代数学 暫定版

@k74226197Y126

2023 年 1 月 8 日

はじめに

この PDF 資料はあくまでも一学生が勉強のため作成したものですので、間違いや不適切な表現、紛らわしい表現があるかもしれません。したがって、あまり信用しないようにしていただければ幸いです。また、もし、そのようなものがございましたら、Twitter の「えのきたけ (@k74226197Y126)」まで DM などでご連絡していただければ幸いです。

この PDF 資料はまだ書きかけです。今後の予定としては、主に群論、表現論、homology 論の拡充を考えております。また、整数環 $\mathbb{Z}$ に関するより詳しい内容や体論、Galois 理論の拡充は余裕がないため、当面の間ないかと思われます。何卒ご了承のほどよろしくお願いいたします。

目次

第 1 部　群論

ここでは、群という集合に算法を入れた代数学的な構造について議論する。まず、群を導入し剰余類、正規部分群、Lagrange の定理をみて、群準同型写像というものを導入し群同型定理を示す。そのあと、共役類や作用、直積、Sylow の定理を目標とする。

1.1　群

1.1.1　群

公理 1.1.1 (群の公理)**.** 空集合でない集合 G に対し算法 $*: G \times G \to G; (a,b) \mapsto a*b$ が与えられたとする。このとき、次の条件たちを満たす集合 G と算法 $*$ を合わせて群といい、集合 G は算法 $*$ に対し群をなすといい、$(G,*)$ と書く。そのような集合 G の元の個数が有限なら、その群 $(G,*)$ は有限群といい、その集合の濃度 $\#G$ をその群 $(G,*)$ の位数といい、$o(G,*)$ と書く。逆に、その集合 G の元の個数が無限ならば、その群 $(G,*)$ は無限群という。単位元 $1_{(G,*)}$ のみからなる群 $\left(\left\{1_{(G,*)}\right\},*\right)$ を単位群という[*1]。

- 算法 $*$ について結合的である、即ち、$\forall a,b,c \in G$ に対し、$(a*b)*c = a*(b*c)$ が成り立つ。
- $\exists b \in G \forall a \in G$ に対し、$a*b = b*a = a$ が成り立つ。この元 b をその群 $(G,*)$ の単位元といい $1_{(G,*)}$ などと書く。
- $\forall a \in G \exists b \in G$ に対し、$a*b = b*a = 1_{(G,*)}$ が成り立つ。この元 b を a の逆元といい、a^{-1} と書く。

さらに次の条件も満たす群 $(G,*)$ を特に可換群、Abel 群という。

- 算法 $*$ は可換的である、即ち、$\forall a,b \in G$ に対し、$a*b = b*a$ が成り立つ。

なお、$a*b = b*a$ が成り立つような元々 a、b は可換であるという。

定理 1.1.1. 群 $(G,*)$ について、その単位元 $1_{(G,*)}$、その集合 G の任意の元 a の逆元 a^{-1} は一意的に存在する。

これはいずれも背理法によって示される。

証明. 群 $(G,*)$ において、$\forall a \in G$ に対し、$a*1_{(G,*)} = 1_{(G,*)}*a = a$ なるその集合 G の元 $1_{(G,*)}$ とは異なる、$\forall a \in G$ に対し、$a*e = e*a = a$ なる元 e がその集合 G に存在するとする。このとき、$1_{(G,*)}*e = 1_{(G,*)}$ かつ $1_{(G,*)}*e = e$ が成り立つので、$1_{(G,*)} = e$ が成り立つこととなり、仮定に矛盾する。よって、$\forall a \in G$ に対し、$a*1_{(G,*)} = 1_{(G,*)}*a = a$ が成り立つようなその単位元 $1_{(G,*)}$ は一意的に存在する。

同様に、$\forall a \in G$ に対し、$a*a^{-1} = a^{-1}*a = 1_{(G,*)}$ なるその集合 G の元 a^{-1} とは異なる $a*b = b*a = 1_{(G,*)}$ なる元 b がその集合 G に存在するとする。このとき、次のようになり、

$$a^{-1} = a^{-1} * 1_{(G,*)}$$

[*1] 余談ですが、集合 G の 1 つの部分集合を S、n つの部分集合たちのうち 1 つを S_i、これの元の 1 つを s_i とおき、写像 $f: \prod_i S_i \to S; (s_i)_i \mapsto f((s_i)_i)$ を考えるとき、紛らわしいことに集合 $\left\{f((s_i)_i) \middle| \forall i\,[s_i \in S_i]\right\}$ を $f(S_i)_i$ と表記することがあります…。例えば、$S_1 * S_2$、$a * S_1$ などといった感じに。

$$
\begin{aligned}
&= a^{-1} * (a * b) \\
&= \left(a^{-1} * a\right) * b \\
&= 1_{(G,*)} * b = b
\end{aligned}
$$

仮定に矛盾する。よって、$\forall a \in G$ に対し、$a * a^{-1} = a^{-1} * a = 1_{(G,*)}$ となる元 a^{-1} が一意的に存在する。 □

定理 1.1.2 (簡易律)**.** 群 $(G, *)$ において、$\forall a, u, v \in G$ に対し、次のことが成り立つ。

- $a * u = a * v$ が成り立つなら、$u = v$ が成り立つ。
- $u * a = v * a$ が成り立つなら、$u = v$ が成り立つ。

この性質を簡易律という。

証明. 群 $(G, *)$ が与えられたとする。$\forall a, u, v \in G$ に対し、$a * u = a * v$ が成り立つなら、次式が成り立つかつ、

$$
\begin{aligned}
a^{-1} * (a * u) &= \left(a^{-1} * a\right) * u \\
&= 1_{(G,*)} * u = u
\end{aligned}
$$

次式が成り立つので、

$$
\begin{aligned}
a^{-1} * (a * u) &= a^{-1} * (a * v) \\
&= \left(a^{-1} * a\right) * v \\
&= 1_{(G,*)} * v = v
\end{aligned}
$$

$u = v$ が得られる。

同様にして、$u * a = v * a$ が成り立つなら、$u = v$ が成り立つことが示される。 □

定理 1.1.3. 群 $(G, *)$ について、$\forall a, b \in G$ に対し、$(a * b)^{-1} = b^{-1} * a^{-1}$ が成り立つ。

証明. 群 $(G, *)$ が与えられたとする。$\forall a, b \in G$ に対し、$(a * b) * (a * b)^{-1} = 1_{(G,*)}$ が成り立つかつ、次式が成り立つので、

$$
\begin{aligned}
(a * b) * \left(b^{-1} * a^{-1}\right) &= \left(a * \left(b * b^{-1}\right)\right) * a^{-1} \\
&= (a * e) * a^{-1} \\
&= a * a^{-1} = 1_{(G,*)}
\end{aligned}
$$

$(a * b) * (a * b)^{-1} = (a * b) * \left(b^{-1} * a^{-1}\right)$ が得られ、したがって、簡易律により $(a * b)^{-1} = b^{-1} * a^{-1}$ が成り立つ。 □

定義 1.1.2. 群 $(G, *)$ をなす集合 G の元 a について $m, n \in \mathbb{Z}$ に対し次式のように記法を定める。

$$
\begin{aligned}
a^m * a^n &= a^{m+n} \\
(a^m)^n &= a^{mn} \\
(a * b)^n &= a^n * b^n \text{ if } a * b = b * a
\end{aligned}
$$

定理 1.1.4. 群 $(G, *)$ について、$\forall a \in G \forall n \in \mathbb{N}$ に対し、次式たちが成り立つ。

$$
a^0 = 1_{(G,*)}, \quad a^1 = a, \quad a^{n+1} = a^n * a, \quad 1_{(G,*)}^{-n} = 1_{(G,*)}^n = 1_{(G,*)}, \quad a^{-n} = \left(a^{-1}\right)^n
$$

証明. 群 $(G,*)$ をなす集合 G について、$\forall a \in G \forall n \in \mathbb{N}$ に対し、次のようになる。

$$\begin{aligned}
a^0 &= 1_{(G,*)} * a^0 \\
&= \left(a^0\right)^{-1} * a^0 * a^0 \\
&= \left(a^0\right)^{-1} * a^{0+0} \\
&= \left(a^0\right)^{-1} * a^0 \\
&= 1_{(G,*)} \\
a^1 &= 1_{(G,*)} * a^1 \\
&= a * a^{-1} * a^1 \\
&= a * a^{-1+1} \\
&= a * a^0 \\
&= a * 1_{(G,*)} = a \\
a^{n+1} &= a^n * a^1 \\
&= a^n * a
\end{aligned}$$

また、上記の議論より $1^{-1}_{(G,*)} = 1^0_{(G,*)} = 1^1_{(G,*)} = 1_{(G,*)}$ が成り立つ。$n = k$ のとき、$1^k_{(G,*)} = 1_{(G,*)}$ と仮定しよう。$n = k+1$ のとき、次のようになる。

$$\begin{aligned}
1^{k+1}_{(G,*)} &= 1^k_{(G,*)} * 1^1_{(G,*)} \\
&= 1_{(G,*)} * 1_{(G,*)} \\
&= 1_{(G,*)}
\end{aligned}$$

逆に、$n = k$ のとき、$1^{-k}_{(G,*)} = 1_{(G,*)}$ と仮定しよう。$n = k+1$ のとき、次のようになる。

$$\begin{aligned}
1^{-(k+1)}_{(G,*)} &= 1^{-k-1}_{(G,*)} \\
&= 1^{-k}_{(G,*)} * 1^{-1}_{(G,*)} \\
&= 1_{(G,*)} * 1_{(G,*)} \\
&= 1_{(G,*)}
\end{aligned}$$

以上より数学的帰納法によって $\forall n \in \mathbb{Z}$ に対し、次式が成り立つ。

$$1^n_{(G,*)} = 1_{(G,*)}$$

また、上記の議論により次のようになる。

$$\begin{aligned}
a^{-n} &= a^{-n} * 1_{(G,*)} \\
&= a^{-n} * \left(a^{-1}\right)^0 \\
&= a^{-n} * \left(a^{-1}\right)^{-n+n} \\
&= a^{-n} * \left(a^{-1}\right)^{-n} * \left(a^{-1}\right)^n \\
&= \left(a * a^{-1}\right)^{-n} * \left(a^{-1}\right)^n \\
&= 1^{-n}_{(G,*)} * \left(a^{-1}\right)^n \\
&= 1_{(G,*)} * \left(a^{-1}\right)^n \\
&= \left(a^{-1}\right)^n
\end{aligned}$$

□

1.1.2　部分群

定義 1.1.3. 群 $(G,*)$ をなす集合 G の部分集合 H が算法 $*$ に関して群をなすとき、この集合 H が算法 $*$ に関してその群 $(G,*)$ の部分群 $(H,*)$ をなすという。

定理 1.1.5. 群 $(G,*)$ をなす集合 G の部分集合 H が算法 $*$ に関して群をなすとき、その集合 H は群 $(G,*)$ の単位元 $1_{(G,*)}$ を含みこれ $1_{(G,*)}$ がその群 $(H,*)$ の単位元である、即ち、次式が成り立つ。

$$1_{(H,*)} = 1_{(G,*)} \in H$$

証明. 群 $(G,*)$ をなす集合 G の部分集合 H が算法 $*$ に関して群をなすならば、$a,b \in H$ が成り立つなら、$a*b \in H$ が成り立つかつ、$a \in H$ が成り立つなら、$a^{-1} \in H$ が成り立つので、$a*a^{-1} \in H$ より単位元 $1_{(G,*)}$ についても $1_{(G,*)} \in H$ が成り立つ。

また、$\forall a \in H$ に対し、$H \subseteq G$ が成り立つのであったので、$a \in G$ が成り立ち、したがって、次式が成り立つ。

$$1_{(G,*)} * a = a * 1_{(G,*)} = a$$

よって、その元 $1_{(G,*)}$ がその群 $(H,*)$ の単位元である。 □

定理 1.1.6. 群 $(G,*)$ をなす集合 G の部分集合 H を用いた組 $(H,*)$ が次の条件を全て満たすならそのときに限り、その組 $(H,*)$ が算法 $*$ に関して部分群 $(H,*)$ をなす。

- $1_{(G,*)} \in H$ が成り立つ。
- $\forall a,b \in H$ に対し、$a*b \in H$ が成り立つ。
- $\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つ。

証明. 群 $(G,*)$ をなす集合 G の部分集合 H を用いた組 $(H,*)$ が算法 $*$ に関して部分群 $(H,*)$ をなすならば、群の定義と上記の定理より明らかに次のことが成り立つ。

- $1_{(G,*)} \in H$ が成り立つ。
- $\forall a,b \in H$ に対し、$a*b \in H$ が成り立つ。
- $\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つ。

また、上の条件を全て満たすとき、群 $(G,*)$ が与えられているので、結合律も成り立ち、単位元 $1_{(G,*)}$ はその群 $(H,*)$ の単位元でもあるから、その部分集合 H が算法 $*$ に関して部分群 $(H,*)$ をなす。 □

定理 1.1.7. 群 $(G,*)$ をなす集合 G の部分集合 H を用いた組 $(H,*)$ が次の条件を全て満たすならそのときに限り、その組 $(H,*)$ が算法 $*$ に関して部分群 $(H,*)$ をなす。

- 集合 H は空集合でない。
- $\forall a,b \in H$ に対し、$a*b \in H$ が成り立つ。
- $\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つ。

証明. 群 $(G,*)$ をなす集合 G の部分集合 H を用いた組 $(H,*)$ が次の条件を全て満たすなら、

- 集合 H は空集合でない。

- $\forall a, b \in H$ に対し、$a * b \in H$ が成り立つ。
- $\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つ。

あるその集合 H の元 a が存在して $a^{-1} \in H$ が成り立ち、したがって、$1_{(G,*)} = a * a^{-1} \in H$ が成り立つので、次の条件が全て満たされることになり、その組 $(H, *)$ が算法 $*$ に関して部分群 $(H, *)$ をなす。

- $1_{(G,*)} \in H$ が成り立つ。
- $\forall a, b \in H$ に対し、$a * b \in H$ が成り立つ。
- $\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つ。

逆に、その組 $(H, *)$ が算法 $*$ に関して部分群 $(H, *)$ をなすなら、上の条件が全て満たされることになり、明らかに集合 H は空集合でないので、次の条件が全て満たされる。

- 集合 H は空集合でない。
- $\forall a, b \in H$ に対し、$a * b \in H$ が成り立つ。
- $\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つ。

□

定理 1.1.8. 群 $(G, *)$ において、集合 H がその集合 G の空集合でない有限な部分集合で、$\forall a, b \in H$ に対し、$a * b \in H$ が成り立つなら、その組 $(H, *)$ はその群 $(G, *)$ の部分群である。

証明. 群 $(G, *)$ において、集合 H がその集合 G の空集合でない有限な部分集合で、$\forall a, b \in H$ に対し、$a * b \in H$ が成り立つとき、$\forall a \in H$ に対し、$a = 1_{(G,*)}$ が成り立つなら、$a^{-1} = 1_{(G,*)} \in H$ が成り立つ。

$a \neq 1_{(G,*)}$ が成り立つなら、$\forall n \in \mathbb{N}$ に対し、$a^n \in H$ が成り立つことになる。ここで、$\forall m, n \in \mathbb{N}$ に対し、$m \neq n$ が成り立つなら、$a^m \neq a^n$ が成り立つと仮定すれば、写像 $(a^n)_{n \in \mathbb{N}} : \mathbb{N} \to H; n \mapsto a^n$ が考えられれば、これは単射であるから、$\#\mathbb{N} = \aleph_0 \leq \#H$ が成り立ちこれはその集合 H が有限集合であることに矛盾する。したがって、$m \neq n$ が成り立つかつ、$a^m = a^n$ が成り立つような自然数たち m、n が存在することになる。これにより、$m < n$ と仮定しても一般性は失われることはなく $a^{n-m} = 1_{(G,*)}$ が成り立つ。したがって、$a * a^{n-m-1} = a^{n-m-1} * a = 1_{(G,*)}$ が成り立つ。ここで、$n - m - 1 = 0$ と仮定すると、$n - m = 1$ であるから、$a = a^{n-m} = 1_{(G,*)}$ が得られるが、これは $a \neq 1_{(G,*)}$ が成り立つことに矛盾する。したがって、$n - m - 1 > 0$ が成り立つことになり、したがって、$a^{n-m-1} \in H$ が成り立つ。これにより、$a^{-1} = a^{n-m-1}$ が得られる。

以上より、$\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つので、次の条件が全て満たされ、

- 集合 H は空集合でない。
- $\forall a, b \in H$ に対し、$a * b \in H$ が成り立つ。
- $\forall a \in H$ に対し、$a^{-1} \in H$ が成り立つ。

よって、その組 $(H, *)$ が算法 $*$ に関して部分群 $(H, *)$ をなす。 □

定義 1.1.4. その集合 H がその集合 G であるとき、または集合 $\left\{1_{(G,*)}\right\}$ であるとき、あきらかに群 $(G, *)$ の部分群 $(H, *)$ をなす。これら 2 つの集合たち G、$\left\{1_{(G,*)}\right\}$ がなす群 $(G, *)$ の部分群たち $(G, *)$、$\left(\left\{1_{(G,*)}\right\}, *\right)$ を自明な部分群といい、その群 $(G, *)$ の部分群のうち、自明な部分群を除いた部分群を真部分群という。これの存在は群 $(G, *)$ に依存する。

定理 1.1.9. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$H*H=H$ が成り立つ。

証明. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$\forall g*h\in H*H$ に対し、$g,h\in H$ が成り立つので、$g*h\in H$ も成り立つ。一方で、$\forall h\in H$ に対し、$h=1_{(G,*)}*h$ が成り立つので、$h\in H*H$ も成り立つ。以上より、$H*H=H$ が得られる。 □

定理 1.1.10. 2 つの集合たち H、I を用いた組々 $(H,*)$、$(I,*)$ が群 $(G,*)$ の部分群たちをなすなら、集合 $H\cap I$ を用いた組 $(H\cap I,*)$ も群 $(G,*)$ の部分群をなす。

証明. 2 つの集合たち H、I を用いた組々 $(H,*)$、$(I,*)$ が群 $(G,*)$ の部分群たちをなすなら、次の条件が全て満たされる。

- $1_{(G,*)}\in H$ が成り立つ。
- $\forall a,b\in H$ に対し、$a*b\in H$ が成り立つ。
- $\forall a\in H$ に対し、$a^{-1}\in H$ が成り立つ。
- $1_{(G,*)}\in I$ が成り立つ。
- $\forall a,b\in I$ に対し、$a*b\in I$ が成り立つ。
- $\forall a\in I$ に対し、$a^{-1}\in I$ が成り立つ。

これにより、次の条件が全て満たされることになるので、

- $1_{(G,*)}\in H\cap I$ が成り立つ。
- $\forall a,b\in H\cap I$ に対し、$a*b\in H\cap I$ が成り立つ。
- $\forall a\in H\cap I$ に対し、$a^{-1}\in H\cap I$ が成り立つ。

集合 $H\cap I$ を用いた組 $(H\cap I,*)$ も群 $(G,*)$ の部分群をなす。 □

定理 1.1.11. 群 $(G,*)$ において、$\forall S\in\mathfrak{P}(G)\setminus\{\emptyset\}$ に対し、集合 $S\cup S^{-1}$ の有限個の元たちの算法 $*$ の像全体の集合を H とおく。このとき、この組 $(H,*)$ は群 $(G,*)$ の部分群となる。

証明. 群 $(G,*)$ において、$\forall S\in\mathfrak{P}(G)\setminus\{\emptyset\}$ を考える。集合 $S\cup S^{-1}$ の有限個の元たちの算法 $*$ の像全体の集合を H とおく。$a,b\in H$ なる元たち a、b を考えると、その元 $a*b$ も集合 $S\cup S^{-1}$ の有限個の元たちの算法 $*$ の像であるから $a*b\in H$ が成り立ち、a^{-1} も始集合の元たちの逆元たちの算法 $*$ の逆元たちの算法 $*$ の像であり、これらの逆元たちは全て集合 S、S^{-1} のいずれかに属するので、$a^{-1}\in H$ である。以上より、次の条件が全て満たされ、

- 集合 H は空集合でない。
- $\forall a,b\in H$ に対し、$a*b\in H$ が成り立つ。
- $\forall a\in H$ に対し、$a^{-1}\in H$ が成り立つ。

この集合 H を用いた組 $(H,*)$ は群 $(G,*)$ の部分群をなす。 □

定義 1.1.5. このような集合 H を集合 S によって生成される群 $(G,*)$ の部分群といい、集合 S を集合 H の生成元の集合、生成系という。特に $S=\{a\}$ が成り立つなら、この集合によって生成される群 $(G,*)$ の部分群をなす集合は $\{a^n\in G|a\in S,n\in\mathbb{Z}\}$ となる。

1.1.3 剰余類

定義 1.1.6. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$a,b\in G$ なる元たち a、b について次のことを定義しよう。このようなことを元たち a、b がその部分群 $(H,*)$ を法として左合同であるという。

$$a\equiv_l b \bmod(H,*)\Leftrightarrow a^{-1}*b\in H$$

定理 1.1.12. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、この関係 $\equiv_l \bmod(H,*)$ はその集合 G における同値関係である。

証明. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$\forall a\in G$ に対し、次のようになるかつ、

$$\begin{aligned}1_{(G,*)}\in G&\Rightarrow 1_{(G,*)}\in H\\&\Leftrightarrow a^{-1}*a\in H\\&\Leftrightarrow a\equiv_l a \bmod(H,*)\end{aligned}$$

$\forall a,b\in G$ に対し、$a\equiv_l b \bmod(H,*)$ が成り立つなら、次のようになるかつ、

$$\begin{aligned}a\equiv_l b \bmod(H,*)&\Leftrightarrow a^{-1}*b\in H\\&\Leftrightarrow \left(a^{-1}*b\right)^{-1}=b^{-1}*\left(a^{-1}\right)^{-1}=b^{-1}*a\in H\\&\Leftrightarrow b\equiv_l a \bmod(H,*)\\a\equiv_l b \bmod(H,*)\wedge b\equiv_l c \bmod(H,*)&\Leftrightarrow a^{-1}*b\in H\wedge b^{-1}*c\in H\\&\Rightarrow \left(a^{-1}*b\right)*\left(b^{-1}*c\right)=\left(a^{-1}*1_{(G,*)}\right)*c=a^{-1}*c\in H\\&\Leftrightarrow a\equiv_l c \bmod(H,*)\end{aligned}$$

この関係 $\equiv_l \bmod(H,*)$ はその集合 G における同値関係である。 □

定理 1.1.13. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、この同値関係 $\equiv_l \bmod(H,*)$ によるその集合 G の元 a の同値類 $C_{\equiv_l \bmod(H,*)}(a)$ は集合 $a*H$ に等しい。

証明. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、次のようなり、

$$\begin{aligned}x\in C_{\equiv_l \bmod(H,*)}(a)&\Leftrightarrow a\equiv_l x \bmod(H,*)\\&\Leftrightarrow a^{-1}*x\in H\end{aligned}$$

ここで、$h=a^{-1}*x$ とすると、次式が成り立ち、

$$\begin{aligned}x&=1_{(G,*)}*x\\&=\left(a*a^{-1}\right)*x\\&=a*\left(a^{-1}*x\right)\\&=a*h\end{aligned}$$

明らかに $h\in H$ かつ $a*h\in G$ が成り立つので、次式が成り立ち、

$$\begin{aligned}a*h\in C_{\equiv_l \bmod(H,*)}(a)&\Leftrightarrow a*h\in G\wedge a\equiv_l a*h \bmod(H,*)\\&\Leftrightarrow a*h\in G\wedge a^{-1}*(a*h)\in H\\&\Leftrightarrow a*h\in G\wedge \left(a^{-1}*a\right)*h\in H\end{aligned}$$

$$\Leftrightarrow a * h \in G \wedge h \in H$$
$$\Leftrightarrow a * h \in \{a * h \in G | h \in H\} = a * H$$

したがって、次のようになる。

$$C_{\equiv_l \bmod(H,*)}(a) = \{a * h \in G | h \in H\} = a * H$$

□

定義 1.1.7. この集合 $a * H$ を部分群 $(H, *)$ を法とする元 a の左剰余類といいこれ全体の集合 $G/\equiv_l \bmod(H, *)$ を G/H と書くが、ここでは、$G/_l H$ と書くことにする。

定理 1.1.14 (左剰余類分解)**.** 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、次式が成り立つ。

$$G = \bigsqcup G/_l H$$

この定理を左剰余類分解という。

証明. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、定理 1.1.12 よりその関係 $\equiv_l \bmod(H, *)$ はその集合 G における同値関係であるので、その関係 $\equiv_l \bmod(H, *)$ による類別が次のようになる。

$$G = \bigsqcup G/\equiv_l \bmod(H, *) = \bigsqcup G/_l H$$

□

定理 1.1.15. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、その集合 H 自身はその部分群 $(H, *)$ を法とする左剰余類でもある。

証明. $\{h \in G | h \in H\} = \left\{1_{(G,*)} * h \in G \middle| h \in H\right\}$ が成り立つので、$H = 1_{(G,*)} * H$ が成り立つことによる。 □

定理 1.1.16. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、その集合 G の元々 a、b が部分群 $(H, *)$ を法として左合同であるなら、$a * H = b * H$ が成り立ち、そうでないなら $a * H \cap b * H = \emptyset$ が成り立つ。

証明. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、その集合 G の元々 a、b が集合 H に関して左合同であるとする、即ち、$a \equiv_l b \bmod(H, *)$ が成り立つとする。このとき、$a \equiv_l b \bmod(H, *) \Leftrightarrow b \equiv_l a \bmod(H, *)$ が成り立ち、$\forall x \in a * H$ に対し、次のようになる。

$$x \in a * H \Leftrightarrow x = a * h \wedge h \in H$$
$$\Leftrightarrow a^{-1} * x = h \in H$$
$$\Leftrightarrow x \equiv_l a \bmod(H, *)$$

ここで、$a \equiv_l b \bmod(H, *)$ が成り立つので、次のようになる。

$$x \equiv_l b \bmod(H, *) \Leftrightarrow b^{-1} * x \in H$$

ここで、$b^{-1} * x = h'$ とおくと、次のようになるので、

$$x = b * b^{-1} * x = b * h'$$

$x \in b * H$ が成り立つ。これにより、$a * H \subseteq b * H$ が得られる。同様にして、$b * H \subseteq a * H$ が得られるので、$a * H = b * H$ が成り立つ。

$a * H \cap b * H \neq \emptyset$ が成り立つなら、$x \in a * H$ かつ $x \in b * H$ が成り立つような元 x がその集合 G に存在し、次のようになる。

$$\begin{aligned} x \in a * H \wedge x \in b * H &\Leftrightarrow a^{-1} * x, b^{-1} * x \in H \\ &\Leftrightarrow a \equiv_l x \bmod(H, *) \wedge b \equiv_l x \bmod(H, *) \\ &\Rightarrow a \equiv_l b \bmod(H, *) \end{aligned}$$

これを対偶律に適用すれば、$\neg a \equiv_l b \bmod(H, *) \Rightarrow a * H \cap b * H = \emptyset$ が成り立つ。 □

定義 1.1.8. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、$a, b \in G$ なる元々 a、b について次のことを定義しよう。このようなことを元々 a、b がその部分群 $(H, *)$ を法として右合同であるという。

$$a \equiv_r b \bmod(H, *) \Leftrightarrow a * b^{-1} \in H$$

定理 1.1.17. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、この関係 $\equiv_r \bmod(H, *)$ はその集合 G における同値関係である。

証明. 定理 1.1.12 と同様にして示される。 □

定理 1.1.18. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、この同値関係 $\equiv_r \bmod(H, *)$ によるその集合 G の元 a の同値類 $C_{\equiv_r \bmod(H,*)}(a)$ は集合 $H * a$ に等しい。

証明. 定理 1.1.13 と同様にして示される。 □

定義 1.1.9. この集合 $H * a$ を部分群 $(H, *)$ を法とする元 a の右剰余類といいこれ全体の集合 $G/\equiv_r \bmod(H, *)$ を $H \setminus G$ と書くが、ここでは、$G/_r H$ と書くことにする。

定理 1.1.19 (右剰余類分解)**.** 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、次式が成り立つ。

$$G = \bigsqcup G/_r H$$

この定理を右剰余類分解という。

証明. 定理 1.1.14 と同様にして示される。 □

定理 1.1.20. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、その集合 H 自身はその部分群 $(H, *)$ を法とする右剰余類でもある。

証明. 定理 1.1.15 と同様にして示される。 □

定理 1.1.21. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、その集合 G の元々 a、b が部分群 $(H, *)$ を法として右合同であるなら、$H * a = H * b$ が成り立ち、そうでないなら $H * a \cap H * b = \emptyset$ が成り立つ。

証明. 定理 1.1.16 と同様にして示される。 □

なお、任意の部分群 $(H, *)$ において、その部分群 $(H, *)$ を法として左合同であることと右合同であることとは必ずしも一致するとは限らないことに注意されたい。

定義 1.1.10. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、その集合 G の元々 a、b がその部分群 $(H,*)$ を法として左合同であることと右合同であることとが一致するとき、それらの元々 a、b が部分群 $(H,*)$ を法として合同である、合同関係であるといい、このことを $a \equiv b \bmod (H,*)$ と書く。さらに同値類 $C_{\equiv \bmod (H,*)}(a)$ を部分群 $(H,*)$ を法とする元 a の剰余類という。

定理 1.1.22. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$\forall a \in G$ に対し、$a*H = H*a$ が成り立つなら、$\forall b \in G$ に対し、$a \equiv_l b \bmod (H,*)$ が成り立つならそのときに限り、$a \equiv_r b \bmod (H,*)$ が成り立つ。

証明. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$\forall a \in G$ に対して、$a*H = H*a$ が成り立つとすると、$\forall b \in G$ に対し、次のことが成り立つので、

- $b \in a*H$ が成り立つならそのときに限り、$b \in H*a$ が成り立つ。
- $b \in a*H$ が成り立つならそのときに限り、$a \equiv_l b \bmod (H,*)$ が成り立つ。
- $b \in H*a$ が成り立つならそのときに限り、$a \equiv_r b \bmod (H,*)$ が成り立つ。

$a \equiv_l b \bmod (H,*)$ が成り立つならそのときに限り、$a \equiv_r b \bmod (H,*)$ が成り立つことがいえる。 □

定理 1.1.23. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$\forall a,b \in G$ に対し、$a*b = b*a$ が成り立つなら、$a \equiv_l b \bmod (H,*)$ が成り立つならそのときに限り、$a \equiv_r b \bmod (H,*)$ が成り立つ。

証明. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$\forall a,b \in G$ に対して、$a*b = b*a$ が成り立つとする、即ち、群 $(G,*)$ が可換群であるとすると、$\forall a \in G$ に対して左剰余類と右剰余類の定義より次式が成り立つので、

$$\begin{aligned} a*H &= \{a*h \in G | h \in H\} \\ &= \{h*a \in G | h \in H\} \\ &= H*a \end{aligned}$$

定理 1.1.22 により $a \equiv_l b \bmod (H,*)$ が成り立つならそのときに限り、$a \equiv_r b \bmod (H,*)$ が成り立つ。 □

定理 1.1.24. 群 $(G,*)$ の部分群たち $(H,*)$、$(I,*)$ が与えられたとき、$H*I = I*H$ が成り立つならそのときに限り、その組 $(H*I,*)$ がその群 $(G,*)$ の部分群をなす。

証明. 群 $(G,*)$ の部分群たち $(H,*)$、$(I,*)$ が与えられたとき、$H*I = I*H$ が成り立つなら、$1_{(G,*)} \in H$ かつ $1_{(G,*)} \in I$ が成り立つので、$1_{(G,*)} = 1_{(G,*)} * 1_{(G,*)} \in H*I$ が成り立つ。また、$h', h'' \in H$、$i', i'' \in I$ とおき $\forall h'*i', h''*i'' \in H*I$ に対し、$H*I = I*H$ が成り立つので、$\exists h''' \in H \exists i''' \in I$ に対し、$h'''*i''' = i'*h''$ が成り立つ。したがって、次のようになり、

$$\begin{aligned} (h'*i')*(h''*i'') &= h'*(i'*h'')*i'' \\ &= h'*(h'''*i''')*i'' \\ &= (h'*h''')*(i'''*i'') \end{aligned}$$

$h'*h''' \in H$ かつ $i'''*i'' \in I$ が成り立つので、$(h'*i')*(h''*i'') \in H*I$ が成り立つ。さらに、$h' \in H$、$i' \in I$ とおき $\forall h'*i' \in H*I$ に対し、$(h'*i')^{-1} = i'^{-1}*h'^{-1}$ が成り立つのであった。ここで、$h'^{-1} \in H$ かつ $i'^{-1} \in I$ が成り立つので、$(h'*i')^{-1} \in I*H$ が成り立つ。ここで、$H*I = I*H$ が成り立つので、$(h'*i')^{-1} \in H*I$ も成り立つ。これにより、次のことが満たされその組 $(H*I,*)$ がその群 $(G,*)$ の部分群をなす。

- $1_{(G,*)} \in H * I$ が成り立つ。
- $\forall h' * i', h'' * i'' \in H * I$ に対し、$(h' * i') * (h'' * i'') \in H * I$ が成り立つ。
- $\forall h' * i' \in H * I$ に対し、$(h' * i')^{-1} \in H * I$ が成り立つ。

逆に、その組 $(H * I, *)$ がその群 $(G, *)$ の部分群をなすなら、$\forall h' * i' \in H * I$ に対し、$(h' * i')^{-1} \in H * I$ が成り立つので、$(h' * i')^{-1} = h'' * i''$ が成り立つようなその集合 H の元 h'' とその集合 I の元 i'' が存在することになる。ここで、$(h'' * i'')^{-1} \in H * I$ かつ $h''^{-1} \in H$ かつ $i''^{-1} \in I$ が成り立つので、次のようになる。

$$\begin{aligned} h' * i' &= \left((h' * i')^{-1}\right)^{-1} \\ &= (h'' * i'')^{-1} \\ &= i''^{-1} * h''^{-1} \in I * H \end{aligned}$$

また、$\forall i' * h' \in I * H$ に対し、$h'^{-1} \in H$ かつ $i'^{-1} \in I$ かつ $\left(h'^{-1} * i'^{-1}\right)^{-1} \in H * I$ が成り立つので、次のようになる。

$$\begin{aligned} i' * h' &= \left(i'^{-1}\right)^{-1} * \left(h'^{-1}\right)^{-1} \\ &= \left(h'^{-1} * i'^{-1}\right)^{-1} \in H * I \end{aligned}$$

以上より、$H * I = I * H$ が得られた。 □

定理 1.1.25. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、$\forall a \in G$ に対し、その組 $\left(a * H * a^{-1}, *\right)$ もその群 $(G, *)$ の部分群をなす。

証明. 群 $(G, *)$ の部分群 $(H, *)$ が与えられたとき、$\forall a \in G$ に対し、集合 $a * H * a^{-1}$ について考えよう。このとき、$1_{(G,*)} \in H$ が成り立つので、次のようになることから、

$$\begin{aligned} 1_{(G,*)} &= a * a^{-1} \\ &= a * 1_{(G,*)} * a^{-1} \in a * H * a^{-1} \end{aligned}$$

$1_{(G,*)} \in a * H * a^{-1}$ が成り立つ。また、$\forall a * g * a^{-1}, a * h * a^{-1} \in a * H * a^{-1}$ に対し、次のようになることから、

$$\begin{aligned} \left(a * g * a^{-1}\right) * \left(a * h * a^{-1}\right) &= a * g * \left(a^{-1} * a\right) * h * a^{-1} \\ &= a * g * 1_{(G,*)} * h * a^{-1} \\ &= a * (g * h) * a^{-1} \end{aligned}$$

$g * h \in H$ が成り立つことにより $\left(a * g * a^{-1}\right) * \left(a * h * a^{-1}\right) \in a * H * a^{-1}$ が成り立つ。さらに、$\forall a * h * a^{-1} \in a * H * a^{-1}$ に対し、次のようになることから、

$$\begin{aligned} \left(a * h * a^{-1}\right)^{-1} &= \left(a^{-1}\right)^{-1} * h^{-1} * a^{-1} \\ &= a * h^{-1} * a^{-1} \end{aligned}$$

$h^{-1} \in H$ が成り立つことにより $\left(a * h * a^{-1}\right)^{-1} \in a * H * a^{-1}$ が成り立つ。以上より、次のことが満たされその組 $\left(a * H * a^{-1}, *\right)$ がその群 $(G, *)$ の部分群をなす。

- $1_{(G,*)} \in a*H*a^{-1}$ が成り立つ。
- $\forall a*g*a^{-1}, a*h*a^{-1} \in a*H*a^{-1}$ に対し、$\left(a*g*a^{-1}\right)*\left(a*h*a^{-1}\right) \in a*H*a^{-1}$ が成り立つ。
- $\forall a*h*a^{-1} \in a*H*a^{-1}$ に対し、$\left(a*h*a^{-1}\right)^{-1} \in a*H*a^{-1}$ が成り立つ。

□

1.1.4 正規部分群

定義 1.1.11. 群 $(G,*)$ とこれの部分群 $(N,*)$ について、部分群 $(N,*)$ を法とする左合同と右合同が一致する、即ち、$\forall a \in G$ に対し、$a*N = N*a$ が成り立つとき、部分群 $(N,*)$ を群 $(G,*)$ について正規な部分群 $(N,*)$、群 $(G,*)$ の正規部分群などといい $(N,*) \trianglelefteq (G,*)$ とかく。

定理 1.1.26. 群 $(G,*)$ 自身、単位部分群 $\left(\left\{1_{(G,*)}\right\},*\right)$、群 $(G,*)$ が可換群であるときの任意の部分群はいずれもその群 $(G,*)$ の正規部分群である、即ち、次式が成り立つ。

$$(G,*) \trianglelefteq (G,*), \quad \left(\left\{1_{(G,*)}\right\},*\right) \trianglelefteq (G,*)$$

証明. 群 $(G,*)$ 自身は、算法 $*$ に適用される 2 つの元の順序付けられた組とこれの順序を逆にしたものどちらも存在するので、その群 $(G,*)$ の正規部分群である。単位部分群 $(\{1_G\},*)$ は、単位元は任意の元に対し可換律が成り立つので、その群 $(G,*)$ の正規部分群である。群 $(G,*)$ が可換群であるときの任意の部分群 $(H,*)$ は、上記の定理より可換律で左剰余類 $a*H$ と右剰余類 $H*a$ の各元が一致するので、その群 $(G,*)$ の正規部分群である。 □

定理 1.1.27. 群 $(G,*)$ とこれの部分群 $(N,*)$ について、次のことは同値である。

- $(N,*) \trianglelefteq (G,*)$ が成り立つ。
- $\forall a \in G$ に対し、$a*N = N*a$ が成り立つ。
- $\forall a \in G$ に対し、$a*N*a^{-1} = N$ が成り立つ。
- $\forall a \in G \forall n \in N$ に対し、$a*n*a^{-1} \in N$ が成り立つ。
- $\forall a \in G$ に対し、$a*N*a^{-1} \subseteq N$ が成り立つ。

証明. 群 $(G,*)$ とこれの部分群 $(N,*)$ について、$(N,*) \trianglelefteq (G,*)$ が成り立つならそのときに限り、$\forall a \in G$ に対し、$a*N = N*a$ が成り立つのであった。したがって、$\forall a*n \in a*N$ に対し、$a*n \in a*N$ が成り立つならそのときに限り、$a*n \in N*a$ が成り立つので、あるその集合 H の元 n' を用いて $a*n = n'*a$ とおくことができる。したがって、これが成り立つならそのときに限り、次のようになる。

$$a*n*a^{-1} = n'*a*a^{-1} = n'$$

これにより、$\forall a*n*a^{-1} \in a*N*a^{-1}$ に対し、$a*n*a^{-1} \in a*N*a^{-1}$ が成り立つならそのときに限り、$a*n*a^{-1} \in N$ が成り立つので、$a*N*a^{-1} = N$ が成り立つ。これで次のことが同値であることが示された。

- $(N,*) \trianglelefteq (G,*)$ が成り立つ。
- $\forall a \in G$ に対し、$a*N = N*a$ が成り立つ。
- $\forall a \in G$ に対し、$a*N*a^{-1} = N$ が成り立つ。

また、$\forall a \in G \forall n \in N$ に対し、$a * n * a^{-1} \in N$ が成り立つなら、元 a の代わりに元 a^{-1} を考えれば、$a^{-1} * n * a \in N$ が成り立ち、したがって、$\forall a * n \in a * N$ に対し、あるその集合 N の元 h' を用いて $a^{-1} * n' * a = n$ とおくことができ次のようになる。

$$\begin{aligned} a * n &= a * \left(a^{-1} * n' * a\right) \\ &= \left(a * a^{-1}\right) * (n' * a) \\ &= 1_{(G,*)} * (n' * a) \\ &= n' * a \in N * a \end{aligned}$$

逆も同様にして考えれば、したがって、$a * n \in a * N$ が成り立つならそのときに限り、$a * n \in N * a$ が成り立つので、$a * N = N * a$ が成り立ち、したがって、部分群 $(N, *)$ が群 $(G, *)$ について正規である。また、明らかに次のことは同値であるので、

- $\forall a \in G \forall n \in N$ に対し、$a * n * a^{-1} \in N$ が成り立つ。
- $\forall a \in G$ に対し、$a * N * a^{-1} \subseteq N$ が成り立つ。

以上の議論により、次のことは同値である。

- $\forall a \in G$ に対し、$a * N = N * a$ が成り立つ。
- $\forall a \in G$ に対し、$a * N * a^{-1} = N$ が成り立つ。
- $\forall a \in G \forall n \in N$ に対し、$a * n * a^{-1} \in N$ が成り立つ。
- $\forall a \in G$ に対し、$a * N * a^{-1} \subseteq N$ が成り立つ。

□

定理 1.1.28. 群 $(G, *)$ の部分群 $(H, *)$ と正規部分群 $(N, *)$ が与えられたとき、$H * N = N * H$ が成り立つ。

証明. 群 $(G, *)$ の部分群 $(H, *)$ と正規部分群 $(N, *)$ が与えられたとき、$h \in H$ かつ $n \in N$ とおいて $\forall h * n \in H * N$ に対し、$h * n \in h * N$ が成り立ち、ここで、$h * N = N * h$ が成り立つので、$h * n \in N * h$ が成り立つ。これにより、$h * n = n' * h$ が成り立つようなその集合 N の元 n' が存在する。したがって、$h * n \in N * H$ が成り立つので、$H * N \subseteq N * H$ が成り立つ。同様にして、$N * H \subseteq H * N$ が成り立つので、$H * N = N * H$ が得られる。 □

定理 1.1.29. 群 $(G, *)$ の部分群 $(H, *)$ と正規部分群 $(N, *)$ が与えられたとき、その組 $(H * N, *)$ もその群 $(G, *)$ の部分群をなす。特に、その部分群 $(H, *)$ が正規であるなら、その部分群 $(H * N, *)$ も正規である。

証明. 群 $(G, *)$ の部分群 $(H, *)$ と正規部分群 $(N, *)$ が与えられたとき、$H * N = N * H$ が成り立つので、定理 1.1.24 よりその組 $(H * N, *)$ もその群 $(G, *)$ の部分群をなす。特に、その部分群 $(H, *)$ が正規であるなら、$\forall a \in G$ に対し、$a * H = H * a$ が成り立つことになるので、$\forall a \in G$ に対し、次のようになり、

$$\begin{aligned} a * (H * N) &= (a * H) * N \\ &= (H * a) * N \\ &= H * (a * N) \\ &= H * (N * a) \\ &= (H * N) * a \end{aligned}$$

これにより、その部分群 $(H*N,*)$ も正規である。 □

定理 1.1.30. 群 $(G,*)$ の 2 つの正規部分群たち $(M,*)$、$(N,*)$ が与えられたとき、その組 $(M\cap N,*)$ もその群 $(G,*)$ の正規部分群をなす、即ち、$(M\cap N,*)\trianglelefteq(G,*)$ が成り立つ。

証明. 群 $(G,*)$ の 2 つの正規部分群たち $(M,*)$、$(N,*)$ が与えられたとき、定理 1.1.10 よりその組 $(M\cap N,*)$ もその群 $(G,*)$ の部分群をなす。ここで、$\forall a\in G\forall n\in M\cap N$ に対し、$n\in M$ が成り立つので、$a*M=M*a$ が成り立つことにより、$a*n=m'*a$ が成り立つような元 m' がその集合 M に存在する。同様にして、$a*n=n'*a$ が成り立つような元 n' がその集合 M に存在する。したがって、$m'*a=n_2*a$ が得られ、これにより、$m'=n'$ が成り立つので、$m'=n'\in M\cap N$ が成り立つ。これにより、$a*n=m'*a$ が成り立つような元 m' がその集合 $M\cap N$ に存在することになるので、$a*(M\cap N)\subseteq(M\cap N)*a$ が得られる。逆も同様にして考えれば、よって、その部分群 $(M\cap N,*)$ は正規である。 □

定理 1.1.31. 群 $(G,*)$ とこれの 1 つの部分群 $(N,*)$ において、$(N,*)\trianglelefteq(G,*)$ が成り立つならそのときに限り、$\forall a,b\in G$ に対し、次式が成り立つ。

$$a*N*b*N=a*b*N$$

証明. 群 $(G,*)$ とこれの 1 つの部分群 $(N,*)$ において、$(N,*)\trianglelefteq(G,*)$ が成り立つなら、$\forall a,b\in G$ に対し、その部分群 $(N,*)$ を法とする 2 つの剰余類たち $a*N$、$b*N$ を用いた集合 $a*N*b*N$ について考えよう。$\forall n\in N$ に対し、$b*n*b^{-1}\in N$ が成り立つかつ、$\forall m,n\in N$ に対し、$m*n\in N$ が成り立つことより、$\forall a*m*b*n\in a*N*b*N$ に対し、次のようになるかつ、

$$\begin{aligned}a*m*b*n&=a*b*b^{-1}*m*b*n\\&=a*b*\left(b^{-1}*m*b\right)*n\in a*b*N\end{aligned}$$

$1_{(G,*)}\in N$ が成り立つことにより、$\forall a*b*n\in a*b*N$ に対し、次のようになるので、

$$a*b*n=a*1_{(G,*)}*b*n\in a*N*b*N$$

$a*N*b*N=a*b*N$ が成り立つ。

逆に、$\forall a,b\in G$ に対し、$a*N*b*N=a*b*N$ が成り立つなら、$a=1_{(G,*)}$ とすれば、$\forall c\in G$ に対し、$c\in 1_{(G,*)}*N*b*N$ が成り立つならそのときに限り、$\exists m,n\in N$ に対し、$c=1_{(G,*)}*m*b*n=m*b*n$ が成り立つので、$c\in N*b*N$ が成り立つ。これにより、$N*b*N=b*N$ が成り立つ。そこで、$\forall n*b\in N*b$ に対し、$1_{(G,*)}\in N$ が成り立つので、$n*b=n*b*1_{(G,*)}\in N*b*N$ が成り立つ。これにより、$N*b\subseteq N*b*N$ が成り立つので、$\forall n*b\in N*b$ に対し、$b^{-1}*N*b\in N$ が成り立つ。定理 1.1.27 よりその部分群 $(N,*)$ は $(N,*)\trianglelefteq(G,*)$ を満たす。 □

1.1.5 商群

定義 1.1.12. 群 $(G,*)$ の正規部分群 $(N,*)$ が与えられたとき、次式のように定義されるように、その部分群 $(N,*)$ を法とする剰余類たち $a*N$ 全体の集合を G/N と書く。

$$G/N=\{a*N|a\in G\}$$

定理 1.1.32. 群 $(G,*)$ の正規部分群 $(N,*)$ が与えられたとき、その組 $(G/N,*)$ は群をなす。このとき、その群 $(G/N,*)$ 上での単位元は $1_{(G,*)}*N=N$、その群 $(G/N,*)$ の任意の元 $a*N$ の逆元は $a^{-1}*N$ となる、即ち、次式が成り立つ。

$$1_{(G/N,*)}=N$$
$$(a*N)^{-1}=a^{-1}*N$$

定義 1.1.13. 群 $(G,*)$ の正規部分群 $(N,*)$ が与えられたとき、その群 $(G/N,*)$ をその正規部分群 $(N,*)$ によるその群 $(G,*)$ の剰余群、商群という。

証明. 群 $(G,*)$ とこれの正規部分群 $(N,*)$ を法とする剰余類たち $a*N$ 全体の集合 G/N において、$\forall a,b,c\in G$ に対し、次のようになることにより、

$$\begin{aligned}(a*N*b*N)*c*N&=(a*b*N)*c*N\\&=a*(b*N*c*N)\\&=a*(b*c*N)\\&=a*(b*c)*N\\&=a*N*(b*c*N)\\&=a*N*(b*N*c*N)\end{aligned}$$

結合律が満たされる。

さらに、次のようになることにより、

$$1_{(G,*)}*N*a*N=1_{(G,*)}*a*N=a*N$$
$$a*N*1_{(G,*)}*N=a*1_{(G,*)}*N=a*N$$

その単位元が $1_{(G,*)}*N=N$ である。

最後に、次のようになることにより、

$$a*N*a^{-1}*N=a*a^{-1}*N=1_{(G,*)}*N=N$$
$$a^{-1}*N*a*N=a^{-1}*a*N=1_{(G,*)}*N=N$$

その集合 G/N の任意の元 $a*N$ のその逆元は $a^{-1}*N$ である。

以上より部分群 $(N,*)$ を法とする剰余類全体の集合 G/N は群 $(G/N,*)$ をなす。 □

1.1.6 群論に関する Lagrange の定理

定理 1.1.33. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、これらについて次のことが成り立つ。

- 集合 Q_l の任意の元 $a*H$ に対し集合 Q_r の元 $H*a^{-1}$ は一意的に決まる。
- 写像 $G/_lH\to G/_rH; a*H\mapsto H*a^{-1}$ は全単射であり、したがって、$\#G/_lH=\#G/_rH$ が成り立つ。

証明. 群 $(G,*)$ の部分群 $(H,*)$ が与えられたとき、$\forall a*H,b*H\in G/_lH$ に対し、$a*H=b*H$ が成り立つならそのときに限り、$a^{-1}*b\in H$ が成り立つことになる。ここで、逆元はもとの群をなす集合に属するので、$\left(a^{-1}*b\right)^{-1}=b^{-1}*a\in H$ が成り立つことから、$H*a=H*b$ が成り立つ。これにより、graph$\mathfrak{G}$ が次のような対応 $G/_lH\multimap G/_rH$ はたしかに写像となっている。

$$\mathfrak{G}=\left\{(a*H,H*b)\in G/_lH\times G/_rH\middle|H*b=H*a^{-1}\right\}$$

写像 $f : G/_lH \to G/_rH; a * H \mapsto H * a^{-1}$ について、上と同様の議論により、この写像の逆対応 $f^{-1} : G/_rH \to G/_lH; H * a^{-1} \mapsto a * H$ も写像であるから、よって、この写像 f は全単射となり、$\#G/_lH = \#G/_rH$ が得られる。 □

定義 1.1.14. 群 $(G, *)$ の部分群 $(H, *)$ について、部分群 $(H, *)$ を法とする互いに異なる左剰余類たちの濃度 $\#G/_lH$ は、部分群 $(H, *)$ を法とする互いに異なる右剰余類たちの濃度 $\#G/_rH$ に等しいので、その濃度は群 $(G, *)$ とこれの部分群 $(H, *)$ によってのみ決定されることができる。したがって、その部分群 $(H, *)$ を法とする互いに異なる左剰余類たちの濃度 $\#G/_lH$ を群 $(G, *)$ における部分群 $(H, *)$ の指数といい、$(G : H)$ と書く。

定理 1.1.34. 群 $(G, *)$ の集合 G の濃度 $\#(G, *)$ が有限であるなら、群 $(G, *)$ における部分群 $(H, *)$ の指数 $(G : H)$ も有限である。

証明. 部分群 $(H, *)$ についても $\#H \leq \#G$ が成り立つことにより、$a \in (G, *)$ と $h \in (H, *)$ との順序付けられた組の個数もせいぜい $\#G\#H$ と有限であるから、定義より群 $(G, *)$ における部分群 $(H, *)$ の指数 $(G : H)$ の濃度 $\#(G : H)$ も有限となる。 □

定理 1.1.35. 群 $(G, *)$ の有限な部分群 $(H, *)$ について、部分群 $(H, *)$ を法とする任意の 1 つの左剰余類 $a * H$ の濃度 $\#a * H$ あるいはこれに対応する右剰余類 $H * a$ の濃度 $\#H * a$ はその部分群 $(H, *)$ の位数 $o(H, *)$ に等しい、即ち、次式が成り立つ。

$$\#a * H = \#H * a = o(H, *)$$

証明. 群 $(G, *)$ の有限な部分群 $(H, *)$ と $g, h \in H$ なる元たち g、h について、写像 $f : H \to a * H; h \mapsto a * h$ が与えられると、簡約律より $g = h \Leftrightarrow a * g = a * h$ が成り立ちこの写像 f は全単射 $f : H \xrightarrow{\sim} a * H$ である。また、写像 $f : H \to H * a; h \mapsto h * a$ も同様にして、全単射 $f : H \xrightarrow{\sim} H * a$ であることが示される。 □

定理 1.1.36 (群論に関する Lagrange の定理)**.** 群 $(G, *)$ の有限な部分群 $(H, *)$ について、次式が成り立つ。

$$o(G, *) = (G : H)o(H, *)$$

この定理を群論に関する Lagrange の定理という。

証明. 群 $(G, *)$ の有限な部分群 $(H, *)$ において、その部分群 $(H, *)$ を法とする左合同な関係によって集合 G は $(G : H)$ つの左剰余類 $a_i * H$ に分割され各左剰余類 $a_i * H$ の濃度 $\#a_i * H$ が $o(H, *)$ に等しいので、次のようになる[*2]。

$$o(G, *) = \sum_{i \in \Lambda_{(G:H)}} \#\left(a_i * H\right) = \sum_{i \in \Lambda_{(G:H)}} o(H, *) = (G : H)o(H, *)$$

□

定理 1.1.37. 群 $(G, *)$ において、群論に関する Lagrange の定理より直ちに次のことが分かる。

- 有限群 $(G, *)$ の任意の部分群 $(H, *)$ の位数 $o(H, *)$ はその群 $(G, *)$ の位数 $o(G, *)$ の約数である。
- $(G : G) = 1$ が成り立つ。

[*2] 集合 Λ_n は 1 から自然数 n までの自然数全体の集合という意味です。ですので、$\Lambda_0 = \emptyset$ となります。

- $\left(G:\left\{1_{(G,*)}\right\}\right)=o(G,*)$ が成り立つ。

証明. 有限群 $(G,*)$ の任意の部分群 $(H,*)$ の位数 $o(H,*)$ はその群 $(G,*)$ の位数 $o(G,*)$ の約数であることは群論に関する Lagrange の定理より明らかである。また、群論に関する Lagrange の定理より $o(G,*)=(G:G)o(G,*)$ が成り立ち、両辺に $o(G,*)$ で割れば、$(G:G)=1$ が得られる。また、$o\left(\left\{1_{(G,*)}\right\},*\right)=1$ が成り立つので、群論に関する Lagrange の定理より $o(G,*)=\left(G,\left\{1_{(G,*)}\right\}\right)o\left(\left\{1_{(G,*)}\right\},*\right)=\left(G,\left\{1_{(G,*)}\right\}\right)$ が得られる。 □

定理 1.1.38. 群 $(G,*)$ の 2 つの部分群たち $(H,*)$、$(I,*)$ が与えられ $H\subseteq I$ が成り立ちその部分群 $(I,*)$ のその群 $(G,*)$ における指数 $(G:I)$、その部分群 $(H,*)$ のその群 $(I,*)$ における指数 $(I:H)$ がともに有限であるとする[*3]。このとき、その部分群 $(H,*)$ のその群 $(G,*)$ における指数 $(G:H)$ は有限で次式が成り立つ。

$$(G:H)=(G:I)(I:H)$$

証明. 群 $(G,*)$ の 2 つの部分群たち $(H,*)$、$(I,*)$ が与えられ $H\subseteq I$ が成り立ちその部分群 $(I,*)$ のその群 $(G,*)$ における指数 $(G:I)$、その部分群 $(H,*)$ のその群 $(I,*)$ における指数 $(I:H)$ がともに有限であるとする。このとき、群論に関する Lagrange の定理より次式が成り立つ。

$$\begin{cases} o(G,*)=(G:H)o(H,*) \\ o(G,*)=(G:I)o(I,*) \\ o(I,*)=(I:H)o(H,*) \end{cases}$$

