Section X.54. Illustrations of Galois Theory

Note. In this section we introduce the idea of a symmetric function which is based on the idea of permutations. The application of these permutations (which we know to be elements of a group) are applied to polynomials in Section 56 to prove the "final goal": A fifth degree polynomial equation is not (in general) algebraically solvable.

Note. Recall that if F is a field then $F[x]$ is an integral domain (Section 22, Exercise 24). By Theorem 21.5, integral domain $F[x]$ can be extended to a field of quotients, denoted $F(x)$ (this is described on page 201). Similarly, integral domain $F[x_1, x_2, \ldots, x_n]$ can be extended to the field of rational functions in n indeterminates over F, denoted $F(x_1, x_2, \ldots, x_n)$. In the following, we denote the indeterminates as $y_1, y_2, \ldots, y_n$.

Note. Let F be a field and let $y_1, y_2, \ldots, y_n$ be indeterminates. Let $\sigma \in S_n$ be a permutation of $\{1, 2, \ldots, n\}$. Then σ gives rise to a natural map $\overline{\sigma} : F(y_1, y_2, \ldots, y_n) \to F(y_1, y_2, \ldots, y_n)$ given by

$$\overline{\sigma}\left(\frac{f(y_1, y_2, \ldots, y_n)}{g(y_1, y_2, \ldots, y_n)}\right) = \frac{f(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)})}{g(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)})}$$

for $f(y_1, y_2, \ldots, y_n), g(y_1, y_2, \ldots, y_n) \in F[y_1, y_2, \ldots, y_n]$ with $g(y_1, y_2, \ldots, y_n) \neq 0$.

Note. As a **homework problem**, you will show that $\overline{\sigma}$ is an automorphism of $F(y_1, y_2, \ldots, y_n)$ leaving F fixed (where we treat F as the subfield of $F(y_1, y_2, \ldots, y_n)$ consisting of constant polynomials)—that is, $\overline{\sigma} \in G(F(y_1, y_2, \ldots, y_n)/F)$.

Definition 54.1. An element $f(y_1, y_2, \ldots, y_n)/g(y_1, y_2, \ldots, y_n)$ of the field of rational functions in n indeterminates over F, $F(y_1, y_2, \ldots, y_n)$, is a *symmetric function* in $y_1, y_2, \ldots, y_n$ over F if it is left fixed by all $\overline{\sigma}$ for $\sigma \in S_n$:

$$\overline{\sigma}\left(\frac{f(y_1, y_2, \ldots, y_n)}{g(y_1, y_2, \ldots, y_n)}\right) = \frac{f(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)})}{g(y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(n)})} \text{ for all } \sigma \in S_n.$$

Note. Let $\overline{S}_n = \{\overline{\sigma} \mid \sigma \in S_n\}$. As a **homework problem**, you will show that $\overline{S}_n$ is a group isomorphic to S_n.

Definition. Let F be a field and $F(y_1, y_2, \ldots, y_n)$ be the field of rational functions in indeterminates $y_1, y_2, \ldots, y_n$. Then

$$f(x) = \prod_{i=1}^{n}(x - y_i) \in (F(y_1, y_2, \ldots, y_n))[x]$$

is a *general polynomial of degree n*. The coefficients of $f(x)$ are *elementary symmetric functions* in $y_1, y_2, \ldots, y_n$. We denote the elementary symmetric functions as s_i where s_i is the coefficient of x^{n-i} for $i = 1, 2, \ldots, n$.

Note. Since $\overline{S}_n$ is a group of automorphisms of $F(y_1, y_2, \ldots, y_n)$, by Theorem 48.11, the collection of elements fixed by all $\overline{\sigma} \in \overline{S}_n$ forms a subfield of $F(y_1, y_2, \ldots, y_n)$, say subfield K. For each $\overline{\sigma} \in \overline{S}_n$, define $\overline{\sigma}_x$ as the extension of $\overline{\sigma}$ from $F(y_1, y_2, \ldots, y_n)$ to $(F(y_1, y_2, \ldots, y_n))[x]$ where $\overline{\sigma}_x(x) = x$. Then the general polynomial of degree n, $f(x)$, is left fixed by each $\overline{\sigma}_x$ since

$$f(x) = \prod_{i=1}^{n}(x - y_i) = \prod_{i=1}^{n}(x - y_{\sigma(i)}).$$

So the coefficients of $f(x)$ are left fixed by $\overline{\sigma}_x$ and the coefficients are in K. (See the notes for Section 53 for the expression of the coefficients in terms of $-y_i$.) That is, the elementary symmetric functions are fixed by all $\overline{\sigma}_x$ for $\sigma \in S_n$.

