2010年度 前期 代数学演習2

更新日時 2010-07-13 21:01:16　担当 和地 輝仁

目 次

1　シラバス抜粋　1

2　授業のノート　2

§1　群と剰余集合 2

§2　環とイデアル 4

§3　剰余環 6

1　シラバス抜粋

到達目標

1. 剰余空間、剰余環、分数環の構成や性質に習熟する。
2. 体論の基礎や作図問題について習熟する。

授業計画　順序を交換する場合もあるので注意すること。

1. 剰余空間の演習1
2. 剰余空間の演習2
3. イデアルの演習1
4. イデアルの演習2
5. 剰余環の演習1
6. 剰余環の演習2
7. 準同型定理の演習1
8. 準同型定理の演習2
9. 分数環の演習1
10. 分数環の演習2
11. 体の拡大の演習1
12. 体の拡大の演習2
13. 作図問題の演習1
14. 作図問題の演習2
15. 期末試験

成績評価　期末試験 (50%) と、毎回の演習問題の状況 (50%) で成績を評価する。原則として全ての時間の出席を求めるが、やむを得ない理由で欠席をする (した) 場合はできるだけ速やかに申し出て、指示を受けること。

2　授業のノート

授業で用いる演習問題や基本事項を記す。

§1　群と剰余集合

(1.1)　**群と部分群**

演算を持つ集合 G が**群**であるとは、次の条件を満たすことを言う。

(G1) 演算が結合法則を満たす。
(G2) 単位元が存在する。
(G3) 任意の元に対してその逆元が存在する。

群が**アーベル群**であるとは、演算が交換法則を満たすときを言う。このとき演算を和 $(+)$ で表し**加法群** と呼ぶこともある。
群 G の空でない部分集合 H が**部分群**であるとは、H が G と同じ演算で群をなすときを言う。

(1.2)　**問題**　次の集合と演算の組が群をなすことを示せ。また、アーベル群か否か答えよ。
(1) $(\mathbb{Z},+)$
(2) $(\mathbb{Q}^\times,\times)$. ただし、$\mathbb{Q}^\times=\mathbb{Q}-\{0\}$.
(3) $(\mathbb{Q}_{>0},\times)$. ただし、$\mathbb{Q}_{>0}=\{x\in\mathbb{Q}\mid x>0\}$.
(4) $(\{\pm1\},\times)$
(5) $(\mathrm{Mat}_n(\mathbb{R}),+)$. ただし、$\mathrm{Mat}_n(\mathbb{R})$ は n 次正方行列全体。
(6) $(GL_n(\mathbb{R}),\text{積})$. ただし、$GL_n(\mathbb{R})$ は n 次正則行列全体。
(7) $(\mathrm{Aut}(X),\circ)$. ただし、$\mathrm{Aut}(X)$ は集合 X から X への全単射全体で、$\circ$ は写像の合成。
(8) $(S_n,\circ)$. ただし、S_n は n 次対称群で、$\circ$ は写像の合成。

(1.3)　**問題**　次の部分集合が部分群であることを示せ。
(1) $2\mathbb{Z}\subset\mathbb{Z}$. 演算は和で、$2\mathbb{Z}$ は 2 の倍数全体の集合。
(2) $31\mathbb{Z}\subset\mathbb{Z}$. 演算は和。
(3) (n 次対角行列全体) $\subset\mathrm{Mat}_n(\mathbb{R})$. 演算は和。
(4) (正則な n 次対角行列全体) $\subset GL_n(\mathbb{R})$. 演算は積。
(5) $A_n\subset S_n$. ただし、A_n は n **次交代群** (S_n の偶置換全体)。

(1.4)　**同値関係**

$\sim$ が集合 S 上の**関係**であるとは、任意の $x,y\in S$ に対して、$x\sim y$ であるかそうでないかが確定することを言う。
集合 S 上の関係 $\sim$ が**同値関係**であるとは、次の 3 条件が満たされるときを言う。

