

(1) اعداد حقیقی \mathbb{Q} همواره با دو عمل ضرب و جمع یک میدان است.
 (2) اگر ρ یک عدد اول باشد:

$$\mathbb{Z}_\rho = \{0, 1, \dots, \rho-1\}$$

همچون ضرب معمولی بسته نیست (مثلاً دارد $\frac{1}{2}$ در مجموعه نیست)

$$[0] = \{x \in \mathbb{R} : \rho | x\}$$

اگر $m \in \mathbb{Z}$ و n آنکه m را هم از n در نامم ضرب $(m \sim n)$ اگر $\rho | m-n$

مجموع روی \mathbb{Z}_ρ $[x] + [y] = [x+y]$ $\mathbb{Z}_\rho = \{[0], [1], \dots, [\rho-1]\}$

مثلاً $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ $[3] + [2] = [5] = [0]$

$$[x][y] = [xy]$$

$[1]$ عضو است

$$\begin{array}{r} 5 \\ \times 2 \\ \hline 10 \\ 10 \\ \hline 10 \end{array} \rightarrow [2] = [5]$$

با همانند تقسیم بر ρ

$$[3]^{-1} = [2]$$