代数学序論演習 II 講義ノート

2024 年 1 月 15 日

http://www.math.u-ryukyu.ac.jp/~suga/introalg/lecturenote2.pdf

序

以下は, 2023 年度, 琉球大学理学部数理科学科 2 年次対象の科目「代数学序論演習 II」の講義ノートである.

1 年次対象の線形代数学 I, II, 数学序論 I, II, 微分積分学 I,II, および, 代数学序論 I で講義されているであろう内容の証明で簡単なものは, 多くを省くか問としてある. 文中の問は授業においてその解答を発表すると, 評価点に加点する. また, そのための時間を, 授業において設ける.

黒字以外の文字はリンクなので, クリック (もしくはタップ) するとそこに飛びます.

文中の問

この講義は演習科目です. 文中の問はその解答を講義中に発表すれば, 評価に加点します. 問題に間違いがある場合は, その間違いを修正して発表してください.

参考書

環の参考書は多数あります. 来年度の代数学 (Galois 理論) に続けるには, [6], [7], [8] あたりが, 良い本だと思います. 単因子論については, [9], [10] を参考にして下さい.

注意

この文書は, まだ作成途中です. 間違っている内容が, 多数含まれている可能性があります. ダウンロードする際には, タイトル下の日付欄を見て下さい. 日付が以前のものと変わっていたら, 加筆や修正 (間違いの訂正) が行われています. 以下の更新履歴も常に確かめてください.

更新履歴

2023 年 9 月: 不完全なまま最初の公開.
2023 年 10 月 30 日: とりあえずの完成版. 以降は, ミスの訂正, 説明の加筆, 問題の追加等を行う.
2023 年 11 月 6 日: いくつかの問の問題文を訂正. 問 2.22 を追加.
2023 年 11 月 20 日: 細かいミスを訂正. 注意 3.3 を追加.
2023 年 12 月 12 日: 細かいミスを訂正. 3 節を修正, 加筆, 3.3.1 節を追加.

記号と言葉遣い

以下で用いる記号をまとめておく.

1. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ はそれぞれ, 自然数, 整数, 有理数, 実数, 複素数全体のなす集合とする. 自然数には, 0 を含めないとする.
2. 多項式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ に対して, $f(\theta) = 0$ となる $\theta \in \mathbb{C}$ を $f(x)$ あるいは f の根 (root) という.
3. 集合 A に対して, $|A|$ を A の濃度 (有限集合の場合は, 個数) とする. 集合の濃度については, 有限が無限かは問題にするが, 無限集合の濃度を問題にすることはない.
4. 共通部分を持たない和集合 (disjoint union) を記号 $\sqcup$ を用いて表す. すなわち, $A = B \sqcup C$ は, $A = B \cup C$ かつ $B \cap C = \emptyset$ の意味で用いる.
5. 集合 A から A への恒等写像を id_A と書く. すなわち, $\mathrm{id}_A : A \to A$, $\mathrm{id}(a) = a$, $a \in A$ である.
6. 集合 A, B と写像 $f : A \to B$ に対して, $f(A) = \mathrm{Im}(f) = \{f(x) \mid x \in A\} \subset B$ を f の像という. また, B の部分集合 C に対して, C の原像を $f^{-1}(C) = \{x \in A \,|f(x) \in C\}$ とする. 特に C が 1 点集合 $\{y\}$ のときには, $f^{-1}(\{y\}) = f^{-1}(y)$ と略記する. 同様に, 1 点集合の場合, 集合と元を区別しないで書くことは多くある.
7. A, B を集合とし, $f : A \to B$ を写像とする. $\mathrm{Im}(f) = B$ であるとき, f を全射, あるいは上への写像 (surjection) という. f が 1 対 1 の写像であるとき, f は単射であるとか, 中への写像 (injection) という. 特に, $A \subset B$ であるとき, A の元を B の元であると見る自然な単射がある. この写像は, 埋め込み (embedding) あるいは包含写像 (inclusion) という. 逆に, $f : A \to B$ が単射であるとき, $f(A) \subset B$ を A と同一視して, B の部分集合であると見ることもある. このときにも, f を埋め込みという. f が全射かつ単射であるとき, f は全単射 (bijection) であるという.
8. A, B を集合, $f : A \to B$ を写像とする. $C \subset A$ に対して f の C への制限で決まる写像を, $f_{|C} : C \to B$ と書く.
9. 整数 a, b に対して, $a \mid b$ は, a は b の約数 (b は a の倍数) を意味する. そうでないときは, $a \nmid b$ と書く. 0 はすべての整数の倍数であり, 0 でないどの整数の約数でもない. (a, b) は, a, b の最大公約数とする.
10. 虚数単位は i を用いる. 複素数 $z = a + bi \in \mathbb{C}$ $(a, b \in \mathbb{R})$ に対してその共役複素数を $\overline{z} = a - bi$ とする. 複素数 $z = a + bi$ の大きさ (ノルム) は, $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$ で定義される.
11. 数ベクトルは, $\boldsymbol{x}$ のように太文字で書くことにする.
12. $\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$ をクロネッカー (Kronecker) の記号として用いる.
13. (漢字圏以外の) 外国人の姓は基本的にアルファベット表記とした.

目次

0　代数学序論演習 I の問

以下の問は, 前学期の代数学序論演習 I の講義ノートにある問題で, 解答を発表されていない問題の抜粋です. 授業中に発表すれば, 評価に加点します.

問 0.1　1. 行列 A, B に対して, $\mathrm{rank}(AB) \leqq \max\{\mathrm{rank}A, \mathrm{rank}B\}$ を示せ.

2. $\det(AB) = \det A \det B$ を証明せよ.

3. $\mathbb{K}^n$ の n 個のベクトル $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ に対して, これらを列ベクトルとして作った行列 $A = (\ \boldsymbol{v}_1\ \cdots \boldsymbol{v}_n)$ が正則であることの必要十分条件は, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ が $\mathbb{K}^n$ の基底になることを示せ.

4. A を n 次正方行列とする.
   (a) P を正則行列とするとき, A の最小多項式と $P^{-1}AP$ の最小多項式は一致することを示せ.
   (b) A が対角化できるとし, A の固有値を $\lambda_1, \ldots, \lambda_n$ とするとき, A の最小多項式を求めよ.

5. $\boldsymbol{v}$, $\boldsymbol{w} \in \mathbb{R}^n$ に対して, これらのなす角を θ とするとき, $(\boldsymbol{v}, \boldsymbol{w}) = |\boldsymbol{v}||\boldsymbol{w}| \cos\theta$ が成立することを示せ.

6. $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ をベクトルとするとき, これらから作られる $m \times m$ 行列 $G = ((\boldsymbol{a}_i, \boldsymbol{a}_j))$ (ij 成分が内積 $(\boldsymbol{a}_i, \boldsymbol{a}_j)$ である行列) を Gram 行列, $\det G$ を Gram 行列式という. 次の問に答えよ.
   (a) $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ が一次独立である必要十分条件は, $\det G \neq 0$ であることであることを示せ.
   (b) $m = n$, $\boldsymbol{a}_i \in \mathbb{C}^n$ として, $A = (\boldsymbol{a}_1\ \boldsymbol{a}_2\ \ldots\ \boldsymbol{a}_n)$ とするとき, $\det G = |\det A|^2$ を示せ.

7. A が 3 次の直交行列で $\det A = 1$ とする. このとき, 行列式の値が 1 の直交行列 B をうまく選べば, ${}^tBAB = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$ とできることを示せ.

8. $X = (x_{ij})$ を n 次正方行列とした時, n^2 個の変数 x_{ij} に対して, $\mathrm{tr}(X^2)$ で定義される 2 次形式の符号を求めよ.

9. Hamilton の 4 元数 $\mathbb{H} \ni q = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mapsto \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in \mathbb{R}^4$ の対応で, $\mathbb{H}$ と $\mathbb{R}^4$ を同一視する.
   $\overline{q} = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$ と置く. 次を示せ.
   (a) 上の $\mathbb{R}^4$ の同一視で, $\mathbb{H}$ に標準内積を定義すると, その内積は, $\frac{1}{2}(q\overline{q'} + q'\overline{q})$ となることを示せ.
   (b) $\mathbb{H}^1 = \{q \in \mathbb{H} \mid |q| = 1\}$ とする. $q \in \mathbb{H}^1$, $x \in \mathbb{H}$ に対して, $q \cdot a = qx\overline{q}$ とおくと, これは, $\mathbb{H}$ を $\mathbb{R}^4$ と同一視したときに線形写像になり, さらに, $(qq') \cdot x = q \cdot (q' \cdot x)$, x, $y \in \mathbb{H}$ に対して, $(q \cdot x,\, q \cdot y) = (x,\, y)$ が成立することを示せ.
   (c) $W = \{b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}\} \subset \mathbb{H}$ とおくと, $q \in \mathbb{H}$, $w \in W$ に対して, $q \cdot w \in W$ となることを示せ.
   (d) (b), (c) より, $q \in \mathbb{H}^1$ と $w \in W$ に対して, $w \mapsto q \cdot w$ は, W の内積を変えない一次変換になる. 従って, W の正規直交基底 $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$ でこの写像を行列表示したとき, 3 次の直交行列になるが, その行列を $A(q)$ と書く. ((i), (ii), (iii) は独立に解答できる ((i) を解かなくても, (ii), (iii) は示せる.).
      i. (割と大変) $q = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ のとき $A(q)$ を求めよ.
      ii. $\det A(q) = 1$ を示せ (きちんと計算しても良いし, 手抜きで, 連続性とか連結性を用いて良い).

iii. $A(q) = E_3 \Longleftrightarrow q = \pm 1$ を示せ.

10. 次の集合は, 自然な和とスカラー倍で, $\mathbb{C}$ 上のベクトル空間になることを示せ.

(a) $\ell^1 = \left\{ \{a_n\}_{n=1,2,\ldots,} \mid \ a_n \in \mathbb{C},\ \sum_{k=1}^{\infty} |a_k| < \infty \right\}$

(b) $\ell^2 = \left\{ \{a_n\}_{n=1,2,\ldots,} \mid \ a_n \in \mathbb{C},\ \sum_{k=1}^{\infty} |a_k|^2 < \infty \right\}$

(c) $a,\ b \in \mathbb{R}$, $a < b$ とするとき, $L^\infty([a,b]) = \left\{ f : [a,b] \to \mathbb{C} \mid \sup_{x \in [a,b]} |f(x)| < \infty \right\}$

11. $\mathbb{C}$ 上の n 次元ベクトル空間 V を $\mathbb{R}$ 上のベクトル空間と見た時, $\dim_{\mathbb{R}} V = 2n$ を示せ.

1 内積とノルム

最初の節は, 代数学序論演習 I で講義できなかった内容のうち, 内積とノルムについて述べる.

この節では, $\mathbb{K}$ は $\mathbb{R}$ もしくは $\mathbb{C}$ とする. ベクトルの大きさを考えるのであるが, (大きさという概念が備わっている)$\mathbb{Q}$ を考えることは, この講義ではほとんどない.

1.1 内積

ベクトルの大きさを考えるのに最も素朴な方法は, 内積の性質を公理として定義して, それをベクトル空間に導入することである.

定義 1.1 $\mathbb{K} = \mathbb{C}$ または $\mathbb{K} = \mathbb{R}$ とし, V を $\mathbb{K}$ 上のベクトル空間とする. $\boldsymbol{u}$, $\boldsymbol{v} \in V$ に対して, $(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{K}$ が次を満たすとき, V 上の (Hermite) 内積という.

1. 任意の $\boldsymbol{v} \in V$ に対して, $(\boldsymbol{v},\ \boldsymbol{v})$ は非負の実数値で, $(\boldsymbol{v},\ \boldsymbol{v}) = 0$ が成立するのは, $\boldsymbol{v} = \boldsymbol{o}$ の場合に限る.
2. $\overline{(\boldsymbol{v}, \boldsymbol{u})} = (\boldsymbol{u}, \boldsymbol{v})$
3. $(\boldsymbol{u}, a\boldsymbol{v}) = a(\boldsymbol{u}, \boldsymbol{v})$, $a \in \mathbb{C}$
4. $(\boldsymbol{u}, \boldsymbol{v} + \boldsymbol{w}) = (\boldsymbol{u}, \boldsymbol{v}) + (\boldsymbol{u}, \boldsymbol{w})$

Hermite 内積が定義されているとき, $||\boldsymbol{v}|| = \sqrt{(\boldsymbol{v}, \boldsymbol{v})}$ を $\boldsymbol{v}$ のノルム (長さ) という.

ふたつのベクトル $\boldsymbol{u}$, $\boldsymbol{v}$ は, $(\boldsymbol{u}, \boldsymbol{v}) = 0$ のとき, 互いに直交するという.

命題 1.1 $a \in \mathbb{C}$ に対して, $(a\boldsymbol{u}, \boldsymbol{v}) = \overline{a}(\boldsymbol{u}, \boldsymbol{v})$

証明.

$$(a\boldsymbol{u}, \boldsymbol{v}) = \overline{(\boldsymbol{v}, a\boldsymbol{u})} = \overline{a(\boldsymbol{v}, \boldsymbol{u})} = \overline{a}\overline{(\boldsymbol{v}, \boldsymbol{u})} = \overline{a}(\boldsymbol{u}, \boldsymbol{v})$$

注意 1.1

1. 数ベクトル空間の場合と同様, ベクトルのスカラー倍の値が, 一方がそのままで, もう一方が複素共役で現れる. この, 複素共役を前の変数にするか, 後の変数にするかは, 両方の流儀が混在している. この講義では, 線形代数の教科書に従ったが, そうでないことも多い.
2. V が実ベクトル空間の場合, 内積の値も実数値になっている. この場合, 複素共役は現れない.

例 1.1 問 0.1, 10. の記号を用いる. 次は内積を定める.

1. 数ベクトル空間の内積.
2. $M_{m,n}(\mathbb{C})(m \times n$ 複素行列全体) を考えた時, $A,\ B \in M_{m,n}(\mathbb{C})$ に対して, $(A, B) = \mathrm{tr}({}^t\overline{A}B)$
3. $V = \ell^2$ とする. $u = (a_i),\ v = (b_i) \in \ell^2$ に対して, $(u, v) = \sum_{i=1}^{\infty} \overline{a}_i b_i$
4. $V = \mathbb{C}[X],\ V = C^0([a, b])$ の時, $(f, g) = \int_a^b \overline{f(x)} g(x) dx$.

問 1.1　1. 上の例 2. が内積になることを示せ.

2. 上の例 3. が内積を定めること, すなわち, $(a_i),\ (b_i) \in \ell^2$ なら, $\sum_{i=1}^{\infty} \overline{a}_i b_i < \infty$ を示せ.
3. 上の例 4. が内積になることを示せ.
4. V を内積を持つベクトル空間, $\boldsymbol{x} \in V$ とする. 任意の $\boldsymbol{v} \in V$ に対して $(\boldsymbol{x}, \boldsymbol{v}) = 0$ が成立するなら, $\boldsymbol{x} = \boldsymbol{o}$ を示せ (内積の非退化性).

次の性質は, 代数学序論演習 I の講義ノートの p. 9 問 1.9 と同じ内容である. この性質は, 抽象的なベクトル空間の内積でも成立する. 実際, 証明には, 内積の具体的な表示は不要で, 内積の定義に現れた式だけで可能だからである.

定理 1.1　次が成立する.

1. $(\boldsymbol{v}, \boldsymbol{w}) = \frac{1}{2}(|\boldsymbol{v} + \boldsymbol{w}|^2 - |\boldsymbol{v}|^2 - |\boldsymbol{w}^2|) + \frac{i}{2}(|\boldsymbol{v} - i\boldsymbol{w}|^2 - |\boldsymbol{v}|^2 - |\boldsymbol{w}|^2)$
   特に, $\mathbb{K} = \mathbb{R}$ なら, $(\boldsymbol{v}, \boldsymbol{w}) = \frac{1}{2}(|\boldsymbol{v} + \boldsymbol{w}|^2 - |\boldsymbol{v}|^2 - |\boldsymbol{w}^2|)$
2. $|(\boldsymbol{v}, \boldsymbol{w})| \leqq |\boldsymbol{v}||\boldsymbol{w}|$　(Cauchy–Schwarz の不等式)
3. $||\boldsymbol{v}| - |\boldsymbol{w}|| \leqq |\boldsymbol{v} + \boldsymbol{w}| \leqq |\boldsymbol{v}| + |\boldsymbol{w}|$　(3 角不等式)

定義 1.2　$\{\boldsymbol{v}_i\}$ が内積を持つベクトル空間の直交基底 (orthogormal basis) であるとは, 次が成立することを言う.

1. $\{\boldsymbol{v}_i\}$ は V の基底である.
2. $(\boldsymbol{v}_i,\ \boldsymbol{v}_j) = 0\ (i \neq j)$

さらに, $(\boldsymbol{v}_i, \boldsymbol{v}_i) = 1$ が $i = 1, \ldots, n$ について成立するとき, 正規直交基底 (orthonomal basis) という.

$\mathbb{K}^n(\mathbb{K} = \mathbb{R}, \mathbb{C})$ の標準基底は, 標準内積に対して正規直交基底である.

注意 1.2　正規直交基底という概念は, 次元によらず上のように定義できるが, 無限次元でこれが現れることはほぼ無い. 実際, $\ell^2 = \{(a_i)_{i=1,2,\ldots,} \mid \sum_{i=1}^{\infty} |a_i|^2 < \infty\ \}$ において, $e_i = (0, \ldots, 0, 1, 0, \ldots)(i$ 番目だけ 1) とすると, 例 1.1 の内積で, $(e_i, e_j) = \delta_{ij}$ である. しかし, $\{e_i\}$ は基底にならない. 実際 $(1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots) \in \ell^2$ であるが, これを e_i の (有限個の) 線形結合で書くことはできない.

問 1.2　$(1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots) \in \ell^2$ を示せ.

Gram–Schmidt の直交化

上の注意にもあるように, 無限次元で基底を考えるのは難しいので, 有限次元に話を限る.

V の基底 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ が与えられた時, これから正規直交基底を作り出す組織的な方法が Gram–Schmidt の直交化と呼ばれるものである. アルゴリズムとしては, 次の帰納的な方法である.

1. $\boldsymbol{u}_1 = \dfrac{\boldsymbol{v}_1}{|\boldsymbol{v}_1|} = \dfrac{\boldsymbol{v}_1}{\sqrt{(\boldsymbol{v}_1, \boldsymbol{v}_1)}}$ とする.

2. $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$ から正規直交基底 $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k\}$ を作ったとき,

$$\boldsymbol{v}'_{k+1} = \boldsymbol{v}_{k+1} - (\boldsymbol{v}_{k+1}, \boldsymbol{u}_1)\boldsymbol{u}_1 - \cdots - (\boldsymbol{v}_{k+1}, \boldsymbol{u}_k)\boldsymbol{u}_k$$

と置くと, $\boldsymbol{v}'_{k+1} \neq \boldsymbol{o}$, $(\boldsymbol{v}'_{k+1}, \boldsymbol{u}_i) = 0$, $(i = 1, \ldots, k)$ が成立するので,

$$\boldsymbol{u}_{k+1} = \frac{\boldsymbol{v}'_{k+1}}{|\boldsymbol{v}'_{k+1}|} = \frac{\boldsymbol{v}'_{k+1}}{\sqrt{(\boldsymbol{v}'_{k+1}, \boldsymbol{v}'_{k+1})}}$$

とする.

問 1.3 $P_2(\mathbb{C}) = \{ax^2 + bx + c \mid a, b, c \in \mathbb{C}\}$ を複素数係数の 3 次以下の多項式がなす $\mathbb{C}$ 上のベクトル空間とする. $P_2(\mathbb{C})$ の基底 $\{1, x, x^2\}$ を次の内積に対して Gram–Schmidt の直交化を施せ.

1. $(f, g) = \displaystyle\int_{-1}^{1} \overline{f(x)} g(x) dx$ (結果は, Legendre(ルジャンドル) の多項式の定数倍)
2. $(f, g) = \displaystyle\int_{-\infty}^{\infty} \overline{f(x)} g(x) e^{-x^2} dx$ (Hermite の多項式の定数倍)

注意 1.3 上の問 1.3 の様に, 多項式の空間に様々な内積を定義することができる (多くは積分を利用して). その際に直交する多項式の列を得るが, これらは直交多項式系と呼ばれ, 様々な応用がある.

定義 1.3 V, W を内積を持つベクトル空間とし, $f : V \to W$ を線形写像とする. 任意の $\boldsymbol{u}, \boldsymbol{v} \in V$ に対して, $(f(\boldsymbol{u}), f(\boldsymbol{v})) = (\boldsymbol{u}, \boldsymbol{v})$ が成立するとき, 等長線形写像という. さらに, f が全単射なら, 等長同型という.

内積を持つ n 次元ベクトル空間 V に正規直交基底 $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ を定めると, $\boldsymbol{v} \in V$ の基底に対する座標を $\boldsymbol{v} = x_1\boldsymbol{v}_1 + \cdots + x_n\boldsymbol{v}_n$ とすると, 対応

$$V \ni \boldsymbol{v} \ \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n$$

は, V から標準内積を入れた $\mathbb{K}^n$ への等長写像を定める.

$f : V \to W$ が等長線形写像なら, $\boldsymbol{v} \in V$ に対して $|f(\boldsymbol{u})| = |\boldsymbol{u}|$ が成立する. これが等長という言葉の由来である. ただし, 任意の $\boldsymbol{u}$ に対して $|f(\boldsymbol{u})| = |\boldsymbol{u}|$ (等長という文字からするとこちらを定義にしたい) が成立するとき, 写像 f が等長線形写像になるかということに関しては, 実ベクトル空間では成立するが, 複素ベクトル空間では反例がある.

問 1.4 1. 等長線型写像は単射であることを示せ.

2. $\mathbb{C}^n$ に自然な内積を入れて, $f : \mathbb{C}^n \to \mathbb{C}^n$ を写像とする. $|f(\boldsymbol{u})| = |\boldsymbol{u}|$ が任意の $\boldsymbol{u} \in \mathbb{C}^n$ について成立するが, 線形写像ではないものの例を与えよ.

定義 1.4（直交補空間）　V を内積 (,) を持つベクトル空間とし, W を部分空間とする. このとき,

$$W^{\perp} = \{\boldsymbol{v} \in V \mid (\boldsymbol{w}, \boldsymbol{v}) = 0,\ \forall \boldsymbol{w} \in W\}$$

を W の直交補空間という.

次の命題の証明は, 数ベクトル空間と全く同じである.

命題 1.2　V が有限次元ベクトル空間で, $W \subset V$ を部分空間とすると, $V = W \oplus W^{\perp}$.

