群・環・体 速習講座

@yfbk271_chigu

2021 年 11 月 3 日

目次

はじめに

速習と書いておきながら，長々と書いてしまった.

1　群

1.1　群の定義

最小限の知識のみ記しておく.

Definition 1.1.1.

G を空集合でない集合とする. G 上の演算が定義されていて次の性質を満たす時, G を群という.
(1) 単位元と呼ばれる元 $e \in G$ が存在し，すべての $a \in G$ に対し $ae = ea = a$ となる.
(2) すべての $a \in G$ に対し $b \in G$ が存在し，$ab = ba = e$ となる．この元 b は a の逆元とよばれ，a^{-1} とかく.
(3) すべての $a, b, c \in G$ に対し，$(ab)c = a(bc)$ が成り立つ.
これらの演算は所謂，掛け算とは異なった概念であることを認識しておいてほしい.

交換法則も成り立つとき，G は可換であるといい，可換群，アーベル群，加群という．ただし，後に，A–加群と呼ばれる概念が登場するため，加群という言葉は以下において使わないことにする.

G が群であるとき，その元の個数を $|G|$ とかき，これを G の位数とよぶ.

Probrem 1.1.2.

x, y, z が群 G の元で $y^{-1}zxy^2z = yz^2$であるとき，x を y, z であらわせ.

$\mathcal{A}$. $y^{-1}zxy^2z = yz^2 \Leftrightarrow xy^2z = z^{-1}y^2z^2 \Leftrightarrow x = z^{-1}y^2zy^{-2}$
定義通りの演算を両辺の式に外側から順番に施す.

単位元の一意性，簡約法則についてはここでは省く.

1.2　置換群

X を集合とするとき，X から X への全単射写像 $\sigma : X \to X$ のことを X の置換という．σ, τ を X の 置換とするとき，その積，$\sigma\tau$ を写像としての合成 $\sigma \circ \tau$ と定義する．これは演算をするとき，$\sigma(\tau)$ のように考えるとわかりやすい.

Definition 1.2.1.

X の置換全体からなる群のことを X の置換群という．$X_n = \{1, 2, \cdots, n\}$ とするとき，X_n の置換のことを n 次の置換という．n 次の置換全体よりなる群のことを $\mathfrak{S}_n$ であらわし，$\mathfrak{S}_n$ を n 次対称群という．これは位数 $n!$ の有限群である.

Example 1.2.2.

$G = \mathfrak{S}_n$ とおく，このとき，

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \in G$$

は $1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 4,\ 4 \mapsto 2$ となる元である．

$1 \leq i_1, i_2, \cdots, i_m \leq n$ を全て異なる整数とするとき，

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_m \mapsto i_1$$

と写し，他の $1 \leq j \leq n$ は変えない置換を $(i_1 \cdots i_m)$ と表し，長さ m の巡回置換という．例 1 の置換を巡回置換を用いて表すと，(1342) である．$1 \leq i < j \leq n$ のとき，$l \neq i, j$ なら $\sigma(l) = l$ で $\sigma(i) = j, \sigma(j) = i$ であるとき，σ は置換である．このような置換を i, j の互換といい (ij) で表す．
例 1.2.2 の置換を互換を用いて表すと，$(12)(14)(13)$ である．このことから想像できるように，一般に巡回置換は互換の積で表せる．

1.3 元の位数

Definition 1.3.1.

G を群，$g \in G$ とする．
(1) $g^n = 1$ となる $n > 0$ があれば，そのような n の最小値を g の位数という．
(2) $g^n = 1$ となる $n > 0$ がなければ，g の位数は ∞ という．

Proposition 1.3.2.

G を群，$g \in G$ を位数が有限である元とする．このとき，$m \in \mathbb{Z}$ に対して以下の二つは同値．
(1) $g^m = 1$.
(2) m は n の倍数．

Proof. $k \in \mathbb{Z}$, $m = kn$ なら，$g^m = (g^n)^m = 1$ である．
逆に $g^m = 1$ とする．m が n の倍数でないと仮定し，$m = qn + r$ と割り算すると，$0 < r < n$ である．$1 = g^m = (g^n)^q g^r$ となるんので，n が g の位数であることに反する．よって m は n の倍数． □

1.4 部分群

Definition 1.4.1.

G を群とする．G の空でない部分集合 H が G の演算で群になる時，H を G の部分群という．

Proposition 1.4.2.

群 G の部分集合 H が G の部分群になるための必要十分条件は，$\forall x, y \in H$ に対して，$xy^{-1} \in H$ が成り立つこと．

Proof. 証明は群定義どおりに手を動かせば簡単に示せるので割愛． □

Definition 1.4.3.

部分集合 $S \subset G$ に対し，S の元，あるいはその弦の逆元の有限個の積により，なる G の部分集合を $\langle S \rangle$ とする．つまり，$\langle S \rangle$ は $x_1, \cdots x_t \in S$ により $x_1^{\pm 1} \cdots x_t^{\pm 1}$ という形をした元全体の集合である．

Proposition 1.4.4.

$\langle S \rangle$ は G の部分群である．

Proof. $1 \in \langle S \rangle$ $x_1, \cdots x_n, y_1, \cdots y_n \in S$ なら，

$$\left(x_1^{\pm 1} \cdots x_n^{\pm 1}\right)\left(y_1^{\pm 1} \cdots y_n^{\pm 1}\right) = x_1^{\pm 1} \cdots x_n^{\pm 1} y_1^{\pm 1} \cdots y_n^{\pm 1} \in \langle S \rangle$$

$x_1^{\pm 1} \cdots x_n^{\pm 1}$の逆元 $x_1^{\mp 1} \cdots x_n^{\mp 1} \in \langle S \rangle$ である．したがって，題意は示された． □

$\langle S \rangle$ を S で生成された部分群といい，S を $\langle S \rangle$ の生成系，S の元を生成元という．G が一つの元で生成される時，G を巡回群という．群の部分群で巡回群であるものは巡回部分群という．

Example 1.4.5.

$\mathbb{Z}$ は $\langle 1 \rangle$ で生成される位数 ∞ の巡回無限群である．また，$n\mathbb{Z}$ は n を生成元とする $\mathbb{Z}$ の位数 ∞ の巡回無限部分群である．

Proposition 1.4.6.

g が群 G の位数を $n > 0$ とする元であるとき，$\langle g \rangle$ の位数は n である．

Proof. 自明． □

1.5 準同型

Definition 1.5.1: 準同型・同型

G_1, G_2 を群，$\phi : G_1 \to G_2$ を写像とする．
(1) $\phi(xy) = \phi(x)\phi(y)$ が $\forall x, y \in G_1$ に対して成り立つ時，ϕ を準同型という．
(2) ϕ が準同型で逆写像を持ち，逆写像も準同型であるとき，ϕ を同型といい $G_1 \cong G_2$ と表す．
(3) ϕ が準同型の時，$\mathrm{Ker}(\phi) = \{x \in G_1 \mid \phi(x) = 1_{G_2}\}$ を ϕ の核という．
(4) ϕ が準同型の時，$\mathrm{Im}(\phi) = \{\phi(x) \mid x \in G_1\}$ を ϕ の像という．

Proposition 1.5.2.

全単写写像 $\phi : G_1 \to G_2$ が群の準同型なら，同型である．

Proof. ϕ の逆写像を ψ とおく．$x, y \in G_2$ とすると ϕ は準同型なので，

$$\phi(\psi(x)\psi(y)) = \phi(\psi(x))\phi(\phi(y)) = xy = \phi(\psi(xy))$$

となり，ϕ は単射なので，ψ は準同型である． □

Proposition 1.5.3.

