Math 111C HW1

Zih-Yu Hsieh

April 3, 2025

1 (Not Done)

Question 1 *Show, using Eisenstein's criterion, that $f(X) = X^3 - 3X - 1$ is irreducible over $\mathbb{Q}$. Let α be a root of f in $\mathbb{C}$. Express $\frac{1}{\alpha}$ and $\frac{1}{\alpha+3}$ as linear combinations of 1, α and α^2.*

Pf:

Consider the ring homomorphism $\phi : \mathbb{Z}[X] \to \mathbb{Z}[X]$ by $\phi(f) = f(X+1)$. Which, ϕ is injective, since if $f(X+1)$ is constantly 0, its leading coefficient $a_n = 0$, which helps us inductively prove that $f = 0$.

Then, for $f(X) = X^3 - 3X - 1$ given above:

$$\phi(f) = f(X+1) = (X+1)^3 - 3(X+1) - 1 = (X^3 + 3X^2 + 3X + 1) - (3X + 3) - 1 = X^3 + 3X^2 - 3$$

Then, since leading coefficient is 1, while the rest of the coefficients (namely $3, 0, -3$) are divisible by 3, and -3 is not divisible by 3^2, so by Eisenstein's criterion, $\phi(f) = X^3 + 3X^2 - 3$ is irreducible over $\mathbb{Q}$. Then, since $\phi(f) = f(X+1)$ is irreducible over $\mathbb{Q}$, then f itself must also be irreducible:

Suppose not, then there exists d fuck it

2

Question 2 *Let $K = F(\alpha)$, where α is a root of the irreducible polynomial*

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$$

Express $\frac{1}{\alpha}$ in terms of α and the coefficients a_i.

Pf:

First, since f is irreducible in $F[x]$, then f has no zeroes in F. Hence, 0 cannot be a zero of f, so $\alpha \neq 0$. This also implies that $a_0 \neq 0$ (or else if $a_0 = 0$, 0 is a zero of f).

Then, consider $K' = F[x]/(f(x))$: Since f is an irreducible polynomial over F, then since $F[x]$ is a PID, the ideal $(f(x))$ is in fact maximal, hence $K' = F[x]/(f(x))$ is a field.

Now, consider $\overline{x} = x \mod (f(x)) \in K'$: since it satisfies the following:

$$f(\overline{x}) = \overline{x}^n + a_{n-1}\overline{x}^{n-1} + ... + a_1\overline{x} + a_0 = \overline{x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0} = 0 \mod (f(x)) \in K'$$

then K' is a field containing a zero of $f(x)$.

Then, consider the ring homomorphism $\phi : K' \to K$, by $\phi(\overline{x}) = \alpha$: Since 0 is not a zero of f, then $\alpha \neq 0 \in F(\alpha)$. Hence, the ring homomorphism ϕ is not the zero map, showing that $\ker(\phi) \neq K'$; then, since K' is a field, while $\ker(\phi) \neq K'$, the map is injective.

Lastly, consider the inverse of $\overline{x} \in K'$: Since $a_0 \neq 0$ in F, then $a_0^{-1}f(x) = a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1x) + 1$. Hence, the following is true:

$$0 = a_0^{-1}f(x) \mod (f(x)) = (a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1x) + 1) \mod (f(x))$$

$$\implies \overline{1} = \overline{a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1x)} \in K' = F[x]/(f(x))$$

So, $\overline{1} = \overline{a_0^{-1}(x^n + a_{n-1}x^{n-1} + ... + a_1x)} = \overline{x} \cdot \overline{a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)}$, hence the inverse of $\overline{x}$ in K' is $\overline{a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)}$. Then, since ring homomorphism maps an element's inverse to the output's inverse, then $\phi(\overline{x}) = \alpha$ implies the following:

$$\frac{1}{\alpha} = \alpha^{-1} = \phi((\overline{x})^{-1}) = \phi\left(\overline{a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)}\right) = a_0^{-1}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + ... + a_1)$$

3

Question 3 *Show that x^4+1 is irreducible over $\mathbb{Q}$, but not over $\mathbb{Q}(\sqrt{2})$.*

Pf:

If consider $x^4+1 \in \mathbb{Z}[x]$, if we do a substitution $x \mapsto (x+1)$, then we get the following:

$$(x^4+1) \mapsto (x+1)^4+1 = (x^4+4x^3+6x^2+4x+1)+1 = x^4+4x^3+6x^2+4x+2$$

Notice that since leading coefficient 1 is not divisible by 2, the other coefficients $4, 6, 4, 2$ are divisible by 2, while the constant term 2 is not divisible by 2^2, then by Eisenstein's criterion, $(x+1)^4+1$ is irreducible over $\mathbb{Q}$. Hence, the original polynomial x^4+1 is also irreducible over $\mathbb{Q}$.

