Álgebra Conmutativa 20 Feb

Ayer: Primos en $\mathbb{Z}[x]$

Hoy: Módulos finitamente generados

Proposición: $P \leq \mathbb{Z}[x]$ ideal primo

$\langle 0 \rangle$; $\langle f \rangle$ $f \in \mathbb{Z}[x]$ irred.

ó P es maximal: $\langle p, f \rangle$ $p \in \mathbb{Z}$ primo
f irred $\mathbb{F}_p$.

Argumento: Si I es principal, entonces

$R := \mathbb{Z}[x]/\langle f \rangle$ dominio $\iff$ f irred $/\mathbb{Z}$.

Asumamos R no es dominio. $\exists\ \bar{a} \cdot \bar{b} = 0$

en R con $\bar{a} \neq 0$ & $\bar{b} \neq 0$. $(a \notin \langle f \rangle;\ b \notin \langle f \rangle$

$\Rightarrow$ $f \mid a \cdot b$ en $\mathbb{Z}[x]$.

si f es irred $\Rightarrow$ $a \in \langle f \rangle$ o $b \in \langle f \rangle$

contradicción. Por tanto f no es irred.

——//——

si $f, g \in \mathbb{P}$ sin factores en común.

$\langle f, g \rangle \subseteq \mathbb{P}$.

$$\begin{array}{ccc} \langle f, g \rangle & \subseteq & \mathbb{Z}[x] \\ | & & | \\ \langle p \rangle & \subseteq & \mathbb{Z} \end{array}$$

primo $\Downarrow$ primo

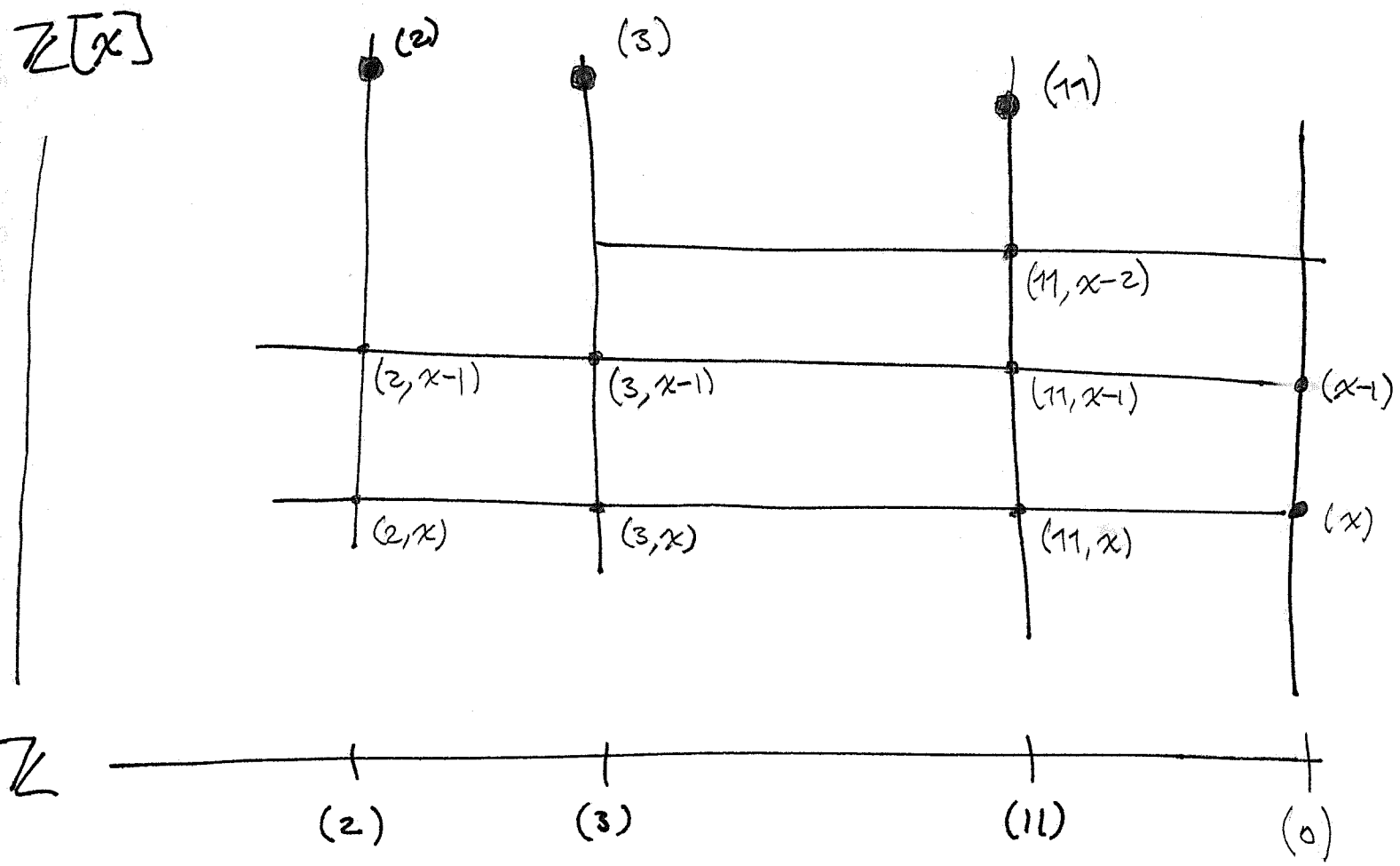
$\Rightarrow$ $\langle f, g \rangle = \langle p, h(x) \rangle$

p: primo en $\mathbb{Z}$

$\mathbb{Z}[x]/\langle p, h(x) \rangle \cong \mathbb{F}_p[x]/\langle h \rangle$ dominio $\Leftrightarrow$ h es irred en $\mathbb{F}_p$.

