Cyclotomic extensions

F, $f(x)=x^n-1$ $\qquad f'(x)=nx^{n-1}$

$\gcd(f(x),f'(x)) = \gcd(x^n-1, nx^{n-1}) = 1$ if n is invertible in F
(char $F=0$ or char $F=p$, $p\nmid n$)

Assume char $F=0$, $\mathbb{Q}\subset F$

Take the splitting field E/F.

Def An element ω of a field K is called an n-th root of unity if $\omega^n=1$. If ω has order n in K^*, say ω is a primitive n-th root of unity. If $F\subset K$, field extension $F(\omega)/F$ is called a cyclotomic extension of F.

$\mu_n(F)=\{\omega \mid \omega^n=1\}$ is a subgroup of F^*. Finite, cyclic

$\mu_n(\mathbb{C})=\{e^{\frac{2\pi i k}{n}} \mid 0\le k\le n-1\}$ $\qquad \mu_n(\mathbb{C})\simeq C_n$ - cyclic group of order n

$\mu_3(\mathbb{R})=\{1\}$.

Let char $F=0$, E - splitting field of x^n-1/F.

Prop 1) $|\mu_n(E)|=n$ $\qquad$ n roots of unity of order n,

2) $\mu_n(E)\simeq C_n$ cyclic group

If $h\in C_n$, $\langle h\rangle\subset C_n$ subgroup $\langle h\rangle\simeq C_d$, d order of h

$\Rightarrow \langle h\rangle = C_n$ iff h has order n.

Prop There are $\varphi(n)$ generators in C_n, $\varphi(n)$ Euler phi function

$\varphi(n)=|\{m : 1\le m\le n-1, \gcd(m,n)=1\}|$ $\qquad$ # of residues mod n coprime to n

Facts: $\varphi(p^k)=p^k-p^{k-1}$, $\qquad \varphi(nm)=\varphi(n)\varphi(m)$ if $\gcd(n,m)=1$

Example $\varphi(1200)=\varphi(3\cdot 4\cdot 4\cdot 25)=\varphi(3\cdot 2^4\cdot 5^2)=\varphi(3)\varphi(2^4)\varphi(5^2)=2\cdot(2^4-2^3)(5^2-5)=$
$=2\cdot 8\cdot 20=320$

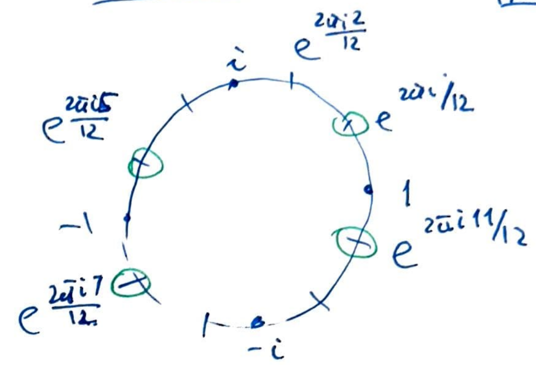
<u>Prop</u> For F, E as above (char $F = 0$, E = splitting field of $x^n - 1$ over F)

$\mu_n(E) \simeq C_n$. E contains n roots of unity, $\varphi(n)$ primitive roots of unity.

For any prim. root of unity ω $\underline{E = F(\omega)}$ $\underline{\omega \text{ is a generator of the splitting field}}$

$\{\omega^m\}_{m=0}^{n-1} = \mu_n(E)$

<u>Example</u> $\mathbb{Q} \subset \mathbb{Q}(e^{\frac{2\pi i}{n}})$ ← primitive



$G = Gal(F(\omega)/F)$

$\sigma \in G$ $\sigma(\omega)$ - a primitive n-th " root of unity

$\varphi(12) = \varphi(4)\varphi(3) = 2 \cdot 2 = 4$

4 primitive 12-th roots of unity

$u = \omega^m$

Once we know $\sigma(\omega)$, know $\sigma(\omega^k) = u^k$ ← all roots of unity.

<u>Corollary</u> $Gal(F(\omega)/F) \subset (\mathbb{Z}/n)^*$ - invertible elements of $\mathbb{Z}/n$

$C_n \longrightarrow \mathbb{Z}/n$

additive notation, need to choose a primitive

$1, \omega, \omega^2, \ldots \omega^{n-1}, \omega^n = 1$ all n-th roots of unity

additive notation

$\{0, 1, 2 \qquad \}$

ω - primitive

$\omega \longmapsto \omega^m$ induces a map

$\omega^k \longmapsto \omega^{km}$ must be a bijection

$Aut(C_n)^* \simeq (\mathbb{Z}/n)^*$

↑ multiplications by m $(m,n) = 1$

$k \longmapsto km$ is an automorphism of C_n if $(m,n) = 1$.

<u>Prop</u> $|(\mathbb{Z}/n)^*| = \varphi(n)$.

