MATD01 Fields and Groups

Assignment 8

Due Sunday March 22 at 10:00 pm
(to be submitted on Crowdmark)

Notes: Please write your solutions neatly and clearly. Note that due to time limitations, only some questions will be graded.

1. The goal of this question is to help us feel comfortable with a key result proved in class on Wednesday March 11th. While the main proofs were given in class, you are asked here to reproduce them. You are not allowed to refer to Lemma 50 of Rotman, as that is simply a variant of the same result. (If it helps, read the proof of Lemma 50. But your argument should be self-sufficient and not contain any referrals to Lemma 50 or its proof.)

Here is the setup: We assume that K/F is a field extension, $f \in F[x]$ is an irreducible polynomial, and $\alpha \in K$ is a root of f. Let F' be a field and $\sigma : F \to F'$ a homomorphism. Suppose K' is an extension of F'. We denote by σ^* the map $F[x] \to F'[x]$ induced by σ (defined by $\sigma^*(\sum_i a_i x^i) = \sum_i \sigma(a_i)x^i$). We shall be interested in homomorphisms $\hat{\sigma} : F(\alpha) \to K'$ which extend σ (i.e. such that $\hat{\sigma}(a) = \sigma(a)$ for every $a \in F$).

$$\begin{array}{ccc} F(\alpha) & \overset{\hat{\sigma}}{\dashrightarrow} & K' \\ | & & | \\ F & \xrightarrow{\sigma} & F' \end{array}$$

(a) Suppose $\hat{\sigma} : F(\alpha) \to K'$ is a homomorphism extending σ. Show that $\hat{\sigma}(\alpha)$ is a root of $\sigma^*(f)$. (Note: Irreducibility of f is irrelavent for this part.)

(b) Show that for every root $\alpha' \in K'$ of $\sigma^*(f)$, there is a unique homomorphism $\hat{\sigma} : F(\alpha) \to K'$ which extends σ and sends $\alpha \mapsto \alpha'$. (Irreducibility of f in $F[x]$ is absolutely crucial here.)

(c) True or false (no explanation necessary): If $\alpha' \in K$ is a root of $\sigma^*(f)$, then the homomorphism $\hat{\sigma} : F(\alpha) \to K$ which extends σ and sends α to α' is given by the formula

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

where the a_i are in F.
(Remark: To prove the existence in (b), instead of using quotients one could have just tried to define $\hat{\sigma}$ with this formula in the first place (since we know that any element of $F(\alpha)$ is an F-linear combination $1, \alpha, \alpha^2, ...$). But then there would be two things to manually check: (1) that the map is well-defined, and (2) that it is a ring homomorphism.)

(d) True or false (no explanation necessary): The number of elements of the set

$$\{\hat{\sigma} \in Hom(F(\alpha), K') : \hat{\sigma} = \sigma \text{ on } F\}$$

is equal to the number of distinct roots of $\sigma^*(f)$ in K'.

(e) Let $\sqrt[6]{2} \in \mathbb{R}$ denote a 6th root of 2. Give explicit formulas for all homomorphisms $\mathbb{Q}(\sqrt[6]{2}) \to \mathbb{C}$, describing them in terms of a basis of $\mathbb{Q}(\sqrt[6]{2})$. Which of these are automorphisms of $\mathbb{Q}(\sqrt[6]{2})$? (Note: Any ring homomorphism $\mathbb{Q}(\sqrt[6]{2}) \to \mathbb{C}$ must fix $\mathbb{Q}$.)

(f) Let $\zeta = e^{2\pi i/n}$. Find all homomorphisms $\mathbb{Q}(\zeta) \to \mathbb{C}$. Which of these are automorphisms of $\mathbb{Q}(\zeta)$?

2. Let a be a rational number which is not the cube of any rational number. Let L be a splitting field of $f(x) = x^3 - a$ over $\mathbb{Q}$.

(a) Show that $Gal(L/\mathbb{Q}) \simeq S_3$. (Hint: Because of Corollary 52 you may assume that L is the splitting field in $\mathbb{C}$. Adjoint the real root of f to $\mathbb{Q}$.)

(b) Let $\alpha \in L$ be a root of f and ω a primitive third root of unity in L. Show that $\mathcal{B} = \{\alpha^i\omega^j : 0 \leq i \leq 2,\ j = 0, 1\}$ is a basis of L over $\mathbb{Q}$. (Hint: Recall from the proof of the degree formula that if $F \subset K \subset L$ are fields and $\{\beta_i : 1 \leq i \leq n\}$ (resp. $\{\gamma_j : 1 \leq j \leq m\}$) is a basis of K over F (resp. L over K), then $\{\beta_i\gamma_j : 1 \leq i \leq n,\ 1 \leq j \leq m\}$ is a basis of L over F.)

(c) Let $\sigma \in Gal(L/\mathbb{Q})$ be the element that acts on the roots of f as the permutation $(\alpha\ \alpha\omega)$ (swapping α and $\alpha\omega$ and fixing $\alpha\omega^2$). Find the matrix of σ in terms of the basis $\mathcal{B}$. (After all, σ is an F-linear transformation $L \to L$. As such, with respect to any basis of L/F the map σ is represented by a matrix.)

