Galois grou

Chapter 10

Galois Theory

04/11/2016

10.1 Galois Group and Separability

Definition 10.1.1. Let E/F be a field extension. The group of automorphisms of this extension, i.e. the automorphism of E that fix F is denoted by $\mathrm{Aut}_F(E)$ or by $\mathrm{Gal}(E:F)$, and is called the *Galois grou* of the extension E/F.[1]

Note that any automorphism of E fixes 1 and therefore it fixes the prime subfield of E. If $\mathrm{char}(E) = 0$ then $\mathrm{Aut}(E) = \mathrm{Aut}_{\mathbb{Q}}(E)$. If $\mathrm{char}(E) = p$, then $\mathrm{Aut}(E) = \mathrm{Aut}_{\mathbb{Z}_p}(E)$.

Examples 10.1.1.

1. $\mathrm{Aut}_F(F) = \{1_F\}$.
2. $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{1_{\mathbb{C}}, \tau\}$, where τ is complex conjugation, i.e. for $a, b \in \mathbb{R}$, we have $\tau(a + bi) = a - bi$.
3. $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{1\}$, since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, and the only real root of $x^3 - 2$ is $\sqrt[3]{2}$.

[1] Some authors reserve the name Galois group for extensions which are Galois extensions. See Definition 10.2.1.

4. We have already seen that $\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)) \approx D_3$. Since any automorphism of F fixes its prime subfield, we have $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega)) \approx D_3$

The following proposition is a special case of Lemma 5.3.24, by taking $\hat{F} = F$, $\hat{K} = K$, and $\varphi = I_F$.

Proposition 10.1.1 *Let E and K be extensions of F. Let $\alpha \in E$ be algebraic over F, and $\beta \in K$ be a root of $\min_F(\alpha)$. There is a homomorphism $\varphi : F(\alpha) \to K$, that fixes F and such that $\varphi(\alpha) = \beta$.*

The following lemma is a partial converse of the previous proposition.

Lemma 10.1.2 *Let E/F be an extension and $u \in E$ algebraic over F. For each $\varphi \in \text{Aut}_F(E)$, $\varphi(u)$ is a root of $\min_F(u)$ in E.*

Proof. Let $p = \min_F(u)$ be the minimal polynomial of u over F, let $n = \deg(p)$ and let $\alpha_1, \ldots, \alpha_k$ be the distinct roots of p in E, with $\alpha_1 = u$. Then $k \le n = [F(u) : F]$. If we write $p = a_n x^n + \cdots + a_1 x + a_0$ then for any $\varphi \in \text{Aut}_F(E)$, if we apply φ to the equation

$$a_n u^n + \cdots + a_1 u + a_0 = 0,$$

we get

$$a_n \varphi(u)^n + \cdots + a_1 \varphi(u) + a_0 = 0,$$

so, $\varphi(u)$ is also a root of p. ∎

Proposition 10.1.3 *Let $E = F(u)$ be a simple finite extension of F. Then*

$$|\text{Aut}_F(E)| \le [E : F]. \tag{10.1}$$

Proof. By Proposition 5.3.1, u is algebraic over F. Let $p = \min_F(u)$, and let $\alpha_1, \ldots, \alpha_k$ be the distinct roots of p in E, with $\alpha_1 = u$. By Lemma 10.1.2, for any $\varphi \in \text{Aut}_F(E)$, $\varphi(u) = \alpha_i$ for some $i = 1, \ldots, k$, i.e. $\varphi(u)$ is a root of p. By Lemma 5.3.24, for each $i = 1, \ldots, k$, there is an automorphism of E/F that maps u to α_i, and therefore $|\text{Aut}_F(E)| = k \le n = [E : F]$. ∎

Note that in order to get equality in Proposition 10.2.1 it is necessary and sufficient that p has all its roots in E, and that p has no multiple roots.

Scholium 10.1.4 *Let $E = F(u)$ be a finite simple extension. $|\mathrm{Aut}_F(E)| = [E : F]$ iff $f = \min_F(u)$ has no multiple roots, and E is the splitting field of p.*

separable
separable
separable
inseparable

In Examples 10.1.1 we have $|\mathrm{Aut}_F(F)| = 1 = [F : F]$, $|\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})| = 2 = [\mathbb{C} : \mathbb{R}]$, $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))| = 1 < 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, and $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \omega))| = 6 = [\mathbb{Q}(\sqrt[3]{2}, \omega)) : \mathbb{Q}]$.

04/13/2016

Definition 10.1.2. An irreducible polynomial $p \in F[x]$ is said to be ***separable*** over F, if it has no multiple roots. A polynomial $f \in F[x]$ is ***separable*** over F it each of its irreducible factors is separable over F. For an extension E/F and $u \in E$, we say that u is ***separable*** over F if its minimal polynomial $\min_F(u)$ is separable over F, and we say that E is separable over F if every element of E is separable over F. When a polynomial, an extension, or an element is not separable over F, we say that it is ***inseparable*** over F.

Proposition 10.1.5 *An irreducible polynomial $p \in F[x]$ is separable iff $p' \neq 0$.*

Proof. Assume $p' \neq 0$. Since p is irreducible and $\deg(p') < \deg(p)$ no root of p can be a root of p'. By Proposition 5.4.2, p has no multiple roots, hence it is separable.
Conversely, assume p has no multiple roots, then for any root u of p we must have $p'(u) \neq 0$, and therefore $p' \neq 0$. ■

Corollary 10.1.6 *In characteristic 0, all polynomials, all elements and all algebraic extensions are separable.*

Corollary 10.1.7 *Let $\mathrm{char}(F) = p$, and $p \in F[x]$ be irreducible. Then p is not separable iff p is of the form $g(x^p)$ for some $g \in F[x]$.*

Proof. ■

Proposition 10.1.8 *The finite field $\mathbb{F}_{p^n}$ is separable over $\mathbb{Z}_p$.*

Proof. Note that the polynomial $f = x^{p^n} - x$ is separable since it has no multiple roots. Any element of $u \in \mathbb{F}_{p^n}$ is a root of f, so $\min_{\mathbb{Z}_p}(u)$ is a factor of f, hence separable. ■

Proposition 10.1.9 *Let $K/E/F$ be an extension tower. If K is separable over F then K is separable over E and E is separable over F.*

rational functions

field of rational functions

Proof. ■

The converse of Proposition 10.1.9, is true, but we will not prove it.

Proposition 10.1.10 *Every algebraic extension of a finite field is separable.*

From Proposition 10.1.10, and Corollary 10.1.6, we see that the only way to find an inseparable extension, is by looking at infinite fields of prime characteristic. We now define one such field.

04/14/2016 **Board presentations** Problem Set 9

Definition 10.1.3. Let F be a field, and $F[x]$ the ring of polynomials with coefficients in F. Since $F[x]$ is an integral domain, it has a field of quotients. We denote by $F(x)$ the field of quotients of $F[x]$. Each element in $F(x)$ is of the from $\frac{f}{g}$ with $f, g \in F[x]$, and $g \neq 0$. The elements of $F(x)$ are called *rational functions* over F, and we call $F(x)$ the *field of rational functions* over F.

Every polynomial is a rational function, and every rational function is a quotient of two polynomials. Sometimes we will use a variable other than x for the rational functions, so that we can consider polynomials on x over a field of rational functions.

Lemma 10.1.11 *Let $0 \neq h \in F(x)$ be a rational function over F. The integer $\deg(f) - \deg(g)$ where $h = \frac{f}{g}$, with $0 \neq f, g \in F[x]$ is well-defined.*

Proof. Use the fact that for non-zero polynomials, the degree of a product is the sum of the degrees. ■

Definition 10.1.4. For $0 \neq h \in F(x)$ a rational function over F, we denote by $\deg(h)$ the integer $\deg(f) - \deg(g)$ where $h = \frac{f}{g}$, with $0 \neq f, g \in F[x]$.

