

4/17/07

p. 582 #5, 7, 11, 12, 13

p. 617 4, 5

Recall

$$\begin{aligned}
 \text{SF } x^8 - 2 / \mathbb{Q} &= \mathbb{Q}(\theta, i) & \theta &= \sqrt[8]{2} \\
 &= \mathbb{Q}(\zeta_8, i) & \zeta_8 &= \theta e^{2\pi i/8}
 \end{aligned}$$

Galois group

$$\begin{aligned}
 \sigma: & \begin{cases} \theta \rightarrow \theta \\ i \rightarrow i \\ \zeta \rightarrow -\zeta \end{cases} & \tau: & \begin{cases} \theta \rightarrow \theta \\ i \rightarrow -i \\ \zeta \rightarrow \zeta^7 \end{cases}
 \end{aligned}$$

$$\text{Gal}(\mathbb{Q}(\sqrt[8]{2}, i) / \mathbb{Q}) = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

Example of Galois correspondence

$$H = \langle \sigma^2, \tau \rangle \cong D_8 \quad [G:H] = 2 \text{ so fixed field is degree 2 / } \mathbb{Q}$$

1. Fixed field of $\langle \sigma^2 \rangle$ is $\mathbb{Q}(i, \theta^4)$
2. Fixed field of $\langle \sigma^2, \tau \rangle$ is $\mathbb{Q}(\theta^4) = \mathbb{Q}(\sqrt{2})$

since

$$\begin{aligned}
 \sigma^2: \theta^4 &\rightarrow \theta^4 \theta^2 \theta^2 \\
 \sigma^2: \theta &\rightarrow \theta \zeta^2 \\
 \sigma^2: \theta^4 + \theta^4 \zeta^2 &= \theta^4
 \end{aligned}$$

$$\text{Conversely } \text{Gal}(\mathbb{Q}(i, \theta^4) / \mathbb{Q}(\sqrt{2})) = H$$

Example $\langle \sigma^4, \tau \rangle$ $\langle \sigma^2 \rangle$ both order 4
 \uparrow \uparrow normal/central
 $\mathbb{Q}(\sqrt{2})$ $\mathbb{Q}(i, \sqrt{2})$
 not normal

Galois Groups of Polynomials

* $\text{Deg } f(x) = n$ then $\text{Gal}(f(x)) \hookrightarrow S_n$

* $n \geq 1$

Lemma If $f(x)$ is irreducible, Galois group is transitive on roots

Open Problem Is every finite group a Galois group of a poly / \mathbb{Q}

Section 14.6 - degree 2, 3 & 4 / \mathbb{Q} ex's

SOLVABLE BY RADICALS

Notation: $\sqrt[n]{a}$ denotes any root of $x^n - a$.

Def K/F is cyclic if it is Galois w/ cyclic Galois group

Prop Suppose $\text{char } F \nmid n$, and F contains n^{th} roots of unity.
Then $F(\sqrt[n]{a})$ is cyclic of degree dividing n .

Proof First note it is a SF of $x^n - a$, * and $\sigma \in \text{Gal}(K/F)$
then $\sigma(\sqrt[n]{a}) = \zeta_n^k \sqrt[n]{a}$ for n^{th} root. Thus

$\sigma \mapsto \zeta_n^k$ gives a homo $\text{Gal}(K/F) \hookrightarrow$ cyclic group of n^{th} roots
Kernel is auto which fix $\sqrt[n]{a}$, i.e. id //

The converse also holds

Prop Suppose K/F cyclic, degree n , char $F \nmid n$, F contains n^{th} roots of 1.
Then $K = F(\sqrt[n]{a})$ some $a \in F$.

Proof Let $\text{Gal}(K/F) = \langle \sigma \rangle$. For any $\alpha \in K$, \exists an n^{th} root ζ , define

$$(\alpha, \zeta) = \alpha + \zeta \sigma(\alpha) + \zeta^2 \sigma^2(\alpha) + \dots + \zeta^{n-1} \sigma^{n-1}(\alpha).$$

Check that $\sigma(\alpha, \zeta) = \zeta^{-1}(\alpha, \zeta)$. Thus

$$(\alpha, \zeta)^n \in F \quad \forall \alpha \in K.$$

Choose ζ primitive, and choose α so $(\alpha, \zeta) \neq 0$ (possible by lifting
of $\zeta, \sigma^2, \dots, \sigma^{n-1}$).

Since no $\sigma^i, i < n$ fixes (α, ζ) we must have

$$K = F((\alpha, \zeta)^{1/n}). \quad \text{But } (\alpha, \zeta)^{1/n} \in F \text{ so}$$

$$K = F(\sqrt[n]{a}) //$$

Assume char $F = 0$

Def. Let α be alg. / F . α can be solved in terms of
radicals if $\alpha \in K$ with

$$F = K_0 \subset K_1 \subset \dots \subset K_s = K \quad K_i = K_{i-1}(\sqrt[r_i]{a_i})$$

$F[x] \in F[x]$ can be solved by radicals if $\alpha \in K$
its roots can be.

RMS Can always put in roots of unity

For example

Prop If α is expressed in terms of radicals then it is in a Gal ext K/F in which each K_i/K_{i-1} is cyclic.

<u>Sketch</u>	$K_{i-1}(\sqrt[n]{a})$	just take	$K_{i-1}(\sqrt[n]{a}, \zeta^n)$
	K_{i-1}		$K_{i-1}(\zeta^n)$
			!
			etc

Theorem $f(x)$ can be solved by radicals iff its Galois group is solvable.

COR For $n \geq 5$ there is no "quadratic equation"

Proof

Use result that "generic" poly has Galois group S_n
or

Ex - $f(x) = x^3 - 6x + 3$ in $E-C$.

- Real roots in $\{-2, 0, 1, 1, 2\}$

But $f'(x) = 3x^2 - 6$ only 2 real roots?

Thus 3 real, 2 complex roots. Thus Gal group is S_3 .

Remark Explicit Formulas exist
for degree 2, 3, 4 valid in char $\neq 2, 3$

Remark Real roots expressible by radicals may
need complex #s inside the radicals !!

Example $x^3 + x^2 - 2x - 1 = 0$

$$A = \sqrt[3]{\frac{7}{2} + \frac{\sqrt{-3}}{2}}$$

$$B = \sqrt[3]{\frac{7}{2} - \frac{\sqrt{-3}}{2}}$$

$$p = e^{2\pi i/3}$$

Roots are $\frac{A+B}{3}, \frac{p^2 A + p B}{3}, \frac{p A + p^2 B}{3}$

