May 5

HW 4.4(b) $\zeta = e^{2\pi i/p}$

ζ is a root of $x^p - 1 = (x-1)(\underbrace{x^{p-1} + x^{p-2} + \cdots + 1}_{\text{min poly of } \zeta})$

irred by HW

$\mathbb{Q} \subset \mathbb{Q}(\zeta)$ degree $p-1$

$\underbrace{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}}$ is basis $\zeta^{p-1} \in \mathbb{Q}(\zeta)$

$\underline{\zeta^{p-1}} + \zeta^{p-2} + \cdots + 1 = 0$

Recap

- Given a field ext $K \subset L$, we say $\alpha \in L$ is <u>separable</u> if its minimal polynomial has distinct roots in its splitting field.
- Say $K \subset L$ is <u>separable</u> if every $\alpha \in L$ separable
- Say $f(x) \in K[x]$ <u>separable</u> if its roots are distinct in a splitting field.

<u>Prop</u> If f and f' $\in K[x]$ are rel. prime ($\not\exists$ non-constant $g \in K[x]$ with $g|f$ & $g|f'$) ← derivative

then f is separable.

<u>Pf</u>: $f(x) = \underbrace{(x-\alpha)^2 g(x)}_{\text{factorization in splitting field.}}$ $\boxed{\alpha \text{ not nec in } K}$

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

$\Rightarrow \underbrace{(x-\alpha) \mid f \text{ and } (x-\alpha) \mid f'}_{\text{in}}$

If $g(x)$ is min poly of α
here $g(x) \in K[x]$ $\boxed{(x-1)^2}$

Since $f(\alpha) = f'(\alpha) = 0$,
$g \mid f$ and $g \mid f'$. ∎

<u>Cor</u>: Any irred. poly $f \in K[x]$ with characteristic of K zero is separable. $(f = x^n + a_{n-1}x^{n-1} + \dots)$

<u>Cor</u>: Any extension $K \subset L$ of field of char $= 0$ separable.

(Reason: In char $= 0$,
$\deg(f) = d \Rightarrow \deg(f') = d-1$)

Not true in char $= p$

Ex: $f = x^p$ $f' = px^{p-1} = 0$

Cor: $f = x^{p^n} - x \in \mathbb{F}_p[x]$ is separable.

Reason: $f' = \cancel{p^n \cdot x^{p^n - 1}} - 1$

$= -1$

f & f' are rel. prime

FINITE FIELDS

Goal: ① For each prime p and each $n \geq 1$, there exists a unique field, denoted by $\mathbb{F}_{p^n}$, with p^n elements.

② Moreover, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.

③ $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ normal & separable of degree n

Strategy: If F is a finite field,

$$\mathbb{Z} \xrightarrow{\phi} F$$

$$n \longmapsto \underbrace{1 + 1 + \cdots + 1}_{n}$$

is not injective

The kernel $\ker(\phi) = (p)$ is prime and p is the characteristic.

$\rightsquigarrow \mathbb{F}_p \subset F$ ← vector space / $\mathbb{F}_p$

$n := [F : \mathbb{F}_p]$ $\quad \# F = p^n$

Example

irreducible

$$\mathbb{F}_2[x]/(\cancel{x^3+x+1})$$

$x \mapsto x+1$ $\quad \cong$ How

$$\mathbb{F}_2[x]/(\cancel{x^3+x^2+1})$$

Both are field of size $8=2^3$

Prop Let K be any field. Let $G \subset K^\times$ finite subgp. Then G is cyclic, i.e. $G \cong \mathbb{Z}/n$ for some n.

Ex: $\mathbb{F}_{11}^\times \cong \mathbb{Z}/10$

Cor: $\mathbb{F}_{p^n}^\times \cong \mathbb{Z}/(p^n-1)$

Prop Any field K of order p^n is the splitting field of $x^{p^n}-x$.

Rmk: Since splitting fields are unique, get uniqueness of fields of size p^n!

Proof: Let's first show every element $\alpha \in K$ satisfies $\alpha^{p^n}=\alpha$.

$\alpha=0$ ✓

$\alpha \in K^\times$ and $|K^\times| = p^n-1$

$\Rightarrow \alpha^{p^n-1}=1 \Rightarrow \alpha^{p^n}=\alpha$

$$\rightsquigarrow x^{p^n}-x = \prod_{\alpha\in K}(x-\alpha)$$

and $K = \mathbb{F}_p(\underbrace{\alpha_1, \ldots, \alpha_{p^n}}_{\text{all of the elements in } K})$

Existence

Let $\mathbb{F}_p \subset K$ be splitting field of $x^{p^n} - x$.

Know K contains all p^n roots of $\boxed{x^{p^n} - x}$. But why not anything else?

Let $\alpha_1, \alpha_2, \ldots, \alpha_{p^n}$ be roots

Claim: $K = \{\alpha_1, \ldots, \alpha_{p^n}\}$

$\Rightarrow \#K = p^n$ & $|K : \mathbb{F}_p| = n$

Reason: K is closed under addition & multiplication

$$(\alpha_i + \alpha_j)^{p^n} = \alpha_i^{p^n} + \alpha_j^{p^n}$$
$$= \alpha_i + \alpha_j$$

$\Rightarrow \alpha_i + \alpha_j$ is also a root of $x^{p^n} - x$.

Similarly, $(\alpha_i \alpha_j)^{p^n} = \alpha_i \alpha_j$

Since is the smallest field containing all the roots, we see $K = \{\alpha_1, \ldots, \alpha_{p^n}\}$

Ex: $\sqrt[3]{2}$ and $\sqrt[3]{2}\omega$ are both roots of $x^3 - 2$ but their sum isn't

Consequence:

K is a field of size p^n