$G = G(\mathbb{K}/\mathbb{F})$

There is a convenient test for whether $G(\mathbb{K}/\mathbb{F}) \leq A_n$ or not,

and hence whether $G = A_3$ or S_3 for $\deg(f(x)) = 3$

whether $G \in \{A_4, V_4\}$ or $G \in \{C_4, D_4, S_4\}$ for $\deg(f(x)) = 4$.

DEF'N: (16.2.1) Given $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots \pm (-1)^n s_n \in \mathbb{F}[x]$

$= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in \mathbb{K}[x]$ where $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ (= $\text{split}_{\mathbb{F}}(f(x))$)

so that $s_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}$ = k^{th} elementary symmetric function of $\alpha_1, \dots, \alpha_n$

define the discriminant of f

$$D := D(f) := D(\alpha_1, \dots, \alpha_n) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

EXAMPLE: $n=2$, $f(x) = x^2 - s_1 x + s_2 = x^2 + bx + c$

$= (x-\alpha_1)(x-\alpha_2) = x^2 - \underbrace{(\alpha_1+\alpha_2)}_{s_1} x + \underbrace{\alpha_1\alpha_2}_{s_2}$

$D = D(f) = D(\alpha_1, \alpha_2) = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2$

$= (\alpha_1+\alpha_2)^2 - 4\alpha_1\alpha_2$ (as in $x = \frac{-b \pm \sqrt{b^2-4c}}{2}$)

$= s_1^2 - 4s_2 = b^2 - 4c$

PROP: $D(f) \in \mathbb{Q}(s_1, \dots, s_n)$, i.e. $\exists$ a rational function $\Delta(s_1, \dots, s_n)$ in $s_1, \dots, s_n$ that equals $D(f)$.

($s_1 = \alpha_1 + \dots + \alpha_n$, $s_n = \alpha_1 \cdots \alpha_n$)

(REMARK: Actually, $\Delta(s_1, \dots, s_n) \in \mathbb{Z}[s_1, \dots, s_n]$, i.e. it is a polynomial in $s_1, \dots, s_n$, but that is slightly trickier to prove – see Artin Thm 16.A.6)

EXAMPLE: $n=3$, $f(x) = x^3 - s_1 x^2 + s_2 x - s_3 = x^3 + bx^2 + cx + d$

$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

has $D = D(f) = D(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 = \alpha_1^4\alpha_2^2 + \alpha_1^2\alpha_2^4 + \alpha_1^4\alpha_3^2 + \alpha_1^2\alpha_3^4 + \dots$

$= s_1^2 s_2^2 - 4s_2^3 - 4s_1^3 s_3 + 18 s_1 s_2 s_3 - 27 s_3^2$ (some brute force algebraic manipulation!)

$= b^2c^2 - 4c^3 - 4b^3 d + 18bcd - 27d^2$

e.g. $f_1(x) = x^3 - 2$ ($b=0, c=0, d=-2$) has $D(f_1) = -27(-2)^2 = -108$, while $f_2(x) = x^3 - 3x + 1$ ($b=0, c=-3, d=1$) has $D(f_2) = -4(-3)^3 - 27(1)^2 = (4-1)3^3 = 3^4$

proof of PROP: Consider the field $\hat{K} = \mathbb{Q}(u_1, \dots, u_n)$ of rational functions in variables $u_1, \dots, u_n$

$$\begin{array}{ccc} \hat{K} & = & \mathbb{Q}(u_1, \dots, u_n) \\ \cup & & \\ \hat{F} & = & \mathbb{Q}(s_1(u), s_2(u), \dots, s_n(u)) \end{array}$$

$s_1(u) = u_1 + u_2 + \cdots + u_n$

$s_2(u) = u_1u_2 + u_1u_3 + \cdots + u_{n-1}u_n$

$s_n(u) = u_1u_2 \cdots u_n$

and $f(x) = x^n - s_1(u)x^{n-1} + s_2(u)x^{n-2} - \cdots + (-1)^n s_n(u) \in \hat{F}[x]$

$= \mathbb{Q}(s_1(u), \dots, s_n(u))[x]$

$= (x-u_1)(x-u_2)\cdots(x-u_n)$ in $\hat{K}[x]$, so $\hat{K} = \text{split}_{\hat{F}}(f(x))$

4/19/2019 > Our strategy will be to show two things about the action of S_n on $\hat{K} = \mathbb{Q}(u_1, \dots, u_n)$ by permuting variables: $\sigma(u_i) = u_{\sigma(i)}$ for $\sigma \in S_n$

(i) $\sigma\left(\prod_{1 \le i < j \le n} (u_i - u_j)\right) = \underbrace{\text{sgn}(\sigma)}_{\pm 1} \cdot \prod_{1 \le i < j \le n} (u_i - u_j)$

and hence $\prod_{1 \le i < j \le n} (u_i - u_j)^2 \in \hat{K}^{S_n}$, i.e. it is fixed by all $\sigma \in S_n$

(ii) $\hat{K}^{S_n} = \hat{F}$, so $\prod_{1 \le i < j \le n} (u_i - u_j)^2 \in \mathbb{Q}(s_1(u), \dots, s_n(u))$ i.e. it is a rational function in $s_1(u), \dots, s_n(u)$.

Checking (i) is easy because each adjacent transposition $(k, k+1)$ will send most factors $u_i - u_j$ ($i<j$) to other factors $u_{i'} - u_{j'}$ ($i'<j'$) with same sign, and it negates one factor: $(k,k+1)(u_k - u_{k+1}) = u_{k+1} - u_k = -(u_k - u_{k+1})$.

e.g. $(u_1-u_2)(u_1-u_3)(u_1-u_4)(u_2-u_3)(u_2-u_4)(u_3-u_4)$ $\xrightarrow{\sigma = (1,3)}$ $(u_3-u_2)(u_3-u_1)(u_3-u_4)(u_2-u_1)(u_2-u_4)(u_1-u_4)$ (negated)

Thus $(k,k+1)$ scales $\prod_{i<j} (u_i - u_j)$ by $-1 = \text{sgn}((k,k+1))$, so every $\sigma \in S_n$ scales it by $\text{sgn}(\sigma)$ since $S_n = \langle (1,2), (2,3), \dots, (n-1,n) \rangle$

For (ii), note that

$\hat{K}$

$\cup$ ← degree $n!$ by Fixed Field Thm

$\hat{K}^{S_n}$

$\cup$

$\hat{F}$

degree $\le n!$ since $\hat{K} = \text{split}_{\hat{F}}(f(x))$

$\Rightarrow \hat{F} = \hat{K}^{S_n}$ ∎

THEOREM: (16.8.5, 16.9.5, 16.9.6) When $\mathrm{char}(\mathbb{F})=0$ and $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(f(x))$ for $f(x)=x^n-s_1x^{n-1}+s_2x^{n-2}-\cdots+(-1)^n s_n \in \mathbb{F}[x]$,
$= \prod_{i=1}^{n}(x-\alpha_i)$, $\alpha_i \in \mathbb{K}$

(i) the roots $\alpha_1,\dots,\alpha_n$ contain repeats $\iff D(f)=\Delta(s_1,\dots,s_n)=0$

(ii) the Galois group $G(\mathbb{K}/\mathbb{F}) \leq A_n \iff D(f)$ is a square in $\mathbb{F}$ i.e. $\Delta(s_1,\dots,s_n)=a^2$ for $a\in\mathbb{F}$

EXAMPLE: $f_1(x)=x^3-2 \in \mathbb{Q}[x]$ had $D(f_1)=\Delta(s_1,s_2,s_3)=-108 \neq a^2$ in $\mathbb{Q}$, and $G(\mathbb{K}/\mathbb{F})=S_3 \neq A_3$

but $f_2(x)=x^3-3x+1$ had $D(f_2)=\Delta(s_1,s_2,s_3)=3^4=(3^2)^2$ in $\mathbb{Q}$, and $G(\mathbb{K}/\mathbb{F})=A_3$

---

proof of THM: (i): is clear from the fact that $\Delta(s_1,\dots,s_n)=D(f)=\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2$
$=0 \iff \alpha_i=\alpha_j$ for some $i\neq j$.

