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 $\varphi(a_0 + a_1X + ... + a_nX^n) = a_0$, 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 $\sigma : K(\theta) \to \Omega$.*

Define the map

$$\cdot^\tau : K[X] \to K^\tau[X] = \tau(K)[X]$$
$$P(X) = \sum_{i=0}^{n} a_i X^i \mapsto P^\tau(X) = \sum_{i=0}^{n} \tau(a_i) X^i$$

- $\cdot^\tau$ 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

$$\begin{aligned}(P+Q)^\tau(X) &= \sum_{i=0}^{n} \tau(p_i + q_i) X^i \\ &= \sum_{i=0}^{n} (\tau(p_i) + \tau(q_i)) X^i \\ &= P^\tau(X) + Q^\tau(X)\end{aligned}$$

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

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

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

- $\cdot^\tau$ preserves irreduciblility, that is, if P is irreducible in $K[X]$ then it is irreducible in $K^\tau[X]$:
  - Suppose that P is irreducible and P^τ 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 $P(X) = \operatorname{Irr}(\theta, K, X)$, $P^\tau(X)$ is irreducible, and $K^\tau \subseteq \Omega$ and Ω is algebraically closed thus there is an element $\theta' \in \Omega$, $P^\tau(\theta') = 0$. We define the map

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

- φ is a homeomorphism which is easy to verify

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

By applying the First Isomorphism Theorem we get that φ 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 $\operatorname{Char} K = 0$ and $[K(\theta) : K] = n$ then there is exactly n extensions to $K(\theta)$.*

Question 1.3.3: *Apply the above to each embedding $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ 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. $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$.
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

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

   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

$$\begin{aligned}(\theta - i)^2 = 2 &\Rightarrow \theta^2 - 3 = 2\theta i \\ &\Rightarrow (\theta^2 - 3)^2 = -4\theta^2 \\ &\Rightarrow \theta^4 - 2\theta^2 + 9 = 0\end{aligned}$$

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 $1, \theta, \ldots, \theta^{n-1}$ 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 $\theta_1, \ldots, \theta_n$ 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 $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(a\sqrt{2} + b\sqrt{3}\right)$.*

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. Finite Fields

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

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

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: 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.

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 eleemnts 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 thhe 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 α, β, γ 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 α and $1 + \gamma$ is a conjugate of β over $\mathbb{F}_2$.*

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

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

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

Question 2.5.7: *Verify that the set of conjugates of γ 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 γ in the group $\mathbb{F}_2(\gamma)^*$ is 5.*

Question 2.5.8: *Prove that α^5 and α^{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. $\mathbb{Q}\left(\sqrt{2}, i\right)/\mathbb{Q}$.
2. $\mathbb{C}/R$.
3. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, i\right)/\mathbb{Q}$.
4. $\mathbb{Q}\left(\sqrt{2}, \sqrt[4]{2}\right)/\mathbb{Q}$.
5. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt[4]{2}\right)$.
6. $\mathbb{Q}\left(\sqrt[3]{5}, i\right)/\mathbb{Q}$.
7. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$
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 $\operatorname{Irr}(\alpha, K, X) = X - \alpha$ which has exactly one root α which is in K, so all conjugates of α 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 $\sigma : L \to \overline{K}$ be a K-embedding into $\overline{K}$. since σ 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 $\sigma : L \to \overline{K} = L$ is an endomorphism and since it is an K-embedding and L/K is algebraic then σ 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 θ 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 θ is just θ which is in $K(\theta)$, else if $[K(\theta) : K] = 2$ then $\operatorname{Irr}(\theta, K, X) = X^2 + aX + b$, let θ' be the conjugate of θ over K, then $\operatorname{Irr}(\theta, K, X) = (X - \theta)(X - \theta') = X^2 - (\theta + \theta')X + \theta\theta' \in K[X]$ thus $a = \theta + \theta' \in K$ and we get $\theta' = a - \theta \in K(\theta) \subseteq L$ thus the conjugates of θ which are θ, θ' 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 $P(X) = X^p - 1 = (X-1)(X^{p-1} + \cdots + X + 1) = (X-1)\Phi(X)$, $\Phi(X)$ 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 σ be a L-embedding of L into Ω, since $K \subseteq L$ then σ is a K-embedding of L into Ω since M/K is normal then σ is an isomorphism of M.

