

# 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  $\varphi : \mathbb{Z}[X] \rightarrow \mathbb{Z}$  such that  $\varphi(a_0 + a_1X + \dots + a_nX^n) = a_0$ ,  $\varphi$  is a ring homomorphism with  $\text{Ker } \varphi = (X)$  and  $\text{Im } \varphi = \mathbb{Z}$  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:**  $K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[3]{5})$  and  $L = \mathbb{C}$ .

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

$$\begin{aligned}\sigma_1 : \sqrt{2} &\mapsto \sqrt{2} \\ \sigma_2 : \sqrt{2} &\mapsto -\sqrt{2}\end{aligned}$$

which are both automorphisms.

- $K = \mathbb{Q}(\sqrt[4]{2})$ : we have that  $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[4]{2})$  then  $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$  and  $X^4 - 2$  nullifies  $\sqrt[4]{2}$  then we have that  $\text{Irr}(\sqrt[4]{2}, \mathbb{Q}, X) = X^4 - 2$ , and we get that the set of conjugates of  $\sqrt[4]{2}$  over  $\mathbb{Q}$  are  $\{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$  and since

$\text{Char}(\mathbb{Q}) = 0$  then the following 4 embeddings are the only ones

$$\begin{aligned}\sigma_1 : \sqrt[4]{2} &\mapsto \sqrt[4]{2} & \sigma_2 : \sqrt[4]{2} &\mapsto -\sqrt[4]{2} \\ \sigma_3 : \sqrt[4]{2} &\mapsto i\sqrt[4]{2} & \sigma_4 : \sqrt[4]{2} &\mapsto -i\sqrt[4]{2}\end{aligned}$$

and only  $\sigma_1, \sigma_2$  are automorphisms.

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

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

and only  $\sigma_1$  is an automorphism.

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

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

$$\begin{aligned}\sigma_1 : \sqrt[4]{2} &\mapsto \sqrt[4]{2} \\ \sigma_2 : \sqrt[4]{2} &\mapsto -\sqrt[4]{2}\end{aligned}$$

**Question 1.2.3:** Determine all embeddings 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  $\text{Irr}(\alpha, \mathbb{F}_2, X) = P(X)$ ,  $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2$  thus there are two conjugates of  $\alpha$  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

$$\begin{aligned}\sigma_1 : \alpha &\mapsto \alpha \\ \sigma_2 : \alpha &\mapsto \alpha^2\end{aligned}$$

which are both automorphisms.

**Question 1.2.4:** Determine all embeddings 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  $\Omega$  an algebraically closed field.

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

Define the map

$$\cdot^\tau : K[X] \rightarrow K^\tau[X] = \tau(K)[X]$$

$$P(X) = \sum_{i=0}^n a_i X^i \mapsto P^\tau(X) = \sum_{i=0}^n \tau(a_i) X^i$$

•  $\cdot^\tau$  is an isomorphism:

►  $\cdot^\tau$  is an homomorphism: Let  $P(X) = \sum_{i=0}^n p_i X^i$  and  $Q(X) = \sum_{i=0}^n q_i X^i$  we have

$$\begin{aligned} (P+Q)^\tau(X) &= \sum_{i=0}^n \tau(p_i + q_i) X^i \\ &= \sum_{i=0}^n (\tau(p_i) + \tau(q_i)) X^i \\ &= P^\tau(X) + Q^\tau(X) \\ (PQ)^\tau &= \sum_{i=0}^{2n} \tau\left(\sum_{j=0}^i p_j q_{i-j}\right) X^i \\ &= \sum_{i=0}^{2n} \sum_{j=0}^i \tau(p_j) \tau(q_{i-j}) X^i \\ &= P^\tau Q^\tau \end{aligned}$$