Now, consider x^4+1 over $\mathbb{Q}(\sqrt{2})$: since $\sqrt{2}$ is an element in the given field, then the following is a factorization of x^4+1:

$$((x^2+1)-\sqrt{2}x)((x^2+1)+\sqrt{2}x) = (x^2+1)^2-(\sqrt{2}x)^2 = (x^4+2x^2+1)-(2x^2) = x^4+1$$

Since x^4+1 can be factored into smaller degree nonconstant polynomial, this indicates x^4+1 is reducible over $\mathbb{Q}(\sqrt{2})$.

4

Question 4

Pf:

5

Question 5

Pf:

6

Question 6

Pf:

7

Question 7 *Let E/F be a field extension, and let $\alpha \in E$. Show that multiplication by α is a linear transformation of E considered as a vector space over F. When is this linear transformation non-singular?*

Pf:

To verify the multiplication by α being a linear transformation of E as a vector space over F, consider all $f, g \in E$, and scalar $\lambda \in F$:

By distributive property of multiplication, we know $\alpha(f+g) = \alpha f + \alpha g$; similarly, since E is a field, the multiplication is commutative, hence $\alpha(\lambda f) = \lambda(\alpha f)$, showing that the multiplication is in fact a linear transformation of E as a vector space over F.

Now, suppose α as a linear transformation is non-singular (i.e. invertible), which we'll verify that such transformation is non-singular iff $\alpha \neq 0$:

$\Longrightarrow$: Suppose $\alpha \neq 0$, then $\alpha^{-1} \in E$ exists since E is a field. Based on the fact that multiplication of any element in E is a linear transformation of E, any $f \in E$ satisfies $\alpha^{-1}(\alpha f) = \alpha(\alpha^{-1} f) = f$, which α^{-1} as a linear transformation over E composes with α to be identity on both sides, this shows that α^{-1} is the inverse transformation of α, hence α is non-singular.

$\Longleftarrow$: We'll prove the contrapositive. Suppose $\alpha = 0$, then since all nonzero $f \in E$ satisfies $\alpha f = 0$, then the transformation α is not injective, hence non-invertible. This shows that α is a singular linear transformation. Then, the contrapositive states that if α is non-singular, the $\alpha \neq 0$.

The above two implication states that α as a linear transformation is non-singular, iff $\alpha \neq 0$.

8

Question 8 *Let E/F be a field extension, and let $p(x)$ be an irreducible polynomial over F. Show that if the degree of $p(x)$ and $[E:F]$ are coprime, then $p(x)$ has no zeros in E.*

Pf:

We'll prove the contrapositive. Given that $p(x)$ is irreducible over F, then it has no zero in F. Hence, $p(0) \neq 0$.

Suppose $p(x)$ has a zero in E, say $\alpha \in E$. Then, since $p(\alpha) = 0$, $\alpha \neq 0$.

First, we'll consider the ring $K' = F[x]/(p(x))$: Since $p(x) \in F[x]$ is irreducible, and $F[x]$ is a PID, the ideal $(p(x)) \subset F[x]$ is in fact maximal. Hence, $K' = F[x]/(p(x))$ is a field.

Now, given that $p(x) = a_n x^n + ... + a_1 x + a_0$, since $\overline{x} = x \mod (p(x)) \in K'$ satisfies the following:

$$p(\overline{x}) = a_n \overline{x}^n + ... + a_1 \overline{x} + a_0 = (a_n x^n + ... + a_1 x + a_0) \mod (p(x)) = p(x) \mod (p(x)) = 0 \in K'$$

Hence, $p(x)$ has a zero over the field K'.

Then, consider the ring homomorphism $\phi : K' \to E$ given by $\phi(\overline{x}) = \alpha$: since $\alpha \neq 0$ in E and $\overline{x} \neq 0$ in K', then such ring homomorphism is nonzero, hence $\ker(\phi) \neq K'$. Now, because K' is a field, then it enforces ϕ to be injective. Then, since $K' \cong \phi(K') \subseteq E$, this shows that K' is isomorphic to a subfield of E. Hence, E/K' is also a field extension.

9

Question 9

Pf:

10

Question 10

Pf: