韓國數學敎育學會誌〈數學敎育〉
1978. 6. Vol. XVI. No. 2

Journal of the Korea Society of Mathematical Education
Jun. 1978. Vol. XVI. No. 2

정수의 곱셈에 관하여

明知專門 姜 信 德

이 論文에서는 整數 전체의 集合 **Z** 에서의 덧셈과 곱셈을 엄밀하게 定義할 수 있으며, 그의 성질들을 증명할 수 있고, **Z** 에서의 보통 意味의 덧셈과 곱셈이 合理的임을 보이고자 한다.

§1. 可換群(**Z**, +)

임의의 自然數 a 에 대하여

a^α : 順序雙 (a+h, h) (h∈**N**) 전체로 이루어진 類

a^β : 順序雙 (a, a+h) (h∈**N**) 전체로 이루어진 類

$o^{\alpha\beta}$: 順序雙 (h, h) (h∈**N**) 전체로 이루어진 類라고

定義하며, a^α, a^β, $o^{\alpha\beta}$ 들을 整數라 부르고, 이들 전체의 集合을 **Z** 과 표시한다.

그리고, (a, b)로 결정되는 類+(c, d)로 결정되는 類=(a+c, b+d)로 결정되는 類로 定義하면 **Z** 는 可換群이다.

그리고, 關係 R 을 다음과 같이 定義하면,

$$a^\alpha R b^\alpha \Longleftrightarrow a \leqq b$$

$$a^\beta R b^\beta \Longleftrightarrow b \leqq a$$

$$a^\beta R o^{\alpha\beta},\quad o^{\alpha\beta} R b^\alpha,\quad a^\beta R b^\alpha$$

이 關係 R 은 덧셈과 兩立할 수 있는 順序關係이며, 全順序이다.

또한, ${}_X R'_Y \Longleftrightarrow {}_Y R_X$ 로 定義되는 逆順序 R′ 도 마찬가지이다.

$$a^\alpha \longrightarrow a^\beta,\quad a^\beta \longrightarrow a^\alpha \ (a>o)\quad o^{\alpha\beta} \longrightarrow o^{\alpha\beta}$$

로 定義되는 **Z** 에서 **Z** 위로의 寫像은 順序群 (**Z**, +, R)에서 順序群(**Z**, +, R′)로의 同型寫像이다.

여기서 順序 R 을 선택하는 것은 集合 $\mathbf{Z}^\alpha = \{o^{\alpha\beta}, 1^\alpha, 2^\alpha, \cdots\}$ 을 **N** 과 同一視하는 것과 같고 順序 R′ 을 선택하는 것은 集合 $\mathbf{Z}^\beta = \{o^{\alpha\beta}, 1^\beta, 2^\beta, \cdots\}$ 을 **N** 과 同一視하는 것과 같다.

N 은 **Z** 위에서 作用한다.

임의의 自然數 n∈**N**(n≒o)과 임의의 整數 x∈**Z** 에 대해

$$n*x = x+x+\cdots+x \quad (x \text{ 가 } n \text{ 개})$$

$$o*x = o^{\alpha\beta}$$

라 놓으면

$$n*(x+y) = (n*x)+(n*y)$$

임을 증명할 수 있다.

즉, 寫像 $f_n : x \longrightarrow n*x$ 는 群(**Z**, +) 위에서의 自己準同型寫像이다. 이 自己準同型寫像은 順序를 保存한다.

즉, $xRy \Longrightarrow n_* x R n_* y$

더우기, 임의의 自然數 m, n∈**N** 에 대하여

$$(m+n)*x = (m*x)+(n*x)$$

이다. 즉 $f_n + f_m = f_{n+m}$ 이다.

§2. (**Z**, +) 위의 環의 構造

(**Z**, +, ×)이 環이 되도록 **Z** 위에 곱셈 ×을 定義해 보자.

$$^\forall x \in \mathbf{Z},\quad ^\forall y \in \mathbf{Z},$$

$$(x \times o^{\alpha\beta}) + (x \times y) = x \times (o^{\alpha\beta} + y) = x \times y$$

이므로 $x \times o^{\alpha\beta} = o^{\alpha\beta}$ 이어야 한다.

마찬가지로, $^\forall x \in \mathbf{Z}$, $o^{\alpha\beta} \times x = o^{\alpha\beta}$ 이어야 한

다.

