

1. We see that $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[8]{2})][\mathbb{Q}(\sqrt[8]{2}) : \mathbb{Q}] = 2 \cdot 8 = 16$. We deduce that the automorphisms of K are determined by $\sqrt[8]{2} \mapsto \zeta_8^j \sqrt[8]{2}$ with $0 \leq j < 8$ and $i \mapsto \pm i$. Note that $\zeta_8 = (1+i)/\sqrt{2}$.

By the fundamental theorem of Galois theory, the subfields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$ are each fixed by a subgroup of order 8. In each case, if we can write down 8 elements of $\text{Gal}(K/\mathbb{Q})$ that fix the field, these are the elements of the Galois group.

- $\mathbb{Q}(i)$: the maps $\sqrt[8]{2} \mapsto \zeta_8^j \sqrt[8]{2}$, $i \mapsto i$ are the ones that fix $\mathbb{Q}(i)$. Note that this map sends $\zeta_8 \mapsto (1+i)/(\zeta_8^j \sqrt[8]{2})^4 = (-1)^j \zeta_8$. One checks that the order of the map with $j = 1$ is 8, so the Galois group is cyclic of order 8.
- $\mathbb{Q}(\sqrt{2})$: the element $\sqrt{2}$ is fixed if and only if j is even, so the maps fixing $\mathbb{Q}(\sqrt{2})$ are $\sqrt[8]{2} \mapsto \zeta_8^j \sqrt[8]{2}$ and $i \mapsto \pm i$, with j even. One checks easily that this group of transformations is isomorphic to D_8 .
- $\mathbb{Q}(\sqrt{-2})$: note that $\sqrt[8]{2} \mapsto \zeta_8^j \sqrt[8]{2}$ sends $\sqrt{2} \mapsto (-1)^j \sqrt{2}$. So, the element $\sqrt{-2}$ is fixed by the automorphisms $\sqrt[8]{2} \mapsto \zeta_8^j \sqrt[8]{2}$ and $i \mapsto (-1)^j i$ with $0 \leq j < 8$. If τ is the map $\sqrt[8]{2} \mapsto -\sqrt[8]{2}$, $i \mapsto i$ (that is, τ has $j = 4$) then every automorphism except the identity and τ has square equal to τ . So, the Galois group is Q_8 .

2. The roots of this polynomial are $\pm\sqrt{2} \pm \sqrt{5}$, so the Galois group is V_4 by the next problem.

3.

- (a) The condition that none of $D_1, D_2, D_1 D_2$ is a square implies that $[K : F] = 4$. The elements of the Galois group must be $\sqrt{D_1} \mapsto \pm\sqrt{D_1}, \sqrt{D_2} \mapsto \pm\sqrt{D_2}$, and these are easily seen to form a group isomorphic to V_4 .
- (b) Suppose $\text{Gal}(K/F) \cong V_4$. Since V_4 has three subgroups of order 2, there are three quadratic fields E_1, E_2, E_3 lying between F and K . Since $\text{char}(F) \neq 2$, each E_i has the form $E_i = F(\sqrt{D_i})$ for nonsquares $D_i \in F$. Then $K = E_1 E_2 = F(\sqrt{D_1}, \sqrt{D_2})$. Since $[K : F] = 4$ we deduce that $D_1 D_2$ is a nonsquare and the third quadratic field inside K/F is $F(\sqrt{D_1 D_2})$.

4. From the conditions of the problem we see that K/F must be separable.

- (a) We know that K has $[K : F]$ embeddings into L ; they are precisely the restrictions to K of the elements of $\text{Gal}(L/F)$. Moreover, the elements of a coset $\sigma H \subset \text{Gal}(L/F)$ all correspond to the same embedding, since elements of H act trivially on K . So $N_{K/F}(\alpha) = \prod_i \sigma_i(\alpha)$ where (σ_i) are any collection of left coset representatives for H in $\text{Gal}(L/F)$.

For any $\sigma \in \text{Gal}(L/F)$ we have

$$\sigma N_{K/F}(\alpha) = \prod_i \sigma \sigma_i(\alpha) = N_{K/F}(\alpha)$$

since $(\sigma \sigma_i)$ is also a collection of left coset representatives for H in $\text{Gal}(L/F)$. Thus $N_{K/F}(\alpha)$ is fixed by $\text{Gal}(L/F)$, and lies in F .

(b),(c) are trivial.

- (d) If $F \subset E \subset K$, I leave it as an exercise to check that $N_{E/F}(N_{K/E}(\alpha))$. Take $E = F(\alpha) \subset K$. You can check from the definition that $N_{F(\alpha)/F}(\alpha)$ is the product of the roots of m_α , so $N_{E/F}(\alpha) = (-1)^d a_0$. Then

$$N_{E/F}(N_{K/E}(\alpha)) = N_{E/F}(\alpha^{n/d}) = (-1)^n a_0^{n/d},$$

the first equality because $N_{K/E}(x) = x^{[K:E]}$ for $x \in E$.

