Discrete Mathematics
Assignment 5

Keerti P. Charantimath
19MA20059

1) Since G is a group, an inverse exists for every element in G
Multiply by inverse to a on both sides &
$a^2 = a$

We get $a = i$, where 'i' is the identity element

This holds true for all $a \in G$. Thus G contains only one distinct element i.e 'i'.

∴ G is abelian

3) One can show that the binomial theorem holds in any commutative ring. Thus,

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$$

Note that, for $1 \le i \le p-1$, we have that

$$\frac{p!}{(p-i)!\, i!} = \binom{p}{i} \in \mathbb{Z}$$

i.e., $(p-i)!\, i!$ divides $p!$.

Since $1 \le i \le p-1$ & p is prime, it follows that $(p-i)!\, i!$ is coprime to p. It follows that $(p-i)!\, i!$ divides $(p-1)!$ (Using the fact that if $a, b, c \in \mathbb{Z}$ and a divides bc and $\gcd(a,b) = 1$ then a divides c). Hence, we can write $(p-i)!\, i!\, k_i = (k-1)!$ for some $k_i \in \mathbb{Z}$. Thus, we have

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + \left[\sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i}\right] + y^p$$

$$= x^p + \left[\sum_{i=1}^{p-1} k_i p \cdot x^i y^{p-i}\right] + y^p$$

$$= x^p + y^p$$

since R is a ~~characteristic~~ of characteristic p.

$$\therefore (x+y)^p = x^p + y^p$$

Hence proved.

5) $Z_3[x]/\langle x^3+cx^2+1\rangle$ is a field if and only if the ideal generated by x^3+cx^2+1 is maximal ideal if and only if x^3+cx^2+1 is irreducible in $Z_3[x]$.

Let $f(x) = x^3+cx^2+1$ since $f(x)$ has degree 3, if $f(x)$ is reducible then one of the factor should have degree one i.e. $f(x)$ should have a root in Z_3.

$f(0) = 1 \neq 0 \pmod 3$
$f(1) = 2+c$
$f(2) = 9+c \equiv c \pmod 3$

So if $c \neq 0$ and $c \neq 1$ in Z_3, then $f(x)$ is irreducible. So for $\boxed{c=2}$, $f(x)$ is irreducible.

4) a) $(Z, +, \cdot)$

For Z to be a field, $(Z,+)$ must be abelian & $(Z,\cdot)$ should also be abelian.

But for inverse in $(Z,\cdot)$

Let $a \in Z$ then $a \cdot a^{-1} = e = 1$ (identity element)

$$a^{-1} = \frac{1}{a} \notin Z$$

$\therefore$ for every $a \in Z$, there doesn't exist an a^{-1} that belongs to Z, wrt. $(Z,\cdot)$

$\therefore Z$ is not a field

4) b) $\mathbb{Z}[\sqrt{3}] = \{ a+b\sqrt{3} \mid a, b \in \mathbb{Z} \}$

for $\mathbb{Z}[\sqrt{3}]$ to be a field, for element there must exist an inverse wrt "." (multiplication)

Let $a, b \in \mathbb{Z} \Rightarrow (a+b\sqrt{3}) \cdot (1+0\sqrt{3}) = a+b\sqrt{3}$
multiplicative identity

for $a+b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ $\forall$ $a, b \in \mathbb{Z}$
$\frac{1}{a+b\sqrt{3}}$ must belong to $\mathbb{Z}[\sqrt{3}]$

$$\frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} = \left(\frac{a}{a^2-3b^2}\right) + \left(\frac{-b\sqrt{3}}{a^2-3b^2}\right)$$
$$\downarrow \qquad\qquad \downarrow$$
$$p \qquad\qquad q$$

here,

p, q are not integers always.

$\therefore p-q \notin \mathbb{Z}[\sqrt{3}]$ $\forall a, b$

$\therefore \mathbb{Z}[\sqrt{3}]$ is not a field.

