Notes on Galois Theory IV

In this final set of notes, we describe some applications and examples of Galois theory.

7 The Fundamental Theorem of Algebra

Recall that the statement of the Fundamental Theorem of Algebra is as follows:

Theorem 7.1. *The field $\mathbb{C}$ is algebraically closed, in other words, if K is an algebraic extension of $\mathbb{C}$ then $K = \mathbb{C}$.*

Despite its name, the Fundamental Theorem of Algebra cannot be a result in pure algebra since the real numbers and hence the complex numbers are not algebraically defined. While there are many proofs, most use some basic facts in complex analysis or plane topology. We describe here a proof based on Galois theory as well as some non-trivial finite group theory, namely the Sylow theorems, but which only depends on two basic facts about the real numbers $\mathbb{R}$ which are usually presented (but not carefully proved!) in a first year calculus class, both of which depend on the Intermediate Value Theorem:

1. Let $f \in \mathbb{R}[x]$ be a polynomial of odd degree. Then f has a real root.
2. Every real number $r \geq 0$ has a real square root.

It follows that every **complex** number $a + bi$ has a complex square root: Choose complex numbers c, d such that

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2}; \qquad d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2},$$

noting that $\pm a + \sqrt{a^2 + b^2} \geq 0$. Then $(c + di)^2 = (c^2 - d^2) + 2cdi$. By construction $c^2 - d^2 = a$, and

$$(2cd)^2 = 4 \cdot \frac{1}{4}(a^2 + b^2 - a^2) = b^2.$$

Hence there is a choice of signs for c, d such that $2cd = b$, and hence $c + di$ is a square root of $a + bi$.

Proof of the Fundamental Theorem of Algebra. Let E be an algebraic extension of $\mathbb{C}$ and let $\alpha \in E$. We shall show that $\alpha \in \mathbb{C}$. Since α is algebraic over $\mathbb{C}$ and $\mathbb{C}$ is algebraic over $\mathbb{R}$, α is algebraic over $\mathbb{R}$. If f is the irreducible polynomial for α over $\mathbb{R}$, we can find a Galois extension K of $\mathbb{R}$ with $\alpha \in K$ and such that $\mathbb{C}$ is a subfield of K (for instance, by taking the splitting field of $(x^2 + 1)f$ over $\mathbb{R}$). Let $G = \mathrm{Gal}(K/\mathbb{R})$. Then, since G is a finite group, we can apply the Sylow theorem for G and the prime 2 to conclude that there exists a 2-Sylow subgroup P of G. In other words, $\#(P)$ is a power of 2 and the index $(G : P) = \#(G)/\#(P)$ is not divisible by 2, i.e. is odd. We claim first that $P = G$, in other words that the order of G is a power of 2. To see this, consider the fixed field K^P. Then K^P is a finite extension of $\mathbb{R}$ and $[K^P : \mathbb{R}] = (G : P)$ is odd. Hence, if $\beta \in K^P$, then $[\mathbb{R}(\beta) : \mathbb{R}]$ divides $[K^P : \mathbb{R}]$, hence $[\mathbb{R}(\beta) : \mathbb{R}] = \deg_{\mathbb{R}} \beta$ is odd. It follows that $\mathrm{irr}(\beta, \mathbb{R})$ is an irreducible polynomial in $\mathbb{R}[x]$ of odd degree. By the first fact above, $\mathrm{irr}(\beta, \mathbb{R})$ has a real root, hence a linear factor in $\mathbb{R}[x]$. Since $\mathrm{irr}(\beta, \mathbb{R})$ is irreducible it must be of the form $x - \beta$ and hence $\beta \in \mathbb{R}$. Thus $K^P = \mathbb{R} = K^G$ and hence $G = P$.

Now consider the subgroup $Q = \mathrm{Gal}(K/\mathbb{C})$ of $G = \mathrm{Gal}(K/\mathbb{R})$. We will show that $Q = \{\mathrm{Id}\}$ and hence that $K = \mathbb{C}$. In any case, Q is a subgroup of $G = P$ and hence its order is a power of 2. Now, another basic group theory fact is that, if H is a group whose order is p^n, where p is a prime, then H has subgroups of every possible order p^k, $k \leq n$. Applying this to Q, we see that, if $Q \neq \{\mathrm{Id}\}$, then $\#(Q) = 2^n$ with $n \geq 1$ and hence that there exists a subgroup Q_0 of Q of order 2^{n-1}. Then if K^{Q_0} is the fixed field, $[K^{Q_0} : \mathbb{C}] = (Q : Q_0) = 2$. Hence K^{Q_0} is a quadratic extension of $\mathbb{C}$. But, as we have seen on the homework, since the characteristic of $\mathbb{C}$ is not 2, there exists an element $\gamma \in \mathbb{C}$ such that $K^{Q_0} = \mathbb{C}(\sqrt{\gamma})$, where $\sqrt{\gamma}$ is some element of K^{Q_0} whose irreducible polynomial is $x^2 - \gamma$ since $[K^{Q_0} : \mathbb{C}] = 2$. On the other hand, by the second fact above, $x^2 - \gamma$ has a root in $\mathbb{C}$, hence is not irreducible. This is a contradiction to the assumption $Q \neq \{\mathrm{Id}\}$. It follows that $Q = \mathrm{Gal}(K/\mathbb{C}) = \{\mathrm{Id}\}$ and thus that $K = \mathbb{C}$. Hence, if α is algebraic over $\mathbb{C}$, then $\alpha \in \mathbb{C}$, so that $\mathbb{C}$ is algebraically closed. □

8 Galois groups of polynomials

For the remainder of these notes, we will shift attention from extension fields to polynomials. Also, to avoid having to worry about separability or other

issues related to positive characteristic, we will always assume for the rest of these notes that F is a field **of characteristic zero**. Hence every finite normal extension of F is a Galois extension.

Definition 8.1. Let $f \in F[x]$ be a non-constant polynomial, in other words, $\deg f \geq 1$ (but f is not necessarily irreducible). We define the *Galois group* of f over F to be $\mathrm{Gal}(E/F)$, where E is any splitting field of f over F. Since two splitting fields of f over F are isomorphic by an isomorphism which is the identity on F, the group $\mathrm{Gal}(E/F)$ is independent of the choice of E.

Thus, if f has degree n and it has no multiple roots (which is always the case if f is irreducible since we have assumed that the characteristic of F is zero), we can number the n distinct roots of f in E as $\alpha_1, \ldots, \alpha_n$. Then the Galois group of f is isomorphic to a subgroup of S_n, the symmetric group on n letters. We will sometimes identify σ with the corresponding permutation of $\{1, \ldots, n\}$. By Lagrange's theorem, the order of $\mathrm{Gal}(E/F)$ must then divide $n!$. We have already seen the following:

Proposition 8.2. *Let $f \in F[x]$ be an irreducible polynomial of degree n and let E be a splitting field of f over F. Then* $\mathrm{Gal}(E/F)$ *acts transitively on the set $\{\alpha_1, \ldots, \alpha_n\}$. Hence n divides the order of* $\mathrm{Gal}(E/F)$. □

9 Symmetric polynomials

Let $f \in F[x]$ be a monic polynomial of degree n, let E be an extension field of F. Suppose that $\alpha_1, \ldots, \alpha_n \in E$ are the n roots of f, not necessarily distinct. Then $G = \mathrm{Gal}(E/F)$ permutes the α_i. Hence any expression in the α_i which is left unchanged after a permutation of the α_i is fixed by every element of G, and hence lies in $E^G = F$. In general, we call a polynomial $P(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ a *symmetric polynomial* if, for all $\sigma \in S_n$,

$$P(t_1, \ldots, t_n) = P(t_{\sigma(1)}, \ldots, t_{\sigma(n)}),$$

in other words the polynomial P is unchanged when we permute the variables,and we call an element of E of the form $P(\alpha_1, \ldots, \alpha_n)$, where P is a symmetric polynomial, a *symmetric expression in the α_i*. The basic examples of such expressions are the *elementary symmetric functions* in the

α_i:

$$
\begin{aligned}
s_1 &= \alpha_1 + \cdots + \alpha_n = \sum_{i=1}^{n} \alpha_i; \\
s_2 &= \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = \sum_{i<j} \alpha_i\alpha_j; \\
s_3 &= \alpha_1\alpha_2\alpha_3 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n = \sum_{i<j<k} \alpha_i\alpha_j\alpha_k; \\
&\vdots \\
s_n &= \alpha_1 \cdots \alpha_n.
\end{aligned}
$$

However, it is easy to see directly that the $s_i \in F$. In fact, since the α_i are the n distinct roots of f,

$$
\begin{aligned}
f &= (x-\alpha_1)\cdots(x-\alpha_n) \\
&= x^n - (\alpha_1 + \cdots + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n)x^{n-2} - \cdots + (-1)^n\alpha_1\cdots\alpha_n \\
&= x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n.
\end{aligned}
$$

Thus the terms $(-1)^i s_i$ are the coefficients of f and hence lie in F. Other examples of symmetric expressions in the α_i are expressions of the form $\alpha_1^k + \cdots + \alpha_n^k$, but in fact these can be written as polynomials in the s_i. In fact, one can show that every symmetric polynomial $P(x_1, \ldots, x_n)$ lies in $F[s_1, \ldots, s_n]$, i.e. is a polynomial in the s_i.

