[14.1] Show that $\mathbb{Q}(\sqrt{2})$ is normal over $\mathbb{Q}$.

We must show that all imbeddings $\sigma : \mathbb{Q}(\sqrt{2}) \to \overline{\mathbb{Q}}$ to an algebraic closure of $\mathbb{Q}$ have the same image. Since (by Eisenstein and Gauss) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, it is the minimal polynomial for any square root of 2 in any field extension of $\mathbb{Q}$. We know that (non-zero) field maps $\mathbb{Q}(\alpha) \to \overline{\mathbb{Q}}$ over $\mathbb{Q}$ can only send roots of an irreducible $f(x) \in \mathbb{Q}[x]$ to roots of the same irreducible in $\overline{\mathbb{Q}}$. Let β be a square root of 2 in $\overline{\mathbb{Q}}$. Then $-\beta$ is another, and is the *only* other square root of 2, since the irreducible is of degree 2. Thus, $\sigma(\sqrt{2}) = \pm\beta$. Whichever sign occurs, the image of the whole $\mathbb{Q}(\sqrt{2})$ is the same. ///

[14.2] Show that $\mathbb{Q}(\sqrt[3]{5})$ is not normal over $\mathbb{Q}$.

By Eisenstein and Gauss, $x^3 - 5$ is irreducible in $\mathbb{Q}[x]$, so $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$. Let α be one cube root of 5 in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Also, observe that $x^3 - 5$ has no repeated factors, since its derivative is $3x^2$, and the *gcd* is readily computed to be 1. Let β be *another* cube root of 5. Then $(\alpha/beta)^3 = 1$ and $\alpha/beta \neq 1$, so that ratio is a primitive cube root of unity ω, whose minimal polynomial over $\mathbb{Q}$ we know to be $x^2 + x + 1$ (which is indeed irreducible, by Eisenstein and Gauss). Thus, the cubic field extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ cannot contain β, since otherwise it would have a quadratic subfield $\mathbb{Q}(\omega)$, contradicting the multiplicativity of degrees in towers.

Since

$$\mathbb{Q}(\alpha) \approx \mathbb{Q}[x]/\langle x^3 - 5\rangle \approx \mathbb{Q}(\beta)$$

we can map a copy of $\mathbb{Q}(\sqrt[3]{5})$ to either $\mathbb{Q}(\alpha)$ or $\mathbb{Q}(\beta)$, sending $\sqrt[3]{5}$ to either α or β. But inside $\overline{\mathbb{Q}}$ the two fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are distinct sets. That is, $\mathbb{Q}(\sqrt[3]{5})$ is not normal. ///

[14.3] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{13})$ where ζ_{13} is a primitive 13^{th} root of unity.

We already know that the Galois group G of the extension is isomorphic to $(\mathbb{Z}/13)^\times$ by

$$a \to (\sigma_a : \zeta \to \zeta^a)$$

and that group is cyclic. Thus, the subgroups are in bijection with the divisors of the order, 12, namely 1,2,3,4,6,12. By the main theorem of Galois theory, the intermediate fields are in bijection with the *proper* subgroups, which will be the fixed fields of the subgroups of orders $2, 3, 4, 6$. We have already identified the quadratic-over-$\mathbb{Q}$ subfield of any cyclotomic field $\mathbb{Q}(\zeta_p)$ with a primitive p^{th} root of unity ζ_p with p *prime*, via Gauss sums, as $\mathbb{Q}(\sqrt{\pm p})$ with the sign being the quadratic symbol $(-1/p)_2$. Thus, here, the subgroup fixed by the subgroup of order 6 is quadratic over $\mathbb{Q}$, and is $\mathbb{Q}(\sqrt{13})$.

