MATD01 Fields and Groups

Assignment 8

Solutions

1. (a) Since f has coefficients in F, we have $\hat{\sigma}^*(f) = \sigma^*(f)$ (where $\hat{\sigma}^*$ is the map $F(\alpha)[x] \to K'[x]$ induced by $\hat{\sigma} : F(\alpha) \to K'$). Thus

$$\sigma^*(f)(\hat{\sigma}(\alpha)) = \hat{\sigma}^*(f)(\hat{\sigma}(\alpha)) = \hat{\sigma}(f(\alpha)) = \hat{\sigma}(0) = 0.$$

(Make sure you are okay with the second equality.)

(b) Let us first prove existence. Since f is irreducible, it generates the kernel of the evaluation map

$$\phi_1 : F[x] \longrightarrow F(\alpha) \qquad g \mapsto g(\alpha).$$

In view of the first isomorphism theorem, ϕ_1 induces an isomorphism

$$\overline{\phi_1} : F[x]/(f) \;\longrightarrow\; Im(\phi_1) = F(\alpha) \qquad g + (f) \mapsto g(\alpha).$$

Now consider the evaluation map

$$\phi_2 : F'[x] \longrightarrow K' \qquad g \mapsto g(\alpha').$$

Since $\sigma^*(f) \in \ker(\phi_2)$, the map ϕ_2 induces a homomorphism

$$\overline{\phi_2} : F'[x]/(\sigma^*(f)) \;\longrightarrow\; K' \qquad g + (\sigma^*(f)) \mapsto g(\alpha')$$

(see Assignment 3, Question 4). Next, let ψ be the composition

$$F[x] \xrightarrow{\sigma^*} F'[x] \overset{\text{quotient}}{\longrightarrow} F'[x]/(\sigma^*(f)).$$

The kernel of ψ contains f and hence the ideal (f), so that ψ induces a map

$$\overline{\psi} : F[x]/(f) \longrightarrow F'[x]/(\sigma^*(f)) \qquad g + (f) \mapsto \;\psi(g) = \sigma^*(g) + (\sigma^*(f)).$$

Let $\hat{\sigma}$ be the composition

$$F(\alpha) \xrightarrow{\overline{\phi_1}^{-1}} F[x]/(f) \xrightarrow{\overline{\psi}} F'[x]/(\sigma^*(f)) \xrightarrow{\overline{\phi_2}} K'.$$

The given any $\sum_i c_i\alpha^i \in F(\alpha)$ with the c_i in F, setting $g(x) = \sum_i c_i x^i \in F[x]$, we have

$$\hat{\sigma}(\sum_i c_i\alpha^i) = \overline{\phi_2} \circ \overline{\psi} \circ \overline{\phi_1}^{-1}(g(\alpha)) = \overline{\phi_2} \circ \overline{\psi}(g + (f)) = \overline{\phi_2}(\sigma^*(g) + (\sigma^*(f))) = \sigma^*(g)(\alpha') = \sum_i \sigma(c_i)\alpha'^i.$$

In particular, $\hat{\sigma}(\alpha) = \alpha'$ and $\hat{\sigma}(c) = \sigma(c)$ for any $c \in F$. (Note: Irreducibility of f is important because we need $\overline{\phi_1}$ above to be an isomorphism, since we used its inverse in the construction.)

The uniqueness is easier: every element of $F(\alpha)$ can be expressed as a linear combination $\sum_i c_i\alpha^i$ with the c_i in F, and if $\hat{\sigma} : F(\alpha) \to K'$ is any extension of σ, we have

$$\hat{\sigma}(\sum_i c_i\alpha^i) = \sum_i \hat{\sigma}(c_i)\hat{\sigma}(\alpha)^i = \sum_i \sigma(c_i)\hat{\sigma}(\alpha)^i,$$

so that $\hat{\sigma}$ is determined by $\hat{\sigma}(\alpha)$.