したがって、$o(G,*)$ と $o(H,*)$、$o(I,*)$ を消去していけば、次のようになり、

$$\begin{aligned} \begin{cases} o(G,*)=(G:H)o(H,*) \\ o(G,*)=(G:I)o(I,*) \\ o(I,*)=(I:H)o(H,*) \end{cases} &\Rightarrow \begin{cases} (G:H)o(H,*)=(G:I)o(I,*) \\ o(I,*)=(I:H)o(H,*) \end{cases} \\ &\Rightarrow (G:H)o(H,*)o(I,*)=(G:I)o(I*)(I:H)o(H,*) \\ &\Leftrightarrow (G:H)o(H,*)o(I,*)=(G:I)(I:H)o(I,*)o(H,*) \\ &\Leftrightarrow (G:H)=(G:I)(I:H) \end{aligned}$$

よって、その部分群 $(H,*)$ のその群 $(G,*)$ における指数 $(G:H)$ は有限であることが分かる。 □

定理 1.1.39. 群 $(G,*)$ の 2 つの部分群たち $(H,*)$、$(I,*)$ が与えられその部分群 $(H,*)$ のその群 $(G,*)$ における指数 $(G:H)$ が有限であるとする。このとき、その部分群 $(H\cap I,*)$ の[*4]その群 $(G,*)$ における指数 $(G:H\cap I)$、その部分群 $(I,*)$ における指数 $(I:H\cap I)$ はいずれも有限で次式が成り立つ[*5]。

$$(I:H\cap I)\leq(G:H\cap I)\leq(G:H)$$

証明. 群 $(G,*)$ の 2 つの部分群たち $(H,*)$、$(I,*)$ が与えられその部分群 $(H,*)$ のその群 $(G,*)$ における指数 $(G:H)$ が有限であるとする。このとき、次式のような写像 f が考えられれば、

$$f:G/_l(H\cap I)\to G/_lH;a*(H\cap I)\mapsto a*H$$

[*3] 疑い深くなっちゃうとついつい見落としがちですが、定理 1.1.7 から分かるようにその部分群 $(H,*)$ はその部分群 $(I,*)$ の部分群でもあることに注意してください…。

[*4] このことは定理 1.1.10 によって保障されますので、ご安心ください。

[*5] 証明で少し自信がないので、間違っていたらご一報ください…。

この写像 f は単射であるから、$\#G/_l(H\cap I)\leq \#G/_lH$ が成り立ち、これにより、$(G:H\cap I)\leq (G:H)$ が成り立つことになる。

ここで、その部分群 $(H\cap I,*)$ を法とするその部分群 $(I,*)$ の左剰余類たち全体の集合を $I/_l(H\cap I)$ とおくと、$I/_l(H\cap I)\subseteq G/_l(H\cap I)$ が成り立つので、$\#I/_l(H\cap I)\leq \#G/_l(H\cap I)$ が成り立ち、これにより、$(I:H\cap I)\leq (G:H\cap I)$ が成り立つことになる。

以上より、次式が得られ、

$$(I:H\cap I)\leq (G:H\cap I)\leq (G:H)$$

よって、その部分群 $(H\cap I,*)$ のその群 $(G,*)$ における指数 $(G:H\cap I)$、その部分群 $(I,*)$ における指数 $(I:H\cap I)$ はいずれも有限であることが分かる。 □

定理 1.1.40 (群論に関する Poincaré の定理)**.** $\forall i\in \Lambda_n$ に対し、群 $(G,*)$ の部分群たち $(H_i,*)$ が与えられどの部分群 $(H_i,*)$ のその群 $(G,*)$ における指数 $(G:H_i)$ も有限であるとする。このとき、その部分群 $\left(\bigcap_{i\in\Lambda_n}H_i,*\right)$ のその群 $(G,*)$ における指数 $\left(G:\bigcap_{i\in\Lambda_n}H_i\right)$ も有限であり次式が成り立つ。

$$\left(G:\bigcap_{i\in\Lambda_n}H_i\right)\leq\prod_{i\in\Lambda_n}(G:H_i)$$

この定理を群論に関する Poincaré の定理という。

証明. $\forall i\in\Lambda_n$ に対し、群 $(G,*)$ の部分群たち $(H_i,*)$ が与えられどの部分群 $(H_i,*)$ のその群 $(G,*)$ における指数 $(G:H_i)$ も有限であるとする。$n=1$ のときは明らかにその部分群 $(H_1,*)$ のその群 $(G,*)$ における指数 $(G:H_1)$ も有限であり次式が成り立つ。

$$(G:H_1)\leq (G:H_1)$$

$n=k$ のとき、定理 1.1.10 より数学的帰納法でその組 $\left(\bigcap_{i\in\Lambda_k}H_i,*\right)$ はその群 $(G,*)$ の部分群をなすことが保証される。ここで、その部分群 $\left(\bigcap_{i\in\Lambda_k}H_i,*\right)$ のその群 $(G,*)$ における指数 $\left(G:\bigcap_{i\in\Lambda_k}H_i\right)$ も有限であり次式が成り立つと仮定しよう。

$$\left(G:\bigcap_{i\in\Lambda_k}H_i\right)\leq\prod_{i\in\Lambda_k}(G:H_i)$$

$n=k+1$ のとき、$\bigcap_{i\in\Lambda_{k+1}}H_i\subseteq\bigcap_{i\in\Lambda_k}H_i$ が成り立つので、定理 1.1.38 より次のようになり、

$$\left(G:\bigcap_{i\in\Lambda_{k+1}}H_i\right)=\left(G:\bigcap_{i\in\Lambda_k}H_i\right)\left(\bigcap_{i\in\Lambda_k}H_i:\bigcap_{i\in\Lambda_{k+1}}H_i\right)$$

ここで、仮定より次のようになる。

$$\begin{aligned}\left(G:\bigcap_{i\in\Lambda_{k+1}}H_i\right)&=\left(G:\bigcap_{i\in\Lambda_k}H_i\right)\left(\bigcap_{i\in\Lambda_k}H_i:\bigcap_{i\in\Lambda_{k+1}}H_i\right)\\&\leq\prod_{i\in\Lambda_k}(G:H_i)\left(\bigcap_{i\in\Lambda_k}H_i:\bigcap_{i\in\Lambda_{k+1}}H_i\right)\end{aligned}$$

ここで、定理 1.1.39 より次式が成り立つので、

$$\begin{aligned}\left(\bigcap_{i\in\Lambda_k} H_i : \bigcap_{i\in\Lambda_{k+1}} H_i\right) &= \left(\bigcap_{i\in\Lambda_k} H_i : \bigcap_{i\in\Lambda_k} H_i \cap H_{k+1}\right)\\ &\leq (G : H_{k+1})\end{aligned}$$

したがって、次式が成り立つ。

$$\begin{aligned}\left(G : \bigcap_{i\in\Lambda_{k+1}} H_i\right) &\leq \prod_{i\in\Lambda_k} (G : H_i)\left(\bigcap_{i\in\Lambda_k} H_i : \bigcap_{i\in\Lambda_{k+1}} H_i\right)\\ &\leq \prod_{i\in\Lambda_k} (G : H_i)\,(G : H_{k+1})\\ &= \prod_{i\in\Lambda_{k+1}} (G : H_i)\end{aligned}$$

このとき、その部分群 $\left(\bigcap_{i\in\Lambda_{k+1}} H_i, *\right)$ のその群 $(G, *)$ における指数 $\left(G : \bigcap_{i\in\Lambda_{k+1}} H_i\right)$ も有限であることが分かる。

以上より、数学的帰納法によってその部分群 $\left(\bigcap_{i\in\Lambda_n} H_i, *\right)$ のその群 $(G, *)$ における指数 $\left(G : \bigcap_{i\in\Lambda_n} H_i\right)$ も有限であり次式が成り立つことが示された。

$$\left(G : \bigcap_{i\in\Lambda_n} H_i\right) \leq \prod_{i\in\Lambda_n} (G : H_i)$$

□

定理 1.1.41. 群 $(G, *)$ の正規部分群 $(N, *)$ を法とする商群 $(G/N, *)$ が与えられたとき、その正規部分群 $(N, *)$ のその群 $(G, *)$ における指数 $(G : N)$ が有限であるなら、次のことが満たされる。

- その商群 $(G/N, *)$ の位数 $o\,(G/N, *)$ も有限で $o\,(G/N, *) = (G : N)$ が成り立つ。
- その群 $(G, *)$ の位数 $o(G, *)$ が有限であるとき、次式が成り立つ。

$$o\,(G/N, *) = \frac{o(G, *)}{o(N, *)}$$

証明. 群 $(G, *)$ の正規部分群 $(N, *)$ を法とする商群 $(G/N, *)$ が与えられたとき、その正規部分群 $(N, *)$ のその群 $(G, *)$ における指数 $(G : N)$ が有限であるなら、その指数 $(G : N)$ は定義よりその部分群 $(N, *)$ を法とするその群 $(G, *)$ の左剰余類たち全体の集合 $G/_l N$ の濃度であるから、$\#G/_l N = (G : N)$ が成り立つ。一方で、その部分群 $(N, *)$ は正規であるから、その部分群 $(N, *)$ を法とするその群 $(G, *)$ の左剰余類たちは剰余類たちでもあるので、$G/_l N = G/N$ が成り立ち、したがって、次式が得られる。

$$\begin{aligned}o\,(G/N, *) &= \#G/N\\ &= \#G/_l N\\ &= (G : N)\end{aligned}$$

これにより、その商群 $(G/N, *)$ の位数 $o\,(G/N, *)$ も有限であることも分かる。

その群 $(G, *)$ の位数 $o(G, *)$ が有限であるとき、群論に関する Lagrange の定理より次式が成り立つ。

$$o(G, *) = (G : N)o(N, *)$$

ここで、上記の議論により $o\left(G/N,*\right)=\left(G:N\right)$ が成り立つので、次式が得られる。

$$\begin{aligned} o\left(G/N,*\right) &= \left(G:N\right) \\ &= \frac{\left(G:N\right)\cdot o(N,*)}{o(N,*)} \\ &= \frac{o(G,*)}{o(N,*)} \end{aligned}$$

□

1.1.7　群の位数に関する積の法則

定理 1.1.42 (群の位数に関する積の法則)**.** 群 $(G,*)$ の有限な部分群たち $(H,*)$、$(I,*)$ が与えられたとき、次式が成り立つ。

$$\#H*I=\frac{o(H,*)o(I,*)}{o(H\cap I,*)}$$

この定理を群の位数に関する積の法則という。

証明. 群 $(G,*)$ の有限な部分群たち $(H,*)$、$(I,*)$ が与えられたとき、集合 $H\times I$ 上で次の関係 R を定義すると、

$$(h,i)R\left(h',i'\right)\Leftrightarrow h*i=h'*i'$$

この関係 R は同値関係となる。実際、$h*i=h*i$ より $(h,i)R(h,i)$ が成り立つし、$h*i=h'*i'$ が成り立つならそのときに限り、$h'*i'=h*i$ が成り立つことにより $(h,i)R\left(h',i'\right)$ が成り立つなら、$\left(h',i'\right)R(h,i)$ が成り立つし、$(h,i)R\left(h',i'\right)$ かつ $\left(h',i'\right)R\left(h'',i''\right)$ が成り立つなら、$h*i=h'*i'=h''*i''$ が成り立つので、したがって、$(h,i)R\left(h'',i''\right)$ が成り立つことになる。これにより、商集合 $(H\times I)/R$ が定義されて次式が成り立つ。

$$H\times I=\bigsqcup(H\times I)/R$$

ここで、次のように写像 f が考えられれば、

$$f:H*I\to(H\times I)/R;h*i\mapsto C_R(h,i)$$

$\forall h*i\in H*I$ に対し、$h*i=h'*i'$ とおかれれば、$(h,i)R\left(h',i'\right)$ が成り立つので、次のようになる。

$$\begin{aligned} C_R(h,i) &= \{(h'',i'')\in H\times I|(h'',i'')\,R(h,i)\wedge(h,i)R\left(h',i'\right)\} \\ &= \{(h'',i'')\in H\times I|(h'',i'')\,R\left(h',i'\right)\wedge\left(h',i'\right)R(h,i)\} \\ &= C_R\left(h',i'\right) \end{aligned}$$

したがって、その対応 f は確かに写像となる。ここで、次のような写像 g が考えられよう。

$$g:(H\times I)/R\to H*I;C_R(h,i)\mapsto h*i$$

上と同様にして考えれば、これ g も確かに写像で、$\forall h*i\in H*I$ に対し、次のようになるかつ、

$$g\circ f(h*i)=g\left(C_R(h,i)\right)=h*i$$

$\forall C_R(h,i) \in (H \times I)/R$ に対し、次のようになるので、

$$f \circ g\left(C_R(h,i)\right) = f(h * i) = C_R(h,i)$$

$g = f^{-1}$ が成り立つ。これにより、$\#H * I = \#(H \times I)/R$ が成り立つ。

$\forall (h,i), (h',i') \in H \times I$ に対し、$(h,i)R\,(h',i')$ が成り立つなら、$h * i = h' * i'$ が成り立ち、したがって、次式が成り立つので、

$$\begin{aligned} h^{-1} * h' &= 1_{(G,*)} * h^{-1} * h' \\ &= i * i^{-1} * h^{-1} * h' \\ &= i * (h * i)^{-1} * h' \\ &= i * (h' * i')^{-1} * h' \\ &= i * i'^{-1} * h'^{-1} * h' \\ &= i * i'^{-1} * 1_{(G,*)} \\ &= i * i'^{-1} \end{aligned}$$

$h^{-1} * h' = i * i'^{-1}$ が得られる。ここで、$h^{-1} * h' \in H$ かつ $i * i'^{-1} \in I$ が成り立つので、$h^{-1} * h' \in H \cap I$ が得られる。逆に、$\forall j \in H \cap I$ に対し、$(h',i') = \left(h * j, j^{-1} * i\right)$ とおかれれば、$j = h^{-1} * h' = i * i^{-1}$ が成り立つので、次のようになることから、

$$\begin{aligned} h * i &= \left(i^{-1} * h^{-1}\right)^{-1} \\ &= \left(i^{-1} * h^{-1} * 1_{(G,*)}\right)^{-1} \\ &= \left(i^{-1} * h^{-1} * h' * h'^{-1}\right)^{-1} \\ &= \left(i^{-1} * i * i'^{-1} * h'^{-1}\right)^{-1} \\ &= \left(1_{(G,*)} * i'^{-1} * h'^{-1}\right)^{-1} \\ &= \left(i'^{-1} * h'^{-1}\right)^{-1} \\ &= h' * i' \end{aligned}$$

$(h,i)R\,(h',i')$ が成り立ち、よって、$(h',i') \in C_R(h,i)$ が成り立つ。

そこで、$\forall (h,i) \in H \times I$ に対し、次のように写像たち f'、g' が定義されれば、

$$f' : C_R(h,i) \to H \cap I; (h',i') \mapsto h^{-1} * h'$$

$$g' : H \cap I \to C_R(h,i); j \mapsto \left(h * j, j^{-1} * i\right)$$

$\forall\, (h',i') \in C_R(h,i)$ に対し、$(h,i)R\,(h',i')$ が成り立つので、$h * i = h' * i'$ が成り立ち、上と同様にして考えれば、$f'\,(h',i') = h^{-1} * h' = i * i'^{-1}$ が成り立つ。したがって、次のようになるかつ、

$$\begin{aligned} g' \circ f'\,(h',i') &= g'\left(h^{-1} * i'\right) \\ &= \left(h * h^{-1} * h', \left(h^{-1} * h'\right)^{-1} * h_2\right) \\ &= \left(h * h^{-1} * h', \left(i * i'^{-1}\right)^{-1} * h_2\right) \end{aligned}$$

$$
\begin{aligned}
&= \left(h * h^{-1} * h', i' * i^{-1} * h_2\right) \\
&= \left(1_{(G,*)} * h', i' * 1_{(G,*)}\right) \\
&= (h', i')
\end{aligned}
$$

$\forall h \in H \cap I$ に対し、次のようになることから、

$$
\begin{aligned}
f' \circ g'(j) &= f'\left(h * j, j^{-1} * i\right) \\
&= h^{-1} * h * j \\
&= 1_{(G,*)} * j = j
\end{aligned}
$$

$g' = {f'}^{-1}$ が成り立つ。これにより、$\#C_R(h,i) = \#H \cap I$ が成り立つ。

以上の議論と定理 1.1.35 より次式が成り立つ。

$$
\begin{aligned}
o(H,*) \cdot o(I,*) &= \#H\#I \\
&= \#H \times I \\
&= \#\bigsqcup (H \times I)/R \\
&= \# \bigsqcup_{C_R(h,i) \in (H \times I)/R} C_R(h,i) \\
&= \sum_{C_R(h,i) \in (H \times I)/R} \#C_R(h,i) \\
&= \sum_{C_R(h,i) \in (H \times I)/R} \#H \cap I \\
&= \sum_{C_R(h,i) \in (H \times I)/R} o(H \cap I, *) \\
&= \#(H \times I)/R \cdot o(H \cap I, *) \\
&= \#H * I \cdot o(H \cap I, *)
\end{aligned}
$$

よって、次式が成り立つ。

$$
\#H * I = \frac{o(H,*)o(I,*)}{o(H \cap I, *)}
$$

□

定理 1.1.43. 有限な群 $(G,*)$ の部分群たち $(H,*)$、$(I,*)$ が与えられたとき、$\sqrt{o(G,*)} < o(H,*)$ かつ $\sqrt{o(G,*)} < o(I,*)$ が成り立つなら、$H \cap I \neq \left\{1_{(G,*)}\right\}$ が成り立つ。

証明. 有限な群 $(G,*)$ の部分群たち $(H,*)$、$(I,*)$ が与えられたとき、$\sqrt{o(G,*)} < o(H,*)$ かつ $\sqrt{o(G,*)} < o(I,*)$ が成り立つなら、$H * I \subseteq G$ が成り立つので、次のようになる。

$$
\begin{aligned}
\frac{o(G,*)}{o(H \cap I, *)} &< \frac{o(H,*)o(I,*)}{o(H \cap I, *)} \\
&= \#H * I \\
&\leq \#G = o(G,*)
\end{aligned}
$$

これにより、$1 < o(H \cap I, *)$ が得られるので、$H \cap I \neq \left\{1_{(G,*)}\right\}$ が成り立つ。 □

1.1.8　さまざまな正規部分群

定義 1.1.15. 任意の群 $(G,*)$ に対し、集合 G の全ての元と可換であるようなその集合 G の元全体の集合、即ち、$\forall a \in G$ に対し、$a*z = z*a$ が成り立つようなその集合 G の元 z 全体の集合を群 $(G,*)$ の群論上中心、または、中心といい $Z(G)$ と書く。

定理 1.1.44. 組 $(Z(G),*)$ はその群 $(G,*)$ の正規部分群である、即ち、$(Z(G),*) \trianglelefteq (G,*)$ が成り立つ。

証明. 群 $(G,*)$ が与えられたとき、これの群論上中心 $Z(G)$ を用いた組 $(Z(G),*)$ について、この群論上中心 $Z(G)$ はその集合 G の部分集合であり、$\forall x,y \in Z(G) \forall a \in G$ に対し、次式が成り立つことにより、

$$\begin{aligned} a*(x*y) &= (a*x)*y \\ &= (x*a)*y \\ &= x*(a*y) \\ &= x*(y*a) \\ &= (x*y)*a \end{aligned}$$

$x*y \in Z(G)$ が成り立ち、さらに、次式が成り立つことにより、

$$\begin{aligned} a*x^{-1} &= (e*a)*x^{-1} \\ &= \left(\left(x^{-1}*x\right)*a\right)*x^{-1} \\ &= x^{-1}*\left((x*a)*x^{-1}\right) \\ &= x^{-1}*\left(a*\left(x*x^{-1}\right)\right) \\ &= x^{-1}*\left(a*1_{(G,*)}\right) \\ &= x^{-1}*a \end{aligned}$$

$x^{-1} \in Z(G)$ が成り立つので、組 $(Z(G),*)$ はその群 $(G,*)$ の部分群となる。また、次式が成り立つので、

$$\begin{aligned} a*Z(G) &= \{a*z \in G | z \in Z(G)\} \\ &= \{z*a \in G | z \in Z(G)\} \\ &= Z(G)*a \end{aligned}$$

その部分群 $(Z(G),*)$ は群 $(G,*)$ の正規部分群である。 □

定義 1.1.16. 群 $(G,*)$ において、その集合 G の元々 a、b を用いて $a*b*a^{-1}*b^{-1}$ の形で書かれる元を群 $(G,*)$ の交換子といい、これらからなる集合によって生成されるその群 $(G,*)$ の部分群 $(H,*)$ をその群 $(G,*)$ の交換子群といい、$(D(G),*)$ と書く。

定理 1.1.45. これについて次のことが成り立つ。

- 群 $(G,*)$ の交換子の逆元も群 $(G,*)$ の交換子である。
- 群 $(G,*)$ が可換的であるなら、その群 $(G,*)$ の交換子群は単位群である。
- 群 $(G,*)$ の部分群 $(N,*)$ とその群 $(G,*)$ の交換子群 $(D(G),*)$ が与えられたとき、$D(G) \subseteq N$ が成り立つなら、$(N,*) \trianglelefteq (G,*)$ が成り立つ。
- $(D(G),*) \trianglelefteq (G,*)$ が成り立つ。

証明. 群 $(G,*)$ において、その集合 G の元々 a、b を用いた交換子 $a*b*a^{-1}*b^{-1}$ の逆元について考えよう。このとき、次のようになる。

$$\begin{aligned}\left(a*b*a^{-1}*b^{-1}\right)^{-1} &= \left(b^{-1}\right)^{-1}*\left(a^{-1}\right)^{-1}*b^{-1}*a^{-1}\\ &= b*a*a^{-1}*b^{-1}\end{aligned}$$

以上より、その群 $(G,*)$ の交換子の逆元もその群 $(G,*)$ の交換子である。

群 $(G,*)$ が可換的であるなら、その集合 G の元々 a、b を用いた交換子 $a*b*a^{-1}*b^{-1}$ について、次のようになる。

$$\begin{aligned}a*b*a^{-1}*b^{-1} &= (a*b)*\left(b^{-1}*a^{-1}\right)\\ &= a*\left(b*b^{-1}\right)*a^{-1}\\ &= a*1_{(G,*)}*a^{-1}\\ &= a*a^{-1} = 1_{(G,*)}\end{aligned}$$

したがって、集合 $\left\{1_{(G,*)}\right\}\cup\left\{1_{(G,*)}^{-1}\right\}$ の有限個の元たちの算法 $*$ の像全体の集合は $\left\{1_{(G,*)}\right\}$ であり、その組 $\left(\left\{1_{(G,*)}\right\},*\right)$ も部分群であるから、その群 $(G,*)$ の交換子群は単位群である。

群 $(G,*)$ の部分群 $(N,*)$ とその群 $(G,*)$ の交換子群 $(D(G),*)$ が与えられたとき、$D(G)\subseteq N$ が成り立つなら、集合 N はその群 $(G,*)$ の全ての交換子を含み、$\forall a\in G\forall n\in N$ に対し、$a*n*a^{-1}*n^{-1}$ は、その組 $(N,*)$ が群 $(G,*)$ の部分群であるので、集合 N の元であり次のようになる。

$$\begin{aligned}\left(a*n*a^{-1}*n^{-1}\right)*n &= \left(a*n*a^{-1}\right)*\left(n^{-1}*n\right)\\ &= \left(a*n*a^{-1}\right)*1_{(G,*)}\\ &= a*n*a^{-1}\in N\end{aligned}$$

よって、定理 1.1.27 より $(N,*)\trianglelefteq(G,*)$ が成り立つ。

特に、$D(G)\subseteq Z(G)$ が成り立つかつ、上記の議論によりその部分群 $(Z(G),*)$ は群 $(G,*)$ について正規であったので、$(D(G),*)\trianglelefteq(G,*)$ が成り立つ。 □

定理 1.1.46. 群 $(G,*)$ の部分群 $(N,*)$ が与えられたとき、$(G:N)=2$ が成り立つなら、$(N,*)\trianglelefteq(G,*)$ が成り立つ。

証明. 群 $(G,*)$ の部分群 $(N,*)$ が与えられたとき、$(G:N)=2$ が成り立つなら、その部分群 $(N,*)$ を法とする左剰余類が 2 つしかないことになる。このようなものうち 1 つはその集合 N 自身であるので、残り 1 つの左剰余類が $a*N$ とおかれることにする。このとき、次のようになることから、

$$\begin{aligned}G &= \bigsqcup G/\equiv_l \mod(N,*)\\ &= \bigsqcup G/_lN\\ &= \bigsqcup_{C\in G/_lN} C\\ &= N\sqcup a*N\end{aligned}$$

$\forall b\in G$ に対し、$b\in N$ が成り立つ場合と $b\in a*N$ が成り立つ場合と場合分けができる。

$b \in N$ が成り立つ場合、$\forall n \in N$ に対し、$b^{-1} * n * b \in N$ が成り立つので、定理 1.1.24 より $(N, *) \trianglelefteq (G, *)$ が成り立つ。

$b \in a * N$ が成り立つ場合、$a^{-1} * b \in N$ が成り立つことになる。$(N, *) \trianglelefteq (G, *)$ が成り立たないと仮定すると、定理 1.1.27 より $\exists n \in N$ に対し、$b * n * b^{-1} \in N$ が成り立たない。ここで、$G = N \sqcup a * N$ より $b * n * b^{-1} \in a * N$ が成り立つことになるので、$a^{-1} * b * n * b^{-1} \in N$ が成り立ち、したがって、次のようになる。

$$\begin{aligned}\left(a^{-1} * b * n * b^{-1}\right)^{-1} * \left(a^{-1} * b\right) * n &= b * n^{-1} * \left(a^{-1} * b\right)^{-1} * \left(a^{-1} * b\right) * n \\ &= b * n^{-1} * 1_{(G,*)} * n \\ &= b * n^{-1} * n \\ &= b * 1_{(G,*)} = b\end{aligned}$$

これにより、$b = \left(a^{-1} * b * n * b^{-1}\right)^{-1} * \left(a^{-1} * b\right) * n \in N$ が成り立つことになるので、$G = N \sqcup a * N$ より $b \in a * N$ が成り立たない。しかしながら、これは仮定の $b \in a * N$ が成り立つことに矛盾する。ゆえに、$(N, *) \trianglelefteq (G, *)$ が成り立つ。 □

定義 1.1.17. 群 $(G, *)$ において、空集合でない任意のその集合 G の部分集合 S に対し、$a * S = S * a$ なる元 a 全体の集合を $N(G, S)$、$\forall s \in S$ に対し、$a * s = s * a$ が成り立つような元 a 全体の集合を $C(G, S)$ とおく。このとき、のちに述べるようにそれらの組々 $(N(G, S), *)$、$(C(G, S), *)$ はその群 $(G, *)$ の部分群をなすことから、これらの部分群たち $(N(G, S), *)$、$(C(G, S), *)$ をその群 $(G, *)$ の正規化群、中心化群という。

定理 1.1.47. 群 $(G, *)$ と空集合でない任意のその集合 G の部分集合 S が与えられたとき、それらの組々 $(N(G, S), *)$、$(C(G, S), *)$ はその群 $(G, *)$ の部分群をなす。

証明. 群 $(G, *)$ と空集合でない任意のその集合 G の部分集合 S が与えられたとき、その組 $(N(G, S), *)$ について、もちろん、$1_{(G,*)} * S = S * 1_{(G,*)} = S$ が成り立つので、$1_{(G,*)} \in N(G, S)$ が成り立つ。$\forall a, b \in N(G, S)$ に対し、$a * S = S * a$ かつ $b * S = S * b$ が成り立つことから、$\forall c \in G$ に対し、$c \in a * b * S$ が成り立つならそのときに限り、$\exists s \in S$ に対し、$c = a * b * s$ が成り立つ。これが成り立つならそのときに限り、$b * s \in b * S = S * b$ より $\exists s' \in S$ に対し、$b * s = s' * b$ が成り立つので、$c = a * s' * b$ が成り立つ。同様にして、$\exists s'' \in S$ に対し、$c = s'' * a * b$ が成り立つことが示されるので、これが成り立つならそのときに限り、$c \in S * a * b$ が成り立つ。以上より、$a * b * S = S * a * b$ が得られたので、$a * b \in N(G, S)$ が成り立つ。さらに、$\forall a \in N(G, S)$ に対し、$a * S = S * a$ が成り立つことから、$\forall c \in G$ に対し、$c \in a^{-1} * S$ が成り立つならそのときに限り、$\exists s \in S$ に対し、$c = a^{-1} * s$ が成り立つ。ここで、$a * S = S * a$ より $\exists s' \in S$ に対し、$s * a = a * s'$ が成り立つので、次のようになる。

$$\begin{aligned}c &= a^{-1} * s \\ &= a^{-1} * s * 1_{(G,*)} \\ &= a^{-1} * s * a * a^{-1} \\ &= a^{-1} * a * s' * a^{-1} \\ &= 1_{(G,*)} * s' * a^{-1} \\ &= s' * a^{-1}\end{aligned}$$

これにより、$\exists s \in S$ に対し、$c = a^{-1} * s$ が成り立つならそのときに限り、$\exists s' \in S$ に対し、$c = s' * a^{-1}$ が成

り立つので、$c \in S * a^{-1}$ が成り立つ。これにより、$a^{-1} * S = S * a^{-1}$ が得られたので、$a^{-1} \in N(G,S)$ が成り立つ。定理 1.1.6 よりその組 $(N(G,S),*)$ はその群 $(G,*)$ の部分群をなす。

その組 $(C(G,S),*)$ について、もちろん、$\forall s \in S$ に対し、$1_{(G,*)} * s = s * 1_{(G,*)}$ が成り立つので、$1_{(G,*)} \in C(G,S)$ が成り立つ。$\forall a,b \in C(G,S) \forall s \in S$ に対し、$a * s = s * a$ かつ $b * s = s * b$ が成り立つので、次のようになる。

$$\begin{aligned} a * b * s &= a * s * b \\ &= s * a * b \end{aligned}$$

以上より $a * b \in C(G,S)$ が成り立つ。$\forall a \in C(G,S) \forall s \in S$ に対し、$a * s = s * a$ が成り立つので、次のようになる。

$$\begin{aligned} a^{-1} * s &= a^{-1} * s * 1_{(G,*)} \\ &= a^{-1} * s * a * a^{-1} \\ &= a^{-1} * a * s * a^{-1} \\ &= 1_{(G,*)} * s * a^{-1} \\ &= s * a^{-1} \end{aligned}$$

以上より $a^{-1} \in C(G,S)$ が成り立つ。定理 1.1.6 よりその組 $(C(G,S),*)$ はその群 $(G,*)$ の部分群をなす。 □

定理 1.1.48. 群 $(G,*)$ と空集合でない任意のその集合 G の部分集合 S が与えられたとき、正規化群 $(N(G,S),*)$ と中心化群 $(C(G,S),*)$ について、$(C(G,S),*) \trianglelefteq (N(G,S),*)$ が成り立つ。

証明. 群 $(G,*)$ と空集合でない任意のその集合 G の部分集合 S が与えられたとき、正規化群 $(N(G,S),*)$ と中心化群 $(C(G,S),*)$ について、$\forall a \in C(G,S)$ に対し、$\forall s \in S$ に対し、$a * s = s * a$ が成り立つので、$\exists s, s' \in S$ に対し、$a * s = s' * a$ が成り立ち、したがって、$a * S = S * a$ が成り立つ。これにより、$a \in N(G,S)$ が成り立つので、$C(G,S) \subseteq N(G,S)$ が成り立つ。そこで、定理 1.1.6 よりその中心化群 $(C(G,S),*)$ はその正規化群 $(N(G,S),*)$ の部分群となる。

$\forall a \in N(G,S) \forall b \in C(G,S)$ に対し、$a * S = S * a$ が成り立つかつ、$\forall s \in S$ に対し、$b * s = s * b$ が成り立つことから、$\exists s' \in S$ に対し、$a * s = s' * a$ が成り立つことにより $a^{-1} * s' = s * a^{-1}$ が成り立つので、次のようになる。

$$\begin{aligned} a^{-1} * b * a * s &= a^{-1} * b * s' * a \\ &= a^{-1} * s' * b * a \\ &= s * a^{-1} * b * a \end{aligned}$$

これにより、$a^{-1} * b * a \in C(G,S)$ が成り立つので、定理 1.1.27 より $(C(G,S),*) \trianglelefteq (N(G,S),*)$ が成り立つ。 □

定理 1.1.49. 群 $(G,*)$ とこれの部分群 $(H,*)$ が与えられたとき、正規化群 $(N(G,H),*)$ について、$(H,*) \trianglelefteq (N(G,H),*)$ が成り立つ。

証明. 群 $(G,*)$ とこれの部分群 $(H,*)$ が与えられたとき、正規化群 $(N(G,H),*)$ について、$\forall a,h \in G$ に対し、$h \in H$ が成り立つとき、$a \in h * H$ が成り立つならそのときに限り、$\exists h' \in H$ に対し、$a = h * h'$ が成り

立つ。このとき、$h*h'*h^{-1} \in H$ が成り立つので、$h'' = h*h'*h^{-1}$ とすれば、これが成り立つならそのときに限り、$\exists h'' \in H$ に対し、$a = h''*h$ が成り立ち、これが成り立つならそのときに限り、$a \in H*h$ が成り立つ。以上より $h*H = H*h$ が得られるので、$h \in N(G,H)$ が成り立つ。以上より $H \subseteq N(G,H)$ が得られる。そこで、定理 1.1.6 よりその部分群 $(H,*)$ はその正規化群 $(N(G,H),*)$ の部分群となる。

ここで、$\forall a \in N(G,H) \forall h \in H$ に対し、$a*H = H*a$ が成り立つことから、$\exists h' \in H$ に対し、$a*h' = h*a$ が成り立つので、$a^{-1}*h = h'*a^{-1}$ が得られ、したがって、次のようになる。

$$\begin{aligned} a^{-1}*h*a &= a^{-1}*a*h' \\ &= 1_{(G,*)}*h' \\ &= h' \in H \end{aligned}$$

これにより、$a^{-1}*h*a \in H$ が成り立つので、定理 1.1.27 より $(H,*) \trianglelefteq (N(G,H),*)$ が成り立つ。 □

定理 1.1.50. 群 $(G,*)$ とこれの部分群 $(H,*)$、この部分群 $(H,*)$ の正規部分群 $(N,*)$ が与えられたとき、$H \subseteq N(G,N)$ が成り立つ。

証明. 群 $(G,*)$ とこれの部分群 $(H,*)$、この部分群 $(H,*)$ の正規部分群 $(N,*)$ が与えられたとする。$\forall h \in G$ に対し、$h \in H$ が成り立つとき、$\forall a \in G$ に対し、$a \in h*N$ が成り立つならそのときに限り、$\exists n \in N$ に対し、$a = h*n$ が成り立ち、定理 1.1.27 より $h*n*h^{-1} \in N$ が成り立つので、$n' = h*n*h^{-1}$ とすれば、次のようになることから、

$$\begin{aligned} a &= h*n \\ &= h*n*1_{(G,*)} \\ &= h*n*h^{-1}*h \\ &= n'*h \end{aligned}$$

$\exists n' \in N$ に対し、$a = n'*h$ が成り立ち、これが成り立つならそのときに限り、$a \in N*h$ が成り立つ。以上より $h*N = N*h$ が成り立つので、$h \in N(G,N)$ が成り立つ。これにより、$H \subseteq N(G,N)$ が得られる。 □

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976. 新装版第 2 刷 p45-65 ISBN978-4-00-029873-5

[2] 花木章秀. ”群論”. 信州大学. http://math.shinshu-u.ac.jp/~hanaki/edu/group/group2011pre.pdf (2022-10-24 4:42 閲覧)

1.2　群準同型写像

1.2.1　群準同型写像

定義 1.2.1. 2 つの群々 $(G, *_G)$、$(H, *_H)$ について、写像 $f : G \to H$ が、$\forall a, b \in G$ に対し、次式を満たすとき、この写像 f をその群 $(G, *_G)$ からその群 $(H, *_H)$ への群準同型写像という。

$$f : G \to H; f\left(a *_G b\right) \mapsto f(a) *_H f(b)$$

定理 1.2.1. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、次のことが成り立つ。

- $f\left(1_{(G,*_G)}\right) = 1_{(H,*_H)}$ が成り立つ。
- $\forall a \in G$ に対し、$f\left(a^{-1}\right) = f(a)^{-1}$ が成り立つ。

証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、次のようになる。

$$\begin{aligned}
f\left(1_{(G,*_G)}\right) &= f\left(1_{(G,*_G)}\right) *_H 1_{(H,*_H)} \\
&= f\left(1_{(G,*_G)}\right) *_H f\left(1_{(G,*_G)}\right) *_H f\left(1_{(G,*_G)}\right)^{-1} \\
&= f\left(1_{(G,*_G)} *_G 1_{(G,*_G)}\right) *_H f\left(1_{(G,*_G)}\right)^{-1} \\
&= f\left(1_{(G,*_G)}\right) *_H f\left(1_{(G,*_G)}\right)^{-1} \\
&= 1_{(H,*_H)}
\end{aligned}$$

また、$\forall a \in G$ に対し、次のようになる。

$$\begin{aligned}
f\left(a^{-1}\right) &= f\left(a^{-1}\right) *_H 1_{(H,*_H)} \\
&= f\left(a^{-1}\right) *_H f(a) *_H f(a)^{-1} \\
&= f\left(a^{-1} *_G a\right) *_H f(a)^{-1} \\
&= f\left(1_{(G,*_G)}\right) *_H f(a)^{-1} \\
&= 1_{(H,*_H)} *_H f(a)^{-1} \\
&= f(a)^{-1}
\end{aligned}$$

□

定理 1.2.2. 3 つの群々 $(G, *_G)$、$(H, *_H)$、$(I, *_I)$ の間の 2 つの群準同型写像たち $f : G \to H$、$g : H \to I$ の合成写像 $g \circ f$ も群準同型写像である。

証明. 3 つの群々 $(G, *_G)$、$(H, *_H)$、$(I, *_I)$ の間の 2 つの群準同型写像たち $f : G \to H$、$g : H \to I$ が与えられたとき、$\forall a, b \in G$ に対し、次のようになる。

$$\begin{aligned}
g \circ f\left(a *_G b\right) &= g\left(f\left(a *_G b\right)\right) \\
&= g\left(f(a) *_H f(b)\right) \\
&= g\left(f(a)\right) *_I g\left(f(b)\right) \\
&= g \circ f(a) *_I g \circ f(b)
\end{aligned}$$

□

1.2.2 群同型写像

定義 1.2.2. 群準同型写像のうち、全射であるもの、単射であるもの、全単射であるものをそれぞれ全射群準同型写像、単射群準同型写像、群同型写像という。

定理 1.2.3. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群同型写像 $f : G \xrightarrow{\sim} H$ の逆写像 f^{-1} も群同型写像である。

証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群同型写像 $f : G \xrightarrow{\sim} H$ の逆対応 f^{-1} は写像でその逆写像 f^{-1} も全単射 $f^{-1} : H \xrightarrow{\sim} G$ であり、$\forall a, b \in H$ に対し、次のようになる。

$$\begin{aligned} f^{-1}\left(a *_H b\right) &= f^{-1}\left(f \circ f^{-1}(a) *_H f \circ f^{-1}(b)\right) \\ &= f^{-1}\left(f\left(f^{-1}(a)\right) *_H f\left(f^{-1}(b)\right)\right) \\ &= f^{-1}\left(f\left(f^{-1}(a) *_G f^{-1}(b)\right)\right) \\ &= f^{-1} \circ f\left(f^{-1}(a) *_G f^{-1}(b)\right) \\ &= f^{-1}(a) *_G f^{-1}(b) \end{aligned}$$

□

定義 1.2.3. 2 つの群々 $(G, *_G)$、$(H, *_H)$ は、その集合 G からその集合 H への群同型写像 $f : G \xrightarrow{\sim} H$ が存在するとき、群同型であるといい $(G, *_G) \cong (H, *_H)$ と書く。

定理 1.2.4. 次のことが成り立つ、即ち、その関係 $\cong$ は同値関係である。

- $(G, *_G) \cong (G, *_G)$ が成り立つ。
- $(G, *_G) \cong (H, *_H)$ が成り立つなら、$(H, *_H) \cong (G, *_G)$ も成り立つ。
- $(G, *_G) \cong (H, *_H)$ かつ $(H, *_H) \cong (I, *_I)$ が成り立つなら、$(G, *_G) \cong (I, *_I)$ も成り立つ。

これにより、群同型な 2 つの群々 $(G, *_G)$、$(H, *_H)$ を考えるとき、その集合 G からその集合 H への群同型写像 $f : G \xrightarrow{\sim} H$ を用いれば、その集合 G がその集合 H に、その集合 G の任意の元 a がその集合 H のある元 $f(a)$ に、その算法 $*_G$ からその算法 $*_H$ に名前の付け替えただけで、群としての構造が保たれることができる。

証明. 群同型な 3 つの群々 $(G, *_G)$、$(H, *_H)$、$(I, *_I)$ が与えられたとする。

その集合 G の恒等写像 I_G を考えると、次のようになり、

$$I_G\left(a *_G b\right) = a *_G b = I_G(a) *_G I_G(b)$$

恒等写像の逆写像はもとのその恒等写像自身であるので、この写像 I_G は群同型写像である。よって、$(G, *_G) \cong (G, *_G)$ が成り立つ。

$(G, *_G) \cong (H, *_H)$ が成り立つなら、その群 $(G, *_G)$ からその群 $(H, *_H)$ への群同型写像 f が存在し、群同型写像の逆対応は群同型写像であったので、その集合 H からその集合 G への群同型写像が存在し $(H, *_H) \cong (G, *_G)$ が成り立つ。

$(G, *_G) \cong (H, *_H)$ かつ $(H, *_H) \cong (I, *_I)$ が成り立つなら、その群 $(G, *_G)$ からその群 $(H, *_H)$ への群同型写像 f が存在するかつ、その群 $(H, *_H)$ からその群 $(I, *_I)$ への群同型写像 g が存在し、定理 1.2.2 よりその写像 $g \circ f$ も群準同型写像であり、定理 1.2.3 よりこれらの逆写像たち f^{-1}、g^{-1} も群同型写像たちであり、

さらに、その合成写像 $f^{-1} \circ g^{-1}$ も群準同型写像である。ここで、次のようになるので、

$$\begin{aligned}(g \circ f) \circ \left(f^{-1} \circ g^{-1}\right) &= g \circ \left(f \circ f^{-1}\right) \circ g^{-1} \\ &= g \circ I_H \circ g^{-1} \\ &= g \circ g^{-1} = I_I \\ \left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) &= f^{-1} \circ \left(g^{-1} \circ g\right) \circ f \\ &= f^{-1} \circ I_H \circ f \\ &= f^{-1} \circ f = I_G\end{aligned}$$

その写像 $f^{-1} \circ g^{-1}$ はその写像 $g \circ f$ の逆写像でありその写像 $g \circ f$ は群同型写像となる。よって、$(G, *_G) \cong (I, *_I)$ が成り立つ。 □

定理 1.2.5. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ の値域 $V(f)$ を用いた群 $(V(f), *_H)$ はその群 $(H, *_H)$ の部分群である。

証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、$f\left(1_{(G,*_G)}\right) = 1_{(H,*_H)}$ が成り立つのであったので、$1_{(H,*_H)} \in V(f)$ が成り立つ。

また、$\forall f(a), f(b) \in V(f)$ に対し、$a, b \in G$ なる元々 a、b が存在し、$f(a *_G b) = f(a) *_H f(b) \in H$ が成り立つかつ、$\forall f(a) \in V(f)$ に対し、$a \in G$ なる元 a、さらに、これの逆元 a^{-1} がその集合 G に存在し、定理 1.2.1 より $f\left(a^{-1}\right) = f(a)^{-1}$ が成り立つのであったので、$f(a)^{-1} = f\left(a^{-1}\right) \in V(f)$ が成り立つ。

以上より、定理 1.1.6 よりその群 $(H, *_H)$ をなすその集合 H のその部分集合 $V(f)$ がその算法 $*_H$ に関して部分群 $(V(f), *_H)$ をなす。 □

定義 1.2.4. 2 つの群々 $(G, *_G)$、$(H, *_H)$ について、ある単射群準同型写像 $f : G \rightarrowtail H$ が与えられたとき、その写像 f の終集合を $V(f)$ とおいた写像 $f' : G \rightarrowtail V(f)$ は明らかに全射であるので、その写像 f' は群同型写像となる。しばしば、このようなその群準同型写像 $f' : G \rightarrowtail V(f)$ をその集合 G からその集合 H の中への群同型写像という。

1.2.3 核

定義 1.2.5. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、$f(a) = 1_{(H,*_H)}$ なるその集合 G_1 の元々 a 全体の集合、即ち、その対応 f の逆対応 f^{-1} で始集合を $\left\{1_{(H,*_H)}\right\}$ としたときの値域 $V\left(f^{-1} \middle| \left\{1_{(H,*_H)}\right\}\right)$ をその写像 f の核といい、$\ker f$ などと書く、即ち、次式のように定められる。

$$\ker f = \left\{a \in G \middle| f(a) = 1_{(H,*_H)}\right\}$$

これは方程式 $f(x) = 0$ の解々全体の集合に少し似ている。

定理 1.2.6. 2 つのそれらの群々 $(G, *_G)$、$(H, *_H)$ の間の任意の群準同型写像 $f : G \to H$ の核 $\ker f$ を用いた組 $(\ker f, *_G)$ は $(\ker f, *_G) \trianglelefteq (G, *_G)$ を満たす。

証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ の核を $\ker f$ とおく。

$\forall a, b \in \ker f$ に対し、群準同型写像と核の定義より次のようになり

$$f(a *_G b) = f(a) *_H f(b)$$

$$
\begin{aligned}
&= 1_{(H,*_H)} *_H 1_{(H,*_H)} \\
&= 1_{(H,*_H)}
\end{aligned}
$$

$a *_G b \in \ker f$ が成り立つかつ、$\forall a \in \ker f$ に対し、$f\left(a^{-1}\right) = f(a)^{-1}$ が成り立つのであったので、群準同型写像と核の定義より次のようになり

$$
\begin{aligned}
f\left(a^{-1}\right) &= f(a)^{-1} \\
&= 1_{(H,*_H)}^{-1} \\
&= 1_{(H,*_H)}^{-1} *_H 1_{(H,*_H)} \\
&= 1_{(H,*_H)}
\end{aligned}
$$

$a^{-1} \in \ker f$ が成り立つ。以上より、定理 1.1.6 よりそれらの群々 $(G, *_G)$、$(H, *_H)$ の間の任意の群準同型写像 $f : G \to H$ の核 $\ker f$ はその群 $(G, *_G)$ の部分群である。

また、$\forall a \in G \forall b \in \ker f$ に対し、$f\left(a^{-1}\right) = f(a)^{-1}$ が成り立つのであったので、群準同型写像と核の定義より次のようになり

$$
\begin{aligned}
f\left(a *_G b *_G a^{-1}\right) &= f(a) *_H f(b) *_H f\left(a^{-1}\right) \\
&= f(a) *_H 1_{(H,*_H)} *_H f(a)^{-1} \\
&= f(a) *_H f(a)^{-1} \\
&= 1_{(H,*_H)}
\end{aligned}
$$

$a *_G b *_G a^{-1} \in \ker f$ が成り立つ。定理 1.1.27 より $(\ker f, *_G) \trianglelefteq (G, *_G)$ が成り立つならそのときに限り、$\forall a \in G \forall b \in \ker f$ に対し $a *_G b *_G a^{-1} \in \ker f$ が成り立つのであったので、その核 $\ker f$ を用いた組 $(\ker f, *_G)$ は $(\ker f, *_G) \trianglelefteq (G, *_G)$ が成り立つ。 □

1.2.4 自然な全射群準同型写像

定理 1.2.7 (自然な全射群準同型写像)**.** 群 $(G, *)$ の正規部分群 $(N, *)$ が与えられたとき、写像 $\varphi : G \to G/N; a \mapsto a * N$ はその群 $(G, *)$ から商群 $(G/N, *)$ への全射群準同型写像であり $\ker \varphi = N$ が成り立つ。

定義 1.2.6. このように次式のような写像 φ をその群 $(G, *)$ からその商群 $(G/N, *)$ への自然な全射群準同型写像、標準的群準同型写像という。

$$
\begin{array}{ccccc}
G & \xrightarrow{\quad\varphi\quad} & G/N & = & G/\ker\varphi \\
\cup & & \cup & & \cup \\
a & \xmapsto{\quad\varphi\quad} & a * N & = & a * \ker\varphi
\end{array}
$$

証明. 群 $(G, *)$ の正規部分群 $(N, *)$ が与えられたとき、写像 $\varphi : G \to G/N; a \mapsto a * N$ について、$\forall a, b \in G$ に対し、次のようになる。

$$
\begin{aligned}
\varphi(a * b) &= (a * b) * N \\
&= (a * b) * (N * N) \\
&= N * (a * b) * N
\end{aligned}
$$

$$
\begin{aligned}
&= (a * N) * (b * N) \\
&= \varphi(a) * \varphi(b)
\end{aligned}
$$

これにより、その写像 φ は群準同型写像である。

また、$\forall a * N$ に対し、次のようになることから、

$$
\begin{aligned}
(a * N) * \left(1_{(G,*)} * N\right) &= \varphi(a) * \varphi\left(1_{(G,*)}\right) \\
&= \varphi\left(a * 1_{(G,*)}\right) \\
&= \varphi(a) = a * N \\
\left(1_{(G,*)} * N\right) * (a * N) &= \varphi\left(1_{(G,*)}\right) * \varphi(a) \\
&= \varphi\left(1_{(G,*)} * a\right) \\
&= \varphi(a) = a * N
\end{aligned}
$$

その群 $(G/N, *)$ の単位元は $1_{(G,*)} * N$ である。したがって、$\forall a \in \ker\varphi$ に対し、次のようになる。

$$
\begin{aligned}
\varphi(a) &= a * N \\
&= 1_{(G,*)} * N \\
&= N
\end{aligned}
$$

ここで、$\forall n \in N$ に対し、$n = a * n'$ なる元 n' がその集合 N に存在し次のようになるので、

$$
\begin{aligned}
a &= a * 1_{(G,*)} \\
&= a * n' * {n'}^{-1} \\
&= n * {n'}^{-1} \in N
\end{aligned}
$$

$a \in N$ が成り立つ。逆に、$\forall a \in N$ が成り立つなら、次のようになるので、

$$
\begin{aligned}
\varphi(a) &= a * N \\
&= \{a * n \in G | n \in N\} \\
&= \{a * n \in G | a * n \in N\} \\
&= N
\end{aligned}
$$

$a \in \ker\varphi$ が成り立つ。以上より、$\ker\varphi = N$ が得られる。

最後に、$\forall a * N \in G/N$ に対し、商群の定義より明らかに $\varphi(a) = a * N$ なるその集合 G の元 a が存在するので、その写像 φ は全射である。これにより、その写像 φ は全射群準同型写像である。 □

1.2.5 群準同型定理

定理 1.2.8. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、$\forall a, b \in G$ に対し、$f(a) = f(b)$ が成り立つならそのときに限り、その群 $(G, *_G)$ の正規部分群 $(\ker f, *_G)$ を法としてその集合 G の元々 a、b が合同である、即ち、$a \equiv b \bmod (\ker f, *_G)$ が成り立つ。

証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、$\forall a, b \in G$ に対し、$f(a) = f(b)$ が成り立つなら、その群準同型写像 f の核 $\ker f$ を用いた組 $(\ker f, *_G)$ は定理 1.2.6 よりその群 $(G, *_G)$ の正規部分群であり群準同型写像と核の定義より次のようになるので、

$$
f\left(a^{-1} *_G b\right) = f\left(a^{-1}\right) *_H f(b)
$$

$$
\begin{aligned}
&= f(a)^{-1} *_H f(b) \\
&= f(b)^{-1} *_H f(b) \\
&= 1_{(H,*_H)}
\end{aligned}
$$

$a^{-1} *_G b \in \ker f$ が得られる。定理 1.1.22 よりその正規部分群 $(\ker f, *_G)$ を法としてその集合 G の元々 a、b が合同である、即ち、$a \equiv b \bmod (\ker f, *_G)$ が成り立つ。 □

定理 1.2.9. これの系として、2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ が単射であるならそのときに限り、その写像 f の核 $\ker f$ が $\ker f = \left\{1_{(G,*_G)}\right\}$ を満たす。

証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、その群 $\left(\left\{1_{(G,*_G)}\right\}, *_G\right)$ は、$1_{(G,*_G)} \in \left\{1_{(G,*_G)}\right\}$ が成り立つかつ、$1_{(G,*_G)} *_G 1_{(G,*_G)} \in \left\{1_{(G,*_G)}\right\}$ が成り立つかつ、次のようになることから、

$$
\begin{aligned}
1^{-1}_{(G,*_G)} &= 1^{-1}_{(G,*_G)} *_G 1_{(G,*_G)} \\
&= 1_{(G,*_G)}
\end{aligned}
$$

$1^{-1}_{(G,*_G)} \in \left\{1_{(G,*_G)}\right\}$ が成り立つので、定理 1.1.6 よりその群 $(G, *_G)$ の部分群で、$\forall a \in G$ に対し、次のようになるので、

$$
\begin{aligned}
1_{(G,*_G)} &= a *_G a^{-1} \\
&= a *_G 1_{(G,*_G)} *_G a^{-1} \in \left\{1_{(G,*_G)}\right\}
\end{aligned}
$$

定理 1.1.27 よりその群 $\left(\left\{1_{(G,*_G)}\right\}, *_G\right) \trianglelefteq (G, *_G)$ が成り立つ。

その写像 f の核 $\ker f$ が $\ker f = \left\{1_{(G,*_G)}\right\}$ を満たすとき、2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、定理 1.2.8 より次のようになる。

$$
\begin{aligned}
f(a) = f(b) &\Leftrightarrow a \equiv b \ \left(\bmod \left\{1_{(G,*_G)}\right\}\right) \\
&\Leftrightarrow a^{-1} *_G b \in \left\{1_{(G,*_G)}\right\} \\
&\Leftrightarrow a^{-1} *_G b = 1_{(G,*_G)} \\
&\Leftrightarrow a *_G a^{-1} *_G b = a *_G 1_{(G,*_G)} \\
&\Leftrightarrow 1_{(G,*_G)} *_G b = a *_G 1_{(G,*_G)} \\
&\Leftrightarrow a = b
\end{aligned}
$$

これにより、その写像 f は単射である。

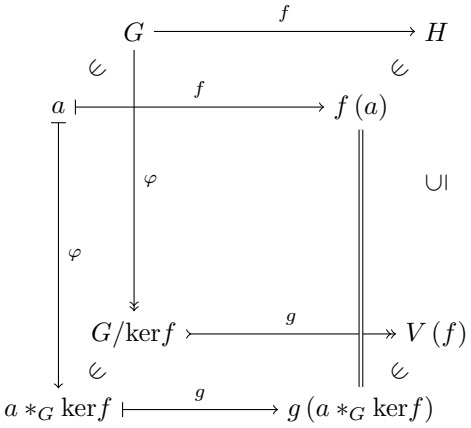
逆に、その写像 f が単射であるなら、$\forall a, b \in G$ に対し、次のようになる。

$$
\begin{aligned}
f(a) = f(b) &\Leftrightarrow a = b \\
&\Leftrightarrow a^{-1} *_G a = a^{-1} *_G b \\
&\Leftrightarrow a^{-1} *_G b = 1_{(G,*_G)} \\
&\Leftrightarrow a^{-1} *_G b \in \left\{1_{(G,*_G)}\right\} \\
&\Leftrightarrow a \equiv b \bmod \left(\left\{1_{(G,*_G)}\right\}, *_G\right)
\end{aligned}
$$

