Practice for the FINAL

ADVISE

• Please make sure that your understanding of the question has a mathematical sense.
• Ask yourself if you have a complete answer to a question before moving to another one.
• Think about all the ways at your disposal to answer the question, try to find out, which one has most chances to succeed.
• Make sure all the assumption of the theorem you want to use are in the exercise before using it.
• Do not forget that there can be connection between the questions. this can make you win a lot of time.
• Start with a problem that you know how to solve to build confidence.
• Remember that partial answers, as long as they make sense, can earn you come points.

You must know well: Finite fields, constructible number, Galois theory.

Exercise 1: (∗)
Show that

1. if \( \cos(\theta) \) is constructible, so is \( \sin(\theta) \).
2. if \( \cos(\theta_1) \) and \( \cos(\theta_2) \) are constructible, so is \( \cos(\theta_1 + \theta_2) \)
3. if \( \cos(2\theta) \) is constructible, so is \( \cos(\theta) \). (The converse, of course, follows from (b))

**Solution:** Everything here is a straightforward consequence of the fact that the constructible numbers form a field closed under taking square roots of positive elements.

1. If \( \cos \theta \) is constructible, then \( 1 - \cos^2 \theta \) is constructible and non-negative, so \( \sin \theta = \pm \sqrt{1 - \cos^2 \theta} \) is constructible.
2. We use
   \[
   \cos(\theta_1 + \theta_2) = \cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2.
   \]
   Since \( \cos \theta_1, \sin \theta_1, \cos \theta_2, \sin \theta_2 \) are all constructible – by hypothesis and part (a) – \( \cos(\theta_1 + \theta_2) \) is constructible.
3. We use
\[
\cos(2\theta) = 2\cos^2 \theta - 1, \quad \text{so} \quad \cos \theta = \pm \sqrt{(\cos(2\theta) + 1)/2},
\]

Since \(\cos(2\theta)\) is constructible, \((\cos(2\theta)+1)/2\) is constructible, so \(\sqrt{(\cos(2\theta) + 1)/2}\) is the square root of a non-negative constructible number and hence constructible.

Exercise 2: (**) Let \(p = 2k + 1\) be an odd prime. Set \(\epsilon = e^{2\pi i/p}\) and set \(K = \mathbb{Q}(\epsilon)\). Let \(\tau\) denote complex conjugation and set \(H = \{1, \tau\}\). Let \(L\) denote the set of real numbers in \(K\).

1. Show that \(L = K^H\).
2. Find \([L : \mathbb{Q}]\).
3. Set \(\gamma = \epsilon + \epsilon^{-1}\). Show \(G_{\mathbb{Q}(\gamma)} = H\).
4. Find the degree of minimal polynomial \(f(x) \in \mathbb{Q}[x]\) with \(\cos(2\pi/p)\) as a root.

Solution:

1. \(\alpha \in K^H\) if and only if \(\text{Id}(\alpha) = \alpha\) and \(\tau(\alpha) = \alpha\). But \(\text{Id}(\alpha) = \alpha\) always so the condition is that \(\alpha\) equals its complex conjugate which occurs precisely when \(\alpha\) is real.
2. As \([K : \mathbb{Q}] = p-1\) we again apply the Galois Correspondence Theorem with values so that \([L : \mathbb{Q}] = [K^H : \mathbb{Q}] = |Gal(K, \mathbb{Q})|/|H| = (p-1)/2\).
3. As \(\epsilon^{-1} = \tau(\epsilon), \tau(\epsilon + \epsilon^{-1}) = \epsilon^{-1} + \epsilon\) so \(\tau \in Q(\gamma^*)\). The elements of \(\text{Gal}(K, \mathbb{Q})\) are given by \(\sigma_j, 1 \leq j \leq p-1\), where \(\sigma_j(\epsilon) = \epsilon^j\). If \(\sigma_j(\gamma) = \gamma\) we have \(\epsilon + \epsilon^{-1} = \epsilon^j + \epsilon^{-j}\). We can suppose \(j \leq (p-1)/2\) as otherwise we could replace it by \(p-j\). Multiplying by \(\epsilon^j\): \(\epsilon^{j+1} + \epsilon^{j-1} = \epsilon^{2j} + 1\). With \(j < (p-1)/2\) this contradicts the independence of \(1, \epsilon, \ldots, \epsilon^{p-2}\). With \(j = (p-1)/2\) you’d have \(\epsilon^{j+1} + \epsilon^{j-1} = \epsilon^{p-1} + 1\). Replacing \(\epsilon^{p-1}\) with \((-1 + \epsilon + \ldots + \epsilon^{p-2})\) one again contradicts the independence of \(1, \epsilon, \ldots, \epsilon^{p-2}\).
4. As \(|G_{\mathbb{Q}(\gamma)}| = 2\), \([\mathbb{Q}(\gamma) : \mathbb{Q}] = (p-1)/2\). But \(\cos(2\pi/p) = \gamma/2\) so \([\mathbb{Q}(\cos(2\pi/p) : \mathbb{Q}] = (p-1)/2\) and so the minimal polynomial has degree \((p-1)/2\). It is an interesting trigonometry problem, using formulae for multiple angles, to find the polynomial.