19MA20059

2) a) $A + B = A \Delta B = (A - B) \cup (B - A)$

$A \cdot B = A \cap B$, $A, B \in R$, $R = P(X)$

X is any set

$(P(X), +)$ → should be abelian group

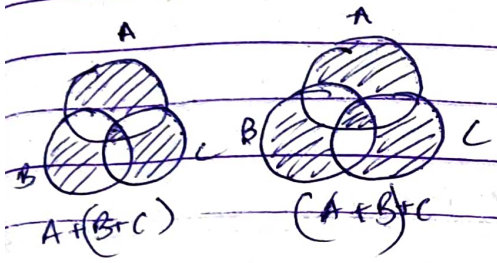
$(P(X), \cdot)$ → " " semi-group

for $(P(X), +)$ ⟹

i) closure :- $A + B = (A - B) \cup (B - A) \in P(X) \quad \forall A, B \in P(X)$

↳ satisfied

ii) Associative :- $A + (B + C) = (A + B) + C$ → to prove



$LHS = A + [(B - C) \cup (C - B)]$

$= [A - [(B - C) \cup (C - B)]] \cup [(B - C) \cup (C - B) - A]$

$RHS = [A - [(B - C) \cup (C - B)]] \cup [(B - C) \cup (C - B) - A]$

↳ satisfied

iii) Identity :- $A + E = A = E + A \Rightarrow E = \phi \in P(X)$

↳ satisfied

iv) Inverse :- $A + A^{-1} = E = \phi$

$(A - A^{-1}) \cup (A^{-1} - A) = \phi$

Both left & Right inverse ← $A^{-1} = A \in P(X) \quad \forall \quad A \in P(X)$

↳ satisfied.

v) Commutative :- $A + B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B + A$

↳ satisfied

$\therefore (P(X), +)$ → abelian group

for $(P(X), \cdot)$

i) closure ⇒ $A \cdot B = A \cap B \in P(X) \quad \forall A, B \in P(X)$

↳ satisfied

ii) Associative ⇒ $(A \cdot B) \cdot C = (A \cap B) \cdot C = A \cap B \cap C = A \cdot (B \cap C)$

$= A \cdot (B \cdot C)$

↳ satisfied.

19MA20059

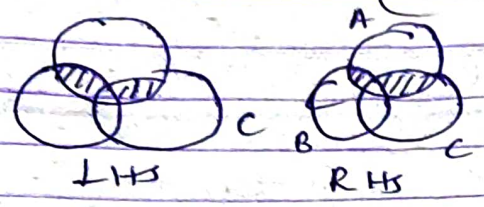
Distributive property

LHS = $A.(B+C) = A \cap [(B-C) \cup (C-B)]$

$= [A \cap (B-C)] \cup [A \cap (C-B)]$

RHS = $A.B + B.C = (A \cap B) + (A \cap C)$

$= (A \cap B - A \cap C) \cup (A \cap C - A \cap B)$



→ satisfied.

∴ $(P(X), \Delta, \cap)$ forms a ring.

b) $A+B = A \cup B, \quad A.B = A \cap B, \quad \forall A, B \in R$

from (a) we know that $A.B = A \cap B$ is a semigroup

now

for $A+B = A \cup B$

i) closure :- $A+B = A \cup B \in P(X) \quad \forall A, B \in P(X)$

↳ satisfied

ii) Associative : $A+(B+C) = A+(B \cup C) = A \cup B \cup C = (A+B) \cup C$

$= (A+B)+C$

↳ satisfied

iii) Identity : $A+E = A \cup E = A = E \cup A \Rightarrow E = \phi \in P(X)$

↳ satisfied

iv) Inverse :- $A+A^{-1} = A \cup A^{-1} = E = \phi$

NOT satisfied

only satisfied when $A = A^{-1} = \phi$

No inverse for other elements of $P(X)$

∴ $(P(X), +)$ is not a group

∴ $(P(X), \cup, \cap)$ does not form a ring

c) $R \rightarrow$ set of all Real valued continuous functions

$(f+g)(x) = f(x)+g(x)$; $(f\cdot g)x = f(g(x))$

$\forall\ f, g \in R$ & $\forall\ x \in \mathbb{R}$

Distributive law

LHS $= (f\cdot(g+h))x = f((g+h)(x)) = f(g(x)+h(x))$

RHS $= ((f\cdot g)+(f\cdot h))(x) = f(g(x)) + f(h(x))$

LHS $\neq$ RHS $\longrightarrow$ Distributive law NOT satisfied

$\therefore$ R is not a ring

d) $R \rightarrow$ set of all twice differentiable real valued functions.