(c) True (see the solution to (b))

(d) True. By parts (a) and (b), there is a bijection

$$\{\hat{\sigma} \in Hom(F(\alpha), K') : \hat{\sigma} = \sigma \text{ on } F\} \longrightarrow \{\alpha' \in K' : \sigma^*(f)(\alpha') = 0\}$$

given by

$$\hat{\sigma} \mapsto \hat{\sigma}(\alpha).$$

(e) The minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}$ is $f(x) = x^6 - 2$ (irreducible by Eisenstein criterion). The polynomial f has 6 roots in $\mathbb{C}$, namely the numbers $\sqrt[6]{2}\zeta^j$ $(0 \leq j \leq 5)$ where $\zeta = e^{2\pi i/6}$. Let $\iota : \mathbb{Q} \to \mathbb{C}$ be the inclusion map. By the solution to (d) we have a bijection

$$Hom(\mathbb{Q}(\sqrt[6]{2}), \mathbb{C}) = \{\phi \in Hom(\mathbb{Q}(\sqrt[6]{2}), \mathbb{C}) : \phi = \iota \text{ on } \mathbb{Q}\} \longrightarrow \{\sqrt[6]{2}\zeta^j : 0 \leq j \leq 5\}$$

given by $\phi \mapsto \phi(\sqrt[6]{2})$. Let $\phi_j : \mathbb{Q}(\sqrt[6]{2}) \to \mathbb{C}$ be the map that sends $\sqrt[6]{2}$ to $\sqrt[6]{2}\zeta^j$. Then ϕ_j is given by

$$\sum_{r=0}^{5} c_r \sqrt[6]{2}^r \mapsto \sum_{r=0}^{5} c_r (\sqrt[6]{2}\zeta_j)^r \qquad (c_r \in \mathbb{Q}).$$

(The numbers $\sqrt[6]{2}^r$ $(0 \leq r \leq 5)$ form a basis of $\mathbb{Q}(\sqrt[6]{2})$ over $\mathbb{Q}$.) Out of these maps only ϕ_1 (which is the inclusion map) maps $\mathbb{Q}(\sqrt[6]{2})$ onto itself. (The image of the rest is not contained in $\mathbb{R}$.)

(f) The minimal polynomial of ζ over $\mathbb{Q}$ is of degree $\varphi(n)$, and its roots are the numbers ζ^j with $0 \leq j < n$ and $gcd(j, n) = 1$. We have

$$Hom(\mathbb{Q}(\zeta), \mathbb{C}) = \{\phi_j : 0 \leq j < n, \ gcd(j, n) = 1\},$$

where ϕ_j is the unique map that sends ζ to ζ^j, and is given by the formula

$$\sum_r c_r \zeta^r \mapsto \sum_r c_r \zeta^{jr} \qquad (c_r \in \mathbb{Q}).$$

For any $\phi : \mathbb{Q}(\zeta) \to \mathbb{C}$, we have $Im(\phi) \subset \mathbb{Q}(\zeta)$. Since ϕ is an injective $\mathbb{Q}$-linear map, by rank-nullity $\dim_{\mathbb{Q}}(Im(\phi)) = \dim_{\mathbb{Q}} \mathbb{Q}(\zeta)$. It follows that $Im(\phi) = \mathbb{Q}(\zeta)$. Thus every homomorphism $\mathbb{Q}(\zeta) \to \mathbb{C}$ gives an automorphism $\mathbb{Q}(\zeta)$.

2. (a) We may think of $Gal(L/\mathbb{Q})$ as a subgroup of the symmetric group on the set of roots of f in L. Since f is of degree 3 and has no rational roots, it is irreducible. Being irreducible over a field of characteristic zero, f is separable and has 3 (= $\deg(f)$) distinct roots in L. Thus $Gal(L/\mathbb{Q})$ is isomorphic to a subgroup of S_3. To show $Gal(L/\mathbb{Q}) \simeq S_3$ it is enough to show that $|Gal(L/\mathbb{Q})| = 6$, or equivalently (since L is a splitting field of a separable polynomial), that $[L : \mathbb{Q}] = 6$. Note that since $Gal(L/\mathbb{Q})$ is isomorphic to a subgroup of S_3, we have $[L : \mathbb{Q}] \mid 6$.

Assume $L \subset \mathbb{C}$. Let α be the real root of f (so the other two roots are $\alpha\omega$ and $\alpha\omega^2$, where $\omega = e^{2\pi i/3}$). Since f is irreducible, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. By the degree formula,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3[L : \mathbb{Q}(\alpha)].$$

Combining with $[L:\mathbb{Q}] \bigm| 6$, we see that $[L:\mathbb{Q}]$ is 3 or 6, corresponding to whether $[L:\mathbb{Q}(\alpha)]$ is 1 or 2, respectively. Since $L \neq \mathbb{Q}(\alpha)$ (as $L \not\subset \mathbb{R}$), we have $[L:\mathbb{Q}(\alpha)] > 1$. Thus $[L:\mathbb{Q}] = 6$.

