

**Exam Questions**  
*Discrete Mathematics 2: Algebra*

Fall 2025

Vincent Van Schependon

**Question 1:** Let  $(S_5, \circ)$  be the group of permutations of  $A = \{1, 2, 3, 4, 5\}$ . Let  $f$  denote the permutation

$$f := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

- (a) Write  $f$  as a composition of disjoint cycles.
- (b) What are the order and the cycle type of  $f$ ?
- (c) What is the smallest natural number  $n$  such that  $S_n$  contains a permutation of order 10? Motivate your answer.
- (d) Does  $S_9$  contain a permutation of order 18? Motivate your answer.
- (e) What is the maximal order a permutation of  $S_6$  can have? Motivate your answer.

**ANSWER**

- (a) The disjoint cycle decomposition of  $f$  is

$$f = c_1 \circ \dots \circ c_k$$

where  $c_i$  are disjoint cycles and  $\text{ord}(c_i) = \ell_i = \text{number of elements in } c_i$ .

- (b) We're looking for the smallest integer  $i \in \mathbb{Z}_{>0}$  such that  $f^i = \text{id}_A$ .

Because the disjoint cycle decomposition of  $f$  consists of  $k$  cycles  $c_i$  of length  $\ell_i$ , it follows from Proposition 2.3.12 that

$$\text{ord}(f) = \text{lcm}(\ell_1, \dots, \ell_k)$$

To compute the cycle type, let  $t_1$  be the number of elements in  $A$  that are fixed by  $f$  and for  $i > 1$ , let  $t_i$  be the number of  $t_i$ -cycles in the DCD of  $f$ . Then the cycle type of  $f$  is

$$(t_1, \dots, t_{\textcolor{red}{n}})$$

- (c) If  $n = 7$  then a permutation  $g \in S_n$  of order 10 can be found, for example

$$g = (1\ 2)(3\ 4\ 5\ 6\ 7)$$

Now we show that such a permutation does not exist if  $n \leq 6$ , which proves that  $n = 7$  is the smallest natural number such that  $S_n$  contains a permutation of order 10.

Assume that  $n \leq 6$ . Assume further that, by contradiction,  $g \in S_n$  of order  $\text{ord}(g) = 10$  exists. We know that, if  $g = c_1 \circ c_2 \circ \dots \circ c_k$  is the disjoint cycles decomposition of  $g$ , and  $c_i$  is a cycle of length  $\ell_i$  for  $i = 1, \dots, k$ , then

$$\text{ord}(g) = \text{lcm}(\ell_1, \dots, \ell_k)$$

This implies that every cycle length  $\ell_i$  must divide 10. Thus,  $\ell_i \in \{1, 2, 5, 10\}$ . Since  $n \leq 6$ , a 10-cycle is impossible, so the lengths must be 1, 2, or 5. The cycles  $c_i$  thus need to be 5-cycles, 2-cycles or 1-cycles.

---

Now it holds that

$$n = 1 \cdot t_1 + 2 \cdot t_2 + \dots + n \cdot t_n = 1 \cdot \textcolor{red}{t_1} + 2 \cdot t_2 + 5 \cdot t_5 \geq 2 \cdot t_2 + 5 \cdot t_5$$

Since  $t_1 \geq 0$  and at least one of *each* needs to appear in the decomposition of  $f$  (i.e.  $t_2 \geq 1$  and  $t_5 \geq 1$ ), it follows that  $n \geq 2 \cdot 1 + 5 \cdot 1 = 7$ , a *contradiction*.

- (d) No. Indeed, if  $f \in S_9$  and we write  $f = c_1 \circ \dots \circ c_k$  as a disjoint cycle decomposition where  $c_i$  is a cycle of length  $\ell_i$ , then  $\text{ord}(f) = \text{lcm}(\ell_1, \dots, \ell_k)$ .