We claim that the subfield fixed by $\zeta \to \zeta^{\pm 1}$ is $\mathbb{Q}(\xi)$, where $\xi = \zeta + \zeta^{-1}$ is obtained by averaging ζ over that group of automorphisms. First, ξ is not 0, since those two powers of ζ are linearly independent over $\mathbb{Q}$. Second, to show that ξ is not accidentally invariant under any *larger* group of automorphisms, observe that

$$\sigma_a(\xi) = \zeta^a + \zeta^{-a} = \zeta^a + \zeta^{13-a}$$

Since $\zeta^1, \zeta^2, \ldots, \zeta^{11}, \zeta^{12}$ are a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta)$, an equality $\sigma_a(\xi) = \xi$ is

$$\zeta^a + \zeta^{13-a} = \sigma_a(\xi) = \xi = \zeta + \zeta^{12}$$

which by the linear independence implies $a = \pm 1$. This proves that this ξ generates the sextic-over-$\mathbb{Q}$ subextension.

To give a second description of ξ by telling the irreducible in $\mathbb{Q}[x]$ of which it is a zero, divide through the equation satisfied by ζ by ζ^6 to obtain

$$\zeta^6 + \zeta^5 + \ldots + \zeta + 1 + \zeta^{-1} + \ldots + \zeta^{-6} = 0$$

Thus,

$$\xi^6 + \xi^5 + (1 - \binom{6}{1})\xi^4 + (1 - \binom{5}{1})\xi^3 + (1 - \binom{6}{2} + 5 \cdot \binom{4}{1})\xi^2$$
$$+ (1 - \binom{5}{2} + 4 \cdot \binom{3}{1})\xi + (1 - \binom{6}{3} + 5 \cdot \binom{4}{2} - 6\binom{2}{1})$$
$$= \xi^6 + \xi^5 - 5\xi^4 - 4\xi^3 + 6\xi^2 + 3\xi - 1 = 0$$

To describe ξ as a root of this sextic is an alternative to describing it as $\xi = \zeta + \zeta^{-1}$. Since we already know that ξ is of degree 6 over $\mathbb{Q}$, this sextic is necessarily irreducible.

The quartic-over-$\mathbb{Q}$ intermediate field is fixed by the (unique) order 3 subgroup $\{1, \sigma_3, \sigma_9\}$ of automorphisms. Thus, we form the average

$$\alpha = \zeta + \zeta^3 + \zeta^9$$

and claim that α generates that quartic extension. Indeed, if σ_a were to fix α, then

$$\zeta^2 + \zeta^{3a} + \zeta^{9a} = \sigma_a(\alpha) = \alpha = \zeta + \zeta^3 + \zeta^9$$

By the linear independence of $\zeta^2, \zeta^2, \ldots, \zeta^{12}$, this is possible only for a among $1, 3, 9$ modulo 13. This verifies that this α exactly generates the quartic extension.

To determine the quartic irreducible of which α is a root, we may be a little clever. Namely, we first find the irreducible *quadratic* over $\mathbb{Q}(\sqrt{13})$ of which α is a root. From Galois theory, the non-trivial automorphism of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}(\sqrt{13})$ is (the restriction of) σ_4, since 4 is of order 6 in $(\mathbb{Z}/13)^\times$. Thus, the irreducible of α over $\mathbb{Q}(\sqrt{13})$ is

$$(x - \alpha)(x - \sigma_4\alpha)$$

in

$$\alpha + \sigma_4\alpha = \zeta + \zeta^3 + \zeta^9 + \zeta^4 + \zeta^{12} + \zeta^{10} \in \mathbb{Q}(\sqrt{13})$$

the exponents appearing are exactly the non-zero squares modulo 13, so

$$\alpha + \sigma_4\alpha = \sum_{\ell:\, \left(\frac{\ell}{13}\right)_2 = 1} \zeta^\ell = \frac{1}{2} \cdot \left(\sum_{1 \le \ell \le 12} \left(\frac{\ell}{13}\right)_2 \zeta^\ell + \sum_{1 \le \ell \le 12} \zeta^\ell \right) = \frac{\sqrt{13} - 1}{2}$$

from discussion of Gauss sums. And

$$\alpha \cdot \sigma_4\alpha = 3 + \zeta^5 + \zeta^{11} + \zeta^7 + \zeta^2 + \zeta^8 + \zeta^6 \in \mathbb{Q}(\sqrt{13})$$

The exponents are exactly the non-squares modulo 13, so this is

$$3 - \frac{1}{2} \cdot \left(\sum_{1 \le \ell \le 12} \left(\frac{\ell}{13}\right)_2 \zeta^\ell - \sum_{1 \le \ell \le 12} \zeta^\ell \right) = 3 - \frac{\sqrt{13} + 1}{2} = \frac{-\sqrt{13} + 5}{2}$$

