Homework09 - MATH 742

Boren(Wells) Guan

Date: May 3, 2025

Before Reading:

To make the proof more readable, I will miss or gap some natural or not important facts or notations during my writing. If you feel it hard to see, you can refer the appendix after the proof, where I will try to explain some simple conclusions (will be marked) more clearly. In case that you misunderstand the mark, I will add the mark just after those formulas between $ and before those between $$.

And I have to claim that the appendix is of course a part of my assignment, so the reference of it is required. Enjoy your grading!

Ex.1(2.3 on JSM)

Construct a splitting field for $X^5 - 2$ over $\mathbb{Q}$. What is its degree over $\mathbb{Q}$?

Sol.

We have $X^5 - 2 = \prod_{i=0}^{4}(X - 2^{1/5}e^{\frac{2\pi}{5}i}) \in \mathbb{C}[X]$ which means $\mathbb{Q}[2^{1/5}, e^{2\pi i/5}]$ will be a splitting field since $e^{2^{1/5},2\pi i/5}$ are algebraic over $\mathbb{Q}$, whose degree is less than 25. Also notice that $[\mathbb{Q}(e^{\frac{2\pi i}{5}}) : \mathbb{Q}] = 4$, since it is the root of $x^4 + x^3 + x^2 + x + 1$ which is irreducible and hence $[\mathbb{Q}(e^{\frac{2\pi i}{5}}) : \mathbb{Q}] \cong \mathbb{Q}/(x^4 + x^3 + x^2 + x + 1)$. Then we know that $[\mathbb{Q}[2^{1/5}, e^{2\pi i/5}], \mathbb{Q}]$ has to be a multiple of 20 and hence it is 20, we are done.

Ex.2(2.5 on JSM)

Let $f \in F[X]$, where F is a field of characteristic 0. Let $d(X) = gcd(f, f')$. Show that $g(X) := f(X)d(X)^{-1}$ has the same roots as $f(X)$, and these are all simple roots of $g(X)$.

Sol.

It is trivial when f is constant. Consider $f(X) = \prod_{i=1}^{k}(X - \alpha_i)\prod_{j=1}^{m}(X - \beta_j)^{m_j}$ with α_i, β_j distinct in some splitting field E of it where $m_j \geq 2$ and then we will know that $\prod_{j=1}^{m}(X - \beta_j)^{m_j - 1}|f, f$ in $E[X]$ and hence $g(X)$ will only have simple roots since $gcd(f, f')$ does not change with the extension. Then it is easy to check α_i is not a root of f' and hence a root of g and it is easy to check $(X - \beta_j)^{m_j}$ do not divide f', since F has 0 characteristic and hence $(X - \beta_j)|g$ and hence β_j is a root of g. Since any root of g will be a root of f and hence we know g have the same roots with f with all simple and we are done.

Ex.3(2.6 on JSM)

Let $f(X)$ be an irreducible polynomial in $F[X]$, where F has characteristic p. Show that $f(X)$ can be written $f(X) = g(X^{p^e})$ where $g(X)$ is irreducible and separable. Deduce that every root of $f(X)$ has the same multiplicity p^e in any splitting field.

Sol.

If f is separable, then it is obvious that $e = 0$. Assume f has multiple root, then we will know $f(X) = g(X^p)$ for some $g \in F[X]$ which has to be irreducible since if not, we will know $f(X) = p(X^p)q(X^p)$ for some $p, q \in F[X]$ which is a contradiction. We know $\deg g = \deg f/p$, so we continue this process and then we will some h such that $f(X) = h(X^{p^e})$ for some integer e and $\deg h < p$, then h can not have multiple roots or $\deg h \geq p$ and then we know h is irreducible and separable and we are done.

Ex.4(Problem A)

Let $E \supset F$ be an algebraic extension. Choose an algebraic closure $\overline{F}$ of F such that $E \subset \overline{F}$. Prove that the following conditions are equivalent:

1. E is the splitting field of a family of polynomials $S \subset F[x] - \{0\}$;
2. For any F-homomorphism $\phi : E \to \overline{F}, \phi(E) \subset E$;
3. The minimal polynomial of every $a \in E$ over F splits over E

Sol.

(1) implies (2): Assume E is the splitting field of a polynomial $f \in F[X] - \{0\}$ with roots $\{\alpha_i\}_{i=1}^k$ and then we know $0 = \phi(f(\alpha_i)) = f(\phi(\alpha_i))$ and hence $\phi(\alpha_i) = \alpha_j$ for some j for any F-homomorphism. Therefore any element in E will be mapped to an element in E. Then since any element E is contained in some splitting field contained in E for general E, so we are done.

(2) implies (3): Assume $a \in E$ and f the minimal polynomial and $f(X) = \prod_{i=1}^m (X - \alpha_i) \in \overline{F}[X]$ where $\alpha_1 = a$. We know there exists $\phi_i : F[a] \to \overline{F}$ F-homomorphisms with $\phi_i(a) = \alpha_i$ and we know there exists $\varphi_i : E \to \overline{F}$ such that $\varphi_i|_{F[a]} = \phi_i$ and hence we know any $\alpha_i \in E$ and we are done.

(3) to (1) is obvious and we are done.

Ex.5(Problem B)

Let F be a field of characteristic p. Prove that if $a \in F - F^p$, then $X^p - a$ is irreducible.

Sol.

If α is a root of $X^p - a$ in some extension of F and then $\alpha^p = a$ and we know $(X - \alpha)^p = X^p - \alpha^p = X^p - a$ and hence all roots of $X^p - a$ should be α. If it is reducible, then we know there exist $1 \leq k < p$ integer such that $(X - \alpha)^k \in F[X]$. Notice that if $f, g \in F[X], g|f$ then $f/g \in F[X]$ and hence there exists $X - \alpha \in F[X]$ since there are integers m, n such that $km + (p - k)n = 1$ and then

$X - \alpha = (X - \alpha)^{km+(p-k)n} \in F[X]$. Therefore, $\alpha \in F$ which is a contradiction.

Ex.6(Problem C)

Let F be a perfect field. Prove that all finite extensions $E \supset F$ are perfect as well.

Sol.

Assume F has zero characteristic. Then E/F obviously have zero characteristic. Then we assume F has characteristic of p and E has a basis $\{e_i\}_{i=1}^{n}$. If there are $a_i \in F[X]$ such that $a_1 e_1^p + a_2 e_2^p + \cdots + a_n e_n^p = 0$, then assume $\beta_i^p = a_i$ and we have $(\beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_n e_n)^p = 0$ which means $\beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_n e_n = 0$ and hence a contradiction, so $e_1^p, \cdots, e_n^p$ is also a basis and hence E is perfect by Frobenius homomorphism.