Example 10.1.2. Let $F = \mathbb{Z}_2(t)$ be the field of rational functions on the variable t. Consider the polynomial $x^2 - t \in F[x]$. Note that for any $0 \neq h = \frac{f}{g} \in F$, we have $\deg(h^2) = \deg(\frac{f^2}{g^2}) = \deg(f^2) - \deg(g^2) = 2\deg(f) -$

$2\deg(g) = 2(\deg(f) - \deg(g)) = 2\deg(h)$ is an even integer. In order to have h as a root of $x^2 - t$ we would neet $h^2 - t = 0$, i.e. $h^2 = t$, but this is impossible since the left hand side has even degree, and the right hand side has degree 1. Being quadratic, with no roots in F, the polynomial $x^2 - t$ is irreducible over F. Let α be a root of this polynomial in some extension E of F. We have $\alpha^2 = t$, and therefore $(x - \alpha)^2 = x^2 - \alpha^2 = x^2 - t$. The irreducible polynomial $x^2 - t$ has α as a root of multiplicity 2, hence it is inseparable. The element α is inseparable over F, and the extension E is inseparable over F. have that

Theorem 10.1.12 [Primitive Element Theorem] *If E/F is a finite, separable extension, then it is a simple extension, that is, there is $u \in E$ such that $E = F(u)$.*

Corollary 10.1.13 *Every finite extension in characteristic 0 is simple.*

04/15/2016 Test 2

04/18/2016

Proof of Primitive Element Theorem. We consider two cases, depending on whether F is finite or not. If F is finite of characteristic p, then E is also finite of characteristic p. By Proposition 10.1.8 E is separable over $\mathbb{Z}_p$, and by Proposition 10.1.9 E is separable over F.

$$\begin{tikzcd}
\mathbb{F}(\beta,\gamma) \arrow[d, dash] \\
\mathbb{F}(\delta) \arrow[d, dash] \\
\mathbb{F}
\end{tikzcd}$$

Now, consider the case when F is infinite. By Proposition 5.3.20, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$, algebraic over F. Using induction, it suffices to show that if $F(\beta, \gamma)$ is a finite separable extension of F, then it is a simple extension of F. Let $p = \min_F(\beta)$, and $q = \min_F(\gamma)$. Let K be a spliting field of $p \cdot q$ that contains $F(\beta, \gamma)$. Let $\beta = \beta_1, \ldots, \beta_m$ be the distinct roots of p in K, and $\gamma = \gamma_1, \ldots, \gamma_n$ the distinct roots of q in K. Since γ is separable over F we have $q = (x - \gamma_1) \cdots (x - \gamma_n)$. There are finitely many elements $\frac{\beta - \beta_i}{\gamma - \gamma_j}$ with $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Since F is infinite, choose $a \in F$ different from all those quotients, and let $\delta = \beta - a\gamma$. Clearly $F(u) \leq F(\beta, \gamma)$. We want to show the other inclusion. Consider the tower $F(\beta, \gamma)/F(\delta)/F$. Let $r = \min_{F(\delta)}(\gamma)$. We have r is a factor of q, since $q(\gamma) = 0$, so the roots of r are some of $\gamma_1, \ldots, \gamma_n$. Consider now $f = p(\delta + ax) \in F(\delta)[x]$. We have

$f(\gamma) = p(\delta + a\gamma) = p(\beta) = 0$, so r is a factor of f, and every root of r is a root of f. For any $i = 1, \dots, m$, and $j = 2, \dots, n$, we have $a(\gamma - \gamma_j) \neq (\beta - \beta_i)$, so $\delta + a\gamma_j = (\alpha - a\gamma) + a\gamma_j = \beta - a(\gamma - \gamma_j) \neq \beta - (\beta - \beta_i) = \beta_i$, and therefore $f(\gamma_j) = p(\delta + a\gamma_j) \neq 0$. Among $\gamma_1, \dots, \gamma_n$ the only root of f is $\gamma_1 = \gamma$, and therefore $r = x - \gamma$, which yields $\deg_{F(\delta)}(\gamma) = 1$, and $\gamma \in F(\delta)$. Since $\beta = \delta + a\gamma$, we also get $\beta \in F(\delta)$, completing the proof that $F(\beta, \gamma) \leq F(\delta)$. ■

Example 10.1.3. For $\omega = \operatorname{cis}(2\pi/3)$ we have $\min_{\mathbb{Q}}(\omega) = x^2 + x + 1$, since $\omega^3 = 1$ and $x^3 - 1 = (x - 1)(x^2 + x + 1)$. The roots of $x^2 + x + 1$ are ω and ω^2, both of which are in $\mathbb{Q}(\omega)$, so we have two automorphisms of $\mathbb{Q}(\omega)$, which depend on where they map ω to. There is the identity $I : \omega \mapsto \omega$ and $\tau : \omega \mapsto \omega^2$. Clearly, $\tau^2 : \omega \mapsto \omega^4 = \omega$ is the identity, and $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) = \{I, \tau\}$ is the cyclic group of order 2.

We generalize this example in the following proposition.

Proposition 10.1.14 *Let p be a prime number, and let $\xi_p = \operatorname{cis}(2\pi/p)$. Then $\min_{\mathbb{Q}}(\xi_p) = x^{p-1} + x^{p-2} + \cdots + x + 1$, and $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi_p)) \approx C_{p-1}$.*

Proof. ξ_p satisfies $\xi_p^p = 1$, so it is a root of $x^p - 1$. This polynomial factors as

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

04/20/2016 and since $\xi_p \neq 1$, it is a root of $\varphi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1$. We want to show that $\varphi_p(x)$ is irreducible over $\mathbb{Q}$. Note that $(x+1)^p - 1 = x \cdot \varphi(x+1)$, and we have

$$\begin{align}
(x^p + 1) - 1 &= \left(\sum_{i=0}^{p} \binom{p}{i} x^i\right) - 1 \tag{10.2}\\
&= \sum_{i=1}^{p} \binom{p}{i} x^i \tag{10.3}\\
&= x \cdot \sum_{i=1}^{p} \binom{p}{i} x^{i-1}, \tag{10.4}\\
& \tag{10.5}
\end{align}$$

so, cancelling the common factor x, we get

$$\begin{align} \varphi_p(x) &= \sum_{i=1}^{p} \binom{p}{i} x^{i-1} \tag{10.6}\\ &= \sum_{i=0}^{p-1} \binom{p}{i+1} x^{i} \tag{10.7}\\ & \tag{10.8} \end{align}$$

We know that for $i = 1, \dots, p-1$ the binomial coefficient $\binom{p}{i}$ is divisible by p, and the constant term, $\binom{p}{1} = p$ is not divisible by p^2. By Proposition 4.1.24[Eisenstein Criterion], we get that $\varphi(x+1)$ is irreducible over $\mathbb{Q}$. Since any factorization of $\varphi(x)$ yields a factorization of $\varphi(x+1)$, and viceversa, it follows that $\varphi(x)$ is also irreducible over $\mathbb{Q}$. ■

Proposition 10.1.15 *Let p be a prime number, $n \geq 1$, and $E = \mathbb{F}_{p^n}$. The automorphism group $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ is cyclic of order n, generated by the Frobenius automorphism Φ_p.*

Proof. Since E is finite and the Frobenius endomorphism $\Phi_p : E \to E$ is injective and fixes the prime subfield, we have $\Phi_p \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$. The elements of E all satisfy $x^{p^n} = x$, i.e $\Phi_p^n(x) = x$, so $\Phi_p^n = I_E$. Since $E/\mathbb{R}_p$ is a simple extension, for a primitive element $u \in E$ of this extension, n is the smallest integer such that $u^{p^n} = u$, so it is also the smallest integer such that $\Phi_p^n = I_E$, and Φ_p has order n. But Proposition 10.1.3 tells us that $|\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})| \leq [E : \mathbb{F}_p] = n$. Therefore $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ is cyclic of orde n, generated by the Frobenius automorphism Φ_p. ■

04/21/2016

Theorem 10.1.16 *Let $E = F(u_1, \dots, u_n)$ be a finite extension of F. Let $m_i = \min_F(u_i)$ and $r_i = \deg(m_i)$. For $\sigma, \tau \in \mathrm{Aut}_F(E)$*

1. *$\sigma(u_i)$ is a root of m_i for each $i = 1, \dots, n$.*
2. *$\sigma = \tau$ iff $\sigma(u_i) = \tau(u_i)$ for each $i = 1, \dots, n$.*
3. *σ is uniquely determined by the choice of $\sigma(u_1), \dots, \sigma(u_n)$.*

4. $|\mathrm{Aut}_F(E)| \leq r_1 \cdot r_2 \cdots r_n$.

Proof.

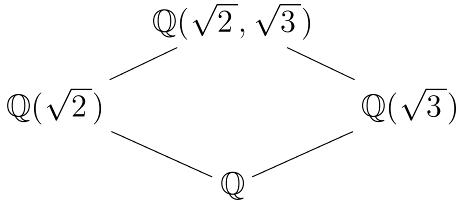
1. This follows from Lemma 10.1.2.

2. ($\Rightarrow$) is obvious.
   ($\Leftarrow$) Let $\lambda = \tau^{-1} \circ \sigma$. Note that $\lambda \in \mathrm{Aut}_F(E)$, and λ fixes every element of F and each u_i, since $\lambda(u_i) = \tau^{-1}\sigma(u_i) = \tau^{-1}\tau(u_i) = u_i$. It follows that the subfield of E, fixed by λ, E_λ contains $F(u_1, \ldots, u_n$, and therefore $E_\lambda = E$. But this tells us that $\lambda = I_E$, and therefore $\sigma = \tau$.

