離散数学 講義資料 (10)

10.1 さまざまな代数

本節は，教科書 4.1.2 節 (pp.157–163) と 4.1.3 節の冒頭 (p.163) に対応する．

10.1.1 半群・モノイド・群

定義 10.1 G を集合とし，$\cdot$ を G 上の 2 項演算とする．

- 条件 (G1) を満たすならば，二つ組 $\langle G, \cdot \rangle$ は**半群** (semigroup) であると呼ばれる．
- 条件 (G1),(G2) を満たすならば，三つ組み $\langle G, \cdot, e \rangle$ は**モノイド** (monoid) であると呼ばれる．ただし，$e \in G$ とする．
- 条件 (G1),(G2),(G3) を満たすならば，三つ組み $\langle G, \cdot, e \rangle$ は**群** (group) であると呼ばれる．ただし，$e \in G$ とする．

(G1) $\forall x, y, z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$

(G2) $\forall x.\ x \cdot e = e \cdot x = x$

(G3) $\forall x. \exists y.\ x \cdot y = y \cdot x = e$

ここで，モノイドと群において，e を $\cdot$ の**単位元** (unit element) と呼ぶ．また，群において，(G3) における x, y に対し，y を x の**逆元** (inverse element) と呼ぶ．なお，命題 9.6 ですでに示したように群において逆元は一意に存在するので，x の逆元を x^{-1} で記す (演算記号として $+$ を用いたときは $-x$ を利用する場合が多い)． □

例 10.2 $\langle \{1, 2, \ldots\}, + \rangle$ は半群であり，$\langle \mathbb{N}, +, 0 \rangle$ はモノイドであり，$\langle \mathbb{Z}, +, 0 \rangle$ は群になる． □

定義 10.3 以下の条件を満たす群 $\langle G, \cdot, e \rangle$ を**可換群** (commutative group) または**アーベル群** (Abelian group) と呼ぶ．

(G4) $\forall x, y.\ x \cdot y = y \cdot x$ □

10.1.2 環

定義 10.4 **環** (ring) とは以下の条件を満たす五つ組み $\langle R, +, \cdot, 0, 1 \rangle$ の事である．

(R1) $\langle R, +, 0 \rangle$ が可換群である．

(R2) $\langle R \setminus \{0\}, \cdot, 1 \rangle$ がモノイドである．

(R3) 分配法則が成立する．すなわち，任意の $x, y, z \in R$ に対し次の関係が成立する．
$x \cdot (y + z) = x \cdot y + x \cdot z, \quad (x + y) \cdot z = x \cdot z + y \cdot z$ □

定義 10.5 以下の条件を満たす環 $\langle R, +, \cdot, 0, 1\rangle$ を**可換環** (commutative ring) と呼ぶ.

(R4) $\forall x, y.\ x \cdot y = y \cdot x$ □

例 10.6 $\langle \mathbb{Z}, +, \times, 0, 1\rangle$ や $\langle Z_n, \oplus_n, \otimes_n, 0, 1\rangle$ は可換環になる. □

10.1.3 整域

定義 10.7 $\langle R, +, \cdot, 0, 1\rangle$ を環とする. $a \neq 0$ かつ $b \neq 0$ であるが $a \cdot b = 0$ となる R の元 a, b を**零因子** (zero divisor) と呼ぶ (より厳密には, a を左零因子, b を右零因子と呼ぶ). □

定義 10.8 **整域** (integral domain) とは零因子を持たない可換環の事である. □

例 10.9 $\langle \mathbb{Z}, +, \times, 0, 1\rangle$ や任意の素数 p に対して $\langle Z_p, \oplus_p, \otimes_p, 0, 1\rangle$ は整域になる. なお, 合成数 n に対して $\langle Z_n, \oplus_n, \otimes_n, 0, 1\rangle$ は整域にならない ($n = ij$ とすると, $i \otimes_n j = 0$ なので i, j は零因子). □

定義 10.10 $\langle R, +, \cdot, 0, 1\rangle$ を整域とし, $a, b \in R$ とする. ある $q \in R$ が存在して $a = bq$ となるとき $b \mid a$ と記す. このとき, a を b の**倍元** (multiple) と呼び, b を a の**約元** (divisor) と呼ぶ. □

定義 10.11 $\langle R, +, \cdot, 0, 1\rangle$ を整域とし, $a \in R$ とする. ある $b \in R$ が存在して $a \cdot b = b \cdot a = 1$ となるならば, a を**可逆元** (invertible element) または**単元**と呼ぶ. また, ある $b \in R$ に対し, $a \mid b$ かつ $b \mid a$ となるとき a は b に**同伴**である (a is associate to b) という. □

定義 10.12 $\langle R, +, \cdot, 0, 1\rangle$ を整域とし, p を 0 でも可逆元でもない R の元とする. p が可逆元および同伴な元以外に約元を持たないとき, p は**素元** (prime element) と呼ばれる. □

NOTE: 整域 $\langle \mathbb{Z}, +, \times, 0, 1\rangle$ において, 倍元と約元は倍数と約数にちょうど対応する. また, 可逆元は $-1, 1$ の 2 つだけである. 素元は素数かある素数に -1 を掛けた値に対応する (-2 は素数ではないが素元ではある).

