MATD01 Fields and Groups
Assignment 5
Solutions

1.

(a) Let $\alpha \in K$ be root of $f(x)$. We show that α is a repeated root of $f(x)$ if and only if $f'(\alpha) = 0$. Indeed, since α is a root of $f(x)$, there is $g(x) \in K[x]$ such that $f(x) = (x - \alpha)g(x)$. Then
$$f'(x) = g(x) + (x - \alpha)g'(x).$$
Substituting α for x we see that $f'(\alpha) = 0$ if and only if $g(\alpha) = 0$. On the other hand, $g(\alpha) = 0$ if and only if $(x - \alpha) \mid g(x)$. We leave it to the reader to check that $(x - \alpha) \mid g(x)$ is equivalent to $(x - \alpha)^2 \mid f(x)$.

(b) The polynomial $f'(x) = 1$ has no roots in any extension of $\mathbb{F}_p$, so that $f(x)$ cannot have a repeated root in any extension of $\mathbb{F}_p$. Since $f(x)$ is monic and splits over K, we have
$$f(x) = (x - \alpha_1) \cdots (x - \alpha_{\deg(f(x))})$$
for some $\alpha_1, \ldots, \alpha_{\deg(f(x)} \in K$. Since $f(x)$ has no repeated roots in K, the α_i ($1 \leq i \leq \deg(f(x))$) are distinct.

(c) Suppose $f(x)$ has a repeated root α is some extension K of F. Then $f'(\alpha) = 0$. Since $f(x)$ is irreducible and has α as a root, it follows that $f(x) \mid f'(x)$. (Indeed, $f(x)$ generates the kernel of the map $F[x] \longrightarrow K$ given by $g(x) \mapsto g(\alpha)$ - see Question 3(b) of Assignment 3.) Writing $f'(x) = f(x)g(x)$, comparing degrees (and in view of the fact that the degree of $f'(x)$ is less than the degree of f), it follows that $g(x) = 0$ and hence, $f'(x) = 0$.

If F has characteristic zero, then $f'(x) \neq 0$ for any irreducible $f(x)$ (as $\deg(f(x)) > 0$). It follows that $f(x)$ has no repeated roots.

2.

(a) true (why?)

(b) True. Indeed, $F(\alpha_1, \ldots, \alpha_n)$ is a subfield of K which contains F and $\alpha_1, ..., \alpha_{n-1}$, hence it contains $F(\alpha_1, \ldots, \alpha_{n-1})$. Combining with $\alpha_n \in F(\alpha_1, \ldots, \alpha_n)$, we get that
$$F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) \subset F(\alpha_1, \ldots, \alpha_n).$$
On the other hand, $F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ is a subfield of K which contains α_n and $F(\alpha_1, \ldots, \alpha_{n-1})$, hence α_n, F, and $\alpha_1, \ldots, \alpha_{n-1}$. It follows that
$$F(\alpha_1, \ldots, \alpha_n) \subset F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n).$$

(c) The equivalence of (i) and (ii) is clear: $F(\alpha)$ is a field so that (i) implies (ii). Conversely, if $F[\alpha]$ is a field, then it is a subfield of K that contains F and α, hence $F(\alpha) \subset F[\alpha]$. The inclusion $F[\alpha] \subset F(\alpha)$ is always true (any subring of K containing F and α contains $F[\alpha]$).

We now establish equivalence of (ii) and (iii). Recall that if R is any PID, an ideal of R is maximal and nonzero if and only if it is prime and nonzero. If R is not a field, then zero is not a maximal ideal of R. Thus if R is a PID which is not a field, then an ideal I of R is maximal if and only if it is prime and nonzero. Apply this to $R = F[x]$ and $I = \ker(ev_\alpha)$ where $ev_\alpha : F[x] \longrightarrow K$ is the evaluation (at α) map $f(x) \mapsto f(\alpha)$. It follows that

$$\ker(ev_\alpha) \text{ is nonzero and prime if and only if it is maximal.} \tag{1}$$