3. Follows from part (2).

4. For each $\sigma \in \mathrm{Aut}_F(E)$ and each $i = 1, \ldots, n$, there are at most r_i choices for $\sigma(u_i)$. Use now part (3). ■

■



Example 10.1.4. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. The minimal polynomials are $x^2 - 2$ and $x^2 - 3$, with roots $\pm\sqrt{2}$ and $\pm\sqrt{3}$, respectively. For $\sqrt{2}$ there are two choices, and for $\sqrt{3}$ there are also two choices, for a total of 4 potential automorphisms. So we get that $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))| \leq 4$. (Note also, that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$) The potential automorphisms are given by

$$\begin{array}{rrcl@{\qquad}rrcl}
I: & \sqrt{2} & \mapsto & \sqrt{2} & \sigma_1: & \sqrt{2} & \mapsto & \sqrt{2} \\
 & \sqrt{3} & \mapsto & \sqrt{3} & & \sqrt{3} & \mapsto & -\sqrt{3} \\[1em]
\sigma_2: & \sqrt{2} & \mapsto & -\sqrt{2} & \sigma_3: & \sqrt{2} & \mapsto & -\sqrt{2} \\
 & \sqrt{3} & \mapsto & \sqrt{3} & & \sqrt{3} & \mapsto & -\sqrt{3}
\end{array}$$

Since $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $x^2 - 3$ over $\mathbb{Q}(\sqrt{2})$, Corollary 5.3.25, tells us that the there are automorphisms doing the above. Moreover, notice that $\sigma_1, \sigma_2, \sigma_3$ have order 2. Therefore, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ is the Klein 4-group.

Example 10.1.5. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ has degree 4, since $\min_{\mathbb{Q}}(\sqrt[4]{2}) = x^4 - 2$ (use Eisenstein' criterion to check irreducibility). However, only

two of the four roots, namely $\pm\sqrt[4]{2}$ are in the extension, and therefore $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}))| \leq 2$. Corollary 5.3.25, guarantees the existence of both automorphisms, $(\sqrt[4]{2} \mapsto \sqrt[4]{2})$, and $(\sqrt[4]{2} \mapsto -\sqrt[4]{2})$. Thus, we have $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}))$ is cyclic of order 2.
The splitting field of $x^4 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\sqrt[4]{2}, i)$, which has degree 8 over $\mathbb{Q}$. In this case, there are four choices of where to map $\sqrt[4]{2}$, i.e. $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. There are two choices of where to map i, i.e. $\pm i$. For a total of 8 potential automorphism of this extension. Therefore, $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))| \leq 8$. We will see, that in this case equality holds.

Recall that an action of a group G on a set X consists of a function $G \times X \to X$, where the image of (σ, u) is written as u^σ, or $\sigma \cdot u$, or $\sigma(u)$, satisfying

1. $1(u) = u$,
2. $\sigma(\tau(u)) = (\sigma\tau)(u)$.

A group action of G on X induces a group homomorphism

$$\begin{array}{rccc} \Theta : & G & \to & S_X \\ & \sigma & \mapsto & \left(\begin{array}{ccc} X & \to & X \\ u & \mapsto & \sigma(u) \end{array}\right) \end{array}$$

Corollary 10.1.17 *In the setting of Theorem 10.1.16, let*

$$X = \{u \in E | m_i(u) = 0 \textit{ for some } i = 1, \dots, n\}$$

i.e. the set of roots in E of all $m_i(x)$, and let $G = \mathrm{Aut}_F(E)$. The group G acts on the set X, and each $\sigma \in G$ induces a permutation of X.

Proof. Part 1 of Theorem 10.1.16, allows us to define the map

$$\begin{array}{c} G \times X \to X \\ (\sigma, u) \mapsto \sigma(u) \end{array}$$

Clearly, this map is a group action. For each $\sigma \in G$, the restriction $\sigma|_X : X \to X$ is a permutation of X. ■

Definition 10.1.5. Let G be a group acting on a set X. We say that the action is ***transitive***, if for all $u, v \in X$ there is $\sigma \in G$, such that $\sigma(u) = v$. We say that the action is ***faithful*** if the induced homomorphism $\Theta : G \to S_X$ is injective.

transitive
faithful

From Theorem 10.1.16.2 we immediately get.

Corollary 10.1.18 *In the setting of Corollary 10.1.17, the action of* $G = \mathrm{Aut}_F(E)$ *on the set* X *of roots, is faithful. In other words,* G *is isomorphic to a subgroup of* S_X.

04/22/2016

Proposition 10.1.19 *Let* E/F *be a finite extension, such that* E *is the splitting field of a non-constant monic polynomial* $f \in F[x]$. *Let* $G = \mathrm{Aut}_F(E)$, *and* X *the set of roots of* f *in* E.

1. *If* f *is irreducible over* F, *then* G *acts transitively on* X.
2. *If* G *acts transitively on* X, *then* f *is a power of an irreducible polynomial over* F, *i.e.* f *has a single irreducible factor.*
3. *If* f *has no repeated irreducible factor, and* G *acts transitively on* X, *then* f *is irreducible.*
4. *If* f *has no multiple roots, and* G *acts transitively on* X, *then* f *is irreducible.*

Proof.

1. Given $u, v \in X$, two roots of f, Proposition 10.1.1 tells us that there is $\sigma \in \mathrm{Aut}_F(E)$ such that $\sigma(u) = v$.
2. We prove the contrapositive. Suppose f has at least two distinct irreducible factors g and h. Let u is a root of g and v is a root of h. WLOG we may assume both g and h are monic, so that $\min_F(u) = g \neq h = \min_F(v)$. Since the minimal polynomial is unique, it follows that v is not a root of g, and by Lemma 10.1.2, there is no $\sigma \in \mathrm{Aut}_F(E)$ such that $\sigma(u) = v$.
3. Follwos immediately from (2).

4. Follwos immediately from (3). ■

$$\begin{tikzcd}
E \arrow[dd, dash] & & & \hat{K} \arrow[ddd, dash] \\
& & \hat{\alpha} & \\
F(\alpha) \arrow[uurrr, "\tilde{\varphi}"] \arrow[d, dash] & \alpha \arrow[ur, mapsto, dashed] & & \\
F \arrow[rrr, "\varphi"] & & & \hat{F}
\end{tikzcd}$$

Lemma 10.1.20 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Let $f \in F[x]$ be an irreducible polynomial, and denote by $\hat{f}$ its image $\varphi(f) \in \hat{F}[x]$. If α is a root of f in some extension E of F, $\hat{K}$ an extension of $\hat{F}$, and $\tilde{\varphi} : F(\alpha) \to \hat{K}$ a homomorphism that extends φ, then $\hat{\alpha} = \tilde{\varphi}(\alpha)$ is a root of $\hat{f}(x)$.*

Proof. $\hat{f}(\hat{\alpha}) = \varphi(f)(\tilde{\varphi}(\alpha)) = \tilde{\varphi}(f)(\tilde{\varphi}(\alpha)) = \tilde{\varphi}(f(\alpha)) = \tilde{\varphi}(0) = 0$ ■

Corollary 10.1.21 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Let E be an extension of F, and $u \in E$ algebraic over F, and $\hat{K}$ an extension of $\hat{F}$. The number of homomorphism $\tilde{\varphi} : F(u) \to \hat{K}$ which extend φ is at most $\deg_F(u)$.*

Proof. Any homomorphism $\tilde{\varphi} : F(u) \to \hat{K}$ that extends φ is completely determined by the value fo $\tilde{\varphi}(u)$. Take $f = \min_F(u)$ in the lemma. Since $\deg_{\hat{F}}(\hat{f}) = \deg_F(f) = \deg_F(u)$, the polynomial $\hat{f}$ has at most this many distinct roots, so there are at most $\deg_F(u)$ choices for $\tilde{\varphi}(u)$. ■

Scholium 10.1.22 *Let F and $\hat{F}$ be fields, and $\varphi : F \to \hat{F}$ a homomorphism. Let E be an extension of F, and $u \in E$ algebraic over F, and $\hat{K}$ an extension of $\hat{F}$. Let $f = \min_F(u)$, and $\hat{f} = \varphi(F)$. The number of homomorphism $\tilde{\varphi} : F(u) \to \hat{K}$ which extend φ is the number of distinct roots of $\hat{f}$ in $\hat{K}$.*

04/25/2016

10.2 The Fundamental Theorem of Galois Theory

The following proposition generalizes Proposition 10.1.3, by removing the hypothesis of simple extension. To prove it we refine the argument used to prove Theorem 10.1.16.4.

