Lecture 13 : Review

$\mathbb{F}_5$

First part, questions 1 to 8

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

$$f(X) = 3X^5 - X^4 + 3X - 1 \qquad \text{and} \qquad g(X) = 3X^2 - 2$$

in the ring $\mathbb{F}_5[X]$. (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 $r(X), s(X) \in \mathbb{F}_5[X]$ such that $f(X)r(X) + g(X)s(X) = t(X)$.

[6 **points**]

(a)

$3X^5 - X^4 + 3X - 1 \;\big|\; 3X^2 - 2$

$3X^5 \quad -2X^3$

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

$-X^4 \quad - X^2$

$2X^3 + X^2 + 3X - 1$

$2X^3 \quad + 2X$

$X^2 + X - 1$

$X^2 \quad - 4$

$X + 3$

$3X^2 - 2 \;\big|\; X + 3$

$3X^2 - X \quad\quad 3X + 1$

$X - 2$

$X - 2$

0

last nontrivial remainder is a $\gcd(f(x), g(x))$

$\Rightarrow \gcd(f(x), g(x)) = X + 3$

(b) Here $X + 3$ is monic. $\therefore$ the leading coefficient is 1

(c) $X + 3 = t(X) = f(X) - g(X)(X^3 + 3X^2 - X + 2)$

$\Rightarrow r(X) = 1$, $s(X) = (-X^3 - 3X^2 + X - 2)$

2. (a) Let R be the group of all rotational symmetries of a regular octahedron around its center (see the picture next page). Find the number of elements in the orbit of vertex 1 under the action of R.

(b) Describe the subgroup $H \subset R$ that stabilizes the vertex 1 and find the order $|H|$.

(c) Cite the orbit-stabilizer theorem and apply it to find the order of the group R.

(d) Each element of R defines a permutation of the vertices of the regular octahedron (see the picture). This gives an injective homomorphism ϕ from R to the symmetric group S_6 of permutations of 6 elements. In particular $\phi(H)$ is a subgroup of S_6. List the elements of $\phi(H)$.

(e) Does R contain an element $a \in R$ of order 2? If so, describe the action of a on the octahedron geometrically and write $\phi(a)$ as a permutation in S_6.

(f) Does R contain an element $b \in R$ of order 3? If so, describe the action of b on the octahedron geometrically and write $\phi(b)$ as a permutation in S_6.

[14 **points**]

(a) $O_1(R) = \{1, 2, 3, 4, 5, 6\}$ = all vertices.

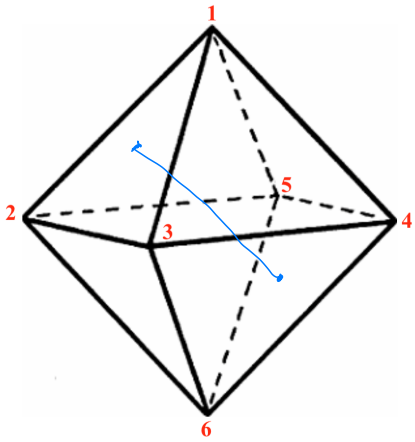
(b) $Stab_1(R)$ = Rotations around (1,6)-axis $\simeq C_4 \simeq H \Rightarrow |H| = 4$
rot. by multiples of 90°.

(c) If a finite group R acts by permutations on a finite set E, and $x \in E$, then $|R| = |Orb_x| \cdot |Stab_x|$
In our case $|R| = 6 \cdot 4 = 24$.

(d) $\varphi: R \to S_6$, $\varphi: H \to S_6$, $\varphi(H) = \{1, \underset{t}{(2345)}, \underset{t^2}{(24)(35)}, \underset{t^3}{(2543)}\}$

(e) Yes, any rotation by 180°, for example $(24)(35)$ about the axis (1,6).
$\varphi(a) = ((24)(35)) \Rightarrow \varphi(a)^2 = 1$
Any rotation about the line connecting mid-sides opposite

(f) Yes, for example the rotation about the axis connecting centers of two opposite sides: $\varphi(b) = (123)(456) \Rightarrow \varphi(b)^3 = 1$.
disjoint 3-cycles.