Theorem 54.2. Let $s_1, s_2, \ldots, s_n$ be the elementary symmetric functions in the indeterminates $y_1, y_2, \ldots, y_n$. Then every symmetric function of $y_1, y_2, \ldots, y_n$ over F is a rational function of the elementary symmetric functions. Also, $F(y_1, y_2, \ldots, y_n)$ is a finite normal extension of degree $n!$ of $F(s_1, s_2, \ldots, s_n)$ and the Galois group of this extension is naturally isomorphic to S_n.

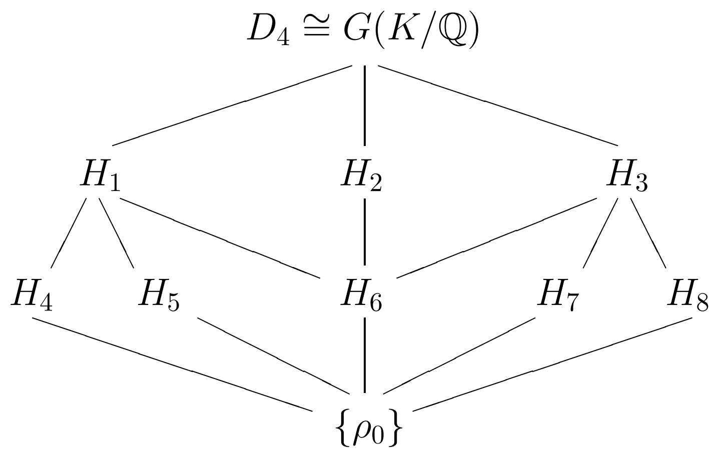
Note. The textbook repeatedly comments as to how the subgroup diagram of a Galois group is (structurally) the same as its inversion. In all examples we have seen so far, the diagrams have been vertically symmetric. The following example involves a diagram that is not vertically symmetric. It is a standard example which can also be found in Hungerford's *Algebra*, page 275 of Section V.4, "The Galois Group of a Polynomial."

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 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 $\mathbb{Q} \leq E = \mathbb{Q}(\alpha) \leq K = \mathbb{Q}(\alpha, i)$.

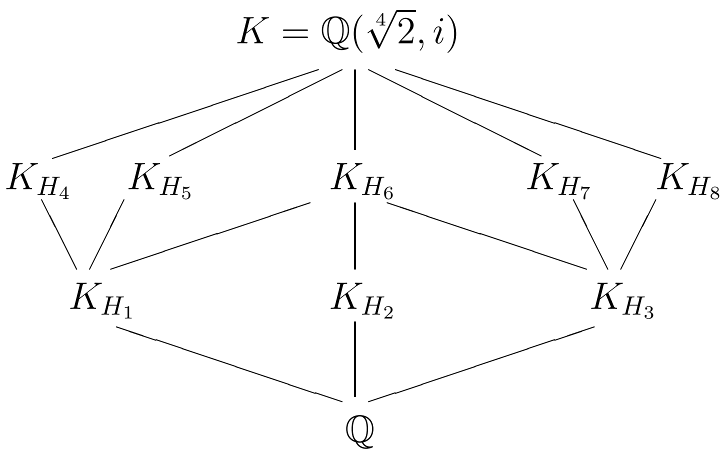
Now, a basis for $E = \mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $\{1, \alpha, \alpha^2, \alpha^3\}$, and a basis for $K = \mathbb{Q}(\alpha, i)$ over $E = \mathbb{Q}(\alpha)$ is $\{1, i\}$. So $[E : \mathbb{Q}] = 4$ and $[K : E] = 2$. So by Theorem 31.4, $[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] = 8$. 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 (and by Note 2 of the notes for Section 51, K is a separable extension of $\mathbb{Q}$), so K is a separable splitting field of $\mathbb{Q}$—that is, K is a finite normal extension of $\mathbb{Q}$. So, by the Main Theorem of Galois Theory, Property 4, $[K : \mathbb{Q}] = |G(K/\mathbb{Q})| = 8$. 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 Corollary 48.5, $\sigma(\alpha)$ 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 as given in Table 8.12 on page 80. The subgroup diagram is given on page 80. Here are both the group diagram and the corresponding field diagram.



