Final exam

January 29, 2024 **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.

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

$$f(X) = 3X^5 - X^4 + 3X - 1 \qquad \text{and} \qquad g(X) = 3X^2 - 2$$

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 R be the group of all rotational symmetries of a regular octahedron around its center (see the picture next page). Find the number of elements in the orbit of vertex 1 under the action of R.

   (b) Describe the subgroup $H \subset R$ that stabilizes the vertex 1 and find the order $|H|$.

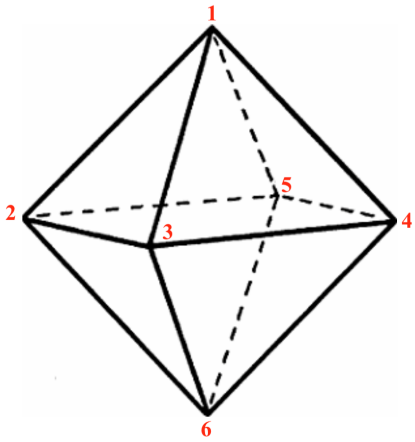
   (c) Cite the orbit-stabilizer theorem and apply it to find the order of the group R.

   (d) Each element of R defines a permutation of the vertices of the regular octahedron (see the picture). This gives an injective homomorphism ϕ from R to the symmetric group S_6 of permutations of 6 elements. In particular $\phi(H)$ is a subgroup of S_6. List the elements of $\phi(H)$.

   (e) Does R contain an element $a \in R$ of order 2? If so, describe the action of a on the octahedron geometrically and write $\phi(a)$ as a permutation in S_6.

   (f) Does R contain an element $b \in R$ of order 3? If so, describe the action of b on the octahedron geometrically and write $\phi(b)$ as a permutation in S_6.

   [14 **points**]


1
2
3
4
5
6

3. Consider the field of 11 elements $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$.

   (a) Let $K = (\mathbb{F}_{11})^*$ be the group of units of $\mathbb{F}_{11}$. Find the order of K and describe its structure. Cite a theorem from the course.

   (b) List the orders of elements that occur in K. Justify your answer.

   (c) Give an example of an element $[a]_{11} \in K$ of order 2 and $[b]_{11} \in K$ of order 5.

   [10 **points**]

4. (a) Let p be an odd prime. How many non-isomorphic abelian groups of order $8p^2$ are there? List the elementary divisors and invariant factors for each of the groups. You can use the notation C_k for the cyclic group of order $k \in \mathbb{N}^+$.

   (b) Show that each of the groups listed above contains an element of order $2p$.

   (c) Which of the groups listed in (a) contain an element of order $4p$? Justify your answer.

   [9 **points**]

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

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

Let

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

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

(b) List all elements in A. In particular, find $|A|$.

(c) Find the inverse of the element $[X+1]_I$ in A.

(d) Is any of the rings B, C a field? Justify your answer.

(e) Can you compute the inverse of $[X+1]_J \in B$ and of $[X+1]_K \in C$?

(f) Is any of the rings A, B, C isomorphic to the ring $\mathbb{Z}/9\mathbb{Z}$? Justify your answer.

[12 **points**]

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 0 \pmod 6 \\ x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod{25}. \end{cases}$$

has infinitely many solutions in $\mathbb{Z}$ (cite a theorem from the course).

(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_5 denote the symmetric group of permutations of 5 elements.

   (a) Consider the element $a = (243)(135)(14) \in S_5$ and write it as a product of disjoint cycles.

   (b) Find the order of a.

   (c) Find the number of elements in the conjugacy class $\{gag^{-1}\}_{g \in S_5}$.

   (d) Let H be the subgroup in S_5 that consists of all permutations of the elements $\{1, 3, 5\}$. List all elements in H and find its order.

   (e) Is H a normal subgroup in S_5? Justify your answer.

   [10 **points**]

8. Let E be a Euclidean domain. Recall that a Euclidean domain is an integral domain where the Euclidean division works, in particular if $\gcd(a,b) = 1$ for two elements $a, b \in E$, then there exist elements $x, y \in E$ such that $xa + yb = 1$. For example, the ring of integers $\mathbb{Z}$ is a Euclidean domain.

   (a) Recall that a *unit* in E is an invertible element with respect to the multiplication. Recall that an element $a \in E$ is *irreducible* if $a \neq 0$, a is not a unit and if $a = st$, then either s or t is a unit. Find the units and the irreducible elements in $\mathbb{Z}$.

   (b) Let a, c be irreducible elements in a Euclidean domain E. Suppose that c does not divide a. Show that in this case $\gcd(a, c)$ is a unit. Since gcd is defined up to a multiplication by a unit, this means that $\gcd(a, c) = 1$.

   (c) Let $a, b, c \in E$ be irreducible elements such that c divides ab but c does not divide a. Use (b) to show that then c divides b.

   (d) Use (c) to prove that in a Euclidean domain a factorization of an element into a product of irreducible factors is unique. Namely, if $x = a_1 a_2 \dots a_k = b_1 b_2 \dots b_r$, where all a_i and b_j are irreducible elements of E, then $k = r$ and up to a permutation of terms, $b_i = a_i u_i$, where u_i are units in E.

   (e) We proved in class that $F[X]$, where F is a field, is a Euclidean domain. Use (d) to show that a polynomial of degree n with coefficients in a field can have at most n roots in F.

   (f) Let $K = \mathbb{Z}/9\mathbb{Z}[X]$. Show by an example that the statement in (e) fails in K. Namely, how many distinct roots does the polynomial $f(X) = X^2$ have in $\mathbb{Z}/9\mathbb{Z}$?

   [14 **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) Let F_1 and F_2 be two fields. Then $F_1 \times F_2$ is a field.

10. (True/False) The ring $\mathbb{Z}/15\mathbb{Z}$ is an integral domain.

11. (True/False) The polynomial $6X^5 + 20X^4 + 15X^2 + 25X + 5$ is irreducible in $\mathbb{Q}[X]$.

12. (True/False) The symmetric group S_7 contains a subgroup isomorphic to the cyclic group C_{10}.

[4 **points**]