$\& f''(0)=0\ \forall\ f \in R$

$(f+g)(x) = f(x)+g(x)$; $(f\cdot g)(x) = f(x)\cdot g(x)$ $\forall\ f, g \in R$ & $\forall\ x \in \mathbb{R}$

for $(R, \cdot)$ $\rightarrow$ to prove to be semigroup

i) closure property:- $f, g \in R \Rightarrow f''(0) = g''(0) = 0$

$(f\cdot g)(x) = f(x)\cdot g(x)$

$(f\cdot g)'(x) = f'(x)g(x) + g'(x)f(x)$

$(f\cdot g)''(x) = f''(x)g(x) + 2g'(x)f'(x) + g''(x)f(x)$

$(f\cdot g)''(x)\big|_{x=0} = \big[f''(x)g(x) + 2g'(x)f'(x) + g''(x)f(x)\big]_{x=0}$

($f''(x)g(x)$ and $g''(x)f(x)$ vanish at $x=0$)

$(f\cdot g)''(0) = 2f'(0)g'(0)$

If closure property holds, then either $f'(0)=0$ or $g'(0)=0$ which is not always case

Hence, closure property is NOT satisfied

$\therefore$ R is not a ring

6) a) $Z_3[x] / \langle x^3 + 2x + 1 \rangle$

elements are

$0 = 0 = [000]$

$x^0 = 1 = [001]$

$x^1 = x = [010]$

$x^2 = x^2 = [100]$

$x^3 = x + 2 = [012]$

$x^4 = 2x^2 + 2x = [120]$

$x^5 = 2x^2 + x + 2 = [212]$

$x^6 = x^2 + x + 1 = [111]$

$x^7 = x^2 + 2x + 2 = [122]$

$x^8 = 2x^2 + 2 = [202]$

$x^9 = x + 1 = [011]$

$x^{10} = x^2 + x = [110]$

$x^{11} = x^2 + x + 2 = [112]$

$x^{12} = x^2 + 2 = [102]$

$x^{13} = 2 = [002]$

$x^{14} = 2x = [020]$

$x^{15} = 2x^2 = [200]$

$x^{16} = 2x + 1 = [021]$

$x^{17} = 2x^2 + 2x = [210]$

$x^{18} = x^2 + 2x + 1 = [121]$

$x^{19} = 2x^2 + 2x + 2 = [222]$

$x^{20} = 2x^2 + x + 1 = [211]$

$x^{21} = x^2 + 1 = [101]$

$x^{22} = 2x + 2 = [022]$

$x^{23} = 2x^2 + 2x = [220]$

$x^{24} = 2x^2 + 2x + 1 = [221]$

$x^{25} = 2x^2 + 1 = [201]$

$x^{26} = 1 = x^0$

19MA20059

b) $[1\ 2\ 1] = x^2+2x+1 = x^{18}$

$(x^{18})^{-1}\ x^{18} = 1 = x^{26}$

$\rightarrow (x^{18})^{-1} = x^8 = 202 = 2x^2+2$

$(x^{18})^{-1} \Longrightarrow$ inverse of $121 = 2x^2+2 = x^8 = [202]$

square root of $121 = \sqrt{x^2+2x+1} = \sqrt{x^{18}} = x^9 = x+1$

$\therefore$ square root of $[121] = x+1 = x^9 = [0\ 1\ 1]$

c) Quaratic residues of $GF(3^3)$

$x^0 = 1 = [00\ 1]$
$x^2 = x^2 = [1\ 0\ 0]$
$x^4 = x^2+2x = [1\ 2\ 0]$
$x^6 = x^2+x+1 = [1\ 1\ 1]$
$x^8 = 2x^2+2 = [2\ 0\ 2]$
$x^{10} = x^2+x = [1\ 1\ 0]$
$x^{12} = x^2+2 = [1\ 0\ 2]$
$x^{14} = 2x = [0\ 2\ 0]$
$x^{16} = 2x+1 = [0\ 2\ 1]$
$x^{18} = x^2+2x+1 = [1\ 2\ 1]$
$x^{20} = 2x^2+x+1 = [2\ 1\ 1]$
$x^{22} = 2x+2 = [0\ 2\ 2]$
$x^{24} = 2x^2+2x+1 = [2\ 2\ 1]$

19MA20059

7) $Z_2[x] / \langle x^5+x^2+1 \rangle$

a) $(x^4+x^2) \times (x^3+x+1)$

$= (x^7+2x^5+x^4+x^3+x^2) \bmod (x^5+x^2+1)$

$= (x^2(x^5+x^2+1) + 2x^5 + x^3) \bmod (x^5+x^2+1)$

$= 0 + 0x^5 + x^3$ $\quad (2 \bmod 2 = 0)$

$= x^3$

$(x^4+x^2) \times (x^3+x+1) = x^3$

b) Extended Euclidean Algorithm.

