MATD01 Fields and Groups

Assignment 9

Solutions

1. (i) $\Rightarrow$ (ii): Let $\alpha_1, \ldots, \alpha_n$ be a basis of K over F. Then $K = F(\alpha_1, \ldots, \alpha_n)$. For each i, let f_i be the minimal polynomial of α_i over F. Then the f_i split over K (why?), and K is a splitting field of $\prod_{i=1}^{n} f_i$ over F (why?).

(ii) $\Rightarrow$ (i): Suppose K is a splitting field of $g \in F[x]$ over F. Let $f \in F[x]$ be an irreducible polynomial with a root $\alpha \in K$. We will show that f splits over K. Let L be a splitting field of f over K. Then L is a splitting field of fg over F (why?). Now let β be an arbitrary root of f in L. We will be done if we show that β is in K. Consider the tower of fields $F \subset K \subset L$. Since K is the splitting field of some polynomial over F, any element of $Gal(L/F)$ maps K onto K. Since L is a splitting field over F and f is irreducible over F, the action of $Gal(L/F)$ on the set of roots of f in L is transitive; thus there is an element $\sigma \in Gal(L/F)$ such that $\sigma(\alpha) = \beta$. Since $\sigma(K) \subset K$ and $\alpha \in K$, we have $\beta = \sigma(\alpha) \in K$.

2. Suppose $\alpha \in K$ is fixed by every element of $Gal(K/F)$. Let f be the minimal polynomial of α over F. We need to show that f has degree 1. By Problem **1.** , f splits over K. Since K/F is separable, f has no repeated roots. Suppose f has degree > 1. Then f has another root $\beta \neq \alpha$ in K. Since K is a splitting field over F and f is irreducible over F, there is an element $\sigma \in Gal(K/F)$ which sends α to β. This contradicts the assumption that α is fixed by every element of $Gal(K/F)$.

Remark: A normal separable extension is called a Galois extension.

3. Note that $K = \mathbb{Q}(\alpha, i)$. Every element of $Gal(K/\mathbb{Q})$ sends α to one of the four roots of $x^4 - 2$ (= the minimal polynomial of α over $\mathbb{Q}$), and i to one of $\pm i$ (= roots of $x^2 + 1$, the minimal polynomial of i over $\mathbb{Q}$). Thus we have a function

$$(1) \qquad Gal(K/\mathbb{Q}) \longrightarrow \{\alpha,\, i\alpha,\, -\alpha,\, -i\alpha\} \times \{i, -i\} \quad \sigma \mapsto (\sigma(\alpha), \sigma(i)),$$

which is injective since every element of $Gal(K/\mathbb{Q})$ is determined by its action on α and i (as $K = \mathbb{Q}(\alpha, i)$). Since $|Gal(K/\mathbb{Q})| = [K : \mathbb{Q}] = 8$ (you can see $[K : \mathbb{Q}] = 8$ easily by earlier techniques, first adjoining a real root of $x^4 - 2$ to $\mathbb{Q}$), the function Eq. (1) is in fact a bijection. As a subgroup of the symmetric group on $\{\alpha,\, i\alpha,\, -\alpha,\, -i\alpha\}$, thus $Gal(K/\mathbb{Q})$ consists of the following elements:

- Id (fixing both α and i)
- $(\alpha i \;\; -\alpha i)$ (this is the element that fixes α and sends $i \mapsto -i$),
- $(\alpha \;\; \alpha i \;\; -\alpha \;\; -\alpha i)$ (this is the element that sends $\alpha \mapsto \alpha i$ and fixes i),
- $(\alpha \;\; \alpha i)(-\alpha \;\; -\alpha i)$ (this is the element that sends $\alpha \mapsto \alpha i$ and $i \mapsto -i$)
- $(\alpha \;\; -\alpha)(\alpha i \;\; -\alpha i)$ (sending $\alpha \mapsto -\alpha$ and fixing i)
- $(\alpha \;\; -\alpha)$ (sending $\alpha \mapsto -\alpha$ and $i \mapsto -i$)
- $(\alpha \;\; -\alpha i \;\; -\alpha \;\; \alpha i)$ (sending $\alpha \mapsto -\alpha i$ and fixing i)
- $(\alpha \;\; -\alpha i)(-\alpha \;\; \alpha i)$ (sending $\alpha \mapsto -\alpha i$ and $i \mapsto -i$).