1
2
3
4
5
6

$\mathbb{F}_{11}$

3. Consider the field of 11 elements $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$.

   (a) Let $K = (\mathbb{F}_{11})^*$ be the group of units of $\mathbb{F}_{11}$. Find the order of K and describe its structure. Cite a theorem from the course.

   (b) List the orders of elements that occur in K. Justify your answer.

   (c) Give an example of an element $[a]_{11} \in K$ of order 2 and $[b]_{11} \in K$ of order 5.

   [10 **points**]

(a) $|K| = |(\mathbb{F}_{11}^*)| = 10$ all nonzero elts are units in a field.

Theorem: The group of units of a finite field is cyclic.

$\Rightarrow$ $K \simeq C_{10}$.

(b) By Lagrange's theorem, the order of an elt divides the order of the group $\Rightarrow$ possible orders are $\{1, 2, 5, 10\}$

$K \simeq C_{10} = \{1, t, t^2, t^3, t^4, t^5, t^6, t^7, t^8, t^9\}$

$\Rightarrow o(t) = 10$, $o(t^2) = 5$, $o(t^5) = 2$ $o(1) = 1$

$\Rightarrow$ elts of orders 1, 2, 5, 10 occur in K.

(c) Note that $[-1]_{11} \cdot [-1]_{11} = [1]_{11} \Rightarrow [-1]_{11} = [10]_{11} = [a]_{11}$

Note $[2]_{11}^5 = [32]_{11} = [-1]_{11} \Rightarrow [2]_{11}$ has order 10

$\Rightarrow [2]_{11}^2 = [4]_{11}$ has order 5 in K

Check: $[4]_{11}^5 = [1]_{11}$, $[6]_{11} = [4]_{11}$

4. (a) Let p be an odd prime. How many non-isomorphic abelian groups of order $8p^2$ are there? List the elementary divisors and invariant factors for each of the groups. You can use the notation C_k for the cyclic group of order $k \in \mathbb{N}^+$.

(b) Show that each of the groups listed above contains an element of order $2p$.

(c) Which of the groups listed in (a) contain an element of order $4p$? Justify your answer.

[9 **points**]

(a) $|G|$ abelian, $|G| = 8p^2$, $p \neq 2$ prime $\Rightarrow |G| = 2^3 \cdot p^2$

partitions: $(3), (2,1), (1,1,1)$ $\quad$ $(2), (1,1)$

$C_8 \times C_{p^2}$	$C_8 \times C_p \times C_p$	$C_4 \times C_2 \times C_{p^2}$	$C_4 \times C_2 \times C_p \times C_p$	$C_2 \times C_2 \times C_2 \times C_{p^2}$	$C_2 \times C_2 \times C_2 \times C_p \times C_p$
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
C_{8p^2}	$C_{8p} \times C_p$	$C_{4p^2} \times C_2$	$C_{4p} \times C_{2p}$	$C_{2p^2} \times C_2 \times C_2$	$C_{2p} \times C_{2p} \times C_2$

$\Rightarrow$ there are 6 groups up to isomorphism

Elementary divisors: $(8, p^2), (8, p, p), (4, 2, p^2), (4, 2, p, p), (2, 2, 2, p^2), (2, 2, 2, p, p)$

Invariant factors: $(8p^2), (8p, p), (4p^2, 2), (4p, 2p), (2p^2, 2, 2), (2p, 2p, 2)$

(b) Each group listed contains as a direct factor a cyclic group of order divisible by $2p$ $\Rightarrow$ it contains an elt of order $2p$.

Say C_n, $d \mid n$ has an elt of order d: $n = d \cdot k \Rightarrow$

if t is a generator of $C_n \Rightarrow t^k$ has order d: $(t^k)^d = t^n = 1$, and this is the smallest power of t^k that gives 1.

For example, $C_{4p^2} \times C_2$ contains $((t^{2p}, 1))^{2p} = (t^{4p^2}, 1) = (1,1)$
$t \quad s$ elt of order $2p$.