To have  $\text{ord}(f) = 18$ , each  $\ell_i$  must be a divisor of 18 and satisfy  $\ell_i \leq 9$ . Thus, the possible cycle lengths are:

$$\ell_i \in \{1, 2, 3, 6, 9\}$$

We distinguish two cases:

- **Case 1: No cycle of length 9 exists.**

In this case, all  $\ell_i \in \{1, 2, 3, 6\}$ . None of these numbers are divisible by 9 (they are either not divisible by 3, or divisible by 3 but not 9). Consequently, their least common multiple cannot be divisible by 9. Since 18 is divisible by 9,  $\text{lcm}(\ell_1, \dots, \ell_k) \neq 18$ .

- **Case 2: A cycle of length 9 exists.**

If there is a cycle of length  $\ell_j = 9$ , then because the cycles are disjoint and the total number of elements is 9 (i.e.,  $\sum \ell_i \leq 9$ ), no other non-trivial cycles can exist in the decomposition. Thus  $f$  is a 9-cycle, which implies  $\text{ord}(f) = 9 \neq 18$ .

Since both cases fail to produce an order of 18, such an element cannot exist in  $S_9$ .

- (e) Let  $f \in S_6$  and write  $f = c_1 \circ c_2 \circ \dots \circ c_k$  as a disjoint cycles decomposition where  $c_i$  is a cycle of length  $\ell_i$  for  $i = 1, \dots, k$ . To compute  $\text{ord}(f) = \text{lcm}(\ell_1, \dots, \ell_k)$  we need to understand how the different cycle lengths  $\ell_i$  can be. To do so, let  $m$  denote the maximum of the lengths  $\ell_i$  of the cycles  $c_i$  with  $i = 1, \dots, k$ . Clearly  $m \leq 6$ . We divide some cases:

- $m = 6$ . Then  $k = 1$  and  $f$  is a 6-cycle. The order of  $f$  is 6 in this case.
- $m = 5$ . Then  $f$  is a 5-cycle (recall that any 1-cycle is just the identity permutation). Hence the order of  $f$  is 5 in this case.
- $m = 4$ . Hence either  $f$  is a 4-cycle, or the composition of a 4-cycle and a 2-cycle. In any case the order of  $f$  is 4 as  $\text{lcm}(4, 2) = 4$ .
- $m = 3$ . Here either  $f$  is a 3-cycle, or the composition of 2 3-cycles or the composition of a 3-cycle and a 2-cycle. In the first 2 cases the order of  $f$  is 3 while in the last case  $\text{ord}(f) = \text{lcm}(3, 2) = 6$ .
- $m = 2$ . Then  $f$  is composition of 2-cycles and hence its order is 2.

We conclude that the order of  $f$  is at most 6. We conclude that the order of  $f$  is at most 6.

Note that for any  $m$ -cycle  $g = (a_0 a_1 \dots a_{m-1})$  of order  $\text{ord}(g) = m$ , we have that

$$g^m = \text{id}$$

and furthermore, we have that

$$g^i = g^{i \bmod m}$$

The above obviously holds if  $0 \leq i < m$ , as in this case  $(i \bmod m) = i$ .

In the general case, we can perform *division with remainder* to write

$$i = qm + r, \quad \text{with } 0 \leq r = (i \bmod m) < m \text{ and } q \text{ possibly negative}$$

and then we have that

$$g^i = g^{qm+r} = (g^m)^q \cdot g^r = \text{id}^q \cdot g^r = g^r,$$

and the result follows, as  $r = i \bmod m$ .

**Question 2:** Consider the group  $(G, \cdot)$  and consider the subgroup  $H := \dots$

- (a) Show that  $H$  is a subgroup of  $G$ .
- (b) Show that  $\varphi : \begin{cases} G \rightarrow V \\ g \mapsto \dots \end{cases}$  is a group homomorphism.
- (c) Determine whether  $(G_1, \cdot_1)$  is isomorphic to  $(G_2, \cdot_2)$ .

