Finite fields - existence

Given p, prime and n a positive integer there exists a finite field of size p^n.

↓

Equivalent to : there exists an irred. poly of deg n in $\mathbb{F}_p[t]$.

We'll construct a field of size p^n differently.

↳ Key role = Frobenius & $X^{p^n} - X$.

Prop: Let F be any field. Let $f(x) \in F[x]$ be a non-const. polynomial.

There exists a finite extⁿ of fields

$$F \subset K$$

such that in $K[x]$, the poly $f(x)$ splits into linear factors.

Pf: Example. $f(x) = (\text{sextic}) \cdot (\text{cubic}) \cdot (\text{quintic})$ in $F[x]$

Let $K_1 = F[t]/(\text{sextic})$

then ~~over~~ in $K_1[x]$, have $f(x) = (\text{linear})(\text{quintic}) \cdot (\text{cubic}) \cdot (\text{quintic})$

or a further.

Pick an irred factor of deg > 2, say $g(x)$

pass to $K_i[t]/g(t) =: K_{i+1}$ further factorisation.

$\square$.

Apply it to $F = \mathbb{F}_p$ $\quad f(x) = x^{p^n} - x$

Get $\mathbb{F}_p \subset K$ s.t. in K, $f(x)$ factors into linear factors.

Let $L \subset K$ be

$$L = \{ \alpha \mid \alpha^{p^n} - \alpha = 0 \}$$
$$= \{ \alpha \mid \varphi^n(\alpha) = \alpha \}$$ is a subfield of K.

$\hookrightarrow$ n^{th} iterate of Frob $\leftarrow$ homomorphism.

only thing left $\rightarrow$ $x^{p^n} - x$ has no repeated factors.

Detecting repeated roots $\leftarrow$ Derivative.

F any field. Can define the derivative of $f(x) \in F[x]$ $f(x) \mapsto f'(x)$

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$\mapsto n a_n x^{n-1} + \cdots + a_1$$

$(f(x)+g(x))' = f'(x) + g'(x) \leftarrow$ easy

$(f(x)\,g(x))' = f'(x)\,g(x) + f(x)\,g'(x) \leftarrow$ bit annoying

Prop: If $(x-\alpha)$ is a repeated factor of $f(x)$, then $(x-\alpha)$ divides $f(x)$ & $(x-\alpha)$ divides $f'(x)$.

Pf:

$$f(x) = (x-\alpha)^2 g(x)$$

$$f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha) g(x)$$

$\square$.

$\Rightarrow$ $f(x)$ & $f'(x)$ have a non-constant common factor.

$\gcd(f(x), f'(x))$ is not 1.

Does $\underbrace{x^{p^n} - x}_{f(x).}$ have repeated factors in $K[x]$

$$f'(x) = p^n \cdot x^{p^n - 1} - 1 = -1$$

So there cannot be a common factor to $f(x)$ & $f'(x)$.

$\Rightarrow$ $f(x)$ cannot have repeated roots!

$x^{p^n} - x = \prod$ distinct lin. factors in $K[x]$

$L = \{\alpha \mid \alpha^{p^n} = \alpha\} \subset K$ a subfield of size p^n.

$\square$.

$$\begin{tikzcd}
 & & \vdots & & \\
 & \mathbb{F}_{p^{18}} & & \mathbb{F}_{p^{12}} & \\
\mathbb{F}_{p^9} \arrow[ur] & & \mathbb{F}_{p^6} \arrow[ul] \arrow[ur] & & \mathbb{F}_{p^4} \arrow[ul] \\
 & \mathbb{F}_{p^3} \arrow[ul] \arrow[ur, "3"] & & \mathbb{F}_{p^2} \arrow[ul, "2"'] \arrow[ur, "2"'] & \\
 & & \mathbb{F}_p \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

$\mathbb{Q}[\alpha]$

$\mathbb{Q}[\beta]$

$\underline{\mathbb{Q}[\alpha, \beta]}$.