Practice exam. Q1. (a) Find the monic $\gcd(f(x), g(x))$ in $\mathbb{Q}[x]$

$$f(x) = 2x^6 + 4x^5 - 2x^2 - x - 3 \quad ; \quad g(x) = 2x^5 - x^2 - 1.$$

$$\begin{array}{l|l} 2x^6 + 4x^5 - 2x^2 - x - 3 & 2x^5 - x^2 - 1 \\ \hline 2x^6 \qquad - x^3 \qquad - x & x + 2 \\ \quad 4x^5 + x^3 - 2x^2 - 3 & \\ \quad 4x^5 \qquad - 2x^2 - 2 & \\ \hline \qquad x^3 \qquad - 1 & \end{array}$$

$$\begin{array}{l|l} 2x^5 - x^2 - 1 & x^3 - 1 \\ \hline 2x^5 - 2x^2 & 2x^2 \\ \hline x^2 - 1 & \end{array} \qquad \begin{array}{l|l} x^3 - 1 & x^2 - 1 \\ \hline x^3 - x & x \\ \hline x - 1 & \end{array}$$

$$\begin{array}{l|l} x^2 - 1 & x - 1 \\ \hline 0 & x + 1 \end{array} \Rightarrow \gcd(f, g) = x - 1 \text{ monic.}$$

$\Rightarrow$ the $\gcd(f(x), g(x)) = x - 1$ (monic)

(b) Find $r(x), s(x) \in \mathbb{Q}[x]$: $f(x) \cdot r(x) + g(x) \cdot s(x) = \gcd(f(x), g(x)) = x - 1$

Read the Euclidean algorithm backwards

$$x - 1 = x^3 - 1 - x(x^2 - 1) = (x^3 - 1) - x(\underbrace{2x^5 - x^2 - 1}_{g(x)} - 2x^2(x^3 - 1)) =$$

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

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

$$= \underbrace{(1 + 2x^3)}_{r(x)} f(x) + \underbrace{(-x - (1 + 2x^3)(x + 2))}_{s(x)} g(x) = x - 1 = \gcd(f(x), g(x)).$$

Q2 $D_3 = \langle r, s \mid r^3 = 1, s^2 = 1, srs = r^{-1} \rangle$ dihedral gp of order 6

$C_4 = \langle t \mid t^4 = 1 \rangle$ cyclic gp of order 4. Let $G = D_3 \times C_4$.

(a) G is not abelian: $(s,1)\cdot(r,1) = (sr,1)$; $(r,1)\cdot(s,1) = (\underbrace{rs}_{\substack{\shortparallel \\ sr^{-1} \neq sr}},1) \neq (sr,1)$.

(b) $H = \langle (r,t^2) \rangle < G$ order of H? is it normal in G?

$x = (r,t^2)$; $x^2 = (r^2, t^4 = 1)$, $x^3 = (1, t^2)$, $x^4 = (r,1)$, $x^5 = (r^2, t^2)$, $x^6 = (1,1)$

$\Rightarrow |H| = 6$. you can show that $(a,b) \in G_1 \times G_2 \Rightarrow o(a,b) = \operatorname{lcm}(o(a), o(b))$

Proof: $(a^k, b^k) = 1 \iff o(a) \mid k$ and $o(b) \mid k \Rightarrow o(a,b) = \operatorname{lcm}(o(a), o(b))$.

Is $H < G$ normal? $g\,(r,t^2)\,g^{-1} \overset{??}{<} H$ for any $g \in G$ (enough to check for generators).

