note

$4 \nmid p-3$ then non zero elements of $Z_p[i]$ does not form a group w.r.t multiplication.

$4 \nmid p-3$ then $Z_p[i]$ is not ID

$\Rightarrow Z_p[i]$ has zero divisors

$\Rightarrow a \neq 0, b \neq 0$, but $ab = 0$

Consider $G = Z_p[i] \setminus \{0\}$, $(G, *)$ is not a group

Logic $\exists\ x, y \in Z_p[i]$

but $xy = 0$

but $0 \notin Z_p[i] \setminus \{0\}$

so $Z_p[i] \setminus \{0\}$ does not form a group if $4 \nmid p-3$

Fundamental Table

S.I	order of ring	# non isomorphic Ring
1	1	1 ($Z_1 = \{0\}$)
2	2 (p)	2 — Z_2, $2Z_4$
3	3 (p)	2 — Z_3, $3Z_9$

note If $O(R) \leq 3$ then R is always commutative

4	4 (2^2)	11 — Z_4, $Z_2 \times Z_2$, $GF(2^2)$
5	5	2 — Z_5, Z_{25}
6	6	4 — Z_6, ...
7	7	2 — Z_7, Z_{49}
8	8	52 — Z_8, $Z_3 \times Z_4$, $GF(2^3)$
9	9 (3^2)	11 — Z_9, ...

order p — 2 — Z_p, pZ_{p^2}

order p^2 — 11

$p_1 - 4 - Z_{p_1 p_2}$

Subring Let S be a non empty subset of R. $(S,+,\cdot)$ is subring of $(R,+,\cdot)$ if

(i) $\forall a \in S, \forall b \in S \Rightarrow a-b \in S \Rightarrow (S,+)$ is subgroup of $(R,+)$

(ii) $\forall a \in S, \forall b \in S \Rightarrow a \cdot b \in S$

(OR)

$(S,+,\cdot)$ is itself a ring

Ex. $\exists z \neq \phi$, $z \subseteq Q/R/C$ and $(z,+,\cdot)$ is a ring then $(z,+,\cdot)$ is subring of $(Q,+,\cdot)$, $(R,+,\cdot)$ and $(C,+,\cdot)$

(2) $z[i] \neq \phi$, $z[i] \subset C[i]$

$(z[i],+,\cdot)$ is a ring

$\Rightarrow (z[i],+,\cdot)$ is subring of $(C[i],+,\cdot)$

only $(z[i],+,\cdot)$ is subring of $(Q[i],+,\cdot)$.

Note:

If $(S,+,\cdot)$ is subring of $(R,+,\cdot)$ then $(S,+)$ is subgroup of $(R,+)$ but converse need not be true.

Q $S = \left\{ A = \begin{bmatrix} a & tr(A) \\ tr(A) & b \end{bmatrix} ; a,b \in R \right\}$ is subring of $M_2(R)$??

Subring $\Rightarrow$ subgroup

Let $A_1 = \begin{bmatrix} a_1 & a_1+b_1 \\ a_1+b_1 & b_1 \end{bmatrix} \in S$

$A_2 = \begin{bmatrix} a_2 & a_2+b_2 \\ a_2+b_2 & b_2 \end{bmatrix} \in S$

$A_1 - A_2 = \begin{bmatrix} a_1-a_2 & a_1+b_1-a_2-b_2 \\ a_1+b_1-a_2-b_2 & b_1-b_2 \end{bmatrix} = \begin{bmatrix} a_1-a_2 & tr(A_1-A_2) \\ tr(A_1-A_2) & b_1-b_2 \end{bmatrix}$

$a_1-a_2 \in R$, $b_1-b_2 \in R$

$\therefore A_1 - A_2 \in S$ is subgroup of $M_2(R)$

$A_1A_2 = \begin{bmatrix} a_1a_2+(a_1+b_1)(a_2+b_2) & a_1(a_2+b_2)+b_2(a_1+b_1) \\ a_2(a_1+b_1)+b_1(a_2+b_2) & (a_1+b_1)(a_2+b_2)+b_1b_2 \end{bmatrix}$

$tr(A_1A_2) \neq a_1(a_2+b_2)+b_2(a_1+b_1)$ $\therefore$ (2) fails $\therefore S$ is not subring

Q Show that $S=\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a,b \in R\right\}$ is subring of $M_2(R)$

$A_1=\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} \in S, \quad A_2=\begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix}$

$A_1-A_2=\begin{bmatrix} a_1-a_2 & b_1-b_2 \\ 0 & 0 \end{bmatrix} \in S$ $\quad a_1-a_2 \in R$, $b_1-b_2 \in R$

$\therefore (S,+,\cdot)$ is subgroup of $M_2(R)$

$A_1A_2=\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a_1a_2+0 & a_1b_2+0 \\ 0 & 0 \end{bmatrix} \in S$

$\therefore (S,+,\cdot)$ is subring of $M_2(R)$

Q $S=\left\{\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} ; b \in R\right\}$ is subring of $M_2(R)$

Q $(mZ,+,\cdot)$ is subring of $(Z,+,\cdot)$ (iff) $(mZ,+)$ is subgroup of $(Z,+)$

Pf If $(mZ,+)$ is subgroup of $(Z,+) \Rightarrow (m,Z,+)$ is subgroup of $(Z,+)$.

Converse: $mZ=\{0, \pm m, \pm 2m, \cdots\}$

$=\{ma ; a \in Z\}$