5. Part (a) is exactly like 4(a). For part (b), $\text{Tr}_{K/F}$ is the linear combination of characters $\sum_{\sigma \in \text{Gal}(K/F)} \sigma$. The result is immediate.

6.

- (a) Follow the hint.
 (b) Since $\alpha^2 = (2 + \sqrt{2})(3 + \sqrt{3})$ generates $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, we know that E contains F . By the previous part E is a quadratic extension of F , so $[E : \mathbb{Q}] = 8$. It's easy to check that the eight given numbers are distinct and are the roots of the same polynomial with rational coefficients, so they are the eight roots of the minimal polynomial of α .
 (c) Each statement in this part is clear from the immediately preceding statement.
 (d) As noted before, α^2 generates $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over \mathbb{Q} ; it is easy to see that there is only one automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ that sends $(2 + \sqrt{2})(3 + \sqrt{3})$ to $(2 - \sqrt{2})(3 + \sqrt{3})$, namely the one that fixes $\sqrt{3}$ and sends $\sqrt{2} \mapsto -\sqrt{2}$. So σ is an extension to E of this map. Now $\alpha\beta = \sqrt{2}(3 + \sqrt{3})$, so $\sigma(\alpha\beta) = -\sqrt{2}(3 + \sqrt{3})$, i.e., $\sigma(\alpha\beta) = -\alpha\beta$. Since $\sigma(\alpha) = \beta$, we have $\sigma(\beta) = -\alpha$. From this we see $\sigma^4(\alpha) = \alpha$, so σ has order 4.
 (e) σ^2, τ^2 both send $\alpha \mapsto -\alpha$, hence are equal. Similarly, $\sigma\tau$ and $\tau\sigma^3$ can both be checked to send $\alpha \mapsto -\sqrt{(2 - \sqrt{2})(3 - \sqrt{3})}$, so are equal.
 (f) is immediate from the elements and relations constructed in (e).

7. Let L_1, \dots, L_n be the Galois conjugates of L over F contained in some algebraic closure of L , so that the Galois closure of L is the composite $L_1 \cdots L_n$. Since K/F is Galois, L_i contains K for each i , and in fact L_i/K is Galois. Since the extensions L_i/K are all Galois, the degree of the composite $[L_1 \cdots L_n : K]$ divides $[L_1 : K] \cdots [L_n : K]$, which is a power of p . Since $[K : F]$ is a power of p as well, we deduce that $[L_1 \cdots L_n : F]$ is a power of p .

For a counterexample with K/F not Galois, take $L = K = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$.

8. Suppose that the polynomial $g(x) = x^n + \cdots + a_1x + a_0$ satisfies $g(\text{Frob}_p) = 0$. Then the equation $g(\text{Frob}_p) = 0$ gives a linear dependence among $\text{Frob}_p^n, \dots, \text{Frob}_p, 1$. By linear independence of characters, two of the characters in this list must be equal, and therefore $n \geq r$. It follows that the characteristic polynomial of Frob is the unique monic polynomial of degree r which vanishes on Frob . Finally, note that $\text{Frob}_p^r(\alpha) = \alpha^{p^r} = \alpha$, so Frob_p is a root of $x^r - 1$; so the characteristic polynomial is $x^r - 1$.

9. In this problem, one needs to be careful about signs: it should bother you to write down an expression like

$$\alpha_n = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$$

without making precise what the right-hand side of that expression means! For instance, you could mean that α_n is defined inductively as the image of x in the abstractly defined field $\mathbb{Q}(\alpha_{n-1})[x]/(x^2 - (2 + \alpha_{n-1}))$; but then it's not at all clear what relation is borne between α_n and the *particular 2^{n+2} th root of unity that we started with*. On the other hand, if you define $\alpha_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$, as the problem does, and then derive the formula $\alpha_n^2 = \alpha_{n-1} + 2$, then the expression $\alpha_n = \sqrt{\alpha_{n-1} + 2}$ is meaningless: the square root is not a function. So, it really does take some caution in order to make the statements of the problem meaningful.