Proposition 10.2.1 *Let E/F be a finite extension. Then*

$$|\mathrm{Aut}_F(E)| \leq [E : F]. \tag{10.9}$$

Proof. Choose $u_1, \ldots, u_n \in E$, recursively such that $u_i \notin F(u_1, \ldots, u_{i-1})$. Let $m_i = \min_{F(u_1,\ldots,u_{i-1})}(u_i)$, and $r_i = \deg(m_i)$. We have $[F(u_1, \ldots, u_i) : F(u_1, \ldots, u_{i-1})] = \deg_{F(u_1,\ldots,u_{i-1})}(u_i) = r_i$, and the multiplicative property of tower extensions yields

$$[E : F] = r_1 \cdot r_2 \cdots r_n.$$

Let $\sigma \in \mathrm{Aut}_F(E)$, and let σ_i be the restriction of σ to $F(u_1, \ldots, u_i)$. Note that σ_0 is the inclusion mape $\iota_F : F \to E$, and $\sigma_n = \sigma$ Since all $\sigma_i : F(u_1, \ldots, u_i) \to E$ agree with σ, we get that $\sigma_i : F(u_1, \ldots, u_i) \to E$ extends $\sigma_{i-1} : F(u_1, \ldots, u_{i-1}) \to E$. By Corollary 10.1.21 there are at most r_i ways to do this extension. As σ is built from $\sigma_0 = \iota_F$, step by step, we end up with at most $r_1 \cdot r_2 \cdots r_n$ possible $\sigma_n = \sigma \in \mathrm{Aut}_E(F)$. ■

To see that Proposition 10.2.1 is indeed more general than Proposition 10.1.3, we need an example of a finite extension that is not simple. The Primitive Element Theorem (10.1.12) tells us that any finite separable extension is simple, so we need to look at inseparable extensions. Example 10.1.2 gives us an example of a finite inseparable extension. However, that extension is simple. But we can extend the idea of that example, to create the example we need.

Example 10.2.1. Let $R = \mathbb{F}_2[s, t]$ be the ring of polynomials in two variables s and t over $\mathbb{F}_2$. As R is an integral domain (it is, in fact, a UFD) it embeds in its field of quotients, that we denote $\mathbb{F}_2(s, t)$, and call the field of rational functions in the two variables s and t. Let $f = x^2 - s, g = x^2 - t \in F[x]$. The same argument used in Example 10.1.2, shows that f and g are irreducible over F. Let α be a root of f and β a root of g. We can write $\alpha = \sqrt{s}$ and $\beta = \sqrt{t}$. $F(\alpha)$ is spanned by $\{1, \alpha\}$ over F, so for any $u \in F(\alpha)$, $u = a + b\alpha$ for some $a, b \in F$. We have $u^2 = a^2 + b^2\alpha^2 = a^2 + b^2 s$, and therefore $\deg_t(u^2)$ is even. Thus, $u^2 \neq t$, and $\beta \notin F(\alpha)$. It follows that $[F(\alpha, \beta) : F(\alpha)] = 2$ and $[F(\alpha, \beta) : F]$=4, with basis $\{1, \alpha, \beta, \alpha\beta\}$. Take $v \in F(\alpha, \beta)$. We can write $v = a + b\alpha + c\beta + d\alpha\beta$, with $a, b, c, d \in F$. It follows that $v^2 = a^2 + b^2\alpha^2 + c^2\beta^2 + d^2\alpha^2\beta^2 = a^2 + b^2 s + c^2 t + d^2 st \in F$. So, we have $\deg_F(v) \leq 2$, and therefore we cannot have $F(\alpha, \beta) = F(v)$. In other words, $F(\alpha, \beta)$ is not a simple extension of F.

Theorem 10.2.2 *[Dedekind-Artin Theorem] Let E be a field, G a finite subgroup of* $\mathrm{Aut}(E)$. *Let E_G be the subfield of E fixed by G. Then E/E_G is a finite extension and $[E : E_G] = |G|$. Moreover,* $\mathrm{Aut}_{E_G}(E) = G$.

04/27/2016 **Board presentations** Problem Set 10

04/28/2016

Proof. Let $F = E_G$. We have $G \leq \mathrm{Aut}_F(E)$, so if E/F is finite, Proposition 10.2.1 yields $|G| \leq |\mathrm{Aut}_F(E)| \leq [E : F]$. It remains to show that E/F is indeed finite, and $[E : F] \leq |G|$. Let $n = |G|$. By way of contradiction, assume $[E : F] > n$. There are $u_0, u_1, \dots, u_n \in E$, distinct, such that $I = \{u_0, u_1, \dots, u_n\}$ is independent over F. Let $G = \{\sigma_1, \dots, \sigma_n\}$ with $\sigma_1 = 1_E$. Consider the $n \times (n+1)$ matrix $M = (\sigma_i(u_j))$, with coefficients in E.

$$M = \begin{bmatrix} u_0 & u_1 & \dots & u_n \\ \sigma_2(u_0) & \sigma_2(u_1) & \dots & \sigma_2(u_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(u_0) & \sigma_n(u_1) & \dots & \sigma_n(u_n) \end{bmatrix}$$

and the system of equations $M \cdot X = 0$.

$$\begin{array}{rrcrl} u_0x_0+ & u_1x_1+ & \cdots & +u_nx_n & = 0 \\ \sigma_2(u_0)x_0+ & \sigma_2(u_1)x_1+ & \cdots & +\sigma_2(u_n)x_n & = 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \sigma_n(u_0)x_0+ & \sigma_n(u_1)x_1+ & \cdots & +\sigma_n(u_n)x_n & = 0 \end{array} \tag{10.10}$$

Since there are more variables than equations, the system has a non-trivial solution $\bar{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_n) \in E^n$. Picke $\bar{\alpha}$ non-trivial, with the smallest number, $(r+1) > 0$, of non-zero entries. Reorder the elements of I (if needed) so that $\bar{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_r, 0, \dots, 0)$, and $\alpha_0, \alpha_1, \dots, \alpha_r \neq 0$. Since the set of solutions of (10.10) is a linear space over E, we may also choose $\bar{\alpha}$, so that $\alpha_0 = 1$. The first of the equations in (10.10) yields

$$u_0\alpha_0 + \cdots + u_r\alpha_r = 0,$$

and by the independence of the set I we must have that at least one of $\alpha_0, \dots, \alpha_r$, say α_k, is not in F. By definition of F, this means that there is $\tau \in G$ such that $\tau(\alpha_k) \neq \alpha_k$. The fact that $\bar{\alpha}$ is a solution of (10.10) means that for each $i = 1 \dots n$,

$$\sigma_i(u_0)\alpha_0 + \sigma_i(u_1)\alpha_1 + \cdots + \sigma_i(u_r)\alpha_r = 0. \tag{10.11}$$

Galois extension
Galois group

Let $\beta_j = \tau(\alpha_j)$, and $\gamma_j = \alpha_j - \beta_j$. Note that $\beta_0 = \tau(\alpha_0) = \tau(1) = 1 = \alpha_0$, so $\gamma_0 = 0$. Also, $\gamma_k = \alpha_k - \beta_k = \alpha_k - \tau(\alpha_k) \neq 0$. Let $\sigma_l = \tau\sigma_i$. Applying τ to Equation (10.11) yields

$$\sigma_l(u_0)\beta_0 + \sigma_l(u_1)\beta_1 + \cdots + \sigma_l(u_r)\beta_r = 0, \tag{10.12}$$

As σ_i ranges over G, σ_l also ranges over all of G. So, for each $i = 1, \ldots n$,

$$\sigma_i(u_0)\beta_0 + \sigma_i(u_1)\beta_1 + \cdots + \sigma_i(u_r)\beta_r = 0, \tag{10.13}$$

and subtracting (10.13) from (10.11), we get

$$\sigma_i(u_0)\gamma_0 + \sigma_i(u_1)\gamma_1 + \cdots + \sigma_i(u_r)\gamma_r = 0. \tag{10.14}$$

Since $\gamma_0 = 0$ and $\gamma_k \neq 0$, this is a non-trivial solution to (10.10) with less than $r+1$ non-zero entries, contradicting the choice of $\bar{\alpha}$. ■

10.2.1 Galois Extensions

The following proposition connects three important properties that a finite extension may have. For the meaning of the terms G^* and F^{**}, see Definition 10.2.2 below.

Proposition 10.2.3 *Let E/F be a finite extension, and $G = \mathrm{Aut}_F(E)$. TFAE:*

1. *$G^* = F$, i.e. $F^{**} = F$*
2. *$[E : F] = |G|$*
3. *E is the splitting field of a separable polynomial over F.*
4. *E is the splitting field of an irreducible separable polynomial over F.*

The proof appears below, after some examples, and the appropriate definitions.