#### ANSWER

---

- (a) The identity element  $e_G$  is in  $H$ : ...

We can now use Lemma 4.1.2 (proven in an exercise), which says that any *non-empty* set  $H \subseteq G$  is a subgroup of  $G$  if and only if

$$\forall f, g \in H : f^{-1} \cdot g \in H$$

- (b) We prove that the two axioms of a group homomorphism (Definition 6.1.1) hold:

- (a)  $\varphi(e_G) = e_V$ : ...
- (b)  $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$ : ...

---

(c) In order to be isomorphic, the cardinalities must match:  $|G_1| = |G_2|$ .

Furthermore, all elements in  $G_1$  must have the same order as the corresponding elements in  $G_2$  in case both groups are isomorphic.

To see this, assume that the groups are isomorphic ( $G_1 \simeq G_2$ ) via the isomorphism  $\psi : G_1 \rightarrow G_2$ . Let  $\text{ord}(g) = n$  for  $g \in G_1$ .

$$\psi(g)^n = \underbrace{\psi(g) \cdot_2 \dots \cdot_2 \psi(g)}_n \stackrel{(2)}{=} \psi(g \cdot_1 \dots \cdot_1 g) = \psi(g^n) \stackrel{\text{ord}(g)=n}{=} \psi(e_1) \stackrel{(1)}{=} e_2.$$

We conclude that  $\psi(g)^n = e_2$ , so because of Lemma 3.1.12,  $\text{ord}(\psi(g))$  divides  $n$ . Now we show that  $n$  is the smallest such positive integer.

Assume there exists a positive integer  $m < n$  such that  $\psi(g)^m = e_2$ . Then, by similar reasoning as above, we have  $\psi(g^m) = e_2$ .

Now we see that

$$\psi \text{ is bijective} \implies \psi \text{ is injective} \stackrel{\text{Lemma 6.1.8}}{\implies} \ker(\psi) = \{e_1\} \implies g^m = e_1$$

But we assumed that  $\text{ord}(g) = n$  and that  $m < n$ . This gives a contradiction, since the order is by definition the smallest positive integer such that  $g^{\text{ord}(g)} = e_1$ . Therefore, no such  $m$  can exist and we conclude that  $\text{ord}(\psi(g)) = n$ .

**Question 3:** Consider the set  $R = \dots$

- (a) Show that  $(R, +, \cdot)$  is a ring.
- (b) Let  $I := \dots \subseteq R$ . Prove that  $I$  is an ideal of  $R$ .
- (c) Determine whether or not  $I = R$ .
- (d) Consider the map  $\varphi : R \rightarrow S$ . Show that  $\varphi$  is a ring homomorphism.
- (e) Compute the kernel and image of  $\varphi$ .
- (f) Prove that the quotient ring  $R/I$  is isomorphic to  $S$ .

**ANSWER**

- 
- (a) We prove that  $(R, +, \cdot)$  is a ring by showing that it satisfies all the ring axioms from Definition 7.1.1. The zero-element is  $0_R = \dots$  and the one-element is  $1_R = \dots$ 
    - (1)  $(R, +)$  is an abelian group.
      - (i) There exists an identity element  $0_R \in R$ .
      - (ii) The operation  $+$  is **associative**. Take  $a, b, c \in R$  arbitrarily.  
*(Associativity holds in the larger group  $G$ : for any  $a', b', c' \in R$  we have  $a' \cdot (b' \cdot c') = (a' \cdot b') \cdot c'$ , so this particularly holds for  $a = a', b = b', c = c'$ )*
      - (iii)  $(R, +)$  is **closed under inverses**. Take  $a \in R$  arbitrarily.  
Then, its additive inverse is  $a^{-1}$  is also in  $R$ .
      - (iv)  $(R, +)$  is **closed under addition**. Take  $r, s \in R$  arbitrarily. Then,  $r + s = \dots \in R$ .
    - (2) There exists an identity element  $1_R \in R$  for the operation  $\cdot$ :

$$\forall f, g \in R : f \cdot 1_R = f = 1_R \cdot g$$

- (3) The operation  $\cdot$  is **associative**.
- (4) The operations  $+$  and  $\cdot$  satisfy the **distributive laws**.
  
