MATD01 Fields and Groups

Assignment 7

Due Sunday March 15 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. Let F be any field, $\alpha \in F$ a nonzero element and $n \geq 1$. Let K be a splitting field of $x^n - \alpha$ over F. Show that K contains a splitting field of $x^n - 1$ over F. (Hint: Fix an n-th root β_0 of α in K. If β is any n-th root of α in K, is β/β_0 an n-th root of unity?)

2. (a) Let K/F be a field extension. Let $\alpha, \beta \in K$ be algebraic over F with $[F(\alpha) : F] = m$ and $[F(\beta) : F] = n$. Show that $[F(\alpha, \beta) : F] \leq mn$.
(b) Suppose moreover that $gcd(m, n) = 1$. Show that $[F(\alpha, \beta) : F] = mn$.
(c) Let p be a prime number. Let K be a splitting field of $x^p - 2$ over $\mathbb{Q}$.* Find $[K : \mathbb{Q}]$.
(d) Show that $\sum_{i=0}^{p-1} x^i$ is irreducible in $\mathbb{Q}(\sqrt[p]{2})[x]$ and $x^p - 2$ is irreducible in $\mathbb{Q}(\zeta_p)[x]$, where ζ_p is a primitive p-th root of unity.

3. (This question will definitely be graded.) In each part, find the degree of the extension K/F.
(a) $\mathbb{C} \supset K$ = the splitting field of $x^3 - 4$ over $F = \mathbb{Q}$
(b) $\mathbb{C} \supset K$ = the splitting field of $x^4 - 4$ over $F = \mathbb{Q}$
(c) $\mathbb{C} \supset K$ = the splitting field of $x^6 - 2$ over $F = \mathbb{Q}$
(d) K = a splitting field of $x^{10} - 2$ over $F = \mathbb{F}_5$ (Hint: Is $x^{10} - 2 = (x^2 - 2)^5$? Is 2 a square in $\mathbb{F}_5$?)
(e) K = a splitting field of $x^5 - 2$ over $F = \mathbb{F}_3$

4. Let $F \subset K \subset L$ be fields. Suppose K/F is algebraic and $\alpha \in L$ is algebraic over K. Show that α is algebraic over F. (Hint: Let $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ be the minimal polynomial of α over K. Consider the field extensions $F \subset F(a_0, ..., a_n) \subset F(a_0, ..., a_n)(\alpha)$. Remember every finite extension is algebraic.)

5. (a) Let L/F be a field extension. Suppose $\alpha, \beta \in L$ are algebraic over F. Show that $\alpha\beta, \alpha + \beta$ and $1/\alpha$ (if $\alpha \neq 0$ for the last one) are also algebraic over F. Conclude that the set

$$K := \{\alpha \in L : \alpha \text{ is algebraic over } F\} \tag{1}$$

is a subfield of L. Is K an algebraic extension of F?
(b) Let

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

*Since every two splitting fields of $x^p - 2$ over $\mathbb{Q}$ are isomorphic, we may assume without loss of generality that K is the one contained in $\mathbb{C}$.

By Part (a), K is an algebraic extension of $\mathbb{Q}$. Show that the extension $K/\mathbb{Q}$ is not finite. (In particular, not every algebraic extension is finite. Hint: Suppose $[K:\mathbb{Q}]=n$. Let $\sqrt[n+1]{2}$ be a real $n+1$-th root of 2. Is $\mathbb{Q}(\sqrt[n+1]{2}) \subset K$? Remember every finite extension is algebraic.)
(c) Recall that we say a field K is algebraically closed if every element of $K[x]$ has a root in K. Taking it for granted that $\mathbb{C}$ is algebraically closed, show that

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$$

is an algebraically closed algebraic extension of $\mathbb{Q}$. (An algebraically closed algebraic extension of a field F is called an algebraic closure of F. Hint: Problem 4.)

6. Let F be a field and p a prime number. Determine if each statement below is true or false. No explanation is necessary (but make sure you know why each statement is true or false).
(a) Every $f(x) \in F[x]$ has a unique splitting field over F.
(b) If K and K' are two splitting fields of $f(x) \in F[x]$ over F, then there exists a unique isomorphism $K \to K'$ which restricts to identity on F.
(c) If K and K' are two splitting fields of $f(x) \in F[x]$ over F, then there exists an isomorphism $K \to K'$ which restricts to identity on F.
(d) If $f(x) \in F[x]$ is irreducible and separable (i.e. has no repeated roots) and K and K' are splitting fields of $f(x)$ over F, then there are $\deg(f(x))$ isomorphisms $K \to K'$ which restrict to identity on F.
(e) If $f(x)$ is separable and K and K' are splitting fields of $f(x)$ over F, then there are $[K:F]$ isomorphisms $K \to K'$ which restrict to identity on F.
(f) Given any fields K and K' with $q=p^n$ elements, there are n isomorphisms $K \to K'$. (Hint: Apply (d) to $f(x)=x^q-x$ and $F=\mathbb{F}_p$.)

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 # 68-77

2. (a) Let F be a field of characteristic p over which $x^n - 1$ splits. Find the number of distinct n-th roots of unity in F. (Hint: You may want to start with writing n as $p^a m$, where $a \geq 0$ and $p \nmid m$.)
(b) Let F be any field and $\mu_n(F)$ the set of n-th roots of unity in F. Let $\alpha \in F$. Show that if α has an n-th root in F, then there is a bijection between $\mu_n(F)$ and the set of n-th roots of α in F.
(b) Suppose F is finite. Let $\alpha \in F$. Factor $x^{p^a} - \alpha$ as a product of irreducibles in $F[x]$. (Hint: If the Fröbenius map $\beta \to \beta^p$ an automorphism of F?)