►  $\cdot^\tau$  is bijective: its surjective by definition

$$\begin{aligned} \text{Ker } \cdot^\tau &= \{P \in K[X] \mid P^\tau(X) = 0\} \\ &= \left\{P \in K[X] \mid \sum_{i=0}^n \tau(p_i) X^i = 0\right\} \\ &= \{P \in K[X] \mid \forall i \in \llbracket 1, n \rrbracket, \tau(p_i) = 0\} \\ &= \{P \in K[X] \mid p_i = 0\} = \{0\} \end{aligned}$$

•  $\cdot^\tau$  preserves irreducibility, that is, if  $P$  is irreducible in  $K[X]$  then it is irreducible in  $K^\tau[X]$ :

► Suppose that  $P$  is irreducible and  $P^\tau$  is reducible, so  $P^\tau(X) = Q(X)R(X)$  then  $P(X) = (Q(X)R(X))^{\tau^{-1}} = Q^{\tau^{-1}}(X)R^{\tau^{-1}}(X)$  and thus  $P$  is reducible, contradiction.

• Consider  $P(X) = \text{Irr}(\theta, K, X)$ ,  $P^\tau(X)$  is irreducible, and  $K^\tau \subseteq \Omega$  and  $\Omega$  is algebraically closed thus there is an element  $\theta' \in \Omega$ ,  $P^\tau(\theta') = 0$ . We define the map

$$\begin{aligned} \varphi : K[X] &\rightarrow K^\tau[X]/(P^\tau(X)) \\ Q(X) &\mapsto Q^\tau(X) + (P^\tau(X)) \end{aligned}$$

•  $\varphi$  is a homeomorphism which is easy to verify

$$\begin{aligned} \text{Ker } \varphi &= \{Q \in K[X] \mid \varphi(Q) = (P^\tau(X))\} \\ &= \{Q \in K[X] \mid Q^\tau(X) = P^\tau(X)R(X)\} \\ &= \{Q \in K[X] \mid Q(X) = P(X)R^{\tau^{-1}}(X)\} \\ &= (P(X)) \end{aligned}$$

By applying the First Isomorphism Theorem we get that  $\varphi$  is an isomorphism between  $K(\theta) \cong K[X]/(P(X)) \cong K^\tau[X]/(P^\tau(X)) \cong K^\tau(\theta')$

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

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

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

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

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

1.  $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ , 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  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\theta)$ .
2. By Eisenstein criterion we have

$$\text{Irr}(\sqrt{2}, \mathbb{Q}, X) = X^2 - 2$$

$$\text{Irr}(i, \mathbb{Q}, X) = X^2 + 1$$

thus the conjugates of  $\sqrt{2}$  are  $\{\sqrt{2}, -\sqrt{2}\}$  and of  $i$  are  $\{i, -i\}$ , thus by the proof of the primitive element theorem, by taking  $k \notin \{0, i\sqrt{2}\}$  thus by taking  $k = 1$  we get  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$ .

2.  $\mathbb{C}/\mathbb{R}$ , its clear that  $\mathbb{C} = \mathbb{R}(i)$  thus  $i$  is a primitive element.
3.  $\mathbb{Q}(\sqrt{2}, i, \sqrt{3})/\mathbb{Q}(\sqrt{3})$ , we have  $\mathbb{Q}(\sqrt{2}, i, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{i})(\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{i})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2} + i)$  thus  $\sqrt{2} + i$  is a primitive element of  $\mathbb{Q}(\sqrt{2}, i, \sqrt{3})/\mathbb{Q}(\sqrt{3})$ .
4.  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)/\mathbb{Q}$ , we have from before that  $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$ , thus  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = \mathbb{Q}(\sqrt{2} + i)(\sqrt{3})$ , now consider  $\theta = \sqrt{2} + i$  we have then

$$(\theta - i)^2 = 2 \Rightarrow \theta^2 - 3 = 2\theta i$$

$$\Rightarrow (\theta^2 - 3)^2 = -4\theta^2$$

$$\Rightarrow \theta^4 - 2\theta^2 + 9 = 0$$

we can see that  $\theta$  is a root of  $P(X) = X^4 - 2\theta^2 + 9$ , notice that if  $a$  is a root of  $P$  then so is  $-a, \bar{a}$  and  $-\bar{a}$  thus we get that the conjugates of  $\theta$  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  $k \notin \{0, \sqrt{2/3}, i/\sqrt{3}, (\sqrt{2} + i)/\sqrt{3}\}$ , so taking  $k = 1$  we get that  $\sqrt{2} + \sqrt{3} + i$  is a primitive element.