- (b) To prove that  $I$  is an ideal of  $R$ , we prove that (1)  $I$  is a subgroup of  $(R, +)$  and (2)  $\forall r \in R, \forall x \in I : rx \in I$ .
  - (1)  $I$  is a subgroup of  $(R, +)$ :
    - ...
  - (2) Take  $r \in R$  and  $x \in I$  arbitrarily. Then,  $rx = \dots \in I$ .

Because both conditions from Definition 8.1.7 are satisfied, we conclude that  $I$  is an ideal of  $R$ .

- (c) We now show that  $I = R$ .

Recall that  $I = R$  if and only if  $I$  contains the one-element  $1_R$ :

$$I = R \iff 1_R \in I$$

(Also recall that if a unit  $u \in R^*$  is in  $I$ , then  $1_R \in I$  and thus  $I = R$ :  $u \in I \Rightarrow 1_R \in I \Leftrightarrow I = R$ )

Our aim is thus to understand if  $I$  contains  $1_R$  (or if  $I$  contains a unit  $u \in R^*$ ).

---

(d) To show that  $\varphi$  is a ring homomorphism, we show that it satisfies all conditions in Definition Definition 8.1.1:

(1)  $\varphi$  is a group homomorphism:

$$(i) \quad \varphi(0_R) = 0_S$$

$$(ii) \quad \varphi(r +_R s) = \varphi(r) +_S \varphi(s) \text{ for all } r, s \in R.$$

$$(2) \quad \varphi(1_R) = 1_S$$

$$(3) \quad \varphi(r \cdot_R s) = \varphi(r) \cdot_S \varphi(s) \text{ for all } r, s \in R.$$

(e) We compute that

$$\begin{aligned} \ker(\varphi) &\stackrel{\Delta}{=} \{r \in R \mid \varphi(r) = 0_S\} \\ &= \dots \\ \text{im}(\varphi) &\stackrel{\Delta}{=} \{\varphi(r) \mid r \in R\} \\ &= \dots \end{aligned}$$

(f) We show that  $I = \ker(\varphi)$  by proving both inclusions.

$\subseteq$  : Take  $x \in I$  arbitrarily. Then,  $\varphi(x) = \dots = 0_S$ .

$\supseteq$  : Take  $x \in \ker(\varphi)$  arbitrarily. Then,  $x \in I$ .

Now we show that  $\text{im}(\varphi) = S$ , i.e.  $\varphi$  is surjective. Take any  $s \in S$  arbitrarily. Then, we can find a preimage  $r \in R$  such that  $\varphi(r) = s$ . This shows that  $\text{im}(\varphi) = S$ .

We now apply the *Isomorphism Theorem for Rings* (Theorem 8.3.5), which states that

$$\bar{\varphi} : \begin{cases} R/\ker(\varphi) & \rightarrow \text{im}(\varphi) \\ r + \ker(\varphi) & \mapsto \varphi(r) \end{cases}$$

is a ring isomorphism. Because  $\ker(\varphi) = I$  and  $\text{im}(\varphi) = S$ , this proves that

$$(R/I, +, \cdot) \cong (S, +_S, \cdot_S)$$

**Question 4:** As usual, the finite field with 5 elements is denoted by  $(\mathbb{F}_5, +, \cdot)$ , while  $(\mathbb{F}_5[X], +, \cdot)$  denotes the ring of polynomials with coefficients in  $\mathbb{F}_5$ . Define the quotient ring  $(R, +, \cdot)$ , where

