MATH110C Homework 1

Boran Erol

April 2024

1 Exercise 1

Lemma 1.1. Let K/F be a field extension. Assume that $char F \neq 2$ and $[K : F] = 2$. Then, there exists $\alpha \in K$ such that $\alpha^2 \in K$.

Proof. Let $\alpha \in K$ but not in F. Then, $[F(\alpha) : F] = 2$. Then, $m_F(\alpha) = x^2 + ax + b$ for some $a, b \in F$. Then, by completing the square, $m_F(\alpha) = (\alpha + \frac{a}{2})^2 + (b - \frac{a^2}{4}) = 0$, so $(\alpha + \frac{a}{2})^2$ is in F. However, $\alpha + + \frac{a}{2}$ is not in F since α is not in F. Thus, we conclude the proof. $\square$

2 Exercise 2

Let K/F be a field extension and let $\alpha, \beta \in K$. Assume α and β are algebraic over F, of respective degrees m and n.

Lemma 2.1. Let m' be the degree of α over $F(\beta)$. Then, β has degree $\frac{m'n}{m}$ over $F(\alpha)$.

Proof. Notice that $[F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F]$.

Since $[F(\alpha) : F] = m$ and $[F(\beta) : F] = n$ and $[F(\alpha, \beta) : F(\beta)] = m'$, the result immediately follows. The only lemma we need to continuously apply is that the degree of an element over a field is also the degree of the extension. $\square$

Lemma 2.2. If m and n are coprime, $[F(\alpha, \beta) : F] = mn$.

Proof. By a lemma proven in class, $[F(\alpha, \beta) : F] \leq [F(\alpha) : F][F(\beta) : F] = mn$.

Also notice that $m \mid [F(\alpha, \beta) : F]$ and $n \mid [F(\alpha, \beta) : F]$. Since m and n are coprime, $mn \leq [F(\alpha, \beta) : F]$.

We thus conclude the proof. $\square$

3 Exercise 3

We give an example where it fails.

Let $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Notice that p is irreducible with two of its roots being $\alpha = \sqrt[3]{2}$ and $\beta = \sqrt[3]{2}w$ with $w = e^{2\pi i/3}$. Then, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.

We showed in lecture on April 14 that $K = \mathbb{Q}(\alpha, \beta)$ is a splitting field of p over $\mathbb{Q}$ with $[K : \mathbb{Q}] = 6$. Notice that this implies $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$ since

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$$

Then, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 3$ and $2 = [\mathbb{Q}(\beta) : \mathbb{Q}]$.

Since $2 \nmid 3$, we have a counterexample.

4 Elman pg.298 Problem 2

Lemma 4.1. Let $u = \sqrt{2} + \sqrt[3]{5}$. Then, $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

Proof. Clearly, $\mathbb{Q}(u) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Thus, we'd like to show the opposite inclusion. It suffices to show that $\sqrt{2} \in \mathbb{Q}(u)$ since $\sqrt[3]{5} = u - \sqrt{2}$.

Cubing both sides of this equation and rearranging by combining all $\sqrt{2}$ terms, we have that

$$\sqrt{2} = \frac{u^{3-6u-5}}{3u^2 + 2}$$

Notice that $3u^2 + 2 \neq 0$ since $u \in \mathbb{R}$. Thus, $\sqrt{2} \in \mathbb{Q}(u)$ and we concluce the proof. $\square$

To find all $w \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ such that $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, we'd need to find all elements of $\mathbb{Q}(u)$ with degree 6 over $\mathbb{Q}$. Then, $[\mathbb{Q}(u) : \mathbb{Q}(w)] = 1$ and therefore they have to be equal.

5 Elman pg.298 Problem 4

Lemma 5.1. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Proof. Notice that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$.

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ since $\sqrt{2} \notin \mathbb{Q}$ and $\sqrt{2}$ satisfies $p(x) = x^2 - 2$.

To show $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, it suffices to show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ since $\sqrt{3}$ satisfies $p(x) = x^2 - 3$.

Now, by contradiction, assume that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then, there exists rationals a, b such that

$$a + b\sqrt{2} = \sqrt{3}$$

Squaring both sides,

$$a^2 + \sqrt{2}ab + 2b^2 = 3$$

Rearranging this equation proves that $\sqrt{2}$ is rational, which is a contradiction.

We thus conclude the proof. $\square$

6 Elman pg.298 Problem 7

Lemma 6.1. Let $\xi = \cos(\pi/6) + i\sin(\pi/6)$. $[Q(\xi) : \mathbb{Q}] = 4$.

Proof. Notice that ξ is a root of $p(x) = x^4 - x^2 + 1$. Thus, it suffices to show that $p(x)$ is irreducible. p doesn't have real roots since $x^4 - x^2 + 1 = (x^2 - \frac{1}{2})^2 + \frac{3}{4} > 0$.

Notice now that $x^4 - x^2 + 1 = (x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1)$. Notice that the polynomials in the RHS are irreducible polynomials in $\mathbb{R}[x]$, so we don't have a factorization of p in $\mathbb{Q}[x]$ using the fact that $\mathbb{R}[x]$ is a UFD. Therefore, p is irreducible. $\square$

7 Elman pg.298 Problem 8

Lemma 7.1. Let $K = F(u)$ where u is algebraic over F with odd degree. Then, $K = F(u^2)$.

Proof. Let f be the minimal polynomial for u and let $\deg(f) = 2k + 1$ for some $k \geq 0$.

Let g be the minimal polynomial for u^2 and let $\deg(g) = s$ for some $s \geq 1$.

Notice that $g(x^2)(u) = 0$ so $2s \geq 2k + 1$. Since they can't be equal as one is odd and the other is even, $2s > 2k + 1$.

Also notice that

$$[F(u) : F] = [F(u) : F(u^2)][F(u^2) : F]$$

. In other words, we have that

$$2k + 1 = [F(u) : F(u^2)]s$$

.

Since $2s > 2k + 1$, the only possible value of $[F(u) : F(u^2)]$ is 1. We thus conclude the proof. □

8 Elman pg.298 Problem 12

Lemma 8.1. If a^n is algebraic over a field F for some $n > 0$, a is algebraic over F.

Proof. Assume that a^n is algebraic over a field F for some $n > 0$. Recall that $[F(a^n) : F] = F[(a^n) : F(a)][F(a) : F]$ with both sides finite or infinite. Also recall that $[F(a^n) : F]$ is finite if and only if a^n is algebraic over F. Then, $F[(a^n) : F(a)][F(a) : F]$ is finite so $[F(a) : F]$ is finite and thus a is algebraic over F. $\square$