ここで、定理 1.2.8 よりその写像 f の核 $\ker f$ がその群 $(G, *_G)$ の単位元 $1_{(G,*_G)}$ のみからなる。 □

定理 1.2.10 (群準同型定理)**.** 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、写像 $g : G/\ker f \to V(f); a * \ker f \mapsto f(a)$ は群 $(G/\ker f, *_G)$ から群 $(V(f), *_H)$ への群同型写像でありこれらの 2 つの群々 $(G/\ker f, *_G)$、$(V(f), *_H)$ は群同型である、即ち、$(G/\ker f, *_G) \cong (V(f), *_H)$ が成り立つ。

この定理を群準同型定理という。この定理は、その群 $(G, *_G)$ からその商群 $(G/\ker f, *_G)$ への自然な全射群準同型写像 φ が用いられれば、次のように与えられる。



証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$ について、写像 $g : G/\ker f \to V(f); a *_G \ker f \mapsto f(a)$ が与えられるとき、$\forall a *_G \ker f, b *_G \ker f \in G/\ker f$ に対し、$a *_G \ker f = b *_G \ker f$ が成り立つなら、定理 1.2.6 より $(\ker f, *_G) \trianglelefteq (G, *_G)$ が成り立つので、$1_{(G,*_G)} \in \ker f$ に注意すれば、$a *_G 1_{(G,*_G)} \in a *_G \ker f = b *_G \ker f$ が成り立つことにより、$\exists n \in \ker f$ に対し、$a *_G 1_{(G,*_G)} = b *_G n$ が成り立つ。したがって、定理 1.1.27 より次のようになる。

$$\begin{aligned} a *_G b^{-1} &= a *_G 1_{(G,*_G)} *_G b^{-1} \\ &= b *_G n *_G b^{-1} \in b *_G \ker f *_G b^{-1} = \ker f \end{aligned}$$

ゆえに、次のようになる。

$$\begin{aligned} g(a *_G \ker f) &= f(a) \\ &= f(a) *_H 1_{(H,*_H)} \\ &= f(a) *_H f(b)^{-1} *_H f(b) \\ &= f(a) *_H f\left(b^{-1}\right) *_H f(b) \\ &= f\left(a *_G b^{-1}\right) *_H f(b) \\ &= 1_{(H,*_H)} *_H f(b) \\ &= f(b) \\ &= g(b *_G \ker f) \end{aligned}$$

ゆえに、その対応 g は写像となっている。

その値域の定義より明らかにその写像 g は全射である。また、$g(a *_G \ker f) = g(b *_G \ker f)$ が成り立つなら、群 $(\ker f, *_G)$ はその群 $(G, *_G)$ の部分群であることにより次のようになる。

$$\begin{aligned} & g(a *_G \ker f) = g(b *_G \ker f) \\ \Leftrightarrow\ & f(a) = f(b) \end{aligned}$$

$$
\begin{aligned}
&\Leftrightarrow f(a) *_H f(b)^{-1} = f(a) *_H f\left(b^{-1}\right) = f\left(a *_G b^{-1}\right) = 1_{(H,*_H)} \\
&\Leftrightarrow a *_G b^{-1} \in \ker f \\
&\Leftrightarrow \left(a *_G b^{-1}\right)^{-1} = a^{-1} *_G b \in \ker f
\end{aligned}
$$

ここで、定理 1.1.20 よりその群 $(G, *_G)$ の部分群 $(\ker f, *_G)$ について、$a^{-1} *_G b \in \ker f$ が成り立つなら、$a *_G \ker f = b *_G \ker f$ が成り立つのであったので、次のようになる。

$$
\begin{aligned}
g\left(a *_G \ker f\right) = g\left(b *_G \ker f\right) &\Leftrightarrow a^{-1} *_G b \in \ker f \\
&\Rightarrow a *_G \ker f = b *_G \ker f
\end{aligned}
$$

したがって、その写像 g は単射である。以上より、その写像 g は全単射 $g : G/\ker f \xrightarrow{\sim} V(f)$ である。

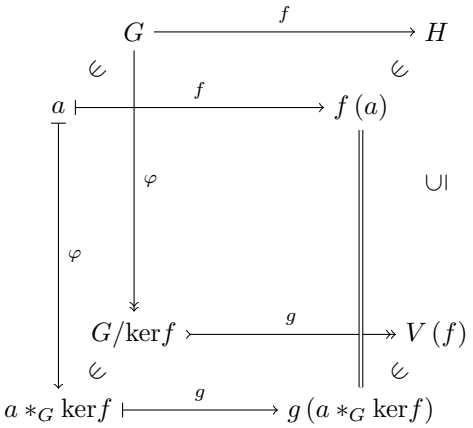
その組 $(\ker f, *_G)$ はその群 $(G, *_G)$ の正規部分群であったので、$\forall a *_G \ker f, b *_G \ker f \in G/\ker f$ に対し、次のようになる。

$$
\begin{aligned}
g\left(\left(a *_G \ker f\right) *_G \left(b *_G \ker f\right)\right) &= g\left(\ker f *_G a *_G b *_G \ker f\right) \\
&= g\left(\ker f *_G \left(a *_G b\right) *_G \ker f\right) \\
&= g\left(\left(a *_G b\right) *_G \ker f *_G \ker f\right) \\
&= g\left(\left(a *_G b\right) *_G \ker f\right) \\
&= f\left(a *_G b\right) \\
&= f(a) *_H f(b) \\
&= g\left(a *_G \ker f\right) *_H g\left(b *_G \ker f\right)
\end{aligned}
$$

これにより、その写像 g は群準同型写像であり、その写像 g は全単射だったので、その写像 g は群同型写像である。

これにより、2 つのそれらの群々 $(G/\ker f, *_G)$、$(V(f), *_H)$ は、その集合 $G/\ker f$ からその集合 $V(f)$ への群同型写像 $g : G/\ker f \to V(f)$ が存在するので、群同型である、即ち、$(G/\ker f, *_G) \cong (V(f), *_H)$ が成り立つ。

よって、その群 $(G, *_G)$ からその商群 $(G/\ker f, *_G)$ への自然な全射群準同型写像 φ が用いられれば、次のように与えられる。



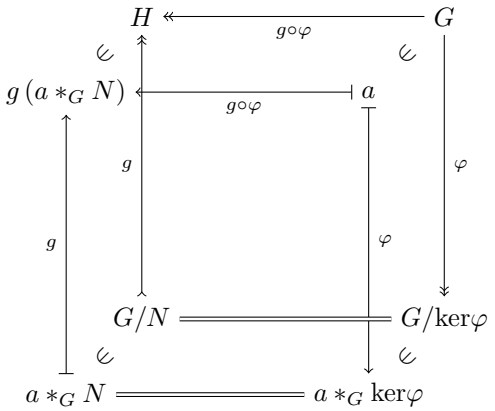
□

定義 1.2.7. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間のある全射群準同型写像 $f : G \twoheadrightarrow H$ が存在するとき、その群 $(H, *_H)$ はその群 $(G, *_G)$ の群準同型像という。

定理 1.2.11. 群 $(H, *_H)$ が群 $(G, *_G)$ の群準同型像であるならそのときに限り、その群 $(H, *_H)$ と群同型であるようなその群 $(G, *_G)$ のある商群が存在する。

証明. 定義より群 $(H, *_H)$ が群 $(G, *_G)$ の群準同型像であるならそのときに限り、それらの群々 $(G, *_G)$、$(H, *_H)$ の間の全射群準同型写像 $f : G \twoheadrightarrow H$ が存在するのであった。このとき、群準同型定理と $V(f) = H$ が成り立つことより写像 $g : G/\ker f \xrightarrow{\sim} H$ は群同型写像でありそれらの群々 $(G/\ker f, *_G)$、$(H, *_H)$ は群同型である。したがって、その群 $(H, *_H)$ と群同型であるようなその群 $(G, *_G)$ のある商群が存在する。

逆に、その群 $(H, *_H)$ と群同型であるようなその群 $(G, *_G)$ のある商群が存在するなら、その群 $(G, *_G)$ のある正規部分群 $(N, *_G)$ を用いてその商群が $(G/N, *_G)$ とおかれれば、群同型写像 $g : G/N \xrightarrow{\sim} H$ が存在できる。また、写像 $\varphi : G \to G/N; a \mapsto a *_G N$ は定理 1.2.7 より全射群準同型写像で $\ker\varphi = N$ が成り立つのであったので、次式のような写像 $g \circ \varphi$ を考えると、



これは全射群準同型写像 $g \circ \varphi : G \twoheadrightarrow H$ であるので、その群 $(H, *_H)$ はその群 $(G, *_G)$ の群準同型像である。 □

1.2.6 群同型定理

定理 1.2.12. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の全射群準同型写像 $f : G \twoheadrightarrow H$ について、その群 $(G, *_G)$ の部分群 $(I, *_G)$ と正規部分群 $(M, *_G)$ を用いた 2 つの組々 $(V(f|I), *_H)$、$(V(f|M), *_H)$ はそれぞれその群 $(H, *_H)$ の部分群、正規部分群である。

また、その群 $(H, *_H)$ の部分群 $(J, *_H)$ と正規部分群 $(N, *_H)$ を用いた 2 つの組々 $\left(V\left(f^{-1}|J\right), *_G\right)$、$\left(V\left(f^{-1}|N\right), *_G\right)$ はそれぞれその群 $(G, *_G)$ の部分群、正規部分群である。

証明. 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の全射群準同型写像 $f : G \twoheadrightarrow H$ について、その群 $(G, *_G)$ の部分群 $(I, *_G)$ と正規部分群 $(M, *_G)$ を用いた 2 つの組々 $(V(f|I), *_H)$、$(V(f|M), *_H)$ が与えられたとする。$f|I(a), f|I(b) \in V(f|I)$ のとき、定理 1.1.6 より $a, b \in I$ が成り立つなら、$a *_G b \in I$ も成り立つので、次のようになる。

$$f|I(a) *_H f|I(b) = f|I(a *_G b) \in V(f|I)$$

$f|I\left(a^{-1}\right)=f|I(a)^{-1}$ が成り立つことと定理 1.1.6 より $a\in I$ が成り立つなら、$a^{-1}\in I$ も成り立つので、次のようになる。

$$f|I(a)^{-1}=f|I\left(a^{-1}\right)\in V\left(f|I\right)$$

したがって、組 $\left(V\left(f|I\right),*_H\right)$ は定理 1.1.6 よりその群 $\left(H,*_H\right)$ の部分群である。

同様にして、群 $\left(V\left(f|M\right),*_H\right)$ はその群 $\left(H,*_H\right)$ の部分群であることが示され、$f|M\left(a^{-1}\right)=f|M(a)^{-1}$ が成り立つことと定理 1.1.27 より $h\in M$ が成り立つなら、$\forall b\in G$ に対し、$b*_G h*_G b^{-1}\in M$ も成り立つので、次のようになる。

$$\begin{aligned}f(b)*_H f|M(a)*_H f(b)^{-1}&=f(b)*_H f(a)*_H f\left(b^{-1}\right)\\&=f\left(b*_G h*_G b^{-1}\right)\in V\left(f|M\right)\end{aligned}$$

したがって、組 $\left(V\left(f|M\right),*_H\right)$ は定理 1.1.27 よりその群 $\left(H,*_H\right)$ の正規部分群である。

また、その群 $\left(H,*_H\right)$ の部分群 $\left(J,*_H\right)$ と正規部分群 $\left(N,*_H\right)$ を用いた 2 つの集合たち $V\left(f^{-1}|J\right)$、$V\left(f^{-1}|N\right)$ が与えられたとする。群準同型写像の定義と定理 1.1.6 より $a,b\in J$ が成り立つなら、$a*_H b\in J$ も成り立つので、次のようになる。

$$\begin{aligned}a,b\in V\left(f^{-1}|J\right)&\Rightarrow f(a),f(b)\in V\left(f|V\left(f^{-1}|J\right)\right)\subseteq J\\&\Rightarrow f(a)*_H f(b)=f\left(a*_H b\right)\in J\\&\Rightarrow a*_G b\in V\left(f^{-1}|J\right)\end{aligned}$$

$f\left(a^{-1}\right)=f(a)^{-1}$ が成り立つことと定理 1.1.6 より $a\in J$ が成り立つなら、$a^{-1}\in J$ も成り立つので、次のようになる。

$$\begin{aligned}a\in V\left(f^{-1}|J\right)&\Rightarrow f(a)\in V\left(f|V\left(f^{-1}|J\right)\right)\subseteq J\\&\Rightarrow f(a)^{-1}=f\left(a^{-1}\right)\in J\\&\Rightarrow a^{-1}\in V\left(f^{-1}|J\right)\end{aligned}$$

したがって、組 $\left(V\left(f^{-1}|J\right),*_G\right)$ はその群 $\left(G,*_G\right)$ の部分群である。

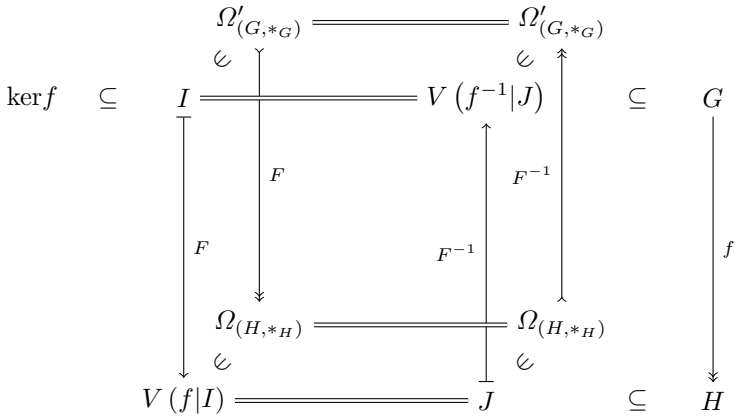
同様にして、組 $\left(V\left(f^{-1}|N\right),*_G\right)$ はその群 $\left(G,*_G\right)$ の部分群であることが示され群準同型写像の定義と $f(a)^{-1}=f\left(a^{-1}\right)$ が成り立つことと正規部分群の定義より次のようになる。

$$\begin{aligned}b\in a*_G V\left(f^{-1}|N\right)&\Leftrightarrow a^{-1}*_G b\in a^{-1}*_G a*_G V\left(f^{-1}|N\right)=1_{(G,*_G)}*_G V\left(f^{-1}|N\right)=V\left(f^{-1}|N\right)\\&\Leftrightarrow f\left(a^{-1}*_G b\right)\in V\left(f|V\left(f^{-1}|N\right)\right)\subseteq N\\&\Rightarrow f\left(a^{-1}\right)*_H f(b)=f(a)^{-1}*_H f(b)\in N\\&\Leftrightarrow f(a)*_H f(a)^{-1}*_H f(b)=1_{(H,*_H)}*_H f(b)=f(b)\in f(a)*_H N\\&\Leftrightarrow f(b)\in f(a)*_H N=N*_H f(a)\\&\Leftrightarrow f(b)*_H f(a)^{-1}\in N*_H f(a)*_H f(a)^{-1}=N*_H 1_{(H,*_H)}=N\\&\Leftrightarrow f(b)*_H f(a)^{-1}=f(b)*_H f\left(a^{-1}\right)=f\left(b*_G a^{-1}\right)\in N\\&\Leftrightarrow b*_G a^{-1}\in V\left(f^{-1}|N\right)\\&\Leftrightarrow b*_G a^{-1}*_G a=b*_G 1_{(G,*_G)}=b\in V\left(f^{-1}|N\right)*_G a\end{aligned}$$

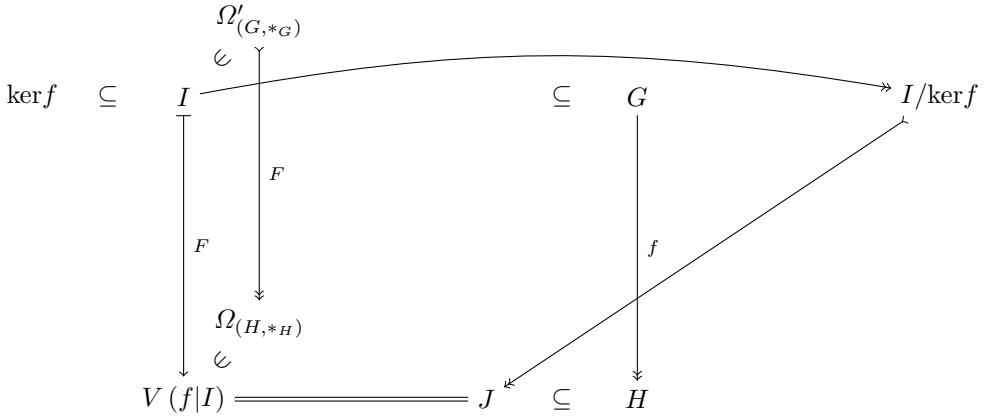
これにより、$a*_G V\left(f^{-1}|N\right)\subseteq V\left(f^{-1}|N\right)*_G a$ が成り立つ。同様にして、$a*_G V\left(f^{-1}|N\right)\supseteq V\left(f^{-1}|N\right)*_G a$ も成り立つことが示されるので、$a*_G V\left(f^{-1}|N\right)=V\left(f^{-1}|N\right)*_G a$ が成り立ち、したがって、組 $\left(V\left(f^{-1}|N\right),*_G\right)$ はその群 $\left(G,*_G\right)$ の正規部分群である。 □

定理 1.2.13 (第 1 群同型定理)**.** 2 つの群々 $(G, *_G)$、$(H, *_H)$ の間の全射群準同型写像 $f : G \twoheadrightarrow H$ について、その群 $(G, *_G)$ の部分群をなす $\ker f \subseteq I$ が成り立つようなその集合 G の部分集合全体の集合を $\Omega'_{(G,*_G)}$、その群 $(H, *_H)$ の部分群をなすその集合 H の部分集合全体の集合を $\Omega_{(H,*_H)}$ とおくと、次のことが成り立つ。

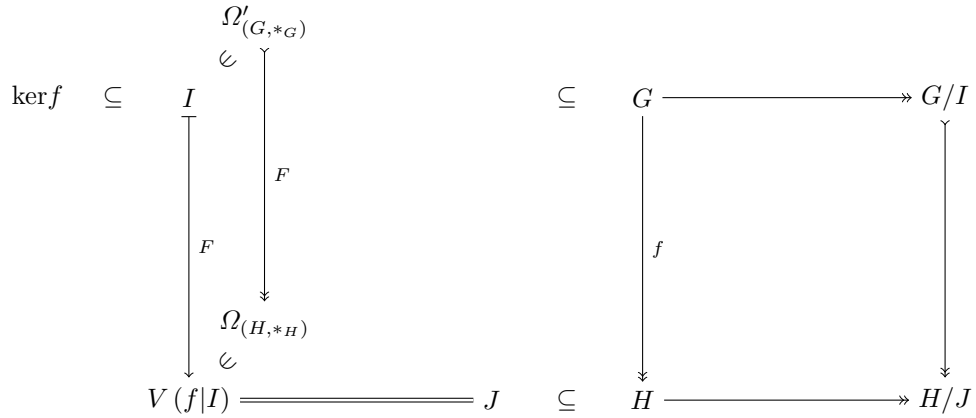
- 次式のように写像 $F : \Omega'_{(G,*_G)} \to \Omega_{(H,*_H)}; I \mapsto V(f|I)$ は全単射でその逆写像 F^{-1} が $F^{-1} : \Omega_{(H,*_H)} \to \Omega'_{(G,*_G)}; J \mapsto V\left(f^{-1}|J\right)$ と与えられる。



- $\forall I \in \Omega'_{(G,*_G)}$ に対し、$(I/\ker f, *_G) \cong (F(I), *_H)$ が成り立つ。これは次式のようにも表される。

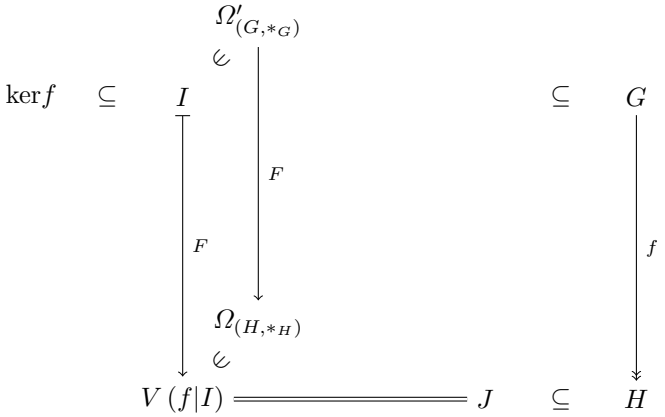


- $\forall I \in \Omega'_{(G,*_G)}$ に対し、その写像 $F : \Omega'_{(G,*_G)} \to \Omega_{(H,*_H)}; I \mapsto V(f|I)$ が与えられたとき、$(I, *_G) \trianglelefteq (G, *_G)$ が成り立つならそのときに限り、$(F(I), *_H) \trianglelefteq (H, *_H)$ が成り立つ。
- $\forall I \in \Omega'_{(G,*_G)}$ に対し、上記の写像 $F : \Omega'_{(G,*_G)} \to \Omega_{(H,*_H)}; I \mapsto V(f|I)$ が与えられたとき、$(I, *_G) \trianglelefteq (G, *_G)$ が成り立つなら、$(G/I, *_G) \cong (H/F(I), *_H)$ が成り立つ。これは次式のようにも表される。

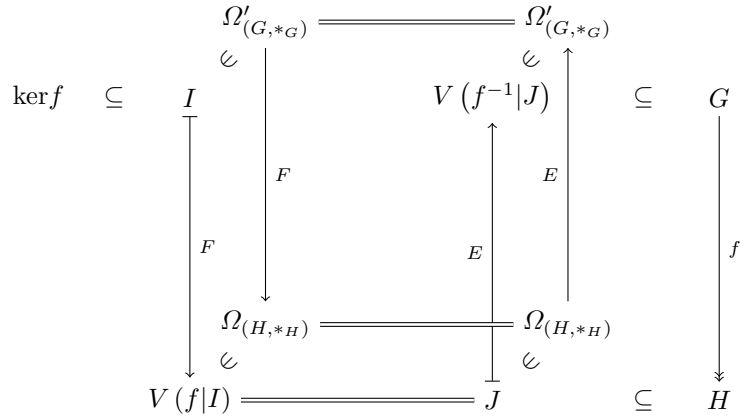


この定理を第 1 群同型定理という。

証明. 2 つの群々 $(G,*_G)$、$(H,*_H)$ の間の全射群準同型写像 $f:G\twoheadrightarrow H$ について、その群 $(G,*_G)$ の部分群をなすその集合 G のその核 $\ker f$ を含む部分集合全体の集合を $\Omega'_{(G,*_G)}$、その群 $(H,*_H)$ の部分群をなすその集合 H の部分集合全体の集合を $\Omega_{(H,*_H)}$ とおく。次式のように写像 $F:\Omega'_{(G,*_G)}\to\Omega_{(H,*_H)};I\mapsto V(f|I)=J$ を考えよう。



$\forall I\in\Omega'_{(G,*_G)}$ に対し、$V(f|I)=J$ とおくと、定理 1.2.12 よりその群 $(G,*_G)$ の部分群 $(I,*_G)$ を用いた組 $(J,*_H)$ はその群 $(H,*_H)$ の部分群であったので、$F(I)=V(f|I)\in\Omega_{(H,*_H)}$ が成り立つ。したがって、写像 $F:\Omega'_{(G,*_G)}\to\Omega_{(H,*_H)};I\mapsto V(f|I)$ が定義できている。ここで、次式のように写像 $E:\Omega_{(H,*_H)}\to\Omega'_{(G,*_G)};J\mapsto V\left(f^{-1}|J\right)=I$ を考えよう。



$\forall J \in \Omega_{(H,*_H)}$ に対し、$V\left(f^{-1}|J\right) = I$ とおくと、$\left\{1_{(H,*_H)}\right\} \subseteq J$ が成り立つことから、$\ker f = V\left(f^{-1}|\left\{1_{(H,*_H)}\right\}\right) \subseteq V\left(f^{-1}|J\right) = I$ が成り立つかつ、定理 1.2.12 よりその群 $(H,*_H)$ の部分群 $(J,*_H)$ を用いた組 $(I,*_G)$ はその群 $(G,*_G)$ の部分群であったので、$E(J) = V\left(f^{-1}|J\right) \in \Omega'_{(G,*_G)}$ が成り立つ。したがって、写像 $E : \Omega_{(H,*_H)} \to \Omega'_{(G,*_G)}; J \mapsto V\left(f^{-1}|J\right)$ が考えられることができる。

まず、$E \circ F = I_{\Omega'_{(G,*_G)}}$ が成り立つことを示そう。このとき、$\forall I \in \Omega'_{(G,*_G)}$ に対し、$V\left(f^{-1}|V\left(f|I\right)\right) \supseteq I$ は明らかに成り立つ。逆に、$\forall a \in G$ に対し、$a \in V\left(f^{-1}|V\left(f|I\right)\right)$ が成り立つなら、$V\left(f|V\left(f^{-1}|V\left(f|I\right)\right)\right) \subseteq V\left(f|I\right)$ が成り立つので、$f(a) \in V\left(f|V\left(f^{-1}|V\left(f|I\right)\right)\right) \subseteq V\left(f|I\right)$ が成り立ち、したがって、$f(a) = f(b)$ なるその集合 I の元 b が存在する。ここで、定理 1.2.8 よりこれが成り立つならそのときに限り、$a \equiv b \bmod (\ker f, *_G)$ が成り立つのであったので、$a *_G b^{-1} \in \ker f$ が成り立ち、その集合 $\Omega'_{(G,*_G)}$ の定義より、$a *_G b^{-1} \in I$ が成り立つ。したがって、$b \in I$ が成り立つことと定理 1.1.6 より次のようになる。

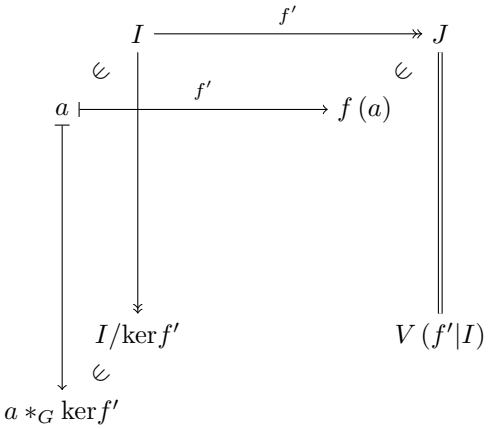
$$\begin{aligned}\left(a *_G b^{-1}\right) *_G b &= a *_G \left(b^{-1} *_G b\right)\\ &= a *_G 1_{(G,*_G)}\\ &= a \in I\end{aligned}$$

以上より、$a \in I$ が成り立つので、$V\left(f^{-1}|V\left(f|I\right)\right) \subseteq I$ が成り立つ。したがって、$V\left(f^{-1}|V\left(f|I\right)\right) = I$ が成り立つので、$E \circ F(I) = I$ が成り立つ。

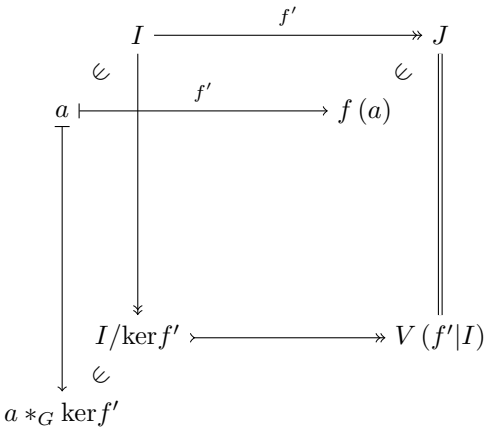
次に、$F \circ G = I_{\Omega_{(H,*_H)}}$ が成り立つことを示そう。$\forall J \in \Omega_{(H,*_H)}$ に対し、その対応 f は写像なので、もちろん、$V\left(f|V\left(f^{-1}|J\right)\right) = J$ は成り立つ。したがって、$F \circ G(J) = V\left(f|V\left(f^{-1}|J\right)\right) = J$ が成り立つ。

以上より、$E \circ F = I_{\Omega'_{(G,*_G)}}$ かつ $F \circ G = I_{\Omega_{(H,*_H)}}$ が成り立つので、その写像 $F : \Omega'_{(G,*_G)} \to \Omega_{(H,*_H)}$ は全単射でその写像 E がその写像 F の逆写像である。よって、次式のように写像 $F : \Omega'_{(G,*_G)} \to \Omega_{(H,*_H)}; I \mapsto V\left(f|I\right)$ は全単射でその逆写像 F^{-1} が $F^{-1} : \Omega_{(H,*_H)} \to \Omega'_{(G,*_G)}; J \mapsto V\left(f^{-1}|J\right)$ と与えられる。

また、$\forall I \in \Omega'_{(G,*_G)}$ に対し、$F(I) = V\left(f|I\right) = J$ とおくと、写像 $f' : I \to J; a \mapsto f(a)$ は明らかに全射群準同型写像であるから、次式のように考えられると、



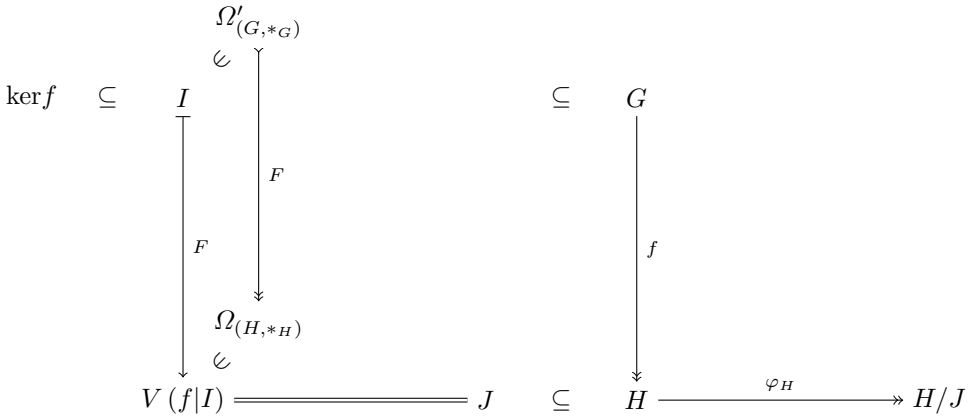
群準同型定理より次式が成り立つので、



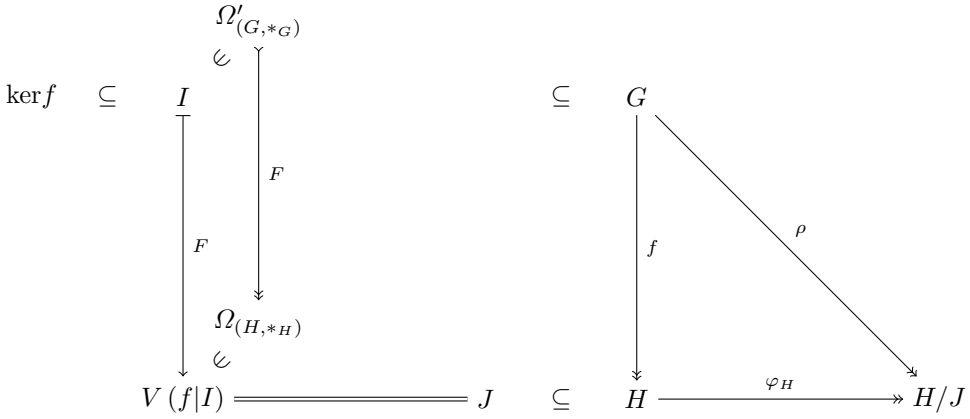
$(I/\ker f', *_G) \cong (V(f'|I), *_H)$ が得られる。$\ker f \subseteq I$ より $V(f'|I) = V(f|I) = J$ が成り立つかつ、$\ker f' = \ker f$ が成り立つので、$(I/\ker f, *_G) \cong (J, *_H)$ が成り立つ。

$\forall I \in \Omega'_{(G,*_G)}$ に対し、その写像 $F : \Omega'_{(G,*_G)} \to \Omega_{(H,*_H)}; I \mapsto V(f|I)$ が与えられたとき、定理 1.2.12 より $(I, *_G) \trianglelefteq (G, *_G)$ が成り立つならそのときに限り、$(F(I), *_H) \trianglelefteq (H, *_H)$ が成り立つことが直ちに分かる。

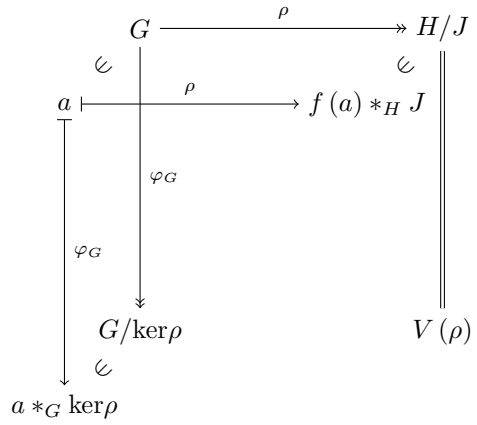
$\forall I \in \Omega'_{(G,*_G)}$ に対し、上記の写像 $F : \Omega'_{(G,*_G)} \to \Omega_{(H,*_H)}; I \mapsto V(f|I)$ が与えられたとき、$(I, *_G) \trianglelefteq (G, *_G)$ が成り立つなら、$F(I) = V(f|I) = J$ とおいて次式のように自然な全射群準同型写像 $\varphi_H : H \twoheadrightarrow H/J$ を考えると、



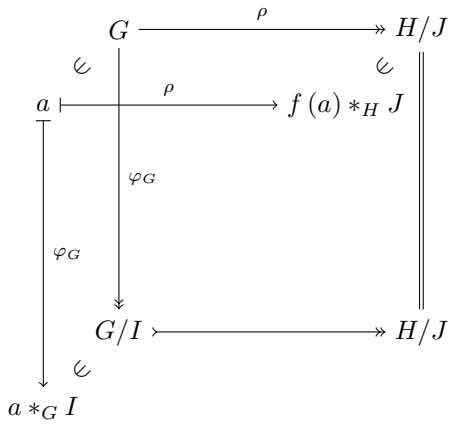
$J = \ker \varphi_H$ が成り立ち、$\varphi_H \circ f = \rho$ とおくと、その写像 ρ は次式のように全射群準同型写像で、



$\forall a \in G$ に対し、$a \in \ker \rho$ が成り立つならそのときに限り、$\rho(a) = f(a) *_H J = J$ が成り立ち、これが成り立つならそのときに限り、$f(a) \in J$ が成り立つ、即ち、$a \in V\left(f^{-1}|J\right)$ が成り立つ。ここで、上記の議論により $a \in F^{-1}(J) = I$ が成り立つので、$\ker \rho = I$ が得られる。以上より、自然な全射群準同型写像 $\varphi_G : G \twoheadrightarrow G/\ker \rho$ を用いれば、次式のように与えられ、



$\ker \rho = I$ が成り立つことに注意すれば、群準同型定理より次のようになるので、



$(G/I, *_G) \cong (H/J, *_H)$ が成り立つ。 □

定理 1.2.14 (第 2 群同型定理)**.** 群 $(G, *)$ の部分群 $(H, *)$、正規部分群 $(N, *)$ が与えられたとする。このとき、次のことが成り立つ。

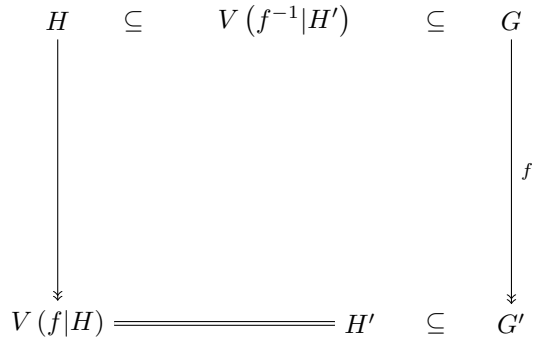
- 群 $(H * N, *)$ はその群 $(G, *)$ の部分群である。
- 群 $(H \cap N, *)$ はその部分群 $(H, *)$ の正規部分群である、即ち、$(H \cap N, *) \trianglelefteq (H, *)$ が成り立つ。
- $(H/(H \cap N), *) \cong ((H * N)/N, *)$ が成り立つ。

この定理を第 2 群同型定理という。

証明. 群 $(G, *)$ の部分群 $(H, *)$、正規部分群 $(N, *)$ が与えられたとする。その群 $(H, *)$ 自身もその群 $(H, *)$ の正規部分群であることに注意すれば、次のことが成り立つことは定理 1.1.29 と定理 1.1.30 より明らかである。

- 群 $(H * N, *)$ はその群 $(G, *)$ の部分群である。
- 群 $(H \cap N, *)$ はその部分群 $(H, *)$ の正規部分群である。

このとき、$\ker f = N$ が成り立つような群準同型写像 f によるその群 $(G, *)$ の群準同型像 $(G', *')$ が存在する。例えば、その群準同型写像 f が自然な全射群準同型写像の場合などが挙げられる。ここで、その値域 $V(f|H)$ を H' とおくと、次のようになる。



$\forall a \in G$ に対し、$a \in V\left(f^{-1}|H'\right)$ が成り立つなら、$f(a) \in V(f|H)$ が成り立つので、$\exists h \in H$ に対し、$f(a) = f(h)$ が成り立つ。ここで、定理 1.2.8 より $a \equiv h \bmod (\ker f, *)$ が成り立つ、即ち、$a \equiv h \bmod (N, *)$

が成り立つので、$h^{-1} * a \in N$ が成り立つ、即ち、次のようになる。

$$\begin{aligned} h * \left(h^{-1} * a\right) &= \left(h * h^{-1}\right) * a \\ &= 1_{(G,*)} * a \\ &= a \in h * N \subseteq H * N \end{aligned}$$

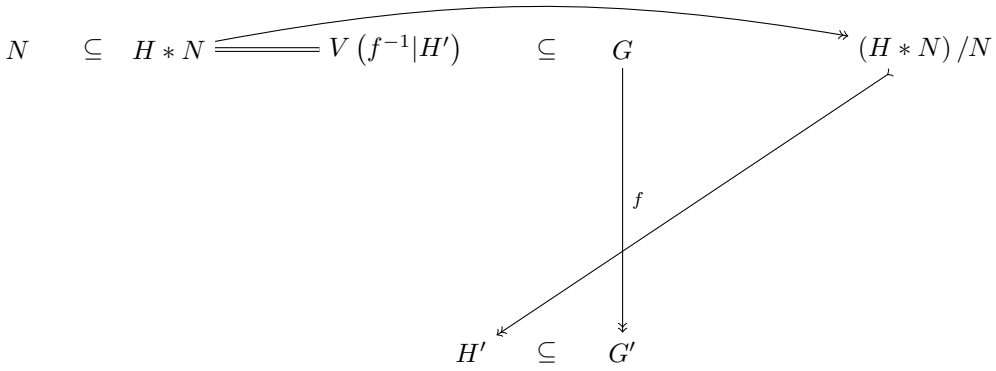
したがって、$V\left(f^{-1}|H'\right) \subseteq H * N$ が成り立つ。逆に、$\forall a \in G$ に対し、$a \in H * N$ が成り立つなら、$\exists h \in H \exists n \in N$ に対し、$a = h * n$ と書かれることができ、このとき、$n \in N = \ker f$ が成り立つことに注意すれば、次のようになる。

$$\begin{aligned} f(a) &= f(h * n) \\ &= f(h) *' f(n) \\ &= f(h) *' 1_{(G',*')} \\ &= f(h) \end{aligned}$$

したがって、$f(a) \in V(f|H)$ が得られるので、$a \in V\left(f^{-1}|H'\right)$ が成り立つ。したがって、$V\left(f^{-1}|H'\right) \supseteq H*N$ が成り立つ。以上より、$V\left(f^{-1}|H'\right) = H * N$ が得られ次式のようになる。

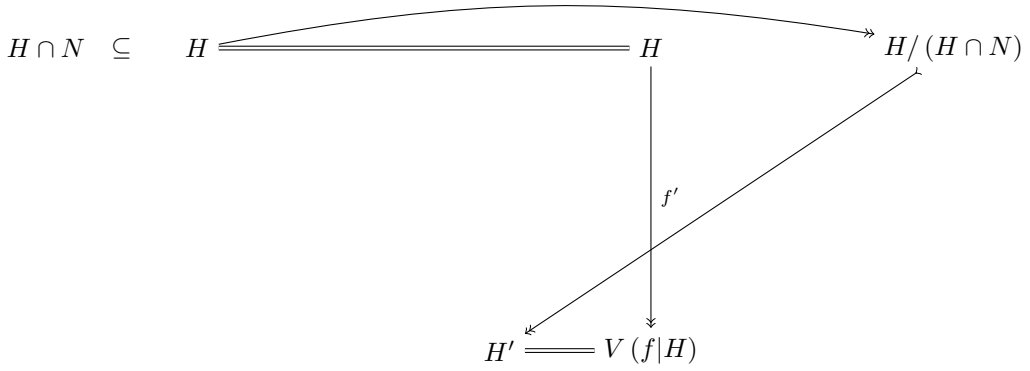
$$\begin{array}{ccccc} H * N & = & V\left(f^{-1}|H'\right) & \subseteq & G \\ & & & & \Big\downarrow f \\ H' & & \subseteq & & G' \end{array}$$

ここで、当然ながら $N \subseteq H * N$ が成り立つので、第 1 群同型定理より次式のようになるので、



$((H * N)/\ker f, *) = ((H * N)/N, *) \cong (H', *')$ が成り立つ。

また、写像 $f' : H \to V(f|H); h \mapsto f(h)$ は全射群準同型写像で、$\forall h \in G$ に対し、$h \in \ker f'$ が成り立つならそのときに限り、$h \in H$ が成り立つかつ、$h \in \ker f$ が成り立ち、したがって、これが成り立つならそのときに限り、$h \in H \cap N$ が成り立つので、$\ker f' = H \cap N$ が成り立つ。ここで、$(H, *) \trianglelefteq (H, *)$ に注意すれば、定理 1.1.30 より $(H \cap N, *) \trianglelefteq (H, *)$ で第 1 群同型定理より次式のようになるので、



$(H/(H \cap N), *) \cong (H', *')$ が成り立つ。

以上より、$(H/(H \cap N), *) \cong (H', *') \cong ((H * N)/N, *)$ が得られたので、$(H/(H \cap N), *) \cong ((H * N)/N, *)$ が成り立つ。 □

定理 1.2.15. 群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$、その群 $(G, *_G)$ の正規部分群 $(N, *_G)$ が与えられたとき、$N \subseteq \ker f$ が成り立つならそのときに限り、次式のような群準同型写像 $\overline{f}$ が存在する。

$$\overline{f} : G/N \to H; a *_G N \mapsto f(a)$$

証明. 群々 $(G, *_G)$、$(H, *_H)$ の間の群準同型写像 $f : G \to H$、その群 $(G, *_G)$ の正規部分群 $(N, *_G)$ が与えられたとき、$N \subseteq \ker f$ が成り立つなら、$\forall a, b \in N$ に対し、$a *_G b^{-1} \in N \subseteq \ker f$ が成り立つので、次のようになる。

$$\begin{aligned} f(a) &= f(a) *_H 1_{(H,*_H)} \\ &= f(a) *_H f(b)^{-1} *_H f(b) \\ &= f(a) *_H f\left(b^{-1}\right) *_H f(b) \\ &= f\left(a *_G b^{-1}\right) *_H f(b) \\ &= 1_{(H,*_H)} *_H f(b) \\ &= f(b) \end{aligned}$$

したがって、$\forall f(a), f(b) \in H$ に対し、$f(a) \neq f(b)$ が成り立つなら、$a *_G b^{-1} \notin N$ が成り立つので、定理 1.1.20 より $a *_G N \neq b *_G N$ が成り立つ。対偶律により $\forall a *_G N, b *_G N \in G/N$ に対し、$a *_G N = b *_G N$ が成り立つなら、$f(a) = f(b)$ が成り立つので、次式のような写像 $\overline{f}$ が存在する。

$$\overline{f} : G/N \to H; a *_G N \mapsto f(a)$$

ここで、$\forall a *_G N, b *_G N \in G/N$ に対し、定理 1.1.31 より次のようになるので、

$$\begin{aligned} \overline{f}\left(a *_G N *_G b *_G N\right) &= \overline{f}\left(a *_G b *_G N\right) \\ &= f\left(a *_G b\right) \\ &= f(a) *_H f(b) \\ &= \overline{f}\left(a *_G N\right) *_H \overline{f}\left(b *_G N\right) \end{aligned}$$

その写像 $\overline{f}$ は群準同型写像である。

逆に、次式のような群準同型写像 $\overline{f}$ が存在するなら、

$$\overline{f} : G/N \to H; a *_G N \mapsto f(a)$$

自然な全射群準同型写像 $\varphi_G : G \twoheadrightarrow G/N; a \mapsto a *_G N$ を用いれば、定義より明らかに $f = \overline{f} \circ \varphi_G$ が成り立つので、$\forall n \in N$ に対し、定理 1.2.1 より次のようになる。

$$\begin{aligned} f(h) &= \overline{f} \circ \varphi_G(n) \\ &= \overline{f}\,(n *_G N) \\ &= \overline{f}(N) \\ &= \overline{f}\left(1_{(G,*_G)} *_G N\right) \\ &= f\left(1_{(G,*_G)}\right) \\ &= 1_{(H,*_H)} \end{aligned}$$

これにより、$n \in \ker f$ が成り立つので、$N \subseteq \ker f$ が成り立つ。 □

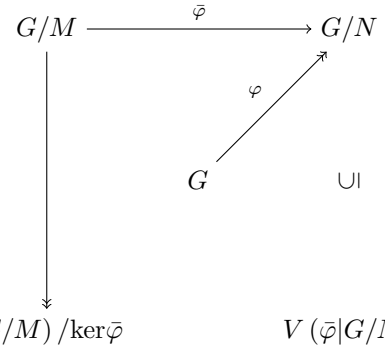
定理 1.2.16 (第 3 群同型定理)**.** 群 $(G, *)$ の正規部分群たち $(M, *)$、$(N, *)$ が与えられ、$M \subseteq N$ が成り立つとき、$(G/N, *) \cong ((G/M)/(N/M), *)$ が成り立つ。

この定理を第 3 群同型定理という。

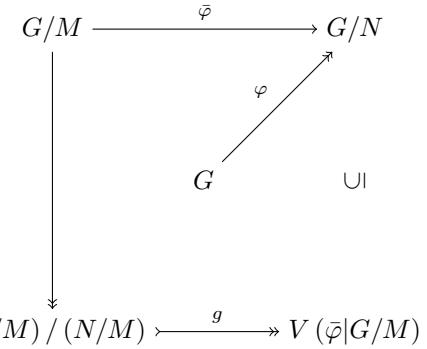
証明. 群 $(G, *)$ の正規部分群たち $(M, *)$、$(N, *)$ が与えられ、$M \subseteq N$ が成り立つとき、自然な全射群準同型写像 $\varphi : G \twoheadrightarrow G/N; a \mapsto a * N$ を用いれば、定理 1.2.7 より $M \subseteq N = \ker \varphi$ が成り立つので、定理 1.2.15 より次式のような群準同型写像 $\overline{f}$ が存在して

$$\overline{\varphi} : G/M \to G/N; a * M \mapsto \varphi(a) = a * N$$

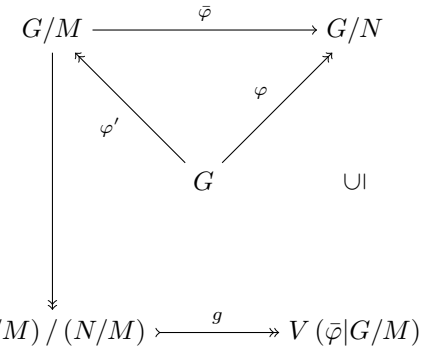
次式のようになる。



ここで、$\forall a * M \in \ker \overline{\varphi}$ に対し、$\overline{\varphi}(a * M) = a * N = N$ が成り立つならそのときに限り、$a \in N$ が成り立つので、$a * M \in N/M$ が成り立つ。したがって、$\ker \overline{\varphi} = N/M$ が得られる。そこで、群準同型定理より次式のような写像 $g : (G/M)/(N/M) \xrightarrow{\sim} V\,(\overline{\varphi}|G/N)$ が存在する。



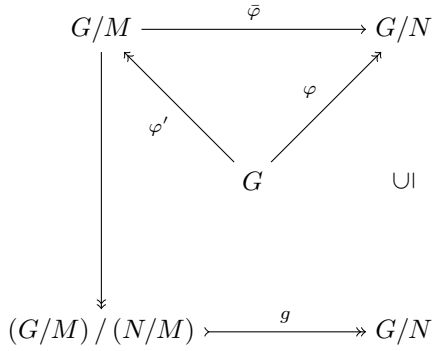
一方で、次式のような自然な全射群準同型写像 $\varphi' : G \twoheadrightarrow G/M; a \mapsto a * M$ が考えられれば、次のようになり



$\varphi = \overline{\varphi} \circ \varphi'$ が成り立つので、$\forall \overline{\varphi}(a * M) \in V\,(\overline{\varphi}|G/M)$ に対し、次のようになるので、

$$\begin{aligned}\overline{\varphi}(a * M) &= \overline{\varphi}\,(\varphi'(a)) \\ &= \overline{\varphi} \circ \varphi'(a) \\ &= \varphi(a) \in V(\varphi)\end{aligned}$$

その写像 φ が全射であることに注意すれば、$\overline{\varphi}(a * M) \in V\,(\overline{\varphi}|G/M)$ が成り立つならそのときに限り、$\varphi(a) \in G/N$ が成り立つので、次式のようになる。



したがって、$(G/N, *) \cong ((G/M)/(N/M), *)$ が成り立つ。 □

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976. 新装版第 2 刷 p65-71 ISBN978-4-00-029873-5

[2] よしいず. ”群の同型定理”. MATHEMATICS.PDF. https://mathematics-pdf.com/pdf/grp_iso_thm.pdf (2021-8-8 15:30 取得)

[3] 花木章秀. ”群論”. 信州大学. http://math.shinshu-u.ac.jp/~hanaki/edu/group/group2011pre.pdf (2021-8-8 16:00 取得)

第 3 部　環論

数学的構造のうち 2 つの算法を備えたものとして環が代表的でありこのような構造をもつ未知の数学的構造を整数や有理数などよく知られた数学的構造におきかえて調べることがしばしばされる。ここでは、まず、環を導入しこれから群にはなかった素元や因数分解など除法に関する話題を扱っていく。

3.1　環

3.1.1　環

公理 3.1.1 (環の公理)**.** 空集合でない集合 R に対し 2 つの算法それぞれ加法 $+ : R \times R \to R; (a, b) \mapsto a + b$、乗法 $\cdot : R \times R \to R; (a, b) \mapsto ab$ が与えられたとする。このとき、次の条件たちを満たす集合 R を環という[*6]。

- 集合 R は加法について可換群 $(R, +)$ をなす。
- $\forall a, b, c \in R$ に対し、$(ab)c = a(bc)$ が成り立つ、即ち、乗法について結合的である。
- $\exists e \in R \forall a \in R$ に対し、$ae = ea = a$ が成り立つ、即ち、乗法について集合 R の単位元 e が存在する。
- $\forall a, b, c \in R$ に対し、$a(b + c) = ab + ac$ かつ $(a + b)c = ac + bc$ が成り立つ、即ち、乗法は加法に対して両側から分配的である。

さらに、次の条件も満たす環 R を特に可換環という。

- $\forall a, b \in R$ に対し、$ab = ba$ が成り立つ、即ち、乗法は可換的である。

定義 3.1.2. 可換群 $(R, +)$ において、その単位元 $1_{(R,+)}$ を零元といい 0 と、逆元 a^{-1} を $-a$ と、$\forall n \in \mathbb{Z}$ に対し、元 a^n を na と、乗法についての単位元 e を 1 と書く。

定理 3.1.1. 環 R が与えられたとき、$\forall a \in R$ に対し、$a0 = 0a = 0$ が成り立つ。

証明. 環 R について、$\forall a \in R$ に対し、次のようになるかつ、

$$\begin{aligned} 0 &= a0 - a0 \\ &= a(0 + 0) - a0 \\ &= a0 + a0 - a0 = a0 \end{aligned}$$

次のようになるので、

$$\begin{aligned} 0 &= 0a - 0a \\ &= (0 + 0)a - 0a \\ &= 0a + 0a - 0a = 0a \end{aligned}$$

$a0 = 0a = 0$ が成り立つ。 □

定義 3.1.3. 環 R について、$0 = 1$ が成り立つとき、$\forall a \in R$ に対し、$a = 1a = 0a = 0$ が成り立ち $R = \{0\}$

[*6] ここから先は心象するのがほぼ不可能な分野になりますので、定義をよく読んでおくことをお勧めします。

が得られる。これを零環という。以下、環の元が 2 つ以上現れるのであれば、その環は零環でないので、断りがない場合、そうする。

定義 3.1.4. 環 R について、$\exists a, b \in R$ に対し、$a \neq 0$ かつ $b \neq 0$ が成り立つかつ、$ab = 0$ が成り立つなら、それらの元々 a、b をそれぞれ左零因子、右零因子といい、あわせて零因子という。これをもたない可換環を、即ち、その環 R が可換環で、$\forall a, b \in R$ に対し、$a \neq 0$ かつ $b \neq 0$ が成り立つなら、$ab \neq 0$ が成り立つような環を整域という。

定義 3.1.5. 環 R について、$\exists a, b \in R$ に対し、$ab = 1$ が成り立つなら、その元 a を環 R の可逆元、単元といい、その元 b を逆元といい、後に示すように a^{-1}、$\frac{1}{a}$ などと書くことができる。以下、その元 a^{-1} はその群 $(R, +)$ における逆元ではなくその可逆元 a の積における逆元を意味するものとする。これにより、可逆元からなる集合は乗法について群をなし、0 以外の元全てが可逆元であるような環を斜体といい、乗法について可換的な斜体を体といい、可換的でない斜体を非可換体という。

斜体を体、体を可換体というときもある。

定理 3.1.2. 環 R の可逆元について、次のことが成り立つ。

- その環 R が零環でなくその環 R の元 a が可逆元なら、これは 0 でない。
- その環 R の元 a が可逆元なら、一意的に逆元 a^{-1} が定まる。
- その環 R が斜体であるなら、零因子をもたない。

証明. 環 R について、$a \in R$ が成り立ちその環 R が零環でなくその元 a が可逆元であり $a^{-1} \in R$ なる元 a^{-1} を a の逆元とする。$a = 0$ が成り立つなら、$aa^{-1} = 0a^{-1} = 0 \neq 1$ が成り立つので、可逆元の定義に矛盾する。よって $a \neq 0$ が成り立つ。

また、その環 R の元 a が可逆元でその元 a^{-1} でないその元 a の逆元 b が与えられたとするとき、次式が成り立つので、

$$\begin{aligned} a^{-1} &= a^{-1}1 \\ &= a^{-1}(ab) \\ &= \left(a^{-1}a\right)b \\ &= 1b = b \end{aligned}$$

仮定に矛盾する。よって、一意的に逆元 a^{-1} が定まる。

環 R が斜体であるなら、0 以外の元全てが可逆元であるので、$\forall a, b \in R$ に対し、$a \neq 0$ かつ $b \neq 0$ が成り立つなら、$a^{-1}, b^{-1} \in R$ が成り立ち、したがって、次のようになる。

$$\begin{aligned} abb^{-1}a^{-1} &= a1a^{-1} \\ &= aa^{-1} = 1 \\ b^{-1}a^{-1}ab &= b^{-1}1b \\ &= b^{-1}b = 1 \end{aligned}$$

したがって、その元 ab は可逆元であることになるので、$ab \neq 0$ が成り立つ。ゆえに、その環 R は零因子をもたない。 □

定理 3.1.3. 環 R の性質として、次のことが成り立つ。

- $\forall a \in R$ に対し、$-(-a) = a$ が成り立つ。
- $\forall a, b \in R$ に対し、$a(-b) = (-a)b = -ab$ が成り立つ。
- $\forall a, b \in R$ に対し、$(-a)(-b) = ab$ が成り立つ。
- $\forall a, b \in R$ に対し、$a = 0$ または $b = 0$ が成り立つなら、$ab = 0$ が成り立つ。
- $\forall a, b \in R$ に対し、$a = 0$ かつ $b = 0$ が成り立つなら、$a^2 + b^2 = 0$ が成り立つ。
- $\forall a \in R$ に対し、その元 a が可逆元なら、その元 $-a$ も可逆元で $(-a)^{-1} = -a^{-1}$ が成り立つ。
- $\forall a \in R$ に対し、それらの元々 a、b が可逆元なら、その元 ab も可逆元で $(ab)^{-1} = b^{-1}a^{-1}$ が成り立つ。

