Lecture 33: Finite fields and cyclotomic fields ①

§13.5-13.6 of [DF] §23, 25, 28, 29 of [R3]

Previously: K/F is a splitting field for $f(x) \in F[x]$ if ⓐ f splits completely into linear factors in $K[x]$. ⓑ f does not split completely in any L with $F \subseteq L \subsetneq K$.

Ex: $f(x) = x^3 - 2$ in $\mathbb{Q}[x]$, $\mathbb{Q}(\sqrt[3]{2}, \rho = e^{2\pi i/3})$

A $f(x) \in F[x]$ is <u>separable</u> when all its roots in its splitting field are simple.

The <u>derivative</u> of $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ in $F[x]$ is $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$.

[This has all the standard props, e.g. $(fg)' = f'g + fg'$ no matter what F is.]

Lemma: $f \in F[x]$ is separable $\iff$ f has no common root with f' in a splitting field for $f \cdot f'$ $\iff$ $\gcd(f(x), f'(x)) = 1$.

Pf idea: In a splitting field for $f \cdot f'$, suppose $f(x) = (x-\alpha)^2 g(x)$. Then $f'(x) = 2(x-\alpha) g(x) + (x-\alpha)^2 \cdot g'(x)$ which has α as a root $\Rightarrow f'(x) = (x-\alpha) h(x) \Rightarrow \gcd(f, f')$ is divisible by $(x-\alpha)$.

Cor: If F has char 0, every irreducible $f \in F[x]$ is separable.

Pf: $\deg f' = \deg f - 1$, so $\gcd(f, f') = 1$. ▨

Suppose F is a field of char p. (e.g. $\mathbb{F}_p(t)$)

The Frobenius map $\phi : F \to F$ where $a \longmapsto a^p$ is an injective homom of fields.

Pf: Hard bit is $\phi(a+b) = \phi(a) + \phi(b)$,

Now
$$\phi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$
$$= a^p + \underbrace{p\, a^{p-1} b + \cdots + p\, a b^{p-1}}_{\text{all coeffs are } 0 \bmod p.} + b^p$$

as needed.

Now $\phi(1) = 1$, so $1 \notin \ker \phi$ which implies $\ker \phi = \{0\}$. ▨

Note: If F is finite, ϕ is an isomorphism.

It's not an isom for $\mathbb{F}_p(t)$ as $t \notin \operatorname{im}(\phi)$.

Finite Fields: Basic: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Others: x^2+x+1 is irred in $\mathbb{F}_2[x]$, so

$L = \mathbb{F}_2[x]/(x^2+x+1)$ is a field which is a 2-dim'l F-vector space $\Rightarrow |L| = 4$.

Thm: p prime, $n \geq 1$. Up to isomorphism, there is a unique field $\mathbb{F}_{p^n}$ with p^n elements, namely the splitting field K of $f(x) = x^{p^n} - x$ in $\mathbb{F}_p[x]$.

Ideas: ① Suppose L has $|L| = p^n$. Then $|L^\times| = p^n - 1$ so $a^{p^n-1} = 1$ for all $a \neq 0$ in $L \Rightarrow a^{p^n} = a$ for all $a \in L \Rightarrow$ every elt of L is a root of $x^{p^n} - x$.

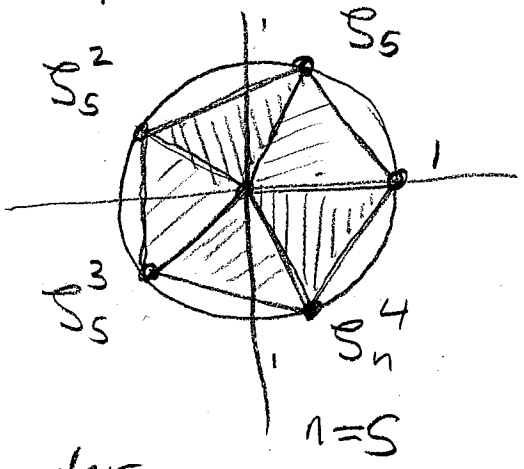
② Set $S = \{$roots of f in $K\}$. Show $S = K$ by

ⓐ S is a subring: $a, b \in S \Rightarrow a^{p^n} = a$, $b^{p^n} = b \Rightarrow$ $f(ab) = 0$, $f(a+b) = (a+b)^{p^n} - (a+b) = a^{p^n} + b^{p^n} - a - b = 0 \Rightarrow ab, a+b$ in S.

ⓑ S is a field as $\forall a \in S$ the map $b \longmapsto ab$ is injective (as S is an it domain), hence surjective (as S is finite).

So $K = S$ and as $f' = -1$, f is separable and so $|S| = \deg f = p^n$.

Cyclotomic Fields: $\mathbb{Q}(\zeta_n)$ where $\zeta_n = e^{2\pi i/n}$



What is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$?

$$\mu_n = \left\{ \begin{matrix} \text{all roots of} \\ X^n - 1 \text{ in } \mathbb{C} \end{matrix} \right\} \subseteq \mathbb{Q}(\zeta_n)$$

Note: μ_n is a cyclic group under multiplication, generated by ζ_n and having order n.

Primitive n^{th} root of unity: a generator of μ_n.

Which ζ_n^k are primitive? Those with $\gcd(k,n) = 1$ since

$$\begin{array}{ccc} \mu_n & \xrightarrow{\cong} & \mathbb{Z}/n\mathbb{Z} \\ \zeta_n^k & \longmapsto & k \end{array}$$

Set $\phi(n) = \#\{1 \le k < n \text{ with } \gcd(k,n) = 1\}$

$= \#\{\text{prim. } n^{th} \text{ roots}\}$

$=$ Euler phi fn.

How to compute: $\phi(p_1^{k_1} \cdots p_m^{k_m}) = \prod_{i=1}^{m} p_i^{k_i-1}(p_i-1)$.

Thm: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Cyclotomic Poly:

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x-\zeta)$$

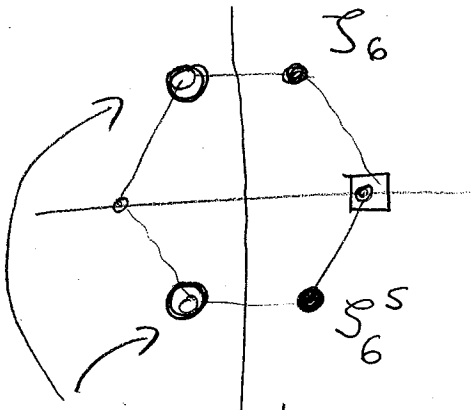
As any $\zeta \in \mu_n$ is a primitive d^{th} root for some $d \mid n$, we have.

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x-\zeta) = \prod_{d \mid n} \prod_{\substack{\zeta \in \mu_d \\ \text{primitive}}} (x-\zeta)$$

$$= \prod_{d \mid n} \Phi_d(x)$$

Ex: $x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6$

$= (x-1)(x+1)(x^2+x+1)(x^2-x+1)$



prim. 3^{rd} roots, set $x^3 - 1 = (x-1)(x^2+x+1)$

Thm: $\Phi_n(x) \in \mathbb{Z}[x]$ and is irreducible.

Pf: See §13.6 of [DF]