$\phi : G_1 \to G_2$ を群の準同型とする時，次が成り立つ．

(1) $\phi(1_{G_1}) = 1_{G_1}$

(2) $\forall x \in G_1, \phi(x^{-1}) = \phi(x)^{-1}$

(3) $\mathrm{Ker}(\phi), \mathrm{Im}(\phi)$ はそれぞれ G_1, G_2 の部分群．

Proof.

(1) $\phi(1_{G_1}) = \phi(1_{G_1} \cdot 1_{G_1}) = \phi(1_{G_1})\phi(1_{G_1})$ より，$\phi(1_{G_1})$ がわかる．

(2) $\phi(1_{G_1}) = \phi(x \cdot x^{-1}) = \phi(x)\phi(x^{-1})$ より，$\phi(1_{G_1}) = \phi(x)\phi(x^{-1})$ の両辺に $\phi(x)^{-1}$ を右側から作用させることで $\phi(x^{-1}) = \phi(x)^{-1}$ がわかる．

(3) $x, y \in \mathrm{Ker}(\phi)$ とすると，$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = 1_{G_2} \cdot 1_{G_2} = 1_{G_2}$ である．よって，1.4.2 から，G_1 の部分群である．

また，$1_{G_2} = \phi(1_{G_1}) \in \mathrm{Im}(\phi), \forall x, y \in G_1$ に対し，$\phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} \in \mathrm{Im}(\phi)$ である．よって，ϕ は G_2 の部分群である． □

Example 1.5.4.

群 $G \ni x, \mathbb{Z} \to G, \phi(x) := n^x$ とすると，ϕは準同型．また，d を x の有限位数とすると，$\mathrm{Im}(\phi) = \langle x \rangle$

Proposition 1.5.5.

(1) 群の準同型写像の合成は準同型写像．

(2) 群の同型写像の合成は同型写像であり，同型写像の逆写像も同型写像．

Proposition 1.5.6.

$\phi : G_1 \to G_2$が準同型である時，次の二つは同値．

(1) ϕは単射．

(2) $\mathrm{Ker}(\phi) = \{1_{G_1}\}$

Proof. (1) → (2) : ϕが単射であるとすると，$1_{G_1} \in \mathrm{Ker}$ は明らか．$\mathrm{Ker}(\phi)$ なら$\phi(g) = 1_{G_2} = \phi(1_{G_1})$ であるが ϕは単射なので，$g = 1_{G_1}$.よって (2) は成り立つ．

(2) → (1) : $\mathrm{Ker}(\phi) = \{1_{G_1}\}$ とする．$g, h \in G_1, \phi(g) = \phi(h)$ なら，$\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = 1_{G_2}$.よって，$gh^{-1} \in \mathrm{Ker}(\phi) = \{1_{G_1}\}$ であり，$g = h$ なので，ϕは単射. □

1.6 同値と剰余

Definition 1.6.1.

集合 S 上の関係 $\sim$ が $\forall a, b, c \in S$ に対して次の条件を満たす時，同値関係という．

(1) $a \sim a$

(2) $a \sim b$ なら $b \sim a$

(3) $a \sim b, b \sim c$ なら $a \sim c$

Example 1.6.2.

$\exists n \in \mathbb{Z}_{>}, x, y \in \mathbb{Z}, n \mid x - y$ のとき，$x \equiv y \bmod n$ と定義すると，このとき同値関係が成り立つことは容易にわかる．

ちなみに，$\exists n \in \mathbb{Z}_{>}, x \in n\mathbb{Z}$ と定義した時，$x^{-1} \notin \mathbb{Z}$ と考えてしまう人がいるが，このとき x^{-1}は $-x$ と同値であり，逆元は存在する．これは $n\mathbb{Z}$ が加法に関して群をなしているからである．

Definition 1.6.3.

$\sim$ を集合 S 上の同値関係とする．$x \in S$ に対し，

$$C(x) = \{y \in S \mid y \sim x\}$$

を x の同値関係という．

Proposition 1.6.4.

$\sim$ を集合 S 上の同値関係，$C(x)$ を $x \in S$ の同値類とする．

(1) $\forall y, z \in C(x)$ に対し，$y \sim z$ である．

(2) $y \in C(x)$ なら $C(x) = C(y)$

(3) $x, y \in S, C(x) \cap C(y) \neq \varnothing$ なら $C(x) = C(y)$

Proof. (1) 自明.

(2) $y \in C(x)$ とする．$x \in C(x)$ なら，$x \sim y$ より，$C(x) \subset C(y)$．$x \in C(y)$ なので同様に，$C(y) \subset C(x)$．よって，$C(x) = C(y)$.

(3) $x, y \in S, x \in C(x) \cap C(y)$ なら (2) より，$C(x) = C(z), C(y) = C(z)$ であるから，$C(x) = C(y)$. □

これらのことから，$S = \coprod_{x \in S} C(x)$ も直ちにわかる．

Definition 1.6.5.

H を群 G の部分群, $x \in G$ とする.
H の左剰余類を G の部分集合である,

$$xH = \{xh \mid h \in H\}$$

と定義する．同様にして右剰余類は $Hx = \{hx \mid h \in H\}$ と定義される．このとき，x は代表元と言われる.

Example 1.6.6.

$G = \mathfrak{S}_3, H = \langle (1\ 2) \rangle$ とすると，H の右剰余類は

$$H = \{1, (1\ 2)\}, H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}, H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 3)\}$$

左剰余類は

$$H = \{1, (1\ 2)\}, (1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}, (1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\}$$

例からわかるように，H の右剰余類と左剰余類は一致しない場合がある.
群 $G \ni x$,G の部分群 H の右剰余類 Hx の集合を $H\backslash G$，同様に xH の集合を G/H と表す.

1.7 ラグランジュの定理

Definition 1.7.1.

~ を集合 S 上の同値関係とする.
(1) S の部分集合で $C(x)(x \in S)$ と表せるもの全体の集合を $S/\sim$ と表す.
(2) S の部分集合 R が $S/\sim$ の同値類の代表元を一つずつのみ含むとき，R を ~ の完全代表系という.

Example 1.7.2.

$\mathbb{Z}/5\mathbb{Z} = \{0 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 1 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$ である．このとき，完全代表系の一つは $\{0, 1, 2, 3, 4, \}$ である．また，$\{10, 11, 12, 13, 14\}$ も完全代表系の一つである.

Proposition 1.7.3.

H が群 G の部分群であるとすると，次の二つが成り立つ.
(1) $|G/H| = |H\backslash G|$
(2) $\forall g \in G, |gH| = |Hg| = |H|$

例 1.6.6 を見ると明らかだろう.

Definition 1.7.4.

$G/H, H\backslash G$ の元の個数を $(G : H)$ と表し，これを H の G における指数という.

Theorem 1.7.5: ラグランジュの定理

$|G| = (G : H)|H|$ が成り立つ.

Proof. G/H の完全代表系 $\{\varepsilon_i\}$ をとると，$G = \coprod_i \varepsilon_i H$ が成り立つ．$\forall i$ に対し $|\varepsilon H| = |H|$ より，定理が従う． □

corollary 1.7.6.

