7/57/

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

$$f(X) = X^3 + X^2 + X + 1$$
 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]

$$\frac{x^{3} + x^{2} + x + 1}{x^{3} - 3x^{2} + 2x} = \frac{x^{2} - 3x + 1}{x + 4}$$

(a) Enclidean division:
$$\frac{x^{3} + x^{2} + x + 1}{x^{3} - 3x^{2} + 2x} = \frac{x^{2} - 3x + 2}{x + 4} = \frac{x^{2} - 3x + 2}{x^{2} - 2x} = \frac{x - 2}{x - 1}$$
(b)
$$\frac{x^{3} + x^{2} + x + 1}{x + 4} = \frac{x^{2} - 3x + 2}{x + 4} = \frac{x - 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{4x^{2} - 2x + 1}{4x^{2} - 2x + 3} = \frac{-x + 2}{x - 2}$$

$$\frac{x - 2}{3x + 2} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 1}$$

$$\frac{x^{2} - 3x + 2}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{x - 2x}{x - 2x}$$

$$\frac{x - 2x}{x - 2x} = \frac{$$

$$x-2 = \underbrace{X^{3} + X^{2} + X + 1}_{f(x)} - \underbrace{(x+4)(x^{2} - 3x + 2)}_{g(x)} = \underbrace{1 \cdot f(x) + (-x-4) \cdot g(x)}_{g(x)}$$

$$= x \cdot f(x) + \underbrace{(-x-4) \cdot g(x)}_{g(x)}$$

$$= x \cdot f(x) + \underbrace{(-x-4) \cdot g(x)}_{g(x)}$$

- 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 => order(t), $t \in G$? Lagrange's theorem: o(t) dividus |G| => possible orders of ells are: 2;5,10.

(6) G abelian, $|G|=10=2.5 \Rightarrow G \simeq C_2 \times C_5 \simeq C_{10}$ only one cyclic group of order $10: C_{10} \simeq C_2 \times C_5$

(c) G is not abelian: Cauchy's theorem: if prime p divides |G|, then
there exist t of order = p in G. => I am elt t of order 5 in G.

What can be $StS \neq St^j$ otherwise $tS = t^j = S = t^{j-1}$ impossible as above impossible $tS = t^j = St^j = St^$

j=1= $j^2=1$, j=2= $j^2=4=-1$, j=3= $j^2=9=-1$; j=4= $j^2=16=1$

 \Rightarrow if G is not abelian \Rightarrow $G \simeq D_5$.

- 3. (a) Let m and n be two integers, $n > m \ge 2$, such that $m \mid n$. Show that $\varphi(m) \mid \varphi(n)$, where φ is Euler's totient function.
 - (b) Compute $\varphi(15)$ and $\varphi(90)$.

$$\mathcal{L}(p^k) = p^k - p^{k-1}$$

- (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)
$$n = \prod p_i^{k_i}$$
; $m = \prod p_i^{l_i}$ since $m \mid n \Rightarrow l_i \leq k_i \neq i$ $\begin{cases} p_i \end{cases}$ distinct primes $Y(n) = \prod (p_i^{k_i} - p_i^{k_i-1})$, $Y(m) = \prod (p_i^{l_i} - p_i^{l_i-1})$

Thm: if p is a prime $\Rightarrow Y(p^k) = p^k - p^{k-1}$ $k \geq 1$

If
$$k_i = l_i \implies (p_i^{l_i-1}) = (p_i^{k_i} - p_i^{k_i-1})$$

If $k_i \ge l_i > 1 \implies p_i^{l_i-1}(p_{i-1}) \mid p_i^{k_{i-1}}(p_{i-1}) \mid p_i^{k_{i-1}}(p_{i-1})$

If $l_i = 0 \implies 1$ dividus everything:

(6)
$$\varphi(15) = \varphi(5) \cdot \varphi(3) = 4 \cdot 2 = 8$$

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

$$(c)(\frac{7}{152})^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\} |(\frac{7}{152})^{*}| = \{(15), (15),$$

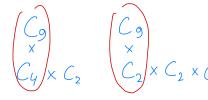
(d)
$$g(d(a, 90) = 1 \Rightarrow g(d(a, 15) = 1 \Rightarrow Euler's thm: $a^{\varphi(15)} \equiv 1 \pmod{15}$
=> $a^8 \equiv 1 \pmod{15} \Rightarrow a^{16} \equiv 1 \pmod{15}$$$

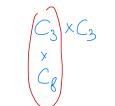
- 4. (a) How many different abelian groups are there of order 72? List these groups without repetition. (You can use the notation C_m to denote the cyclic group of order m.)
 - (b) For each group provide its elementary divisors and invariant factors.
 - (c) List all abelian groups of order 72 that contain an element of order 9.
 - [9 points]

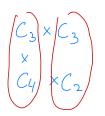
$$|G| = 72 = 2^3 \cdot 3^2$$

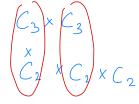
 $|G| = 72 = 2^3 \cdot 3^2$ partitions: (3), (2,1), (1,1,1) and (2) (1,1)











=> 6 different abelian groups

(6) Elementary divisors:

(9,8), (9,4,2), (9,2,2,2), (3,3,8), (3,3,4,2), (3,3,2,2,2)

Invariant factors:

(72) (36,2) (18,2,2) (24,3) (12,6) (6,6,2)

(c) An elf of order 9 can belong to a cyclic gp 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

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

Thm:

