Final exam

January 26, 2023 **N°**

Last name :

First name :

- Please leave a margin of at least 1.5cm inside the booklet.
- Below $\mathbb{Z}$ denotes the ring of integers, $\mathbb{R}$ the field of real numbers, $\mathbb{Q}$ the field of rational numbers, $\mathbb{N}$ the natural numbers and $\mathbb{N}^+$ the set of positive natural numbers.
- No document is allowed.
- Calculators, smartphones and laptops are not allowed.
- Please provide clear, concise and easily readable arguments.
- You can answer in English or in French, but please do not mix the two languages.
- Scrap paper will not be read by the graders.

Leave this space blank

Question	1	2	3	4	5	6	7	8	T/F	Exam	Total
max	6	14	10	9	12	6	14	10	4	85	100
score											

First part, questions 1 to 8

1. (a) Let $\mathbb{F}_5$ be the field of 5 elements. Find a greatest common divisor $d(X)$ of the polynomials

$$f(X) = X^5 + 2X^4 - X - 2 \qquad \text{and} \qquad g(X) = X^3 + X^2 + 3$$

in the ring $\mathbb{F}_5[X]$. (Provide the details of your computation.)

(b) If $d(X)$ is not monic, find the unique monic greatest common divisor $t(X)$ of $f(X)$ and $g(X)$.

(c) Find $r(X), s(X) \in \mathbb{F}_5[X]$ such that $f(X)r(X) + g(X)s(X) = t(X)$.

[6 **points**]

2. (a) Let G be a finite group. Recall that the center of a group $Z(G)$ is the set of all elements $z \in G$ such that $zg = gz$ for any $g \in G$. Show that $Z(G)$ is a subgroup in G.

   (b) Fix an element $x \in G$. Recall that the centralizer $H \subset G$ of an element $x \in G$ is the set of all elements $h \in G$ such that $hx = xh$. Show that H is a subgroup of G, and that $Z(G)$ is a subgroup of H: $Z(G) \subset H \subset G$.

   (c) Let $|G| = 9$. Show that $|Z(G)| \geq 3$. *Hint:* Recall the class equation of G: $|G| = |Z(G)| + \sum_i [G : H_i]$, where H_i are the stabilizers of representatives of the nontrivial conjugacy classes in G.

   (d) Let $|G| = 9$. Fix an element $x \in G$ and let H be the centralizer of x in G. Use (b) and (c) to show that $|H| \geq 4$.

   (e) Derive from (d) that any group of order 9 is abelian.

   (f) Let $|G| = p^2$, where p is a prime. Generalize (c), (d), (e) to show that a group of order p^2 is abelian.

   [14 **points**]

3. (a) Define the Euler totient function $\varphi(n)$ for a natural $n \geq 2$ and state the Euler theorem about congruences.
   (b) Let p_1, p_2, p_3 be three primes, not necessarily distinct. Express $\varphi(p_1 p_2 p_3)$ in terms of p_1, p_2, p_3. Consider cases.
   (c) Show that $a = p^{88} - p^{16}$ is divisible by 30 for any prime $p \geq 7$.
   [10 **points**]

4. Let C_k denote the cyclic group of order $k \in \mathbb{N}^+$.

   (a) How many different (non-isomorphic) abelian groups of order 144 are there? List the elementary divisors and invariant factors for each of the groups.

   (b) Let m_G be the maximal order of an element in G. Among the groups listed in (a), find the one where m_G is the smallest. Justify your answer.

   (c) Among the groups listed in (a), find all groups of the form $H \times K$ where $|H| = |K| = 12$. Justify your answer.

   [9 **points**]

5. Let $\mathbb{F}_3$ be the field of 3 elements. Define the ideal in $\mathbb{F}_3[X]$

$$I = \langle X^2 - X - 1 \rangle$$

Let

$$A = \mathbb{F}_3[X]/I$$

(a) Show that A is a field. Justify your answer (cite a theorem from the course).

(b) List all elements in A.

(c) Consider the group of units (invertible elements) A^* in A. List all elements in A^*. Find the order and structure of A^* (cite a theorem from the course).

(d) Find all elements of the multiplicative order 2 in the group of units A^*.

(e) Does A^* have an element of order 8? If so, give an example of such an element.

[12 **points**]

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 14 \pmod{20} \\ x \equiv 1 \pmod{3} \\ x \equiv 0 \pmod{11}. \end{cases}$$

has infinitely many solutions in $\mathbb{Z}$.

(b) Find all integer solutions of the system.

(c) Find the smallest positive integer that solves the system in (a).

[6 **points**]

7. Let S_n denote the symmetric group of permutations of $n \in \mathbb{N}^+$ elements.

   (a) Consider the element $a = (1234567)(38) \in S_9$ and write it as a product of disjoint cycles. Find the order of a.

   (b) Consider the element $b = (1234567)(25) \in S_9$ and write it as a product of disjoint cycles. Find the order of b.

   (c) Let $2 \leq k < n$ and consider the element $c = (12 \dots k)(im) \in S_n$ where $1 \leq i \leq k$ and $k < m \leq n$. Write c as a product of disjoint cycles in S_n. Find the order of c as it depends on k.

   (d) Let $2 \leq k \leq n$ and consider the element $d = (12 \dots k)(ij) \in S_n$ where $1 \leq i < j \leq k$. Write c as a product of disjoint cycles in S_n. Express the order of d in terms of i, j, k.

   (e) Let $4 \leq k + 2 \leq n$ and $k < i < j \leq n$. Find the order of the element $e = (12 \dots k)(ij)$ as it depends on k.

   (f) If an element is a product of a k-cycle and a 2-cycle (not necessarily disjoint) in a symmetric group, what can be the disjoint cycle decomposition of such an element? Use (c), (d), (e) to formulate a general statement.

   [14 **points**]

8. (a) State the definition of the characteristic of a ring.

   (b) Let A and B be two rings of characteristics $c_A > 0$ and $c_B > 0$. Express the characteristic of the direct product $A \times B$ in terms of c_A, c_B.

   (c) Suppose that $\gcd(n, m) = d \neq 1$ for integers $n > 1, m > 1$. Show that the rings $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/nm\mathbb{Z}$ are not isomorphic. *Hint*: use the characteristic of a ring.

   (d) Find the number of units (invertible elements) in rings $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and in $\mathbb{Z}/108\mathbb{Z}$. Justify your answer,

   (e) Show that if $\gcd(n, m) > 1$, then the rings $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/nm\mathbb{Z}$ have different number of units.

   [10 **points**]

Second part, questions 9 to 12.

The following questions do not require any justification. Only your answer will be evaluated: +1 point for a correct answer, -1 for a wrong answer and 0 for no answer.

---

9. (True/False) The ideal $I = (6\mathbb{Z}) \cap (15\mathbb{Z}) \cap (10\mathbb{Z}) \subset \mathbb{Z}$ is equal to $(30\mathbb{Z})$.

10. (True/False) The polynomial $3X^7 + 12X^6 - 9X^4 - 24X^3 + 15X + 10$ is irreducible in $\mathbb{Q}[X]$.

11. (True/False) There is a nontrivial group homomorphism between the cyclic groups $f : C_{15} \to C_{30}$.

12. (True/False) There is a nontrivial ring homomorphism $\phi : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/30\mathbb{Z}$.

[4 **points**]