$(\mathbb{Z}/n)^*$ is not <u>always</u> cyclic

$(\mathbb{Z}/p)^* \simeq C_{p-1}$ cyclic.

<u>Prop</u> $Gal(F(\omega)/F) \subset (\mathbb{Z}/n)^*$ subgroup

For $F = \mathbb{Q}$, ω - primitive n-th root of unity $\qquad x^n - 1$

<u>Thm</u> $[\mathbb{Q}(\omega):\mathbb{Q}] = \varphi(n)$ - max. possible

$Gal(\mathbb{Q}(\omega)/\mathbb{Q}) = (\mathbb{Z}/n)^*$ $\qquad \mathbb{Q}(\omega) \simeq \mathbb{Q}(e^{\frac{2\pi i}{n}}) \subset \mathbb{C}$

<u>Special case</u>

$n = p$ $\qquad x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + 1)$

$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1$ $\qquad$ p-th cyclotomic polynomial

Recall that $\Phi_p(x)$ irreducible (use Eisenstein crit on $\Phi_p(x+1)$).

ω - root of $\Phi_p(x)$ $\qquad \mathbb{Q}(\omega)/\mathbb{Q}$ $\qquad [\mathbb{Q}(\omega):\mathbb{Q}] = p-1$

$\omega \neq 1$ $\qquad$ already a splitting field $\qquad \omega \mapsto \omega^m$ induces Galois symmetry

$\underbrace{1, \omega, \omega^2, \omega^3, \ldots \omega^{p-1}}_{p-1 \text{ primitive roots}}$ $\qquad \omega^k \mapsto \omega^{km}$

$\omega \mapsto e^{2\pi i/p}$ embedding in $\mathbb{C}$.

$x^p - 1 = (x-1)\underbrace{(x-\omega)(x-\omega^2)\ldots(x-\omega^{p-1})}_{x^{p-1}+x^{p-2}+\ldots+1}$.

$|Gal(\mathbb{Q}(\omega)/\mathbb{Q})| = p-1$ $\qquad Gal(\mathbb{Q}(\omega)/\mathbb{Q}) \simeq (\mathbb{Z}/p)^* \simeq C_{p-1}$ cyclic, $p-1$ elements

$\Phi_n(x)$ - n-th cyclotomic polynomial

$\Phi_n(x) = \prod_{\substack{\zeta \in \mathbb{C} \\ \zeta^n = 1,\ \zeta \text{- primitive } n\text{-th root of unity}}} (x - \zeta)$ $\qquad \Phi_n(x)$ - monic, $\deg \Phi_n(x) = \varphi(n)$

<u>Thm</u> $\prod_{d|n} \Phi_d(x) = x^n - 1$

$x^p - 1 = (x-1)(x^{p-1} + \ldots + 1) = \Phi_1(x)\Phi_p(x)$

$(x+i)(x-i)$

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

$\Phi_1(x) \quad \Phi_2(x) \quad \Phi_4(x)$

$x^8 - 1 = \ldots$ $\qquad \Phi_8(x) = x^4 + 1$

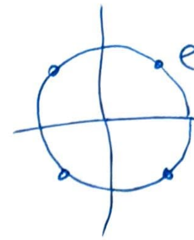
$\Phi_3(x) = x^2 + x + 1$

$f = x^8 - 1$ $\qquad E = \mathbb{Q}(\omega) \subset \mathbb{C}$ splitting field

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

$\uparrow$ irreducible / $\mathbb{Q}$

$\omega = e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}$



8 roots of unity in E

$\underline{\underline{1, \omega}}, \omega^2 = i, \underline{\underline{\omega^3}}, \omega^4 = -1, \underline{\underline{\omega^5}}; \omega^6 = -i, \underline{\underline{\omega^7}},$

$x^4+1 = (x-\omega)(x-\omega^3)(x-\omega^5)(x-\omega^7)$

4 primitive roots $\qquad \varphi(8) = 2^3 - 2^2 = 4$

Galois group $G = \mathrm{Gal}(E/\mathbb{Q}) \qquad |G| = 4$

$\omega \xrightarrow{id} \omega$

$\sigma: \omega \mapsto \omega^3 \qquad \sigma^2 = 1$

$\tau: \omega \mapsto \omega^5 \qquad \tau^2 = 1$

$\sigma\tau \quad \omega \to \omega^7$

$G \simeq C_2 \times C_2$ Klein 4 group

not cyclic

5 subgroups $\{1\}$, $\langle\sigma\rangle\ \langle\tau\rangle\ \langle\sigma\tau\rangle$, G

fixed fields E ... $\mathbb{Q}$

$\sigma\tau$ = complex conj $\omega \mapsto \omega^7 = \omega^{-1}$

$\omega + \omega^{-1} = \sqrt{2}$

fixed by $\sigma\tau$

E

$\cup 2$

$\mathbb{Q}(\sqrt{2}) = E^{\langle\sigma\tau\rangle}$

$\cup 2$

$\mathbb{Q}$

$\tau: \omega \to \omega^5$

$\omega^2 \to \omega^{10} = \omega^2$ fixed $\qquad \omega^2 = \underline{\underline{i}}$

$\mathbb{Q}(i) = E^{\langle\tau\rangle}$

$\mathbb{Q}(-\sqrt{2}) = E^{\langle\sigma\rangle}$

$\omega + \omega^3$ fixed by σ.