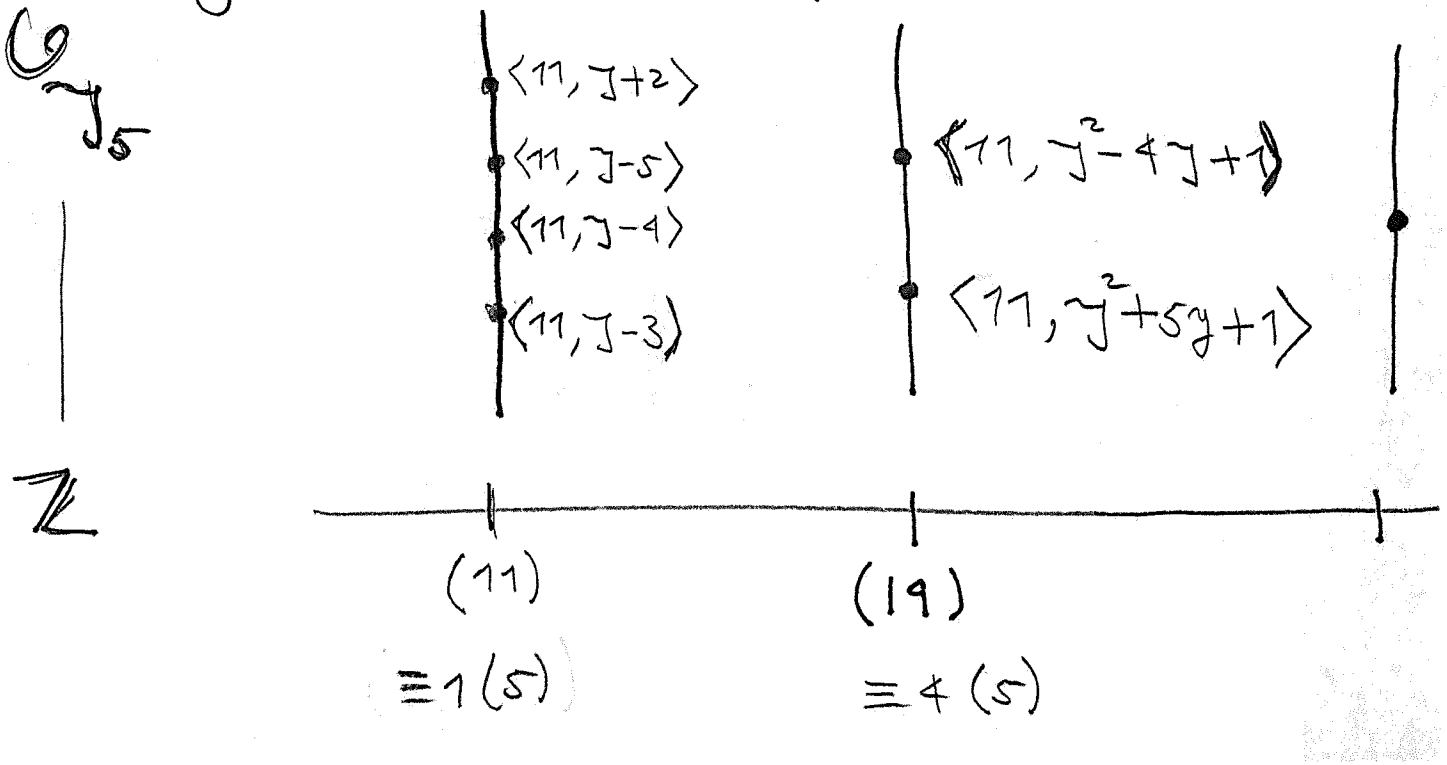
——//——

Resumiendo: ∎



primos em $\mathbb{Z}[x]$ & primos em $\mathbb{Z}$.

Enteros ~~algebraicos de~~ "campo ~~$\mathbb{Q}[\sqrt{5}]$~~":



Conjetura: $\ell, p \in \mathbb{Z}$ primos impares y

$$\ell^* = (-1)^{\frac{\ell-1}{2}}$$

γ_ℓ = raíz ℓ-ésima primitiva de 1.

Entonces:

$p \leq \mathbb{Q}(\sqrt{\ell^*})$ escinde si:

$p \leq \mathcal{O}_{\gamma_\ell}$ escinde en un número par de ideales primos.

$\mathcal{O}_{\gamma_\ell} \leq \mathbb{Q}(\gamma_\ell)$ denota el anillo de enteros algebraicos del campo $\mathbb{Q}(\gamma_\ell)$.

Evidencia: γ_5, γ_{11}, γ_{13}.

Ej: $P_1 * \cdots * P_{12} \leq \mathcal{O}_{\gamma_{13}} \leq \mathbb{Q}[\gamma_{13}]$ i.e.

$\langle 53 \rangle \leq \mathbb{Z} \text{ —— } \mathbb{Q}$

$\langle 53 \rangle = P_1 * \cdots * P_{12}$ escinde en 12 factores primos.

Módulos

Def.- Un módulo sobre A es un gp abeliano con

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, m) &\longmapsto a \cdot m \end{aligned}$$

tal que
$$a(m_1 + m_2) = am_1 + am_2$$
$$(a_1 + a_2)m = am + am$$
$$a\,a'\,m = a(a'm)$$
$$1m = m$$

Def.-
Un A-módulo se dice finitamente generado si existen $m_1, \dots, m_k$ con (generadores)

$$M = Am_1 + \dots + Am_k.$$

(Eg) ?

Obs. Los generadores de un módulo pueden tener relaciones algebraicas entre ellos. Si no existen relaciones entre ellos, se dice libre.

el módulo

Si $A \subset B$ inclusión de anillos, entonces

B es un A-módulo.