On the other hand, the first isomorphism theorem gives an isomorphism

$$F[x]/\ker(ev_\alpha) \longrightarrow Im(ev_\alpha) = F[\alpha].$$

Being a subring of a field, $F[\alpha]$ is an integral domain, so that $F[x]/\ker(ev_\alpha)$ is an integral domain as well. Hence $\ker(ev_\alpha)$ is a prime ideal of $F[x]$. Combining with Eq. (1) (since primality of $\ker(ev_\alpha)$ is automatic), we get that

$$\ker(ev_\alpha) \text{ is nonzero if and only if it is maximal.} \tag{2}$$

The first statement in Eq. (2) is equivalent to (iii), while the second statement holds if and only if $F[x]/\ker(ev_\alpha)$ (or equivalently, $F[\alpha]$) is a field.

Finally, we turn our attention to the equivalence of (iii) and (iv). Let us first show that (iii) implies (iv). Let α be algebraic over F. Let $g(x) \in F[x]$ be the minimal polynomial of α over F. Thus $g(x)$ is monic, irreducible (in $F[x]$), and generates the kernel of $ev_\alpha : F[x] \longrightarrow K$. Let $n = \deg(g(x))$. We have an isomorphism

$$F[x]/(g(x)) \longrightarrow F[\alpha] = F(\alpha) \qquad \overline{f(x)} \mapsto f(\alpha), \tag{3}$$

where $\overline{f(x)} = f(x) + (g(x))$ is the image of $f(x)$ in $F[x]/(g(x))$ under the quotient map. Note that this isomorphism of rings is also an isomorphism of vector spaces over F (make sure you understand this sentence and agree with it; in particular, how is $F[x]/(g(x))$ considered as a vector space over F?). The set $\{\overline{x}^j : 0 \leq j < n\}$ is a basis of $F[x]/(g(x))$ as a vector space over F. Indeed, given any $f(x) \in F[x]$, let $r(x)$ be the remainder of $f(x)$ in division by $g(x)$. Then $r(x)$ is an F-linear combination of $\{x^j : 0 \leq j < n\}$, so that $\overline{r(x)}$ is an F-linear combination of $\{\overline{x}^j : 0 \leq j < n\}$ (if $r(x) = \sum_{j=0}^{n-1} a_j x^j$, then $\overline{r(x)} = \sum_{j=0}^{n-1} a_j \overline{x}^j$). Moreover, $\overline{f(x)} = \overline{r(x)}$ (why?). This shows that $\{\overline{x}^j : 0 \leq j < n\}$ spans $F[x]/(g(x))$ as a vector space over F. For linear independence, note that if $\sum_{j=0}^{n-1} a_j \overline{x}^j = 0$ for some $a_0, ...a_{n-1} \in F$, then

$$\overline{\sum_{j=0}^{n-1} a_j x^j} = 0$$

in $F[x]/(g(x))$, which means $\sum_{j=0}^{n-1} a_j x^j \in (g(x))$. Since $g(x)$ has degree n, it follows that $\sum_{j=0}^{n-1} a_j x^j = 0$, i.e. all the a_j are zero.

We have established that $\{\overline{x}^j : 0 \leq j < n\}$ is a basis of $F[x]/(g(x))$ as a vector space over F. In view of the isomorphism Eq. (3), $\{\alpha^j : 0 \leq j < n\}$ is a basis of $F(\alpha)$ as a vector space over F. In particular, $F(\alpha)$ is an n-dimensional vector space over F, i.e. $[F(\alpha) : F] = n$.

What remains is to show that (iv) implies (iii). This is easy: if $F(\alpha)$ is a finite extension of F, say of degree n, then the elements α^j $(0 \leq j \leq n)$ must be F-linearly dependent (why?), i.e. there must be $a_0, ..., a_n \in F$, not all zero, such that $\sum_{j=0}^{n} a_j \alpha^j = 0$. Then α is a root of the nonzero polynomial $\sum_{j=0}^{n} a_j x^j \in F[x]$.

3.

(a) By Eisenstein criterion for prime 3, the polynomial is irreducible in $\mathbb{Q}[x]$. The polynomial is primitive (i.e. the gcd of its coefficients is 1) so it is also irreducible in $\mathbb{Z}[x]$.

