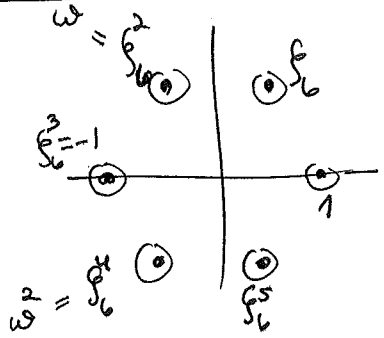
§16.10 (Prime) cyclotomic extensions

DEFN: If $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$ then $\mathbb{Q}(\zeta_n) = (n^{th})$ cyclotomic field $= \text{split}_{\mathbb{Q}}(x^n - 1)$

$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$

not irreducible, so not $m_{\mathbb{Q},\zeta_n}(x)$, unless n is prime.

EXAMPLES: (1) $n=6$

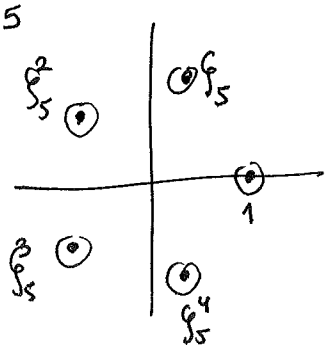


$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$

$= (x-\zeta_6^0)(x-\zeta_6^3)(x-\zeta_6^2)(x-\zeta_6^4)\cdot(x-\zeta_6^1)(x-\zeta_6^5)$

$m_{\mathbb{Q},\omega}(x)$ $m_{\mathbb{Q},\zeta_6}(x)$

(2) $n=5$



$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$

$= (x-1)(x-\zeta_5)(x-\zeta_5^2)(x-\zeta_5^3)(x-\zeta_5^4)$

4/22/2019 >

PROPOSITION (16.19.2): For p prime, the p^{th} cyclotomic polynomial $\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$, so $\Phi_p(x) = m_{\mathbb{Q},\zeta_p}(x)$

and $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has degree $p-1$, and is Galois

with Galois group $G = G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{F}_p^\times \left(\cong (\mathbb{Z}/(p-1)\mathbb{Z})^+ \text{ cyclic}\right)$

via $\left(\sigma_i(\zeta_n) = \zeta_n^i\right) \longleftarrow i$

proof: Back in §12.4 we skipped a cute Eisenstein proof that $\Phi_p(x) = \frac{x^p-1}{x-1}$ is irreducible because $\Phi_p(x+1)$ is:

$$(x-1)\Phi_p(x) = x^p - 1 \quad \overset{\text{replace } x \text{ by } x+1}{\rightsquigarrow} \quad x\Phi_p(x+1) = (x+1)^p - 1$$

$$= x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \dots + \binom{p}{p-2}x^2 + \binom{p}{p-1}x$$

i.e. $\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \underbrace{\binom{p}{p-1}}_{=p}$

all divisible by p (as in our "Freshman dream" proof)
but constant term not divisible by p^2,
so irred. by Eisenstein at p.

Certainly then $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois of degree $p-1 = \deg(\Phi_p(x))$,
and then note that every $\sigma \in G = G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is determined
by $\sigma(\zeta_p) =$ some root of $\Phi_p(x)$
$= \zeta_p^i$ for some i

so $\sigma = \sigma_i$ as described in the PROP, and the map

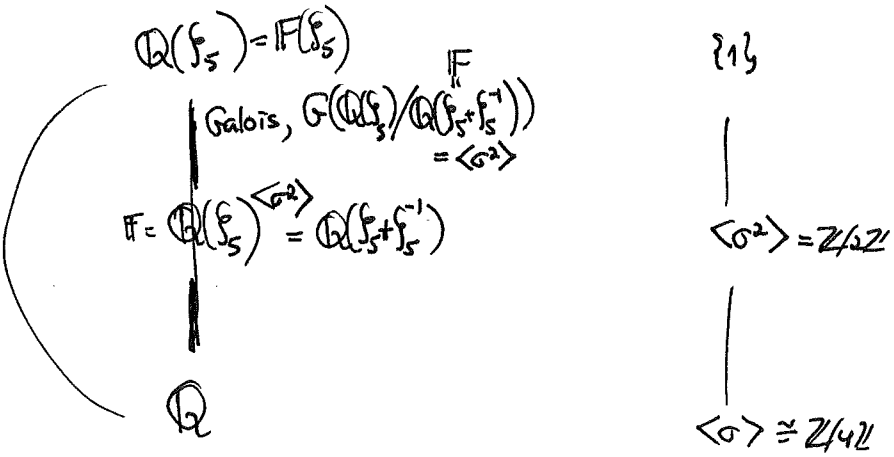
$$\begin{aligned} \mathbb{F}_p^\times &\xrightarrow{\varphi} G \\ \bar{i} &\longmapsto \left(\sigma_i(\zeta_p) = \zeta_p^i\right) \end{aligned}$$