$$R := \mathbb{F}_5[X]/\langle X^4 + 2X^3 + X + 2 \rangle$$

- (a) Compute the standard form of the coset  $X^7 + X^6 + 2X^5 + X^4 + 2 + \langle X^4 + 2X^3 + X + 2 \rangle$ .
- (b) Write the polynomial  $X^4 + 2X^3 + X + 2 \in \mathbb{F}_5[X]$  as the product of irreducible polynomials.
- (c) Find  $z$  distinct zero-divisors in  $R$ .  
*(Only possible if  $f(X)$  is not irreducible, otherwise  $R$  is a field and thus a domain!)*
- (d) Show that  $X + 3 + \langle X^4 + 2X^3 + X + 2 \rangle$  is a unit of  $R$  and compute its multiplicative inverse.
- (e) Which are the primitive elements in  $\mathbb{F}_5[X]/\langle X^4 + 2X^3 + X + 2 \rangle$ ?
- (f) Does  $R$  contain zero divisors? Motivate your answer.
- (g) Determine how many units  $R$  contains.
- (h) Compute the multiplicative order of the element  $\alpha := X + \langle X^2 + X + 1 \rangle$  in the quotient ring  $(\mathbb{F}_5[X]/\langle X^2 + X + 1 \rangle, +, \cdot)$ .

---

#### ANSWER

- (a) Because  $p$  is a prime,  $\mathbb{Z}_p = \mathbb{F}_p$  is a *field* and we can apply Lemma 8.2.6, which says that any coset  $g(X) + \langle f(X) \rangle$  of the ideal  $I := \langle f(X) \rangle$  can be *uniquely* described in the standard form

$$r(X) + \langle f(X) \rangle \quad \text{where either} \quad \begin{cases} r(X) = 0 \Leftrightarrow \deg(r(X)) = -\infty \\ 0 \leq \deg(r(X)) < \deg(f(X)) \end{cases}$$

where  $r(X) \in \mathbb{F}_p[X]$  is the *unique* remainder of long polynomial division of  $g(X)$  by  $f(X)$ :

$$g(X) = q(X) \cdot f(X) + r(X)$$

- (b) Denote the polynomial that generates the ideal  $I := \langle f(X) \rangle$  as

$$f(X) := X^4 + 2X^3 + X + 2$$

Whenever  $a \in \mathbb{F}_5$  is a root of  $f(X)$ , then  $(X - a) \in \mathbb{F}_p[X]$  divides  $f(X)$ , providing a proper factor, as Proposition 7.4.3 states that in this case  $f(X)$  can be factored as

$$f(X) = (X - a) \cdot q(X)$$

with  $\deg(q(X)) = \deg(f(X)) - 1 = 3$ . Because furthermore  $(X - a)$  has degree 1, Lemma 9.2.4 says that it is our first *irreducible* factor of  $f(X)$ , which we will denote as  $h_1(X) := X - a$ . We check all  $a \in \mathbb{F}_5$  to see if  $f(a) \equiv 0 \pmod{5}$ . Because  $-1 \equiv 4 \pmod{5}$  and  $-2 \equiv 3 \pmod{5}$ , we have to check if  $f(0), f(1), f(2), f(-1), f(-2) \equiv 0 \pmod{5}$  to check if  $f(X)$  has any roots.

...

We see that  $a \in \mathbb{F}_5$  is a root of  $f(X)$ . We now compute the factor  $q(X)$  from above by performing long polynomial division of  $f(X)$  by the factor  $h_1 := (X - a)$ .

...

We now apply the same principle to  $q(X)$  to find the remaining factors of  $f(X)$ .

...

