Section V.4. The Galois Group of a Polynomial (Partial)

Note. We present some of the results from this section of the text. We only give the results which are needed for our future explorations (in particular, the unsolvability of the quintic in the appendix to Section V.9).

Definition V.4.1. Let K be a field. The *Galois group of polynomial* $f \in K[x]$ is the group $\mathrm{Aut}_K(F)$ where F is a splitting field of f over K.

Note. By Corollary V.3.9, any two splitting fields of f over K are K-isomorphic (that is, are isomorphic under an isomorphism which fixes K).

Recall. A subgroup G of the symmetric group S_n is *transitive* if given any $i \neq j$ (with $1 \leq i, j \leq n$) there exists $\sigma \in G$ such that $\sigma(i) = j$ (see Exercise II.4.6 for a more general definition).

Theorem V.4.2. Let K be a field and $f \in K[x]$ a polynomial with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

(ii) If irreducible f is separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.

Note. Theorem V.4.2 allows us to discuss Galois groups of a polynomial in terms of their isomorphic image which is a subgroup of S_n (the permutation group of the roots of the polynomial). See the supplement to this section of notes for results concerning Galois groups of polynomials of degrees 2, 3, and 4.

Note. We now present two examples from Fraleigh's *A First Course in Abstract Algebra*, 7th edition. The following example is on pages 275-76 of Hungerford (but Hungerford uses some of the results we have skipped), but we present it in a way independent of the skipped results and with a slightly different notation from what Hungerford has used (in the diagrams of groups and intermediate fields, we always include the larger structures at the top of the diagram).

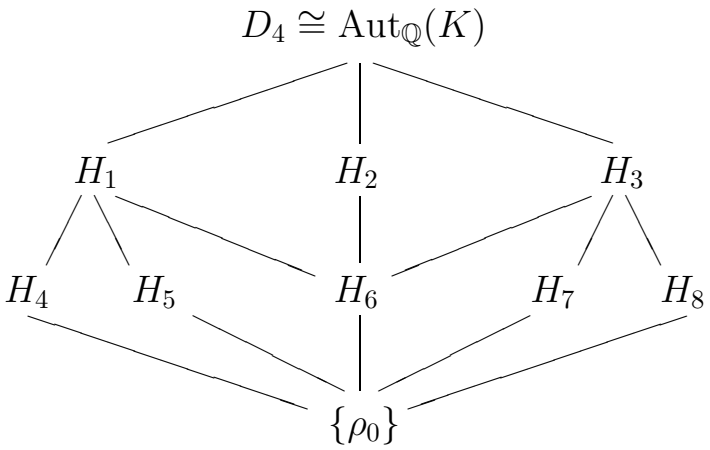
Example. (Fraleigh, Example 54.3) Let K be the splitting field of x^4-2 over $\mathbb{Q}$. Now x^4-2 is irreducible over $\mathbb{Q}$ (by Eisenstein's Criterion, Theorem III.6.15, with $p=2$). In $\mathbb{C}$, the zeros of x^4-2 are $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$. Denote $\alpha=\sqrt[4]{2}$. Since K must contain both α and $i\alpha$, then K must contain $i\alpha/\alpha=i$. So $K\neq\mathbb{Q}(\alpha)$. Since K must contain i and α, and $\mathbb{Q}(\alpha,i)$ contains all zeros of x^4-2, then $K=\mathbb{Q}(\alpha,i)$. Denote $E=\mathbb{Q}(\alpha)$ and we then have $\mathbb{Q}\leq E=\mathbb{Q}(\alpha)\leq K=\mathbb{Q}(\alpha,i)$.

Now, a basis for $E=\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $\{1,\alpha,\alpha^2,\alpha^3\}$, and a basis for $K=\mathbb{Q}(\alpha,i)$ over $E=\mathbb{Q}(\alpha)$ is $\{1,i\}$. So $[E:\mathbb{Q}]=4$ and $[K:E]=2$. So by Theorem V.1.2, $[K:\mathbb{Q}]=[K:E][E:\mathbb{Q}]=8$. A basis for K over $\mathbb{Q}$ is $\{1,\alpha,\alpha^2,\alpha^3,i,i\alpha,i\alpha^2,i\alpha^3\}$. Since K is the splitting field of x^4-2 and since each zero of x^4-2 is of multiplicity 1 then by Theorem V.3.11 (the (ii) implies (i) part) K is Galois over $\mathbb{Q}$. So by the Fun-

