Final exam

February 1, 2022 **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	14	6	12	10	4	85	100
score											

First part, questions 1 to 8

1. (a) Let $\mathbb{F}_7$ be the field of 7 elements. Find a greatest common divisor $d(X)$ of the polynomials

$$f(X) = X^4 - 2X^3 + 2X^2 - 3X - 1 \qquad \text{and} \qquad g(X) = X^3 - 2X^2 - 2$$

in the ring $\mathbb{F}_7[X]$. (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 $r(X), s(X) \in \mathbb{F}_7[X]$ such that $f(X)r(X) + g(X)s(X) = t(X)$.

[6 **points**]

2. Let G be a group of order 12.

   (a) List all possible orders of elements in G.

   (b) How many different **abelian** groups are there of order 12? Find the elementary divisors of these groups.

   (c) Let S_4 be the symmetric group of permutations of 4 elements. Recall that the alternating group $A_4 \subset S_4$ is the subgroup of all **even** permutations in S_4. List all elements of $A_4 \subset S_4$ in terms of products of disjoint cycles. In particular, show that $|A_4| = 12$.

   (d) Show that any subgroup $H \subset A_4$ of order 3 is **not normal** in A_4.

   (e) There is a unique subgroup $K \subset A_4$ of order 4. List all elements in K and prove that it is **normal**.

   (f) Is there a subgroup of order 6 in A_4? Justify your answer.

   (g) Give an example (in terms of generators and relations) of a group G of order 12 that is **not abelian** and **not isomorphic to** A_4.

   [14 **points**]

3. Let φ denote the Euler totient function.

   (a) Compute $\varphi(7)$, $\varphi(49)$, $\varphi(6)$ and $\varphi(36)$.

   (b) Let p be a prime. Which is bigger, $\varphi(p^2)$ or $(\varphi(p))^2$? Prove your answer.

   (c) Let $n > 1$ be a natural number. Which is bigger, $\varphi(n^2)$ or $(\varphi(n))^2$? Prove your answer.

   [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 162 are there? List the elementary divisors and invariant factors for each of the groups above.

   (b) Among the groups listed above, find all that contain a subgroup of order 27 that is **not cyclic.** Justify your answer.

   (c) Among the groups listed above, find all that contain **no element of order 9**. Justify your answer.

   [9 **points**]

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

$$I = \langle X^3 + X^2 + X - 1 \rangle, \quad J = \langle X^3 + X^2 + X + 1 \rangle, \quad K = \langle X^3 - X^2 + X + 1 \rangle$$

Let

$$A = \mathbb{F}_3[X]/I, \qquad B = \mathbb{F}_3[X]/J, \qquad C = \mathbb{F}_3[X]/K.$$

(a) Which of the rings A, B, C are fields? (justify your answer, cite theorems from the course).

(b) Find the number of elements in A.

(c) Find the inverses of the elements $[X]_I$ in A, $[X]_J$ in B and $[X]_K$ in C, if they exist.

(d) Which of the ring(s) are not integral domain(s)? In this case give an example of a nontrivial zero divisor.

(e) Which of the rings A, B, C are isomorphic to each other? Justify your answer.

(f) What is the structure of the abelian group of units of A? (justify your answer, cite a theorem from the course).

[14 **points**]

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 7 \\ x \equiv 3 \pmod{15}. \end{cases}$$

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 elements $a = (2143)(234) \in S_6$ and $b = (2143)(235) \in S_6$. Write a and b as products of disjoint cycles and find their orders.

   (b) Recall that for any $g \in S_n$ and any cycle $(x_1....x_k) \in S_n$, we have $g(x_1...x_k)g^{-1} = (g(x_1)...g(x_k))$ in S_n. Use this identity to find the number of elements in the conjugacy class $\{gag^{-1}\}_{g \in S_6}$.

   (c) Find the number of elements in the conjugacy class $\{gbg^{-1}\}_{g \in S_6}$.

   (d) What is the maximal order of an element in S_6? Justify your answer.

   (e) What is the maximal order of an element in S_7? Justify your answer.

   [12 **points**]

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

   (b) State the definition of a homomorphism of rings.

   (c) Let A and B be two rings and suppose that $f : A \to B$ is a ring homomorphism. Prove that $\mathrm{char}(B)$ divides $\mathrm{char}(A)$.

   (d) Let $A_1 = \mathbb{Z}$, $A_2 = \mathbb{Z}/5\mathbb{Z}$, $A_3 = \mathbb{Z}/15\mathbb{Z}$. Use (c) to determine which of the ring homomorphisms

$$f_{ij} : A_i \to A_j, \qquad i \neq j \in \{1, 2, 3\}$$

   can exist. Describe all possible ring homomorphisms between these rings.

   [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) If G is a non-abelian group, then the direct product group $G \times H$ is non-abelian for any group H.

10. (True/False) If $\gcd(n, m) > 1$, then the equation $nx + my = 6$ can never have integer solutions x, y.

11. (True/False) The polynomial $5X^5 + 4X^4 + 8X^3 + 10X^2 + 2$ is irreducible in $\mathbb{Q}[X]$.

12. (True/False) The dihedral group D_n is isomorphic to a direct product of cyclic groups of orders n and 2.

[4 **points**]