MATH 403/503 - L41

[Judson §23.2]

The Fundamental Theorem of Galois theory.

Let E/F be a field extension, and let $G = Gal(E/F)$ be its Galois group.

To any intermediate field M (i.e. a subfield of E containing F) we can associate a subgroup of G, namely $Gal(E/M)$.

Conversely, given any subgroup $H \leq G$, we get an intermediate field, given by

$$E^H := \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$$

called the fixed field of H in E

Exercise i) Show that if $F \subseteq M \subseteq E$ then $Gal(E/M) \leq Gal(E/F)$

ii) Show that if $H \leq Gal(E/F)$, then $F \subseteq E^H \subseteq E$ and E^H is a field.

Def A field extension E/F is *Galois* if E is the splitting field over F of a separable polynomial.

Example $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois because the minimum pol $m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2$ does not split completely over $\mathbb{Q}(\sqrt[3]{2})$. So $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of some pol over $\mathbb{Q}$. x^3-2 is separable though, so $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ is Galois, where $\zeta_3 = \exp(2\pi i/3)$.

Prop 23.17 Let E/F be a Galois extension and $G = Gal(E/F)$ the Galois group. Then $E^G = F$.

Proof $F \subseteq E^G$ is trivial since $\sigma|_F = Id \ \forall \sigma \in G$.

Furthermore, $Gal(E/E^G) = \{\sigma \in Aut(E) \mid \sigma|_{E^G} = Id\}$

~~$= \{\sigma \in Aut(E) \mid \sigma(\alpha) = \alpha \ \forall \alpha \in E \text{ s.t. } [\tau(\alpha) = \alpha \ \forall \tau \in Gal(E/F)]\}$~~

If $\tau \in G$ and $\sigma(\alpha) = \alpha \ \forall \sigma \in G$ then $\tau(\alpha) = \alpha$

so $Gal(E/F) \leq Gal(E/E^G)$

while $Gal(E/E^G) \leq Gal(E/F)$ since $F \subset E^G$

so $G = Gal(E/E^G)$

By theorem 23.7 last time,

$$|\mathrm{Gal}(E/E^G)| = [E : E^G] \quad (\text{since } E/E^G \text{ is also Galois})$$

$$\|$$

$$|\mathrm{Gal}(E/F)| = [E : F]$$

Degree Formula now implies $E^G = F$. ∎

Lemma 23.18. $[E : E^H] \leq |H|$ for any finite $H \leq \mathrm{Aut}(E)$.

Proof Linear alg (see [J. Lem 23.18])

Thm 23.19 TFAE for an extension E/F:

i) E/F is Galois

ii) $F = E^H$ for some finite $H \leq \mathrm{Aut}(E)$.

Proof i) ⇒ ii): By Prop 23.17, $F = E^G$, $G = \mathrm{Gal}(E/F)$.

By Th 23.7 $|G| = [E : F] < \infty$.

ii) ⇒ i): Skip. ∎

Corollary 23.20 If $F \subset M \subset E$ and $M = E^H$ for some finite $H \leq \mathrm{Gal}(E/F)$ then $H = \mathrm{Gal}(E/M)$.

Proof $[E : M] \leq |H| \leq |\mathrm{Gal}(E/M)| = [E : M]$

($\leq$ by Lemma 23.18; second $\leq$ trivial: $\sigma(\alpha) = \alpha$ for every $\sigma \in H, \alpha \in M$; $=$ by Th. 23.7) ∎

Thm (Fundamental Thm of Galois Theory)
Let E/F be a Galois extension, $G = Gal(E/F)$
Then there is a bijective correspondence:

$$\left\{\begin{array}{c}\text{intermediate}\\ \text{fields } M:\\ E\\ |\\ M\\ |\\ F\end{array}\right\} \longleftrightarrow \left\{\begin{array}{cc}\text{subgroups} & G\\ H \text{ of } G: & |\\ & H\\ & |\\ & 1\end{array}\right\}$$

$$M \xmapsto{\Gamma} Gal(E/M) =: \Gamma(M)$$

$$\Phi(H) = E^H \xleftarrow{\Phi} H$$

Furthermore

(1) $M_1 \subseteq M_2 \iff \Gamma(M_1) \geq \Gamma(M_2)$
$H_1 \geq H_2$
i.e. the correspondence is <u>order-reversing</u>

(2) $[E : M] = H$ $\quad (\Rightarrow [M:F] = |G:H|)$

(3) M/F is Galois $\iff H \trianglelefteq G$
in which case
$Gal(M/F) \cong G/H$

Proof Suppose $\Gamma(M_1) = \Gamma(M_2)$. That is,

$F \subset M_1 \subset E$ and $Gal(E/M_1) = Gal(E/M_2) =: H$

$F \subset M_2 \subset E$

Then by Prop 23.17, $M_1 = E^H = M_2$. Thus Γ is injective. Let $H \leq G$ be arbitrary. Let $M = \Phi(H) = E^H$. Then $Gal(E/E^H) = H$ by Cor 23.20, that is, $H = \Gamma(M)$. Thus Γ is surjective.