(b) Irreducible by Eisenstein criterion for prime p. (Remark: Corollary 42 of Rotman is incorrect as stated, e.g. $x^n - b^n$ is not irreducible for any $b \in \mathbb{Z}$ and $n > 1$.)

(c) (i) is irreducible since it is of degree 2 and with no rational roots (use the quadratic formula). (Note: Let $a \in \mathbb{Z}$. By Problem 63 of Rotman, every rational root of $x^n - a$ is actually an integer. This $\sqrt[n]{a}$ is rational if and only if it is an integer, i.e. if and only if $a = b^n$ for some $b \in \mathbb{Z}$.)

(ii) $6x^3 - 3x - 18$ is irreducible over $\mathbb{Q}[x]$ if and only if $2x^3 - x - 6$ is. Being of degree 3, the latter is irreducible if and only if it has no rational roots. By Problem 63, the rational roots of $2x^3 - x - 6$ must be of the forms (1) an integer a dividing 6, and (2) $a/2$ with $a = \pm 1, \pm 3$. A simple check shows that none of these are roots of $2x^3 - x - 6$.

(iii) The degree is 3 so we only need to check if the polynomial has any roots in $\mathbb{Q}$. In view of Problem 63 the only candidates for a root are ± 1, neither of which is a root. Thus the polynomial is indeed irreducible.

(d) In view of Gauss lemma (Theorem 39), it is enough to show that $f(x)$ cannot be expressed as $g(x)h(x)$ for any $g(x), h(x) \in \mathbb{Z}[x]$ of positive degree. If one of the factors is of degree 1, then $f(x)$ has a rational root. In view of Problem 63, the only possible rational roots of $f(x)$ are ± 1. Neither of these is a root.

Now we will argue that $f(x)$ does not factor as a product of two polynomials in $\mathbb{Z}[x]$ of degree > 1. If it does, the two factors must both be of degree 2. Suppose

$$x^4 - 10x^2 + 1 = (ax^2 + bx + c)(a'x^2 + b'x + c')$$

with $a, b, c, a', b', c' \in \mathbb{Z}$. Comparing the coefficients of x^4 on the two sides we get $aa' = 1$, so $a = a' = \pm 1$. We may assume that $a = a' = 1$ (if necessary, multiple the two factors by -1). Comparing the coefficients of x^3 (resp. the constant terms) we get $b' + b = 0$ (resp. $c = c' = \pm 1$). Thus our factorization looks like

$$x^4 - 10x^2 + 1 = (x^2 + bx + c)(x^2 - bx + c), \quad \text{where } c = \pm 1.$$

Comparing coefficients of x^2 we get $-b^2 \pm 2 = -10$, so that $b^2 \in \{8, 12\}$. But $b \in \mathbb{Z}$ so this is absurd.

(e) By Gauss lemma it is enough to show that the polynomial $f(x) = x^3 + 70000x + 4000$ does not factor in $\mathbb{Z}[x]$ as a product of two polynomials of positive degree. For this, it is enough to show that the polynomial is irreducible after passing to $\mathbb{F}_7[x]$. Reducing mod 7, we get the polynomial

$$x^3 + 3 \in \mathbb{F}_7[x].$$

This polynomial is irreducible as it is of degree 3 and has no root in $\mathbb{F}_7$. Indeed, for any nonzero $\alpha \in \mathbb{F}_7$, we have

$$(\alpha^3)^2 = \alpha^6 \overset{\text{why?}}{=} 1,$$

so that $\alpha^3 = \pm 1$ (the only solutions to $x^2 - 1 = 0$ in the field $\mathbb{F}_7$ are ± 1).

REMARK. (1) Checking irreducibility of a given polynomial over a finite field is usually easier than that over $\mathbb{Z}$. In the worst case scenario, it can always be done brute-force in a finite number of operations. After all, there are only finitely many polynomials of bounded degree with coefficients in a finite field.

(2) The original polynomial in this question was $x^3 + 70000x + 4$. For that polynomial, the only candidates for a rational root are $\pm 1, \pm 2, \pm 4$. None of those is a root so the polynomial has no rational root and being of degree 3, it is irreducible in $\mathbb{Q}[x]$.