証明. 環 R が与えられたとき、$\forall a \in R$ に対し、次のようになる。

$$\begin{aligned} -(-a) &= 0 - (-a) \\ &= a - a - (-a) \\ &= a + (-a) - (-a) \\ &= a + 0 = a \end{aligned}$$

$\forall a, b \in R$ に対し、次のようになる。

$$\begin{aligned} a(-b) &= 0 + a(-b) \\ &= -ab + ab + a(-b) \\ &= -ab + a\left(b + (-b)\right) \\ &= -ab + a0 \\ &= -ab + 0 \\ &= -ab \end{aligned}$$

$\forall a, b \in R$ に対し、次のようになる。

$$\begin{aligned} (-a)b &= (-a)b + 0 \\ &= (-a)b + ab - ab \\ &= \left((-a) + a\right) b - ab \\ &= 0b - ab \\ &= a - ab \\ &= -ab \end{aligned}$$

$\forall a, b \in R$ に対し、次のようになる。

$$\begin{aligned} (-a)(-b) &= (-a)(-b) + 0 \\ &= (-a)(-b) + (-a)b - (-a)b \\ &= (-a)\left((-b) + b\right) - (-ab) \\ &= (-a)0 + ab \\ &= 0 + ab \\ &= ab \end{aligned}$$

$\forall a, b \in R$ に対し、$a = 0$ または $b = 0$ が成り立つなら、次のようになるので、

$$\begin{aligned} a = 0 \vee b = 0 &\Rightarrow ab = 0 \vee ab = 0 \\ &\Leftrightarrow ab = 0 \end{aligned}$$

$ab = 0$ が成り立つ。

$\forall a, b \in R$ に対し、$a = 0$ かつ $b = 0$ が成り立つなら、次のようになるので、

$$\begin{aligned} a = 0 \wedge b = 0 &\Rightarrow a^2 = 0 \wedge b^2 = 0 \\ &\Rightarrow a^2 + b^2 = 0 \end{aligned}$$

$a^2 + b^2 = 0$ が成り立つ。

$\forall a \in R$ に対し、その元 a が可逆元なら、次のようになるので、

$$\begin{aligned} \left(-a^{-1}\right)(-a) &= a^{-1}a = 1 \\ (-a)\left(-a^{-1}\right) &= aa^{-1} = 1 \end{aligned}$$

その元 $-a$ も可逆元で $(-a)^{-1} = -a^{-1}$ が成り立つ。

$\forall a \in R$ に対し、それらの元々 a、b が可逆元なら、次のようになるので、

$$\begin{aligned} \left(b^{-1}a^{-1}\right)(ab) &= b^{-1}\left(a^{-1}a\right)b \\ &= b^{-1}1b = b^{-1}b = 1 \\ (ab)\left(b^{-1}a^{-1}\right) &= a\left(bb^{-1}\right)a^{-1} \\ &= a1a^{-1} = aa^{-1} = 1 \end{aligned}$$

その元 ab も可逆元で $(ab)^{-1} = b^{-1}a^{-1}$ が成り立つ。 □

3.1.2 環の例

定義 3.1.6. 環 R が与えられたとき、空集合でない集合 S を用いて $\forall f, g \in \mathfrak{F}(S, R)$ に対し、次のように写像 $f + g$、fg が定義される。

- $\forall a \in S$ に対し、$(f + g)(a) = f(a) + g(a)$ が成り立つ。
- $\forall a \in S$ に対し、$(fg)(a) = f(a)g(a)$ が成り立つ。

定理 3.1.4. 環 R が与えられたとき、空集合でない集合 S を用いた集合 $\mathfrak{F}(S, R)$ は環であり次式のように与えられる。

$$\begin{aligned} 0 &: S \to R; a \mapsto 0 \\ 1 &: S \to R; a \mapsto 1 \\ -f &: S \to R; a \mapsto -f(a) \end{aligned}$$

証明. 環 R が与えられたとき、空集合でない集合 S を用いた集合 $\mathfrak{F}(S, R)$ について、次のようにおかれれば、

$$\begin{aligned} 0 &: S \to R; a \mapsto 0 \\ 1 &: S \to R; a \mapsto 1 \\ -f &: S \to R; a \mapsto -f(a) \end{aligned}$$

次のようになる。

$$\begin{aligned} ((f + g) + h)(a) &= (f + g)(a) + h(a) \\ &= (f(a) + g(a)) + h(a) \end{aligned}$$

$$
\begin{aligned}
&= f(a) + (g(a) + h(a)) \\
&= f(a) + (g + h)(a) \\
&= (f + (g + h))\,(a) \\
(f + 0)(a) &= f(a) + 0(a) \\
&= f(a) + 0 = f(a) \\
(0 + f)(a) &= 0(a) + f(a) \\
&= 0 + f(a) = f(a) \\
(f - f)(a) &= f(a) + (-f)(a) \\
&= f(a) - f(a) = 0 \\
(-f + f)(a) &= (-f)(a) + f(a) \\
&= -f(a) + f(a) = 0 \\
(f + g)(a) &= f(a) + g(a) \\
&= g(a) + f(a) \\
&= (g + f)(a)
\end{aligned}
$$

したがって、その組 $(\mathfrak{F}(S, R), +)$ は可換群をなす。

さらに、次のようになるので、

$$
\begin{aligned}
((fg)h)\,(a) &= (fg)(a)h(a) \\
&= (f(a)g(a))\,h(a) \\
&= f(a)\,(g(a)h(a)) \\
&= f(a)(gh)(a) \\
&= (f(gh))\,(a) \\
(f1)(a) &= f(a)1(a) \\
&= f(a)1 = f(a) \\
(1f)(a) &= 1(a)f(a) \\
&= 1f(a) = f(a) \\
(f(g + h))\,(a) &= f(a)(g + h)(a) \\
&= f(a)\,(g(a) + h(a)) \\
&= f(a)g(a) + f(a)h(a) \\
&= (fg)(a) + (fh)(a) \\
&= (fg + fh)(a) \\
((f + g)h)\,(a) &= (f + g)(a)h(a) \\
&= (f(a) + g(a))\,h(a) \\
&= f(a)h(a) + g(a)h(a) \\
&= (fh)(a) + (gh)(a) \\
&= (fh + gh)(a)
\end{aligned}
$$

よって、その集合 $\mathfrak{F}(S, R)$ は環である。 □

定理 3.1.5. 可換群 $(G, *)$ での自己準同型写像 $f : G \to G$、即ち、$\forall a, b \in G$ に対し、$f(a * b) = f(a) * f(b)$

なる写像 f 全体の集合 $\mathrm{end}(G,*)$ が与えられたとき[*7]、算法 $*$、合成 $\circ$ がそれぞれ加法、乗法とみなされれば、その集合 $\mathrm{end}(G,*)$ は環であり次式のように与えられる。なお、$1_{(G,*)}$ はその群 $(G,*)$ の単位元である。

$$\begin{aligned} 0 &: S \to R; a \mapsto 1_{(G,*)} \\ 1 &: S \to R; a \mapsto a \\ -f &: S \to R; a \mapsto f(a)^{-1} \end{aligned}$$

定義 3.1.7. この集合 $\mathrm{end}(G,*)$ をその可換群 $(G,*)$ の自己準同型環という。

証明. 可換群 $(G,*)$ での自己準同型写像 $f : G \to G$、即ち、$\forall a, b \in G$ に対し、$f(a*b) = f(a)*f(b)$ なる写像 f 全体の集合 $\mathrm{end}(G,*)$ が与えられたとき、$\forall a, b \in G \forall f, g, h \in \mathfrak{F}(S,R)$ に対し、次のようになるので、

$$\begin{aligned} (f*g)(a*b) &= f(a*b)*g(a*b) \\ &= f(a)*f(b)*g(a)*g(b) \\ &= f(a)*g(a)*f(b)*g(b) \\ &= (f*g)(a)*(f*g)(b) \\ f\circ g(a*b) &= f\left(g(a*b)\right) \\ &= f\left(g(a)*g(b)\right) \\ &= f\left(g(a)\right)*f\left(g(b)\right) \\ &= f\circ g(a)*f\circ g(b) \end{aligned}$$

$f*g, f\circ g \in \mathrm{end}(G,*)$ が成り立つ。

さらに、次式のように与えられると、

$$\begin{aligned} 0 &: S \to R; a \mapsto 1_{(G,*)} \\ 1 &: S \to R; a \mapsto a \\ -f &: S \to R; a \mapsto f(a)^{-1} \end{aligned}$$

次のようになるので、

$$\begin{aligned} \left((f*g)*h\right)(a) &= (f*g)(a)*h(a) \\ &= \left(f(a)*g(a)\right)*h(a) \\ &= f(a)*\left(g(a)*h(a)\right) \\ &= f(a)*(g*h)(a) \\ &= \left(f*(g*h)\right)(a) \\ (f*0)(a) &= f(a)*0(a) \\ &= f(a)*1_{(G,*)} = f(a) \\ (0*f)(a) &= 0(a)*f(a) \\ &= 1_{(G,*)}*f(a) = f(a) \\ \left(f*(-f)\right)(a) &= f(a)*(-f)(a) \\ &= f(a)*f(a)^{-1} = 1_{(G,*)} \\ \left((-f)*f\right)(a) &= (-f)(a)*f(a) \\ &= f(a)^{-1}*f(a) = 1_{(G,*)} \end{aligned}$$

[*7] 自己準同型写像を英語でいうと endomorphism というそうです。終わりの end とは全く関係ございません。

$$\begin{aligned}(f*g)(a) &= f(a)*g(a)\\ &= g(a)*f(a)\\ &= (g*f)(a)\end{aligned}$$

その組 $(\mathrm{end}(G,*),*)$ は可換群をなす。

さらに、合成 $\circ$ が結合的なのはいうまでもなく、次のようになるので、

$$\begin{aligned}f\circ 1(a) &= f\left(1(a)\right) = f(a)\\ 1\circ f(a) &= 1\left(f(a)\right) = f(a)\\ f\circ(g*h)(a) &= f\left((g*h)(a)\right)\\ &= f\left(g(a)*h(a)\right)\\ &= f\left(g(a)\right)*f\left(h(a)\right)\\ &= f\circ g(a)*f\circ h(a)\\ &= (f\circ g*f\circ h)(a)\\ (f*g)\circ h(a) &= (f*g)\left(h(a)\right)\\ &= f\left(h(a)\right)*g\left(h(a)\right)\\ &= f\circ h(a)*g\circ h(a)\\ &= (f\circ h*g\circ h)(a)\end{aligned}$$

算法 $*$、合成 $\circ$ がそれぞれ加法、乗法とみなされれば、その集合 $\mathrm{end}(G,*)$ は環である。 □

定義 3.1.8. 環 R が与えられたとき、$\forall a\in R$ に対し、$a^2=a$ が成り立つようなものを Boole 環という。

定理 3.1.6. Boole 環は可換環である。

証明. Boole 環が与えられたとき、$\forall a,b\in R$ に対し、次のようになる。

$$\begin{aligned}a+b &= (a+b)^2\\ &= (a+b)(a+b)\\ &= (a+b)a+(a+b)b\\ &= a^2+ba+ab+b^2\\ &= a+b+ab+ba\end{aligned}$$

したがって、次のようになる。

$$\begin{aligned}ab &= a+b+ab+ba-a-b-ba\\ &= a+b-a-b-ba\\ &= -ba\end{aligned}$$

特に、$b=1$ とすれば、$a=-a$ が得られる。これにより、次のようになる。

$$\begin{aligned}ab &= -ba\\ &= b(-a)\\ &= ba\end{aligned}$$

□

定理 3.1.7. 集合 S が与えられたとき、次のように和と積が定義されるとする。

$$+ : \mathfrak{P}(S) \times \mathfrak{P}(S) \to \mathfrak{P}(S); (A, B) \mapsto (A \cup B) \setminus (A \cap B)$$
$$\cdot : \mathfrak{P}(S) \times \mathfrak{P}(S) \to \mathfrak{P}(S); (A, B) \mapsto A \cap B$$

このとき、その集合 $\mathfrak{P}(S)$ は Boole 環であり次のようになる。

$$0 = \emptyset, \quad 1 = S, \quad -A = A$$

証明. 集合 S が与えられたとき、次のように和と積が定義されるとする。

$$+ : \mathfrak{P}(S) \times \mathfrak{P}(S) \to \mathfrak{P}(S); (A, B) \mapsto (A \cup B) \setminus (A \cap B)$$
$$\cdot : \mathfrak{P}(S) \times \mathfrak{P}(S) \to \mathfrak{P}(S); (A, B) \mapsto A \cap B$$

このとき、$\forall A, B, C \in \mathfrak{P}(S)$ に対し、次のようおかれると、

$$D = A \cap B \cap C$$
$$A' = A \cap B \setminus D$$
$$B' = B \cap C \setminus D$$
$$C' = C \cap A \setminus D$$
$$A'' = A \setminus (A' \sqcup D \sqcup C')$$
$$B'' = B \setminus (B' \sqcup D \sqcup A')$$
$$C' = C \setminus (C' \sqcup D \sqcup B')$$

次のようになるかつ、

$$\begin{aligned}
(A + B) + C &= ((A \cup B) \setminus (A \cap B) \cup C) \setminus ((A \cup B) \setminus (A \cap B) \cap C) \\
&= ((A'' \sqcup C' \sqcup B'' \sqcup B' \sqcup A' \sqcup D) \setminus (A' \sqcup D) \cup (C' \sqcup C'' \sqcup B' \sqcup D)) \\
&\quad \setminus ((A'' \sqcup C' \sqcup B'' \sqcup B' \sqcup A' \sqcup D) \setminus (A' \sqcup D) \cap (C' \sqcup C'' \sqcup B' \sqcup D)) \\
&= ((A'' \sqcup C' \sqcup B'' \sqcup B') \cup (C' \sqcup C'' \sqcup B' \sqcup D)) \\
&\quad \setminus ((A'' \sqcup C' \sqcup B'' \sqcup B') \cap (C' \sqcup C'' \sqcup B' \sqcup D)) \\
&= (A'' \sqcup C' \sqcup B'' \sqcup B' \sqcup C'' \sqcup D) \setminus (C' \sqcup B') \\
&= A'' \sqcup B'' \sqcup C'' \sqcup D
\end{aligned}$$

次のようになるので、

$$\begin{aligned}
A + (B + C) &= (A \cup (B \cup C) \setminus (B \cap C)) \setminus (A \cap (B \cup C) \setminus (B \cap C)) \\
&= ((A' \sqcup A'' \sqcup C' \sqcup D) \cup (B'' \sqcup A' \sqcup C'' \sqcup C' \sqcup B' \sqcup D) \setminus (B' \sqcup D)) \\
&\quad \setminus ((A' \sqcup A'' \sqcup C' \sqcup D) \cap (B'' \sqcup A' \sqcup C'' \sqcup C' \sqcup B' \sqcup D) \setminus (B' \sqcup D)) \\
&= ((A' \sqcup A'' \sqcup C' \sqcup D) \cup (B'' \sqcup A' \sqcup C'' \sqcup C')) \\
&\quad \setminus ((A' \sqcup A'' \sqcup C' \sqcup D) \cap (B'' \sqcup A' \sqcup C'' \sqcup C')) \\
&= (A' \sqcup A'' \sqcup C' \sqcup D \sqcup B'' \sqcup C'') \setminus (A' \sqcup C') \\
&= A'' \sqcup B'' \sqcup C'' \sqcup D
\end{aligned}$$

次式が成り立つ。

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

また、次のようになるので、

$$\begin{aligned}
A+0 &= (A\cup\emptyset)\setminus(A\cap\emptyset) = A\setminus\emptyset = A\\
0+A &= (\emptyset\cup A)\setminus(\emptyset\cap A) = A\setminus\emptyset = A\\
A-A &= A+A = (A\cup A)\setminus(A\cap A) = A\setminus A = 0\\
-A+A &= A+A = (A\cup A)\setminus(A\cap A) = A\setminus A = 0\\
A+B &= (A\cup B)\setminus(A\cap B) = (B\cup A)\setminus(B\cap A) = B+A
\end{aligned}$$

その組 $(\mathfrak{P}(S),+)$ は可換群をなす。

さらに、次のようになるので、

$$\begin{aligned}
(AB)C &= (A\cap B)\cap C\\
&= A\cap(B\cap C)\\
&= A(BC)\\
A1 &= A\cap S = A\\
1A &= S\cap A = A\\
A(B+C) &= A\cap(B\cup C)\setminus(B\cap C)\\
&= (A\cap(B\cup C))\setminus(B\cap C)\\
&= ((A\cap B)\cup(A\cap C))\setminus(A\cap B\cap C)\\
&= ((A\cap B)\cup(A\cap C))\setminus((A\cap B)\cap(A\cap C))\\
&= AB+AC\\
(A+B)C &= (A\cup B)\setminus(A\cap B)\cap C\\
&= ((A\cup B)\cap C)\setminus(A\cap B)\\
&= ((A\cap C)\cup(B\cap C))\setminus(A\cap B\cap C)\\
&= ((A\cap C)\cup(B\cap C))\setminus((A\cap C)\cap(B\cap C))\\
&= AC+BC
\end{aligned}$$

その集合 $\mathfrak{P}(S)$ は環をなす。

さらに、$A^2 = A\cap A = A$ が成り立つので、その集合 $\mathfrak{P}(S)$ は Boole 環をなし次のようになる。

$$0=\emptyset,\quad 1=S,\quad -A=A$$

□

3.1.3 二項定理

定理 3.1.8. 環 R の元の族たち $\{a_i\}_{i\in\Lambda_m}$、$\{b_j\}_{j\in\Lambda_n}$ が与えられたとき、次式が成り立つ。

$$\left(\sum_{i\in\Lambda_m} a_i\right)\left(\sum_{j\in\Lambda_n} b_j\right) = \sum_{(i,j)\in\Lambda_m\times\Lambda_n} a_ib_j$$

証明. 環 R の元の族たち $\{a_i\}_{i\in\Lambda_m}$、$\{b_j\}_{j\in\Lambda_n}$ が与えられたとき、$n=1$ のとき、数学的帰納法により明らかに次のようになる。

$$\left(\sum_{i\in\Lambda_m} a_i\right)b_1 = \sum_{i\in\Lambda_m} a_ib_1$$

$$= \sum_{(i,j)\in\Lambda_m\times\Lambda_1} a_i b_j$$

$n = k$ のとき、次式が成り立つと仮定しよう。

$$\left(\sum_{i\in\Lambda_m} a_i\right)\left(\sum_{j\in\Lambda_k} b_j\right) = \sum_{(i,j)\in\Lambda_m\times\Lambda_k} a_i b_j$$

$n = k+1$ のとき、次のようになる。

$$\begin{aligned}
\left(\sum_{i\in\Lambda_m} a_i\right)\left(\sum_{j\in\Lambda_{k+1}} b_j\right) &= \left(\sum_{i\in\Lambda_m} a_i\right)\left(\sum_{j\in\Lambda_k} b_j + b_{k+1}\right) \\
&= \left(\sum_{i\in\Lambda_m} a_i\right)\left(\sum_{j\in\Lambda_k} b_j\right) + \left(\sum_{i\in\Lambda_m} a_i\right) b_{k+1} \\
&= \sum_{(i,j)\in\Lambda_m\times\Lambda_k} a_i b_j + \sum_{i\in\Lambda_m} a_i b_{k+1} \\
&= \sum_{i\in\Lambda_m}\sum_{j\in\Lambda_k} a_i b_j + \sum_{i\in\Lambda_m} a_i b_{k+1} \\
&= \sum_{i\in\Lambda_m}\left(\sum_{j\in\Lambda_k} a_i b_j + a_i b_{k+1}\right) \\
&= \sum_{i\in\Lambda_m} a_i\left(\sum_{j\in\Lambda_k} b_j + b_{k+1}\right) \\
&= \sum_{i\in\Lambda_m} a_i \sum_{j\in\Lambda_{k+1}} b_j \\
&= \sum_{i\in\Lambda_m}\sum_{j\in\Lambda_{k+1}} a_i b_j \\
&= \sum_{(i,j)\in\Lambda_m\times\Lambda_k} a_i b_j
\end{aligned}$$

以上、数学的帰納法により次式が成り立つことが示された。

$$\left(\sum_{i\in\Lambda_m} a_i\right)\left(\sum_{j\in\Lambda_n} b_j\right) = \sum_{(i,j)\in\Lambda_m\times\Lambda_n} a_i b_j$$

□

定義 3.1.9. $k \leq n$ なる非負整数に対し、次式のような有理数 $\binom{n}{k}$ が定義される。この有理数 $\binom{n}{k}$ を二項係数といい ${}_n\mathrm{C}_k$ とも書かれることがある。

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

定理 3.1.9. このとき、次のことが成り立つ。

- $k \leq n$ なる非負整数に対し、$\binom{n}{k} = \binom{n}{n-k}$ が成り立つ。

- $1 \leq k \leq n-1$ なる非負整数に対し、$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ が成り立つ。
- $k \leq n$ なる非負整数に対し、$\binom{n}{k} \in \mathbb{N}$ が成り立つ。

証明. $k \leq n$ なる非負整数に対し、次のようになる。

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(n-k)!\,(n-(n-k))!} \\ &= \binom{n}{n-k}\end{aligned}$$

$1 \leq k \leq n-1$ なる非負整数に対し、次のようになる。

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k!(n-k)!} \\ &= \frac{(n-1)!}{(k-1)!}\frac{n}{k(n-k)!} \\ &= \frac{(n-1)!}{(k-1)!}\left(\frac{k}{k(n-k)!} + \frac{n-k}{k(n-k)!}\right) \\ &= \frac{(n-1)!}{(k-1)!}\left(\frac{1}{(n-k)!} + \frac{1}{k(n-k-1)!}\right) \\ &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{(k-1)!k(n-k-1)!} \\ &= \frac{(n-1)!}{(k-1)!\,((n-1)-(k-1))!} + \frac{(n-1)!}{k!\,((n-1)-k)!} \\ &= \binom{n-1}{k-1} + \binom{n-1}{k}\end{aligned}$$

$k \leq n$ なる非負整数に対し、$n = 0$ のとき、次のようになる。

$$\binom{0}{0} = \frac{0!}{0!0!} = 1$$

$n = 1$ のとき、次のようになる。

$$\binom{1}{0} = \frac{1!}{0!1!} = 1, \quad \binom{1}{1} = \frac{1!}{1!0!} = 1$$

ここで、$n = l$ のとき、$\binom{l}{k} \in \mathbb{N}$ が成り立つと仮定しよう。$n = l+1$ のとき、$1 \leq k \leq l$ が成り立つなら、次のようになる。

$$\binom{l+1}{k} = \binom{l}{k-1} + \binom{l}{k} \in \mathbb{N}$$

$k = 0$ が成り立つなら、次のようになる。

$$\binom{l+1}{0} = \frac{(l+1)!}{0!(l+1)!} = 1 \in \mathbb{N}$$

$k = l + 1$ が成り立つなら、次のようになる。

$$\begin{aligned}\binom{l+1}{l+1} &= \frac{(l+1)!}{(l+1)!\,((l+1)-(l+1))!} \\ &= \frac{(l+1)!}{(l+1)!0!} = 1 \in \mathbb{N}\end{aligned}$$

以上、数学的帰納法により $\binom{n}{k} \in \mathbb{N}$ が成り立つことが示された。 □

定理 3.1.10 (二項定理)**.** 環 R について、$\forall a, b \in R \forall n \in \mathbb{N}$ に対し、次式が成り立つ。

$$(a+b)^n = \sum_{k \in \Lambda_n \cup \{0\}} \binom{n}{k} a^{n-k} b^k$$

この定理を二項定理という。

証明. 環 R について、$\forall a, b \in R \forall n \in \mathbb{N}$ に対し、$n = 1$ のとき、次のようになる。

$$\begin{aligned}a + b &= \frac{1!}{0!1!} a^1 b^0 + \frac{1!}{1!0!} a^0 b^1 \\ &= \sum_{k \in \Lambda_1 \cup \{0\}} \frac{n!}{k!(n-k)!} a^{n-k} b^k\end{aligned}$$

$n = l$ のとき、次式が成り立つと仮定しよう。

$$(a+b)^l = \sum_{k \in \Lambda_l \cup \{0\}} \binom{l}{k} a^{l-k} b^k$$

$n = l + 1$ のとき、次のようになる。

$$\begin{aligned}(a+b)^{l+1} &= (a+b)(a+b)^l \\ &= (a+b) \sum_{k \in \Lambda_l \cup \{0\}} \binom{l}{k} a^{l-k} b^k \\ &= \sum_{k \in \Lambda_l \cup \{0\}} \binom{l}{k} a^{l-k+1} b^k + \sum_{k \in \Lambda_l \cup \{0\}} \binom{l}{k} a^{l-k} b^{k+1} \\ &= \sum_{k \in \Lambda_l} \binom{l}{k} a^{(l+1)-k} b^k + \binom{l}{0} a^{l+1} + \sum_{k \in \Lambda_l \cup \{0\}} \binom{l}{k} a^{l-k} b^{k+1} \\ &= \binom{l}{0} a^{l+1} + \sum_{k \in \Lambda_l} \binom{l}{k} a^{(l+1)-k} b^k + \sum_{k \in \Lambda_{l+1}} \binom{l}{k-1} a^{(l+1)-k} b^k \\ &= a^{l+1} + \sum_{k \in \Lambda_l} \left(\binom{l}{k} + \binom{l}{k-1} \right) a^{(l+1)-k} b^k + b^{l+1} \\ &= \binom{l+1}{0} a^{l+1} + \sum_{k \in \Lambda_l} \binom{l+1}{k} a^{(l+1)-k} b^k + \binom{l+1}{l+1} b^{l+1} \\ &= \sum_{k \in \Lambda_{l+1} \cup \{0\}} \binom{l}{k} a^{l-k} b^k\end{aligned}$$

よって、数学的帰納法により $\forall a, b \in R \forall n \in \mathbb{N}$ に対し、次式が成り立つことが示された。

$$(a+b)^n = \sum_{k \in \Lambda_n \cup \{0\}} \binom{n}{k} a^{n-k} b^k$$

□

定理 3.1.11 (多項定理)**.** 添数集合 Λ_m によって添数づけられた環 R の元の族 $\{a_i\}_{i \in \Lambda_m}$ が与えられたとき、$\forall n \in \mathbb{N}$ に対し、次式が成り立つ。

$$\left(\sum_{i \in \Lambda_m} a_i \right)^n = \sum_{\substack{\sum_{i \in \Lambda_m} k_i = n \\ k_i \in \mathbb{N} \cup \{0\}}} \frac{n!}{\prod_{i \in \Lambda_m} k_i!} \prod_{i \in \Lambda_m} a_i^{k_i}$$

この定理を多項定理という。

証明. 添数集合 Λ_m によって添数づけられた環 R の元の族 $\{a_i\}_{i \in \Lambda_m}$ が与えられたとき、$\forall n \in \mathbb{N}$ に対し、$m = 1$ のときは明らかに次のようになる。

$$\begin{aligned} \left(\sum_{i \in \Lambda_1} a_i \right)^n &= a_1^n = \frac{n!}{n!} a_1^n \\ &= \sum_{k_1 = n} \frac{n!}{k_1!} a_1^{k_1} \\ &= \sum_{\substack{\sum_{i \in \Lambda_1} k_i = n \\ k_i \in \mathbb{N} \cup \{0\}}} \frac{n!}{\prod_{i \in \Lambda_1} k_i!} \prod_{i \in \Lambda_1} a_i^{k_i} \end{aligned}$$

$m = k$ のとき、次式が成り立つと仮定しよう。

$$\left(\sum_{i \in \Lambda_k} a_i \right)^n = \sum_{\substack{\sum_{i \in \Lambda_k} k_i = n \\ k_i \in \mathbb{N} \cup \{0\}}} \frac{n!}{\prod_{i \in \Lambda_k} k_i!} \prod_{i \in \Lambda_k} a_i^{k_i}$$

$m = k+1$ のとき、$a = \sum_{i \in \Lambda_k} a_i$ とおかれると、二項定理より次のようになる。

$$\begin{aligned} \left(\sum_{i \in \Lambda_{k+1}} a_i \right)^n &= \left(\sum_{i \in \Lambda_k} a_i + a_{k+1} \right)^n \\ &= (a + a_{k+1})^n \\ &= \sum_{k_{k+1} \in \Lambda_n \cup \{0\}} \binom{n}{k_{k+1}} a^{n-k_{k+1}} a_{k+1}^{k_{k+1}} \\ &= \sum_{k_{k+1} \in \Lambda_n \cup \{0\}} \frac{n!}{k_{k+1}!\,(n-k_{k+1})!} \sum_{\substack{\sum_{i \in \Lambda_k} k_i = n - k_{k+1} \\ k_i \in \mathbb{N} \cup \{0\}}} \frac{(n-k_{k+1})!}{\prod_{i \in \Lambda_k} k_i!} \prod_{i \in \Lambda_k} a_i^{k_i} a_{k+1}^{k_{k+1}} \\ &= \sum_{k_{k+1} \in \Lambda_n \cup \{0\}} \sum_{\substack{\sum_{i \in \Lambda_k} k_i = n - k_{k+1} \\ k_i \in \mathbb{N} \cup \{0\}}} \frac{n!}{k_{k+1}!\,(n-k_{k+1})!} \frac{(n-k_{k+1})!}{\prod_{i \in \Lambda_k} k_i!} \prod_{i \in \Lambda_{k+1}} a_i^{k_i} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{\sum_{i\in\Lambda_k} k_i + k_{k+1} = n \\ k_i \in \mathbb{N}\cup\{0\} \\ k_{k+1} \in \Lambda_n \cup \{0\}}} \frac{(n-k_{k+1})!}{(n-k_{k+1})!} \frac{n!}{\prod_{i\in\Lambda_{k+1}} k_i!} \prod_{i\in\Lambda_{k+1}} a_i^{k_i} \\
&= \sum_{\substack{\sum_{i\in\Lambda_{k+1}} k_i = n \\ k_i \in \mathbb{N}\cup\{0\}}} \frac{n!}{\prod_{i\in\Lambda_{k+1}} k_i!} \prod_{i\in\Lambda_{k+1}} a_i^{k_i}
\end{aligned}
$$

よって、数学的帰納法により $\forall n \in \mathbb{N}$ に対し、次式が成り立つことが示された。

$$
\left(\sum_{i\in\Lambda_m} a_i\right)^n = \sum_{\substack{\sum_{i\in\Lambda_m} k_i = n \\ k_i \in \mathbb{N}\cup\{0\}}} \frac{n!}{\prod_{i\in\Lambda_m} k_i!} \prod_{i\in\Lambda_m} a_i^{k_i}
$$

□

3.1.4 整域

定義 3.1.10. 環 R について、$\exists a, b \in R \setminus \{0\}$ に対し、$ab = 0$ が成り立つなら、それらの元々 a、b をそれぞれ左零因子、右零因子といい、あわせて零因子という。これをもたない可換環を整域という。

例えば、集合 $\mathbb{Z}$ が挙げられる。

定義 3.1.11 (定義 3.1.5 の再掲)**.** 環 R について、$\exists a, b \in R$ に対し、$ab = 1$ が成り立つなら、その元 a を環 R の可逆元、単元といい、その元 b を逆元といい、a^{-1} などと書く。これにより、可逆元からなる集合は乗法について群をなし、0 以外の元全てが可逆元であるような環を斜体といい、乗法について可換的な斜体を体といい、可換的でない斜体を非可換体という。

例えば、集合 $\mathbb{Q}$、$\mathbb{R}$、$\mathbb{C}$ などが挙げられる。斜体を体、体を可換体というときもある。

定理 (定理 3.1.2 の再掲)**.** 環 R について、元 a が可逆元なら、これは 0 でなく一意的に逆元 a^{-1} が定まる。

定理 3.1.12. 任意の体 K は整域である。

証明. 任意の体 K について、可逆元からなる集合 K' は乗法について群をなし、体の定義よりその群 $(K', \cdot)$ は可換群で $K' = K \setminus \{0\}$ が成り立つので、$\forall a, b \in K' = K \setminus \{0\}$ に対し、$ab \in K' = K \setminus \{0\}$ が成り立つ。したがって、その体 K は整域である。 □

定理 3.1.13. 有限集合である整域は体である。

証明. 有限集合である整域 R について、$\forall c \in R \setminus \{0\}$ に対し、次式のような写像 f が与えられたとき、

$$
f : R \to R; a \mapsto ca
$$

$f(a) = f(b)$ が成り立つなら、次のようになるので、

$$
\begin{aligned}
0 &= f(a) - f(b) \\
&= ca - cb \\
&= c(a - b)
\end{aligned}
$$

ここで、その可換環 R は零因子をもたないので、$a-b=0$ が成り立つ。したがって、その写像 f は単射である。ここで、その可換環 R は有限集合であるから、その写像 f は全単射である。したがって、$f(a)=ca=1$ なる元 a が存在する。よって、有限集合である整域は体であることが示された。 □

3.1.5 部分環

定義 3.1.12. 環 R が与えられたとき、これの部分集合もまた環となっており、しかも、その環 R と同じ単位元をもつものをその環 R の部分環という。特に、これが斜体、体となっているものをそれぞれその環 R の部分斜体、部分体という。

定理 3.1.14. 環 R の部分集合 R' が与えられたとき、これがその環 R の部分環であるならそのときに限り、次のことをいづれも満たす。

- その部分集合 R' がその環 R の単位元 1 に属される。
- $\forall a,b\in R'$ に対し、$-a, a+b, ab\in R'$ が成り立つ。

証明. 環 R の部分集合 R' が与えられたとき、これがその環 R の部分環であるなら、定義より次のことを満たす。

- その部分集合 R' がその環 R の単位元 1 に属される。
- $\forall a,b\in R'$ に対し、$-a, a+b, ab\in R'$ が成り立つ。

逆に、その部分集合 R' が上記のことを満たすなら、$\forall a,b,c\in R'$ に対し、$-a\in R'$ が成り立つので、$-a+a=0\in R'$ が成り立つ。これにより、$a,b,c\in R$ が成り立ち、次のことを満たすので、

$$(a+b)+c=a+(b+c),\quad a+0=0+a,\quad a+(-a)=-a+a=0,\quad a+b=b+a$$

その組 $(R',+)$ は可換群をなす。

さらに、次のことを満たすので、

$$(ab)c=a(bc),\quad a1=1a=a,\quad a(b+c)=ab+ac,\quad (a+b)c=ac+bc$$

その集合 R' は環をなす。 □

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976. 新装版第 2 刷 p107-115 ISBN978-4-00-029873-5

[2] チャート研究所, チャート式 基礎からの数学 II+B, 数研出版, 平成 11 年. 新課程第 6 刷 p14 ISBN978-4-410-10585-2

[3] 理系のための備忘録. ”二項係数 n C m が整数になることの証明”. 理系のための備忘録. https://science-log.com/%E6%95%B0%E5%AD%A6/%E4%BA%8C%E9%A0%85%E4%BF%82%E6%95%B0n%EF%BD%83m%E3%81%8C%E6%95%B4%E6%95%B0%E3%81%AB%E3%81%AA%E3%82%8B%E3%81%93%E3%81%A8%E3%81%AE%E8%A8%BC%E6%98%8E/ (2021-8-20 12:00 閲覧)

3.2　環準同型写像

3.2.1　ideal

公理 3.2.1 (ideal の公理)**.** 環 R が与えられたとき、これの空集合でない部分集合 J が次のことを満たすとき、その集合 J をその環 R の左 ideal という。

- $\forall a, b \in J$ に対し、$a + b \in J$ が成り立つ。
- $\forall a \in J \forall r \in R$ に対し、$ra \in J$ が成り立つ。

同様に、環 R が与えられたとき、これの空集合でない部分集合 J が次のことを満たすとき、その集合 J をその環 R の右 ideal という。

- $\forall a, b \in J$ に対し、$a + b \in J$ が成り立つ。
- $\forall a \in J \forall r \in R$ に対し、$ar \in J$ が成り立つ。

さらに、環 R の左 ideal であるかつ、右 ideal であるものをその環 R の ideal、両側 ideal という。

例えば、集合 $2\mathbb{Z}$ はその集合 $\mathbb{Z}$ の ideal である。

定理 3.2.1. 環 R の左 ideal$J$ が与えられたとき、組 $(J, +)$ は可換群をなし、これの単位元を $1_{(J,+)}$ とおくと、次のことを満たす。

$$1_{(J,+)} = 0, \quad a^{-1} = -a$$

同様に環 R の右 ideal$J$ が与えられたとき、組 $(J, +)$ は可換群をなし、これの単位元を $1_{(J,+)}$ とおくと、次のことを満たす。

$$1_{(J,+)} = 0, \quad a^{-1} = -a$$

証明. 環 R の左 ideal$J$ が与えられたとき、$\forall a \in J$ に対し、$-1 \in R$ より $(-1)a = -a \in J$ が成り立つ。したがって、$a - a = 0 \in J$ が成り立つことになるので、次のようになる。

$$\begin{aligned} (a + b) + c &= a + (b + c) \\ 0 + a &= a + 0 = a \\ a - a &= -a + a = 0 \\ a + b &= b + a \end{aligned}$$

したがって、組 $(J, +)$ は可換群をなし、これの単位元を $1_{(J,+)}$ とおくと、次のことを満たす。

$$1_{(J,+)} = 0, \quad a^{-1} = -a$$

右 ideal についても同様にして、示される。 □

定理 3.2.2. 可換環 R の左 ideal$J$ が与えられたとき、これは ideal でもある。同様に、可換環 R の右 ideal$J$ が与えられたとき、これは ideal でもある。

証明. 可換環 R の左 ideal$J$ が与えられたとき、この部分集合 J は定義より次のことを満たす。

- $\forall a, b \in J$ に対し、$a + b \in J$ が成り立つ。
- $\forall a \in J \forall r \in R$ に対し、$ra \in J$ が成り立つ。

ここで、その環 R は乗法について可換的なので、$ra = ar$ が成り立つ。したがって、次のことを満たす。

- $\forall a, b \in J$ に対し、$a + b \in J$ が成り立つ。
- $\forall a \in J \forall r \in R$ に対し、$ra \in J$ が成り立つ。

よって、その左 ideal$J$ はその環 R の右 ideal でもあるので、その左 ideal はその環 R の ideal でもある。その環 R の右 ideal についても同様にして示される。 □

定理 3.2.3. 添数集合 Λ_n によって添数づけられた環 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、その環 R の元の族 $\{r_i\}_{i\in\Lambda_n}$ を用いて $\sum_{i\in\Lambda_n} r_i a_i$ の形で書かれるその環 R の元全体の集合、即ち、集合 $\sum_{i\in\Lambda_n} Ra_i$ はその環 R の左 ideal となる。同様に、集合 $\sum_{i\in\Lambda_n} a_i R$ もその環 R の右 ideal である。

定義 3.2.2. そのような集合たち $\sum_{i\in\Lambda_n} Ra_i$、$\sum_{i\in\Lambda_n} a_i R$ をそれぞれその元の族 $\{a_i\}_{i\in\Lambda_n}$ から生成されたその環 R の左 ideal、右 ideal という。特に、$n = 1$ のとき、その元 a_1 から生成されたその環 R の単項左 ideal、単項右 ideal という。特に、単項左 ideal であるかつ、単項右 ideal であるものを単項 ideal といい、ある整域 R の ideal が全て単項 ideal であるようなその整域 R を単項 ideal 整域という。

定義 3.2.3. 零元 0 から生成された環 R の単項左 ideal$R0$ は明らかに単項右 ideal でもあり集合 $0R$ を零 ideal という。

証明. 添数集合 Λ_n によって添数づけられた環 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、その環 R の元の族 $\{r_i\}_{i\in\Lambda_n}$ を用いて $\sum_{i\in\Lambda_n} r_i a_i$ の形で書かれるその環 R の元全体の集合、即ち、集合 $\sum_{i\in\Lambda_n} Ra_i$ について、$\forall \sum_{i\in\Lambda_n} r_i a_i \in \sum_{i\in\Lambda_n} Ra_i$ に対し、加法と乗法の定義より $\sum_{i\in\Lambda_n} r_i a_i \in R$ が成り立つので、その集合 $\sum_{i\in\Lambda_n} Ra_i$ はその環 R の部分集合である。さらに、$\forall \sum_{i\in\Lambda_n} r_i a_i,\ \sum_{i\in\Lambda_n} s_i a_i \in \sum_{i\in\Lambda_n} Ra_i$ に対し、次のようになり、

$$\begin{aligned}\sum_{i\in\Lambda_n} r_i a_i + \sum_{i\in\Lambda_n} s_i a_i &= \sum_{i\in\Lambda_n} (r_i a_i + s_i a_i) \\ &= \sum_{i\in\Lambda_n} (r_i + s_i)\, a_i\end{aligned}$$

$\forall i \in \Lambda_n$ に対し、$r_i + s_i \in R$ が成り立つので、$\sum_{i\in\Lambda_n} r_i a_i + \sum_{i\in\Lambda_n} s_i a_i \in \sum_{i\in\Lambda_n} Ra_i$ が成り立つかつ、$\forall r \in R \forall \sum_{i\in\Lambda_n} r_i a_i \in \sum_{i\in\Lambda_n} Ra_i$ に対し、次のようになり、

$$\begin{aligned}r \sum_{i\in\Lambda_n} r_i a_i &= \sum_{i\in\Lambda_n} r r_i a_i \\ &= \sum_{i\in\Lambda_n} (r r_i)\, a_i\end{aligned}$$

$\forall i \in \Lambda_n$ に対し、$r r_i \in R$ が成り立つので、$r \sum_{i\in\Lambda_n} r_i a_i \in \sum_{i\in\Lambda_n} Ra_i$ が成り立つ。以上より、その集合 $\sum_{i\in\Lambda_n} Ra_i$ はその環 R の左 ideal となる。同様にして、集合 $\sum_{i\in\Lambda_n} a_i R$ もその環 R の右 ideal であることが示される。 □

定理 3.2.4. 零環でない環 R が斜体であるならそのときに限り、その環 R は零 ideal$0R$ とその環 R 自身以外に左 ideal をもたない。

同様に、環 R が斜体であるならそのときに限り、その環 R は零 ideal$R0$ とその環 R 自身以外に右 ideal をもたない[*8]。

証明. 零環でない環 R が斜体であるとする。その環 R の任意の左 ideal$J$ が与えられたとき、これが零 ideal でないなら、$a \neq 0$ なるその左 ideal$J$ の元 a が存在し、その環 R は斜体なので、元 a^{-1} がその環 R に存在することになり、したがって、$a^{-1}a = 1 \in J$ が成り立つ。したがって、$\forall a \in R$ に対し、$a1 = a \in J$ が成り立つことになり、よって、$R = J$ が成り立つ。ゆえに、その環 R は零 ideal$0R$ とその環 R 自身以外に左 ideal をもたない。

逆に、零環でない環 R は零 ideal$0R$ とその環 R 自身以外に左 ideal をもたないとしよう。このとき、$\forall a \in R$ に対し、$a \neq 0$ が成り立つなら、これによって生成されたその環 R の単項左 idealRa は零 ideal でないので、$Ra = R$ が成り立つことになる。したがって、$\forall a' \in R$ に対し、$a'a \neq 1$ が成り立つなら、$Ra \subset R$ が成り立つので、対偶律より $a'a = 1$ なるその環 R の元 a' が存在する。これが 0 であるなら、$1 = 0$ となり矛盾しているので、$a' \neq 0$ が成り立つ。同様にして、$a''a' = 1$ なる元 a'' がその環 R に存在することになり、したがって、次のようになる。

$$\begin{aligned} a'' &= a''1 \\ &= a''\left(a'a\right) \\ &= \left(a''a'\right)a \\ &= 1a = a \end{aligned}$$

これにより、$a'a = aa' = 1$ なる元 a' がその環 R に存在することになり、したがって、$\forall a \in R$ に対し、$a \neq 0$ が成り立つなら、これは可逆元であるから、その環 R は斜体である。 □

定理 3.2.5. 環 R の左 ideal たち I、J が与えられたとき、集合たち $I \cap J$、$I + J$ もその環 R の左 ideal である。

同様に、環 R の右 ideal たち I、J が与えられたとき、集合たち $I \cap J$、$I + J$ もその環 R の右 ideal である。

証明. 環 R の左 ideal たち I、J が与えられたとき、集合 $I \cap J$ はもちろんその環 R の部分集合であり、$\forall a, b \in I \cap J$ に対し、$a, b \in I$ かつ $a, b \in J$ が成り立つので、$a + b \in I$ かつ $a + b \in J$ が成り立ち、したがって、$a + b \in I \cap J$ が成り立つ。$\forall a \in I \cap J$ に対し、$a \in I$ かつ $a \in J_2$ が成り立つので、$\forall r \in R$ に対し、$ra \in I$ かつ $ra \in J$ が成り立ち、したがって、$ra \in I \cap J$ が成り立つ。

$\forall a \in I \forall b \in J$ に対し、$a + b \in I + J$ が成り立つ。ここで、$a, b \in R$ が成り立つので、$a + b \in R$ が成り立ち、したがって、その集合 $I + J$ はその環 R の部分集合である。このとき、$\forall a, b \in I \forall c, d \in J$ に対し、$a + b \in I$ かつ $c + d \in J$ が成り立つので、$(a + c) + (b + d) = (a + b) + (c + d) \in I + J$ が成り立つ。さらに、$\forall a \in I \forall b \in J \forall r \in R$ に対し、$ra \in I$ かつ $rb \in J$ が成り立つので、$r(a + b) = ra + rb \in I + J$ が成り立つ。

よって、環 R の左 ideal たち I、J が与えられたとき、集合たち $I \cap J$、$I + J$ もその環 R の左 ideal である。

同様にして、環 R の右 ideal たち I、J が与えられたとき、集合たち $I \cap J$、$I + J$ もその環 R の右 ideal であることが示される。 □

[*8] ただ、その環 R は零 ideal$R0$ とその環 R 自身以外に ideal をもたないなら、その環 R は斜体であるということは成り立たないということにお気をつけて…。

3.2.2 商環

定義 3.2.4. 環 R とこれの 1 つの ideal$J$ を考え $a,b \in R$ なる元々 a、b について次のことを定義しよう。このようなことを元たち a、b がその ideal$J$ を法として合同であるという。

$$a \equiv b \bmod J \Leftrightarrow b - a \in J$$

これは群論でいう可換群 $(R,+)$ の部分群 $(J,+)$ を法として合同であるという概念と一致する。ゆえに、次の定理 3.2.6、定理 3.2.7、定理 3.2.8 が成り立つ。なお、より一般的な証明は群論の書籍などに参照されたい[*9]。

定理 3.2.6. 環 R の ideal$J$ が与えられたとき、$J + J = J$ が成り立つ。

証明. 環 R の ideal$J$ が与えられたとき、$\forall a + b \in J + J$ に対し、$a,b \in J$ が成り立つので、$a + b \in J$ も成り立つ。一方で、$\forall a \in J$ に対し、組 $(J,+)$ は単位元 0、元 a の逆元 $-a$ の可換群をなすので、$-a \in J$ が成り立つ。したがって、$a - a = 0 \in J$ が成り立ち、したがって、$a = 0 + a$ が成り立つので、$a \in J + J$ も成り立つ。以上より、$J + J = J$ が得られる。 □

定理 3.2.7. 環 R の ideal$J$ が与えられたとき、関係 $\equiv \bmod J$ はその環 R における同値関係である。

証明. 環 R の ideal$J$ が与えられたとき、$\forall a,b,c \in R$ に対し、組 $(J,+)$ は単位元 0、元 a の逆元 $-a$ の可換群をなすので、次のようになる。

$$\begin{aligned}
0 \in R &\Rightarrow 0 \in J \\
&\Leftrightarrow a - a \in J \\
&\Leftrightarrow a \equiv a \bmod J \\
a \equiv b \bmod J &\Leftrightarrow b - a \in J \\
&\Leftrightarrow -(b-a) = a - b \in J \\
&\Leftrightarrow b \equiv a \bmod J \\
a \equiv b \bmod J \wedge b \equiv c \bmod J &\Leftrightarrow b - a \in J \wedge c - b \in J \\
&\Rightarrow (b-a) + (c-b) = c - a \in J \\
&\Leftrightarrow a \equiv c \bmod J
\end{aligned}$$

□

定理 3.2.8. 環 R の ideal$J$ が与えられたとき、同値関係 $\equiv \bmod J$ によるその環 R の元 a の同値類 $C_{\equiv \bmod J}(a)$ は集合 $a + J$ に等しい。

定義 3.2.5. この集合 $a + J$ をその ideal$J$ を法とする元 a の剰余類という。

証明. 環 R の ideal$J$ が与えられたとき、同値関係 $\equiv \bmod J$ によるその環 R の元 a の同値類 $C_{\equiv \bmod J}(a)$ について、次のようなり、

$$\begin{aligned}
x \in C_{\equiv \bmod J}(a) &\Leftrightarrow a \equiv x \bmod J \\
&\Leftrightarrow x - a \in J
\end{aligned}$$

[*9] たとえば、雪江明彦「群論入門」、松坂和夫「代数系入門」などが挙げられます。

ここで、$y = x - a$ とすると、次式が成り立ち、

$$\begin{aligned} x &= 0 + x = (a - a) + x \\ &= a + (x - a) \\ &= a + y \end{aligned}$$

明らかに $y \in J$ かつ $a + y \in R$ が成り立つので、次式が成り立ち、

$$\begin{aligned} a + y \in C_{\equiv \bmod J}(a) &\Leftrightarrow a + y \in R \wedge a \equiv a + y \bmod J \\ &\Leftrightarrow a + y \in R \wedge (a + y) - a \in J \\ &\Leftrightarrow a + y \in R \wedge y \in J \\ &\Leftrightarrow a + y \in \{a + y \in R | y \in J\} = a + J \end{aligned}$$

したがって、次のようになる。

$$\begin{aligned} C_{\equiv \bmod J}(a) &= \{a + y \in R | y \in J\} \\ &= a + J \end{aligned}$$

□

定義 3.2.6. 環 R の ideal$J$ が与えられたとき、その ideal$J$ を法とする剰余類たち $a + J$ 全体の集合を R/J と書く、即ち、次式のようにおく。

$$R/J = \{a + J | a \in R\}$$

定理 3.2.9 (ideal を法とする剰余類分解)**.** 環 R の ideal$J$ が与えられたとき、次式が成り立つ。

$$R = \bigsqcup R/J$$

この定理を ideal を法とする剰余類分解という。

証明. 環 R の ideal$J$ が与えられたとき、定理 3.2.7 よりその関係 $\equiv \bmod J$ はその集合 R における同値関係であるので、その関係 $\equiv \bmod J$ による類別が次のようになる。

$$R = \bigsqcup R/\equiv \bmod J = \bigsqcup R/J_l$$

□

定理 3.2.10. その組 $(R/J, +)$ は可換群をなす。このとき、その可換群 $(R/J, +)$ 上での単位元は $0 + J = J$、その可換群 $(R/J, +)$ の任意の元 $a + J$ の逆元は $-a + J$ となる。

証明. 環 R の ideal$J$ が与えられたとき、その ideal$J$ を法とする剰余類たち $a + J$ 全体の集合 R/J において、$\forall a, b, c \in R$ に対し、次のようになるかつ、

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

次のようになるかつ、

$$(0 + J) + (a + J) = (0 + a) + (J + J) = a + J$$

$$(a+J)+(0+J)=(a+0)+(J+J)=a+J$$

次のようになるかつ、

$$(a+J)+(-a+J)=(a-a)+(J+J)=0+J=J$$
$$(-a+J)+(a+J)=(-a+a)+(J+J)=0+J=J$$

次のようになるので、

$$(a+J)+(b+J)=(b+J)+(a+J)$$

よって、その組 $(R/J,+)$ は可換群をなす。このとき、その可換群 $(R/J,+)$ 上での単位元は $0+J=J$、その可換群 $(R/J,+)$ の任意の元 $a+J$ の逆元は $-a+J$ となる。 □

定理 3.2.11. 環 R の ideal$J$ が与えられたとき、$a\equiv b \bmod J$ かつ $c\equiv d \bmod J$ が成り立つなら、$ac\equiv bd \bmod J$ が成り立つ。

証明. 環 R の ideal$J$ が与えられたとき、$a\equiv b \bmod J$ かつ $c\equiv d \bmod J$ が成り立つなら、$u=b-a$、$v=d-c$ とおかれると、$u,v\in J$ が成り立つので、したがって、次のようになる。

$$\begin{aligned} ac &= (b-u)(d-v)\\ &= bd+b(-v)+(-u)d+(-u)(-v)\\ &= bd+(-b)v+u(-d)+uv \end{aligned}$$

ここで、$(-b)v, u(-d), uv\in J$ が成り立つので、$(-b)v+u(-d)+uv\in J$ が成り立つ。ゆえに、$ac-bd\in J$ が成り立つので、$ac\equiv bd \bmod J$ が成り立つ。 □

定理 3.2.12. 環 R の ideal$J$ が与えられたとき、$a+J=b+J$ かつ $c+J=d+J$ が成り立つなら、$ac+J=bd+J$ が成り立つ。

証明. 環 R の ideal$J$ が与えられたとき、$a+J=b+J$ かつ $c+J=d+J$ が成り立つなら、、$a\equiv b \bmod J$ かつ $c\equiv d \bmod J$ が成り立つ。ここで、定理 3.2.11 より $ac\equiv bd \bmod J$ が成り立つことになる。よって、$ac+J=bd+J$ が成り立つ。 □

定理 3.2.13. 環 R の ideal$J$ を法とする剰余類たち $a+J$ 全体の集合 R/J は次式のように加法と乗法が定義されれば、

$$+ : R/J\times R/J\to R/J; (a+J,b+J)\mapsto (a+b)+J$$
$$\cdot : R/J\times R/J\to R/J; (a+J,b+J)\mapsto ab+J$$

環をなし、このとき、零元、単位元はそれぞれ J、$1+J$ となる。

定義 3.2.7. この環 R/J をその環 R のその ideal$J$ による商環、剰余環という。

証明. 環 R の ideal$J$ を法とする剰余類たち $a+J$ 全体の集合 R/J は次式のように加法と乗法が定義されれば、

$$+ : R/J\times R/J\to R/J; (a+J,b+J)\mapsto (a+b)+J$$
$$\cdot : R/J\times R/J\to R/J; (a+J,b+J)\mapsto ab+J$$

定理 3.2.10 よりその組 $(R/J,+)$ は可換群をなし、このとき、その可換群 $(R/J,+)$ 上での単位元は $0+J=J$、その可換群 $(R/J,+)$ の任意の元 $a+J$ の逆元は $-a+J$ となる。さらに、$\forall a+J, b+J, c+J \in R/J$ に対し、次のようになるので、

$$\begin{aligned}
((a+J)(b+J))(c+J) &= (ab+J)(c+J) \\
&= (ab)c+J \\
&= a(bc)+J \\
&= (a+J)(bc+J) \\
&= (a+J)((b+J)(c+J)) \\
(a+J)(1+J) &= a1+J \\
&= a+J \\
(1+J)(a+J) &= 1a+J \\
&= a+J \\
(a+J)((b+J)+(c+J)) &= (a+J)((b+c)+J) \\
&= a(b+c)+J \\
&= (ab+ac)+J \\
&= (ab+J)+(ac+J) \\
&= (a+J)(b+J)+(a+J)(c+J) \\
((a+J)+(b+J))(c+J) &= ((a+b)+J)(c+J) \\
&= (a+b)c+J \\
&= (ac+bc)+J \\
&= (ac+J)+(bc+J) \\
&= (a+J)(c+J)+(b+J)(c+J)
\end{aligned}$$

環 R の ideal$J$ を法とする剰余類たち $a+J$ 全体の集合 R/J は環をなし、このとき、零元、単位元はそれぞれ J、$1+J$ となる。 □

3.2.3 環準同型写像

定義 3.2.8. 2 つの環々 R、S が与えられこれらの零元をそれぞれ 0_R、0_S、単位元をそれぞれ 1_R、1_S とするとき、次のことを満たすような写像 $f : R \to S$ をその環 R からその環 S への環準同型写像という。

- $\forall a, b \in R$ に対し、$f(a+b) = f(a)+f(b)$ が成り立つ。
- $\forall a, b \in R$ に対し、$f(ab) = f(a)f(b)$ が成り立つ。
- $f(1_R) = 1_S$ が成り立つ。