(E1) 任意の $x\in S$ に対し、$x\sim x$ (反射律)
(E2) $x\sim y$ ならば $y\sim x$ (対称律)
(E3) $x\sim y$ かつ $y\sim z$ ならば $x\sim z$ (推移律)

(1.5)　**問題**　次のものが関係であることを示せ。また、それが同値関係かどうか答えよ。
(1) $\mathbb{R}$ 上の不等号 $<$
(2) $\mathbb{R}$ 上の等号 $=$
(3) $x,y\in\mathbb{Z}$ に対して、$x\equiv y \pmod 3$ のとき $x\sim y$ と定める。
(4) 写像 $f:A\to B$ があるとき、$x,y\in A$ に対して、$f(x)=f(y)$ のとき $x\sim y$ と定める。
(5) あるクラスの学生に対して、x さんと y さんの血液型が同じとき、$x\sim y$ と定める。
(6) 集合 X の部分集合全体のなす集合を S とするとき、S における包含関係 $\subset$.
(7) 47 の都道府県庁所在地のなす集合において、x から y へ陸続きで行けるならば $x\sim y$ と定める。

(1.6)　商集合

　S 上に同値関係 $\sim$ があるとき、$[x] = \{y \in S \mid y \sim x\}$ $(\subset S)$ と定め、$\sim$ に関する**代表元** x の**同値類**と呼ぶ。
　$S = \coprod_{C:\text{同値類}} C$ を S の $\sim$ に関する**同値類別**と呼ぶ。
　$S/\!\sim\, = \{C \mid C \text{ は同値類 }\}$ と定め、S の $\sim$ による**商集合** と呼ぶ。
　$\pi : S \to S/\!\sim$ $(x \mapsto [x])$ をを**自然な写像**と呼ぶ。S の部分集合 X が自然な写像 π により $S/\!\sim$ を 1 対 1 に対応するとき、X を $S/\!\sim$ の**完全代表系**と呼ぶ。

(1.7)　問題　(1.5) で同値関係だったものについて、[a] 同値類の具体的な形、[b] 同値類の個数は有限個か無限個か。また、有限なら何個か、[c] 商集合、[d] (ひとつの) 完全代表系を求めよ。

(1.8)　問題　平面 $\mathbb{R}^2$ において、$\mathrm{P}, \mathrm{Q} \in \mathbb{R}^2$ に対して、P と Q が等しいか、または、直線 PQ の傾きが 1 であるとき、$\mathrm{P} \sim \mathrm{Q}$ と定める。
(1) $\sim$ が同値関係であることを示せ。
(2) 同値類の具体的な形を図示せよ
(3) $\mathbb{R}^2/\!\sim$ の完全代表系を 1 つ与えよ。

(1.9)　問題　原点を除いた平面 $(\mathbb{R}^2)^\times$ において、$u, v \in (\mathbb{R}^2)^\times$ に対して、$u/|u| = v/|v|$ であるとき、$u \sim v$ と定める。ただし、点と (位置) ベクトルを同一視し、$|u|$ は u の大きさである。
(1) $\sim$ が同値関係であることを示せ。
(2) 同値類の具体的な形を図示せよ
(3) $(\mathbb{R}^2)^\times/\!\sim$ の完全代表系を 1 つ与えよ。

(1.10)　剰余集合

　群 G の部分群 H があるとき、G 上の同値関係 $\sim$ を、$x^{-1}y \in H$ のとき $x \sim y$ と定める。このとき、$\sim$ に関する同値類を H に関する**左剰余類**と呼び、xH $(\subset G)$ と書く。また、商空間 $G/\!\sim$ を G/H と書き、G の H による**左剰余集合** (H **で右から割った集合**) と呼ぶ。
　最初の同値関係を $xy^{-1} \in H$ のとき $x \sim y$ と定めても同様の議論ができ、**右剰余類**、**右剰余集合** (H **で左から割った集合**) が定まる。

