Review: Exam - 2021.

1. (a) Let $\mathbb{F}_7$ be the field of 7 elements. Find a greatest common divisor $d(X)$ of the polynomials

$$f(X) = X^4 - 2X^3 + 2X^2 - 3X - 1 \qquad \text{and} \qquad g(X) = X^3 - 2X^2 - 2$$

in the ring $\mathbb{F}_7[X]$. (Provide the details of your computation.)

(b) If $d(X)$ is not monic, find the unique monic greatest common divisor $t(X)$ of $f(X)$ and $g(X)$.

(c) Find $r(X), s(X) \in \mathbb{F}_7[X]$ such that $f(X)r(X) + g(X)s(X) = t(X)$.

[6 **points**]

$\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$.

(a)

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

$\underbrace{2X^2-X-1}_{deg=2<3}$

$$\begin{array}{l|l} X^3-2X^2-2 & 2X^2-X-1 \\ \hline X^3-4X^2-4X & 4X+1 \\ \hline 2X^2+4X-2 & \\ 2X^2-X-1 & \\ \hline 5X-1 & \end{array}$$

$5X-1$ last nontrivial remainder $= gcd(f,g)$

$$\begin{array}{l|l} 2X^2-X-1 & 5X-1 \\ \hline -5X^2+X & -X+1 \\ \hline -2X-1 & \\ 5X-1 & \\ \hline 0 & \end{array}$$

$$\Rightarrow gcd(f(x),g(x)) = \boxed{5X-1 = d(x)}$$

(b) $t(x) = \frac{1}{5}d(x) = \boxed{X-3}$

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

$= f(x)(-4x-1)+g(x)(4X^2+X+1)$; $\boxed{t(x) = f(x)(-5X-3)+g(x)(5X^2+3X+3)}$

2. Let G be a group of order 12.

(a) List all possible orders of elements in G.

(b) How many different **abelian** groups are there of order 12? Find the elementary divisors of these groups.

(c) Let S_4 be the symmetric group of permutations of 4 elements. Recall that the alternating group $A_4 \subset S_4$ is the subgroup of all **even** permutations in S_4. List all elements of $A_4 \subset S_4$ in terms of products of disjoint cycles. In particular, show that $|A_4| = 12$.

(d) Show that any subgroup $H \subset A_4$ of order 3 is **not normal** in A_4.

(e) There is a unique subgroup $K \subset A_4$ of order 4. List all elements in K and prove that it is **normal**.

(f) Is there a subgroup of order 6 in A_4? Justify your answer.

(g) Give an example (in terms of generators and relations) of a group G of order 12 that is **not abelian** and **not isomorphic to** A_4.

(a) $|G| = 12 \Rightarrow$ possible order of elements in G : 1, 2, 3, 4, 6, 12.

(b) $|G| = 12$ abelian $\quad 12 = 2^2 \cdot 3 \quad$ partitions of 2: (2), (1,1)

$C_3 \times C_4 \qquad C_3 \times C_2 \times C_2 \qquad \Rightarrow$ 2 groups C_{12}, $C_6 \times C_2$.

$C_{12} \qquad C_6 \times C_2 \qquad$ Elementary divisors: (3,4), (3,2,2).

(c) S_4 ; $A_4 \subset S_4$ what are the cycle types possible in S_4?

(1) $\quad$ (ab) $\quad$ (abc) $\quad$ (abcd) , $\quad$ (ab)(cd)

even $\quad$ odd $\quad$ even $\quad$ odd $\quad$ even

$A_4 = \{(1), (123), (132), (134), (143), (234), (243), (124), (142), (12)(34), (13)(24), (14)(23)\} \Rightarrow |A_4| = 12.$

(d) $A_4 = \{(1), (123), (132), (134), (143), (234), (243), (124), (142), (12)(34), (13)(24), (14)(23)\}$

$H < A_4$, $|H| = 3 \simeq C_3 \Rightarrow \exists$ a generator $t \in H$, $\{t, t^2, 1\} = H$

$t = (abc)$ any 3-cycle $\Rightarrow \{1, (abc), (acb)\} = H$

$\forall g \in A_4$ $\quad g(abc)g^{-1} \overset{?}{\in} H$; but $(acd)(abc)(adc) = (cbd) \notin H$. $\Rightarrow H < A_4$ is not normal

$$g(x_1 x_2 \ldots x_k)g^{-1} = (g(x_1)\, g(x_2) \ldots g(x_k))$$

(e) $|K| = 4 \Rightarrow$ orders of elts in K: 1, 2 or 4.