Thus, the quadratic over $\mathbb{Q}(\sqrt{13})$ is

$$x^2 - \frac{\sqrt{13} - 1}{2} x + \frac{-\sqrt{13} + 5}{2}$$

It is interesting that the discriminant of this quadratic is

$$\sqrt{13} \cdot \frac{3 - \sqrt{13}}{2}$$

and that (taking the *norm*)

$$\frac{3-\sqrt{13}}{2}\cdot\frac{3+\sqrt{13}}{2} = -1$$

To obtain the quartic over $\mathbb{Q}$, multiply this by the same expression with $\sqrt{13}$ replaced by its negative, to obtain

$$\begin{aligned}(x^2+\frac{x}{2}+\frac{5}{2})^2 - 13(\frac{x}{2}+\frac{1}{2})^2 &= x^4+\frac{x^2}{4}+\frac{25}{4}+x^3+5x^2+\frac{5x}{2}-\frac{13x^2}{4}-\frac{13x}{2}-\frac{13}{4}\\ &= x^4+x^3+2x^2-4x+3\end{aligned}$$

Finally, to find the cubic-over-$\mathbb{Q}$ subfield fixed by the subgroup $\{1,\sigma_5,\sigma{-}1,\sigma_8\}$ of the Galois group, first consider the expression

$$\beta = \zeta+\zeta^5+\zeta^{12}+\zeta^8$$

obtained by averaging ζ by the action of this subgroup. This is not zero since those powers of ζ are linearly independent over $\mathbb{Q}$. And if

$$\zeta^a+\zeta^{5a}+\zeta^{12a}+\zeta^{8a} = \sigma_a(\beta) = \beta = \zeta+\zeta^5+\zeta^{12}+\zeta^8$$

the the linear independence implies that a is among $1,5,12,8$ mod 13. Thus, β is not accidentally invariant under a larger group.

Of course we might want a second description of β by telling the irreducible cubic it satisfies. This was done by brute force earlier, but can also be done in other fashions to illustrate other points. For example, we know *a priori* that it *does* satisfy a cubic.

The linear coefficient is easy to determine, as it is the negative of

$$\beta+\sigma_2(\beta)+\sigma_2^2(\beta) = (\zeta+\zeta^5+\zeta^{12}+\zeta^8)+(\zeta^2+\zeta^{10}+\zeta^{11}+\zeta^3)+(\zeta^4+\zeta^7+\zeta^9+\zeta^6) = -1$$

since the powers of ζ are ζ^i with i running from 1 to 12. Thus, the cubic is of the form x^3+x^2+ax+b for some a,b in $\mathbb{Q}$.

We know that $\beta = \zeta+\zeta^5+\zeta^{12}+\zeta^8$ is a zero of this equation, and from

$$\beta^3+\beta^2+a\beta+b = 0$$

we can determine a and b. Expanding β^3 and β^2, we have

$$\begin{gathered}\big(\zeta^3+\zeta^2+\zeta^{10}+\zeta^{11}\\ +3(\zeta^7+\zeta^4+\zeta+\zeta^{12}+\zeta^{10}+\zeta^4+\zeta^9+\zeta^3+\zeta^5+|zeta^8+\zeta^6+\zeta^2)\\ +6(\zeta^5+\zeta+\zeta^8+\zeta^{12}\big)\\ +\big(\zeta^2+\zeta^{10}+\zeta^{11}+\zeta^3+2(\zeta^6+1+\zeta^9+\zeta^4+1+\zeta^7)\big)\\ +a\cdot(\zeta+\zeta^5+\zeta^{12}+\zeta^8)+b = 0\end{gathered}$$

Keeping in mind that

$$\zeta^{12} = -(1+\zeta+\zeta^2+\ldots+\zeta^{10}+\zeta^{11})$$

using the linear independence of $1,\zeta,\zeta^2,\ldots,\zeta^{10},\zeta^{11}$ by looking at the coefficients of 1, ζ, ζ^2, ζ^3, $\ldots$ we obtain relations, respectively,

$$\begin{array}{lcl}-3-6+2\cdot 2-a+b &=& 0\\ 0 &=& 0\\ 1-6+1-a &=& 0\\ 1-6+1-a &=& 0\\ \ldots && \end{array}$$

From this, $a = -4$ and $b = 1$, so

$$x^3 + x^2 - 4x + 1$$

is the cubic of which $\beta = \zeta + \zeta^5 + \zeta^{12} + \zeta^8$ is a zero. ///

[0.0.1] **Remark:** It is surprising that the product of β and its two conjugates is -1.