1.  $\mathbb{Q}(\sqrt[4]{2}, \sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{3}, \sqrt[4]{2})$  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  $\alpha$ ,  $\alpha^2 = \alpha + 1 \in \mathbb{F}(\alpha)$  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  $\alpha$  is a primitive element.

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

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

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

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

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

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

**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  $\text{Irr}(\alpha + \beta, \mathbb{Q}, X)$  is cubic and  $\deg \text{Irr}(\alpha - \beta, \mathbb{Q}, X) = 6$ .

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

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

## 2. Finite Fields

**Exercise 2.1:** Decide whether there exists a finite field having the given number of elements.

$$\begin{array}{l} 4095 \quad - \quad 191 \quad - \quad 12345678910 \\ 81 \quad - \quad 12396 \quad - \quad 128 \end{array}$$

the fields have a cardinal of the form  $p^n$  with  $p$  prime, If a number has more than one prime divisor then it is not of the form  $p^n$  thus there is no field with such cardinality. There are no fields with cardinality 4095, 12345678910, 12396 since their prime decomposition have multiple primes while 191, 81, 128 are powers of primes thus there exists a field having their cardinality which are  $\mathbb{F}_{191}$ ,  $\mathbb{F}_{3^4}$ ,  $\mathbb{F}_{2^7}$  respectively.

**Exercise 2.2:** 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:  $\alpha$  with  $\alpha^2 + \alpha + 1 = 0$ .
    - Basis Over  $\mathbb{F}_2$ :  $\{1, \alpha\}$
    - Generator:  $\alpha$ .
  - $n = 3$ :
    - Field:  $\mathbb{F}_{2^3} = \mathbb{F}_8$ .
    - Primitive Element:  $\alpha$  with  $\alpha^3 + \alpha + 1 = 0$ .
    - Basis Over  $\mathbb{F}_2$ :  $\{1, \alpha, \alpha^2\}$ .
    - Generator:  $\alpha$ .
- $p = 3$ :
  - $n = 1$ :
    - 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:  $\alpha$  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.

**Exercise 2.3:** Let  $p$  denote a prime number and let  $m, n$  be positive integers.

**Question 2.3.1:** Let  $P \in \mathbb{F}_p[X]$  be irreducible, show that  $P$  is a factor of the polynomial  $X^{p^n} - X$  for some  $p$  prime and  $n \in \mathbb{N}$ .

**Question 2.3.2:** Prove that a finite field with  $p^n$  elements admits exactly one subfield having  $p^m$  elements for each divisors of  $m$  in  $n$ .

**Question 2.3.3:** Suppose  $\mathbb{F}_{p^m}$  is a subfield of  $\mathbb{F}_{p^n}$  prove that  $m$  divides  $n$ .

**Question 2.3.4:** Deduce that the number of subfields of  $\mathbb{F}_{p^n}$  is equal to the number of divisors of  $n$ .

**Exercise 2.4:** Let  $p$  be a prime number and  $n \in \mathbb{N}$ , show that the polynomial  $x^{p^n} - x \in \mathbb{F}_p[X]$  is the product of all irreducible monic polynomials in  $\mathbb{F}_p[X]$  with degrees dividing  $n$ .

**Exercise 2.5:** Verify certain results from Chapter 2

**Question 2.5.1:** Using the fact that  $P_0(X) = X^2 + X + 1$  is the unique quadratic irreducible element of  $\mathbb{F}_2[X]$ . Prove that the polynomials  $P_1(X) = X^4 + X + 1$ ,  $P_2(X) = X^4 + X^3 + 1$ ,  $P_3(X) = X^4 + X^3 + X^2 + X + 1$  are irreducible over  $\mathbb{F}_2$ .

