# 数学序論に対する追加説明 $\sharp 9$

- 演習問題 4.8, 4.9 について $a^{m+n} = a^m a^n$ のみを解説する。

  数学的帰納法は，使ってよい事と使ってはいけない事を区別することが大切である。

  使っていけないのは「証明すべき命題」である。当たり前の様に思えるが，うっかりすると使ってしまう場合がある。

- 使ってよいのは
  - 定義
  - すでに証明された事
  - 帰納法の仮定

  である。

- 演習問題 4.8 を解くために必要な定義はべき乗の定義である。

$$a^1 = a$$
$$a^{k+1} = a^k \cdot a \qquad (k \in \mathbb{N})$$

- 演習問題 4.8 を示すためには，次の命題を $P(n)$ とするとき，すべての $n \in \mathbb{N}$ に対し $P(n)$ を示せばよい。

$$P(n) \ : \ \forall m \in \mathbb{N} \quad a^{m+n} = a^m a^n$$

- 最初に $P(1)$ の成立を示す。

$$\begin{aligned} a^{m+1} &= a^m \cdot a && (\text{定義}) \\ &= a^m a^1 && (\text{定義}) \end{aligned}$$

- 次に $P(k)$ の成立を仮定して $P(k+1)$ の成立を示す。$P(k)$ 即ち $a^{m+k} = a^m a^k$ は帰納法の仮定だから使用してよい (というか，帰納法の仮定を使用しないで，帰納法で示すことはできない) 。

$$\begin{aligned} a^{m+(k+1)} &= a^{(m+k)+1} && (\text{和の結合法則}) \\ &= a^{m+k} \cdot a && (\text{定義}) \end{aligned}$$

$$
\begin{aligned}
&= \left(a^m a^k\right) \cdot a && \text{(帰納法の仮定)} \\
&= a^m \left(a^k \cdot a\right) && \text{(積の結合法則)} \\
&= a^m a^{k+1} && \text{(定義)}
\end{aligned}
$$

- 次に 4.9 を考える。証明すべきことは

  $$\boxed{\forall m, n \in \mathbb{Z} \quad a^{m+n} = a^m a^n}$$

  である。

- 整数のべき乗の定義は

  $$
  \begin{aligned}
  a^0 &= 1 \\
  a^{-1} &= \frac{1}{a} \\
  a^n &= \left(a^{-1}\right)^p && (n = -p, p \in \mathbb{N})
  \end{aligned}
  $$

  である。

- 最初に

  $$\forall n \in \mathbb{Z} \quad a^{n+1} = a^n \cdot a$$

  を示す。

  $n \in \mathbb{N}$ のときは定義そのものである。$n = 0$ のときは

  $$
  \begin{aligned}
  a^{0+1} = a^1 = a = 1 \cdot a && \text{(定義)} \\
  = a^0 \cdot a && \text{(定義)}
  \end{aligned}
  $$

  となり成立している。$n = -1$ のときは

  $$
  \begin{aligned}
  a^{-1+1} = a^0 = 1 && \text{(定義)} \\
  = a^{-1} \cdot a && \text{(定義)}
  \end{aligned}
  $$

  より成立する。$n < -1$ のとき $n = -p$ とおくと，$p$ および $p - 1$ は自然数である。

  $$
  \begin{aligned}
  a^{n+1} = a^{-p+1} = a^{-(p-1)} = \left(a^{-1}\right)^{p-1} && \text{(定義)} \\
  = \left(a^{-1}\right)^{p-1} \cdot 1 = \left(a^{-1}\right)^{p-1} \cdot \left(a^{-1} \cdot a\right) && \text{(定義)}
  \end{aligned}
  $$

$$= \left(\left(a^{-1}\right)^{p-1} \cdot a^{-1}\right) \cdot a \qquad \text{(結合法則)}$$

$$= \left(a^{-1}\right)^{(p-1)+1} \cdot a = \left(a^{-1}\right)^{p} \cdot a \qquad \text{(定義)}$$

$$= a^{-p} \cdot a = a^{n} \cdot a \qquad \text{(定義)}$$

よって証明された。

- 証明された式は任意の整数で成立するので，$n$ を $n-1$ に置き換えれば，任意の整数 $n$ に対し

  $$a^{n-1+1} = a^{n-1} \cdot a$$

  が成立している。これを移項して

  $$a^{n} \cdot \left(a^{-1}\right) = a^{n-1}$$

  を得る。

- 数学的帰納法で証明する。そのために

  $$Q(n) \quad : \quad \forall m \in \mathbb{Z} \quad a^{m+n} = a^{m}a^{n}$$

  とする。

- 最初に $n \geqq 0$ のとき帰納法で証明する。

  $n = 0$ のとき

  $$a^{m+0} = a^{m} = a^{m} \cdot 1 = a^{m} \cdot a^{0} \qquad \text{(定義)}$$

  より $Q(0)$ は成立する。

  $Q(k)$ の成立を仮定する。

  $$\begin{aligned} a^{m+(k+1)} &= a^{(m+k)+1} && \text{(結合法則)} \\ &= a^{m+k} \cdot a && \text{(証明済)} \\ &= \left(a^{m} \cdot a^{k}\right) \cdot a && \text{(帰納法の仮定)} \\ &= a^{m} \cdot \left(a^{k} \cdot a\right) && \text{(結合法則)} \\ &= a^{m}a^{k+1} && \text{(定義)} \end{aligned}$$

  $Q(k+1)$ が成立するので 0 以上の整数 $n$ に対し $Q(n)$ が成立する。

- $n$ が負のときは $n=-p$ とおく。

$$R(p) \quad : \quad \forall m \in \mathbb{Z} \quad a^{m+(-p)} = a^m \cdot a^{-p}$$

とし，$p$ に関する帰納法で証明する。

- $p=0$ のときは成立している。$p=k$ のとき成立を仮定する。

$$\begin{aligned}
a^{m+(-(k+1))} &= a^{(m-k)-1} = a^{m-k} \cdot a^{-1} && \text{(証明済)} \\
&= \left(a^m \cdot a^{-k}\right) \cdot a^{-1} && \text{(帰納法の仮定)} \\
&= a^m \cdot \left(a^{-k} \cdot a^{-1}\right) && \text{(結合法則)} \\
&= a^m \cdot \left(\left(a^{-1}\right)^k \cdot a^{-1}\right) && \text{(定義)} \\
&= a^m \cdot \left(a^{-1}\right)^{k+1} && \text{(定義)} \\
&= a^m \cdot a^{-(k+1)} && \text{(定義)}
\end{aligned}$$

$R(k+1)$ が成立するので，0 以上の自然数 $p$ に対し $R(p)$ が成立する。