Cyclotomic polynomials

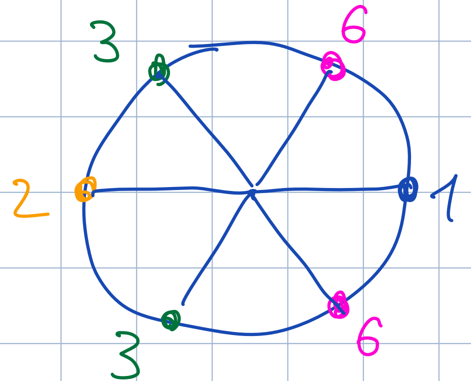
Lecture 7

We want to factorize the polynomial x^n-1 into irreducible factors. If $n=p$ is a prime number, then we know that

$$x^p-1=(x-1)(x^{p-1}+\dots+1), \quad \mu^{\mathbb{Q}}_{\varepsilon_p}=x^{p-1}+\dots+1$$

Exm
$$(x-1)(x^2+x+1) \qquad n=3$$
$$(x-1)(x+1)(x^2+1) \qquad n=4$$
$$(x-1)(x^4+x^3+x^2+x+1) \qquad n=5$$
$$(x-1)(x+1)(x^2+x+1)(x^2-x+1) \qquad n=6$$

For example $(n=6)$



$\mathrm{ord}(\bullet)=6$
$\mathrm{ord}(\bullet)=3$
$\mathrm{ord}(\bullet)=2$

So, define
$$\Phi_n(x):=\prod_{\substack{\varepsilon\in\sqrt[n]{1}\\ \mathrm{ord}(\varepsilon)=n}}(x-\varepsilon).$$

Clearly, $\deg\Phi_n=|\mathbb{Z}_n^*|=\varphi(n)$ ($\mathrm{ord}(\varepsilon)=n$ iff $\varepsilon\in\mathbb{Z}_n^*$)

Let us prove that $\Phi_n\in\mathbb{Z}[x]$. We have

$$\sqrt[n]{1}=\underbrace{\bigsqcup_{d\mid n}}_{\text{disjoint union}}\{\delta\in\sqrt[n]{1}\mid \mathrm{ord}(\delta)=d\}.$$ Thus

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \Rightarrow \Phi_n(x) = \frac{x^n-1}{\prod_{d|n,\, d<n} \Phi_d(x)} \quad (1)$$

$\in \mathbb{Z}[x]$

Clearly, $\Phi_1(x) = x-1$ and therefore by induction $\Phi_n(x) \in \mathbb{Z}[x]$ (indeed, by induction $\prod_{d|n,\, d<n} \Phi_d(x) \in \mathbb{Z}[x]$ and $\forall d$ the leading coefficient of $\Phi_d(x)$ is one $\Rightarrow \Phi_n \in \mathbb{Z}[x]$).

The polynomial $\Phi_n(x)$ is called the n^{th} cyclotomic polynomial and (1) is a recursive formula for $\Phi_n(x)$.

Thm Φ_n is irreducible over $\mathbb{Q}$.

Pf. Let $\varepsilon = e^{\frac{2\pi i}{n}}$ and $\mu := \mu_\varepsilon^{\mathbb{Q}}$ (clearly, $\mu \mid \Phi_n$)

It is enough to prove:

$$\boxed{\mu(\delta) = 0 \Rightarrow \forall p \nmid n \quad \mu(\delta^p) = 0}$$

We have $x^n - 1 = \mu(x)\, g(x)$, $\mu, g \in \mathbb{Z}[x]$ and (Gauss lemma $\rightarrow$) let us fix a prime p, $p \nmid n$. We have $\mu(\delta) = 0$, $\mu(\delta^p) \neq 0$ (otherwise there is nothing to prove). Then $g(\delta^p) = 0$ (since $\delta^p \in \sqrt[n]{1}$) and hence δ is a root of $g(x^p) \Rightarrow \mu(x) \mid g(x^p)$.

Having $f \in \mathbb{Z}[x]$ we write $\bar{f} \in \mathbb{Z}_p[x]$:

$f = \sum c_j x^j \Rightarrow \overline{f} = \sum c_j \pmod p \cdot x^j$.

