MATD01 Fields and Groups
Assignment 7
Solutions

1. Let $f(x) = x^n - \alpha$. Suppose

$$f(x) = \prod_{i=1}^{n}(x - \beta_i),$$

in $K[x]$. Since α is nonzero, each β_i is nonzero. Then

$$\prod_{i=1}^{n}(x - \frac{\beta_i}{\beta_1}) = \frac{1}{\beta_1^n}\prod_{i=1}^{n}(\beta_1 x - \beta_i) = \frac{1}{\alpha}\cdot f(\beta_1 x) = \frac{(\beta_1 x)^n - \alpha}{\alpha} = \frac{\alpha x^n - \alpha}{\alpha} = x^n - 1,$$

so that $x^n - 1$ splits over K.

2. (a) We have

$$F \ \subset\ F(\alpha)\ \subset\ F(\alpha,\beta) = F(\alpha)(\beta). \tag{1}$$

Let f be the minimal polynomial of β over F. Then $\deg(f) = [F(\beta) : F] = n$. The minimal polynomial of β over $F(\alpha)$ divides f (why?), hence its degree is at most n. Thus $[F(\alpha)(\beta) : F(\alpha)] \le n$ (why?). The degree formula applied to the extensions Eq. (1) gives the result.

(b) By the degree formula applied to Eq. (1) and $F \subset F(\beta) \subset F(\alpha,\beta)$ we see that both m and n divide $[F(\alpha,\beta) : F]$. Since m and n are relatively prime, it follows that mn divides $[F(\alpha,\beta) : F]$. Combining with Part (a) we get $[F(\alpha,\beta) : F] = mn$.

(c) By Problem 1, K contains a splitting field of $x^p - 1$ over $\mathbb{Q}$. Let $\alpha \in K$ be a root of $x^p - 2$ and $\zeta \in K$ a primitive p-th root of unity (see the remark below). Then $K = F(\alpha,\zeta)$ (why?). The minimal polynomials of α and ζ over $\mathbb{Q}$ are respectively $x^p - 2$ (irreducible by Eisenstein) and the p-th cyclotomic polynomial; they are respectively of degrees p and $p - 1$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Since p is a prime, p and $p - 1$ are relatively prime. By Part (b), $[\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}] = p(p-1)$.

REMARK. Let L be an extension of $\mathbb{Q}$ in which $x^n - 1$ splits. Then the group of n-th roots of unity in L is cyclic of order n. At this stage of the course, we can see this by using the fact that every two splitting fields of $x^n - 1$ are $\mathbb{Q}$ are isomorphic. Indeed, let $L' \subset L$ be a splitting field of $x^n - 1$ over $\mathbb{Q}$. Then the group of n-th roots of unity in L' is the same as the group of n-th roots of unity in L. Now L' is isomorphic to the splitting field of $x^n - 1$ over $\mathbb{Q}$ in $\mathbb{C}$. In the latter field we know the group of n-th roots of unity is cyclic of order n.

Soon we shall see that any finite subgroup of the multiplicative group of units of a field is cyclic. This means that for any n, the group of n-th roots of unity in any field is cyclic. Since $x^n - 1$ has no repeated roots in characteristic zero (just look at the derivative), in any splitting field it has n roots and those roots form a cyclic group of order n.

(d) Let $f(x)$ be the minimal polynomial of ζ_p over $\mathbb{Q}(\sqrt[p]{2})$. Applying the degree formula to

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[p]{2}) \subset \mathbb{Q}(\sqrt[p]{2}, \zeta_p) = \mathbb{Q}(\sqrt[p]{2})(\zeta_p),$$

in view of Part (c) we get

$$\deg(f(x)) = [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}(\sqrt[p]{2})] = \frac{[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}]} = p - 1.$$

Since $\sum\limits_{i=0}^{p-1} x^i$ is in $\mathbb{Q}[x] \subset \mathbb{Q}(\sqrt[p]{2})[x]$ and vanishes at ζ_p, we have $f(x) \bigm| \sum\limits_{i=0}^{p-1} x^i$. Comparing degrees and leading coefficients we see that $f(x) = \sum\limits_{i=0}^{p-1} x^i$. Thus $\sum\limits_{i=0}^{p-1} x^i$ is irreducible over $\mathbb{Q}(\sqrt[p]{2})$.

