MATD01 Fields and Groups

Assignment 5

Due Wednesday Feb 19 at 10:00 pm
(to be submitted on Crowdmark)

Notes: By a ring we always mean a commutative ring with $1 \neq 0$. For any prime number p, the field $\mathbb{Z}/p\mathbb{Z}$ is denoted by $\mathbb{F}_p$. For brevity, we denote the element $r + I$ of a quotient ring R/I by $\bar{r}$. Given rings R and S, we denote the set of all ring homomorphisms $R \to S$ by $\mathrm{Hom}(R, S)$. For a field F, the characteristic of F is denoted by $\mathrm{char}(F)$.

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

1. Let F be a field and $f(x) \in F[x]$. We say $\alpha \in F$ is a repeated root of $f(x)$ if

$$(x - \alpha)^2 \mid f(x)$$

. We say $f(x)$ has repeated roots if it has a repeated root in some field $K \supset F$ (that is, if there is a field $K \supset F$ and $\alpha \in K$ which is a repeated root of $f(x)$).

The goal of this question is to give a criterion for when a polynomial has repeated roots. Given $f(x) = \sum_{i \geq 0} a_i x^i \in F[x]$, define the (formal) derivative of $f(x)$ to be the polynomial $f'(x) := \sum_{i \geq 1} i a_i x^{i-1} \in F[x]$. It is straightforward to check that

$$(f(x) + g(x))' = f'(x) + g'(x)$$

and

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$$

for any $f(x), g(x) \in F[x]$. You can take these for granted for this question.

(a) Suppose $f(x)$ has a repeated root α in some field $K \supset F$. Show that $f'(\alpha) = 0$.

(b) Use Part (a) to conclude that the if $f(x) = x^{2p} + x^p + x + 1 \in \mathbb{F}_p[x]$ and K is field over which $f(x)$ splits, then $f(x)$ has $2p$ distinct roots in K.

(c) Let $f(x) \in F[x]$ be irreducible. Show that if $f(x)$ has repeated roots, then $f'(x) = 0$ (the zero polynomial). Conclude that if $\mathrm{char}(F) = 0$, then any irreducible $f(x) \in F[x]$ has no repeated roots.

2. Let K/F be a field extension (that is, F and K are fields and $F \subset K$). Let $\alpha_1, \ldots, \alpha_n \in K$. Define

$$F(\alpha_1, \ldots, \alpha_n) := \bigcap_{\substack{F \subset E \subset K \\ \alpha_1, \ldots, \alpha_n \in E}} E\,,$$

where the intersection is over the collection of all subfields E of K which contain F and the α_i ($1 \leq i \leq n$). The intersection of a nonempty collection of subfields of K is itself a subfield of K; thus $F(\alpha_1, \ldots, \alpha_n)$ is a subfield of K. It is referred to as the subfield obtained by adjoining $\alpha_1, \ldots, \alpha_n$ to F.

(a) true or false: if E is any subfield of K containing F and the α_i ($1 \leq i \leq n$), then E contains $F(\alpha_1, \ldots, \alpha_n)$.

(b) true or false:

$$F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = F(\alpha_1, \ldots, \alpha_n).$$

(c) Let L/F be a field extension. We say L is a finite extension of F (or that L/F is finite) if L is finite-dimensional as a vector space over F. The dimension of L as a vector space over F is then called the degree of the extension L/F, and is denoted by $[L : F]$. (Thus for instance, $[\mathbb{C} : \mathbb{R}] = 2$.)
Let $\alpha \in K$. Let $F[\alpha]$ be the image of the evaluation map $F[x] \to K$ sending $f(x) \mapsto f(\alpha)$ (in other words, $F[\alpha] = \{f(\alpha) : f(x) \in F[x]\}$). It is clear that $F[\alpha] \subset F(\alpha)$ (why?). Show that the following statements are equivalent:
(i) $F[\alpha] = F(\alpha)$
(ii) $F[\alpha]$ is a field.
(iii) α is algebraic over F.
(iv) The field $F(\alpha)$ is a finite extension of F.
Moreover, if any (or all) of these statements hold, then $[F(\alpha) : F]$ equals the degree of the minimal polynomial of α over F.
(Hints: Equivalence of (i) and (ii) should follow from definitions. For (ii) $\Rightarrow$ (iii) apply the first isomorphism theorem to the evaluation at α map $F[x] \to K$ (and remember $F[x]$ is not a field). For (iii) $\Rightarrow$ (ii) use the first isomorphism theorem and the fact that nonzero prime ideals in a PID are maximal. For (iii) $\Rightarrow$ (iv), let $g(x)$ be the minimal polynomial of α over F with $n = \deg(g(x))$; show that $\{\alpha^i : 0 \leq i < n\}$ is a basis of $F(\alpha)$ over F (this would also give the "moreover" statement). One way to do this would be by using the isomorphism $F[x]/(g(x)) \simeq F(\alpha)$ (here we used the already proved result that if α is algebraic then $F(\alpha) = F[\alpha]$) and the fact that $\{\overline{x}^i : 0 \leq i < n\}$ is a basis of $F[x]/(g(x))$ over F (the latter follows from Question 5 of Assignment 2). But you can also do it more directly if you prefer: by Problem 1 of Assignment 1*, if α is algebraic with the degree of its minimal polynomial equal to n, then $\{\alpha^i : 0 \leq i < n\}$ spans $F[\alpha]$ over F. Linear independence should follow from that n is the degree of the <u>minimal</u> polynomial. Finally, for (iv)$\Rightarrow$ (iii) consider the elements $\{\alpha^i : 0 \leq i \leq n\}$ with $n = [F(\alpha) : F]$.)