Because  $\deg(h_k(X)) \in \{2, 3\}$ , and  $h_k(X)$  has no roots in  $\mathbb{F}_5$ , it follows from Lemma 9.2.5 that  $h_k(X)$  is irreducible. We conclude that the factorization of  $f(X)$  into irreducible polynomials is

$$f(X) = h_1(X) \cdot \dots \cdot h_k(X)$$

- 
- (c) To find  $k$  distinct zero-divisors in  $R$ , we first note that *any proper monic factor*  $h(X)$  of  $f(X)$  leads to a zero-divisor  $h(X) + \langle f(X) \rangle$ . In fact, for such polynomial

$$\deg(\gcd[h(X), f(X)]) = \deg(h(X)) \quad (1)$$

and since  $h(X)$  is a *proper* factor of  $f(X)$ , it follows that

$$0 < \deg(h(X)) < \deg(f(X)) \quad \xrightarrow{(1)} \quad 0 < \deg(\gcd[h(X), f(X)]) < \deg(f(X))$$

Now we can apply Proposition 9.1.2 to conclude that  $h(X) + \langle f(X) \rangle$  is a zero-divisor. Because in part (a) we found that

$$f(X) = h_1(X) \cdot \dots \cdot h_k(X)$$

a proper monic factor  $h(X) \in \{h_1(X), \dots, h_k(X)\}$  leads to a zero-divisor. We thus already found  $k$  distinct zero-divisors in  $R$ .

To find more zero-divisors, we note that any multiple  $a(X) \cdot h(X)$  of a proper monic factor  $h(X)$  of  $f(X)$  with degree

$$\begin{aligned} \deg(a(X) \cdot h(X)) &= \deg(a(X)) + \deg(h(X)) \quad (\mathbb{F}_p \text{ is a domain} \Rightarrow \mathbb{F}_p[X] \text{ is a domain}) \\ &< \deg(f(X)) \end{aligned}$$

strictly smaller than  $\deg(f(X))$  leads to a zero-divisor  $(a(X) \cdot h(X)) + \langle f(X) \rangle$  in the quotient ring  $\mathbb{F}_q = \mathbb{F}_{p^q} = \mathbb{F}_5[X]/\langle f(X) \rangle$ . Why? Because  $h(X)$  divides both  $f(X)$  and  $a(X) \cdot h(X)$ , it follows that  $\deg(\gcd[f(X), a(X) \cdot h(X)]) \geq \deg(h(X))$ . Furthermore, since  $h(X)$  is a proper factor, it holds that  $\deg(h(X)) < \deg(f(X))$ . We conclude that

$$0 < \deg(\gcd[f(X), a(X) \cdot h(X)]) < \deg(f(X)),$$

so again by Proposition 9.1.2,  $h(X) \cdot a(X) + \langle f(X) \rangle$  is a zero divisor in  $\mathbb{F}_p[X]/\langle f(X) \rangle$ .

We start with the  $p-1$  constant multiples of each of the proper monic factors  $h_i(X)$  ( $i = 1, \dots, k$ ) of  $f(X)$ . We thereby find  $(p-1) \cdot k$  more distinct zero-divisors in  $R$  on top of the  $k$  zero-divisors we found above.

Now consider the  $p-1$  constant multiples of each of the proper monic factors  $h_i(X)$  ( $i = 1, \dots, k$ ) of  $f(X)$ .

- (d) The given coset  $X+3+\langle f(X) \rangle =: g(X)+\langle f(X) \rangle$  is a unit of  $R$  if and only if  $\deg(\gcd[f(X), g(X)]) = 0$  by Proposition 9.1.2. From the proof of this proposition, the inverse of this coset is given by

$$[g(X) + \langle f(X) \rangle]^{-1} = s(X) + \langle f(X) \rangle,$$

in this case, where  $s(X)$  is obtained by performing the *Extended Euclidean algorithm* on  $f(X)$  and  $g(X)$  to obtain

$$\gcd[f(X), g(X)] = 1 = s(X) \cdot f(X) + r(X) \cdot g(X)$$

We now apply the Extended Euclidean algorithm to find  $s(X)$  and  $r(X)$ :

$$\left[ \begin{array}{c|cc} f(X) & 1 & 0 \\ g(X) & 0 & 1 \end{array} \right] \rightarrow \dots \rightarrow \left[ \begin{array}{c|cc} c & s(X) & r(X) \\ \dots & \dots & \dots \end{array} \right]$$

The identity in row 1 is almost the one we are looking for. To ensure uniqueness, we now make the GCD monic by multiplying the identity in row 1 by  $c^{-1}$ .

