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

Final exam

January 14, 2019 **N°**

Last name : Solutions

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

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

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**]

(a) Euclidean division of polynomials:

$$\begin{array}{r|l} X^3+X^2+X+1 & X^2-3X+2 \\ \cline{2-2} X^3-3X^2+2X & X+4 \\ \cline{1-1} 4X^2-X+1 & \\ 4X^2-2X+3 & \\ \cline{1-1} X-2 & \end{array} \qquad \begin{array}{r|l} X^2-3X+2 & X-2 \\ \cline{2-2} X^2-2X & X-1 \\ \cline{1-1} -X+2 & \\ \cline{1-1} 0 & \end{array}$$

$\Rightarrow \boxed{gcd(f,g) = X-2 = X+3}$ in $\mathbb{F}_5[X]$

(b) Read the Euclidean division backwards:

$$X-2 = X^3+X^2+X+1 - (X^2+3X+2)(X+4)$$
$$= 1 \cdot f(X) + (-X-4)g(X)$$

$\Rightarrow \boxed{r(X) = 1}$, $\boxed{S(X) = -X-4 = -X+1}$

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**]

(a) $|G| = 10$, $t \neq 1 \Rightarrow \langle t \rangle \subset G$ subgroup $\Rightarrow |\langle t \rangle|$ divides $|G| = 10$

$\Rightarrow$ order $(t) = 2$, or order $(t) = 5$, or order $(t) = 10$

(b) $10 = 2 \cdot 5 \Rightarrow G_{ab} = C_2 \times C_5 \simeq C_{10}$ the only abelian group of order 10.

(c) If $t^{10} = 1 \Rightarrow G$ is abelian $\approx C_{10}$

If the order of any nontrivial element of G is 2, then G is abelian:

$t^2 = 1$, $s^2 = 1$, $(ts)^2 = tsts = 1 \Rightarrow tsts^2 = s \Rightarrow tst = s \Rightarrow ts = st$.

$\Rightarrow$ If G is non-abelian, it has to have an elt of order 5.

(d) Let $t \in G$, $t^5 = 1$ of order 5, $|G| = 10$, non-abelian $\Rightarrow \exists s \in G$ such that $s \neq t^i$ (otherwise a cyclic gp). If s is of order 5 $\Rightarrow$ G contains $\{1, t, \ldots t^4, s, st \ldots st^4, s^2, s^2t \ldots s^2t^4 \ldots\}$ too large $\Rightarrow s$ is of order 2.

$\Rightarrow t^5 = 1$, $s^2 = 1 \Rightarrow sts = t^j$ because $|\{1, t, t^4, s, st, \ldots st^4\}| = 10$

$\Rightarrow s t^j s = t$; $(sts)^j = sts(sts)$ $(sts) = st^j s = t$

$(t^{4j})^j = t^{j^2}$

$j^2 = 1 \Rightarrow j = \pm 1 \Rightarrow sts = t^{-1} \Rightarrow G \simeq D_5$

if $sts = t \Rightarrow G$ abelian

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**]

(a) Let $n = \prod p_i^{k_i}$, $m = \prod p_j^{\ell_j}$ $\quad m \mid n \Rightarrow \ell_i \leq k_i$, where $\{p_i\}$ are distinct primes

$\varphi(n) = \prod (p_i^{k_i} - p_i^{k_i - 1})$, $\varphi(m) = \prod (p_j^{\ell_j} - p_j^{\ell_j - 1})$

If $k_i = \ell_i \geq 1 \Rightarrow (p_i^{\ell_i} - p_i^{\ell_i - 1}) = (p_i^{k_i} - p_i^{k_i - 1})$

If $k_i > \ell_i \geq 1 \Rightarrow p_i^{\ell_i - 1}(p_i - 1) \mid p_i^{k_i - 1}(p_i - 1)$

(b) $\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$

$\varphi(90) = \varphi(2) \cdot \varphi(5) \cdot \varphi(9) = 1 \cdot 4 \cdot (9 - 3) = 24$

(c) $\{1, 2, 4, 7, 8, 11, 13, 14\}$ prime to 3 and to 5.