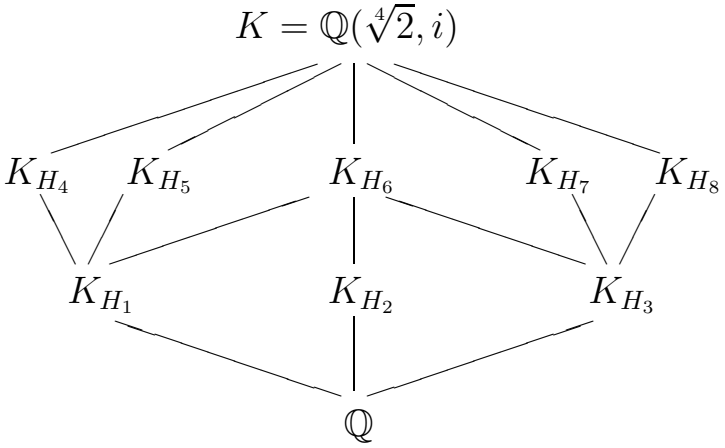
damental Theorem of Galois Theory (Theorem V.2.5(i)) $[K:\mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(K)| = 8$. So there are 8 automorphisms of K leaving $\mathbb{Q}$ fixed. Such an automorphism is determined by its behavior on the basis $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$, and hence determined by its value on i and α. Let σ be such an automorphism. By Theorem V.2.2 $\sigma(\alpha)$ must be a conjugate of α—that is, a zero of $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 2$—so there are 4 such permutations. Similarly, $\sigma(i)$ must be a zero of $\mathrm{irr}(i, \mathbb{Q}) = x^2 + 1$ and there are 2 such resulting permutations. This leads to the following 8 permutations in terms of the images of α and i:

Permutation σ	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	δ_1	μ_2	δ_2
$\sigma(\alpha)$	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

With this notation, we find that these 8 permutations produce the permutation group D_4 (see Fraleigh's Table 8.12 on page 80 of the 7th edition; the subgroup diagram is also given on page 80). Here are both the group diagram and the corresponding field diagram.



$H_1 = \{\rho_0, \rho_2, \mu_1, \mu_2\}$
$H_2 = \{\rho_0, \rho_1, \rho_2, \rho_3\}$
$H_3 = \{\rho_0, \rho_2, \delta_1, \delta_2\}$
$H_4 = \{\rho_0, \mu_1\}$
$H_5 = \{\rho_0, \mu_2\}$
$H_6 = \{\rho_0, \rho_2\}$
$H_7 = \{\rho_0, \delta_1\}$
$H_8 = \{\rho_0, \delta_2\}$



$K_{H_1} = \mathbb{Q}(\sqrt{2})$
$K_{H_2} = \mathbb{Q}(i)$
$K_{H_3} = \mathbb{Q}(i\sqrt{2})$
$K_{H_4} = \mathbb{Q}(\sqrt[4]{2})$
$K_{H_5} = \mathbb{Q}(i\sqrt[4]{2})$
$K_{H_6} = \mathbb{Q}(\sqrt{2}, i)$
$K_{H_7} = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$
$K_{H_8} = \mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2})$

Example. (Fraleigh, Example 54.7) Consider the splitting field of $x^4 + 1$ over $\mathbb{Q}$. The roots of $x^4 + 1$ are

$$\alpha = \frac{1+i}{\sqrt{2}},\ \alpha^3 = \frac{-1+i}{\sqrt{2}},\ \alpha^5 = \frac{-i-i}{\sqrt{2}},\ \alpha^7 = \frac{1-i}{\sqrt{2}}.$$

So the splitting field K of $x^4 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha)$ and $[K : \mathbb{Q}] = 4$ since a basis for K over $\mathbb{Q}$ is $\{1, 1/\sqrt{2}, i/\sqrt{2}, i\}$. Now to find $\mathrm{Aut}_{\mathbb{Q}}(K)$. By Theorem V.4.2(ii), $\mathrm{Aut}_{\mathbb{Q}}(K)$ is isomorphic to a transitive subgroup of S_4, so there is an automorphism of K mapping α to each conjugate of α. Such an automorphism σ is determined by the value of $\sigma(\alpha)$, so there are four such automorphisms:

Permutation σ	σ_1	σ_3	σ_5	σ_7
$\sigma(\alpha)$	α	α^3	α^5	α^7

We can verify that the group $\langle\{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}, \cdot\rangle$ is isomorphic to $\langle\{1, 3, 5, 7\}, \cdot_8\rangle$ which in turn is isomorphic to the Klein 4-group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. The proper nontrivial

