mathbb{Z}$ tq. $a^2 \equiv -1\ (p)$.

$p \mid (a^2+1) = (a+i)(a-i)$ $\quad$ $p \nmid a \pm i \Rightarrow p$ no es primo.

$p = \pi \cdot \rho$, donde π y ρ no son invertibles.

$$\Rightarrow \underset{p^2}{\underset{\|}{N(p)}} = \underset{p}{\underset{\|}{\underline{N(\pi)}}} \cdot \underset{p}{\underset{\|}{\underline{N(\rho)}}} \Rightarrow p = N(\pi) = \pi \cdot \overline{\pi}.$$

π es primo.

Proposición (Fermat) Un primo impar p es una suma de dos cuadrados $\Leftrightarrow$ $p \equiv 1\ (4)$.

Además, si $p = x^2 + y^2$, x e y están bien definidos (salvo signo y permutación).

Dem Si $p = x^2 + y^2 \Rightarrow p \equiv 1 \ (4)$.

Viceversa, si $p \equiv 1 \ (4) \Rightarrow p = \pi \cdot \overline{\pi}$ en $\mathbb{Z}[i]$

donde $\pi = x + y \cdot i$ primo,

$N(\pi) = x^2 + y^2 = p$.

Por qué x e y son únicos?

$$p = x^2 + y^2 = x'^2 + y'^2 \qquad x, y, x', y' > 0.$$

S.p.d.g. $x, x' \equiv 1 \ (2)$,

$y, y' \equiv 0 \ (2)$

$\pi \cdot \overline{\pi} = \pi' \cdot \overline{\pi'}$ donde $\pi = x + y \cdot i$

$\pi' = x' + y' \cdot i$

$\pi \sim \pi'$ ó $\pi \sim \overline{\pi'}$

$(\pi = u \cdot \pi'$ ó $\pi = u \cdot \overline{\pi'}$, $u = \pm 1, \pm i)$

$\Rightarrow \cdots \Rightarrow x = x', \ y = y'$. $\blacksquare$

Ejemplos

$$\left.\begin{aligned} 5 &= 2^2 + 1^2 \\ 13 &= 3^2 + 2^2 \\ 17 &= 4^2 + 1^2 \\ 29 &= 5^2 + 2^2 \\ &\cdots\cdots \end{aligned}\right\}$$

La próxima sesión: ◦) $\mathbb{Z}[\zeta_3]$ — enteros de Eisenstein.

◦) Más ejemplos.