
Final exam

January 14, 2017 **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) Find the greatest common divisor $d(X)$ of the polynomials

$$f(X) = 2X^6 + 4X^5 - 2X^2 - X - 3 \text{ et } g(X) = 2X^5 - X^2 - 1$$

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

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

2. Let $D_3 = \langle r, s \,|r^3 = 1, s^2 = 1, srs = r^{-1}\rangle$ be the dihedral group of order 6, and $C_4 = \langle t \mid t^4 = 1\rangle$ cyclic of order 4. Let $G = D_3 \times C_4$.

(a) Show that G is not abelian.

(b) Let $H = \langle (r, t^2)\rangle$ be the subgroup in G generated by (r, t^2). Find the order of H. Is H normal in G?

(c) Let $K = \langle (s, t)\rangle$ be the subgroup in G generated by (s, t). Find the order of K. Is K normal in G?

3. (a) Let p be a prime number and $a \in \mathbb{Z}$, $a \geq 1$. Give a formula (without a proof) for $\varphi(p^a)$, where φ is the Euler totient function.
   (b) Compute $\varphi(20)$.
   (c) List all the units in $\mathbb{Z}/20\mathbb{Z}$.
   (d) Find the inverse of $[13]_{20}$ in the ring $\mathbb{Z}/20\mathbb{Z}$.
   (e) Show that for $a \in \mathbb{Z}$ such that $(a, 60) = 1$ we have $a^{16} \equiv 1 \pmod{20}$.

.

.

4. (a) List all abelian groups of order 200 up to isomorphism.
   (b) For each group give the set of elementary divisors and invariant factors.
   (c) Exactly one of the groups is cyclic. Find it and justify your answer.

5. Let (X^2+2) be an ideal in the ring $\mathbb{R}[X]$.

   (a) Show that X^3+6X is congruent to $4X$ modulo (X^2+2), meaning that $[X^3+6X]_{(X^2+2)} = [4X]_{(X^2+2)}$.

   (b) Show that $K = \mathbb{R}[X]/(X^2+2)$ is a field (cite a theorem from the course).

   (c) Denote $\alpha = [X]_{(X^2+2)} \in K$, the class of X modulo (X^2+2). Show that $\alpha \neq [0]_{(X^2+2)}$ and find an inverse of α in K.

.

6. Which of the following rings are integral domains? Which are principal ideal domains? Justify your answer.

   (a) $\mathbb{Z}$

   (b) $\mathbb{Z}/6\mathbb{Z}$.

   (c) $\mathbb{Z}/6\mathbb{Z}[X]$.

   (d) $\mathbb{Z}[X]$.

7. Let S_6 be the group of permutations of 6 elements.

   (a) Find the order of $(23)(156)$ in S_6.

   (b) Show that there exists a cyclic subgroup $C_k \subset S_6$ for $k = 2, 3, 4, 5, 6$.

   (c) Is there $C_7 \subset S_6$? Cite a theorem from the course.

   (d) Is there $C_8 \subset S_6$?

8. Show that any $a \in \mathbb{Z}$ has the property $a^{17} \equiv a \pmod{30}$.

Second part, questions 9 to 14.

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. Which one of the following rings has a zero divisor? $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$.

10. (True/False) The characteristic of the field of 125 elements is 25.

11. (True/False) Let D_n be the dihedral group of order $2n$, and $H \subset D_n$ the stabilizer subgroup of one of the vertices of the regular n-gon. Then $|H| = 2$.

12. (True/False) There exists a field of 18 elements.

13. (True/False) Let $I = (25)$, $J = (15)$ and $K = (7)$ be three ideals in the ring $\mathbb{Z}$. Check which of the following statements are true:

    - $I + J = \mathbb{Z}$.
    - The ring $\mathbb{Z}/K$ Is an integral domain
    - $I \cap J = (375)$.
    - There exists exactly three ideals J_1, J_2, J_3 in $\mathbb{Z}$ such that $J \subset J_i$ and $J \neq J_i$ for $i = 1, 2, 3$.

14. (True/False) Let G be a group of units in the ring $\mathbb{Z}/10\mathbb{Z}$. Then G is cyclic generated by $[3]_{10}$.