G を有限群とするとき，次の (1), (2) が成り立つ.
(1) H が G の部分群なら，$|H|$ は $|G|$ の約数.
(2) $g \in G$ の位数は $|G|$ の約数.

Probrem 1.7.7: Fermat の小定理

$p \in \mathbb{F}, p \nmid x \in \mathbb{Z}$ なら $x^{p-1} \equiv 1 \bmod p$ であることを証明せよ.

Probrem 1.7.8.

$p \in \mathbb{F}, n \in \mathbb{Z}_{>}$なら，$|(\mathbb{Z}/p^n\mathbb{Z})^\times| = (p-1)p^{n-1}$ であることを証明せよ. [a]

[a] $(\mathbb{Z}/p^n\mathbb{Z})^\times$とは $\mathbb{Z}/p^n\mathbb{Z}$ が乗法に関して群を成しているということである.

1.8 正規部分群

Definition 1.8.1.

H を群 G の部分群とする．$\forall g \in G, h \in H$ に対し $ghg^{-1} \in H$ となる時，H を G の正規部分群といい，$H \triangleleft G$ とあらわす.

Example 1.8.2.

G が可換群で H が任意の部分群の時 $gh^{-1} = h \in H$ なので，H は正規部分群である．$2\mathbb{Z}.3\mathbb{Z} \subset \mathbb{Z}$ などは正規部分群.

Proposition 1.8.3.

G_1, G_2が群で$\phi : G_1 \to G_2$が準同型なら $\mathrm{Ker}(\phi)$ は G_1の正規部分群である.

Proof. $g \in G_1, h \in \mathrm{Ker}(\phi)$ とすると，

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = 1_{G_2}$$

であり，$ghg^{-1} \in \mathrm{Ker}(\phi)$ のため, $\mathrm{Ker}(\phi) \triangleleft G_1$である． □

Lemma 1.8.4.

H が G の部分群なら，次の二つの主張は同値である．
(1) H は G の正規部分群である．
(2) $\forall g \in G$ に対し，$gH = Hg$ である．

Proof. (1) $\Rightarrow$ (2) $h \in H$ なら，$h' = ghg^{-1} \in H$ である．よって，$gh = h'g \in Hg$ である．これは，$\forall h$ に対して成り立つため，$gH \subset Hg$ である．同様に，$Hg \subset gH$ であるため，$gH = Hg$ が成り立つ．
(2) $\Rightarrow$ (1) $g \in G, h \in H$ なら，$gn \in gH = Hg$ より，$\exists h' \in H, gh = h'g$ が成り立つ．よって，$ghg^{-1} = h' \in H$ であるため，H は正規部分群である． □

この補題から正規部分群とは左剰余群と右剰余群が一致するということを示している．

Proposition 1.8.5.

H を群 G の正規部分群，x, y を G の代表元とすると，

$$(xH)(yH) = xyH$$

が成り立つ．

Proof. $h, h' \in H$ とすると，$xhyh' \in (xH)(yH)$ である．$xhyh' = xy(y^{-1}hy)h$ より，$\exists h'' \in H$ に対して $y^{-1}hy = h''$が成り立つ．よって，$xhyh' = xyh''h \in xyH$ である． □

Proposition 1.8.6.

N を G の正規部分群とした時，G/N は命題 1.8.5 の演算により群をなす．

Proof. N が単位元となるのは明らか．先の命題より結合法則が成り立つのは明らか．逆元の存在は明らか．
□

Proposition 1.8.7.

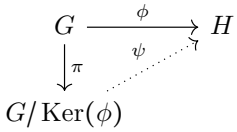
H を群 G の正規部分群とすると，$\phi : G \to G/H$ は群の全写準同型であり，$\mathrm{Ker}(\phi) = H$ である．

Proof. $x, y \in G, \phi(x) \coloneqq xH$ とすると，$\phi(xy) = \phi(x)\phi(y) = xHyH = xyH$ であり，この写像は全写である．また，G/H の単位元は H であるから，$g \in \mathrm{Ker}(\phi), \phi(g) = gN = N$ より，$\mathrm{Ker}(\phi) = N$ であることは明らか．
□

1.9 準同型定理

Theorem 1.9.1: 準同型定理 (第一同型定理)

$\phi : G \to H$ を群の準同型とする．$\pi : G \to G/\mathrm{Ker}(\phi)$ を準同型とするとき，下図が可換図式[a]となるような準同型 $\psi : G/\mathrm{Ker}(\phi) \to H$ がただ一つ存在し，ψ は $G/\mathrm{Ker}(\phi)$ から $\mathrm{Im}(\phi)$ への同型となる．



[a] 等しい集合間の異なる経路の写像の合成が等しくなる時，図は可換図式であるという．

Proof. $x, y \in G, \mathrm{Ker}(\phi) = K$ とする．命題 1.8.3 より，$\mathrm{Ker}(\phi)$ は G の正規部分群である．ψ が準同型であることを示す．

Lemma 1.9.2.

$xK = yK \Leftrightarrow y^{-1}x \in K$ である．
$(\Rightarrow)$ $xK = yK \Leftrightarrow K = y^{-1}xK$．$K$ は群であるから，$h \in K$ に対して $,\exists h' \in K$ であり，$h = y^{-1}xh'$ が成り立つ．
$(\Leftarrow)$ $\phi(y^{-1}x) = \phi(y^{-1})\phi(x) = \phi(y)^{-1}\phi(x) = 1_H$．よって，$\phi(y)^{-1}\phi(x) = 1_H \Leftrightarrow \phi(x) = \phi(y)$.

補題より，$\psi(xK) = \phi(x)$ という写像を考える．これは，$\psi : G/K \to H$ の対応が定まり，ψ は単写であることがわかる．また，K は正規部分群であるから，

$$\psi(xKyK) = \psi(xyK) = \phi(xy) = \phi(x)\phi(y) = \psi(xK)\psi(yK)$$

よって，ψ は準同型である．写像 π は命題 1.8.7 から明らか．$\psi(xK) = \phi(x)$ が全写であることは明らか．よって全単写であり，$G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$ である． □

Example 1.9.3.

$G := \langle x \rangle, |G| = n$．$\phi : \mathbb{Z} \ni m \mapsto x^m \in G$ とする．これが準同型なのは明らか．x は生成元なので全写であることは明らか．$\mathrm{Ker}(\phi) = n\mathbb{Z}$ なので第一同型定理より，$\mathbb{Z}/n\mathbb{Z} \cong G$ である．

Theorem 1.9.4: 第二同型定理

H, N を群 G の部分群，$N \triangleleft G$ と定める．この時，次の (1), (2) が成り立つ．
(1) HN は G の部分群であり，$HN = NH$ である．
(2) $H \cap N \triangleleft H, HN/N \cong H/H \cap N$.

Proof. (1) $h, h' \in H, n, n' \in N$ とする．$(hn)(h'n')^{-1} \in hNh'^{-1}N = hh'^{-1}NN \subset HN$．また，補題 1.9.2 より，$HN = NH$ は明らか.

(2) $x \in H$ とする．$H \to HN/N$ となる写像 $\phi(x) = xN$ は全写準同型である．$\mathrm{Ker}(\phi) = H \cap N$ なので同様に，$H \cap N \lhd H$ であり，第一同型定理より，$HN/N \cong H/H \cap N$ である． □

Theorem 1.9.5: 第三同型定理

G を群，$G \rhd N \subset N'$ とするとき，次の (1), (2) が成り立つ．
(1) 準同型写像 $\phi : G/N \to G/N'$ で $\phi(xN) = xN'$ となるものが存在する．
(2) $(G/N)(N'/N) \cong G/N'$

Proof. 第一同型定理より自明． □

2　環と体

2.1　環と多項式

Definition 2.1.1.

