1. Tutorial Series 1: Embeddings

Exercise 1.1: *Consider the ring of polynomials $\mathbb{Z}[X]$ with indeterminate X.*

Question 1.1.1: *Show that $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$.*

Take the map $\varphi : \mathbb{Z}[X] \to \mathbb{Z}$ such that $\varphi(a_0 + a_1 X + \ldots + a_n X^n) = a_0$, φ is a ring homomorphism with $\operatorname{Ker} \varphi = (X)$ and $\operatorname{Im} \varphi = \mathbb{Z}$ then by the first isomorphism theorem $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$.

Question 1.1.2: *Show that $(2) + (x)$ is not generated by a singleton.*

Suppose there exists $P \in \mathbb{Z}[X]$ such that $(P) = (2) + (X)$, since $2 \in (2) + (X)$ then $2 \in (P)$ so $2 = PQ$ with $Q \in \mathbb{Z}[X]$ but that means that $\deg(P) + \deg(Q) = 0 \Rightarrow \deg P = 0$ so $P = p \in \mathbb{Z}$, since $2 \in (p)$ then $p \mid 2 \Rightarrow p = \pm 1$ or $p = \pm 2$ which are both impossible since $1 \in \mathbb{Z}[X] \setminus ((2) + (X))$ and $2 + X \in (2) + (X) \setminus (2)$.

Question 1.1.3: *Deduce that $\mathbb{Z}[X]$ is not a PID.*

- From 1.1.1 we have that $\mathbb{Z}[X]$ is a PID and X is irreducible then (X) is a maximal ideal so $\mathbb{Z}[X]/(X)$ is a field but $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ which means that $\mathbb{Z}$ is a field, contradiction.
- From 1.1.2 we have that $(2) + (x)$ is an ideal of $\mathbb{Z}[X]$ but it is not a principle ideal.

Question 1.1.4: *Is $\mathbb{Z}[X]$ a Euclidean domain ?*

$\mathbb{Z}[X]$ is not a Euclidean domain since it is not a PID.

Exercise 1.2: *Find embeddings and automorphisms in the following cases.*

Question 1.2.1: *$K = \mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\left(\sqrt[4]{2}\right), \mathbb{Q}\left(\sqrt[3]{5}\right)$ and $L = \mathbb{C}$.*

- $K = \mathbb{Q}\left(\sqrt{2}\right)$: we have that $\operatorname{Irr}\left(\sqrt{2}, K, X\right) = X^2 - 2$ since it is a monic 2-Eisenstein that nullifies $\sqrt{2}$ and we have that $\operatorname{Char} \mathbb{Q} = 0$ and $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$ so there are only two embeddings

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2}$$
$$\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$$

which are both automorphisms.

- $K = \mathbb{Q}\left(\sqrt[4]{2}\right)$: we have that $\mathbb{Q}\left(\sqrt[4]{2}\right) = \mathbb{Q}\left(\sqrt{2}\right)\left(\sqrt[4]{2}\right)$ then $\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[4]{2}\right), \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4$ and $X^4 - 2$ nullifies $\sqrt[4]{2}$ then we have that $\operatorname{Irr}\left(\sqrt[4]{2}, \mathbb{Q}, X\right) = X^4 - 2$, and we get that the set of conjugates of $\sqrt[4]{2}$ over $\mathbb{Q}$ are $\left\{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\right\}$ and since $\operatorname{Char}(\mathbb{Q}) = 0$ then the following 4 embeddings are the only ones

$$\sigma_1 : \sqrt[4]{2} \mapsto \sqrt[4]{2} \qquad \sigma_2 : \sqrt[4]{2} \mapsto -\sqrt[4]{2}$$
$$\sigma_3 : \sqrt[4]{2} \mapsto i\sqrt[4]{2} \qquad \sigma_4 : \sqrt[4]{2} \mapsto -i\sqrt[4]{2}$$

and only σ_1, σ_2 are automorphisms.