(ii): Let $\sqrt{D} := \prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j) \in \mathbb{K}$.

Since every $\sigma \in G(\mathbb{K}/\mathbb{F})$ permutes $\alpha_1,\dots,\alpha_n$, i.e. $\sigma(\alpha_i)=\alpha_{\sigma(i)}$ for some $\sigma\in S_n$

and since we already noted that

$$\sigma(\sqrt{D})=\sigma\Big(\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)\Big)=\prod_{1\leq i<j\leq n}(\alpha_{\sigma(i)}-\alpha_{\sigma(j)})=\underbrace{\mathrm{sgn}(\sigma)}_{\pm 1}\cdot\sqrt{D},$$

one concludes that D is a square ($D=a^2$) in $\mathbb{F}$

$\iff \sqrt{D} \in \mathbb{F} = \mathbb{K}^{G(\mathbb{K}/\mathbb{F})}$

since if $D=a^2$ for $a\in\mathbb{F}$, then $(\sqrt{D})=a^2 \Rightarrow \sqrt{D}=\pm a \in \mathbb{F}$

$\iff \sigma(\sqrt{D})=\sqrt{D} \quad \forall \sigma \in G(\mathbb{K}/\mathbb{F})$

$\iff \mathrm{sgn}(\sigma)=+1 \quad \forall \sigma \in G(\mathbb{K}/\mathbb{F})$

$\iff G(\mathbb{K}/\mathbb{F}) \leq A_n$ ∎

REMARKS: (1) The THM part (i) might suggest a relation between common roots of $f(x), f'(x)$ and vanishing of $\Delta(s_1,\dots,s_n)$, and in fact one can show that in $\mathbb{Z}[s_1,\dots,s_n][x]$ one has $\Delta(s_1,\dots,s_n) \in (f(x),f'(x))$. ← (compare this with EXER. 15.7.11) Keyword: "resultant"

---

(2) Artin discusses in §16.9 Lagrange's resolvent cubic of a quartic $f(x)=x^4-s_1x^3+s_2x^2-s_3x+s_4$ that can be used together with $\Delta(s_1,s_2,s_3,s_4)$ to quickly decide whether $\mathbb{K}=\mathrm{split}_{\mathbb{F}}(f(x))$ has $G(\mathbb{K}/\mathbb{F})=V_4$ or A_4 or S_4 or one of $\{C_4, D_4\}$

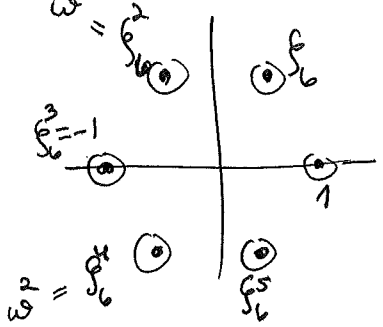
§16.10 (Prime) cyclotomic extensions

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

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

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

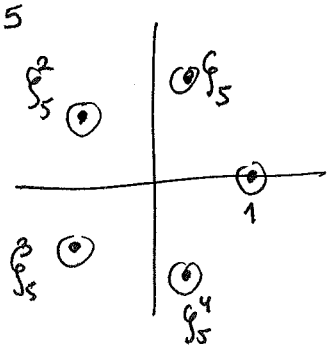
EXAMPLES: (1) $n=6$



$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$
$= (x-\zeta_6^0)(x-\zeta_6^3)(x-\zeta_6^2)(x-\zeta_6^4)\cdot(x-\zeta_6^1)(x-\zeta_6^5)$

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

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

and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 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 $\left(\sigma_i(\zeta_n) = \zeta_n^i\right) \longleftarrow i$