(b) From the above, $[L:\mathbb{Q}(\alpha)] = 2$. Since $L = \mathbb{Q}(\alpha, \omega)$, it follows that $1, \omega$ form a basis of L over $\mathbb{Q}(\alpha)$. On the other hand, since $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$, the elements $1, \alpha, \alpha^2$ form a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. The desired conclusion is now immediate from the proof of the degree formula.

(c) We need to express the image of each element of $\mathcal{B}$ under σ in terms of the basis $\mathcal{B}$. We have

$$\sigma(\omega) = \sigma(\alpha^{-1}\alpha\omega) = \sigma(\alpha)^{-1}\sigma(\alpha\omega) = (\alpha\omega)^{-1}\alpha = \omega^{-1} = -1-\omega,$$
$$\sigma(\alpha^2) = \sigma(\alpha)^2 = \alpha^2\omega^2 = -\alpha^2 - \alpha^2\omega,$$

and

$$\sigma(\alpha^2\omega) = \sigma(\alpha)\sigma(\alpha\omega) = \alpha^2\omega.$$

Ordering the elements of $\mathcal{B}$ as

$$\mathcal{B} = \{1,\, \omega,\, \alpha,\, \alpha\omega,\, \alpha^2,\, \alpha^2\omega\},$$

the matrix of σ is

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{pmatrix}.$$

3. (a) One sees easily using Exercise 63 of Rotman that f has no rational roots. Since $\deg(f) = 3$, it follows that f is irreducible over $\mathbb{Q}$. Since the derivative $f'(x) = 3x^2 + 1$ is positive for all real x, the polynomial f is increasing on $\mathbb{R}$ and hence has exactly one real root (the degree is 3 so we know there is at least one real root). The same argument as in Part (a) of the previous question shows that $[L:\mathbb{Q}] = 6$ and $Gal(L/\mathbb{Q}) \simeq S_3$.
As for whether there is an isomorphism $L \to L$ which acts on the set of roots of f as the permutation $(\alpha\,\beta)$, the answer is yes since $Gal(L/\mathbb{Q})$ is the full symmetric group on the set of roots of f.

(b) α is real while β and γ are not. Let $\sigma \in Gal(L/\mathbb{Q})$ be complex conjugation. Then σ fixes any element λ if and only if λ is real. Thus σ fixes α, and it does no fix β and γ. It follows that $\sigma = (\beta\,\gamma)$.

4. (a) One uses Exercise 63 to see that f has no rational roots and hence is irreducible over $\mathbb{Q}$. Note that $f(-2) < 0$, $f(0) > 0$, $f(1) < 0$, and $f(2) > 0$, so that by the intermediate value theorem f has 3 real roots (and these are all the roots of f in $\mathbb{C}$). So the argument we gave in the previous two problems does not settle the question of whether $[L:\mathbb{Q}]$ is 3 or 6. (Recall that $[L:\mathbb{Q}] = 3$ is equivalent to $Gal(L:\mathbb{Q}) \simeq A_3$, as the only subgroup of order 3 in S_3 is A_3.)

We recall a result from the lectures (stated without proof). Let $char(F) \neq 2, 3$. Suppose $f(x) = x^3 + qx + r \in F[x]$ is irreducible over F, and that L is a splitting field of f over F. Let $R = r^2 + 4q^3/27$. Then $[L:F] = 3$ if and only if $-3R$ is a square in F.

For the polynomial $f \in \mathbb{Q}[x]$ given in this part, $-3R = 9$ is a square in $\mathbb{Q}$, so $[L : \mathbb{Q}] = 3$ and hence $Gal(L/\mathbb{Q}) \simeq A_3$. The transposition $(\alpha\ \beta)$ does not belong to $Gal(L/\mathbb{Q})$.

(b) This time $R = -229/27$ and $-3R$ is not a square in $\mathbb{Q}$ (as 229 is not a square in $\mathbb{Q}$), so that $[L : \mathbb{Q}] = 6$ and $Gal(L/\mathbb{Q}) \simeq S_3$.

5. (a) That $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is clear. We have

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

Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 = 5 + 2\sqrt{6}$. Squaring both sides of $\alpha^2 - 5 = 2\sqrt{6}$ we see that α is a root of $g(x) = x^4 - 10x^2 + 1$. The polynomial g is irreducible over $\mathbb{Q}$, by Exercise 67 of Rotman. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Combining with $\mathbb{Q}(\alpha) \subset L$ (why does this hold?) and $[L : \mathbb{Q}] \leq 4$ it follows that $L = \mathbb{Q}(\alpha)$.