$\Rightarrow K = \{1, (12)(34), (13)(24), (14)(23)\}$ $\qquad K \lhd A_4$ because.

$g(ab)(cd)g^{-1} = (xy)(zt) \in K$ (conjugation preserves cycle type)

(f) $g(abc)g^{-1}$ where g is another 3-cycle (adc), or $(ab)(cd)$

always leads to a different 3-cycle

$(bcd)(abc)(bdc) = (acd) \Rightarrow$ get too may elts more than 6

$\Rightarrow$ no subgp of order 6 in A_4.

(e) $D_6 = \langle r, s \mid r^6 = 1, s^2 = 1, srs = r^{-1} \rangle$

is not isomorphic to A_4 because A_4 has no elts of order 6.

3. Let φ denote the Euler totient function.

(a) Compute $\varphi(7)$, $\varphi(49)$, $\varphi(6)$ and $\varphi(36)$.

(b) Let p be a prime. Which is bigger, $\varphi(p^2)$ or $(\varphi(p))^2$? Prove your answer.

(c) Let $n > 1$ be a natural number. Which is bigger, $\varphi(n^2)$ or $(\varphi(n))^2$? Prove your answer.

(a) $\varphi(p^k) = p^k - p^{k-1}$ $\qquad \varphi(n,m) = \varphi(n)\cdot\varphi(m)$ if $\gcd(n,m) = 1$

$\varphi(7) = 6$; $\varphi(49) = 49 - 7 = 42$, $\varphi(6) = \varphi(2)\cdot\varphi(3) = (2-1)(3-1) = 2$

$\varphi(36) = \varphi(4)\cdot\varphi(9) = (4-2)(9-3) = 12.$

(b) $\varphi(p^2) = p^2 - p$, $(\varphi(p))^2 = (p-1)^2 = p^2 - 2p + 1$

$p^2 - p > p^2 - 2p + 1 \iff p > 1$ true for any prime p.

(c) $\varphi(n^2)$ or $(\varphi(n))^2$? $\qquad n = p_1^{k_1} \cdots p_r^{k_r}$ prime factorization

$\varphi(n^2) = \prod_{i=1}^{r} p_i^{2k_i - 1}(p_i - 1)$; $\quad \varphi(n) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1) \Rightarrow \varphi(n)^2 = \prod_{i=1}^{r} p_i^{2k_i - 2}(p_i - 1)^2$

$\| \quad >$

$\prod_{i=1}^{r} p_i^{2k-2}(p_i^2 - p_i)$

$p_i^2 - p_i > p_i^2 - 2p_i + 1$

$\Rightarrow \varphi(n^2) > (\varphi(n))^2. \qquad \forall n > 1.$

. Let C_k denote the cyclic group of order $k \in \mathbb{N}^+$.

$C_n \times C_m \simeq C_{nm} \iff \gcd(n,m) = 1$

(a) How many different (non-isomorphic) abelian groups of order 162 are there? List the elementary divisors and invariant factors for each of the groups above.

(b) Among the groups listed above, find all that contain a subgroup of order 27 that is **not cyclic.** Justify your answer.

(c) Among the groups listed above, find all that contain **no element of order 9**. Justify your answer.

$|G| = 162 = 2 \cdot 3^4$

Partitions: of 4: $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$

of 1: (1)

Elementary divisors →	$C_2 \times C_{3^4}$	$C_2 \times C_{3^3} \times C_3$	$C_2 \times C_{3^2} \times C_{3^2}$	$C_2 \times C_{3^2} \times C_3 \times C_3$	$C_2 \times C_3 \times C_3 \times C_3 \times C_3$
Invariant factors →	C_{162}	$C_{54} \times C_3$	$C_{18} \times C_9$	$C_{18} \times C_3 \times C_3$	$C_6 \times C_3 \times C_3 \times C_3$

(b) contain a subgp of order 27 that is not cyclic

(c) $C_6 \times C_3 \times C_3 \times C_3$ is the only group with no elt of order 9.

5. Let $\mathbb{F}_3$ be the field of 3 elements. Define the ideals in $\mathbb{F}_3[X]$

$$I = \langle X^3 + X^2 + X - 1\rangle, \quad J = \langle X^3 + X^2 + X + 1\rangle, \quad K = \langle X^3 - X^2 + X + 1\rangle$$

Let

$$A = \mathbb{F}_3[X]/I, \qquad B = \mathbb{F}_3[X]/J, \qquad C = \mathbb{F}_3[X]/K.$$

(a) Which of the rings A, B, C are fields? (justify your answer, cite theorems from the course).