(1.11)　問題　群 G とその部分群 H があるとき、$x \in G$ に対して次を示せ。
(1) $xH = \{xh \mid h \in H\}$　　(2) $Hx = \{hx \mid h \in H\}$

(1.12)　問題　有限群 G とその部分群 H があるとき、次を示せ。有限集合については濃度は要素の数と読み換えられる。また、有限群とは限らない場合にも示せ。
(1) 左剰余類 xH や右剰余類 Hx の濃度は、$x \in G$ によらず一定である。
(2) $\#G = \#(G/H) \cdot \#H.$ ただし、$\#X$ は集合 X の濃度を表す。

(1.13)　問題　有限群 G とその部分群 $H \supset K$ があるとき、$\#(G/K) = \#(G/H) \cdot \#(H/K)$ を示せ。また有限群とは限らない場合にも示せ。

(1.14)　正規部分群と剰余群

　群 G の部分群 H が**正規部分群**であるとは、任意の $x \in G$ に対して、$xHx^{-1} = H$ なることを言い、$H \triangleleft G$ と書く。ただし、$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$ である。
　このとき、G/H を G の H による**剰余群**と呼ぶ。

(1.15)　問題　アーベル群 G の部分群 H は、常に正規部分群であることを示せ。

(1.16)　問題　群 G の部分群 H が正規部分群であるための必要十分条件は、$G/H = H\backslash G$ が成立することであることを示せ。

(1.17)　**問題**　群 G の部分群 H について、$\#(G/H) = 2$ ならば H は G の正規部分群であることを示せ。

(1.18)　**問題**　(1.3) の部分群のうち、正規部分群であるものはどれか。また、正規部分群であるものについて、剰余群の具体的な形を与えよ。

(1.19)　**問題**　$G \triangleright H$ のとき、G/H が群になることを次の手順で示せ。
(1) $xH, yH \in G/H$ に対して、$xH \cdot yH = (xy)H$ と (代表元 x, y の選び方によらず) 積を定めることができることを示せ。つまり、$xH = x'H$ かつ $yH = y'H$ ならば $(xy)H = (x'y')H$ であることを示せ。
(2) こうして定めた積が群の公理を満たすことを示せ。

(1.20)　**問題**　$G \triangleright H$ のとき次の問に答えよ。
(1) G がアーベル群ならば G/H もアーベル群であることを示せ。
(2) G がアーベル群ではないが G/H はアーベル群である例をあげよ。
(3) G が有限群ならば G/H も有限群であることを示せ。
(4) G が有限群ではないが G/H は有限群である例をあげよ。

(1.21)　**問題**　$\mathbb{R}^2$ を加法群と見て、$H = \{(x, x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ とおくとき次の問に答えよ。
(1) H は $\mathbb{R}^2$ の正規部分群であることを示せ。
(2) H に関する剰余類の具体的な形を与えよ。
(3) $\mathbb{R}^2/H$ の完全代表系を 1 つ与えよ。

§2　環とイデアル

(2.1)　環

　2 つの演算、積と和を持つ集合 R が**環**であるとは、次の条件を満たすことを言う。

(R1) 和に関して加法群である (和に関する単位元を 0 と書く)。
(R2) 積が結合法則を満たす
(R3) 積に関する単位元 1 を持つ。
(R4) 分配法則を満たす:

$$x(y+z) = xy + xz, \quad (x+y)z = xz + yz \quad (x, y, z \in R).$$

　また、積が交換法則 $xy = yx$ を満たすとき、R を**可換環**と呼ぶ。
　可換環 R の元 x が**零因子**であるとは、ある 0 ではない元 $a \in R$ があって、$ax = 0$ となることを言う。0 以外に零因子のない可換環を**整域**と呼ぶ。

(2.2)　**問題**　次の集合が指定された和と積に関して環であることを証明せよ。また、可換環であるかどうかも言え。
(1) $\mathbb{Z}$, 整数の和, 整数の積
(2) 成分が実数である n 次正方行列全体の集合 $\mathrm{Mat}_n(\mathbb{R})$, 行列の和, 行列の積
(3) R を任意の可換環とするとき、R の元を成分に持つ n 次正方行列全体の集合 $\mathrm{Mat}_n(R)$, 行列の和, 行列の積