**Question 2.5.2:** Let  $\alpha, \beta, \gamma$  be the zeros of  $P_1, P_2, P_3$  respectively, in a fixed algebraic closure  $\overline{\mathbb{F}_2}$ . Find bases of  $\mathbb{F}_2(\alpha), \mathbb{F}_2(\beta), \mathbb{F}_2(\gamma)$ , what is the number of elements of each of these fields.

**Question 2.5.3:** Show that  $1/\beta$  is a conjugate of  $\alpha$  and  $1 + \gamma$  is a conjugate of  $\beta$  over  $\mathbb{F}_2$ .

**Question 2.5.4:** Express  $\alpha^5$  in terms of  $1, \alpha, \alpha^2, \alpha^3$ . Deduce that  $\alpha$  generates  $\mathbb{F}_2(\alpha)^*$ .

**Question 2.5.5:** Express  $\alpha^8$  in terms of  $1, \alpha, \alpha^2, \alpha^3$ . Deduce that the conjugates of  $\alpha$  over  $\mathbb{F}_2$  are  $\alpha, \alpha^2, \alpha^4, \alpha^8$ .

**Question 2.5.6:** Deduce from the the last two points that  $\beta$  generates  $\mathbb{F}_2(\beta)^*$  and the set of conjugates of  $\beta$  over  $\mathbb{F}_2$  is  $\{\alpha^{14}, \alpha^{13}, \alpha^{11}, \alpha^7\}$ .

**Question 2.5.7:** Verify that the set of conjugates of  $\gamma$  over  $\mathbb{F}_2$  is  $\{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\} = \{\gamma, \gamma^2, \gamma^4, \gamma^8\}$ ,  $\mathbb{F}_2(\alpha) = \mathbb{F}_2(\beta) = \mathbb{F}_2(\gamma)$  and the order of  $\gamma$  in the group  $\mathbb{F}_2(\gamma)^*$  is 5.

**Question 2.5.8:** Prove that  $\alpha^5$  and  $\alpha^{10}$  are zeros of  $P_0$  and  $\mathbb{F}_2(\alpha^5)$  is a quadratic subfield of  $\mathbb{F}_2(\alpha)$ . Verify that the decomposition of the polynomial  $X^{16} - X$  into irreducible elements of  $\mathbb{F}_2[X]$  is given by  $X(X - 1)P_0P_1P_2P_3$ .

### 3. Normal Extensions

**Exercise 3.1:** Decide whether each of the following extensions is normal:

1.  $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ .
2.  $\mathbb{C}/\mathbb{R}$ .
3.  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)/\mathbb{Q}$ .
4.  $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2})/\mathbb{Q}$ .
5.  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[4]{2})/\mathbb{Q}(\sqrt[4]{2})$ .
6.  $\mathbb{Q}(\sqrt[3]{5}, i)/\mathbb{Q}$ .
7.  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ .
8.  $\mathbb{F}_2(\alpha, \beta, \alpha + \beta)/\mathbb{F}_2$  with  $\alpha^2 + \alpha + 1 = 0$  and  $\beta^{2025} + \beta + 1 = 0$ .

**Exercise 3.2:** Show in three different ways that each of the following field extensions  $L/K$  is normal.

**Question 3.2.1:**  $L = K$ .

1. **Conjugates:** Let  $\alpha \in K$  then  $\text{Irr}(\alpha, K, X) = X - \alpha$  which has exactly one root  $\alpha$  which is in  $K$ , so all conjugates of  $\alpha$  are in  $L$ , thus  $L/K$  is normal.
2. **Splitting Field:** Take the family  $\mathcal{F} = \{X - \alpha \mid \alpha \in K\}$  so every  $f \in \mathcal{F}$  splits over  $K$  since  $\forall \alpha \in K, K(\alpha) = K$ . So  $L/K$  is normal since it's splitting field of the family  $\mathcal{F}$ .
3. **Embeddings:** Let  $\sigma : L \rightarrow \overline{K}$  be a  $K$ -embedding into  $\overline{K}$ . since  $\sigma$  is the identity on  $K$  then its an automorphism so  $L/K$  is normal.