(f) $x^9 - 13$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein crieterion with $p = 13$. We will show that $x^9 - 13$ is not irreducible in $\mathbb{F}_{29}[x]$. In fact, $x^9 - 13$ has a root in $\mathbb{F}_{29}$. Consider the map $\psi : \mathbb{F}_{29}^\times \longrightarrow \mathbb{F}_{29}^\times$ given by $\alpha \mapsto \alpha^9$. This is a group homomorphism. Its kernel consists of those $\alpha \in \mathbb{F}_{29}$ which satisfy $\alpha^9 = 1$. This is equivalent to the order of α (as an element of $\mathbb{F}_{29}^\times$) dividing 9. Since the order of every element of $\mathbb{F}_{29}^\times$ divides $|\mathbb{F}_{29}^\times| = 28$, it follows that $\ker(\psi) = \{1\}$. Thus ψ is injective, and hence surjective (why?). In particular, there is $\alpha \in \mathbb{F}_{29}$ such that $\alpha^9 = 13$.

(g) Recall that in a ring of characteristic prime p, the map $r \mapsto r^p$ is a ring homomorphism. Applying this to $\mathbb{F}_p[x]$, we have

$$(x^{p^2} + 2x^p + x + 3)^p = x^{p^3} + 2^p x^{p^2} + x^p + 3^p = x^{p^3} + 2x^{p^2} + x^p + 3$$

(recall that $a^p = a$ for any $a \in \mathbb{F}_p$). Thus the given polynomial is not irreducible.

(h) Same as Part (g). (In any field F of characteristic p with its prime field denoted by F_0, one has $a^p = a$ for any element a of F_0. This is because one has a (unique) isomorphism $\mathbb{F}_p \simeq F_0$.)

4.

(a) First we recall a few facts from group theory. Let G be a group, with the operation written in multiplicative notation and the identity denoted by e. Recall that for any $g \in G$, the order of g, usually denoted by $|g|$, is defined as follows:

- if there is a positive integer n such that $g^n = e$, then $|g|$ is defined to be the smallest such n;
- otherwise, i.e. if there is no positive integer n such that $g^n = e$, then we define $|g| := \infty$.

If $|g| = n$, then for any integer a one has $g^a = e$ if and only if $n \mid a$. More generally, $g^a = g^b$ if and only if $a \equiv b \pmod{n}$. The subgroup $\langle g \rangle := \{g^k : k \in \mathbb{Z}\}$ has then exactly n distinct elements, namely

$$g^k \qquad (1 \le k \le n)$$

(or k coming from any complete set of residues mod n). If $|g| = \infty$, then the elements g^k ($k \in \mathbb{Z}$) are all distinct, and $\langle g \rangle$ has infinitely many elements. In either case $|\langle g \rangle| = |g|$.

Suppose $|g|$ is finite. There is a formula that relates the order of a power of g to the order of g:

$$|g^k| = \frac{|g|}{gcd(|g|, k)}.$$

In particular,$|g^k|$ divides $|g|$, and moreover $|g^k| = |g|$ if and only if $gcd(|g|, k) = 1$. Since $\langle g \rangle$ is finite and $\langle g^k \rangle \leq \langle g \rangle$, we have $\langle g^k \rangle = \langle g \rangle$ if and only if $|\langle g^k \rangle| = |\langle g \rangle|$, i.e. if and only if $|g^k| = |g|$. Thus g^k is a generator of the cyclic group $\langle g \rangle$ if and only if $gcd(|g|, k) = 1$. In particular, if G is a cyclic group of order n generated by g, then G has exactly $\varphi(n)$ (= the number of positive integers $\leq n$ which are relatively prime to n) generators, namely the elements

$$g^k \qquad (1 \leq k \leq n,\ gcd(n, k) = 1).$$

Now back to the homework question. The group μ_n of the n-roots of unity (i.e. 1) in $\mathbb{C}$ is a cyclic group of order n, generated by $e^{2\pi i/n}$. It has $\varphi(n)$ generators

$$e^{2\pi ik/n} \qquad (1 \leq k \leq n,\ gcd(n, k) = 1).$$

These are the primitive n-th roots of unity.