Exercise 3: (*)
Let \(f(x) = x^7 - 2\). Since \(f'(x) > 0\) for \(x \neq 0\), it follows from calculus that \(f(x)\) has no real root other than the familiar one \(2^{1/7}\). Let \(\lambda\) be a nonzero rational number, and write \(\gamma\) for \(2^{1/7} + \lambda \cdot 2^{1/2}\)

1. Using the uniqueness of the real root of \(f(x)\), find the (monic) greatest common divisor of \(x^2 - 2\) and \(f(\gamma - \lambda x)\) in \(\mathbb{Q}(2^{1/2}, 2^{1/7})[x]\).
2. Show that \(\mathbb{Q}(\gamma) = \mathbb{Q}(2^{1/2}, 2^{1/7})\), i.e., that \(2^{1/7} + \lambda \cdot 2^{1/2}\) is a primitive element for the field extension \(\mathbb{Q} \subset \mathbb{Q}(2^{1/2}, 2^{1/7})\).

Solution: Write \(g(x)\) for \(x^2 - 2\) and \(h(x)\) for \(f(\gamma - \lambda \cdot x)\). Over the field \(\mathbb{Q}(2^{1/2})\), \(g(x)\) factorizes as \((x + 2^{1/2})(x - 2^{1/2})\). Polynomials of degree 1 are always irreducible, so this
is also the factorization of $g(x)$ into irreducibles over $\mathbb{Q}(2^{1/2}, 2^{1/7})$. Now

$$h(2^{1/2}) = f(2^{1/7} + \lambda \cdot 2^{-1/2} - \lambda \cdot 2^{-1/2}) = f(2^{1/7}) = 0,$$

so $x - 2^{1/2}$ divides $h(x)$ over $\mathbb{Q}(2^{1/2}, 2^{1/7})$. On the other hand $x + 2^{1/2}$ does not divide $h(x)$ because

$$h(-2^{1/2}) = f(2^{1/7} + \lambda \cdot 2^{1/2} - \lambda \cdot (-2^{1/2})) = f(2^{1/7} + 2\lambda \cdot 2^{1/2}) \neq 0,$$

since $2^{1/7}$ is the only real root of $f(x)$. Thus, $x - 2^{1/2}$ is the only irreducible divisor of $g(x)$ in $\mathbb{Q}(2^{1/2}, 2^{1/7})$ which also divides $h(x)$, so the monic greatest common factor of $g(x)$ and $h(x)$ over $\mathbb{Q}(2^{1/2}, 2^{1/7})$ is $x - 2^{1/2}$. But $g(x)$ and $h(x)$ both have coefficients in $\mathbb{Q}(\gamma)$, so their greatest common divisor over $\mathbb{Q}(\gamma)$ is the same as over the larger field $\mathbb{Q}(2^{1/2}, 2^{1/7})$, so $x - 2^{1/2} \in \mathbb{Q}(\gamma)[x]$, so $2^{1/2} \in \mathbb{Q}(\gamma)$. But then $2^{1/7} = \gamma - \lambda \cdot 2^{1/2}$ is also in $\mathbb{Q}(\gamma)$ — remember that $\lambda \in \mathbb{Q}$, so both $2^{1/2}$ and $2^{1/7}$ are in $\mathbb{Q}(\gamma)$, so $\mathbb{Q}(2^{1/2}, 2^{1/7}) \subset \mathbb{Q}(\gamma)$. The opposite inclusion is immediate, so $\mathbb{Q}(2^{1/2}, 2^{1/7}) = \mathbb{Q}(\gamma)$ i.e., $\gamma$ generates $\mathbb{Q}(2^{1/2}, 2^{1/7})$ over $\mathbb{Q}$.

**Exercise 4: (**)**

In this exercise, $p$ denotes an odd prime, i.e., any prime other than 2.

1. Let $a$ be an integer not divisible by $p$. Show that the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution in $\mathbb{Z}$ if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

**Hint:** Since $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$, this is purely a question about the structure of this cyclic group.