注意 1.4　上で, 有限次元という仮定は重要である. 無限次元では, 上は成り立たない. 実際, $V = \ell^2$ として, $e_i \in \ell^2$, $i = 1, 2, \ldots$ を注意 1.2 の元とし, $W =< \{e_i\}_{i=1,2,\ldots} >$ とする. このとき $W^{\perp} = \{\boldsymbol{o}\}$ となる. しかし, 注意 1.2 のように, $W \neq \ell^2$ である.

問 1.5　命題 1.2 の証明を書け.

上のように無限次元では, 代数的な議論 (有限和だけで収束を考えない議論) では, うまくいかない事が多く, 収束の概念を定義して無限和も考える事が多い.

対称変換, Hermite 変換, ユニタリ変換, 直交変換

定義 1.5　V を内積 (,) を持つベクトル空間とし, $T : V \to V$ を V の線形変換とする.

1. 任意の $\boldsymbol{u}, \boldsymbol{v} \in V$ に対して, $(T^*\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}, T\boldsymbol{v})$ が成立するとき, 写像 $T^* : V \to V$ を T の随伴 (adjoint) という.
2. V が実ベクトル空間で, $(T\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}, T\boldsymbol{v})$ が任意の $\boldsymbol{u}, \boldsymbol{v} \in V$ について成立するとき, T を対称変換という.
3. V が実ベクトル空間で, $(T\boldsymbol{u}, T\boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{v})$ が任意の $\boldsymbol{u}, \boldsymbol{v} \in V$ について成立するとき, T を直交変換という.
4. V が複素ベクトル空間で, $(T\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}, T\boldsymbol{v})$ が任意の $\boldsymbol{u}, \boldsymbol{v} \in V$ について成立するとき, T を Hermite 変換 (あるいは, 自己共役, self-adjoint) という.
5. V が複素ベクトル空間で, $(T\boldsymbol{u}, T\boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{v})$ が任意の $\boldsymbol{u}, \boldsymbol{v} \in V$ について成立するとき, T をユニタリ (unitary) 変換という.

問 1.6　T の随伴 T^* は線形写像になる事を示せ.

問 1.7　複素係数の多項式全体のなすベクトル空間 $\mathbb{C}[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{C}\}$ を考える.

1. 内積を $(f, g) = \displaystyle\int_{-1}^{1} \overline{f(x)} g(x) dx$ で定義するとき, $T(f) = (1 - x^2) f'' - 2x f'$ は Hermite 変換になることを示せ.
2. 内積を $(f, g) = \displaystyle\int_{-\infty}^{\infty} \overline{f(x)} g(x) e^{-x^2} dx$, $f, g \in \mathbb{C}[x]$ で定義するとき, $T(f) = f'' - 2x f'$ は Hermite 変換になることを示せ.

上の定義の言葉遣いは, 有限次元ベクトル空間のときに用いられる言葉であるが, 無限次元の場合, 変換ではなく「作用素 (operator)」という言葉が用いられる.

固有値と固有ベクトル

V をベクトル空間として, $T : V \to V$ を線形変換とする. $\lambda \in \mathbb{K}$ に対して, $T(\boldsymbol{v}) = \lambda \boldsymbol{v}$, $\boldsymbol{v} \neq \boldsymbol{o}$ となる時, λ を T の固有値, $\boldsymbol{v}$ を T の固有値 λ に対する固有ベクトルという.

問 1.8 V を内積を持つ $\mathbb{R}$ もしくは $\mathbb{C}$ 上のベクトル空間とする. 次の問に答えよ.

1. $T : V \to V$ が Hermite 変換 ($\mathbb{K} = \mathbb{C}$) もしくは対称変換 ($\mathbb{K} = \mathbb{R}$) のとき, T の固有値は実数になることを示せ.
2. 問 1.3, 問 1.7 の記号を用い, $P_2(\mathbb{C}) = \{\, ax^2 + bx + c \mid a, b, c \in \mathbb{C} \,\}$ とする.
   (a) $T(f) = (1 - x^2)f'' - 2xf'$ の $P_2(\mathbb{C})$ での固有値と固有ベクトルを求めよ.
   (b) $T(f) = f'' - 2xf'$ の $P_2(\mathbb{C})$ での固有値と固有ベクトルを求めよ.
   (固有ベクトルは, 問 1.3 の定数倍になります.)

1.2 ノルム

上で述べたように, 内積を持てば長さを決めることができるが, 内積が自然に定義できないベクトル空間でも長さを考えたいことがある. 「ベクトルの長さ」を公理化したものが, これから定義するノルム (norm) である.

定義 1.6 $\mathbb{K}$ を $\mathbb{R}$ または $\mathbb{C}$ とする. V を $\mathbb{K}$ 上のベクトル空間とし, V から $\mathbb{R}$ への写像 $\boldsymbol{v} \mapsto ||\boldsymbol{v}||$ が次の性質を満たすとき, ノルム (norm) という.

1. $||\boldsymbol{v}|| \geqq 0$ で, $||\boldsymbol{v}|| = 0$ となるのは, $\boldsymbol{v} = \boldsymbol{o}$ のときに限る.
2. $a \in \mathbb{K}$, $\boldsymbol{v} \in V$ に対して, $||a\boldsymbol{v}|| = |a|\,||\boldsymbol{v}||$.
3. $\boldsymbol{v}, \boldsymbol{w} \in V$ に対して, $||\boldsymbol{v} + \boldsymbol{w}|| \leqq ||\boldsymbol{v}|| + ||\boldsymbol{w}||$ (3 角不等式).

注意 1.5 $||\boldsymbol{v}|| \geqq 0$ は他の公理から導出できる. 実際, 次を見れば良い.

$$0 = ||\boldsymbol{o}|| = \left|\left|\frac{1}{2}\boldsymbol{v} - \frac{1}{2}\boldsymbol{v}\right|\right| \leqq \left|\left|\frac{1}{2}\boldsymbol{v}\right|\right| + \left|\left|-\frac{1}{2}\boldsymbol{v}\right|\right| = \frac{1}{2}||\boldsymbol{v}|| + \frac{1}{2}||\boldsymbol{v}|| = ||\boldsymbol{v}||$$

しかし, ノルムの正値性を強調する意味で, 通常は公理に書かれる.

内積が定義された空間では, 内積から定まるベクトルの大きさ (長さ) はノルムの公理を満たす. $\mathbb{K} = \mathbb{R}$ のとき, 内積から決まるノルムの事を, Euclid ノルムと言う. しかし, そのような空間でも別のノルムを考えることもある. さらに, 内積が定義されていなくとも, ノルムが定義できる空間もある.

問 1.9（ノルムの例） 問 0.1 の記号を用いる. 次は, 与えられた空間のノルムである事を示せ.

1. $V = \mathbb{K}^n \ni \boldsymbol{x} = (x_i)$ に対して, $||\boldsymbol{x}||_1 = |x_1| + \cdots + |x_n|$
2. $V = \mathbb{K}^n \ni \boldsymbol{x} = (x_i)$ に対して, $||\boldsymbol{x}||_\infty = \max_i\{|x_i|\}$
3. (行列の作用素ノルム) $V = M_{m,n}(\mathbb{K}) \ni A$ に対して, $||A|| = \sup_{\boldsymbol{x} \in \mathbb{R}^n,\, |\boldsymbol{x}|=1} |A\boldsymbol{x}|$. ここで, $|\boldsymbol{x}|$, $|A\boldsymbol{x}|$ はそれぞれ, $\mathbb{K}^n$, $\mathbb{K}^m$ 内積から定まるノルム ($\mathbb{K} = \mathbb{R}$ または $\mathbb{C}$).
4. $\ell^\infty \ni \boldsymbol{v} = (a_i)$ に対して, $||\boldsymbol{v}||_\infty = \sup_i |a_i|$

5. $\ell^1 \ni \boldsymbol{v} = (a_i)$ に対して, $||\boldsymbol{v}||_1 = \sum_i |a_i|$
6. $L^\infty([a,b]) \ni f$ に対して, $||f||_\infty = \sup_{x\in[a,b]} |f(x)|$

V にノルム $||\ ||$ が定義されると, $\boldsymbol{v}, \boldsymbol{w} \in V$ に対して, $d(\boldsymbol{v},\boldsymbol{w}) = ||\boldsymbol{v}-\boldsymbol{w}||$ とおくと, d は V に距離を定め, V は距離空間になる (幾何序論で距離空間は講義されると思う). これにより,「ベクトル列の収束」などが定義され, 解析学に応用される. これについては, この講義の範疇を超えるので, これ以上は述べない.

問 1.10　上で述べた, $d(\boldsymbol{x},\boldsymbol{y})$ は V 上の距離を定めることを示せ.

注意 1.6　符号理論で現れる有限体上のベクトル空間においても, 内積や距離の概念が定義され, 誤り訂正符号等に応用される. 但し, それらは, これまでの定義とは微妙にずれた定義になる.

2　環と加群

この節では, 有限生成アーベル群の基本定理や Jordan 標準形の理論を統一的に導く単因子論を述べる準備として, 環と加群についての初等的な内容を述べる.

2.1　環 (言葉遣いについて少し)

単因子論では, 多項式を成分に持つ行列などを扱う. 実際, 単因子論では, 考える行列の成分は単項イデアル整域の元なのであるが, まずは, この言葉の意味を解説していく.

定義 2.1 (環)　集合 R が (単位元を持つ) 環 (ring) であるとは, R に加法 $R\times R \to R,\ (a,b)\mapsto a+b$ と乗法 $R\times R\to R,\ (a,b)\mapsto ab$ が定義されており, 次を満たすことを言う.

1. R は加法において, 可換群をなす. 加法に関する単位元は 0 と記す.
2. $(ab)c = a(bc),\ a,b,c\in R$. すなわち, R の乗法は結合律を満たす.
3. $1\in R$ が存在して, $a1 = 1a = a,\ \forall a\in R$. すなわち, 乗法における単位元が存在する.
4. $a(b+c) = ab+ac,\ (a+b)c = ac+bc,\ \forall a,b,c\in R$ (分配律).

R の乗法が可換であるとき, R を**可換環 (commutative ring)** という.

注意 2.1
1. 環に対して, 単位元の存在を仮定しないこともある (解析学系で出てくる) が, 下の例 2.1 以外は, この講義では扱わない.
2. 昔 (といっても 50 年くらい前まで) は, 和と積の 2 種類の演算が定義されている代数系を, 一般的に環と呼んでいた (日本だけでなく外国でも). 例えば Lie 環, Jordan 環[*1], C^*-環などである. 現在はこのような代数系は, 基本的に Lie 代数, Jordan 代数, C^*-代数と呼ばれているが, 今でも話し言葉では Lie 環, Jordan 環, C^*-環と言うことがある. [*2]

[*1] Jordan は Jordan 標準形の人とは別人の物理学者, 物理の人はヨルダンとドイツ語読みしている.
[*2] 英語などでも, Lie ring → Lie algebra と, ring から algebra に言葉が変化している. 特に, 日本語だと,「だいすう」というより「かん」といった方が短くて言いやすいのが理由ではないかと思う. ちなみに Hecke 環は, ここの定義どおりの環であるが, 現在でも, Hecke algebra と呼ばれたり, Hecke ring と呼ばれたりする (日本語だと Hecke 環ということの方が多い).

例 2.1（乗法の単位元の存在以外は，可換環の公理を満たす代数系の例）

$$C_0(\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{C} \mid f \text{ は連続かつ } \mathrm{supp}(f) \text{ はコンパクト} \}$$

とおく．ここで $\mathbb{R}$ 上の関数 f に対して，$\mathrm{supp}(f) = \overline{\{x \in \mathbb{R} \mid f(x) \neq 0\}}$ (上付きのバーは，閉包の意味) で，f の台 (support) と呼ばれる集合である．$C_0(\mathbb{R})$ は通常の関数の和と積で積の単位元の存在以外の可換環の公理を満たす．積の単位元は，存在するなら 1 という定数関数であるが，この関数の台はコンパクトではない．

$C_0(\mathbb{R})$ には，合成積 (convolution) と呼ばれる積が入り，その積を用いても，単位元のない可換環になる (単位元を無理に入れようとすると，Dirac(ディラック) の δ 関数と呼ばれる「超関数」が必要になる)．合成積 (合成積の演算記号は $*$ が通常用いられる) は，次で定義される．

$$(f * g)(x) = \int_{-\infty}^{\infty} f(x-y)g(y)dy$$

前期の講義ノート p. 28, 定義 4.1 で体の定義があるが，環は体の定義から「0 でない元が乗法の逆元を持つ」の部分を抜いたものである．すなわち，体は環である．当然逆は成立しない．

例 2.2　1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

2. $\{0\}$ は $(1 = 0$ と見て) 環とみなすことができる．これを零環という．これ以外の環では，$0 \neq 1$ となる．
3. R を環とするとき，$R[X] = \left\{ \sum_{\text{有限和}} a_i X^i \mid a_i \in R \right\}$ を R 上の 1 変数多項式環という．積は，$X^i X^j = X^{i+j}$, $aX = Xa$, $(a \in R)$ という規則で入れる．R が可換環なら，$R[X]$ も可換環である．X は不定元 (indeterminate) という．
4. R を環，$X_1, \ldots, X_l$ を l 個の不定元とするとき，n 変数多項式環 $R[X_1, \ldots, X_l]$ が同様に定義される．$R[X_1, \ldots, X_{l-1}][X_l] = R[X_1, \ldots, X_l]$ と，l について帰納的に定義しても良い．
5. R を可換環とするとき，$M_n(R) = \{$ 成分が R の元である $n \times n$ 行列 $\}$ とおく．通常の行列の積と和で環になる．$n \geqq 2$ であるとき，これは非可換な環になる．(成分が非可換な環の元である行列を考えないこともないが，行列式の定義などが大変になるので，この講義では取り扱わない.)

例 2.3（形式的冪級数環）　R を環，X を不定元とする．次の集合の元を，R 係数の形式的冪級数という．

$$R[[X]] = \{ \sum_{n \geqq 0,\ \text{形式和}} a_n X^n \mid a_n \in R \}$$

形式和という意味は，$\sum_{n \geqq 0} a_n X^n$ は無限和ではあるが，収束は考えないという事である．基本的に R の元の数列 $a_0, a_1, \ldots$ を考えている事と同じである．X という不定元を入れるのは，解析関数の Maclaurin 展開との類似性を引きずっているからである．$R[[X]]$ に $X^i X^j = X^{i+j}$ の規則で積を入れると，$R[[X]]$ は環になる．$a(X) = \sum a_n X^n$, $b(X) = \sum b_n X^n$, $a(X)b(X) = \sum c_n X^n$ とすると，$c_n = \sum_{i=0}^{n} a_i b_{n-i}$ となるので，積の計算に無限和は現れない (i.e. 積はきちんと定義される)．不定元の個数を増やして，n 変数冪級数環 $R[[X_1, \ldots, X_n]]$ も同様に定義される．

問 2.1　1. 零環以外では，$0 \neq 1$ が成立することを示せ．

2. 例 2.1 で，合成積が定義できること，すなわち，$f, g \in C_0(\mathbb{R})$ なら，$f * g \in C_0(\mathbb{R})$ となること，および，これが可換な演算であることを示せ．

R を環, $R[X]$ を R 上の多項式環とし, $f = \sum a_i X^i \in R[X]$ としたとき, $\deg f = \max\{i \mid a_i \neq 0\}$ とおき (すなわち, $a_i \neq 0$ となる最大の次数), f の次数という. ただし, $\deg 0 = -\infty$ と約束する.

R を環とするとき, 積に関して可逆な元全体の集合を,

$$R^\times = \{x \in R \mid y \in R \text{ が存在して, } xy = yx = 1\}$$

とおく, $R^\times$ の元を R の単元あるいは可逆元という. $R^\times$ は積に対して群をなす. これを R の単元群 (unit group) という.

問 2.2 R を可換環としたとき, $M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}$ を示せ. この集合を $GL_n(R)$ と書き, R 上の一般線形群 (general linear group) という.

環の準同型写像についても, 群と同様に定義される. ただし, 群のときと違い, 環の場合 $f(1) = 1$ という性質は,「演算を保つ」ということから導くことができない. したがって, この性質を定義に加えておく.

定義 2.2 R, R' を環とし, $f : R \to R'$ を写像とする. 次の性質を持つとき, f は環の準同型写像という.

1. $f(a+b) = f(a) + f(b), \qquad a, b \in R$
2. $f(ab) = f(a)f(b), \qquad a, b \in R$
3. $f(1) = 1$

さらに f が全単射であるとき, f は同型写像という. 同型写像 $f : R \to R'$ が存在するとき, R と R' は同型であるといい, $R \cong R'$ と書く.

注意 2.2 上の定義では, 零写像, すなわち $f(x) = 0,\ \forall x \in R$ は, $R' = \{0\}$ のときだけ準同型写像になる.

問 2.3 R, R' を (単位元を持つ) 環とする. $f : R \to R',\ (f \neq 0)$ で, 上の定義の 1., 2. を満たすが, 3. を満たさない写像の例を作れ.

2.2 基本事項

以下, R は常に単位元を持つ環とする. 可換環を主に扱い, 述べてある内容は可換環の初歩的な内容が中心である (特に例は, ほぼ可換環について書いてある). 環の例は, 例 2.2 に挙げた以外にも, 下の例のような, $\mathbb{Z}$ に整数係数代数方程式の根を付け加えてできる環も考えることが多い.

例 2.4
1. $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ (Gauss の整数環, $\sqrt{-1}$ は $x^2 + 1 = 0$ の根)
2. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$
3. $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

整数環や 1 変数多項式環で成り立つ性質が, 一般の (可換) 環でどの程度類似のことが成立するか? という問題意識が, 環の性質を調べる第一歩である.

問 2.4
1. $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}$ を示せ.
2. $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ を示し, これを利用して, $\left|\mathbb{Z}[\sqrt{2}]^\times\right| = \infty$ を示せ.

定義 2.3 R を可換環とし $R \ni a \neq 0$ とする. $0 \neq b \in R$ が存在し, $ab = 0$ となるとき, a, b を R の零因子

(zero divisor) という. 可換環 R は, 零因子を持たないとき, R を整域 (integral domain) という.

非可換な環に対しては, 右零因子, 左零因子が同様に定義される.

R を可換環とし $a, b \in R$ とする. R が整域なら, $ab = 0$ から $a = 0$ または $b = 0$ が従う. このノートでは, 整域という言葉は, 常に可換環に対して用いることにする.

問 2.5　1. 例 2.4 に挙げた環は, すべて整域になることを示せ.

2. R を環 a, b, $c \in R$ とする. R が整域かつ $a \neq 0$ なら, $ab = ac \Rightarrow b = c$ が成立する事を示せ.
3. 有限個の元からなる整域は体になることを示せ. (特に $\mathbb{Z}/n\mathbb{Z}$ は整域なら体である.)
4. R を可換環, $R[X]$ を R 上の 1 変数多項式環とするとき, $R[X]$ が整域である条件は, R が整域であることを示せ.
5. R, R' を環, $f : R \to R'$ を写像とし, $f \neq 0$ とする. R' が整域なら, $f(ab) = f(a)f(b)$ から $f(1) = 1$ が従うことを示せ.

定義 2.4　R を環, $S \subset R$ とする. S が R の部分環であるとは, 次が成立することを言う.

1. $a, b \in S \Longrightarrow a \pm b \in S,\ ab \in S$
2. $1 \in S$

注意 2.3　群とは異なり, 単に演算で閉じているだけでは, 部分環とは言わない. 例えば, 偶数の集合 $2\mathbb{Z}$ は, 和 (差) と積の演算で閉じているが, 1 を含まないので, $\mathbb{Z}$ の部分環とは言わない.

例 2.5　$R[X]$ で, R を定数多項式 (次数 0 の多項式) の全体と同一視すると, R は $R[X]$ の部分環である.

定義 2.5 (環の直和 (非可換な環でも, 直和は同じ定義))　$R_1, \ldots, R_n$ を可換環とするとき, これらの加法群としての直積を, $R_1 \oplus \cdots \oplus R_n$ と書く.

$$R_1 \oplus \cdots \oplus R_n = \{(a_1, \ldots, a_n) \mid a_i \in R_i\}$$

和を, 加法群としての直積群の演算で定義し, 積も成分ごとの積として定義する.

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$

この演算で, $R_1 \oplus \cdots \oplus R_n$ は単位元 $(1, \ldots, 1)$ を持つ可換環になる. これを, $R_1, \ldots, R_n$ の直和という.

注意 2.4　群の直積とは異なり, 上で, 各成分 R_i は $R_1 \oplus \cdots \oplus R_n$ の部分環ではない. 積の単位元が異なるからである. R_i の単位元 1_{R_i} を $R_1 \oplus \cdots \oplus R_n$ の元 $e_i = (0, \ldots, 0, 1_{R_i}, 0, \ldots, 0)$ と同一視すると. これは, 直和の単位元ではないが, $e_i^2 = e_i$ を満たす. このように, 2 乗しても変化しない環の元を, **ベキ等元**という.

問 2.6　R_1, R_2 を可換環とするとき, 単元群について, $(R_1 \oplus R_2)^\times \cong R_1^\times \times R_2^\times$ が成立することを示せ. ここで, 右辺は群の直積である.

2.3　イデアルと剰余環, 可換環の準同型定理

環の準同型写像や, 環の同型については, 定義 2.2 で定義してあるので, 改めて述べない.

定義 2.6　可換環 R の部分集合 I が次の条件を満たすとき, I を R のイデアルであるという.

1. I は R の加法群の部分群である.
2. 任意の $r \in R$, $a \in I$ に対して, $ra \in I$

注意 2.5　可換環を考えているので, イデアルに左右の区別はないが, 非可換環では, 「右イデアル」「左イデアル」「両側イデアル」の 3 通りが考えられる. (非可換環では, 上の定義は, 左イデアルの定義になる.) 下の剰余環や準同型定理は, イデアルを「両側イデアル」に置き換えれば, 非可換環でもそのまま成立する.

環論ではイデアルを調べることが, 環の性質の解明につながることが知られているので, 以下, イデアルについての様々な性質を順に述べていく. もともとイデアルは整数環 $\mathbb{Z}$ の素因数分解を他の環に拡張するために, Kummer(クンマー) によって導入された.

例 2.6　　1.　R 及び $\{0\}$ はイデアルである. これらを自明なイデアルという.
2.　$\mathbb{Z}$ において, $n \in \mathbb{Z}$ に対して, n の倍数全体 $n\mathbb{Z} = \{\, na \,|\, a \in \mathbb{Z}\}$ はイデアルになる.

問 2.7　イデアル I に対して, $I = R$ であるための必要十分条件は, $I \ni 1$ であることを示せ.