集合 A に二つの演算，加法と乗法が定義され，次の性質を満たす時，A を環という．

(1) A は加法に関してアーベル群となる．

(2) 結合法則が成り立つ．

(3) 分配法則が成り立つ．

(4) 乗法に関して単位元が 1 である．

以下，明示がない限り，環は可換環として扱う．

Definition 2.1.2.

R が環である時，R に係数を持つ多項式 $f(x)$，すなわち R 上の多項式を，$\forall i, c_i \in R$ であり，$i > n$ に対して $c_i = 0$ が成り立つ列

$$f(x) = (c_0, c_1, \ldots, c_n, 0, 0, \ldots)$$

と定義する．

$g(x) = (d_0, d_1, \ldots)$ を R 上の多項式とすると，$f(x) = g(x)$ となる必要十分条件は，任意の i に対して $c_i = d_i$ が成り立つことである．また，R 上の多項式の集合を $R[x]$ と表す．零多項式を $(0, 0, \ldots)$ と定義し，加法と乗法を次のように定義する

$$(c_0, c_1, \ldots) + (d_0, d_1, \ldots) = (c_0 + d_0, c_1 + d_1, \ldots)$$

$$(c_0, c_1, \ldots)(d_0, d_1, \ldots) = \left(\sum_{i+j=0} c_i d_j, \sum_{i+j=1} c_i d_j, \ldots \right)$$

このように定義した時，$R[x]$ は環となる．$R[x]$ を R 上の多項式環という．

$f(x) = c_0 + c_1 x + c2x^2 + \cdots + c_n x^n$ とし，$f(x)$ が零多項式でない時，c_n を最高次係数，n を $f(x)$ の次数といい $\partial(f)$ で表す．また，最高次係数が 1 でるとき，$f(x)$ をモニックという．

Definition 2.1.3.

環 R の部分集合 S が 1 を含み加法と乗法に関して閉じている時，S を R の部分環という．

Probrem 2.1.4.

R を環とし，$f(x) \in R[x]$ が $f(x) = \sum r_i x^i$ の形をしている時，その微分を

$$f'(x) = r_1 + 2r_2 x + \cdots n r_n x^{n-1}$$

で定義する．このとき次を証明せよ．

$$[f(x)+g(x)]' = f'(x)+g'(x)$$
$$[f(x)g(X)]' = f'(x)g(x)+f(x)g'(x)$$

2.2 整域と体

Definition 2.2.1.

環 R は，R の 0 でない任意の二つの元の積が 0 にならない時，整域であるという．

Theorem 2.2.2.

環 R が整域であるための必要十分条件は，簡約法則が成り立つことである．

Proof. R が整域で $r \neq 0, ra = rb$ が成り立つと仮定する．このとき，$r(a-b) = 0$ だが，R は整域なので $a-b = 0$ すなわち $a = b$ である．
逆に，R において簡約法則が成り立つと仮定する．$ra = 0$ となる 0 でない $r, a \in R$ が存在したとすると，$ra = 0 = r0$．よって $a = 0$ となり矛盾． □

Theorem 2.2.3.

$\mathbb{Z}$ が整域であるための必要十分条件は，n が素数であることである．

Proof. n が合成数である時，$1 < a < n, 1 < b < n$ で $n = ab$ が成り立つ $a, b \in \mathbb{Z}$ が存在する．このとき，$[a][b] = [ab] = [n] = 0$ であるが，$[a], [b] \neq 0$ なので，$\mathbb{Z}_n$ 整域ではない．
逆に，p を素数とする．$[a][b] = 0$ ならば，$ab \equiv 0 \bmod p$ なので，$p \mid ab$．よって，$p \mid a, p \mod b$ すなわち $a = [0]$ または $b = [0]$． □

Definition 2.2.4.

R を環とする.$a \in R$ に対して，$ab = 1$ となる $b \in R$ が存在するとき，a を単元という．

Definition 2.2.5.

環 R に対して 0 でない任意の $r \in R$ が単元である時，R を体という．

Theorem 2.2.6.

p が素数であれば $\mathbb{Z}_p$ は体となる．

Proof. $[a] \in \mathbb{Z}$ とする．$[a] \neq 0$ であれば，$p \nmid a$ である．$\gcd(a, p) = 1$ を示す．p は素数なので，$1, p$ のみが gcd の候補である．$p \nmid a$ なので $\gcd(a, p) = 1$ となり，1 は a と p の線型結合となる．よって $\exists s \in \mathbb{Z}_p$ となり，$[1] = [sa] = [s][a]$ なので，$[a]$ の乗法に関する逆元は $[s]$ であり $\mathbb{Z}_p$ は体となる． □

Theorem 2.2.7.

任意の整域 R に対して，R を部分環として含み，$a, b \in R, b \neq 0, \forall q \in \mathrm{Frac}(R)$ に対して $q = ab^{-1}$ を満たす $\mathrm{Frac}(R)$ が存在する．

Proof. $\mathrm{Frac}(R)$ の加法，乗法を

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bc}$$

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$$

と定義する．これらが代表元の選び方によらず定まることは明らか．$\mathrm{Frac}(R)$ が体になることは明らか．$a, b \neq 0$ ならば a/b の逆元が b/a になることも明らか．a を $a/1$ と同一視すれば R は $\mathrm{Frac}(R)$ の部分環とみなせる．

また，$q \in \mathrm{Frac}(R)$ なら $q = a/b = a(1/b) = ab^{-1}$ となり，題意が示た． □

Definition 2.2.8.

R が整域のとき $\mathrm{Frac}(R)$ はその商体という．

Example 2.2.9.

$\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ である．

K が体である時，$\mathrm{Frac}(K[x])$ は K 上の有理関数体と言われる．

2.3 イデアルと商環

Definition 2.3.1.

R, S を環とする．写像 $\phi : R \to S$ が環準同型であるとは，$\forall r, r' \in R$ に対して，ϕ が
(1) $\phi(r + r') = \phi(r) + \phi(r')$.
(2) $\phi(rr') = \phi(r)\phi(r')$.
(3) $\phi(1) = 1$.
を満たす時にいう．

Example 2.3.2.

R を整域とし，$F = \mathrm{Frac}(R)$ とする．このとき，$R' = \{r/1 \in F \mid r \in R\}$ は F の部分環で，$\phi : r \mapsto r/1$ が R から R' への同型となる．

Definition 2.3.3.

$\phi : R \mapsto S$ が環準同型のとき，
(1) $\mathrm{Ker}(\phi) = \{r \in R \mid \phi(r) = 0\}$ を ϕ の核という．

(2) $\mathrm{Im}(\phi) = \{s \in S \mid s = \phi(r)\}$ を ϕ の像という．

Definition 2.3.4.

環 R のイデアルとは 0 を含み，次の (1), (2) を満たすような部分集合 $\mathfrak{a}$ のことである．
(1) $a, b \in \mathfrak{a}$ なら $a - b \in \mathfrak{a}$.
(2) $a \in \mathfrak{a}, r \in R$ なら $ra \in \mathfrak{a}$.

環 R のイデアル $\mathfrak{a}$ が $\mathfrak{a} \neq R$ なら $\mathfrak{a}$ は真イデアルという．

Proposition 2.3.5.