2. Using the result of (a), determine whether

(a) $3$ is a square mod 17

(b) $10$ is a square mod 13

3. Again using the result of (a), show that $-1$ is a square modulo $p$ if and only if $p \equiv 1 \pmod{4}$.

**Solution:**

1. It is a good idea to invoke the fact that the multiplicative group $\mathbb{F}_p^\times$ is isomorphic to the additive group $\mathbb{Z}/(p - 1)\mathbb{Z}$. Since $p$ is odd, $p - 1$ is even, so, for given $n$, the congruence $n \equiv 2m \pmod{p - 1}$ has a solution $m$ is and only if $n$ is even. We can write

$$p - 1 = 2^k q \quad \text{with } q \text{ odd;}$$

from this — and the uniqueness of the factorization of integers into primes — it follows that $n \cdot (p - 1)/2 = n \cdot 2^{k-1} \cdot q$ is divisible by $(p - 1) = 2^k \cdot q$ if and only
if “n provides a factor of 2”, i.e., if and only if n is even. Thus: The congruence 
\( n \equiv 2m \mod (p - 1) \) can be solved if and only if \( n \cdot (p - 1)/2 \) is divisible by \( p - 1 \).
Translated back into the multiplicative notation, this says that the equation \( a = x^2 \) 
has a solution in \( \mathbb{F}_p \) if and only if \( a^{(p-1)/2} = 1 \) (again, in \( \mathbb{F}_p \)).

2. (a) By (a), 3 is a square mod 17 – \( p = 17 \) so \( (p-1)/2 = 8 \) – if and only if \( 3^8 \equiv 1 \) (mod 17). This is a routine calculation:

\[
3^2 = 9, \quad 3^4 = 81 = 5 \cdot 17 - 4 \equiv -4, \quad 3^8 \equiv (-4) \cdot (-4) = 16 \equiv -1 \neq 1,
\]

so 3 is not a square in \( \mathbb{F}_{17} \).

(b) 10 is a square mod 13 if and only if \( 10^6 \equiv 1 \) (mod 13):

\[
10^2 = 100 = 13 \cdot 7 + 9 \equiv 9, \quad 10^3 \equiv 10 \cdot 10^2 \equiv 90 = 13 \cdot 7 - 1 \equiv -1, \\
10^6 = 10^3 \cdot 10^3 \equiv (-1) \cdot (-1) = 1,
\]

so 10 does turn out to be a square mod 13.

3. Again by (a), \(-1\) is a square mod \( p \) if and only if \((-1)^{(p-1)/2} \equiv 1 \) (mod \( p \)), which is the case if and only if \( (p-1)/2 \) is even, which is the case if and only if \( (p-1)/2 \) 
has the form \( 2k \), i.e., if and only if \( p \) has the form \( 4k + 1 \).

**Exercise 5:** (⋆) Let \( p \) be a prime integer, \( m \) an integer \( \geq 1 \). As in lecture, we denote 
by \( \mathbb{F}_{p^m} \) the (essentially unique) field with \( p^m \) elements. Let \( \sigma \) denote the Frobenius 
amorphism of \( \mathbb{F}_{p^m} \), i.e., \( \sigma(a) = a^p \).

1. Show that, \( a \in \mathbb{F}_{p^m} \) is in the prime field \( \mathbb{F}_p \) if and only if it is left fixed by \( \sigma \).

2. Show that the powers of \( \sigma \) form a cyclic group of order \( m \), i.e., that \( \sigma^m \) is the 
identity mapping and the powers \( \sigma, \sigma^2, \ldots, \sigma^m \) are all distinct.

**Solution:** By the general theory of finite fields, applied in the simple case \( m = 1 \), 
says that all elements of \( \mathbb{F}_p \) are roots of \( x^p - x \), and that there are no more roots in 
any extension field. Put into the language of the Frobenius homomorphism, this says 
extactly that every element of \( \mathbb{F}_p \) is left fixed by \( \sigma \), and no element outside \( \mathbb{F}_p \) in any 
extension is. In particular: \( a \in K \) is left fixed by \( \sigma \) if and only if \( a \in \mathbb{F}_p \).

By the general theorem proved in lecture, \( a^{p^m} - a = 0 \) for all \( a \in K \). Expressed 
in terms of the Frobenius homomorphism, this says that \( \sigma^m(a) = a \) for all \( a \in K \), which 
means that \( \sigma^m \) is the identity mapping on \( K \). Thus, the order of \( \sigma \) in the group of 
amorphisms of \( K \) divides \( m \). We need to show that it is actually equal to \( m \). If its 
order is \( k < m \), then \( \sigma^k(a) = a \) for all \( a \in K \). Translating back: \( a^{p^k} - a = 0 \) for all \( p^m \) 
a’s in \( K \). But the polynomial \( x^{p^k} - x \) has at most \( p^k \) roots, while \( K \) has \( p^m \) elements, 
so \( k < m \) is not possible.

**Exercise 6:** (★★) Let \( f(x) \) be an irreducible cubic polynomial over a field \( F \), and 
let \( K \) be an extension field of \( F \) of degree 2. Show that \( f(x) \) is (still) irreducible over 
\( K \).

**Solution:** Since \( f(x) \) is cubic, if it is not irreducible over \( K \), it must have a root
in $K$. But if $\alpha$ is a root of $f(x)$ (in any extension field of $K$), its degree over $F$ must be 3. Since $[K : F] = 2$, no element of $K$ can have degree 3 over $F$.

**Exercise 7: (⋆⋆) Preliminaries:** Let $f(x)$ be a monic cubic polynomial over a subfield $F$ of $C$. We can then factorize

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \quad \text{with } \alpha_1, \alpha_2, \alpha_3 \text{ in } \mathbb{C}.$$ 

The **discriminant** of $f(x)$ is defined as

$$D := (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

It has been shown (or will be shown) in lecture that $D$ is in the base field $F$, and you can assume this fact for these exercises.

Define also

$$\delta := (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3), \quad \text{so } \delta^2 = D.$$ 

The quantity $\delta$ is in the splitting field for $f(x)$; it may or may not be in the base field $F$, and it changes sign if the labeling of the roots is subjected to an odd permutation.

Recall that, by analysis, a cubic polynomial with real coefficients has either three real roots (which may coincide, i.e., may be a single root of multiplicity 3), or one real root and a complex-conjugate pair of non-real roots.

1. Let $f(x)$ be an irreducible cubic polynomial over a field $F$, and let $K$ be an extension field of $F$ of degree 2. Show that $f(x)$ is (still) irreducible over $K$.
2. Show that, if the monic cubic $f(x)$ is irreducible over $F$, then $D \neq 0$.
3. If $f(x)$ has real coefficients, show that $D < 0$ if and only if $f(x)$ has only one real root.

The polynomial $f(x) = x^3 - 2$ was analyzed in some detail in lecture. We review here the main points: Its roots are

$$\alpha_1 := \sqrt[3]{2} =: \alpha, \quad \alpha_2 := \omega \alpha_1, \quad \alpha_3 := \omega^2 \alpha_1,$$

with

$$\omega := e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$ 

For brevity, we denote by $K$ its splitting field $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. We showed – modulo one step, to be filled in below – that the group of automorphism of the field extension $K/\mathbb{Q}$, regarded as acting on the labels of the roots $\alpha_i$, is the full symmetric group $S_3$ on three objects. One of these automorphisms is complex conjugation, which interchanges $\alpha_2$ and $\alpha_3$, leaving $\alpha_1$ fixed. This exercise concerns the polynomial $f(x) = x^3 - 2$.

1. Compute $\delta$ for this polynomial directly from the definition above, and verify that it is not in $\mathbb{Q}$ but that its square is (as it must be, by the general theory.) Show that

$$\mathbb{Q}(\delta) = \mathbb{Q}(\omega).$$
2. Filling in a point left without proof in lecture: Show that there is an automorphism
\( \sigma \) of \( \mathbb{Q}(\omega, \alpha)/\mathbb{Q}(\omega) \) sending \( \alpha_1(=\alpha) \) to \( \alpha_2 = \omega \alpha \).

3. Show that
\[
1, \alpha, \alpha^2, \omega, \omega \alpha, \omega \alpha^2
\]
form a basis for \( K := \mathbb{Q}(\omega, \alpha) \) over \( \mathbb{Q} \).

4. Show that \( \beta \in K \) is left fixed by complex conjugation if and only if \( \beta \in \mathbb{Q}(\alpha) \).

5. Show that the set of elements of \( K \) left fixed by all of \( G(K/\mathbb{Q}) \) is exactly \( \mathbb{Q} \).

6. Let \( H \) denote the subgroup of \( G(\mathbb{Q}(\omega, \alpha)/\mathbb{Q}) \) leaving all elements of \( \mathbb{Q}(\omega) \) fixed.
   Show that the action of \( H \) on the roots of \( f(x) \), represented by permutations of the labels, is the cyclic subgroup
   \[
   \{ \epsilon, (123), (132) \} \subset S_3
   \]

   From Algebra I, this is a normal subgroup of \( S_3 \); it is in fact the alternating group \( A_3 \) in this simple case. Show that \( S_3/H \) is isomorphic to \( G(\mathbb{Q}(\omega)/\mathbb{Q}) \).

