Lecture 13: review.

First part, questions 1 to 8

$= \mathbb{Z}/5\mathbb{Z}$

1. (a) Let $\mathbb{F}_5$ be the finite field of 5 elements. Find the monic greatest common divisor $d(X)$ of the polynomials

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

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**]

(a) Euclidean division:

$$\begin{array}{r|l} x^3+x^2+x+1 & x^2-3x+2 \\ \underline{x^3-3x^2+2x} & x+4 \\ 4x^2-x+1 & \\ \underline{4x^2-2x+3} & \\ \underbrace{x-2}_{\gcd(f,g)} & \end{array} \qquad \begin{array}{r|l} x^2-3x+2 & x-2 \\ \underline{x^2-2x} & x-1 \\ -x+2 & \\ \underline{-x+2} & \\ 0 & \end{array}$$

(b)

$\Rightarrow \boxed{\gcd(f,g) = x-2 = x+3}$ in $\mathbb{F}_5[x]$, monic (the leading coeff $=1$)

(b): Read the Euclidean division backwards:

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

$$\Rightarrow \boxed{r(x) = 1 \qquad s(x) = -x-4 = -x+1}$$

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) $|G| = 10 \Rightarrow$ order(t), $t \in G$? Lagrange's theorem: $o(t)$ divides $|G|$

$\Rightarrow$ possible orders of elts are: $\underline{2;\ 5,\ 10.}$

(b) G abelian, $|G| = 10 = 2 \cdot 5 \Rightarrow G \simeq C_2 \times C_5 \simeq C_{10}$ only one cyclic group of order 10: $\underline{C_{10} \simeq C_2 \times C_5}$ coprime!

(c) G is not abelian: Cauchy's theorem: if prime p divides $|G|$, then there exist t of order $= p$ in G. $\Rightarrow \exists$ an elt t of order 5 in G.

(d) G, $|G| = 10$, $\exists t : o(t) = 5$, $\exists s : o(s) = 2$

$G = \{1, t, t^2, t^3, t^4, s, st, st^2, st^3, st^4\}$ 10 elts.

if $t^i = t^j \Rightarrow t^{i-j} = 1 \Rightarrow (i-j) \equiv 0 \pmod 5 \Rightarrow i = j$

$st^i = st^j \Rightarrow t^{i-j} = 1$ — " —

$t^i = st^j \Rightarrow s = t^{i-j} \Rightarrow s^2 = 1 = t^{2(i-j)} = 1 \Rightarrow 2(i-j) \equiv 0 \pmod 5$ $\Rightarrow i = j$

$\Rightarrow i - j \equiv 0 \pmod 5$ $\Rightarrow s = 1$ impossible $o(s) = 2$

What can be $sts \neq st^j$ otherwise $ts = t^j \Rightarrow s = t^{j-1}$ impossible as above

$\Rightarrow sts = t^j \Rightarrow st^js = t$; $(sts)^j = sts\,sts \ldots sts = st^js = t$ ($s^2 = 1$)
$j = 0, 1, 2, 3, 4$

$(sts)^j = (t^j)^j = t$

$\Rightarrow t^{j^2} = t \Rightarrow j^2 \equiv 1 \pmod 5$

$\underline{j = 1} \Rightarrow j^2 = 1$, $j = 2 \Rightarrow j^2 = 4 = -1$, $j = 3 \Rightarrow j^2 = 9 = -1$; $\underline{j = 4} \Rightarrow j^2 = 16 \equiv 1$

$\Rightarrow$ 2 possibilities: $sts = t$ $(j = 1) \Rightarrow st = ts$, G abelian $\Rightarrow G \simeq \underline{C_{10}}$

$sts = t^4$ $(j = 4) \Rightarrow sts = t^{-1} \Rightarrow D_5$.

$\Rightarrow$ if G is not abelian $\Rightarrow G \simeq \underline{D_5}.$

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

(b) Compute $\varphi(15)$ and $\varphi(90)$.

(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**]

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

(a) $n = \prod p_i^{k_i}$; $m = \prod p_i^{l_i}$ since $m \mid n \Rightarrow l_i \leq k_i \ \forall i$ $\{p_i\}$ distinct primes.

$\varphi(n) = \prod (p_i^{k_i} - p_i^{k_i - 1})$, $\varphi(m) = \prod (p_i^{l_i} - p_i^{l_i - 1})$

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

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

If $k_i \geq l_i \geq 1 \Rightarrow p_i^{l_i - 1}(p_i - 1) \mid p_i^{k_i - 1}(p_i - 1)$ $\Rightarrow \varphi(m) \mid \varphi(n)$.