$f(x) = x^5+x^2+1$

$g(x) = x^3+x^2$

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

$\gcd(f(x), g(x)) = 1$

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

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

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

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

$(x^3+x^2)^{-1} = x^2-x+1 \Rightarrow x^2+x+1$ $\quad (-1 = 1 \bmod 2)$

$(x^3+x^2)^{-1} = x^2+x+1$

8) $y^2 = x^3+3x \pmod{17}$

a)

x	$x^3+3x \pmod{17}$	in QR(17)	y
0	0	yes	0
1	4	yes	(2,15)
2	14	No	
3	2	yes	(6,11)
4	8	yes	(5,12)
5	4	yes	(2,15)
6	13	yes	(8,9)
7	7	NO	
8	9	yes	(3,14)
9	8	yes	(3,3)
10	10	No	
11	4	yes	(2,15)
12	13	yes	(8,9)
13	9	yes	(3,14)
14	15	yes	(6,11)
15	3	No	
16	13	yes	(8,9)

19MA20059

$E = \{(0,0)(1,2)(1,15)(3,6)(3,11)(4,5)(4,12)(5,2)(5,12)$
$(6,8)(6,9)(8,3)(8,14)(9,5)(9,12)(11,2)(11,13)(12,8)$
$(12,9)(13,3)(13,14)(14,7)(14,10)(16,8)(16,9), O\}$

Total no. of elements in E (order of E) = 26

b) $2(8,14) \Rightarrow (x_1, y_1) = (x_2, y_2) = (8,14)$

$m = \frac{3(x_1^2+1)}{2y_1}$ $\quad x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

$\Rightarrow m = \frac{3(8^2+1)}{2\times 14} = 195(28)^{-1} = 8\times 14 \bmod 17$

$= 112 \bmod 17$

$\boxed{m = 10}$

$x_3 = 10^2 - 8 - 8 = 84 \bmod 17 = 16$

$y_3 = 10(8-16) - 14 = -94 \bmod 17 = 8 \bmod 17 = 8$

$(8,14) + (8,14) = 2(8,14) = (16,8)$

c) from b $\quad 2(8,14) = (16,8)$

$4(8,14) = 2(16,8)$

$m = \frac{3(16^2+1)}{16} = \frac{771}{16} = 6\times 16^{-1} = 6\times 16 \bmod 17 = 96 \bmod 17$

$= 11$

$x_3 = 121 - 16 - 16 = 4, \quad y_3 = 11(16-4) - 8 = 5$

$4(8,14) = (4,5)$

Now $8(8,14) = 2(4,5)$

$m = \frac{3(4^2+1)}{2\times 5} = \frac{3\times 17}{2\times 5} = 0$

$x_3 = -8 = 9, \quad y_3 = -5 = 12$

$8(8,14) = (9,12)$

19MA20059

$16(8,14) = 2(9,12)$

$m = \frac{3(9^2+1)}{2\times 12} = \frac{264}{24} = 8 \times 24^{-1} = 40 \bmod 17 = 6$

$x_3 = 36 - 9 - 9 = 18 = 1 \qquad y_3 = 6(9-1) - 12 = 36 = 2$

$16(8,14) = (1,2)$

$\Rightarrow$ $1(8,14) = (8,14)$, $2(8,14) = (16,8)$, $4(8,14) = (4,5)$
$8(8,14) = (9,12)$, $16(8,14) = (1,2)$

Order of elliptic curve = 26

$\Rightarrow$ Order of $(8,14)$ must be 1, 2, 13, 26

$1 \Rightarrow (8,14) = (8,14)$ — 1 is not the order.

$2 \Rightarrow 2(8,14) = (16,8)$ — 2 " " " "

$13 \Rightarrow 13(8,14) = 8(8,14) + 4(8,14) + (8,14)$
$= (9,12) + (4,5) + (8,14)$
$(x_1, y_1) \quad (x_2, y_2)$

$m = 12-5/9-4 = 7/5 = 7 \cdot 5^{-1} \bmod 17 = 49 \bmod 17 = 15$

$x_3 = 225 - 9 - 4 = 8, \quad y_3 = 15(9-8) - 12 = 3$

$\Rightarrow 13(8,14) = (8,3) + (8,14)$

$\because (8,3) \neq \oplus \Rightarrow -(8,3) = (8,-3) = (8,14)$

if $P = (x_1, y_1) \neq \oplus \Rightarrow -P = (x_1, -y_1)$

$\Rightarrow 13(8,14) = (8,3) - (8,3) = \oplus$

$13(8,14) = \oplus$

$\boxed{ord_E((8,14)) = 13}$