**Solution:**

1. Using \( \omega^2 = \overline{\omega} \) (complex conjugate):

\[
\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\
= \alpha(1 - \omega) \cdot \alpha(1 - \overline{\omega}) \cdot \alpha(\omega - \overline{\omega}) \\
= (\alpha^3)[1 - \omega^2](\omega - \overline{\omega}) \\
= 2 \cdot ((3/2)^2 + (\sqrt{3}/2)^2)(i \sqrt{3}) \\
= 2 \cdot 3 \cdot i \sqrt{3} = 6i \sqrt{3},
\]

which indeed is not in \( \mathbb{Q} \) but whose square \(-108\) is. Since

\[
i \sqrt{3} = 2\omega + 1 = \delta/6,
\]

\[
\mathbb{Q}(\omega) = \mathbb{Q}(i \sqrt{3}) = \mathbb{Q}(\delta).
\]

2. Write \( L := \mathbb{Q}(\omega) \) and \( K := \mathbb{Q}(\omega, \alpha) \); then \( K = L(\alpha_1) = L(\alpha_2) \).
   Since \([L : \mathbb{Q}] = 2\), \( x^3 - 2 \) is irreducible over \( L \) by exercise 1. As argued in lecture, there are isomorphisms

(a) \( L[x]/(f(x)) \rightarrow L(\alpha_1) = K \) sending \( x \) to \( \alpha_1 \)

(b) \( L[x]/(f(x)) \rightarrow L(\alpha_2) = K \) sending \( x \) to \( \alpha_2 \).

Composing the inverse of the first of these with the second is an isomorphism \( K \rightarrow K \) sending \( \alpha_1 \) to \( \alpha_2 \) and leaving elements of \( L \) fixed.

3. We can write \( K = L(\alpha) \). \( \{1, \omega\} \) is a basis for \( L \) over \( \mathbb{Q} \), and \( \{1, \alpha, \alpha^2\} \) a basis for \( L(\alpha) \) over \( L \). By the proof of the Tower Theorem, the set of products of one factor from \( \{1, \omega\} \) and a second from \( \{1, \alpha, \alpha^2\} \) forms a basis for \( K \) over \( \mathbb{Q} \).
4. This time we write $K = (\mathbb{Q}(\alpha))(\omega)$ and use the fact that $\{1, \omega\}$ is a basis for $K$ over $\mathbb{Q}(\alpha)$. We can thus write the general element of $K$ as $\beta = a + b\omega$, with $a, b$ in $\mathbb{Q}(\alpha) \subset \mathbb{R}$. Complex conjugation maps this general element

$$\beta = a + b\omega \mapsto a + b\bar{\omega} = a + b\omega + b(\bar{\omega} - \omega) = \beta + b(\bar{\omega} - \omega).$$

Since $\bar{\omega} - \omega \neq 0$, $\beta = a + b\omega$ is left fixed by complex conjugation if and only if $b = 0$, i.e., if and only if $\beta \in \mathbb{Q}(\alpha)$

5. By the preceding part, if $\beta \in K$ is left fixed by complex conjugation, it must have the form $c_1 + c_2\alpha + c_3\alpha^2$ (with $c_1, c_2, c_3 \in \mathbb{Q}$). By part (b), there is a $\sigma \in G(K/\mathbb{Q})$ such that $\sigma(\alpha) = \omega\alpha$. Then

$$\sigma(\beta) = c_1 + c_2\sigma(\alpha) + c_3(\sigma(\alpha))^2 = c_1 + c_2\omega\alpha + c_3\omega^2\alpha^2.$$

By the linear independence of $1, \alpha, \alpha^2$ over $\mathbb{Q}(\omega)$, $\sigma(\beta)$ cannot be equal to $\beta$ unless $c_2 = c_3 = 0$, i.e., unless $\beta \in \mathbb{Q}$.

6. If $\sigma$ be the automorphism of $K/\mathbb{Q}$ constructed in (b). Then, by that construction, $\sigma(\alpha_1) = \alpha_2 (= \omega\alpha_1)$. Further, $\sigma$ leaves $\omega$ fixed, so

$$\sigma(\alpha_2) = \sigma(\omega\alpha_1) = \sigma(\omega)\sigma(\alpha_1) = \omega \cdot \omega\alpha_1 = \alpha_2$$

$$\sigma(\alpha_3) = \sigma(\omega^2\alpha_1) = \omega^2 \cdot \omega \cdot \alpha_1 = \alpha_1$$

Thus, expressed in terms of its action on the indices on the roots, $\sigma$ is the cyclic permutation $(123)$, so $\sigma^2 = (123)(123) = (132)$. Now let $\tau$ be any automorphism of $K/\mathbb{Q}$ leaving $\omega$ fixed. Then $\tau$ must map $\alpha_1$ to a root, i.e, there are three possibilities

(a) $\tau(\alpha_1) = \alpha_1$, which implies $\tau = \text{id}$

(b) $\tau(\alpha_1) = \alpha_2$, which implies $\tau = \sigma$

(c) $\tau(\alpha_1) = \alpha_3$, which implies $\tau = \sigma^2$.