$= \frac{1+i}{\sqrt{2}} + \frac{-1+i}{\sqrt{2}} = \sqrt{2}\,i = \sqrt{-2}$

Want to understand radical extensions, add roots of $x^n - c$, $c \in F$, $c \neq 0$

$\uparrow$ has simple roots in char 0.

F, E - splitting field of $x^n - c = f(x)$

contains n roots of $f(x)$. $\alpha_1 \dots \alpha_n$

$$\left(\frac{\alpha_i}{\alpha_j}\right)^n = \frac{\alpha_i^n}{\alpha_j^n} = \frac{c}{c} = 1 \quad \Rightarrow \frac{\alpha_i}{\alpha_j} \text{ is an } n\text{-th root of unity}$$

vice versa, if α - root, ω a n-th root of unity $\Rightarrow \omega\alpha$ is a root of $f(x)$.

$\Rightarrow$ E contains all n-th roots of unity.

E - splitting field of $x^n - c$
|
K - splitting field of $x^n - 1$ $\quad K = F(\omega)$
n-th roots of unity. $\quad \uparrow$ primitive n-th root
|
F

$\Rightarrow$ $Gal(E/F)$ has a normal subgroup $Gal(E/K)$; quotient group $Gal(K/F)$.

$Gal(K/F)$ - abelian, $Gal(E/K)$ - abelian (will see shortly!)

$Gal(E/F)$ - not abelian, in general; built from two ab groups (Rotman, Th. 70)

Thm Let K contain a primitive n-th root of unity, $f(x) = x^n - c \in F[x]$.

If E/K is a splitting field of f, then $\exists$ an injection

$$\gamma: G = Gal(E/F) \longrightarrow \mathbb{Z}/n$$

f irreducible iff γ is surjective.

Proof ω - primitive n-th root $\quad \alpha \in E$ - root of $f \Rightarrow \alpha^n = c$,

$\alpha, \alpha\omega, \dots, \alpha\omega^{n-1}$ are the n roots. $\Rightarrow E = K(\alpha)$.

$\sigma \in G = Gal(E/K) \Rightarrow \sigma(\alpha) = \alpha\omega^i \quad$ σ is determined by i

$\hookrightarrow \sigma(\alpha\omega^k) = \alpha\omega^{i+k} \quad \sigma(\omega) = \omega$

Define $\gamma(\sigma) = \underline{i} \in \mathbb{Z}/n$ (coset)

if $\tau \in G \quad \tau(\alpha) = \alpha\omega^j$

$\tau\sigma: \alpha \longmapsto \alpha\omega^i \longrightarrow \tau(\alpha\omega^i) = \tau(\alpha)\tau(\omega^i) = \alpha\omega^j\omega^i = \alpha\omega^{i+j}$

$\gamma(\tau\sigma) = \gamma(\tau)\gamma(\sigma) = j + i$

γ injective

γ surjective iff G acts transitively on roots of f. $\Leftrightarrow f$ is irreducible

$n=p$ prime case. x^p-c, E, k as before

$\gamma: G \to \mathbb{Z}/p$ $\qquad \gamma(G)=\mathbb{Z}/p$ or $\varphi(G)=\{0\}$ trivial subgroup

$\downarrow$ $\qquad\qquad\qquad\qquad \downarrow \qquad\qquad\qquad\qquad \downarrow$

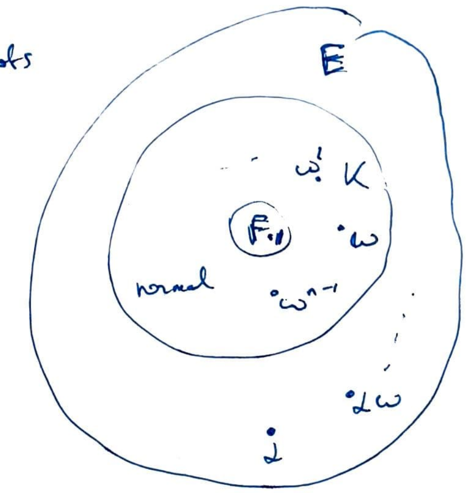
$G \cong \mathbb{Z}/p$ cyclic of order p, x^p-c irreducible

$G=\{0\}$ $\quad E=k$ $\quad x^p-c$ splits into lin. factors in k

Also see Rotman Corollary 72 (page 70) for a related result, where k does not have to contain roots of unity.