定理 3.2.14. 2 つの環々 R、S、その環 R からその環 S への環準同型写像 f が与えられこれらの 2 つの環々 R、S の零元をそれぞれ 0_R、0_S、単位元をそれぞれ 1_R、1_S とするとき、次のことが成り立つ。

- $f(0_R) = 0_S$ が成り立つ。
- $\forall a \in R$ に対し、$f(-a) = -f(a)$ が成り立つ。

証明. 2 つのの環々 R、S、その環 R からその環 S への環準同型写像 f が与えられこれらの 2 つの環々 R、S

の零元をそれぞれ 0_R、0_S、単位元をそれぞれ 1_R、1_S とするとき、次のようになる。

$$\begin{aligned} f\left(0_R\right) &= f\left(0_R\right) + 0_S \\ &= f\left(0_R\right) + f\left(0_R\right) - f\left(0_R\right) \\ &= f\left(0_R + 0_R\right) - f\left(0_R\right) \\ &= f\left(0_R\right) - f\left(0_R\right) = 0_S \end{aligned}$$

また、$\forall a \in R$ に対し、次のようになる。

$$\begin{aligned} f(-a) &= f(-a) + 0_S \\ &= f(-a) + f(a) - f(a) \\ &= f(-a + a) - f(a) \\ &= f\left(0_1\right) - f(a) \\ &= 0_S - f(a) \\ &= -f(a) \end{aligned}$$

□

定理 3.2.15. 3 つの環々 R、S、T、その環 R からその環 S への環準同型写像 f、その環 S からその環 T への環準同型写像 g が与えられこれらの 3 つの環々 R、S、T の単位元をそれぞれ 1_R、1_S、1_T とするとき、その合成写像 $g \circ f$ も環準同型写像である。

証明. 3 つの環々 R、S、T、その環 R からその環 S への環準同型写像 f、その環 S からその環 T への環準同型写像 g が与えられこれらの 3 つの環々 R、S、T の単位元をそれぞれ 1_R、1_S、1_T とするとき、$\forall a, b \in R$ に対し、次のようになる。

$$\begin{aligned} g \circ f(a + b) &= g\left(f(a + b)\right) \\ &= g\left(f(a) + f(b)\right) \\ &= g\left(f(a)\right) + g\left(f(b)\right) \\ &= g \circ f(a) + g \circ f(b) \\ g \circ f(ab) &= g\left(f(ab)\right) \\ &= g\left(f(a) f(b)\right) \\ &= g\left(f(a)\right) g\left(f(b)\right) \\ &= g \circ f(a) g \circ f(b) \\ g \circ f\left(1_R\right) &= g\left(f\left(1_R\right)\right) \\ &= g\left(1_S\right) = 1_T \end{aligned}$$

□

定義 3.2.9. 環準同型写像のうち、全射であるもの、単射であるもの、全単射であるものをそれぞれ全射環準同型写像、単射環準同型写像、環同型写像という。

定理 3.2.16. 2 つの環々 R、S、その環 R からその環 S への環同型写像 f が与えられこれらの 2 つの環々 R、S の単位元をそれぞれ 1_R、1_S とするとき、その写像 f の逆写像 f^{-1} も環同型写像である。

証明. 2 つの環々 R、S、その環 R からその環 S への環同型写像 f が与えられこれらの 2 つの環々 R、S の単位元をそれぞれ 1_R、1_S とするとき、$\forall a, b \in S$ に対し、次のようになる。

$$\begin{aligned}
f^{-1}(a+b) &= f^{-1}\left(f \circ f^{-1}(a) + f \circ f^{-1}(b)\right) \\
&= f^{-1}\left(f\left(f^{-1}(a)\right) + f\left(f^{-1}(b)\right)\right) \\
&= f^{-1}\left(f\left(f^{-1}(a) + f^{-1}(b)\right)\right) \\
&= f^{-1} \circ f\left(f^{-1}(a) + f^{-1}(b)\right) \\
&= f^{-1}(a) + f^{-1}(b) \\
f^{-1}(ab) &= f^{-1}\left(f \circ f^{-1}(a) f \circ f^{-1}(b)\right) \\
&= f^{-1}\left(f\left(f^{-1}(a)\right) f\left(f^{-1}(b)\right)\right) \\
&= f^{-1}\left(f\left(f^{-1}(a) f^{-1}(b)\right)\right) \\
&= f^{-1} \circ f\left(f^{-1}(a) f^{-1}(b)\right) \\
&= f^{-1}(a) f^{-1}(b) \\
f^{-1}\left(1_S\right) &= 1_R
\end{aligned}$$

□

定義 3.2.10. 2 つの環々 R、S は、その環 R からその環 S への環準同型写像 $f : R \xrightarrow{\sim} S$ が存在するとき、環同型であるといい $R \cong S$ と書く。

定理 3.2.17. 次のことが成り立つ、即ち、その関係 $\cong$ は同値関係である。

- $R \cong R$ が成り立つ。
- $R \cong S$ が成り立つなら、$S \cong R$ も成り立つ。
- $R \cong S$ かつ $S \cong T$ が成り立つなら、$R \cong T$ も成り立つ。

証明. 環同型な 3 つの環々 R、S、T が与えられこれらの単位元をそれぞれ 1_R、1_S、1_T とする。

その環 R の恒等写像 I_R を考えると、$\forall a, b \in R$ に対し、次のようになり、

$$\begin{aligned}
I_R(a+b) &= a + b = I_R(a) + I_R(b) \\
I_R(ab) &= ab = I_R(a) I_R(b) \\
I_R\left(1_R\right) &= 1_R
\end{aligned}$$

恒等写像の逆写像はもとのその恒等写像自身であるので、この写像 I_R は環同型写像である。よって、$R \cong R$ が成り立つ。

$R \cong S$ が成り立つなら、その環 R からその環 S への環同型写像 f が存在し、環同型写像の逆対応は環同型写像であったので、その環 S からその環 R への環同型写像が存在し $S \cong R$ が成り立つ。

$R \cong S$ かつ $S \cong T$ が成り立つなら、その環 R からその環 S への環同型写像 f が存在するかつ、その環 S からその環 T への環同型写像 g が存在し、ここで、その写像 $g \circ f$ も環準同型写像であり、さらに、これらの逆写像たち f^{-1}、g^{-1} も環同型写像たちであるので、その合成写像 $f^{-1} \circ g^{-1}$ も環準同型写像である。ここで、次のようになるので、

$$\begin{aligned}
(g \circ f) \circ \left(f^{-1} \circ g^{-1}\right) &= g \circ \left(f \circ f^{-1}\right) \circ g^{-1} \\
&= g \circ I_S \circ g^{-1}
\end{aligned}$$

$$
\begin{aligned}
&= g \circ g^{-1} = I_T \\
\left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) &= f^{-1} \circ \left(g^{-1} \circ g\right) \circ f \\
&= f^{-1} \circ I_S \circ f \\
&= f^{-1} \circ f = I_R
\end{aligned}
$$

その写像 $f^{-1} \circ g^{-1}$ はその写像 $g \circ f$ の逆写像でありその写像 $g \circ f$ は環同型写像となる。よって、$R \cong T$ が成り立つ。 □

定理 3.2.18. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ の値域 $V(f)$ はその環 S の部分環である。

証明. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ の値域 $V(f)$ について、これらの環々の単位元をそれぞれ 1_R、1_S とおくと、$f(1_R) = 1_S$ が成り立つのであったので、$1_S \in V(f)$ が成り立つ。また、$\forall f(a), f(b) \in V(f)$ に対し、$a, b \in R$ なる元々 a、b が存在し、$f(-a) \in V(f)$ で $-f(a) = f(-a)$ が成り立つので、$-f(a) \in V(f)$ が成り立つ。さらに、$f(a+b) = f(a) + f(b) \in V(f)$ が成り立つかつ、$f(ab) = f(a)f(b) \in V(f)$ が成り立つので、その値域 $V(f)$ はその環 S の部分環である。 □

定義 3.2.11. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ について、この環 S の零元を 0_S とおくと、$f(a) = 0_S$ なるその環 R の元々 a 全体の集合をその写像 f の核といい、$\ker f$ などと書く、即ち、次式のように定められる[*10]。

$$\ker f = \{a \in R | f(a) = 0_S\}$$

定理 3.2.19. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ の核 $\ker f$ はその環 R の ideal である。

証明. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ の核 $\ker f$ について、この環 S の零元を 0_S とおくと、$\forall a, b \in \ker f$ に対し、次のようになるので、

$$
\begin{aligned}
f(a+b) &= f(a) + f(b) \\
&= 0_S + 0_S = 0_S
\end{aligned}
$$

$a + b \in \ker f$ が成り立つかつ、$\forall a \in \ker f \forall r \in R$ に対し、次のようになるので、

$$
\begin{aligned}
f(ra) &= f(r)f(a) \\
&= f(r)0_S = 0_S
\end{aligned}
$$

$ra \in \ker f$ が成り立つ。以上より、その核 $\ker f$ はその環 R の左 ideal である。同様にして、その核 $\ker f$ はその環 R の右 ideal であることが示される。 □

3.2.4 自然な全射環準同型写像

定理 3.2.20. 環 R の ideal$J$ が与えられたとき、写像 $\varphi : R \to R/J; a \mapsto a + J$ はその環 R から商環 R/J への全射準同型写像であり $\ker \varphi = J$ が成り立つ。

定義 3.2.12. このように次式のような写像 φ をその環 R からその商環 R/J への自然な全射環準同型写像、標準的環準同型写像という。

[*10] なお、その環 S が零環でないかぎり、その環 R の単位元はその核 $\ker f$ に属しえませんので、$R = \ker f$ が成り立つことはありません。

$$
\begin{array}{ccccc}
R & \xrightarrow{\quad\varphi\quad} & R/J & = & R/\ker\varphi \\
\cup & & \cup & & \cup \\
a & \longmapsto^{\varphi} & a+J & = & a+\ker\varphi
\end{array}
$$

証明. 環 R の ideal$J$ が与えられたとき、写像 $\varphi : R \to R/J; a \mapsto a+J$ について、$\forall a, b \in R$ に対し、次のようになる。

$$
\begin{aligned}
\varphi(a+b) &= (a+b)+J \\
&= (a+J)+(b+J) \\
&= \varphi(a)+\varphi(b) \\
\varphi(ab) &= ab+J \\
&= (a+J)(b+J) \\
&= \varphi(a)\varphi(b) \\
\varphi(1) &= 1+J
\end{aligned}
$$

これにより、その写像 φ は環準同型写像である。

また、その商環 R/J の零元は J であるので、$\forall a \in \ker\varphi$ に対し、次のようになる。

$$
\varphi(a) = a+J = J
$$

ここで、$\forall b \in J$ に対し、$b = a+b'$ なる元 b' がその ideal$J$ に存在し次のようになるので、

$$
\begin{aligned}
a &= a+0 \\
&= a+b'-b' \\
&= b-b' \in J
\end{aligned}
$$

$a \in J$ が成り立つ。逆に、$\forall a \in J$ が成り立つなら、次のようになるので、

$$
\begin{aligned}
\varphi(a) &= a+J \\
&= \{a+b \in R | b \in J\} \\
&= \{a+b \in R | a+b \in J\} \\
&= J
\end{aligned}
$$

$a \in \ker\varphi$ が成り立つ。以上より、$\ker\varphi = J$ が得られる。

最後に、$\forall a+J \in R/J$ に対し、商環の定義より明らかに $\varphi(a) = a+J$ なるその環 R の元 a が存在するので、その写像 φ は全射である。これにより、その写像 φ は全射環準同型写像である。 □

3.2.5 環準同型定理

定理 3.2.21. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ が与えられたとき、その環 R が斜体でそれらの環々 R、S が零環でないなら、その写像 f は単射環準同型写像である。

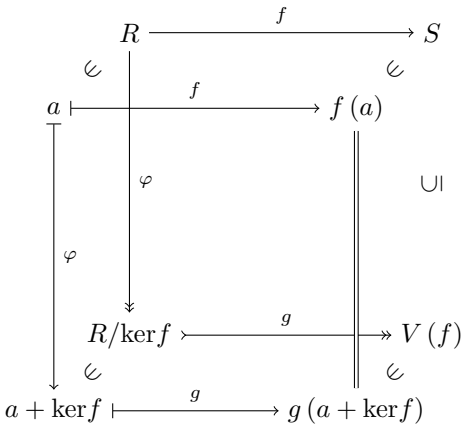
証明. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ が与えられたとき、その環 R が斜体でそれらの環々 R、S が零環でないなら、その環 R の ideal は定理 3.2.4 より零 ideal かその環 R 自身しかもたないことにな

る。ここで、その環 S が零環でないので、その核 $\ker f$ はその環 R 自身になりえないので、その核 $\ker f$ は零 ideal であることになる。このとき、$\forall f(a), f(b) \in V(f)$ に対し、$f(a) = f(b)$ が成り立つなら、その環 S の零元を 0_S として次のようになり、

$$\begin{aligned} f(a) = f(b) &\Leftrightarrow f(a) - f(b) = f(a) + f(-b) = f(a-b) = 0_S \\ &\Leftrightarrow a - b \in \ker f \\ &\Leftrightarrow a - b \in R0 \\ &\Leftrightarrow a - b = 0 \\ &\Leftrightarrow a = b \end{aligned}$$

その写像 f は単射である。よって、その環 R が斜体でそれらの環々 R、S が零環でないなら、その写像 f は単射環準同型写像である。 □

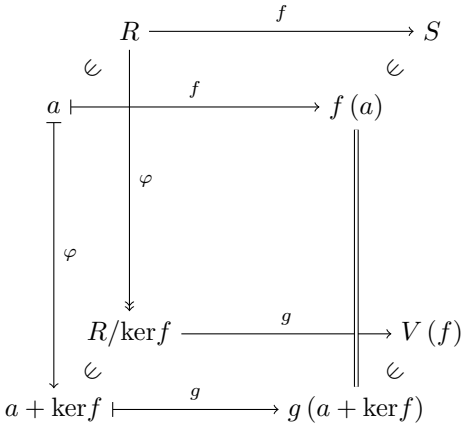
定理 3.2.22 (環準同型定理)**.** 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ の核 $\ker f$ が与えられたとき、その環 R からその商環 $R/\ker f$ への自然な全射環準同型写像を φ とおいた次式のような写像 g は環同型写像である。



これにより、$R/\ker f \cong V(f)$ が成り立つ。

この定理を環準同型定理という。

証明. 2 つの環々 R、S の間の環準同型写像 $f : R \to S$ の核 $\ker f$ が与えられたとき、その環 R からその商環 $R/\ker f$ への自然な全射環準同型写像を φ とおいた次式のような写像 g について、



この環 R の単位元を 1_R、この環 S の零元を 0_S、単位元を 1_S とおくと、その値域の定義より明らかにその写像 g は全射である。また、$g\left(a+\ker f\right)=g\left(b+\ker f\right)$ が成り立つなら、その核 $\ker f$ はその環 R の ideal であることにより次のようになる。

$$\begin{aligned} g\left(a+\ker f\right)=g\left(b+\ker f\right) &\Leftrightarrow f(a)=f(b) \\ &\Leftrightarrow f(a)-f(b)=0_S \\ &\Leftrightarrow f(a)+f(-b)=0_S \\ &\Leftrightarrow f(a-b)=0_S \\ &\Leftrightarrow a-b\in\ker f \\ &\Leftrightarrow b-a\in\ker f \end{aligned}$$

ここで、$b-a\in\ker f$ が成り立つなら、$a\equiv b\ \left(\mathrm{mod}\ker f\right)$ が成り立ち、したがって、$a+\ker f=b+\ker f$ が成り立つので、その写像 g は単射である。以上より、その写像 g は全単射である。

その組 $(\ker f,+)$ は群をなすのであったので、$\forall a+\ker f,b+\ker f\in R/\ker f$ に対し、次のようになる。

$$\begin{aligned} g\left(\left(a+\ker f\right)+\left(b+\ker f\right)\right) &= g\left(\left(a+b\right)+\ker f\right) \\ &= f(a+b) \\ &= f(a)+f(b) \\ &= g\left(a+\ker f\right)+g\left(b+\ker f\right) \\ g\left(\left(a+\ker f\right)\left(b+\ker f\right)\right) &= g\left(ab+\ker f\right) \\ &= f(ab) \\ &= f(a)f(b) \\ &= g\left(a+\ker f\right)g\left(b+\ker f\right) \\ g\left(1_R+\ker f\right) &= f\left(1_R\right)=1_S \end{aligned}$$

これにより、その写像 g は環準同型写像であり、その写像 g は全単射だったので、その写像 g は環同型写像である。

これにより、2 つのそれらの環々 $R/\ker f$、$V(f)$ は、その環 $R/\ker f$ からその環 $V(f)$ への環同型写像 $g:R/\ker f\to V(f)$ が存在するので、環同型である、即ち、$R/\ker f\cong V(f)$ が成り立つ。 □

3.2.6　環同型定理

定理 3.2.23. 2 つの環々 R、S の間の全射環準同型写像 $f : R \twoheadrightarrow S$ について、その環 R の左 ideal$I$、右 ideal$J$ を用いた 2 つの集合たち $V(f|I)$、$V(f|J)$ はそれぞれその環 S の左 ideal、右 ideal である。また、その環 S の左 ideal$I$、右 ideal$J$ を用いた 2 つの集合たち $V\left(f^{-1}|I\right)$、$V\left(f^{-1}|J\right)$ はそれぞれその環 R の左 ideal、右 ideal である。

証明. 2 つの環々 R、S の間の全射環準同型写像 $f : R \twoheadrightarrow S$ について、その環 R の左 ideal$I$ が与えられたとき、$\forall f(a),\ f(b) \in V(f|I)$ に対し、定義より $a+b \in I$ も成り立つので、次のようになる。

$$f(a)+f(b) = f(a+b) \in V(f|I)$$

$\forall f(a) \in V(f|I)\, \forall s \in S$ に対し、その写像 f は全射であるから、$\exists r \in R$ に対し、$f(r) = s$ が成り立ち、定義より $ra \in I$ も成り立つので、次のようになる。

$$\begin{aligned} sf(a) &= f(r)f(a) \\ &= f(ra) \\ &= f(ra) \in V(f|I) \end{aligned}$$

したがって、集合 $V(f|I)$ はその環 S の左 ideal である。同様にして、その環 R の右 ideal$J$ が与えられたとき、集合 $V(f|J)$ はその環 S の右 ideal であることが示される。

また、その環 S の左 ideal$I$ が与えられたとき、環準同型写像の定義と左 ideal の定義より、$\forall a, b \in V\left(f^{-1}|I\right)$ に対し、次のようになる。

$$\begin{aligned} a, b \in V\left(f^{-1}|I\right) &\Rightarrow f(a), f(b) \in V\left(f|V\left(f^{-1}|I\right)\right) \subseteq I \\ &\Rightarrow f(a)+f(b) = f(a+b) \in I \\ &\Rightarrow a+b \in V\left(f^{-1}|I\right) \end{aligned}$$

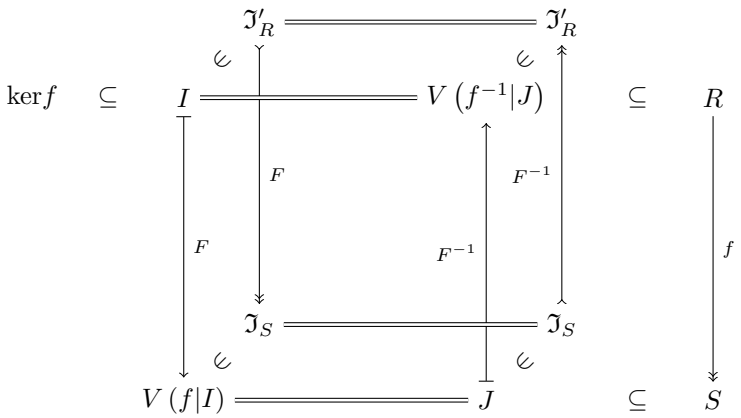
$f(-a) = -f(a)$ が成り立つことと左 ideal の定義より、$\forall a \in V\left(f^{-1}|I\right)\, \forall r \in R$ に対し、次のようになる。

$$\begin{aligned} a \in V\left(f^{-1}|I\right) &\Rightarrow f(a) \in V\left(f|V\left(f^{-1}|I\right)\right) \subseteq I \\ &\Rightarrow f(r)f(a) = f(ra) \in I \\ &\Rightarrow ra \in V\left(f^{-1}|I\right) \end{aligned}$$

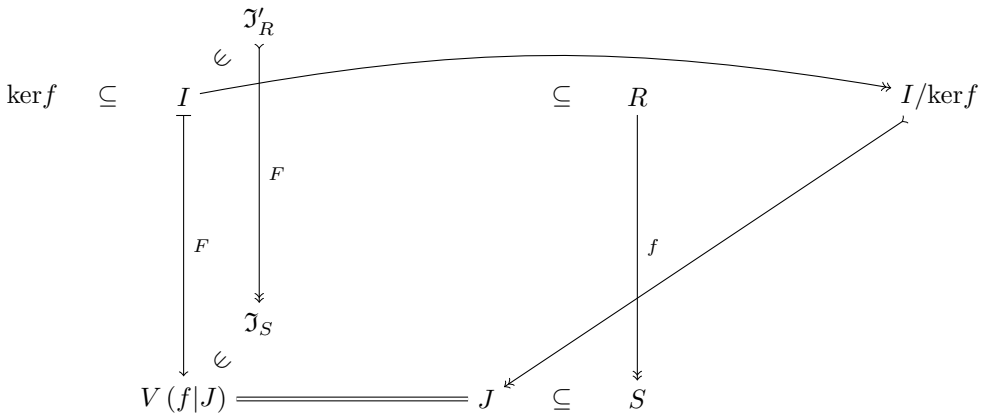
したがって、集合 $V\left(f^{-1}|I\right)$ はその環 R の左 ideal である。同様にして、その環 S の右 ideal$J$ が与えられたとき、集合 $V\left(f^{-1}|J\right)$ はその環 R の右 ideal であることが示される。 □

定理 3.2.24 (環同型定理)**.** 2 つの環々 R、S の間の全射環準同型写像 $f : R \twoheadrightarrow S$ について、その核 $\ker f$ を含むその環 R の左 ideal 全体の集合を $\mathfrak{I}'_R$、その環 S の左 ideal 全体の集合を $\mathfrak{I}_S$ とおくと、次のことが成り立つ。右 ideal についても同様である。この定理を環同型定理という。

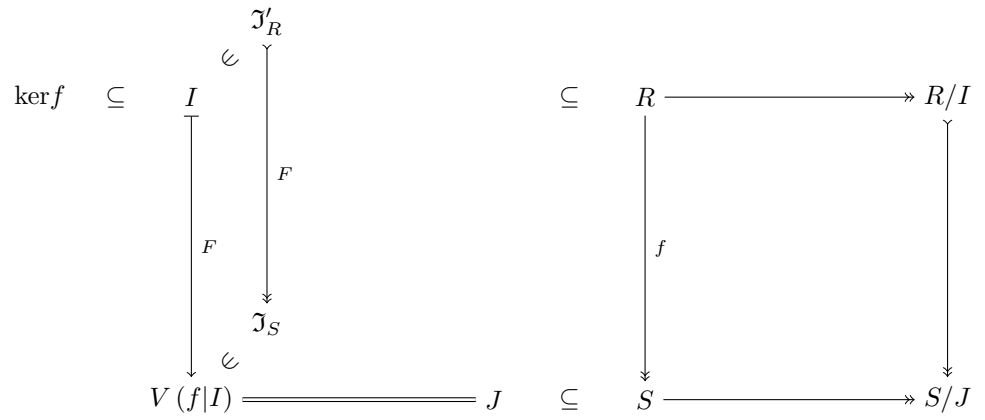
- 次式のように写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V(f|I) = J$ は全単射でその逆写像 F^{-1} が $F^{-1} : \mathfrak{I}_S \to \mathfrak{I}'_R; J \mapsto V\left(f^{-1}|J\right) = I$ と与えられる。これは次式のようにも表される。



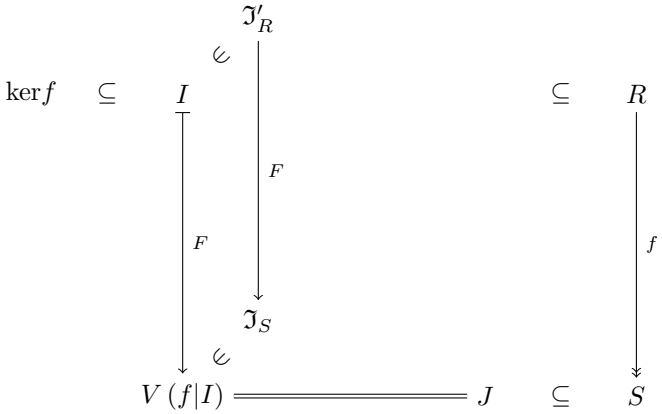
- $\forall I \in \mathfrak{I}'_R$ に対し、$F(I) = V\left(f|I\right) = J$ とおくと、次式のようになり、さらに、$I/\ker f \cong J$ が成り立つ。



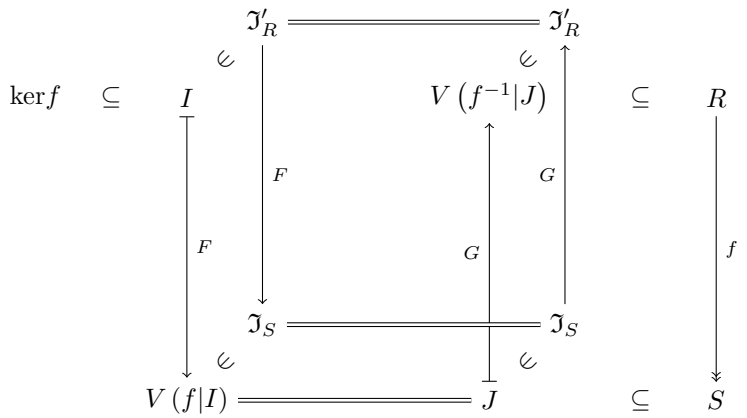
- $\forall I \in \mathfrak{I}'_R$ に対し、その写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V\left(f|I\right)$ が与えられたとき、$F(I) = V\left(f|I\right) = J$ とおくと、その左 ideal$I$ がその環 R の ideal であるならそのときに限り、その左 ideal$J$ がその環 S の ideal である。
- $\forall I \in \mathfrak{I}'_R$ に対し、その写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V\left(f|I\right)$ が与えられたとき、$F(I) = V\left(f|I\right) = J$ とおくと、その左 ideal$I$ がその環 R の ideal であるなら、次式のようになり、さらに、$R/I \cong S/J$ が成り立つ。



証明. 2 つの環々 R、S の間の全射環準同型写像 $f : R \twoheadrightarrow S$ について、その核 $\ker f$ を含むその環 R の左 ideal 全体の集合を $\mathfrak{I}'_R$、その環 S の左 ideal 全体の集合を $\mathfrak{I}_S$ とおきその環 S の零元を 0_S とおく。次式のように写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V(f|I) = J$ を考えよう。



$\forall I \in \mathfrak{I}'_R$ に対し、定理 3.2.23 よりその集合 $V(f|I)$ はその環 S の左 ideal であるので、$V(f|I) \in \mathfrak{I}_S$ が成り立つ。したがって、写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V(f|I)$ が定義できている。ここで、次式のように写像 $G : \mathfrak{I}_S \to \mathfrak{I}'_R; J \mapsto V\left(f^{-1}|J\right) = I$ を考えよう。



$\forall J \in \mathfrak{I}_S$ に対し、定理 3.2.23 よりその集合 $V\left(f^{-1}|J\right)$ はその環 R の左 ideal であるかつ、$\forall a \in J$ に対し、$-a \in J$ が成り立ち、したがって、$a - a = 0_S \in J$ が成り立つことから、$\ker f = V\left(f^{-1}|\{0_S\}\right) \subseteq V\left(f^{-1}|J\right)$ が成り立つので、$V\left(f^{-1}|J\right) \in \mathfrak{I}'_R$ が成り立つ。したがって、写像 $G : \mathfrak{I}_S \to \mathfrak{I}'_R; J \mapsto V\left(f^{-1}|J\right)$ が定義できている。

まず、$G \circ F = I_{\mathfrak{I}'_R}$ が成り立つことを示そう。このとき、$\forall I \in \mathfrak{I}'_R$ に対し、$V\left(f^{-1}|V(f|I)\right) \supseteq I$ は明らかに成り立つ。逆に、$\forall a \in R$ に対し、$a \in V\left(f^{-1}|V(f|I)\right)$ が成り立つなら、$V\left(f|V\left(f^{-1}|V(f|I)\right)\right) = V(f|I)$ が成り立つので、$f(a) \in V(f|I)$ が成り立ち、$\exists a \in I$ に対し、$f(a) = f(b)$ が成り立つ。したがって、次のようになり、

$$\begin{aligned} f(a) = f(b) &\Leftrightarrow f(a) - f(b) = f(a) + f(-b) = f(a-b) = 0_S \\ &\Leftrightarrow a - b \in \ker f \end{aligned}$$

したがって、次のようになる。

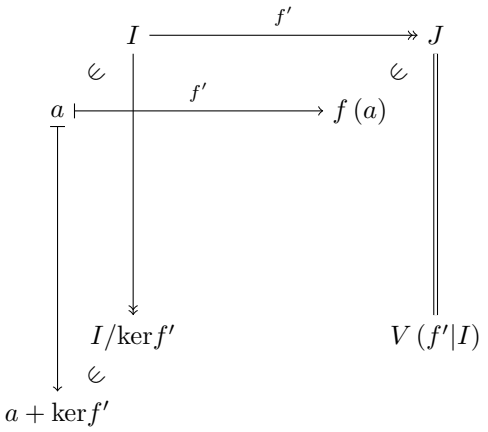
$$\begin{aligned}(a-b)+b &= a+0\\ &= a \in I\end{aligned}$$

以上より、$V\left(f^{-1}|V\left(f|I\right)\right) \subseteq I$ が成り立つ。したがって、$G \circ F(I) = V\left(f^{-1}|V\left(f|I\right)\right) = I$ が成り立つので、$G \circ F = I_{\mathfrak{I}'_R}$ が得られた。

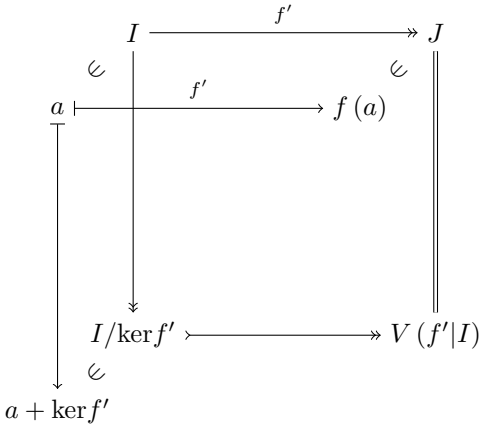
次に、$F \circ G = I_{\mathfrak{I}_S}$ が成り立つことを示そう。もちろん、$\forall J \in \mathfrak{I}_S$ に対し、$V\left(f|V\left(f^{-1}|J\right)\right) \subseteq J$ は成り立つ。逆に、$\forall a \in S$ に対し、$a \in J$ が成り立つなら、その写像 f は全射であるので、$\exists b \in R$ に対し、$f(b) = a$ が成り立つ。$a \in J$ より $V\left(f^{-1}|\{a\}\right) \subseteq V\left(f^{-1}|J\right)$ が成り立つので、$b \in V\left(f^{-1}|\{a\}\right) \subseteq V\left(f^{-1}|J\right)$ が成り立ち、したがって、$f(b) = a \in V\left(f|V\left(f^{-1}|J\right)\right)$ が成り立つ。以上より、$J \subseteq V\left(f|V\left(f^{-1}|J\right)\right)$ が成り立つ。したがって、$F \circ G(J) = V\left(f|V\left(f^{-1}|J\right)\right) = J$ が成り立つので、$F \circ G = I_{\mathfrak{I}_S}$ が得られた。

以上より、$G \circ F = I_{\mathfrak{I}'_R}$ かつ $F \circ G = I_{\mathfrak{I}_S}$ が成り立つ。このようなその写像 $G : \mathfrak{I}_S \to \mathfrak{I}'_R$ が存在するので、その写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S$ は全単射でその写像 G はその写像 F の逆写像である。よって、その写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V\left(f|I\right) = J$ は全単射でその逆写像 F^{-1} が $F^{-1} : \mathfrak{I}_S \to \mathfrak{I}'_R; J \mapsto V\left(f^{-1}|J\right) = I$ と与えられる。

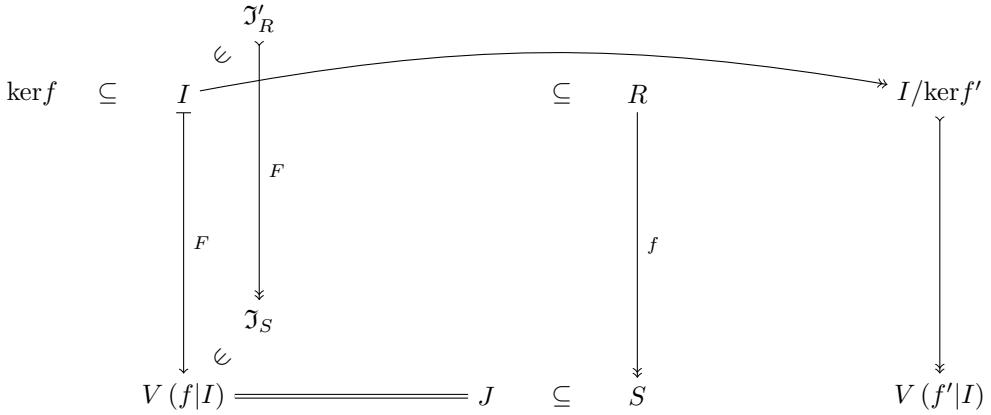
また、$\forall I \in \mathfrak{I}'_R$ に対し、写像 $f' : I \to V\left(f|I\right); a \mapsto f(a)$ を考え $F(I) = V\left(f|I\right) = J$ とおくと、この写像 f' は明らかに全射環準同型写像であるから、次式のように考えられると、



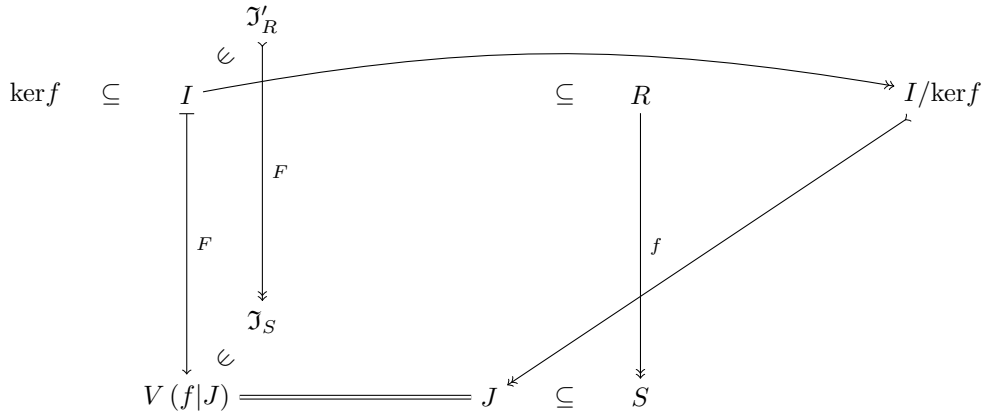
環準同型定理より次式が成り立つので、



次式のようになり、



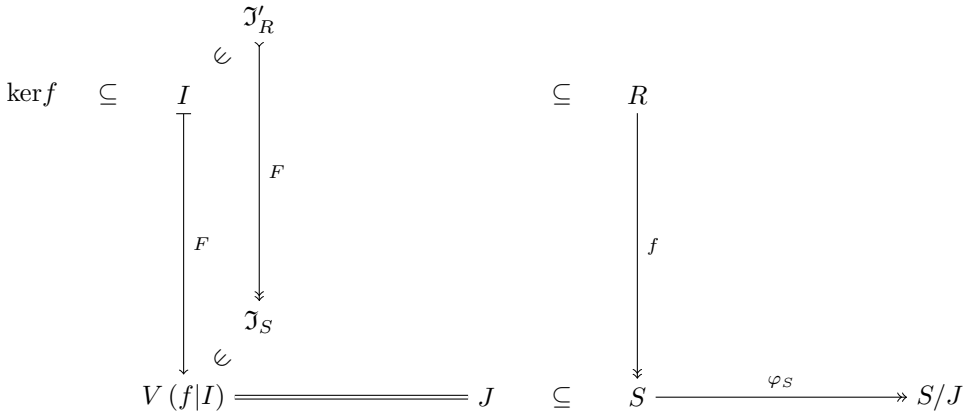
$I/\ker f' \cong V(f'|I)$ が得られる。ここで、$V(f'|I) = V(f|I) = J$ が成り立つかつ、$\ker f' = \ker f$ が成り立つので、次式のようになり、



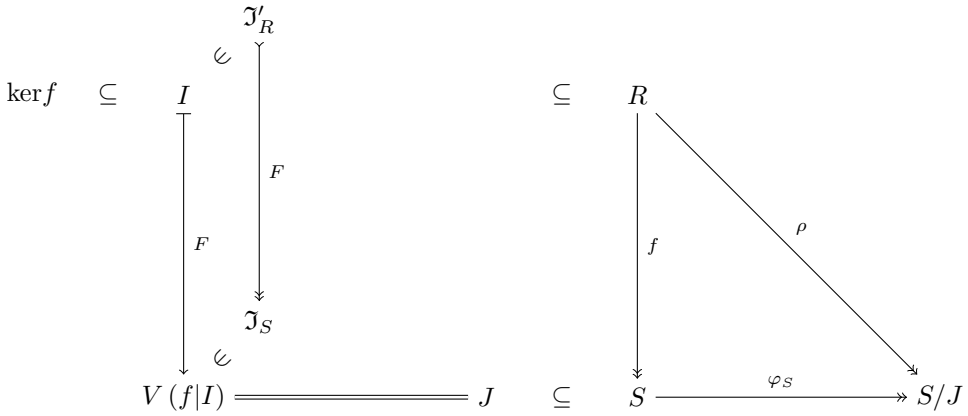
$I/\ker f \cong J$ が成り立つ。

$\forall I \in \mathfrak{I}'_R$ に対し、その写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V(f|I)$ が与えられたとき、$F(I) = V(f|I) = J$ とおくと、定理 3.2.23 よりその左 ideal$I$ がその環 R の ideal であるならそのときに限り、その左 ideal$J$ がその環 S の ideal であることが直ちに分かる。

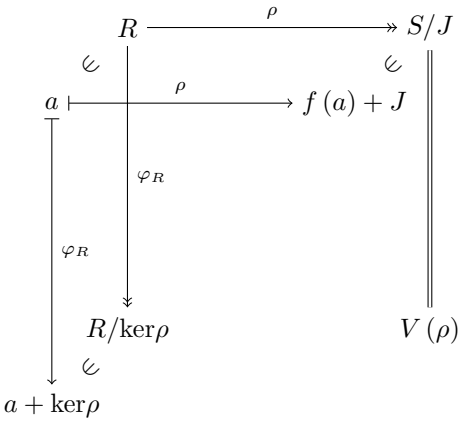
$\forall I \in \mathfrak{I}'_R$ に対し、その写像 $F : \mathfrak{I}'_R \to \mathfrak{I}_S; I \mapsto V(f|I)$ が与えられたとき、$F(I) = V(f|I) = J$ とおくと、その左 ideal$I$ がその環 R の ideal であるなら、上記の議論により集合 J はその環 S の ideal で次式のように自然な全射環準同型写像 $\varphi_S : S \twoheadrightarrow S/J$ を考えると、



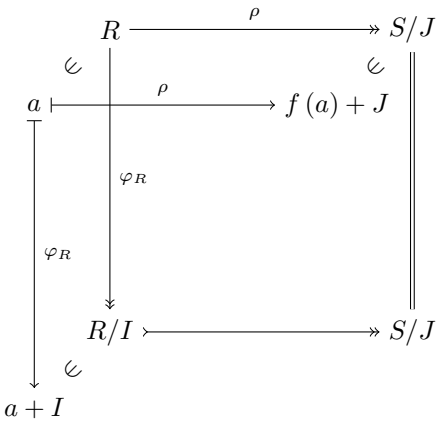
$J = \ker \varphi_S$ が成り立ち、$\varphi_S \circ f = \rho$ とおくと、その写像 ρ は次式のように全射環準同型写像で、



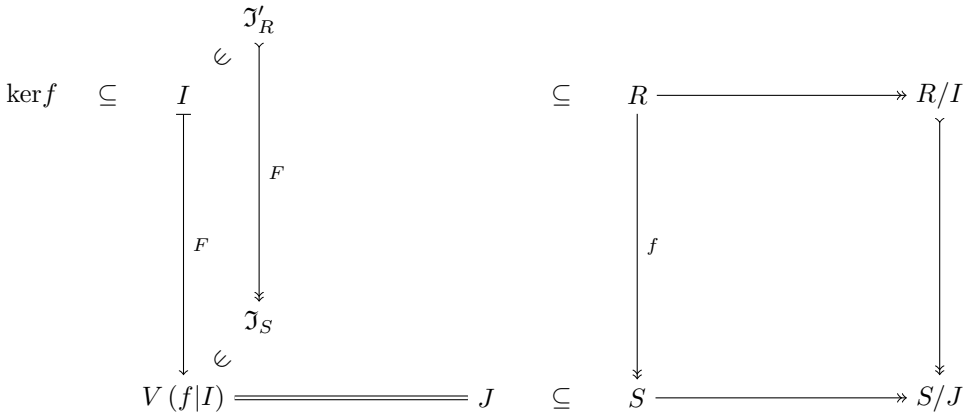
$\forall a \in R$ に対し、$a \in \ker \rho$ が成り立つならそのときに限り、$\rho(a) = f(a) + J = J$ が成り立ち、これが成り立つならそのときに限り、$f(a) \in J$ が成り立つ、即ち、$a \in V\left(f^{-1}|J\right)$ が成り立つ。ここで、上記の議論により $a \in F^{-1}(J) = I$ が成り立つので、$\ker \rho = I$ が得られる。以上より、自然な全射環準同型写像 $\varphi_R : R \twoheadrightarrow R/\ker \rho$ を用いれば、次式のように与えられ、



$\ker \rho = I$ かつ $S/J = V(\rho)$ が成り立つことに注意すれば、環準同型定理より次のようになるので、



次式が成り立ち



$R/I \cong S/J$ が成り立つ。 □

3.2.7 極大 ideal

定義 3.2.13. 環 R のこれ自身でない左 ideal$J$ を含むその環 R の左 ideal がその環 R とその左 ideal$J$ 以外に存在しないとき、その左 ideal$J$ をその環 R の極大左 ideal という。同様に、環 R のこれ自身でない右 ideal$J$ を含むその環 R の右 ideal がその環 R とその右 ideal$J$ 以外に存在しないとき、その右 ideal$J$ をその環 R の極大右 ideal という。

定理 3.2.25. 可換環 R が与えられたとき、その環 R の極大左 ideal と極大右 ideal とは一致する。

定義 3.2.14. 可換環 R での極大左 ideal を単に極大 ideal という。

証明. 可換環 R が与えられたとき、その環 R の極大左 ideal$J$ について、$\forall a \in J \forall r \in R$ に対し、$ra = ar \in J$ が成り立つので、その極大左 ideal$J$ はその環 R の右 ideal でもある。ここで、これを含むその環 R 自身、その右 ideal$J$ 自身でないその環 R の右 idealJ' が存在したとすれば、その環は乗法について可換的なので、$\forall a \in J' \forall r \in R$ に対し、$ar = ra \in J'$ が成り立つので、その右 idealJ' はその環 R の左 ideal でもあり $J \subset J'$ が成り立つが、これはその左 ideal$J$ がその環 R の極大左 ideal であることに矛盾する。したがって、その極大左 ideal$J$ はその環 R の極大右 ideal でもある。極大右 ideal についても同様にして示される。 □

定理 3.2.26. 環 R のこれ自身でない ideal$J$ が与えられたとき、次のことは同値である。

- その商環 R/J は斜体である。
- その ideal$J$ はその環 R の極大左 ideal である。
- その ideal$J$ はその環 R の極大右 ideal である。

証明. 環 R のこれ自身でない ideal$J$ が与えられたとき、その商環 R/J が斜体であるならそのときに限り、定理 3.2.4 よりその商環 R/J はこれ自身か零 ideal 以外の左 ideal をもたないので、これが成り立つならそのときに限り、自然な全射環準同型写像 $\varphi : R \to R/J$ は全射であるから、定理 3.2.24 より次のようになる。

$$V\left(\varphi^{-1}|R/J\right) = R, \quad V\left(\varphi^{-1}|\,(R/J)\,0\right) = J$$

これがその左 ideal$J$ を含むその環 R の左 ideal 全てであるから、その ideal$J$ はその環 R の極大左 ideal である。ゆえに、次のことは同値である。

- その商環 R/J は斜体である。
- その ideal$J$ はその環 R の極大左 ideal である。

同様にして次のことは同値であることが示される。

- その商環 R/J は斜体である。
- その ideal$J$ はその環 R の極大左 ideal である。

□

定理 3.2.27. 可換環 R のこれ自身でない ideal$J$ が与えられたとき、その商環 R/J が斜体であるならそのときに限り、その ideal$J$ はその環 R の極大 ideal である。

証明. 可換環 R のこれ自身でない ideal$J$ が与えられたとき、その商環 R/J が斜体であるならそのときに限り、定理 3.2.26 よりその ideal$J$ はその環 R の極大左 ideal であった。ここで、定理 3.2.25 よりその極大左 ideal$J$ はその環 R の極大 ideal でもある。 □

3.2.8 素 ideal

定義 3.2.15. 可換環 R の ideal$P$ がその環 R 自身でなく、$\forall a, b \in R$ に対し、$ab \in P$ が成り立つなら、$a \in P$ または $b \in P$ が成り立つとき、その ideal$P$ をその環 R の素 ideal という。

定理 3.2.28. 可換環 R の ideal$P$ が与えられたとき、その ideal$P$ がその環 R の素 ideal であるならそのときに限り、その商環 R/P は整域である。

証明. 可換環 R の ideal$P$ が与えられたとき、その商環 R/P はもちろん可換環である。その ideal$P$ がその環 R の素 ideal であるなら、$\exists a + P, b + P \in R/P$ に対し、$a + P \neq P$ かつ $b + P \neq P$ が成り立つかつ、$(a + P)(b + P) = P$ が成り立つと仮定しよう。このとき、次のようになるので、

$$(a + P)(b + P) = ab + P = P$$

$ab \equiv 0 \bmod P$ が成り立つ、即ち、$ab \in P$ が成り立つので、$a \in P$ または $b \in P$ が成り立つ。ここで、$a \in P$ とすれば、$a \equiv 0 \bmod P$ が成り立つ、即ち、$a + P = P$ が成り立つことになるが、これは仮定に矛盾する。

$b \in P$ についても同様であるから、$a+P \neq P$ かつ $b+P \neq P$ が成り立つかつ、$(a+P)(b+P) = P$ が成り立つことは矛盾している。したがって、$\forall a+P, b+P \in R/P$ に対し、$a+P \neq P$ かつ $b+P \neq P$ が成り立つなら、$(a+P)(b+P) \neq P$ が成り立つことになる、即ち、その商環 R/P は整域である。

逆に、その商環 R/P が整域であるとすると、$\forall a, b \in P$ に対し、$a \notin P$ かつ $b \notin P$ が成り立つなら、$a \equiv 0 \bmod P$ または $b \equiv 0 \bmod P$ が成り立たないので、$a+P \neq P$ かつ $b+P \neq P$ が成り立ち、したがって、$(a+P)(b+P) \neq P$ が成り立つことになる。ゆえに、$ab+P \neq P$ が成り立つので、$ab \equiv 0 \bmod P$ が成り立たない、即ち、$ab \notin P$ が成り立つことになる。対偶律よりその ideal$P$ は素 ideal でもある。 □

定理 3.2.29. 可換環 R の極大 ideal は素 ideal である。

証明. 可換環 R の極大 ideal$P$ が与えられたとき、定理 3.2.27 よりその商環 R/P は斜体であり、さらに、零因子をもたない。また、その環 R は乗法について可換的で、もちろん、その商環 R/P も可換的であるので、その商環 R/P は整域である。定理 3.2.28 よりよって、可換環 R の極大 ideal$P$ は素 ideal である。 □

3.2.9 商の体

定理 3.2.30. 体 K の部分環 K' が与えられたとき、その環 K' は整域である。

証明. 体 K の部分環 K' が与えられたとき、$\forall a, b \in K'$ に対し、$a, b \in K$ が成り立つので、$ab = ba$ が成り立つ。したがって、その環 K' は可換環である。さらに、その環 K' が零因子をもつとすれば、その零因子はその体 K の元でもあるので、体の定義に矛盾する。したがって、その環 K' は零因子をもたない。ゆえに、その環 K' は整域である。 □

定理 3.2.31. 零環でない環 R から体 K への単射環準同型写像 $f : R \to K$ が存在するなら、その環 R は整域である。

証明. 零環でない環 R から体 K への単射環準同型写像 $f : R \to K$ が存在するなら、その値域 $V(f)$ は定理 3.2.18 よりその体 K の部分環であり、定理 3.2.30 よりその環 $V(f)$ は整域である。ここで、写像 $f' : R \to V(f); a \mapsto f(a)$ は全単射で、さらに、環同型写像でもある。したがって、環同型写像 $f'^{-1} : V(f) \to R$ が存在し $\forall a, b \in R$ に対し、次のようになる。

$$\begin{aligned} ab &= f^{-1} \circ f(ab) \\ &= f^{-1}\left(f(ab)\right) \\ &= f^{-1}\left(f(a)f(b)\right) \\ &= f^{-1}\left(f(b)f(a)\right) \\ &= f^{-1}\left(f(ba)\right) \\ &= f^{-1} \circ f(ba) = ba \end{aligned}$$

ゆえに、その環 R は可換環である。

さらに、その環 R が零因子をもつと仮定すると、$\exists a, b \in R$ に対し、$a \neq 0$ かつ $b \neq 0$ が成り立つなら、$ab = 0$ が成り立つことになる。このとき、$f(a) \neq 0$ かつ $f(b) \neq 0$ が成り立ち、したがって、$f(a)f(b) = f(ab) = f(0) = 0$ が成り立つによりその環 $V(f)$ は零因子をもつことになるが、これはその環 $V(f)$ が整域であることに矛盾する。ゆえに、その環 R は零因子をもたない。

以上よりよって、その環 R は整域である。 □

定義 3.2.16. 2 つの環々 R_1、R_2 の間の単射環準同型写像 $f : R_1 \to R_2$ が与えられたとき、その値域 $V(f)$ はその環 R_2 の部分環となるのであった。ここで、その値域 $V(f)$ をその環 R_1 と同一視するとき、その写像 f をその環 R_1 のその環 R_2 への埋め込みという。このような埋め込みが存在するとき、その環 R_1 はその環 R_2 へ埋め込み可能であるという。

定義 3.2.17. 体 K の部分環 K' が与えられたとき、$\forall a, b \in K'$ に対し、$a\frac{1}{b}$ を $\frac{a}{b}$ と書く。

定理 3.2.32. 体 K の部分環 K' が与えられたとき、$\forall a, b, c, d \in K'$ に対し、定義可能であるかぎり次式が成り立つ。

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

証明. 体 K の部分環 K' が与えられたとき、$\forall a, b, c, d \in K'$ に対し、定義可能であるかぎり次のようになる。

$$\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= a\frac{1}{b} + c\frac{1}{d} \\
&= ad\frac{1}{d}\frac{1}{b} + cb\frac{1}{b}\frac{1}{d} \\
&= ad\frac{1}{bd} + cb\frac{1}{db} \\
&= ad\frac{1}{bd} + bc\frac{1}{bd} \\
&= (ad + bc)\frac{1}{bd} \\
&= \frac{ad + bc}{bd} \\
\frac{a}{b}\frac{c}{d} &= a\frac{1}{b}c\frac{1}{d} \\
&= ac\frac{1}{b}\frac{1}{d} \\
&= ac\frac{1}{db}ac\frac{1}{bd} \\
&= \frac{ac}{bd}
\end{aligned}$$

□

定理 3.2.33. 体 K の部分環 K' が与えられたとき、次式のようにして定義される集合 L は

$$L = \left\{ \frac{a}{b} \in K \middle| a, b \in K' \right\}$$

その体 K の部分体である。さらに、その集合 L はその部分環 K' を含むその体 K の部分体たちのうち順序関係 $\subseteq$ の意味で最小なものである。

定義 3.2.18. その集合 L をその部分環 K' のその体 K における商の体、分数体という。

証明. 体 K の部分環 K' が与えられたとき、次式のようにして定義される集合 L について、

$$L = \left\{ \frac{a}{b} \in K \middle| a, b \in K', \ \ b \neq 0 \right\}$$

定理 3.1.14 より $1 \in K'$ が成り立つので、$\frac{1}{1} = 1 \in L$ が成り立つ。さらに、$\forall \frac{a}{b}, \frac{c}{d} \in L$ に対し、$-a \in K'$ が成り立つので、$-\frac{a}{b} = \frac{-a}{b} \in L$ が成り立つかつ、定理 3.2.32 より $\frac{a}{b} + \frac{c}{d}, \frac{a}{b}\frac{c}{d} \in L$ が成り立つので、定理 3.1.14

よりその集合 L はその体 K の部分環である。さらに、$\forall \frac{a}{b}, \frac{c}{d} \in L$ に対し、次のようになることから、

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\frac{a}{b}$$

その部分環 L は可換環である。ここで、$\forall \frac{a}{b} \in L$ に対し、$\frac{a}{b} \neq 0$ が成り立つなら、$a \neq 0$ かつ $\frac{1}{b} \neq 0$ が成り立つ。$a \in K$ が成り立つので、元 $\frac{1}{a}$ がその体 K に存在し $\frac{b}{a} \in L$ が成り立つ。ゆえに、その部分環 L は斜体である。よって、その集合 L はその体 K の部分体である。

さらに、$\forall a \in K'$ に対し、$a = \frac{a}{1} \in L$ が成り立つので、$K' \subseteq L$ が成り立つ。ここで、その集合 L はその部分環 K' を含むその体 K の部分体 K'' が与えられたとき、$\forall \frac{a}{b} \in L$ に対し、$a, b \in K'$ が成り立つので、$a, b \in K''$ が成り立ち、$b \neq 0$ より体の定義より $\frac{1}{b} \in K''$ が成り立つことになる。定理 3.1.14 より $\frac{a}{b} = a\frac{1}{b} \in K''$ が成り立つことになるので、$L \subseteq K''$ が成り立つ。よって、その集合 L はその部分環 K' を含むその体 K の部分体たちのうち順序関係 $\subseteq$ の意味で最小なものである。 □

3.2.10 整域からの埋め込みによる体の構成

定理 3.2.34. 整域 R が与えられたとき、次のことを満たすような体 L と環準同型写像 $\varphi : R \to L$ が存在する。

- その写像 φ はその整域 R のその体 L への埋め込みである。
- $\forall l \in L$ に対し、その整域 R の元々 a、b が存在して $b \neq 0$ が成り立つかつ、$l = \frac{\varphi(a)}{\varphi(b)}$ が成り立つ。

詳しくいえば、その体 L は、集合 $R \times R \setminus \{0\}$ の元々 (a, b)、(c, d) に対し、$ad = cb$ が成り立つとき、$(a, b)\, D\, (c, d)$ と関係 D が定義されたときの商集合 $(R \times R \setminus \{0\})/D$ で、$\forall C_D(a, b), C_D(c, d) \in (R \times R \setminus \{0\})/D$ に対し、次式のように定義される。

$$C_D(a, b) + C_D(c, d) = C_D(ad + bc, bd), \quad C_D(a, b)C_D(c, d) = C_D(ac, bd)$$

このときの零元、単位元はそれぞれ $C_D(0, 1)$、$C_D(1, 1)$ である。また、その写像 φ も次式のように定義される。

$$\varphi : R \to L; a \mapsto C_D(a, 1)$$

定義 3.2.19. このときの体 L をその整域 R の商の体、分数体という。

証明. 整域 R が与えられたとき、集合 $R \times R \setminus \{0\}$ の元々 (a, b)、(c, d) に対し、$ad = cb$ が成り立つとき、$(a, b)D(c, d)$ と関係 D が定義される。このとき、$ab = ab$ が成り立つので、$(a, b)D(a, b)$ が成り立つ。$(a, b)D(c, d)$ が成り立つなら、$ad = cb$ が成り立つならそのときに限り、$cb = ad$ が成り立つので、$(c, d)D(a, b)$ が成り立つ。最後に、$(a, b)D(c, d)$ かつ $(c, d)D(e, f)$ が成り立つなら、$ad = cb$ かつ $cf = ed$ が成り立つので、$adf = cbf = cfb = edb$ が成り立ち、したがって、$adf - edb = (af - eb)d = 0$ が成り立つ。ここで、その環 R は整域であるから、$d \neq 0$ より $af - eb = 0$ が成り立つ。ゆえに、$af = eb$ が得られ $(a, b)D(e, f)$ が成り立つので、その関係 D は同値関係である。

したがって、商集合 $(R \times R \setminus \{0\})/D$ が得られる。ここで、$\forall C_D(a, b), C_D(c, d) \in (R \times R \setminus \{0\})/D$ に対し、次式のように定義されるとする。

$$C_D(a, b) + C_D(c, d) = C_D(ad + bc, bd), \quad C_D(a, b)C_D(c, d) = C_D(ac, bd)$$

このとき、$C_D(a,b) = C_D\left(a',b'\right)$ かつ $C_D(c,d) = C_D\left(c',d'\right)$ が成り立つなら、次のようになることから、

$$\begin{aligned}(ad+bc)b'd' &= ab'dd' + bb'cd' \\ &= a'bdd' + bb'c'd \\ &= \left(a'd' + b'c'\right)bd \\ acb'd' &= ab'cd' \\ &= a'bc'd \\ &= a'c'bd\end{aligned}$$

次式が成り立つ。

$$\begin{aligned}C_D(a,b) + C_D(c,d) &= C_D(ad+bc,bd) \\ &= C_D\left(a'd' + b'c', b'd'\right) \\ &= C_D\left(a',b'\right) + C_D\left(c',d'\right) \\ C_D(a,b)C_D(c,d) &= C_D(ac,bd) \\ &= C_D\left(a'c',b'd'\right) \\ &= C_D\left(a',b'\right)C_D\left(c',d'\right)\end{aligned}$$

ここで、$\forall C_D(a,b), C_D(c,d), C_D(e,f) \in (R \times R \setminus \{0\})/D$ に対し、次のようになるので、

$$\begin{aligned}\left(C_D(a,b) + C_D(c,d)\right) + C_D(e,f) &= C_D(ad+bc,bd) + C_D(e,f) \\ &= C_D\left((ad+bc)f + bde, bdf\right) \\ &= C_D(adf + cfb + ebd, bdf) \\ &= C_D\left(dfa + (cf+de)b, bdf\right) \\ &= C_D(a,b) + C_D(cf+de,df) \\ &= C_D(a,b) + \left(C_D(c,d) + C_D(e,f)\right) \\ C_D(a,b) + C_D(0,1) &= C_D(a1+b0,b1) = C_D(a,b) \\ C_D(0,1) + C_D(a,b) &= C_D(0b+1a,1b) = C_D(a,b) \\ C_D(a,b) + C_D(-a,b) &= C_D\left(ab-ba,b^2\right) = C_D(0,1) \\ C_D(-a,b) + C_D(a,b) &= C_D\left(-ab+ba,b^2\right) = C_D(0,1) \\ C_D(a,b) + C_D(c,d) &= C_D(ad+bc,bd) \\ &= C_D(cb+da,db) \\ &= C_D(c,d) + C_D(a,b)\end{aligned}$$

その組 $((R \times R \setminus \{0\})/D, +)$ は可換群をなす。さらに、次のようになるので、

$$\begin{aligned}\left(C_D(a,b)C_D(c,d)\right)C_D(e,f) &= C_D(ac,bd)C_D(e,f) \\ &= C_D\left((ac)e,(bd)f\right) \\ &= C_D\left(a(ce),b(df)\right) \\ &= C_D(a,b)C_D(ce,df) \\ &= C_D(a,b)\left(C_D(c,d)C_D(e,f)\right) \\ C_D(a,b)\left(C_D(c,d) + C_D(e,f)\right) &= C_D(a,b)C_D(cf+de,df) \\ &= C_D\left(a(cf+de),bdf\right) \\ &= C_D(acf+ade,bdf)\end{aligned}$$

$$
\begin{aligned}
&= C_D\left(acbf + aebd, b^2df\right) \\
&= C_D(ac, bd) + C_D(ae, bf) \\
&= C_D(a, b)C_D(c, d) + C_D(a, b)C_D(e, f) \\
\left(C_D(a, b) + C_D(c, d)\right) C_D(e, f) &= C_D(ad + bc, bd)C_D(e, f) \\
&= C_D\left((ad + bc)e, bdf\right) \\
&= C_D(aed + ceb, bdf) \\
&= C_D\left(aedf + cebf, bdf^2\right) \\
&= C_D(ae, bf) + C_D(ce, df) \\
&= C_D(a, b)C_D(e, f) + C_D(c, d)C_D(e, f) \\
C_D(a, b)C_D(1, 1) &= C_D(a1, b1) = C_D(a, b) \\
C_D(1, 1)C_D(a, b) &= C_D(1a, 1b) = C_D(a, b) \\
C_D(a, b)C_D(c, d) &= C_D(ac, bd) \\
&= C_D(ca, db) \\
&= C_D(c, d)C_D(a, b)
\end{aligned}
$$

その集合 $(R \times R \setminus \{0\})/D$ は可換環をなす。

さらに、$\forall C_D(a, b) \in (R \times R \setminus \{0\})/D$ に対し、$C_D(a, b) \neq C_D(0, 1)$ が成り立つなら、$a = a1 \neq 0b = b$ が成り立つので、$a \in R \setminus \{0\}$ が成り立ち、したがって、$C_D(b, a) \in (R \times R \setminus \{0\})/D$ なるものが存在する。ここで、次のようになるので、

$$
\begin{aligned}
C_D(a, b)C_D(b, a) &= C_D(ab, ba) \\
&= C_D(ab, ab) \\
&= C_D(1, 1) \\
C_D(b, a)C_D(a, b) &= C_D(ba, ab) \\
&= C_D(ab, ab) \\
&= C_D(1, 1)
\end{aligned}
$$

その元 $C_D(a, b)$ は可逆元である。よって、その集合 $(R \times R \setminus \{0\})/D$ は体をなす。

ここで、その集合 $(R \times R \setminus \{0\})/D$ が L とおかれ次式のように写像 φ が定義されると、

$$
\varphi : R \to L; a \mapsto C_D(a, 1)
$$

$\forall C_D(a, 1), C_D(c, 1) \in V(\varphi)$ に対し、$C_D(a, 1) = C_D(c, 1)$ が成り立つなら、$a = a1 = c1 = c$ が得られるので、その写像 φ は単射である。さらに、$\forall a, b \in R$ に対し、次のようになるので、

$$
\begin{aligned}
\varphi(a + b) &= C_D(a + b, 1) \\
&= C_D(a1 + b1, 1) \\
&= C_D(a, 1) + C_D(b, 1) \\
&= \varphi(a) + \varphi(b) \\
\varphi(ab) &= C_D(ab, 1) \\
&= C_D(a, 1)C_D(b, 1) \\
&= \varphi(a)\varphi(b)
\end{aligned}
$$

その写像 φ は単射環準同型写像である。ゆえに、その写像 φ はその整域 R のその体 L への埋め込みである。

さらに、$\forall C_D(a,b) \in L$ に対し、その整域の元々 a、b が存在して $b \neq 0$ が成り立つかつ、次のようになる。

$$\begin{aligned} C_D(a,b) &= C_D(a1, 1b) \\ &= C_D(a,1)C_D(1,b) \\ &= C_D(a,1)\frac{1}{C_D(b,1)} \\ &= \frac{C_D(a,1)}{C_D(b,1)} = \frac{\varphi(a)}{\varphi(b)} \end{aligned}$$

□

定理 3.2.35. 整域 R から体 K への埋め込み $f : R \to K$ が与えられたとき、その整域 R の商の体 L のその体 K への埋め込み $f^* : L \to K$ でその埋め込み f の延長となっているものがただ 1 つ存在する。

証明. 整域 R から体 K への埋め込み $f : R \to K$ が与えられたとき、定理 3.2.34 より次式のような写像 $f^* : L \to K$ が定義されると、

$$f^* : L \to K; \frac{a}{b} \mapsto \frac{f(a)}{f(b)}$$

$\forall \frac{a}{b}, \frac{c}{d} \in L$ に対し、定理 3.2.32 より次のようになるので、

$$\begin{aligned} f^*\left(\frac{a}{b} + \frac{c}{d}\right) &= f^*\left(\frac{ad+bc}{bd}\right) \\ &= \frac{f(ad+bc)}{f(bd)} \\ &= \frac{f(a)f(d)+f(b)f(c)}{f(b)f(d)} \\ &= \frac{f(a)}{f(b)} + \frac{f(c)}{f(d)} \\ &= f^*\left(\frac{a}{b}\right) + f^*\left(\frac{c}{d}\right) \\ f^*\left(\frac{a}{b}\frac{c}{d}\right) &= f^*\left(\frac{ac}{bd}\right) \\ &= \frac{f(ac)}{f(bd)} \\ &= \frac{f(a)f(c)}{f(b)f(d)} \\ &= \frac{f(a)}{f(b)}\frac{f(c)}{f(d)} \\ &= f^*\left(\frac{a}{b}\right) f^*\left(\frac{c}{d}\right) \\ f^*(1) &= f^*\left(\frac{1}{1}\right) \\ &= \frac{f(1)}{f(1)} = \frac{1}{1} = 1 \end{aligned}$$

その写像 f^* は環準同型写像である。さらに、$\forall f^*\left(\frac{a}{b}\right), f^*\left(\frac{c}{d}\right) \in V(f^*)$ に対し、$f^*\left(\frac{a}{b}\right) = f^*\left(\frac{c}{d}\right)$ が成り立つなら、次のようになるので、

$$f^*\left(\frac{a}{b}\right) = f^*\left(\frac{c}{d}\right) \Leftrightarrow \frac{f(a)}{f(b)} = \frac{f(c)}{f(d)}$$

$$
\begin{aligned}
&\Leftrightarrow f(a)f(d) = f(b)f(c) \\
&\Leftrightarrow f(ad) = f(bc) \\
&\Rightarrow ad = bc \\
&\Leftrightarrow \frac{a}{b} = \frac{c}{d}
\end{aligned}
$$

その写像 f^* は単射環準同型写像である。したがって、その写像 f^* はその整域 R の商の体 L のその体 K への埋め込みである。

さらに、$\forall \frac{a}{1} \in L$ に対し、次のようになるので、

$$
f^* \left(\frac{a}{1} \right) = \frac{f(a)}{f(1)} = \frac{f(a)}{1}
$$

確かにその写像 f^* はその埋め込み f の延長となっている。

最後に、その整域 R の商の体 L のその体 K への埋め込み $f^* : L \to K$ でその埋め込み f の延長となっているものがこの写像 f^* のほかに存在すると仮定しこれを f^{**} とおこう。このとき、$\forall \frac{a}{b} \in L$ に対し、その写像 f^{**} は環準同型写像であるから、次のようになる。

$$
\begin{aligned}
f^{**} \left(\frac{a}{b} \right) &= f^{**} \left(\frac{a}{1} \frac{1}{b} \right) \\
&= f^{**} \left(\frac{a}{1} \right) f^{**} \left(\frac{1}{b} \right)
\end{aligned}
$$

ここで、次式が成り立つので、

$$
\begin{aligned}
f^{**} \left(\frac{1}{b} \right) f^{**} \left(\frac{b}{1} \right) &= f^{**} \left(\frac{1}{b} \frac{b}{1} \right) \\
&= f^{**} \left(\frac{b}{b} \right) \\
&= f^{**}(1) = 1 \\
f^{**} \left(\frac{b}{1} \right) f^{**} \left(\frac{1}{b} \right) &= f^{**} \left(\frac{b}{1} \frac{1}{b} \right) \\
&= f^{**} \left(\frac{b}{b} \right) \\
&= f^{**}(1) = 1
\end{aligned}
$$

次のようになる。

$$
\begin{aligned}
f^{**} \left(\frac{a}{b} \right) &= f^{**} \left(\frac{a}{1} \right) \frac{1}{f^{**} \left(\frac{b}{1} \right)} \\
&= \frac{f^{**} \left(\frac{a}{1} \right)}{f^{**} \left(\frac{b}{1} \right)}
\end{aligned}
$$

さらに、その写像 f^{**} はその埋め込み f の延長となっているので、次のようになる。

$$
\begin{aligned}
f^{**} \left(\frac{a}{b} \right) &= \frac{f^{**} \left(\frac{a}{1} \right)}{f^{**} \left(\frac{b}{1} \right)} \\
&= \frac{f(a)}{f(b)}
\end{aligned}
$$

$$= f^*\left(\frac{a}{b}\right)$$

したがって、$f^{**} = f^*$ が成り立つことになるが、これは仮定に矛盾している。よって、その整域 R の商の体 L のその体 K への埋め込み $f^* : L \to K$ でその埋め込み f の延長となっているものがただ 1 つ存在する。 □

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976. 新装版第 2 刷 p57-58,65-73,123-128,130-134 ISBN978-4-00-029873-5

3.3　多項式環

3.3.1　非負整数全体の集合から零環でない可換環への写像

定義 3.3.1. 非負整数、即ち、負でない整数全体の集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、元の列の定義と同じようにして、$\forall f\in\widetilde{P}$ に対し、次式のように書かれる。

$$f=(f(n))_{n\in\mathbb{N}\cup\{0\}}=(f(0),f(1),f(2),\cdots)$$

定義 3.3.2. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、$\forall f,g\in\widetilde{P}$ に対し、次式のように定義される。

$$f+g=(f(n)+g(n))_{n\in\mathbb{N}\cup\{0\}},\quad fg=\left(\sum_{i+j=n}f(i)g(j)\right)_{n\in\mathbb{N}\cup\{0\}}$$

定義 3.3.3. 次式のように定義される写像を Kronecker の δ という。

$$\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z};\binom{i}{j}\mapsto\delta_i^j=\begin{cases}1 & \text{if} \quad i=j\\ 0 & \text{otherwise}\end{cases}$$

定義 3.3.4. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、$\forall a\in R$ に対し、次式のようにその集合 $\widetilde{P}$ の元 $\overline{a}$ が定義される。

$$\overline{a}=\left(a\delta_n^0\right)_{n\in\mathbb{N}\cup\{0\}}$$

定理 3.3.1. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ は可換環をなす。このとき、零元、単位元はそれぞれ $\overline{0}$、$\overline{1}$ と、その元 f に対する元 $-f$ は次式のように与えられる。

$$-f=(-f(n))_{n\in\mathbb{N}\cup\{0\}}$$

証明. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、$\forall f,g,h\in\widetilde{P}$ に対し、その元 f に対する元 $-f$ は次式のようにおかれると、

$$-f=(-f(n))_{n\in\mathbb{N}\cup\{0\}}$$

次のようになる。

$$\begin{aligned}(f+g)+h&=\Big((f(n))_{n\in\mathbb{N}\cup\{0\}}+(g(n))_{n\in\mathbb{N}\cup\{0\}}\Big)+(h(n))_{n\in\mathbb{N}\cup\{0\}}\\&=(f(n)+g(n))_{n\in\mathbb{N}\cup\{0\}}+(h(n))_{n\in\mathbb{N}\cup\{0\}}\\&=((f(n)+g(n))+h(n))_{n\in\mathbb{N}\cup\{0\}}\\&=(f(n)+(g(n)+h(n)))_{n\in\mathbb{N}\cup\{0\}}\\&=(f(n))_{n\in\mathbb{N}\cup\{0\}}+(g(n)+h(n))_{n\in\mathbb{N}\cup\{0\}}\\&=(f(n))_{n\in\mathbb{N}\cup\{0\}}+\Big((g(n))_{n\in\mathbb{N}\cup\{0\}}+(h(n))_{n\in\mathbb{N}\cup\{0\}}\Big)\\&=f+(g+h)\\f+\overline{0}&=(f(n))_{n\in\mathbb{N}\cup\{0\}}+(0)_{n\in\mathbb{N}\cup\{0\}}\\&=(f(n)+0)_{n\in\mathbb{N}\cup\{0\}}\end{aligned}$$

$$
\begin{aligned}
&= (f(n))_{n\in\mathbb{N}\cup\{0\}} = f \\
\overline{0} + f &= (0)_{n\in\mathbb{N}\cup\{0\}} + (f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (0 + f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (f(n))_{n\in\mathbb{N}\cup\{0\}} = f \\
f - f &= (f(n))_{n\in\mathbb{N}\cup\{0\}} + (-f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (f(n) - f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (0)_{n\in\mathbb{N}\cup\{0\}} = \overline{0} \\
-f + f &= (-f(n))_{n\in\mathbb{N}\cup\{0\}} + (f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (-f(n) + f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (0)_{n\in\mathbb{N}\cup\{0\}} = \overline{0} \\
f + g &= (f(n))_{n\in\mathbb{N}\cup\{0\}} + (g(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (f(n) + g(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (g(n) + f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= (g(n))_{n\in\mathbb{N}\cup\{0\}} + (f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= g + f
\end{aligned}
$$

以上より、その組 $\left(\widetilde{P}, +\right)$ は可換群をなす。

さらに、$\forall f, g, h \in \widetilde{P}$ に対し、次のようになる。

$$
\begin{aligned}
(fg)h &= \left((f(n))_{n\in\mathbb{N}\cup\{0\}} (g(n))_{n\in\mathbb{N}\cup\{0\}}\right) (h(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{i+j=n} f(i)g(j)\right)_{n\in\mathbb{N}\cup\{0\}} (h(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{k+l=n}\sum_{i+j=k} f(i)g(j)h(l)\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i+j=k \\ k+l=n}} f(i)g(j)h(l)\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{i+j+k=n} f(i)g(j)h(k)\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i+j=k \\ k+l=n}} f(l)g(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{k+l=n} f(l) \sum_{i+j=k} g(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= (f(n))_{n\in\mathbb{N}\cup\{0\}} \left(\sum_{i+j=n} g(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}}
\end{aligned}
$$

$$
\begin{aligned}
&= (f(n))_{n\in\mathbb{N}\cup\{0\}} \left((g(n))_{n\in\mathbb{N}\cup\{0\}} (h(n))_{n\in\mathbb{N}\cup\{0\}} \right) = f(gh) \\
f\overline{1} &= (f(n))_{n\in\mathbb{N}\cup\{0\}} \left(\delta_n^0\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{i+j=n} f(i)\delta_j^0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i+j=n \\ j=0}} f(i)\delta_j^0 + \sum_{\substack{i+j=n \\ j\neq 0}} f(i)\delta_j^0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i+j=n \\ j=0}} f(i) + \sum_{\substack{i+j=n \\ j\neq 0}} 0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i=n \\ j=0}} f(i) + 0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{i=n} f(i) \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= (f(n))_{n\in\mathbb{N}\cup\{0\}} = f \\
\overline{1}f &= \left(f(i)\delta_n^0\right)_{n\in\mathbb{N}\cup\{0\}} (f(n))_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{i+j=n} \delta_j^0 f(i) \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i+j=n \\ j=0}} \delta_j^0 f(i) + \sum_{\substack{i+j=n \\ j\neq 0}} \delta_j^0 f(i) \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i+j=n \\ j=0}} f(i) + \sum_{\substack{i+j=n \\ j\neq 0}} 0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{i=n \\ j=0}} f(i) + 0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{i=n} f(i) \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= (f(n))_{n\in\mathbb{N}\cup\{0\}} = f \\
(f+g)h &= \left((f(n))_{n\in\mathbb{N}\cup\{0\}} + (g(n))_{n\in\mathbb{N}\cup\{0\}} \right) (h(n))_{n\in\mathbb{N}\cup\{0\}}
\end{aligned}
$$

$$
\begin{aligned}
&= (f(n)+g(n))_{n\in\mathbb{N}\cup\{0\}}\,(h(n))_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}(f(i)+g(i))\,h(j)\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}f(i)h(j)+\sum_{i+j=n}g(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}f(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}}+\left(\sum_{i+j=n}g(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= (f(n))_{n\in\mathbb{N}\cup\{0\}}\,(h(n))_{n\in\mathbb{N}\cup\{0\}}+(g(n))_{n\in\mathbb{N}\cup\{0\}}\,(h(n))_{n\in\mathbb{N}\cup\{0\}}\\
&= fh+gh\\
f(g+h) &= (f(n))_{n\in\mathbb{N}\cup\{0\}}\left((g(n))_{n\in\mathbb{N}\cup\{0\}}+(h(n))_{n\in\mathbb{N}\cup\{0\}}\right)\\
&= (f(n))_{n\in\mathbb{N}\cup\{0\}}\,(g(n)+h(n))_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}f(i)\,(g(j)+h(j))\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}f(i)g(j)+\sum_{i+j=n}f(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}f(i)g(j)\right)_{n\in\mathbb{N}\cup\{0\}}+\left(\sum_{i+j=n}f(i)h(j)\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= (f(n))_{n\in\mathbb{N}\cup\{0\}}\,(g(n))_{n\in\mathbb{N}\cup\{0\}}+(f(n))_{n\in\mathbb{N}\cup\{0\}}\,(h(n))_{n\in\mathbb{N}\cup\{0\}}\\
&= fg+fh\\
fg &= (f(n))_{n\in\mathbb{N}\cup\{0\}}\,(g(n))_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}f(i)g(j)\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= \left(\sum_{i+j=n}g(i)f(j)\right)_{n\in\mathbb{N}\cup\{0\}}\\
&= (g(n))_{n\in\mathbb{N}\cup\{0\}}\,(f(n))_{n\in\mathbb{N}\cup\{0\}}=gf
\end{aligned}
$$

よって、集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ は可換環をなす。このとき、零元、単位元はそれぞれ $\overline{0}$、$\overline{1}$ と、その元 f に対する元 $-f$ は次式のように与えられる。

$$-f=(-f(n))_{n\in\mathbb{N}\cup\{0\}}$$

□

定義 3.3.5. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、次式のようにその集合 $\widetilde{P}$ の元 X が定義される。

$$X=\left(\delta_n^1\right)_{n\in\mathbb{N}\cup\{0\}}$$

定理 3.3.2. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、$X^0=\overline{1}$ とおかれれば、$\forall i\in\mathbb{N}\cup\{0\}$ に対し、次式が成り立つ。

$$X^i=\left(\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}$$

証明. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、$X^0=\overline{1}$ とおかれれば、次式が成り立つ。

$$X^0=\left(\delta_n^0\right)_{n\in\mathbb{N}\cup\{0\}},\quad X^1=\left(\delta_n^1\right)_{n\in\mathbb{N}\cup\{0\}}$$

ここで、$i=k$ のとき、次式が成り立つと仮定しよう。

$$X^k=\left(\delta_n^k\right)_{n\in\mathbb{N}\cup\{0\}}$$

$i=k+1$ のとき、次のようになる。

$$\begin{aligned}
X^{k+1}&=X^kX\\
&=\left(\delta_n^k\right)_{n\in\mathbb{N}\cup\{0\}}\left(\delta_n^1\right)_{n\in\mathbb{N}\cup\{0\}}\\
&=\left(\sum_{i+j=n}\delta_i^k\delta_j^1\right)_{n\in\mathbb{N}\cup\{0\}}\\
&=\left(\sum_{\substack{i+j=n\\ i=k\wedge j=1}}\delta_i^k\delta_j^1+\sum_{\substack{i+j=n\\ \neg(i=k\wedge j=1)}}\delta_i^k\delta_j^1\right)_{n\in\mathbb{N}\cup\{0\}}\\
&=\left(\sum_{\substack{i+j=n\\ i=k\wedge j=1}}1+\sum_{\substack{i+j=n\\ \neg(i=k\wedge j=1)}}0\right)_{n\in\mathbb{N}\cup\{0\}}\\
&=\left(\delta_n^{k+1}+0\right)_{n\in\mathbb{N}\cup\{0\}}\\
&=\left(\delta_n^{k+1}\right)_{n\in\mathbb{N}\cup\{0\}}
\end{aligned}$$

以上、数学的帰納法により $\forall i\in\mathbb{N}\cup\{0\}$ に対し、次式が成り立つ。

$$X^i=\left(\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}$$

□

定理 3.3.3. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、$\forall a\in R\forall i\in\mathbb{N}\cup\{0\}$ に対し、次式が成り立つ。

$$\overline{a}X^i=\left(a\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}$$

証明. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、$\forall a\in R\forall i\in\mathbb{N}\cup\{0\}$ に対し、定理 3.3.2 より次のようになる。

$$\overline{a}X^i=\left(a\delta_n^0\right)_{n\in\mathbb{N}\cup\{0\}}\left(\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}$$

$$
\begin{aligned}
&= \left(\sum_{k+j=n} a\delta_k^0 \delta_j^i \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{k+j=n \\ k=0\wedge j=i}} a\delta_k^0\delta_j^i + \sum_{\substack{k+j=n \\ \neg(k=0\wedge j=i)}} a\delta_k^0\delta_j^i \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(\sum_{\substack{k+j=n \\ k=0\wedge j=i}} a + \sum_{\substack{k+j=n \\ \neg(k=0\wedge j=i)}} 0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(a \sum_{\substack{k+j=n \\ k=0\wedge j=i}} 1 + \sum_{\substack{k+j=n \\ \neg(k=0\wedge j=i)}} 0 \right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(a\delta_n^i + 0\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \left(a\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}
\end{aligned}
$$

□

3.3.2 多項式環

定義 3.3.6. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、ある非負整数 N が存在して、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$N<n$ が成り立つなら、$f(n)=0$ が成り立つようなその集合 $\widetilde{P}$ の元 f 全体の集合は $R[X]$ と書かれるとする。

定理 3.3.4. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、ある非負整数 N が存在して、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$N<n$ が成り立つなら、$f(n)=0$ が成り立つようなその集合 $\widetilde{P}$ の元 f 全体の集合 $R[X]$ はその集合 $\widetilde{P}$ の部分環で乗法について可換的である。

証明. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、ある非負整数 N が存在して、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$N<n$ が成り立つなら、$f(n)=0$ が成り立つようなその集合 $\widetilde{P}$ の元 f 全体の集合 $R[X]$ について、$\forall f,g\in R[X]$ に対し、ある非負整数 M が存在して、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$M<n$ が成り立つなら、$f(n)=0$ が成り立つかつ、ある非負整数 N が存在して、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$N<n$ が成り立つなら、$g(n)=0$ が成り立つとする。このとき、$M\leq N$ が成り立つと仮定しても一般性は失われない。

もちろん、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$M<n$ が成り立つなら、$-f(n)=0$ が成り立つので、$-f\in R[X]$ が成り立つ。さらに、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$M\leq N<n$ が成り立つなら、$f(n)=0$ かつ $g(n)=0$ が成り立つので、$f(n)+g(n)=0$ が成り立ち、したがって、$f+g\in R[X]$ が成り立つ。最後に、$\forall n\in\mathbb{N}\cup\{0\}$ に対し、$M+N+1<n$ が成り立つなら、$i+j=n$ が成り立つとき、$i,j\in\mathbb{N}\cup\{0\}$ が成り立つことから、$0\leq i$ かつ $0\leq j$ が成り立ち、したがって、$0\leq i\leq n-j\leq n$ かつ $0\leq j\leq n-i\leq n$ が成り立つ。ここで、$i\leq M$ かつ $j\leq N$ が成り立つと仮定すると、$i+j\leq M+N$ が成り立ち、したがって、$M+N+1<n=i+j\leq M+N$ が成り立つことになり、$1<0$ が得られるが、これは矛盾している。したがって、$M<i$ または $N<j$ が成

り立つことになる。このとき、次のようになる。

$$\begin{aligned}\sum_{i+j=n} f(i)g(j) &= \sum_{\substack{i+j=n\\ M<i\wedge j\leq N}} f(i)g(j) + \sum_{\substack{i+j=n\\ M<i\wedge N<j}} f(i)g(j) + \sum_{\substack{i+j=n\\ i\leq M\wedge N<j}} f(i)g(j)\\ &= \sum_{\substack{i+j=n\\ M<i\wedge j\leq N}} 0g(j) + \sum_{\substack{i+j=n\\ M<i\wedge N<j}} 0 + \sum_{\substack{i+j=n\\ i\leq M\wedge N<j}} f(i)0 = 0\end{aligned}$$

したがって、$fg \in R[X]$ が成り立つ。さらに、もちろん、$\overline{1} \in R[X]$ が成り立つので、定理 3.1.14 よりその集合 $R[X]$ はその集合 $\widetilde{P}$ の部分環である。

ここで、その集合 $\widetilde{P}$ は可換環であるかつ、その集合 $R[X]$ はその集合 $\widetilde{P}$ の部分集合であるから、その集合 $R[X]$ は乗法について可換的である。 □

定理 3.3.5. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、ある非負整数 N が存在して、$\forall n \in \mathbb{N}\cup\{0\}$ に対し、$N < n$ が成り立つなら、$f(n) = 0$ が成り立つようなその集合 $\widetilde{P}$ の元 f 全体の集合 $R[X]$ の元 f が与えられたとき、次式が成り立つ。

$$f = \sum_{n\in\Lambda_N\cup\{0\}} \overline{f(n)}X^n$$

定義 3.3.7. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、ある非負整数 N が存在して、$\forall n \in \mathbb{N}\cup\{0\}$ に対し、$N < n$ が成り立つなら、$f(n) = 0$ が成り立つようなその集合 $\widetilde{P}$ の元 f 全体の集合 $R[X]$ をその可換環 R 上の多項式環といい、このとき、その可換環 R をその多項式環 $R[X]$ の係数環、写像 X を変数、不定元、その多項式環 $R[X]$ の元をその可換環 R 上の変数 X の多項式という。

定義 3.3.8. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、上記の議論に倣って、$\forall f \in \widetilde{P}$ に対し、その写像 f は次式のように書かれる。

$$f = \sum_{n\in\mathbb{N}\cup\{0\}} \overline{f(n)}X^n$$

このとき、冪級数のようにみえることから、この集合 $\widetilde{P}$ の元を形式的冪級数という。

証明. 集合 $\mathbb{N}\cup\{0\}$ から零環でない可換環 R への写像全体の集合 $\widetilde{P}$ が与えられたとき、ある非負整数 N が存在して、$\forall n \in \mathbb{N}\cup\{0\}$ に対し、$N < n$ が成り立つなら、$f(n) = 0$ が成り立つようなその集合 $\widetilde{P}$ の元 f 全体の集合 $R[X]$ の元 f が与えられたとき、定理 3.3.3 より次のようになる。

$$\begin{aligned}f &= (f(n))_{n\in\mathbb{N}\cup\{0\}}\\ &= \left(f(n) + \sum_{i\in\Lambda_N\cup\{0\}\setminus\{n\}} 0\right)_{n\in\mathbb{N}\cup\{0\}}\\ &= \left(\sum_{i\in\Lambda_N\cup\{0\}} f(n)\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}\\ &= \sum_{i\in\Lambda_N\cup\{0\}} \left(f(n)\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}\\ &= \sum_{i\in\Lambda_N\cup\{0\}} \left(f(i)\delta_n^i\right)_{n\in\mathbb{N}\cup\{0\}}\end{aligned}$$

$$= \sum_{i \in \Lambda_N \cup \{0\}} \overline{f(i)} X^i$$
$$= \sum_{n \in \Lambda_N \cup \{0\}} \overline{f(n)} X^n$$

□

定理 3.3.6. 零環でない可換環 R 上の多項式環 $R[X]$ が与えられたとき、次式のような写像 φ はその可換環 R からその多項式環 $R[X]$ への埋め込みである。

$$\varphi : R \to R[X]; a \mapsto \overline{a}$$

証明. 零環でない可換環 R 上の多項式環 $R[X]$ が与えられたとき、次式のような写像 φ が定義されるとする。

$$\varphi : R \to R[X]; a \mapsto \overline{a}$$

このとき、$\overline{a} = \overline{b}$ が成り立つなら、$\forall n \in \mathbb{N} \cup \{0\}$ に対し、$n = 1$ のとき、$a = b$、それ以外のとき、$0 = 0$ が成り立つことになる。したがって、$a = b$ が得られるので、その写像 φ は単射である。

さらに、$\forall a, b \in R$ に対し、次のようになる。

$$\begin{aligned}
\varphi(a+b) &= \overline{a+b} \\
&= \left((a+b)\delta_n^0\right)_{n \in \mathbb{N} \cup \{0\}} \\
&= \left(a\delta_n^0\right)_{n \in \mathbb{N} \cup \{0\}} + \left(b\delta_n^0\right)_{n \in \mathbb{N} \cup \{0\}} \\
&= \overline{a} + \overline{b} \\
&= \varphi(a) + \varphi(b) \\
\varphi(ab) &= \overline{ab} \\
&= \left(ab\delta_n^0\right)_{n \in \mathbb{N} \cup \{0\}} \\
&= \left(ab \sum_{\substack{i+j=n \\ i=j=0}} 1 + 0 \right)_{n \in \mathbb{N} \cup \{0\}} \\
&= \left(\sum_{\substack{i+j=n \\ i=j=0}} ab\delta_i^0\delta_j^0 + \sum_{\substack{i+j=n \\ \neg(i=j=0)}} ab\delta_i^0\delta_j^0 \right)_{n \in \mathbb{N} \cup \{0\}} \\
&= \left(\sum_{i+j=n} a\delta_i^0 b\delta_j^0 \right)_{n \in \mathbb{N} \cup \{0\}} \\
&= \left(a\delta_n^0\right)_{n \in \mathbb{N} \cup \{0\}} \left(b\delta_n^0\right)_{n \in \mathbb{N} \cup \{0\}} \\
&= \overline{a}\overline{b} \\
&= \varphi(a)\varphi(b)
\end{aligned}$$

もちろん、$\varphi(1) = \overline{1}$ が成り立つので、その写像 φ は環準同型写像である。

よって、その写像 φ はその可換環 R からその多項式環 $R[X]$ への埋め込みである。 □

3.3.3 次数

定義 3.3.9. 可換環 R 上の多項式環 $R[X]$ の元 f が次式のように与えられたとき、

$$f = \sum_{n \in \Lambda_N \cup \{0\}} \overline{f(n)} X^n$$

$\overline{f(N)} \neq \overline{0}$ かつ $N \neq 0$ が成り立つなら、その非負整数 N をその多項式 f の次数といい $\deg f$ と書く。このときの多項式 f を N 次多項式という。さらに、多項式 $\overline{0}$ の次数 $\deg \overline{0}$ は $-\infty$ と定義される。その次数 $\deg f$ が 0 または $-\infty$ に等しいとき、その多項式 f を定数という。その N 次多項式 f において、その多項式環 $R[X]$ の各元 $\overline{f(n)}X^n$、$\overline{f(n)}$ をそれぞれその多項式 f の項、係数といい、特に、項 $\overline{f(N)}X^N$、係数 $\overline{f(N)}$ をそれぞれその多項式 f の主項、主係数といい、ここでは、$f_{\mathrm{l.c.}}$ と書くことにする。特に、主係数が $\overline{1}$ であるような多項式を monic という。

定理 3.3.7. 可換環 R 上の多項式環 $R[X]$ が与えられたとき、$\forall f, g \in R[X]$ に対し、次のことが成り立つ。

- $\deg(f+g) \leq \deg f + \deg g$ が成り立つ。特に、$\deg f < \deg g$ が成り立つなら、$\deg(f+g) = \deg g$ が成り立つ。
- $0 \leq \deg f$ かつ $0 \leq \deg g$ が成り立つなら、$\deg fg \leq \deg f + \deg g$ が成り立つ。
- 特に、その可換環 R が整域であるとき、$0 \leq \deg f$ かつ $0 \leq \deg g$ が成り立つなら、$\deg fg = \deg f + \deg g$ が成り立つ。

証明. 可換環 R 上の多項式環 $R[X]$ が与えられたとき、$\forall f, g \in R[X]$ に対し $\deg f < \deg g$ が成り立つなら、次のようになるので、

$$\begin{aligned} f+g &= \sum_{n \in \Lambda_{\deg f} \cup \{0\}} \overline{f(n)} X^n + \sum_{n \in \Lambda_{\deg g} \cup \{0\}} \overline{g(n)} X^n \\ &= \sum_{n \in \Lambda_{\deg f} \cup \{0\}} \overline{f(n)} X^n + \sum_{n \in \Lambda_{\deg f} \cup \{0\}} \overline{g(n)} X^n + \sum_{n \in \Lambda_{\deg g} \setminus \Lambda_{\deg f}} \overline{g(n)} X^n \\ &= \sum_{n \in \Lambda_{\deg f} \cup \{0\}} \left(\overline{f(n)} + \overline{g(n)} \right) X^n + \sum_{n \in \Lambda_{\deg g} \setminus \Lambda_{\deg f}} \overline{g(n)} X^n \end{aligned}$$

$g_{\mathrm{l.c.}} \neq \overline{0}$ より $\deg(f+g) = \deg g$ が成り立つ。

$\deg f = \deg g$ が成り立つなら、これが k とおかれると、次のようになるので、

$$\begin{aligned} f+g &= \sum_{n \in \Lambda_{\deg f} \cup \{0\}} \overline{f(n)} X^n + \sum_{n \in \Lambda_{\deg g} \cup \{0\}} \overline{g(n)} X^n \\ &= \sum_{n \in \Lambda_k \cup \{0\}} \overline{f(n)} X^n + \sum_{n \in \Lambda_k \cup \{0\}} \overline{g(n)} X^n \\ &= \sum_{n \in \Lambda_k \cup \{0\}} \left(\overline{f(n)} + \overline{g(n)} \right) X^n \end{aligned}$$

$\deg(f+g) \leq \deg f + \deg g$ が成り立つ。

$0 \leq \deg f$ かつ $0 \leq \deg g$ が成り立つなら、定理 3.1.8、定理 3.3.5 より次のようになる。

$$fg = \left(\sum_{n \in \Lambda_{\deg f} \cup \{0\}} \overline{f(n)} X^n \right) \left(\sum_{n \in \Lambda_{\deg g} \cup \{0\}} \overline{g(n)} X^n \right)$$

$$= \sum_{(m,n)\in \Lambda_{\deg f}\cup\{0\}\times\Lambda_{\deg g}\cup\{0\}} \overline{f(m)}X^m\overline{g(n)}X^n$$
$$= \sum_{(m,n)\in \Lambda_{\deg f}\cup\{0\}\times\Lambda_{\deg g}\cup\{0\}} \overline{f(m)}\ \overline{g(n)}X^{m+n}$$

よって、$\deg fg \leq \deg f + \deg g$ が成り立つ。

特に、その可換環 R が整域であるとき、$f_{\text{l.c.}} \neq 0$ かつ $g_{\text{l.c.}} \neq 0$ が成り立つので、$f_{\text{l.c.}}\ g_{\text{l.c.}} \neq 0$ が成り立つ。したがって、$\deg fg = \deg f + \deg g$ が成り立つ。 □

定理 3.3.8. 整域 R 上の多項式環 $R[X]$ は整域である。

証明. 定理 3.3.7 より整域 R 上の多項式環 $R[X]$ が与えられたとき、$\forall f, g \in R[X]$ に対し、$f \neq \overline{0}$ かつ $g \neq \overline{0}$ が成り立つなら、$0 \leq \deg f$ かつ $0 \leq \deg g$ が成り立つことになり、$0 \leq \deg fg = \deg f + \deg g$ が成り立つ。ゆえに、$fg \neq \overline{0}$ が成り立つので、その多項式環 $R[X]$ は整域である。 □

3.3.4 多項式写像

定義 3.3.10. 可換環 R の部分環 R' 上の多項式環 $R'[X]$ の元 f が与えられたとき、その可換環 R の元 c を用いた次式のようなその可換環 R の元 $s_c(f)$ をその多項式 f の変数 X にその元 c を代入した元という。

$$s_c(f) = \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n$$

定義 3.3.11. 可換環 R の部分環 R' 上の多項式環 $R'[X]$ の元 f が与えられたとき、次式のように定義される写像 P_f をその多項式 f から定まるその可換環 R からその可換環 R への多項式写像という。

$$P_f : R \to R; c \mapsto \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n$$

定理 3.3.9. 可換環 R の部分環 R' 上の多項式環 $R'[X]$ の元 f が与えられたとき、$\forall c \in R$ に対し、次式のように定義される写像 s_c は環準同型写像である[*11]。

$$s_c : R'[X] \to R; f \mapsto \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n$$

これにより、可換環 R の部分環 R' 上の多項式環 $R'[X]$ の元 f が与えられたとき、これから明らかにその多項式 f から定まるその可換環 R からその可換環 R への多項式写像へ移す写像も環準同型写像である。

証明. 可換環 R の部分環 R' 上の多項式環 $R'[X]$ の元 f が与えられたとき、$\forall c \in R$ に対し、次式のように定義される写像 s_c について、

$$s_c : R'[X] \to R; f \mapsto \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n$$

$\forall f, g \in R'[X]$ に対し、$\deg f \leq \deg g$ が成り立つとしても一般性は失われなく次のようになる。

$$s_c(f+g) = s_c\left((f(n))_{n\in\mathbb{N}\cup\{0\}} + (g(n))_{n\in\mathbb{N}\cup\{0\}}\right)$$

[*11] なお、その写像 s_c は単射であるとは限りません。

$$
\begin{aligned}
&= s_c\left(f(n)+g(n)\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \sum_{n\in\Lambda_{\deg g}\cup\{0\}} \left(f(n)+g(n)\right)c^n \\
&= \sum_{n\in\Lambda_{\deg g}\cup\{0\}} f(n)c^n + \sum_{n\in\Lambda_{\deg g}\cup\{0\}} g(n)c^n \\
&= \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n + \sum_{n\in\Lambda_{\deg g}\setminus\Lambda_{\deg f}} f(n)c^n + \sum_{n\in\Lambda_{\deg g}\cup\{0\}} g(n)c^n \\
&= \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n + \sum_{n\in\Lambda_{\deg g}\setminus\Lambda_{\deg f}} 0 + \sum_{n\in\Lambda_{\deg g}\cup\{0\}} g(n)c^n \\
&= \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n + \sum_{n\in\Lambda_{\deg g}\cup\{0\}} g(n)c^n = s_c(f)+s_c(g) \\
s_c(fg) &= s_c\left(\left(f(n)\right)_{n\in\mathbb{N}\cup\{0\}}\left(g(n)\right)_{n\in\mathbb{N}\cup\{0\}}\right) \\
&= s_c\left(\sum_{i+j=n} f(i)g(j)\right)_{n\in\mathbb{N}\cup\{0\}} \\
&= \sum_{n\in\Lambda_{\deg g}\cup\{0\}} \sum_{i+j=n} f(i)g(j)c^n \\
&= \sum_{m+n\in\Lambda_{\deg g}\cup\{0\}} f(m)g(n)c^{m+n} \\
&= \sum_{m+n\in\Lambda_{\deg g}\cup\{0\}} f(m)g(n)c^{m+n} + \sum_{m+n\in\Lambda_{\deg f+\deg g}\setminus\Lambda_{\deg g}} 0 \\
&= \sum_{m+n\in\Lambda_{\deg g}\cup\{0\}} f(m)g(n)c^{m+n} + \sum_{m+n\in\Lambda_{\deg f+\deg g}\setminus\Lambda_{\deg g}} f(m)g(n)c^{m+n} \\
&= \sum_{m+n\in\Lambda_{\deg f+\deg g}\cup\{0\}} f(m)g(n)c^{m+n} \\
&= \sum_{(m,n)\in\Lambda_{\deg f}\cup\{0\}\times\Lambda_{\deg g}\cup\{0\}} f(m)c^m g(n)c^n \\
&= \left(\sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n\right)\left(\sum_{n\in\Lambda_{\deg g}\cup\{0\}} g(n)c^n\right) = s_c(f)s_c(g)
\end{aligned}
$$

さらに、もちろん、$s_c\left(\overline{1}\right)=1$ が成り立つので、よって、その写像 s_c は環準同型写像である。 □

定理 3.3.10. 定理 3.3.9、定理 3.2.18 より可換環 R の部分環 R' 上の多項式環 $R'[X]$ の元 f が与えられたとき、$\forall c\in R$ に対し、次式のように定義される環準同型写像 s_c の値域 $V\left(s_c\right)$ はその環 R の部分環であるのであった。

$$
s_c : R'[X]\to R; f\mapsto \sum_{n\in\Lambda_{\deg f}\cup\{0\}} f(n)c^n
$$

このとき、その値域 $V\left(s_c\right)$ はその環 R' の全ての元とその元 c に属されるその環 R の部分環のうち、順序関係 $\subseteq$ の意味で最小なものである。

証明. 定理 3.3.9、定理 3.2.18 より可換環 R の部分環 R' 上の多項式環 $R'[X]$ の元 f が与えられたとき、$\forall c\in R$ に対し、次式のように定義される環準同型写像 s_c の値域 $V\left(s_c\right)$ はその環 R の部分環であるので

あった。

$$s_c : R'[X] \to R; f \mapsto \sum_{n \in \Lambda_{\deg f} \cup \{0\}} f(n)c^n$$

もちろん、$\forall a \in R'$ に対し、次のようになるので、

$$s_c\left(\overline{a}\right) = a, \quad s_c(X) = c$$

その値域 $V\left(s_c\right)$ はその環 R' の全ての元とその元 c に属されるその環 R の部分環である。このとき、その環 R' の全ての元とその元 c に属されるその環 R の部分環 R'' が与えられたとき、$\forall f \in R'[X]$ に対し、$f(n) \in R'$ が成り立つので、$f(n), c \in R''$ が成り立つかつ、定理 3.1.14 より $f(n)c^n$ が成り立ち、したがって、$\sum_{n \in \Lambda_{\deg f} \cup \{0\}} f(n)c^n \in R''$ が成り立つ。ゆえに、$V\left(s_c\right) \subseteq R''$ が成り立つことになり、したがって、その値域 $V\left(s_c\right)$ はその環 R' の全ての元とその元 c に属されるその環 R の部分環のうち、順序関係 $\subseteq$ の意味で最小なものである。 □

3.3.5 除法の定理

定理 3.3.11. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、元 f がその多項式環 $K[X]$ の可逆元であるならそのときに限り、$\deg f = 0$ が成り立つ。

証明. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、元 f がその多項式環 $K[X]$ の可逆元であるなら、定理 3.3.8 より $fg = \overline{1}$ なる多項式 g がその多項式環 $K[X]$ に存在するが、定理 3.3.7 より $\deg f = \deg g = 0$ が成り立つことになる。

逆に、$\deg f = 0$ が成り立つなら、$f = \overline{f(0)} \neq \overline{0}$ が成り立つことになる。ここで、定理 3.3.6 より $\overline{f(0)f(0)}^{-1} = \overline{f(0)\frac{1}{f(0)}} = \overline{1}$ が成り立つので、その元 f がその多項式環 $K[X]$ の可逆元である。 □

定理 3.3.12 (除法の定理)**.** 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f, g \in K[X]$ に対し、$1 \leq \deg g$ が成り立つなら、次式が成り立つような $\deg r < \deg g$ なる多項式たち q、r がその多項式環 $K[X]$ に一意的に存在する。

$$f = gq + r$$

この定理を除法の定理という。

証明. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f, g \in K[X]$ に対し、$1 \leq \deg g$ が成り立つとする。$\deg f < \deg g$ のとき、$q = \overline{0}$、$r = f$ とおかれればよくて、$\deg g \leq \deg f$ が成り立つなら、$g_{\text{l.c.}} \neq \overline{0}$ で $0 \leq \deg f - \deg g$ が成り立ち、$h = \frac{f_{\text{l.c.}}}{g_{\text{l.c.}}} X^{\deg f - \deg g}$ とおかれると、次のようになるので、

$$\begin{aligned} gh &= \sum_{i \in \Lambda_{\deg g} \cup \{0\}} \overline{g(i)} X^i \frac{f_{\text{l.c.}}}{g_{\text{l.c.}}} X^{\deg f - \deg g} \\ &= \sum_{i \in \Lambda_{\deg g} \cup \{0\}} \frac{\overline{g(i)}\ f_{\text{l.c.}}}{g_{\text{l.c.}}} X^{\deg f - \deg g + i} \\ &= \sum_{i \in (\Lambda_{\deg f} \cup \{0\}) \setminus \Lambda_{\deg f - \deg g - 1}} \frac{\overline{g(i)}\ f_{\text{l.c.}}}{g_{\text{l.c.}}} X^i \end{aligned}$$

多項式 gh の主項は $f_{\mathrm{l.c.}}X^{\deg f}$ である。

ここで、$\deg f = 1$ のとき、次のようになるので、明らかである。

$$\begin{aligned} f &= \overline{f(0)} + \overline{f(1)}X \\ &= \overline{f(0)} + \frac{\overline{f(1)}}{\overline{g(1)}}\left(\overline{g(0)} + \overline{g(1)}X - \overline{g(0)}\right) \\ &= \overline{f(0)} - \frac{\overline{f(1)}\ \overline{g(0)}}{\overline{g(1)}} + \frac{\overline{f(1)}}{\overline{g(1)}}\left(\overline{g(0)} + \overline{g(1)}X\right) \end{aligned}$$

$\deg f = k$ のとき、$f = gq + r$ が成り立つような $\deg r < \deg g$ なる多項式たち q、r がその多項式環 $K[X]$ に存在すると仮定しよう。$\deg f = k+1$ のとき、次のようになる。

$$\begin{aligned} f - gh &= \sum_{i\in\Lambda_{k+1}\cup\{0\}} \overline{f(i)}X^i - \sum_{i\in(\Lambda_{k+1}\cup\{0\})\setminus\Lambda_{k+1-\deg g-1}} \frac{\overline{g(i)}\ \overline{f(k+1)}}{g_{\mathrm{l.c.}}}X^i \\ &= \sum_{i\in(\Lambda_{k+1}\cup\{0\})\setminus\{k+1\}} \overline{f(i)}X^i + \overline{f(k+1)}X^{k+1} \\ &\quad - \sum_{i\in(\Lambda_{k+1}\cup\{0\})\setminus(\Lambda_{k-\deg g}\cup\{k+1\})} \frac{\overline{g(i)}\ \overline{f(k+1)}}{g_{\mathrm{l.c.}}}X^i - \overline{f(k+1)}X^{k+1} \\ &= \sum_{i\in(\Lambda_{k+1}\cup\{0\})\setminus\{k+1\}} \overline{f(i)}X^i - \sum_{i\in(\Lambda_{k+1}\cup\{0\})\setminus(\Lambda_{k-\deg g}\cup\{k+1\})} \frac{\overline{g(i)}\ \overline{f(k+1)}}{g_{\mathrm{l.c.}}}X^i \\ &= \sum_{i\in\Lambda_k\cup\{0\}} \overline{f(i)}X^i - \sum_{i\in(\Lambda_k\cup\{0\})\setminus\Lambda_{k-\deg g}} \frac{\overline{g(i)}\ \overline{f(k+1)}}{g_{\mathrm{l.c.}}}X^i \end{aligned}$$

これにより、$\deg(f - gh) < k$ が成り立つので、$f - gh = gq' + r'$ が成り立つような $\deg r' < \deg g$ なる多項式たち q'、r' がその多項式環 $K[X]$ に存在することになる。したがって、次のようになる。

$$\begin{aligned} f &= f - gh + gh \\ &= gq' + r' + gh \\ &= g\left(q' + h\right) + r' \end{aligned}$$

よって、$f = gq + r$ が成り立つような $\deg r < \deg g$ なる多項式たち q、r がその多項式環 $K[X]$ に存在する。

次にそのような多項式たち q、r の一意性について、議論しよう。$f = gq + r = gq' + r'$ かつ $\deg r < \deg g$ かつ $\deg r < \deg g$ なる多項式たち q、q'、r、r' がその多項式環 $K[X]$ に存在するとする。このとき、次のようになる。

$$\begin{aligned} \deg\left(r - r'\right) &= \deg\left(f - gq - f + gq'\right) \\ &= \deg\left(gq' - gq\right) \\ &= \deg g\left(q' - q\right) \\ &= \deg g + \deg\left(q' - q\right) \end{aligned}$$

ここで、$\deg r < \deg g$ かつ $\deg r' < \deg g$ が成り立つので、$\deg\left(r - r'\right) = \deg g + \deg\left(q' - q\right) < \deg g$ が成り立つことになる。したがって、$\deg\left(q' - q\right) < 0$、即ち、$q' - q = \overline{0}$ が成り立つので、$q' = q$ が得られる。このとき、次のようになるので、

$$r = f - gq$$

$$= f - gq' = r'$$

$q = q'$ かつ $r = r'$ が得られる。よって、$f = gq + r$ が成り立つような $\deg r < \deg g$ なる多項式たち q、r がその多項式環 $K[X]$ に一意的に存在する。 □

定理 3.3.13. 体 K 上の多項式環 $K[X]$ は単項 ideal 整域である。

証明. 体 K 上の多項式環 $K[X]$ の ideal$J$ が与えられたとき、これが零 ideal なら単項 ideal である。ここで、その ideal$J$ が $\overline{0}$ 以外の体 K の元 a に属されるなら、その環 K は体なので、$\frac{1}{a} \in K$ なる元 $\frac{1}{a}$ が存在して $\overline{\frac{1}{a}}a = \overline{1} \in J$ が成り立つことになり、したがって、定数全てがその ideal$J$ に属する。ゆえに、$J = K\overline{1}$ が成り立ちその ideal$J$ は単項 ideal である。ここで、その ideal$J$ は零 ideal ではなく $\overline{0}$ 以外の定数に属されないものとする。その ideal$J$ のうち $\overline{0}$ でない多項式たちのうち最も次数が低いものを g とすると $1 \leq \deg g$ が成り立ち、したがって、$\forall f \in J$ に対し、除法の定理より $f = gq + r$ かつ $\deg r < \deg g$ なる多項式たち q、r がその多項式環 $K[X]$ に存在する。ここで、$-q \in K[X]$ より $f - gq \in J$ が成り立つので、$r \in J$ が成り立つ。ここで、$r \neq \overline{0}$ が成り立つと仮定すると、その多項式 r は定数でなく $\deg r < \deg g$ が成り立つことになるが、その多項式 g のおき方に矛盾する。したがって、$r = \overline{0}$ が成り立つ。これにより、$\forall f \in J \exists q \in K[X]$ に対し、$f = gq$ が成り立つので、その ideal$J$ は単項 ideal である。 □

定義 3.3.12. 体 K 上の多項式環 $K[X]$ の商の体をその体 K 上の有理式体といい、これの元をその体 K 上の変数 X の有理式、分数式という。

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976. 新装版第 2 刷 p135-142,150 ISBN978-4-00-029873-5

3.4　素元

3.4.1　割り切れる

定義 3.4.1. 整域 R の元々 a、b が与えられ $a = bq$ なるその整域 R の元 q が存在するとき、その元 a はその元 b で割り切られる、整除されるなどといい、$b|a$ と書く。さらに、その元 a をその元 b の倍元、その元 b をその元 a の約元という。

定理 3.4.1. 整域 R が与えられたとき、$\forall a, b, c$ に対し、次のことが成り立つ。

- $a|a$ が成り立つ。
- $a|0$ が成り立つ。
- $1|a$ が成り立つ。
- $a \neq 0$ が成り立つなら、$0|a$ が成り立たない。
- その元 b が可逆元であるなら、$b|a$ が成り立つ。
- $b|a$ かつ $c|b$ が成り立つなら、$c|a$ が成り立つ。
- $c|a$ かつ $c|b$ が成り立つなら、$c|a + b$ が成り立つ。
- $b|a$ が成り立つなら、$b|ac$ が成り立つ。

証明. 整域 R が与えられたとき、$\forall a, b, c$ に対し、$a = a1$、$0 = a0$、$a = 1a$ が成り立つことから、$a|a$、$a|0$、$1|a$ が成り立つ。

$a \neq 0$ が成り立つかつ、$0|a$ が成り立つと仮定すると、$a = 0q$ となる元 q がその整域 R に存在することになるが、$0q = 0$ より $a \neq 0$ が成り立つことに矛盾している。よって、$a \neq 0$ が成り立つなら、$0|a$ が成り立たない。