(2.3)　**問題**　R を環とするとき、環の定義を用いて次を証明せよ。
(1) $0x = 0$ $(x \in R)$　(2) $(-1)x = -x$ $(x \in R)$　(3) $1 = 0$ ならば $R = \{0\}$
[ヒント: (2) の左辺は積、右辺は加法の逆元。(3) は、すべての $x \in R$ について、$1 = 0$ を利用して $x = 0$ を示す。]

(2.4)　**問題**　次の問に答えよ。
(1) 0 ではない可換環 R において、0 は零因子であることを証明せよ。
(2) $\mathbb{Z}$ は整域であることを証明せよ。

(2.5)　**問題**　環 R を有限集合とするとき次の問に答えよ。
(1) 零因子ではない $a \in R$ を取ったとき、写像 $R \to R$ $(x \mapsto ax)$ は単射であることを証明せよ。
(2) (1) の写像が全射であることを示せ。
(3) 0 以外のすべての元が逆元を持つような可換環を**体**と呼ぶ。有限環 R が整域ならば、体であることを証明せよ。

(2.6)　**多項式環**

R を可換環とする。$a_j \in R$ を係数に持つ X の多項式 $p(X) = a_0 + a_1X^1 + \cdots + a_nX^n$ 全体の集合

$$R[X] = \left\{ \sum_{j=0}^{n} a_jX^j \mid n \geq 0, a_j \in R \right\}$$

R 係数の (R 上の) X の (X を変数とする) **1 変数多項式環**と呼ぶ。

$p(X)$ における X^j の係数を a_j としたとき、a_j が 0 ではないような最大の j を $p(X)$ の**次数**と呼び、$\deg p(X)$ と書く。ただし、$p(X) = 0$ のときは、便宜的に $\deg p(X) = -\infty$ とおく。

$R[X_1, X_2] = (R[X_1])[X_2]$ と定め、R 上の X_1 と X_2 を変数とする **2 変数多項式環**と呼ぶ。以下帰納的に n 変数多項式環を定義する。

(2.7)　**問題**　次の問に答えよ。
(1) $R[X]$ が通常の和と積に関して可換環をなすことを証明せよ。これにより、多項式環という呼称が正当化される。
(2) R が整域ならば、$R[X]$ も整域であることを証明せよ。

(2.8)　**イデアル**

環 R の空ではない部分集合 I が R の**左イデアル**であるとは、次を満たすときを言う。

(I1) 任意の $x, y \in I$ に対して、$x + y \in I.$
(I2) 任意の $a \in R,\ x \in I$ に対して $ax \in I.$

また、I が R の**右イデアル**であるとは、(I2) に代えて、

(I2') 任意の $a \in R,\ x \in I$ に対して $xa \in I.$

を満たすときを言い、I が左イデアルかつ右イデアルであるとき、**両側イデアル**であると言う。

可換環では左イデアルと右イデアルは同じものであるから、単に**イデアル**と呼んで構わない。

(2.9)　**問題**　次の問に答えよ。
(1) 環 R のイデアル I は、和に関して R の部分群であることを証明せよ。
(2) m を整数とするとき、m の倍数全体のなす $\mathbb{Z}$ の部分集合は、$\mathbb{Z}$ のイデアルであることを証明せよ。
(3) 環 R のイデアル I に対して、$R = I$ であるための必要十分条件は、$1 \in I$ であることを証明せよ。

(2.10)　**問題 (イデアルの和、積)**　可換環 R の 2 つのイデアル I, J について、

$$I + J = \{x + y \mid x \in I, y \in J\},$$
$$IJ = \{ \sum_{\text{有限和}} x_iy_i \mid x_i \in I, y_i \in J\}$$