(b) For simplicity, let us write ζ for ζ_n. First note that since K_n contains every root of $x^n - 1$, in particular, it contains ζ. Therefore, being a subfield of $\mathbb{C}$ which contains ζ (and $\mathbb{Q}$), the field K_n contains $\mathbb{Q}(\zeta)$. On the other hand, every complex root of $x^n - 1$ is power of ζ, hence belongs to $\mathbb{Q}(\zeta)$. Thus $x^n - 1$ splits over the field $\mathbb{Q}(\zeta)$. It follows that $K_n = \mathbb{Q}(\zeta)$. (By definition of K_n, the polynomial $x^n - 1$ does not split over any proper subfield of K_n.)

(c) We go through $1 \leq n \leq 9$ one by one. In each case, we write ζ for a primitive n-th root of unity.

- $n = 1 :$ $\mu_1 = \{1\}$, $\zeta = 1$, and the minimal polynomial of ζ is $x - 1$.
- $n = 2 :$ $\mu_2 = \{1, -1\}$, the only primitive root is $\zeta = -1$, and its minimal polynomial is $x + 1$.
- $n = 3 :$ We have $x^3 - 1 = (x - 1)(x^2 + x + 1)$. Since $\zeta \neq 1$, it is a root of $x^2 + x + 1$. This polynomial is irreducible in $\mathbb{Q}[x]$ (why?) and hence is the minimal polynomial of ζ (over $\mathbb{Q}$).
- $n = 4 :$ We have $x^4 - 1 = (x^2 - 1)(x^2 + 1)$. Since $\zeta^2 \neq 1$ (why?), it follows that ζ is a root of $x^2 + 1$. This polynomial is irreducible in $\mathbb{Q}[x]$ (why?) and hence is the minimal polynomial of ζ.
- $n = 5 :$ $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ and ζ is a root of $x^4 + x^3 + x^2 + x + 1$. The polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$ (recall that $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Q}[x]$ if p is prime). Hence it is the minimal polynomial of ζ.
- $n = 6 :$ We have $x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$. Since ζ is a primitive 6th root of unity, it is not a root of $x^3 - 1$ or $x + 1$, and hence must be a root of $x^2 - x + 1$. This polynomial is irreducible over $\mathbb{Q}$ (why?) and hence is the minimal polynomial of ζ.
- $n = 7 :$ This is similar to $n = 5$ case. The minimal polynomial is $\frac{x^7 - 1}{x - 1} = x^6 + x^5 + \cdots + x + 1$.
- $n = 8 :$ We have $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. Since ζ is a primitive 8th root of unity, it must be a root of $x^4 + 1$. We claim that $x^4 + 1$ is irreducible in $\mathbb{Q}[x]$

(and hence is the minimal polynomial of ζ). Indeed, use the same trick as the one used when we proved irreducibility of $\frac{x^p-1}{x-1}$: since the map $\mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]$ defined by $f(x) \mapsto f(x+1)$ is an isomorphism, we can equivalently show that $(x+1)^4+1$ is irreducible. The constant term of $(x+1)^4+1$ is 2 and its leading coefficient is 1, so we can hope that Eisenstien criterion with $p=2$ might apply. Let us calculate the coefficients of $(x+1)^4+1$ mod 2. Of course, the exponent here is small enough that one can just expand and see that the intermediate coefficients are all even (they are 4,6,4), so Eisenstein criterion for prime 2 indeed applies and $(x+1)^4+1$ (and hence x^4+1) is irreducible. But let us try to avoid expanding $(x+1)^4+1$.
Working mod 2, since 2 is a prime number and 4 is a power of 2, we have

$$(x+1)^4+1 = ((x+1)+1)^4 = (x+2)^4 = x^4. \tag{4}$$

Thus the coefficients of$(x+1)^4+1$ are indeed all multiples of 2, except for the leading coefficient. (See the remark below for a more detailed explanation.)