3. Determine if each of the following polynomials is irreducible in the given ring(s).
(a) $5x^8 + 6x^2 + 9x - 6$ in $\mathbb{Q}[x]$ and $\mathbb{Z}[x]$
(b) $x^n - a$ in $\mathbb{Q}[x]$, where $a \in \mathbb{Z}$ and there is a prime number p such that $p \mid a$ and $p^2 \nmid a$.
(c) Problem 64(i-iii) of Rotman (Hint: The degrees are 2 and 3 so irreducibility in $\mathbb{Q}[x]$ is the same as not having a root in $\mathbb{Q}$. Problem 63 on the same page can be very useful in order to determine if polynomial has roots in $\mathbb{Q}$ (basically it reduces the process to a finite search).)
(d) Problem 67 of Rotman
(e) $x^3 + 70000x + 4000$ in $\mathbb{Q}[x]$ (Hint: By Gauss' lemma it is enough to show that the polynomial does not factor in $\mathbb{Z}[x]$ as a product of two polynomials of smaller degree. To verify the latter, by Theorem 34, it is enough to show that the polynomial is irreducible after passing to $\mathbb{F}_7[x]$.)
(f) $x^9 - 13$ in $\mathbb{F}_{29}[x]$ and $\mathbb{Q}[x]$ (Hint for over $\mathbb{F}_{29}$: See if the polynomial has any roots in $\mathbb{F}_{29}$. Is the map $\mathbb{F}_{29}^\times \to \mathbb{F}_{29}^\times$ given by $\alpha \mapsto \alpha^9$ injective (and hence surjective)? Use group theory (things about the order of an element).)

*The fields there were $F = \mathbb{Q}$ and $K = \mathbb{C}$, but the argument worked over arbitrary fields.

(g) $x^{p^3} + 2x^{p^2} + x^p + 3$ in $\mathbb{F}_p[x]$ (Hint: Fröbenius.)
(h) $x^{p^3} + 2x^{p^2} + x^p + 3$ in $F[x]$, where F is an arbitrary field of characteristic p. (Hint: Is it still true that $2^p = 2$? Think about the prime field of F.)

4. Let $n \geq 1$. The group μ_n of n-th roots of 1 in $\mathbb{C}$ is cyclic of order n, generated by $e^{2\pi i/n}$. Let $K_n \subset \mathbb{C}$ be the splitting field of $x^n - 1$ over $\mathbb{Q}$.
(a) A generator of μ_n is called a primitive n-th root of 1. Equivalently, a primitive n-th root of 1 is an element of μ_n that has order n, i.e. a complex number $\zeta \in \mathbb{C}$ satisfying $\zeta^n = 1$ and $\zeta^k \neq 1$ for $1 \leq k < n$. List all primitive n-th roots of 1.
(b) Let $\zeta_n \in \mathbb{C}$ be any primitive n-th root of 1. Show that $K_n = \mathbb{Q}(\zeta_n)$.
(c) By finding the minimal polynomial of ζ_n for $1 \leq n \leq 9$, find the degree $[K_n : \mathbb{Q}]$ for these values of n. Formulate a conjecture about the value of $[K_n : \mathbb{Q}]$ in general. (Hints: You might want to see the "moreover" statement in Question 2(c). For irreducibility of $x^4 + 1$, use the same trick as in the proof of irreducibility of the p-cyclotomic polynomial.) Note: Your answer won't depend on which primitive n-th root ζ_n is. All you need to use about ζ_n in your reasoning is that $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ if $1 \leq k < n$.
(d) Give a basis of $\mathbb{Q}(\zeta_9)$ over $\mathbb{Q}$.
(e) Prove that in general (for any n) we have $[K_n : \mathbb{Q}] \leq \varphi(n)$, where φ is Euler's totient function. (Hint: Let ζ_n be a fixed primitive n-th root of 1. Let $g(x)$ be the minimal polynomial of ζ_n over $\mathbb{Q}$. So $[K_n : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(g(x))$. Try to argue that any complex root of $g(x)$ is also a primitive n-th roots of 1.)

