L4 - 14/08/2024

Multiplication

1. $0 \times m := 0$
2. $(n{+}{+}) \times m := (n \times m) + m$

To prove that multiplication is commutative, we first need to prove the following 2 lemmas.

1. $m \times 0 = 0$
2. $n \times (m{+}{+}) = (n \times m) + n$

Q. PT. $m \times 0 = 0$

Pf - Let $P(m)$ be true if $m \times 0 = 0$.

BC - $0 \times 0 = 0$ ($\because 0 \times m = 0$ by def^n)

$\therefore P(0)$ is true

IH - Given $m \times 0 = 0$, PT $(m++) \times 0 = 0$

$$
\begin{aligned}
(m++) \times 0 &= (m \times 0) + 0 \quad (\text{Def}^n) \\
&= 0 + 0 \quad (\text{Given } m \times 0 = 0) \\
&= 0
\end{aligned}
$$

$\therefore P(m)$ is true $\Rightarrow P(m++)$ is true

$\therefore$ By PMI, $P(m)$ is true for all natural nos. m. $\square$

Q PT $n \times (m{+}{+}) = (n \times m) + n$

Pf - Fix a natural no. m.

Let $P(n)$ be true if

$$n \times (m{+}{+}) = (n \times m) + n$$

BC - $0 \times (m{+}{+}) = 0 = (0 \times m) + 0$

$\therefore$ $P(0)$ is true.

IH - Given $n \times (m{+}{+}) = (n \times m) + n$,

PT $(n{+}{+}) \times (m{+}{+}) = ((n{+}{+}) \times m) + (n{+}{+})$

$$\begin{aligned}
(n{+}{+}) \times (m{+}{+}) &= (n \times (m{+}{+})) + (m{+}{+}) \\
&= (n \times m) + n + (m{+}{+}) \\
&= (n \times m) + ((n+m){+}{+}) \\
&= (n \times m) + ((n{+}{+}) + m) \\
&= ((n \times m) + m) + (n{+}{+}) \\
&= ((n{+}{+}) \times m) + (n{+}{+})
\end{aligned}$$

$\therefore$ $P(n)$ is true $\Rightarrow$ $P(n{+}{+})$ is true

$\therefore$ By PMI, $P(n)$ is true for all natural nos. n $\square$

Commutativity

$$(m \times n) = (n \times m)$$

Pf - Fix a natural no. m.

Let $P(n)$ be true if

$$(m \times n) = (n \times m)$$

BC - $m \times 0 = 0 = 0 \times m$

$\therefore$ $P(0)$ is true

IH - Given $m \times n = n \times m$,

PT $m \times (n{+}{+}) = (n{+}{+}) \times m$

$$\begin{aligned} m \times (n{+}{+}) &= (m \times n) + m \\ &= (n \times m) + m \\ &= (n{+}{+}) \times m \end{aligned}$$

$\therefore$ $P(n)$ is true $\Rightarrow$ $P(n{+}{+})$ is true

$\therefore$ By PMI, $P(n)$ is true for all natural nos. n. $\square$

Q. PT if n, m are positive, then $(n \times m)$ is also positive

Pf – $\because$ n, m are positive

$\therefore$ $\exists$ natural nos. p, q s.t

$$n = (p{+}{+})$$
$$m = (q{+}{+})$$

Now,
$$\begin{aligned} n \times m &= (p{+}{+}) \times (q{+}{+}) \\ &= (p \times (q{+}{+})) + (q{+}{+}) \\ &= (p \times (q{+}{+}) + q){+}{+} \\ &\neq 0 \quad \text{(By Axiom 3)} \end{aligned}$$

$\therefore$ $(n \times m)$ is positive $\square$

Associativity

$$(a\times b)\times c = a\times(b\times c)$$

Pf - Fix natural nos. a & c.
Let $P(b)$ be true if

$$(a\times b)\times c = a\times(b\times c)$$

BC - $(a\times 0)\times c = 0 = a\times(0\times c)$

$\therefore$ $P(0)$ is true.

IH - Given $(a\times b)\times c = a\times(b\times c)$,
PT $(a\times(b{+}{+}))\times c = a\times((b{+}{+})\times c)$

$$\begin{aligned}(a\times(b{+}{+}))\times c &= ((a\times b)+a)\times c\\ &= (a\times b)\times c + ac\\ &= a\times(b\times c) + ac\\ &= a\times((b\times c)+c)\\ &= a\times((b{+}{+})\times c)\end{aligned}$$

$\therefore$ $P(b)$ is true $\Rightarrow$ $P(b{+}{+})$ is true

$\therefore$ By PMI, $P(b)$ is true for all natural nos. b $\square$

Euclidean Algorithm

Let n be a natural no. & q be a positive no.

Then $\exists$ natural nos. m, r s.t $0 \leq r < q$ & $n = mq + r$

Pf - Fix a natural no. q.

Let $P(n)$ be true if $\exists$ natural nos. m, r s.t $0 \leq r < q$ & $n = mq + r$

BC - $0 = 0 \times q + 0 \Rightarrow m = 0$ & $r = 0$

$\therefore P(0)$ is true

IH - Given $\exists$ natural nos. m, r s.t $0 \leq r < q$ & $n = mq + r$

PT $\exists$ natural nos. m', r' s.t $0 \leq r' < q$ & $(n{+}{+}) = m'q + r'$

Now, $(n{+}{+}) = n+1 = mq + (r+1)$

CI - If $0 \le r < (q-1) \Rightarrow (r+1) < q$

$\therefore \quad m' = m \;\&\; r' = (r+1) = (r{+}{+})$

CII - If $r = (q-1) \Rightarrow (r+1) = q$

$\Rightarrow \quad (n{+}{+}) = mq + q = (m+1)q$

$\therefore \quad m' = m+1 = m{+}{+} \;\&\; r' = 0$

$\therefore$ $P(n)$ is true $\Rightarrow$ $P(n{+}{+})$ is true

$\therefore$ By PMI, $P(n)$ is true for all natural nos. n.

NOTE - For given n & q, m & r are unique.

Pf - Let $\exists$ natural nos. m_1, m_2, r_1, r_2;

s.t $0 \leq r_1, r_2 < q$, $m_1 \neq m_2$ & $r_1 \neq r_2$.

$$n = m_1 q + r_1 = m_2 q + r_2$$

By trichotomy of order on natural nos.,

$m_1 > m_2$ or $m_1 < m_2$.

WLOG, let $m_1 > m_2 \Rightarrow \exists$ natural no. M

s.t $m_1 = M + m_2$

$$\Rightarrow \quad m_1 q + r_1 = m_2 q + r_2$$

$$\Rightarrow \quad m_2 q + (Mq + r_1) = m_2 q + r_2$$

$$\Rightarrow \quad Mq + r_1 = r_2$$

which is a contd^n $\because$ $0 \leq r_2 < q$

while $Mq \leq Mq + r_1 < (M+1)q$

Hence $m_1 = m_2$

$\Rightarrow r_1 = r_2$

$\square$