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



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

Note. Recall that for fields $F \leq E$ and for $H \leq G(E/F)$, we denote by K_H the subfield of E left fixed by the elements of H. We now discuss how K_H is determined in part of the previous example. For $H_4 = \{\rho_0, \mu_1\}$, we need an algebraic extension of $\mathbb{Q}$ of degree 4 (since $[K : K_{H_4}] = |\lambda(K_{H_4})| = |H_4| = 2$ by the Main Theorem of Galois Theory, Properties 3 and 4, and by Theorem 31.4 $[K : \mathbb{Q}] = [K : K_{H_4}][K_{H_4} : \mathbb{Q}]$ or $8 = 2[K_{H_4} : \mathbb{Q}]$ or $[K_{H_4} : \mathbb{Q}] = 4$) which is left fixed by ρ_0 (the identity) and μ_1 (where $\mu_1(i) = -i$). So we cannot have any purely imaginary numbers in K_{H_4}. If we take $K_{H_4} = \mathbb{Q}(\alpha)$, then this is certainly left fixed by $H_4 = \{\rho_0, \mu_1\}$. By the Main Theorem of Galois Theory, the subgroup of $G(K/F)$ leaving E fixed (where $F \leq E \leq K$) is denoted $\lambda(E)$ and λ is a one to one map of the set of intermediate fields onto the set of all subgroups of $G(K/F)$, so, by Property 3, $\lambda(K_{H_4}) = H_4$ and there is only one such K_{H_4} left fixed by H_4—since $\mathbb{Q}(\alpha)$ satisfies this property, it must be that $K_{H_4} = \mathbb{Q}(\alpha)$.

Note. For $H_7 = \{\rho_0, \delta_1\}$ in the above example, we again cannot have any purely imaginary numbers in K_{H_7} since $\delta_1(i) = -i$. Also, as in the previous note, we need an extension of $\mathbb{Q}$ of degree 4. So we must choose between $\mathbb{Q}(\alpha)$, $\mathbb{Q}(i\alpha)$, $\mathbb{Q}(\alpha + i\alpha)$, $\mathbb{Q}(\alpha - i\alpha)$, and $\mathbb{Q}(\sqrt{2}, i)$ (the last one is an extension of degree 4 since $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \times 2 = 4$ by Theorem 31.4). So we can apply δ_1 to α, $i\alpha$, $\alpha + i\alpha$, $\alpha - i\alpha$, and ($\sqrt{2}$ and i) to see which is fixed. We find $\delta_1(\alpha + i\alpha) = \delta_1(\alpha) + \delta_1(i)\delta_1(\alpha) = i\alpha + (-i)(i\alpha) = \alpha + i\alpha$. So $\mathbb{Q}(\alpha + i\alpha)$ is fixed by H_7 and so $K_{H_7} = \mathbb{Q}(\alpha + i\alpha)$. (We can also check that no other subgroup of order 2 of $G(K/\mathbb{Q})$ fixes $\alpha + i\alpha$, but this is not necessary based on the one to one property of the mapping λ.)

Note. Now, suppose we wish to find $\mathrm{irr}(\sqrt[4]{2}+i\sqrt[4]{2},\mathbb{Q}) = \mathrm{irr}(\alpha+i\alpha,\mathbb{Q})$. First, for every conjugate of $\alpha+i\alpha$ (in the sense defined in Section 48, not "complex conjugate"), there is an automorphism of K mapping $\alpha+i\alpha$ to that conjugate (by Theorem 48.3). So if we find all the conjugates of $\alpha+i\alpha$ by applying the 8 elements of $G(K/\mathbb{Q})$ to $\alpha+i\alpha$, then we can find $\mathrm{irr}(\alpha+i\alpha,\mathbb{Q})$. We find

$$\rho_0(\alpha+i\alpha) = \alpha+i\alpha = \delta_1(\alpha+i\alpha),$$

$$\rho_1(\alpha+i\alpha) = i\alpha-\alpha = \mu_2(\alpha+i\alpha),$$

$$\rho_2(\alpha+i\alpha) = -\alpha-i\alpha = \delta_2(\alpha+i\alpha),$$

$$\rho_3(\alpha+i\alpha) = -i\alpha+\alpha = \mu_1(\alpha+i\alpha).$$

So $\mathrm{irr}(\alpha+i\alpha,\mathbb{Q}) = (x-(\alpha+i\alpha))(x-(i\alpha-\alpha))(x-(-\alpha-i\alpha))(x-(-i\alpha+\alpha)) = x^4+8$.

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 $G(K/\mathbb{Q})$. By Theorem 48.3, 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

$$\sigma_1(\alpha) + \sigma_3(\alpha) = \alpha + \alpha^3 = i\sqrt{2}$$

$$\sigma_1(\alpha) + \sigma_7(\alpha) = \alpha + \alpha^7 = \sqrt{2}$$

$$\sigma_1(\alpha)\sigma_5(\alpha) = -i$$

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:

$$\begin{tikzcd}
& G(K/\mathbb{Q}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{\sigma_1, \sigma_3\} \arrow[dr, dash] & \{\sigma_1, \sigma_5\} \arrow[d, dash] & \{\sigma_1, \sigma_7\} \arrow[dl, dash] \\
& \{\sigma_1\} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& K = \mathbb{Q}(\alpha) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(i\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Revised: 5/1/2015