Other examples of this idea may be found in these notes and in the homework. A related idea is the following: Given a subgroup H of $G = \mathrm{Gal}(E/F)$, we can look for expressions in the α_i which are invariant under the action of H but not under the action of the full Galois group G. Such expressions will give elements of the fixed field E^H which do not lie in F. We have already seen examples of this, in the discussion of $\mathbb{Q}(\alpha)$, where α is a root of $x^4 - 10x^2 + 1$, in Example 4.2 of the handout, "Notes on Galois Theory," as well as in the discussion of D_4 extensions. We will give more examples of this idea below.

10 The discriminant

Let f be a polynomial in $F[x]$ of degree n with roots $\alpha_1, \ldots, \alpha_n$ in some normal extension field E of F, which for the moment are not necessarily assumed to be distinct. Let $G = \mathrm{Gal}(E/F)$. If $E = F(\alpha_1, \ldots, \alpha_n)$, then G is

isomorphic to a subgroup of S_n, but in general we still get a homomorphism from G to S_n. Now S_n has a subgroup of fundamental importance, the alternating group A_n, and we wish to see under what conditions the image of the Galois group is actually a subgroup of A_n. The answer is given by looking at the following element of E:

Definition 10.1. Define the *discriminant*

$$\Delta = \Delta(f) = \left(\prod_{i<j} (\alpha_j - \alpha_i) \right)^2 .$$

By construction, there is also a square root of Δ in E, defined by

$$\sqrt{\Delta} = \prod_{i<j} (\alpha_j - \alpha_i).$$

Note that $\Delta(f) = 0 \iff f$ has a multiple root.

For example, let f be monic of degree 2, say $f = x^2 + bx + c$. If $f = (x - \alpha_1)(x - \alpha_2)$, then $-b = \alpha_1 + \alpha_2$ and $c = \alpha_1\alpha_2$. Thus

$$\begin{aligned} \Delta(f) &= (\alpha_2 - \alpha_1)^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 \\ &= \alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2 - 4\alpha_1\alpha_2 = (\alpha_2 + \alpha_1)^2 - 4\alpha_1\alpha_2 \\ &= b^2 - 4c. \end{aligned}$$

For degrees larger than 2, $\Delta(f)$ is given by a very complicated expression in the coefficients of f. In degree 3, assuming that $f = x^3 + a_2x^2 + a_1x + a_0$ is monic, we can always arrange that the coefficient of x^2 is 0 by "completing the cube," i.e. by replacing x by $x - a_2/3$ (this works for any field not of characteristic 3). Thus, we can assume that $f = x^3 + px + q$ for some $p, q \in F$. In this case, a computation given below shows that

$$\Delta(f) = -4p^3 - 27q^2.$$

Proposition 10.2. *Assume that E is a splitting field of f. For every polynomial $f \in F[x]$, $\Delta = \Delta(f) \in F$. Moreover, if f does not have a multiple root, then the Galois group of f is a subgroup of $A_n \iff \sqrt{\Delta} \in F$, i.e. Δ is the square of an element of F. More generally, for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma \in A_n \iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta}$*

Proof. Clearly, if $\sigma \in \mathrm{Gal}(E/F)$, then σ permutes the $n(n-1)/2$ pairs of two elements $\{\alpha_i, \alpha_j\}$ with $i \neq j$, but it does not necessarily preserve the

condition $i < j$. Thus

$$\sigma(\sqrt{\Delta}) = \sigma\left(\prod_{i<j}(\alpha_j - \alpha_i)\right) = \prod_{i<j}(\sigma(\alpha_j) - \sigma(\alpha_i)) = \pm\sqrt{\Delta}.$$

Then

$$\sigma(\Delta) = \sigma((\sqrt{\Delta})^2) = (\pm\sqrt{\Delta})^2 = \Delta,$$

hence $\Delta \in E^{\mathrm{Gal}(E/F)} = F$. Moreover, identifying $\sigma \in \mathrm{Gal}(E/F)$ with the corresponding permutation (also denoted σ) of $\{1, 2, \ldots, n\}$ by the rule $\sigma(\alpha_i) = \alpha_{\sigma(i)}$, one of the many definitions of the sign of a permutation says that the sign of σ (often written as $\mathrm{sign}(\sigma)$ or as $\varepsilon(\sigma)$) is given by

$$\prod_{i<j}(\alpha_{\sigma(j)} - \alpha_{\sigma(i)}) = \mathrm{sign}(\sigma)\prod_{i<j}(\alpha_j - \alpha_i).$$

It follows that $\sigma \in A_n \iff \sigma(\sqrt{\Delta}) = \sqrt{\Delta}$ (since we have assumed that $\Delta \neq 0$ and the characteristic of F is not 2). Hence $\sigma \in A_n$ for all $\sigma \in \mathrm{Gal}(E/F)$ $\iff$ $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$ for all $\sigma \in \mathrm{Gal}(E/F)$ $\iff$ $\sqrt{\Delta} \in E^{\mathrm{Gal}(E/F)} = F$. $\square$

Example 10.3. As we have seen, the Galois group of $f = x^3 - 2$ over $\mathbb{Q}$ is the full symmetric group S_3. Note that $\Delta(f) = -4 \cdot 27$, which is not a square in $\mathbb{Q}$ (or even in $\mathbb{R}$). On the other hand, consider the polynomial $g = x^3 - 3x + 1$, irreducible since its degree is 3 and by the rational roots test. Then

$$\Delta(g) = -4(-27) - 1(27) = 3 \cdot 27 = 9^2.$$

Hence the Galois group of g is isomorphic to A_3. Note however that we had to be somewhat lucky in the choice of the coefficients of g, and expect that, for a "random" cubic polynomial, its discriminant will not be a square, hence the Galois group of such a cubic will not be contained in A_3.

Remark 10.4. In general, if $f \in \mathbb{Q}[x]$ is irreducible of degree 3, then f does not have multiple roots, and hence (since complex roots occur in conjugate pairs) f has either one or three real roots. If f has exactly one real root, then the two non-real roots are exchanged by complex conjugation, and hence complex conjugation defines a nontrivial automorphism of the splitting field E of f over $\mathbb{Q}$ of order 2. In particular, $\mathrm{Gal}(E/\mathbb{Q})$ cannot be isomorphic to A_3. Thus, if the discriminant of f is a square, then f must have three real roots. For example, for the polynomial $g = x^3 - 3x + 1$ above, since $g' = 3(x^2 - 1)$, the critical points of g are ± 1, with $g(-1) = 3 > 0$ and

$g(1) = -1 < 0$. From sketching the graph of g, it is easy to see directly that g has exactly 3 real roots.

If $f \in \mathbb{R}[x]$ is a cubic polynomial with real coefficients, f will not be irreducible in $\mathbb{R}[x]$ since it has at least one real root. However, we can still define the discriminant of f and it is nonzero $\iff$ f does not have a multiple root. In this case, it is an easy exercise that the discriminant is positive (i.e. is a square in $\mathbb{R}$) $\iff$ f has three (distinct) real roots, and the discriminant is negative (i.e. is not a square in $\mathbb{R}$) $\iff$ f has one real and two nonreal (conjugate) roots.