$\phi : R \mapsto S$ が環準同型であれば，その核は真イデアルとなる．また，ϕ が単写であることと，$\mathrm{Ker}(\phi) = 0$ であることは同値である．

Proof. $\mathfrak{a} = \mathrm{Ker}(\phi), a \in \mathfrak{a}, r \in R$ とする．

$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0$$

より，$ra \in \mathfrak{a}$ となるので $\mathrm{Ker}(\phi)$ は R のイデアルとなる．
省略 (命題 1.8.3 参考) □

Probrem 2.3.6.

R を体 F の部分環とし，R を含む F の部分体すべての共通部分を K とする．このとき，$K \cong \mathrm{Frac}(R)$ を示せ．

Definition 2.3.7.

群と同様に剰余環 (商環)$R/\mathfrak{a}$ の加法と乗法が十分に定義される．$r, r' \in R$ とする．
(1) $(r + \mathfrak{a}) + (r' + \mathfrak{a}) = (r + r') + \mathfrak{a}$.
(2) $(r + \mathfrak{a})(r' + \mathfrak{a}) = rr' + \mathfrak{a}$

(1) は明らかなので (2) について示す．
$r + \mathfrak{a} = s + \mathfrak{a}, r' + \mathfrak{a} = s' + \mathfrak{a}$ と仮定する．このとき代表元によらず $rr' + \mathfrak{a} = ss' + \mathfrak{a}$ となることを示せば良い．

$$rr' - ss' = (rr' - rs') + (rs' - ss') = r(r' - s') + (r - s)s'$$

であり，仮定より $r - s, r' - s' \in \mathfrak{a}$ で $\mathfrak{a}$ はイデアルなので $r(r' - s'), (r - s)s' \in \mathfrak{a}$ よってこの定義は矛盾なく定義されている．

2.4 多項式

Definition 2.4.1.

$a \in R$ に対して，$\{ra \mid r \in R\}$ は R のイデアルになる．これを a によって生成された主イデアル (単項イデアル) と呼び，(a) で表す．

Proposition 2.4.2.

F が体であれば，$F[x]$ の任意のイデアルは主イデアルとなる．

Proof. $\mathfrak{f}$ を $F[x]$ のイデアルとする．$\mathfrak{f} = \{0\}$ であれば $\mathfrak{f} = (0)$ は 0 で生成される主イデアルである．$\mathfrak{f} \neq \{0\}$ なら $\mathfrak{f}$ の中で最低次数の多項式 $m(x)$ を選ぶ．$\mathfrak{f} = (m(x))$ を示す．明らかに $(m(x)) \subset \mathfrak{f}$ である．$(m(x)) \supset \mathfrak{f}$ を示すために $\mathfrak{f}$ の多項式 $f(x)$ をとる．多項式の演算により，$f(x) = q(x)m(x) + r(x)$ が成り立つような多項式 $q(x), r(x)$ の存在は明らか．ここで，$r(x) = 0$ または $\partial(r) < \partial(m)$ である．さて，$r(x) = f(x) - q(x)m(x)$ なので $r(x) \neq 0$ なら $m(x)$ が $m(x)$ が $\mathfrak{f}$ の多項式の中で最低字数を持つことに反する．よって，$r(x) = 0$ であり，$f(x) \in (m(x))$ が成り立つ． □

Definition 2.4.3.

環 R は，R の任意のイデアルが主イデアルである整域になるとき，主イデアル整域 (PID) と呼ばれる．

Definition 2.4.4.

R を整域として，$f(x), g(x) \in R[x]$ という．$f(x)$ と $g(x)$ の最大公約多項式とは，次の条件を満たす多項式 $d(x) \in R[x]$ のことである．
(1) $d(x)$ は $f(x)$ と $g(x)$ の共通因子である．
(2) $c(x)$ が $f(X)$ と $g(x)$ の共通因子であれば $c(x) \mid d(x)$ である．
(3) $d(x)$ はモニックである．

Definition 2.4.5.

F を体，$f(x), g(x) \in F[x]$ とする．$f(x)$ と $g(x)$ の最小公倍多項式とは次の条件を満たす多項式 $m(x) \in F[x]$ である．
(1) $m(x)$ は $f(x)$ と $g(x)$ で割り切れる．
(2) $c(x)$ が $f(x)$ と $g(x)$ で割り切れれば $m(x) \mid c(x)$ である．
(3) $m(x)$ はモニックである．

Proposition 2.4.6.

F が体であり，$f(x), g(x) \in F[x]$ なら，それらの最小公倍多項式は $(f) \cap (g)$ の生成元となるモニックである．

Proof. $F[x]$ は PID なので,$\exists m(x) \in F[x]$ に対して $(f) \cap (g) = (m)$ となる．さて，$m \in (f)$ なので，$\exists r(x) \in F[x]$ に対して $m(x) = f(x)r(x)$ となり，また，$m \in (g)$ なので，$s(x) \in F[x]$ に対して $m(x) = g(x)s(x)$ となる．よって $m(x)$ が f と g の公倍多項式になる．$h(x)$ が f と g の別の公倍多項式ならば，$h(x) = f(x)r'(x) = g(x)s'(x)$ となる．すなわち，$h \in (f) \cap (g) = (m)$ になり，$m \mid h$. □

Proposition 2.4.7.

$f(x) \in F[x], a \in F$ とする．このとき，

$$f(x) = q(x)(x-a) + f(a)$$

が成り立つような $q(x) \in F[x]$ が存在する．

Proof. 多項式の割り算により，$F[x]$ において，$f(x) = q(x)(x-a) + r(x)$ であり，ここで $r(x) = 0$ であるが，$\partial(r) < 1 = \partial(x-a)$ なので，$r(x)$ は定数．x に a を代入すれば $f(a) = q(a)(a-a) + r = r$ である． □

2.5 素イデアルと極大イデアル

Definition 2.5.1.

環 R のイデアル $\mathfrak{p}$ は，$\mathfrak{p} \neq (1)$ を満たし，$xy \in \mathfrak{p}$ なら $x \in \mathfrak{p}$ または $y \in$ が成り立つ時，A の素イデアルという．

Definition 2.5.2.

R のイデアル $\mathfrak{m}$ は，$\mathfrak{m} \neq (1)$ かつ $m \subset \mathfrak{a} \subset (1)$ を満たす A のイデアル $\mathfrak{a}$ が存在しない時，R の極大イデアルという．

Proposition 2.5.3: ideal 対応定理

$\mathfrak{a}$ を環 R のイデアルとする，$\pi : R \to R/\mathfrak{a}$ を自然な準同型とする．$R/\mathfrak{a}$ のイデアルの集合と $\mathfrak{a}$ を含む R のイデアルの集合は互いの逆像となる行った 1 対 1 対応となる．

Proof. I, J をそれぞれ，$R/\mathfrak{a}$ のイデアル $\overline{\mathfrak{b}}$ の集合，R の $\mathfrak{a}$ を含むイデアル $\mathfrak{b}$ の集合，

$$\phi : I \ni \overline{\mathfrak{b}} \to \pi^{-1}(\overline{\mathfrak{b}}) \in J, \quad \psi : J \ni \mathfrak{b} \to \pi(\mathfrak{b}) \in I.$$

