Splitting field

Example $\mathbb{Q} \subseteq \mathbb{C}$

$f(x) = x^4 - 2$ over $\mathbb{Q}$

over $\mathbb{C}$:

the roots of f are

$\pm \sqrt[4]{2}$, $\pm \sqrt[4]{2} \cdot i$

f is prime in $\mathbb{Q}[x]$

1) $k_1 = \mathbb{Q}[x]/(f)$ is a field

w/ a root α of

$f(x) \in k_1[x]$

$k_1 = \mathbb{Q}(\alpha)$

Say $\alpha = \sqrt[4]{2}$.

$$\mathbb{K}_1 \cong \mathbb{Q}(\sqrt[4]{2}) = \left\{ a + b\sqrt[4]{2} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

over $\mathbb{K}_1$, $f(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2}) \cdot (x^2 + \sqrt{2})$

$$f_1(x) = x^2 + \sqrt{2}$$

$$\mathbb{K}_2 := \mathbb{K}_1[x] / (x^2 + \sqrt{2})$$

f_1 has a root α_1 over $\mathbb{K}_2$

$$\Rightarrow \mathbb{K}_2 = \mathbb{K}_1(\alpha_1)$$

and $f_1(x)$ splits

over $\mathbb{k}_2$

$$f_1(x) = (x - \sqrt[4]{2}\, i)(x + \sqrt[4]{2}\, i)$$

$\Rightarrow$ f splits over $\mathbb{k}_2$

$\Rightarrow$ $\mathbb{k}_2$ is a spliting field of f over $\mathbb{Q}$

$$\mathbb{k}_2 = \mathbb{Q}(\sqrt[4]{2}, i)$$

Last time: a splitting field E for $f(x) \in F[x]$

is unique up to ...

ie if $\mathbb{E}'$ is

also a splitting field

for f (over $\mathbb{F}$)

then $\mathbb{E} \cong \mathbb{E}'$.

observe: Let $\mathbb{F}$ be a field

and $f(x) = \sum_{i=0}^{n} a_i x^i$.

A root α of f is

called repeated root if

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

for some $g(x)$.

Consider the formal n

derivative $Df(x) = \sum_{i=0} i \cdot a_i \cdot x^{(i-1)}$

Then if f has a repeated root then

$f(x)$ and $Df(x)$ have a common factor of deg ≥ 1:

$$\begin{cases} f(x) = (x-2)^2 g(x) \\ Df(x) = 2(x-2) \cdot g'(x) \end{cases}$$

Thm (structure theorem of finite field):

Let p be a prime. Then for any $n \in \mathbb{N}$ there is

a field $\mathbb{F}_q$ with $q = p^n$ elements. Moreover $\mathbb{F}_q$ is unique up to iso.

Proof: (Existence) Consider $f(x) = x^q - x \in \mathbb{F}_p[x]$, and let $\mathbb{E}$ be a splitting field of f.

Then $\mathbb{E}$ has char $= p$ and we may view f as a polynomial over $\mathbb{E}$

Since $Df(x) = q \cdot x^{q-1} - 1 = -1$,

f has no repeated roots in $\mathbb{E}$.

Let $\mathbb{k} = \{ a \in \mathbb{E} \mid a^q - a = 0 \}$

Then $\mathbb{k} \subseteq \mathbb{E}$ is a subfield:

1) $0 \in \mathbb{k}$

2) if $a, b \in \mathbb{k}$ then

$$(a-b)^q = a^q - b^q = a - b$$

so $a - b \in \mathbb{k}$

3) for $a, b \in \mathbb{k}$ w/ $b \neq 0$

$$(a \cdot b^{-1})^q = a^q \cdot (b^q)^{-1} = a \cdot b^{-1}$$

so $ab^{-1} \in \mathbb{k}$.

But f splits over $\mathbb{k}$

so $\mathbb{k} = \mathbb{E}$

Thus $\#\mathbb{E} = q = p^n$

(Uniqueness) Let $\mathbb{E}$ be a field with $q = p^n$ elements.

Then $\mathbb{E}$ is of char $= p$

so there is $\mathbb{F} \subseteq \mathbb{E}$ s.th

$$\mathbb{F} \cong \mathbb{F}_p.$$

Now $\mathbb{E}^\times = (\mathbb{E} \setminus \{0\}, \cdot, 1)$

is an abelian gp of size $q-1$, so $\forall\, a \in \mathbb{E}$,

$$a^{q-1} = 1 \iff a^q - a = 0$$

Thus $\mathbb{E}$ is contained in

thus $\mathbb{E}$ is also a splitting field of

$$f(x) = x^q - x \quad \text{over } \mathbb{F}$$

Since $\#\mathbb{E} = q = p^n$ then $\mathbb{E}$ is a splitting field of f and uniqueness now follows from uniqueness of splitting fields. //

$$f'(x) = \lambda \cdot (x^q - x)$$

Recall: if $\phi(x) \in F[x]$ is a prime poly of deg $\phi = n$ then

$$\mathbb{K} = \mathbb{F}[x]/(\phi) \quad \text{is a field}$$

$$\# \mathbb{K} = \# \mathbb{F}^n$$

$$\left\{ r(x) = a_0 + a_1 x + \dots + a_k x^k \,\middle|\, \begin{matrix} a_i \in \mathbb{F} \\ k < n \end{matrix} \right\}$$

Thus if $\mathbb{F} = \mathbb{F}_p$

then $\# \mathbb{F}_p[x]/(\phi) = \underline{\underline{p^n}} = q$

so $\mathbb{F}_p[x]/(\phi) \cong \mathbb{F}_q$

$$\left(\mathbb{F}_q = GF(p^n) \right)$$

Proposition: Let p be prime.