[14.4] Find all fields intermediate between $\mathbb{Q}$ and a splitting field of $x^3 - x + 1$ over $\mathbb{Q}$.

First, we check the irreducibility in $\mathbb{Q}[x]$. By Gauss this is irreducible in $\mathbb{Q}[x]$ if and only if so in $\mathbb{Z}[x]$. For irreducibility in the latter it suffices to have irreducibility in $(\mathbb{Z}/p)[x]$, for example for $\mathbb{Z}/3$, as suggested by the exponent. Indeed, an earlier example showed that for prime p and $a \neq 0 \bmod p$ the polynomial $x^p - x + a$ is irreducible modulo p. So $x^3 - x + 1$ is irreducible mod 3, so irreducible in $\mathbb{Z}[x]$, so irreducible in $\mathbb{Q}[x]$.

Even though we'll see shortly that in characteristic 0 irreducible polynomials always have distinct zeros, we briefly note why: if $f = g^2h$ over an extension field, then $\deg \gcd(f, f') > 0$, where as usual f' is the derivative of f. If $f' \neq 0$, then the *gcd* has degree at most $\deg f' = \deg f - 1$, and is in $\mathbb{Q}[x]$, contradicting the irreducibility of f. And the derivative can be identically 0 if the characteristic is 0.

Thus, any of the three distinct zeros α, β, γ of $x^3 - x + 1$ generates a cubic extension of $\mathbb{Q}$.

Now things revolve around the discriminant

$$\Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = -27 \cdot 1^3 - 4 \cdot (-1)^3 = -27 + 4 = -23$$

from the computations that show that the discriminant of $x^3 + bx + c$ is $-27c^2 - 4b^3$. From its explicit form, if two (or all) the roots of a cubic are adjoined to the groundfield $\mathbb{Q}$, then the square root of the discriminant also lies in that (splitting) field. Since -23 is *not* a square of a rational number, the field $\mathbb{Q}(\sqrt{-23})$ is a subfield of the splitting field.

Since the splitting field K is normal (and in characteristic 0 inevitably separable), it is Galois over $\mathbb{Q}$. Any automorphism σ of K over $\mathbb{Q}$ must permute the 3 roots among themselves, since

$$\sigma(\alpha)^3 - \sigma(\alpha) + 1 = \sigma(\alpha^3 - \alpha + 1) = \sigma(0) = 0$$

Thus, the Galois group is a *subgroup* of the permutation group S_3 on 3 things. Further, the Galois group is *transitive* in its action on the roots, so cannot be merely of order 1 or 2. That is, the Galois group is either cyclic of order 3 or is the full permutation group S_3. Since the splitting field has a quadratic subfield, via the main theorem of Galois theory we know that the order of the Galois group is *even*, so is the full S_3.

By the main theorem of Galois theory, the intermediate fields are in inclusion-reversing bijection with the proper subgroups of S_3. Since the discriminant is not a square, the 3 subfields obtained by adjoining the different roots of the cubic are distinct (since otherwise the square root of the discriminant would be there), so these must give the subfields corresponding to the 3 subgroups of S_3 of order 2. The field $\mathbb{Q}(\sqrt{-23})$ must correspond to the single remaining subgroup of order 3 containing the 3-cycles. There are no other subgroups of S_3 (by Lagrange and Sylow, or even by direct observation), so there are no other intermediate fields. ///

[14.5] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{21})$ where ζ_{21} is a primitive 21st root of unity.

