Lecture 17: Finite and Cyclotomic Fields.

Previously: $f(x) \in F(x)$ if all its roots are simple, i.e. no multiple roots.

Lemma: $f(x)$ is separable iff it has no common root with $f'(x)$ iff $\gcd(f, f') = 1$.

Frobenius map: F a field of char p
$$\varphi : F \to F \quad \text{with} \quad a \mapsto a^p$$
is a 1-1homomorphism of fields.

Cor For F finite, φ is an isomorphism

Def: A field is perfect if (a) char $= 0$, or
(b) char $= p$ and $x \mapsto x^p$ is an isom

Ex: $\mathbb{Q}, \mathbb{R}, \mathbb{F}_p$ **Non Ex**: $\mathbb{F}_p(t)$

Any alg. closed field

e.g. $\overline{\mathbb{F}_p}$, since $\exists\, b \in F$ with $\varphi(b) = a$ iff $x^p - a$ has a root.

Thm: If F is perfect, then every irreducible polynomial is separable.

Pf: Char 0: Last time.

Char p: Suppose $f \in F[x]$ is irred. with a repeat root. Then as $\gcd(f,f') = 1 \Rightarrow f'(x) = 0$

$$\Rightarrow \quad f(x) = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0$$

$$= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p$$

b_i exist as Frob. is onto

$$= (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0)^p$$

$\Rightarrow f$ is reducible, a contradiction. $\blacksquare$

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

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

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

Thm: p prime, $n \geq 1$. Up to isomorphism, there is a unique field $\mathbb{F}_{p^n}$ with p^n elts.

[In general any finite field has p^n elts]

Construction: Let K be the splitting field of

$$f(x) = x^{p^n} - x \text{ over } \mathbb{F}_p$$

Note f is sep. as $f'(x) = -1$.

Set $S = \{\text{all roots of } f\} \subseteq K$.

Notes: 1 $\mathbb{F}_p \subseteq S$ since $|\mathbb{F}_p^\times| = p-1 \Rightarrow a^{p-1} = 1 \Rightarrow a^p = a$ in $\mathbb{F}_p$.

2 S is a subring

- $a, b \in S$ then $a^{p^n} = a$ and $b^{p^n} = b$.

  So $f(ab) = a^{p^n} b^{p^n} - ab = 0$, and

  $f(a+b) = (a+b)^{p^n} - (a+b) = a^{p^n} - a + b^{p^n} - b = 0$

3 S is a field, as $\forall a \in S$ the map $b \mapsto ab$ is 1-1 (as $S \subseteq K$ has no zero div) and hence onto as S is finite.

So $S = K$ and since f is separable, have $|K| = p^n$.

Uniqueness: Suppose $K/\mathbb{F}_p$ has p^n elts. Then

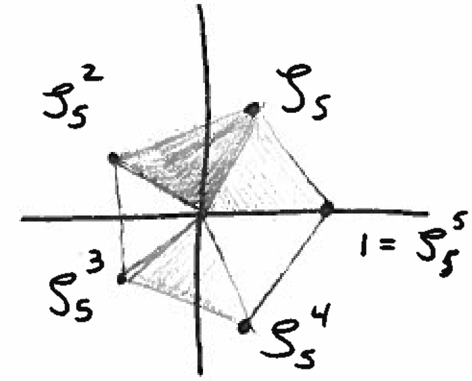
~~K~~ $(K \setminus \{0\}, \times)$ is a gp of order $p^n - 1$

$\Rightarrow a^{p^n-1} = 1 \Rightarrow a^{p^n} - a = 0$ for all $a \in K$.

So K is also a splitting field of $X^{p^n} - X$, and all such are isomorphic. $\square$

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: a generator of μ_n, i.e. $\zeta^k \neq 1$ for $k < n$.

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

$$\mu_n \xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z}$$
$$\zeta_n^k \longmapsto k$$

Set $\varphi(n) = \# \{ 1 \leq k < n \text{ and } \gcd(k,n) = 1 \}$

$= \# \{ \text{prim } k^{th} \text{ roots in } \mu_n \}$

$=$ Euler phi fn.

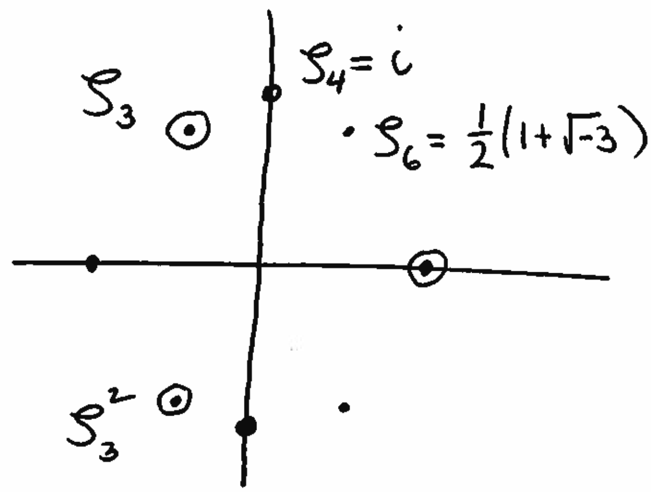
How to compute: $\varphi(p_1^{k_1} \cdots p_m^{k_m}) = \prod_{i=1}^{m} p_i^{k_i - 1}(p_i - 1)$

<u>Thm</u>: $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

<u>Cyclotomic Poly</u>:

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta) = \prod_{\substack{1 \le k < n \\ \gcd(n,k)=1}} (x - \zeta_n^k)$$

<u>Ex</u>: $\Phi_1 = X - 1$



$\Phi_2 = X + 1$

$\Phi_3 = X^2 + X + 1$

$\Phi_4 = X^2 - 1$

$\Phi_5 = X^4 + X^3 + X^2 + X + 1$

$\Phi_6 = (x - \zeta_6)(x - \bar{\zeta}_6) = X^2 - X + 1$

As any $\zeta \in \mu_n$ is a primitive d^{th} root for some $d | n$ 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: $X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1)$

Note: $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$.

Next time: $\Phi_n(x) \in \mathbb{Z}[X]$ and is irreducible