定義 10.13 整域 $\langle R, +, \cdot, 0, 1\rangle$ は, 以下の条件を満たす自然数値関数 $v : R \to \mathbb{N}$ が存在するとき**ユークリッド整域** (Euclidean domain) と呼ばれる.

- 任意の $a, b \in R$ に対し, $b \neq 0$ ならば次の関係を満たす $q, r \in R$ が存在する.

$$a = bq + r, \quad r = 0 \text{ または } v(r) < v(b)$$

なお, 関数 v を**付値** (valuation) または**ノルム** (norm) と呼ぶ. □

NOTE: 直感的に言うと, ユークリッド整域とはユークリッドの互除法が適用可能な整域である.

例 10.14 $\langle \mathbb{Z}, +, \times, 0, 1\rangle$ はユークリッド整域である. ここで付値 v は $v(n) = |n|$ で定義される. □

例 10.15 集合 $\mathbb{Z}[i]$ を $\{a+bi \mid a,b \in \mathbb{Z}\}$ で定義する (ガウスの整数と呼ばれる)．このとき，$\langle \mathbb{Z}[i], +, \times, 0, 1\rangle$ はユークリッド整域になる．ここで付値 v は $v(a+bi) = a^2+b^2$ で定義される．なお，この整域における素元は，整域 $\langle \mathbb{Z}, +, \times, 0, 1\rangle$ における素元を有理素数と呼ぶことにすると

(i) $1+i$ とその同伴元

(ii) $p = 4n+3$ の形の有理素数とその同伴元

(iii) $p = 4n+1$ の形の有理素数の約元である $a \pm bi$ (ただし $a^2+b^2 = p$) とその同伴元

のいずれかとなる． □

NOTE: 整域には他にも**一意分解整域**や**単項イデアル整域**等重要な概念があるが，本講義の枠組みを外れるので割愛する．なお，直感的に言うと，一意分解整域とは素因数分解の一意性に対応する性質が成立する整域であり，単項イデアル整域とは最大公約数に対応する概念が定義可能な整域である．

10.1.4 体

定義 10.16 体 (field) とは以下の条件を満たす五つ組み $\langle R, +, \cdot, 0, 1\rangle$ の事である．

(F1) $\langle R, +, \cdot, 0, 1\rangle$ が環である．

(F2) $\langle R \setminus \{0\}, \cdot, 1\rangle$ が群である．

特に，$\langle R \setminus \{0\}, \cdot, 1\rangle$ が可換群となるときには**可換体** (commutative field) とも呼ぶ． □

NOTE: 文献によっては，“体” のことを “斜体 (skew field)”，“可換体” のことを “体” と呼ぶことがある．注意されたし．

例 10.17 $\langle \mathbb{Q}, +, \times, 0, 1\rangle$ や $\langle \mathbb{R}, +, \times, 0, 1\rangle$ や $\langle \mathbb{C}, +, \times, 0, 1\rangle$ は体となる (それぞれ有理数体，実数体，複素数体と呼ばれる)．また，p を素数とすると $\langle Z_p, \oplus_p, \otimes_p, 0, 1\rangle$ は体となる． □

10.1.5 加群・線形空間

定義 10.18 $\langle R, +', \cdot, 0', 1\rangle$ を環とし，$\langle M, +, 0\rangle$ を可換群とする．もし，$R \times M$ から M への写像 s が存在し (以下では単に $s(n,x)$ を nx で記す)，次の条件が全て成立するならば M を R の上の**加群** (module) であると言う．

(M1) 任意の $a \in R,\ x, y \in M$ に対し，$a(x+y) = ax + ay$.

(M2) 任意の $a, b \in R,\ x \in M$ に対し，$(a +' b)x = ax + bx$.

(M3) 任意の $a, b \in R,\ x \in M$ に対し，$(a \cdot b)x = a(bx)$.

(M4) 任意の $x \in M$ に対し，$1x = x$.