- 
- (e) Denote  $\mathbb{F}_q = \mathbb{F}_{p^d} = \mathbb{F}_5[X]/\langle f(X) \rangle$ . Because  $f(X)$  is irreducible, by Theorem 9.3.2,  $\mathbb{F}_q$  is a field with  $q = p^d$  elements.

Because of Theorem 9.4.1, we know that the finite field  $\mathbb{F}_q$  with  $q = p^d$  for prime  $p$  and  $d \geq 1$  has *at least one primitive element*  $\alpha \in \mathbb{F}_q$ . In this case,  $(\mathbb{F}_q^*, \cdot)$  is a *cyclic group* of order

$$\text{ord}(\mathbb{F}_q^*) = |\mathbb{F}_q^*| = \text{ord}(\alpha) = q - 1$$

generated by a primitive element  $\alpha$ :

$$\mathbb{F}_q^* = \{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{q-2}\}$$

Because of Lagranges Theorem (more specifically Proposition 4.4.4), we know that

$$\forall g \in \mathbb{F}_q^* : \quad \text{ord}(g) \text{ divides } |\mathbb{F}_q^*| = q - 1$$

The possible orders of elements in  $\mathbb{F}_q^*$  are thus the divisors of  $q - 1$ :

$$D = \{d \in \mathbb{Z}_{>0} \mid d \text{ divides } (q - 1)\}$$

A primitive element is an element  $\alpha \in \mathbb{F}_q^*$  with order  $\text{ord}(\alpha) = q - 1$ . We thus find a primitive element  $\alpha$  by finding an element whose order is not any of the other divisors of  $q - 1$ :

$$\text{ord}(\alpha) \notin D \setminus \{q - 1\}$$

- (f) Yes,  $R$  contains zero divisors. From part (b), we know that  $f(X) = X^4 + 2X^3 + X + 2$  is reducible in  $\mathbb{F}_5[X]$ , factoring as:

$$f(X) = (X + 1)(X + 2)(X^2 + 4X + 1)$$

Since  $f(X)$  is not irreducible, the quotient ring  $R = \mathbb{F}_5[X]/\langle f(X) \rangle$  is not a field and therefore contains zero divisors (for example, the coset  $(X + 1) + \langle f(X) \rangle$ ), because  $(X + 1)$  is a proper monic factor of  $f(X)$ .

- (g) *NOTE: In this exercise, we use a different  $f$ , namely  $f(X) = X^3 + X - 2$ .*

An element  $g(X) + \langle f(X) \rangle \in R$  in this quotient group is either a zero-element, a unit, or a zero-divisor. Because we can write each coset in standard form, let's assume all these elements  $g(X) + \langle f(X) \rangle$  are in standard form.

- The only zero-element is  $0 + \langle f(X) \rangle = \langle f(X) \rangle$ .
- Units are elements with  $\deg(\text{gcd}[f(X), g(X)]) = 0$ .
- Zero-divisors are elements with  $0 < \deg(\text{gcd}[f(X), g(X)]) < \deg(f(X))$ .

We conclude that a non-zero coset  $u = g(X) + \langle f(X) \rangle$  in standard form (with thus  $g(X) \neq 0$  and  $\deg(g(X)) < \deg(f(X))$ ) is a zero-divisor if and only if  $\deg(\text{gcd}[g(X), f(X)]) > 0$ .