Exercise 3.4:

Question 3.4.1: *Find the normal closure of the following fields.*

1. $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$.
2. $\mathbb{Q}\left(\sqrt[3]{5}\right)/\mathbb{Q}$.
3. $\mathbb{C}/\mathbb{Q}\left(\sqrt{3}\right)$.
4. $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5}\right)/\mathbb{Q}$.
5. $\mathbb{Q}\left(\sqrt[40]{2}\right)/\mathbb{Q}\left(\sqrt[20]{2}\right)$.
6. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt[4]{2}\right)$.
7. $\mathbb{Q}\left(\sqrt[3]{5}, i\right)/\mathbb{Q}$.

1. $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ is normal thus the algebraic closure.
2. $\mathbb{Q}\left(\sqrt[3]{5}\right)/\mathbb{Q}$, $\sqrt[3]{5}$ is a root of $X^3 - 5$ which is 5-Eisenstein and thus $\operatorname{Irr}\left(\sqrt[3]{5}, \mathbb{Q}, X\right) = X^3 - 5$, and thus the extension $\mathbb{Q}\left(\sqrt[3]{5}, j\sqrt[3]{5}, j^2\sqrt[3]{5}^2\right) = \mathbb{Q}\left(\sqrt[3]{5}, j\sqrt[3]{5}\right)$ is the normal closure of $\mathbb{Q}\left(\sqrt[3]{5}\right)$ which is normal since it is the splitting field of $X^3 - 5$.
3. $\mathbb{C}/\mathbb{Q}\left(\sqrt{3}\right)$ is a normal extension since $\mathbb{C}$ is an algebraically closed field containing $\mathbb{Q}$ then $\mathbb{C}/\mathbb{Q}$ is normal and since $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{3}\right) \subseteq \mathbb{C}$ then $\mathbb{C}/\mathbb{Q}\left(\sqrt{3}\right)$ is normal.
4. $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5}\right)/\mathbb{Q}$: we have that $\operatorname{Irr}\left(\sqrt{2}, \mathbb{Q}, X\right) = X^2 - 2, \operatorname{Irr}\left(\sqrt[3]{3}, \mathbb{Q}, X\right) = X^3 - 3, \operatorname{Irr}\left(\sqrt[5]{5}, \mathbb{Q}, X\right) = X^5 - 5$ and thus by considering the family $\mathcal{F} = \{X^2 - 2, X^3 - 3, X^5 - 5\}$ we get that the normal closure of $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5}\right)$ is $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5}, j, \xi\right)$ where ξ is a root of $X^5 - 1 = 0$.
5. $\mathbb{Q}\left(\sqrt[40]{2}\right)/\mathbb{Q}\left(\sqrt[20]{2}\right)$

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

4. Series: Groups.

Exercise 4.5: *Let G be a group such that the intersection of all its subgroups other than $\{e\}$ is a subgroup of G different from $\{e\}$. Prove that every element of G has a finite order.*

Let $\{H_i\}_{i\in I}$ be the set of non-trivial subgroups of G, and suppose $\exists y \in \bigcap_{i\in I} H_i \setminus \{e\}$. Let $x \in G$, we have that $\langle x\rangle$ is a subgroup of G thus $y \in \langle x\rangle$ and since it is a subgroup then $y^{-1} \in \langle x\rangle$ too, thus $\exists n, m \in \mathbb{Z}\setminus\{0\}$ (this comes from the fact that $y \neq e$), $y = x^n, y^{-1} = x^m$ and thus we have that $x^{n+m} = x^n \cdot x^m = y \cdot y^{-1} = e$ hence x has finite order.

Exercise 4.6: *Let G be a group, H a subgroup of G and $a \in G$, prove that aHa^{-1} is a subgroup of G isomorphic to H. What happens when H is finite, H is normal.*

1. **aHa^{-1} is a subgroup of G**:
   - $e = aa^{-1} = aea^{-1} \in aHa^{-1}$.
   - Let $axa^{-1}, aya^{-1} \in aHa^{-1}$, $(axa^{-1})^{-1}aya^{-1} = ax^{-1}a^{-1}aya^{-1} = a(x^{-1}y)a^{-1} \in aHa^{-1}$.
2. **aHa^{-1} is isomorphic to H**:
   Consider the map $\varphi : H \to aHa^{-1}, x \mapsto axa^{-1}$, we have $\operatorname{Im}\varphi = aHa^{-1}$ by definition, and $\operatorname{Ker}\varphi = \{h \in H \mid aha^{-1} = e\} = \{h \in H \mid h = a^{-1}a = e\} = \{e\}$ thus φ is an isomorphism from H to aHa^{-1}.
3. **What happens when**
   - H is normal in G: then $aHa^{-1} = H$ for any $a \in G$.
   - H is finite: ?