(c) The groups C_{8p^2}, $C_{8p} \times C_p$, $C_{4p^2} \times C_2$, $C_{4p} \times C_{2p}$

contain an elt of order $4p$.

Others do not: $C_a \times C_b \times C_c$ => the max order of an elt is $\text{lcm}(a, b, c) = a$

since $c \mid b \mid a$

So for the groups $C_{2p^2} \times C_2 \times C_2$, $C_{2p} \times C_{2p}, C_2$

$\text{lcm} = 2p^2$ $\text{lcm} = 2p$

both not divisible by $4p$.

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

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

Let

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

(a) Show that A is a field. Justify your answer (cite a theorem from the course).

(b) List all elements in A. In particular, find $|A|$.

(c) Find the inverse of the element $[X+1]_I$ in A.

(d) Is any of the rings B, C a field? Justify your answer.

(e) Can you compute the inverse of $[X+1]_J \in B$ and of $[X+1]_K \in C$?

(f) Is any of the rings A, B, C isomorphic to the ring $\mathbb{Z}/9\mathbb{Z}$? Justify your answer.

[12 **points**]

$\mathbb{F}_3$

(a) $I = \langle X^2+X-1 \rangle$, X^2+X-1 has deg $= 2$ $\Rightarrow$ it is irreducible $\Leftrightarrow$ has no roots in $\mathbb{F}_3$

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

by a theorem from the course $k[X]/\langle f(x) \rangle$ is a field $\Leftrightarrow$ $f(x)$ is irreducible

$\Rightarrow$ $A = \mathbb{F}_3[X]/I$ is a field.

(b) By a result from the course, elt in A have the form $aX+b$, $a, b \in \mathbb{F}_3$

since $f(x)$ has degree 2

$A = \{0, 1, -1, X, X+1, X-1, -X, -X+1, -X-1\}$. $|A| = 9 = 3^2$

(c) Inverse of $[X+1]_I$ in A

Consider $[X+1]_I [X]_I = [X^2+X]_I = [1]_I$ $\Rightarrow$ $[X]_I = [X+1]_I^{-1}$

$(X^2+X) - (X^2+X-1) = 1$

(d) $J = \langle X^2+1 \rangle$ $f(0) = 1$, $f(1) = f(-1) = -1 \neq 0$ $\Rightarrow$ no roots, deg $= 2$ $\Rightarrow$ irreducible

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

$K = \langle X^2-X+1 \rangle$ $f(0) = 1$, $f(1) = 1$, $f(-1) = 1+1+1 = 0$ $\Rightarrow$ not irreducible

$X^2-X+1 = (X+1)(X+1)$ $\Rightarrow$ $C = \mathbb{F}_3[X]/K$ is not a field.

by the theorems listed in (a).

(e) B is a field $\Rightarrow [X+1]_J$ is invertible

$(X+1)(X-1) = X^2-1 = X^2+(-2) \equiv [-2]_J \equiv [1]_J$

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

C is not a field, $[X+1]_K$ is not invertible because it is a zero divisor: $[X+1]_K [X+1]_K = [X^2-X+1]_K = [0]_K$.

(f) $\mathbb{Z}/9\mathbb{Z}$ is not a field $\Rightarrow A \neq \mathbb{Z}/9\mathbb{Z}$, $B \neq \mathbb{Z}/9\mathbb{Z}$

fields.

$C \neq \mathbb{Z}/9\mathbb{Z}$ since $c(C) = 3 = c(\mathbb{F}_3)$

$c(\mathbb{Z}/9\mathbb{Z}) = 9$

6. (a) Show that the system of congruences

$$\begin{cases} x \equiv 0 \pmod 6 \\ x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod{25}. \end{cases}$$

has infinitely many solutions in $\mathbb{Z}$ (cite a theorem from the course).

(b) Find all integer solutions of the system.

