Adjoining roots

Q want to solve $x^3 - x + 1 = 0$

can ~~also~~ always "borrow" a sol^n from $\mathbb{C}$. (alg. closed.)

$\mathbb{F}_3 := \mathbb{Z}/3\mathbb{Z}$ $\quad$ $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

Want to solve $x^3 - x + 1 = 0$ $\quad$ $x^3 - x + 1 = 0$.

Consider $K = \mathbb{F}_3[x]/(x^3 - x + 1)$

$K = \mathbb{F}_3[t]/(t^3 - t + 1)$

Elts of K : $\{ a + bt + ct^2 \mid a, b, c \in \mathbb{F}_3 \}$

$$K = \mathbb{F}_3[t] / (t^3 - t + 1)$$

$$= \{ a + bt + ct^2 \mid a, b, c \in \mathbb{F}_3 \}$$

addition = component wise

mult = multiply polys, go mod $t^3 - t + 1$.

Example of a finite field of size 27.

Ex. of a field with 25 elements.

$$\mathbb{F}_5[t] / (t^2 + 3).$$

"$\mathbb{F}_5[\sqrt{-3}]$"

"$\mathbb{F}_5[i]$"

NONSENSE.

Finite fields - Basic facts

① A finite field has size p^n for p prime number & $n \geq 1$.

② For every p prime & $n \geq 1$, there is a finite field of size p^n.

③ A finite field of size p^n is isomorphic to $\mathbb{F}_p[t] / f(t)$ where $f(t) \in \mathbb{F}_p[t]$ is irred. of deg n.

④ Any two finite fields of the same size are isomorphic.

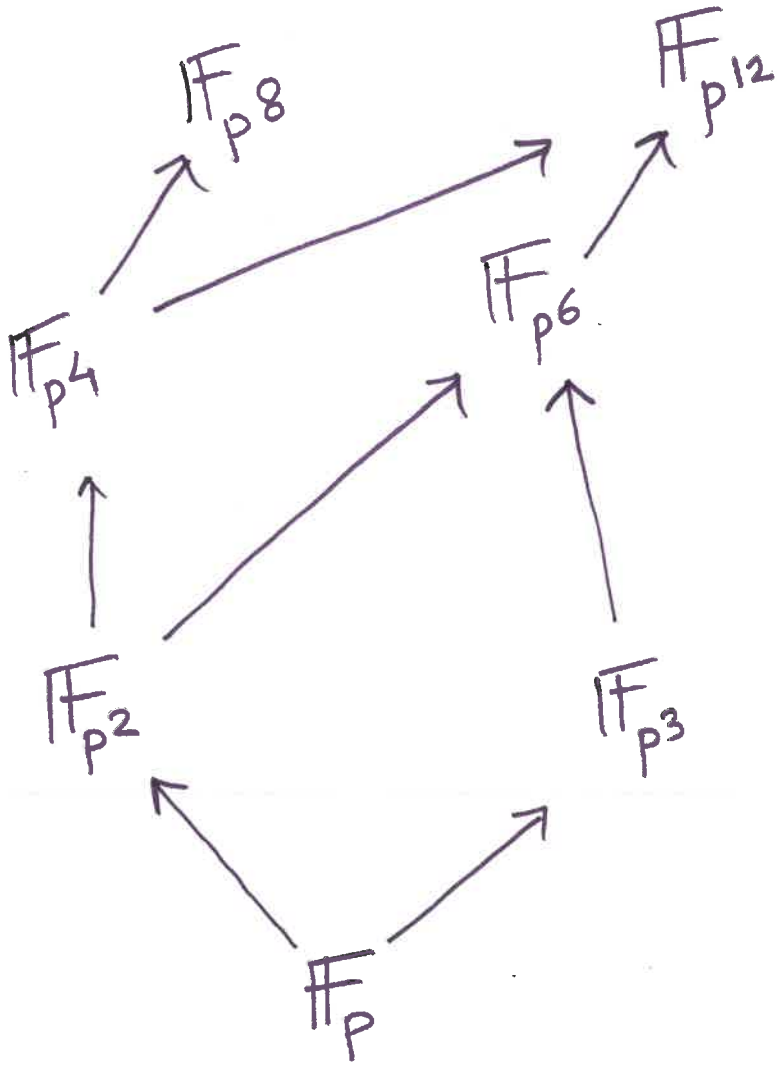
$K \rightrightarrows L$ (n isomorphisms.)

size p^n

$K = GF(243)$.
$K.\text{modulus}()$

Relationships:

Fields of size p^n & q^m have no homs between them if $p \neq q$.



$\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ exists iff $n \mid m$ & then there are exactly n of them.

Any hom. between fields is inj.