is a group homomorphism since $\bar{i}\cdot\bar{j} \overset{\varphi}{\mapsto} \sigma_{ij}(\zeta_p) = \zeta_p^{ij} = \left(\zeta_p^j\right)^i$
$= \sigma_i(\sigma_j(\zeta_p))$
$= (\sigma_i \circ \sigma_j)(\zeta_p)$

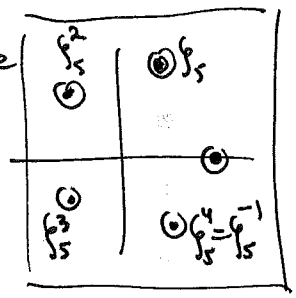
Also since φ surjects, it also injects because $|G| = p-1 = |\mathbb{F}_p^\times|$ ∎

REMARK: Same proof shows for any $\mathbb{F} \overset{\text{subfield}}{\subset} \mathbb{C}$ that $\mathbb{F}(\zeta_p)/\mathbb{F}$ is Galois with $G(\mathbb{F}(\zeta_p)/\mathbb{F})$ a subgroup of $\mathbb{F}_p^\times$, hence a cyclic group (subgroups of cyclic groups are cyclic)

EXAMPLE:

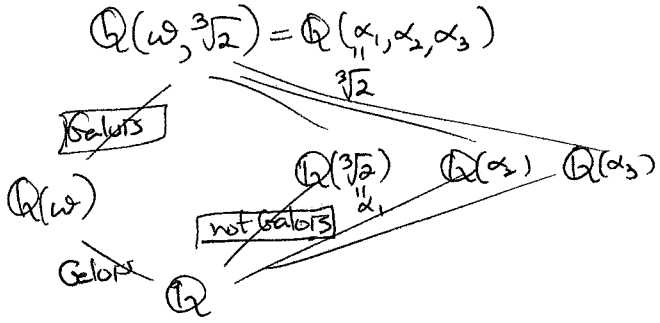


where $\sigma(\zeta_5) = \zeta_5^2$



§16.11 (Prime) Kummer extensions

Generalizing



Its better to have n^{th} roots of unity present in $\mathbb{F}$, before you adjoin n^{th} roots $\sqrt[n]{a}$.
$\{\zeta_n, \zeta_n^2, \cdots\}$

THEOREM: (16.11.1, 16.11.2) Let $\mathbb{Q}(\zeta_p) \subset \mathbb{F} \subset \mathbb{C}$ for some prime p

(a) Any $a \in \mathbb{F}$ either has $x^p - a$ splitting completely in $\mathbb{F}[x]$

or is irreducible in $\mathbb{F}[x]$, in which case

$\mathbb{K} = \text{split}_{\mathbb{F}}(x^p - a) = \mathbb{F}(\sqrt[p]{a})$ has $\mathbb{K}/\mathbb{F}$ Galois of degree p

with Galois group $G = G(\mathbb{K}/\mathbb{F}) = \langle \sigma \rangle$ cyclic of order p

where $\sigma(\sqrt[p]{a}) = \zeta_p \sqrt[p]{a}$

(b) Conversely, if $\mathbb{K}/\mathbb{F}$ is Galois of degree p (and hence $G = G(\mathbb{K}/\mathbb{F})$ is cyclic of order p since $|G| = p$)

then $\mathbb{K} = \mathbb{F}(\sqrt[p]{a})$ for some $a \in \mathbb{F}$ with $x^p - a$ irreducible in $\mathbb{F}[x]$.

proof: (a): Consider $\mathbb{K} = \text{split}_{\mathbb{F}}(\underbrace{x^p - a}_{(x - \sqrt[p]{a})(x - \zeta_p\sqrt[p]{a}) \cdots (x - \zeta_p^{p-1}\sqrt[p]{a})}) = \mathbb{F}(\sqrt[p]{a}, \zeta_p\sqrt[p]{a}, \ldots, \zeta_p^{p-1}\sqrt[p]{a}) = \mathbb{F}(\sqrt[p]{a})$ (since $\mathbb{Q}(\zeta_p) \subseteq \mathbb{F}$)

which has $\mathbb{K}/\mathbb{F}$ Galois. If $[\mathbb{K}:\mathbb{F}] = 1$ then $\mathbb{K} = \mathbb{F}$ and $x^p - a$ splits completely in $\mathbb{F}$.