Here is one approach. Let us regard $\mathbb{Q}(\zeta_{2^{n+2}})$ as a subfield of \mathbb{C} , and choose $\zeta_{2^{n+2}}$ to be the specific element $e^{\frac{2\pi i}{2^{n+2}}}$, so that $\zeta_{2^i} = e^{\frac{2\pi i}{2^i}}$ for $i \leq n+2$. Now the expression

$$\sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$$

is perfectly well-defined: we are only taking square roots of positive numbers, and we always choose the positive square root. Let $\alpha_i = \zeta_{2^{i+2}} + \zeta_{2^{i+2}}^{-1}$. Notice that

$$\alpha_i = \zeta_{2^{i+2}} + \zeta_{2^{i+2}}^{-1} = e^{\frac{2\pi i}{2^{i+2}}} + e^{-\frac{2\pi i}{2^{i+2}}} = 2 \cos\left(\frac{2\pi}{2^{i+2}}\right).$$

So $\alpha_1 = \sqrt{2}$, and it's easy enough to check that $\alpha_i^2 = \alpha_{i-1} + 2$. Suppose by induction that

$$\alpha_{i-1} = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$$

(with $i-1$ twos in the expression). The formula $\alpha_i^2 = \alpha_{i-1} + 2$ implies that

$$\alpha_i = \pm \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$$

(with i twos in the expression). But the formula $\alpha_i = 2 \cos\left(\frac{2\pi}{2^{i+2}}\right)$ shows in particular that α_i is a *positive* real number. Therefore

$$\alpha_i = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$$

(with i twos in the expression) and the induction is complete.

Now the quadratic formula gives

$$\zeta_{2^{n+2}} = \frac{\alpha_n \pm \sqrt{\alpha_n^2 - 4}}{2};$$

again there is a sign ambiguity that we must resolve. Note that this may be rewritten

$$\zeta_{2^{n+2}} = \frac{\sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}} \pm \sqrt{-2 + \sqrt{2 + \cdots + \sqrt{2}}}}{2}.$$

Since the expression inside the square root is a negative real number, we may rewrite the expression again as

$$\zeta_{2^{n+2}} = \frac{\sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}} \pm i\sqrt{2 - \sqrt{2 + \cdots + \sqrt{2}}}}}{2}$$

(where i is the root of -1 in the upper half plane). Finally, since $e^{\frac{2\pi i}{2^{n+2}}}$ has *positive* imaginary part, we conclude that

$$\zeta_{2^{n+2}} = e^{\frac{2\pi i}{2^{n+2}}} = \frac{\sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}} + i\sqrt{2 - \sqrt{2 + \cdots + \sqrt{2}}}}}{2}.$$

This is a *better theorem* than a vaguer statement that the process of repeatedly adding two and taking a square root yields *some* 2^{n+2} th root of unity.

10. Typically in a problem like this, you write down some permutations of the roots of the polynomial, and prove that any automorphism must come from one of these permutations. One subtlety to be aware of is that it's not always obvious that the permutations you've written down really all give you maps; that is, you have to give a *lower bound* on the size of the Galois group, and not just the upper bound that you get from writing down the obvious relations among the roots of the polynomial.

In this case, let z be a root of the quadratic $t^2 - 4t + 1$; for instance, $z = 2 + \sqrt{3}$ will do; note that z^{-1} is the other root. Let y be a cube root of z . Then the roots of $f(x) = x^6 - 4x^3 + 1$ are $y, \zeta_3 y, \zeta_3^{-1} y$ and $y^{-1}, \zeta_3 y^{-1}, \zeta_3^{-1} y^{-1}$. Let K be the splitting field of $f(x)$; then an automorphism of K is determined entirely by where it sends y (six choices), and where it sends ζ_3 (two choices). Thus $\#\text{Gal}(K/\mathbb{Q}) \leq 12$. We suspect that equality may hold — i.e., that we can make these two choices independently — but we still have to prove that the choice for y does not determine the choice for ζ_3 . (In fact we also have to prove that $f(x)$ is irreducible, so that the six choices for y are all possible.)

In this case, you can see that $f(x) = x^6 - 4x^3 + 1$ is irreducible; for instance, $f(x+1)$ is Eisenstein at 2. Let K be the splitting field of $f(x)$ over \mathbb{Q} inside \mathbb{C} . Note that the roots of K is not contained in \mathbb{R} (e.g. because K must contain cube roots of unity), so $[K : K \cap \mathbb{R}] = 2$. On the other hand, $f(x)$ has two real roots; letting α be one of these roots, we see that $\mathbb{Q}(\alpha) \subset K \cap \mathbb{R}$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$, It follows that $[K : \mathbb{Q}] = [K : K \cap \mathbb{R}][K \cap \mathbb{R} : \mathbb{Q}]$ is divisible by 12; in particular $[K : \mathbb{Q}] \geq 12$. Therefore our 12 proposed automorphisms really are automorphisms.

Finally, we can check that $\text{Gal}(K/\mathbb{Q}) \cong D_{12}$. Let σ be the map sending $y \mapsto \zeta_3/y$ and $\zeta_3 \mapsto \zeta_3^{-1}$. Let τ be the map sending $y \mapsto y^{-1}$, $\zeta_3 \mapsto \zeta_3$. Then σ has order six, τ has order two, and $\tau\sigma = \sigma^{-1}\tau$ both map $y \mapsto \zeta_3 y$, $\zeta_3 \mapsto \zeta_3^2$. This gives a presentation.