REMARK. Here is a more expanded version of the calculation of the coefficients of $f(x)=(x+1)^4+1$ mod 2. What we are doing is the following: we are calculating the image of $f(x)$ under the map $\mathbb{Z}[x] \longrightarrow \mathbb{F}_2[x]$ which reduces the coefficients mod 2; in other words, in the notation of your textbook (see page 38), the image of $f(x)$ under the map $\pi^*: \mathbb{Z}[x] \longrightarrow \mathbb{F}_2[x]$, where $\pi: \mathbb{Z} \longrightarrow \mathbb{F}_2$ is the quotient map (= reduction mod 2 map). The key ingredients are that (i) π^* is a ring map, and (ii) since the characteristic of $\mathbb{F}_2[x]$ is 2 and prime, the map $\mathbb{F}_2[x] \longrightarrow \mathbb{F}_2[x]$ given by $g(x) \mapsto g(x)^2$ is a ring homomorphism. Since a composition of ring homomorphisms is a ring homomorphism, the map $\mathbb{F}_2[x] \longrightarrow \mathbb{F}_2[x]$ given by $g(x) \mapsto g(x)^{2^k}$ is a ring homomorphism for any k.
The polynomial $(x+1)^4+1$ in Eq. (4) is an element of $\mathbb{F}_2[x]$; it is the image of $(x+1)^4+1 \in \mathbb{Z}[x]$ under π^*. Here we used the fact that π^* is a ring map:

$$\pi^*((x+1)^4+1) = (\pi^*(x+1))^4 + \pi^*(1) = (x+1)^4+1$$

(where the first occurrence of $(x+1)^4+1$ in the last line is an element of $\mathbb{Z}[x]$ and the second an element of $\mathbb{F}_2[x]$). The fact that $\mathbb{F}_2[x]$ is of characteristic 2 and (4 is a power of 2) implies that in $\mathbb{F}_2[x]$,

$$(x+1)^4+1 = ((x+1)+1)^4.$$

The rest of the computation in Eq. (4) is clear. In the end, we have obtained that

$$\pi^*((x+1)^4+1) = x^4.$$

On recalling the definition of π^* (which reduces the coefficients mod 2), we conclude that the coefficient of x^4 in $(x+1)^4+1 \in \mathbb{Z}[x]$ is 1 mod 2 while the other coefficients are all 0 mod 2.

– $n=9:$ We have $x^9-1=(x^3-1)(x^6+x^3+1)$. Every primitive 9th root of unity must be a root of x^6+x^3+1. We show that x^6+x^3+1 is irreducible (and hence the minimal polynomial of any primitive 9th root of unity). Let's see if the same trick as before works: consider

$$(x+1)^6+(x+1)^3+1.$$

The constant term is 3 so we are hoping that we can apply Eisenstein criterion for prime 3. Working mod 3, since 3 is a prime number, we have

$$(x+1)^6 + (x+1)^3 + 1 = ((x+1)^2 + (x+1) + 1)^3 = (x^2 + 3x + 3)^3 = x^6.$$

Thus the coefficients of $(x+1)^6 + (x+1)^3 + 1$ are all divisible by 3, except the leading coefficient which is 1 mod 3. Eisenstein criterion for $p = 3$ indeed applies. (Make sure you are okay with the last few lines of the argument starting with "working mod 3". See the remark in $n = 8$ case.)
For all $1 \leq n \leq 9$, the degree of the minimal polynomial of ζ is $\varphi(n)$, so that $[K_n : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ (by Problem 2). We shall see later that this is in fact true for all n.

REMARK. Note that for each $1 \leq n \leq 9$, the primitive n-th roots of unity have the same minimal polynomial over $\mathbb{Q}$ (that is, for each n, the minimal polynomial is the same for all primitive n-th roots of unity). More precisely, for each n above, this minimal polynomial factors over $\mathbb{C}$ as

$$\prod_{|\zeta|=n} (x - \zeta),$$

where the product is over the primitive n-th roots of unity in $\mathbb{C}$. We shall see later that this is in general true for any positive integer n.

