EPFL

Algebra MATH-310
January 27, 2025
15:15 - 18:15
Anna Lachowska

283

Extra 1

SCIPER: **n/a** Signature: Lachowska

Instructions

- Please write your answers inside the provided frames
- No document is allowed.
- No electronic devices are allowed.
- Please provide clear, concise and easily readable arguments. You can aswer in English or in French but please do not mix the two laguages.
- Scrap paper will not be read by the graders.
- 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 set of natural numbers

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											

Question 1 *(6 pts.)*

(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 $f(X)r(X) + g(X)s(X) = t(X)$.

(a) $X^6 - 1 \mid X^2 - 2X + 1$

$X^6 - 2X^5 + X^4 \mid X^4 + 2X^3 + 3X^2 + 4X + 5$

$2X^5 - X^4 - 1$

$2X^5 - 4X^4 + 2X^3$

$3X^4 - 2X^3 - 1$

$3X^4 - 6X^3 + 3X^2$

$4X^3 - 3X^2 - 1$

$4X^3 - 8X^2 + 4X$

$5X^2 - 4X - 1$

$5X^2 - 10X + 5$

$6X - 6$

$X^2 - 2X + 1 \mid 6X - 6$

$X^2 - X \mid \frac{1}{6}X - \frac{1}{6}$

$-X + 1$

$-X + 1$

$\Rightarrow \gcd(f(x), g(x)) = 6x - 6 = d(x)$ in $\mathbb{Q}[x]$

(b) Monic $\gcd(f(x), g(x)) = \frac{1}{6}(6x - 6) = x - 1 = t(x)$

(c) $d(x) = 6x - 6 = f(x) \cdot 1 - g(x) \cdot (x^4 + 2x^3 + 3x^2 + 4x + 5)$

$t(x) = f(x) \cdot \frac{1}{6} + g(x) \cdot \left(-\frac{1}{6}x^4 - \frac{1}{3}x^3 - \frac{1}{2}x^2 - \frac{2}{3}x + \frac{5}{6}\right)$

$r(x) = \frac{1}{6}$, $s(x) = -\frac{1}{6}x^4 - \frac{1}{3}x^3 - \frac{1}{2}x^2 - \frac{2}{3}x + \frac{5}{6}$

Question 2 *(12 pts.)*

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.

(a) A subgroup is a subset of the group that forms a group with respect to the group operation and the identity element.

Let $K = \langle r^6 \rangle \subset D_8$. Then $(r^6)^2 = r^4, (r^6)^3 = r^2, (r^6)^4 = 1 \in K$

$(r^6)^{-1} = r^2, (r^4)^{-1} = r^4 \Rightarrow K = \{1, r^2, r^4, r^6\}$, $|K| = 4$.

(b) A subgroup $H \lhd G$ is normal if for any $h \in H$, any $g \in G \Rightarrow ghg^{-1} \in H$.

Consider $K \subset G = D_8$. Since r^{2k} commutes with r, we have $r r^{2k} r^{-1} = r^{2k}$ $\forall k = 1, 2, 3$.

$$s r^{2k} s^{-1} = s r^{2k} s = \underbrace{(srs)(srs) \cdots (srs)}_{2k} = r^{-2k} \in K.$$

Therefore, since r and s generate D_8, we have $K \lhd D_8$ is normal.

(c) $T = D_8/K$ is the group of left cosets with respect to K.

$|T| = [D_8 : K] = |D_8|/|K| = 16 : 4 = 4$.

$T = \{1 \cdot K, s \cdot K, r \cdot K, sr \cdot K\} = \{[1], [s], [r], [sr]\}$

We have: $sr^{2k} sr^{2k} = r^{-2k} r^{2k} = 1$, $r \cdot r^{2k} \cdot r \cdot r^{2k} = r^{4k+2} \in 1K$

$sr^{2k} \cdot r r^{2k} = sr^{4k+1} = sr \cdot r^{4k} \in srK$

$r r^{2k} \cdot s \cdot r^{2k} = s(s r^{2k+1} s) r^{2k} = sr^{-2k-1} r^{2k} \in sr^{-1} \cdot K = sr^1 \underbrace{r^6 \cdot K}_{\in K} \in srK$

$\Rightarrow$ T is abelian.

Alternatively, any group of order 4 is abelian: If $t \in T$, $|T| = 4$ if t has order 4 $\Rightarrow T \simeq C_4$ abelian; otherwise $t^2 = 1$ and t generates a subgroup of index 2 in $T \Rightarrow \langle t \rangle \lhd T$ is normal $\Rightarrow$ if $h \in T \Rightarrow hth^{-1} \in \langle t \rangle \Rightarrow hth^{-1} = t$, $h^2 = 1$ and T is abelian.