$(1,t)(r\,t^2)(1,t^{-1}) = (r, t t^2 t^{-1}) = (r,t^2) \in H$

$(r,1)(r,t^2)(r^{-1},1) = (r r r^{-1}, t^2) = (r,t^2) \in H$ $\Rightarrow H \triangleleft G$ is normal

$(s,1)(r,t^2)(s,1) = (srs, t^2) = (r^{-1}, t^2) = (r^2, t^2) \in H$

(c) $K = \langle (s,t) \rangle < G$; $|K| = ?$ is it normal in G?

order $(s) = 2$, order $(t) = 4 \Rightarrow$ order $(s,t) = \operatorname{lcm}(2,4) = 4 \Rightarrow |K| = 4$

$(r,1)(s,t)(r^{-1},1) = (rsr^{-1}, t) = (sr^{-1}r^{-1}, t) = (sr, t) \notin K$.

$rs = sr^{-1}$

$\Rightarrow K < G$ is not normal.

Q3. (a) Formula for $\varphi(p^a)$, p prime, $a \in \mathbb{N}^+$ $= p^a - p^{a-1} = p^{a-1}(p-1)$ (See PS 1).

(b) $\varphi(20) = \varphi(2^2 \cdot 5) = \varphi(2^2) \cdot \varphi(5) = (4-2)\cdot(5-1) = 8.$

(c) Units in $\mathbb{Z}/20\mathbb{Z}$ $\rightarrow$ $\{\bar{1}, \bar{3}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}$

(d) Inverse of $[13]_{20}$ $\Leftrightarrow$ $x, y \in \mathbb{Z}: x \cdot 13 + y \cdot 20 = 1.$

$20 = 1 \cdot 13 + 7, \quad 13 = 1 \cdot 7 + 6, \quad 7 = 1 \cdot 6 + 1$

$\Rightarrow 1 = 7 - 6 = 7 - (13 - 7) = 2 \cdot 7 - 13 =$

$= 2(20-13) - 13 = 2 \cdot 20 - 3 \cdot 13 = 1$

$\Rightarrow [x]_{20} = [-3]_{20} = [17]_{20} \Rightarrow ([13]_{20})^{-1} = [17]_{20}$

(e) Suppose $\gcd(a, 60) = 1$. Show $a^{16} \equiv 1 \pmod{20}$

Euler's thm: If $\gcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$\gcd(a, 20) = 1 \Rightarrow a^{\varphi(20)} \equiv 1 \pmod{20} \Rightarrow a^8 \equiv 1 \pmod{20}$

take a square

$a^{16} \equiv 1 \pmod{20}.$

Q4. (a) List all abelian groups of order 200. $= 5^2 \cdot 2^3$

Partitions of 2: (2), (1,1) partitions of 3: (3), (2,1), (1,1,1).

$C_{25} \times C_8$ $C_{25} \times C_4 \times C_2$ $C_{25} \times C_2 \times C_2 \times C_2$ $C_5 \times C_5 \times C_8$ $C_5 \times C_5 \times C_4 \times C_2$ $C_5 \times C_5 \times C_2 \times C_2 \times C_2$

C_{200} $C_{100} \times C_2$ $C_{50} \times C_2 \times C_2$ $C_{40} \times C_5$ $C_{20} \times C_{10}$ $C_{10} \times C_{10} \times C_2$

(b) Elementary divisors (25, 8), (25, 4, 2), (25, 2, 2, 2), (5, 5, 8), (5, 5, 4, 2), (5, 5, 2, 2, 2).

Invariant factors: (200), (100, 2) (50, 2, 2), (40, 5), (20, 10), (10, 10, 2)

(c) Exactly one of them is cyclic: C_{200} (other gps do not have an elt of order 200)

Q5. Ideal generated by (x^2+2) in $\mathbb{R}[x]$

(a) Show that x^3+6x is congruent to $4x$ modulo (x^2+2)

$$\begin{array}{r|l} x^3+6x & x^2+2 \\ \cline{2-2} x^3+2x & x \\ \hline 4x & \end{array}$$

$\Rightarrow 4x = x^3+6x - x(x^2+2) \Rightarrow x^3+6x = 4x + \underbrace{x(x^2+2)}_{\in I}$

$\Rightarrow [x^3+6x]_{(x^2+2)} = [4x]_{(x^2+2)}$.