I を可換環 R のイデアルとする. 加法群としての商群 R/I に積を,

$$(a + I)(b + I) = ab + I, \quad a, b \in R$$

で定義する. これは, 代表元の取り方によらず, well–defined である. 実際, $a - a' \in I$, $b - b' \in I$ とすると,

$$ab - a'b' = a(b - b') + (a - a')b' \in I$$

が得られる. この積において, $1 + I$ が積の単位元の性質を持つことは, 明らかである. また, 積の結合律, 交換律, 分配律は, もとの R のそれから従う. このように, R/I に環の構造を入れたものを, R の I による剰余環という. 前期の講義と同様に, $a \in R$ に対して, $a + I \in R/I$ を $\overline{a}$ とも書くことにする.

例 2.7　$n \in \mathbb{N}$ とするとき, $\mathbb{Z}/n\mathbb{Z}$ は, 代数学序論 I で学習したと思う. これが,「環」という言葉の語源である (アナログ時計の文字盤は, $\mathbb{Z}/12\mathbb{Z}$ を表しており, 円環状に並んでいる.).

問 2.8　$(\mathbb{Z}/n\mathbb{Z})^\times = \{\, \overline{a} \mid (a, n) = 1 \,\}$ を示せ. ここで, (a, n) は a と n の最大公約数.

定義 2.7　$n \in \mathbb{N}$ に対して, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ を Euler(オイラー) の関数という.

定理 2.1**（可換環の準同型定理）**　R, R' を可換環とし, $f : R \to R'$ を準同型写像とする. このとき, 次が成立する.

1. $f(R) = \mathrm{Im}(f)$ は R' の部分環である.
2. $f^{-1}(0) = \mathrm{Ker}(f)$ は R のイデアルである.
3. 自然な可換環の同型写像 $\overline{f} : R/\mathrm{Ker}(f) \xrightarrow{\simeq} \mathrm{Im}(f)$ が存在する

証明.　1.　$f(1) = 1$ より, $1 \in \mathrm{Im}(f)$ である. $a', b' \in \mathrm{Im}(f)$, $a' = f(a)$, $b' = f(b)$ とすると, $a' + b' = f(a + b) \in \mathrm{Im}(f)$, $a'b' = f(ab) \in \mathrm{Im}(f)$ より, $\mathrm{Im}(f)$ は部分環になる.

2.　f は加法群としての準同型写像なので, $\mathrm{Ker}(f)$ は R の加法群の部分群になる. $a \in \mathrm{Ker}(f)$, $r \in R$ に対して, $f(ra) = f(r)f(a) = 0$ なので, $ra \in \mathrm{Ker}(f)$ となり, $\mathrm{Ker}(f)$ は R のイデアルである.

3. 群の準同型定理から, 加法群として自然な同型写像 $\overline{f} : R/\mathrm{Ker}(f) \xrightarrow{\simeq} \mathrm{Im}(f)$ が存在する. これが環の準同型であることは, 剰余環の積の定義から明らかである.

2.4 イデアルの演算と孫子の剰余定理

R を可換環, $S \subset R$ を部分集合とする.

$$RS = (S) = \left\{ \sum_{\text{有限和}} r_i s_i \mid r_i \in R,\, s_i \in S \right\} = \bigcap_{\substack{S \subset I \\ I \text{ はイデアル}}} I$$

とおく. すなわち, (S) は集合 S を含む最小のイデアルである. これを S から生成されたイデアルという.

S が一点集合 $\{a\}$ であるとき, (S) を (a) と書く. このようにただ 1 つの元から生成されるイデアルを, **単項イデアル**, あるいは主イデアル (対応する英語 principal ideal の日本語訳) という.

I, J を可換環 R のイデアルとする. このとき, $I \cap J$ はイデアルになる. また,

$$I + J = \{a + b \mid a \in I,\, b \in J\}$$

もイデアルになる. これを, イデアル I, J の和という.

イデアル I, J に対して, I, J の積を I の元と J の元の積から生成されるイデアルと定義する. 実際には, 次の集合に一致することは, 容易にわかる.

$$IJ = \left\{ \sum a_i b_i \mid a_i \in I,\, b_i \in J \right\}$$

また, $IJ \subset I \cap J$ であることも, 容易にわかる. 同じイデアルの積については, $II = I^2, III = I^3, \cdots$ という記号を用いる.

問 2.9　1. $\mathbb{Z}$ のイデアル I, J で $I \cup J$ がイデアルとなる例, ならない例を挙げよ.

2. $a, b \in \mathbb{Z}$ として, 単項イデアル $(a), (b)$ について, $(a) + (b)$, $(a)(b)$ を求めよ (共に単項イデアルとなるので, その生成元を求めよ).
3. $\mathbb{Z}$ において, $(a)(b) \subsetneqq (a) \cap (b)$ となる例を与えよ.
4. I を可換環 R のイデアルとするとき,

$$\sqrt{I} = \mathrm{rad}(I) = \{x \in R \mid \text{ある自然数 } n \text{ が存在して}, x^n \in I\}$$

も R のイデアルになることを示せ. このように定まる $\sqrt{I}$ をイデアル I の根基 (radical) という. 自明なイデアル $\{0\}$ の根基, $\sqrt{0}$ をべき零根基 (nilradical) という.

可換環 R の非自明なイデアル I, J は $I + J = R$ が成立するとき, **互いに素である**という.

問 2.10　1. $\mathbb{Z}$ のイデアル $m\mathbb{Z}$ と $n\mathbb{Z}$ が互いに素であることと, m, n が互いに素 (最大公約数が 1) な整数であることは, 同値であることを示せ.

2. 可換環 R のイデアル I, J が互いに素なら, $IJ = I \cap J$ が成立することを示せ.

互いに素なイデアルに対しては, 次の定理が成立する. 定理の名称は, 孫子算経という 5 世紀頃の中国の算術書に由来する.

定理 2.2（Chinese Remainder Theorem (中国式剰余定理, あるいは孫子の剰余定理)） R を可換環とし, $I_1, \ldots, I_n$ を R の互いに素なイデアルとする. すなわち, $i \neq j$ なら, $I_i + I_j = R$ がすべての i, j について成立しているとする. このとき, 次が成立する.

1. $I_i + \bigcap_{j \neq i} I_j = R$
2. 任意の $a_1, \ldots, a_n \in R$ に対して, $a \in R$ が存在して, $a - a_i \in I_i$ がすべての i について成立する.
3. $I = \bigcap_{i}^{n} I_i$ とすると, $R/I \cong R/I_1 \oplus \cdots \oplus R/I_n$.

証明. 1. i を固定する. すべての j $(\neq i)$ に対して, $I_i + I_j = R$ なので, j ごとに $u_j + v_j = 1$, $u_j \in I_i, v_j \in I_j$ となる u_j, v_j が取れる. このとき,

$$\begin{aligned} 1 &= (u_1 + v_1)(u_2 + v_2) \cdots (u_{i-1} + v_{i-1})(u_{i+1} + v_{i+1}) \cdots (u_n + v_n) \\ &= u_1 u_2 \cdots u_n + u_1 \cdots u_{n-1} v_n + \cdots + v_1 v_2 \cdots v_{n-1} u_n + v_1 v_2 \cdots v_n \\ &= x_i + y_i \end{aligned}$$

となる. 上では, 最後の項 (u_k を因子に含まない項) を y_i とし, それ以外の項 (u_k を因子に含む項) の和を x_i とおいた. すなわち,

$$\begin{aligned} x_i &= u_1 u_2 \cdots u_n + u_1 \cdots u_{n-1} v_n + \cdots + v_1 v_2 \cdots v_{n-1} u_n \\ y_i &= v_1 v_2 \cdots v_n \end{aligned}$$

上の和において, y_i は $v_j \in I_j$ より, $y_i \in \bigcap_{j \neq i} I_j$ であり, x_i は $u_j \in I_i$ より, $x_i \in I_i$ となる. 従って, $1 = x_i + y_i,\ x_i \in I_i,\ y_i \in \bigcap_{j \neq i} I_j$ となる x_i, y_i が取れる. $r \in R$ を任意の元とすると, この式の両辺に r を掛けることにより, $r = rx_i + ry_i,\ rx_i \in I_i,\ ry_i \in \bigcap_{j \neq i} I_j$ となり, $R = I_i + \bigcap_{i \neq j} I_j$ である.

2. 1 の証明で定めた $y_i \in \bigcap_{j \neq i} I_j,\ i = 1, \ldots, n$ を考える. $a_1, \ldots, a_n \in R$ に対し, $a = a_1 y_1 + \cdots + a_n y_n \in R$ とおく. このとき,

$$\begin{aligned} a - a_i &= a_1 y_1 + \cdots + a_{i-1} y_{i-1} + a_i (y_i - 1) + a_{i+1} y_{i+1} + \cdots a_n y_n \\ &= a_1 y_1 + \cdots + a_{i-1} y_{i-1} - a_i x_i + a_{i+1} y_{i+1} + \cdots a_n y_n \end{aligned}$$

となる. $x_i \in I_i$ なので, $-a_i x_i \in I_i$ である. また, $j \neq i$ に対して, $y_j \in \bigcap_{k \neq j} I_k \subset I_i$ なので, $a_j y_j \in I_i$ となる. よって, $a - a_i \in I_i$ がすべての i について成立する.

3. $f_i : R \to R/I_i$ を自然な射影とし,

$$f : R \to R/I_1 \oplus \cdots \oplus R/I_n, \quad f(a) = (f_1(a), \ldots, f_n(a))$$

とする. f が環の準同型写像になることは, 明らかである. 2 より, f は全射になる. 実際, $(\overline{a_1}, \ldots, \overline{a_n})$ に対して, $a_1, \ldots a_n$ をそれぞれの R での代表元とすると, 2 で定まる a を取れば, $f(a) = (\overline{a_1}, \ldots, \overline{a_n})$ である.

$$\mathrm{Ker}(f) = \{ a \in R \mid f_i(a) = \overline{0},\ \forall i = 1, \ldots, n \} = \{ a \in R \mid a \in I_i,\ \forall i = 1, \ldots, n \} = \bigcap_{i=1}^{n} I_i = I$$

なので, 準同型定理より, 証明を得る.

問 2.11（百五算）　上の証明を参考に, 次の百五算の解法を与えよ.

$n \in \mathbb{N}$, $0 \leqq n \leqq 104$ として, n を 3 で割った余り x, 5 で割った余り y, 7 で割った余り z が与えられた時, n の計算法を与えよ.

例 2.8（Euler の関数）　孫子の剰余定理より, $I_1, \ldots, I_m$ が全て互いに素であるなら, 単元群に対して, 次の群の直積分解が成立する (問 2.6).

$$(R/(I_1 \cap \cdots \cap I_m))^\times \cong (R/I_1)^\times \times \cdots \times (R/I_m)^\times$$

$R = \mathbb{Z}$ に対して, これを適用する. $n \in N$ とし, n の素因数分解を $n = p_1^{r_1} \cdots p_m^{r_m}$ とする. $I_i = p_i^{r_i}\mathbb{Z}$ とすると, $I_1, \ldots, I_m$ は互いに素なイデアルになる (問 2.10). また, $I_1 \cap \cdots \cap I_m = n\mathbb{Z}$ である. よって, 群としての直積分解

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_m^{r_m}\mathbb{Z})^\times$$

を得る. 数 $1, 2, \ldots, p_k^{r_k}$ の中で, p_k の倍数は, $p_k, 2p_k, \ldots, p_k^{r_k-1} \cdot p_k$ であるので, その個数は $p_k^{r_k-1}$ 個ある. これら以外が, $\mathbb{Z}/p_k^{r_k}\mathbb{Z}$ の単元の代表元のすべてなので, $|(\mathbb{Z}/p_k^{r_k}\mathbb{Z})^\times| = p_k^{r_k} - p_k^{r_k-1}$ となる. 従って,

$$\begin{aligned}\varphi(n) &= |(\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times| \cdots |(\mathbb{Z}/p_m^{r_m}\mathbb{Z})^\times| = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_n^{r_n} - p_m^{r_m-1}) \\ &= p_1^{r_1}\left(1 - \frac{1}{p_1}\right) \cdots p_m^{r_m}\left(1 - \frac{1}{p_m}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right)\end{aligned}$$

を得る.

問 2.12　1. $A_1, \ldots, A_m$ を有限集合とする. このとき, 集合の個数に対して, 次が成立することを示せ. ($|M|$ は集合 M の個数とする.)

$$|A_1 \cup \cdots \cup A_m| = \sum_{1 \leqq i_1 < \cdots < i_k \leqq m} (-1)^{k-1} |A_{i_1} \cap \cdots \cap A_{i_k}|$$

2. $n \in \mathbb{N}$ とし, $n = p_1^{r_1} \cdots p_m^{r_m}$ を n の素因数分解とする. $A_i = \{\, 1 \leqq a \leqq n \mid (a, p_i) = p_i \,\}$ と置いて, 1. の式を利用することにより, 例 2.8 の Euler 関数の公式を証明せよ.

2.5　極大イデアルと素イデアル

可換環 R のイデアル $\mathfrak{m}$ が極大イデアル (maximal ideal) であるとは, $\mathfrak{m}$ を真に含むイデアルは, R となることを言う. ここで, R 自身は極大イデアルとは言わないことに注意する.

定理 2.3　可換環 R のイデアル $\mathfrak{m}$ に対して, 次の条件は同値である.

1. $\mathfrak{m}$ は極大イデアルである.
2. 剰余環 $R/\mathfrak{m}$ が体になる.

証明.　$1 \Rightarrow 2$. $a \in R$ として, $R/\mathfrak{m}$ で $\overline{a} \neq 0$ とする. これは, $a \notin \mathfrak{m}$ と同値である. $\mathfrak{m}$ は, 極大イデアルであるので, $a, \mathfrak{m}$ から生成されるイデアル $(a, \mathfrak{m})$ は R と一致する. よって, $r \in R$ と $m \in \mathfrak{m}$ が存在して, $ra + m = 1$ となる. このとき, $R/\mathfrak{m}$ で $\overline{ra} = 1$ なので, $\overline{a}$ は可逆になり, $R/\mathfrak{m}$ は体である.

$2 \Rightarrow 1$. $I \supsetneqq \mathfrak{m}$ をイデアルとする. $a \in I \setminus \mathfrak{m}$ をとると, $R/\mathfrak{m} \ni \overline{a} \neq 0$ である. $R/\mathfrak{m}$ は体なので, $r \in R$ が存在して, $\overline{ra} = 1$ となる. このとき, $ar - 1 = m$, $m \in \mathfrak{m}$ となり, $ar + m = 1$ である. $a \in I$, $m \in \mathfrak{m} \subset I$ なの

で, $ar + m \in I$ となり, $1 \in I$ となる. このとき, $I = R$ となるから, $\mathfrak{m}$ を真に含むイデアルは R と一致し, $\mathfrak{m}$ は極大イデアルになる.

問 2.13 X をコンパクトな位相空間 (コンパクトの意味がわからなければ, X は $\mathbb{R}^n$ の有界閉集合としてよい), $C(X) = \{\, f : X \to \mathbb{C} \mid f \text{ は連続} \,\}$ とする. $C(X)$ は通常の関数の和と積により単位元を持つ可換環になる. $a \in X$ に対して, $\mathfrak{m}_a = \{\, f \in C(X) \mid f(a) = 0 \,\}$ は, $C(X)$ の極大イデアルになることを示せ.

問 2.14（局所環の例） $\mathbb{K}$ を体, $\mathbb{K}[[X]]$ を $\mathbb{K}$ 上の (1 変数) 形式的冪級数環とする. X から生成される単項イデアル (X) は, $\mathbb{K}[[X]]$ の唯一の極大イデアルになることを示せ.

上の問のように, 極大イデアルをただ 1 つしか持たない可換環を, 局所環という. 整域の素イデアルに対して, それの局所化と呼ばれるものを作ると, 局所環が作られる (D.1 節)

定理 2.4 R を可換環, I を R の自明でないイデアルとすると, I を含む極大イデアルが存在する.

一般的な状況のもとでこの定理を証明するには, Zorn の補題が必要なので, C.1 節に書いておくことにし, ここでは省略する.

定義 2.8 可換環 R のイデアル $\mathfrak{p}$ が素イデアル (prime ideal) であるとは, $\mathfrak{p} \neq R$ かつ $a, b \in R$ に対して,

$$ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \text{ または } b \in \mathfrak{p}$$

が成立することを言う.

素イデアルは, 整数での素数 p の持つ性質のひとつ,

$$a, b \in \mathbb{Z},\ ab \text{ が } p \text{ の倍数} \Longrightarrow a \text{ が } p \text{ の倍数, または } b \text{ が } p \text{ の倍数.}$$

のイデアルへの一般化である.

命題 2.1 R を可換環とする.

1. $\mathfrak{p}$ が R の素イデアルであるための必要十分条件は, $a, b \in R$ に対して,

   $$a \notin \mathfrak{p} \text{ かつ } b \notin \mathfrak{p} \Longrightarrow ab \notin \mathfrak{p}$$

   が成立することである.
2. $\mathfrak{p}$ が R の素イデアルであるための必要十分条件は, 剰余環 $R/\mathfrak{p}$ が整域であることである.

証明. 1. これは定義 2.8 の条件の対偶を述べたものである.

2. 1. より, $\mathfrak{p}$ が素イデアルなら, $a, b \in R \setminus \mathfrak{p}$ とすると, $ab \notin \mathfrak{p}$ となる. これは, $\overline{a}, \overline{b} \in R/\mathfrak{p}$ に対して, $\overline{a} \neq 0$ かつ $\overline{b} \neq 0$ なら $\overline{a}\overline{b} \neq 0$ が成立することであるから, $R/\mathfrak{p}$ は整域である. 逆に, $R/\mathfrak{p}$ が整域なら, この議論を逆にたどれば, $a \notin \mathfrak{p}$ かつ $b \notin \mathfrak{p}$ なら $ab \notin \mathfrak{p}$ が成立する.

上の命題 2.1, 2. より特に次が成立する.

命題 2.2 極大イデアルは素イデアルである.

上の命題の逆は成立しない.

例 2.9　$\mathbb{C}$ 上の 2 変数多項式環 $\mathbb{C}[X,Y]$ と 1 変数多項式環 $\mathbb{C}[X]$ を考える．$\varphi : \mathbb{C}[X,Y] \to \mathbb{C}[X]$ を，$(\varphi(f))(X) = f(X,0)$, $f \in \mathbb{C}[X,Y]$ で定義すると，φ は環の全射準同型写像である．環の準同型定理より，$\mathbb{C}[X] \cong \mathbb{C}[X,Y]/\mathrm{Ker}(\varphi)$ であるが，$\mathbb{C}[X]$ は整域であるので，$\mathrm{Ker}(\varphi)$ は素イデアルである．しかし $\mathbb{C}[X]$ は体ではないので，$\mathrm{Ker}(\varphi)$ は極大イデアルではない．

問 2.15　R を可換環，$\mathfrak{a}$, $\mathfrak{b}$ を R のイデアル，$\mathfrak{p}$ を素イデアルとするとき，$\mathfrak{ab} \subseteq \mathfrak{p}$ ならば $\mathfrak{a} \subseteq \mathfrak{p}$ または $\mathfrak{b} \subseteq \mathfrak{p}$ が成立することを示せ．

定理 2.5　$f : R \to R'$ を可換環の準同型写像とする．$R' \supset \mathfrak{p}$ を素イデアルとすると $f^{-1}(\mathfrak{p})$ は R の素イデアルになる．

証明.　$f^{-1}(\mathfrak{p})$ は R のイデアルになる．実際，$a, b \in f^{-1}(\mathfrak{p})$ なら，$f(a+b) = f(a) + f(b) \in \mathfrak{p}$ より $a+b \in f^{-1}(\mathfrak{p})$ であり，$r \in R$ に対して，$f(ra) = f(r)f(a) \in \mathfrak{p}$ となり，$ra \in f^{-1}(\mathfrak{p})$ である．

$a, b \in R$, $ab \in f^{-1}(\mathfrak{p})$ とすると，$f(a)f(b) = f(ab) \in \mathfrak{p}$ となる．$\mathfrak{p}$ は素イデアルなので，$f(a) \in \mathfrak{p}$ または $f(b) \in \mathfrak{p}$ である．よって，$a \in f^{-1}(\mathfrak{p})$ または $b \in f^{-1}(\mathfrak{p})$ となり，$f^{-1}(\mathfrak{p})$ は素イデアルである．

2.6　Euclid(ユークリッド) 整域, 単項イデアル整域

$\mathbb{Z}$ や，体上の 1 変数多項式環においては，「素因数分解の一意性」が成立する．これを証明する際に利用する性質を公理化したものが，Euclid 整域である．すなわち，可換環において，何らかの形の「大きさ」が定義され，割り算で「割る数より小さい余りが決まる」という性質が，「素因数分解の一意性」の根拠となっている．

イデアルも 2.3 節で可換環の準同型写像の核 (kernel) と捉えたが，もともとは，「素因数分解」を環に一般化するために導入された．例えば，$\mathbb{Z}[\sqrt{-5}]$ においては，

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

と 2 通りの積に書けるが，ここに現れる因子，2, 3, $1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ において単元以外の約数を持たない (例えば，$ab = 2$, $a, b \in \mathbb{Z}[\sqrt{-5}]$ とすると，a または b が ± 1 になる)．すなわち，$\mathbb{Z}[\sqrt{-5}]$ は，素朴な意味での「一意的」な積への分解ができないのである．

この節と次の節では，「素因数分解」を問題にする．この節では，環 R は可換環で常に整域 (零因子を持たない) であるとする．

定義 2.9　R を整域とし，N を整列集合 (全順序集合で，任意の空でない部分集合が最小元を持つ集合，例えば，自然数全体) とする．R から N への写像 $\varphi : R \to N$ で，次の性質を満たすものが存在するとき，R をユークリッド整域であるという．($>$ は N に入っている順序関係とする.)