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

[6 **points**]

CRT for $\mathbb{Z}$:

(a) A system of congruences in $\mathbb{Z}$ has infinitely many solutions if and only if the modules are pairwise coprime

$6, 7, 25$ are pairwise coprime

$\Rightarrow$ the system has solutions

(b) $\begin{cases} x \equiv 0 \pmod 6 \\ x \equiv 1 \pmod 7 \end{cases}$

$\Rightarrow 6t = 7s + 1$

$6t - 7s = 1 \Rightarrow s = t = -1$

$a = -6 \pmod{42}$

$\begin{cases} a \equiv -6 \pmod{42} \\ a \equiv 2 \pmod{25} \end{cases}$

$-6 + 42t = 2 + 25q$

$42t - 25q = 8$

$t = -1, q = -2 \Rightarrow -42 + 50 = 8$

$\Rightarrow x = -48 \equiv 0 \pmod 6$

$\equiv 1 \pmod 7$

$\equiv 2 \pmod{25}$

$\Rightarrow$ All solutions are $x \in \{-48 + 1050\mathbb{Z}\} = \{-48 + 6 \cdot 7 \cdot 25\,\mathbb{Z}\}$

(c) The smallest positive solution is $x = -48 + 1050 = 1002$

7. Let S_5 denote the symmetric group of permutations of 5 elements.

(a) Consider the element $a = (243)(135)(14) \in S_5$ and write it as a product of disjoint cycles.

(b) Find the order of a.

(c) Find the number of elements in the conjugacy class $\{gag^{-1}\}_{g \in S_5}$.

(d) Let H be the subgroup in S_5 that consists of all permutations of the elements $\{1, 3, 5\}$. List all elements in H and find its order.

(e) Is H a normal subgroup in S_5? Justify your answer.

[10 **points**]

(a) $a = (243)(135)(14) = \underline{(135)(24)}$

(b) a is a product of 2-cycle and a disjoint 3-cycle $\Rightarrow o(a) = \text{lcm}(2,3) = 6$.

(c) Conj class $\{gag^{-1}\}_{g \in S_5}$

Theorem: $a \in S_5$ the conj class of a contains all elts in S_5 of the same cycle type: all products of disjoint 2 and 3-cycles.

$\binom{5}{2}$ Choose 2 elt $\Rightarrow$ 2-cycle, 3 elts $\Rightarrow$ 3-cycle

$$\#\{gag^{-1}\}_{g \in S_5} = \binom{5}{2} \cdot 2 = \frac{5!}{2!3!} \cdot 2 = \frac{5 \cdot 4}{2} \cdot 2 = \underline{20}$$

$\binom{5}{2}$: choices of 2 elts out of 5

2: cycles (abc) (acb) are different cycles

(d) $H \subset S_5$, $H = \{1, (13), (15), (35), (135), (153)\} \simeq S_3$

$|H| = 6$

(e) $H \subset S_5$ is normal $\Leftrightarrow$ $ghg^{-1} \in H$ $\forall h \in H$ $\forall g \in S_5$

$(12)(13)(12)^{-1} = (23) \notin H \Rightarrow H$ is not normal in S_5.

8. Let E be a Euclidean domain. Recall that a Euclidean domain is an integral domain where the Euclidean division works, in particular if $\gcd(a,b) = 1$ for two elements $a, b \in E$, then there exist elements $x, y \in E$ such that $xa + yb = 1$. For example, the ring of integers $\mathbb{Z}$ is a Euclidean domain.

   (a) Recall that a *unit* in E is an invertible element with respect to the multiplication. Recall that an element $a \in E$ is *irreducible* if $a \neq 0$, a is not a unit and if $a = st$, then either s or t is a unit. Find the units and the irreducible elements in $\mathbb{Z}$.

   (b) Let a, c be irreducible elements in a Euclidean domain E. Suppose that c does not divide a. Show that in this case $\gcd(a, c)$ is a unit. Since gcd is defined up to a multiplication by a unit, this means that $\gcd(a, c) = 1$.

   (c) Let $a, b, c \in E$ be irreducible elements such that c divides ab but c does not divide a. Use (b) to show that then c divides b.

