Recordar: • $p \in \mathbb{Z}$ es primo, $\#Div(p) = 4$ (irreducible)

$\mathbb{Z}$, unidades $= \{d \in \mathbb{Z} : \frac{1}{d} \in \mathbb{Z}\} = \{\pm 1\}$

Vale: 1. Si p primo, $a, b \in \mathbb{Z}$, $p \mid a \cdot b \Rightarrow p \mid a$ ó $p \mid b$.

(primo)

2. Si $n \in \mathbb{Z}$, $n \neq 0, \pm 1$, se factoriza como producto de primos de forma única (salvo el orden)

$$6 = 2 \cdot 3 = 3 \cdot 2 \quad \text{(y un signo)}$$

$$-10 = (-1) \cdot 2 \cdot 5 = (-5) \cdot 2 = (-2) \cdot 5$$

Objetivo: entender qué pasa en contextos más generales.

Entender: • ¿Qué es $\mathbb{Z}$?

• ¿Qué es un primo?

• ¿Hay factorización? ¿única?

($6 = 2 \cdot 3 = (1+\sqrt{5})(1-\sqrt{5})$)

Aplicación (Gauss): ¿Qué números son suma de 2 cuadrados? $a, b \in \mathbb{Z}$

$$G = \{n \in \mathbb{N} : n = a^2 + b^2\}$$

Ejemplo: • $2 = 1^2 + 1^2$ • $5 = 2^2 + 1^2$

• 3 NO • 7 NO

$2 \in G$, $3 \in G$, ¿$10 \in G$? Sí

$$2 = (1+i)(1-i), \quad 5 = (2+i)(2-i)$$

$$2 \cdot 5 = 10 = ((1+i)(2+i))((1-i)(2-i))$$

$$= (1+3i)(1-3i) \rightsquigarrow 10 = 1^2 + 3^2$$

Notar que los cuentas son $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$

enteros de Gauss

¿Qué estructura tienen los enteros de Gauss?

Def: un anillo es una terna $(R, +, \cdot)$, donde R es un conjunto, $+, \cdot : R \times R \to R$ operaciones binarias, que satisfacen las siguientes propiedades.

1. $(R,+)$ es un grupo conmutativo.
(asociativo, conmutativo, neutro, inversos)

2. $(R,\cdot)$ es asociativo, además tiene neutro 1
$0 \neq 1$

3. Distributivo: $a.(b+c) = a.b + a.c$
$(b+c).a = ba + ca$

Si además, $(R,\cdot)$ es conmutativo, se llama anillo conmutativo, y si además, $(R\setminus\{0\},\cdot)$ hay inversos (todo ello no solo tiene inverso) $\Rightarrow R$ se llama un cuerpo.

Ejemplos: 1. $(\mathbb{Z},+,\cdot)$ anillo conmutativo.

2. $(\mathbb{R},+,\cdot)$ es un cuerpo.
$(\mathbb{Q},+,\cdot)$, $(\mathbb{C},+,\cdot)$

3. $M_{2\times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R} \right\}$ es un anillo, $+,\cdot$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}$
no conmutativo.

4. Ejercicio: $\mathbb{Z}[i]$ es un anillo conmutativo.

Cono. El conjunto $\mathbb{C}$ es multiplicativamente cerrado, $n,m \in \mathbb{C} \Rightarrow n.m \in \mathbb{C}$

$n = a^2+b^2 = (a+bi)(a-bi)$

$m = c^2+d^2 = (c+di)(c-di)$

$m.n = \underbrace{((a+bi)(c+di))}_{\in \mathbb{Z}[i]}\ ((a-bi)(c-di))$

Obs: En $\mathbb{Q}$, la definición de $\mathbb{Z}$ es "natural" pero en otros contextos no están claro.

$\mathbb{Q}[i] = \{a+bi : a,b \in \mathbb{Q}\}$ es un cuerpo.

U1
$\mathbb{Z}[i]$
U1

$\{a+bi : a \in \mathbb{Z},\ b \in 2\mathbb{Z}\}$ es un anillo.

¿Qué son los enteros?

$\{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}\cup\{0\}\} \subseteq \mathbb{Q}$ Ir II be back

es un anillo.