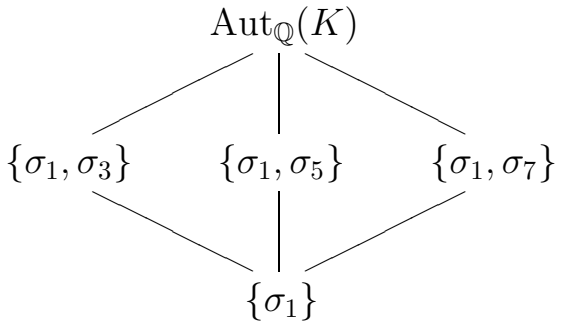
subgroups of $\{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$ are $\{\sigma_1, \sigma_3\}$, $\{\sigma_1, \sigma_5\}$, and $\{\sigma_1, \sigma_7\}$. The intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha) = \mathbb{Q}((1+i)/\sqrt{2})$ are $\mathbb{Q}(i\sqrt{2})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{2})$. We find

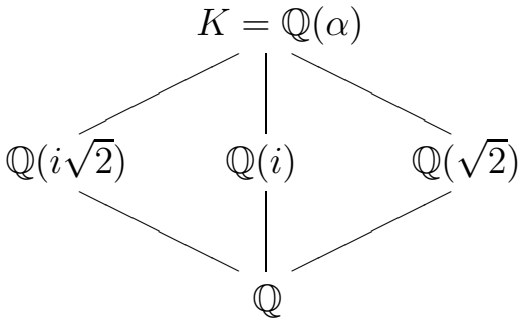
1. $\sigma_1(\alpha) + \sigma_3(\alpha) = \alpha + \alpha^3 = i\sqrt{2}$, so $\sigma_1(i\sqrt{2}) = \sigma_1(\alpha + \alpha^3) = \sigma_1(\alpha) + \sigma_1(\alpha^3) = \alpha + \alpha^3 = i\sqrt{2}$ and $\sigma_3(i\sqrt{2}) = \sigma_3(\alpha + \alpha^3) = \sigma_3(\alpha) + \sigma_3(\alpha^3) = \alpha^3 + \alpha = i\sqrt{2}$.

2. $\sigma_1(\alpha) + \sigma_7(\alpha) = \alpha + \alpha^7 = \sqrt{2}$, so $\sigma_1(\sqrt{2}) = \sigma_1(\alpha + \alpha^7) = \sigma_1(\alpha) + \sigma_1(\alpha^7) = \alpha + \alpha^7 = \sqrt{2}$ and $\sigma_7(\sqrt{2}) = \sigma_7(\alpha + \alpha^7) = \sigma_7(\alpha) + \sigma_7(\alpha^7) = \alpha^7 + \alpha = \sqrt{2}$.

3. $\sigma_1(\alpha)\sigma_5(\alpha) = \alpha\alpha^5 = \alpha^6 = -i$, so $\sigma_1(-i) = \sigma_1(\alpha\sigma_5(\alpha)) = \sigma_1(\alpha)\sigma_5(\alpha) = \alpha\alpha^5 = \alpha^6 = -i$ and $\sigma_5(-i) = \sigma_5(\alpha\sigma_5(\alpha)) = \sigma_5(\alpha)\sigma_5(\alpha^5) = \alpha^5\alpha = \alpha^6 = -i$.

and so $K_{\{\sigma_1,\sigma_3\}} = \mathbb{Q}(i\sqrt{2})$, $K_{\{\sigma_1,\sigma_7\}} = \mathbb{Q}(\sqrt{2})$, and $K_{\{\sigma_1,\sigma_5\}} = \mathbb{Q}(i)$. Therefore the group diagram and field diagram are:





Theorem V.4.12. If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers $\mathbb{Q}$ which has precisely two nonreal roots in the field of complex numbers $\mathbb{C}$ and $p-2$ real roots, then the Galois group of f is isomorphic to S_p.

Note. Hungerford gives examples of the computation of Galois groups for several 4th degree polynomials on pages 274–276. He then states that "Specific techniques for computing Galois groups of polynomials of degree greater than 4 over arbitrary fields are rather scarce." Theorem V.4.12 allows us to show that the Galois group of a certain type of polynomial is S_p.

Example. Consider $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. We can use Calculus I to show that f has exactly three distinct real roots and, by the Fundamental Theorem of Algebra, two complex roots. By Eisenstein's Criterion (Theorem III.6.15) with $p = 2$, f is irreducible. So by Theorem V.4.12, the Galois group is S_5.

Revised: 5/2/2016