Definition 10.2.1. Let E/F be a finite extension. We say that E/F is a (finite) *Galois extension* if it satisfies the properties in Proposition 10.2.3. The group $\mathrm{Aut}_F(E)$ is called the *Galois group* of the extension.

Examples 10.2.2. 1. The Dedkind-Artin theorem tells us that for G a finite subgroup of $\mathrm{Aut}(E)$, the extension E/E_G is a Galois extension, with Galois group G.

2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Example 5.3.6 shows that the extension $E/\mathbb{Q}$ is a Galois extension, with Galois group isomorphic to K_4, the Klein 4-group.

3. Let $E = \mathbb{Q}(\sqrt[4]{2})$. Example 10.1.5 shows that $E/\mathbb{Q}$ is **not** a Galois extension, as $[E : \mathbb{Q}] = 4$, but $|\mathrm{Aut}_{\mathbb{Q}}(E)| = 2$.

4. On the other hand, $\mathbb{Q}(\sqrt[4]{2}, i)$ is the splitting field of $x^4 - 2$ over $\mathbb{Q}$, and this polynomial is separable. Thus, $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is a Galois extension, and therefore $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))$ has order 8. Note that an automorphism $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(E)$ is completely determined by where it maps $\sqrt[4]{2}$ and i. By Lemma 10.1.2, $\sqrt[4]{2}$ has to be mapped to a root of its minimal polynomial $x^4 - 2$. For this, there are 4 possibilities $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. On the other hand, i has to be mapped to one of the roots of its minimal polynomial $x^2 + 1$, and these are $\pm i$. Combining these possibilities, yields 8 potential automorphims of $E/\mathbb{Q}$, but since there are exactly 8 such automorphism, all possibilities yield an automorphims.

$$\begin{array}{rcl@{\qquad}rcl}
I : \sqrt[4]{2} & \mapsto & \sqrt[4]{2} & \sigma_1 : \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \\
i & \mapsto & i & i & \mapsto & -i \\
\\
\sigma_2 : \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} & \sigma_3 : \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} \\
i & \mapsto & i & i & \mapsto & -i \\
\\
\sigma_4 : \sqrt[4]{2} & \mapsto & i\sqrt[4]{2} & \sigma_5 : \sqrt[4]{2} & \mapsto & i\sqrt[4]{2} \\
i & \mapsto & i & i & \mapsto & -i \\
\\
\sigma_6 : \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2} & \sigma_7 : \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2} \\
i & \mapsto & i & i & \mapsto & -i
\end{array}$$

Note that σ_1, σ_2, σ_3, σ_5, and σ_7 have order 2, and $\sigma_4^2 = \sigma_2 = \sigma_6^2$, so σ_4 and σ_6 have order 4. Moreover, $\sigma_1\sigma_4 = \sigma_7$, and $\sigma_4\sigma_1 = \sigma_5$, so $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i))$ is a non-abelian group of order 8, with 2 elements of order 4. It follows that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}, i)) \approx D_4$.

04/29/2016

subgroup lattice
partially ordered set
reflexive
transivite
anti-symmetric
lattice
meet
join
intermediate field lattice

5. Propositio 10.1.15 shows that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension. Its Galois group is cyclic of order n, generated by the Frobenius automorphism.

6. Proposition 10.1.14 shows that the extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is a Galois extension, with Galois group cyclic of order $p-1$.

7. In Examples 5.3.7 and 10.1.1.3, we have seen that the extension $\mathbb{Q}(\sqrt[3]{2}\,,\omega)/\mathbb{Q}$ is the splitting field of x^3-2 over $\mathbb{Q}$. It has degree 6, and Galois group isomorphic to D_3. On the other hand, the extension $\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q}$ has degree 3, but $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}\,)$ is trivial, so this extension is not Galois. $\mathbb{Q}(\sqrt[3]{2}\,)$ cannot be the splitting field of any polynomial over $\mathbb{Q}$.

10.2.2 Galois Connection

Recall that given a group G, the ***subgroup lattice*** of G as the set

$$\mathrm{Sub}(G) := \{H | H \leq G\}$$

of all subgroups of G, ordered by inclusion. This is an example of a ***partially ordered set***, poset for short, since the binary relation of inclusion is ***reflexive***, ***transivite***, and ***anti-symmetric***. It is called a ***lattice*** as it has the following two properties. Given $H_1, H_2 \in \mathrm{Sub}(G)$, there is a greatest lower bound of H_1 and H_2 in $\mathrm{Sub}(G)$, given by $H_1 \cap H_2$, which we call the ***meet*** of H_1 and H_2. And a least upper bound of H_1 and H_2 in $\mathrm{Sub}(G)$, given by $H_1 \vee H_2$, the ***join*** of H_1 and H_2, which is the subgroup generated by the union $H_1 \cup H_2$.

$$H_1 \wedge H_2 := H_1 \cap H_2 \qquad H_1 \vee H_2 := \langle H_{\cup} H_2 \rangle.$$

Given a field extension E/F, we define is a similar way, the ***intermediate field lattice*** of the extension E/F, as the set

$$\mathrm{Sub}_F(E) := \{L | F \leq L \leq E\}$$

of all subfields L of E that contain F. It is ordered by inclusion, and for any $L_1, L_2 \in \mathrm{Sub}_F(E)$, there is a greatest lower bound in $\mathrm{Sub}_F(E)$ given by $L_1 \cap L_2$, and a least upper bound given by $L_1 \vee L_2$, the subfield of E generated by the union $L_{\cup} L_2$.

$$L_1 \wedge L_2 := L_1 \cap L_2 \qquad L_1 \vee L_2 := \langle L_1 \cup L_2 \rangle.$$

Definition 10.2.2. Let E be a field and G a subgroup of $\mathrm{Aut}(E)$. Let $F = E_G$, the subfield of E fixed by G. We define two maps between $\mathrm{Sub}(G)$, the subgroup lattice of G, and $\mathrm{Sub}_F(E)$, the intermediate field lattice of the extension E/F as follows. The maps go in one in each direction, and both maps are denoted by *. The context will tell which is which. For $H \in \mathrm{Sub}(G)$, let

fixer subgroup
Galois Connection

$$H^* = E_H = \{a \in E | \sigma(a) = a, \text{ for all } \sigma \in H\}.$$

For $L \in \mathrm{Sub}_F(E)$, let

$$L^* = \{\sigma \in G | \sigma(a) = a, \text{ for all } a \in L\}.$$

Just like we showed in Corollary 5.4.4, that E_H, the subfield fixed by H, is indeed a subfield of E, it is easy to show that L^* is a subgroup of G. It is called the *fixer subgroup* of L. (see Exercise 10.2.1 below)
The pair of posets $(\mathrm{Sub}_F(E), \mathrm{Sub}(G)$ together with the maps just defined, is called a *Galois Connection*, as it satisfies the properties in Lemma 10.2.4 below.

Exercise 10.2.1. Let E be a field, G a finite subgroup of $\mathrm{Aut}(E)$, $F = E_G$, and $L \in \mathrm{Aut}_F(E)$. Show that $L^* = \mathrm{Aut}_L(E)$, and it is a subgroup of G.

Lemma 10.2.4 *Let E be a field, G a subgroup of $\mathrm{Aut}(E)$, and $F = E_G$. For any $H, H_1, H_2 \in \mathrm{Sub}(G)$, and any $L, L_1, L_2 \in \mathrm{Sub}_F(E)$*

1. *If $H_1 \leq H_2$ then $H_2^* \leq H_1^*$. (* is order reversing)*
2. *If $L_1 \leq L_2$ then $L_2^* \leq L_1^*$. (* is order reversing)*
3. *$H \leq H^{**}$ ($1 \leq {}^{**}$)*
4. *$L \leq L^{**}$ ($1 \leq {}^{**}$)*

Exercise 10.2.2. Prove Lemma 10.2.4.

Corollary 10.2.5 *Let E be a field, G a subgroup of $\mathrm{Aut}(E)$, and $F = E_G$. For any $H \in \mathrm{Sub}(G)$, and any $L \in \mathrm{Sub}_F(E)$*

1. *$H^{***} = H^*$*

2. $L^{***} = L^*$

Proof. ∎

We often refer to the properties in Corollary 10.2.5 as the "3 = 1" property.

Note that in Theorem 10.2.2 we have $F = G^*$ and $G^{**} = G$.

05/02/2016

Proof of Proposition 10.2.3.
We have E/F a finite extension, and $G = \mathrm{Aut}_F(E) = F^*$.

(1)⇒(2) Assume $F = G^* = E_G$. By the Dedekind-Artin Theorem, $|G| = [E : E_G] = [E : F]$.