とすると，ϕ, ψ はそれぞれ well-difined であることを示す．

$\overline{\mathfrak{b}} \in I$ なら $0_{R/\mathfrak{a}} \in \overline{\mathfrak{b}}$ より，$\mathfrak{a} = \pi^{-1}(0_{R/\mathfrak{a}}) \subset \pi^{-1}(\overline{\mathfrak{b}})$ である．$x, y \in \pi^{-1}(\overline{\mathfrak{b}})$ なら，$\pi(xy^{-1}) = \pi(x)\pi(y)^{-1} \in \overline{\mathfrak{b}}$ より，$xy^{-1} \in \pi^{-1}(\overline{\mathfrak{b}})$ であるため，$\pi^{-1}(\overline{\mathfrak{b}})$ は R の部分アーベル群である．また，$\overline{\mathfrak{b}} \in I, a \in A, x \in \mathfrak{b}$ なら $\pi(ax) = \pi(a)\pi(x) \in \overline{\mathfrak{b}}$ である．よって $ax \in \mathfrak{b}$ なので，$\mathfrak{b}$ はイデアルである．

逆に，$\mathfrak{b} \in J, x \in \mathfrak{b}$ に対して，$x + \mathfrak{a} \in \overline{\mathfrak{b}}, a + \mathfrak{a} \in A/\mathfrak{a}$, なら，$(a + \mathfrak{a}) \cdot (x + \mathfrak{a}) = ax + \mathfrak{a}$ である．よって，$\mathfrak{b}$ はイデアルであるから，$ax \in \mathfrak{b}$ である．よって，$ax + \mathfrak{a} \in \overline{\mathfrak{b}}$ である．よって，$\mathfrak{b}, \overline{\mathfrak{b}}$ はそれぞれイデアルであるから，写像 ϕ, ψ は well-defined である． □

Proposition 2.5.4.

R を環とするとき，次は同値である．
(1) R は体である．
(2) R は自明でないイデアルを持たない．
(3) R から 0 でない環 R' への任意の準同型写像は単射である．

Proof. (1) → (2)：R を体，$\mathfrak{a} \neq 0$ を R のイデアルとする．$\mathfrak{a}$ が 0 でない元 x を含む．x は単元であるから，$\mathfrak{a} \supseteq (x) = (1)$ となり，$\mathfrak{a} = (1)$ となる．
(2) → (3)：$\phi : R \to R'$ を自然な準同型写像とする．このとき，$\mathrm{Ker}(\phi)$ は (1) と異なるイデアルであるから $\mathrm{Ker}(\phi) = 0$ となる．よって，命題 15 より ϕ は単写である．
(3) → (1)：x を単元でない R の元とする．$(x) \neq (1)$ より，$R' = R/(x) = \{0\}$ でない．$R \to R'$ を自然な準同型写像とすると $\mathrm{Ker}(x) = (x)$ である．仮定より，ϕ は単写であるから $(x) = 0$ である． □

Proposition 2.5.5.

環 R の真イデアル $\mathfrak{a}$ が素イデアルとなるための必要十分条件は，$R/\mathfrak{a}$ が整域となることである．

Proof. $\mathfrak{a}$ を素イデアルとする．$0 = (a+\mathfrak{a})(b+\mathfrak{a}) = ab + \mathfrak{a}$ なら $ab \in \mathfrak{a}$ であり，$\mathfrak{a}$ は素イデアルなので $a \in \mathfrak{a}$ または $b \in \mathfrak{a}$ が成り立つ．すなわち $a + \mathfrak{a} = 0$ または $b + \mathfrak{a}$ となり，$R/\mathfrak{a}$ は整域となる．逆は自明． □

Proposition 2.5.6.

環 R の真イデアル $\mathfrak{a}$ が極大イデアルとなるための必要十分条件は $R/\mathfrak{a}$ 体となることである．

Proof. 対応定理より $\mathfrak{a}$ が極大イデアルであるための必要十分条件は $R/\mathfrak{a}$ が $R/\mathfrak{a}$ と $\{0\}$ 以外にイデアルを持たないことである．命題 22 よりこれを満たすための必要十分条件は $R/\mathfrak{a}$ が体となることである． □

corollary 2.5.7.

環 R の任意の極大イデアルは素イデアルである．

Proposition 2.5.8.

R が単項イデアル整域であれば，任意の (0) でない素イデアル $\mathfrak{a}$ は極大イデアルとなる．

Proof. $(p) \subset (q)$ と仮定すると，$p = uq (x \in R)$ と表せるが，このとき $uq \in (p)$ かつ $q \notin (x)$ なので $u \in (q)$ である．すると $u = tp (t \in R)$ と表せる．よって $p = uq = utq$ が成り立つので $ut = 1$ である．したがって $(y) = (1)$ となる．$(q) \neq R$ なので q は単元ではない． □

Example 2.5.9.

環 R が整域なら零イデアル (0) は素イデアルとなる．$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, 多項式環 $\mathbb{C}[x]$ の零イデアル (0) は素イデアルである．

Proposition 2.5.10.

F が体で，$p(x) \in F[x]$ が既約であれば，商環 $F[x]/(p(x))$ は F(と同型な体) と $p(x)$ の根を含む体である．

Proof. $p(x)$ は既約より，単項イデアル $I = (p(x))$ は零でない素イデアルである．$F[x]$ は PID だから，I は極大イデアルであり，したがって $E = F[x]/I$ は体である．このとき，写像 $a \mapsto a + I$ は F から $F' = \{a + I : a \in F \subset E\}$ への同型となる．
$\omega = x + I \in E$ とおく．ω が $p(x)$ の根になることを示す．$p(x) = a_0 + a_1 x + \cdots a_n x^n$ とおく．このとき，$a_i \in F$ より，E において，

$$\begin{aligned} p(x) &= (a_0 + I) + (a_1 + I)\omega + \cdots + (a_n + I)\omega^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\ &= a_0 + a_1 x + \cdots + a_n x^n + I \\ &= p(x) + I \\ &= I \end{aligned}$$

が成り立つ．これは $I = (p(x))$ によるからである．$I = 0 + I$ は $F[x]/I$ の零元であり，ゆへに ω は $p(x)$ の根である． □

Definition 2.5.11.

多項式 $f(x) \in F[x]$ は，線形因子の積になるとき，F 上分解するという．

$f(x)$ が F 上分解する必要十分条件は F が $f(x)$ の全ての根を含むことである．

Theorem 2.5.12: クロネッカー (Kronecker)

F は体で，$f(x) \in F[x]$ とする．このとき $f(x)$ を分解し F を含む体 E が存在する．

Proof. 帰納法により証明する．$\partial(f) = 1$ なら，$f(x)$ は線形なので $E = F$ を選べば良い．$\partial(f) > 1$ のとき，$f(x) = p(x)g(x)$ と書く．ただし $p(x)$ は既約とする．命題 2.5.10 より F と $p(x)$ の根 ω を含む体 B が存在する．ゆえに $B[x]$ において $p(x) = (x - \omega)h(x)$ となる．帰納法の仮定により，$h(x)g(x)$ を分解し B を含む体 E が存在する．よって $f(x)$ は E 上で分解する． □

Definition 2.5.13.

体 F の素体とは F のすべての部分体の共通部分である．

素体は部分体となる

Proposition 2.5.14.