その元 b が可逆元であるなら、$bb^{-1} = 1$ なる元 b^{-1} がその整域 R に存在するので、$a = 1a = bb^{-1}a$ より $b|a$ が成り立つ。

$b|a$ かつ $c|b$ が成り立つなら、$a = bq$、$b = cr$ なる元々 q、r がその整域 R に存在することになる。このとき、$a = bq = crq$ より $c|a$ が成り立つ。

$c|a$ かつ $c|b$ が成り立つなら、$a = cq$、$b = cr$ なる元々 q、r がその整域 R に存在することになる。ここで、$a + b = cq + cr = c(q + r)$ より $c|a + b$ が成り立つ。

$b|a$ が成り立つなら、$a = bq$ なる元 q がその整域 R に存在することになる。このとき、$ac = bqc$ より $b|ac$ が成り立つ。 □

定理 3.4.2. 整域 R が与えられたとき、$\forall a \in R$ に対し、$a|1$ が成り立つならそのときに限り、その元 a は可逆元である。

証明. 整域 R が与えられたとき、$\forall a \in R$ に対し、$a|1$ が成り立つなら、$1 = aa'$ なるその整域 R の元 a' が存在する。このとき、その環 R は整域なので、$aa' = a'a = 1$ が成り立つので、その元 a は可逆元である。逆に、その元 a が可逆元であるなら、これの逆元 a^{-1} がその整域 R に存在して $1 = aa^{-1}$ が成り立つので、$a|1$ が成り立つ。 □

定義 3.4.2. 整域 R が与えられたとき、$b|a$ かつ $a|b$ が成り立つことをそれらの元々 a、b は同伴であるとい

い、aAb と書くことにする。

定理 3.4.3. その関係 A は同値関係である。

証明. 整域 R が与えられたとき、$b|a$ かつ $a|b$ が成り立つことを aAb と書くことにする。このとき、もちろん、$\forall a \in R$ に対し、$a|a$ かつ $a|a$ が成り立つので、aAa が成り立つ。$\forall a, b \in R$ に対し、$b|a$ かつ $a|b$ が成り立つなら、もちろん、$a|b$ かつ $b|a$ が成り立つので、aAb が成り立つなら、bAa が成り立つ。$\forall a, b, c$ に対し、$a|b$ かつ $b|c$ が成り立つなら、$a|c$ が成り立つので、aAb かつ bAc が成り立つなら、$a|b$ かつ $b|a$ かつ $b|c$ かつ $c|b$ が成り立つので、$a|c$ かつ $c|a$ が成り立ち、したがって、aAc が成り立つ。

よって、その関係 A は同値関係である。 □

定理 3.4.4. 整域 R が与えられたとき、$\forall a, b \in R$ に対し、aAb が成り立つならそのときに限り、ある可逆元 q がその整域 R に存在して $a = bq$ が成り立つ。

これにより、例えば、$\forall a, b \in \mathbb{Z}$ に対し、aAb が成り立つならそのときに限り、可逆元である整数が ± 1 のみであるから、$a = \pm b$ が成り立つ。$\forall a, b \in \mathbb{Q}$ に対し、aAb が成り立つならそのときに限り、可逆元である有理数が 0 以外の有理数すべてであるから、$\exists q \in \mathbb{Q} \setminus \{0\}$ に対し、$a = bq$ が成り立つ。

証明. 整域 R が与えられたとき、$\forall a, b \in R$ に対し、aAb が成り立つなら、$a = bq$ かつ $b = ar$ なる元々 a、b がその整域 R に存在することになる。このとき、$a = bq = arq$ が成り立つので、定理 3.4.1 より $a \neq 0$ が成り立つことによりこれの逆元 a^{-1} がその整域 R に存在して $1 = a^{-1}a = a^{-1}arq = rq$ が成り立つ。ここで、その整域 R は乗法について可換的であるので、それらの元々 q、r は可逆元である。よって、ある可逆元 q がその整域 R に存在して $a = bq$ が成り立つ。

逆に、ある可逆元 q がその整域 R に存在して $a = bq$ が成り立つなら、ある元 q^{-1} が存在して $b = bqq^{-1} = aq^{-1}$ が成り立つ。以上より、$b|a$ かつ $a|b$ が成り立つので、aAb が成り立つ。 □

3.4.2 素元

定義 3.4.3. 整域 R の元 p が与えられたとき、次のことを満たすとき、その元 p を素元という。

- その元 p は 0 でない。
- その元 p は可逆元でない。
- $q|p$ が成り立つなら、$qA1$ または qAp が成り立つ。

例えば、素元な整数は素数かこれの符号を変えたものである。

定理 3.4.5. 整域 R の素元 p が与えられたとき、これに同伴な元も素元である。

証明. 整域 R の素元 p が与えられたとき、pAq なる元 q について、定理 3.4.1 より $q \neq 0$ が成り立つ。また、その元 q が可逆元であると仮定すると、定理 3.4.4 よりある可逆元 r がその整域 R に存在して $p = qr$ が成り立つ。ここで、次のようになることから、

$$pr^{-1}q^{-1} = qrr^{-1}q^{-1} = q1q^{-1} = qq^{-1} = 1$$

その元 p も可逆元であるが、これは素元の定義に矛盾する。したがって、その元 q は可逆元でない。$r|q$ が成り立つなら、定理 3.4.4 よりある可逆元 a が存在して $q = ar$ が成り立つことになる。ここで、定理 3.4.1 より

$r|p$ が成り立つので、$rA1$ または rAp が成り立つ。ここで、その関係 A は同値関係であるから、$rA1$ または rAq が成り立つ。よって、その元 q も素元である。 □

定義 3.4.4. 添数集合 Λ_n によって添数づけられた整域 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、これの任意の元が割り切られるその整域 R の元をその族 $\{a_i\}_{i\in\Lambda_n}$ の公約元という。さらに、その整域 R の元 d がその族 $\{a_i\}_{i\in\Lambda_n}$ の公約元でその族 $\{a_i\}_{i\in\Lambda_n}$ の任意の公約元 e に対し、$e|d$ が成り立つとき、その公約元 d をその族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元という。

定理 3.4.6. 添数集合 Λ_n によって添数づけられた整域 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、この族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元 d が存在すれば、$\forall e \in R$ に対し、eAd が成り立つならそのときに限り、その元 e もその族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元である。

証明. 添数集合 Λ_n によって添数づけられた整域 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、この族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元 d が存在するとする。$\forall e \in R$ に対し、eAd が成り立つなら、ある可逆元 q が存在して $d = eq$ が成り立つ。このとき、$\forall i \in \Lambda_n$ に対し、$d|a_i$ が成り立ち、$\exists d_i \in R$ に対し、$a_i = dd_i = eqd_i$ が成り立つので、その元 e もその族 $\{a_i\}_{i\in\Lambda_n}$ の公約元である。さらに、その族 $\{a_i\}_{i\in\Lambda_n}$ の任意の公約元 c に対し、$c|d$ が成り立つので、$\exists d_c \in R$ に対し、$d = cd_c$ が成り立ち、したがって、$e = eqq^{-1} = dq^{-1} = cd_cq^{-1}$ が成り立つ。これにより、その元 e もその族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元でもある。

逆に、その整域 R の元 e もその族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元であるなら、最大公約元の定義より $d|e$ かつ $e|d$ が成り立つので、eAd が成り立つ。 □

定理 3.4.7. 添数集合 Λ_n によって添数づけられた単項 ideal 整域 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、この族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元 d は存在して $Rd = \sum_{i\in\Lambda_n} Ra_i$ が成り立つ。

証明. 添数集合 Λ_n によって添数づけられた単項 ideal 整域 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、定理 3.2.3 より集合 $\sum_{i\in\Lambda_n} Ra_i$ はその整域 R の ideal であるので、その整域 R のある元 d が存在して $Rd = \sum_{i\in\Lambda_n} Ra_i$ が成り立つ。ここで、もちろん、$d \in Rd$ が成り立つので、その整域 R のある元々 r_i を用いて $d = \sum_{i\in\Lambda_n} r_ia_i$ が成り立つ。これにより、$\forall i \in \Lambda_n$ に対し、$a_i \in Rd = \sum_{i\in\Lambda_n} Ra_i$ が成り立つので、その元 a_i はその元 d の倍元となり、したがって、その元 d がその族 $\{a_i\}_{i\in\Lambda_n}$ の公約元でもある。ここで、その族 $\{a_i\}_{i\in\Lambda_n}$ の任意の公約元 e が与えられたとき、$\forall i \in \Lambda_n$ に対し、$a_i = ee_i$ なるその整域 R の元 e_i が存在するので、次のようになる。

$$d = \sum_{i\in\Lambda_n} r_ia_i = \sum_{i\in\Lambda_n} r_iee_i = e\sum_{i\in\Lambda_n} r_ie_i$$

これにより、$e|d$ が成り立つので、その元 d がその族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元となる。よって、この族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元 d は存在して $Rd = \sum_{i\in\Lambda_n} Ra_i$ が成り立つ。 □

定義 3.4.5. 単項 ideal 整域 R の部分集合 $\{a, b\}$ が与えられたとき、1 がこの集合 $\{a, b\}$ の最大公約元であるとき、それらの元々 a、b は互いに素であるという。

定理 3.4.8. 単項 ideal 整域 R の素元 p が与えられたとき、$\forall a \in R$ に対し、$p|a$ が成り立たないなら、それらの元々 p、a は互いに素である。

証明. 単項 ideal 整域 R の素元 p が与えられたとき、$\forall a \in R$ に対し、$p|a$ が成り立たないなら、集合 $\{p, a\}$ の最大公約元 d は $d|p$ を満たすので、素元の定義より $dA1$ または dAp が成り立つ。ここで、dAp が成り立つ

とすれば、$d|a$ が成り立つので、$p|d$ が成り立つことと定理 3.4.1 より $p|a$ が成り立つことになるが、これは仮定に矛盾する。したがって、$dA1$ が成り立つことになる。このとき、定理 3.4.6 より 1 もその集合 $\{p, a\}$ の最大公約元であるから、それらの元々 p、a は互いに素である。 □

定理 3.4.9. 単項 ideal 整域 R の素元 p と添数集合 Λ_n によって添数づけられたその整域 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、$p|\prod_{i\in\Lambda_n} a_i$ が成り立つなら、$\exists i \in \Lambda_n$ に対し、$p|a_i$ が成り立つ。

証明. 単項 ideal 整域 R の素元 p と添数集合 Λ_n によって添数づけられたその整域 R の元の族 $\{a, b\}$ が与えられたとき、$p|ab$ が成り立つかつ、$p|a$ が成り立たないなら、定理 3.4.8 よりそれらの元々 p、a は互いに素であるので、定理 3.4.7 より $R = Rp + Ra$ が成り立ち、したがって、$\exists r, s \in R$ に対し、$1 = rp + sa$ が成り立つ。このとき、$\exists c \in R$ に対し、$ab = pc$ が成り立って次のようになるので、

$$\begin{aligned} b &= (rp + sa)b \\ &= rpb + sab \\ &= rpb + spc \\ &= (rb + sc)p \end{aligned}$$

$p|b$ が成り立つ。以上より、$p|ab$ が成り立つなら、$p|a$ または $p|b$ が成り立つ。これにより、添数集合 Λ_n によって添数づけられたその整域 R の元の族 $\{a_i\}_{i\in\Lambda_n}$ についても同様に成り立つ。 □

定理 3.4.10. 単項 ideal 整域 R の 0 でない元の列 $(a_n)_{n\in\mathbb{N}}$ が与えられたとき、$\forall n \in \mathbb{N}$ に対し、$a_{n+1}|a_n$ が成り立つなら、$\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}$ に対し、$n_0 \leq n$ が成り立つなら、$a_{n_0} A a_n$ が成り立つ。

証明. 単項 ideal 整域 R の 0 でない元の列 $(a_n)_{n\in\mathbb{N}}$ が与えられたとき、$\forall n \in \mathbb{N}$ に対し、$a_{n+1}|a_n$ が成り立つとする。このとき、$\forall a, b \in \bigcup_{n\in\mathbb{N}} Ra_n$ に対し、ある自然数たち i、j が存在して $a \in Ra_i$ かつ $b \in Ra_j$ が成り立つ。ここで、$i \leq j$ が成り立つなら、仮定より $a_j|a_i$ が成り立つので、$a_j|a$ が成り立つ。以上より、$a_j|a$ かつ $a_j|b$ が成り立つので、定理 3.4.1 より $a_j|a + b$ が成り立つことになり、したがって、$a + b \in \bigcup_{n\in\mathbb{N}} Ra_n$ が成り立つ。さらに、$\forall a \in \bigcup_{n\in\mathbb{N}} Ra_n \forall r \in R$ に対し、ある自然数 i が存在して $a \in Ra_i$ が成り立つ。ここで、その集合 Ra_i は ideal であったので、$ra \in Ra_i$ が成り立つ。これにより、$ra \in \bigcup_{n\in\mathbb{N}} Ra_n$ が成り立つ。以上より、その集合 $\bigcup_{n\in\mathbb{N}} Ra_n$ はその整域 R の ideal である。

ここで、その整域 R は単項 ideal 整域であるから、$Rd = \bigcup_{n\in\mathbb{N}} Ra_n$ なる元 d がその集合 R に存在するので、$\forall n \in \mathbb{N}$ に対し、$a_n \in Rd$ が成り立ち、したがって、$d|a_n$ が成り立つ。一方で、$d \in \bigcup_{n\in\mathbb{N}} Ra_n$ が成り立つので、$\exists n_0 \in \mathbb{N}$ に対し、$d \in Ra_{n_0}$、即ち、$a_{n_0}|d$ が成り立つので、$\forall n \in \mathbb{N}$ に対し、$n_0 \leq n$ が成り立つなら、定理 3.4.1 より $a_n|d$ が成り立つ。以上より、$d|a_n$ かつ $a_n|d$ が成り立つので、$a_n Ad$ が成り立つかつ、$a_{n_0} Ad$ が成り立つ。ここで、その関係 A は同値関係であるので、$a_{n_0} A_n$ が成り立つ。

よって、$\forall n \in \mathbb{N}$ に対し、$a_{n+1}|a_n$ が成り立つなら、$\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}$ に対し、$n_0 \leq n$ が成り立つなら、$a_{n_0} A a_n$ が成り立つ。 □

定理 3.4.11 (素元分解の基本定理)**.** 単項 ideal 整域 R が与えられたとき、$\forall a \in R$ に対し、その元 a が可逆元でないかつ、0 でないなら、その整域 R の素元の族 $\{p_i\}_{i\in\Lambda_n}$ が存在して $a = \prod_{i\in\Lambda_n} p_i$ が成り立つ。しかも、そのような族が $\{p_i\}_{i\in\Lambda_m}$、$\{q_i\}_{i\in\Lambda_n}$ と与えられたとき、$m = n$ が成り立ち、$\exists s : \Lambda_n \xrightarrow{\sim} \Lambda_m \forall i \in \Lambda_n$ に対し、$p_i A q_{s(i)}$ が成り立つ。

この定理を素元分解の基本定理といい、その族 $\{p_i\}_{i\in\Lambda_n}$ を求めることをその元 a を素元分解するという。

証明. 単項 ideal 整域 R が与えられたとき、$\exists a \in R$ に対し、その元 a が可逆元でないかつ、0 でないかつ、その整域 R の素元の任意の族 $\{p_i\}_{i\in\Lambda_n}$ に対し、$a = \prod_{i\in\Lambda_n} p_i$ が成り立たないと仮定しよう。このとき、仮定よりその元 a は素元でないことになるので、$\exists b \in R$ に対し、$b|a$ かつ $\neg bA1$ かつ $\neg aAb$ が成り立つ。このとき、定理 3.4.2 よりその元 b は可逆元ではなく、$\exists c \in R$ に対し、$a = bc$ が成り立つかつ、その元 c は可逆元でない。ゆえに、その元 a と同伴でない元々 b、c を用いて $a = bc$ が成り立つ。ここで、これらの元々 b、c がどちらも素元たちの積で表されることができるとすれば、その元 a もそうなり仮定に反する。したがって、これらの元々 b、c どちらかは素元たちの積で表されることができないことになる。このとき、その元 b またはその元 c は可逆元でないかつ、0 でないかつ、その整域 R の素元の任意の族 $\{p_i\}_{i\in\Lambda_n}$ に対し、$b = \prod_{i\in\Lambda_n} p_i$ が成り立たない。ここで、$a = a_1$ かつ $b = a_2$ または $a = a_1$ かつ $c = a_2$ とおかれるとし、$\forall k \in \mathbb{N}$ に対し、その元 a_k が可逆元でないかつ、0 でないかつ、その整域 R の素元の任意の族 $\{p_i\}_{i\in\Lambda_n}$ に対し、$a_k = \prod_{i\in\Lambda_n} p_i$ が成り立たないとすると、同様にして、$a_{k+1}|a_k$ かつその元 a_{k+1} が可逆元でないかつ、0 でないかつ、その整域 R の素元の任意の族 $\{p_i\}_{i\in\Lambda_n}$ に対し、$a_{k+1} = \prod_{i\in\Lambda_n} p_i$ が成り立たないようなもの a_{k+1} が存在することが示される。このようにしてその整域 R の元の列 $\{a_n\}_{n\in\mathbb{N}}$ が得られる。このとき、$\forall n \in \mathbb{N}$ に対し、$a_{n+1}|a_n$ が成り立つかつ、$\forall n_0 \in \mathbb{N}\exists n \in \mathbb{N}$ に対し、$n_0 \leq n$ が成り立つかつ、$a_{n_0} A a_n$ が成り立たないことになる。しかしながら、これは定理 3.4.10 に矛盾する。よって、$\forall a \in R$ に対し、その元 a が可逆元でないかつ、0 でないなら、その整域 R の素元の族 $\{p_i\}_{i\in\Lambda_n}$ が存在して $a = \prod_{i\in\Lambda_n} p_i$ が成り立つ。

上記の議論により、$\forall a \in R$ に対し、その元 a が可逆元でないかつ、0 でないなら、その整域 R の素元の族 $\{p_i\}_{i\in\Lambda_n}$ が存在して $a = \prod_{i\in\Lambda_n} p_i$ が成り立つのであった。このとき、そのような族が $\{p_i\}_{i\in\Lambda_m}$、$\{q_i\}_{i\in\Lambda_n}$ と与えられたなら、$p_1|\prod_{i\in\Lambda_n} q_i$ が成り立つ。定理 3.4.9 より $\exists i' \in \Lambda_n$ に対し、$p_1|q_{i'}$ が成り立つ。ここで、$\exists s : \Lambda_m \to \Lambda_n$ に対し、$s(1) = i'$ とすれば、$p_1|q_{s(1)}$ が成り立ちその元 p_1 は可逆元でなく定理 3.4.2、定理 3.4.8 より $p_1 A q_{s(1)}$ が成り立つ。$\exists k+1 \in \Lambda_m$ に対し、$p_k A q_{s(k)}$ が成り立つようなその族 $\{q_i\}_{i\in\Lambda_n}$ の元 $q_{s(k)}$ が存在すると仮定すると、ある可逆元 ε_k がその整域 R に存在して $p_k = \varepsilon_k q_{s(k)}$ が成り立つ。したがって、次のようになる。

$$
\begin{aligned}
0 &= a - a \\
&= \prod_{i\in\Lambda_n} p_i - \prod_{i\in\Lambda_n} q_i \\
&= \prod_{i\in\Lambda_k} p_i \prod_{i\in\Lambda_m\setminus\Lambda_k} p_i - \prod_{s(i)\in\Lambda_k} q_i \prod_{s(i)\in\Lambda_n\setminus\Lambda_k} q_i \\
&= \prod_{i\in\Lambda_k} p_i \prod_{i\in\Lambda_m\setminus\Lambda_k} p_i - \prod_{i\in\Lambda_k} \varepsilon_i p_i \prod_{s(i)\in\Lambda_n\setminus\Lambda_k} q_i \\
&= \prod_{i\in\Lambda_k} p_i \prod_{i\in\Lambda_m\setminus\Lambda_k} p_i - \prod_{i\in\Lambda_k} \varepsilon_i \prod_{i\in\Lambda_k} p_i \prod_{s(i)\in\Lambda_n\setminus\Lambda_k} q_i \\
&= \prod_{i\in\Lambda_k} p_i \left(\prod_{i\in\Lambda_m\setminus\Lambda_k} p_i - \prod_{i\in\Lambda_k} \varepsilon_i \prod_{s(i)\in\Lambda_n\setminus\Lambda_k} q_i \right)
\end{aligned}
$$

ここで、$\prod_{i\in\Lambda_k} p_i \neq 0$ が成り立つので、$\prod_{i\in\Lambda_m\setminus\Lambda_k} p_i = \prod_{i\in\Lambda_k} \varepsilon_i \prod_{s(i)\in\Lambda_n\setminus\Lambda_k} q_i$ が成り立つことになる。ここで、$k \geq n$ が成り立つと仮定すると、次式が成り立つことになる。

$$
\prod_{i\in\Lambda_m\setminus\Lambda_k} p_i = \prod_{i\in\Lambda_n} \varepsilon_i
$$

しかしながら、これは素元の定義に矛盾している。したがって、$k < n$ が成り立つことになり、したがって、

$p_{k+1}|\prod_{i\in\Lambda_k}\varepsilon_i\prod_{s(i)\in\Lambda_n\setminus\Lambda_k}q_{s(i)}$ が成り立つ。定理 3.4.9 より $\exists i'\in\Lambda_n\setminus\Lambda_k$ に対し、$p_{k+1}|q_{i'}$ が成り立つ。ここで、$s(k+1)=i'$ とすれば、$p_{k+1}|q_{s(k+1)}$ が成り立ちその元 p_{k+1} は可逆元でなく定理 3.4.2、定理 3.4.8 より $p_{k+1}Aq_{s(k+1)}$ が成り立つ。

以上、数学的帰納法により $\forall k\in\Lambda_m$ に対し、$p_kAq_{s(k)}$ が成り立つようなその族 $\{q_i\}_{i\in\Lambda_n}$ の元 $q_{s(k)}$ が存在する。このとき、$m\leq n$ が成り立つことになる。$m<n$ が成り立つと仮定すると、$k=m$ のとき、次式が成り立つことになる。

$$1=\prod_{i\in\Lambda_n}\varepsilon_i\prod_{i\in\Lambda_n\setminus\Lambda_m}q_{s(i)}$$

しかしながら、これは素元の定義に矛盾している。以上より、$m=n$ が成り立つことになる。このとき、その写像 s は全単射である。

よって、そのような族が $\{p_i\}_{i\in\Lambda_m}$、$\{q_i\}_{i\in\Lambda_n}$ と与えられたとき、$m=n$ が成り立ち、$\exists s:\Lambda_n\xrightarrow{\sim}\Lambda_m\forall i\in\Lambda_n$ に対し、$p_iAq_{s(i)}$ が成り立つ。 □

定理 3.4.12. 整域 R が与えられたとき、$\forall a,b\in R$ に対し、$a\neq0$ かつ $b\neq0$ が成り立つなら、$b|a$ が成り立つならそのときに限り、$Ra\subseteq Rb$ が成り立つ。特に、aAb が成り立つならそのときに限り、$Ra=Rb$ が成り立つ。

証明. 整域 R が与えられたとき、$\forall a,b\in R$ に対し、$a\neq0$ かつ $b\neq0$ が成り立つとする。$b|a$ が成り立つなら、$\exists q\in R$ に対し、$a=bq$ が成り立つので、$\forall ra\in Ra$ に対し、$ra=rbq=rqb$ が成り立つので、$ra\in Rb$ が成り立つ。逆に、$Ra\subseteq Rb$ が成り立つなら、$a\in Ra$ より $a\in Rb$ が成り立つことになる。したがって、$\exists q\in R$ に対し、$a=qb=bq$ が成り立つ。よって、$b|a$ が成り立つ。

特に、aAb が成り立つならそのときに限り、$b|a$ かつ $a|b$ が成り立つので、これが成り立つならそのときに限り、$Ra\subseteq Rb$ かつ $Rb\subseteq Ra$ が成り立つ。これが成り立つならそのときに限り、$Ra=Rb$ が成り立つ。 □

定理 3.4.13. 単項 ideal 整域 R が与えられたとき、$\forall p\in R$ に対し、$p\neq0$ が成り立つなら、次のことは同値である。

- その元 p は素元である。
- idealRp はその整域 R の素 ideal である。
- idealRp はその整域 R の極大 ideal である。

証明. 単項 ideal 整域 R が与えられたとき、$\forall p\in R$ に対し、$p\neq0$ が成り立つとする。その元 p は素元であるなら、その元 p は可逆元でなく $1\notin Rp$ が成り立つので、$Rp\neq R$ が成り立つ。さらに、$\forall a,b\in R$ に対し、$ab\in Rp$ が成り立つなら、$p|ab$ が成り立つことになる。ここで、定理 3.4.9 より $p|a$ または $p|b$ が成り立つことになり、したがって、$a\in Rp$ または $b\in Rp$ が成り立つので、その idealRp は素 ideal である。

idealRp がその整域 R の素 ideal であるなら、$\forall a,b\in R$ に対し、$ab\in Rp$ が成り立つなら、$a\in Rp$ または $b\in Rp$ が成り立つことになる。ここで、$Rp\subseteq J$ なる任意の ideal に対し、あるその整域 R の元 q が存在して $J=Rq$ が成り立つ。このとき、定理 3.4.12 より $q|p$ が成り立つことになるので、$\exists s\in R$ に対し、$p=qs$ が成り立つ。$\forall rq\in J=Rq$ に対し、$rqs=rp$ が成り立つので、$rq\in Rp$ または $s\in Rp$ が成り立つ。ここで、$rq\in Rp$ が成り立つなら、$Rq\subseteq Rp$ が得られるので、$Rp=J=Rq$ が成り立つ。$s\in Rp$ が成り立つなら、$\exists t\in R$ に対し、$s=tp$ が成り立つことになるので、$p=qs=qtp$ が成り立つ。したがって、$p(1-qt)=0$ が成り立ち、$p\neq0$ より $qt=1$ が成り立つことになる。このとき、その元 q は可逆元であるので、$\forall u\in R$ に

対し、$u = uq^{-1}q \in Rq$ が成り立つことになり、したがって、$J = Rq = R$ が成り立つ。これにより、その idealRp はその整域 R の極大 ideal である。

idealRp がその整域 R の極大 ideal であるとする。なら、$Rp \subseteq J$ なる任意の ideal に対し、$J = Rp$ または $J = R$ が成り立つ。ここで、その元 p が可逆元であるとすれば、$\forall r \in R$ に対し、$r = rp^{-1}p \in Rp$ が成り立つので、$Rp = R$ が成り立つことになるが、これは極大 ideal の定義に矛盾する。したがって、その元 p は可逆元ではない。ここで、$\forall q \in R$ に対し、$q|p$ が成り立つなら、定理 3.4.12 より $Rp \subseteq Rq$ が成り立つ。このとき、その idealRp がその整域 R の極大 ideal であるので、$Rq = Rp$ または $Rq = R$ が成り立つ。$Rq = Rp$ が成り立つなら、定理 3.4.12 より qAp が成り立つ。$Rq = R$ が成り立つなら、$1 \in Rq$ が成り立つので、その元 q は可逆元で定理 3.4.1、定理 3.4.2 より $qA1$ が成り立つ。以上より、その元 p は可逆元ではなく、$\forall q \in R$ に対し、$q|p$ が成り立つなら、$qA1$ または qAp が成り立つ。したがって、この元 p は素元である。 □

定理 3.4.14. 単項 ideal 整域 R が与えられたとき、$\forall p \in R$ に対し、その元 p が素元であるなら、商環 R/Rp は体である。

証明. 単項 ideal 整域 R が与えられたとき、$\forall p \in R$ に対し、その元 p が素元であるなら、定理 3.4.13 より idealRp はその整域 R の素 ideal であり定理 3.2.28 より商環 R/Rp は整域である。さらに、定理 3.4.13 より idealRp はその整域 R の極大 ideal であり定理 3.2.27 よりその商環 R/Rp は斜体である。以上より、その商環 R/Rp は体である。 □

3.4.3 Euclid 整域

定義 3.4.6. 整域 R と次式のような写像 d が与えられたとき、

$$d : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

$\forall a, b \in R$ に対し、$a \neq 0$ かつ $b \neq 0$ が成り立つなら、$\exists q, r \in R$ に対し、次式が成り立つようなその整域 R を写像 d を大きさとする Euclid 整域といいその写像 d を Euclid 写像という。このとき、その元 q をその元 a をその元 b で割った商、その元 r をその元 a をその元 b で割った余り、剰余という。

例えば、集合 $\mathbb{Z}$、体 K 上の多項式環 $K[X]$ などが挙げられる。

$$a = bq + r \wedge (r = 0 \vee d(r) < d(b))$$

定理 3.4.15. 写像 d を大きさとする Euclid 整域 R は単項 ideal 整域である。

証明. 写像 d を大きさとする Euclid 整域 R が与えられたとき、その整域 R の任意の ideal$J$ に対し、これが零 ideal であるなら、これは単項 ideal である。その ideal$J$ が零元でないその整域 R の元に属されるなら、これらのうち、Euclid 写像 d の像が最も小さいもの a がとられると、定義より $\forall b \in J$ に対し、次式が成り立つようなその整域 R の元々 q、r が存在する。

$$b = aq + r \wedge (r = 0 \vee d(r) < d(a))$$

このとき、$-qa \in J$ より $r = b - qa \in J$ が成り立つので、$d(r) < d(a)$ が成り立つとすれば、その元 a のおき方に矛盾するので、$r = 0$ が成り立つ。したがって、$\forall b \in J$ に対し、$b = aq = qa$ が成り立つので、$J = Ra$ が成り立つ。よって、その整域 R は単項 ideal 整域である。 □

定理 3.4.16. 写像 d を大きさとする Euclid 整域 R が与えられたとき、$\forall a, b \in R$ に対し、$a \neq 0$ かつ $b \neq 0$ が成り立つなら、$\exists q, r \in R$ に対し、次式が成り立つのであった。

$$a = bq + r \wedge (r = 0 \vee d(r) < d(b))$$

このとき、族 $\{a, b\}$ の最大公約元は族 $\{b, r\}$ の最大公約元の同伴である。

証明. 写像 d を大きさとする Euclid 整域 R が与えられたとき、$\forall a, b \in R$ に対し、$a \neq 0$ かつ $b \neq 0$ が成り立つなら、$\exists q, r \in R$ に対し、次式が成り立つのであった。

$$a = bq + r \wedge (r = 0 \vee d(r) < d(b))$$

このとき、族 $\{a, b\}$ の最大公約元 d が与えられたとき、$d|a$ かつ $d|b$ が成り立つのであった。このとき、$d|a - bq$ が成り立つので、$d|r$ が成り立つことになる。これにより、その元 d はその族 $\{b, r\}$ の公約元であり、族 $\{b, r\}$ の最大公約元 e が与えられたとき、最大公約元の定義よりしたがって、$d|e$ が成り立つ。一方で、$e|b$ かつ $e|r$ が成り立ち、したがって、$e|bq + r$ が成り立つので、$e|a$ が成り立つことになる。これにより、その元 e はその族 $\{a, b\}$ の公約元であり、最大公約元の定義よりしたがって、$e|d$ が成り立つ。以上より、dAe が成り立つので、族 $\{a, b\}$ の最大公約元は族 $\{b, r\}$ の最大公約元の同伴である。 □

定理 3.4.17. 写像 d を大きさとする Euclid 整域 R が与えられたとき、$\forall a_1, a_2 \in R$ に対し、$a_1 \neq 0$ かつ $a_2 \neq 0$ が成り立つなら、その整域 R の元の列 $(a_n)_{n\in\mathbb{N}}$ が、$\forall n \in \mathbb{N}$ に対し、次式のように与えられると、

$$a_n = a_{n+1}q_n + a_{n+2} \wedge (a_{n+2} = 0 \vee d(a_{n+2}) < d(a_{n+1}))$$

$\exists n_0 \in \mathbb{N}$ に対し、$a_{n_0+2} = 0$ が成り立つ。

証明. 写像 d を大きさとする Euclid 整域 R が与えられたとき、$\forall a_1, a_2 \in R$ に対し、$a_1 \neq 0$ かつ $a_2 \neq 0$ が成り立つなら、その整域 R の元の列 $(a_n)_{n\in\mathbb{N}}$ が、$\forall n \in \mathbb{N}$ に対し、次式のように与えられたとする。

$$a_n = a_{n+1}q_n + a_{n+2} \wedge (a_{n+2} = 0 \vee d(a_{n+2}) < d(a_{n+1}))$$

$\forall n \in \mathbb{N}$ に対し、$a_{n+2} \neq 0$ が成り立つと仮定すると、$\forall n \in \mathbb{N}$ に対し、$d(a_{n+2}) < d(a_{n+1})$ が成り立つことになるので、$\forall n \in \mathbb{N}\exists m \in V(d) \subseteq \mathbb{N}\cup\{0\}$ に対し、$m < d(a_{n+1})$ が成り立つ、即ち、$\exists n \in \mathbb{N}\forall m \in V(d) \subseteq \mathbb{N}\cup\{0\}$ に対し、$d(a_{n+1}) \leq m$ が成り立たないことになるが、$\forall N \in \mathfrak{P}(\mathbb{N}\cup\{0\})$ に対し、最小元 $\min N$ がその集合 N に存在することに矛盾する。したがって、$\exists n_0 \in \mathbb{N}$ に対し、$a_{n_0+2} = 0$ が成り立つ。 □

定理 3.4.18 (Euclid 互除法)**.** 写像 d を大きさとする Euclid 整域 R が与えられたとき、$\forall a_1, a_2 \in R$ に対し、$a_1 \neq 0$ かつ $a_2 \neq 0$ が成り立つなら、その整域 R の元の列 $(a_n)_{n\in\mathbb{N}}$ が、$\forall n \in \mathbb{N}$ に対し、次式のように与えられると、

$$a_n = a_{n+1}q_n + a_{n+2} \wedge (a_{n+2} = 0 \vee d(a_{n+2}) < d(a_{n+1}))$$

$\exists n \in \mathbb{N}$ に対し、$a_{n+2} = 0$ が成り立つのであった。このような自然数のうち最も小さいものを n_0 とおくと、族 $\{a_1, a_2\}$ の最大公約元は元 a_{n_0+1} に同伴である。この定理を Euclid 互除法という。

証明. 写像 d を大きさとする Euclid 整域 R が与えられたとき、$\forall a_1, a_2 \in R$ に対し、$a_1 \neq 0$ かつ $a_2 \neq 0$ が成り立つなら、その整域 R の元の列 $(a_n)_{n\in\mathbb{N}}$ が、$\forall n \in \mathbb{N}$ に対し、次式のように与えられると、

$$a_n = a_{n+1}q_n + a_{n+2} \wedge (a_{n+2} = 0 \vee d(a_{n+2}) < d(a_{n+1}))$$

$\exists n \in \mathbb{N}$ に対し、$a_{n+2} = 0$ が成り立つのであった。このような自然数のうち最も小さいものを n_0 とおく。$\forall n \in \mathbb{N}$ に対し、族 $\{a_n, a_{n+1}\}$ の最大公約元の 1 つを g_n とおくと、定理 3.4.16 より族 $\{a_1, a_2\}$ の最大公約元 g_1 は族 $\{a_2, a_3\}$ の最大公約元 g_2 の同伴であるので、$g_1 A g_2$ が成り立つ。ここで、$n = k \leq n_0 - 1$ のとき、$g_1 A g_k$ が成り立つと仮定すると、$n = k + 1 \leq n_0$ のとき、$a_k = a_{k+1} q_k + a_{k+2} \wedge (a_{k+2} = 0 \vee d(a_{k+2}) < d(a_{k+1}))$ が成り立ち、定理 3.4.16 より $g_k A g_{k+1}$ が成り立つので、$g_1 A g_{k+1}$ が成り立つ。以上、数学的帰納法により $\forall n \in \Lambda_{n_0}$ に対し、$g_1 A g_n$ が成り立つ。特に、$g_1 A g_{n_0}$ が成り立ち、ここで、$a_{n_0} = a_{n_0+1} q_{n_0}$ が成り立つので、その元 a_{n_0+1} がその族 $\{a_{n_0}, a_{n_0+1}\}$ の公約元である。$\exists q \in R$ に対し、$a_{n_0+1} = q g_{n_0}$ が成り立つので、$g_{n_0} | a_{n_0+1}$ が成り立つことになり、したがって、$g_{n_0} A a_{n_0+1}$ が成り立つ。以上より、$g_1 A a_{n_0+1}$ が成り立つので、族 $\{a_1, a_2\}$ の最大公約元は元 a_{n_0+1} に同伴である。 □

3.4.4 既約多項式

定義 3.4.7. 体 K 上の多項式環 $K[X]$ が与えられたとき、これの素元をその多項式環 $K[X]$ における既約多項式という。特に、$f \in K[X]$ なる多項式 f が素元であるなら、その多項式 f は既約であるという。逆に、$f \in K[X]$ なる多項式 f が零元でないかつ、素元でないなら、その多項式 f は可約であるという。

定理 3.4.19. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall p \in K[X]$ に対し、その多項式 p が既約でないならそのときに限り、$\deg p < 1$ が成り立つ、または、$\exists f, g \in K[X]$ に対し、次式が成り立つ。

$$p = fg \wedge 1 \leq \deg f \wedge 1 \leq \deg g$$

証明. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall p \in K[X]$ に対し、その多項式 p が既約でないなら、その多項式 p は零元であるか可逆元である、または、$\exists f \in K[X]$ に対し、$f|p$ が成り立つかつ、$fA\overline{1}$ が成り立たないかつ、fAp が成り立たない。ここで、定理 3.3.11 よりその多項式 p は零元であるか可逆元であるなら、$\deg p < 1$ が成り立つ。さらに、$\exists f \in K[X]$ に対し、$f|p$ が成り立つかつ、$fA\overline{1}$ が成り立たないかつ、fAp が成り立たないなら、$\exists g \in K[X]$ に対し、$p = fg$ が成り立つかつ、定理 3.4.11 より $1 \leq \deg f$ が成り立つかつ、その多項式 g は可逆元でないので、定理 3.4.11 より $1 \leq \deg g$ が成り立つ。以上より、$\deg p < 1$ が成り立つ、または、$\exists f, g \in K[X]$ に対し、次式が成り立つことになる。

$$p = fg \wedge 1 \leq \deg f \wedge 1 \leq \deg g$$

逆に、$\deg p < 1$ が成り立つ、または、$\exists f, g \in K[X]$ に対し、次式が成り立つとする。

$$p = fg \wedge 1 \leq \deg f \wedge 1 \leq \deg g$$

$\deg p < 1$ が成り立つなら、定理 3.4.11 よりその多項式 p は $\overline{0}$ であるか可逆元である。さらに、多項式たち f、g は定理 3.4.11 より零元でないかつ、可逆元でないので、$fA\overline{1}$ が成り立たないかつ、fAp が成り立たない。これにより、その多項式 p は零元であるか可逆元である、または、$f|p$ が成り立つかつ、$fA\overline{1}$ が成り立たないかつ、fAp が成り立たないので、その多項式 p は既約でない。 □

定理 3.4.20. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall p \in K[X]$ に対し、$\deg p = 1$ が成り立つなら、その多項式 p は既約である。

証明. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall p \in K[X]$ に対し、$\deg p = 1$ が成り立つとする。$\exists f, g \in K[X]$ に対し、次式が成り立つと仮定すると、

$$p = fg \wedge 1 \leq \deg f \wedge 1 \leq \deg g$$

定理 3.3.7 より $2 \leq \deg f + \deg g = \deg fg = \deg p$ が成り立つが、その多項式 p が $\deg p = 1$ を満たすことに矛盾する。したがって、$\deg p < 1$ が成り立たないかつ、$\forall f, g \in K[X]$ に対し、次式が成り立たない。

$$p = fg \wedge 1 \leq \deg f \wedge 1 \leq \deg g$$

定理 3.4.19 よりこれが成り立つならそのときに限り、その多項式 p は既約である。 □

定理 3.4.21. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f, g, h \in K[X]$ に対し、$f|gh$ が成り立つかつ、それらの多項式たち f、g が互いに素であるなら、$f|h$ が成り立つ。

証明. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f, g, h \in K[X]$ に対し、$f|gh$ が成り立つかつ、それらの多項式たち f、g が互いに素であるなら、定理 3.4.7 より $K[X] = K[X]f + K[X]g$ が成り立つので、$\exists a, b \in K[X]$ に対し、$af + bg = \overline{1}$ が成り立つ。したがって、$\exists a, b, q \in K[X]$ に対し、$gh = fq$ かつ $af + bg = \overline{1}$ が成り立つことになる。ここで、次のようになるので、

$$\begin{aligned}
\begin{cases} gh = fq \\ af + bg = \overline{1} \end{cases} &\Rightarrow \begin{cases} bgh = bfq \\ bg = \overline{1} - af \end{cases} \\
&\Rightarrow \left(\overline{1} - af\right) h = bfq \\
&\Leftrightarrow h - afh = bfq \\
&\Leftrightarrow h = fah + fbq \\
&\Leftrightarrow h = f(ah + bq) \\
&\Rightarrow f|h
\end{aligned}$$

よって、$f|h$ が成り立つ。 □

定理 3.4.22. 体 K 上の任意の 0 でない有理式 φ が与えられたとき、$\exists f, g \in K[X]$ に対し、これらの多項式たち f、g は互いに素で $\varphi = \frac{f}{g}$ が成り立つ。また、このような多項式たちが $\varphi = \frac{f}{g} = \frac{f'}{g'}$ と与えられたとき、$\exists k \in K$ に対し、$f = \overline{k}f'$ かつ $g = \overline{k}g'$ が成り立つ。

証明. 体 K 上の任意の 0 でない有理式 φ が与えられたとき、$\exists f, g \in K[X]$ に対し、商の体の定義より $\varphi = \frac{f}{g}$ が成り立つ。ここで、それらの多項式たち f、g を素元分解すると、ある既約多項式たちの族々 $\{p_i\}_{i \in \Lambda_m}$、$\{q_i\}_{i \in \Lambda_n}$ が存在して次式が成り立つ。

$$f = \prod_{i \in \Lambda_m} p_i, \quad g = \prod_{i \in \Lambda_n} q_i$$

ここで、$\mathfrak{p} = \{p_i\}_{i \in \Lambda_m} \cap \{q_i\}_{i \in \Lambda_n}$ とおかれると、$\prod \mathfrak{p} | f$ かつ $\prod \mathfrak{p} | g$ が成り立つので、$\exists q, r \in K[X]$ に対し、$f = \prod \mathfrak{p} q$ かつ $g = \prod \mathfrak{p} r$ が成り立つことになる。ここで、これらの多項式たち q、r が互いに素でないとすれば、族 $\{f, g\}$ の最大公約元が $\overline{1}$ でないことになるので、任意のその族 $\{f, g\}$ の最大公約元 d に対し、$dA\overline{1}$ が成り立つことになる。定理 3.4.2 よりその多項式 d は可逆元でなく定理 3.3.11 よりその多項式 d は $\deg d = 1$ を満たさない。ここで、$d = \overline{0}$ とすれば、$g = \overline{0}$ が成り立つが、これは商の体の定義に反する。したがって、$1 \leq \deg d$ が成り立つことになる。その多項式 d を素元分解すると、ある既約多項式たちの族 $\{r_i\}_{i \in \Lambda_o}$ が存在して $d = \prod_{i \in \Lambda_o} r_i$ が成り立つ。このとき、$\exists q', r' \in K[X]$ に対し、次式が成り立つ。

$$f = \prod \mathfrak{p} q = \prod \mathfrak{p} d q' = \prod \mathfrak{p} \prod_{i \in \Lambda_o} r_i q'$$

$$g = \prod \mathfrak{p} r = \prod \mathfrak{p} d r' = \prod \mathfrak{p} \prod_{i \in \Lambda_o} r_i r'$$

しかしながら、これは $\{r_i\}_{i \in \Lambda_o} \subseteq \mathfrak{p} = \{p_i\}_{i \in \Lambda_m} \cap \{q_i\}_{i \in \Lambda_n}$ が成り立たないことを意味しておりその族 $\mathfrak{p}$ の定義に矛盾する。したがって、これらの多項式たち q、r が互いに素であり次式が成り立つ。

$$\varphi = \frac{f}{g} = \frac{\prod \mathfrak{p} q}{\prod \mathfrak{p} r} = \frac{\prod \mathfrak{p}}{\prod \mathfrak{p}} \frac{q}{r} = \frac{q}{r}$$

また、このような多項式たちが $\varphi = \frac{f}{g} = \frac{f'}{g'}$ と与えられたとき、$\frac{f}{g} = \frac{f'}{g'}$ が成り立つならそのときに限り、$fg' = f'g$ が成り立つことになり、それらの多項式たち f、g が互いに素であるなら、定理 3.4.7 より $K[X] = K[X]f + K[X]g$ が成り立つので、$\exists a, b \in K[X]$ に対し、$af + bg = \overline{1}$ が成り立つ。同様にして、$\exists a', b' \in K[X]$ に対し、$a'f' + b'g' = \overline{1}$ が成り立つ。このとき、$a'f' = \overline{1} - b'g'$ かつ $af = \overline{1} - bg$ が成り立つので、次のようになる。

$$\begin{aligned}
g &= g - b'g'g + b'g'g \\
&= \left(\overline{1} - b'g'\right) g + b'g'g \\
&= a'f'g + b'g'g \\
&= a'fg' + b'gg' \\
&= \left(a'f + b'g\right) g' \\
g' &= g' - bgg' + bgg' \\
&= \left(\overline{1} - bg\right) g' + bgg' \\
&= afg' + bgg' \\
&= af'g + bg'g \\
&= \left(af' + bg'\right) g
\end{aligned}$$

したがって、$gg' \neq 0$ が成り立つことに注意すれば、次のようになる。

$$\begin{aligned}
\overline{0} &= gg' - gg' \\
&= gg' - \left(a'f + b'g\right)\left(af' + bg'\right) gg' \\
&= \left(\overline{1} - \left(a'f + b'g\right)\left(af' + bg'\right)\right) gg'
\end{aligned}$$

したがって、$\left(a'f + b'g\right)\left(af' + bg'\right) = \overline{1}$ が得られる。これにより、多項式たち $a'f + b'g$、$af' + bg'$ は可逆元である。ここで、定理 3.3.11 より $\deg\left(a'f + b'g\right) = \deg\left(af' + bg'\right) = 1$ が成り立つので、$\exists k \in K$ に対し、$a'f + b'g = \overline{k}$ が成り立ち、したがって、$g = \overline{k}g'$ が成り立つ。また、同様にして、$b'g' = \overline{1} - a'f'$ が成り立つので、次のようになる。

$$\begin{aligned}
b'fg' &= \left(\overline{1} - a'f'\right) f \\
&= f - a'f'f \\
&= b'f'g
\end{aligned}$$

これが成り立つならそのときに限り、$f = \left(b'g + a'f\right) f' = \overline{k}f'$ が成り立つ。よって、$\exists k \in K$ に対し、$f = \overline{k}f'$ かつ $g = \overline{k}g'$ が成り立つ。 □

定義 3.4.8. 体 K 上の 0 でない有理式 $\varphi = \frac{f}{g}$ が $\deg f < \deg g$ を満たすとき、その有理式 φ を真分数式という。

定理 3.4.23. 体 K 上の任意の 0 でない有理式 $\varphi = \frac{f}{g}$ が与えられたとき、真分数式 φ' とその多項式環 $K[X]$ の多項式 h が一意的に存在して次式が成り立つ[*12]。

$$\varphi = \frac{f}{g} = \varphi' + h$$

証明. 体 K 上の任意の 0 でない有理式 $\varphi = \frac{f}{g}$ が与えられたとき、定理 3.4.22 より $\exists f', g' \in K[X]$ に対し、これらの多項式たち f'、g' は互いに素で $\varphi = \frac{f'}{g'}$ が成り立つ。このとき、$fg' = f'g$ が成り立ち、それらの多項式たち f'、g' が互いに素であるなら、定理 3.4.7 より $K[X] = K[X]f' + K[X]g'$ が成り立つので、$\exists a', b' \in K[X]$ に対し、$a'f' + b'g' = \overline{1}$ が成り立つ。ここで、$a' = \overline{0}$ または $b' = \overline{0}$ が成り立つなら、$a' = b' = \overline{0}$ は成り立たずこの場合、その多項式 f' が可逆元である、または、その多項式 g' が可逆元であることになる。その多項式 f' が可逆元であるなら、定理 3.3.11 より $\deg f' < \deg g'$ が成り立つので、すでに求める命題が示されている。その多項式 g' が可逆元であるなら、$\frac{f'}{g'}$ は多項式であるから、すでに求める命題が示されている。$a' \neq \overline{0}$ かつ $b' \neq \overline{0}$ が成り立つとき、$\deg g' = 0$ が成り立つなら、$\frac{f'}{g'}$ は多項式であるから、すでに求める命題が示されている。最後に、$0 < \deg g'$ が成り立つとき、次のようになる。

$$\begin{aligned}
\varphi = \frac{f}{g} = \frac{f'}{g'} &= \frac{a'f'}{a'g'} \\
&= \frac{\overline{1} - b'g'}{a'g'} \\
&= \frac{a'g' - a'g'b'g'}{a'g'a'g'} \\
&= \frac{\overline{1}}{a'g'} - \frac{b'g'}{a'g'} \\
&= \frac{\overline{1}}{a'g'} - \frac{b'}{a'}
\end{aligned}$$

このとき、$-\frac{b'}{a'}$ は多項式であり $\deg a'g' = \deg a' + \deg g' > \deg \overline{1} = 0$ が成り立つので、求める命題が示されている。

このとき、真分数式 $\varphi' = \frac{f'}{g'}$ とその多項式環 $K[X]$ の多項式 h が存在して次式が成り立つとき、

$$\varphi = \frac{f}{g} = \frac{f'}{g'} + h$$

$fg' = f'g + gg'h$ が成り立つので、除法の定理より多項式 f' と多項式 $gg'h$ が一意的に存在することになる。さらに、$gg'h = s$ とおくと、除法の定理より多項式 $g'h$ が一意的に存在する。同様にして、多項式 h が一意的に存在するので、真分数式 φ' とその多項式環 $K[X]$ の多項式 h が一意的に存在して次式が成り立つ[*13]。

$$\varphi = \frac{f}{g} = \varphi' + h$$

□

定理 3.4.24. 体 K 上の任意の 0 でない有理式 $\varphi = \frac{f}{g}$ が与えられたとき、これらの多項式たち f、g が互いに素でその多項式 g が monic であり、素元分解の基本定理より、互いに異なる既約な monic の族 $\{p_i\}_{i \in \Lambda_n}$ と自然

[*12] 証明するとき、除法の定理で一発じゃんと思うかもしれませんが (実際、僕も一瞬思いましたが)、φ' は多項式ではないので、除法の定理が使えないことになることに注意してください…。

[*13] この辺りの議論に少し不満があるので、もっといい方法があれば教えてください!