Exercise 4.7: *Let H and K be two subgroups of G with finite indices in G. Prove that $H \cap K$ is of finite index in G, and find an upperbound for this index.*

Suppose $[G : H]$ and $[G : K]$ are finite. We have

$$\begin{aligned}
[G : H \cap K] &= \#G/(H \cap K) \\
&= \#\{g(H \cap K) \mid g \in G\} \\
&= \#\{(gH) \cap (gK) \mid g \in G\} \\
&\leq \#\{(gH) \cap (g'K) \mid g, g' \in G\} \\
&\leq \#\{h \cap k \mid h \in G/H, k \in G/K\} \\
&\leq \#G/H \cdot \#G/K = [G : H] \cdot [G : K].
\end{aligned}$$

the last inequality comes from the fact that if $h \cap k = h' \cap k'$ then $\exists x \in (h \cap k) \cap (h' \cap k') \Rightarrow x \in (h \cap h')$ and $x \in (k \cap k')$ so $h = h'$ and $k = k'$. Since both $[G : H]$ and $[G : K]$ are finite then so is $[G : H \cap K] \leq [G : H] \cdot [G : K]$.

Exercise 4.8:

Question 4.8.1: *Let a be an element of G and define $N(a) = \{g \in G \mid ga = ag\}$. Show that $N(a)$ is a subgroup of G called the normalized of a in G.*

Let $x, y \in N(a)$ we have that $ax = xa$ and $ay = ya$

- $e \in N(a)$: $ea = a = ae$.
- $x^{-1} \in N(a)$: $(ax)^{-1} = (xa)^{-1} \Rightarrow x^{-1}a^{-1} = a^{-1}x^{-1} \Rightarrow ax^{-1} = x^{-1}a$
- $xy \in N(a)$: $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$.

Thus, $N(a)$ is a subgroup.

Question 4.8.2: *Let H be a subgroup of G, define*
- *Centralizer: $Z(H) = \{g \in G \mid \forall h \in H, gh = hg\}$.*
- *Normalizer: $N(H) = \{g \in G \mid gHg^{-1} = H\}$.*

Prove that $Z(H)$ and $N(H)$ are subgroups of G.

- Centralizer: Notice that $Z(H) = \bigcap_{h\in H} N(h)$ which are all subgroups so $Z(H)$ is a subgroup.
- Normalizer: let $x, y \in N(H)$
  - $e \in N(H)$: $eHe^{-1} = H$.
  - $x^{-1} \in N(H)$: $xHx^{-1} = H \Rightarrow H = x^{-1}Hx$.
  - $xy \in N(H)$: $xyH(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H$.

Question 4.8.3:
- *Prove that $H \subseteq N(H)$.*
- *Give an example of $Z(H) \neq N(H)$.*

- let $x \in H$ then $\forall h \in H, xhx^{-1} \in H$ since it is closed.
- it is easy to notice that $Z(H) \subseteq N(H)$. Consider $G = S_3$ and $H = \langle\sigma\rangle$ with

$$\sigma = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$$

notice that $Z(H) = H$ and $N(H) = G$ so $Z(H) \neq N(H)$.

Exercise:
- ▸ *Prove that $N(H)$ is the largest subgroup of G in which H is normal.*
  ▸ *Prove that H is normal in $G \Leftrightarrow N(H) = G$.*
- ▸ *Prove that $Z(G)$ is a normal subgroup in G.*
  ▸ *Deduce that a group of order 9 is abelian.*

- ▸ It is clear that H is normal in $N(H)$. Let K be a subgroup of G such that H is normal in K, let $k \in K$, since H is normal in K then $kHk^{-1} = H$ but since $K \subseteq G$ then $k \in N(H)$. Thus, $K \subseteq N(H)$, $N(H)$ is the largest subgroup of G where H is normal.
  ▸ $\Rightarrow$ suppose H is normal, then $\forall g \in G, gHg^{-1} = H$ thus $G \subseteq N(H) \subseteq G \Rightarrow G = N(H)$. $\Leftarrow$ if $N(H) = G$ then $\forall g \in G, gHg^{-1} = H$ so H is normal in G.