1. $x \neq 0 \Longrightarrow \varphi(x) > \varphi(0)$
2. $b \in R$, $b \neq 0$ なら任意の $a \in R$ に対して，$a = bq + r$, $\varphi(r) < \varphi(b)$ となる q, $r \in R$ が存在する．

問 2.16　次を示せ．

1. $\mathbb{Z}$ は，$N = \mathbb{N} \cup \{0\}$, $\varphi(x) = |x|$ としてユークリッド整域である．
2. $\mathbb{K}$ を体とし，$\mathbb{K}[X]$ を K 上の 1 変数多項式環とする．$N = \{-\infty, 0\} \cup \mathbb{N}$ とする ($-\infty < 0 < 1 < \cdots$ で N には順序を入れる)．$f \in \mathbb{K}[X]$ に対して，$\varphi(f) = \deg f$ と定義する．ただし，$\deg 0 = -\infty$ とする．1 変数多項式環の割り算の計算より，$\mathbb{K}[X]$ はユークリッド整域になる．

3. Gauss の整数環 $\mathbb{Z}[\sqrt{-1}] = \{x + y\sqrt{-1} \mid x, y \in \mathbb{Z}\}$ を考える．$\varphi(x + y\sqrt{-1}) = x^2 + y^2$ とすると，これはユークリッド整域になることを示せ．($a, b \in \mathbb{Z}[\sqrt{-1}]$ に対して，a/b を複素数として計算して，これにもっとも近い点 $q \in \mathbb{Z}[\sqrt{-1}]$ をとり，$r = a - bq$ とおけば，定義の条件を満たす．)

定義 2.10（単項イデアル整域, PID） R を整域とする．R の任意のイデアルが単項イデアルであるとき，すなわち I を R のイデアルとすると，$a \in R$ が存在して $I = (a)$ となるとき，R を単項イデアル整域 (英語で Principal ideal domain, 略して PID) という．

Principal ideal は直訳すると主イデアルなので，単項イデアル整域は主イデアル整域ともいう．

命題 2.3 ユークリッド整域は単項イデアル整域である．

証明. R をユークリッド整域，N を全順序集合で，$\varphi : R \to N$ を定義 2.9 にある写像とする．R の自明なイデアルは，それぞれ，(0), (1) と書けるので，単項イデアルである．I を R の非自明なイデアルとする．N は整列集合だから，$\varphi(I) \setminus \{\varphi(0)\} \subset N$ には最小元 n が存在する．$a \in I$ を $\varphi(a) = n$ となる元とする．定義 2.9, 1. より，$a \neq 0$ となることに注意する．このとき，$I = (a)$ が成立する．

実際，$a \in I$ だから $(a) \subset I$ が従う．逆に $b \in I$ とする．定義 2.9, 2. から，$q, r \in R$ が存在して，$b = aq + r$, $\varphi(r) < \varphi(a)$ となる．このとき，$r = b - aq \in I$ となるが，$\varphi(a)$ の最小性から，$\varphi(r) = \varphi(0)$ となり，定義 2.9, 1. より $r = 0$ となる．よって，$b = aq \in (a)$ となり．$I \subset (a)$ を得る．

注意 2.6 上の命題の逆は成立しない．例えば，$\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$ は PID だがユークリッド整域ではない (B 節を参照)．計算機概論で $e^{\sqrt{163}\pi}$ が整数値にとても近いという話をする予定だが，(例えば http://www.math.u-ryukyu.ac.jp/~suga/joho/2016/12/node5.html)，これは $\mathbb{Z}\left[\dfrac{1+\sqrt{-163}}{2}\right]$ が PID であることと関係している．ちなみに $\mathbb{Z}\left[\dfrac{1+\sqrt{-163}}{2}\right]$ もユークリッド整域ではない．(このように，一見無関係に見える，ある種の環の性質と指数関数の特殊値が結びついてしまうところが，数学の面白いところである．)

また，ある環が PID であることを証明するのも，それほど易しいことではない．ユークリッド整域になることは十分条件だが必要条件ではないので，上の例のような場合には，別の手段で PID であることを示さなければならない．

2.7 素元分解整域

この節でも，R は可換環で整域であるとする．一般の整域においても約数・倍数の関係は同様に定義される．次の定義の，素元・既約元の言葉遣いは，多項式環を例として考えた方が，わかりやすいと思う．

定義 2.11 R を整域とする．

1. $a = bc$, $b, c \in R$ となるとき，b, c は a の約数，a は b, c の倍数という．このとき，$b|a$, $c|a$ と書く．
2. $a|b$ かつ $b|a$ であるとき，a と b は同伴であるという．このとき，$a \approx b$ と書く．
3. $a = bc$, $b, c \in R$ と a を積に分解したとき，b, c のどちらかが常に単元になるとき，すなわち，単元以外に約数を持たないとき，a を既約元という．

4. $p \in R$ が素元であるとは, $p \neq 0$ かつ $p \notin R^\times$ で,

$$p|ab \Longrightarrow p|a \text{ または } p|b$$

が成立することを言う.

問 2.17 0 は任意の元の倍数, 単元は任意の元の約数であることを述べよ.

命題 2.4 R を整域とする.

1. 0 でない元 $a, b \in R$ が同伴であるなら, ある単元 $\varepsilon \in R^\times$ が存在して, $b = \varepsilon a$ となる. 特に, 同伴であるという条件は, 同値関係である.
2. 素元は既約元である.

証明. 1. 条件より, $a|b$ なので, $b = ac$, $c \in R$ と書ける. 同様に $b|a$ なので, $a = bc'$, $c' \in R$ と書ける. よって $b = bcc'$ となり, $b(1 - cc') = 0$ である. R は整域なので, $1 - cc' = 0$ となり, $c \in R^\times$ となり, 前半の証明を得る. 同伴が同値関係であることは, このことと, $R^\times$ が積に関して群であることから従う.

2. $p \in R$ が素元であるとする. $p = ab$, $a, b \in R$ とする. $p|p$ かつ p は素元なので, $p|a$ または, $p|b$ が成立する. $p|a$ と仮定すると, ある c が存在して, $a = pc$ となる. このとき, $p = ab = pbc$ となり, $p(1 - bc) = 0$ を得る. R は整域で $p \neq 0$ なので, $bc = 1$ となって, b は単元になる. $p|b$ のときも同様に考えると a が単元になる. よって, p は既約元である.

上の命題の 2. の逆は成立しない.

問 2.18 1. 既約元と同伴な元は既約元であり, 素元と同伴な元は素元であることを示せ.

2. 2, 3, $1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ において既約元であることを示せ.
3. $\mathbb{Z}[\sqrt{-5}]$ において, $2 \not| (1 + \sqrt{-5})$ かつ $2 \not| (1 - \sqrt{-5})$ を示せ. $(2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ なので, このことから, 2 は $\mathbb{Z}[\sqrt{-5}]$ で素元ではない.)
4. $\mathbb{Z}[\sqrt{-5}]$ において, 2 と $1 + \sqrt{-5}$ から生成されるイデアル $(2, 1 + \sqrt{-5})$ を $\mathfrak{m}$ とするとき, $\mathfrak{m}$ は単項イデアルではないことを示せ.
5. 準同型写像 $\mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/2\mathbb{Z}$ を $f(a + b\sqrt{-5}) = \overline{a + b}$ で定める ($\overline{\ }$ は, $\mathbb{Z}/2\mathbb{Z}$ での同値類の意味). f を利用して, 上の $\mathfrak{m}$ は極大イデアルであることを示せ.

命題 2.5 R を整域とし, $p \in R$ とする. p が素元である必要十分条件は, p から生成される単項イデアル (p) が素イデアルであることである.

証明. $x \in (p)$ であることと, $p|x$ は同値であることに注意する. よって, p が素元と仮定すると, $ab \in (p)$ なら $a \in (p)$ または $b \in (p)$ が成立するので, (p) は素イデアルである. 逆に (p) が素イデアルであるとする. $p|ab$ とすると, $ab \in (p)$ である. (p) は素イデアルであるから, $a \in (p)$ または $b \in (p)$ となり, $p|a$ または $p|b$ が成立する.

これまでに, $\mathbb{Z}[\sqrt{-5}]$ で何度か例示したことは, 上の言葉遣いをすると, 「一般の整域において既約元による因数分解は一意性が成り立たない.」ということになる. しかし, 素元を用いれば, もし素因数分解ができれば一意的であることが証明できる. $\mathbb{Z}[\sqrt{-5}]$ は, 残念ながら, 素朴な意味での素因数分解はできない[*3].

[*3] $\mathbb{Z}[\sqrt{-5}]$ において, 任意のイデアルは素イデアルの積で一意的に書ける」という定理は証明できる. 歴史的には, イデアル, 素イデアルは, この形の定理のために導入された.

補題 2.1　R を整域とし, $p, q \in R$ を素元とする. このとき, $q \in (p)$ ならば, $p \approx q$ で, 特に $(p) = (q)$ が成立する.

証明.　$q \in (p)$ だから, $r \in R$ が存在して, $q = pr$ となる. q は素元なので, 命題 2.4, 2. より, 既約元である. (p) は素イデアルなので, p は単元ではない. よって, q の既約性より, $r \in R^\times$ となり, $p \approx q$ である. このとき, $(p) = (q)$ であることは, 容易に分かる.

問 2.19　$p \approx q$ なら $(p) = (q)$ を示せ.

定理 2.6（整域における素元分解の一意性）　R を整域とし, $a \in R$ が素元の積に分解できたとすると, その分解は本質的に一意的である. すなわち, $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ を R の素元とし,

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

であるとすると, $r = s$ であり, 積の順を入れかえると $p_1 \approx q_1, \ldots, p_r \approx q_r$ が成立する.

証明.　$r \leqq s$ と仮定して良い. $q_1 \cdots q_s = p_1 \cdots p_r$ より, $p_1 | q_1 \cdots q_s$ である. p_1 は素元なので, ある j が存在して, $p_1 | q_j$ である. 積の順を入れかえることにより, $j = 1$ として良い. p_1, q_1 は素元なので, 上の補題から, $p_1 \approx q_1$ となり, $q_1 = \varepsilon_1 p_1$ を得る. よって, $p_1 \cdots p_r = \varepsilon_1 p_1 q_2 \cdots q_s$ となる. R は整域なので ($ab = ac$, $a \neq 0 \Rightarrow b = c$ が成立するので), $p_2 \cdots p_r = \varepsilon_1 q_2 \cdots q_s$ となる. p_2 に対して, 上と同じことを実行すると, $q_2 = \varepsilon_2 p_2$, $\varepsilon_2 \in R^\times$ を得る. この操作を p_r まで実行すると, $q_i = \varepsilon_i p_i$, $\varepsilon_i \in R^\times$, $i = 1, \ldots, r$ となる. このとき, $1 = \varepsilon_1 \cdots \varepsilon_r q_{r+1} \cdots q_s$ となり, $q_{r+1}, \ldots, q_s \in R^\times$ であり, これらは素元ではありえない. よって, $r = s$ かつ $p_i \approx q_i$, $i = 1, \ldots, r$ である.

定義 2.12（素元分解整域, 一意分解整域, UFD）　R を整域とする. 任意の $a \in R \setminus \{0\}$ が素元の積に分解できるとき, R を素元分解整域, あるいは一意分解整域 (Unique factorization domain, 略して UFD) という.

上の定理 2.6 より, UFD での素元分解は常に一意的である. また, UFD では, 既約元と素元の概念が一致する. 再三例示してきた $\mathbb{Z}[\sqrt{-5}]$ は, UFD ではなく, 既約元が素元にならない.

命題 2.6　UFD では, 既約元は素元である.

証明.　R を UFD とし, $a \in R$, $(a \neq 0)$ を既約元とする. R は UFD なので, $a = p_1 \cdots p_r$ と素元の積に分解できる. a は既約元なので, このような分解があると, ある 1 つの p_i 以外は単元である. 従って, ある素元 p を用いて, $a = \varepsilon p$, $\varepsilon \in R^\times$ となり, a は素元である.

UFD なら素元分解の一意性があるが, そのような環の重要な例として, PID と, UFD 上の多項式環がある. 後者の証明は, 少し準備が必要なので D 節で与え, ここでは前者だけを証明する.

定理 2.7　PID は UFD である.

証明.　R を PID とし, $a \in R (a \neq 0)$ とする. a が素元なら素元分解はすでに終わっているので, 素元ではないとする. 定理 2.4 より, R の中で, イデアル (a) を含む極大イデアル $\mathfrak{m}_1$ が存在する. R は PID なので, $p_1 \in R$ が存在して, $\mathfrak{m}_1 = (p_1)$ である. $R/\mathfrak{m}_1$ は整域 (実際には体) なので, p_1 は素元である (命題 2.5). $a \in (a) \subset (p_1)$ なので, $a_1 \in R$ が存在して, $a = a_1 p_1$ である. a_1 が素元なら, これが a の素元の積への分解を与える. そうでなければ, a_1 に対して同じ操作をすると, 素元 p_2 と $a_2 \in R$ が存在して, $a = a_2 p_1 p_2$ となる. 以下, この操作を繰り返したとき, それが有限回で終わることを示す.

この操作で現れる R の元の列, $a_1, a_2, \ldots$, から作られる単項イデアルの列を考えると. $a = a_1p_1$, $a_1 = a_2p_2$, $a_2 = a_3p_3, \ldots$ なので, $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ が成立する. ここで, $I = \bigcup_{i=1}^{\infty}(a_i)$ を考えると, これは R のイデアルになることが, 簡単に確かめられる. R は PID なので, ある $b \in R$ が存在して, $I = (b)$ となる. $b \in I$ で, I の作り方から, ある n が存在して, $b \in (a_n)$ である. このとき, $(b) \subset (a_n)$ となり, $I = (a_n)$ となる. よって, $(a_n) = (a_{n+1}) = \cdots$ を得る. これは, 上の操作法に従うと, (a_n) を真に含む極大イデアルが存在しないことになる. よって, (a_n) は極大イデアルで, a_n は素元であり, $a_n = a_{n+1} = \cdots$ を得る. すなわち, 上の操作は有限回で終了する.

問 2.20　定理 2.4 では, 極大イデアルの存在に Zorn の補題を用いている. しかし, PID に関しては, 上の証明の後半と同じ考え方で, Zorn の補題を用いず, 任意のイデアル I に対して, I を含む極大イデアルの存在を証明できる. その証明を書け.

これまでの結果から,

ユークリッド整域 $\Longrightarrow$ PID $\Longrightarrow$ UFD

が示された. 従って, よく知られているように, $\mathbb{Z}$ や体 K 上の 1 変数多項式環 $K[X]$ は PID であり, UFD である. また, Gauss の整数環 $\mathbb{Z}[\sqrt{-1}]$ もユークリッド整域なので, PID であり, さらに UFD でもある.

注意 2.7　ここで, 言葉遣いを少し整理しておく. 自然数 p が素数であることの通常の定義は, これまでに述べた環での言葉では, p が整数環 $\mathbb{Z}$ の既約元であるという定義になる. これが $\mathbb{Z}$ の素元になることは, $\mathbb{Z}$ が UFD であることと上の命題から従う. すなわち, 整数環において, 素数 ($\mathbb{Z}$ の既約元) が素元であることは自明ではなく, 証明を要することなのである.

なおこれまでの証明では, PID という概念を用いて $\mathbb{Z}$ において素数が素元であることを示しているが, (PID を使わない) 直接的な証明も可能である (A 節).

定理 2.7 の逆は成立しない. 例えば, 体 K 上の 2 変数多項式環 $K[X, Y]$ は, D 節で示すように UFD である. しかし, 次の説明で見るように, 一般的に, これは PID ではない.

例 2.10（$\mathbb{C}[X, Y]$ が PID ではないことの説明.）　$\mathbb{C}[X, Y]$ のイデアル I に対して, $\mathcal{V}(I) = \{(x, y) \in \mathbb{C}^2 \mid g(x, y) = 0,\ \forall g \in I\}$ とおく. すなわち, 方程式 $g(x, y) = 0$ が定める曲線の集合を, g をイデアルの元を全て動かしたときの共通部分である. これをイデアル I に対する代数的集合という. I が $f(X, Y) \in \mathbb{C}[X, Y]$ から生成される単項イデアル $I = (f)$ であるとすると, 容易に分かるように, これから定まる代数的集合は, $\mathcal{V}((f)) = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\}$ となる. すなわち, 1 つの方程式 $f(x, y) = 0$ で定まる曲線に一致する. 一方, $\mathbb{C}[X, Y]$ の 2 つの単項式 X, Y から生成されるイデアル, $I = (X, Y)$ を考える. このとき, $\mathcal{V}((X, Y))$ は原点のみからなる 1 点集合 $\{(0, 0)\} \subset \mathbb{C}^2$ となる. しかし, $f \in \mathbb{C}[X, Y]$ に対して, $f(x, y) = 0$ が 1 点集合となることはありえない (無限集合になるか, 空集合 (f が 0 でない定数の場合) である.) ので, (X, Y) は単項イデアルではない.

問 2.21　$f(X, Y) \in \mathbb{C}[X, Y]$ とし, f は定数多項式ではないとする. $\mathbb{C}$ が代数的に閉じている ($\mathbb{C}$ 係数の代数方程式は, $\mathbb{C}$ に必ず根を持つ) ことを利用して, $\{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\ \}$ は無限集合になることを示せ.

ここで, この節の内容から導かれる PID の性質についてまとめた命題を挙げておく. 代数方程式を考える際に, 体上の 1 変数多項式環でよく用いられる性質である.

命題 2.7（PID の性質のまとめ）　R を PID とする．

1. R の素イデアルは, 既約元から生成される単項イデアルである．
2. R の素イデアルは, 極大イデアルである．

特に, R のひとつの既約元から生成される単項イデアルは, R の極大イデアルになる．

証明. 1. I を R の素イデアルとし, p を生成元とすると, 命題 2.5 より, p は素元であり, 特に既約元である．PID R は UFD なので既約元は素元であり, それから生成されるイデアルは, 素イデアルである．

2. $I=(p)$ を R の素イデアルとし, $J=(q)$ を I を含む R のイデアルとする．$p\in J$ なので, $r\in R$ が存在して, $p=qr$ となる．このとき, $p|qr$ であるが, p が素元であるので, $p|q$ または $p|r$ である．$p|q$ なら, p, q は互いに同伴となるので, $I=(p)=(q)=J$ となる．$p|r$ とすると, $r=ps,\ s\in R$ となるが, このとき, $p=pqs$ となり, R が整域であることより $qs=1$ を得る．よって, q は可逆元となり $J=R$ となる．これらのことから, I は極大イデアルである．

注意 2.8　上で, PID なら任意の素イデアルは極大イデアルであることを示したが, 逆は成立しない．例えば, 次の問にあるように, $\mathbb{Z}[\sqrt{-5}]$ では任意の素イデアルは極大イデアルであることが示されるが, これが PID でないことは, 既に述べたとおりである．

問 2.22　$x=a+b\sqrt{-5}\in\mathbb{Z}\left[\sqrt{-5}\right]$ に対して, $N(x)=a^2+5b^2$ とおく．

1. $x\in\mathbb{Z}[\sqrt{-5}]$ とする．x から生成される $\mathbb{Z}[\sqrt{-5}]$ の単項イデアル (x) について, $\left|\mathbb{Z}[\sqrt{-5}/(x)\right|=N(x)$ を示せ (3 節．B 節を参照せよ.)
2. $I\subset\mathbb{Z}[\sqrt{-5}]$ を $\{0\}$ でないイデアルとするとき, $|\mathbb{Z}[\sqrt{-5}]/I|<\infty$ を示せ．
3. $\mathfrak{p}\subset\mathbb{Z}[\sqrt{-5}]$ を素イデアルとすると, $\mathfrak{p}$ は極大イデアルになることを示せ．

注意 2.9　上の問のようなことは,「代数体の整数環」というものについて, 一般的に成立することである．詳しくは, 代数的整数論に関連する専門書を参照してください．

2.8　環上の加群

M を加法群 (演算を加法として, 単位元を 0 で表す可換群) とし, R を (単位元を持つ) 環とする (一般的に非可換とする)．環が加法群 M に作用するという状況が, 数学において多く現れるので, その定義と性質の基本を, ここで述べておく．

定義 2.13　M が左 R–加群 (left R–module) であるとは, R の M への左からの作用が存在することを言う．ここで, R の左からの作用は次を満たす写像, $R\times M\to M,\ (r,m)\mapsto rm$ である．

1. $(rr')m=r(r'm),\ 1m=m,\quad r,r'\in R,\quad m\in M$
2. $(r+r')m=rm+r'm,\ r(m+m')=rm+rm',\quad r,r'\in R,\quad m,m'\in M$

右 R–加群も同様に定義される．

問 2.23　1. 右 R–加群の定義を書き下せ．
2. 左 R–加群の公理から, $0a=0$, $(-1)a=-a$ $(\forall a\in M)$ を導け．

注意 2.10　R が可換環ならば, 左加群, 右加群の区別をする必要はない (積の可換性から, 右加群の公理と左加群の公理が同値になる) が, 非可換環なら異なる概念となる.

両側加群という概念もあり (その場合, 左からの作用と右からの作用が異なる環になることもある), 重要ではあるが, それについてはここでは述べない.

例 2.11　1.　M を任意の加法群とする. $a \in M$, $n \in \mathbb{Z}$ に対して $na = \begin{cases} a+a+\cdots+a & (n \geqq 0) \\ -a-a-\cdots-a & (n<0) \end{cases}$ ($|n|$ 項の和または差) と定義すると, M は $\mathbb{Z}$–加群になる. すなわち, 任意の加法群は $\mathbb{Z}$–加群である.

2.　R 自身, 左右の積を作用だと思えば, 左右の R–加群である.

3.　R を可換環とし, $M_n(R)$ を R 上の行列環とする. $R^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in R \right\}$ を R を成分とする n 項列ベクトルのなす加法群とすると, 通常の行列の積で R^n は左 $M_n(R)$–加群である. 同様に, $R_n = \{(a_1, \ldots, a_n) \mid a_i \in R\}$ を n 項の行ベクトル全体がなす加法群とすると, R_n は行列の積で, 右 $M_n(R)$–加群である.

以下では, 左 R–加群について述べるが, 右 R–加群についても同様のことが成立する.

定義 2.14　M を左 R–加群とし, $N \subset M$ とする. 次が成立するとき, N を部分 R–加群 (R–submodule, R の作用が明らかな場合は, 単に部分加群) という.

1.　N は加法群として, M の部分群
2.　$RN \subset N$

他の代数系の用語と同じように, $\{0\}$, M は, 自明な部分加群と呼ばれる. R が可換環であるとき, R 自身を R–加群と見たとき, その部分加群とはイデアルのことである.

$N \subset M$ を部分 R–加群とする. M が可換群なので, N は群として正規部分群である. よって, 商群 M/N を考えることができる. $a+N \in M/N$ と $r \in R$ に対して, $ra+N \in M/N$ は $a+N$ の代表元 a の取り方によらず, well–defined である. 実際, $a+N = a'+N$ とすると, $ra-ra' = r(a-a')$ で $a-a' \in N$ より $r(a-a') \in N$ となり, $ra+N = ra'+N$ である. この R の作用により, M/N は左 R–加群になる. これを, 商加群という. R を可換環とすると, R のイデアル I は部分加群である. R 自身も R–加群なので, 剰余環 R/I は商加群として R–加群である.

定義 2.15　M, N を左 R–加群とし, $f : M \to N$ を写像とする. f が R–加群の準同型写像 (略して, R–準同型写像あるいは, R–線形写像) であるとは, 次を満たすことを言う.

1.　$f(a+b) = f(a)+f(b), \qquad a, b \in M$
2.　$f(ra) = rf(a), \qquad r \in R,\ a \in M$

さらに f が全単射であるとき, f を R–同型写像であるという.

$f : M \to N$ を R–加群の準同型写像とすると,

$$\mathrm{Im}(f) = f(M) = \{f(a) \mid a \in M\} \subset N$$
$$\mathrm{Ker}(f) = f^{-1}(0) = \{a \in M \mid f(a) = 0\} \subset M$$

はそれぞれ, N, M の部分加群となる.