Finally, we calculate the discriminant for the special cubic polynomials under consideration:

Proposition 10.5. *Let $f = x^3 + px + q \in F[x]$. Then the discriminant $\Delta(f)$ of f is $-4p^3 - 27q^2$.*

Proof. If the roots of f (in some extension field E of F) are $\alpha_1, \alpha_2, \alpha_3$, then $f = x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Equating coefficients, we see that

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0; \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= p; \\ \alpha_1\alpha_2\alpha_3 &= -q. \end{aligned}$$

To calculate the discriminant, note that, by the product rule,

$$f' = (x - \alpha_2)(x - \alpha_3) + (x - \alpha_1)(x - \alpha_3) + (x - \alpha_1)(x - \alpha_2),$$

and hence

$$\begin{aligned} f'(\alpha_1) &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3); \\ f'(\alpha_2) &= (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3); \\ f'(\alpha_3) &= (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2). \end{aligned}$$

Keeping track of the signs, it then follows that

$$f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) = (-1)^3\Delta(f) = -\Delta(f).$$

On the other hand, $f' = 3x^2 + p$, and hence

$$-\Delta(f) = f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) = (3\alpha_1^2 + p)(3\alpha_2^2 + p)(3\alpha_3^2 + p).$$

Expanding this out gives

$$-\Delta(f) = 27\alpha_1^2\alpha_2^2\alpha_3^2 + 9p(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) + 3p^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + p^3.$$

Note that $\alpha_1^2\alpha_2^2\alpha_3^2 = q^2$. Since $\alpha_1 + \alpha_2 + \alpha_3 = 0$,

$$0 = (\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3),$$

and hence

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = -2p.$$

Similarly,

$$\begin{aligned} p^2 &= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 \\ &= \alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2 + 2(\alpha_1\alpha_2\alpha_3)(\alpha_1 + \alpha_2 + \alpha_3) \\ &= \alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2, \end{aligned}$$

again using $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Plugging in these values gives

$$-\Delta(f) = 27q^2 + 9p(p^2) + 3p^2(-2p) + p^3 = 27q^2 + 4p^3,$$

and hence $\Delta(f) = -4p^3 - 27q^2$ as claimed. □

11 Some abelian extensions

Definition 11.1. Let E be a Galois extension of a field F, Then E is an *abelian extension* if $\mathrm{Gal}(E/F)$ is abelian. Likewise, if $f \in F[x]$ is a non-constant polynomial, we say that the Galois group of f is abelian if the Galois group of its splitting field over F is abelian.

Note that, if E is an abelian extension of F, then every subgroup of $\mathrm{Gal}(E/F)$ is normal and hence every intermediate field K between E and F is a Galois extension of F.

There are two main examples of abelian extensions: cyclotomic extensions and n^{th} root extensions. A *cyclotomic extension* is roughly one that is obtained via roots of unity:

Proposition 11.2. *Let E be a splitting field of $x^n - 1$ over F, let μ_n denote the set of roots of $x^n - 1$ in E, and let ζ be a generator for the cyclic group $\mu_n \leq E^*$. Then $E = F(\zeta)$ and $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. In particular, $\mathrm{Gal}(E/F)$ is abelian.*

Proof. By the definition of a splitting field, $x^n - 1$ factors into linear factors in E. All of these linear factors are distinct: the characteristic of F is zero and hence $Df = nx^{n-1}$ has all roots equal to 0. But 0 is not a root of $x^n - 1$, so $x^n - 1$ and $D(x^n - 1)$ have no roots in common, so that $x^n - 1$ has no multiple roots. Thus the set μ_n of n^{th} roots of unity in E is a subgroup of E^* of order n, and it is cyclic because every finite subgroup of E^* is cyclic. If ζ is a generator of μ_n, then $F(\zeta)$ is a subfield of E containing all the roots of $x^n - 1$, hence $F(\zeta) = E$ since E is generated over F by the roots of $x^n - 1$. If $\sigma \in \mathrm{Gal}(E/F)$, then $\sigma(\zeta)$ is also a root of $x^n - 1$, hence $\sigma(\zeta) = \zeta^i$. If $d = \gcd(i, n)$, then $(\zeta^i)^{n/d} = 1$, hence ζ^i is a root of $x^{n/d} - 1$. But then $\zeta = \sigma^{-1}(\zeta^i)$ is also a root of $x^{n/d} - 1$. Since ζ is a generator of μ_n, which has order n, the order of ζ is n. Thus $n/d \geq n$. As $n/d \leq n$, $n/d = n$, $d = 1$ and i is relatively prime to n. Hence we have shown that, if ζ is a generator for μ_n and $\sigma \in \mathrm{Gal}(E/F)$, then $\sigma(\zeta)$ is also a generator of μ_n and in particular that $\sigma(\zeta) = \zeta^i$ where $\gcd(i, n) = 1$.

Define a function $\varphi\colon \mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^*$ by the formula

$$\sigma(\zeta) = \zeta^{\varphi(\sigma)},$$

where $\varphi(\sigma)$ is an integer i, which we can take mod n. As we have seen, $\gcd(i, n) = 1$, i.e. $\varphi(\sigma)$ is a well-defined element of $(\mathbb{Z}/n\mathbb{Z})^*$. To see that φ is a homomorphism, note that by definition

$$(\sigma \circ \tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{\varphi(\tau)}) = (\sigma(\zeta))^{\varphi(\tau)} = (\zeta^{\varphi(\sigma)})^{\varphi(\tau)} = \zeta^{\varphi(\sigma)\varphi(\tau)}.$$

Hence by definition $\varphi(\sigma \circ \tau) = \varphi(\sigma)\varphi(\tau)$, so that φ is a homomorphism. It is injective since $\varphi(\sigma) = 1 \implies \sigma(\zeta) = \zeta \implies \sigma = \mathrm{Id}$ since $E = F(\zeta)$, thus $\operatorname{Ker}\varphi = \{1\}$ and φ is injective. □

In the above situation, we define a *primitive n^{th} root of unity* to be a generator of μ_n. Note that, as μ_n is cyclic of order n, there are exactly $\varphi(n)$ generators of μ_n, where φ is the Euler φ-function, and hence exactly $\varphi(n)$ primitive n^{th} roots of unity. The proof above shows that $\mathrm{Gal}(E/F)$ permutes the primitive n^{th} roots of unity. Thus, if we define

$$\Phi_n = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitive}}} (x - \zeta),$$

then $\deg \Phi_n = \varphi(n)$, and since the coefficients of Φ_n are the elementary symmetric functions in the primitive n^{th} roots of unity, they are fixed by $\mathrm{Gal}(E/F)$ and hence lie in $F[x]$. In particular $\Phi_n \in \mathbb{Q}[x]$, and in fact one

can show that $\Phi_n \in \mathbb{Z}[x]$. For a general field F, E is a splitting field for Φ_n, but whether or not Φ_n is irreducible will depend on the field F. Likewise, the order of $\mathrm{Gal}(E/F)$ will divide $\varphi(n)$, since $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and by Lagrange's theorem, but $\mathrm{Gal}(E/F) \cong (\mathbb{Z}/n\mathbb{Z})^*$ $\iff$ $\#(\mathrm{Gal}(E/F)) = \varphi(n)$ $\iff$ Φ_n is irreducible in $F[x]$.

Example 11.3. Take $F = \mathbb{Q}$ and $n = p$, a prime number. As we have seen, Φ_p is irreducible. If $\zeta_p \in \mathbb{C}$ is a root of Φ_p, then $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg \Phi_p = p-1$ and hence the order of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is $p-1$. Since the order of $(\mathbb{Z}/p\mathbb{Z})^*$ is also $p-1$, an injective homomorphism $\varphi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^*$ is also surjective and hence an isomorphism. Thus $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

A somewhat more involved argument shows that Φ_n is irreducible in $\mathbb{Q}[x]$, and hence $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ for all positive integers n.

Taking various values of p (or more generally n), we can construct abelian extensions of $\mathbb{Q}$ by looking at subfields of $\mathbb{Q}(\zeta_n)$. A famous theorem due to Kronecker-Weber, one of the landmark theorems of algebraic number theory, says that every abelian extension of $\mathbb{Q}$ arises in this way:

Theorem 11.4. *Let E be an abelian extension of $\mathbb{Q}$. Then there exists a positive integer n such that $E \leq \mathbb{Q}(\zeta_n)$ for some n.* □

One can show that every finite abelian group is a quotient of $(\mathbb{Z}/n\mathbb{Z})^*$. Thus every finite abelian group is the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ of some Galois extension of $\mathbb{Q}$. This leads to the following natural question:

Conjecture 11.5. *Let G be a finite group. Then there exists a Galois extension E of $\mathbb{Q}$ such that $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to G.*

The conjecture is known for many large classes of groups: abelian groups, solvable groups (which we will define below), S_n, A_n, and many other simple groups. It is an easy consequence of the Main Theorem of Galois theory and Cayley's theorem (that every finite group G is isomorphic to a subgroup of S_n for some n) that, given a finite group G, there exists some field F, which we can take to be a finite extension of $\mathbb{Q}$, and a Galois extension E of F, such that $\mathrm{Gal}(E/F) \cong G$. In other words, every finite group arises as the Galois group of some Galois extension. However, it is unknown if we can always take the base field F to be $\mathbb{Q}$.

We turn now to the second class of abelian extensions, n^{th} root extension. It turns out that, if we impose a strong assumption on the base field F, then these extensions are exactly those for which the Galois group is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$, or equivalently are cyclic of order dividing n.