- ▸ Proving that $Z(G)$ is a normal subgroup of G, let $z \in Z(G), g \in G$, $gzg^{-1} = (gz)g^{-1} = (zg)g^{-1} = z(gg^{-1}) = z \in Z(G)$.
  ▸ ?

Exercise 4.9:

Question 4.9.1: *Let G be a finite group of order p^2. Show that G is abelian when its center is not reduced to the identity element.*

Suppose $Z(G) \neq \{e\}$, then we have that $\#\, G/Z(G) = p$ so $G/Z(G) \cong F_p$ which is cyclic, and thus G is abelian.

Question 4.9.2: *Show that a group G of order 6 is isomorphic to S_3 or $\mathbb{Z}_6$.*

- Case 1: $\exists x \in G, o(x) = 6$, then $G = \langle x \rangle$ so $G \cong \mathbb{Z}_6$.
- Case 2: G has no element of order 6.

Exercise 4.10: *Let G be a group and let $G' = \{[x : y] \mid x, y \in G\}$ be the commutator of G.*

Question 4.10.1: *Prove that G' is a normal subgroup of G.*

Let $g \in G$, then let $x, y, g \in G$, we have that

$$\begin{aligned} [g : [x : y]] &= g[x : y]g^{-1}[x : y]^{-1} \\ \Rightarrow g[x : y]g^{-1} &= [g : [x : y]][x : y] \end{aligned}$$

notice that both $[g : [x : y]], [x : y] \in G'$ then $g[x : y]g^{-1} \in G'$ so $\forall g \in G, gG'g \subseteq G'$ so G' is a normal subgroup of G.

Question 4.10.2: *Prove that G/G' is abelian.*

Let $x, y \in G$, $xG' \cdot yG' = xyG'$ but since $x, y \in G$ then $[x : y] \in G'$ so $[x : y]^{-1} \in G'$, then $yx = [x : y]^{-1}xy \in xyG'$ thus $xyG' = yxG'$ so the group G/G' is abelian.

Question 4.10.3: *Let H be a normal subgroup of G, if G/H is abelian then $G' \subseteq H$.*

Let H be a normal subgroup of G and G/H is abelian. Let $x, y \in G$ we have then

$$\begin{aligned} [x : y]H &= xyx^{-1}y^{-1}H \\ &= (xy)H \cdot (x^{-1}H)(y^{-1}H) \\ &= (xy)H \cdot (y^{-1}H)(x^{-1}H) \\ &= xyy^{-1}x^{-1}H = H \end{aligned}$$

thus $G' \subseteq H$.

Question 4.10.4: *If H is a subgroup of G and $G' \subseteq H$, then H is normal in G.*

Let H be a subgroup of G with $G' \subseteq H$, let $g \in G$ and $h \in H$. We have that $[g : h] = ghg^{-1}h^{-1}$ thus $ghg^{-1} = [g : h]h^{-1}$, and since $[g : h] \in G' \subseteq H$ and $h^{-1} \in H$ then $ghg^{-1} = [g : h]h^{-1} \in H$ thus H is normal in G.

Exercise 4.11: *Let $n \in \mathbb{N}$ and s, r two formal variables satisfying $s^2 = e, r^n = e, sr = r^{-1}s$, define $D_{2n} = \{s^i r^i \mid i, j \in \mathbb{N}\}$.*

Question 4.11.1: *Find the number of subgroups of order 2, 3 of D_{2n}.*

- Subgroups of order 2: The subgroups of order 2 should be of the form $\{e, x\}$ with $o(x) = 2$, thus we start with finding the elements of order 2.
  ▸ Case 1: $x = sr^k \Rightarrow x^2 = \left(sr^k\right)^2 = sr^k sr^k = sr^k r^{-k}s = s^2 = e$ thus any element of the form sr^k is of order 2.
  ▸ Case 2: $x = r^k \Rightarrow x^2 = \left(r^k\right)^2 = r^{2k}$ but r has order n thus if x is of order 2, n is even and we have that $x = r^{n/2}$ is the only element of the form r^k that has order 2.

  To count now we have that the number of subgroups of order 2, we count how many different elements of order 2 do we have: we have n elements from the first case $sr^k, k \in [\![0, n-1]\!]$, if n is even then there is an extra element so:
  ▸ if n is even: $n + 1$ subgroups of order 2.
  ▸ if n is odd: n subgroups of order 2.
- Subgroups of order 3: it is the same here, since any group of order 3 is cyclic then necessarily any subgroup would be of the form $\langle x \rangle$ where $o(x) = 3$.
  ▸ Case 1: $x = sr^k \Rightarrow x^3 = \left(sr^k\right)^2 sr^k = sr^k = x$ thus $x = e$ so there is no element of the form sr^k that has order 3.
  ▸ Case 2: $x = r^k \Rightarrow x^3 = r^{3k}$ then 3 should divide n and we get one element of order 3.

  so same as before:
  ▸ if n is divisible by 3: there is one subgroup of order 3.
  ▸ if n is not divisible by 3: there is no subgroup of order 3.

Question 4.11.2: *Determine the center of the Dihedral group D_{2n}.*

For the ease of calculation, we can easily prove by induction that $r^j s^i = s^i r^{(-1)^i j}$, consider the element $x \in \mathcal{Z}(D_{2n})$ and $y \in D_{2n}$ of the form $y = s^i r^j$ for all i, j, there are two cases

- $x = r^k$: $xy = yx \Rightarrow r^k s^i r^j = s^i r^j r^k \Rightarrow s^i r^{(-1)^i k} r^j = s^i r^j r^k \Rightarrow r^{(-1)^i k} = r^k \Rightarrow r^{(1-(-1)^i)k} = e$ thus by taking i odd we get that $2k = n$ so if n is even then $r^{n/2}$ is in the center.

- $x = sr^k$: $xy = yx \Rightarrow sr^k s^i r^j = s^i r^j sr^k \Rightarrow s^{i+1} r^{j-k} = s^{i+1} r^{k-j} \Rightarrow \left(r^{j-k}\right)^2 = e$ which is impossible for all j.

Thus the center of D_{2n} is

$$\mathcal{Z}(D_{2n}) = \begin{cases} \{e\} \text{ if } n \text{ odd} \\ \{e, r^{n/2}\} \text{ if } n \text{ even} \end{cases}$$

Question 4.11.3: *Prove that the commutator of D_{2n} is generated by r^2.*

Let $x, y \in D_{2n}$, $x = s^i r^j$ and $y = s^{i'} r^{j'}$ then

$$\begin{aligned} xy &= s^i r^j s^{i'} r^{j'} \\ &= s^i s^{i'} r^{(-1)^{i'} j} r^{j'} \\ &= s^{i+i'} r^{(-1)^{i'} j + j'} \\ xyx^{-1} &= s^{i+i'} r^{(-1)^{i'} j + j'} r^{-j} s^{-i} \\ &= s^{i+i'} r^{(-1)^{i'} j + j' - j} s^{-i} \\ &= s^{i'} r^{(-1)^i \left((-1)^{i'} j + j' - j\right)} \\ [x, y] = xyx^{-1}y^{-1} &= s^{i'} r^{(-1)^i \left((-1)^{i'} j + j' - j\right)} r^{-j'} s^{-i'} \\ &= s^{i'} r^{(-1)^i \left((-1)^{i'} j + j' - j\right) - j'} s^{-i'} \\ &= r^{(-1)^{-i'} \left((-1)^i \left((-1)^{i'} j + j' - j\right) - j'\right)} \end{aligned}$$

by expanding the last term we get $[x, y] = r^{\left((-1)^{i'} - (-1)^i\right) j}$ and since $(-1)^{i'} - (-1)^i \in \{0, 2, -2\}$ then $[x, y] \in \langle r^2 \rangle$, and by taking $k \in \mathbb{N}, r^{2k} = \left[sr^k, r^k\right]$ thus $[D_{2n}, D_{2n}] = \langle r^2 \rangle$.

Exercise 4.12: *Let H and K be two subgroups of G.*

Question 4.12.1: *Prove that if H or K is normal then HK is a subgroup of G.*

Suppose that H is normal, we have from the course that HK is a subgroup if and only if $HK = KH$. Since H is normal, then $\forall k \in K, kHk^{-1} = H$ and thus $\forall k \in K, kH = Hk \Rightarrow KH = HK$, so HK is a subgroup of G.

Question 4.12.2: *Prove that if H and K are normal then so are HK and $H \cap K$.*

Suppose that H and K are normal

- HK is normal: Let $g \in G$, $gHKg^{-1} = gHg^{-1}gKg^{-1} = (gHg^{-1})(gKg^{-1}) = HK$ thus HK is normal.
- $H \cap K$ is normal: Let $g \in G$, $g(H \cap K)g^{-1} = (gHg^{-1}) \cap (gKg^{-1}) = H \cap K$ thus $H \cap K$ is normal.

Question 4.12.3: *Prove that HK/K and $H/(H \cap K)$ are isomorphic.*

Define the map $\varphi : H \to HK, h \mapsto h$, it is well defined and it is a homomorphism. We have that $\varphi^{-1}(K) = \{h \in H \mid h \in K\} = H \cap K$ and since $H \cap K$ is normal in G then it is in H and thus we get by the course lemma that $H/(H \cap K) \cong HK/K$.

Question 4.12.4: *Prove that HK/H and $K/(H \cap K)$ are isomorphic.*

In similar fashion, take $\varphi : K \to HK, k \mapsto k$, $\varphi^{-1}(k) = K \cap H$ and thus $HK/H \cong K/(H \cap K)$.

Exercise 4.13: *Let G be a non-abelian group of order 8.*

Question 4.13.1: *Show there exists $y \in G$ of order 4 and $x \in G \setminus H$ where $H = \langle y \rangle$ and $G = H \cup xH$.*

Since the group is non-abelian then all non-neutral elements have order either 2 or 4. If every non-neutral element of G has order 2, then G would be abelian since $\forall x, y \in G, x = x^{-1}, y = y^{-1}, xy = (xy)^{-1}$, $yx = y^{-1}x^{-1} = (xy)^{-1} = xy$, thus there is necessarily an element of order 4, denote it y. Let $x \in G \setminus H$, we have that $H \cap xH = \emptyset$ since if $H \cap xH \neq \emptyset$ then $\exists n, m \in \mathbb{N}, y^n = xy^m \Rightarrow x = y^{n-m} \in H$ thus $x \in H$ which is a contradiction, and since $H \cup xH \subseteq G$ and $\#(H \cup xH) = \# H + \# xH - \#(H \cap xH) = \# H + \# xH = 8$ then $H \cup xH = G$. ($\# xH = 4$ since $\forall n, m \in \mathbb{N}, xy^n = xy^m \Rightarrow n = m \bmod 4$ thus are the same element).

Question 4.13.2: *Prove that $x^2 \in \{e, y^2\}$.*

We have that $G = H \cup xH$, since G is a group then $x^2 \in G \Rightarrow x^2 \in H \cup xH$, $x^2 \notin xH$ since if it was, then $x^2 = xy^m \Rightarrow x = y^m \in H$ which is a contradiction, thus $x^2 \in H$. The order of x is either $2, 4$ since the order of the element should divide the order of the group, if x has order 2 then $x^2 = e$, else then the order of x^2 is 2, and the order of elements of H are as follows: $o(y) = 4, o(y^2) = 2, o(y^3) = 4$ thus $x^2 = y^2$.

Question 4.13.3: *Show that if $xy = yx$ then $\forall i, j \in \mathbb{Z}, x^i y^j = y^j x^i$ thus G is abelian.*

Suppose that $xy = yx$. We prove by double induction that $x^i y^j = y^j x^i$, it is enough to prove for $i, j \in \mathbb{N}$ since x, y have finite order.

- $i = 0, j = 0$: $x^0 y^0 = e = y^0 x^0$.
- suppose its true for i, j:
  - $x^{i+1} y^j = x x^i y^j = x y^j x^i = y^j x x^i = y^j x^{i+1}$.
  - $x^i y^{j+1} = x^i y^j y = y^j x^i y = y^j y x^i = y^{j+1} x^i$.

Since the elements of G are of the form $x^i y^j$ then taking two elements $x^i y^j, x^{i'} y^{j'} \in G$ we have

$$\begin{aligned}
\left(x^i y^j\right)\left(x^{i'} y^{j'}\right) &= x^i \left(y^j x^{i'}\right) y^{j'} \\
&= x^i x^{i'} y^j y^{j'} \\
&= x^{i+i'} y^{j+j'} \\
&= x^{i'+i} y^{j'+j} \\
&= x^{i'} \left(x^i y^{j'}\right) y^j \\
&= \left(x^{i'} y^{j'}\right)\left(x^i y^j\right)
\end{aligned}$$

thus G is abelian.