- $K = \mathbb{Q}\left(\sqrt[3]{5}\right)$: we have that $X^3 - 5$ is 5-Eisenstein and nullifies $\sqrt[3]{5}$ then $\operatorname{Irr}\left(\sqrt[3]{5}, \mathbb{Q}, X\right) = X^3 - 5$ so the conjugates of $\sqrt[3]{5}$ over $\mathbb{Q}$ are $\left\{\sqrt[3]{5}, j\sqrt[3]{5}, j^2\sqrt[3]{5}\right\}$ with $j = e^{\frac{2\pi}{3}i}$, thus we get exactly 3 embeddings

$$\sigma_1 : \sqrt[3]{5} \mapsto \sqrt[3]{5}$$
$$\sigma_2 : \sqrt[3]{5} \mapsto j\sqrt[3]{5}$$
$$\sigma_3 : \sqrt[3]{5} \mapsto j^2\sqrt[3]{5}$$

and only σ_1 is an automorphism.

Question 1.2.2: *Find all $\mathbb{Q}\left(\sqrt{2}\right)$-embeddings of $\mathbb{Q}\left(\sqrt[4]{2}\right)$ into $\mathbb{C}$.*

we have that $\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$ and its easy to verify that $\operatorname{Irr}\left(\sqrt[4]{2}, \mathbb{Q}\left(\sqrt{2}\right), X\right) = X^2 - \sqrt{2}$, thus the conjugates of $\sqrt[4]{2}$ over $\mathbb{Q}\left(\sqrt{2}\right)$ are $\left\{\sqrt[4]{2}, -\sqrt[4]{2}\right\}$ thus we get only two embeddings since $\operatorname{Char} \mathbb{Q}\left(\sqrt{2}\right) = 0$ which are

$$\sigma_1 : \sqrt[4]{2} \mapsto \sqrt[4]{2}$$
$$\sigma_2 : \sqrt[4]{2} \mapsto -\sqrt[4]{2}$$

Question 1.2.3: *Determine all embeddigns of $K = \mathbb{F}_2(\alpha)$ into an algebraic closure $\overline{K}$ and all automorphisms with $\alpha^2 + \alpha + 1 = 0$ then $\alpha^3 + \alpha^2 + 1 = 0$.*

- $\alpha^2 + \alpha + 1 = 0$: let $P(X) = X^2 + X + 1$, $P(0) = P(1) = 1 \neq 0$ thus P is irreducible over $\mathbb{F}_2[X]$ and $P(\alpha) = 0$ so $\operatorname{Irr}(\alpha, \mathbb{K}, X) = P(X)$, $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2$ thus there are two conjugates of α over $\mathbb{F}_2$. $P(\alpha^2) = \alpha^4 + \alpha^2 + 1$, we have $\alpha^2 + \alpha + 1 = 0 \Rightarrow \alpha^2 = \alpha + 1 \Rightarrow \alpha^3 = 1 \Rightarrow \alpha^4 = \alpha$ thus $P(\alpha^2) = \alpha^2 + \alpha + 1 = 0$. So the conjugates are $\{\alpha, \alpha^2\}$ and thus we get the embeddings are

$$\sigma_1 : \alpha \mapsto \alpha$$
$$\sigma_2 : \alpha \mapsto \alpha^2$$

which are both automorphisms.

Question 1.2.4: *Determine all embeddigns of $K = \mathbb{F}_3(\beta)$ into an algebraic closure $\overline{K}$ and all automorphisms with $\beta^2 + \beta + 2 = 0$ then $\beta^3 + \beta^2 + 2 = 0$.*

- the process is just the same as before.

Exercise 1.3: *Let L/K be an algebraic extension and Ω an algebraically closed field.*

Question 1.3.1: *Let $\theta \in L$, and $\tau : K \to \Omega$ an embedding, show that τ can be extended to $\sigma : K(\theta) \to \Omega$.*

Question 1.3.2: *If $\operatorname{Char} K = 0$ and $[K(\theta) : K] = n$ then there is exactly n extensions to $K(\theta)$.*

Question 1.3.3: *Apply the above to each embedding $\sigma : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{C}$ with $\theta = \sqrt[4]{2}$.*

Question 1.3.4: *Using the 1.3.1 and Zorn's Lemma, prove that τ can be extended to $\sigma : L \to \Omega$.*

Exercise 1.4: *Find the primitive element of the following extensions*

1. $\mathbb{Q}\left(\sqrt{2}, i\right)/\mathbb{Q}$.
2. $\mathbb{C}/\mathbb{R}$.
3. $\mathbb{Q}\left(\sqrt{2}, i, \sqrt{3}\right)/\mathbb{Q}\left(\sqrt{3}\right)$.
4. $\mathbb{Q}\left(\sqrt{2}, i, \sqrt{3}\right)/\mathbb{Q}$.
5. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt[4]{2}\right)/\mathbb{Q}$.
6. $\mathbb{F}_2(\alpha, \alpha^2, \alpha + \alpha^2)/\mathbb{F}_2$ with $\alpha^2 + \alpha + 1 = 0$.

1. $\mathbb{Q}\left(\sqrt{2}, i\right)/\mathbb{Q}$, we consider two methods to find the primitive element
   1. Let $\theta = i + \sqrt{2}$, we have that $\theta - i = \sqrt{2} \Rightarrow (\theta - i)^2 = 2$, by distributing the factors, we have $\theta^2 - 2i\theta + 1 = 2 \Rightarrow i = \frac{\theta^2 - 3}{2\theta} \in \mathbb{Q}(\theta)$ and also $\sqrt{2} = \theta - i \in \mathbb{Q}(\theta)$ thus we get that $\mathbb{Q}\left(i, \sqrt{2}\right) = \mathbb{Q}(\theta)$.
   2. By Eisenstein criterion we have
   $$\operatorname{Irr}\left(\sqrt{2}, \mathbb{Q}, X\right) = X^2 - 2$$
   $$\operatorname{Irr}(i, \mathbb{Q}, X) = X^2 + 1$$
   thus the conjugates of $\sqrt{2}$ are $\left\{\sqrt{2}, -\sqrt{2}\right\}$ and of i are $\{i, -i\}$, thus by the proof of the primitive element theorem, by taking $k \notin \left\{0, i\sqrt{2}\right\}$ thus by taking $k = 1$ we get $\mathbb{Q}\left(i, \sqrt{2}\right) = \mathbb{Q}\left(i + \sqrt{2}\right)$.
2. $\mathbb{C}/\mathbb{R}$, its clear that $\mathbb{C} = \mathbb{R}(i)$ thus i is a primitive element.
3. $\mathbb{Q}\left(\sqrt{2}, i, \sqrt{3}\right)/\mathbb{Q}\left(\sqrt{3}\right)$,
   we have $\mathbb{Q}\left(\sqrt{2}, i, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{i}\right)\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{i}\right)\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{3}\right)\left(\sqrt{2} + i\right)$ thus $\sqrt{2} + i$ is a primitive element of $\mathbb{Q}\left(\sqrt{2}, i, \sqrt{3}\right)/\mathbb{Q}\left(\sqrt{3}\right)$.
4. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, i\right)/\mathbb{Q}$, we have from before that $\mathbb{Q}\left(\sqrt{2}, i\right) = \mathbb{Q}\left(\sqrt{2} + i\right)$, thus $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, i\right) = \mathbb{Q}\left(\sqrt{2} + i\right)\left(\sqrt{3}\right)$, now consider $\theta = \sqrt{2} + i$ we have then
   $$(\theta - i)^2 = 2 \Rightarrow \theta^2 - 3 = 2\theta i$$
   $$\Rightarrow \left(\theta^2 - 3\right)^2 = -4\theta^2$$
   $$\Rightarrow \theta^4 - 2\theta^2 + 9 = 0$$
   we can see that θ is a root of $P(X) = X^4 - 2\theta^2 + 9$, notice that if a is a root of P then so is $-a$, $\overline{a}$ and $-\overline{a}$ thus we get that the conjugates of θ are $\sqrt{2} + i, -\sqrt{2} + i, \sqrt{2} - i, -\sqrt{2} - i$ and we know that the conjugates of $\sqrt{3}$ over $\mathbb{Q}$ are $\sqrt{3}$ and $-\sqrt{3}$, by the proof of the primitive element theorem we have that $k \notin \{0, \sqrt{2/3}, i/\sqrt{3}, \left(\sqrt{2} + i\right)/\sqrt{3}\}$, so taking $k = 1$ we get that $\sqrt{2} + \sqrt{3} + i$ is a primitive element.

1. $\mathbb{Q}\left(\sqrt[4]{2}, \sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{3}, \sqrt[4]{2}\right)$ with the same method.
2. $\mathbb{F}(\alpha, \alpha^2, \alpha^2 + \alpha)/\mathbb{F}$, its easy to notice that $\alpha + \alpha^2 \in \mathbb{F}(\alpha, \alpha^2)$ and from the definition of α, $\alpha^2 = \alpha + 1 \in \mathbb{F}(\alpha)$ thus we get
   $$\mathbb{F}(\alpha, \alpha^2, \alpha^2 + \alpha) = \mathbb{F}(\alpha, \alpha^2) = \mathbb{F}(\alpha)(\alpha^2) = \mathbb{F}(\alpha)$$
   thus α is a primitive element.

Exercise 1.5: *Let K be a field with $\operatorname{Char} K = 0$, L/K an n-degree extension and θ a primitive element of L/K and an algebraically closed field Ω.*

Question 1.5.1: *Showing that $1, \theta, ..., \theta^{n-1}$ is a basis of the vector space L over K.*

Question 1.5.2: *Proving that the embeddings $\sigma_i : L \to \Omega$ are of the forma $\sigma_i(\theta) = \theta_i$ where $\theta_1, ..., \theta_n$ are distinct conjugates of θ over K.*

Question 1.5.3: *For any $\eta \in L$, the conjugates of η are contained in $\{\sigma_i(\eta) \mid i \in [\![1, n]\!]\}$.*

Question 1.5.4: *η is a primitive element if and only if $\forall i, j \in [\![1, n]\!], \sigma_i(\eta) = \sigma_j(\eta) \Rightarrow i = j$.*

Question 1.5.5: *Deduce that for any $(a, b) \in \mathbb{Q}^\star \times \mathbb{Q}^\star$ we have $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(a\sqrt{2} + b\sqrt{2}\right)$.*

Exercise 1.6: *Let $\alpha = \sqrt[3]{2}$, $\omega = e^{\frac{2\pi}{3}i}$ and $\beta = \alpha\omega$, prove the following statements*

Question 1.6.1: *For any $c \in \mathbb{Q}$, $\gamma = \alpha + c\beta$ is a zero of $x^6 + ax^3 + b$ for some $a, b \in \mathbb{Q}$.*

Question 1.6.2: *the polynomial $\operatorname{Irr}(\alpha + \beta, \mathbb{Q}, X)$ is cubic and $\deg \operatorname{Irr}(\alpha - \beta, \mathbb{Q}, X) = 6$.*

Question 1.6.3: $\forall c \in \mathbb{Q}^\star, \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\omega + c\alpha)$.

Question 1.6.4: $\mathbb{Q}\left(\omega, \sqrt{5}\right) = \mathbb{Q}\left(\omega\sqrt{5}\right)$.

2. Tutorial Series 2: Finite Fields

Exercise 2.7: *Decide whether there exists a finite field having the given number of elements.*

$$4095 \ - \ 191 \ - \ 12345678910$$
$$81 \ - \ 12396 \ - \ 128$$

We do prime factorization for each of the elements below.

Exercise 2.8: *Determine all finite fields having n elements where $n \leq 15$. Find a basis, a primitive element, a generator for the multiplicative group for every field.*

We will find all the fields of the form $\mathbb{F}_{p^n}$ such that $p^n \leq 15$.

- $p = 2$:
  - $n = 1$:
    - Field: $\mathbb{F}_2$.
    - Primitive Element: 1 or 0.
    - Basis Over $\mathbb{F}_2$: $\{1\}$.
    - Generator: 1.
  - $n = 2$:
    - Field: $\mathbb{F}_{2^2} = \mathbb{F}_4$.
    - Primitive Element: α with $\alpha^2 + \alpha + 1 = 0$.
    - Basis Over $\mathbb{F}_2$: $\{1, \alpha\}$
    - Generator: α.
  - $n = 3$:
    - Field: $\mathbb{F}_{2^3} = \mathbb{F}_8$.
    - Primitive Element: α with $\alpha^3 + \alpha + 1 = 0$.
    - Basis Over $\mathbb{F}_2$: $\{1, \alpha, \alpha^2\}$.
    - Generator: α.
- $p = 3$:
  - $n = 1$:
    - Field: $\mathbb{F}_3$.
    - Primitive Element: 1 or 0.
    - Basis Over $\mathbb{F}_3$: $\{1\}$.
    - Generator: 2.
  - $n = 2$:
    - Field: $\mathbb{F}_{3^2} = \mathbb{F}_9$.
    - Primitive Element: α with $\alpha^2 + 1 = 0$.
    - Basis Over $\mathbb{F}_3$: $\{1, \alpha\}$.
    - Generator: .
- for the remaining for any $p \in \{5, 7, 11, 13\}$ we have
  - Field: $\mathbb{F}_p$.
  - Primitive Element: 1 or 0.
  - Basis Over $\mathbb{F}_p$: $\{1\}$.
  - Generator: respectively.