1. (a) (2 points). What is the minimal polynomial of \( \sqrt[3]{2} \) over \( \mathbb{Q} \)? \( x^3 - 2 \)

(b) (10 points). Let \( u = (\sqrt[3]{2})^2 + \sqrt[3]{2} \).
What is the minimal polynomial of \( u \) over \( \mathbb{Q} \)? \( x^3 - 6x - 6 \)

(c) (3 points). Is \( \mathbb{Q}(u) = \mathbb{Q}(\sqrt[3]{2}) \)? Explain. Yes: The degree of \( \mathbb{Q}(\sqrt[3]{2}) \) over \( \mathbb{Q} \) is a prime number, so by the product formula, any subfield \( \neq \mathbb{Q} \) can only be \( \mathbb{Q}(\sqrt[3]{2}) \).

(d) (5 points). Do there exist \( a_0, a_1, a_2 \in \mathbb{Q} \) for which \( \sqrt[3]{2} = a_0 + a_1u + a_2u^2 \)? Yes because every element of \( \mathbb{Q}(u) \) is of this form, and \( \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(u) \) (that last equation is the previous exercise).

2. (a) (5 points). Let \( K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \). Write down a basis of \( K \) as a vector space over \( \mathbb{Q} \) (it suffices to give just the answer, no proof is necessary). A basis is \( \sqrt{2}^i \sqrt{3}^j \sqrt{5}^k \) for all \( i, j, k \in \{0, 1\} \) (so this basis has \( 2^3 = 8 \) elements).

(b) (2 points). What is \( [K : \mathbb{Q}] \)? 8

(c) (2 points). What is \( [K : \mathbb{Q}(\sqrt{2})] \)? We can use the product formula to find that this equals \( 8/2 = 4 \).

(d) (2 points). What is \( [K : K] \)? That’s always 1.

(e) (4 points). Let \( u = 2\cos(\frac{2\pi}{9}) \). The minimal polynomial over \( \mathbb{Q} \) is \( x^3 - 3x + 1 \). Use this information to explain why \( u \not\in K \). If \( u \in K \) then \( \mathbb{Q}(u) \subseteq K \) but then the degree of \( \mathbb{Q}(u) \) (which is 3) would, by the product formula, divide the degree of \( K \) (which is 8).

(f) (5 points). Can you write \( \frac{1}{u} = a_0 + a_1u + a_2u^2 \) for some \( a_0, a_1, a_2 \in \mathbb{Q} \)? Yes because all elements of \( \mathbb{Q}(u) \) are of this form, and \( 1/u \in \mathbb{Q}(u) \) since in a field we can divide by non-zero elements.

3. Suppose \( F \subset K \subset L \) are fields, and suppose that \( 1, \alpha, \alpha^2 \) is a basis of \( K \) as a vector space over \( F \). Suppose also that \( 1, \beta \) is a basis of \( L \) as a vector space over \( K \). Then write down (no proofs are necessary here) a basis of \( L \) as a vector space over \( F \).

\( \alpha^i\beta^j \) with \( i \in \{0, 1, 2\} \) and \( j \in \{0, 1\} \).

4. Compute the minimal polynomial of \( \sqrt{2} + \sqrt{3} \) over \( \mathbb{R} \). \( x - \sqrt{2} - \sqrt{3} \).

5. Compute the minimal polynomial of \( \sqrt[3]{2} + \sqrt[3]{3} \) over \( \mathbb{Q}(\sqrt[3]{3}) \). \( (x - \sqrt[3]{3})^2 - 2 \) (it is OK if you expand this but it is not necessary).

6. Compute the minimal polynomial of \( \sqrt{2} + \sqrt{3} \) over \( \mathbb{Q} \). \( x^4 - 10x^2 + 1 \).
7. If \( u = \sqrt{2} + \sqrt{3} \) then what is \( [\mathbb{Q}(u) : \mathbb{Q}] \)? This is 4 by the previous exercise. Now prove or disprove \( \mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). The left side is a subfield of the right side, but both have the same degree, namely 4, so they are equal.