(d) $F \subset D_8$ s.t. $s \in F$, $|F| = 8$

Let $F = \langle s, r^2 \rangle \simeq D_4 \subset D_8$ $\quad F = \{1, r^2, r^4, r^6, sr^2, sr^4, sr^6\}$

we have $sr^2s = r^{-2} = r^6 \in F$

$$r^{2k} s r^{2m} = ss r^{2k} s r^{2m} = sr^{2(m-k)} \in F$$

$$sr^{2k} \cdot sr^{2m} = r^{2(m-k)} \in F$$

$$(r^{2k})^{-1} = r^{-2k} = r^{8-2k} \in F$$

$$(sr^{2k})^{-1} = r^{-2k} s = ss r^{-2k} s = sr^{2k} \in F$$

$\Rightarrow F \subset D_8$ is a subgroup

Question 3 *(12 pts.)*

(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 $\mathbb{Z}/15\mathbb{Z}$. (wrt multiplication)

(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

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

(a) $\varphi(p^n) = p^n - p^{n-1}$

(b) $\varphi(15) = \varphi(3)\cdot\varphi(5) = (3-1)(5-1) = 8$ (3 and 5 coprime)

$\varphi(6) = \varphi(3)\cdot\varphi(2) = (3-1)(2-1) = 2$

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

(c) $\{[1], [2], [4], [7], [8], [11], [13], [14]\}$ 8 invertible elts in $\mathbb{Z}/15\mathbb{Z}$

(d) $[14]_{15} = [-1]_{15} \Rightarrow [14]_{15}\cdot[14]_{15} = [-1]_{15}[-1]_{15} = [1]_{15}$

$\Rightarrow ([14]_{15})^{-1} = [14]_{15}$

(e) Let m, n positive integers > 1, $\gcd(m,n) = p$ a prime.

Let $m = p^k t$, $n = ps \Rightarrow \gcd(t,s) = 1$, $k \geq 1$, $\gcd(p,t) = \gcd(p,s) = 1$

$\varphi(m) = \varphi(p^k)\varphi(t)$, $\varphi(n) = \varphi(p)\varphi(s)$, $\varphi(nm) = \varphi(p^{k+1}ts) = \varphi(p^{k+1})\varphi(t)\varphi(s)$

$(p^k - p^{k-1})\varphi(t)$ $\quad$ $(p-1)\varphi(s)$ $\quad$ $(p^{k+1} - p^k)\varphi(t)\varphi(s)$

$\Rightarrow \varphi(mn) = p^k(p-1)\varphi(t)\varphi(s) = \frac{p}{p-1}p^{k-1}(p-1)^2\varphi(t)\varphi(s) = \frac{p}{p-1}\varphi(m)\varphi(n)$

For example, in (b) we have $\varphi(15\cdot 6) = \frac{3}{3-1}\varphi(15)\cdot\varphi(6)$

$\gcd(15,6) = 3$

$24 = \frac{3}{2}\,8\cdot 2$

Question 4 *(12 pts.)*

(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.

(a) $900 = 100 \cdot 9 = 25 \cdot 4 \cdot 9 = 2^2 \cdot 3^2 \cdot 5^2$ partitions of 2: (2) (1,1)

Groups:

C_4	$C_2 \times C_2$	C_4	$C_2 \times C_2$	C_4	$C_2 \times C_2$	C_4	$C_2 \times C_2$
C_9	C_9	$C_3 \times C_3$	$C_3 \times C_3$	C_9	$C_3 \times C_3$	$C_3 \times C_3$	C_9
C_{25}	C_{25}	C_{25}	C_{25}	$C_5 \times C_5$	$C_5 \times C_5$	$C_5 \times C_5$	$C_5 \times C_5$

There are 8 groups

(b) (4, 9, 25), (2, 2, 9, 25) (4, 3, 3, 25), (2, 2, 3, 3, 25) (4, 9, 5, 5), (2, 2, 3, 3, 5, 5) (4, 3, 3, 5, 5), (2, 2, 9, 5, 5).

(c) Computing the invariant factors of each group, we get:

C_{900} ; $C_{450} \times C_2$; $C_{300} \times C_3$; $C_{150} \times C_6$; $C_{180} \times C_5$; $C_{30} \times C_{30}$;

$C_{60} \times C_{15}$; $C_{90} \times C_{10}$

Each group contains a cyclic subgroup of order a multiple of 30.

C_{30k} contains an element of order 30: its generator t^k

$(t^k) \in C_{30k}$ has order 30.

(d) By a theorem from the course we know that an abelian G, $|G| = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ is isomorphic to a direct product of abelian groups of prime power orders, where $p_1 \dots p_m$ are distinct primes.