F が体であれば，その素体は $\mathbb{Q}$ に同型，または，ある素数 p に対する $\mathbb{Z}$ に同型となる．

Proof. $f : \mathbb{Z} \to F$ を $n \mapsto n1$ によって定まる写像とする．f は準同型写像になることは明らか．$\mathfrak{a} = \mathrm{Ker}(f)$ とすれば，$\mathbb{Z}/\mathfrak{a}$ は体 F の部分間に同型となるため，$\mathbb{Z}/\mathfrak{a}$ は整域である．したがって，$\mathfrak{a}$ は素イデアルであり，

$\mathfrak{a} = (0)$ または，ある素数 p に対し $\mathfrak{a} = (p)$ となる．$\mathfrak{a} = (0)$ のとき，体 F の素体は $\mathbb{Q}$ に同型となることは容易に示せる．$\mathfrak{a} = (p)$ のとき，第一同型定理により，$\mathrm{Im}(f) \cong \mathbb{Z}/\mathfrak{a} = \mathbb{Z}_p$ になり，これは体である．よって $\mathrm{Im}(f)$ は F の素体である． □

Definition 2.5.15.

体の標数が 0 であるとは，その素体が $\mathbb{Q}$ に同型であることをいう．体の標数が 0 が p であるとは，その素体は $\mathbb{Z}_p$ に同型であることをいう．

Lemma 2.5.16.

体 F の標数を $p > 0$ とする．このとき，すべての $a, b \in F$ と任意の正整数 k に対して $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ が成り立つ．

Proof. 二項定理と数学的帰納法より容易に示せる． □

Proposition 2.5.17: Galois

任意の素数 p と任意の正整数 n に対して，ちょうど p^n この元からなる体が存在する．

Proof. $|K| = p^n = q$ となる体 K が存在したとすれば，$K^\times = K - 0$ は位数 $q-1$ の乗法群となる．ラグランジュの定理により，すべての $a \in K^\times$ に対して $a^{q-1} = 1$ が成り立つ．したがって，K の任意の元は多項式 $g(x) = x^q - x$ の根となる．定理 2.5.12 より，$g(x)$ を分解するような $\mathbb{Z}_p$ を含む体 E が存在する．$F = \{\alpha \in E : g(\alpha) = 0\}$ とおく．すなわち，F は $g(x)$ のすべての根の集合である．$g'(x) = qx^{q-1} - 1 = -1$ であるから，補題 2.5.16 より，$\gcd(g, g') = 1$ がわかり，$g(x)$ は重根を持たない．よって $|F| = q = p^n$ である．F が体になることを示せば十分である．$a, b \in F$ ならば，$a^q = a$ であり $b^q = b$ が成り立つ．したがって，$(ab)^q = ab$ であり，$ab \in F$ である．補題 2.5.16 より b を $-b$ に置き換えると，$(a-b)^q = a^q - b^q = a - b$ がわかり，$a - b \in F$ が成り立つ．$a \neq 0$ であれば，$a^{q-1} = 1$ より，したがって，$a^{-1} = a^{q-2} \in F$．以上より題は示された． □

Probrem 2.5.18.

標数 p の無限体を一つ作れ．

Probrem 2.5.19.

(1) 環 R の零イデアルが素イデアルになるための必要十分条件は，R が整域であることを示せ．
(2) 環 R の零イデアルが極大イデアルになるための必要十分条件は，R が体であることを示せ．

Probrem 2.5.20.

(1) $F[x]$ の零でない任意の多項式 $f(x)$ に対し，ある零でない定数 a とある既約なモニック多項式 $p_i(x)$ が存在し．

$$f(x) = ap_1(x)\cdots p_t(x)$$

の形に因数分解できることを示せ.

(2) この因数分解は一意的であることを示せ.

2.6 線型空間

既に線型代数を学んだ者は読み飛ばしてもらっても以降の節で問題のない節である.
ここでは，あくまで体論を進める上で必要最低限の論理のみを扱い，また，例，命題などはほとんどないため，今後の節でわからないものがでてきたときに，その都度確認するような形で用いてくれて構わない．後，この節は今後発展させていく可能性がある.

Definition 2.6.1.

$\mathbb{R}$ の二つの元 m, n に対し，mn 個の複素数 $a_{ij}(1 \leq i \leq m, 1 \leq j \leq n)$ を，縦 m 個，横 n 個の長方形に並べたものを，(m, n) 型の行列という．これを大文字 A で表す.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

横に並んだ一列を行，縦に並んだ一列を列という．各 a_{ij} を行列の成分という.

F 上の (m, n) 型の行列の集合を $\mathrm{M}_{m,n}(F)$ であらわす．$m = n$ のとき，$\mathrm{M}_n = (F)$ であらわす.
$(m, 1)$ 型の行列を m 項列ベクトル，ないし，m 項縦ベクトルという．列ベクトルは一般の $m \times n$ 行列と区別するため，原則，太い小文字で表す.

$$\boldsymbol{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$$

対して，$(1, n)$ 型の行列は，n 項行ベクトル，ないし，n 項横ベクトルという.
行列の任意の成分が 0 であるような行列を O で表すことにする.

Definition 2.6.2.

行列に対して，次の演算が成り立つ.

1. $(A + B) + C = A + (B + C)$
2. $A + B = B + A$
3. $c(A + B) = cA + cB$
4. $(c + d)A = cA + dA$
5. $(cd)A = c(dA)$
6. $1A = A$
7. $0A = O$

一部，具体的に明示すると，

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

とし，

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{pmatrix}, \quad AB = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}$$

となる．ただし，c_{ij} は

$$c_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{im} b_{mj}$$

である．

(n, n) 型の所謂，正方行列，n 次行列において，(i, i) 成分 $(1 \leq i \leq n)$ のみが 1 であり，その他の成分が全て 0 であるような行列を n 次単位行列といい，E_n，ないし，混同の恐れのない場合においては E で表す．

$$E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

単位行列 E_n の n 個の列ベクトル

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots, \quad \boldsymbol{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

は n 項単位ベクトルという．(m, n) 型の行列 A において，A の縦成分と横成分を逆にした (n, m) 型の行列を A の転置行列といい，${}^tA$ で表す．

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \quad {}^tA = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix},$$

Definition 2.6.3.

n 次行列 A に対し，$XA = AX = E$ となる行列 X が存在するとき，A を正則行列といい，X を A の逆行列という．

n 次正則行列全体の集合 F は群の定義を満たす．この集合を $\mathrm{GL}_n(F)$ であらわす．

n 項列ベクトル全体の集合を C^n と表す．

Definition 2.6.4.

集合 F が次の二つの条件 (1), (2) を満たすとき，F を複素線型空間，ないし，複素ベクトル空間という．

(1) F の 2 つの元 $\boldsymbol{x}, \boldsymbol{y}$ に対して，第三の元 $\boldsymbol{x}+\boldsymbol{y}$，すなわち，加法が定まり次の法則が成り立つ．
   (a) $(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z}=\boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$ (結合法則)
   (b) $\boldsymbol{x}+\boldsymbol{y}=\boldsymbol{y}+\boldsymbol{x}$ (交換法則)
   (c) 単位元 $\boldsymbol{e}$ が存在し，$\boldsymbol{x}+\boldsymbol{e}=\boldsymbol{x}$ となる．
   (d) 逆元が存在し，$\boldsymbol{x}+(-\boldsymbol{x})=\boldsymbol{e}$ となる．この $-\boldsymbol{x}$ を $\boldsymbol{x}$ の逆ベクトルという．

(2) A の任意の元と任意の複素数 a に対し，$\boldsymbol{x}$ の a 倍と呼ばれるもう一つの元の A の元が定まり，次の法則が定まる．
   (A) $(a+b)\boldsymbol{x}=a\boldsymbol{x}+b\boldsymbol{x}$ (分配律)
   (B) $a(\boldsymbol{x}+\boldsymbol{y})=a\boldsymbol{x}+a\boldsymbol{y}$ (分配律)
   (C) $(ab)\boldsymbol{x}=a(b\boldsymbol{x})$
   (D) $1\boldsymbol{x}=\boldsymbol{x}$

F の元をベクトルという．また，複素数をスカラーという．上記の「複素数」のを「実数」に置き換えると，実線型空間，実ベクトル空間が定義される．

Definition 2.6.5.