The argument for irreducibility of $x^p - 2$ over $\mathbb{Q}(\zeta_p)$ is similar and we leave it to the reader. (Now you will be looking at $\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\sqrt[p]{2}, \zeta_p) = \mathbb{Q}(\zeta_p)(\sqrt[p]{2})$.)

3. (a) Let α be the real root of $x^3 - 4$. Let ω be a primitive 3rd root of 1 in $\mathbb{C}$. Then $K = \mathbb{Q}(\alpha, \omega)$ (why?). The polynomial $x^3 - 4$ has no rational roots (as being monic with integral coefficients any rational root of it is an integer (Exercise 63 of Rotman), and $x^3 - 4$ has no roots in $\mathbb{Z}$). Being of degree 3, $x^3 - 4$ is thus irreducible over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. On the other hand, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ (why?), which implies $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] \leq 2$ (why?). Since $\mathbb{Q}(\alpha) \subset \mathbb{R}$ and $\mathbb{Q}(\alpha, \omega) \not\subset \mathbb{R}$, we must have $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$. By the degree formula,

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 6.$$

(b) We have $x^4 - 4 = (x^2 - 2)(x^2 + 2)$. The roots of $x^4 - 4$ are $\pm\sqrt{2}, \pm i\sqrt{2}$. We have $K = \mathbb{Q}(\sqrt{2}, i)$ and

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

(Why is $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$?)

(c) We have $K = \mathbb{Q}(\sqrt[6]{2}, \zeta)$, where $\sqrt[6]{2}$ is a real 6th root of 2 and ζ a primitive 6th root of unity. Since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(6) = 2$, we have $[\mathbb{Q}(\sqrt[6]{2}, \zeta) : \mathbb{Q}(\sqrt[6]{2})] \leq 2$. Since $\mathbb{Q}(\sqrt[6]{2})$ is real and $\mathbb{Q}(\sqrt[6]{2}, \zeta)$ is not, $\mathbb{Q}(\sqrt[6]{2}) \neq \mathbb{Q}(\sqrt[6]{2}, \zeta)$. Thus $[\mathbb{Q}(\sqrt[6]{2}, \zeta) : \mathbb{Q}(\sqrt[6]{2})] = 2$. By the degree formula

$$[\mathbb{Q}(\sqrt[6]{2}, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}, \zeta) : \mathbb{Q}(\sqrt[6]{2})] \cdot [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 2 \cdot 6 = 12.$$

($[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ because $x^6 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein criterion.)

(d) In $\mathbb{F}_5[x]$, we have

$$x^{10} - 2 = (x^2 - 2)^5$$

so that any splitting field of $x^{10} - 2$ over $\mathbb{F}_5$ is also a splitting field of $x^2 - 2$ over $\mathbb{F}_5$. Let $\sqrt{2}$ denote one of the roots of $x^2 - 2$ in K. Then $K = \mathbb{F}_5(\sqrt{2})$. Note that 2 is not a square in $\mathbb{F}_5$, so that $x^2 - 2$ has no root in $\mathbb{F}_5$. Thus $x^2 - 2$ is irreducible over $\mathbb{F}_5$ and $[\mathbb{F}_5(\sqrt{2}) : \mathbb{F}_5] = 2$.

(e) Let α be a root of $x^5 - 2 = x^5 + 1$, i.e. $\alpha^5 = -1$. Then $(-\alpha)^5 = 1$, so that $-\alpha$ is a root of $x^5 - 1$. Conversely, if β is a root of $x^5 - 1$, then $-\beta$ is a root of $x^5 + 1$. It follows that K is also a splitting field of $x^5 - 1$ over $\mathbb{F}_3$.