   (d) Use (c) to prove that in a Euclidean domain a factorization of an element into a product of irreducible factors is unique. Namely, if $x = a_1 a_2 \dots a_k = b_1 b_2 \dots b_r$, where all a_i and b_j are irreducible elements of E, then $k = r$ and up to a permutation of terms, $b_i = a_i u_i$, where u_i are units in E.

   (e) We proved in class that $F[X]$, where F is a field, is a Euclidean domain. Use (d) to show that a polynomial of degree n with coefficients in a field can have at most n roots in F.

   (f) Let $K = \mathbb{Z}/9\mathbb{Z}[X]$. Show by an example that the statement in (e) fails in K. Namely, how many distinct roots does the polynomial $f(X) = X^2$ have in $\mathbb{Z}/9\mathbb{Z}$?

   [14 **points**]

(a) Units in $\mathbb{Z}$: $\{\pm 1\}$ invertible wrt $\mathbb{Z}$-mult.

irreducibles: $n = \pm 1 \cdot k \Rightarrow \pm p \in \mathbb{Z}$ are the irreducibles.

(b) Let $d = \gcd(a, c) \Rightarrow a = ds$, $c = dt$ irreducibles $\Rightarrow$ either d or t is a unit. If t is a unit $\Rightarrow d = ct^{-1} \Rightarrow a = ct^{-1}s \Rightarrow c$ divides a. But c does not divide $a \Rightarrow d$ is a unit $\Rightarrow \gcd(a, c) = d$ is a unit.

(c) From (b) $\Rightarrow \gcd(a, c) = 1 \Rightarrow xa + yc = 1 \quad \exists x, y \in E$

$\Rightarrow \underbrace{xab}_{c\,|} + \underbrace{ycb}_{c\,|} = b \Rightarrow c$ divides b.

(d) $x = a_1 a_2 \dots a_k = b_1 b_2 \dots b_r$ where a_i, b_j are irreducibles $\Rightarrow$

a_1 divides $b_1 \dots b_r \Rightarrow a_1$ divides one of them by (c)

Say $b_1 = a_1 u_1$ u_1 is a unit

$\Rightarrow a_2 \dots a_k = u_1 b_2 \dots b_k$, continue with a_2 and so on

$\Rightarrow$ get $k = r$ and $b_i = a_i u_i$ u_i is a unit.

(e) $F[X] = E$ Euclidean division $\downarrow \deg = 0$

If a_1 is a root of $f(x)$ $\Rightarrow f(x) = (x-a_1)d(x) + r(x)$

$0 = f(a_1) = (a_1 - a_1)d(a_1) + r = 0 + r \Rightarrow r = 0$

$\Rightarrow f(x) = (x-a_1)\,d(x)$ $\quad \uparrow \deg = n-1$ continue by induction

$\Rightarrow f(x) = (x-a_1)(x-a_2)\ldots(x-a_n)$ and the factorization is unique up to units

$\Rightarrow f$ has at most n distinct roots for a polynomial of degree n.

(f) $\mathbb{Z}/9\mathbb{Z}[X]$, $f(x) = X^2$ $\quad f(0) = 0$

$f(3) = [9] = [0]$ $\quad$ 3 roots.

$f(6) = [36] = [0]$

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 F_1 and F_2 be two fields. Then $F_1 \times F_2$ is a field.

10. (True/(False)) The ring $\mathbb{Z}/15\mathbb{Z}$ is an integral domain.

11. ((True)/False) The polynomial $6X^5 + 20X^4 + 15X^2 + 25X + 5$ is irreducible in $\mathbb{Q}[X]$. Irreducible by Eisenstein
5✗ 5| 5| 5| 5| 25✓

12. ((True)/False) The symmetric group S_7 contains a subgroup isomorphic to the cyclic group C_{10}.

[4 **points**]

9 $F_1 \times F_2$: $(1,0)\cdot(0,1) = (0,0)$ nontrivial zero divisors

10. $\mathbb{Z}/15\mathbb{Z}$: $3 \cdot 5 = 0$

11. Irreducible by Eisenstein, $p = 5$

12. $(12)(34567) = a$
(2-cycle)×(5-cycle) disjoint => order(a) = 10 => yes