(b) Show that $K = \mathbb{R}[x]/(x^2+2)$ is a field

Thm: $F[x]/(f(x)) = K$ is a field $\Leftrightarrow$ $f(x)$ is irreducible in $F[x]$.

(x^2+2) in $\mathbb{R}[x]$: (x^2+2) of degree $=2 \Rightarrow$ irreducible $\Leftrightarrow$ no roots in $\mathbb{R}$ - true.

$\Rightarrow$ $K = \mathbb{R}[x]/(x^2+2)$ is a field.

(c) Show that $[x]_{(x^2+2)} \neq [0]_{(x^2+2)}$ and find its inverse in K.

because $\underset{\deg = 2}{(x^2+2)}$ does not divide $\underset{\deg = 1}{x}$ for degree reasons

Need to find $f(x), g(x) \in \mathbb{R}[x]$: $f(x)\cdot x + g(x)\cdot(x^2+2) = 1$ $\quad$ (x and (x^2+2) are coprime in $\mathbb{R}[x]$)

$$\underbrace{-\tfrac{1}{2}x}_{f(x)} \cdot x + \underbrace{\tfrac{1}{2}}_{g(x)}(x^2+2) = 1.$$

$$\Rightarrow \left([x]_{(x^2+2)}\right)^{-1} = \left[-\tfrac{1}{2}x\right]_{(x^2+2)} \text{ in } K.$$

Q6. Integral domains? PID?

(a) $\mathbb{Z}$ integral domain (no zero divisors); PID (follows from the Euclidean division).

(b) $\mathbb{Z}/6\mathbb{Z}$ $\bar{2}\cdot\bar{3}=\bar{0}$ in $\mathbb{Z}/6\mathbb{Z}$ => not an integral domain => not a PID

(c) $\mathbb{Z}/6\mathbb{Z}[x]$ $\bar{2}\cdot\bar{3}=\bar{0}$ in $\mathbb{Z}/6\mathbb{Z}[x]$ => not an integral domain => not a PID.

(d) $\mathbb{Z}[x]$ $\mathbb{Z}$ has no zero divisors => integral domain. Not a PID
=> $\mathbb{Z}[x]$ no zero divisors

Not a PID: Ideal $(2, X) \subset \mathbb{Z}[x]$ is not generated by a single elt.

Let $(p(x)) = (2, X)$ in $\mathbb{Z}[x]$. => $2 = p(x)\cdot q(x)$ => $\deg p(x) = \deg(q(x)) = 0$.

=> $p(x) = \pm 1, \pm 2$. If $p(x) = \pm 1$ => $I = (p(x)) = \mathbb{Z}[x] \neq (2, X)$.

If $p(x) = \pm 2$ => any $a_0 + a_1 X + \ldots + a_n X^n$ has only even coefficients, but $(2, X)$ contains X with coefficient 1 => contradiction.

Q7. S_6 of permutations of 6 elements.

(a) Find the order of $(23)(156)$ in S_6. Suppose $c_1, c_2 \in S_6$ disjoint cycles.
$(c_1c_2)^k = c_1^k c_2^k = 1 \iff o(c_1) \mid k$ and $o(c_2) \mid k \Rightarrow o(c_1c_2) = \operatorname{lcm}(o(c_1), o(c_2))$.
Here $o((23)(156)) = \operatorname{lcm}(2,3) = 6$

(b) Show that $\exists\, C_k \subset S_6$ for $k = 2,3,4,5,6$
$C_2 = \langle (12) \rangle$; $C_3 = \langle (123) \rangle$, $C_4 = \langle (1234) \rangle$, $C_5 = \langle (12345) \rangle$; $C_6 = \langle (123456) \rangle$

(c) Is there $C_7 \subset S_6$? Cite a theorem from the course.
Lagrange's thm : If $H \subset S_6 \Rightarrow |H|$ divides $|S_6| = 6!$
$\Rightarrow 7 \nmid 6! \Rightarrow$ no subgp of order 7 in S_6.