Thus, the subgroup of the group of automorphisms of $K/\mathbb{Q}$ leaving $\omega$ fixed is $\{\text{id}, (123), (132)\}$, i.e., the alternating group $A_3$. The full symmetric group $S_3$ has 6 elements, so the above cyclic subgroup has index 2 in $S_3$, so the quotient group $S_3/A_3$ is isomorphic to the cyclic group with 2 elements $C_2$, which in turn is isomorphic to the group of automorphisms of $\mathbb{Q}(\omega)/\mathbb{Q}$ (since this latter is a field extension of degree 2.)

Exercise 8: (⋆) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subset \mathbb{R}$

1. Determine the degree $[K : \mathbb{Q}]$

2. Show that $K/\mathbb{Q}$ is a normal extension

3. Find the Galois group of $K/\mathbb{Q}$. Describe each automorphism by saying how it acts on the generators $\sqrt{2}, \sqrt{3}, \sqrt{5}$, and also identify the group “abstractly.”
4. Find all fields intermediate between $K$ and $\mathbb{Q}$.

**Solution:**

$K$ is the splitting field of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ over $\mathbb{Q}$; hence, is a normal extension of $\mathbb{Q}$. To determine the degree of the extension, and its Galois group, we use the results about biquadratic extensions proved in lecture. To start with: $K_1 := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 4 over $\mathbb{Q}$, and $K$ is obtained by adjoining $\sqrt{5}$ to $K_1$. Thus $[K : \mathbb{Q}]$ is 4 if $\sqrt{5} \in K_1$ and 8 otherwise. We argue that $\sqrt{5} \notin K_1$, from which it will follow that $[K : \mathbb{Q}] = 8$.

From the theory of biquadratic extensions:

- $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $K_1$ over $\mathbb{Q}$
- the Galois group for $K_1/K$ has four elements; the three elements other than the identity can be labeled as $\sigma_1$, $\sigma_2$, $\sigma_3 = \sigma_1\sigma_2$ which are characterized by:

$$
\begin{align*}
\sigma_1 &: \begin{cases} 
\sqrt{2} &\mapsto -\sqrt{2} \\
\sqrt{3} &\mapsto \sqrt{3}
\end{cases} \\
\sigma_2 &: \begin{cases} 
\sqrt{2} &\mapsto \sqrt{2} \\
\sqrt{3} &\mapsto -\sqrt{3}
\end{cases} \\
\sigma_3 &: \begin{cases} 
\sqrt{2} &\mapsto -\sqrt{2} \\
\sqrt{3} &\mapsto -\sqrt{3}
\end{cases}
\end{align*}
$$

Now suppose that there is an element $\beta$ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $\beta^2 = 5$, i.e., a root of $x^2 - 5$. Then $\beta$ can be written as

$$
\beta = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}
$$

with $a, b, c, d$ in $\mathbb{Q}$. But then also $-\beta, \pm \sigma_1\beta, \pm \sigma_2\beta, \pm \sigma_3\beta$ are all roots of $x^2 - 5$, i.e., all expressions of the form $\pm a \pm b\sqrt{2} \pm c\sqrt{3} \pm d\sqrt{6}$ are roots of $x^2 - 5$. There can only be two roots, so only one of $a, b, c, d$ can be different from 0. It is then easy to rule out each of these possibilities. For example, if $d$ is rational, then $(d\sqrt{6})^2 = 6d^2 = 5$, which is impossible because $\sqrt{5/6}$ is not rational (because $6x^2 - 5$ is irreducible over $\mathbb{Q}$, by the Eisenstein criterion with $p = 5$). By three more similar arguments: $\sqrt{5}$ cannot be written in the form (*), so $[K : \mathbb{Q}] = 8$. Since $K/\mathbb{Q}$ is normal and has degree 8, $G := G(K/\mathbb{Q})$ has 8 elements. We are going to show that it is isomorphic to $C_2 \times C_2 \times C_2$. We can write $K$ as $\mathbb{Q}(\sqrt{2}, \sqrt{3})(\sqrt{5})$ so there is an automorphism $\sigma_3$ of $K$ reducing to the identity on $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $\sigma_3(\sqrt{5}) = -\sqrt{5}$. Similarly, there exist automorphisms $\sigma_1$ and $\sigma_2$ of $K$ with