We have already shown that the Galois group G is isomorphic to

$$(\mathbb{Z}/21)^\times \approx (\mathbb{Z}/7)^\times \times (\mathbb{Z}/3)^\times \approx \mathbb{Z}/6 \oplus \mathbb{Z}/2 \approx \mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

(isomorphisms via Sun-Ze's theorem), using the fact that $(\mathbb{Z}/p)^\times$ for p prime is *cyclic*.

Invoking the main theorem of Galois theory, to determine all intermediate fields (as fixed fields of subgroups) we should determine all subgroups of $\mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$. To understand the collection of all subgroups, proceed as follows. First, a subgroup H either contains an element of order 3 or not, so H either contains that copy of $\mathbb{Z}/3$ or not. Second, $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ is a two-dimensional vector space over $\mathbb{F}_2$, so its proper subgroups correspond to one-dimensional subspaces, which correspond to non-zero vectors (since the scalars are just $\{0,1\}$), of which there are exactly 3. Thus, combining these cases the complete list of *proper* subgroups of G is

$$\begin{array}{rcc} H_1 &=& \mathbb{Z}/3 \oplus 0 \oplus 0 \\ H_2 &=& \mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus 0 \\ H_3 &=& \mathbb{Z}/3 \oplus 0 \oplus \mathbb{Z}/2 \\ H_4 &=& \mathbb{Z}/3 \oplus \mathbb{Z}/2 \cdot (1,1) \\ H_5 &=& \mathbb{Z}/3 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \\ H_6 &=& 0 \oplus \mathbb{Z}/2 \oplus 0 \\ H_7 &=& 0 \oplus 0 \oplus \mathbb{Z}/2 \\ H_8 &=& 0 \oplus \mathbb{Z}/2 \cdot (1,1) \\ H_9 &=& 0 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \end{array}$$

At worst by trial and error, the cyclic subgroup of order 3 in $(\mathbb{Z}/21)^\times$ is $\{1,4,16\}$, and the $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ subgroup is $\{1,8,13,-1\}$.

An auxiliary point which is useful and makes things conceptually clearer is to verify that in $\mathbb{Q}(\zeta_n)$, where $n = p_1 \dots p_t$ is a product of *distinct* primes p_i, and ζ_n is a primitive n^{th} root of unity, the powers

$$\{\zeta^t : 1 \le t < n, \ \text{ with } \ \gcd(t,n) = 1\}$$

is (as you might be hoping[1]) a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta_n)$.

Prove this by induction. Let ζ_m be a primitive m^{th} root of unity for any m. The assertion holds for n prime, since for p prime

$$\frac{x^p - 1}{x - 1}$$

is the minimal polynomial for a primitive p^{th} root of unity. Suppose the assertion is true for n, and let p be a prime not dividing n. By now we know that the np^{th} cyclotomic polynomial is irreducible over $\mathbb{Q}$, so the degree of $\mathbb{Q}(\zeta_{np})$ over $\mathbb{Q}$ is (with Euler's totient function φ)

$$[\mathbb{Q}(\zeta_{np})\mathbb{Q}] = \varphi(np) = \varphi(n) \cdot \varphi(p) = [\mathbb{Q}(\zeta_n)\mathbb{Q}] \cdot [\mathbb{Q}(\zeta_p)\mathbb{Q}]$$

since p and n are relatively prime. Let a, b be integers such that $1 = an + bp$. Also note that $\zeta = \zeta_n \cdot \zeta_p$ is a primitive np^{th} root of unity. Thus, in the explicit form of Sun-Ze's theorem, given i mod p and j mod n we have

$$an \cdot i + bp \cdot j = \begin{cases} i & \bmod p \\ j \bmod n & \end{cases}$$

Suppose that there were a linear dependence relation

$$0 = \sum_i c_\ell \, \zeta_{np}^\ell$$

with $c_i \in \mathbb{Q}$ and with ℓ summed over $1 \le \ell < np$ with $\gcd(\ell, np) = 1$. Let $i = \ell \bmod p$ and $j = \ell \bmod n$. Then

$$\zeta_{np}^{ani+bpj} = \zeta_n^j \cdot \zeta_p^i$$

and

$$0 = \sum_{i=1}^{p} \zeta_p^i \left(\sum_j c_{ani+bpj} \, \zeta_n^j \right)$$

[1] For $n = 4$ and $n = 9$ the assertion is definitely false, for example.