ここで，R の元を**スカラー** (scalar) と呼び，写像 $(n,x) \mapsto nx$ を**スカラー倍** (scalar multiple) と呼ぶ． □

定義 10.19 体上の加群を**線形空間** (linear space) または**ベクトル空間** (vector space) と呼ぶ. □

NOTE: 線形空間の概念は他の講義 (線形代数等) で習ったと思われる．当然のことながら，上記の代数的な定義は皆様が習った線形空間の定義と等価である．ちなみに，上記の定義の下で基底の存在を示すのは結構難しい (一般には選択公理なるものを必要とする).

10.2 代数間の関係

補題 10.20 $\langle R, +, \cdot, 0, 1\rangle$ を環とする．このとき任意の $a, b \in R$ に対し以下が成立.

(i) $0a = a0 = 0$

(ii) $(-a)b = a(-b) = -ab$

(iii) $-(-a) = a$

(vi) $(-a)(-b) = ab$

証明

(i) $0a = 0a + 0a - 0a = (0+0)a - 0a = 0a - 0a = 0$
$a0 = a0 + a0 - a0 = a(0+0) - a0 = a0 - a0 = 0$

(ii) $(-a)b = (-a)b + ab - ab = (-a+a)b - ab = 0b - ab = 0 - ab = -ab$
$a(-b) = a(-b) + ab - ab = a(-b+b) - ab = a0 - ab = 0 - ab = -ab$

(iii) 命題 9.8(3) ですでに示してある.

(vi) (ii) と (iii) を用いて，$(-a)(-b) = -((-a)b) = -(-ab) = ab$ □

定理 10.21 $\langle R, +, \cdot, 0, 1\rangle$ をある代数とする (R は集合であり，$+$ と $\cdot$ は R 上の 2 項演算であり，$0, 1 \in R$ とする)．このとき以下の関係が成立する ($\langle R, +, \cdot, 0, 1\rangle$ を R で略記する).

(i) R が有限整域ならば R は体である.

(ii) R が体ならば R は整域である.

(iii) R が整域ならば R は環である.

証明 $0 = 1$ の場合を考える．R が整域の場合でも体の場合でも環ではあるので，任意の $a \in R$ に対し $a = 1a = 0a = 0$ となり，$R = \{0\}$ となる．この場合は明らかに R は整域であり体でもある．以下では $0 \neq 1$ の場合のみ考える ($0 \neq 1$ を環や整域や体の公理として要求することも多い．注意されたし．).

(i) 集合 R が有限であることを考えて，$R = \{0, a_1, \ldots, a_m\}$ とする．代数 R が体であることを示すためには，任意の $a \in R \setminus \{0\}$ に対し，ある a_i が存在して $aa_i = 1$ であることを示せば十分．ここで，R の全ての要素に左から a を掛けて得られる列

$$a0, aa_1, aa_2, \ldots, aa_m$$

を考える．このとき，これらは全て互いに異る．なぜならば，$a_j \neq a_k$ かつ $aa_j = aa_k$ と仮定すると，

$$a(a_j - a_k) = aa_j - aa_k = 0 \text{ かつ } a_j - a_k \neq 0$$

となる．ところが，R は整域，すなわち零因子を持たないので $a = 0$ となる．これは仮定に反する．したがって，$a0 = 0$ を考えて $R = \{0, aa_1, aa_2, \ldots, aa_m\}$ となる．よって，$1 \in R \setminus \{0\}$ であるので，ある a_i で $aa_i = 1$.

(ii) R を体とする．任意の $a \in R \setminus \{0\}$ が零因子でないことを示せば十分．ある $a \in R \setminus \{0\}$ が零因子であると仮定する．このとき，ある $b \in R \setminus \{0\}$ に対し $ab = 0$．R は体なので，$a^{-1} \in R \setminus \{0\}$．よって，$b = 1b = a^{-1}ab = a^{-1}0 = 0$ となり矛盾.

(iii) 定義より明らか. □

演習課題

問 10.1 以下の表を完成させよ．ただし，○を記したところの証明は必要ないが，×をつけたところの反例は記しておくこと．

	環	整域	体
$\langle \mathbb{N}, +, \times, 0, 1 \rangle$			
$\langle \mathbb{Z}, +, \times, 0, 1 \rangle$	○	○	
$\langle \mathbb{Q}, +, \times, 0, 1 \rangle$			○
$\langle Z_n, \oplus_n, \otimes_n, 0, 1 \rangle$	○	×	
$\langle Z_p, \oplus_p, \otimes_p, 0, 1 \rangle$		○	
$\langle \mathbb{Z}[i], +, \times, 0, 1 \rangle$		○	
$\langle \{true, false\}, \vee, \wedge, false, true \rangle$			
$\langle \{true, false\}, \oplus, \wedge, false, true \rangle$	○		
$\langle \{true, false\}, \oplus, \wedge, true, false \rangle$			

ただし，n は合成数，p は素数とし，最後の 2 つのところの $\oplus$ は排他的論理和である．