(d) $\gcd(a, 90) = 1 \Rightarrow \gcd(a, 15) = 1 \Rightarrow$ by Euler's theorem

$a^{\varphi(15)} \equiv 1 \pmod 5$

$\Rightarrow a^8 \equiv 1 \pmod{15}$ (square of the congruence $\Rightarrow$)

$\Rightarrow a^{16} \equiv 1 \pmod{15}$

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**]

(a) $72 = 2^3 \cdot 3^2$. By the theorem of classification of finite abelian groups:

$C_9 \times C_8$ $\quad$ $C_9 \times C_4 \times C_2$ $\quad$ $C_9 \times C_2 \times C_2 \times C_2$ $\quad$ $C_3 \times C_3 \times C_8$ $\quad$ $C_3 \times C_3 \times C_4 \times C_2$ $\quad$ $C_3 \times C_3 \times C_2 \times C_2 \times C_2$

(b) Elementary divisors:

$(9,8)$. $(9,4,2)$ $\quad$ $(9,2,2,2)$ $\quad$ $(3,3,8)$. $(3,3,4,2)$ $\quad$ $(3,3,2,2,2)$

Invariant factors: along the columns

(72) $\quad$ $(36,2)$ $\quad$ $(18,2,2)$ $\quad$ $(24,3)$ $\quad$ $(12,6)$ $\quad$ $(6,6,2)$

(c) An element of order 9 can only belong to a cyclic group of order divisible by 9: C_{72}, $C_{36} \times C_2$, $C_{18} \times C_2 \times C_2$.

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**]

(a) The polynomial X^3+X-2 has a root $X=1$ in $\mathbb{F}_3$

$\Rightarrow$ X^3+X-2 is not irreducible in $\mathbb{F}_3[X]$ $\Rightarrow$ $\mathbb{F}_3[X]/\langle X^3+X-2\rangle$ is not a field.

In fact $X^3+X-2 = (X-1)(X^2+X+2)$. in $\mathbb{F}_3[X]$.

(b) The polynomial $f(X)=X^3+X^2-1$ is irreducible in $\mathbb{F}_3[X]$.

It has degree 3 and no roots in $\mathbb{F}_3$: $f(0)=-1$, $f(1)=1$, $f(-1)=-1$.

Therefore, by the theorem seen in the course, $\mathbb{F}_3[X]/\langle X^3+X^2-1\rangle$ is a field.

(c) $[X+1]_J \neq 0$ in $\mathbb{F}_3[X]/J$ because $\deg(X+1) = 1 < 3$ $\Rightarrow$ it is invertible in the field $\mathbb{F}_3[X]/J$.

Need to find $f(X)$: $f(X)\cdot(X+1) = \underbrace{g(X)\cdot(X^3+X^2-1)}_{\in J} + 1$

$X^2\cdot(X+1) = X^3+X^2 = 1\cdot(X^3+X^2-1)+1$

$\Rightarrow$ $[X^2]_J \cdot [X+1]_J = 1_J$ in $\mathbb{F}_3[X]/J$ $\Rightarrow$ $\boxed{([X+1]_J)^{-1} = [X^2]_J}$

(d) $\operatorname{char} K[X] = \operatorname{char}(K)$ for a ring K. Quotient by a non-constant polynomial does not change the characteristic.

$\Rightarrow \operatorname{char} A = \operatorname{char} B = \operatorname{char} \mathbb{F}_3 = 3$.

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**]

(a) Since $5, 3, 14$ are pairwise coprime, by the Chinese remainder theorem the system is solvable and if $n \in \mathbb{Z}$ is a solution, then $n + 5 \cdot 3 \cdot 14k$ is also a solution for any $k \in \mathbb{Z}$.

$n + 210k$

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

(b) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 0 \pmod 3 \end{cases} \Rightarrow 3t = 5s + 3$, for example $t = 1, s = 0$

$\Rightarrow x \equiv 3 \pmod{15}$

$\begin{cases} x \equiv 3 \pmod{15} \\ x \equiv 2 \pmod{14} \end{cases} \Rightarrow 14t + 2 = 15s + 3$

$-1 = 15s - 14t \Rightarrow$ for example $s = -1, t = -1$.