Proposition 11.6. *Suppose that n is a positive integer and that $\mu_n \leq F^*$, i.e. the equation $x^n - 1$ has n distinct roots in F. Let $a \in F$, $a \neq 0$. If E is a splitting field for $x^n - a$ and $\alpha \in E$ is a root of $x^n - a$, then $E = F(\alpha)$. Moreover,* $\mathrm{Gal}(E/F)$ *is abelian and is isomorphic to a subgroup of* $\mathbb{Z}/n\mathbb{Z}$.

Proof. Since $\mu_n \subseteq F \subseteq E$, if $\alpha \in E$ is a root of $x^n - a$, then for every $\zeta \in \mu_n$, $\zeta\alpha$ is a root of $x^n - a$ as well, and $\zeta\alpha \in E$ since $\alpha \in E$ and $\zeta \in F \leq E$. Thus there are at least n distinct linear factors $x - \zeta\alpha$ of $x^n - a$ in $E[x]$, so that $\prod_{\zeta \in \mu_n}(x - \zeta\alpha)$ divides $x^n - a$ in $E[x]$. Since both sides are monic of degree n, they must be equal. In particular, $x^n - a$ splits into linear factors in $F(\alpha)$, and since α is a root of $x^n - a$, the field $F(\alpha)$ must be a splitting field for $x^n - a$. Thus $E = F(\alpha)$.

Fixing the root α of $x^n - a$, given $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(\alpha)$ is a root of $x^n - a$ and hence $\sigma(\alpha) = \zeta\alpha$ for some $\zeta \in \mu_n$, uniquely specified by σ since $\alpha \neq 0$. Define a function $\varphi\colon \mathrm{Gal}(E/F) \to \mu_n$ by the formula $\varphi(\sigma) = \sigma(\alpha)/\alpha$, i.e. $\varphi(\sigma)$ is the unique n^{th} root of unity such that $\sigma(\alpha) = \varphi(\sigma) \cdot \alpha$. A calculation shows that $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$, i.e. that $\varphi\colon \mathrm{Gal}(E/F) \to \mu_n$ is a homomorphism. In fact,

$$\begin{aligned}\varphi(\sigma_1 \circ \sigma_2) &= (\sigma_1 \circ \sigma_2)(\alpha)/\alpha = \sigma_1(\sigma_2(\alpha))/\alpha = \sigma_1(\varphi(\sigma_2) \cdot \alpha)/\alpha \\ &= \varphi(\sigma_2)\sigma_1(\alpha)/\alpha = \varphi(\sigma_2)\varphi(\sigma_1),\end{aligned}$$

where we have used the hypothesis $\mu_n \subseteq F$ to conclude that $\sigma_1(\zeta) = \zeta$ for all $\zeta \in \mu_n$, in particular for $\zeta = \varphi(\sigma_2)$. Thus $\varphi\colon \mathrm{Gal}(E/F) \to \mu_n$ is a homomorphism, and it is injective since $E = F(\alpha)$: $\sigma \in \operatorname{Ker}\varphi \iff \sigma(\alpha) = \alpha \iff \sigma = \mathrm{Id}$. Hence $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$. □

Remark 11.7. (i) In the situation of the previous proposition, $x^n - a$ is irreducible $\iff$ $[E : F] = n$ $\iff$ the order of $\mathrm{Gal}(E/F)$ is n $\iff$ $\mathrm{Gal}(E/F) \cong \mathbb{Z}/n\mathbb{Z}$.

(ii) If the extension E is generated by several n^{th} roots, in other words if $E = F(\alpha_1, \ldots, \alpha_k)$, where $\alpha_i^n = a_i \in F$ for every i, with $a_i \neq 0$, then (still under the assumption that $\mu_n \subseteq F$) E is a splitting field for the polynomial $(x^n - a_1) \cdots (x^n - a_k) \in F[x]$, hence E is a Galois extension of F. Moreover, by the arguments above, if $\sigma \in \mathrm{Gal}(E/F)$, then for every i, $\sigma(\alpha_i) = \zeta_i\alpha_i$ for some $\zeta_i \in \mu_n$, and the function $\varphi\colon \mathrm{Gal}(E/F) \to \mu_n \times \cdots \times \mu_n$ which sends σ to the k-tuple $(\zeta_1, \ldots, \zeta_k)$ is an injective homomorphism. Hence $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of $\mu_n \times \cdots \times \mu_n = \mu_n^k \cong (\mathbb{Z}/n\mathbb{Z})^k$ and is again abelian. Still more generally, suppose $n_1, \ldots, n_k$ are positive integers and that F contains μ_n for some positive integer n such that $n_i | n$ for every i.

Let E be generated by several n_i^{th} roots, in other words $E = F(\alpha_1, \ldots, \alpha_k)$, where $\alpha_i^{n_i} = a_i \in F$ for every i, with $a_i \neq 0$. Then E is a splitting field for $(x^{n_1} - a_1) \cdots (x^{n_k} - a_k)$, and as before the Galois group $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of $\mu_{n_1} \times \cdots \times \mu_{n_k} \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$ and is once again abelian.

There is a partial converse to Proposition 11.6:

Proposition 11.8. *Suppose that n is a positive integer and that $\mu_n \leq F^*$, i.e. the equation $x^n - 1$ has n distinct roots in F. Suppose that E is a Galois extension of F and that $\mathrm{Gal}(E/F)$ is cyclic of order n. Then there exists an $a \in F$ such that $E = F(\sqrt[n]{a})$, in other words there exists an $\alpha \in E$ such that $E = F(\alpha)$ and $\alpha^n \in F$.*

The basic idea in general is as follows: if $\sigma \in \mathrm{Gal}(E/F)$ is a generator, then we view σ as an F-linear function $E \to E$ and search for an eigenvector α of σ with eigenvalue ζ, where ζ is a primitive n^{th} root of unity, i.e. $\sigma(\alpha) = \zeta\alpha$. For example, if we begin with any $\beta \in E$, then

$$\alpha = \beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma^2(\beta) + \cdots + \zeta^{-n+1}\sigma^{n-1}(\beta)$$

is an eigenvector of σ with eigenvalue ζ, as long as we can show that $\alpha \neq 0$, since

$$\sigma(\alpha) = \sigma(\beta) + \zeta^{-1}\sigma^2(\beta) + \cdots + \zeta^{-n+1}\beta = \zeta\alpha,$$

where we have used the fact that $\sigma^n = \mathrm{Id}$ and $\zeta^n = 1$. The problem then is to find a β for which the above expression is not 0. Once we have found such an α, it follows easily that $E = F(\alpha)$ and $\alpha^n \in F$. However, the assumption that $\mu_n \subseteq F$ is rarely satisfied. For example, the only n^{th} roots of unity in $\mathbb{Q}$ are ± 1. Hence Proposition 11.8 does not apply to many of the most interesting fields.

12 Solvability by radicals

There are various ways to interpret the statement that the polynomial equation $f = 0$ is "solvable by radicals:"

1. We could ask for a "universal formula" for the roots as expressions involving the coefficients of f via repeating the field operations and taking n^{th} roots. For example, given the quadratic polynomial $f = x^2 + bx + c$, the roots α are given by the quadratic formula

$$\alpha = \frac{1}{2}(-b \pm \sqrt{b^2 - 4c}).$$

In terms of algebra, we think about a universal formula as follows: let $E = \mathbb{Q}(t_1, \ldots, t_n)$, where we could replace $\mathbb{Q}$ by some other field of characteristic 0, where the t_i are indeterminates, and consider the "universal polynomial"

$$f = (x - t_1) \cdots (x - t_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n.$$

Then f is a monic polynomial with coefficients $(-1)^k s_k$, where the s_k are polynomials in $t_1, \ldots, t_n$. For example,

$$s_1 = t_1 + \cdots + t_n, s_2 = \sum_{i<j} t_i t_j, \ldots, s_n = t_1 \cdots t_n.$$

The polynomials s_i are called the *elementary symmetric functions in the* t_i, and, if we set $F = \mathbb{Q}(s_1, \ldots, s_n)$, then one can show that the field extension $F \leq E$ is a finite extension, in fact a Galois extension with Galois group S_n. In particular $[E : F] = n!$. A universal formula in this context is a way to express the roots $t_1, \ldots, t_n$ in terms of the coefficients $s_1, \ldots, s_n$. Then, given explicit values for the s_i, we could evaluate the t_i for those values of s_i and thus write down the roots of every polynomial in $\mathbb{Q}[x]$ of degree n. (Strictly speaking, some of the expressions for the roots in terms of the s_i might involve rational functions in the s_i whose denominators would be 0 for some values of the s_i, hence would not always be defined. It turns out in fact that a universal formula involving rational expressions of the coefficients exists $\iff$ a universal formula involving polynomial expressions exists, so we don't find any new possibilities by allowing rational functions.)