3. Let L be the splitting field of $f(x) = x^3 + x + 1$ over $\mathbb{Q}$ contained in $\mathbb{C}$. Let α, β, γ be the roots of f in L, with $\alpha \in \mathbb{R}$.

(a) Show that $[L : \mathbb{Q}] = 6$. Conclude that $Gal(L/\mathbb{Q}) \simeq S_3$. Is there an isomorphism $L \to L$ which acts on the set of roots of f as the permutation $(\alpha\,\beta)$.

(b) Find the image of complex conjugation under the restriction map $Gal(\mathbb{C}/\mathbb{Q}) \to Gal(L/\mathbb{Q})$ as an element of the group of permutations of $\{\alpha, \beta, \gamma\}$.

4. (a) Let L be the splitting field of $f(x) = x^3 - 3x + 1$ over $\mathbb{Q}$ contained in $\mathbb{C}$. Let α, β, γ be the roots of $f(x)$ in L. Calculate $Gal(L/\mathbb{Q})$ as a group of permutations of $\{\alpha, \beta, \gamma\}$. Is there an automorphism of L that acts on $\{\alpha, \beta, \gamma\}$ as $(\alpha\ \beta)$?
(b) Same question as in Part (a), with $f(x) = x^3 - 4x + 1$.

5. Let L be a splitting field of $f(x) = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

(a) Show that $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ and has degree 4 over $\mathbb{Q}$. (We did this in class last week. You should reproduce the proof. You may refer to past assignments.)

(b) Find $Gal(L/\mathbb{Q})$ as a group of permutations of the roots of f.

(c) Which elements of your answer to (b) belong to the subgroup $Gal(L/\mathbb{Q}(\sqrt{6}))$?

(d) Find the image of $\sqrt{2}+\sqrt{3}$ under each element of $Gal(L/\mathbb{Q})$. Are these images all the roots of the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$?

6. Exercise 79 of Rotman. (Note that acting transitively does not imply including every permutation: for example, the subgroup $\langle(12\ldots n)\rangle$ of S_n acts transitively on $\{1, 2, \ldots, n\}$.)

Extra Practice Problems: The following problems are for your practice. They are not to be handed in for grading.

1. Galois Theory by J. Rotman, second edition: Exercises # 78, 80
2. Show that every extension of degree 2 is a splitting field. More explicitly, let K/F be an extension of degree 2. Show that there is a polynomial $f(x) \in F[x]$ such that K is a splitting field of $f(x)$ over F.
3. Let K/F be a finite extension. Show that there is a polynomial $f(x) \in F[x]$ such that K is contained in a splitting field of $f(x)$ over F.
4. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic polynomial with exactly one real root. Let L be a splitting field of $f(x)$ over $\mathbb{Q}$. What is $Gal(L/\mathbb{Q})$? What are the possibilities if $f(x)$ has three real roots?
5. Let F be a field, $f(x) \in F[x]$ and K a splitting field of $f(x)$ over F. Is each statement below true or false?
   (a) Given any two roots α, β of $f(x)$ in K, there is an element $\sigma \in Gal(K/F)$ such that $\sigma(\alpha) = \beta$.
   (b) If $f(x)$ is irreducible over F, then given any two roots α, β of $f(x)$ in K, there is an element $\sigma \in Gal(K/F)$ such that $\sigma(\alpha) = \beta$.
   (c) If $f(x)$ is irreducible over F, then given any three distinct roots α, β, γ of $f(x)$ in K, there is an element $\sigma \in Gal(K/F)$ which sends $\alpha \mapsto \beta$ and $\beta \mapsto \gamma$.
   (d) $|Gal(K/F)| = [K : F]$
   (e) If every irreducible factor of $f(x)$ over F is separable, then for every $\sigma \in Gal(K/F)$ we have $\sigma^{[K:F} = Idendity$.
6. Let K be the splitting field of the polynomial $x^2 - t \in \mathbb{F}_2(t)[x]$ over $\mathbb{F}_2(t)$ (= the field of rational functions with coefficients in $\mathbb{F}_2$ and in indeterminant t). Show that $[K : F]$ has degree 2 but $Gal(K/F)$ is the trivial group (i.e. has only one element). (Thus the separability hypothesis in Theorem 51 of Rotman is essential.)
7. (on degree formula) Let K/F be a field extension of prime degree. Are there any fields L with $F \subsetneq L \subsetneq K$?
8. True or false, don't use any results from Chapter 12: If L is any field of characteristic 0 and n is any positive integer, the group of n-th roots of unity in L is cyclic. (Hint: Denoting the group of n-th roots of unity in any field F by $\mu_n(F)$, consider the subfield $\mathbb{Q}(\mu_n(L))$ of L; it's a finite extension of $\mathbb{Q}$ (why?), and it is contained in a splitting field K of $x^n - 1$ over $\mathbb{Q}$ (why?). Now K is isomorphic to the splitting field of $x^n - 1$ over $\mathbb{Q}$ in $\mathbb{C}$ (why?). Thus $\mu_n(K) \simeq \mu_n(\mathbb{C})$ is cyclic. Is a subgroup of a cyclic group cyclic?)