$$
\begin{align*}
\sigma_1 &: \begin{cases} 
\sqrt{2} &\mapsto -\sqrt{2} \\
\sqrt{3} &\mapsto +\sqrt{3} \\
\sqrt{5} &\mapsto +\sqrt{5}
\end{cases} \\
\sigma_2 &: \begin{cases} 
\sqrt{2} &\mapsto +\sqrt{2} \\
\sqrt{3} &\mapsto -\sqrt{3} \\
\sqrt{5} &\mapsto +\sqrt{5}
\end{cases} \\
\sigma_3 &: \begin{cases} 
\sqrt{2} &\mapsto +\sqrt{2} \\
\sqrt{3} &\mapsto +\sqrt{3} \\
\sqrt{5} &\mapsto -\sqrt{5}
\end{cases}
\end{align*}
$$

Since an automorphism of $K/\mathbb{Q}$ is uniquely determined by its action on the generators $\sqrt{2}, \sqrt{3}, \sqrt{5}$, it is easy to check that

$$
\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = e,
$$

that the $\sigma_i$ commute, and that

$$
\{e, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3\}
$$
are distinct automorphisms of $K/Q$. Since there are only 8 automorphisms, these are all of them, which shows that $G(K/Q)$ is the internal direct product of the 2-element subgroups $\{e, \sigma_1\}, \{e, \sigma_2\}, \{e, \sigma_3\}$. The (proper) intermediate fields are in one-one correspondence with the (proper) subgroups of $G \cong C_2 \times C_2 \times C_2$. Since $G$ has 8 elements, the possible orders of proper subgroups are 2 and 4. A 2-element subgroup has the form $\{e, \tau\}$ with $\tau$ an element of $G$ other than the identity, and every subset of this form is a 2-element subgroup. Thus, there are 7 2-element subgroups. If $H$ is a 2-element subgroup, and if $L$ is the fixed field of $H$, then $[K:L] = |H| = 2$, so $[L:Q] = [K:Q]/[K:L] = 4$, so there are 7 intermediate fields of degree 4 over $Q$. It is a straightforward – but tedious – matter to work out the correspondence between $e, \tau$ and the fixed field of $\{e, \tau\}$. To do just one example: Let $\tau = \sigma_1\sigma_2$, and abbreviate $\{e, \tau\}$ by $H$ and the fixed field of $H$ by $L$. Then $\tau(\sqrt{5}) = \sqrt{5}$, and

$$\tau(\sqrt{6}) = \tau(\sqrt{2})\tau(\sqrt{3}) = (\sqrt{2})(\sqrt{3}) = 2\sqrt{3} = \sqrt{6}$$

so $\sqrt{5}$ and $\sqrt{6}$ are in $L$, so $Q(\sqrt{5}, \sqrt{6})$ is an intermediate field contained in $L$ and with degree 4 over $Q$, which is the same as the degree of $L$ over $Q$, so it coincides with $L$: If $H = \{e, \sigma_1\sigma_2\}$ then $K^H = Q(\sqrt{5}, \sqrt{6})$. The fixed fields of the other 6 2-element subgroups can be worked out similarly. The question of 4-element subgroups: By the same sort of degree calculation done above, the fixed field of any 4-element subgroup has degree 2 over $Q$, i.e., is a quadratic extension of $Q$. Given any two distinct elements $\tau_1, \tau_2$ of $G \setminus \{e\}$, $\{e, \tau_1, \tau_2, \tau_1\tau_2\}$ is a 4-element subgroup, and every 4-element subgroup has this form. The number of two element subsets of $G \setminus \{e\}$ is $(7 \cdot 6)/2 = 21$. Each 4-element subgroup has 3 different labelings by 2-element subsets; for example, $\{\sigma_1, \sigma_2\}$, $\{\sigma_1, \sigma_1\sigma_2\}$, $\{\sigma_2, \sigma_1\sigma_2\}$ give the same 4-element subgroup $\{e, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$. Thus, the number of 4-element subgroups is $21/3 = 7$. On the other hand, the 7 elements

$$\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}$$

generate distinct degree-2 subfields of $K$, so these are all of them. Again, the concrete correspondence between 4-element subgroups and quadratic intermediate fields can be worked out in a routine way. For example, if $H = \{e, \sigma_1\sigma_2, \sigma_1\sigma_3\}$, then $\sqrt{5}$ is in the fixed field of $H$ so – “by counting dimensions” – the fixed field of $H$ is $Q(\sqrt{5})$.

**Exercise 9:** *(*) Let $K$ be a normal extension of $Q$ such that $G(K/Q)$ is isomorphic to $C_2 \times C_2$ (where $C_2$ denotes the cyclic group of order 2.) Show that $K$ can be written as $Q(\sqrt{a}, \sqrt{b})$ with $a, b$ rational. (More precisely: Show that $K = Q(\alpha, \beta)$, with $\alpha^2 (= a)$ and $\beta^2 (= b)$ rational.)