2. We could ask for a somewhat weaker result: given a specific polynomial f, we could ask how to describe its roots via field operations and radicals. For example, the quadratic polynomial $f = x^2 + 2x + 3$ has roots
$$\frac{1}{2}(-2 \pm \sqrt{-8}) = -1 \pm \sqrt{-2}.$$

Note that the quadratic formula in (1) or (2) involves the field element 2. In general, we will allow constants to appear in the formulas as long as they are given by radicals themselves. For example, n^{th} roots of unity are roots of $x^n - 1$ and so will count as radicals.

Clearly, if (2) is not possible, then (1) is also not possible. We shall show that, for $n \geq 5$, (2) and hence (1) are impossible.

For future reference, let us make the idea of "expressions given by field operations and radicals" more precise:

Definition 12.1. Let $f \in F[x]$. Then f *has a root expressible by radicals* if there exist

(i) a sequence of extension fields

$$F = E_1 \leq E_2 = E_1(\alpha_1) \leq E_3 = E_2(\alpha_2) \leq \cdots \leq E_k = E_{k-1}(\alpha_{k-1});$$

(ii) positive integers $n_i, 1 \leq i \leq k-1$, such that $\alpha_i^{n_i} \in E_i$ for every i;

(iii) an element $\alpha \in E_k$ such that $f(\alpha) = 0$, i.e. α is a root of f and α is an element in a field given by taking successive n^{th} roots (for possibly different n).

The polynomial f is *solvable by radicals* if there exists a sequence of extensions satisfying (i) and (ii) above and a splitting field L of f over F contained in E_k, i.e. every root of f is expressible by radicals.

Remark 12.2. As will follow from arguments below, if f is irreducible and has a root expressible by radicals, then f is solvable by radicals.

13 Cardano's formula

For $n = 3$, there is a universal "cubic formula," sometimes called Cardano's formula. We shall write down this formula below (although it is not of practical use for a variety of reasons). Before doing so we explain what the general nature of the formula must be, via Galois theory. Let F be a field of characteristic zero and let $f \in F[x]$ be a cubic polynomial, which we can assume after completing the cube to be of the form $x^3 + px + q$. We shall also assume that $\mu_3 \subseteq F$, since this can always be arranged by enlarging F, and in any case the elements of μ_3 are radicals. Let ω be a generator for μ_3. In general, we expect that the Galois group of f is S_3, in particular that the discriminant $\Delta = \Delta(f)$ is not a square. If E is a splitting field for f over F, then there is a sequence of field extensions

$$F \leq F(\sqrt{\Delta}) \leq E.$$

Clearly $F(\sqrt{\Delta})$ is a degree two extension of F obtained by throwing in a square root, and it is a Galois extension of F corresponding to the normal subgroup $\mathrm{Gal}(E/F(\sqrt{\Delta})) \cong A_3$ of $\mathrm{Gal}(E/F) \cong S_3$. As A_3 is cyclic of order 3, we expect by Proposition 11.8 that, since F contains all of the cube roots of unity, E is of the form $F(\sqrt{\Delta})(\alpha)$ for some $\alpha \in E$ such that $\alpha^3 \in F(\sqrt{\Delta})$.

Thus the roots of f should be expressible in terms of elements of F and $\sqrt{\Delta}$ and a cube root of such an expression. In fact, Cardano's formula reads as follows: define

$$Z = \sqrt[3]{-\frac{27q}{2} + \frac{3}{2}\sqrt{-3\Delta}};$$
$$Z' = \sqrt[3]{-\frac{27q}{2} - \frac{3}{2}\sqrt{-3\Delta}}.$$

Note that $(\omega - \omega^2)^2 = -3$, so $\sqrt{-3} \in F$. Also, to avoid the ambiguity in having to choose square and cube roots for both Z and Z', we have

$$(ZZ')^3 = \frac{1}{4}((27q)^2 + 27\Delta) = \frac{27}{4}(27q^2 - 4p^3 - 27q^2) = -27p^3,$$

and hence we can take $Z' = -3p/Z$ as long as $Z \neq 0$. (If $Z = 0$, then $p = 0$ and $f = x^3 + q$ trivially has roots $-\sqrt[3]{q}$, $-\omega\sqrt[3]{q}$, $-\omega^2\sqrt[3]{q}$.)

Cardano's formula: For an appropriate choice of sign of the square and cube roots in the formula for Z, the roots of f are

$$\frac{Z + Z'}{3}; \qquad \frac{\omega^2 Z + \omega Z'}{3}; \qquad \frac{\omega Z + \omega^2 Z'}{3}.$$

To derive Cardano's formula, we follow the ideas that have been described in Sections 3 and 4. We keep the assumption (which we can always arrange after completing the cube) that $f = x^3 + px + q$, with roots $\alpha_1, \alpha_2, \alpha_3$ satisfying $\alpha_1 + \alpha_2 + \alpha_3 = 0$, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$, and $\alpha_1\alpha_2\alpha_3 = -q$. The discriminant $\Delta = -4p^3 - 27q^2$. As noted above, in general we expect that the splitting field E is a Galois extension of $F(\sqrt{\Delta})$ whose Galois group is cyclic of order 3, generated by, say σ. Thus, we can label the roots $\alpha_1, \alpha_2, \alpha_3$ of f so that σ corresponds to the permutation (123). In this case, if we set

$$Z = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3;$$
$$Z' = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3,$$

then $\sigma(Z) = \omega^2 Z$ and $\sigma(Z') = \omega Z'$, so that Z and Z' are eigenvectors of σ with eigenvalues respectively either $\omega^2 = \omega^{-1}$ or ω. Thus we expect that Z^3 and $(Z')^3$ are fixed by σ and hence, by Galois theory, are elements of $F(\sqrt{\Delta})$. In fact, we will check this directly. Before doing so, note that, as $\alpha_1 + \alpha_2 + \alpha_3 = 0$ and $1 + \omega + \omega^2 = 0$,

$$Z + Z' = 2\alpha_1 - \alpha_2 - \alpha_3 = 3\alpha_1,$$

and hence $\alpha_1 = \frac{1}{3}(Z + Z')$. Similar computations show that

$$\alpha_2 = \frac{1}{3}(\omega^2 Z + \omega Z')$$
$$\alpha_2 = \frac{1}{3}(\omega Z + \omega^2 Z') = -\alpha_1 - \alpha_2.$$

It is also easy to check directly that

$$ZZ' = -3p.$$

To compute $Z^3 = (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3$, it will help to record the trinomial expansion

$$(x + y + z)^3 = x^3 + y^3 + x^3 + 3x^2(y + z) + 3y^2(x + z) + 3z^2(x + y) + 6xyz.$$

Then we expand:

$$\begin{aligned} Z^3 &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 6\alpha_1\alpha_2\alpha_3 \\ &\quad + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1^2\alpha_3 + \alpha_2^2\alpha_1 + \alpha_3^2\alpha_2). \end{aligned}$$

Note that $6\alpha_1\alpha_2\alpha_3 = -6q$. The expression $\alpha_1^3 + \alpha_2^3 + \alpha_3^3$ is also a symmetric expression in $\alpha_1, \alpha_2, \alpha_3$ and hence can be written in terms of the elementary symmetric polynomials $\alpha_1 + \alpha_2 + \alpha_3 = 0$, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$, and $\alpha_1\alpha_2\alpha_3 = -q$. In fact, using the trinomial expansion above,

$$\begin{aligned} 0^2 &= (\alpha_1 + \alpha_2 + \alpha_3)^3 \\ &= \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + 3\alpha_1^2(\alpha_2 + \alpha_3) + 3\alpha_2^2(\alpha_1 + \alpha_3) + 3\alpha_3^2(\alpha_1 + \alpha_2) + 6\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Using

$$\begin{aligned} 0 &= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)(\alpha_1 + \alpha_2 + \alpha_3) \\ &= \alpha_1^2(\alpha_2 + \alpha_3) + \alpha_2^2(\alpha_1 + \alpha_3) + \alpha_3^2(\alpha_1 + \alpha_2) + 3\alpha_1\alpha_2\alpha_3, \end{aligned}$$

we see that

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = -3(-3\alpha_1\alpha_2\alpha_3) - 6\alpha_1\alpha_2\alpha_3 = 9\alpha_1\alpha_2\alpha_3 = -3q.$$

Finally, to deal with the remaining terms, let $A = \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1$ and $B = \alpha_1^2\alpha_3 + \alpha_2^2\alpha_1 + \alpha_3^2\alpha_2$, so that the remaining terms in the expression for Z^3 are $3\omega A$ and $3\omega^2 B$. Then one computes that

$$\begin{aligned} A - B &= (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) = \sqrt{\Delta}; \\ A + B &= -(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) = 3q. \end{aligned}$$

Hence $A = \frac{1}{2}(3q + \sqrt{\Delta})$ and $B = \frac{1}{2}(3q - \sqrt{\Delta})$. Plugging this all in, we see that

$$Z^3 = -3q - 6q + 3\omega A + 3\omega^2 B = -9q + \frac{9}{2}(\omega + \omega^2)q + \frac{3}{2}(\omega - \omega^2)\sqrt{\Delta},$$

which reduces to the given expression for Z above since $\omega + \omega^2 = -1$ and $\omega - \omega^2 = \sqrt{-3}$. The expression for $(Z')^3$ is similar.

