Algebra MATH-310 **fall 2019** **Anna Lachowska**

Final exam

January 20, 2020 **N°**

Last name :

First name :

- Below $\mathbb{Z}$ denotes the ring of integers, $\mathbb{R}$ the field of real numbers, $\mathbb{Q}$ the field of rational numbers, and $\mathbb{F}_q$ the finite field of q elements.
- No document is allowed.
- Calculators and smartphones 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.
- Scratch paper will not be read by the graders.

Leave this space blank

Question	1	2	3	4	5	6	7	8	second part
score									

Total /85

First part, questions 1 to 8

1. (a) Let $\mathbb{Q}$ be the field of rational numbers. Find a greatest common divisor $d(X)$ of the polynomials

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

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

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

(c) If $d(X)$ is not monic, find the unique monic greatest common divisor $t(X)$ of $f(X)$ and $g(X)$, and two polynomials $p(X), q(X) \in \mathbb{Q}[X]$ such that $f(X)p(X) + g(X)q(X) = t(X)$.

[7 **points**]

.

2. Let S_4 be the symmetric group of permutations of 4 elements. Let $A_4 \subset S_4$ be the alternating subgroup, the subgroup of all even permutations in S_4 (even permutations are products of an even number of transpositions, not necessarily disjoint).

   (a) List all elements in A_4.

   (b) Let G be a group of order 4. Show that G is abelian.

   (c) Find an abelian subgroup K of order 4 in A_4 and show that it is normal in A_4.
   Hint: Let $\rho, \pi \in S_n$ be two permutations. The disjoint cycle decomposition of $\pi\rho\pi^{-1}$ is obtained from that of ρ by replacing each integer i in the disjoint cycle decomposition of ρ by the integer $\pi(i)$.

   (d) Is the subgroup K found in (c) normal in S_4?

   (e) Show that there is no subgroup of order 6 in A_4.
   Hint: What can be the order of an element in a group of order 6?

   [14 **points**]

.

3. Let φ denote the Euler totient function.

   (a) Compute $\varphi(16)$ and $\varphi(128)$.

   (b) Describe all units (invertible elements) in the rings $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/128\mathbb{Z}$.

   (c) Let p be a prime and $n \geq 1$. Derive a formula for $\sum_{k=0}^{n} \varphi(p^k)$ and prove it by induction (recall that by definition $\varphi(1) = 1$). The answer should depend on p and on n.

   (d) Find all positive integers m such that $\varphi(m)$ is odd.

   [11 **points**]

.

4. (a) How many different (non-isomorphic) abelian groups of order 32 are there?

   (b) Let p be a prime. How many different (non-isomorphic) abelian groups of order p^5 are there? List these groups without repetition. (You can use the notation C_m to denote the cyclic group of order m.)

   (c) List all abelian groups of order p^5 that contain an element of order p^3. Justify your answer.

   (d) Let $p_1, p_2, \ldots p_r$ be r distinct primes. How many different abelian groups of order $n = p_1 p_2 \ldots p_r$ are there? Justify your answer.

   [10 **points**]

.

5. Let $\mathbb{F}_2$ be the field of 2 elements. Let $I = \langle X^3 \rangle$ be the ideal in the ring $\mathbb{F}_2[X]$, generated by the polynomial X^3, and let

$$A = \mathbb{F}_2[X]/I.$$

   (a) Show that the ring A is not a field (cite a theorem). How many elements does it have? List all elements in A as classes modulo I.

   (b) Which of the elements in A are zero divisors?

   (c) Find the inverse of the element $[X^2 + 1]_I$ and the inverse of the element $[X^2 + X + 1]_I$ in A.

   (d) Show that A is not isomorphic to either of the rings $B = \mathbb{Z}/8\mathbb{Z}$, $C = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Hint:* compute the characteristic of each ring.

   (e) Let $D = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Are the rings A and D isomorphic? *Hint:* consider the number of invertible elements in A and D.

   [13 **points**]

.

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv -6 \pmod{22} \\ x \equiv 0 \pmod 7. \end{cases}$$

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

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

[6 **points**]

.

7. Let S_6 denote the symmetric group of permutations of 6 elements.

   (a) Let $a = (12) \in S_6$, and $b = (234) \in S_6$. Write the element bab^{-1} in terms of disjoint cycles.

   (b) Write the elements b^2 and b^2ab^{-2} in terms of disjoint cycles.

   (c) Express every transposition of the form (ij) for $1 \leq i < j \leq 4$ as a product of elements a, b and their inverses. What can you conclude about the subgroup $H \subset S_6$ generated by a and b?

   (d) Find the orbit of 1 under the action of the group H. Find the stabilizer subgroup of 1 in H, $\mathrm{Stab}_H(1) \subset H$ and check explicitly that the orbit-stabilizer theorem holds for this action.

   [12 **points**]

.

8. Let A be a commutative ring. Recall that an element $c \in A$ is irreducible if $c \neq 0$, c is not a unit, and if $c = ab$ for $a, b \in A$, then either a or b is a unit.

   (a) Find all irreducible elements in the ring of integers $\mathbb{Z}$.

   (b) Are there any irreducible elements in the ring $\mathbb{Z}/4\mathbb{Z}$? Find them or prove that they don't exist.

   (c) Is there an irreducible polynomial of degree 10 in $\mathbb{Q}[X]$? If so, provide an example and an explanation.

   [8 **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 dihedral group $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$ is isomorphic to the direct product of cyclic groups $C_4 \times C_2$.

10. (True/False) The ring $\mathbb{F}_5[X]/\langle X^3 - X^2 + 2 \rangle$ is a field.

11. (True/False) The number $13^{33} - 13$ is divisible by 20.

12. (True/False) Let p, q be two distinct primes. Then $\mathbb{Z}/(pq)\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ is a ring isomorphism.

[4 **points**]

.

.