Geometría de Curvas algebraicas : 30 de enero

Hoy: Teorema: $f = x^5 + ax + b \in F[x]$

irreducible/F con $a \neq 0$ & $ch(F) = 0$.

Entonces f es soluble por radicales/F sii

$\exists\ \lambda, \mu \in F$ tal que

$$a = \frac{3125\lambda\mu^4}{(\lambda-1)(\lambda^2-6\lambda+25)} \quad ; \quad b = \frac{3125\lambda\mu^5}{(\lambda-1)(\lambda^2-6\lambda+25)}$$

Demostración: Sabemos* que el discriminante

$$\Delta(f) = 256a^5 + 3125b^4 \quad \&$$

el resolvente

$$\Theta_f(y) = \left(y^3 - 20ay^2 + 240a^2y + 320a^3\right)^2 - 2^{10}\Delta(f)y$$

Por la tabla de la clase anterior:

f es soluble por radicales $\iff$

$\Theta_f(y)$ tiene una raiz en F.

Como $a \neq 0$, una raiz $\beta = a\lambda$ para $\lambda \in F$.

Igualmente $b = a\mu$; $\mu \in F$.

Por tanto f es soluble por radicales $\iff$

$\exists\ \lambda \in F$ tal que

$$0 = \Theta_f(a\lambda) = \left((a\lambda)^3 - 20a(a\lambda)^2 + \dots\right)$$

$$= 2^2 a^5 \left[\left(\lambda^6 - 10\lambda^5 + 55\lambda^4 - 140\lambda^3 + 175\lambda^2 - 106\lambda + 25\right)a - 3125\lambda\mu^4\right]$$

$(a \neq 0)$

$\Rightarrow$

$$a = \frac{3125\lambda\mu^4}{\lambda^6 - 10\lambda^5 + 55\lambda^4 - \dots}$$

$$b = \dots$$

} Fórmulas del teorema

(Relación con campos finitos:)

Ejemplos (reveladores)

1) $f = x^5 + 20x + 16 \in \mathbb{Z}[x]$

$\Delta(f) = 2^{16} \cdot 5^6$

$\overline{f} = (x+2)(x+3)(x^3+2x^2+5x+5) \in \mathbb{Z}/7[x]$

(!?)

$\Rightarrow \quad 3 \mid |Gal(f)|$

$\Rightarrow \quad Gal(f) \cong A_5$

2) $f = x^5 - 6x + 3 \in \mathbb{Z}[x]$

$\overline{f} = (x+2)(x+7)(x+13)(x^2+12x+13) \in \mathbb{Z}/17[x]$

$\overline{f} = x^5 + 4x + 3 \in \mathbb{Z}/5[x]$

$\overset{(!?)}{\Longrightarrow}$ $Gal(f)$ contiene un 5-ciclo y un 2-ciclo

$\overset{\checkmark}{\Longrightarrow}$ $Gal(f) \cong S_5$

Ejemplo (de largo aliento):

¿~~Cuándo~~ para qué primos $p \in \mathbb{Z}$ f tiene una raiz modulo p?

$$f = (x^3 - 10x)^2 + 31(x^2-1)^2 \in \mathbb{Z}[x]$$

Si $p > 3$ y $p \neq 31$

Kronecker:

$f(x) \equiv 0 \pmod p$ $x \in \mathbb{Z} \Longleftrightarrow p = x^2 + 31y^2$ para $x, y \in \mathbb{Z}$.