Cardano's formula is too complicated to be of practical use, for many reasons. First, there is the ambiguity in the choice of the square and cube roots; notice that, in the end, there will only be three roots of f. (However, using the formula $ZZ' = -3p$ to fix Z' once we have chosen Z, it is easy to see that the six choices corresponding to the two choices of $\sqrt{\Delta}$ and the three choices of cube root defining Z correspond to the six ways of ordering the roots $\alpha_1, \alpha_2, \alpha_3$.) Second, for $f \in \mathbb{Q}[x]$ or $\mathbb{R}[x]$, even if f has only rational or real roots, the terms that appear in Cardano's formula are unavoidably (nonreal) complex numbers. Finally, even if we only want approximations to the roots, it is inefficient to compute the square and cube roots that appear in the formula. Newton's method is a far more efficient method for directly approximating the roots.

14 Degree four

One can also write down a formula for polynomials of degree 4. Here, the basic idea is to look at the subgroup $H = \{1, (12)(34), (13)(24), (14)(23)\}$ of S_4, which is a normal subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. The quotient $S_4/H \cong S_3$. Explicitly, S_4 acts on the 3 element set X of partitions of $\{1, 2, 3, 4\}$ into two subsets, each with two elements. Thus there is an induced homomorphism $S_4 \to S_3$, and H is the kernel of this homomorphism. If F is a field of characteristic zero, $f \in F[x]$ has Galois group S_4, and E is a splitting field for f, then the fixed field E^H is a Galois extension of F with Galois group S_3, hence is the splitting field of an irreducible cubic polynomial $g \in F[x]$ (compare HW 13, problem 3). In fact, one can write down such a cubic explicitly: if

$$\begin{aligned}
\beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4; \\
\beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4; \\
\beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3,
\end{aligned}$$

then $\mathrm{Gal}(E/F)$ permutes the β_i and it follows from Galois theory that $g = (x - \beta_1)(x - \beta_2)(x - \beta_3) \in F[x]$. The polynomial g is called the *resolvent*

cubic of f, and an exercise in symmetric functions shows how to write it explicitly in terms of the coefficients of f. For example, assuming (as we may, by completing the fourth power) that $f = x^4 + px^2 + qx + r$, the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of f satisfy

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 &= 0; \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 &= p; \\ \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 &= -q; \\ \alpha_1\alpha_2\alpha_3\alpha_4 &= r, \end{aligned}$$

the resolvent cubic is then given by

$$g = x^3 - px^2 - 4rx + (-q^2 + 4pr).$$

One computes for example that

$$\beta_1 - \beta_2 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3),$$

and similarly for the other differences. Hence

$$\Delta(g) = [(\beta_1 - \beta_2)(\beta_1 - \beta_2)(\beta_1 - \beta_2)]^2 = \left(\prod_{i<j}(\alpha_i - \alpha_j)\right)^2 = \Delta(f).$$

Thus the degree 4 polynomial f and its resolvent cubic g have the same discriminant. Finally, the roots β_i of g are all fixed by H, and so the splitting field for g is contained in E^H.

It is then possible to describe the Galois group of f, i.e. $\mathrm{Gal}(E/F)$, in terms of the discriminant and the resolvent cubic. Assuming that f is irreducible, the image G of $\mathrm{Gal}(E/F)$ in S_4 is a transitive subgroup of S_4 (i.e. it acts transitively on $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, and it is well-defined up to conjugation, which corresponds to choosing a numbering of the roots. Up to conjugation, there are only four transitive subgroups of S_4: S_4, A_4, D_4, $H = \{1, (12)(34), (13)(24), (14)(23)\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and $C = \langle(1234)\rangle \cong \mathbb{Z}/4\mathbb{Z}$. The following almost completely describes which cases arise:

Proposition 14.1. *Let $f \in F[x]$ be an irreducible quartic polynomial with resolvent cubic g and discriminant Δ, and let G be the image in S_4 of* $\mathrm{Gal}(E/F)$.

(i) *If Δ is not a square in F and g is irreducible in $F[x]$, then $G = S_4$.*

(ii) *If Δ is a square in F and g is irreducible in $F[x]$, then $G = A_4$.*

(iii) *If Δ is not a square in F and g is reducible in $F[x]$, then G is conjugate either to D_4 or to C.*

(iv) *If Δ is a square in F and g is reducible in $F[x]$, then $G = H$.* □

Example 14.2. We give some examples of the various possibilities for $f \in \mathbb{Q}[x]$. If $f = x^4 + px^2 + r$, so that $q = 0$, then

$$g = x^3 - px^2 - 4rx + 4pr = (x^2 - 4r)(x - p)$$

is reducible, with p a root (and also $\pm 2\sqrt{r}$ if r is a square). Then

$$\Delta(f) = \Delta(g) = [(p + 2\sqrt{r})(p - 2\sqrt{r})(4\sqrt{r})]^2 = 16(p^2 - 4r)^2 r,$$

and hence $\Delta(f)$ is a square $\iff$ r is a square, in which case we are in case (iv) of the proposition. For example, this is the case for the irreducible polynomial $x^4 - 10x^2 + 1$, whose splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Another example is $x^4 + 1 = \Phi_8$; here $x^4 + 1$ is irreducible by Problem 1(g) of HW 10, and thus the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. On the other hand, for $x^4 - 2$, $\Delta(f)$ is not a square, and, as we have seen, the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ is isomorphic to D_4.

To find an example with Galois group S_4, let $f = x^4 + x + 1$. Then f is irreducible, since its reduction mod 2 is irreducible in $\mathbb{F}_2[x]$. Its resolvent cubic is $g = x^3 - 4x - 1$, which is irreducible by the rational roots test. Finally, the discriminant of f is the discriminant of g, namely $-4(-4)^3 - 27(1^2) = 256 - 27 = 229$, which is not a square in $\mathbb{Q}$. Hence $\mathrm{Gal}(E/\mathbb{Q}) \cong S_4$.

Now assume that F contains the cube roots of unity (i.e. ω). It turns out that we do not need to assume that F contains the fourth roots of unity (i.e. an element i such that $i^2 = -1$). The strategy for solving a degree four equation by radicals is then the following: given f, which we can assume to be of the form $x^4 + px^2 + qx + r$, we first compute the resolvent cubic g and then use Cardano's formula (possibly after further completing the cube in g) to find the three roots $\beta_1, \beta_2, \beta_3$ of g, expressed in terms of radicals. Finally we must solve for the roots α_i in terms of the β_j. Again, Galois theory suggest how to do this: We expect in general that the Galois group $\mathrm{Gal}(E/F(\beta_1, \beta_2, \beta_3)) = H = \{1, (12)(34), (13)(24), (14)(23)\}$. Let $\sigma_1 = (12)(34)$, $\sigma_2 = (13)(24)$, $\sigma_3 = (14)(23)$. Then we are looking for elements $\gamma_i \in E$ which are eigenvectors of the σ_i with eigenvalues ± 1. For example, using the fact that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, let

$$\gamma_1 = \alpha_1 + \alpha_2 = -(\alpha_3 + \alpha_4).$$

Then $\sigma_1(\gamma_1) = \gamma_1$, $\sigma_2(\gamma_1) = \alpha_3 + \alpha_4 = -\gamma_1$, and hence $\sigma_3(\gamma_1) = -\gamma_1$. Thus γ_1^2 is fixed by H, and so we expect that $\gamma_1^2 \in F(\beta_1, \beta_2, \beta_3)$. Explicitly,

$$2\gamma_1^2 = (\alpha_1 + \alpha_2)^2 + (-(\alpha_3 + \alpha_4))^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + 2\alpha_1\alpha_2 + 2\alpha_3\alpha_4.$$

Thus, again using $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ and hence

