１０．ブール環と体

代数２

ブール代数

- **可換律** $A + B = B + A$

  $A * B = B * A$

- **分配律** $A * (B + C) = (A * B) + (A * C)$

  $A + (B * C) = (A + B) * (A + C)$

- **単位元** $\mathrm{A} + 0 = \mathrm{A}$

  $\mathrm{A} * 1 = \mathrm{A}$

- **補元** $A + \bar{A} = 1$

  $A * \bar{A} = 0$

体

・集合Fが2つの演算（加法と乗法）をもち，
（１）Fは加法群であり，
（２）F＊=F－ {0} が乗法において可換群

・（３）分配律

$$a(b+c)=ab+ac$$

行列算

- **可換律は不成立**

$$AB \neq BA$$

- **零因子が存在**

$$AB = O \quad (A \neq O, B \neq O)$$

- **簡約律は不成立**

$$AC = BC, C \neq O$$

$A = B$とは限らない

法p(素数)の剰余類

$$Z_p = \{0,1,2,\cdots, p-1\} (\mathrm{mod}\ p)$$

- 体となる　剰余体
- 例p=5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

既約剰余類

・素数ではないときに、既約な要素だけを抽出した集合について考える

$$Z_m = \{1,2,\cdots,m-1\} \pmod m$$

$$Z_m^{\times} = \{1,\cdots,m-1\} \pmod m$$

・例　m=6のとき $Z_6^{\times} = \{\overline{1},\overline{5}\}$

・例　m=8のとき $Z_8^{\times} = \{\overline{1},\overline{3},\overline{5},\overline{7}\}$