(b) $Gal(L/\mathbb{Q})$ is a subgroup of of order 4 (why) of the symmetric group on the set $\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}$ of roots of f. Every element of $Gal(L/\mathbb{Q})$ must permute $\{\sqrt{2}, -\sqrt{2}\}$ (why?), and similarly must permute $\{\sqrt{3}, -\sqrt{3}\}$. It follows that

$$Gal(L/\mathbb{Q}) \subset \{Id,\ (\sqrt{2}\ \ -\sqrt{2}),\ (\sqrt{3}\ \ -\sqrt{3}),\ (\sqrt{2}\ \ -\sqrt{2})(\sqrt{3}\ \ -\sqrt{3})\}.$$

Combining with $|Gal(L/\mathbb{Q})| = 4$ we see that the inclusion above must actually be equality.

(c) $Gal(L/\mathbb{Q}(\sqrt{6}))$ is the subgroup of $Gal(L/\mathbb{Q})$ consisting of the elements that fix $\mathbb{Q}(\sqrt{6})$. An element of $Gal(L/\mathbb{Q})$ fixes $\mathbb{Q}(\sqrt{6})$ if and only if it fixes $\sqrt{6}$. The elements of $Gal(L/\mathbb{Q})$ that fix $\sqrt{6}$ are Id and $(\sqrt{2}, -\sqrt{2})(\sqrt{3}, -\sqrt{3})$.

(d) The images of $\alpha = \sqrt{2} + \sqrt{3}$ under the action of $Gal(L/\mathbb{Q})$ are α (= Id applied to α), $-\sqrt{2} + \sqrt{3}$ (= $(\sqrt{2}, -\sqrt{2})$ applied to α), $\sqrt{2} - \sqrt{3}$ (= $(\sqrt{3}, -\sqrt{3})$ applied to α), and $-\sqrt{2} - \sqrt{3}$ (= $(\sqrt{2}, -\sqrt{2})(\sqrt{3}, -\sqrt{3})$ applied to α). The numbers $\pm\sqrt{2} \pm \sqrt{3}$ are indeed the four roots of $g(x) = x^4 - 10x^2 + 1$.

Remark: What is happening in this question is not an accident: if L is a splitting field (of some polynomial) over F, and $g \in F[x]$ is an irreducible polynomial with one root in L, then g splits over L and moreover the action of $Gal(L/F)$ on the set of roots of g in L is transitive. (The second assertion is proved in 6(i) below, and is used to prove the first assertion (see Assignment 10, Question 1).)

6. (i) Suppose E is a splitting field of some polynomial in $F[x]$, say g, over F. Let $f \in F[x]$ be an irreducible polynomial. We shall show that the action of $Gal(E/F)$ on the set of roots of f in E is transitive. Indeed, let $\alpha, \beta \in E$ be roots of f. Since f is irreducible over F, by Lemma 50 of Rotman (or Problem 1 of this assignment), there is an isomorphism $\sigma : F(\alpha) \longrightarrow F(\beta)$ which fixes F and sends α to β (in the notation of Lemma 50, σ is $\hat{Id}$ where $Id : F \longrightarrow F$ is the identity map). Note that E is a splitting field of g over $F(\alpha)$ and $F(\beta)$, and $\sigma^*(g) = g$ because $g \in F[x]$ and σ fixes F. By Theorem 51, the isomorphism $\sigma : F(\alpha) \longrightarrow F(\beta)$ extends to an isomorphism $\hat{\sigma} : E \longrightarrow E$. Then $\hat{\sigma} \in Gal(E/F)$ and $\hat{\sigma}(\alpha) = \beta$.

Remark: In this argument we did not assume that E was a splitting field of f.

(ii) Suppose E is again a splitting field of some polynomial over F. Let $f \in F[x]$ be a polynomial which splits over E and such that the action of $Gal(E/F)$

on the set of roots of f in E is transitive. We shall show that if f has no repeated roots, then f is irreducible over F.

Indeed, suppose f is not irreducible. Then $f = gh$ for some $g, h \in F[x]$ with both g and h of positive degree. Since f splits over E, so do g and h. Let α be a root of g and β a root of h. By transitivity of the action of $Gal(E/F)$ on the set of roots of f, there is $\sigma \in Gal(E/F)$ such that $\sigma(\alpha) = \beta$. But $\sigma(\alpha)$ is also a root of g, as α is a root of $g \in F[x]$ and σ fixes F. It follows that β is a root of both of g and h, and hence is a repeated root of f.