数の族 $\{\alpha_i\}_{i\in\Lambda_n}$ が存在して $g=\prod_{i\in\Lambda_n}p_i^{\alpha_i}$ が成り立つのであった。このとき、多項式 h と、$\deg h_i<\deg p_i^{\alpha_i}$ が成り立つかつ、$p_i|h_i$ が成り立たない多項式の族 $\{h_i\}_{i\in\Lambda_n}$ が一意的に存在して次式が成り立つ。

$$\varphi=\sum_{i\in\Lambda_n}\frac{h_i}{p_i^{\alpha_i}}+h$$

証明. 体 K 上の任意の 0 でない有理式 $\varphi=\frac{f}{g}$ が与えられたとき、これらの多項式たち f、g が互いに素でその多項式 g が monic であり、素元分解の基本定理より、互いに異なる既約な monic の族 $\{p_i\}_{i\in\Lambda_n}$ と自然数の族 $\{\alpha_i\}_{i\in\Lambda_n}$ が存在して $g=\prod_{i\in\Lambda_n}p_i^{\alpha_i}$ が成り立つなら、族 $\left\{\prod_{i\in\Lambda_n\setminus\{i'\}}p_i^{\alpha_i}\right\}_{i'\in\Lambda_n}$ の最大公約元の 1 つとして 1 が挙げられるので、定理 3.4.7 より次式が成り立つ。

$$K[X]=\sum_{i'\in\Lambda_n}K[X]\prod_{i\in\Lambda_n\setminus\{i'\}}p_i^{\alpha_i}$$

このとき、ある体 K 上の多項式たちの族 $\{k_{i'}\}_{i'\in\Lambda_n}$ が存在して次式が成り立つ。

$$f=\sum_{i'\in\Lambda_n}k_{i'}\prod_{i\in\Lambda_n\setminus\{i'\}}p_i^{\alpha_i}$$

両辺に g で割れば次のようになり

$$\begin{aligned}\varphi&=\frac{f}{g}\\&=\sum_{i'\in\Lambda_n}\frac{k_{i'}}{g}\prod_{i\in\Lambda_n\setminus\{i'\}}p_i^{\alpha_i}\\&=\sum_{i'\in\Lambda_n}\frac{k_{i'}\prod_{i\in\Lambda_n\setminus\{i'\}}p_i^{\alpha_i}}{\prod_{i\in\Lambda_n}p_i^{\alpha_i}}\\&=\sum_{i'\in\Lambda_n}\frac{k_{i'}\prod_{i\in\Lambda_n\setminus\{i'\}}p_i^{\alpha_i}}{p_{i'}^{\alpha_{i'}}\prod_{i\in\Lambda_n\setminus\{i'\}}p_i^{\alpha_i}}\\&=\sum_{i'\in\Lambda_n}\frac{k_{i'}}{p_{i'}^{\alpha_{i'}}}\\&=\sum_{i\in\Lambda_n}\frac{k_i}{p_i^{\alpha_i}}\end{aligned}$$

定理 3.4.23 より多項式 h と $\deg h_i<\deg p_i^{\alpha_i}$ が成り立つ多項式の族 $\{h_i\}_{i\in\Lambda_n}$ が一意的に存在して次式が成り立つ。

$$\varphi=\sum_{i\in\Lambda_n}\frac{h_i}{p_i^{\alpha_i}}+h$$

$\exists i'\in\Lambda_n$ に対し、$p_{i'}|h_{i'}$ が成り立つとすれば、$\exists q\in K[X]$ に対し、$h_{i'}=p_{i'}q$ が成り立つことになる。このとき、次のようになるので、

$$\begin{aligned}\varphi&=\sum_{i\in\Lambda_n}\frac{h_i}{p_i^{\alpha_i}}+h\\&=\sum_{i''\in\Lambda_n}\frac{h_{i''}}{p_{i''}^{\alpha_{i''}}}+h\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i'' \in \Lambda_n} \frac{h_{i''} \prod_{i \in \Lambda_n \setminus \{i''\}} p_i^{\alpha_i}}{p_{i''}^{\alpha_{i''}} \prod_{i \in \Lambda_n \setminus \{i''\}} p_i^{\alpha_i}} + \frac{h \prod_{i \in \Lambda_n} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} \\
&= \sum_{i'' \in \Lambda_n} \frac{h_{i''} \prod_{i \in \Lambda_n \setminus \{i''\}} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} + \frac{h \prod_{i \in \Lambda_n} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} \\
&= \sum_{i'' \in \Lambda_n \setminus \{i'\}} \frac{h_{i''} \prod_{i \in \Lambda_n \setminus \{i''\}} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} + \frac{h_{i'} \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} + \frac{h \prod_{i \in \Lambda_n} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} \\
&= \frac{\sum_{i'' \in \Lambda_n \setminus \{i'\}} h_{i''} \prod_{i \in \Lambda_n \setminus \{i''\}} p_i^{\alpha_i} + h_{i'} \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i} + h \prod_{i \in \Lambda_n} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} \\
&= \frac{\sum_{i'' \in \Lambda_n \setminus \{i'\}} h_{i''} p_{i'}^{\alpha_{i'}} \prod_{i \in \Lambda_n \setminus \{i', i''\}} p_i^{\alpha_i} + p_{i'} q \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i} + h p_{i'} \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i}}{\prod_{i \in \Lambda_n} p_i^{\alpha_i}} \\
&= \frac{p_{i'} \left(\sum_{i'' \in \Lambda_n \setminus \{i'\}} h_{i''} p_{i'}^{\alpha_{i'} - 1} \prod_{i \in \Lambda_n \setminus \{i', i''\}} p_i^{\alpha_i} + q \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i} + h \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i} \right)}{g}
\end{aligned}
$$

次式のようにおかれると、

$$
s = \sum_{i'' \in \Lambda_n \setminus \{i'\}} h_{i''} p_{i'}^{\alpha_{i'} - 1} \prod_{i \in \Lambda_n \setminus \{i', i''\}} p_i^{\alpha_i} + q \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i} + h \prod_{i \in \Lambda_n \setminus \{i'\}} p_i^{\alpha_i}
$$

次式が成り立つ。

$$
\varphi = \frac{f}{g} = \frac{p_{i'} s}{g}
$$

これにより、$fg = p_{i'} sg$ が成り立ち、したがって、これが成り立つならそのときに限り、$(f - p_{i'} s)\, g = 0$ が成り立つ。ここで、$g \neq \overline{0}$ より $f = p_{i'} s$ が成り立ち、したがって、族 $\{f, g\}$ の公約元の 1 つが既約多項式 $p_{i'}$ で定理 3.4.19 より $p_{i'} A1$ が成り立たない。しかしながら、これはこれらの多項式たち f、g が互いに素であることに矛盾する。よって、多項式 h と、$\deg h_i < \deg p_i^{\alpha_i}$ が成り立つかつ、$p_i | h_i$ が成り立たない多項式の族 $\{h_i\}_{i \in \Lambda_n}$ が一意的に存在して次式が成り立つ。

$$
\varphi = \sum_{i \in \Lambda_n} \frac{h_i}{p_i^{\alpha_i}} + h
$$

□

定理 3.4.25 (ψ 進展開)**.** 体 K 上の定数でない多項式 ψ と体 K 上の任意の多項式 f が与えられたとき、添数集合 $\Lambda_n \cup \{0\}$ によって添数づけられた $\deg s_i < \deg \psi$ なる多項式たちの族 $\{s_i\}_{i \in \Lambda_n \cup \{0\}}$ が一意的に存在して次式が成り立つ。

$$
h = \sum_{i \in \Lambda_n \cup \{0\}} s_i \psi^i
$$

このように表すことをその多項式 h の ψ 進展開という。

これは次のようにして示される。

1 除法の定理より $\deg s_0 < \deg \psi$ かつ $h = q_1 \psi + s_0$ なる多項式たち q_1、s_0 が一意的に存在する。
2 数学的帰納法により $\forall n \in \mathbb{N}$ に対し、$\deg s_n < \deg \psi$ かつ $q_n = q_{n+1} \psi + s_n$ なる多項式たち q_{n+1}、s_n が一意的に存在するかつ、$\deg q_{n+1} < \deg q_n$ かつ $\deg s_n < \deg \psi$ も成り立つ。

3 背理法により $\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}$ に対し、$q_{n_0} = \overline{0}$ が成り立つことが示される。

4 このようにして、多項式の族々 $\{q_n\}_{n \in \Lambda_{n_0}}$、$\{s_n\}_{n \in \Lambda_{n_0} \cup \{0\}}$ が得られる。

5 数学的帰納法によりその族 $\{q_n\}_{n \in \Lambda_{n_0}}$ を消去することで $\forall n \in \Lambda_{n_0 - 1}$ に対し、$q_{n_0 - k} = \sum_{i \in \Lambda_k} s_{n_0 - i} \psi^{k-i}$ が成り立つ。

6 その多項式 h に代入することで求める命題が示される。

例えば、多項式環 $\mathbb{Q}[x]$ において、多項式 $x^4 + x + 1$ の $x + 1$ 進展開を求めよう。

1 除法の定理より次式が成り立つ。

$$x^4 + x + 1 = (x + 1)\left(x^3 - x^2 + x\right) + 1$$

2 これを繰り返すことで次式が成り立つ。

$$\begin{aligned} x^3 - x^2 + x &= (x + 1)\left(x^2 - 2x + 3\right) - 3 \\ x^2 - 2x + 3 &= (x + 1)(x - 3) + 6 \\ x - 3 &= (x + 1) - 4 \end{aligned}$$

3 このとき、確かに次式が成り立つ。

$$1 = (x + 1)0 + 1$$

4 このようにして、多項式の族々 $\left\{x^3 - x^2 + x,\ \ x^2 - 2x + 3,\ \ x - 3,\ \ 1,\ \ 0\right\}$、$\{1,\ -3,\ \ 6,\ -4\}$ が得られる。

5 したがって、次のようになる。

$$\begin{aligned} x^3 - x^2 + x &= (x + 1)\left(x^2 - 2x + 3\right) - 3 \\ &= (x + 1)\left((x + 1)(x - 3) + 6\right) - 3 \\ &= (x + 1)^2(x - 3) + 6(x + 1) - 3 \\ &= (x + 1)^2\left((x + 1) - 4\right) + 6(x + 1) - 3 \\ &= (x + 1)^3 - 4(x + 1)^2 + 6(x + 1) - 3 \end{aligned}$$

6 その多項式 $x^4 + x + 1$ に代入することで次式が得られる。

$$\begin{aligned} x^4 + x + 1 &= (x + 1)\left((x + 1)^3 - 4(x + 1)^2 + 6(x + 1) - 3\right) + 1 \\ &= (x + 1)^4 - 4(x + 1)^3 + 6(x + 1)^2 - 3(x + 1) + 1 \end{aligned}$$

証明. 体 K 上の定数でない多項式 ψ と体 K 上の任意の多項式 f が与えられたとき、除法の定理より $\deg s_0 < \deg \psi$ かつ $h = q_1\psi + s_0$ なる多項式たち q_1、s_0 が一意的に存在する。$q_1 = \overline{0}$ が成り立つなら、すでに求める命題が示されている。以下、$q_1 \neq \overline{0}$ が成り立つとする。このとき、再び除法の定理より $\deg s_1 < \deg \psi$ かつ $q_1 = q_2\psi + s_1$ なる多項式たち q_2、s_1 が一意的に存在する。ここで、$q_2 = \overline{0}$ が成り立つなら、$\deg q_2 < \deg q_1$ が成り立つ[*14]。以下、$q_1 \neq \overline{0}$ が成り立つとするとき、次式が成り立つことから、

$$\begin{aligned} \deg q_2 &= \deg q_2 + \deg \psi - \deg \psi \\ &= \deg q_2\psi - \deg \psi \end{aligned}$$

[*14] 実は、$h = q_1\psi + s_0 = s_1\psi + s_0$ が成り立ちますので、求める命題がもうこれで示されています。

$$
\begin{aligned}
&= \deg(q_1 - s_1) - \deg\psi \\
&\leq \deg q_1 + \deg(-s_1) - \deg\psi \\
&= \deg q_1 + \deg s_1 - \deg\psi \\
&< \deg q_1 + \deg\psi - \deg\psi \\
&= \deg q_1
\end{aligned}
$$

$\deg q_2 < \deg q_1$ が成り立つ。

ここで、$n = k$ のとき、$\deg s_k < \deg\psi$ かつ $q_k = q_{k+1}\psi + s_k$ なる多項式たち q_{k+1}、s_k が一意的に存在するかつ、$\deg q_{k+1} < \deg q_k$ が成り立つと仮定する。$n = k+1$ のとき、$q_k \neq \overline{0}$ が成り立つことにより、再び除法の定理より $\deg s_{k+1} < \deg\psi$ かつ $q_{k+1} = q_{k+2}\psi + s_{k+1}$ なる多項式たち q_{k+2}、s_{k+1} が一意的に存在する。ここで、$q_{k+2} = \overline{0}$ が成り立つなら、$\deg q_2 < \deg q_1$ が成り立つ。以下、$q_{k+2} \neq \overline{0}$ が成り立つとすると、次式が成り立つことから、

$$
\begin{aligned}
\deg q_{k+2} &= \deg q_{k+2} + \deg\psi - \deg\psi \\
&= \deg q_{k+2}\psi - \deg\psi \\
&= \deg(q_{k+1} - s_{k+1}) - \deg\psi \\
&\leq \deg q_{k+1} + \deg(-s_{k+1}) - \deg\psi \\
&= \deg q_{k+1} + \deg s_{k+1} - \deg\psi \\
&< \deg q_{k+1} + \deg\psi - \deg\psi \\
&= \deg q_{k+1}
\end{aligned}
$$

$\deg q_{k+2} < \deg q_{k+1}$ が成り立つ。

以上、数学的帰納法により $\forall n \in \mathbb{N}$ に対し、$\deg s_n < \deg\psi$ かつ $q_n = q_{n+1}\psi + s_n$ なる多項式たち q_{n+1}、s_n が一意的に存在するかつ、$\deg q_{n+1} < \deg q_n$ が成り立つ。ここで、除法の定理より $\deg s_n < \deg\psi$ も成り立つ。このとき、$\forall n \in \mathbb{N}$ に対し、$\deg q_{n+1} < \deg q_n$ が成り立つとすれば、$\deg q_n \in \mathbb{N} \cup \{0\}$ が成り立つことに矛盾する。したがって、$\exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}$ に対し、$\deg q_{n_0} < \deg q_n$ が成り立つ、即ち、$q_{n_0} = \overline{0}$ が成り立つことになる。このようにして、多項式の族々 $\{q_n\}_{n\in\Lambda_{n_0}}$、$\{s_n\}_{n\in\Lambda_{n_0}\cup\{0\}}$ が得られる。

ここで、$n_0 = 1$ のときはすでに示されてるので、$2 \leq n_0$ が成り立つとする。このとき、次のようになる。

$$
q_{n_0-1} = q_{n_0}\psi + s_{n_0-1} = s_{n_0-1}
$$

$n = k$ のとき、$q_{n_0-k} = \sum_{i\in\Lambda_k} s_{n_0-i}\psi^{k-i}$ が成り立つと仮定すると、$n = k+1$ のとき、$q_{n_0-k-1} = q_{n_0-k}\psi + s_{n_0-k-1}$ なる多項式たち q_{n_0-k-1}、s_{n_0-k-1} が一意的に存在するので、次のようになる。

$$
\begin{aligned}
q_{n_0-k-1} &= q_{n_0-k}\psi + s_{n_0-k-1} \\
&= \sum_{i\in\Lambda_k} s_{n_0-i}\psi^{k-i}\psi + s_{n_0-k-1} \\
&= \sum_{i\in\Lambda_k} s_{n_0-i}\psi^{k+1-i} + s_{n_0-k-1} \\
&= \sum_{i\in\Lambda_k} s_{n_0-i}\psi^{(k+1)-i} + s_{n_0-(k+1)}\psi^{(k+1)-(k+1)} \\
&= \sum_{i\in\Lambda_{k+1}} s_{n_0-i}\psi^{(k+1)-i}
\end{aligned}
$$

これにより、数学的帰納法により $\forall n \in \Lambda_{n_0-1}$ に対し、$q_{n_0-k} = \sum_{i\in\Lambda_k} s_{n_0-i}\psi^{k-i}$ が成り立つことが示された。

したがって、次のようになる。

$$\begin{aligned}
h &= q_1\psi + s_0 \\
&= q_{n_0-(n_0-1)}\psi + s_0 \\
&= \sum_{i\in\Lambda_{n_0-1}} s_{n_0-i}\psi^{n_0-i-1}\psi + s_0 \\
&= \sum_{i\in\Lambda_{n_0-1}} s_{n_0-i}\psi^{n_0-i} + s_0 \\
&= \sum_{i\in\Lambda_{n_0-1}} s_i\psi^i + s_0 \\
&= \sum_{i\in\Lambda_{n_0-1}\cup\{0\}} s_i\psi^i
\end{aligned}$$

よって、添数集合 $\Lambda_{n_0}\cup\{0\}$ によって添数づけられた $\deg s_i < \deg\psi$ なる多項式たちの族 $\{s_i\}_{i\in\Lambda_{n_0}\cup\{0\}}$ が一意的に存在して次式が成り立つ。

$$h = \sum_{i\in\Lambda_{n_0}\cup\{0\}} s_i\psi^i$$

□

定理 3.4.26. 体 K 上の多項式環 $K[X]$ 上の既約多項式 p、自然数 α が与えられたとき、$\deg h < \deg p^\alpha$ なる零元でないその多項式環 $K[X]$ 上の任意の多項式 h が与えられたとき、次式を満たすような $\deg u_i < \deg p$ なる添数集合 Λ_α によって添数づけられた多項式の族 $\{u_i\}_{i\in\Lambda_\alpha}$ が一意的に存在する。

$$\frac{h}{p^\alpha} = \sum_{i\in\Lambda_\alpha} \frac{u_i}{p^i}$$

証明. 体 K 上の多項式環 $K[X]$ 上の既約多項式 p、自然数 α が与えられたとき、$\deg h < \deg p^\alpha$ なる零元でないその多項式環 $K[X]$ 上の任意の多項式 h が与えられたとき、その多項式 h の p 進展開を求めると、$\deg s_i < \deg p$ が成り立つかつ、次のようになる。

$$h = \sum_{i\in\Lambda_n\cup\{0\}} s_i p^i$$

ここで、$\alpha - 1 < n$ が成り立つと仮定すると、次のようになる。

$$\begin{aligned}
\frac{h}{p^\alpha} &= \sum_{i\in\Lambda_n\cup\{0\}} \frac{s_i p^i}{p^\alpha} \\
&= \sum_{i\in\Lambda_{\alpha-1}\cup\{0\}} \frac{s_i p^i}{p^\alpha} + \frac{s_\alpha p^\alpha}{p^\alpha} + \sum_{i\in\Lambda_n\setminus\Lambda_\alpha} \frac{s_i p^i}{p^\alpha} \\
&= \sum_{i\in\Lambda_{\alpha-1}\cup\{0\}} \frac{s_i p^i}{p^\alpha} + s_\alpha + \sum_{i\in\Lambda_n\setminus\Lambda_\alpha} s_i p^{i-\alpha} \\
&= \sum_{i\in\Lambda_{\alpha-1}\cup\{0\}} \frac{s_i p^i}{p^\alpha} + s_\alpha + \sum_{i\in\Lambda_{n-\alpha}} s_{i+\alpha} p^i \\
&= \frac{\sum_{i\in\Lambda_{\alpha-1}\cup\{0\}} s_i p^i}{p^\alpha} + s_\alpha + \sum_{i\in\Lambda_{n-\alpha}} s_{i+\alpha} p^i
\end{aligned}$$

しかしながら、有理式 $\frac{h}{p^\alpha}$ は真分数式であることから、これは定理 3.4.23 に矛盾している。したがって、$n \leq \alpha - 1$ が成り立つことになる。このとき、次のように添数集合 Λ_α によって添数づけられた多項式の族 $\{u_i\}_{i\in\Lambda_\alpha}$ が次式のようにおかれると、

$$u_i = \begin{cases} 0 & \text{if} \quad i \in \Lambda_{\alpha-n-1} \\ s_{\alpha-i} & \text{if} \quad i \in \Lambda_\alpha \setminus \Lambda_{\alpha-n-1} \end{cases}$$

次のようになる。

$$\begin{aligned} \frac{h}{p^\alpha} &= \sum_{i\in\Lambda_n\cup\{0\}} \frac{s_i p^i}{p^\alpha} \\ &= \sum_{i\in\Lambda_n\cup\{0\}} \frac{s_i}{p^{\alpha-i}} \\ &= \sum_{i\in\Lambda_\alpha\setminus\Lambda_{\alpha-n-1}} \frac{s_{\alpha-i}}{p^i} \\ &= \sum_{i\in\Lambda_{\alpha-n-1}} \frac{0}{p^i} + \sum_{i\in\Lambda_\alpha\setminus\Lambda_{\alpha-n-1}} \frac{s_{\alpha-i}}{p^i} \\ &= \sum_{i\in\Lambda_{\alpha-n-1}} \frac{u_i}{p^i} + \sum_{i\in\Lambda_\alpha\setminus\Lambda_{\alpha-n-1}} \frac{u_i}{p^i} \\ &= \sum_{i\in\Lambda_\alpha} \frac{u_i}{p^i} \end{aligned}$$

よって、次式を満たすような $\deg u_i < \deg p$ なる添数集合 Λ_α によって添数づけられた多項式の族 $\{u_i\}_{i\in\Lambda_\alpha}$ が一意的に存在する。

$$\frac{h}{p^\alpha} = \sum_{i\in\Lambda_\alpha} \frac{u_i}{p^i}$$

□

定理 3.4.27 (部分分数分解)**.** 体 K 上の任意の 0 でない有理式 $\varphi = \frac{f}{g}$ が与えられたとき、これらの多項式たち f、g が互いに素であるなら、多項式 h と、$\deg u_{ij} < \deg p_i$ なる添数集合 $\Lambda_n \times \Lambda_{\alpha_i}$ によって添数づけられた多項式の族 $\{u_{ij}\}_{(i,j)\in\Lambda_n\times\Lambda_{\alpha_i}}$ が一意的に存在して次式が成り立つ。

$$\varphi = \sum_{i\in\Lambda_n} \sum_{j\in\Lambda_{\alpha_i}} \frac{u_{ij}}{p^j} + h$$

このように有理式 φ を表すことをその有理式 φ の部分分数分解という。

例えば、$\mathbb{R}$ 上の有理式 φ が次式のように与えられたとき、

$$\varphi = \frac{x^8 + 2x^7 + 3x^6 + 4x^5 + 3x^4 + 2x^3 + x^2 + 1}{x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1}$$

次式が成り立つことから、

$$x^6 + 2x^5 + 3x^4 + 4x^3 + 3x^2 + 2x + 1 = (x+1)^2 \left(x^2+1\right)^2$$

次のようになり、

$$\varphi = \frac{x^2(x+1)^2 \left(x^2+1\right)^2 + 1}{(x+1)^2 \left(x^2+1\right)^2}$$

$$= \frac{1}{(x+1)^2\left(x^2+1\right)^2} + x^2$$

次のようにおくと、

$$\varphi = \frac{a}{x+1} + \frac{b}{(x+1)^2} + \frac{cx+d}{x^2+1} + \frac{ex+f}{\left(x^2+1\right)^2} + x^2$$

あとは、これらの定数たち a、b、c、d、e、f を求めればよく、したがって、次のようになる、

$1 = (a+c)x^5 + (a+b+2c+d)x^4 + (2a+2c+2d+e)x^3 + (2a+2b+2c+2d+2e+f)x^2 + (a+c+2d+e+2f)x + (a$

即ち、次式が成り立つ。

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 2 & 2 & 1 & 0 & 0 \\ 1 & 0 & 1 & 2 & 1 & 2 & 0 \\ 1 & 0 & 1 & 2 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

これを解くと、次のようになるので、

$$\begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/4 \\ -1/2 \\ 1/4 \\ -1/2 \\ 0 \end{pmatrix}$$

したがって、次のようになる。

$$\varphi = \frac{\frac{1}{2}}{x+1} + \frac{\frac{1}{4}}{(x+1)^2} + \frac{-\frac{1}{2}x + \frac{1}{4}}{x^2+1} + \frac{-\frac{1}{2}x}{\left(x^2+1\right)^2} + x^2$$

証明. 体 K 上の任意の 0 でない有理式 $\varphi = \frac{f}{g}$ が与えられたとき、これらの多項式たち f、g が互いに素であるなら、素元分解の基本定理より、互いに異なる既約な monic の族 $\{p_i\}_{i\in\Lambda_n}$ と自然数の族 $\{\alpha_i\}_{i\in\Lambda_n}$ が存在して $g = g_{\mathrm{l.c.}} \prod_{i\in\Lambda_n} p_i^{\alpha_i}$ が成り立つのであった。このとき、次のようになり、

$$\begin{aligned} \varphi = \frac{f}{g} &= \frac{f}{g_{\mathrm{l.c.}} \prod_{i\in\Lambda_n} p_i^{\alpha_i}} \\ &= \frac{1}{g_{\mathrm{l.c.}}} \frac{f}{\prod_{i\in\Lambda_n} p_i^{\alpha_i}} \end{aligned}$$

定理 3.4.24 より多項式 $g_{\mathrm{l.c.}}h$ と、$\deg h_i < \deg p_i^{\alpha_i}$ が成り立つかつ、$p_i | h_i$ が成り立たない多項式の族 $\{h_i\}_{i\in\Lambda_n}$ が一意的に存在して次式が成り立つ。

$$\begin{aligned} \varphi &= \frac{1}{g_{\mathrm{l.c.}}} \left(\sum_{i\in\Lambda_n} \frac{h_i}{p_i^{\alpha_i}} + g_{\mathrm{l.c.}}h \right) \\ &= \sum_{i\in\Lambda_n} \frac{\frac{h_i}{g_{\mathrm{l.c.}}}}{p_i^{\alpha_i}} + h \end{aligned}$$

ここで、$\deg h_i = \deg \frac{h_i}{g_{\mathrm{l.c.}}} < \deg p_i^{\alpha_i}$ が成り立つので、定理 3.4.26 より $\forall i \in \Lambda_n$ に対し、$\deg u_{ij} < \deg p_i$ なる添数集合 Λ_α によって添数づけられた多項式の族 $\{u_{ij}\}_{j\in\Lambda_{\alpha_i}}$ が一意的に存在して次式が成り立つ、

$$\varphi = \sum_{i\in\Lambda_n} \sum_{j\in\Lambda_{\alpha_i}} \frac{u_{ij}}{p^j} + h$$

即ち、多項式 h と、$\deg u_{ij} < \deg p_i$ なる添数集合 $\Lambda_n \times \Lambda_{\alpha_i}$ によって添数づけられた多項式の族 $\{u_{ij}\}_{(i,j)\in\Lambda_n\times\Lambda_{\alpha_i}}$ が一意的に存在して次式が成り立つ。

$$\varphi = \sum_{i\in\Lambda_n} \sum_{j\in\Lambda_{\alpha_i}} \frac{u_{ij}}{p^j} + h$$

□

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976. 新装版第 2 刷 p144-152 ISBN978-4-00-029873-5

3.5　代数的閉体と一意分解整域

3.5.1　因数定理

定理 3.5.1. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、$X - \overline{a}$ で割った余りはその多項式 f の変数 X にその元 a を代入した元である、即ち、この元を $s_a(f)$ とおくと、その商 q を用いて次式が成り立つ。

$$f = (X - \overline{a})\, q + \overline{s_a(f)}$$

証明. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、剰余の定理より $\exists q, r \in K[X]$ に対し、$f = (X - \overline{a})\, q + r$ が成り立つかつ、$\deg r < \deg (X - \overline{a}) = 1$ が成り立つ。このとき、その余り r は定数であることになるので、$\exists b \in K$ に対し、$r = \overline{b}$ が成り立つ。さらに、定理 3.3.9 より $\forall c \in K$ に対し、次式のように定義される写像 s_c は環準同型写像であるので、

$$s_c : K[X] \to K; f \mapsto \sum_{n \in \Lambda_{\deg f} \cup \{0\}} f(n) c^n$$

その多項式 f の変数 X にその元 a を代入した元を $s_a(f)$ とおくと、次のようになる。

$$\begin{aligned} s_a(f) &= s_a\left((X - \overline{a})\, q + r\right) \\ &= s_a\left(X - \overline{a}\right) s_a(q) + s_a(r) \\ &= (a - a) s_a(q) + s_a(r) \\ &= s_a(r) = s_a\left(\overline{b}\right) = b \end{aligned}$$

以上より、次のようになる。

$$\begin{aligned} f &= (X - \overline{a})\, q + r \\ &= (X - \overline{a})\, q + \overline{b} \\ &= (X - \overline{a})\, q + \overline{s_a(f)} \end{aligned}$$

□

定義 3.5.1. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、その多項式 f から定義される多項式写像 P_f によるその体 K の元 a の像 $P_f(a)$ が 0 であるとき、その元 a はその多項式 f の根、解などという。

定理 3.5.2 (因数定理)**.** 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、その多項式 f が多項式 $X - \overline{a}$ で割り切れるならそのときに限り、その元 a がその多項式 f の根の 1 つである。その定理を因数定理という。

証明. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、その多項式 f が多項式 $X - \overline{a}$ で割り切れるなら、$\exists q \in K[X]$ に対し、$f = (X - \overline{a})\, q$ が成り立つ。したがって、その多項式 f から定義される多項式写像 P_f はその多項式 q から定義される多項式写像 P_q を用いて次のようになる。

$$P_f : K \to K; k \mapsto (k - a) P_q(k)$$

したがって、定理 3.3.9 より次式のようになる。

$$P_f(a) = (a - a)P_q(a) = 0$$

逆に、その元 a がその多項式 f の根の 1 つであるとする。除法の定理より $\exists q, r \in K[X]$ に対し、$f = (X - \overline{a})\, q + r$ が成り立つかつ、$\deg r < \deg (X - \overline{a}) = 1$ が成り立つので、その多項式 r は定数である。ここで、$r \neq \overline{0}$ と仮定すると、$\exists b \in K$ に対し、$r = \overline{b}$ が成り立ち、その多項式 f から定義される多項式写像 P_f について、その多項式 q から定義される多項式写像 P_q を用いて次のようになるので、

$$P_f : K \to K; k \mapsto (k - a)P_q(k) + b$$

次のようになる。

$$P_f(a) = (a - a)P_q(a) + b = b$$

ここで、その元 a がその多項式 f の根の 1 つなので、$P_f(a) = b = 0$ が成り立つ。しかしながら、$r = \overline{b} = \overline{0}$ が成り立つことになり、先ほどの仮定に矛盾する。よって、$r = \overline{0}$ が成り立ちその多項式 f がその多項式 $X - \overline{a}$ で割り切れる。 □

3.5.2 代数的閉体

定義 3.5.2. 体 K 上の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、$1 \leq \deg f$ が成り立つなら、その多項式 f がその体 K の中にその多項式 f の根を必ずもつようなその体 K を代数的閉体という。

定理 3.5.3 (代数学の基本定理)**.** 複素数全体の集合 $\mathbf{C}$ は代数的閉体である。この定理を代数学の基本定理という。

しかしながら、その証明は、代数学的な手法というよりむしろ解析学的な手法のほうが重要で、このことを述べるとかなり長くなってしまうので、ここでは解析学に譲ることにする。

定理 3.5.4. 代数的閉体 K の多項式環 $K[X]$ が与えられたとき、$\forall p \in K[X]$ に対し、その多項式 p が既約多項式であるならそのときに限り、$\deg p = 1$ が成り立つ。

証明. 代数的閉体 K の多項式環 $K[X]$ が与えられたとき、$\forall p \in K[X]$ に対し、その多項式 p が既約多項式であるかつ、$\deg p = 1$ が成り立たないと仮定すると、素元の定義より $1 < \deg p$ が成り立つことになる。このとき、その多項式 f がその体 K の中にその多項式 f の根 a を必ずもち、さらに、その多項式 p は因数定理より多項式 $X - \overline{a}$ で割り切れる。このとき、商 q の次数は次式を満たすので、

$$0 < \deg p - 1 = \deg (X - \overline{a})\, q - 1 = \deg (X - \overline{a}) + \deg q - 1 = 1 + \deg q - 1 = \deg q$$

その商 q は可逆元でない。しかしながら、その多項式 $X - \overline{a}$ は単位元 $\overline{1}$ もその多項式 p も同伴でないことになり、したがって、これはその多項式 p が既約多項式であることに矛盾する。したがって、その多項式 p が既約多項式であるなら、$\deg p = 1$ が成り立つ。定理 3.4.20 より $\deg p = 1$ が成り立つなら、その多項式 p が既約多項式である。 □

定理 3.5.5. 代数的閉体 K の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、その体 K の元の族 $\{a_i\}_{i \in \Lambda_{\deg f}}$ が一意的に存在し次式が成り立つ。

$$f = f_{\text{l.c.}} \prod_{i \in \Lambda_{\deg f}} (X - \overline{a_i})$$

証明. 代数的閉体 K の多項式環 $K[X]$ が与えられたとき、$\forall f \in K[X]$ に対し、素元分解の基本定理よりその多項式環 $K[X]$ の monic である既約多項式の族 $\{p_i\}_{i\in\Lambda_n}$ が一意的に存在して次式が成り立つ。

$$f = f_{\text{l.c.}} \prod_{i\in\Lambda_n} p_i$$

このとき、定理 3.5.4 より $\forall i \in \Lambda_n$ に対し、$\deg p_i = 1$ が成り立つので、その体 K の元の族 $\{a_i\}_{i\in\Lambda_n}$ が一意的に存在し $p_i = X - \overline{a_i}$ が成り立つ。さらに、次のようになるので、

$$\begin{aligned}\deg f &= \deg f_{\text{l.c.}} \prod_{i\in\Lambda_n} p_i \\ &= \deg f_{\text{l.c.}} + \sum_{i\in\Lambda_n} \deg p_i \\ &= 0 + \sum_{i\in\Lambda_n} 1 = n\end{aligned}$$

よって、その体 K の元の族 $\{a_i\}_{i\in\Lambda_{\deg f}}$ が一意的に存在し次式が成り立つ。

$$f = f_{\text{l.c.}} \prod_{i\in\Lambda_{\deg f}} (X - \overline{a_i})$$

□

3.5.3 一意分解整域

定義 3.5.3. 整域 R が与えられたとき、$\forall a \in R$ に対し、その元 a が可逆元でないかつ、0 でないなら、その整域 R の素元の族 $\{p_i\}_{i\in\Lambda_n}$ が存在して $a = \prod_{i\in\Lambda_n} p_i$ が成り立ち、しかも、そのような族が $\{p_i\}_{i\in\Lambda_m}$、$\{q_i\}_{i\in\Lambda_n}$ と与えられたとき、$m = n$ が成り立ち、$\exists s : \Lambda_m \xrightarrow{\sim} \Lambda_n \forall i \in \Lambda_n$ に対し、$p_i A q_{s(i)}$ が成り立つようなその整域 R を一意分解整域という。このときも、そのような族 $\{p_i\}_{i\in\Lambda_n}$ を求めることをその元 a を素元分解するという。単項 ideal 整域はもちろん一意分解整域である。

定理 3.5.6. 一意分解整域 R の零元でない元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、この族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元が存在する。

証明. 一意分解整域 R の零元でない元の族 $\{a_i\}_{i\in\Lambda_n}$ が与えられたとき、この族のうち可逆元でないもの全体の族を $\{a_i\}_{i\in\Lambda}$ とおくと、$\forall i \in \Lambda$ に対し、その元 a_i が $a_i = \prod_{j\in\Lambda_{n_i}} p_{ij}$ と素元分解されるとすると、次式のように元 p がおかれれば、

$$p = \prod \bigcap_{i\in\Lambda} \{p_{ij}\}_{j\in\Lambda_{n_i}}$$

$p|a_i$ が成り立つので、その元 p はその族 $\{a_i\}_{i\in\Lambda}$ の公約元である。さらに、$\exists d \in R$ に対し、その元 d はその族 $\{a_i\}_{i\in\Lambda_n}$ の公約元で $p|d$ が成り立つかつ、$d|p$ が成り立たないと仮定すると、あるその一意分解整域 R の可逆元でない元 q が存在して $d = pq$ が成り立つことになる。その元 q もまたその族 $\{a_i\}_{i\in\Lambda_n}$ の公約元であることに注意すれば、その元 q が $q = \prod_{i\in\Lambda_m} q_i$ と素元分解されると、その族 $\{q_i\}_{i\in\Lambda_m}$ は、$\forall i \in \Lambda$ に対し、それらの族々 $\{p_{ij}\}_{j\in\Lambda_{n_i}}$ に含まれるので、その積集合 $\bigcap_{i\in\Lambda} \{p_{ij}\}_{j\in\Lambda_{n_i}}$ にも含まれることになる。しかしながら、これは素元分解の仕方が 2 通りあることになり素元分解の基本定理に矛盾する。ゆえに、その元 p はその族 $\{a_i\}_{i\in\Lambda}$ の最大公約元であり、また、その族 $\{a_i\}_{i\in\Lambda_n}$ の最大公約元でもある。 □

定理 3.5.7. 一意分解整域 R の素元 p が与えられたとき、$\forall a, b \in R$ に対し、$p|ab$ が成り立つなら、$p|a$ または $p|b$ が成り立つ。

証明. 一意分解整域 R の素元 p が与えられたとき、$\forall a, b \in R$ に対し、$a = \prod_{i \in \Lambda_m} p_i$、$b = \prod_{i \in \Lambda_n} q_i$ と素元分解されたとし、$p|a$ が成り立たないかつ、$p|b$ が成り立たないなら、$p \notin \{p_i\}_{i \in \Lambda_m}$ または $p \notin \{q_i\}_{i \in \Lambda_n}$ が成り立つことになり、したがって、$p \notin \{p_i\}_{i \in \Lambda_m} \cup \{q_i\}_{i \in \Lambda_n}$ が成り立つことになる。このとき、次式が成り立つので、

$$ab = \prod \{p_i\}_{i \in \Lambda_m} \cup \{q_i\}_{i \in \Lambda_n}$$

これにより、$p|ab$ が成り立たない。あとは、対偶律による。 □

3.5.4 原始多項式

定義 3.5.4. 一意分解整域 R 上の多項式環 $R[X]$ が与えられたとき、$\forall f \in R[X]$ に対し、$1 \leq \deg f$ が成り立つなら、その多項式 f の係数たちの族 $\{f(i)\}_{i \in \Lambda_{\deg f}}$ の最大公約元をその多項式 f の容量といい、その多項式 f の容量が単位元 1 と同伴であるとき、その多項式 f を原始多項式という。

定理 3.5.8. 一意分解整域 R 上の多項式環 $R[X]$ が与えられたとき、$\forall f \in R[X]$ に対し、$1 \leq \deg f$ のとき、その一意分解整域 R の元 d がその多項式 f の容量であるならそのときに限り、$\exists g \in R[X]$ に対し、その多項式 g は原始多項式で $f = \overline{d}g$ が成り立つ。

証明. 一意分解整域 R 上の多項式環 $R[X]$ が与えられたとき、$\forall f \in R[X]$ に対し、$1 \leq \deg f$ のとき、その一意分解整域 R の元 d がその多項式 f の容量であるかつ、$\forall g \in R[X]$ に対し、その多項式 g は原始多項式でないか、$f = \overline{d}g$ が成り立たないと仮定する。容量の定義より $f = \overline{d}g$ が成り立たないことはないので、その多項式 g は原始多項式でないことになる。このとき、その多項式 g の容量が単位元 1 と同伴でなくその容量の 1 つが可逆元でない元 e であることになる。このとき、その一意分解整域 R の元の族 $\{b_i\}_{i \in \Lambda_{\deg g}}$ が存在して次のようになるので、

$$\begin{aligned} g &= \sum_{i \in \Lambda_{\deg g}} \overline{g(i)} X^i \\ &= \sum_{i \in \Lambda_{\deg g}} \overline{eb_i} X^i \\ &= \overline{e} \sum_{i \in \Lambda_{\deg g}} \overline{b_i} X^i \end{aligned}$$

次式が成り立つ。

$$\begin{aligned} f &= \overline{d}g \\ &= \overline{de} \sum_{i \in \Lambda_{\deg g}} \overline{b_i} X^i \\ &= \overline{de} \sum_{i \in \Lambda_{\deg g}} \overline{b_i} X^i \end{aligned}$$

このとき、その元 de はその多項式 f の係数たちの族 $\{f(i)\}_{i \in \Lambda_{\deg f}}$ の公約元であり、さらに、$d|de$ が成り立つ。しかしながら、これはその元 d がその多項式 f の容量であることに矛盾する。したがって、$1 \leq \deg f$ の

とき、その一意分解整域 R の元 d がその多項式 f の容量であるなら、$\exists g \in R[X]$ に対し、その多項式 g は原始多項式で $f = \overline{d}g$ が成り立つ。

逆に、$\exists g \in R[X]$ に対し、その多項式 g は原始多項式で $f = \overline{d}g$ が成り立つかつ、その元 d がその多項式 f の容量でないと仮定すると、その多項式 f の係数たちの族 $\{f(i)\}_{i \in \Lambda_{\deg f}}$ の公約元で可逆元でない元 q を用いて $e = dq$ なるもの e が存在することになる。このとき、その元 q がその多項式 g の係数たちの族 $\{g(i)\}_{i \in \Lambda_{\deg g}}$ の公約元であり単位元 1 と同伴でないことになる。しかしながら、これはその多項式 g は原始多項式であることに矛盾する。したがって、$\exists g \in R[X]$ に対し、その多項式 g は原始多項式で $f = \overline{d}g$ が成り立つなら、その元 d がその多項式 f の容量であることになる。 □

定理 3.5.9. 一意分解整域 R 上の多項式環 $R[X]$ が与えられたとき、原始多項式たちの積も原始多項式である。

証明. 一意分解整域 R 上の多項式環 $R[X]$ が与えられたとき、ある原始多項式たち f、g が存在して多項式 fg は原始多項式でないと仮定すると、その多項式 fg の全ての係数たちを割り切るようなその一意分解整域 R の元が存在して、これが素元分解されると、ある素元 p がその多項式 fg の全ての係数たちを割り切る。一方で、それらの多項式たち f、g は原始多項式なので、素元の定義より素元は単位元 1 と同伴でなくその素元 p はそれらの多項式たち f、g の係数たちを割り切ることができない。このとき、$\exists r \in \Lambda_{\deg f} \cup \{0\}\, \exists s \in \Lambda_{\deg g} \cup \{0\}\, \forall i \in \Lambda_{r-1} \cup \{0\}\, \exists j \in \Lambda_{s-1} \cup \{0\}$ に対し、$p | f(i)$ かつ $p | g(i)$ が成り立つかつ、$\neg p | f(r)$ かつ $\neg p | g(s)$ が成り立つ。このとき、定理 3.1.8 より次式が成り立つ。

$$\begin{aligned}(fg)(r+s) &= \sum_{i+j=r+s} f(i)g(j) \\ &= \sum_{\substack{i+j=r+s \\ i<r}} f(i)g(j) + f(r)f(s) + \sum_{\substack{i+j=r+s \\ j<s}} f(i)g(j)\end{aligned}$$

このとき、元 $f(r)f(s)$ はその素元 p で割り切れないので、その係数 $(fg)(r+s)$ もその素元 p で割り切れないことになる。しかしながら、これはある素元 p がその多項式 fg の全ての係数たちを割り切ることに矛盾している。したがって、全ての原始多項式たち f、g の積 fg は原始多項式である。 □

定理 3.5.10. 一意分解整域 R 上の多項式環 $R[X]$、その一意分解整域 R の商の体 L が与えられたとき、次のことが成り立つ[*15]。

- $\forall f, g \in R[X]$ に対し、それらの多項式たち f、g が原始多項式で、$\exists \rho \in L$ に対し、$\overline{\rho} f = g$ が成り立つなら、その元 ρ はその一意分解整域 R の可逆元である。
- $\forall \varphi \in L[X]$ に対し、$\varphi \neq \overline{0}$ が成り立つなら、$\exists \rho \in L$ に対し、多項式 $\overline{\rho}\varphi$ はその多項式環 $R[X]$ の原始多項式である。

証明. 一意分解整域 R 上の多項式環 $R[X]$、その一意分解整域 R の商の体 L が与えられたとき、$\forall f, g \in R[X]$ に対し、それらの多項式たち f、g が原始多項式で、$\exists \rho = \frac{c}{d} \in L$ に対し、$\overline{\rho} f = g$ が成り立つなら、両辺に $\overline{d}$ をかけることで $\overline{c} f = \overline{d} g$ が成り立つ。このとき、両辺はその多項式環 $R[X]$ の多項式であり、それらの多項式たち f、g が原始多項式であるから、定理 3.5.8 より多項式たち $\overline{c}f$、$\overline{d}g$ の容量はそれぞれ c、d となる。このとき、$\exists q \in R$ に対し、その元 q は可逆元でなく $c = dq$ が成り立つとすれば、$d \neq 0$ が成り立つかつ、次のよ

[*15] この定理は簡単に示されると参考文献に書いてありましたが、どうなんでしょうかね…汗

うになることから、

$$\begin{aligned}\overline{c}f = \overline{dq}f = \overline{d}\overline{q}f = \overline{d}g &\Leftrightarrow \overline{d}\left(\overline{q}f - g\right) = 0\\ &\Rightarrow \overline{q}f = g\\ &\Rightarrow \overline{q}fg = g^2\end{aligned}$$

多項式 $\overline{q}fg$ は原始多項式でないことになるが、定理 3.5.9 より多項式 g^2 は原始多項式であることに矛盾する。したがって、それらの元々 c、d は互いに同伴であることになる。$c = \rho d$ が成り立つことに注意すれば、よって、その元 ρ はその一意分解整域 R の可逆元である。

$\forall\varphi \in L[X]$ に対し、$\varphi \neq \overline{0}$ が成り立つなら、その多項式 φ の各係数が $\varphi(i) = \frac{a_i}{b_i}$ とおかれると、多項式 $\overline{\prod_{i\in\Lambda_{\deg\varphi}} b_i}\varphi$ は多項式環 $R[X]$ の多項式となる。これの容量を d とおくと、定理 3.5.8 よりある原始多項式 g がその多項式環 $R[X]$ に存在して $\overline{\prod_{i\in\Lambda_{\deg\varphi}} b_i}\varphi = \overline{d}g$ が成り立つ。先ほどの議論と同様にして、それらの元々 $\prod_{i\in\Lambda_{\deg\varphi}} b_i$、$d$ は互いに同伴であることになる。したがって、その一意分解整域 R の可逆元 ρ が存在して $\prod_{i\in\Lambda_{\deg\varphi}} b_i = \rho d$ が成り立つことに注意すれば、よって、その多項式 $\overline{\rho}\varphi$ はその原始多項式 g そのものであるので、その多項式 $\overline{\rho}\varphi$ はその多項式環 $R[X]$ の原始多項式である。 □

定理 3.5.11. 一意分解整域 R 上の多項式環 $R[X]$、その一意分解整域 R の商の体 L が与えられたとき、$\forall f \in R[X]$ に対し、その多項式 f は原始多項式で $1 \leq \deg f$ が成り立つかつ、$1 \leq \deg\varphi_i$ なる多項式環 $L[X]$ の元の族 $\{\varphi_i\}_{i\in\Lambda_s}$ が存在して $f = \prod_{i\in\Lambda_s}\varphi_i$ が成り立つなら、その体 L の元の族 $\{\rho_i\}_{i\in\Lambda_s}$ が存在して多項式 $\overline{\rho_i}\varphi_i$ がその多項式環 $R[X]$ における原始多項式であり $f = \prod_{i\in\Lambda_s}\overline{\rho_i}\varphi_i$ が成り立つ。

証明. 一意分解整域 R 上の多項式環 $R[X]$、その一意分解整域 R の商の体 L が与えられたとき、$\forall f \in R[X]$ に対し、その多項式 f は原始多項式で $1 \leq \deg f$ が成り立つかつ、$1 \leq \deg\varphi_i$ なる多項式環 $L[X]$ の元の族 $\{\varphi_i\}_{i\in\Lambda_s}$ が存在して $f = \prod_{i\in\Lambda_s}\varphi_i$ が成り立つなら、定理 3.5.10 よりその体 L の元の族 $\{\rho'_i\}_{i\in\Lambda_s}$ が存在して多項式 $\overline{\rho'_i}\varphi_i$ がその多項式環 $R[X]$ における原始多項式であることができる。このとき、次のようになることから、

$$\prod_{i\in\Lambda_s}\overline{\rho'_i}\varphi_i = \prod_{i\in\Lambda_s}\overline{\rho'_i}\prod_{i\in\Lambda_s}\varphi_i = \overline{\prod_{i\in\Lambda_s}\rho'_i}f$$

定理 3.5.9 よりその多項式 $\overline{\prod_{i\in\Lambda_s}\rho'_i}f$ も原始多項式であり、定理 3.5.10 よりその元 $\overline{\prod_{i\in\Lambda_s}\rho'_i}$ も可逆元であることになる。ここで、$\frac{\rho'_i}{\overline{\prod_{i\in\Lambda_s}\rho'_i}} = \rho_i$ とおかれることで得られる体 L の元の族 $\{\rho_i\}_{i\in\Lambda_s}$ を用いた多項式 $\overline{\rho_i}\varphi_i$ もまた原始多項式である。よって、$f = \prod_{i\in\Lambda_s}\overline{\rho_i}\varphi_i$ が成り立つ。 □

定理 3.5.12. 一意分解整域 R 上の多項式環 $R[X]$ が与えられたとき、$\forall p \in R[X]$ に対し、その多項式 p が素元であるならそのときに限り、$\exists a \in R$ に対し、その元 a が素元で $p = \overline{a}$ が成り立つか、その一意分解整域 R の商の体 L 上の既約な定数でない原始多項式である。

定義 3.5.5. ここで、前者のような素元を定数素元、後者のような素元を固有の素元ということにする。

証明. 一意分解整域 R 上の多項式環 $R[X]$ が与えられたとき、$\forall p \in R[X]$ に対し、その多項式 p が素元であるなら、$0 \leq \deg p$ が成り立つ。$\deg p = 0$ のとき、$\exists a \in R$ に対し、$p = \overline{a}$ が成り立つことになる。ここで、その元 a は零元でないかつ、定理 3.3.6 よりその元 a は可逆元でもない。さらに、その多項式 p を割り切る多項式 q が存在するなら、定理 3.3.7 よりその多項式 q は $\deg q = 0$ が成り立つ、即ち、$\exists b \in R$ に対し、$q = \overline{b}$ が成り立つことになる。ここで、定理 3.3.6 と素元の定義より $b|a$ が成り立つなら、$bA1$ または bAa が成り立

つことになるので、その元 a は素元である。したがって、$\exists a \in R$ に対し、その元 a が素元で $p = \overline{a}$ が成り立つ。一方で、$1 \leq \deg p$ のとき、その多項式 p の容量 d が与えられたとき、$\overline{d}|p$ が成り立つので、$\deg \overline{d} = 0$ が成り立つかつ、その商 q は可逆元でもないので、$\overline{d}Ap$ が成り立たない。したがって、$\overline{d}A\overline{1}$ が成り立つので、定理 3.3.7 よりその元 d は可逆元である。定理 3.5.8 よりその多項式 p は原始多項式であることになる。さらに、その多項式 p はこれ以上素元分解できないので、定理 3.5.11 と対偶律よりその多項式 p はその体 L 上の既約な定数でない多項式であることになる。

逆に、$\exists a \in R$ に対し、その元 a が素元で $p = \overline{a}$ が成り立つか、その一意分解整域 R の商の体 L 上の既約な定数でない原始多項式であるとする。$\exists a \in R$ に対し、その元 a が素元で $p = \overline{a}$ が成り立つなら、定理 3.3.7 より直ちにその多項式 p は素元である。その一意分解整域 R の商の体 L 上の既約な定数でない原始多項式であるなら、その多項式 p はこれ以上素元分解できないので、係数すべてに適切に定数倍すれば、その多項式 p はその多項式環 $R[X]$ での既約多項式となる。 □

定理 3.5.13. 一意分解整域 R 上の多項式環 $R[X]$ も一意分解整域である。

証明. 一意分解整域 R 上の多項式環 $R[X]$ が整域となるのはすでに定理 3.3.8 でみてきた。$\forall f \in R[X]$ に対し、その多項式 f が零元でも可逆元でもないとする。$\deg f = 0$ のとき、$\exists a \in R$ に対し、$f = \overline{a}$ が成り立ち、定理 3.3.6 よりしたがって、その元 a が $a = \prod_{i \in \Lambda_n} p_i$ と素元分解されると、$f = \prod_{i \in \Lambda_n} \overline{p_i}$ が成り立つので、定理 3.5.12 よりこれでその多項式 f は定数素元に素元分解された。

$1 \leq \deg f$ のとき、その多項式 f の容量 d が与えられたとき、定理 3.5.8 より $\deg \widetilde{f} = \deg f$ なる原始多項式 $\widetilde{f}$ が存在して $f = \overline{d}\widetilde{f}$ が成り立つ。ここで、その容量 d が $d = \prod_{i \in \Lambda_n} p_i$ と素元分解されることができるかつ、定理 3.3.13 と素元分解の基本定理よりその一意分解整域 R の商の体 L 上の零元でない既約多項式の族 $\{\varphi_i\}_{i \in \Lambda_s}$ が存在して $\widetilde{f} = \prod_{i \in \Lambda_s} \varphi_i$ と素元分解されることができる。定理 3.5.11 よりその体 L の元の族 $\{\rho_i\}_{i \in \Lambda_s}$ が存在して多項式 $\overline{\rho_i}\varphi_i$ がその多項式環 $R[X]$ における原始多項式であり $\widetilde{f} = \prod_{i \in \Lambda_s} \overline{\rho_i}\varphi_i$ が成り立つことができる。このとき、それらの多項式たち $\overline{\rho_i}\varphi_i$ は原始多項式であるから、原始多項式の定義より $\rho_i \neq 0$ が成り立つ。このとき、それらの元々 $\overline{\rho_i}$ は可逆元であることになるので、それらの多項式たち $\overline{\rho_i}\varphi_i$ はそれぞれそれらの多項式たち φ_i と同伴であるから、それらの多項式たち $\overline{\rho_i}\varphi_i$ はその商の体 L 上で既約である。定理 3.5.12 よりしたがって、それらの多項式たち $\overline{\rho_i}\varphi_i$ は固有な素元であることになる。以上より、次式が成り立つので、

$$\begin{aligned} f &= \overline{d}\widetilde{f} \\ &= \overline{\prod_{i \in \Lambda_n} p_i} \prod_{i \in \Lambda_s} \varphi_i \\ &= \prod_{i \in \Lambda_n} \overline{p_i} \prod_{i \in \Lambda_s} \overline{\rho_i}\varphi_i \end{aligned}$$

その多項式 f はその多項式環 $R[X]$ 上で素元分解された。

$\forall f \in R[X]$ に対し、その多項式 f が零元でも可逆元でもないとするとき、定数素元たちの族々 $\{p_i\}_{i \in \Lambda_m}$、$\{q_i\}_{i \in \Lambda_n}$ と固有な素元たちの族々 $\{g_i\}_{i \in \Lambda_r}$、$\{h_i\}_{i \in \Lambda_s}$ が存在して次式が成り立つなら、

$$\begin{aligned} f &= \prod_{i \in \Lambda_m} \overline{p_i} \prod_{i \in \Lambda_r} g_i \\ &= \prod_{i \in \Lambda_n} \overline{q_i} \prod_{i \in \Lambda_s} h_i \end{aligned}$$

定理 3.5.9 よりそれらの多項式たち $\prod_{i\in\Lambda_r} g_i$、$\prod_{i\in\Lambda_s} h_i$ は原始多項式であり、定理 3.3.6 と定理 3.5.8 よりそれらの元々 $\prod_{i\in\Lambda_m} p_i$、$\prod_{i\in\Lambda_n} q_i$ はその多項式 f の容量なので、これらは互いに同伴である。したがって、その一意分解整域 R の可逆元 ε を用いて次式が成り立つことになる。

$$\prod_{i\in\Lambda_m} p_i = \varepsilon \prod_{i\in\Lambda_n} q_i$$

このとき、素元分解の基本定理より $m = n$ が成り立ち、$\exists\sigma : \Lambda_n \xrightarrow{\sim} \Lambda_m \forall i \in \Lambda_n$ に対し、$p_i A q_{\sigma(i)}$ が成り立つ。さらに、$\prod_{i\in\Lambda_m} \overline{q_i} \neq \overline{0}$ が成り立つことによりしたがって、次のようになる。

$$\prod_{i\in\Lambda_m} \overline{p_i} \prod_{i\in\Lambda_r} g_i = \overline{\varepsilon} \prod_{i\in\Lambda_m} \overline{q_i} \prod_{i\in\Lambda_r} g_i = \prod_{i\in\Lambda_n} \overline{q_i} \prod_{i\in\Lambda_s} h_i \Leftrightarrow \prod_{i\in\Lambda_m} \overline{q_i} \left(\overline{\varepsilon} \prod_{i\in\Lambda_r} g_i - \prod_{i\in\Lambda_s} h_i \right) = \overline{0}$$
$$\Rightarrow \overline{\varepsilon} \prod_{i\in\Lambda_r} g_i = \prod_{i\in\Lambda_s} h_i$$

このとき、素元分解の基本定理より $r = s$ が成り立ち、$\exists\tau : \Lambda_s \xrightarrow{\sim} \Lambda_r \forall i \in \Lambda_r$ に対し、$g_i A h_{\tau(i)}$ が成り立つ。したがって、定理 3.3.11 より $\exists\lambda_i \in K$ に対し、$\overline{\lambda_i} g_i = h_{\tau(i)}$ が成り立つことになり、それらの多項式たち g_i、$h_{\tau(i)}$ は原始多項式であるから、定理 3.5.10 よりその元 λ_i はその一意分解整域 R の可逆元である。このとき、その多項式 $\overline{\lambda_i}$ はその多項式環 $R[X]$ の可逆元であるので、それらの多項式たち g_i、$h_{\tau(i)}$ はその多項式環 $R[X]$ において同伴である。

以上より、その多項式環 $R[X]$ も一意分解整域でもある。 □

定理 3.5.14 (Eisenstein の規準)**.** 一意分解整域 R とこれの商の体 L が与えられたとき、その一意分解整域 R 上の多項式環 $R[X]$ の $1 \leq \deg f$ なる任意の多項式 f に対し、あるその一意分解整域 R の素元 p が存在して、次のことが成り立つなら、

- $p | f_{\text{l.c.}}$ が成り立たない。
- $\forall i \in \Lambda_{\deg f - 1} \cup \{0\}$ に対し、$p | f(i)$ が成り立つ。
- $p^2 | f(0)$ が成り立たない。

その多項式 f はその商の体 L 上で既約である。この定理を Eisenstein の規準という。

証明. 一意分解整域 R とこれの商の体 L が与えられたとき、その一意分解整域 R 上の多項式環 $R[X]$ の $1 \leq \deg f$ なる任意の多項式 f に対し、その多項式 f はその商の体 L 上で可約であるなら、定理 3.4.19 より $\exists g, h \in P[X]$ に対し、$f = gh$ かつ $1 \leq \deg g$ かつ $1 \leq \deg h$ が成り立つ。ここで、あるその一意分解整域 R の素元 p が存在して、次のことが成り立つと仮定すると、

- $p | f_{\text{l.c.}}$ が成り立たない。
- $\forall i \in \Lambda_{\deg f - 1} \cup \{0\}$ に対し、$p | f(i)$ が成り立つ。
- $p^2 | f(0)$ が成り立たない。

$f(0) = g(0)h(0)$ が成り立つので、$p | g(0)$ または $p | h(0)$ が成り立つことになり、$p^2 | f(0)$ が成り立たないので、$p | g(0)$ かつ $p | h(0)$ が成り立つことはない。ここで、$p | h(0)$ が成り立たないと仮定しても一般性は失われないので、そうすると、その多項式 g の全ての係数たちがその素元 p で割り切れると仮定すると、$f_{\text{l.c.}} = g_{\text{l.c.}} h_{\text{l.c.}}$ が成り立つことにより $p | f_{\text{l.c.}}$ が成り立つことになるが、これは仮定に矛盾する。したがって、その多項式 g のある係数が存在してこれがその素元 p で割り切れないことになる。このとき、$\exists r \in \Lambda_{\deg g} \forall i \in \Lambda_{\deg g - 1} \cup \{0\}$

に対し、$p|g(i)$ が成り立つかつ、$p|g(r)$ が成り立たなく、このとき、$p|g(0)$ が成り立つかつ、$\deg g < \deg f$ が成り立つことにより $0 < r < \deg f$ が成り立つ。このとき、定理 3.1.8 より次のようになり、

$$\begin{aligned} f(r) &= \sum_{i+j=r} g(i)h(j) \\ &= \sum_{\substack{i+j=r \\ i<r}} g(i)h(j) + g(r)h(0) \end{aligned}$$

したがって、$p|g(r)$ が成り立たないかつ、$p|h(0)$ が成り立たないので、$p|f(r)$ も成り立たないことになるが、これは仮定の、$\forall i \in \Lambda_{\deg f-1} \cup \{0\}$ に対し、$p|f(i)$ が成り立つことに矛盾している。したがって、その一意分解整域 R の全ての素元 p に対し、次のことのうちいづれかが成り立たない。

- $p|f_{\text{l.c.}}$ が成り立たない。
- $\forall i \in \Lambda_{\deg f-1} \cup \{0\}$ に対し、$p|f(i)$ が成り立つ。
- $p^2|f(0)$ が成り立たない。

あとは、対偶律による。 □

参考文献

[1] 松坂和夫, 代数系入門, 岩波書店, 1976. 新装版第 2 刷 p156-166 ISBN978-4-00-029873-5