Homework09 - MATH 742

Boren(Wells) Guan

Date: April 30, 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.

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' 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 $f(X) = g(X^p)$ where $g(X)$ is irreducible and separable. Deduce that every root of $f(X)$ jas the same multiplicity p^e in any splitting field.

Sol.

Ex.4(Problem A)

Sol.

$1 \Rightarrow 2$: If E is the splitting field of a family of polynomials $S \subset F[x] - \{0\}$, then any $\alpha \in E$ is a linear combination of roots of polynomials in $S \subset F[x] - \{0\}$. Therefore, any F-homomorphism fixing F doesn't change S, which sends roots of polynomials to some roots of the same polynomials. Since E is the splitting field, all these roots are in E, hence $\phi(E) \subset E$.

$2 \Rightarrow 3$: For $a \in E$, the minimal polynomial over F, denoted by $m_{a,F}$ is irreducible. Since $a \in E$, we may regard E as an extension of $F(a)$. Since ϕ sends E to E, we know the conjugates of a, i.e. other roots of $m_{a,F}$, are in E as well. Therefore, $m_{a,F}$ splits over E.

$3 \Rightarrow 1$: Since for any $a \in E$, $m_{\alpha,F}$ splits over F, we may regard E as the splitting field of $m_{a,F}$ for all $a \in E$.

We are done.

Ex.5(Problem B)

Sol.

Denote $f(x) = x^p - a$. So we need to prove that if f is reducible, then $x^p - a$ has a root in F.

If f reducible, then there is $g \mid f$ and $\deg g < \deg f$. In the splitting field of F, we may write $f = \prod_{i=1}^{p}(x - x_i)$. We also know $\prod_{i=1}^{p}(-x_i) = -a$.

On the other hand, $g = \prod_{j=1}^{k}(x - x_j)$ divides f. We also have $g(0) = \prod_{j=1}^{k}(-x_j) = b$. We also know that $b^p = \prod_{j=1}^{k}(-x_j)^p = (-1)^p \prod_{j=1}^{k}(x_j)^p = (-1)^p a^k$, i.e. $a^k = (-b)^p$.

We also know that $k = \deg g < \deg f = p$, hence $\gcd(k, p) = 1$, so there are m, n such that $km + pn = 1$. We have $a = a^{km+pn} = a^{np}(-b)^{mp} = ((-b)^m a^n)^p$, so $a \in F^p$. Contradiction.

Ex.6(Problem C)

Sol.

If $\mathrm{char}(F) = 0$, then E/F is perfect automatically. Now assume $\mathrm{char}(F) = p$.

We prove that E is perfect if and only if for any α, we have $\sqrt[p]{\alpha} \in F$. For the "$\Leftarrow$", consider an irreducible polynomial over F, say $p(x)$. Assume p is not separable, then we know that $p(x) = a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1 x^p + a_0$. For each i, find $b_i \in F$ such that $b_i^p = a_i$, then $f(x) = (b_n x^n + \cdots + b_1 x + b_0)^p$,

then f cannot be irreducible. Conversely, if E is perfect, and $f(x) = x^p - a$ has no root in E, then it is not separable, but by the last problem, it is irreducible, so it is not perfect.

Since F is perfect, $F^p = F$. Now, consider $F(a)$ for $a \in E$. We find $m_{a,F}$, the minimal polynomial of a over F, then it is irreducible. Since F is perfect, $m_{\alpha,F}$ is separable.

If F is perfect, then every algebraic extension is separable. For any $\alpha \in E$, we have $m_{\alpha,E} \mid m_{\alpha,F}$, and since $m_{\alpha,F}$ is separable, so is $m_{\alpha,E}$. So, α is separable over E.