(b) Find the number of elements in A.

(c) Find the inverses of the elements $[X]_I$ in A, $[X]_J$ in B and $[X]_K$ in C, if they exist.

(d) Which of the ring(s) are not integral domain(s)? In this case give an example of a nontrivial zero divisor.

(e) Which of the rings A, B, C are isomorphic to each other? Justify your answer.

(f) What is the structure of the abelian group of units of A? (justify your answer, cite a theorem from the course).

(a) $deg = 3$ $\qquad \mathbb{F}_3 = \{0, 1, -1\} = \{0, 1, 2\}$

Check for $0, 1, -1$ as roots $\Rightarrow$ find X^3+X^2+X-1 and X^3-X^2+X+1 are irreducible ($deg = 3$)

but $X^3+X^2+X+1 = (X+1)(X^2+1)$ is not irreducible

Thm: $F[x]/\langle f(x)\rangle$ is a field $\Leftrightarrow$ $f(x)$ is irreducible over F. $\Rightarrow$ A, C are fields; B is not a field.

(b) $|A| = 3^3 = 27$ (Thm: $F[x]/\langle f(x)\rangle$ a finite field $\Rightarrow$ $|F[x]/\langle f(x)\rangle| = |F|^{\deg f(x)}$)

(c) $[X]_I [X^2+X+1]_I = [1]_I + [X^3+X^2+X-1]_I = [1]_I \Rightarrow [X]_I^{-1} = [X^2+X+1]_I$

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

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

(d) B is not an integral domain: $[x+1]_J \cdot [x^2+1]_J = [x^3+x^2+x+1]_J = [0]_J$.

nontrivial zero divisors in B.

(e) Thm: $\exists!$ field of order 27 $\Rightarrow A \simeq C$

B is not a field $\Rightarrow$ not isomorphic to A or C.

(f) $A = \mathbb{F}_3[x]/I$ is a field. Thm: The group of units of a finite field is cyclic. $\Rightarrow A^* \simeq$ Cyclic gp

$|A| = 27 \Rightarrow |A^*| = 26 \Rightarrow A^* \simeq C_{26}$.

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 7 \\ x \equiv 3 \pmod{15}. \end{cases}$$

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

(b) Find all integer solutions of the system.

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

(a) $\{2, 7, 15\}$ are pairwise coprime. Thm: If the moduli are pairwise coprime, then the system of congruences has infinitely many integer solutions (CRT for $\mathbb{Z}$).

(b) $\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 7 \end{cases}$ $\begin{cases} x \equiv 8 \pmod{14} \\ x \equiv 3 \pmod{15} \end{cases}$ $\Rightarrow$ $8 + 14t = 3 + 15s$

$5 = 15s - 14t$

$s = t = 5$

$\Rightarrow$ $x = 8 + 70 = 3 + 75 = 78 \pmod{210}$

$\Rightarrow$ $\boxed{x = 78 + 210k, \quad k \in \mathbb{Z}}$

(c) $\boxed{x = 78.}$

7. Let S_n denote the symmetric group of permutations of $n \in \mathbb{N}^+$ elements.

(a) Consider the elements $a = (2143)(234) \in S_6$ and $b = (2143)(235) \in S_6$. Write a and b as products of disjoint cycles and find their orders.

(b) Recall that for any $g \in S_n$ and any cycle $(x_1....x_k) \in S_n$, we have $g(x_1...x_k)g^{-1} = (g(x_1)...g(x_k))$ in S_n. Use this identity to find the number of elements in the conjugacy class $\{gag^{-1}\}_{g\in S_6}$.

(c) Find the number of elements in the conjugacy class $\{gbg^{-1}\}_{g\in S_6}$.

(d) What is the maximal order of an element in S_6? Justify your answer.

(e) What is the maximal order of an element in S_7? Justify your answer.

(a) $a = (2143)(234) = (14)\cancel{(2)}\cancel{(3)} = (14) \Rightarrow \text{order}(a) = 2$

$b = (2143)(235) = (1435)\cancel{(2)} = (1435) \Rightarrow \text{order}(b) = 4$

(b) S_6 ; $\{1,2,3,4,5,6\}$; $a = (14) \in S_6$.

