

Lecture 19: Cyclotomic fields

53

$\mathbb{Q}(\zeta_n)$ with $\zeta_n = e^{2\pi i/n}$

$\Phi_n = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta)$. Then $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

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

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

Proof: Suppose Φ_n factors as $f(x)g(x)$ for $f, g \in \mathbb{Z}[x]$ and f is irred.

Claim: If ζ is a root of f . If p is prime, $p \nmid n$, then ζ^p is also a root of f .

if so, let ζ be a fixed root of f . Then any prim. n^{th} root is ζ^m where $m = p_1 \cdots p_k$ and no $p_i \mid n$.

As $\zeta^m = (((\zeta^{p_1})^{p_2})^{p_3} \dots)^{p_k}$ applying the claim repeatedly gives ζ^m is a root of $f(x)$. So $f(x) = \Phi_n(x)$.

Pf of claim: Suppose instead $g(\zeta^p) = 0$. $\zeta \in \sqrt[n]{\mathbb{Z}[x]}$.

Thus ζ is a root of $g(x^p) \Rightarrow g(x^p) = f(x)h(x)$

Let's look in $\mathbb{F}_p[x]$. Some observations

① $X^n - 1$ is separable, since der is $nX^{n-1} \neq 0$.


So $\overline{\Phi}_n(x)$ has distinct roots.

② The Frob. map $\mathbb{F}_p \rightarrow \mathbb{F}_p$ is trivial, since $a^{p-1} - 1 = 0$ for $\forall a \in \mathbb{F}_p \Rightarrow a^p = a$ for all $a \in \mathbb{F}_p$.

Hence

$$\overline{g}(x^p) = \overline{g}(x)^p \quad \text{for any } \overline{g} \in \mathbb{F}_p[x]$$

③ As $\overline{g}(x)^p = \overline{f}(x)\overline{h}(x)$, then \overline{g} and \overline{f} have a common root.

But then $\overline{\Phi}_n(x) = \overline{g}(x)\overline{f}(x)$ has a mult. root, a contradiction. 

Thm: $m \in \mathbb{N}$. There exist ∞ -many primes $p \equiv 1 \pmod m$, i.e. $p = cm + 1$.

[Special case of Dirichlet's Thm on Primes in Arithmetic Progression.]

Proof: Consider $\Phi_m(a)$ for $a \in \mathbb{N}$. Then

- ① There are infinitely many primes dividing some $\Phi_m(a)$.
- ② Any $p \mid \Phi_m(a)$ with $p \nmid m$ has $p \equiv 1 \pmod m$.

[One is true for all m in $\mathbb{Z}[x]$, so focus on ②]

Pf of ②: In \mathbb{F}_p we have

$$a^m - 1 = \Phi_m(a) \cdot \prod_{\substack{d \mid m \\ d < m}} \Phi_d(a) = 0$$

Claim: The order of a in \mathbb{F}_p^\times is m .

Suppose $a^d = 1$ for $d < m$. Now $d \mid m$ and so a is the root of some $\Phi_{d'}$ for $d' \mid m$.

But then $a^m - 1$ has a mult root, which isn't poss since the der of $x^m - 1$ is $mx^{m-1} \neq 0$.
So the order of a in \mathbb{F}_p is m .

Thus $m \mid p-1 \Rightarrow p \equiv 1 \pmod{m}$ as needed.

Proof of ①: More gen, let $f(x) \in \mathbb{Z}[x]$ be monic.

Suppose $\{f(a) \mid a \in \mathbb{N}\}$ have only finitely many prime divisors p_1, \dots, p_k . Choose a so that $f(a) = c \neq 0$

Consider

$$g(x) = c^{-1} f\left(a + \overbrace{c p_1 \cdots p_k x}^y\right) \quad n = \deg f.$$

$$= c^{-1} \left(f(a) + f'(a)cy + \frac{f''(a)}{2}c^2y^2 + \cdots + \frac{f^{(n)}(a)}{n!}c^ny^n \right)$$

$$= 1 + f'(a)y + \frac{f''(a)}{2}cy^2 + \cdots + \underbrace{\frac{f^{(n)}(a)}{n!}c^{n-1}}_{\text{in } \mathbb{Z}}y^n$$

which is in $\mathbb{Z}[x]$.

For any b , have $g(b) \equiv 1 \pmod{p_1 \cdots p_k}$.

Pick b large so that $|g(b)| > 1$. Let

p be any prime factor of $g(b)$. Then

$p \neq \text{any } p_i$, and $p \mid f(a + c p_1 \cdots p_k b)$. \square