For (1)-(3), read [J, Th 23.23]. ∎

hence, $\sigma(\alpha)$ must be in the fixed field of $G(E/K)$. Let $\overline{\sigma}$ be the restriction of σ to K. Then $\overline{\sigma}$ is an automorphism of K fixing F, since $\sigma(\alpha) \in K$ for all $\alpha \in K$; hence, $\overline{\sigma} \in G(K/F)$. Next, we will show that the fixed field of $G(K/F)$ is F. Let β be an element in K that is fixed by all automorphisms in $G(K/F)$. In particular, $\overline{\sigma}(\beta) = \beta$ for all $\sigma \in G(E/F)$. Therefore, β belongs to the fixed field F of $G(E/F)$.

Finally, we must show that when K is a normal extension of F,

$$G(K/F) \cong G(E/F)/G(E/K).$$

For $\sigma \in G(E/F)$, let σ_K be the automorphism of K obtained by restricting σ to K. Since K is a normal extension, the argument in the preceding paragraph shows that $\sigma_K \in G(K/F)$. Consequently, we have a map $\phi : G(E/F) \to G(K/F)$ defined by $\sigma \mapsto \sigma_K$. This map is a group homomorphism since

$$\phi(\sigma\tau) = (\sigma\tau)_K = \sigma_K\tau_K = \phi(\sigma)\phi(\tau).$$

The kernel of ϕ is $G(E/K)$. By (2),

$$|G(E/F)|/|G(E/K)| = [K : F] = |G(K/F)|.$$

Hence, the image of ϕ is $G(K/F)$ and ϕ is onto. Applying the First Isomorphism Theorem, we have

$$G(K/F) \cong G(E/F)/G(E/K).$$

■

$$\begin{array}{ccc} E & \longrightarrow & \{\mathrm{id}\} \\ \uparrow & & \downarrow \\ L & \longrightarrow & G(E/L) \\ \uparrow & & \downarrow \\ K & \longrightarrow & G(E/K) \\ \uparrow & & \downarrow \\ F & \longrightarrow & G(E/F) \end{array}$$

Figure 23.24 Subgroups of $G(E/F)$ and subfields of E

Example 23.25 In this example we will illustrate the Fundamental Theorem of Galois Theory by determining the lattice of subgroups of the Galois group of $f(x) = x^4 - 2$. We will compare this lattice to the lattice of field extensions of $\mathbb{Q}$ that are contained in the splitting field of $x^4 - 2$. The splitting field of $f(x)$ is $\mathbb{Q}(\sqrt[4]{2}, i)$. To see this, notice that $f(x)$ factors as $(x^2+\sqrt{2})(x^2-\sqrt{2})$; hence, the roots of $f(x)$ are $\pm\sqrt[4]{2}$ and $\pm\sqrt[4]{2}\,i$. We first adjoin the root $\sqrt[4]{2}$ to $\mathbb{Q}$ and then adjoin the root i of x^2+1 to $\mathbb{Q}(\sqrt[4]{2})$. The splitting field of $f(x)$ is then $\mathbb{Q}(\sqrt[4]{2})(i) = \mathbb{Q}(\sqrt[4]{2}, i)$.

Since $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and i is not in $\mathbb{Q}(\sqrt[4]{2})$, it must be the case that $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Hence, $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. The set

$$\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3, i, i\sqrt[4]{2}, i(\sqrt[4]{2})^2, i(\sqrt[4]{2})^3\}$$

is a basis of $\mathbb{Q}(\sqrt[4]{2}, i)$ over $\mathbb{Q}$. The lattice of field extensions of $\mathbb{Q}$ contained in $\mathbb{Q}(\sqrt[4]{2}, i)$ is illustrated in Figure 23.26(a).

