Algebra MATH-310 **fall 2024** **Anna Lachowska**

Final exam

January 27, 2025 **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	12	12	12	12	6	10	12	3	85	100
score											

First part, questions 1 to 8

1. (a) Use the Euclidean algorithm to find a greatest common divisor $d(X)$ of the polynomials

$$f(X) = X^6 - 1 \quad \text{and} \quad g(X) = X^2 - 2X + 1$$

in the ring $\mathbb{Q}[X]$. (Show your computations)

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

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

[6 **points**]

2. Consider the dihedral group $D_8 = \langle r, s | s^2 = 1, r^8 = 1, srs = r^{-1} \rangle$. We have $|D_8| = 16$.

   (a) Define a subgroup of a group. Consider the smallest subgroup $K \subset D_8$ that contain the element r^6 (equivalently, this is the subgroup in D_8 generated by r^6). What is the order of this subgroup? List all elements in K.

   (b) Define a normal subgroup. Show that K normal in D_8.

   (c) Consider the quotient group $T = D_8/K$. Find its order. Is T abelian? Justify your answer.

   (d) Find a subgroup $F \subset D_8$ such that $s \in F$ and $|F| = 8$. List all elements in F.

   [12 **points**]

3. (a) Let p be a prime number, and $n \in \mathbb{Z}$, $n \geq 1$. Give a formula for $\varphi(p^n)$, where φ is the Euler's totient function (without a proof).

   (b) Compute $\varphi(15)$, $\varphi(6)$, $\varphi(90)$.

   (c) List the invertible elements in the ring $\mathbb{Z}/15\mathbb{Z}$.

   (d) Find the inverse of $[14]_{15}$ in the ring $\mathbb{Z}/15\mathbb{Z}$. Justify your answer.

   (e) Let $m, n \in \mathbb{Z}$, $m, n > 1$ be such that $\gcd(m, n) = p$ where p is a prime. Show that

$$\varphi(mn) = \frac{p}{p-1}\varphi(m)\varphi(n).$$

   [12 **points**]

4. (a) How many non-isomorphic abelian groups are there of order 900? Give a list of these groups without repetitions (You can use the notation C_m for a cyclic group of order m.)

   (b) For each group in the list, provide the elementary divisors.

   (c) Show that any abelian group of order 900 contains an element of order 30.

   (d) Show that an abelian group of order $|G|$ divisible by a product of distinct primes $n = p_1 p_2 \dots p_k$, contains an element of order n.

   [12 **points**]

5. (a) Show that $p(x) = \frac{x^5-1}{x-1}$ is a polynomial in $\mathbb{Q}[x]$ and compute it.

   (b) Consider the polynomial $\widetilde{p}(y) = \frac{(y+1)^5-1}{y}$ obtained by the change of variables $y = x - 1$ in $p(x)$. Use the binomial theorem $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ and the Eisenstein criterion to show that $\widetilde{p}(y)$ is an irreducible polynomial in $\mathbb{Q}[y]$.

   (c) Use (b) to show that $p(x)$ is irreducible over $\mathbb{Q}[x]$. *Hint:* Assume that $p(x)$ is a product of two non-constant polynomials in $\mathbb{Q}[x]$ and derive that $\widetilde{p}(y)$, where $y = x - 1$, is a product of two non-constant polynomials in $\mathbb{Q}[y]$.

   (d) (*Bonus question*). Use the same method to show that the polynomial $\frac{x^p-1}{x-1}$ is irreducible over $\mathbb{Q}[x]$ for any prime p.

   [12 **points**]

6. (a) Show that the following system of congruences has a solution $a \in \mathbb{Z}$ (cite a theorem from the course and check the conditions of the theorem).

$$\begin{cases} a \equiv 10 \pmod{13} \\ a \equiv 3 \pmod{4} \\ a \equiv 4 \pmod{3}. \end{cases}$$

(b) Describe the set of all integer solutions of the given system.

(c) Find the smallest positive solution $a \in \mathbb{Z}$ of the system.

[6 **points**]

7. Let $\mathbb{F}_2$ denote the field of 2 elements.

   (a) List all polynomials of degree 2 in $\mathbb{F}_2[X]$. Which of them are irreducible?

   (b) Use (a) to show that $X^4 + X^3 + 1$ is irreducible in the ring $\mathbb{F}_2[X]$.

   (c) Let $K = \mathbb{F}_2[X]/\langle X^4 + X^3 + 1\rangle$. Show that K is a field, citing a theorem from the course, and determine the number of elements in K.

   (d) Find the inverse element for $[X]_{(X^4+X^3+1)} \in K$.

   [10 **points**]

8. Let S_5 denote the symmetric group of permutations of 5 elements.

   (a) Write $a = (314)(2145)$ as a product of disjoint cycles.

   (b) What is the order of the element $a \in S_5$?

   (c) Find the number of elements in the conjugacy class of a in S_5.

   (d) Let K be the smallest subgroup in S_5 that contains (13) and (15). What is the order of this subgroup?

   (e) Let H be the smallest subgroup in S_5 that contains the 3-cycle (135). List all elements of H.

   (f) Is H a subgroup in K? Justify your answer.

   [12 **points**]

Second part, questions 9 to 14.

In the following questions, you get 1 point for correct answer, -1 point for incorrect answer and 0 point for no answer.

---

9. (True/False) $[4]_7$ and $[5]_7$ are associates in $\mathbb{Z}/7\mathbb{Z}$.

10. (True/False) The group $C_8 \times C_9$ is isomorphic to the group $C_{12} \times C_6$.

11. (True/False) The group S_7 does not contain an element of order 8.

[3 **points**]