Antes de hablar de enteros, hablemos de cuerpos

Sea K un cuerpo, tenemos un morfismo natural

$$f: \mathbb{Z} \longrightarrow K$$

$1 \to 1$

Def: un morfismo de anillos $f: R_1 \to R_2$

es una función que cumple: $\cdot f(a+b) = f(a)+f(b)$

$\cdot f(a.b) = f(a).f(b)$

$\cdot f(1) = 1$

Obs: f está unívocamente determinado, $f(n) = \underbrace{f(1)+\cdots+f(1)}_{n\text{-veces}}$

Si f es un morfismo, $Nu(f) = \{z \in \mathbb{Z} : f(z)=0\} \subset \mathbb{Z}$

es un ideal.

Si R es un anillo, un ideal $\mathcal{J} \subset R$ es un subcjto

t.f: 1. $\mathcal{J}$ es cerrado para la suma ($\alpha,\beta \in \mathcal{J} \Rightarrow \alpha+\beta \in \mathcal{J}$)

2. $\mathcal{J}$ es cerrado para el producto de R.

(si $\alpha \in \mathcal{J}$, $r \in R$, $r.\alpha \in \mathcal{J}$)

ojo si R no es conmutativo.

Ejercicio: todo ideal de $\mathbb{Z}$ es principal, o

sea si: $\mathcal{J} \subset \mathbb{Z}$ es ideal, $\exists n \in \mathcal{J}$ t.f. $\mathcal{J} = (n) =$

$= \{a.n : a \in \mathbb{Z}\}$

Eg: Algoritmo de Euclides $\quad \frac{6, 6 \in \mathcal{J}}{\Downarrow}$

$2 \in \mathcal{J}$

$f: \mathbb{Z} \to K$

Luego, $Nu(f) = (a)$ ¿Qué posibles valores

toma a?

$\rightsquigarrow$ si $a=0$, decimos que K tiene característica 0.

Luego $\mathbb{Z} \subset K$, y como K cuerpo, $\mathbb{Q} \subset K$.

$\rightsquigarrow$ ¿si $a \neq 0$? ¿$a=6$?

$Nu(f) = 6.\mathbb{Z}$

$\mathbb{Z} \hookrightarrow K$

$2 \to \alpha \neq 0$

$3 \to \beta \neq 0$

$2.3 \to \alpha.\beta = 0$.

Obs: un cuerpo es íntegro, si $a.b=0 \Rightarrow a=0$ ó $b=0$.

¿p?

Luego a debe ser primo (ejercicio)

$\mathbb{Z} \longrightarrow K$

$p \longrightarrow 0$

es un cuerpo

$\mathbb{F}_p = \boxed{\mathbb{Z}/p} \hookrightarrow K$ Decimos que K tiene característica p.

Recordando: 1. $\mathbb{Q} \subset K$

2. $\exists\, p$ primo t.q. $\mathbb{F}_p \subset K$.

Ejemplo: $\cdot\ car(\mathbb{R}) = 0 = car(\mathbb{Q}) = car(\mathbb{C})$

$\cdot\ car(\mathbb{Z}/5) = 5$

Luego si K cpo, $\mathbb{Q} \subset K$ o $\mathbb{F}_p \subset K$ ($\mathbb{F}_p$-e.v.)

K es un $\mathbb{Q}$-e.v.

tiene sentido mirar $\dim_{\mathbb{Q}} K = [K:\mathbb{Q}]$ (resp. $[K:\mathbb{F}_p]$)

en el curso nos va a interesar el caso $[K:\mathbb{Q}] < \infty$.

Ejercicio: si K, L, M son cuerpos, $K \subset L \subset M$, entonces

$\dim_K(M) = \dim_K(L) \cdot \dim_L(M)$

$[M:K] = [M:L] \cdot [L:K]$ (suponemos todos finitos)

Recordar: K cuerpo, $K[X]$ = anillo de polinomios en una variable $= \{ \sum_{n=0}^{N} a_n X^n : a_n \in K \}$

Obs: Si K cuerpo, $d := [K:\mathbb{Q}] < \infty$, $\alpha \in K \setminus \mathbb{Q}$,

$\mathbb{Q}[\alpha] = \{ \sum_{n=0}^{N} a_n \alpha^n \} \subset K$

anillo $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \dots, \alpha^d\}$ d+1 ellos.

$\Rightarrow$ son l.d., o sea $\exists\, a_0, \dots, a_d \in \mathbb{Q}$:

(*) $a_0 + a_1\alpha + \dots + a_d\alpha^d = 0 \quad (a_0 \neq 0)$

$p(X) = a_0 + a_1 X + \dots + a_d X^d \in \mathbb{Q}[X]$, $p(\alpha) = 0$.