**Question 3.2.2:**  $L$  is an algebraic closure of  $K$ .

1. **Definition:** Let  $P \in K[X]$  irreducible and  $\alpha \in L$  such that  $P(\alpha) = 0$ . As  $L$  is the algebraic closure then  $L$  is algebraically closed thus all zeros of  $P$  are in  $L$  and we have that  $L/K$  is normal.
2. **Splitting Field:** Since  $L$  is the algebraic closure of  $K$  then  $L$  is the splitting field of the family  $\mathcal{F} = K[X]$  thus the extension  $L/K$  is normal.
3. **Embeddings:** Let  $\sigma : L \rightarrow \overline{K} = L$  is an endomorphism and since it is an  $K$ -embedding and  $L/K$  is algebraic then  $\sigma$  is surjective by the course Proposition 1.1.6 thus it is an automorphism from  $L$  to  $L$ .

**Question 3.2.3:**  $L$  is a quadratic extension of  $K$ .

**Note:** If  $[L : K] = p$  prime number, then there exists  $\theta$  a primitive element for  $L/K$ , that is because by taking  $\theta \in L$ ,  $K \subseteq K(\theta) \subseteq L$  and we have that  $[L : K] = [L : K(\theta)] \cdot [K(\theta) : K]$  and thus we get that  $[K(\theta) : K] = 1$  if and only if  $\theta \in K$  thus by taking  $\theta \in L \setminus K$  we have that  $[K(\theta) : K] = p$  necessarily and thus  $K(\theta) = L$ .

1. **Conjugates:** Let  $\theta \in L$ , if  $[K(\theta) : K] = 1$  then the conjugates of  $\theta$  is just  $\theta$  which is in  $K(\theta)$ , else if  $[K(\theta) : K] = 2$  then  $\text{Irr}(\theta, K, X) = X^2 + aX + b$ , let  $\theta'$  be the conjugate of  $\theta$  over  $K$ , then  $\text{Irr}(\theta, K, X) = (X - \theta)(X - \theta') = X^2 - (\theta + \theta')X + \theta\theta' \in K[X]$  thus  $a = \theta + \theta' \in K$  and we get  $\theta' = a - \theta \in K(\theta) \subseteq L$  thus the conjugates of  $\theta$  which are  $\theta, \theta'$  are in  $L$  thus it is normal.

**Exercise 3.3:** Show that the degree of a splitting field of the polynomial  $X^p - 1 \in \mathbb{Q}[X]$  over  $\mathbb{Q}$  with  $p$  prime is equal to  $p - 1$ .

Consider  $P(X) = X^p - 1 = (X - 1)(X^{p-1} + \dots + X + 1) = (X - 1)\Phi(X)$ ,  $\Phi(X)$  is irreducible and its zeros are the roots of unity thus the splitting field of  $P$  is  $\mathbb{Q}(\xi)$ ,  $\xi = e^{\frac{2\pi}{p}i}$  which has degree  $[\mathbb{Q}(\xi), \mathbb{Q}] = \deg \Phi = p - 1$ . The polynomial  $\varphi(X)$  is irreducible since  $\varphi(X + 1)$  is  $p$ -Eisenstein.

**Question 3.3.1:** Give another proof for Proposition 3.10

Let  $\sigma$  be a  $L$ -embedding of  $L$  into  $\Omega$ , since  $K \subseteq L$  then  $\sigma$  is a  $K$ -embedding of  $L$  into  $\Omega$  since  $M/K$  is normal then  $\sigma$  is an isomorphism of  $M$ .

**Exercise 3.4:**

**Question 3.4.1:**

**Question 3.4.2:** Let  $\alpha, \beta \in \overline{K}$ , and  $S_\alpha, S_\beta$  the splitting fields of  $\text{Irr}(\alpha, K, X)$  and  $\text{Irr}(\beta, K, X)$ .