$g(14)g^{-1} = (xy)$ for some $x, y \in \{1, 2, .., 6\}$, $x \neq y$

$\Rightarrow \{g(14)g^{-1}\}_{g\in S_6} = \#$ transpositions in $S_6 = C_6^2 = \frac{6!}{4!\cdot 2!} = \frac{6\cdot 5}{2} = \boxed{15 \text{ elts}}$

(c) $g(1435)g^{-1} = (x\,y\,z\,u) \Rightarrow \{g(1435)g^{-1}\}_{g\in S_6} = \#$ of 4-cycles in S_6

$(abcd)$, (a,bdc), $(adbc)$ $(adcb)$, $(acbd)$ $(acdb)$

$C_6^4 \cdot 3! = \frac{6!}{4!2!}\cdot 3! = \frac{6\cdot 5}{2}\cdot 6 = 15\cdot 6 = 90 \Rightarrow \boxed{90 \text{ elts.}}$

(d) S_6 : find $n_1 + n_2 + .. + n_r \leq 6$

$lcm(n_1, n_2 . n_r)$ is maximal

if 3 cycles: $(2,2,2)$ $= lcm = 2$

if 2 cycles: $(2,4)$ or $(3,3)$ $(3,2)$ $\Rightarrow$ max $lcm = 6$

1 cycle: (6) $\Rightarrow$ max $= 6$

$\Rightarrow$ max order $= 6$ in S_6.

(e) S_7 : $n_1 + n_2 .. \leq 7$

$(2,2,3)$ $lcm = 6$

$(5,2)$ $(4,3)$ $lcm = 10$, $lcm = 12$ $\Rightarrow$ max order $= 12$ in S_7.

(7)

8. (a) State the definition of the characteristic of a ring.

(b) State the definition of a homomorphism of rings.

(c) Let A and B be two rings and suppose that $f : A \to B$ is a ring homomorphism. Prove that $\mathrm{char}(B)$ divides $\mathrm{char}(A)$.

(d) Let $A_1 = \mathbb{Z}$, $A_2 = \mathbb{Z}/5\mathbb{Z}$, $A_3 = \mathbb{Z}/15\mathbb{Z}$. Use (c) to determine which of the ring homomorphisms

$$f_{ij} : A_i \to A_j, \qquad i \neq j \in \{1, 2, 3\}$$

can exist. Describe all possible ring homomorphisms between these rings.

(a) $\exists !\ \mathbb{Z} \xrightarrow[\text{homomorphism}]{\tau} A$ $\quad \ker \tau = d\mathbb{Z} \quad \Rightarrow d =$ char of A.

(b) $F : A \to B$ is a ring homomorphism if $F(0) = 0$, $F(1) = 1$, $F(ab) = F(a)F(b)$, $F(a+b) = F(a) + F(b)$ $\forall a, b \in A$.

(c) $f : A \to B$ homom. Then $f(1_A) = 1_B \Rightarrow f(\underbrace{n \cdot 1_A}_{\overset{n = \mathrm{char} A}{=0 \text{ in } A}}) = n f(1_A) = n \cdot 1_B = 0$ in B

$\Rightarrow (\mathrm{char} A) \cdot 1 = 0$ in B

But $(\mathrm{char}\, B) \cdot 1 = 0$, char B is the smallest with this property.

$\Rightarrow$ char B has to divide char A.

(d)

$$\begin{tikzcd} & \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z} \arrow[ur] \arrow[dr] & \\ & \mathbb{Z}/15\mathbb{Z} \arrow[uu] \end{tikzcd}$$

are all possible ring homomorphisms by (c).

9. (True/False) If G is a non-abelian group, then the direct product group $G \times H$ is non-abelian for any group H.

10. (True/False) If $\gcd(n, m) > 1$, then the equation $nx + my = 6$ can never have integer solutions x, y.

11. (True/False) The polynomial $5X^5 + 4X^4 + 8X^3 + 10X^2 + 2$ is irreducible in $\mathbb{Q}[X]$.

12. (True/False) The dihedral group D_n is isomorphic to a direct product of cyclic groups of orders n and 2.

9. True. If $t, s \in G$: $ts \neq st \Rightarrow (t,1)(s,1) = (ts,1) \neq (st,1) = (s,1)(t,1)$ in $G \times H$

10. False: if $\gcd(n,m)$ divides 6 $\Rightarrow$ possible to have a solution
Ex: $12x + 6y = 6$ has solution $x = 1, y = -1$.

11. True: $p = 2$ divides $a_{n-1} \dots a_0$, $p^2 = 4$ does not divide a_0, p does not divide a_n $\Rightarrow$
by Eisenstein irreducible over $\mathbb{Q}$.

12. False: The dihedral gp is not abelian, but $C_n \times C_2$ is an abelian gp.
$sr \neq rs$