Algebra MATH-310 **fall 2018** **Anna Lachowska**

Final exam

January 14, 2019 **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.
- Color paper serves only for scratch and will not be read by the graders.

Leave this space blank

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

Total /80

First part, questions 1 to 8

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

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

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

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

[5 **points**]

.

2. Let G be a finite group of order 10.

   (a) Let $t \in G$, $t \neq 1$. What can be the order of t?

   (b) Let G be abelian. Use the classification theorem for finite abelian groups to describe the structure of G.

   (c) Let G be non-abelian. Show that G contains an element of order 5.

   (d) If G is non-abelian, show that G is isomorphic to the dihedral group $D_5 = \langle r, s \mid r^5 = 1, s^2 = 1, srs = r^{-1} \rangle$. *Hint*: Use the fact that the equation $m^2 = 1$ has at most two solutions in a field.

   [13 **points**]

.

3. (a) Let m and n be two integers, $n > m \geq 2$, such that $m \mid n$. Show that $\varphi(m) \mid \varphi(n)$, where φ is Euler's totient function.

   (b) Compute $\varphi(15)$ and $\varphi(90)$.

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

   (d) Show that for any integer $a \in \mathbb{Z}$ such that $\gcd(a, 90) = 1$, we have $a^{16} \equiv 1 \pmod{15}$.

   [12 **points**]

.

4. (a) How many different abelian groups are there of order 72? List these groups without repetition. (You can use the notation C_m to denote the cyclic group of order m.)

   (b) For each group provide its elementary divisors and invariant factors.

   (c) List all abelian groups of order 72 that contain an element of order 9.

   [9 **points**]

.

5. Let $\mathbb{F}_3$ be the field of 3 elements. Let I and J be two ideals in the ring $\mathbb{F}_3[X]$, generated by the following polynomials

$$I = \langle X^3 + X - 2 \rangle \qquad J = \langle X^3 + X^2 - 1 \rangle.$$

Let $A = \mathbb{F}_3[X]/I$ and $B = \mathbb{F}_3[X]/J$.

(a) Show that the ring A is not a field.

(b) Is the ring B a field? Justify your answer.

(c) Show that the class $[X + 1]_J$ invertible in B and find its inverse.

(d) Find the characteristic of the rings A and B.

[12 **points**]

.

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 0 \pmod 3 \\ x \equiv 2 \pmod{14}. \end{cases}$$

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

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

[6 **points**]

.

7. Let S_7 denote the symmetric group of permutations of 7 elements, and C_k the cyclic group or order k for any integer $k \geq 1$.

   (a) Let $a = (12)(123) \in S_7$, and $b = (135)(246) \in S_7$. Find the order of a and the order of b.

   (b) Show that there exists a subgroup isomorphic to C_{12} in S_7 and provide an element in S_7 that generates it.

   (c) Show that the elements $s = (135)$ and $t = (246)$ together generate an abelian subgroup of order 9 in S_7.

   (d) Is there a subgroup isomorphic to C_9 in S_7? If so, provide a generator in the cycle notation. If not, explain why.

   [13 **points**]

.

8. Recall that if a polynomial $p(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ has a root $\frac{r}{s} \in \mathbb{Q}$ with $\gcd(r, s) = 1$, then $s \mid a_n$ and $r \mid a_0$.

   (a) Show that the polynomial $f(X) = 3X^3 - 2X^2 + 1$ is irreducible in $\mathbb{Q}[X]$.

   (b) Is the polynomial $g(X) = 2X^3 + 3X^2 + 2X - 2$ irreducible in $\mathbb{Q}[X]$? Justify your answer.

   [6 **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 $H \subset G$ be a subgroup of index 2. Then H is normal in G.

10. (True/False) The ring $\mathbb{Z}/8\mathbb{Z}$ is a field.

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

12. (True/False) Let $I = (10)$, $J = (12)$ be two ideals in the ring $\mathbb{Z}$. Then $I \cdot J = I \cap J$.

[4 **points**]