where j is summed over $1 \le j < n$ with $\gcd(j, n) = 1$. Such a relation would imply that $\zeta_p, \ldots, \zeta_p^{p-1}$ would be linearly dependent over $\mathbb{Q}(\zeta_n)$. But the minimal polynomial of ζ_p over this larger field is the same as it is over $\mathbb{Q}$ (because the degree of $\mathbb{Q}(\zeta_n, \zeta_p)$ over $\mathbb{Q}(\zeta_n)$ is still $p - 1$), so this implies that all the coefficients are 0. ///

[14.6] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{27})$ where ζ_{27} is a primitive 27^{th} root of unity.

We know that the Galois group G is isomorphic to $(\mathbb{Z}/27)^\times$, which we also know is *cyclic*, of order $(3-1)3^{3-1} = 18$, since 27 is a power of an odd prime (namely, 3). The subgroups of a cyclic group are in bijection with the divisors of the order, so we have subgroups precisely of orders $1, 2, 3, 6, 9, 18$. The proper ones have orders $2, 3, 6, 9$. We can verify that $g = 2$ is a generator for the cyclic group $(\mathbb{Z}/27)^\times$, and the subgroups of a cyclic group are readily expressed in terms of powers of this generator. Thus, letting $\zeta = \zeta_{27}$, indexing the alphas by the order of the subgroup fixing them,

$$\begin{aligned}
\alpha_2 &= \zeta + \zeta^{-1} \\
\alpha_3 &= \zeta + \zeta^{2^6} + \zeta^{2^{12}} \\
\alpha_6 &= \zeta + \zeta^{2^3} + \zeta^{2^6} + \zeta^{2^9} + \zeta^{2^{12}} + \zeta^{2^{15}} \\
\alpha_9 &= \zeta + \zeta^{2^2} + \zeta^{2^4} + \zeta^{2^6} + \zeta^{2^8} + \zeta^{2^{10}} \zeta^{2^{12}} + \zeta^{2^{14}} + \zeta^{2^{16}}
\end{aligned}$$

But there are some useful alternative descriptions, some of which are clearer. Since ζ_{27}^3 is a primitive 9^{th} root of unity ζ_9, which is of degree $\varphi(9) = 6$ over $\mathbb{Q}$, this identifies the degree 6 extension generated by α_3 $(3 \cdot 6 = 18)$ more prettily. Similarly, ζ_{27}^9 is a primitive cube root of unity ζ_3, and $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ from earlier examples. This is the quadratic subfield also generated by α_9. And from

$$0 = \frac{\zeta_9^9 - 1}{\zeta_9^3 - 1} = \zeta_9^6 + \zeta_9^3 + 1$$

we use our usual trick

$$\zeta_9^3 + 1 + \zeta_9^{-3} = 0$$

and then

$$(\zeta_9 + \zeta_9^{-1})^3 - 3(\zeta_9 + \zeta_9^{-1}) - 1 = 0$$

so a root of

$$x^3 - 3x - 1 = 0$$

generates the degree 3 field over $\mathbb{Q}$ also generated by α_6. ///

[14.7] Find all fields intermediate between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Before invoking the main theorem of Galois theory, note that it really is true that $[K : \mathbb{Q}] = 2^3$, as a special case of a more general example we did earlier, with an arbitrary list of primes.

To count the proper subgroups of the Galois group $G \approx \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$, it is useful to understand the Galois group as a 3-dimensional vector space over $\mathbb{F}_2$. Thus, the proper subgroups are the one-dimensional subspace and the two-dimensional subspaces, as vector spaces.