Otherwise $G = G(\mathbb{K}/\mathbb{F}) \neq \{1\}$ since $|G| = [\mathbb{K}:\mathbb{F}] \geq 2$.

So pick $\sigma \neq 1$ in G, which will be determined by $\sigma(\sqrt[p]{a}) = \zeta_p^i \sqrt[p]{a}$ for some $\bar{i} \in \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$

But $\bar{i} \neq \bar{0}$ implies $\bar{i}$ generates $\mathbb{Z}/p\mathbb{Z}$ (since p is prime), so $\langle \sigma \rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\} \cong \mathbb{Z}/p\mathbb{Z}$

and hence $\deg(m_{\mathbb{F}, \sqrt[p]{a}}(x)) = |G| = p$, so $m_{\mathbb{F}, \sqrt[p]{a}}(x) = x^p - a$ which must be irreducible in $\mathbb{F}[x]$.

(b): Assume $\mathbb{K}$ / degree p, Galois / $\mathbb{F}$ / $\mathbb{Q}(\zeta_p)$, so $G = G(\mathbb{K}/\mathbb{F}) = \langle\sigma\rangle \cong \mathbb{Z}/p\mathbb{Z}$ for some σ (since $|G|=p$).

CLAIM: $\exists$ some $\alpha \in \mathbb{K}$ with $\beta := \alpha + \zeta_p\sigma(\alpha) + \zeta_p^2\sigma^2(\alpha) + \cdots + \zeta_p^{p-1}\sigma^{p-1}(\alpha) \neq 0$.

Assuming the CLAIM for the moment, then note

$$\sigma(\beta) = \sigma(\alpha) + \zeta_p\sigma^2(\alpha) + \zeta_p^2\sigma^3(\alpha) + \cdots + \zeta_p^{p-2}\sigma^{p-1}(\alpha) + \zeta_p^{p-1}\underbrace{\sigma^p(\alpha)}_{=\alpha} = \zeta_p^{-1}\cdot\beta$$

and hence $a := \beta^p$ has $\sigma(a) = \sigma(\beta^p) = \sigma(\beta)^p = (\zeta_p^{-1}\cdot\beta)^p = \underbrace{\zeta_p^{-p}}_{=1}\cdot\beta^p = a$

so $a \in \mathbb{K}^{\langle\sigma\rangle} = \mathbb{K}^{G(\mathbb{K}/\mathbb{F})} = \mathbb{F}$

Also $\beta = \sqrt[p]{a} \notin \mathbb{F}$, else $\sigma(\beta) = \beta$, so $\mathbb{K} = \mathbb{F}(\beta) = \mathbb{F}(\sqrt[p]{a})$ with $a \in \mathbb{F}$, and we'd be done.
($\zeta_p^{-1}\cdot\beta \neq \beta$; $\deg p$ / $\mathbb{F}$)

4/24/2019 >

To prove the CLAIM, we prove a well-known stronger fact

THEOREM (On linear independence of characters)

For any group H, any set of distinct homomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$

$$H \xrightarrow{\sigma_1, \sigma_2, \ldots, \sigma_n} \mathbb{K}^\times$$ into a field $\mathbb{K}$

are $\mathbb{K}$-linearly independent, i.e. $c_1\sigma_1(h) + c_2\sigma_2(h) + \cdots + c_n\sigma_n(h) = 0$ with $c_1, \ldots, c_n \in \mathbb{K}$ $\forall h \in H$

$$\Longrightarrow c_1 = \cdots = c_n = 0.$$

REMARKS: ① This proves the CLAIM taking $H = \mathbb{K}^\times$ and $\sigma_1, \sigma_2, \ldots, \sigma_n$ to be $1, \sigma, \sigma^2, \ldots, \sigma^{p-1}$

② It also proves for any finite extension $[\mathbb{K}:\mathbb{F}] < \infty$ that $|G(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K}:\mathbb{F}]$ without assuming $\mathrm{char}(\mathbb{F}) = 0$, ($G(\mathbb{K}/\mathbb{F}) = \{\sigma_1, \ldots, \sigma_n\}$) using a little work/thought.

proof of THM: Pick a nontrivial dependence $c_1\sigma_1(h) + \cdots + c_{m-1}\sigma_{m-1}(h) + c_m\sigma_m(h) \overset{(*)}{=} 0$ $\forall h \in H$ with $c_1, \ldots, c_m$ all nonzero and m smallest.

We'll produce a nontrivial dependence with smaller m, giving a contradiction.