Examples 16.9.2 Here F denotes the field $\mathbb{Q}$ of rational numbers.

(a) Let α be the "nested" square root $\alpha = \sqrt{4+\sqrt{5}}$. To determine the irreducible polynomial for α over F, we guess that its roots might be $\pm\alpha$ and $\pm\alpha'$, where $\alpha' = \sqrt{4-\sqrt{5}}$. Having made this guess, we expand the polynomial

$$f(x) = (x-\alpha)(x+\alpha)(x-\alpha')(x+\alpha') = x^4 - 8x^2 + 11.$$

It isn't very hard to show that this polynomial is irreducible over F. We'll leave the proof as an exercise. So it is the irreducible polynomial for α over F. Let K be the splitting field of f. Then

$$F \subset F(\alpha) \subset F(\alpha, \alpha') \quad \text{and} \quad F(\alpha, \alpha') = K.$$

Since f is irreducible, $[F(\alpha):F] = 4$ and since $\sqrt{5}$ is in $F(\alpha)$, $\alpha' = \sqrt{4-\sqrt{5}}$ has degree at most 2 over $F(\alpha)$. We don't yet know whether or not α' is in the field $F(\alpha)$. In any case, $[K:F]$ is 4 or 8. The Galois group G of K/F also has order 4 or 8, so it is D_4, C_4, or D_2.

Which of the conjugate subgroups D_4 might operate depends on how we number the roots. Let's number them this way:

$$\alpha_1 = \alpha, \quad \alpha_2 = \alpha', \quad \alpha_3 = -\alpha, \quad \alpha_4 = -\alpha'.$$

With this ordering, an automorphism that sends $\alpha_1 \rightsquigarrow \alpha_i$ also sends $\alpha_3 \rightsquigarrow -\alpha_i$. The permutations with this property form the dihedral group D_4 generated by

$$\sigma = (\mathbf{1234}) \text{ and } \tau = (\mathbf{24}). \tag{16.9.3}$$

Our Galois group is a subgroup of this group. It can be the whole group D_4, the cyclic group C_4 generated by σ, or the dihedral group D_2 generated by σ^2 and τ.

Note: We must be careful: Every element of this group D_4 permutes the roots, but we don't yet know which of these permutations come from automorphisms of K. A permutation that doesn't come from an automorphism tells us nothing about K. □

There is one permutation, $\rho = \sigma^2 = (\mathbf{13})(\mathbf{24})$, that is in all three of the groups D_4, C_4, and D_2, so it extends to an F-automorphism of K that we denote by ρ too. This automorphism generates a subgroup N of G of order 2.

To compute the fixed field K^N, we look for expressions in the roots that are fixed by ρ. It isn't hard to find some: $\alpha^2 = 4+\sqrt{5}$ and $\alpha\alpha' = \sqrt{11}$. So K^N contains the field $L = F(\sqrt{5}, \sqrt{11})$. We inspect the chain of fields $F \subset L \subset K^N \subset K$. We have $[K:F] \le 8$, $[L:F] = 4$, and $[K:K^N] = 2$ (Fixed Field Theorem). It follows that $L = K^N$, that $[K:F] = 8$, and that G is the dihedral group D_4.

(b) Let $\alpha = \sqrt{2+\sqrt{2}}$. The irreducible polynomial for α over F is $x^4 - 4x^2 + 2$. Its roots are $\alpha, \alpha' = \sqrt{2-\sqrt{2}}, -\alpha, -\alpha'$ as before. Here $\alpha\alpha' = \sqrt{2}$, which is in the field $F(\alpha)$. Therefore α' is also in that field. The degree $[K:F]$ is 4, and G is either C_4 or D_2.

Because the operation of G on the roots is transitive, there is an element σ' of G that sends $\alpha \rightsquigarrow \alpha'$. Since $\alpha^2 = 2+\sqrt{2}$ and $\alpha'^2 = 2-\sqrt{2}$, σ' sends $\sqrt{2} \rightsquigarrow -\sqrt{2}$ and $\alpha\alpha' \rightsquigarrow -\alpha\alpha'$.

This implies that $\alpha' \rightsquigarrow -\alpha$. So $\sigma' = \sigma$. The Galois group is the cyclic group C_4.

(c) Let $\alpha = \sqrt{4+\sqrt{7}}$. Its irreducible polynomial over F is $x^4 - 8x^2 + 9$. Here $\alpha\alpha' = 3$. Again, α' is in the field $F(\alpha)$, and the degree $[K:F]$ is 4. If an automorphism σ' sends $\alpha \rightsquigarrow \alpha'$, then since $\alpha\alpha' = 3$, it must send $\alpha' \rightsquigarrow \alpha$. The Galois group is D_2.

One can analyze any quartic polynomial of the form $x^4 + bx^2 + c$ in this way. □

It is harder to analyze a general quartic

(16.9.4)
$$f(x) = x^4 - a_1x^3 + a_2x^2 - a_3x + a_4,$$

because its roots $\alpha_1, \ldots, \alpha_4$ can rarely be written explicitly in a useful way. The main method is to look for expressions in the roots that are fixed by some, but not all, of the permutations in S_4. The square root of the discriminant D is the first such expression:

$$\delta = \prod_{i<j}(\alpha_i - \alpha_j) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4).$$

Because the roots are distinct, δ isn't zero, and as is true for cubic equations (16.8.4), a permutation σ of the roots multiplies δ by the sign of the permutation. Even permutations fix δ and odd permutations do not fix δ.

Proposition 16.9.5 Let G be the Galois group of an irreducible quartic polynomial f. The discriminant D of f is a square in F if and only if G contains no odd permutation. Therefore

- If D is a square in F, then G is A_4 or D_2.
- If D is not a square in F, then G is S_4, D_4, or C_4.

Proof. D is a square in F if and only if δ is in F, which happens when every element of G fixes δ. The permutations that fix δ are the even permutations. The last statements are proved by looking at the list (16.9.1) of transitive subgroups of S_4. □

There is an analogous statement for splitting fields of a polynomial of any degree.

Proposition 16.9.6 Let K be a splitting field over F of an irreducible polynomial f of degree n in $F[x]$, and let D be the discriminant of f. The Galois group $G(K/F)$ is a subgroup of the alternating group A_n if and only if D is a square in F. □

Lagrange found another useful expression in the roots α_i, one that is special to quartic polynomials. Let

(16.9.7)
$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3,$$

and let

$$g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3).$$