定理 2.8（R–加群の準同型定理） M, N を左 R–加群とし, $f : M \to N$ を R–準同型写像とすると, f から誘導される自然な R–同型写像

$$\overline{f} : M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

が存在する.

定理の証明は, 群や環の準同型定理の証明と同じである.

問 2.24 上の定理の証明を書け.

定義 2.16（直積と直和） $\{M_i\}_{i \in I}$ を左 R–加群の族とする.

1. 直積

$$\prod_{i \in I} M_i = \{(a_i)_{i \in I} \mid a_i \in M_i\}$$

を集合としての直積とし, 和と R の作用は成分ごとに定義する. すなわち,

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}, \qquad r(a_i)_{i \in I} = (ra_i)_{i \in I}$$

これにより, 直積集合 $\prod_{i \in I} M_i$ は左 R-加群となる. これを R-加群 $\{M_i\}_{i \in I}$ の直積という.

2. 直和は直積の中の次の部分集合として定義される.

$$\bigoplus_{i \in I} M_i = \{(a_i)_{i \in I} \in \prod_{i \in I} M_i \mid \text{有限個の } i \text{ を除いて } a_i = 0\}$$

これが, $\prod_{i \in I} M_i$ の部分加群になることは容易に確かめられる.

上で, I が有限集合であれば, 直積と直和は同じものになるが, I が無限集合のときは, 一般に $\bigoplus_{i \in I} M_i \subsetneqq \prod_{i \in I} M_i$ である. $l \in \mathbb{N}$ に対して, R^l は, R 自身を R–加群と見たものの l 個の直和を表すことにする.

定義 2.17 M を左 R–加群とし $U \subset M$ を部分集合とする.

$$< U >= \left\{ \sum_{\text{有限和}} r_i u_i \mid r_i \in R,\ u_i \in U \right\}$$

は部分 R–加群となる. $< U >$ を U から生成された部分加群という.

定義 2.18 M を左 R–加群とし, $U \subset M$ を部分集合とする.

1. $u_1, \ldots, u_n$ が R 上 1 次独立 (あるいは線形独立) とは,

$$r_1u_1 + r_2u_2 + \cdots + r_nu_n = 0 \Longrightarrow r_1 = \cdots = r_n = 0$$

が成り立つことを言う.

2. U が M の基底であるとは, 次が成立することという.
   (a) $< U >= M$
   (b) U の任意の有限部分集合は, 1 次独立である.
3. M が基底を持つとき, 自由 R–加群 (free R–module) という.

注意 2.11　環上の加群においては, 基底を持たないことの方が通常である. 例えば, $n \in \mathbb{N}$ として, $\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}$–加群と見ると, これに基底は存在しない. $\{\overline{1}\}$ は生成元集合であるが, 1 次独立性が成り立たない $(n \cdot \overline{1} = \overline{0})$. もちろん, $\mathbb{Z}/n\mathbb{Z}$–加群と見る場合には, $\{\overline{1}\}$ は基底になる. よって, M だけでなくスカラーの集合 R の性質も重要になる.

例 2.12　R^l は自由 R–加群である. $e_i = (\delta_{ij})_j \in R^l$ (第 i 成分だけが 1 で残りの成分は 0) が基底になる. これを R^l の標準基底という.

3　単因子論

3.1　R–自由加群での線形代数

環上の加群に対する線形代数学は, ホモロジー代数と呼ばれるものになるが, ホモロジー代数について述べるのは大変なので, この講義では取り上げない.

この講義では, 線形代数学で学んだ「行列の基本変形」の話が拡張できる対象として, PID 上の自由加群を考える. 有限生成アーベル群の基本定理 (有限生成アーベル群は巡回群の直積に同型である) と Jordan 標準形の理論が, これの応用として統一的に証明できることを知るのが目標である. 以下では R は可換環とする.

M を l 個の基底 $\{e_1, \ldots, e_l\}$ を持つ R 自由加群とする. このとき, 次が成立する.

補題 3.1　M の基底の個数は, 取り方によらず一定である. この個数を M のランク (rank, 階数) という.

上の補題の証明は, R の極大イデアルを考えて, それに対する剰余体のベクトル空間を考え, ベクトル空間の次元に帰着させるのが簡単である. ここでは証明は省略する.

R を可換環, M, N をそれぞれランク m, n の R 上の自由加群とする. $f : M \to N$ を R 加群の準同型写像とし, $\{u_1, u_2, \ldots, u_m\}$, $\{v_1, v_2, \ldots, v_n\}$ をそれぞれ M, N の基底とする. このとき, $f(u_j) = \sum_{i=1}^{n} a_{ij}v_i$, $(a_{ij} \in R)$, $j = 1, \ldots, m$ の規則で, 成分が R の元である $n \times m$ 行列 $(a_{ij}) \in M_{n,m}(R)$ を定める. これを基底 $\{u_1, u_2, \ldots, u_m\}$, $\{v_1, v_2, \ldots, v_n\}$ に対する f の行列表示という. R が PID の場合, 線形代数学で学んだ行列の基本変形の理論が, ほぼそのままで成立し, それが有限生成 Abel 群の基本定理や Jordan 標準形の計算に利用できるというのが, これから述べる単因子論である.

単因子について述べる前に, 行列の基本変形について復習する. 考えるものは, 線形代数学で学んだものと同じであるが, 行列の要素は R の元であるとする.

R の元を成分とする行列の基本変形は, 次の 3 つの操作をいう.

(T1)　ある行もしくは列を単元倍する.

(T2)　2 つの行もしくは 2 つの列を入れ替える.

(T3)　ある行もしくはある列に別の行もしくは列のスカラー倍を加える.

(T1) が線形代数学とずれる部分で, 線形代数学では 0 でないスカラー倍としていたが, ここでは R が環なので, 逆変換の存在を保証するために単元倍に変わってる. 基本変型が可逆な変形であることは直ちにわかるが, これらの操作が, 可逆な行列の積で与えられることからもわかる. 実際, 次の n 次正方行列を導入する $(i \neq j)$.

$$E_{ij}(\alpha,\beta,\gamma,\delta) = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & \alpha & \cdots & \beta & & & \\ & & & & 1 & & & & \\ & & & \vdots & \ddots & \vdots & & & \\ & & & & & & 1 & & \\ & & & \gamma & \cdots & \delta & & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}, \quad \alpha,\beta,\gamma,\delta \in R \quad \alpha\delta - \beta\gamma \in R^{\times} \tag{3.1}$$

$$E_i(\alpha) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \alpha & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}, \qquad \alpha \in R^{\times} \tag{3.2}$$

ここで, α は i,i–成分, β は i,j–成分, γ は j,i–成分, δ は j,j–成分にあり, 数字が書かれていない成分は, 全て 0 であるとしている. この行列を, 基本行列という. $\det E_{ij}(\alpha,\beta,\gamma,\delta) = \alpha\delta - \beta\gamma \in R^{\times}$. $\det E_i(\alpha) = \alpha \in R^{\times}$ だから, これらの行列は逆行列を持つ. すなわち, $E_{ij}(\alpha,\beta,\gamma,\delta)$, $E_i(\alpha) \in GL_n(R)$ である. 基本変形は, 行列の積を用いて次で実現される.

(T1)　i 行の単元倍：$E_i(\alpha)$ を左から掛ける.
　　i 列の単元倍：$E_i(\alpha)$ を右から掛ける.

(T2)　i 行, j 行の入れ替え：$E_{ij}(0,1,1,0)$ を左から掛ける.
　　i 列, j 列の入れ替え：$E_{ij}(0,1,1,0)$ を右から掛ける.

(T3)　i 行に j 行の γ 倍を加える: $E_{ij}(1,\gamma,0,1)$ を左から掛ける $(i<j)$.
　　i 行に j 行の β 倍を加える: $E_{ij}(1,0,\beta,1)$ を左から掛ける $(i>j)$.
　　i 列に j 列の γ 倍を加える: $E_{ij}(1,\gamma,0,1)$ を右から掛ける $(i<j)$.
　　i 列に j 列の β 倍を加える: $E_{ij}(1,0,\beta,1)$ を右から掛ける $(i>j)$.

$A, B \in M_{m,n}(R)$ が基本変形で移りあえるとき, 互いに相似であるといい, $A \sim B$ と書くことにする. これは, 同値関係になる. 線形代数学で学んだ行列の基本変形の議論を, PID の元を成分とする行列に適用すると, 線形代数学での結果に類似した結果が得られることを示す.

定理を述べる前に, PID に対する性質を少し補足しておく. 整数環で用いられる約数, 公約数, 倍数という言葉遣いを PID でも用いることにする. すなわち, $a = bc$ となるとき, a は b, c の倍数, b, c は a の約数である. d が a, b の約数であるとき, a, b の公約数という. a, b が単元以外に公約数を持たない時, a, b は互いに素であるという.

補題 3.2 R を PID, $a, b \in R$ とする. a, b から生成されるイデアル (a, b) の生成元を $d \in R$ とするとき, $ax + by = d$ となる $x, y \in R$ が存在し, この x, y は互いに素である.

特に, a, b が互いに素ならば, $ax + by = 1$ となる互いに素な $x, y \in R$ が存在する.

証明. $(a, b) = \{au + bv \mid u, v \in R\}$ なので, $(a, b) = (d)$ なら, $ax + by = d$ となる $x, y \in R$ が存在する. $d' \in R$ が x, y の公約数とする. このとき, $d = ax + by$ は d' の倍数になる. $x' = \dfrac{x}{d'}$, $y' = \dfrac{y}{d'}$, $d'' = \dfrac{d}{d'}$ とすると, $ax' + by' = d''$ となるので, イデアルで見て $(a, b) \ni d''$ となり, $(a, b) \supset (d'')$ である. 一方, $(a, b) = (d)$ だから, $(d'') \subset (d)$ となり, d'' は d の倍数である. すなわち, d'' は, d の約数かつ倍数になるから, d と d'' は同伴になり, $d' \in R^\times$ である.

$a \in (d)$ なら, d は a の約数である. 従って, $(a, b) = (d)$ なら, d は a, b の公約数である. よって, a, b が互いに素なら, $(a, b) = (1) = R$ となり, 後半を得る.

定理 3.1 R を PID とし, $A \in M_{m,n}(R)$ を R を成分にもつ $m \times n$ 行列とする. このとき, $d_1, \ldots, d_r \in R$ で, $d_i \mid d_{i+1}$, $(i = 1, \ldots, r-1)$, $d_r \neq 0$ となるものが単元倍を除いて一意的に存在し, M を基本変形することにより, 次の形の対角行列にできる.

$$\begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

$(d_1, \ldots, d_r)$ を A の単因子という.

証明. まず, 基本変形で上の形の対角行列にできることを示す. 次で与えられる R のイデアルの族 $\mathcal{I}$ を考える.

$$\mathcal{I} = \{Rb_{ij} = (b_{ij}) \subset R \mid B = (b_{ij}),\ B \sim A\}$$

すなわち, A と相似な行列の成分から生成される単項イデアルを全て集めたものである. $\mathcal{I}$ に包含関係で順序を入れる. $\mathcal{I}$ の全順序部分集合

$$(b_1) \subset (b_2) \subset \cdots$$

を考える. 定理 2.7 の証明と同じことをすれば, このイデアルの増大列に対して, ある $l \in \mathbb{N}$ が存在して, $(b_l) = (b_{l+1}) = \cdots$ となる. この状況で, 集合族 $\mathcal{I}$ には, (包含関係を順序とする) 極大元 I が存在する. もしそうでなければ, $I \in \mathcal{I}$ に対して, 常に $I' \supsetneqq I$ となる $I' \in \mathcal{I}$ が取れることになり, R が PID から導かれる上に述べたこと (全順序部分集合はいつか一定になる) に矛盾する.

$I \in \mathcal{I}$ の極大元とし, その生成元を b とする. b を要素に持つ A とと相似な行列を $B = (b_{ij})$ とする. B に行と列の交換を施すことにより, $b_{11} = b$ としてよい. このとき, B の 1 行と 1 列の要素はすべて b の倍数で

ある．実際, b の倍数でない要素 b_{1j} が存在すれば, これと b から生成される R のイデアル (b, b_{1j}) を考えると, $(b, b_{1j}) \supsetneqq (b)$ である．しかし, R は単項イデアル整域だから, ある b' が存在して, $(b, b_{ij}) = (b')$ となる．このとき, 上の補題から, $b' = \alpha b + \beta b_{1j}$ となる, 互いに素な $\alpha, \beta \in R$ が存在する．α, β は互いに素なので, $\gamma, \delta \in R$ で, $\alpha\delta - \beta\gamma = 1$ となるものが存在する．よって, 行列 $E_{1j}(\alpha, \gamma, \beta, \delta)$ を右から B に掛ける基本変形で, (11) 成分が b' となる行列が作れる．これは $I = (b)$ の極大性に矛盾する．B の第一列についても同様である

以上のことから, b を (11) 成分に持ち, 1 行と 1 列の他成分は b の倍数となる行列 B が, A と相似な行列として取れる．(11) 成分 b を要 (pivot) として, 1 行, 1 列に対してはき出し (基本変型) をすれば, 各成分が b_{11} の倍数なので, A は次の形の行列に相似であることがわかる ($d_1 = b_{11} = b$ とする).

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}$$

ここで, B' に対して上と同じ操作を繰り返す．その際, 上の行列に, $b_{11} = b$ で行った同じ議論をすると, B' の要素は全て d_1 の倍数であることが示される．特に, 同じ操作で現れる対角成分の先頭要素は, $d_1 (= b_{11} = b)$ の倍数である．この操作を繰り返すことにより, 定理の形の行列に基本変型で写ることが証明される．

A の部分行列で, i 次の正方行列であるものの行列式の値全体から生成される R のイデアルの生成元を e_i(すなわち, 小行列式全体の最大公約数) とする．基本変型の定義と行列式の性質から, 基本変型を行って起こる小行列式の変化は単元倍と和を組み合わせて得られるものなので, e_i も基本変形によって単元倍しか変化しない．従って, A が定理の形の対角行列に基本変型で写されたとすると,

$$d_1 = e_1, \quad d_1 d_2 = e_2, \quad d_1 d_2 d_3 = e_3, \ldots$$

を満たさなければならない．PID は UFD なので, このような $d_1, d_2, \ldots$ は単元倍を除いて一意的に定まる．

注意 3.1　上の証明でわかるように, 1 番目から i 番目の単因子の積は, A の $i \times i$ 小行列の行列式全体の最大公約数である．R が Euclid 整域なら, この数は Euclid の互除法で具体的に計算するアルゴリズムがあるが, 一般の PID では, それがあるとは限らない．また, Euclid 整域なら, 対角行列にするための基本変形のアルゴリズムも, 互除法を用いて与えることができる．

問 3.1　次の行列の整数環上の単因子を求めよ.(実際に単因子行列に変形する基本変形も計算せよ.)

1. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$　2. $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$　3. $\begin{pmatrix} 10 & 4 & 6 \\ 18 & 12 & 30 \end{pmatrix}$　4. $\begin{pmatrix} 1 & 0 & 3 \\ 1 & -3 & 3 \\ 1 & 3 & -3 \end{pmatrix}$

5. $\begin{pmatrix} 3 & 7 \\ 10 & 22 \\ 9 & 21 \end{pmatrix}$　6. $\begin{pmatrix} 14 & 11 \\ 6 & 5 \\ 2 & 4 \end{pmatrix}$　7. $\begin{pmatrix} 5 & 2 & 5 \\ 6 & 3 & 10 \\ 10 & 4 & 16 \\ 11 & 5 & 15 \end{pmatrix}$　8. $\begin{pmatrix} 6 & 46 & 29 & 155 \\ 18 & 146 & 90 & 492 \\ 6 & 48 & 30 & 162 \end{pmatrix}$

3.2　有限生成アーベル群の基本定理

単因子論を利用して, 有限生成 Abel 群の基本定理を証明するが, その前に次の補題を証明しておく．

補題 3.3　R を PID, M を有限生成 R–加群とすると, R の部分加群も有限生成である.

証明. M の生成元の個数に関する帰納法を用いる. M が 1 つの生成元 u から生成されているとする. $N \subset M$ を N の部分 R–加群とする.

$$I = \{\, r \in R \mid ru \in N \}$$

とおくと, I は R のイデアルになる. 実際, $r_1, r_2 \in I$ なら $(r_1 + r_2)u = r_1u + r_2u \in N$ より, $r_1 + r_2 \in I$ であり, $a \in R$ に対して $(ar_1)u = a(r_1u) \in N$ より $ar_1 \in I$ となる. R は PID なので, $b \in R$ が存在して $I = (b)$ となる. このとき, N は bu で生成される. 実際, $bu \in N$ は定義より明らかで, N は部分加群だから, $Rbu \subset N$ である. 逆に, $n \in N$ とすると, M が u で生成されているから, $r \in R$ が存在して, $n = ru$ となる. このとき, I の定義から $r \in I$ となるが, I は b で生成されているので, $r = r'b$ となり, $n = r'bu$ となる. よって, 生成元が 1 つのときの補題が証明された.

$n-1$ 個の生成元を持つ加群に対して, 補題が成立すると仮定する. M を n 個の生成元 $u_1, \dots, u_n$ を持つ R–加群とし, $N \subset M$ をその部分加群とする. u_1 が生成する M の部分加群 Ru_1 による商加群を $M_1 = M/Ru_1$ とし, $f : M \to M_1 = M/Ru_1$ を自然な射影とする. M_1 は $n-1$ 個の元 $f(u_2), \dots, f(u_n)$ から生成されるので, 帰納法の仮定から, その部分加群 $f(N)$ は有限生成である. その生成元を $v_2, \dots, v_m$ とし, それらの f に対する原像を 1 つずつ取って, $w_2, \dots, w_m \in M$ とする. 準同型定理から, $f(N) \cong N/(N \cap Ru_1)$ である. ここで, $N \cap Ru_1$ は, Ru_1 の部分加群だから上の議論より 1 つの元から生成されるので, これの生成元 w_1 が存在する. このとき, $w_1, w_2, \dots, w_m$ は N の生成元である. 実際, $x \in N$ に対して, $f(x) = \sum_{i=2}^{m} a_i v_i$ とすると, $f\left(x - \sum_{i=2}^{m} a_i w_i\right) = 0$ だから, $x - \sum_{i=1}^{m} a_i w_i \in N \cap Ru_1$ となり, x は $w_1, w_2, \dots, w_m$ の線形結合で表示される.

定理 3.2　R を PID, M を有限生成 R–加群とすると, 自然数 $l \in \mathbb{N}$ と $d_1, \dots, d_r \in R$ で $d_i | d_{i+1}$, $(i = 1, \dots, r-1)$ が存在して, R–加群として次の同型が存在する. ここで, (d_i) は d_i から生成される R の単項イデアルである.

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^l$$

証明. M の生成元を $\{u_1, \dots, u_n\}$ とする. $N = R^n$ とし, N の標準基底を $e_1, \dots, e_n$ とする. R–加群の準同型写像, $\varphi : N \to M$ を次で定義する.

$$\varphi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} r_i u_i, \quad r_i \in R$$

$\{u_1, \dots, u_n\}$ が M を生成するから, φ は全射である. 従って, 準同型定理より, $M \cong N/\mathrm{Ker}(\varphi)$ である. N は有限生成 R–加群なので, 上の補題から, $\mathrm{Ker}(\varphi)$ は有限生成である. その生成元を $\{v_1, \dots, v_m\}$ とする. v_i を標準基底の線形結合で書く.

$$v_i = a_{1i}e_1 + \cdots + a_{ni}e_n, \quad i = 1, 2, \dots, m$$

上を行列表示すると, 次のように書ける.

$$(v_1 \ \cdots \ v_m) = (e_1 \ \cdots \ e_n)A, \qquad A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \tag{3.3}$$

A を $\mathrm{Ker}(\varphi)$ の生成行列と呼ぶことにする.

$\mathrm{Ker}(\varphi)$ の生成元 $\{v_1, \ldots, v_n\}$ を次のように取り替えることができる.

(R1)　v_i をその単元倍に変える.

(R2)　v_i と v_j を入れ替える.

(R3)　$c \in R$ と $j \neq i$ に対して, v_i を $v_i + cv_j$ に変える.

上の操作を行っても, 生成元になる. 実際, (R1), (R2) は明らかだし, (R3) についても, $v_i = (v_i + cv_j) - cv_j$ に注意すれば良い. これらの操作は, 3.3 式に対して, 右から列基本変形の行列を掛ける操作に対応するのは, 明らかである. すなわち, 列基本変形を施した行列に対応する生成元は, 元の部分加群と同じ部分加群を生成する.

次に, R–加群の同型写像 $g : N \to N$ を考える. $N/\mathrm{Ker}(\varphi) \cong N/g(\mathrm{Ker}(\varphi))$ である. 一方, g は同型写像なので, $\{g(e_1), \ldots, g(e_n)\}$ も R^l の基底になる. 逆に, R^l の基底 $\{f_1, \ldots, f_n\}$ を与えると, $e_i \mapsto f_i$, $(i = 1, \ldots, n)$ で R^n の R–同型写像が定まる. すなわち, R^n の R–同型写像は, 基底の取り換えに他ならない. そこで, 次の基底の取り換えを考える.

(L1)　i 番目の基底をその単元倍に変える.

(L2)　i 番目の基底と j 番目の基底を入れ替える.

(L3)　$c \in R$ と $j \neq i$ に対して, i 番目の基底に j 番目の基底の c 倍を加える.

これらの操作で, 基底が基底に移されることは, (R1)–(R3) の場合と同様にわかる. また, これらの操作を行うと, $\mathrm{Ker}(\varphi)$ の生成行列は, 対応する行基本変形が施されることも容易にわかる. よって, 定理 3.1 より, $N = R^n$ の基底をうまく選ぶと, $\mathrm{Ker}(\varphi)$ の生成行列が

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \end{pmatrix}, \qquad d_i \mid d_{i+1},\ i = 1, 2 \ldots$$

とできる. このとき $M \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^l, \quad (l = n - r)$ となるのは, 明らかである.

補題 3.4　R を PID とする. $a, b \in R$ を, 最大公約数が 1(a, b を素因子分解したとき, 共通に現れる素元を持たない) とき, 単項イデアル (a), (b) は互いに素である.

証明. R は PID なので, $(c) = (a) + (b)$ となる $c \in R$ が存在する. このとき, $a, b \in (c)$ なので, $c|a$, $c|b$ となり, c は a, b の公約数である. a, b は互いに素なので, c は 1 と同伴になり, $(a) + (b) = R$ が成立する.

上の補題と孫子の剰余定理 (Chinese remainder theorem, 定理 2.2) より, 次が成立する.

系 3.1　R を PID とし, $d = p_1^{k_1} \cdots p_r^{k_r}$ を $d \in R$ の素因数分解とする. このとき, 環として次の同型が成立する.

$$R/(d) \cong R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_r^{k_r})$$

上の定理で, $R = \mathbb{Z}$ とすると次を得る.