4. (a) Note that $K = \mathbb{Q}(\alpha, \zeta)$. Every element of $Gal(K/\mathbb{Q})$ sends α to one of $\alpha\zeta^i$ $(0 \le i \le 6)$ (why?), and ζ to one of ζ^i $(1 \le i \le 6)$ (why?). Thus we have a function

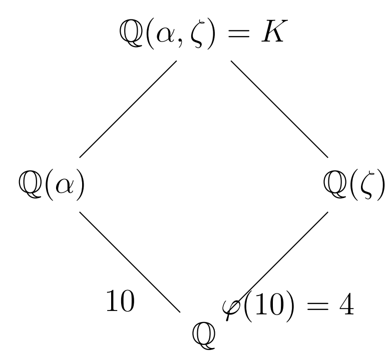
(2) $$Gal(K/\mathbb{Q}) \longrightarrow \{\alpha\zeta^i : 0 \le i \le 6\} \times \{\zeta^i : 1 \le i \le 6\} \qquad \sigma \mapsto (\sigma(\alpha), \sigma(\zeta)),$$

which is injective since every element of $Gal(K/\mathbb{Q})$ is determined by its action on α and ζ (why?). We leave it to the reader to check that $[K : \mathbb{Q}] = 42$ (see Problem 2 of Assignment 7). Thus $|Gal(K/\mathbb{Q})| = 42$ (why?). It follows that the function Eq. (2) is in fact a bijection. The element of $Gal(K/\mathbb{Q})$ which sends $\alpha \mapsto \alpha\zeta$ and fixes ζ is easily seen to be δ, and the element which fixes α and sends $\zeta \mapsto \zeta^3$ is easily seen to be τ. Thus $\langle\delta, \tau\rangle \subset Gal(K/\mathbb{Q})$. To show that $\langle\delta, \tau\rangle = Gal(K/\mathbb{Q})$, first note that $(\mathbb{Z}/7\mathbb{Z})^\times = \langle 3\rangle$ (verify this). Now given $0 \le i \le 6$ and $1 \le j \le 6$, let r be such that $3^r \equiv j \pmod 7$; then one easily checks that $\delta^i\tau^r$ maps $\alpha \mapsto \alpha\zeta^i$ and $\zeta \mapsto \zeta^j$. (Does this show that every element of $Gal(K/\mathbb{Q})$ is generated by δ and τ?)

We now show that $Gal(K/\mathbb{Q}(\zeta)) = \langle\delta\rangle$. Indeed, $Gal(K/\mathbb{Q}(\zeta))$ is the subgroup of $Gal(K/\mathbb{Q})$ which fixes $Q(\zeta)$, or equivalently fixes ζ. Thus $\delta \in Gal(K/\mathbb{Q}(\zeta))$, so that $\langle\delta\rangle \subset Gal(K/\mathbb{Q}(\zeta))$. Now note that both $\langle\delta\rangle$ and $Gal(K/\mathbb{Q}(\zeta))$ have 7 elements. (Why is $|Gal(K/\mathbb{Q}(\zeta))| = 7$?)

(b) We have $\delta\tau(\alpha) = \alpha\zeta$ and $\tau\delta(\alpha) = \alpha\zeta^3$. Thus $\delta\tau \ne \tau\delta$ and $Gal(K/\mathbb{Q})$ is not abelian. Hence K is not contained in any cyclotomic extension of $\mathbb{Q}$. (If L is a cyclotomic extension of $\mathbb{Q}$, then $Gal(L/\mathbb{Q})$ is abelian. If further we have $\mathbb{Q} \subset K \subset L$, then (since both K and L are normal extension of $\mathbb{Q}$) we have a natural surjection $Gal(L/\mathbb{Q}) \longrightarrow Gal(K/\mathbb{Q})$, and hence $Gal(K/\mathbb{Q})$ would also be abelian.)

5. (a) We may assume that $K \subset \mathbb{C}$. We have a diagram of fields



where the numbers written next to the extensions are their degrees (justify them). We leave it to the reader to argue that

$$20 = lcm(10, 4) \mid [K : \mathbb{Q}] \le 40,$$

so that $[K : \mathbb{Q}]$ is either 20 or 40. The goal is to show that $[K : \mathbb{Q}] = 40$.

We will prove that

(3) $$\sqrt{5} \in \mathbb{Q}(\zeta).$$

Before we prove this, let us see how it will help us to show that $[K : \mathbb{Q}] = 40$. Suppose $[K : \mathbb{Q}] = 20$. Then $[K : \mathbb{Q}(\zeta)] = 5$. Let h be the minimal polynomial of α

over $\mathbb{Q}(\zeta)$. Then h is monic of degree 5 and it divides

$$f(x) = \prod_{i=0}^{9}(x - \alpha\zeta^i).$$

It follows that h is the product of 5 of the factors $x - \alpha\zeta^i$. Considering the constant term of h, we see that $\alpha^5 \in \mathbb{Q}(\zeta)$ (as the constant term of h is α^5 times a power of ζ), so that $\sqrt{2} \in \mathbb{Q}(\zeta)$. Combining with (3), we get $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subset \mathbb{Q}(\zeta)$. We leave it to the reader to show that there are no rational numbers a, b such that $a + b\sqrt{2} = \sqrt{5}$ (square both sides and use linear independence of 1 and $\sqrt{2}$ over $\mathbb{Q}$). This implies $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$ (why?), so that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \overset{why?}{=} 2 \cdot 2 = 4.$$

Combining with $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subset \mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ we get $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\zeta)$, which is absurd since $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subset \mathbb{R}$ and $\mathbb{Q}(\zeta) \not\subset \mathbb{R}$.