따라서 配分法則에 의해 $1^\alpha\times1^\alpha$, $1^\beta\times1^\beta$, $1^\beta\times1^\alpha$, $1^\beta\times1^\beta$의 곱셈 結果가 결정되면 임의의 두 整數의 곱을 계산할 수 있다. 예를 들면,

$2^\alpha\times3^\beta=(1^\alpha+1^\alpha)\times(1^\beta+1^\beta+1^\beta)=6*(1^\alpha\times1^\beta)$

그래서 $1^\alpha\times1^\alpha=u$라 놓으면

$$(1^\alpha\times1^\beta)+(1^\alpha\times1^\alpha)=1^\alpha\times(1^\beta+1^\alpha)$$
$$=1^\alpha\times0^{\alpha\beta}=0^{\alpha\beta}$$

그러므로 $1^\alpha\times1^\beta=-u$

마찬가지로 $1^\beta\times1^\alpha=-u$ 그리고 $1^\beta\times1^\beta=u$이다. 그러므로 $1^\alpha\times1^\alpha=u$의 값에 의하여 **Z**에서의 곱셈은 완전히 정의된다.

(1) $1^\alpha\times1^\alpha=0^{\alpha\beta}$인 경우

$$^\forall x\in\mathbf{Z},\ ^\forall y\in\mathbf{Z},\ x\times y=0^{\alpha\beta}$$

(2) $1^\alpha\times1^\alpha=k^\alpha$ $(k\in\mathbf{N},\ k\neq0)$인 경우

Z에서의 곱셈은 다음과 같이 定義된다.

$$a^\alpha\times b^\alpha=(kab)^\alpha \qquad a^\beta\times b^\beta=(kab)^\alpha$$
$$a^\alpha\times b^\beta=(kab)^\beta \qquad a^\beta\times b^\alpha=(kab)^\beta$$

이 때, 이와 같은 덧셈과 곱셈에 관하여 **Z**가 環을 이룸을 알 수 있다. 더우기 이 環은 可換環임을 증명할 수 있다.

(3) $1^\alpha\times1^\alpha=k^\beta$ $(k\in\mathbf{N},\ k\neq0)$인 경우

Z에서의 곱셈은 다음과 같이 定義된다.

$$a^\beta\times'b^\alpha=(kab)^\beta \qquad a^\alpha\times'b^\alpha=(kab)^\beta$$
$$a^\beta\times'b^\beta=(kab)^\alpha \qquad a^\alpha\times'b^\beta=(kab)^\alpha$$

이 때에도, 이와 같은 덧셈과 곱셈에 관하여 **Z**가 環을 이루며, 可換環임을 증명할 수 있다.

이 環에는 單位元(곱셈에 관한 恒等元)이 存在하는가를 알아보자.

(1)의 경우

존재하지 않는다.

(2)의 경우

a^α가 곱셈에 관한 恒等元이라면

$$a^\alpha\times a^\alpha=a^\alpha$$

따라서, 곱셈 정의에 의하여

$$(ka^2)^\alpha=a^\alpha$$

즉 $ka^2=a$

그런데 $a\neq0$, $k\neq0$이므로 $k=1$, $a=1$

즉 $1^\alpha\times1^\alpha=1^\alpha$일 때에만 **Z**는 恒等元을 갖고 그 恒等元은 1^α이다. 따라서 **Z**위의 곱셈은 다음과 같이 定義된다.

$$a^\alpha\times b^\alpha=(ab)^\alpha=a^\beta\times b^\beta$$
$$a^\alpha\times b^\beta=(ab)^\beta=a^\beta\times b^\alpha$$
$$^\forall x\in\mathbf{Z},\ x\times0^{\alpha\beta}=0^{\alpha\beta}\times x=0^{\alpha\beta}$$

(3)의 경우

a^β가 곱셈에 관한 恒等元이라면

$$a^\beta\times'a^\beta=a^\beta$$

따라서 곱셈 정의에 의하여

$$(ka^2)^\beta=a^\beta$$

즉 $ka^2=a$

그런데 $a\neq0$, $k\neq0$이므로 $k=1$, $a=1$

즉 $1^\beta\times'1^\beta=1^\beta$일 때에만 **Z**는 恒等元을 갖고 그 恒等元은 1^β이다. 따라서 **Z**위의 곱셈은 다음과 같이 定義된다.

$$a^\beta\times'b^\beta=(ab)^\beta=a^\alpha\times'b^\alpha$$
$$a^\beta\times'b^\alpha=(ab)^\alpha=a^\alpha\times'b^\beta$$
$$^\forall x\in\mathbf{Z},\ x\times'0^{\alpha\beta}=0^{\alpha\beta}\times'x=0^{\alpha\beta}$$

그러므로 **Z**위에는 두 가지 방법으로 單位元을 갖는 可換環의 構造를 줄 수 있다.