(d) Is there $C_8 \subset S_6$? Clearly $8 \mid 6!$
If $t \in S_6$: $t^8 = 1 \Rightarrow t = c_1$, $t = c_1c_2$, $t = c_1c_2c_3$ product of disjoint cycles
order $(t) = \operatorname{lcm}(c_1, c_2)$ or $\operatorname{lcm}(c_1, c_2, c_3)$; $t^8 = 1 \Rightarrow$
c_1, c_2, c_3 can be of length 2, 4
but $\operatorname{lcm}(4,2) = 4$, $\operatorname{lcm}(2,2,2) = 2 \Rightarrow$ no cyclic subgroup $C_8 \subset S_6$.

Q8 Show that any $a \in \mathbb{Z}$ has the property $a^{17} \equiv a \pmod{30}$.

$30 = 2 \cdot 3 \cdot 5$ Show that $a^{17} - a$ is divisible by 2, by 3, and by 5

(1) $a^k \equiv a \pmod 2$ $\forall k \in \mathbb{N}^*$, $a \in \mathbb{Z}$.

(2) $a^3 \equiv a \pmod 3$ $\Rightarrow$ $a^{15} \equiv a^5 \pmod 3$ $\qquad$ $a^3 \equiv a \pmod 3$ $\Rightarrow$ $a^5 \equiv a^3 \equiv a \pmod 3$

3 prime $\qquad$ $\equiv a \pmod 3$ $\qquad$ $a^2 \equiv a^2 \pmod 3$

$\Rightarrow$ $a^{17} \equiv a^3 \equiv a \pmod 3$.

(3) $a^5 \equiv a \pmod 5$ $\Rightarrow$ $a^{15} \equiv a^3 \pmod 5$ $\Rightarrow$ $a^{17} \equiv a^5 \equiv a \pmod 5$

$a^2 \equiv a^2 \pmod 5$

$\Rightarrow$ $(a^{17} - a)$ is divisible by 2, by 3 and by 5 $\Rightarrow$ by 30.

for any $a \in \mathbb{Z}$.

Q9 - Q14. (a) Which of $\mathbb{Z}/7\mathbb{Z}$ or $\mathbb{Z}\times\mathbb{Z}$ has a nontrivial zero divisor?

$\cong \mathbb{F}_7$ a field $\qquad (1,0)\times(0,1) = (0,0)$ zero divisors

T/F (b) F_{125} has characteristic $= 25$ False: characteristic (field) $\in \{0, \text{prime}\}$

T/F (c) D_n dihedral; $H \subset D$ stabiliser of a vertex of a regular n-gon. Then $|H| = 2$.

Orbit-stabilizer thm: $|H| \cdot |\underset{n \text{ vertices}}{\text{Orbit}}| = |D_n| = 2n \Rightarrow |H| = 2$

T/F (d) There exists a field of 18 elements

$|F| = p^n$, p a prime. (thm).

(e) $I = (25)$, $J = (15)$, $K = (7) \subset \mathbb{Z}$ ideals. Then:

T/F $I + J = \mathbb{Z}$ $\qquad (25)+(15) = \gcd(25,15) = (5)$

T/F $\mathbb{Z}/K$ is an integral domain $\qquad \mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7$ a field (7 a prime)

T/F $I \cap J = (375)$ $\qquad (25)\cap(15) = (\text{lcm}(25,15)) = (75)$

T/F There are exactly 3 ideals $J_1, J_2, J_3 \subset \mathbb{Z}$: $J \subset J_i$ and $J \neq J_i$

$(15) \subset (5)$, $(15) \subset (3)$, $(15) \subset (1) = \mathbb{Z}$

T/F (f) $(\mathbb{Z}/10\mathbb{Z})^* = G$. Then G is cyclic generated by $[3]_{10}$. $\varphi(10) = 1 \cdot 4 = 4$.

$[1], [3], [7], [9]$; $[3]^2 = [9]$, $[3]^3 = [7]$; $[3]^4 = [1]$