8. Let \( \alpha \) be a root of the irreducible polynomial \( x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x] \). What is \( [\mathbb{Q}(\alpha) : \mathbb{Q}] \)? Answer: 4. Simplify \( \alpha^4 \) and \( \alpha^5 \) to elements of the form \( \sum_{i=0}^{3} a_i \alpha^i \) for some \( a_i \in \mathbb{Q} \).

\( \alpha^3 - \alpha^2 - \alpha - 1 \) and 1.

Now let \( \beta = \alpha + \alpha^4 \). Compute \( 1, \beta, \beta^2 \) and simplify them to the form \( \sum_{i=0}^{3} a_i \alpha^i \).

\( 1, -1 - \alpha^2 - \alpha^3, 2 + \alpha^2 + \alpha^3 \)

Now find the minimal polynomial of \( \beta \) over \( \mathbb{Q} \).

\[ x^2 + x - 1. \]

9. If \( F \subseteq K \subseteq L \) are fields and if \( [F : L] = 7 \) (there was a typo here in the original handout) then prove that \( K \) is either \( F \) or \( L \). It follows from the product rule that \( [F : K] \cdot [K : L] = 7 \) and thus either \( [F : K] = 1 \) (then \( F = K \)) or \( [K : L] = 1 \) (then \( K = L \)).

10. (a) (5 points). Let \( K = \mathbb{Q}(\sqrt[6]{-3}) \). Write down a basis of \( K \) as a vector space over \( \mathbb{Q} \) (it suffices to give just the answer, no proof is necessary).

If \( \alpha = \sqrt[6]{-3} \) then this basis is \( 1, \alpha, \ldots, \alpha^5 \).

(b) (3 points). What is \( [K : \mathbb{Q}] \)? 6

(c) (3 points). What is \( [K : \mathbb{Q}(\sqrt[6]{3})] \)? \( 6/2 = 3 \).

Note: \( \sqrt[6]{-3} \in K \) because it is the cube of \( \sqrt[6]{3} \) which is in \( K \).

(d) (3 points). What is \( [K : K] \)? 1

(e) (3 points). What is the minimal polynomial of \( \sqrt[6]{-3} \) over \( \mathbb{Q} \)?

\[ x^6 + 3 \]

(f) (3 points). What is the minimal polynomial of \( \sqrt[6]{-3} \) over \( \mathbb{Q}(\sqrt[6]{-3}) \)?

\[ x^3 - \sqrt[6]{-3} \]

(g) (5 points). Let \( f(x) \in \mathbb{Q}[x] \) be an irreducible polynomial of degree 4. Explain why \( f(x) = 0 \) has no solutions in \( K \).

If \( u \) is a root of \( f \) then \( \mathbb{Q}(u) \) has degree 4, which does not divide 6, the degree of \( K \), so \( \mathbb{Q}(u) \) can not be contained in \( K \), so \( u \) can not be in \( K \).

(h) (5 points). Is \( K \) a normal extension of \( \mathbb{Q} \)? Explain.

Yes, because all roots of \( x^6 + 3 \) are in \( K \). Namely, let \( \zeta_6 = (1 + \sqrt[6]{-3})/2 \in K \) then the 6 roots are powers of \( \zeta_6 \) times \( \sqrt[6]{-3} \).
11. True or false? If true, give some explanation, if false, give a counter example.

(a) If \( f(x) \) and \( g(x) \) have the same splitting field, must \( f(x) \) and \( g(x) \) then have the same roots?

\[ \text{No, for instance, take } f = x^2 - 2 \text{ and } g = x^2 - 8, \text{ they have the same splitting field but not the same roots.} \]

(b) If \( f(x) \in \mathbb{R}[x] \) then the splitting field of \( f(x) \) over \( \mathbb{R} \) can only be \( \mathbb{R} \) or \( \mathbb{C} \).

That is true.

12. Let \( u \) be some number for which \( u^3 - 3u + 1 = 0 \).

(a) What is the minimal polynomial of \( u^2 \) over \( \mathbb{Q} \)?

\[ x^3 - 6x^2 + 9x - 1 \]

(b) \( u \) and \( u^2 - 2 \) are two of the three solutions of \( x^3 - 3x + 1 = 0 \).