**Solution:** Since the Galois group of $K/Q$ has 4 elements, $[K:Q] = 4$. A group isomorphic to $C_2 \times C_2$ can be written as $\{e, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$ with

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^2 = e.$$ 

Corresponding to the subgroup $\{e, \sigma_1\}$ is a intermediate field not equal to $Q$ or $K$. This intermediate field must have degree 2 over $Q$, so it must have the form $Q(\alpha)$ with $\alpha^2 \in Q$. Similarly, the fixed field for $\sigma_2$ must have the form $Q(\beta)$ with $\beta^2 \in Q$. The intersection of $Q(\alpha)$ and $Q(\beta)$ is a proper subfield of $Q(\alpha)$, so can only be $Q$, so $\beta \notin Q(\alpha)$,
so $\mathbb{Q}(\alpha, \beta)$ – which is contained in $K$ – also has degree 4 over $\mathbb{Q}$ so is equal to $K$.

**Exercise 9:** (⋆) Let $K$ be a normal extension of $\mathbb{Q}$ such that $G(K/\mathbb{Q})$ is isomorphic to $C_2 \times C_2$ (where $C_2$ denotes the cyclic group of order 2.) Show that $K$ can be written as $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b$ rational. (More precisely: Show that $K = \mathbb{Q}(\alpha, \beta)$, with $\alpha^2 (= a)$ and $\beta^2 (= b)$ rational.)

**Solution:** Since the Galois group of $K/\mathbb{Q}$ has 4 elements, $[K : \mathbb{Q}] = 4$. A group isomorphic to $C_2 \times C_2$ can be written as $\{e, \sigma_1, \sigma_2, \sigma_1 \sigma_2\}$ with

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1 \sigma_2)^2 = e.$$ 

Corresponding to the subgroup $\{e, \sigma_1\}$ is a intermediate field not equal to $\mathbb{Q}$ or $K$. This intermediate field must have degree 2 over $\mathbb{Q}$, so it must have the form $\mathbb{Q}(\alpha)$ with $\alpha^2 \in \mathbb{Q}$. Similarly, the fixed field for $\sigma_2$ must have the form $\mathbb{Q}(\beta)$ with $\beta^2 \in \mathbb{Q}$. The intersection of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ is a proper subfield of $\mathbb{Q}(\alpha)$, so can only be $\mathbb{Q}$, so $\beta \notin \mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha, \beta)$ – which is contained in $K$ – also has degree 4 over $\mathbb{Q}$ so is equal to $K$.

**Exercise 9:** (⋆) Convince yourself that $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ is a normal extension and figure out what its Galois group is.

1. Find the orbit of $i + \sqrt{2}$ under the action of $G(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$.
2. Find – using Galois theory – the monic minimal polynomial for $i + \sqrt{2}$ over $\mathbb{Q}$.

**Solution:** The Galois group is generated by two automorphisms, one of which maps $i$ to $-i$ leaving $\sqrt{2}$ fixed, and the other of which maps $\sqrt{2}$ to $-\sqrt{2}$ leaving $i$ fixed.

1. Hence the orbit of $\zeta := i + \sqrt{2}$ is

$$\{i + \sqrt{2}, i - \sqrt{2}, -i + \sqrt{2}, -i - \sqrt{2}\} = \{\zeta_1, \zeta_2, \zeta_3, \zeta_4\}$$

2. The minimal polynomial of $\zeta$ is given by

$$(x - \zeta_1)(x - \zeta_2)(x - \zeta_3)(x - \zeta_4)$$

i.e., the product of linear factors over the orbit. Now

$$(x - (i - \sqrt{2}))(x - (i - \sqrt{2})) = (x - i)^2 - (\sqrt{2})^2 = x^2 - 2ix - 1 - 2 = x^2 - 2ix - 3,$$

and

$$(x - (-i + \sqrt{2}))(x - (-i - \sqrt{2})) = (x + i)^2 - 2 = x^2 + 2i - 3,$$

so the minimal polynomial is

$$(x - i - \sqrt{2})(x - i + \sqrt{2})(x + i - \sqrt{2})(x + i + \sqrt{2})$$

$$= (x^2 - 2ix - 3)(x^2 + 2i - 3) = (x^2 - 3)^2 - (2ix)^2$$

$$= x^4 - 6x^2 + 9 + 4x^2 = x^4 - 2x^2 + 9$$

\[\text{(⋆)} = \text{easy}, \ (⋆⋆) = \text{medium}, \ (⋆⋆⋆) = \text{challenge}\]