系 3.2（有限生成アーベル群の基本定理） A を有限生成アーベル群とする．$d_1, \dots, d_n$ を上で述べた A の単因子とし，$d_i = \prod_{j=1}^{k_i} p_{ij}^{r_{ij}}$ を d_i の素因数分解とする．このとき，A は次の巡回群の直積と同型になる．

$$A \cong \prod_{i=1}^{n} \left(\prod_{j=1}^{k_i} \mathbb{Z}/p_{ij}^{r_{ij}}\mathbb{Z} \right)$$

3.3 Jordan 標準形

線形代数学の講義の最後の方で，Jordan 標準形の話が出たと思う．その際には，一般化された固有空間を考えて，行列の標準形を求めた．ここでは，単因子論を用いた Jordan 標準形の求め方を述べる．単因子論を用いる利点は，特性多項式，最小多項式の計算が不要 (自動的に出てくる) であることにある．欠点は，Jordan 標準形に変換する変換行列が求まらない事である．

この節での設定は，$\mathbb{K}$ を体とし，$V = \mathbb{K}^n$ を $\mathbb{K}$ 上の n 次元ベクトル空間，$\boldsymbol{u}_i$ を $\mathbb{K}^n$ の標準基底 (i 番目の成分が 1 で他の成分は 0)，$A = (a_{ij})$ を $\mathbb{K}$ を成分とする $n \times n$ 行列，$R = \mathbb{K}[T]$ を T を不定元とする $\mathbb{K}$ 係数の多項式環とする．$\mathbb{K}[T]$ は Euclid 整域なので，PID でもある．

V を次の作用で左 R–加群としたものを V_A と書くことにする．

$$\mathbb{K}[T] \times V \ni (f, \boldsymbol{v}) \mapsto f(A)\boldsymbol{v} \in V$$

ここで，$f(T) = a_n T^n + \cdots + a_1 T + a_0$ に対して，$f(A) = a_n A^n + \cdots + a_1 A + a_0 E$ としている．

$\mathbb{K} \subset \mathbb{K}[T]$ なので，V の基底，$\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ は $\mathbb{K}[T]$–加群として，V_A を生成する．すなわち，V_A は，上の作用で有限生成 $\mathbb{K}[T]$–加群である

さて，単因子論を利用すると，$d_1(T), \dots, d_n(T) \in \mathbb{K}[T]$，$d_i(T) \,|\, d_{i+1}(T)$，$(i = 1, \dots, n-1)$ が存在して，$\mathbb{K}[T]$–加群として，V_A は次の直和に分解される．

$$\bigoplus_{i=1}^{n} \mathbb{K}[T]/(d_i(T))$$

ここで，$(d_i(T))$ は，$d_i(T)$ から生成される $\mathbb{K}[T]$ の単項イデアルである．定数倍を掛けることにより，$d_i(T)$ は monic(最高次の係数は 1) であると仮定して良い．

ここで問題とするのは，次の 2 つである．A を与えて V_A を考えたとき，

1. $d_i(T)$ の計算法.
2. $d_i(T)$ が求まったとして，それからわかること．

2 の問題から考えていく．$d(T) = T^m + a_{m-1}T^{m-1} + \cdots + a_0$ としたとき，$\mathbb{K}$ 上のベクトル空間としての $\mathbb{K}[T]/(d(T))$ を考える．$f(T) \in \mathbb{K}[T]$ に対して，多項式の割り算を実行すると，

$$f(T) = d(T)q(T) + r(T), \quad \deg r < \deg d = m$$

となる．従って，$\mathbb{K}[T]$ の元の剰余環 $\mathbb{K}[T]/(d(T))$ での類を $\overline{\ }$ を用いて表すと，$\{\, \overline{T}^{m-1}, \cdots, \overline{T}, \overline{1} \,\}$ が基底になることがわかる．すなわち，$\dim_{\mathbb{K}} \mathbb{K}[T]/(d(T)) = m$ である．この基底に対する T の作用を行列表示すると，

$T\cdot\overline{T}^i=\overline{T}^{i+1}\,(i=0,\dots,m-2)$, $T\cdot\overline{T}^{m-1}=-a_{m-1}\overline{T}^{m-1}-\cdots-a_0$ より, 次を得る.

$$\begin{pmatrix} -a_{m-1} & 1 & 0 & \cdots & 0\\ -a_{m-2} & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \ddots & \vdots\\ -a_1 & 0 & \cdots & \ddots & 1\\ -a_0 & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

V_A において, T を掛ける作用は行列 A を掛ける作用となるので, V_A の部分空間 $\mathbb{K}[T]/(d(T))$ では, 行列 A は上の形で表示される基底を持つ. 上の行列は, A の同伴行列と呼ばれる.

さらに特別な場合として, $d(T)=(T-\lambda)^m$, $\lambda\in\mathbb{K}$ の場合を考える. このとき, $\mathbb{K}[T]/(d(T))$ の基底として, $\{\,(\overline{T}-\lambda)^{m-1},\dots,(\overline{T}-\lambda),1\,\}$ を取ると, 上と同様の計算により, $T-\lambda$ は次の行列で表される線形変換になる.

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

V_A では, T の作用は行列 A の積なので, 上の基底を用いると,

$$A-\lambda E=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0\\ 0 & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \ddots & \vdots\\ 0 & 0 & \cdots & \ddots & 1\\ 0 & 0 & \cdots & \cdots & 0 \end{pmatrix},\qquad A=\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0\\ 0 & \lambda & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \ddots & \vdots\\ 0 & 0 & \cdots & \ddots & 1\\ 0 & 0 & \cdots & \cdots & \lambda \end{pmatrix}=J(\lambda,m)$$

となるので, A は Jordan 細胞の形での行列表示になる.

上の議論から, 定理 3.2 の単因子の計算ができれば, A の Jordan 標準形を求められることがわかる. 定理 3.2 の証明を見ると,

$$\varphi:\mathbb{K}[T]^n\ni\begin{pmatrix} g_1(T)\\ \vdots\\ g_n(T)\end{pmatrix}\mapsto g_1(A)\boldsymbol{u}_1+\cdots+g_n(A)\boldsymbol{u}_n\in V$$

に対して, $\mathrm{Ker}(\varphi)$ の生成行列の基本変形で単因子が計算できることがわかる.

補題 3.5 $\mathrm{Ker}(\varphi)$ の生成行列は, $T-A=\begin{pmatrix} T-a_{11} & \cdots & -a_{1n}\\ \vdots & \ddots & \vdots\\ -a_{n1} & \cdots & T-a_{nn}\end{pmatrix}$ で与えられる.

証明. N を $T-A$ を生成行列として定まる $\mathbb{K}[T]^n$ の部分加群とする. N の生成元は, 次で与えられる.

$$v_i=\begin{pmatrix} -a_{1i}\\ \vdots\\ T-a_{ii}\\ \vdots\\ -a_{ni}\end{pmatrix}\in\mathbb{K}[T]^n,\quad i=1,\dots,n$$

$\varphi(v_i) = -a_{1i}\boldsymbol{u}_1 - \cdots + A\boldsymbol{u}_i - a_{ii}\boldsymbol{u}_i - \cdots - a_{ni}\boldsymbol{u}_n = \boldsymbol{o}$, $i = 1, \ldots, n$ が成立するので, $N \subseteq \mathrm{Ker}(\varphi)$ である. 一方, $T - A$ に対する $\mathbb{K}[T]$ での単因子を $d_1(T), \ldots, d_n(T)$ とすると, 基本変形において, $\mathbb{K}^\times$ の元の掛け算が許されるので, $d_i(T)$ の最高次の係数は 1 とできる. このとき, $\det(T - A) = d_1(T) \cdots d_n(T)$ となる. よって, $\dim_{\mathbb{K}} \mathbb{K}[T]^n/N = \sum_{i=1}^{n} \deg d_i(T) = \deg \det(T - A) = n$ となる. ベクトル空間の準同型定理より, $\dim_{\mathbb{K}} \mathbb{K}[T]^n/\mathrm{Ker}(\varphi) = \dim_{\mathbb{K}} V = n$ だから, $N = \mathrm{Ker}(\varphi)$ となる. よって, $T - A$ が $\mathrm{Ker}(\varphi)$ の生成行列となる.

上の $T - A$ の基本変形によって得られる情報をまとめておく. まず, A の最小多項式が, 基本変形から自動的に出てくる.

命題 3.1 上の設定の下で, $T - A$ の $\mathbb{K}[T]$ での単因子を $d_1(T), \ldots, d_n(T)$ とすると, A の特性多項式は $\prod_{i=1}^{n} d_i(T)$ であり, $d_n(T)$ は A の最小多項式である.

証明. 基本変形で用いる行列の行列式は, $R^\times = \mathbb{K}[T]^\times = \mathbb{K}^\times$ の元である. 従って, 基本変形では, 行列式は 0 でない定数倍される. 単因子を求める際に, $\mathbb{K}^\times$ の元を掛ける事により, $d_i(T)$ はモニック (最高次の係数が 1) にできる. よって, $\det(TE_n - A) = d_1(T) \cdots d_n(T)$.

$f \in \mathbb{K}[T]$ とする. 多項式の因数定理から, V の $\mathbb{K}[T]/(d_i(T))$ と同型な直和成分において, $f(A) = O$ となることと, $d_i(T)|f(T)$ は同値になる. 従って $f(A) = O$ なら, $d_i(T)|f(T)$, $i = 1, \ldots, n$ となるが, $d_i(T)|d_{i+1}(T)$ なので, $d_n(T)|f(T)$ が成立することと, $f(A) = O$ は同値になる. よって, $d_n(T)$ は A の最小多項式になる.

以下では, 体 $\mathbb{K}$ は代数的に閉じているとする. 代数的に閉じているとは, $\mathbb{K}[T]$ の任意の多項式は, $\mathbb{K}$ に根を持つという意味である. $\mathbb{C}$ は代数的に閉じている体であるが, これ以外にもこのような体はある. また, 任意の体は代数的に閉じた体の部分体であることも証明できる (例えば, 実数体は複素数体の部分体 (虚部が 0 の集合)). このあたりのことは, 来年の代数学の講義で学ぶことになっている (と思う).

$\mathbb{K}$ が代数的に閉じていると, 定数でない多項式 $f(T) \in \mathbb{K}[T]$ に対して $\alpha \in \mathbb{K}$ が存在して, $f(\alpha) = 0$ となる. これは, $f(T) = (T - \alpha)g(T)$ と因数分解ができることと同じである. これを繰り返すと, $f(T)$ は次の形の 1 次式のベキの積に書ける.

$$f(T) = (T - \alpha_1)^{k_1}(T - \alpha_2)^{k_2} \cdots (T - \alpha_r)^{k_r}, \quad \alpha_i \neq \alpha_j \ (i \neq j), \ k_i \geqq 1, \ i = 1, \ldots, r$$

上のことと補題 3.4 を利用すると, $\mathbb{K}$ が代数的に閉じている時, $T - A$ を $\mathbb{K}[T]$ で基本変形すると, A の Jordan 標準形が計算できる. ここで重要なのは, A の特性多項式や最小多項式が行列式の計算とかではなく, 基本変形で出てくることである. 系 3.2 と同様に次を得る.

系 3.3 上の状況のもとで, $T - A$ の単因子が $d_i(T) = \prod_{j=1}^{k_i} (T - \lambda_{ij})^{r_{ij}}$ と因数分解されたとすると, A の Jordan 標準形は, 次の形の直和となる.

$$\bigoplus_{i=1}^{n} \left(\bigoplus_{j=1}^{k_i} J(\lambda_{ij}, r_{ij}) \right)$$

ここで, $A \oplus B = \begin{pmatrix} A & O \\ O & B \end{pmatrix}$ という記号を用いている.

例 3.1　1. $A=\begin{pmatrix}5&-4&12\\1&0&3\\-1&1&-2\end{pmatrix}$ の Jordan 標準形の計算.

$$T-A=\begin{pmatrix}T-5&4&-12\\-1&T&-3\\1&-1&T+2\end{pmatrix}\ \begin{matrix}2\text{ 行}\times(-1)\text{ と }1\text{ 行を交換}\\\longrightarrow\end{matrix}\ \begin{pmatrix}1&-T&3\\T-5&4&-12\\1&-1&T+2\end{pmatrix}$$

$$\begin{matrix}2\text{ 行}-1\text{ 行}\times(T-5)\\3\text{ 行}-1\text{ 行}\\\longrightarrow\end{matrix}\ \begin{pmatrix}1&-T&3\\0&T^2-5T+4&-3T+3\\0&T-1&T-1\end{pmatrix}$$

$$\begin{matrix}\text{列基本変形で }12,13\text{ 成分を }0\text{ にする}\\2\text{ 行と }3\text{ 行を交換}\\\longrightarrow\end{matrix}\ \begin{pmatrix}1&0&0\\0&T-1&T-1\\0&T^2-5T+4&-3T+3\end{pmatrix}$$

$$\begin{matrix}3\text{ 行}-2\text{ 行}\times(T-4)\\\longrightarrow\end{matrix}\ \begin{pmatrix}1&0&0\\0&T-1&T-1\\0&0&-(T-1)^2\end{pmatrix}\ \begin{matrix}3\text{ 列}-2\text{ 列}\\3\text{ 行}\times(-1)\\\longrightarrow\end{matrix}\ \begin{pmatrix}1&0&0\\0&T-1&0\\0&0&(T-1)^2\end{pmatrix}$$

$A=\begin{pmatrix}5&-4&12\\1&0&3\\-1&1&-2\end{pmatrix}$ の Jordan 標準形は, $\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}$, 最小多項式は $(T-1)^2$,
特性多項式は, $(T-1)^3$

2. $A=\begin{pmatrix}0&1&0\\1&0&1\\-1&0&0\end{pmatrix}$ の Jordan 標準形 (基本変形は各自見出してください.)

$$T-A=\begin{pmatrix}T&-1&0\\-1&T&-1\\1&0&T\end{pmatrix}\to\begin{pmatrix}1&0&T\\-1&T&-1\\T&-1&0\end{pmatrix}\to\begin{pmatrix}1&0&T\\0&T&T-1\\0&-1&-T^2\end{pmatrix}\to\begin{pmatrix}1&0&0\\0&1&T^2\\0&T&T-1\end{pmatrix}$$

$$\to\begin{pmatrix}1&0&0\\0&1&T^2\\0&0&-T^3+T-1\end{pmatrix}\to\begin{pmatrix}1&0&0\\0&1&0\\0&0&T^3-T+1\end{pmatrix}$$

$T^3-T+1=0$ の異なる 3 根を λ_1, λ_2, λ_3 とすると, A の Jordan 標準形は $\begin{pmatrix}\lambda_1&0&0\\0&\lambda_2&0\\0&0&\lambda_3\end{pmatrix}$

注意 3.2　上の例では, 敢えて基本変形で Jordan 標準形を計算している. しかし, 「Jordan 標準形を求める」だけを目標とするなら, 基本変形以外の方法も考えるべきである.

例えば, 上の例の 2 番目に対しては, 特性多項式が次で簡単に計算できる.

$$\det(TE_3 - A) = \det \begin{pmatrix} T & -1 & 0 \\ -1 & T & -1 \\ 1 & 0 & T \end{pmatrix} = T^3 - T + 1$$

$T^3 - T + 1 = 0$ が重根を持たないことをチェックすれば, $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$ は, 特性多項式の根を対角成分に持つ行列に対角化できるのはわかる.

同様に, 1 番目の例に関しても, 特性多項式は次で与えられる.

$$\det(TE_3 - A) = \det \begin{pmatrix} T-5 & 4 & -12 \\ -1 & T & -3 \\ 1 & -1 & T+2 \end{pmatrix} = T^3 - 3T^2 + 3T - 1 = (T-1)^3$$

また,

$$1 \cdot E - A = \begin{pmatrix} -4 & 4 & -12 \\ -1 & 1 & -3 \\ 1 & -1 & 3 \end{pmatrix} \neq O, \qquad (1 \cdot E - A)^2 = \begin{pmatrix} -4 & 4 & -12 \\ -1 & 1 & -3 \\ 1 & -1 & 3 \end{pmatrix} \begin{pmatrix} -4 & 4 & -12 \\ -1 & 1 & -3 \\ 1 & -1 & 3 \end{pmatrix} = O,$$

がわかるので, A の最小多項式は, $(T-1)^2$ となる. これより, 上の単因子論の議論から, $T - A$ の単因子は $\begin{pmatrix} 1 & 0 & 0 \\ 0 & T-1 & 0 \\ 0 & 0 & (T-1)^2 \end{pmatrix}$ となることがわかるので, A の Jordan 標準形もわかる.

下の Jordan 標準形を求める問では, 無理に基本変形を利用する必要は無い.

ただし, 行列のサイズが大きくなると, 定義に基づいた特性多項式の計算が大変になるので, 単因子論の方が, 一般的には計算がやさしくなる.

問 3.2 次の行列の Jordan 標準形を求めよ.

1. $\begin{pmatrix} 1 & 3 & 3 \\ 3 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}$ 2. $\begin{pmatrix} 5 & 4 & 3 \\ -1 & 0 & -3 \\ 1 & -2 & 1 \end{pmatrix}$ 3. $\begin{pmatrix} 2 & 2 & -1 \\ -1 & -1 & 1 \\ -1 & -2 & 2 \end{pmatrix}$ 4. $\begin{pmatrix} 4 & -1 & -3 \\ -3 & -5 & 10 \\ 0 & -3 & 4 \end{pmatrix}$

5. $\begin{pmatrix} 2 & 0 & -1 \\ -2 & 3 & 2 \\ 1 & 0 & 0 \end{pmatrix}$ 6. $\begin{pmatrix} 2 & -1 & 1 \\ 2 & 2 & -1 \\ 1 & 2 & -1 \end{pmatrix}$ 7. $\begin{pmatrix} 1 & -1 & 1 \\ 0 & 3 & -2 \\ 0 & 2 & -1 \end{pmatrix}$ 8. $\begin{pmatrix} 0 & 2 & -1 \\ 1 & -1 & 4 \\ 1 & -2 & 4 \end{pmatrix}$

9. $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ 10. $\begin{pmatrix} 3 & -4 & 3 & -3 \\ 1 & -1 & 1 & -1 \\ -1 & 2 & -3 & 4 \\ -1 & 2 & -4 & 5 \end{pmatrix}$ 11. $\begin{pmatrix} 3 & -4 & 3 & 0 \\ 4 & -6 & 9 & 1 \\ 3 & -5 & 9 & 1 \\ -10 & 17 & -28 & -2 \end{pmatrix}$

12. $\begin{pmatrix} 2 & 1 & 0 & -2 \\ 2 & 2 & 2 & 0 \\ 0 & -2 & 2 & 4 \\ 1 & 0 & 1 & 2 \end{pmatrix}$ 13. $\begin{pmatrix} 1 & 4 & 4 & 3 \\ 3 & 4 & 5 & 4 \\ -1 & -1 & -2 & -1 \\ -4 & -8 & -8 & -7 \end{pmatrix}$ 14. $\begin{pmatrix} 1 & 2 & 1 & -2 \\ 0 & 1 & 3 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

15. $\begin{pmatrix} 2 & 3 & -1 & -2 \\ 2 & 1 & -2 & 0 \\ 3 & 3 & -2 & -2 \\ 2 & 2 & -2 & 1 \end{pmatrix}$　　16. $\begin{pmatrix} -5 & 4 & -6 & 3 & 8 \\ -2 & 3 & -2 & 1 & 2 \\ 4 & -3 & 4 & -1 & -6 \\ 4 & -2 & 4 & 0 & -4 \\ -1 & 0 & -2 & 1 & 2 \end{pmatrix}$

注意 3.3（単因子とコンピュータ）　整数行列の単因子や上の Jordan 標準形の計算においては, $\mathbb{Z}$ なり $\mathbb{C}[T]$ が Euclid 整域であることが本質的に計算を易しくしている. 例えば, 下の B 節にあるように, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ は PID であるので, 定理 3.2 が成立する. 定理の証明をみると, 行列要素の最大公約数を求める方法があれば, 単因子は帰納的に決定できる. しかし, $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ で, 例えば, 6 と $1+\sqrt{-19}$ の最大公約数が 2 であることを示すのは, 少し面倒である (アルゴリズムが無いわけではない). $\mathbb{Z}$ や $\mathbb{C}[T]$ のような Euclid 整域では, 下の Euclide の互除法で最大公約数は計算する簡明なアルゴリズムがある. さらに, 拡張 Euclid アルゴリズムは, 単因子行列への基本変形の方法まで与える.

明解なアルゴリズムがあると, それを計算するコンピュータプログラムを書くことが難しくない. 実際, 計算機概論で講義する予定の Maple では, 線形代数パッケージの `smith` (Jordan 標準形), `ismith` (整数環) がそれを実行してくれる (単因子行列は, Smith form と呼ばれる). 以下は, 計算例である.

```
> with(linalg);

[BlockDiagonal, GramSchmidt, JordanBlock, LUdecomp, QRdecomp, Wronskian,
    addcol, addrow, adj, adjoint, angle, augment, backsub, band, basis, bezout,
    blockmatrix, charmat, charpoly, cholesky, col, coldim, colspace, colspan,
    companion, concat, cond, copyinto, crossprod, curl, definite, delcols,
    delrows, det, diag, diverge, dotprod, eigenvals, eigenvalues, eigenvectors,
    eigenvects, entermatrix, equal, exponential, extend, ffgausselim,
    fibonacci, forwardsub, frobenius, gausselim, gaussjord, geneqns, genmatrix,
    grad, hadamard, hermite, hessian, hilbert, htranspose, ihermite, indexfunc,
    innerprod, intbasis, inverse, ismith, issimilar, iszero, jacobian, jordan,
    kernel, laplacian, leastsqrs, linsolve, matadd, matrix, minor, minpoly,
    mulcol, mulrow, multiply, norm, normalize, nullspace, orthog, permanent,
    pivot, potential, randmatrix, randvector, rank, ratform, row, rowdim,
    rowspace, rowspan, rref, scalarmul, singularvals, smith, stackmatrix,
    submatrix, subvector, sumbasis, swapcol, swaprow, sylvester, toeplitz,
    trace, transpose, vandermonde, vecpotent, vectdim, vector, wronskian]
```

```
> A:=matrix([[4, 0 ,0], [0, 5, 0],[0,0,6]]);
                                    [4    0    0]
                                    [           ]
                                    [0    5    0]
                               A := [           ]
                                    [0    0    6]

> ismith(A);
                                  [1    0     0]
                                  [           ]
                                  [0    2     0]
                                  [           ]
                                  [0    0    60]

> B:=matrix([[T-5,4,-12],[-1,T,-3],[1,-1,T+2]]);
                                [T - 5    4      -12 ]
                                [                    ]
                           B := [ -1      T      -3  ]
                                [                    ]
                                [  1      -1    T + 2]

> smith(B,T);
                          [1      0           0      ]
                          [                          ]
                          [0    T - 1         0      ]
                          [                          ]
                          [               2          ]
                          [0      0      T  - 2 T + 1]
```

3.3.1 行列の冪乗について

行列 A に対して, その冪乗 A^n の計算は, 一般には難しい. 前期の講義で, Jordan 標準形があればやさしいことは述べたが (講義ノート p.8, 問 1.8), その際には変換行列の計算が必要になる. すなわち, A の Jordan 標準形を J とすると, 正則な行列 P を用いて, $P^{-1}AP = J$ とできるから, $A^n = PJ^nP^{-1}$ として, A^n を求める方法である.