$\Rightarrow \boxed{x \equiv -12 \pmod{210}}$.

The smallest positive solution is $210 - 12 = \boxed{198}$

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**]

(a) We will write a as a product of disjoint cycles.

$a = (12)(123) = (1)(23) = (23) \Rightarrow$ a has order $\boxed{2}$.

$b = (135)(246)$ is a product of two disjoint cycles of order 3

$\Rightarrow$ order$(b) = \text{lcm}(3,3) = \boxed{3}$.

(b) For example, the element $r = (123)(4567) \in S_7$ is a product of disjoint cycles of order 3 and 4 $\Rightarrow$ order$(r) = \text{lcm}(3,4) = 12$.
Then the subgroup generated by r in S_7 is the cyclic group of order 12: $\langle r \rangle \approx C_{12}$.

(c) $s = (135)$, $t = (246)$ commute (disjoint cycles)

$s^3 = 1$, $t^3 = 1 \Rightarrow$ the group generated by s and t in S_7 has the elements:

$$\{1, s, s^2, t, t^2, st, st^2, s^2t, s^2t^2\}$$

$\Rightarrow |G| = 9$ and G is abelian because $st = ts$.

(d) Suppose that $t \in S_7$ generates C_9. Let $t = \pi_1 \pi_2 \cdots \pi_k$, a product of disjoint cycles of lengths $l_1, \ldots l_k$ $\Rightarrow \text{lcm}(l_1, \ldots l_k) = 9 \Rightarrow \exists l_i = 9$ but this is impossible, because there is no cycle of length 9 in the group of permutations of 7 elements. The longest cycle in S_7 has length = 7.

$\Rightarrow$ There is no subgroup isomorphic to C_9 in S_7.

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**]

(a) $f(X) = 3X^3 - 2X^2 + 1$ has degree 3 $\Rightarrow$ it is irreducible in $\mathbb{Q}[X]$ if it has no root in $\mathbb{Q}$.

Using the theorem, we need to check only candidates of the form

$\frac{r}{s}$: $s \mid 3$ and $r \mid 1$ $\Rightarrow$ $\frac{r}{s} \in \{\pm 1, \pm \frac{1}{3}\}$.

We have $f(1) = 2$, $f(-1) = -4$, $f(\frac{1}{3}) = \frac{1}{9} - \frac{2}{9} + 1 \neq 0$, $f(-\frac{1}{3}) = -\frac{1}{9} - \frac{2}{9} + 1 \neq 0$.

$\Rightarrow$ $f(X)$ is irreducible in $\mathbb{Q}[X]$.

(b) $g(X) = 2X^3 + 3X^2 + 2X - 2$ has degree 3 $\Rightarrow$ irreducible $\Leftrightarrow$ no roots in $\mathbb{Q}$.

By the theorem, a candidate is of the form $\frac{r}{s}$: $s \mid 2$ and $r \mid -2$

$\Rightarrow$ $\frac{r}{s} \in \{\pm 1, \pm \frac{1}{2}, \pm 2\}$.

We compute: $g(\pm 1) \neq 0$, $g(2) > 0$, $g(-2) < 0$

$g(-\frac{1}{2}) = -\frac{1}{4} + \frac{3}{4} - 1 - 2 < 0$, $g(\frac{1}{2}) = \frac{1}{4} + \frac{3}{4} + 1 - 2 = 0$ $\Rightarrow g(X) = (X - \frac{1}{2})p(X)$

$\Rightarrow$ $g(X)$ is not irreducible in $\mathbb{Q}[X]$.

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**]

9: Thm in the course

10: $\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow$ $n = p$ is a prime.

11: By Eisenstein's criterion, 3 divides $a_0 \dots a_{n-1}$, does not divide a_n, and 3^2 does not divide a_0 $\Rightarrow$ irreducible in $\mathbb{Q}[X]$.

12. $I \cdot J = (120)$, $I \cap J = (\text{lcm}(10, 12)) = (60)$.