空間 (平面) において，向きと長さの等しい矢印を全て同一視したものを幾何ベクトルという．

Example 2.6.6.

空間 (平面) の幾何ベクトルの全体 $F^3(F^2)$ は自明に実線型空間となる．

複素数全体の集合 $\mathbb{C}$，ないし，実数集合 $\mathbb{R}$ を，統一的に $\mathbb{K}$ で表す．

Definition 2.6.7.

$\mathbb{K}$ 上の線型空間 F, E とする．写像 $\phi : F \to E$ が次の二つの条件を満たすとき，ϕ を線型写像という．

1. $\phi(\boldsymbol{x}+\boldsymbol{y})=\phi(\boldsymbol{x})+\phi(\boldsymbol{y})$
2. $\phi(a\boldsymbol{x})=a\phi(\boldsymbol{x})$

F から F への線型写像を F の線型変換という．

Definition 2.6.8.

$\mathbb{K}$ 上の線型空間 F において，F のベクトル $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_k$ に対し，

$$c_1\boldsymbol{a}_1+c_2\boldsymbol{a}_2+\cdots+c_k\boldsymbol{a}_k, \quad c_i \in K \ (1 \le i \le k)$$

の形のベクトルを $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_k$ の線型結合という．

$\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_k$ の間の関係

$$c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \cdots + c_k\boldsymbol{a}_k = 0$$

を線型関係という．このとき，$c_1 = c_2 = \cdots = c_k = 0$ としたものは自明な線型関係という．自明な線型関係は必ず存在する．$\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_k$ の間に自明でない線形関係が存在するとき，$\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_k$ は線形従属であるといい，自明でない線型関係が存在しないとき，$\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_k$ は線型独立であるという．

Definition 2.6.9.

線型空間 F の有限個のベクトル $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ が次の二つの条件を満たすとき，$\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ は F の基底であるという．

1. $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ は線型独立である．
2. F の任意のベクトルは，$\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ の線型結合として表される．

基底において単なる集合としてではなく，順序を保持した集合として扱う必要がある．

Proposition 2.6.10.

$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ が線型独立ならば，ベクトル $\boldsymbol{x}$ を $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ での表し方は一意的である．

Proof.

$$\boldsymbol{x} = b_1\boldsymbol{a}_1 + b_2\boldsymbol{a}_2 + \cdots + b_n\boldsymbol{a}_n = c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \cdots + c_n\boldsymbol{a}_n$$

ならば,

$$(b_1 - c_1)\boldsymbol{a}_1 + (b_2 - c_2)\boldsymbol{a}_2 + \cdots + (b_n - c_n)\boldsymbol{a}_n = \boldsymbol{e}$$

なので，仮定より $b_1 = c_1, b_2 = c_2, \cdots, b_n = c_n$ が成り立つ．よって，一意性は示された． □

任意の環上において，基底が存在するとは限らない．

Theorem 2.6.11.

体 F 上のベクトル空間 E において，E が基底 $D = e_1, e_2, \cdots, e_n$ を持つなら，E の任意の基底は n 個の元よりなる．

Proof. 証明略. □

体 F 上のベクトル空間 E が n 個の元よりなる基底を持つとき，$\dim_F E = n$，ないし，$\dim E = n$ と表し，この n を E の次元という．

Example 2.6.12.

体 F 上の多項式環 $F[x]$ をベクトル空間と見なすとき，$F[x]$ は $E = \{1, x, x^2, \cdots\}$ を基底に持つ．このとき，$\dim F[x] = \infty$ である．

2.7 拡大体

Definition 2.7.1.

(1) F が体 E の部分体であるとき，E は F の拡大体であるといい，E/F で表す．
(2) E/F が体の拡大であるとき，$F \subset D \subset E$ となるような体 D を中間体という．

E/F が体の拡大であるとき，E は F 上の線形空間とみなすことができる．そこで，F 上の線型空間としての E の次元を E の拡大次数といい，$[E:F]$ で表す．$[E:F]$ が有限であるとき，E は F の有限次拡大といい，どうでないとき，無限次拡大という．$d = [E:F] < \infty$ なら E/F は d 次拡大という．

Definition 2.7.2.

(1) E/F を体の拡大，$x \in E$ とする．x が $F[x]$ のあるモニック多項式の根となるとき，すなわち，ある $a_1, \ldots, a_n \in F$ が存在して，$x^n + a_1 x^{n-1} + \cdots + a_n = 0$ が成り立つとき，x は F 上代数的であるといい，そうでないとき，x は F 上超越的であるという．
(2) E の全ての元が F 上代数的であるとき，E/F は代数拡大であるという．また，そうでないとき，超越拡大であるという．

π や e は，$\mathbb{Q}$ 上超越的であるため超越数とわれている．
E/F が代数拡大で D が中間体であるなら，F 上の多項式は D 上の多項式とみなせるため，E/D は代数拡大である．

Proposition 2.7.3.

E/F が有限次拡大であれば，E/F は代数拡大となる．

Proof. E/F であれば，ある $n > 0$ が存在し，$[E:F] = n$ となる．$x \in E$ とすると，$1, x, \ldots, x^n$ は 1 次従属[*1]である．よって，$a_0, \ldots, a_n \in F$ に対して，ある $a_i = 0$ が存在し，$a_0 + \ldots + a_n x^n = 0$ となる．したがって，x は F 上代数拡大であある． □

E/F を体の拡大，$D = \{a_1, \ldots, a_n\} \subset E$ を部分集合とする．このとき，F 上 D で生成された体，ないし，F に D を添加した体，$F(D)$ とは，

$$F[a_1, \ldots, a_n] \coloneqq \{f(a_1, \ldots, a_n) \mid f \in F[x_1, \ldots, x_n]\}$$

とし，

$$F(D) = F(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \,\middle|\, f, g \in F[x_1, \ldots, x_n] \right\}$$

のことであり，これはすなわち，商体 $F(D) = \mathrm{Frac}(F[D])$ である．

[*1] 1 次従属，ないし，線形従属であるとは，環 R の元 $x_1, \ldots, x_n$ とスカラー $a_1, \ldots, a_n$ において，ある $a_i \neq 0$ が存在して，$a_1 x_1 + \cdots + a_n x_n = 0$ が成り立つことをいう．

2.8 分解体

2.9 ガロア群

2.10 ガロア理論

参考文献

[1] 雪江明彦,『群論入門』(代数学 1),日本評論社,2010.

[2] 雪江明彦,『環と体のガロア理論』(代数学 2),日本評論社,2010.

[3] M. F. Atiyah, L. G.MacDonald (著),新妻弘 (訳),『Atiyah-MacDonald 可換代数入門』,共立出版,2006.

[4] J. Rotman (著),関口次郎 (訳),『改訂新版 ガロア理論』,丸善出版,2012.

[5] 齋藤正彦,『線形代数入門』,東京大学出版,1966.