冪乗の計算だけなら, よりやさしい方法として, 最小多項式を利用する方法がある. すなわち, A の最小多項式を $m_A(T)$ とする. T^n を $m_A(T)$ で割り算をする.

$$T^n = m_A(T)q(T) + r_n(T)$$

この式に, A を代入すると, $m_A(A) = O$ なので $A^n = r_n(A)$ となる. $\deg m_A = k$ とすると, $\deg r_n < k$ なの

で, A, A^2, …, A^{k-1} の計算をすれば, A^n が求まる.

上で述べた通り, 最小多項式は基本変形で求まるので, 方程式を解いて固有値を求めたり, 変換行列を計算する (一般化された固有ベクトルを求める) 必要は無い.

例 3.2 $A = \begin{pmatrix} 5 & -4 & 12 \\ 1 & 0 & 3 \\ -1 & 1 & -2 \end{pmatrix}$ の n 乗の計算. この行列の最小多項式は, $(T-1)^2$ である.

$$T^n = (T-1)^2 q(T) + aT + b$$

において, $T = 1$ を代入すると, $a + b = 1$. 両辺を微分して,

$$nT^{n-1} = 2(T-1)q(T) + (T-1)^2 q'(T) + a$$

これに $T = 1$ を代入して, $a = n$. 従って,

$$T^n = (T-1)^2 q(T) + nT + 1 - n \qquad (\text{i. e. } r_n(T) = nT + 1 - n\,)$$

これに A を代入して,

$$A^n = nA + (1-n)E = \begin{pmatrix} 4n+1 & -4n & 12n \\ n & 1-n & 3n \\ -n & n & 1-3n \end{pmatrix}$$

なお, 上の計算は, $n \leqq 0$ の場合にも成立していることに注意する.

問 3.3 問 3.2 のそれぞれの行列に対して, その n 乗を求めよ.

A Euclid の互除法

Euclid の互除法は, Euclid 整域において最大公約数を効率良く求めるアルゴリズムである. 高校の時に学習していると思うが, 改めて Euclid 整域に対して述べておく.

整数環と異なり, 一般の環の場合, 自然な大小関係が存在しない. そこで, 最大公約数は次のように定義される.

定義 A.1 R を整域, $a, b \in R$ とする. $d \in R$ が a, b の最大公約数 (最大公約元) であるとは, 次を満たすことを言う.

1. $d \mid a$ かつ $d \mid b$
2. $d' \mid a$ かつ $d' \mid b$ ならば $d' \mid d$

このとき $d = (a, b)$ とも書く.

問 A.1 R が整域なら, 最大公約数は単元倍を除いて一意的であることを示せ. すなわち, d, d' を a, b の最大公約数とすると, $\varepsilon \in R^\times$ が存在して, $d' = \varepsilon d$ が成立する.

上の問より, 最大公約数は単元倍を除いて一意的なので, 以下の議論では, 単元倍の違いは無視する.

R を Euclid 整域とし, N を整列集合, $\varphi : R \to N$ を, Euclid 整域の定義に現れる割り算を定義する写像とする. $a, b \in R$ とするとき,

$$a = bq + r, \quad \varphi(r) < \varphi(b)$$

となるとき, q を商, r を余り (剰余) という. Euclid の互除法は, 次のことに基づく.

以下, R は Euclid 整域とする.

補題 A.1 $a, b \in R$ として, $r = a - bq$ を a を b で割った余りとする. このとき,

$$(a, b) = (b, r)$$

証明. $r = a - bq$ なので, a, b の公約数は, b, r の公約数になる. $a = bq + r$ を利用すると, b, r の公約数は, a の約数なので, a, b の公約数になる. すなわち, a, b の公約数の集合と b, r の公約数の集合は一致するから, 最大公約数も一致する.

互除法

$a, b \in R$ とする. 次のルールで数列, r_0, r_1, $r_2, \ldots$, を定める.

$$r_0 = a, \qquad r_1 = b, \qquad r_2 = r_0 - r_1 q_1, \qquad \ldots \qquad r_{k+1} = r_{k-1} - r_k q_k, \qquad \ldots$$

ここで, q_i は r_{i-1} を r_i で割った商, r_{i+1} はその余りである. 補題 A.1 より, $(r_{i-1}, r_i) = (r_i, r_{i+1})$, $\forall i$ が成立する. R が Euclid 整域なので, ある n が存在して, $r_{n+1} = 0$ となる. 実際, N の部分集合, $\{\varphi(r_i)\} \subset N$ は最小元を持つから, それを $\varphi(r_k)$ とする. $r_k \neq 0$ なら, 割り算の決め方から $\varphi(r_{k+1}) < \varphi(r_k)$ となり, $\varphi(r_k)$ の最小性に矛盾する. $r_{n+1} = 0$ とすると, $(r_n, 0) = r_n$(左辺は最大公約数の意味) となるので, $r_n = (a, b)$ となる.

拡張 Euclid アルゴリズム

解説には行列を利用した方が分かりやすい. 互除法の漸化式 $r_k = r_{k-2} - r_{k-1} q_{k-1}$ を行列で書くと,

$$\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1} \end{pmatrix} \begin{pmatrix} r_{k-2} \\ r_{k-1} \end{pmatrix} = A_{k-1} \begin{pmatrix} r_{k-2} \\ r_{k-1} \end{pmatrix}, \qquad A_{k-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1} \end{pmatrix}$$

となる. よって,

$$\begin{pmatrix} r_n \\ 0 \end{pmatrix} = A_n \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = A_n A_{n-1} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = A_n A_{n-1} \cdots A_0 \begin{pmatrix} r_1 \\ r_0 \end{pmatrix} = A_n A_{n-1} \cdots A_0 \begin{pmatrix} b \\ a \end{pmatrix}$$

となるので, $A_n A_{n-1} \cdots A_0 = \begin{pmatrix} y & x \\ z & u \end{pmatrix}$ とすると, $r_n = ax + by$ となる. よって次を得る.

系 A.1 $a, b \in R$, $d = (a, b)$ とすると, $ax + by = d$ となる $x, y \in R$ が存在する.

上の議論では, x, y を具体的に計算する方法を Euclid の互除法が与えることがわかる. この計算法を, 拡張 Euclid アルゴリズムという. Euclide の互除法やこのアルゴリズムは, とても効率が良く, 数字の桁数の数倍程度の計算で, 最大公約数にたどり着くことがわかる.

例 A.1　上では解説に行列を利用したが, 現実の計算は, 互除法の計算を書いて後ろから代入して行く. $(629, 391)$ の計算で例示する.

$$629 = 391 + 238, \quad 391 = 238 + 153, \quad 238 = 153 + 85, \quad 153 = 85 + 68, \quad 85 = 68 + 17, \quad 68 = 17 \times 4$$

となるので, $(629, 391) = 17$ である. この式を後ろから読む.

$$\begin{aligned} 17 &= 85 - 68 = 85 - (153 - 85) = 2 \times 85 - 153 = 2 \times (238 - 153) - 153 = 2 \times 238 - 3 \times 153 \\ &= 2 \times 238 - 3 \times (391 - 238) = 5 \times 238 - 3 \times 391 = 5 \times (629 - 391) - 3 \times 391 \\ &= 5 \times 629 - 8 \times 391 \end{aligned}$$

系 A.1 を利用すると, 素数 p は, 整数環の素元であることが証明できる (自然数 p が素数であることの通常の定義は, p が $\mathbb{Z}$ の既約元であることであって, それが, 素元になることは証明すべきことである.). 下の証明は, PID や UFD といった概念を用いない, 初等的な証明になる.

系 A.2　$p \in \mathbb{N}$ が素数で, $p|ab$, $a, b \in \mathbb{Z}$ とすると, $p|a$ または $p|b$ が成立する.

証明.　$p|a$ なら証明は終わっているので, $p \not| a$ とする. p の約数は 1, p の 2 つだけなので, $p \not| a$ なら $(p, a) = 1$ となる. よって, 系 A.1 より, $x, y \in \mathbb{Z}$ で, $ax + py = 1$ となるものが存在する. 両辺に b を掛けると, $abx + pby = b$ となるが, $p|ab$ より, 左辺は p の倍数である. よって, 右辺も p の倍数となり, $p|b$.

B　$\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$ (注意 2.6)

$\alpha = \dfrac{1+\sqrt{-19}}{2}$ とする. ここでは, $R = \mathbb{Z}[\alpha] = \{a + b\alpha \,|\, a, b \in \mathbb{Z}\}$ と固定する. R は, PID であるが, Euclid 整域ではないことの初等的な証明を与える. PID であることは, ここに述べた証明よりも, 2 次体の整数論において類数公式を証明しておき, R の類数を計算して, それが 1 となることを利用するのが標準的な手法のようである. ここでは, 類数公式を用いない証明を与える.

$\overline{\alpha} = \dfrac{1-\sqrt{-19}}{2}$ (α の複素共役) とし, $x = a + b\alpha$, $a, b \in \mathbb{Z}$ に対して, $\overline{x} = a + b\overline{\alpha}$ (x の複素共役) とする. α, $\overline{\alpha}$ は, 方程式 $X^2 - X + 5 = 0$ の 2 根になることに注意する. $\alpha\overline{\alpha} = 5$ なので, $\dfrac{1}{\alpha} = \dfrac{1-\sqrt{-19}}{10}$ であり, 特に R の商体は $\mathbb{Q}(\sqrt{-19})$ となる.

$x \in R$ に対して, $N(x) = x\overline{x}$ とする. $N(x)$ を x のノルムという. これは, x を複素数と見たときの大きさの 2 乗である. $x = a + b\alpha \in R$ $(a, b \in \mathbb{Z})$ とすると, $N(x) = a^2 + ab + 5b^2$ である.

補題 B.1　1.　任意の $x \in R$ に対して, $N(x) \in \mathbb{N} \sqcup \{0\}$ である.

2.　$x, y \in R$ に対して, $N(xy) = N(x)N(y)$

3.　$x \in R$ に対して,

(a)　$N(x) = 0 \Longleftrightarrow x = 0$.

(b)　$N(x) = 1 \Longleftrightarrow x = \pm 1$. これと 2. より, $R^\times = \{\pm 1\}$.

4.　$x \in R$, $(x \neq 0)$ に対して, x から生成される単項イデアルを $(x) = xR$ とするとき, $|R/xR| = N(x)$.

証明. 1, 2, 3 は, 容易に示すことができるので, 演習問題とする.

4. は上の節の単因子論 (3 節) の応用である. R を 1, α から生成される自由 $\mathbb{Z}$–加群 $R = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \alpha$ とみる. $x = a + b\alpha \in R$ $(a, b \in \mathbb{Z})$ とし, x を掛けるという $\mathbb{Z}$–加群の準同型写像を, この基底に対して行列表示す

る. $\alpha^2-\alpha+5=0$ を利用すると,

$$x\cdot 1 = a\cdot 1 + b\cdot\alpha,$$
$$x\cdot\alpha = a\alpha + b\alpha^2 = -5b\cdot 1 + (a+b)\cdot\alpha$$

より, 求める行列表示は, $\begin{pmatrix} a & -5b \\ b & a+b \end{pmatrix}$ である. 特に, この行列の行列式は, $N(x)$ に一致する. $\mathbb{Z}$ は PID なので, 単因子論を利用して, R の $\mathbb{Z}$–基底を取り替えることにより[*4], x の行列表示は $\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}(d_i\in\mathbb{N})$ の形にできる. さらにこの際, 行列式の値は符号 ($\mathbb{Z}$ の単元倍) だけが変化するので, $d_1d_2=N(x)$ である. この基底を利用すると, 加法群として $R/xR\cong\mathbb{Z}/d_1\mathbb{Z}\oplus\mathbb{Z}/d_2\mathbb{Z}$ である. よって, $|R/xR|=d_1d_2=N(x)$ が成立する.

問 B.1　上の補題の 1, 2, 3 を証明せよ.

定理 B.1　R は Euclid 整域ではない.

証明.　R が Euclid 整域であるとし, $\varphi: R\to N$ を定義 2.9 にある, R から整列集合 N への写像とする. $S=R\setminus\{0,\pm1\}$ とする. N は整列集合なので, $\varphi(S)$ には最小元が存在する. $x\in S$ を $\varphi(x)$ が $\varphi(S)$ の最小元になる元とする. このとき, $|R/xR|\leqq 3$ である. 実際, $a\in R$ とすると, $a=xq+r$, $\varphi(r)<\varphi(x)$ となる $q,r\in R$ が存在するが, x の取り方から, $r=0,\pm1$ となり, R の任意の元は xR を法として, $0,\pm1$ と一致する. すなわち $|R/xR|\leqq 3$ である. 一方, $x\neq 0,\pm1$ なら, $N(x)\geqq 4$ が成立する (下の問 B.2) ので, 補題 B.1, 4. より $|R/xR|=N(x)\geqq 4$ となり矛盾する.

問 B.2　$x\in R$, $x\neq 0,\pm1$ なら, $N(x)\geqq 4$ を示せ.

R が PID であることを示すには, 次の補題をまず用意する.

補題 B.2　A を可換環, N を整列集合とする. 写像 $\psi: A\to N$ で次の性質 (P) を持つものが存在すれば, A は PID である[*5].

$$\text{(P)}\begin{cases} 1. & x\in R, x\neq 0 \text{ に対して, } \psi(0)<\psi(x). \\ 2. & x,y\in A,\ x\neq 0,\ \psi(y)\geqq\psi(x) \implies x\mid y \text{ または } \exists z,w\in A,\ \text{s.t. } \psi(0)<\psi(xw+yz)<\psi(x). \end{cases}$$

証明. Euclid 整域が PID になることの証明と同じである. $I\in A$ を A のイデアルとする. $x\in I$ を $\psi(x)$ が $\psi(I\setminus\{0\})$ の最小元を与えるものとする. このとき, $I=(x)$ が成立する. 実際, $y\in I$, $y\neq 0$ とする. x の取り方から, $\psi(y)\geqq\psi(x)$ である. $x\nmid y$ とすると, 仮定より $z,w\in A$ が存在して, $\psi(0)<\psi(xz+yw)<\psi(x)$ となる. $x,y\in I$ なので, $xz+yw\in I$ となるが, これは x の取り方に矛盾する. よって, $x\mid y$ となり, $y\in(x)$ となって, $I=(x)$ である.

上の性質 (P) の ψ が存在する場合, 2. において常に $z=1$ と取ることができれば, ψ は定義 2.9 の φ と同じ性質を持ち, R は Euclid 整域になる.

命題 B.1　$R=Z\left[\dfrac{1+\sqrt{-19}}{2}\right]$ において, ノルム写像 $N: R\to\mathbb{Z}_{\geqq 0}=\{k\in\mathbb{Z}\mid k\geqq 0\}$ は, 補題 B.2 の性質 (P) を持つ. 特に R は PID である.

[*4] x を掛ける前に使う基底と掛けた後に使う基底は同じものではない

[*5] 左辺の不等号は本質的である. $w=y$, $z=-x$ とすると, $\psi(xy+y(-x))=\psi(0)$ となることに注意せよ.

証明. $x \in R$, $x \neq 0$ なら $N(x) > N(0) = 0$ が成立するので, N は (P) 1. の性質を満たす.

以下では, R 及びその全商体 $\mathbb{Q}(\sqrt{-19})$ を複素数体 $\mathbb{C}$ の部分環及び部分体とみなして議論をする. そのとき $N(x)$ の値は, 複素数としての大きさの 2 乗であることを利用する. 下の図を補助的に利用する. 図は, 複素平面内で R の点 0, 1, α, $1+\alpha$ を頂点とする平行 4 辺形と 0, 1, α, $1+\alpha$ を中心とする半径 1 の 4 つの円, $\dfrac{\alpha}{2}$, $\dfrac{1}{2}+\dfrac{\alpha}{2}$, $1+\dfrac{\alpha}{2}$ を中心とする半径 $\dfrac{1}{2}$ の 3 つの円が書かれている.

x, $y \in R$ として, $x \neq 0$, $N(y) \geqq N(x)$ かつ $x \nmid y$ とする. $\dfrac{y}{x} \in \mathbb{Q}(\sqrt{-19})$ を考えると, R の定義から, $a \in R$ が存在して,

$$\frac{y}{x} = a + r + s\alpha, \quad s, r \in \mathbb{Q},\ 0 \leqq r < 1,\ 0 \leqq s < 1,\ r + s\alpha \neq 0 \tag{B.1}$$

とできる. すなわち, $r + s\alpha$ を図の平行 4 辺形の中 (一部境界を含む) にとる.

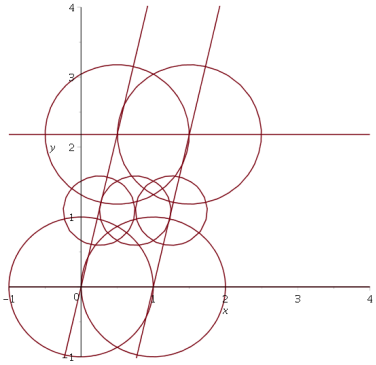
このとき, $r + s\alpha$ に最も近い R の点を b (b は $0, 1, \alpha, 1+\alpha$ のどれか) として, $r' = r + s\alpha - b$ とおくと,

$$\frac{y}{x} = a + b + r', \quad a + b \in R,\ r' \in \mathbb{Q}(\sqrt{-19}),\ r' \neq 0$$

となる. $N(r') < 1$ なら (図において, 半径 1 の 4 つのどれかの円の内部に r が含まれるとき), $w = -(a+b)$, $z = 1$ とおくと,

$$0 < N(r'x) = N(r')N(x) < N(x), \quad r'x = -(a+b)x + y = xw + yz$$

となり, 補題 B.2 の (P) 2. が満たされる.



$N(r') \geqq 1$ とする. このとき, 図の小さい 3 つの円を見ると, $r + s\alpha$ と 3 点 $\dfrac{\alpha}{2}$, $\dfrac{1}{2}+\dfrac{\alpha}{2}$, $1+\dfrac{\alpha}{2}$ のどれかとの距離は $\dfrac{1}{2}$ より小さいことがわかる. 全体を 2 倍すると, $2(r + s\alpha)$ と α, $1+\alpha$, $2+\alpha$ のどれかとの距離は 1 より小さい. 上と同様に考えると, $a' \in R$ が存在して, $N\left(\dfrac{2y}{x} - a'\right) < 1$ である.

ここで, $\dfrac{2y}{x} - a' \neq 0$ なら, $w = -a'$, $z = 2$ とすれば, 補題 B.2 の (P) 2. の性質を満たすことは, 上と同様である.

$\dfrac{2y}{x} - a' = 0$ とする. このとき, (B.1) で定まる $r + s\alpha$ は, $r + s\alpha \in \dfrac{1}{2}R = \left\{\dfrac{q}{2} \mid q \in R\right\}$ とその取り方から, $\dfrac{\alpha}{2}$ であるか $\dfrac{1+\alpha}{2}$ のいずれかである. これらについて, 場合分けをして考える.

- $\dfrac{y}{x} = a + \dfrac{\alpha}{2}$, $a \in R$ のとき. $\alpha(1-\alpha) = 5$ に注意する. $-ax + y = \dfrac{\alpha}{2}x$ の両辺に $1-\alpha$ を掛けると,

$$-(1-\alpha)ax + (1-\alpha)y = \frac{\alpha(1-\alpha)}{2}x = \frac{5}{2}x$$

$2x$ を左辺に移して,

$$-\{2+(1-\alpha)a\}x+(1-\alpha)y=\frac{1}{2}x\neq 0.$$

よって, 補題 B.2 (P) 2. において, $w=-2-(1-\alpha)a$, $z=1-\alpha$ を取ることができる.

- $\dfrac{y}{x}=a+\dfrac{1+\alpha}{2}$, $a\in R$ のとき. $\alpha(\alpha+1)=2\alpha-5$ を用いる. $-ax+y=\dfrac{1+\alpha}{2}$ の両辺に α を掛けて,

$$-a\alpha x+\alpha y=\frac{2\alpha-5}{2}x=\alpha x-\frac{5}{2}x.$$

左辺に, $(\alpha-2)x$ を移行して,

$$-(a\alpha+\alpha-2)x+\alpha y=-\frac{1}{2}x\neq 0.$$

となり, 上と同じように, 補題 B.2 (P) 2. の成立が示される.

問 B.3　領域 $\left\{a+b\dfrac{1+\sqrt{-19}}{2}\mid 0\leqq a\leqq 1,\ 0\leqq b\leqq 1\right\}$ が上の図の 7 つの円で被覆されることを示せ.

問 B.4　$\mathbb{Z}\left[\dfrac{1+\sqrt{-15}}{2}\right]$ では, 上のような証明が成立しない. 実際, この環は PID ではない. どこがうまくいかなくなるかを確かめよ.

C　Zorn の補題の応用

次が Zorn の補題と呼ばれるものである. 順序集合の定義, 順序集合での上界, 極大等の定義は, 幾何序論で学ぶであろうから, ここでは省略する. Zorn の補題は, 選択公理, 整列可能性定理と同値な命題で, 現代の数学では, 通常これを仮定して議論をする. 選択公理は, 現代数学で通常用いられる Zermero–Fraenkel(ツェルメロ–フレンケル) の集合論の公理からは独立した命題であること, すなわち, 集合論の公理系からは肯定も否定も証明できないことが知られている.

補題 C.1（Zorn の補題）　M を空でない (半) 順序集合とする. M の (空でない) 全順序部分集合が常に上界をもつなら, M には極大元が存在する.

C.1　極大イデアルの存在

定理 C.1　R を可換環, I を R の自明でないイデアルとすると, I を含む極大イデアルが存在する.

証明.

$$\mathcal{I}=\{J\subsetneqq R\mid J\text{ は }I\text{ を含むイデアル}\}$$

とおく. 集合の包含関係で順序を入れると, $\mathcal{I}$ は帰納的順序集合になることを示す.

