3/22

Friday, March 22, 2019 11:33

$F = \mathbb{F}_p(t)$

$f(x) = x^p - t$.

<u>Claim</u> f is irreducible

Let α be a root of f (in some extension), $\alpha = \sqrt[p]{t}$.

Then in $F(\alpha)$, $f(x) = (x-\alpha)^p$.

If f is reducible, $f = gh$ (irreducible g), so $g = (x-\alpha)^k$, $h = (x-\alpha)^{p-k}$
(in $F[x]$)

for some $k \neq 1, p-1$. (if $k=1$, $x - \alpha \in F[x]$ so $\alpha \in F$).

but then g is inseparable (have multiple roots).

but it's not inseparable bc inseparable

polynomials have the form $u(x^p)$ for $u \in F[x]$.

<u>Theorem</u> F ($\operatorname{char} F = p$) is perfect iff $\forall a \in F$, $\sqrt[p]{a} \in F$.

(that is, Frobenius endomorphism is surjective).

<u>Proof</u> $\Leftarrow$ let f be an irreducible inseparable pol-l in $F[x]$.

then $f(x) = a_n x^{np} + \cdots + a_1 x^p + a_0$, $a_i \in F$.

$\forall i$, let $b_i = \sqrt[p]{a_i}$. Then $f(x) = (b_n x^n + \cdots + b_1 x + b_0)^p$,

so f is not irreducible

$\Rightarrow$ Hw. hint: follow above example.

Fields of char 0 are perfect,

finite fields are perfect since Frobenius is surjective.

on $\mathbb{F}_p$, $\Phi = \mathrm{Id}$ by FLT. ($a \in \mathbb{F}_p$ is a root of $x^p - x$ which has $\leq p$ roots, so $\mathbb{F}_p$ is all of them).

f is separable iff $(f, f') = 1$, so if f is irreducible then (since $f' \neq f$), f is separable.

K/F is separable iff any $\alpha \in K$ is separable (has $\deg_F \alpha$ conjugates)

<u>Theorem</u>: If K_1/F, K_2/F are separable, then $K_1 \cap K_2$ is separable. If K/L, L/F are separable, K/F is separable.

<u>Proof</u> Let $\alpha \in K$. Let $f = m_{\alpha,F}$, let $g = m_{\alpha,L}$.

(?)

<u>next time</u>

Cyclotomic Extensions

Roots of unity Let K be a field. The n^{th} roots of unity in K are elements ω s.t. $\omega^n = 1$.

They form a group of order $\leq n$.

roots of unity are roots of $x^n - 1$.

Theorem If G is a finite subgroup of $K^\times$ (mutiplicative group of K), then G is cyclic

Proof if $|G| = n$, then $\forall \alpha \in G$, $\alpha^n = 1$.

Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ s.t. $n_m | \cdots | n_1$.

Then $\forall \alpha \in G$, $\alpha^{n_1} = 1$. So all elements of G are n_1^{th} roots of unity, and roots of $x^{n_1} - x$.

So $|G| \leq n_1$. Thus $n = n_1$, so $G = \mathbb{Z}_{n_1}$.

$n \rightsquigarrow P_n = \{\omega \in K : \omega^n = 1\}$. $|P_n| \leq n$.

P_n is cyclic : $\exists \omega$ s.t. $P_n = \{\omega^k : k \in \mathbb{Z}\}$.

forget about this for a while

Def ω is a primitive root of unity of degree n if $|\omega| = n$.

That is, if $\omega^d \neq 1$ $\forall d < n$.

$x^n - 1$ is separable if char $F = 0$ or if char $F = p$, $p \nmid n$.

Then it has n roots in the splitting field.

The splitting field of $x^n - 1$ is called the cyclotomic Extension of K.

E

in E, $|P_n| = n$.

defn works here in E.

If $p \mid n$, let $n = p^r m$ where $p \nmid m$.

then $x^n - 1 = x^{p^r m} - 1 = (x^m - 1)^{p^r}$.

So $P_n = P_m$.

So we just ignore this case.

E/K - cyclotomic extension.

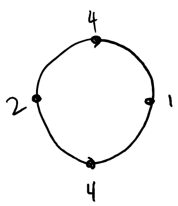
$$\{m : (n,m) = \}$$
$$\|$$
$|P_n| = n$, $P_n \cong \mathbb{Z}_n$, P_n has $\varphi(n)$ generators

These $\varphi(n)$ generators are the primitive roots of unity.

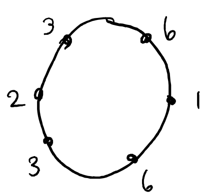
For $K = \mathbb{Q}$, E = cyclotomic extn, $P_n = \{1, \omega, \ldots, \omega^{n-1}\}$

$$\omega = e^{2\pi i/n}$$

$n=4$



$n=6$



$$P_n = \{\text{primitie roots}\} \cup \bigcup_{d|n} P_d.$$

any root of unity is primitive in some degree

$X^n - 1$ Define $\Phi_n(x) = \prod_{\substack{\alpha \text{ is a primitive} \\ \text{root of } 1 \\ \text{of degree } n}} (x-\alpha) = \prod_{\substack{(m,n)=1 \\ 0 \le m < n}} (x - \omega^m)$, ω is primitive of degree n.

Φ_n is the n^{th} cyclotomic polynomial.

$\deg \Phi_n = \varphi(n)$.

We have $x^n - 1 = \prod_{d|n} \Phi_d(x)$ (any root of x^n-1 is a root of exactly one cyclotomic pol-l).

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \nmid n}} \Phi_d(x)}$$

<u>Theorem</u>: Φ_n has integer coefficients