可換環 $(\mathbf{Z},+,\times)$는 다음과 같은 모든 順序關係 R에 관한 順序環이다.

$$\left.\begin{matrix}0^{\alpha\beta}Rx\\0^{\alpha\beta}Ry\end{matrix}\right\}\Longrightarrow 0^{\alpha\beta}R(x_\times y)$$

또 可換環$(\mathbf{Z},\ +,\times')$는 다음과 같은 모든 順序關係 R'에 관한 順序環이다.

$$\left.\begin{matrix}0^{\alpha\beta}R'x\\0^{\alpha\beta}R'y\end{matrix}\right\}\Longrightarrow 0^{\alpha\beta}R'(x_\times y)$$

따라서 다음 命題들은 서로 同値이다.

i) 두 集合 $\mathbf{Z}^\alpha$, $\mathbf{Z}^\beta$중 어느 하나를 선택하여 **N**과 同一視하는것.

ii) 順序關係 R, R'중 어느 하나를 선택하는 것.

iii) 곱셈 演算 $\times$, $\times'$중 어느 하나를 선택하는 것.

이 선택이 이루어지면 기호 α와 β는 本質的으로 같은 役割을 한다. 그러므로 單位元과 같은 기호를 갖는 元素들을 양의 整數라 하고 그와 반대 기호를 갖는 元素들을 음의 整數라

定義하여도 좋다.

§3. $(\mathbf{Z}, +)$의 自己準同型環

덧셈群 $\mathbf{Z}$의 한 自己準同型寫像 f는 $f(1^\alpha)=v$에 의하여 완전히 결정된다.

실제로

$f(1^\alpha)=k^\alpha$라 하면,

$f(a^\alpha)=(ka)^\alpha$이고 $f(a^\beta)=(ka)^\beta$

$f(1^\alpha)=k^\beta$라 하면,

$f(a^\alpha)=(ka)^\beta$이고 $f(a^\beta)=(ka)^\alpha$

$f(1^\alpha)=0^{\alpha\beta}$라 하면,

$^\forall x\in\mathbf{Z},\quad f(x)=0^{\alpha\beta}$

또한 $f_n: x\longrightarrow n*x$인 順序를 保存하는 自己準同寫像 f_n(§1의 끝부분에서 定義된 것)에 대응하여 $f_{n'}: x\longrightarrow -(n*x)$인 自己準同型寫像을 생각할 수 있다.

두 自己準同型寫像의 합은 自己準同型이고, 또 寫像 $n^\alpha\longrightarrow f_n$, $n^\beta\longrightarrow f_n'$, $0^{\alpha\beta}\longrightarrow f_0$은 $(\mathbf{Z}, +)$으로부터 $(\mathbf{Z}, +)$의 自己準同型環 $\mathcal{E}$ 위로의 同型寫像이다.

$\mathcal{E}$의 元素를 $\mathbf{Z}$의 元素와 同一視할 수 있고 양의 整數와 음의 整數를 구별할 수 있다. 따라서, $(\mathbf{Z}, +)$와 同型인 群을 도입하여 그 元素들을 $\cdots, 2^-, 1^-, 0^{+-}, 1^+, 2^+, \cdots$으로 표시하자.

$f_{n+}: x\longrightarrow n\times x$

$f_{n-}: \longrightarrow -(n\times x)$로 놓고

$\mathbf{Z}$에서의 곱셈을

$a^+\times b^-=a^-\times b^+=(ab)^+$

$a^+\times b^-=a^-\times b^+=(ab)$

로 定義하면 自己準同型寫像의 合成은 $f_x\circ f_y=f_{xy}$로 됨을 증명할 수 있다. 그러므로 덧셈群 $(\mathbf{Z}, +)$의 自己準同型寫像 전체의 集合 $\mathcal{E}$는 $(\mathbf{Z}, +, \times)$에 同型인 環을이룬다.