と定める。このとき次の問に答えよ。
(1) $I + J,\ I \cap J,\ IJ$ はどれも R のイデアルであることを証明せよ。
(2) $I + J \supset I \supset I \cap J \supset IJ$ を証明せよ。

(2.11)　**問題**　整数環 $\mathbb{Z}$ のイデアルを

$$I = \{4\ \text{の倍数全体}\}, \qquad J = \{6\ \text{の倍数全体}\}$$

とおくとき、次のイデアルはどのようなイデアルか答えよ。
(1) $I + J$　(2) $I \cap J$　(3) IJ

(2.12)　**問題 (イデアルの生成系)**　環 R の部分集合 S に対して

$$RS = \{ \sum_{\text{有限和}} a_ix_i \mid a_i \in R, x_i \in S\}$$

と定め、S で**生成される**左イデアルと呼び、S を RS の**生成系**と呼ぶ。

また、$S = \{f_1, f_2, \ldots, f_k\}$ のとき、RS のことを $(f_1, f_2, \ldots, f_k)$ とも書く。このとき次の問に答えよ。
(1) RS は R の左イデアルであることを証明せよ。
(2) $f_1, f_2, \ldots, f_k \in R$ に対して、$(f_1, f_2, \ldots, f_k) = (f_1) + (f_2) + \cdots + (f_k)$ であることを証明せよ。
(3) $f, g \in R$ のとき、$(f)(g) = (fg)$ であることを証明せよ。

(2.13)　**問題 (単項イデアル整域)**　環 R のイデアル I が 1 つの元 $f \in R$ で生成されるとき、I を**単項イデアル**と呼び、f を I の**生成元**と呼ぶ。また、整域 R のイデアルがすべて単項イデアルであるとき、R を**単項イデアル整域 (PID)** と呼ぶ。次の問に答えよ。
(1) $\mathbb{Z}$ は単項イデアル整域であることを証明せよ。
(2) $\mathbb{Z}$ のイデアル $(m) \cap (n)$ の生成元を求めよ。
(3) $\mathbb{Z}$ のイデアル $(m) + (n)$ の生成元を求めよ。
(4) K を体とするとき、$K[X]$ は単項イデアル整域であることを証明せよ。

(2.14)　**問題**　上の 2 つの問題の結果を用いて、次の $\mathbb{Z}$ のイデアルの生成元を求めよ。
(1) $(2,3)$　(2) $(2)+(4)$　(3) $(2) \cap (3)$　(4) $(4) \cap (6)$　(5) $(2)(3)$
(6) $(4)(6)$

§3　剰余環

(3.1)　剰余環

R を環、I をその両側イデアルとするとき、加法群として I は R の正規部分群である (なぜか)。したがって、剰余類を加法的に、

$$\overline{x} = x + I \quad (x \in R)$$

と書くと、R/I の和を

$$\overline{x} + \overline{y} = \overline{x+y} \quad (\overline{x}, \overline{y} \in R/I)$$

と定めることで、加法に関する剰余群として R/I が構成できた。さらに、R/I の積を

$$\overline{x}\,\overline{y} = \overline{xy} \quad (\overline{x}, \overline{y} \in R/I)$$

で定めることができて ((3.2) 参照) 、これらの演算に関して R/I は環になる。これを R の I による**剰余環**と呼ぶ。

(3.2)　**問題**　R を環、I をその両側イデアルとする。このとき次を示し、R/I が環構造を持つことを証明せよ。
(1) $\overline{x}\,\overline{y} = \overline{xy}$ という演算は、代表元 x や y の選び方によらず、矛盾なく定まっていることを示せ。つまり、$\overline{x} = \overline{x'}$ かつ $\overline{y} = \overline{y'}$ ならば、$\overline{xy} = \overline{x'y'}$ であることを示せ。
(2) 和の単位元と、積の単位元を言え。
(3) 積が結合法則 (R2) を満たし、和と積が分配法則 (R4) を満たすことを示せ。