5. Let $f(x) = x^n - 2 \in \mathbb{Q}[x]$ with $n \geq 1$. Let $\alpha \in \mathbb{C}$ be an arbitrary n-th root of 2, and $\zeta_n = e^{2\pi i/n}$ (or any other primitive complex n-th root of 1). Let K be the splitting field of $f(x)$ over $\mathbb{Q}$ in $\mathbb{C}$.
(a) Show that $K = \mathbb{Q}(\alpha, \zeta_n)$.
(b) Let $n \geq 3$. Show that $\mathbb{Q}(\alpha) \neq K$ and $\mathbb{Q}(\zeta_n) \neq K$. (Hint: First consider $\mathbb{Q}(\sqrt[n]{2})$ with $\sqrt[n]{2}$ a real n-th root of 2. Once you have argued that $\mathbb{Q}(\sqrt[n]{2}) \neq K$ (which should be easy, since $\mathbb{Q}(\sqrt[n]{2}) \subset \mathbb{R}$), use it to show that $[K : \mathbb{Q}] > n$.)

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

1. From Galois Theory by J. Rotman, second edition: Exercises # 56-66, particularly questions 56, 58, 60-62, 66
2. True or false: If K/F is a field extension and $f(x) \in F[x]$ is irreducible and monic, then $f(x)$ is the minimal polynomial of any of its roots in K.
3. Let $n \geq 2$. Let $\zeta_n \in \mathbb{C}$ be a primitive n-th root of 1 and $\alpha \in \mathbb{C}$ a root of $x^n - 10$. Show that $\alpha \notin \mathbb{Q}(\zeta_n)$.
4. Let p be a prime and K a field with $q = p^n$ elements. Denote the prime field of K by F. There is a unique isomorphism $\mathbb{F}_p \to F$, so that (identifying $\mathbb{F}_p$ with its image under this isomorphism) we may think of K as a field extension of $\mathbb{F}_p$. True or false: K is a splitting field of $x^q - x$ over $\mathbb{F}_p$.
5. Let K be a field extension of $\mathbb{F}_p$ over which $x^{p^3} - x$ splits. The L be the set of roots of $x^{p^3} - x$ in K. Is each statement below true or false? If a statement is true, prove it.
   (a) L has p^3 elements.
   (b) L is a subfield of K. (If true, then L is the splitting field of $x^{p^3} - x$ in K, because it is the smallest subfield that contains all the roots.)
6. Let F be a field, $f(x) \in F[x]$, and K/F a field extension in which $f(x)$ splits. Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of $f(x)$ in K. True or false: (1) Given any field E with $F \subset E \subset K$, the polynomial $f(x)$ splits over E if and only if E contains $F(\alpha_1, \ldots, \alpha_n)$. (2) The field $F(\alpha_1, \ldots, \alpha_n)$ is the unique subfield of K which is a splitting field of $f(x)$ over F.
7. True or false: If $f(x) \in \mathbb{Z}[x]$ is a polynomial with content (i.e. the gcd of its coefficients) equal to 1, then $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$. (One implication should be very quick and elementary, while the other implication is by Gauss' lemma.)
8. Let F be a field and $f(x), g(x) \in F[x]$. Let K be a field containing F over which both $f(x)$ and $g(x)$ split. Show that $f(x)$ and $g(x)$ are relatively prime if and only if they don't have a common root in K.
9. Let F be a field. Consider $f(x) = x^m - 1 \in F[x]$, $m \geq 1$. Show that $f(x)$ has repeated roots if and only if $\mathrm{char}(F) \mid m$.
10. (on earlier material) Let F be a field and $f(x), g(x) \in F[x]$. Suppose

$$f(x) = u \prod_{i=r}^{n} h_i(x)^{m_i} \qquad \text{and} \qquad g(x) = v \prod_{i=r}^{n} h_i(x)^{n_i},$$

where $h_1(x), \ldots, h_n(x) \in K[x]$ are irreducible, monic and distinct, and the exponents m_i, n_i are ≥ 0. Show that the gcd of $f(x)$ and $g(x)$ is

$$\prod_{i=r}^{n} h_i(x)^{\min(m_i, n_i)}.$$

11. Show that over any field F, the gcd of $x^m - 1$ and $x^n - 1$ is $x^{\gcd(m,n)} - 1$. (Hint: The gcd does not change if we extend the field (as the computations in Euclid's algorithm do not change whether we consider the polynomials over F or a larger field). So we may assume that F is large enough so that both polynomials split (e.g. replace F by a splitting field of $(x^m - 1)(x^n - 1)$). Now first consider the case where the characteristic of F does not divide m and n. Then $x^m - 1$, $x^n - 1$ and $x^{\gcd(m,n)} - 1$ do not have any repeated roots. Now use the previous question. Are the common roots of $x^m - 1$ and $x^n - 1$ exactly the roots of $x^{\gcd(m,n)} - 1$? In the case where $\mathrm{char}(F)$ divides m or n you have to modify the argument to deal with repeated roots: start with writing $m = p^a m'$ and $n = p^b n'$ with $p \nmid m', n'$. Then $x^m - 1 = (x^{m'} - 1)^{p^a}$ and $x^n - 1 = (x^{n'} - 1)^{p^b}$. The two polynomials $x^{m'} - 1$ and $x^{n'} - 1$ don't have any repeated roots.)