(2)⇒(1) Assume $[E : F] = |G|$. Note that $F^{**} = G^* = E_G$. Since $F \leq F^{**}$, we have $[E : F] = [E : F^{**}][F^{**} : F] = [E : E_G][F^{**} : F]$. By assumption $[E : F] = |G|$, and by the Dedekind-Artin Theorem $[E : E_G] = |G|$. Therefore $[F^{**} : F] = 1$, and $F^{**} = F$, as desired.

(1)⇒(4) Assume $E_G = F$. We first prove the following claim.
Claim 1: E/F is separable.
Write $G = \{1, \sigma_2, \ldots, \sigma_n\}$. Let $u \in E$, and consider the elements

$$u, \sigma_2(u), \ldots, \sigma_n(u) \tag{10.15}$$

in E. This list may contain repetitions. Let $u, u_2, \ldots, u_r$ be the distinct elements in (10.15). Consider the polynomial

$$f = (x - u)(x - u_2) \cdots (x - u_r).$$

Each $\tau \in G$ permutes the list (10.15), and therefore it also permutes the elements $u, u_2, \ldots, u_r$. It follows that when we apply τ to f, its coefficients are unchanged. In other words, the coefficients of f are in $E_G = F$, and $f \in F[x]$. Since f has no multiple roots, it follows that $\min_F(u)$, which is a factor of f, is separable, and splits in E. The element u is separable over F. Since $u \in E$ was arbitrary, we have E/F is separable.
By the Primitive Element Theorem, there is $u \in E$ such that $E = F(u)$.

Since $\min_F(u)$ splits in E, E is the splitting field of $\min_F(u)$, an irreducible separable polynomial.

normal extension

(4)⇒(3) is clear.

(3)⇒(2) Assume E is the splitting field of aseparable polynomial $f \in F[x]$. We prove, by induction on $n = [E : F]$ the following claim.
Claim 2: Given $\varphi : F \to E$, there are $[E : F]$ different extensions of a homomorphism φ to $\hat{\varphi} : E \to E$.
The statement is clear when $[E : F] = 1$. Let $n > 1$. Let $u \in E - F$ be a root of f and $m = \min_F(u)$. Since m is an irreducible factor of f, it is separable, and it splits in E. By Scholium 10.1.22, there are $r = \deg(m)$ different extensions of φ to $\tilde{\varphi} : F(u) \to E$ that extend φ. The extension $E/F(u)$ has degree $[E : F(u)] = n/r < n$, and E is the splitting field of the separable polynomial $f \in F(u)[x]$. By induction, there are n/r different extensions of $\tilde{\varphi}$ to $\hat{\varphi} : E \to E$. Therefore there are $r \cdot (n/r) = n$ different extensions of φ to $\widehat{varphi} : E \to E$.
Apply now the claim to the inclusion map $i : F \to E$, to get n homomorphism $\hat{\varphi} : E \to E$ that fix the elements of F. Each of these is injective, and F-linear. Since E is finite dimensional over F, each $\hat{\varphi}$ is a bijection, hence an element of $\mathrm{Aut}_F(E)$. In other words, we have $\mathrm{Aut}_F(E) = [E : F]$. ■

Definition 10.2.3. A finite extension E/F is said to be a *normal extension*, if E is the splitting field of a polynommial $f \in F[x]$.

Corollary 10.2.6 *Let E/F be a finite extension. E/F is a Galois extension iff it is normal and separable.*

Proof. (⇒) Assume E/F is Galois. The fact that E/F is separable is a scholium to Proposition 10.2.3. By Part (10.2.3.3) of the proposition, E is the splitting field of a polynomial over F, i.e. E/F is normal.
(⇐) Assume E/F is normal and separable. By normality, let $f \in F[x]$ be such that E is the splitting field of f. Let $q \in F[x]$ be a monic irreducible factor of f, and let $u \in E$ be a root of q. Then $q = \min_F(u)$, and by separability q is separable over F. ■

05/04/2016

Given a field tower $E/L/F$, some properties of the big extension E/F

imply the same properties for the two step extensions, E/L and L/F. That is the case for the properties:

Finite See Corollary 5.3.14, the Multiplicative Property of Extension Degrees.

Algebraic See Corollary 5.3.21.

Separable See Proposition 10.1.9.

However, this is not the case for normal extensions. For example, in the tower $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, the big extension $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is normal, the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$. However, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal (see Example 10.2.2.7).

We do get, however, the following lemma, whose proof is immediate.

Lemma 10.2.7 *Let $E/L/F$ be a field tower. If E/F is normal, then E/L is normal.*

Combining this lemma with Proposition 10.1.9 and Corollary 10.2.6, we get:

Proposition 10.2.8 *Let $E/L/F$ be a field tower. If E/F is a Galois extension, then E/L is also Galois.*

Proposition 10.2.9 *Let E/F be a finite Galois extension. If $f \in F[x]$ is irreducible and has a root in E, then it splits in E, and is separable.*

$$\begin{tikzcd}
E \arrow[r, "\hat{\varphi}"] \arrow[d, dash] & E \\
L \arrow[ur, "\varphi"] \arrow[d, dash] & \\
F \arrow[uur, "i"'] &
\end{tikzcd}$$

Proof. Let $u \in E$ be a root of f, and let $L = F(u)$. Let $r = \deg(f)$. By Scholium 10.1.22, the number of ways of extensing the inclusion map $i : F \to E$ to a homomorphism $\varphi : F(u) \to E$ is the number s of distinct roots of f in E. By Propositions 10.2.8, E/L is also a Galois extension, so by the second Claim in the proof of Proposition 10.2.3, there are $[E : L]$ ways to extend each $\varphi : L \to E$ to a homomorphism $\hat{\varphi} : E \to E$. The same claim, applied to the Galois extension E/F, yields $[E : F]$ ways of extending the inclusion map to a homomorphism $\hat{\varphi} : E \to E$. We, thus have

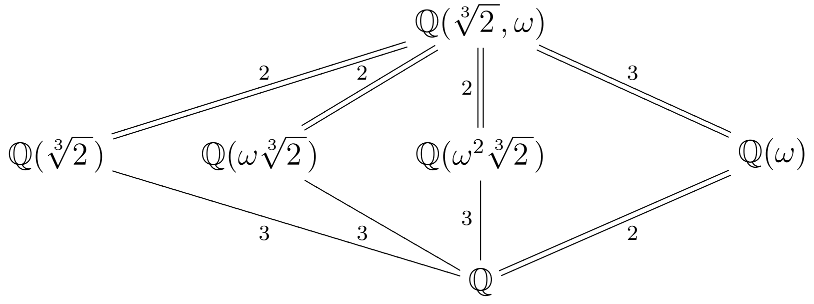
$$[E : F] = s \cdot [E : L] \leq r \cdot [E : L] = [L : F] \cdot [E : L] = [E : F]$$

and therefore $s = r$, i.e. f has r distinct roots in E; it splits in E, and is separable. ■

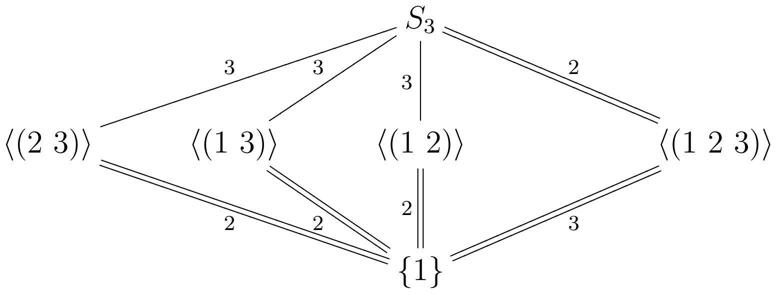
10.2.3 The Fundamental Theorem

We now have all the elements needed to state and prove the Fundamental Theorem of Galois Theory. As indicated earlier, we have limited our attention to the finite extension case. We should point out, however, that there is a slightly weaker, and more complicated version that holds for arbitrary extensions, finite or infinite, but we will not cover it here.

Before stating and proving the Fundamental Theorem, let's take a look at the following example. Recall from Examples 5.3.7 and 10.1.1.4, that $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$, and $\mathrm{Gal}_{\mathbb{Q}}(E) \approx D_3 \approx S_3$. Some of the intermediate fields of this extension appear in the following diagram. The numbers indicate the degree of each extension. Double lines denote normal extensions.


$\mathbb{Q}(\sqrt[3]{2}, \omega)$
2
2
2
3
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\omega\sqrt[3]{2})$
$\mathbb{Q}(\omega^2\sqrt[3]{2})$
$\mathbb{Q}(\omega)$
3
3
3
2
$\mathbb{Q}$

On the other hand, we have that the lattice of subgroups of S_3 looks like:



where double lines denote normal subgroups, and the numbers next to the edges denote the index.