Question 4.13.4: *Deduce that $yx = xy^3$, $y^2 x = xy^2$, $y^3 x = xy$.*

We have that $yx \notin H$ since $yx = y^m \Rightarrow x = y^{m-1} \in H$, $yx \neq x$ since $yx = x \Rightarrow y = e$, $yx \neq xy$ since G is not abelian, and $yx \neq xy^2$ since if $yx = xy^2$ then $x = y^{-1}xy^2 \Rightarrow x^2 = y^{-1}xyxy^2$, if $x^2 = y^2$ then $y^{-1}xyx = e \Rightarrow y^{-1}xy^3 = x$ which results in $y = e$ contradiction, if $x^2 = e$ then $y^{-1}xyxy^2 = e \Rightarrow (xy)^2 = e \Rightarrow yxy = x \Rightarrow yx = xy^3$ then $y = e$ contradiction. So the only element yx can be is xy^3. $yx = xy^3 \Rightarrow y^2 x = yxy^3 = xy^3 y^3 = xy^6 = xy^2 \Rightarrow y^3 x = yxy^2 = xy^3 y^2 = xy^5 = xy$.

Question 4.13.5: *Suppose that $x^2 = e$, prove that G is the Dihedral group D_8.*

If $x^2 = e$, then by taking the mapping $\varphi : G \to D_8$ such that $\varphi(x) = s$ and $\varphi(y) = r$ then we get that φ is an isomorphism.

Question 4.13.6: *Suppose that $x^2 = y^2$, dress the multiplication table of G and verify it is a group.*

$\cdot$	e	y	y^2	y^3	x	xy	xy^2	xy^3
e	e	y	y^2	y^3	x	xy	xy^2	xy^3
y	y	y^2	y^3	e	xy	xy^2	xy^3	x
y^2	y^2	y^3	e	y	xy^2	xy^3	x	xy
y^3	y^3	e	y	y^2	xy^3	x	xy	xy^2
x	x	xy^3	xy^2	xy	y^2	y	e	y
xy	xy	x	xy^3	xy^2	y^3	y^2	y	e
xy^2	xy^2	xy	x	xy^3	e	y^3	y^2	y
xy^3	xy^3	xy^2	xy	x	y	e	y^3	y^2

Which is indeed a group generated by $\langle x, y \rangle$.

Question 4.13.7: *Deduce there are exactly 2 non-abelian groups of order 8.*

The group will either be isomorphic to D_8 or Q_8.

Exercise 4.14: *Let Q_8 be the quaternion group.*

Notice that $Q_8 = \langle x, y \rangle$. To simplify the calculations, we use the formula that is easy to prove by induction $y^j x^i = x^i y^{(-1)^i j}$ and the following lemma

Lemma: *Let $G = \langle S \rangle$ be a group, and $\mathcal{Z}(G)$ be its center. We have that $x \in \mathcal{Z}(G) \Leftrightarrow \forall s \in S, sx = xs$.*

Proof. $\Rightarrow$ Trivial since $S \subseteq G$. $\Leftarrow$ Suppose that $\forall s \in S, sx = xs$, let $y \in G$ then $y = \prod_{i=1}^{n} s_i$ with $s_i \in S$, then $yx = \prod_{i=1}^{n} s_i x = \prod_{i=1}^{n-1} s_i(s_n x) = \prod_{i=1}^{n-1} s_i x s_n = \cdots = x\prod_{i=1}^{n} s_i = xy$. □

Question 4.14.1: *Determine the center and commutator of Q_8.*

- The center $\mathcal{Z}(Q_8)$: let $x^i y^j \in \mathcal{Z}(Q_8)$. We have $xx^i y^j = x^{i+1}y^j$ and $x^i y^j x = x^{i+1}y^{-j}$ so $j = -j \bmod 4 \Rightarrow 2j = 4k \Rightarrow j = 2k$ thus j should be even. $yx^i y^j = x^i y^{(-1)^i + j}$ and $x^i y^j y = x^i y^{j+1}$ thus $j + 1 = (-1)^i + j \bmod 4 \Rightarrow (-1)^i - 1 = 4k$ so necessarily $i = 0$. Thus we obtain that $\mathcal{Z}(Q_8) = \{e, y^2\}$.
- The commutator $[Q_8, Q_8]$:

Question 4.14.2: *Proving that $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_2 \times Q_8$ are not isomorphic even though they have elements all of the same orders.*

Notice that in this case the order of an element (x, y) is the same as the order of an element (y, x). The tables below show the order of each element of the form (x, y).