Now we turn our attention to the task of proving (3). Let $\lambda = \zeta + 1/\zeta = \zeta + \overline{\zeta}$ (bar standing for complex conjugation). Let us find the minimal polynomial g of λ over $\mathbb{Q}$. Since $\mathbb{Q}(\zeta)$ is a splitting field over $\mathbb{Q}$, (i) the polynomial g splits over $\mathbb{Q}(\zeta)$ (Problem 1) and (ii) the Galois group $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts transitively on the set of roots of g (the numbering of these two statements is for future referencing in the argument). Recall that we have an isomorphism

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/10\mathbb{Z})^\times$$

given by $\sigma \mapsto i$, where $\sigma(\zeta) = \zeta^i$ (Theorem 69 and its proof together with $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(10)$, see Problem 2 of Assignment 6). The group $(\mathbb{Z}/10\mathbb{Z})^\times$ is cyclic generated by 3, so that $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic and generated by the element τ satisfying $\tau(\zeta) = \zeta^3$. The Galois conjugates of λ over $\mathbb{Q}(\zeta)$ are

$$Id(\lambda) = \lambda = \tau^2(\lambda), \quad \tau(\lambda) = \zeta^3 + 1/\zeta^3 = \tau^3(\lambda).$$

Thus

$$g(x) = (x - \lambda)(x - (\zeta^3 + 1/\zeta^3)) = x^2 - (\zeta + \zeta^3 + \zeta^7 + \zeta^9)x + (\zeta^2 + \zeta^4 + \zeta^6 + \zeta^8).$$

(Here we used the earlier statements (i) and (ii) together with the fact that in characteristic zero irreducible polynomials do not have repeated roots.) Note that

$$a := \zeta + \zeta^3 + \zeta^7 + \zeta^9$$

and

$$b := \zeta^2 + \zeta^4 + \zeta^6 + \zeta^8$$

are respectively the sum of primitive 10th and 5th roots of unity. The 5th and 10th cyclotomic polynomials are

$$\phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

and

$$\phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

It follows that $a = 1$ and $b = -1$ (note that if $x^n + a_{n-1}x^{n-1} + \cdots = \prod_{i=1}^{n}(x - \beta_i)$ then $a_{n-1} = -\sum_{i=1}^{n}\beta_i$). Thus

$$g(x) = x^2 - x - 1,$$

so that

$$\lambda = (1 \pm \sqrt{5})/2.$$

Thus $\sqrt{5} \in \mathbb{Q}(\lambda) \subset \mathbb{Q}(\zeta)$, as claimed.

REMARK. That $\deg(g) = 2$ is easily seen without using Galois theory. Indeed, $\zeta\lambda = \zeta^2 + 1$ so that ζ is a root of $x^2 - \lambda x + 1$. This implies that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\lambda)] \leq 2$. Since $\zeta \notin \mathbb{R}$ and $\lambda \in \mathbb{R}$ (as λ is fixed by complex conjugation), it follows that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\lambda)] = 2$. Combining with $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ by the degree formula we get $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2$. (The same argument show that for $n > 2$, if ζ_n is a primitive n-th root of unity and $\lambda_n = \zeta^n + 1/\zeta^n$, then $[\mathbb{Q}(\lambda_n) : \mathbb{Q}] = \frac{1}{2}[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)/2$.)

(b) Now that we know $|Gal(K/\mathbb{Q})| = 40$, a very similar argument to the one for Part (a) of the previous problem shows that $Gal(K/\mathbb{Q})$ is generated by the two elements

$$\delta = (\alpha \;\; \alpha\zeta \;\; \alpha\zeta^2 \;\; \cdots \;\; \alpha\zeta^9)$$