If $l_i = 0 \Rightarrow 1$ divides everything :)

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

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

(c) $\left(\mathbb{Z}/15\mathbb{Z}\right)^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ $\left|\left(\mathbb{Z}/15\mathbb{Z}\right)^*\right| = \varphi(15)$.

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

$\Rightarrow a^8 \equiv 1 \pmod{15} \Rightarrow a^{16} \equiv 1 \pmod{15}$

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**]

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

$C_9 \times C_8$ $\quad C_9 \times C_4 \times C_2$ $\quad C_9 \times C_2 \times C_2 \times C_2$ $\quad C_3 \times C_3 \times C_8$ $\quad C_3 \times C_3 \times C_4 \times C_2$ $\quad C_3 \times C_3 \times C_2 \times C_2 \times C_2$

=> 6 different abelian groups

(b) 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 elt 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: $\mathbb{F}_3[x]/\langle f(x)\rangle$ is a field $\Leftrightarrow$ $f(x)$ irreducible in $\mathbb{F}_3[x]$

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) $\Leftrightarrow$ x^3+x-2 not irreducible in $\mathbb{F}_3[x]$ $\quad x=1$ is a root $\Rightarrow$ not irreducible.

$\Rightarrow x^3+x-2 = (x-1)(x^2+x+2) \Rightarrow A = \mathbb{F}_3[x]/\langle x^3+x-2\rangle$ is not a field

(b) $\mathbb{F}_3[x]/\langle f(x)\rangle$ is a field $\Leftrightarrow$ $f(x)$ irreducible in $\mathbb{F}_3[x]$. $\quad x^3+x^2-1 = g(x)$ is irreducible

$\deg g = 3 \Rightarrow$ irreducible $\Leftrightarrow$ no roots in $\mathbb{F}_3$.

$g(0) = -1,\ g(1) = 1,\ g(-1) = -1 \Rightarrow$ no roots $\Rightarrow g(x)$ is irreducible

and $B = \mathbb{F}_3[x]/J$ is a field.

(c) B is a field $\quad [x+1]_J \neq [0]_J$ since $\deg(x+1) < \deg(x^3+x^2-1)$.

$\Rightarrow [x+1]_J$ is invertible in B.

Need to find $h(x)$: $\quad h(x)\cdot(x+1) = k(x)(x^3+x^2-1)+1$ (Euclidean division in general)

$x^2(x+1) = (x^3+x^2-1)+1 \Rightarrow h(x) = [x^2]_J$

$\Rightarrow [x^2]_J\cdot[x-1]_J = [1]_J \quad \Rightarrow \quad ([x+1]_J)^{-1} = [x^2]_J.$

(d) Thm: $\operatorname{char}(\mathbb{K}[x]) = \operatorname{char}\mathbb{K}$

$\Rightarrow \operatorname{char}(\mathbb{K}[x]/\langle f(x)\rangle) = \operatorname{char}(\mathbb{K}[x]/\langle g(x)\rangle) = \operatorname{char}(\mathbb{K})$

since $\deg f(x) = 3 \quad \deg g(x) = 3$

$\Rightarrow \operatorname{char} A = \operatorname{char} B = \operatorname{char}\mathbb{F}_3 = 3.$

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 $\gcd(5,3)=1$, $\gcd(5,14)=1$ $\gcd(3,14)=1$
$\Rightarrow \exists$ a solution for the system given by
$a + (3\cdot 5\cdot 14)\mathbb{Z} = a + 210\mathbb{Z} \Rightarrow$ infinitely many solutions.

(b) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 0 \pmod 3 \end{cases} \Rightarrow x = 3$; $\begin{cases} x \equiv 3 \pmod{15} \\ x \equiv 2 \pmod{14} \end{cases}$

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

$-1 = 15s - 14t \Rightarrow s = -1, t = -1$ works.

In general: Euclidean division since 14, 15 coprime

$\Rightarrow x = -15 + 3 = -12$.

$\Rightarrow x = -12$ is a solution

$\Rightarrow$ all solutions are $\{-12 + 210n\}_{n \in \mathbb{Z}}$

$\Rightarrow -12 + 210 = \underline{198}$ 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 $k \geq 1$.

   (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**]

(a) $a = (12)(123) = (1)(23) = (23)$, $b = (135)(246)$ disjoint

$o(a) = 2$, $o(b) = 3$ (disjoint 3-cycles).

(b) $C_{12} < S_7$. Need to find an elt of order 12 in S_7

Thm: $x \in S_n$, $x = c_1 c_2 .. c_k$ disjoint cycles $\Rightarrow o(x) = \mathrm{lcm}(o(c_1) o(c_2) .. o(c_k))$

$x^m = 1 \Rightarrow c_1^m c_2^m .. c_k^m = 1 \iff c_1^m = 1, c_2^m = 1, .. c_k^m = 1$

because disjoint cycles act on separate orbits; if $c_1^n = c_2^k \Rightarrow c_1^n = c_2^k = 1$.