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^2 - 2\sum_{i<j} \alpha_i\alpha_j = -2p,$$

we see that

$$2\gamma_1^2 = -2p + 2\beta_1$$

and hence $\gamma_1 = \sqrt{\beta_1 - p}$ (for an appropriate choice of sign). There are similar results for $\gamma_2 = \alpha_1 + \alpha_3 = \sqrt{\beta_2 - p}$ and $\gamma_3 = \alpha_1 + \alpha_4 = \sqrt{\beta_3 - p}$. Now

$$\gamma_1 + \gamma_2 + \gamma_3 = 3\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 2\alpha_1,$$

using again $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. Hence

$$\alpha_1 = \frac{1}{2}(\sqrt{\beta_1 - p} + \sqrt{\beta_2 - p} + \sqrt{\beta_3 - p}).$$

Similarly

$$\begin{aligned}
\gamma_1 - \gamma_2 - \gamma_3 &= \alpha_2 - \alpha_1 - \alpha_3 - \alpha_4 = 2\alpha_2; \\
-\gamma_1 + \gamma_2 - \gamma_3 &= \alpha_3 - \alpha_1 - \alpha_2 - \alpha_4 = 2\alpha_3; \\
-\gamma_1 - \gamma_2 + \gamma_3 &= \alpha_4 - \alpha_1 - \alpha_2 - \alpha_3 = 2\alpha_4.
\end{aligned}$$

Thus we can express all of the α_i in terms of the radicals $\sqrt{\beta_j - p}$. Note that, since the Galois group $\mathrm{Gal}(E/F(\beta_1, \beta_2, \beta_3))$ is in general isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, we expect that E is obtained from $F(\beta_1, \beta_2, \beta_3)$ by adding just two square roots, and hence the three square roots $\gamma_i = \sqrt{\beta_i - p}$ should be related. In fact,

$$\gamma_1^2\gamma_2^2\gamma_3^2 = (\beta_1 - p)(\beta_2 - p)(\beta_3 - p) = -g(p),$$

where g is the resolvent cubic. Using our computation of g, we see that

$$\gamma_1^2\gamma_2^2\gamma_3^2 = -(p^3 - pp^2 - 4rp - q^2 + 4rp) = q^2,$$

and hence (depending on the choice of signs) $\gamma_1\gamma_2\gamma_3 = \pm q$. With our choice of the γ_i, we see that in fact

$$\begin{aligned}
\gamma_1\gamma_2\gamma_3 &= (\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4) \\
&= \alpha_1^3 + \alpha_1^2(\alpha_2 + \alpha_3 + \alpha_4) + \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 \\
&= \alpha_1^2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) - q = -q.
\end{aligned}$$

15 Insolvability of the quintic

Regarding the situation for polynomials of degree $n \geq 5$, we have the following:

Theorem 15.1. *Suppose that $n \geq 5$. Let $f \in F[x]$ be a polynomial of degree n whose Galois group is S_n. Then no root of f is expressible by radicals.*

The proof of the theorem involves some non-trivial group theory as well as Galois theory. We begin by outlining the group theory we shall need. Recall that a group $G \neq \{1\}$ is *simple* if the only normal subgroups of G are either $\{1\}$ or G, i.e. G has no non-trivial normal subgroups. We then have:

Theorem 15.2. *For $n \geq 5$, the alternating group A_n is simple.* □

Actually, we shall use the following, which is an easy consequence:

Corollary 15.3. *For $n \geq 5$, if H is a normal subgroup of S_n, then $H = S_n$, A_n, or $\{1\}$.* □

The other notion we shall need is that of a *solvable group* (the terminology is motivated by the problem of solvability by radicals):

Definition 15.4. Let G be a group. Then G is *solvable* if there exist a sequence of subgroups

$$H_0 = \{1\} \leq H_1 \leq \cdots \leq H_N = G$$

such that $H_i \lhd H_{i+1}$ for every i, and such that the quotient group H_{i+1}/H_i is abelian.

For example, S_4 is solvable, as one sees by looking at the sequence of subgroups (here as usual $H = \{1, (12)(34), (13)(24), (14)(23)\}$)

$$\{1\} \leq H \leq A_4 \leq S_4.$$

Here $A_4/H \cong \mathbb{Z}/3\mathbb{Z}$ and $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$, but in fact $H \lhd S_4$ and $S_4/H \cong S_3$. The sequence above then arises from looking at the surjective homomorphism $\pi\colon S_4 \to S_3$ and the sequence $\{1\} \leq A_3 \leq S_3$: in fact, the subgroup A_4 of S_4 is $\pi^{-1}(A_3)$. Our analysis of degree 4 polynomials above used the sequence $H \leq S_4$, but the analysis of the roots of the resolvent cubic involved looking at the quotient group $S_4/H \cong S_3$.

It is easy to see that S_n is not solvable for $n \geq 5$ and that, if $\varphi\colon G \to G'$ is a surjective homomorphism of groups from G to G' and G is solvable, then G' is also solvable. Let us prove the only part of the above statements that we need:

Proposition 15.5. *Let G be a solvable group. If $n \geq 5$, then there does not exist a surjective homomorphism from G to S_n.*

Proof. Suppose instead that G is solvable, that $H_0 = \{1\} \leq H_1 \leq \cdots \leq H_N = G$ is a sequence of subgroups as in the definition, and that $\varphi\colon G \to S_n$ is a surjective homomorphism of groups; we shall derive a contradiction. Here we use the straightforward fact that, if $\varphi\colon G \to G'$ is a **surjective** homomorphism of groups and $H \lhd G$, then $\varphi(H) \lhd G'$. Now by assumption $\varphi\colon G \to S_n$ is surjective and $H_{N-1} \lhd G = H_N$, so $\varphi(H_{N-1}) \lhd S_n$. Thus $\varphi(H_{N-1}) = S_n, A_n, \{1\}$. Also, the case $\varphi(H_{N-1}) = \{1\}$ is impossible, because then there would be an induced surjection, also denoted φ, from H_N/H_{N-1} to $S_n/\{1\} \cong S_n$. But H_N/H_{N-1} is abelian by assumption, whereas S_n is not abelian for $n \geq 5$ (in fact $n \geq 3$), hence $\varphi(H_{N-1}) \neq \{1\}$.

A similar argument shows that, if $\varphi(H_{i+1}) = S_n$, then $\varphi(H_i) = S_n$ or A_n. Likewise, if $\varphi(H_{i+1}) = A_n$, then $\varphi(H_i) = A_n$, since A_n is simple, hence as $\varphi(H_i) \lhd A_n$, $\varphi(H_i) = \{1\}$ or A_n. But $\varphi(H_i) = \{1\}$ is impossible since then there would be a surjective homomorphism from H_{i+1}/H_i to $A_n/\{1\}$. Since H_{i+1}/H_i is abelian, $A_n/\{1\}$ would be abelian as well, a contradiction since A_n is not abelian for $n \geq 4$.

So finally by downward induction on i, $\varphi(H_0)$ is either S_n or A_n. But since $H_0 = \{1\}$, this is clearly impossible. □

Now we turn to the Galois theory side of the proof of Theorem 15.1. The main point will be to show the following theorem:

Theorem 15.6. *Let $f \in F[x]$ be irreducible, and suppose that f has a root expressible by radicals. Then there exists a sequence of fields $L_0 = F \leq L_1 \leq \cdots \leq L_k = E$ such that*

(i) *For all i, L_i is a Galois extension of F.*

(ii) *There exist $\beta_{i1}, \ldots, \beta_{i,a_i} \in L_{i+1}$ and positive integers n_i such that, for all i, j, $\beta_{ij}^{n_i} \in L_i$ and $L_{i+1} = L_i(\beta_{i1}, \ldots, \beta_{i,a_i})$.*

(iii) *The Galois group $\mathrm{Gal}(L_{i+1}/L_i)$ is abelian.*

(iv) *There exists a subfield K of $E = L_k$ which is a splitting field of f, and hence every root of f is expressible by radicals.*

Before we launch into the technical details of the proof of Theorem 15.6, we show how to use it toward the insolvability of the quintic:

Corollary 15.7. *Suupose that $f \in F[x]$ is irreducible and has a root expressible by radicals. Let K be a splitting field of f. Then there exists a solvable group G and a surjective group homomorphism from G to $\mathrm{Gal}(K/F)$. In particular, if $\mathrm{Gal}(K/F) \cong S_n$, $n \geq 5$, then this is impossible.*

Proof. Let $E = L_k$ and K be as constructed in Theorem 15.6. Given the increasing sequence of field extensions

$$L_0 = F \leq L_1 \leq \cdots \leq L_k = E,$$

there is a corresponding decreasing sequence of subgroups

$$\mathrm{Gal}(E/L_k) = \{\mathrm{Id}\} \leq \mathrm{Gal}(E/L_{k-1}) \leq \cdots \leq \mathrm{Gal}(E/L_0) = \mathrm{Gal}(E/F).$$