$\mathbb{Z}_4 \times \mathbb{Z}_4$

·	0	1	2	3
0	1	4	2	4
1	4	4	4	4
2	2	4	2	4
3	4	4	4	4

$\mathbb{Z}_2 \times Q_8$

·	0	1
e	1	2
y	4	4
y^2	2	2
y^3	4	4
x	4	4
xy	4	4
xy^2	4	4
xy^3	4	4

Thus, they both have 1 element of order 1, 3 elements of order 2 and 12 elements of order 4. Suppose that $\mathbb{Z}_4 \times \mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_2 \times Q_8$,

5. Series: Symmetric Groups.

Exercise 5.1: *Let G be a non-abelian group with order 10. Show that G is isomorphic to D_{10}.*

It is easy to generalize, so we prove the following proposition.

Theorem: *Let G be a non-abelian group with order $2p$, then G is isomorphic to D_{2p}.*

Proof. We separate the proof into claims.

- *Claim 1*: $\exists r \in G, o(y) = p$. Suppose by contradiction that there is no element of order p, then every element has order 2, but this makes G abelian, contradiction, thus there is $r \in G$ such that $o(r) = p$. Take $H = \langle r \rangle$.
- *Claim 2*: $\exists s \in G \setminus H, G = H \cup sH$. Consider $s \in G \setminus H$, we have that $\#H = \#sH = p$ and $H \cap sH = \emptyset$ (since if $H \cap sH \neq \emptyset$ then $\exists n, m \in \mathbb{N}, sr^n = r^m \Rightarrow s = r^{m-n} \in H$ which is a contradiction) thus $H \cap sH = \emptyset$, thus $H \cup sH \subseteq G$ and $\#(H \cup sH) = \#G \Rightarrow G = H \cup sH$.
- *Claim 3*: $s^2 = e$. We have that $s^2 \notin sH$, since if it were then $s^2 = sz, z \in H$ thus $s = z \in H$ contradiction, therefore $s^2 \in H$, thus s^2 has either order 1 or p, if its order is p then s has order s^{2p} thus G is cyclic so abelian so it is necessarily 1, thus $s^2 = e$.
- *Claim 4*: $rs = sr^{-1}$. Through the same proof as the previous exercise we get that $rs = sr^{-1}$.

Therefore, we have that G is isomorphic to D_{2p}. □

Exercise 5.2:

Exercise 5.3: *Consider the permutation*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$$

Question 5.3.1: *Computing σ^k for $k \in \mathbb{N}$, and calculate the order of each σ^k.*

$$\sigma^1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix} \qquad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 6 & 5 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 2 & 1 \end{pmatrix} \qquad \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

We have that σ has order 4, σ^2 has order 2 and $\sigma^3 = \sigma^{-1}$ which has order 4.

Question 5.3.2: *Find the cycles of σ and write it as a product of transpositions.*

We have that (1625) and (34) are the cycles of σ thus $\sigma = (1625)(34)$. We use the fact that $(i_1 ... i_k) = (i_1 i_k) \cdots (i_1 i_2)$ then we have that $\sigma = (15)(12)(16)(34)$.

Question 5.3.3: *Find the parity of σ and the parity of each σ^k, $k \in \mathbb{Z}$.*

The parity of σ is even since it has 4 transpositions, thus σ^k would have parity even too, since $\sigma^k = ((15)(12)(16)(34))^k$, which would have $4k$ transpositions.

Exercise 5.4:

Question 5.4.1: *Prove* $(1\ 2 ... n)^{-1} = (n\ n-1 ... 1)$.

$$(1\ 2 ... n) \cdot (n\ n-1 ... 1) = (1)$$

Question 5.4.2: *What is the order of an l-cycle, and the order of products of disjoint cycles of lengths $l_1, ..., l_s$.*