$\Rightarrow o(c_i) \mid m \ \forall i$, m the smallest $\Rightarrow o(x) = \mathrm{lcm}(o(c_1) .. o(c_k))$.

$\Rightarrow \mathrm{lcm}(n, m) = 12$, $n + m \leq 7$

$\Rightarrow n = 3, m = 4$ works.

$x = (123)(4567) \Rightarrow o(x) = 12. \Rightarrow \langle x \rangle \simeq C_{12} < S_7$.

(c) $s = (135)$ $t = (246)$ generate $H = \langle s, t : s^3 = 1, t^3 = 1, st = ts \rangle$

$\Rightarrow H = \{1, s, s^2, t, t^2, st, st^2, s^2t, s^2t^2\} \Rightarrow |H| = 9$

any elt in H: $s^m t^k$ $m \leq 2, k \leq 2$

$s^m t^k = t^k s^m$

In fact: $H \simeq \underset{s}{C_3} \times \underset{t}{C_3}$

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

$\mathrm{lcm}(c_1, c_2 .. c_k) = 9$, $c_1 + c_2 + .. + c_k \leq 7$

no solutions $\Rightarrow$ 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) $\deg f = 3 \Rightarrow f(x)$ is irreducible $\Leftrightarrow$ no roots in $\mathbb{Q}$.

If $\alpha = \frac{r}{s}$ is a root of $f(x)$ in $\mathbb{Q} \Rightarrow$ $s/3$ and $r/1$ $\Rightarrow \frac{r}{s} \in \{\pm 1, \pm\frac{1}{3}\}$

We have: $f(1) = 2,\ f(-1) = -4,\ f(\frac{1}{3}) = \frac{1}{9} - \frac{2}{9} + 1 \neq 0,\ f(-\frac{1}{3}) = -\frac{1}{9} - \frac{2}{9} + 1 \neq 0.$

$\Rightarrow$ $f(x)$ is irreducible.

(b) $\deg g = 3 \Rightarrow g(x)$ is irreducible over $\mathbb{Q}$ $\Leftrightarrow$ no roots in $\mathbb{Q}$.

If $\alpha = \frac{r}{s}$ is a root of $g(x)$ in $\mathbb{Q} \Rightarrow s \mid 2$, $r \mid 2 \Rightarrow \frac{r}{s} \in \{\pm 1, \pm 2, \pm \frac{1}{2}\}$

We have: $g(\pm 1) \neq 0,\quad g(2) > 0,\ g(-2) < 0.$

$g(-\frac{1}{2}) = -\frac{1}{4} + \frac{3}{4} - 1 - 2 < 0,\ g(\frac{1}{2}) = \frac{1}{4} + \frac{3}{4} + 1 - 2 = 0.\quad g(x) = (x - \frac{1}{2})p(x).$

$\Rightarrow g(x)$ is not irreducible in $\mathbb{Q}[x]$.

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 $I \cdot J \not= I \cap J$.

[4 **points**]

T 9. $[G:H]=2 \Rightarrow G = H \cup kH,\ k \notin H$ Thm: $H \subset G$ index 2 is normal in G. [PS 5].

$\forall h \in h,\ \forall g \in G.\ ghg^{-1} \in H.$ $G = H \cup kH,\ k \notin H.$

$h_1 h h_1^{-1} \in H$; $k h_1 h (kh_1)^{-1} =$

$= k h_1 h h_1^{-1} k^{-1} \overset{\text{Suppose}}{=} k h_2 \Rightarrow h_1 h h_1^{-1} k^{-1} = h_2 \Rightarrow k^{-1} = h_1 h^{-1} h_1^{-1} h_2$

$\Rightarrow k = h_2^{-1} h_1 h h_1^{-1} \in H.$ contradiction

$\Rightarrow ghg^{-1} \in H\ \forall g \in G.$ $\Rightarrow H$ is normal.

F 10. $\mathbb{Z}/8\mathbb{Z}$ $2 \cdot 4 = 0 \pmod 8$ nontrivial zero divisors $\Rightarrow$ not a field.

char $\mathbb{Z}/8\mathbb{Z} = 8$; char(field) $\in \{0$ or a prime$\}$.

T 11. $X^7 + 15X^6 - 12X^3 - 6X + 6$ $\Rightarrow$ irreducible over $\mathbb{Q}$ by Eisenstein.

$3 \nmid$ $3 \mid$ $3 \mid$ $3 \mid$ $3 \mid$

$9 \nmid$

F 12. $I = (10)$, $J = (12)$: $I \cap J = (\mathrm{lcm}(10,12)) = (60)$.

$I \cdot J = (10 \cdot 12)$ $\not=$