We have $\overline{x^n - 1} = \overline{\mu(x)} \cdot \overline{g(x)}$. Further $\mu(x) \mid g(x^p) \Leftrightarrow \exists h : g(x^p) = \mu(x) h(x)$. Thus, $\overline{g(x^p)} = \overline{\mu(x)} \cdot \overline{h(x)}$. One has

$(a+b)^p \equiv a^p + b^p \pmod p$ (this formula takes place for $\forall$ field $\mathbb{F}$ s.t. char $\mathbb{F} = p$)

It follows that $\overline{g(x)}^{\,p} = \overline{g(x^p)} = \overline{\mu(x)}\,\overline{h(x)}$ (we also have: $a^p \equiv a \pmod p$) and therefore $\gcd(\overline{\mu}, \overline{g}) \neq 1 \Leftrightarrow \exists\, \overline{\rho} \mid \gcd(\overline{\mu}, \overline{g})$, $\deg \overline{\rho} > 0$. Recalling $\overline{x^n - 1} = \overline{\mu(x)}\,\overline{g(x)} \,\vdots\, \overline{\rho}^2$. We have $(\overline{x^n - 1})' = nx^{n-1}$ and the derivative $\not\equiv 0$ (by assumption $p \nmid n$) $\Rightarrow \overline{x^n - 1}$ has no multiple roots. This is a contradiction. ∎

Cor. 1) $[\mathbb{Q}(e^{\frac{2\pi i}{n}}) : \mathbb{Q}] = \varphi(n)$.
2) $[\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}] = \varphi(n)/2$.
(consider the tower $\mathbb{Q} - \mathbb{Q}(\cos\frac{2\pi}{n}) \overset{2}{-} \mathbb{Q}(e^{\frac{2\pi i}{n}})$, $x^2 - 2\cos\frac{2\pi}{n} \cdot x + 1 = 0$ has roots $\cos\frac{2\pi}{n} \pm i \sin\frac{2\pi}{n}$)

Further $\cos\frac{2\pi}{n} = \dfrac{e^{\frac{2\pi i}{n}} + (e^{\frac{2\pi i}{n}})^{n-1}}{2} =: f(e^{\frac{2\pi i}{n}})$
$\Rightarrow$ (see lecture 6) all algebraic conjugates

of $\cos\frac{2\pi}{n}$ are $\cos\frac{2\pi k}{n}$, $\gcd(k,n)=1$ (we have exactly $\frac{\varphi(n)}{2}$ conjugates, $n>2$).

3) Let $c=\frac{a+bi}{a-bi}\in\sqrt[\infty]{1}$, where $a,b\in\mathbb{Z}$. Then $c\in\{\pm1,\pm i\}$

(Hint. Assume that $b\neq 0 \Rightarrow \mathbb{Q}(c)=\mathbb{Q}(i)$ and since $c\in\sqrt[n]{1}$, it follows that $\varphi(n)=\deg i=2$ $\Rightarrow n\in\{3,4,6\}$ (number theory) $\Rightarrow n=4$ (otherwise $\deg\geq 3$))

Now let K be any field and we want to factorize x^n-1 over K. In this case it is possible to have multiple roots.

Exm $\operatorname{char}K=p \Rightarrow x^p-1=(x-1)^p$

$\exists$ multiple roots $\Leftrightarrow (x^n-1, nx^{n-1})\neq 1 \Leftrightarrow \underset{\uparrow\ \operatorname{char}K}{p}\mid n$
$\Leftrightarrow n=p^k m$, $p\nmid m$. Thus

$$x^n-1=(x^m)^{p^k}-1=(x^m-1)^{p^k} \Rightarrow \sqrt[n]{1}=\sqrt[m]{1}$$

As $p\nmid m$ we see that this problem disappeared.
Further, define $\Phi_1(x):=x-1$ and
$\Phi_n(x):=\dfrac{x^n-1}{\prod\limits_{d\mid n,\, d<n}\Phi_d(x)}$ over any field K.

It follows that $\Phi_n(x) = \prod_{ord(\varepsilon)=n} (x-\varepsilon)$ (exercise),
provided char $K \not| \, n$.
we have the same recursive formula

In general, Φ_n can be reducible, even if char $K \nmid n$.

The same method as above proves

L. Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}^* = \mathbb{F}\setminus\{0\}$ is cyclic group.

Pf. Let $n = |\mathbb{F}^*|$. Then

$$\mathbb{F}^* = \bigsqcup_{d|n} \{\delta \in \mathbb{F}^* \mid ord(\delta) = d\} = \bigsqcup_{d|n} H_d$$

In particular, we obtain $\boxed{\sum_{d|n} \varphi(d) = n \; (*)}$

Take any non-empty $H_d \Rightarrow \exists\, a \in H_d \Rightarrow a^d = 1$ and consider the cyclic group $H = \{1, a, .., a^{d-1}\}$ $\Rightarrow H \subseteq \{x \in \mathbb{F}^* \mid x^d = 1\}$ and in $\mathbb{F}$ there are at most d solutions to this equation. Hence $H = \{x \in \mathbb{F}^* \mid x^d = 1\} \Rightarrow \exists\, \varphi(d)$ elements $x \in H$ s.t. $ord(x) = d$. Therefore, either $|H_d| = 0$ or $|H_d| = \varphi(d)$. But $(*)$ implies that $|H_d| = \varphi(d)$ for all d. In particular, $|H_n| = \varphi(n)$ and hence $\exists$ so many elements of order n in $\mathbb{F}^*$. ∎