We can thus calculate the number of units  $N_u$  by **first counting the number of zero-divisors  $N_z$** . We know that the total number of elements in  $R$  is  $|R| = p^d = 5^4 = 625$ . The ring is partitioned into units, zero-divisors, and the zero element:

$$|R| = N_u + N_z + 1$$

To find  $N_z$ , we analyze the factorization of  $f(X)$  in  $\mathbb{Z}_5[X]$  to determine the conditions under which  $\deg(\text{gcd}[f(X), g(X)]) > 0$ .

We find the following factorization into irreducible polynomials in  $\mathbb{Z}_5[X]$ :

$$X^3 + X + 3 = (X + 4)(X^2 + X + 2)$$

The quadratic factor  $X^2 + X + 2$  is irreducible in  $\mathbb{Z}_5$  because it has no roots (checking values 0, 1, 2, 3, 4 yields no zeros).  $(X + 4)$  is a factor of degree 1, which is always irreducible.

For a non-zero coset  $g(X) + \langle f(X) \rangle$ ,  $\gcd[f(X), g(X)]$  is either  $X + 4$  or  $X^2 + X + 2$ , because the GCD is *unique* if it's monic. We count the possibilities for  $g(X)$  in these two disjoint cases:

(a) **Case 1:**  $\boxed{\gcd[f(X), g(X)] = X + 4}$

The polynomial  $g(X)$  must be a multiple of  $X + 4$ . Further, since it is in standard form,  $\deg(g(X)) < 3$ . From these two conditions, we find that  $g(X)$  must take the form:

$$g(X) = (X + 4)(aX + b)$$

where  $a, b \in \mathbb{Z}_5$ . There are  $5 \cdot 5 = 25$  choices for the pair  $(a, b)$ . Excluding the zero-coset case where  $(a, b) = (0, 0)$  (giving  $g(X) = 0$ ), we have:

$$25 - 1 = 24 \text{ zero-divisors.}$$

(b) **Case 2:**  $\boxed{\gcd[f(X), g(X)] = X^2 + X + 2}$

The polynomial  $g(X)$  must be a multiple of  $X^2 + X + 2$ . Further, since it is in standard form,  $\deg(g(X)) < 3$ . From these two conditions, we find that  $g(X)$  must take the form:

$$g(X) = a(X^2 + X + 2)$$

where  $a \in \mathbb{Z}_5$ . There are 5 choices for  $a$ . Excluding  $a = 0$ , we have:

$$5 - 1 = 4 \text{ zero-divisors.}$$

Summing these cases, the total number of zero-divisors is:

$$N_z = 24 + 4 = 28$$

Finally, we calculate the number of units  $N_u$ . Recalling that the total number of elements is  $|R| = p^d = 5^3 = 125$ :

$$N_u = |R| - 1 - N_z = 125 - 1 - 28 = 96$$

Thus,  $R$  contains **96 units**.

(h) Let's find the multiplicative order of  $\alpha$ , i.e. the integer  $i > 0$  such that  $\alpha^i = 1_R = 1 + \langle f(X) \rangle$ .

Note that  $\deg(\alpha) < \deg(f(X))$ , in other words, it is **already in standard form**. This means that  $\alpha \neq 0 + \langle f(X) \rangle$ . Furthermore, this also means that  $\alpha \neq 1 + \langle f(X) \rangle$  and thus  $\text{ord}(\alpha) \neq 1$ .

We compute  $\alpha^2$ :

$$\alpha^2 = [X + \langle f(X) \rangle] \cdot [X + \langle f(X) \rangle] = X^2 + \langle f(X) \rangle$$

This is not in standard form, since  $\deg(X^2) = 2 \not< \deg(f(X))$ , so we perform long division of  **$X^2$  by  $f(X)!$**  to find the standard form

$$\alpha^2 = -(X + 1) + \langle f(X) \rangle \neq 1 + \langle f(X) \rangle$$

For  $\alpha^3$ , note that  $\alpha^3 = \alpha \cdot \alpha^2 = -(X^2 + X) + \langle f(X) \rangle = 1 + \langle f(X) \rangle$ .