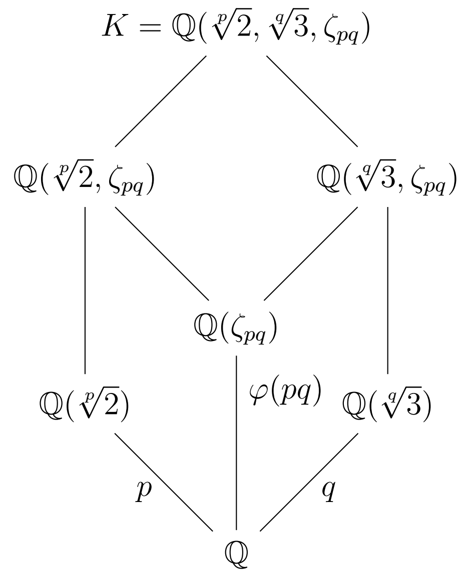
(which sends $\alpha \mapsto \alpha\zeta$ and fixes ζ) and

$$\tau = (\alpha\zeta \;\; \alpha\zeta^3 \;\; \alpha\zeta^9 \;\; \alpha\zeta^7)\,(\alpha\zeta^2 \;\; \alpha\zeta^6 \;\; \alpha\zeta^8 \;\; \alpha\zeta^4)$$

(which fixed α and sends $\zeta \mapsto \zeta^3$). We leave the details to the reader. Things to keep in mind as you give the argument: (i) The conjugates of ζ over $\mathbb{Q}$ (i.e. the roots of the minimal polynomial of ζ over $\mathbb{Q}$) are the primitive 10th roots of unity, i.e. the elements ζ^j with $1 \leq j \leq 9$ and $gcd(j, 10) = 1$ (Assignment 6, Problem 2). (ii) $(\mathbb{Z}/10\mathbb{Z})^\times$ is cyclic and generated by 3.

6. Let K be the splitting field of $(x^p - 2)(x^q - 3)$ over $\mathbb{Q}$ in $\mathbb{C}$. Then $K = \mathbb{Q}(\sqrt[p]{2}, \zeta_p, \sqrt[q]{3}, \zeta_q) = \mathbb{Q}(\sqrt[p]{2}, \sqrt[q]{3}, \zeta_{pq})$ (note that $\mathbb{Q}(\zeta_{pq}) = \mathbb{Q}(\zeta_p, \zeta_q)$ since $\zeta_{pq}^p = \zeta_q$ and $\zeta_p\zeta_q$ is a primitive pq-th root of unity as $\gcd(p + q, pq) = 1$ thanks to p and q being distinct primes).

Let us calculate $[K:\mathbb{Q}]$ first. We have a diagram of fields



(justify the degrees). Looking at the left diamond, since p and $\varphi(pq)=(p-1)(q-1)$ are relatively prime, we have $[\mathbb{Q}(\sqrt[p]{2},\zeta_{pq}):\mathbb{Q}(\zeta_{pq})]=p$ (why?). Similarly, considering the right diamond, since q and $(p-1)(q-1)$ are relatively prime, we get $[\mathbb{Q}(\sqrt[q]{3},\zeta_{pq}):\mathbb{Q}(\zeta_{pq})]=q$. Now considering the top diamond (in view of $gcd(p,q)=1$) we get $[K:\mathbb{Q}(\sqrt[q]{3},\zeta_{pq})]=p$. It follows that $[K:\mathbb{Q}]=pq(p-1)(q-1)$ (why?).

For any $\alpha\in K$, let f_α be the minimal polynomial of α over $\mathbb{Q}$. Denote the set of roots of f_α in K by $C(\alpha)$; since K is a splitting field over $\mathbb{Q}$, this is the same as the set $\{\sigma(\alpha):\sigma\in Gal(K/\mathbb{Q})\}$, and we have

$$f_\alpha(x)=\prod_{\beta\in C(\alpha)}(x-\beta)$$

(because f_α splits over K by Problem 1 and we are in characteristic zero so irreducible polynomials are separable).

There is an injection

$$Gal(K/\mathbb{Q})\longrightarrow C(\sqrt[p]{2})\times C(\sqrt[q]{3})\times C(\zeta_{pq})\qquad \sigma\mapsto(\sigma(\sqrt[p]{2}),\,\sigma(\sqrt[q]{3}),\,\sigma(\zeta_{pq}))$$

(why is this injective?). Both domain and codomain of this map have $pq(p-1)(q-1)$ elements (why?), so that this map is actually a bijection. On recalling that $C(\sqrt[p]{2})=\{\sqrt[p]{2}\zeta_p^r:0\le r<p\}$ and $C(\sqrt[q]{3})=\{\sqrt[q]{3}\zeta_q^r:0\le r<q\}$, it follows that

$$C(\sqrt[p]{2}+\sqrt[q]{3})=\{\sqrt[p]{2}\zeta_p^r+\sqrt[q]{3}\zeta_q^s:\,0\le r<p,\,0\le s<q\}.$$

This gives the desired conclusion.