Then $\forall \underline{\underline{N}} \in \mathbb{N} \quad \exists\ n > N$

and ϕ prime only $\phi(x) \in \mathbb{F}_p[x]$

and a prime poly $\phi(x) \in \mathbb{F}_p[x]$!

of $\deg \phi = n$.

Proof: Assume by contradiction that the claim is false.

Then there are only finitely many prime poly's over $\mathbb{F}_p$,

Say $\phi_1, \dots, \phi_k$.

But then $\phi = \phi_1 \cdot \dots \cdot \phi_k + 1$

is prime since

$\forall i \;\; \phi_i \nmid \phi$ — Contradiction. //

Recall: $(\mathbb{F}_q, +, 0) \qquad q = p^n$

$$\cong \mathbb{F}_p \oplus \dots \oplus \mathbb{F}_p$$

$\underbrace{\quad\quad}_{n\text{ - times}}$

Thm: Let p be a prime and $q = p^n$. Then the multiplicative gp $\mathbb{F}_q^\times = (\mathbb{F}_q \setminus \{0\}, \cdot, 1)$ is cyclic ie $\exists\, \eta \in \mathbb{F}_q^\times$ s.th $o(\eta) = q-1$.

(η is called a primitive element).

Proof: Let $N = \max\{ord(x) \mid x \in \mathbb{F}_q^\times\}$

Since $N \mid \#\mathbb{F}_q^\times = q-1 = p^n - 1$

so $N \leq p^n - 1$.

Applying the 2nd version of the classification of finite

abelian gps, $a \longmapsto \bar{a}$

$\to \mathbb{F}_q^\times \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$

w/ $m_i \mid m_{i+1}$ $\quad m_i \mid m_r$

The maximal order of an element in the RHS is

m_r so $N = m_r$

Thus $\forall\ a \in \mathbb{F}_q^\times \leftarrow$

$\operatorname{ord}(a) \mid m_r = N$

ie $a^N - 1 = 0$

Thus the poly $X^N - 1$

$\in \mathbb{F}_q[X]$ admits at

roots, so

$$p^n - 1 \leq N \leq p^n - 1$$

$$\Rightarrow N = p^n - 1$$

We conclude that $\exists \eta \in \mathbb{F}_q^\times$ s.th $\eta^{q-1} = 1$

$\Rightarrow \mathbb{F}_q^\times$ is cyclic. //

What we had:

$\mathbb{Z}$	$\mathbb{F}[x]$
n	deg n poly
prime	prime poly

long div:

$k = n \cdot q + r$

$r < n$

$g = f \cdot q + r$

$\deg r < \deg f$

$\gcd(k, n)$

$$\begin{cases} k = p_1^{a_1} \cdots p_r^{a_r} \\ n = p_1^{b_1} \cdots p_r^{b_r} \end{cases}$$

$f = p_1^{a_1} \cdots p_r^{a_r}$

w/ p_i prime poly's

$\gcd(f, g)$

Bézout:

$\forall a, b \in \mathbb{Z}$

$\exists u, v \in \mathbb{Z}$:

$au + bv = \gcd(a, b)$

$\Rightarrow \mathbb{Z}_p$ is

a field:

$\varnothing \in \mathbb{F}[x]$ prime

$\mathbb{F}[x]/(\varnothing)$

$a \in \mathbb{F}[x]/(\varnothing)$

$\gcd(a, \varnothing) = 1$

for $a \in \mathbb{Z}_p$

$\gcd(a, p) = 1$

$\Rightarrow \exists\, u, v \in \mathbb{Z}$

$au + pv = 1$

$\Rightarrow au \equiv 1 \bmod p$

$\exists\, u, v \in \mathbb{F}[x]$:

$au + \phi v = 1$

$\Rightarrow au \equiv 1 \bmod \phi$

$\Rightarrow$

$\mathbb{F}[x]/(\phi)$ is a field.

In $k = \mathbb{F}[x]/(\phi)$ $\quad \deg \phi = n$

ϕ has a root

$$k = \left\{ r(x) = a_0 + a_1 x + \cdots + a_k x^k \;\middle|\; \begin{array}{l} a_i \\ \in \mathbb{F} \\ k < n \end{array} \right.$$

$\Rightarrow \underline{F} \subseteq \mathbb{k}$

$$\mathbb{k}[X] = \left\{ r_0(x) + r_1(x)X + \cdots + r_d(x)X^d \;\middle|\; r_i \in \mathbb{k} \right.$$

eg

$$\left(r_0(x) + r_1(x)\,X\right)\cdot\left(r_1'(x)\,X\right)$$

$$= \left(r_0(x)\,r_1'(x) \bmod \phi\right)X + \left(r_1(x)\cdot r_1'(x) \bmod \phi\right)X^2$$

$$\phi(X) \in \mathbb{k}[X]$$

$\wr$

$\pi(x) = r(x) = x \in \mathbb{k}$

$$\phi(X)\Big|_{X=x} = \phi(x) \in \mathbb{k}$$

$$= \begin{vmatrix} x & 0 \end{vmatrix}$$

$$\Rightarrow \phi(x) = (x-2)\cdot\psi(x)$$

over $\mathbb{k}$.

$$\mathbb{k}_1 = F[x]/(\phi)$$

$$\mathbb{k}_1 = F(\alpha)$$

$\psi_1(x)$ over $\mathbb{k}_1$

$$\mathbb{k}_2 = \mathbb{k}_1[x)/(\psi_1)$$

$$\mathbb{k}_2 = \mathbb{k}_1(\alpha_1)$$