Math250aHw11

Trustin Nguyen

November 9, 2023

Exercise 1: Let $E = \mathbb{Q}(\alpha)$, where α is a root of the equation

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0$$

Express $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ and $(\alpha - 1)^{-1}$ in the form

$$a\alpha^2 + b\alpha + c$$

with $a, b, c \in \mathbb{Q}$.

Proof. (First Expression) Since $\alpha^3 + \alpha^2 + \alpha + 2 = 0$, we know that

$$\alpha^3 + \alpha^2 + \alpha = -2$$

Algebra manipulations:

$$\begin{aligned}(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha) &= \alpha(\alpha^2 + \alpha + 1)(\alpha + 1)\\ &= (\alpha^3 + \alpha^2 + \alpha)(\alpha + 1)\\ &= (-2)(\alpha + 1)\\ &= -2\alpha - 2\end{aligned}$$

So $a = 0, b = -2, c = -2$.

For the second, let $(\alpha - 1)^{-1} = a\alpha^2 + b\alpha + c$. We have:

$$\begin{aligned}(\alpha - 1)^{-1}(\alpha - 1) &= 1\\ (a\alpha^2 + b\alpha + c)(\alpha - 1) &= 1\end{aligned}$$

Rewriting, we get:

$$(a\alpha^3 + b\alpha^2 + c\alpha) - (a - 1)^{-1} = 1$$

Using $a\alpha^3 + a\alpha^2 + a\alpha + 2a = 0$, we have:

$$\begin{aligned}(b - a)\alpha^2 + (c - a)\alpha - 2a - (a - 1)^{-1} &= 1\\ (b - 2a)\alpha^2 + (c - a - b)\alpha - 2a - c &= 1\end{aligned}$$

Since we only have a degree 3 relation:

$$\alpha^3 + \alpha^2 + \alpha + 3 = 1$$

And there is probably no polynomial that divides x^3+x^2+x+2, in $\mathbb{Z}[x]$, set the coefficients of

$$(b - 2a)\alpha^2 + (c - a - b)\alpha - 2a - c = 1$$

To 0 to get the system:

$$\begin{aligned}b - 2a &= 0\\ c - a - b &= 0\\ -2a - c &= 1\end{aligned}$$

Solving this system, we get $a = \frac{-1}{5}, b = \frac{-2}{5}, c = \frac{-3}{5}$. Therefore,

$$(\alpha - 1)^{-1} = \frac{-1}{5}\alpha^2 - \frac{2}{5}\alpha - \frac{3}{5}$$

□

Exercise 3: Let α and β be two elements which are algebraic over F. Let $f(X) = \mathrm{Irr}(\alpha, F, X)$ and $g(X) = \mathrm{Irr}(\beta, F, X)$. Suppose the deg f and deg g are relatively prime. Show that g is irreducible in the polynomial ring $F(\alpha)[X]$.

Proof. Consider the field extensions:

$$F \subset F(\alpha) \subset F(\alpha, \beta)$$
$$F \subset F(\beta) \subset F(\alpha, \beta)$$

Let deg $f(x) = m$ and deg $g(x) = n$. Then $\gcd(m, n) = 1$. We will use the fact that

$$[F(\alpha, \beta) : F(\beta)][F(\beta) : F] = [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F]$$

So we have:

$$n[F(\alpha, \beta) : F(\beta)] = m[F(\alpha, \beta) : F(\alpha)]$$

because the gcd is 1, we have $n \mid [F(\alpha, \beta) : F(\alpha)]$. So the irreducible polynomial of $F(\alpha, \beta)$ over $F(\alpha)$ that kills β is of degree n. Furthermore, this polynomial must divide $g(X)$. So this polynomial is $g(X)$, which concludes the proof. □

Exercise 4: Let α be the real positive fourth root of 2. Find all intermediate fields in the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$.