(*) $\boxed{\left(-\frac{1}{a_0}\right) \cdot (a_1 + a_2\alpha + \dots + a_d\alpha^{d-1}) \cdot \alpha = 1}$

$\Rightarrow \frac{1}{\alpha} \in \mathbb{Q}[\alpha]$

En particular, si $\dim_{cl} K < \infty$, todos los ellos de K son raíces de algún polinomio en $cl[X]$.

Recordar: Si k cuerpo, $k[X]$ tiene algoritmo de división: dados $p(X), f(X) \in k[X]$, $f \neq 0$, existen únicos $r(X), t(X) \in k[X]$ t.q.:

1. $p(X) = f(X)t(X) + r(X)$
2. $r(X) = 0$ ó $gr(r(X)) < gr(f(X))$

$$\begin{array}{r|l} \boxed{2}X^2 + X + 1 & \boxed{3X+1} \\ \underline{2X^2 + \frac{2}{3}X} & 2 \cdot \frac{1}{3}X \\ \vdots & \end{array} \quad \left| \begin{array}{l} X^2+X+1 = \\ 2 \cdot \left(\frac{1}{2}X^2 + \frac{1}{2}X - \frac{1}{2}\right) \end{array} \right.$$

$\hookrightarrow$ hay factorización única.

Dentro de esto: $\hookrightarrow$ irreducible: $p(X) \in k[X]$ se dice irreducible si no tiene divisores con grado entre 1 y $gr(p(X)) - 1$.

$\rightarrow$ Primo: si $p \mid a \cdot b \Rightarrow p \mid a$ ó $p \mid b$

Vale: irreducible $\Rightarrow$ primo. $\Leftarrow$ vale casi siempre.

Ejercicio: completar los detalles.

Dado $p(X) \in k[X]$, $p(X) \mid f(X)$ si existe $r(X) \in k[X]$: $f(X) = p(X) \cdot r(X)$.

Podemos definir una relación de equivalencia.

$$f(X) \sim g(X) \iff p(X) \mid (f(X) - g(X)).$$

$(f \equiv g \pmod{p})$ $\quad p(X)$ mónico

Lema: $k[X]/_{p(X)}$ es un cuerpo $\iff p(X)$ es irreducible

D/ $\Rightarrow$) Si $p = a \cdot b \Rightarrow \overline{a}\,\overline{b} = 0 \Rightarrow \overline{a} = 0$ ó $\overline{b} = 0$

$\overline{a} = 0 \Rightarrow p \mid a$ y $a \mid p \Rightarrow a(X) = p(X) \cdot k \Rightarrow$ irreducible.

$\Leftarrow$) Si $\overline{f(X)}$ no nulo $\Rightarrow$ tiene inverso.

$mcd(f(X), p(X)) = p(X)$ ó 1

$p(X) \mid f(X) \Rightarrow \overline{f(X)} = 0$.

$\Rightarrow \overline{1} = \overline{f(x)}\,\overline{q(x)} + \overline{p(x)\cdot s(x)}$

Ejemplo: $p(x) = x^2+1$ en $\mathbb{Q}[x]$, $x+1 = f(x)$

$$\begin{array}{r|l} x^2+1 & x+1 \\ \hline -x^2-x & x-1 \\ \hline -x+1 & \\ \hline +x+1 & \\ \hline 2 & \end{array}$$

$x^2+1 = (x+1)(x-1)+2$

$\Rightarrow 1 = \frac{1}{2}(x^2+1) - \frac{(x-1)}{2}(x+1)$

$\mathbb{Q}[x]/(x^2+1) \xrightarrow{\sim} \mathbb{Q}[i]$

$x \longrightarrow i$

$q \longrightarrow q$

$x+1 \longrightarrow 1+i$, $(1+i)^{-1} = \frac{1-i}{2}$

$\frac{1}{2} - \frac{x}{2}$ ←

Corolario: tenemos una fabrica de cuerpos.

$K = \mathbb{Q}[x]/(p(x))$, $p(x)$ irred. , $\operatorname{gr}(p(x)) = d$

Propuesta: $\dim_{\mathbb{Q}} K = d$ $\quad p(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$

$K = \langle 1, x, x^2, \dots, x^{d-1} \rangle_{\mathbb{Q}}$

Ejemplo: $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$ cpo. , $\dim_{\mathbb{F}_2} \mathbb{F}_4 = 2$

$\# \mathbb{F}_4 = 4$ $\quad \{1, x\}$ base.