 $F_3[x]/$ is a field \iff f(x) inveducible in $F_3[x]$

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) $\angle = \times \times^3 + \times -2$ no f irreducible in $F_3[x]$ x = 1 is a roof \Rightarrow not irreducible. $= \times \times^3 + \times -2 = (x-1)(x^2 + x + 2) \Rightarrow A = F_3[x]/(x^3 + x 2)$ is not a field
- (b) $F_3[x]/$ is a field \iff $X^3 + X^2 1 = g(x)$ is irreducible f(x) irreducible and f(x) deg g = 3 \iff irreducible \iff ho roofs in F_3 . $g(0) = -1, \quad g(1) = 1, \quad g(-1) = -1 \implies \text{no roofs} \implies g(x) \text{ is irreducible}$ and $B = F_3[x]/g$ is a field.
- (c) B is a field $[x+1]_J \neq [0]_J$ since $deg(x+1) < deg(x^3+x^2-1)$. => $[x+1]_J$ is invertible in B.

Need to find h(x): $h(x) \cdot (x+1) = k(x)(x^3 + x^2 - 1) + 1$ (Euclidean $\chi^2(x+1) = (x^3 + x^2 - 1) + 1 => h(x) = [x^2]_2$ $=> [x^2]_2 \cdot [x-1]_2 = [1]_2 => ([x+1]_2)^2 = [x^2]_2.$

(d) Thm: $\operatorname{char}(K[x]) = \operatorname{char}(K)$ $= \operatorname{char}(K[x]) = \operatorname{char}(K[x]/g(x)) = \operatorname{char}(K)$ $\operatorname{Since} \operatorname{deg} f(x) = 3 \operatorname{deg} g(x) = 3$ $= \operatorname{char} A = \operatorname{char} B = \operatorname{char} F_3 = 3.$

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) By CRT since gcd(5,3)=1, gcd(5,14)=1 gcd(3,14)=1 $=> \exists a \ solution \ for the system given by <math>a+(3.5.14)Z=a+210Z \Rightarrow infinitely many solutions.$

$$\begin{cases} X \equiv 3 \pmod{5} \\ X \equiv 0 \pmod{3} \end{cases} \implies X \equiv 3 \qquad \begin{cases} X \equiv 3 \pmod{5} \\ X \equiv 2 \pmod{4} \end{cases}$$

$$14t+2 = 15s+3$$

- 1 = 15s-14t => s=-1, t=-1 works.

In general: Euclidean division since 14, 15 coprime
$$=> X = -15 + 3 = -12$$
.

=>
$$X = -12$$
 is a solution
=> all solutions are $\int -12 + 210 h \int_{h \in \mathbb{Z}}$

$$=>$$
 -12+210 = 198 is the smallest positive solution.

- 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 $k \ge 1$.
 - (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]

(d)
$$C_9 \subset S_7$$
? $y \in S_7 : o(y) = 9$

$$\operatorname{lcm}(C_1, C_2 ... C_k) = 9 , C_1 + C_2 + ... + C_k \neq 7$$
no solutions => no elt of order 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) $dig f = 3 \Rightarrow f(x)$ is irreducible \iff no roots in \mathbb{Q} .

 If $J = \frac{1}{5}$ is a root of f(x) in $\mathbb{Q} = 3$ = 3/3 and 1/3 = 3/5 = 3/4.

 We have: f(1) = 2, f(-1) = -4, $f(\frac{1}{3}) = \frac{1}{9} \frac{2}{9} + 1 \neq 0$, $f(-\frac{1}{3}) = -\frac{1}{9} \frac{2}{9} + 1 \neq 0$. = 3/3 and 1/3 = 3/3 and 1/3
- (8) $\deg g = 3 \Rightarrow g(x)$ is irreducible over G $L \Rightarrow ho roots in <math>G$. If $\chi = \frac{1}{5}$ is a root of g(x) in $G \Rightarrow S[2], r[2 \Rightarrow \frac{1}{5}e\{\pm 1, \pm 2, \pm \frac{1}{2}\}\}$ We have: $g(\pm 1) \neq 0$, g(2) > 0, g(-2) < 0. $g(-\frac{1}{2}) = -\frac{1}{4} + \frac{3}{4} - 1 - 2 < 0$, $g(\frac{1}{2}) = \frac{1}{4} + \frac{3}{4} + 1 - 2 = 0$. $g(x) = (x - \frac{1}{2})p(x)$. => g(x) is not irreducible in 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 $I \cdot J \neq I \cap J$.

[4 points]

7 9.
$$(G:H)=2 \Rightarrow G=HVkH, k\notin H$$
 Thm: HCG index 2 is normal theh, $\forall g\in G$. $ghg'\in H$. $G=HVkH, k\notin H$. (PS5]. $h_1h_1h_2'\in H$; $kh_1h(kh_1)'=$

=
$$k h_1 h_1^{-1} k_1^{-1} = k h_2 = \lambda h_1 h_1^{-1} k_1^{-1} = \lambda h_1 h_1^{-1} h_1^{-1} k_1^{-1} = \lambda h_1 h_1^{-1} k_1^{-1} = \lambda h_1^{-1} h_1 h_1^{-1} h_1^$$

7 11.
$$X^7 + 15X^6 - 12X^3 - 6X + 6$$
 =) irreductly over Q by Eisenstein. 31 31 31

F 12.
$$I = (10)$$
, $J = (12)$: $I \cap J = (e_{cm}(10,12)) = (60)$.
 $I \cdot J = (10 \cdot 12)$