Notice the remarkable similarity between these two lattices. The Fundamental Theorem of Galois Theory tells us, among other things, that this is not a coincidence. That such similarity holds for any Galois Extension, and we will make precise the sense in which these lattices are *similar*. Something else that we will get from the FTGT is that in the first lattice there are no other intermediate fields, something we have not established yet, and not at all obvious.

Theorem 10.2.10 [The Fundamental Theorem of Galois Theory] *Let E/F be a (finite) Galois extension, with Galois group $G = \mathrm{Gal}_F(E)$.*

1. *The maps*

$$\begin{array}{rccc} ^*: & \mathrm{Sub}_F(E) & \to & \mathrm{Sub}(G) \\ & L & \mapsto & L^* = \mathrm{Aut}_L(E) \end{array} \qquad \begin{array}{rccc} ^*: & \mathrm{Sub}(G) & \to & \mathrm{Sub}_F(E) \\ & H & \mapsto & H^* = E_H \end{array}$$

   are inverse of each other, and hence bijective.

2. *The maps * are order reversing, i.e. for intermediate subfields L_1 and L_2,*

$$L_1 \leq L_2 \Rightarrow L_2^* \leq L_1^*$$

   and for subgroups $H_1, H_2 \leq G$,

$$H_1 \leq H_2 \Rightarrow H_2^* \leq H_1^*$$

05/05/2016

3. *The maps * preserve index, i.e. for intermediate subfields $L_1 \leq L_2$,*

$$[L_2 : L_1] = [L_1^* : L_2^*]$$

and for subgroups $H_1 \leq H_2 \leq G$,

$$[H_2 : H_1] = [H_1^* : H_2^*]$$

4. *The maps * preserve normality, i.e. for intermediate subfields $L_1 \leq L_2$, L_2/L_1 is a normal extension iff L_2^* is a normal subgroup of L_1^*. Moreover, when L_2/L_1 is a normal extension, we have*

$$\mathrm{Gal}_{L_1}(L_2) \approx \frac{L_1^*}{L_2^*}$$

Proof. 1. We need to show that $L^{**} = L$ and $H^{**} = H$, for any $L \in \mathrm{Sub}_F(E)$ and any $H \in \mathrm{Sub}(G)$. From Lemma 10.2.4 we already know that $L \leq L^{**}$ and $H \leq H^{**}$.
Let $L \in \mathrm{Sub}_F(E)$. By Propositions 10.2.8 and 10.1.9, E/L is normal and separable. By Corollary 10.2.6 E/L is Galois, and Proposition 10.2.3 yields $L^{**} = L$.
Let $H \in \mathrm{Sub}(G)$. From Corollary 10.2.5, the “$3 = 1$” property, we have $H^* = H^{***}$. By the Dedeking-Artin Theorem,

$$|H| = [E : E_H] = [E : H^*] = [E : H^{***}] = [E : E_{H^{**}}] = |H^{**}|.$$

Therefore, $H = H^{**}$.

2. This was proved in Lemma 10.2.4.

3. Let $L \in \mathrm{Sub}_F(E)$. Since E/L is Galois, by Proposition 10.2.3, $[E : L] = |\mathrm{Aut}_L(E)| = |L*|$. Now, if $L_1, L_2 \in \mathrm{Sub}_F(E)$ are such that $L_1 \leq L_2$, then, using the multiplicative property of extension degrees,

$$[L_2 : L_1] = \frac{[E : L_1]}{[E : L_2]} = \frac{|L_1^*|}{|L_2^*|} = [L_1^* : L_2^*].$$

Let $H \in \mathrm{Sub}(G)$. By the Dedekind-Artin Theorem, $|H| = [E : E_H]$. Now, if $H_1, H_2 \in \mathrm{Sub}(G)$ are such that $H_1 \leq H_2$, then

$$[H_2 : H_1] = \frac{|H_2|}{|H_1|} = \frac{[E : E_{H_2}]}{[E : E_{H_1}]} = [E_{H_1} : E_{H_2}] = [H_1^* : H_2^*].$$

4. Note first that it suffice to consider the case when $L_1 = F$.
Let $L \in \mathrm{Sub}_F(E)$. We want to show that L is a normal extension of F iff L^* is a normal subgroup of $F^* = G$. Since L/F is a finite, separable extension, by the Primitive Element Theorem, there is $u \in L$ such that $L = F(u)$. Since any $\sigma \in G$ fixes F, we have $\sigma \in L*$ iff σ fixes L, iff $\sigma(u) = u$.
Assume L/F is a normal extension. By Proposition 10.2.9, $\min_F(u)$ splits in L. Let $\sigma \in L*$ and $\tau \in G$. We want to show $\tau^{-1}\sigma\tau \in L^*$. By Proposition 10.1.1 $\tau(u)$ is a root of $\min_F(u)$, and therefore $\tau(u) \in L$. Therefore $\sigma(\tau(u)) = \tau(u)$, and $\tau^{-1}\sigma\tau(u) = u$. So, $\tau^{-1}\sigma\tau \in L^*$.
Conversely, assume L^* is a normal subgroup of G.
Claim: $\min_F(u)$ splits in L. Suppose otherwise, i.e. there is a root $v \in E$ of $\min_F(u)$ such that $v \notin L$. By Proposition 10.1.1 there is a homomorphism $\varphi : F(u) \to E$ such that $\varphi(u) = v$. By Corollary 5.3.25, φ can be extended to an automorphism $\tau : E \to E$, that is, $\tau \in \mathrm{Aut}_F(E)$, such that $\tau(u) = v$. Since $v \notin L = L^{**}$, there is $\sigma \in L^*$ such that $\sigma(v) \neq v$. Since $L^* \trianglelefteq G$, we have $\tau^{-1}\sigma\tau \in L^*$. If follows that

$$u = \tau^{-1}\sigma\tau(u) = \tau^{-1}\sigma(v), \text{ and } \tau(u) = \sigma(v) \neq v,$$

a contradiction.
Since $\min_F(u)$ splits in L and $L = F(u)$, L is the splitting field of $\min_F(u)$, and L/F is a normal extension.
To prove the second part of the statement, namely, that

$$\mathrm{Gal}_F(L) \approx \frac{F^*}{L^*} = \frac{G}{L^*}, \tag{10.16}$$

note that for any $\tau \in G$, $\tau(u)$ is a root of $\min_F(u)$, hence an element of L. The restriction $\tau|_L$ maps L to L, fixing F. This tells us that $\tau|_L$ is an injective F-linear transformation from the finite dimensional vector space L to itself. It follows that $\tau|_L$ is bijective, and $\tau|_L \in \mathrm{Aut}_F(L)$. The restriction map

$$\begin{array}{rccc}\rho : & \mathrm{Aut}_F(E) & \to & \mathrm{Aut}_F(L) \\ & \tau & \mapsto & \tau|_L\end{array}$$

is a group homomorphism, and $\ker(\rho) = \mathrm{Aut}_L(E)$. It is easy to show that ρ is surjective (see Exercise 10.2.3 below). By the First Isomorphism Theorem, we get (10.16). ■

Exercise 10.2.3. Show that the restriction map ρ in the proof of Theorem 10.2.10 is a group epimorphism.

05/09/2016

10.2.4 Examples

1. If E is a finite field $E = \mathbb{F}_{p^n}$. By Proposition **??**, E is separable over $F = \mathbb{F}_p$. In the proof of Theorem 5.4.5 we showed that E is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$, so E/F is a normal extension. It is a Galois extension. The subfields of E are all the finite fields of the form $\mathbb{F}_{p^d}$ as d ranges over the divisors of n. It follows that the lattice of subfields of E is isomorphic to the lattice of divisors of n. On the other hand, the Galois group $G = \mathrm{Gal}_F(E)$ is cyclic of order n. The subgroups of G are cyclic groups of order d where d ranges over the divisors of n. As G is abelian, all subgrops of G are normal. On the other hand, all subfields of E are normal over $\mathbb{F}_p$.