(3.3)　**問題**　剰余環 $\mathbb{Z}/(2)$ について答えよ。
(1) $\mathbb{Z}/(2)$ の元の個数を言え。
(2) $\mathbb{Z}/(2)$ の和について、$\overline{x} + \overline{y}$ $(\overline{x}, \overline{y} \in \mathbb{Z}/(2))$ の値をすべて列挙せよ。
(3) $\mathbb{Z}/(2)$ の積について、(2) と同じことをせよ。
(4) 零因子があるかどうか答えよ。

(3.4)　**問題**　剰余環 $\mathbb{Z}/(4)$ について (3.3) と同じことをせよ。

(3.5)　**問題**　m を整数とするとき次の問に答えよ。
(1) 剰余環 $\mathbb{Z}/(m)$ が整域 (零因子のない可換環) であるための必要十分条件は、「$m = 0$ または m が素数」であることを証明せよ。
(2) 剰余環 $\mathbb{Z}/(m)$ が体であるための必要十分条件は、「m が素数」であることを証明せよ。

(3.6)　**問題**　m を整数とし剰余環 $\mathbb{Z}/(m)$ を考える。$\overline{a} \in \mathbb{Z}/(m)$ が逆元を持つための必要十分条件は、「m と n が互いに素」であることを証明せよ。ただし、$m = 0$ のとき、m と n が互いに素であるとは、$n = \pm 1$ であることを言う。

(3.7)　**問題**　逆元を持つ元のことを**単元**と呼ぶ。上の問題を用いて次の剰余環の単元をすべて言え。
(1) $\mathbb{Z}/(8)$　(2) $\mathbb{Z}/(12)$

(3.8)　**問題**　次の剰余環の零因子をすべて言え。
(1) $\mathbb{Z}/(8)$　(2) $\mathbb{Z}/(12)$

(3.9)　**問題**　実数係数の多項式環 $\mathbb{R}[x]$ について次の問に答えよ。
(1) $\mathbb{R}[x]$ の単項イデアル (x) による剰余環 $\mathbb{R}[x]/(x)$ の元は、$\overline{a}$ $(a \in \mathbb{R})$ と書けることを証明せよ。
(2) 剰余環 $\mathbb{R}[x]/(x^2)$ の元は、$\overline{a + bx}$ $(a, b \in \mathbb{R})$ と書けることを証明せよ。
(3) $f \in \mathbb{R}[x]$ を、(0 次式ではない) 1 次式とするとき、剰余環 $\mathbb{R}[x]/(f)$ の元は、$\overline{a}$ $(a \in \mathbb{R})$ と書けることを証明せよ。
(4) $f \in \mathbb{R}[x]$ を、(1 次式ではない) 2 次式とするとき、剰余環 $\mathbb{R}[x]/(f)$ の元は、$\overline{a + bx}$ $(a, b \in \mathbb{R})$ と書けることを証明せよ。

(3.10)　**問題**　剰余環 $\mathbb{R}[x]/(x^2 + x)$ について答えよ。
(1) $\mathbb{R}[x]/(x^2 + x)$ は整域ではないことを証明せよ。
(2) $\mathbb{R}[x]/(x^2 + x)$ の 0 ではない零因子を 3 つ求めよ。

(3.11)　**問題**　剰余環 $\mathbb{R}[x]/(x^2 + x + 1)$ について答えよ。
(1) $\mathbb{R}[x]/(x^2 + x + 1)$ は整域であることを証明せよ。
(2) $\overline{x^2 + 1} \in \mathbb{R}[x]/(x^2 + x + 1)$ は単元であるが、その逆元を求めよ。

(3.12)　**問題**　剰余環 $\mathbb{R}[x]/(x^2 + 1)$ について答えよ。
(1) $\mathbb{R}[x]/(x^2 + 1)$ は整域か否か答えよ。
(2) $\overline{x} \in \mathbb{R}[x]/(x^2 + 1)$ が零因子かどうか答えよ。
(3) $\overline{x} \in \mathbb{R}[x]/(x^2 + 1)$ が単元かどうか答えよ。単元ならば逆元も答えよ。