$\Rightarrow G \simeq G_{p_1^{a_1}} \times G_{p_2^{a_2}} \times \dots \times G_{p_m^{a_m}}$

Let $p_1 \dots p_k$ be a subset of $p_1 \dots p_k \dots p_m$ distinct primes

By theorem of Cauchy we know that an abelian groups whose order is divisible by p contains an element of order p, p a prime.

$\Rightarrow G_{p_i^{a_i}}$ contains an element of order p_i for each i.

$\Rightarrow (t_1, t_2 \ldots t_k, 1) \in G$ is an element of G where each $t_i \in G_{p_i^{a_i}}$ (1 trivial in the remaining factors)

of order p_i. The order of the direct product of elements is the lcm (orders of elements) $\Rightarrow o(t_1, t_2 \ldots t_k) = p_1 p_2 \ldots p_k$.

Alternatively, the highest invariant factor of G is divisible by the product of all of its prime divisors. $\Rightarrow G_{p_1 \ldots p_k} \subset G$.

Question 5 *(12 pts.)*

(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 $\tilde{p}(y) = \frac{(y+1)^5-1}{y}$ 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 $\tilde{p}(y)$ 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 $\tilde{p}(y)$, 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.

(a) $x^5-1 \mid x-1$

x^5-x^4

x^4-1

x^4-x^3

x^3-1

x^2-1

$x-1$

0

$x^4+x^3+x^2+x+1 \in \mathbb{Q}[x]$

(b) $\tilde{p}(y) = \frac{(y+1)^5-1}{y} = \frac{y^5+5y^4+10y^3+10y^2+5y+1-1}{y} = y^4+5y^3+10y^2+10y+5$

$\times 5 \quad 15 \quad 15 \quad 15 \quad 15$

$\times 5^2$

$\tilde{p}(y)$ is irreducible in $\mathbb{Q}[y]$ by the Eisenstein criterion.

(c) Suppose $p(x) = f(x) \cdot g(x) \Rightarrow \tilde{p}(y) = \tilde{f}(y) \cdot \tilde{g}(y) = f(y+1)g(y+1)$

$\deg f \geq 1, \deg g \geq 1 \qquad y = x-1 \Leftrightarrow x = y+1$

The leading coefficient of $f(x)$ equals the leading coeff. of $\tilde{f}(y)$

$\Rightarrow \deg \tilde{f} = \deg f, \deg \tilde{g} = \deg g$

$\Rightarrow \tilde{p}(y) = \tilde{f}(y) \cdot \tilde{g}(y)$ is reducible $\Rightarrow$ contradiction.

$\deg \geq 1 \quad \deg \geq 1$

$\Rightarrow$ if $\tilde{p}(y)$ is irreducible, so is $p(x) = x^4+x^3+x^2+x+1$ in $\mathbb{Q}[x]$

(d) $\frac{x^p-1}{x-1} = p(x) \Rightarrow \tilde{p}(y) = \frac{(y+1)^p-1}{y} = \frac{y^p + \binom{p}{1}y^{p-1} + \dots + \binom{p}{k}y^{p-k} + \dots \binom{p}{p-1}y + 1 - 1}{y} =$

$= y^{p-1} + \binom{p}{1}y + \dots + \binom{p}{k}y^{p-k-1} + \dots + \binom{p}{p-1}$

The coefficients $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ are divisible by p $\forall k: 1 \le k \le p-1$
and not divisible by p^2,
since p is a prime.

$\Rightarrow$ By the Eisenstein criterion $\tilde{p}(y)$ is irreducible in $\mathbb{Q}[y]$

$\Rightarrow$ $p(x)$ is irreducible in $\mathbb{Q}[x]$.

Question 6 *(6 pts.)*

(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.

(a) Since the numbers 13, 4, 3 are pairwise coprime, the system of congruences $\begin{cases} a \equiv x_1 \pmod{13} \\ a \equiv x_2 \pmod{4} \\ a \equiv x_3 \pmod{3} \end{cases}$ has a solution in $\mathbb{Z}$.

The set of all integer solutions is $\{x + 3 \cdot 4 \cdot 13k\}_{k \in \mathbb{Z}}$ where x is a solution

(b) $\begin{cases} a \equiv -1 \pmod{4} \\ a \equiv 1 \pmod{3} \end{cases}$ For example, $x = 7$ is a solution.

$\Rightarrow 7 + 12k$ is a solution $\forall k \in \mathbb{Z}$

$\Rightarrow \begin{cases} a \equiv 7 \pmod{12} \\ a \equiv 10 \pmod{13} \end{cases}$ $\Rightarrow 7 + 12k = 10 + 13m$

$13m - 12k = -3 \quad m = k = -3$

$-39 + 36 = -3 \Rightarrow x = 10 - 39 = -29$ is a solution.