Let $f(x) = x^5 - 1$. Note that f has no repeated roots. Indeed, the only root of $f'(x) = 5x^4$ is zero, which is not a root of f. Let μ_5 be the set of roots of f in K. Then μ_5 is a subgroup of $K^\times$ (as the set of n-th roots of unity in any field F forms a subgroup of $F^\times$), and has order 5 (because f splits in K and has no repeated roots). Take an element $\zeta \in \mu_5$ with $\zeta \neq 1$. Then $1 \neq |\zeta| \mid |\mu_5| = 5$. Since 5 is a prime number, we get $|\zeta| = 5$, so that μ_5 is cyclic and generated by ζ. It follows that $K = \mathbb{F}_3(\zeta)$.
Let $d = [\mathbb{F}_3(\zeta) : \mathbb{F}_3]$. We have

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$

so ζ is a root of $x^4 + x^3 + x^2 + x + 1$. Thus $d \leq 4$ (why?). We shall show that in fact, $d = 4$. Indeed, since μ_5 is a subgroup of $\mathbb{F}_3(\zeta)^\times$, by Lagrange's theorem $|\mu_5| \mid |\mathbb{F}_3(\zeta)^\times|$. That is, $5 \mid 3^d - 1$ (since $|\mathbb{F}_3(\zeta)| = 3^d$). Combining with $d \leq 4$ we easily see that the only possibility is $d = 4$.

4. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ be the minimal polynomial of α over K. Let $F' = F(a_0, ..., a_n)$. Then α is algebraic over F' (why?), so that $F'(\alpha)$ is a finite extension of F'. On the other hand, since K/F is algebraic, every a_i is algebraic over F, hence F' is a finite extension of F. By the degree formula, $F'(\alpha)$ is a finite extension of F, and hence an algebraic extension of F. In particular, $\alpha \in F'(\alpha)$ is algebraic over F.

5. (a) Since α and β are algebraic over F, the extension $F(\alpha, \beta)/F$ is finite and hence algebraic. Thus every element of $F(\alpha, \beta)$, and in particular, the elements $\alpha\beta, \alpha + \beta$ and $1/\alpha$, are algebraic over F.
That

$$K := \{\alpha \in L : \alpha \text{ is algebraic over } F\}$$

is a subfield is now immediate: K contains ± 1 and is closed under addition, multiplication, and taking multiplicative inverses for nonzero elements.
It is clear that K contains F (every $a \in F$ is a root of $x - a \in F[x]$). Also, by definition, every element of K is algebraic over F, so that K is an algebraic extension of F

(b) Let

$$K := \{\alpha \in \mathbb{R} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

Let n be any positive integer. Let $\sqrt[n]{2}$ be a real root of $x^n - 2$. Then $\sqrt[n]{2} \in K$. Consider the subfield $\mathbb{Q}(\sqrt[n]{2})$ of K. By Eisenstein criterion, $x^n - 2$ is irreducible over $\mathbb{Q}$, so that $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Since $\mathbb{Q}(\sqrt[n]{2}) \subset K$, it follows that $\dim_{\mathbb{Q}}(K) \geq n$ (where $\dim_{\mathbb{Q}}(K)$ means the dimension of K as a vector space over $\mathbb{Q}$). Since this is true for all n, it follows that $\dim_{\mathbb{Q}}(K)$ is infinite.

(c) By (a) we know $\overline{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$. Take a polynomial $f \in \overline{\mathbb{Q}}[x] \subset \mathbb{C}[x]$ of positive degree. Since $\mathbb{C}$ is algebraically closed, f has a root α in $\mathbb{C}$. Then α is algebraic over $\overline{\mathbb{Q}}$. Since $\overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$, in view of Problem 4 it follows that α is algebraic over $\mathbb{Q}$. Hence α belongs to $\overline{\mathbb{Q}}$.

6. (a) False
(b) False
(c) True

(d) False
(e) True
(f) True