2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $F = \mathbb{Q}$. In Example 10.1.4 we have seen that E is the splitting field of $(x^2-2)(x^2-3)$, so E/F is a Galois extension. We also showed that $\mathrm{Gal}_F(E)$ is the Klein 4-group $V = \{I, \sigma_1, \sigma_2, \sigma_3\}$, where
$$\begin{array}{rrcl} I: & \sqrt{2} & \mapsto & \sqrt{2} \\ & \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \begin{array}{rrcl} \sigma_1: & \sqrt{2} & \mapsto & \sqrt{2} \\ & \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$
$$\begin{array}{rrcl} \sigma_2: & \sqrt{2} & \mapsto & -\sqrt{2} \\ & \sqrt{3} & \mapsto & \sqrt{3} \end{array} \qquad \begin{array}{rrcl} \sigma_3: & \sqrt{2} & \mapsto & -\sqrt{2} \\ & \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

The lattice of subgroups of V is

$$\begin{tikzcd} & V \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle \sigma 1 \rangle \arrow[dr, dash] & \langle \sigma_3 \rangle \arrow[d, dash] & \langle \sigma_2 \rangle \arrow[dl, dash] \\ & \{I\} & \end{tikzcd}$$

so the diagram of subfields of E on page 50 is missing one subfield. $\mathbb{Q}(\sqrt{2})$ is the subfield fixed by $\langle \sigma_1 \rangle$, and $\mathbb{Q}(\sqrt{3})$ is the subfield fixed by $\langle \sigma_2 \rangle$. We are missing the subfield fixed by $\langle \sigma_3 \rangle$. It is easy to see that $\sigma_3(\sqrt{6}\,) = \sqrt{6}$, and it follows that the subfield fixed by $\langle sigma_3 \rangle$ is precisely $\mathbb{Q}(\sqrt{6}\,)$. Moreover, the Fundamental Theorem of Galois Theory tells us that there are no other subfields of E. Hese is the lattice of subfields.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}\,, \sqrt{3}\,) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}\,) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}\,) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}\,) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

3. From Example 10.2.2.4, on page 57, we have that $E = \mathbb{Q}(\sqrt[4]{2}\,, i)$, the splitting field of $x^4 - 2$ over $\mathbb{Q}$ has Galois group

$$G = D_4 = \{I, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7\}.$$

If we denote the roots of $x^4 - 2$ as follows:

$$\alpha_1 = \sqrt[4]{2}\,, \quad \alpha_2 = i\sqrt[4]{2}\,, \quad \alpha_3 = -\sqrt[4]{2}\,, \quad \alpha_4 = -i\sqrt[4]{2}\,,$$

then the elements of G are permutations of $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

$$\begin{array}{rcl}
I : \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \\
i & \mapsto & i \\
& \epsilon &
\end{array}
\qquad
\begin{array}{rcl}
\sigma_1 : \sqrt[4]{2} & \mapsto & \sqrt[4]{2} \\
i & \mapsto & -i \\
& (\alpha_2\ \alpha_4) &
\end{array}$$

$$\begin{array}{rcl}
\sigma_2 : \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} \\
i & \mapsto & i \\
& (\alpha_1\ \alpha_3)(\alpha_2\ \alpha_4) &
\end{array}
\qquad
\begin{array}{rcl}
\sigma_3 : \sqrt[4]{2} & \mapsto & -\sqrt[4]{2} \\
i & \mapsto & -i \\
& (\alpha_1\ \alpha_3) &
\end{array}$$

$$\begin{array}{rcl}
\sigma_4 : \sqrt[4]{2} & \mapsto & i\sqrt[4]{2} \\
i & \mapsto & i \\
& (\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4) &
\end{array}
\qquad
\begin{array}{rcl}
\sigma_5 : \sqrt[4]{2} & \mapsto & i\sqrt[4]{2} \\
i & \mapsto & -i \\
& (\alpha_1\ \alpha_2)(\alpha_3\ \alpha_4) &
\end{array}$$

$$\begin{array}{rcl}
\sigma_6 : \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2} \\
i & \mapsto & i \\
& (\alpha_1\ \alpha_4\ \alpha_3\ \alpha_2) &
\end{array}
\qquad
\begin{array}{rcl}
\sigma_7 : \sqrt[4]{2} & \mapsto & -i\sqrt[4]{2} \\
i & \mapsto & -i \\
& (\alpha_1\ \alpha_4)(\alpha_2\ \alpha_3) &
\end{array}$$

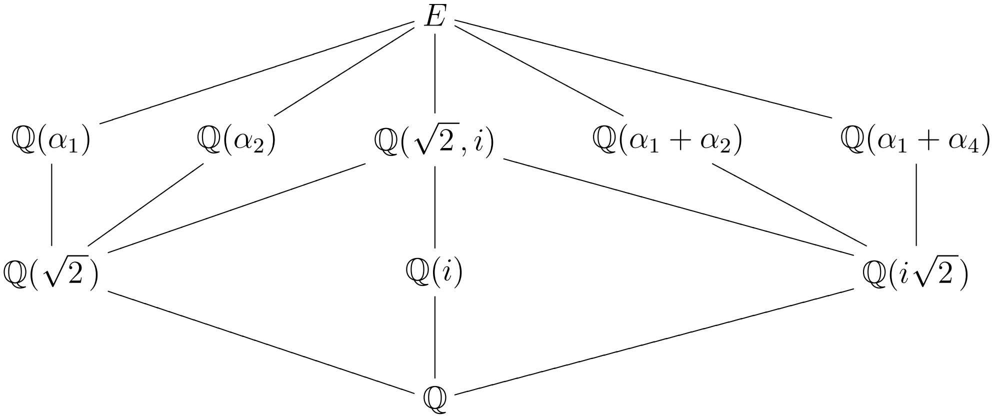
The lattice of subgroups of G is

$$\begin{tikzcd}
 & & D_4 \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\langle \sigma_1, \sigma_2 \rangle \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \langle \sigma_4 \rangle \arrow[d, dash] & & \langle \sigma_2, \sigma_7 \rangle \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\langle \sigma_1 \rangle \arrow[drr, dash] & \langle \sigma_3 \rangle \arrow[dr, dash] & \langle \sigma_2 \rangle \arrow[d, dash] & \langle \sigma_5 \rangle \arrow[dl, dash] & \langle \sigma_7 \rangle \arrow[dll, dash] \\
 & & \{I\} & &
\end{tikzcd}$$

The fixed subfields are:

$$\begin{array}{rclrcl}
E_{\sigma_1} & = & \mathbb{Q}(\alpha_1) & E_{\sigma_3} & = & \mathbb{Q}(\alpha_2) \\
E_{\sigma_5} & = & \mathbb{Q}(\alpha_1+\alpha_2) & E_{\sigma_2} & = & \mathbb{Q}(\sqrt{2}\,, i) \\
E_{\sigma_7} & = & \mathbb{Q}(\alpha_1+\alpha_4) & E_{\sigma_4} & = & \mathbb{Q}(i) \\
E_{\langle\sigma_1,\sigma_2\rangle} & = & \mathbb{Q}(\alpha_1^2) = \mathbb{Q}(\sqrt{2}\,) & E_{\langle\sigma_2,\sigma_7\rangle} & = & \mathbb{Q}(\alpha_1\alpha_2) = \mathbb{Q}(i\sqrt{2}\,)
\end{array}$$

and the lattice of subfields is:


E
$\mathbb{Q}(\alpha_1)$
$\mathbb{Q}(\alpha_2)$
$\mathbb{Q}(\sqrt{2}\,, i)$
$\mathbb{Q}(\alpha_1+\alpha_2)$
$\mathbb{Q}(\alpha_1+\alpha_4)$
$\mathbb{Q}(\sqrt{2}\,)$
$\mathbb{Q}(i)$
$\mathbb{Q}(i\sqrt{2}\,)$
$\mathbb{Q}$

05/11/2016

4. Let E be the splitting field of $f = x^5 - 20x + 6 \in \mathbb{Q}[x]$. It is a Galois extension of $\mathbb{Q}$. Let $G = \mathrm{Gal}_{\mathbb{Q}}(E) = \mathrm{Aut}_{\mathbb{Q}}(E)$. Using the Eisenstein Criterion one shows that f is irreducible over $\mathbb{Q}$, and using the Intermediate Value Theorem from Calculus, one can show that it has exactly 3 real roots, call them $\alpha_1, \alpha_2, \alpha_3$. The two non-real roots are conjugate of each other. Call them $\alpha_4, \alpha_5 = \overline{\alpha_4}$. Complex conjugation $\tau : \mathbb{C} \to \mathbb{C}$, given by $a + bi \mapsto a - bi$, fixes the coefficients of f, and therefore it permutes its roots. Restricting τ to E yields an automorphism of E that fixes $\mathbb{Q}$, i.e. $\tau \in G$. Since τ fixes all real numbers, as a permutation of the roots, we can write it $\tau = (\alpha_4\ \alpha_5)$.
   Since f is irreducible over $\mathbb{Q}$, the extension $\mathbb{Q}(\alpha_1)$ has degree 5 over $\mathbb{Q}$. By the multiplicative property of extension degrees, we get that 5 divides $[E : \mathbb{Q}] = |G| \leq S_5$. The only elements in S_5 of order 5 are 5-cycles, so by Caucy's Theorem G contains a 5-cycle, call it ρ. It is easy to see that ρ and τ generate all of S_5, and therefore $G \approx S_5$.