The Galois group G of $f(x)$ must be of order 8. Let σ be the automorphism defined by

$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\sigma(i) = i$, and τ be the automorphism defined by complex conjugation; that is, $\tau(i) = -i$. Then G has an element of order 4 and an element of order 2. It is easy to verify by direct computation that the elements of G are $\{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ and that the relations $\tau^2 = \mathrm{id}$, $\sigma^4 = \mathrm{id}$, and $\tau\sigma\tau = \sigma^{-1}$ are satisfied; hence, G must be isomorphic to D_4. The lattice of subgroups of G is illustrated in Figure 23.26(b). □

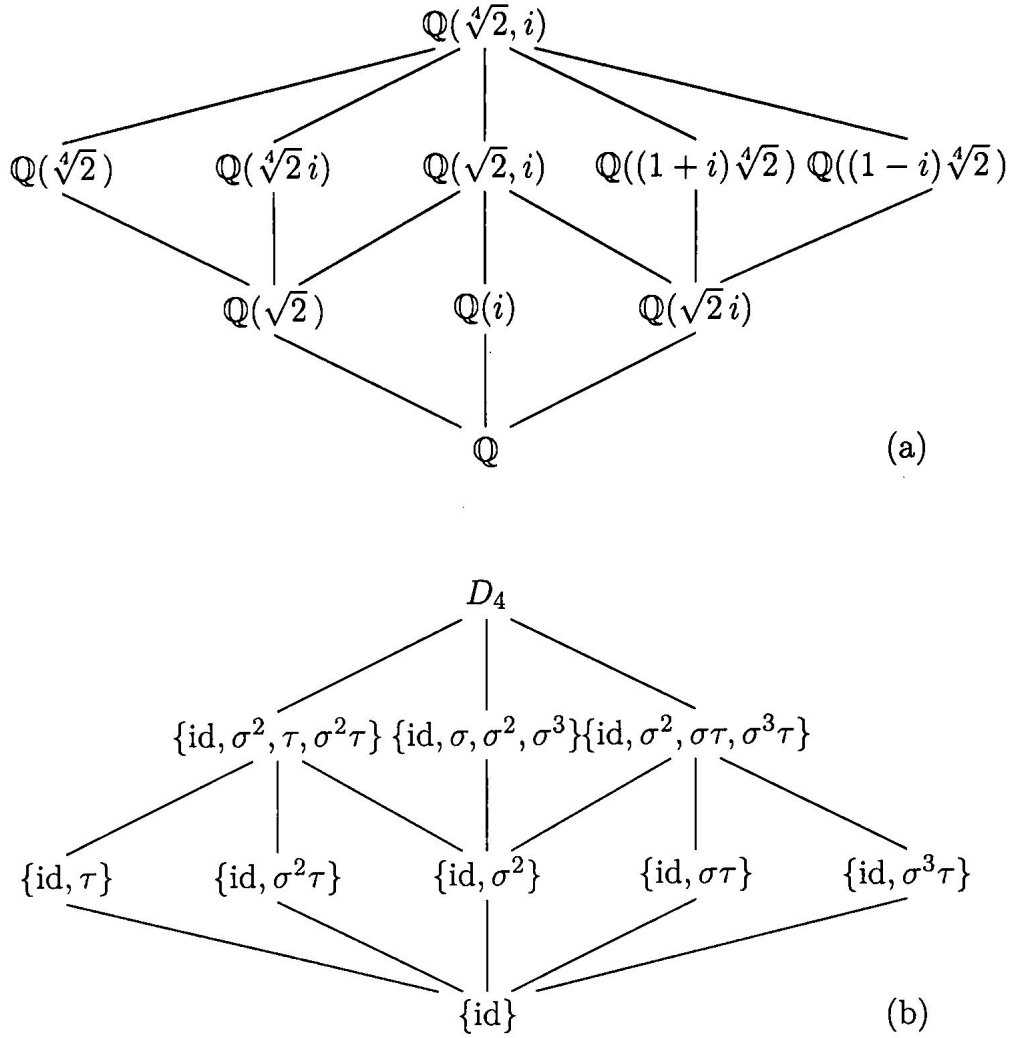

Figure 23.26 Galois group of $x^4 - 2$

Historical Note

Solutions for the cubic and quartic equations were discovered in the 1500s. Attempts to find solutions for the quintic equations puzzled some of history's best mathematicians. In 1798, P. Ruffini submitted a paper that claimed no such solution could be found; however, the paper was not well received. In 1826, Niels Henrik Abel (1802–1829) finally offered the first correct proof that quintics are not always solvable by radicals.

Abel inspired the work of Évariste Galois. Born in 1811, Galois began to display extraordinary mathematical talent at the age of 14. He applied for entrance to the École Polytechnique several times; however, he had great difficulty meeting the formal entrance re-