Proof. We know that

$$\alpha^4 - 2 = 0$$

So $\mathbb{Q}(\alpha) \cong \mathbb{Q}[\alpha] \cong \mathbb{Q}[X]/(X^4 - 2)$. Let F be an intermediate field. Then we know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : F][F : \mathbb{Q}]$. Then

$$4 = [\mathbb{Q}(\alpha) : F][F : \mathbb{Q}]$$

If $[F : \mathbb{Q}] = 4$, then we know there is an isomorphism between $\mathbb{Q}(\alpha), F$. Otherwise, if $[F : \mathbb{Q}] = 2$, then we can consider α^2, which satisfies the equation $x^2 - 2 = 0$. So $\mathbb{Q}(\alpha^2)$ is the intermediate field. So we have the intermediate field ordering as:

$$\mathbb{Q} \subset \mathbb{Q}(\alpha^2) \subset \mathbb{Q}(\alpha)$$

There are no other intermediate field extensions, because the degree of the extension will divide 2:

$$2 = [\mathbb{Q}(\alpha)^2 : E][E : \mathbb{Q}], 2 = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2][\mathbb{Q}(\alpha^2) : \mathbb{Q}]$$

in which case, one of the extensions is of degree 1 and is trivial. □

Exercise 10: Let α be a real number such that $\alpha^4 = 5$.

(a) Show that $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$.

Proof. We have that $(i\alpha^2)^2 = -\alpha^4$. So $(i\alpha^2)^2 + 5 = 0$. Then $[\mathbb{Q}(i\alpha^2) : \mathbb{Q}] = 2$ because $1, i\alpha$ forms a basis for $\mathbb{Q}(i\alpha^2)$ over $\mathbb{Q}$. But any extension of degree 2 is normal. This is because if the irreducible poly is $x^2 + bx + c = (x - \alpha)(x - \beta)$, we have $b = -\alpha - \beta$. So $\beta = b + \alpha$ and $\beta \in \mathbb{Q}(i\alpha^2)$. □

(b) Show that $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$.

Proof. We have $(\alpha + i\alpha)^2 = \alpha^2 + 2i\alpha^2 - \alpha^2 = 2i\alpha^2$. Therefore, $(\alpha + i\alpha)^2 - 2i\alpha^2 = 0$. The minimal polynomial is $x^2 - 2i\alpha^2$, which is of degree 2. This polynomial is irreducible in $\mathbb{Q}(i\alpha^2)[x]$. So $[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}(i\alpha^2)] = 2$ and any extension of degree 2 is normal. □

(c) Show that $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$.

Proof. By the previous problems, we have:

$$[\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}(i\alpha^2)][\mathbb{Q}(i\alpha^2) : \mathbb{Q}] = 4$$

We have $x^2 - 2i\alpha^2 = 0$ if $x = (\alpha + i\alpha)$. We need a polynomial in $\mathbb{Q}[X]$ that kills $(\alpha + i\alpha)$ so $(x^2 - 2i\alpha^2)(x^2 + 2i\alpha^2) = 0$, $x^4 + 4\alpha^4 = x^4 + 20 = 0$. If $\mathbb{Q}(\alpha + i\alpha)$ is a normal extension, then it must contain all roots of $x^4 + 20$.

So $x^2 + 2i\alpha^2 = 0$ for some $x \in \mathbb{Q}(\alpha + i\alpha)$. We see that $i(\alpha + i\alpha) = i\alpha - \alpha$ is a root. But if $i\alpha - \alpha \in \mathbb{Q}(\alpha + i\alpha)$, Then $\mathbb{Q}(\alpha + i\alpha) = \mathbb{Q}(i\alpha^2)$, which is not true, because there is a degree 2 extension from $\mathbb{Q}(i\alpha^2) \subseteq \mathbb{Q}(\alpha + i\alpha)$.

Then this is not a normal extension because not all roots of $x^4 + 20$ are in $\mathbb{Q}(\alpha + i\alpha)$. □