(d) Since the minimal polynomial of ζ_9 over $\mathbb{Q}$ (i.e $x^6 + x^3 + 1$) has degree 6, by the argument given in the solution to Problem 2 the elements ζ_9^j $(0 \leq j \leq 5)$ form a basis of $\mathbb{Q}(\zeta_9)$ (= K_9) over $\mathbb{Q}$.

(e) Let ζ be a primitive n-th root of unity (here n is an arbitrary positive integer). Let $g(x)$ be the minimal polynomial of ζ over $\mathbb{Q}$. Since $K_n = \mathbb{Q}(\zeta)$, in view of Problem 2, we have $[K_n : \mathbb{Q}] = \deg(g(x))$. We shall show that $\deg(g(x)) \leq \varphi(n)$.

Since ζ is a root of $x^n - 1$ and $g(x)$ is the minimal polynomial of ζ, we have $g(x) \mid x^n - 1$ (make sure you agree with this!). Let $\alpha \in \mathbb{C}$ be a root of $g(x)$. It follows from $g(x) \mid x^n - 1$ that α is also a root of $x^n - 1$, i.e. α is an n-th root of unity. In fact, we claim that α must be a primitive n-th root of unity, for if $\alpha^k = 1$ for some $1 \leq k < n$, then the minimal polynomial of α, which is $g(x)$ (why?), must divide $x^k - 1$. But then ζ will also be a root of $x^k - 1$, contradicting the fact that it is a primitive n-th root of unity.

We have proved that any complex root of $g(x)$ is a primitive n-th root of unity. Since $g(x)$ has no repeated roots (why?) and it splits over $\mathbb{C}$, we have

$$\begin{aligned} \deg(g(x)) &= \text{the number of distinct roots of } g(x) \text{ in } \mathbb{C} \\ &\leq \text{the number of primitive } n\text{-th roots of unity in } \mathbb{C} \\ &= \varphi(n). \end{aligned}$$

REMARK. Here we proved that every root of $g(x)$ is a primitive n-th root of unity. To prove that $\deg(g(x)) = \varphi(n)$, we would also need to prove that every primitive n-th root of unity is a root of $g(x)$.

5.

(a) Writing ζ instead of ζ_n for simplicity, the roots of $x^n - 2$ in $\mathbb{C}$ are the numbers $\alpha\zeta^j$ ($0 \leq j < n$) (and we have $x^n - 2 = \prod_{0 \leq j < n} (x - \alpha\zeta^j)$). The splitting field K contains all these roots, so that it contains α and ζ (why ζ?). Thus $\mathbb{Q}(\alpha, \zeta) \subset K$. On the other hand, $x^n - 2$ already splits over $\mathbb{Q}(\alpha, \zeta)$, hence $\mathbb{Q}(\alpha, \zeta) = K$.

(b) Firstly, it is clear that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta)$ are both contained in $K = \mathbb{Q}(\alpha, \zeta)$ (do you agree?). We want to show that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\zeta)$ are both proper subfield of K. By Eisenstien criterion with $p = 2$, the polynomial $x^n - 2$ is irreducible over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Combining with our first observation that $\mathbb{Q}(\alpha) \subset K$ it follows that $[K : \mathbb{Q}] \geq n$ (remember from linear algebra that if W is a subspace of V, then $\dim(W) \leq \dim(V)$). We know from Part (e) of the previous question that $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq \varphi(n) < n$ (since $n > 1$), so that $\mathbb{Q}(\zeta) \neq K$.

To see that $\mathbb{Q}(\alpha) \neq K$, first let us work with a specific n-th root of 2, namely a real n-th root of 2, which we denote by α_0. Since α_0 is real, we have $\mathbb{Q}(\alpha_0) \subset \mathbb{R}$. Since $n \geq 3$, some of the n-th roots of 2 are not real, so that $K \not\subset \mathbb{R}$. Thus $\mathbb{Q}(\alpha_0) \neq K$. Since $\mathbb{Q}(\alpha_0) \subsetneq K$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, we have $[K : \mathbb{Q}] > n$. Now for any n-th root α of 2, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, so that $\mathbb{Q}(\alpha) \neq K$.