In general $f = x^n-c$ splitting field $/F$ char $F=0$ (for simplicity)
$F=\mathbb{Q}$ for instance

E
$|$
$K \leftarrow$ add n-th roots of unity
$|$
F

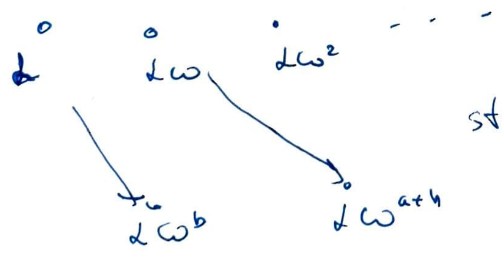


$\omega \overset{\sigma}{\longmapsto} \omega^a$ some a

$\alpha \overset{\sigma}{\longmapsto} \alpha\omega^b$ some b

$\sigma(\alpha\omega)=\sigma(\alpha)\sigma(\omega)=$
$=\alpha\omega^b\omega^a$

$\sigma(\alpha$



stretches by a, shifts by b.

Affine maps $\mathbb{R}\to\mathbb{R}$

$x \longmapsto ax+b$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax+b \\ 1 \end{pmatrix}$$

stretch by a, shift by b.

write down composition

get a group

$\mathrm{Aff}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \begin{array}{l} a\in\mathbb{R}^* \\ b\in\mathbb{R} \end{array} \right\}$

acts on $\mathbb{R}$

$\mathrm{Aff}(\mathbb{Z}/n)$ acts on $\mathbb{Z}/n$ $\quad x \longmapsto ax+b$

$a, b, x \in \mathbb{Z}/n$, a - invertible
$a \in (\mathbb{Z}/n)^*$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ 1 \end{pmatrix}$$

<u>Prop</u> If E/F is a splitting field of $x^n - c$, $c \in F$, char $F = 0$.

There is an injection $\underset{\substack{\parallel \\ G}}{\mathrm{Gal}(E/F)} \xrightarrow{\gamma} \mathrm{Aff}(\mathbb{Z}/n)$.

$$\mathrm{Aff}(\mathbb{Z}/n) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in (\mathbb{Z}/n)^\times,\ b \in \mathbb{Z}/n \right\}.$$

$$\begin{array}{c} E \\ | \\ K = F(\omega) \\ | \\ F \end{array}$$

[illegible] gonal matrices

intersect $\gamma(G)$ with $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{Z}/n \right\}$.

$$\begin{tikzcd} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{Gal}(E/F) \arrow[d, "a \,(\text{forget } b)"'] & \mathrm{Gal}(E/K) \ni \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \arrow[l, hook'] \\ \mathrm{Gal}(K/F) & \end{tikzcd}$$

$x^3 - 2$ $\quad \mathrm{Aff}(\mathbb{Z}/3) \cong S_3$. $\quad x^3 - p$ also get S_3.

full group.

$\mathbb{F}_p \rightarrow \overline{\mathbb{F}_p}$ algebraic closure of $\mathbb{F}_p$

$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^6}$, $\mathbb{F}_p \subset \mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$ or $\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \underbrace{\mathbb{F}_{p^6}}_{3!} \subset \underbrace{\mathbb{F}_{p^{24}}}_{4!} \ldots \subset \mathbb{F}_{p^{n!}} \subset \ldots$

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}$$

$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^{m!}}$

$\mathbb{F}_{p^m}$ - splitting field of $x^{p^m} - x$

$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^{mk}}$

$x^{p^m} - x$ + add all roots of $x^{p^{mk}} - x = (x^{p^m} - x)\, g(x)$.

<u>Thm</u> $\overline{\mathbb{F}_p}$ is alg. closed. $F = \overline{\mathbb{F}_p}$

<u>Proof</u> $f(x) \in F[x]$, monic coeff $a_i \in \mathbb{F}_{p^{n!}}$ some n. $\forall i$

$\deg f = m$. choose $k, {=}\ell!$ $mn! \mid k$ $k = (mn)!$ works.

then $f(x)$ factors in $\mathbb{F}_{p^k}$

$\mathbb{F}_q$ $q = p^r$, f, $\deg f = m$, irr. $\rightarrow \mathbb{F}_{q^m} \supset$ roots of f

$q^m = p^{rm}$

<u>remark</u>

$\overline{\mathbb{F}_p} \simeq \overline{\mathbb{F}_q}$ $q = p^n$

σ: a $\mapsto a^p$ extends to aut. of $\overline{\mathbb{F}_p}$

$|\overline{\mathbb{F}_p}| = \infty$ countable.

σ has ∞ order in $\overline{\mathbb{F}_p}$