There are $2^3 - 1$ non-zero vectors, and since the field is $\mathbb{F}_2$, this is the number of subgroups of order 2. Invoking the main theorem of Galois theory, these are in bijection with the intermediate fields which are of degree 4 over $\mathbb{Q}$. We can easily think of several quartic fields over $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{6}, \sqrt{5})$, $\mathbb{Q}(\sqrt{10}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{15})$, and the least obvious $\mathbb{Q}(\sqrt{6}, \sqrt{15})$. The argument that no two of these are the same is achieved most efficiently by use of the automorphisms σ, τ, ρ of the whole field which have the effects

$$\begin{array}{ccc}
\sigma(\sqrt{2}) = -\sqrt{2} & \sigma(\sqrt{3}) = \sqrt{3} & \sigma(\sqrt{5}) = \sqrt{5} \\
\tau(\sqrt{2}) = \sqrt{2} & \tau(\sqrt{3}) = -\sqrt{3} & \tau(\sqrt{5}) = \sqrt{5} \\
\rho(\sqrt{2}) = \sqrt{2} & \rho(\sqrt{3}) = \sqrt{3} & \rho(\sqrt{5}) = -\sqrt{5}
\end{array}$$

which are restrictions of automorphisms of the form $\zeta \to \zeta^a$ of the cyclotomic field containing all these quadratic extensions, for example $\mathbb{Q}(\zeta_{120})$ where ζ_{120} is a primitive 120^{th} root of unity.

To count the subgroups of order $4 = 2^2$, we might be a little clever and realize that the two-dimensional $\mathbb{F}_2$-vectorsubspaces are exactly the kernels of non-zero linear maps $\mathbb{F}_2^3 \to \mathbb{F}_2$. Thus, these are in bijection with the non-zero vectors in the $\mathbb{F}_2$-linear dual to $\mathbb{F}_2^3$, which is again 3-dimensional. Thus, the number of two-dimensional subspaces is again $2^3 - 1$.

Or, we can count these two-dimensional subspaces by counting ordered pairs of two linearly independent vectors (namely $(2^3-1)(2^3-2) = 42$) and dividing by the number of changes of bases possible in a two-dimensional space. The latter number is the cardinality of $GL(2, \mathbb{F}_2)$, which is $(2^2-1)(2^2-2) = 6$. The quotient is 7 (unsurprisingly).

We can easily write down several quadratic extensions of $\mathbb{Q}$ inside the whole field, namely $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{30})$. That these are distinct can be shown, for example, by observing that the effects of the automorphisms σ, τ, ρ differ. ///

[14.8] Let a, b, c be independent indeterminates over a field k. Let z be a zero of the cubic

$$x^3 + ax^2 + bx + c$$

in some algebraic closure of $K = k(a, b, c)$. What is the degree $[K(z) : K]$? What is the degree of the splitting field of that cubic over K?

First, we prove that $f(x) = x^3+ax^2+bx+c$ is irreducible in $k(a,b,c)[x]$. As a polynomial in x with coefficients in the ring $k(a,b)[c]$, it is monic and has *content* 1, so its irreducibility in $k(a,b,c)[x]$ is equivalent to its irreducibility in $k(a,b)[c][x] \approx k(a,b)[x][c]$. As a polynomial in c it is monic and linear, hence irreducible. This proves the irreducibility in $k(a,b,c)[x]$. Generally, $[K(z) : K]$ is equal to the degree of the minimal polynomial of z over K. Since f is irreducible it *is* the minimal polynomial of z over K, so $[K(z) : K] = 3$.

To understand the degree of the *splitting field*, let the three roots of $x^3 + ax^2 + bx + c = 0$ be z, u, v. Then (the discriminant)

$$\Delta = (z-u)^2(u-v)^2(v-z)^2$$

certainly lies in the splitting field, and is a *square* in the splitting field. But if Δ is *not* a square in the ground field K, then the splitting field contains the quadratic field $K(\sqrt{\Delta})$, which is of degree 2 over K. Since $\gcd(2,3) = 1$, this implies that the splitting field is of degree at least 6 over K. But $f(x)/(x-z)$ is of degree 2, so the degree of the splitting field cannot be *more* than 6, so it is *exactly* 6 if the discriminant is *not* a square in the ground field K.