$\Rightarrow$ all solutions are $\{-29 + 156\mathbb{Z}\} = \{-29 + 156n\}_{n \in \mathbb{Z}}$ ($156 = 3 \cdot 4 \cdot 13$)

(c) The smallest positive solution is $156 - 29 = 127$

Question 7 *(10 pts.)*

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 $[X]_{(X^4+X^3+1)} \in K$.

(a) Polynomials of degree 2 in $\mathbb{F}_2[x]$:

x^2 ; x^2+1, x^2+x, x^2+x+1

0 is a root; 1 is a root; 0 and 1 are roots

the only irreducible polynomial of deg 2 in $\mathbb{F}_2[x]$.

(b) If $x^4+x^3+1 = f(x)\cdot g(x)$ ($\deg f \geq 1$, $\deg g \geq 1$) $\Rightarrow$ either one of $f(x), g(x)$ is of degree 1 $\Rightarrow$ x^4+x^3+1 has a root in $\mathbb{F}_2$

or x^4+x^3+1 = a product of irreducible polynomials of degree 2

clearly x^4+x^3+1 has no roots in $\mathbb{F}_2$

Also, by (a) (x^2+x+1) is the only irreducible polynomial of degree 2

But $(x^2+x+1)^2 = x^4+x^2+1 \neq x^4+x^3+1$

Therefore, x^4+x^3+1 is irreducible in $\mathbb{F}_2[x]$.

(c) $K = \mathbb{F}_2[x]/\langle f(x)\rangle$ is ~~irreducible~~ a field $\Leftrightarrow$ $f(x)$ is irreducible over $\mathbb{F}_2$.

by (b), $K = \mathbb{F}_2[x]/\langle x^4+x^3+1\rangle$ is a field

The number of elements of K equals $2^4 = 16$ by a theorem from the course.

(d) $[x]\cdot[x^3+x^2] = [x^4+x^3+1] + [1] = [1]$

$\Rightarrow [x]^{-1} = [x^3+x^2]$

Question 8 *(12 pts.)*

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.

(a) $a = (314)(2145) = (13)(245)$

(b) a is a product of disjoint cycles of length 2 and 3

$\Rightarrow o(a) = \text{lcm}(2,3) = 6$

(c) The conjugacy class of a consists of all products of a 2-cycle and a disjoint 3-cycle. The cycle type of a permutation is preserved by conjugation, and by conjugation we can obtain any element of the same cycle type. $|C_a| = (\#\text{choices of 3 out of 5 elts}) \times 2$ ← since for every choice of 3 elts (abc) there are 2 different permutations: (abc) (acb)

$a \in S_5$

The remaining 2 elements form a 2-cycle, which determines a unique transposition.

$\Rightarrow |C_a| = \binom{5}{3} \cdot 2 = \frac{5!}{3!2!} \cdot 2 = \frac{5 \cdot 4}{2} \cdot 2 = 20$

$\Rightarrow |C_a| = 20$

(d) $K = \{1, (13), (15), \ldots\}$ Since transpositions generate a symmetric group, $K \cong S_3$ on the elements $\{1, 3, 5\}$ $\Rightarrow K = \{1, (13), (15), (35), (135), (153)\}$

Can compute explicitly: $(13)(15) = (153)$, $(15)(13) = (135)$

$(13)(15)(13) = (35)$

$|K| = 6$

(e) Let $t = (135) \Rightarrow t^2 = (135)(135) = (153)$, $t^3 = 1$, $\Rightarrow (135)^{-1} = (153)$

$\Rightarrow H = \{1, (135), (153)\}$

(cf) $H \subset K$ by the list of elements, or because

$\{1, (135), (153)\} = H \subset K = \{1, (13), (15), (35), (135), (153)\}$

$(135) = (15)(13) \in K$

$\Rightarrow$ the subgroup generated by $t = (135)$ is contained in K.

Question 9 *(In each of the following questions, you get 1 point for correct answer, −1 point for incorrect answer and 0 point for no answer.)*

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

Two elements are associates if one can be obtained from another by multiplication by a unit. Here: $[4]_7 \cdot [3]_7 = [5]_7$; $[5]_7 \cdot [5]_7 = [4]_7$ associates

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

By classification theorem, (8, 9) and (4, 2, 3, 3) describe non-isomorphic groups. (elt of order 9; no elt of order 9 $\cong C_4 \times C_3 \times C_3 \times C_2$)

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

There is no 8-cycle in S_7, and no product of disjoint cycles with lcm of lengths = 8