Let $H_i = \mathrm{Gal}(E/L_{k-i})$, so that $H_0 = \{\mathrm{Id}\}$, $H_k = \mathrm{Gal}(E/F)$, and there is a sequence

$$H_0 = \{\mathrm{Id}\} \leq H_1 \leq \cdots \leq H_k = \mathrm{Gal}(E/F).$$

By the Main Theorem of Galois theory, $H_i = \mathrm{Gal}(E/L_{k-i}) \lhd \mathrm{Gal}(E/L_{k-i-1}) = H_{i+1}$ since L_{k-i} is a normal extension of F and hence of L_{k-i-1}, and

$$H_{i+1}/H_i = \mathrm{Gal}(E/L_{k-i-1}) \Big/ \mathrm{Gal}(E/L_{k-i}) \cong \mathrm{Gal}(L_{k-i}/L_{k-i-1}),$$

which is abelian. Thus E is solvable. Moreover, again by the Main Theorem, there is a surjection from the solvable group $G = \mathrm{Gal}(E/F)$ to $\mathrm{Gal}(K/F)$. Finally, no such surjection can exist if $\mathrm{Gal}(K/F) \cong S_n$ with $n \geq 5$, by Proposition 15.5. □

Proof of Theorem 15.6. To find the sequence of field extensions L_i, we start with the sequence of extensions given in the definition of being expressible by radicals: the root α is expressible by radicals if there exist a sequence of extension fields

$$F = E_1 \leq E_2 = E_1(\alpha_1) \leq E_3 = E_2(\alpha_2) \leq \cdots \leq E_k = E_{k-1}(\alpha_{k-1})$$

and positive integers $n_i, 1 \leq i \leq k$, such that $\alpha_i^{n_i} = a_i \in E_{i-1}$ for every i, and such that $\alpha \in E_k$. If in addition F contains the n_i^{th} roots of unity for every i, it follows from Proposition 11.6 that E_{i+1} is a normal extension of E_i and that $\mathrm{Gal}(E_{i+1}/E_i)$ is abelian. Unfortunately, the extension E_k need not be a Galois extension of F, so we must modify the construction somewhat.

Let $L_0 = F$, and let $L_1 = F(\mu_n)$ where n is the least common multiple of $n_1, \ldots, n_k$, or any positive integer which is divisible by all of the n_i.

This will insure that we always have as many roots of unity as we need. Note that $\mathrm{Gal}(L_1/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and hence is abelian. At the next stage, let $L_2 = L_1(\sqrt[n_1]{a_1})$, where $a_1 \in F$. Then L_2 is Galois over F since it is a splitting field for $(x^n - 1)(x^{n_1} - a_1)$, hence L_2 is Galois over F, and $\mathrm{Gal}(L_2/L_1)$ is isomorphic to a subgroup of $\mathbb{Z}/n_1\mathbb{Z}$ and hence is abelian. Finally, using the Isomorphism Extension Theorem for the simple extension $E_2 = E_1(\alpha_1)$, the root $\sqrt[n_1]{a_1}$ of $x^{n_1} - a_1 \in F[x]$ defines a homomorphism $\varphi_1 \colon E_2 \to L_2$ which is the identity on the subfield F and satisfies: $\varphi_1(\alpha_1) = \sqrt[n_1]{a_1}$.

Now inductively suppose we have found a sequence

$$L_0 = F \leq L_1 \leq \cdots \leq L_i,$$

with the property that L_i is Galois over $L_0 = F$, $\mathrm{Gal}(L_j/L_{j-1})$ is abelian for $1 \leq j \leq i$, and there exists a homomorphism $\varphi_i \colon E_i \to L_i$. Using φ_i to identify E_i with a subfield of L_i, we have the element $a_i \in E_i$, and E_i is obtained by taking an n_i^{th} root of a_i. Now $x^{n_i} - a_i$ only has coefficients in $L_i[x]$, not in $F[x]$, so that a splitting field of $x^{n_i} - a_i$ over L_i need not be Galois over F. To fix this, consider

$$f_i = \prod_{\sigma \in \mathrm{Gal}(L_i/F)} (x^{n_i} - \sigma(a_i)).$$

For all $\tau \in \mathrm{Gal}(L_i/F)$,

$$\tau(f_i) = \prod_{\sigma \in \mathrm{Gal}(L_i/F)} (x^{n_i} - \tau\sigma(a_i)) = \prod_{\sigma \in \mathrm{Gal}(L_i/F)} (x^{n_i} - \sigma(a_i)),$$

since multiplying all of the σ in $\mathrm{Gal}(L_i/F)$ is a permutation of $\mathrm{Gal}(L_i/F)$. Hence all of the coefficients of f_i are fixed by $\mathrm{Gal}(L_i/F)$, i.e. $f_i \in F[x]$. Let L_{i+1} be a splitting field for f_i over L_i. It is clear that L_{i+1} is obtained from L_i by adding n_i^{th} roots of $\sigma(a_i)$ for all of the $\sigma \in \mathrm{Gal}(L_i/F)$. Hence, since F and therefore L_i contain all of the n_i^{th} roots of unity, L_{i+1} is a Galois extension of L_i with abelian Galois group, by (ii) of Remark 11.7. It is easy to see that L_{i+1} is a normal, hence Galois extension of F: by assumption, L_i is a normal extension of F, hence a splitting field for some polynomial $g_i \in F[x]$. Then L_{i+1} is generated by L_i and the roots of f_i, hence L_{i+1} is a splitting field for $g_{i+1} = g_i f_i$ and is thus a normal extension of F. Given the homomorphism φ_i of E_i and a root of $x^{n_i} - a_i$ in L_{i+1}, we use the Isomorphism Extension Theorem (the easy case for a simple extension) to find an extension of φ_i to a homomorphism $\varphi \colon E_{i+1} = E_i(\alpha_i) \to L_{i+1}$. This completes the inductive step of the construction.

Finally, we reach L_k, which contains an isomorphic copy of E_k and hence a root of f, which we continue to denote by α. Since $E = L_k$ is a normal extension of F, E contains a root of f and f is irreducible in $F[x]$, the polynomial f splits into a product of linear factors in $E[x]$. Hence E contains a splitting field K of f. $\square$

Let us actually exhibit an explicit polynomial of degree 5 whose Galois group is S_5, and hence for which the roots cannot be expressed as radicals.

Example 15.8. Let $f = x^5 - 16x + 2 \in \mathbb{Q}[x]$. It is irreducible over $\mathbb{Q}$ by the Eisenstein criterion (with $p = 2$). The Galois group G of f is thus isomorphic to a subgroup of S_5, and 5 divides the order of G. Hence by the Sylow theorem G has a subgroup of order 5, and hence an element of order 5. Since the only elements of S_5 of order 5 are 5-cycles, G contains a 5-cycle. Next we claim that G also contains a 2-cycle. In fact, we claim that f has three real and hence two non-real roots, and thus that complex conjugation is an automorphism of the splitting field of f in $\mathbb{C}$ which fixes the three real roots and exchanges the two non-real roots. To see that f has exactly three real roots, note that $f' = 5x^4 - 16$, so there are two critical points $\pm\sqrt[4]{16/5}$. By checking the sign of f', f is increasing for $x < -\sqrt[4]{16/5}$, decreasing for $-\sqrt[4]{16/5} < x < \sqrt[4]{16/5}$, and increasing for $x > \sqrt[4]{16/5}$. Writing

$$f = x(x^4 - 16) + 2$$

and using $\sqrt[4]{16/5} > 1$, it is easy to see that $f(-\sqrt[4]{16/5}) > 0$ and $f(\sqrt[4]{16/5}) < 0$. The Intermediate Value Theorem then implies that f has exactly three real roots. The Galois group G of f thus contains a 5-cycle σ and a 2-cycle τ, i.e. a transposition. A straightforward exercise (this was a HW problem in Modern Algebra I) then shows that $G = S_5$. More explicitly, label the two nonreal roots as α_1 and α_2. Then τ corresponds to the transposition $(1, 2)$. After labeling the remaining roots, σ is a 5-cycle which we can start at 1: $\sigma = (1, a_1, a_2, a_3, a_4)$. If $2 = a_k$, $1 \leq k \leq 4$, then σ^k is still a 5-cycle and $\sigma^k = (1, 2, b_1, b_2, b_3)$. After relabeling the three real roots we can assume that $\sigma^k = (1, 2, 3, 4, 5)$. Thus G contains $(1, 2)$ and $(1, 2, 3, 4, 5)$. But a subgroup G of S_5 containing $(1, 2)$ and $(1, 2, 3, 4, 5)$ is all of S_5: it is easy to check that G then contains $(1, a)$, $2 \leq a \leq 5$, and then every transposition (i, j). Since S_5 is generated by transpositions, we see that $G = S_5$ as claimed.