Now we use the fact that the a, b, c are indeterminates. Gauss' lemma assures us that a polynomial A in a, b, c is a square in $k(a,b,c)$ if and only it is a square in $k[a,b,c]$, since the reducibilities of $x^2 - A$ in the two rings are equivalent. Further, if A is square in $k[a,b,c]$ then it is a square in any homomorphic image of $k[a,b,c]$. If the characteristic of k is not 2, map $a \to 0$, $c \to 0$, so that $f(x)$ becomes $x^3 + bx$. The zeros of this are 0 and $\pm\sqrt{b}$, so the discriminant is

$$\Delta = (0-\sqrt{b})^2(0+\sqrt{b})^2(-\sqrt{b}-\sqrt{b})^2 = b \cdot b \cdot 4b = 4b^3 = (2b)^2 \cdot b$$

The indeterminate b is not a square. (For example, $x^2 - b$ is irreducible by Gauss, using Eisenstein's criterion.) That is, because this image is not a square, we know that the genuine discriminant is not a square in $k(a,b,c)$ without computing it.

Thus, the degree of the splitting field is always 6, for characteristic not 2.

For characteristic of k equal to 2, things work differently, since the cubic expression $(z-u)(u-v)(v-z)$ is already invariant under any group of permutations of the three roots. But, also, in characteristic 2, separable quadratic extensions are not all obtained via square roots, but, rather, by adjoining zeros of *Artin-Schreier* polynomials $x^2 - x + a$. ... ///

[14.9] Let $x_1, \ldots, x_n$ be independent indeterminates over a field k, with elementary symmetric polynomials $s_1, \ldots, s_n$. Prove that the Galois group of $k(x_1, \ldots, x_n)$ over $k(s_1, \ldots, s_n)$ is the symmetric group S_n on n things.

Since $k[x_1, \ldots, x_n]$ is the free (commutative) k-algebra on those n generators, for a given permutation p we can certainly map $x_i \to x_{p(i)}$. Then, since this has trivial kernel, we can extend it to a map on the fraction field $k(x_1, \ldots, x_n)$. So the permutation group S_n on n things does act by automorphisms of $k(x_1, \ldots, x_n)$. Certainly such permutations of the indeterminates leaves $k[s_1, \ldots, s_n]$ pointwise fixed, so certainly leaves the fraction field $k(s_1, \ldots, s_n)$ pointwise fixed.

Each x_i is a zero of

$$f(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \ldots + (-1)^n s_n$$

so certainly $k(x_1, \ldots, x_n)$ is *finite* over $k(s_1, \ldots, s_n)$. Indeed, $k(x_1, \ldots, x_n)$ is a splitting field of $f(X)$ over $k(s_1, \ldots, s_n)$, since no smaller field could contain $x_1, \ldots, x_n$ (with or without $s_1, \ldots, s_n$). So the extension is *normal* over $k(s_1, \ldots, s_n)$. Since the x_i are mutually independent indeterminates, certainly no two are equal, so $f(X)$ is separable, and the splitting field is separable over $k(s_1, \ldots, s_n)$. That is, the extension is Galois.

The degree of $k(x_1, \ldots, x_n)$ over $k(s_1, \ldots, s_n)$ is *at most* $n!$, since x_1 is a zero of $f(X)$, x_2 is a zero of the polynomial $f(X)/(X - x_1)$ in $k(x_1)[X]$, x_3 is a zero of the polynomial $f(X)/(X - x_1)(X - x_2)$ in $k(x_1, x_2)[X]$, and so on. Since the Galois group contains S_n, the degree is *at least* $n!$ (the order of S_n). Thus, the degree is exactly $n!$ and the Galois group is exactly S_n.

Incidentally, this proves that $f(X) \in k(s_1, \ldots, s_n)[X]$ is irreducible, as follows. Note first that the degree of the splitting field of *any* polynomial $g(X)$ of degree d is at most $d!$, proven best by induction: given one root α_1, in $k(\alpha_1)[X]$ the polynomial $g(X)/(X - \alpha_1)$ has splitting field of degree at most $(d-1)!$, and with that number achieved *only* if $g(X)/(X - \alpha_1)$ is *irreducible* in $k(\alpha_1)[X]$. And $[k(\alpha_1) : k] \leq d$, with the maximum achieved if and only if $g(X)$ is irreducible in $k[X]$. Thus, by induction, the maximum possible degree of the splitting field of a degree d polynomial is $d!$, and for this to occur it is *necessary* that the polynomial be irreducible.

Thus, in the case at hand, if $f(X)$ were *not* irreducible, its splitting field could not be of degree $n!$ over $k(s_1, \ldots, s_n)$, contradiction. ///