Use this information to factor \( x^3 - 3x + 1 \) over \( \mathbb{Q}(u) \) (i.e. factor \( x^3 - 3x + 1 \) in \( \mathbb{Q}(u)[x] \)).

\[ (x - u)(x - u^2 + 2)(x + u^2 - u - 2) \]

To find that third factor, divide the first two away (there is a quicker way that I’ll explain in class).

(c) The splitting field of \( x^3 - 3x + 1 \) over \( \mathbb{Q} \) has degree \( \ldots \) over \( \mathbb{Q} \).

Degree 3 because \( \mathbb{Q}(u) \) contains all three roots.

13. (a) Suppose that \( u \) is a number with minimal polynomial \( x^3 - x - 1 \) over \( \mathbb{Q} \). Let \( v = u^2 \). What is the minimal polynomial of \( v \) over \( \mathbb{Q} \)?

(b) Is \( \mathbb{Q}(u) \) equal to \( \mathbb{Q}(v) \)? Explain.

(c) Let \( w \) be a solution of the polynomial \( x^3 - x - 2 \). Now \( [\mathbb{Q}(u) : \mathbb{Q}] = 3 \) and \( [\mathbb{Q}(w) : \mathbb{Q}] = 3 \). It turns out that \( x^3 - x - 1 \) (the minimal polynomial of \( u \)) has no solutions in \( \mathbb{Q}(w) \). Show that this implies that \( \mathbb{Q}(u) \) can not be isomorphic to \( \mathbb{Q}(w) \).

(showing the weaker statement that \( \mathbb{Q}(u) \) can not be equal to \( \mathbb{Q}(w) \) is enough to get full credit. Hint: You have to somehow use the information that \( x^3 - x - 1 = 0 \) has no solutions in \( \mathbb{Q}(w) \) because without this information you can not prove what is asked).

(d) (5 bonus). Explain that the above information implies that \( x^3 - x - 2 \) (the minimal polynomial of \( w \)) can not have solutions in \( \mathbb{Q}(u) \). You may use the fact that \( \mathbb{Q}(u) \) and \( \mathbb{Q}(w) \) both have degree
3 over \( \mathbb{Q} \) but are not isomorphic (even if you did not prove this fact).

14. (a) True or false: If the minimal polynomial of \( u \) over \( \mathbb{Q} \) has degree \( n \) then \([\mathbb{Q}(u) : \mathbb{Q}]\) must be equal to \( n \).

(b) What is the splitting field of \( x^5 - 1 \) over \( \mathbb{Q} \)?
What is the degree of this splitting field over \( \mathbb{Q} \)? (hint: the irreducible factors of \( x^5 - 1 \) are \( x - 1 \) and \( x^4 + x^3 + x^2 + x + 1 \)).

(c) Let \( \zeta \) denote a root of \( x^4 + x^3 + x^2 + x + 1 \). Let \( u = \zeta + \zeta^4 \).
We have \([\mathbb{Q}(\zeta) : \mathbb{Q}] = 4\), \( \zeta \not\in \mathbb{R} \), \( u \in \mathbb{R} \) and \( u \not\in \mathbb{Q} \). Use this information to prove that \([\mathbb{Q}(u) : \mathbb{Q}] = 2\).

(d) Compute the minimal polynomial of \( u \) over \( \mathbb{Q} \).

(e) What is the splitting field of \( x^5 - 2 \) over \( \mathbb{Q} \)?
What is the degree of this splitting field over \( \mathbb{Q} \)?

15. (a) (5 bonus). Prove that if \( F \) is a field, and if \( S \) is the set of solutions of the equation \( x^4 = 1 \) in \( F \), that then \( ab \in S \) for every \( a, b \in S \).

(b) (5 bonus). Must such \( S \) always be a group under multiplication? Explain.

(c) (10 points). Compute all solutions of the equation \( x^4 = 1 \) in \( \mathbb{Z}_{13} \) (so compute \( S \) for the case \( F = \mathbb{Z}_{13} \)).

16. Find a polynomial with integer coefficients that has \( 2 + \sqrt{3} \) as a root.