全順序部分集合 $\mathcal{I}'\subset\mathcal{I}$ に対して,

$$J'=\bigcup_{J\in\mathcal{I}'}J$$

とおくと, J' は, $\mathcal{I}'$ の上界になる. 実際, $J' \supset I$ は明らかである. また, 任意の $\mathcal{I}'$ の元 J に対して, $1 \notin J$ なので, $1 \notin J'$ である. よって, $J' \neq R$ である. また, $a, b \in J'$ とすると, $a \in J_1$, $b \in J_2$ となる $J_1, J_2 \in \mathcal{I}'$ が存在する. J_1, J_2 のうち, 順序の大きい方を J'' とすると, $a, b \in J''$ で, J'' はイデアルだから, $a+b \in J'' \subset J'$ である. この状況のもとで, $r \in R$ に対して, $ra \in J_1 \subset J'$ でもある. よって, J' は R の真のイデアルであり, $\mathcal{I}'$ の上界である.

ここで, Zorn の補題 (定理 C.1) を用いると, $\mathcal{I}$ には極大元 $\mathfrak{m}$ が存在する. $\mathfrak{m} \in \mathcal{I}$ なので, $\mathfrak{m}$ は R の真のイデアルである. $\mathfrak{m} \subset J$ となる真のイデアル J が存在すると, $I \subset J$ となるので, $J \in \mathcal{I}$ となり, $\mathcal{I}$ での $\mathfrak{m}$ の極大性から $\mathfrak{m} = J$ となり, $\mathfrak{m}$ は R の極大イデアルである.

C.2 ベクトル空間の基底の存在

定義 C.1（ベクトル空間） $\mathbb{K}$ を体 (斜体でも良い) としたときに, $\mathbb{K}$–加群の M のことを $\mathbb{K}$ 上のベクトル空間という. K が斜体であるなら, 左加群, 右加群に応じて, 左ベクトル空間, 右ベクトル空間という.

定理 C.2 ベクトル空間には, 基底が存在する. ベクトル空間の基底の濃度は, 取り方によらず一定である.

証明. 左ベクトル空間について証明する.

M を体 $\mathbb{K}$ 上の左ベクトル空間とし, M の次のような部分集合の族を考える.

$$\mathcal{B} = \{B \subset M \mid B \text{ の任意の有限部分集合は, 1 次独立な元からなる } \}$$

$\mathcal{B}$ は, 集合の包含関係で順序を入れたときに, 帰納的順序集合となる. 実際, $\mathcal{B}' \subset \mathcal{B}$ を全順序部分集合とする. このとき,

$$B' = \bigcup_{B \in \mathcal{B}'} B$$

は $\mathcal{B}'$ の上界になる. なぜなら, B' の任意の有限部分集合 S をとると, $S \subset B$ となる $B \in \mathcal{B}'$ が取れるので, S の元は 1 次独立だからである.

Zorn の補題より, $\mathcal{B}$ には極大元 E が存在する. E は M の基底になる. 実際, $E \in \mathcal{B}$ だから, E の有限部分集合は, 1 次独立である. さらに, 任意の $x \notin E$, $x \neq 0$ に対して, $E \cup \{x\} \notin \mathcal{B}$ だから, ある有限集合 $S \subset E$ が存在して, $S \cup \{x\}$ は 1 次独立な集合ではない. よって

$$ax + \sum_{s \in S} a_s s = 0, \quad a,\ a_s \in \mathbb{K}$$

となる非自明な線形関係が存在する. $a = 0$ とすると, S の元の 1 次独立性から $a_s = 0, \forall s \in S$ となって, 自明な線形関係になる. よって, $a \neq 0$ となり,

$$x = -\frac{1}{a} \sum_{s \in S} a_s s$$

となる. このことから, M の任意の元は, E の元の線形結合で表示できるのがわかる.

無限次元の場合の基底の濃度が一定であることは, その事実を要求される事が少ないので, 証明は省略する. 有限次元の場合の基底の個数の一意性は, 線形代数学の教科書を参照すること.

定義 C.1　$\mathbb{K}$ を体, V を $\mathbb{K}$ 上のベクトル空間とするとき, 上で定まる V の基底の濃度を V の $\mathbb{K}$ 上の次元といい, $\dim_{\mathbb{K}} V$ で表す.

包含関係 $\mathbb{Q} \subset \mathbb{R}$ を考えると, $\mathbb{R}$ は $\mathbb{Q}$ 上のベクトル空間になる. この $\mathbb{Q}$ ベクトル空間としての基底は, Lebesgue(ルベーグ) 非可測集合になることが証明できる. (来年度の関数解析学の講義で出てくるかも.)

D　UFD 上の多項式環が UFD になること

D.1　局所化 (分数化) と商体

環の極大イデアルに対する剰余環は体になる. これとは別に, 環の元の分数を考えることによって体を作る方法がある. 整数環 $\mathbb{Z}$ から有理数体 $\mathbb{Q}$ を作る内容を公理化するのである. 分数の和と積を考えると, 分数の分母に現れる集合は, 「0 でない」という条件より少し弱くできて,「積で閉じている」でも分数計算が可能であることがわかる. すなわち, この分母の条件を少し弱くして分数を考えるのが, 局所化と呼ばれるもので, 「0 でない」のを全て分母に許容するのが, 商体と呼ばれるものである.

なお,「局所化」という日本語 (英語でも localization という) は, 「分数」とは無関係であるように見える.「局所化」という言葉遣いは, 下の例で, 素イデアル (の補集合) から定まる分数化に対して通常用いられる. なぜこのような言葉遣いをするのかは, 代数幾何学や代数的整数論を詳しく勉強しないとわからないので, 知りたい人は, 適当な参考書を参照していただきたい.

定義 D.1　R を可換環とする. R の部分集合 $R \supset S$ が積閉集合 (あるいは乗法的閉集合, multiplicatively closed set) であるとは, 次を満たすことを言う.

1. $a, b \in S \Longrightarrow ab \in S$
2. $1 \in S, \quad 0 \notin S$

例 D.1　R を可換環とするとき, 次は積閉集合である.

1. $x \in R$ とし, x が零因子でないとしたとき, $\{\ x^n \mid n = 0, 1, 2, \dots\ \}$
2. $S = \{a \in R \mid a \neq 0,\ a$ は零因子でない $\}$. 特に R が整域であるとき, $S = R \setminus \{0\}$. (R が整域でなければ, $R \setminus \{0\}$ は, 定義の 2. の $0 \notin S$ が問題となる).
3. $\mathfrak{p}$ を R の素イデアルとするとき, $R \setminus \mathfrak{p}$ (命題 2.1, 1.)

問 D.1　上の例の集合が積閉集合になることを確かめよ.

R を可換環, S を R の積閉集合であるとして, 直積集合 $R \times S$ に次で同値関係を入れる. 分数において「約分しても同じ分数」であることを環の場合に拡張したものであるが,「割り算」をするわけにはいかないので, 下のような定義になる.

$$(a_1, s_1) \sim (a_2, s_2) \Longleftrightarrow \text{ある } s \in S \text{ が存在して, } (a_1 s_2 - a_2 s_1)s = 0, \quad (a_i, s_i) \in R \times S,\ (i = 1, 2)$$

定義から, $s \in S$ に対して, $(s, s) \sim (1, 1)$ となることに注意する.

問 D.2　上で定めた $\sim$ が $R \times S$ の同値関係になることを示せ.

$R \times S/\sim$ を R_S あるいは $S^{-1}R$ と書く. $(a, s) \in R \times S$ とし (a, s) を代表元とする R_S の元を (a/s) と書

くことにする．R_S に次の規則で和と積を定義する (分数の和と積の規則).

$$(a_1/s_1) + (a_2/s_2) = ((a_1s_2 + a_2s_1)/s_1s_2)$$
$$(a_1/s_1)(a_2/s_2) = (a_1a_2/s_1s_2), \qquad (a_i/s_i) \in R_S,\ (i = 1, 2)$$

命題 D.1　上の和と積の規則は well–defined で, R_S は零元 $(0/1)$, 単位元 $(1/1)$ を持つ可換環になる．

証明.　和が well–defined であることだけを示す (残りは下の問). $(a_1/s_1) = (a_1'/s_1')$, $(a_2/s_2) = (a_2'/s_2')$ とする．このとき, $s,\ t \in S$ が存在して, $(a_1s_1' - a_1's_1)s = 0$, $(a_2s_2' - a_2's_2)t = 0$ となる．このとき,

$$\{(a_1s_2 + a_2s_1)s_1's_2' - (a_1's_2' + a_2's_1')s_1s_2\}\, st = (a_1s_1' - a_1's_1)s(s_2s_2't) + (a_2s_2' - a_2's_2)t(s_1s_1's) = 0$$

となるので, $(a_1/s_1) + (a_2/s_2) = (a_1'/s_1') + (a_2'/s_2')$ が成立する．

問 D.3　上の定理の証明の省略された部分を埋めよ．

上で定義された R_S を R の S による商環あるいは局所化という (商環と剰余環という 2 つの言葉が出てきているが, その違いに注意すること). $\mathfrak{p}$ を R の素イデアルとして, $S = R \setminus \mathfrak{p}$ であるときには, (記号に統一性が無いが) $R_{S\setminus\mathfrak{p}}$ とは書かずに, $R_{\mathfrak{p}}$ と書く．

例 D.2　$R = \mathbb{Z}$ とし, $p \in \mathbb{Z}$ を素数とする．(p) を p が生成する素イデアル, $S = \mathbb{Z} \setminus (p)$ とする．$\mathbb{Z}$ の S による局所化を $\mathbb{Z}_p$ と書き, p–進整数環という．整数論では重要な環である．「p–進」という言葉遣いをする理由を解説するのは大変なので, 興味のある人は, 代数的整数論の専門書を参照していただきたい.

$$\mathbb{Z}_p = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0,\ (b, p) = 1 \right\}$$

問 D.4　R を整域, $\mathfrak{p}$ を R の素イデアルであるとする．$\mathfrak{p}$ を下の写像 i で $R_{\mathfrak{p}}$ の部分集合と見た時, $R_{\mathfrak{p}}$ は $\mathfrak{p}$ を唯一の極大イデアルに持つ局所環になることを示せ.

R_S の積と和の定義, および零元と積の単位元の定義から, 写像

$$i : R \ni a \mapsto (a/1) \in R_S$$

は, 環の準同型写像になる．これによる S の像を考える．$s \in S$ に対して, $i(s) = (s/1)$ は, R_S の中で積に関する逆元 $(1/s)$ を持つ．すなわち, $i(S) \subset (R_S)^\times$ である．R_S は S の積に関する逆元を付け加えた環であるとも言える．

i の核を考えると, $R \times S$ で $(a, 1) \sim (0, 1)$ となる条件を書き下せば,

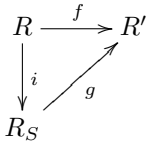
$$\mathrm{Ker}(i) = \{a \in R \mid s \in S \text{ が存在して, } as = 0\}$$

となる．よって, S が零因子を含まなければ, i は単射となり, R と $i(R)$ を同一視することにより, R は R_S の部分環であると思うことにする.

R の積閉集合 S に対して, S の積における逆元を付け加えて環を作るという操作において, R_S が最も一般的な環であることを, 次の定理は述べている.

定理 D.1（**商環の普遍性** (universality)）　R を可換環, $S \subset R$ を積閉集合とし, $i : R \to R_S$ を上で定めた自然な準同型写像とする．R' を別の可換環, $f : R \to R'$ を環の準同型写像で, $f(S) \subset (R')^\times$ となるものとする.

このとき, 環の準同型写像 $g : R_S \to R'$ で, $f = g \circ i$ となるものが, 一意的に存在する.



証明. $(x/s) \in R_S,\ x \in R,\ s \in S$ に対して, $g((x/s)) = f(x)f(s)^{-1}$ で定義する ($f(S) \in (R')^\times$ だから, $f(s)$ は R' の単元であることに注意する). まず, これが well–defined であることに注意する. R_S において, $(x/s) = (x'/s')$ であるとすると, $t \in S$ が存在して, $(xs'-x's)t = 0$ となる. このとき, $(f(x)f(s')-f(x')f(s))f(t) = 0$ となるが, $f(t)$ は R' の単元だから $f(x)f(s') = f(x')f(s)$ となり, $f(x)f(s)^{-1} = f(x')f(s')^{-1}$ を得る.

g が環の準同型写像になることは, f が準同型写像であることから従い, $f = g \circ i$ となることは, 定義から明らかである. また, 上のような性質を持つ g が存在すれば, $g((x/s)) = g((x/1)(1/s)) = g((x/1)(s/1)^{-1}) = f(x)f(s)^{-1}$ でなければならないので, これから一意性が従う.

S として, R の非零因子全体の集合を取ったとき, $R_S = Q(R)$ と書いて, R の全商環という. R が整域なら, $S = R \setminus \{0\}$ となり, 全商環は体になる. これを整域 R の (全) 商体という.

例 D.3　1. $R = \mathbb{Z}$ ならその全商体は $\mathbb{Q}$ になる.

2. K を体として $R = K[X_1, \ldots, X_n]$ を K 上の n 変数多項式環とする. 全商体の定義から, R の全商体は 0 でない元を分母にした元からなる体である. これを $K(X_1, \ldots, X_n)$ と書き, K の n 変数の有理関数体という.

$$K(X_1, \ldots, X_n) = \left\{ \frac{f(X_1, \ldots, X_n)}{g(X_1, \ldots, X_n)} \mid f,\, g \in K[X_1, \ldots, X_n],\ g \neq 0 \right\}$$

D.2　UFD 上の多項式環は UFD

全商体を導入することにより, 次の定理が証明できるようになる.

定理 D.2　R を UFD とすると, R 上の多項式環 $R[X]$ も UFD である.

この定理を仮定すると, n に関する帰納法で次の系が証明できる. 実際, $n = 1$ のときには, $K[X]$ はユークリッド整域なので UFD であり, $n \geqq 2$ のときは, $K[X_1, \ldots, X_n] = K[X_1, \ldots, X_{n-1}][X_n]$ を利用すれば良い.

系 D.1　K を体とすると K 上の n 変数多項式環 $K[X_1, \ldots, X_n]$ は UFD である.

定理 D.2 を証明するために, 少し準備をする.

以下では, R は UFD とする. よって, 任意の $a \in R$, $(a \neq 0)$ は素元の積に (単元倍を除いて) 一意的に書くことができる. また UFD では, 素元と既約元の概念が一致することも, 思い出しておく. 今後, 素因数分解を考えるときには, 単元倍だけの差異は無視して考える.

素元の積への一意的な分解を利用すると, $a, b \in R$ に対して, a, b の最大公約数が (単元倍を除いて) 一意的に決まる. 通常の整数で考えることを, 素元の積への分解を利用して実行すれば良いのである.

K を R の全商体とする. R は整域なので, 上で述べたように, 自然に K の部分環であるとみなす ($r \in R$ は $(r/1) \in K$ と見る). $f(X) \in R[X]$ もこの埋め込みを利用して, $K[X]$ の元と見る.

$f(X) = a_nX^n + \cdots + a_1X + a_0 \in R[X]$ は, $a_0, \ldots, a_n$ の最大公約数が 1 であるとき, すなわち, $a_0, \ldots, a_n$ の全てを割り切る素元が存在しないとき, $f(X)$ は原始的 (primitive) であるという.

補題 D.1 R を UFD, $R \subset K$ を R の全商体とする. $f(X) \in K[X]$ に対して, $c \in K$ と原始的な多項式 $f_0(X) \in R[X]$ が存在して, $f(X) = cf_0(X)$ と書ける. c は R の単元倍を除いて, $f(X)$ から一意的に定まる.

証明.

$$f(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in K[X]$$

とする. $c_i \in K$ だから, $c_i = \dfrac{a_i}{b_i}$, $a_i, b_i \in R$ と書ける. 各項の係数の分母をまとめると,

$$f(X) = \frac{1}{b_n \cdots b_0}\left\{(a_nb_{n-1}\cdots b_0)X^n + (a_{n-1}b_nb_{n-2}\cdots a_0)X^{n-1} + \cdots + (a_1b_n\cdots b_2b_0)X + (a_0b_n\cdots b_1)\right\}$$

となる. ここで, 左辺の括弧の中の多項式の係数に注目する.

$$a_nb_{n-1}\cdots b_0, \quad a_{n-1}b_nb_{n-2}, \ \ldots\ , a_1b_n\cdots b_2b_0, \quad a_0b_n\cdots b_1$$

の最大公約数を a とおき, $b = b_n\cdots b_0 \in R$ とする. 括弧の中の X^i の係数から, $a_ib_n\cdots b_{i+1}b_{i-1}\cdots b_0 = ac_i'$ で, c_i' を定めると, a は左辺の約数であるから, $c_i' \in R$ である. $f_0(X) = c_n'X^n + c_{n-1}'X^{n-1} + \cdots + c_1'X + c_0'$, $c = \dfrac{a}{b}$ とおくと, $f(X) = cf_0(X)$ で, $f_0(X) \in R[X]$ は原始的である.

$f(X)$ が $R[X]$ の原始的な多項式 $h(X)$ と $c' \in K$ を用いて, $f(X) = c'h(X)$ と別の書き方ができたとする. $c' = \dfrac{a'}{b'}$, $a', b' \in R$ とする. 約分をすることにより, 上で定めた a, b および a', b' の最大公約数は 1 であるとして良い.

$$f(X) = \frac{a}{b}f_0(X) = \frac{a'}{b'}h(X)$$

となる. これより分母を払えば,

$$b'af_0(X) = ba'h(X)$$

となる. よって, a は $ba'h(X)$ の係数の公約数になるが, a と b の最大公約数は 1 で, $h(X)$ は原始的なので, $a|a'$ となる. 逆のことを考えると, $a'|a$ となり, 命題 2.4, 1. より, $a \approx a'$ となる. b, b' についても同様の考察ができ, $b \approx b'$ となるので, c, c' は単元倍を除いて一致する.

定義 D.2 R を UFD, K を R の全商体とする. $f(X) \in K[X]$ に対して, 上の命題 D.1 で定まる c を f の内容 (content) といい, $I(f)$ で表す (I はドイツ語の Inhalt が由来).

補題 D.2（Gauss の補題） 上の定義の仮定の元で, 次が成立する.

1. $f(X), g(X) \in R[X]$ が原始的であれば, $f(X)g(X)$ も原始的である.
2. $f(X), g(X) \in K[X]$ とすると, $I(f)I(g)$ と $I(fg)$ は R の単元倍を除いて一致する.

証明. 1.

$$f(X) = a_mX^m + a_{m-1}X^{m-1} + \cdots + a_0$$
$$g(X) = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_0$$

とする．R は UFD だから, $f(X)g(X)$ のすべての係数を約数であるような素元が存在しないことを示せばよい．$p \in R$ を素元とする．$f(X)$, $g(X)$ は原始的だから, $a_m, \ldots, a_0$, $b_n, \ldots, b_0$ それぞれの中に, p が約数とならない元が存在する．$p \nmid a_i$ となる最小の i と $p \nmid b_j$ となる最小の j をとる．このとき, $f(X)g(X)$ の X^{i+j} の係数は,

$$(a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0)$$

となるが, $a_0, \ldots, a_{i-1}$ は p の倍数, $b_0, \ldots, b_{j-1}$ は p の倍数だから, 上の式の括弧で括られた部分は p の倍数である．しかし, a_i, b_j はともに p を約数に持たず, p が素元であることから, a_ib_j も p を約数に持たない．よって上の式は, 全体として p を約数に持たない．p は任意の素元として取れるので, 結局 $f(X)g(X)$ の係数の公約数であるような素元は存在しない．

2. $f(X) = I(f)f_0(X)$, $g(X) = I(g)g_0(X)$ だから, 両辺の積を取ると $f(X)g(X) = I(f)I(g)f_0(X)g_0(X)$ である．1. より, $f_0(X)g_0(X)$ も原始的であるから, 補題 D.1 より, $I(fg)$ と $I(f)I(g)$ は R の単元倍を除いて, 一致する．

命題 D.2　R を UFD とし, K を R の全商体とする．R は K の部分環なので, $f(X) \in R[X]$ は自然に (f の係数の元を K の元だと思って) $K[X]$ の元であると思える．このとき, $f(X)$ が $R[X]$ で既約なら, $K[X]$ でも既約である．

証明.　f が $K[X]$ で, $f(X) = g(X)h(X)$, $g, h \in K[X]$ と分解されたとする．両辺の内容を考えると, 補題 D.2, 2. より, $I(g)I(h) = \varepsilon I(f)$, $\varepsilon \in R^\times$ となる．一方, I の定義から, $f \in R[X]$ なら $I(f) \in R$ であり, $R[X]$ の原始的な多項式, f_0, g_0, h_0 が存在して, $f(X) = I(f)f_0(X)$, $g(X) = I(g)g_0(X)$, $h(X) = I(h)h_0(X)$ となる．よって,

$$\begin{aligned} f(X) &= I(f)f_0(X) \\ &= g(X)h(X) = I(g)I(h)g_0(X)h_0(X) = \varepsilon I(f)g_0(X)h_0(X) \end{aligned}$$

となる．$I(f)$, $\varepsilon \in R$ だから, $\varepsilon I(f)g_0$, $h_0 \in R[X]$ となるが, これは, f の $R[X]$ での因数分解を与えている．f は $R[X]$ で既約であるので, g_0 か h_0 のいずれかは, 次数が 0 となり, これより, f の $K[X]$ での既約性が従う．

注意 D.1　1. R を UFD とし, $f(X) \in R[X]$ が $f(X) = g(X)h(X)$, $g(X), h(X) \in K[X]$ と $K[X]$ の元で因数分解できたとする．このとき, 上の証明から, $g(X)$, $h(X)$ の係数を定数倍して $g(X), h(X) \in R[X]$ と取れることが示されている．

2. $R = \mathbb{Z}$, $K = \mathbb{Q}$ のとき, 上の命題は高校の数学で, 暗に利用されている．例えば, $f(X) = X^3 + 3X + 1$ が $\mathbb{Q}$ 上で既約であることを確かめるのに, $f(\pm 1) \neq 0$ だけを確かめている．しかし, 冷静に考えてみると, これは $\mathbb{Z}$ 上の既約性を確かめているだけに過ぎない．しかし, 上の命題から, $f(X)$ は $\mathbb{Q}$ 上の多項式と見ても既約であることが分かる．

補題 D.3　R を UFD とする．

1. $p \in R$ を素元とすると, p は $R[X]$ でも素元である．
2. $f(X) \in R[X]$ を既約な原始的多項式とすると, $f(X)$ は $R[X]$ の素元である．

証明.　1. $f(X), g(X) \in R[X]$ とし, $p \mid f(X)g(X)$ とする．内容と原始的な多項式を用いて, $f(X) = I(f)f_0(X)$, $g(X) = I(g)g_0(X)$ と書く．このとき, $f(X)g(X) = I(f)I(g)f_0(X)g_0(X)$ で, $I(f)$, $I(g) \in R$ と

なる．ガウスの補題 (補題 D.2) より，$f_0(X)g_0(X)$ は原始的である．よって，$p \mid I(f)I(g)$ を得る．p は R の素元なので，$p \mid I(f)$ または $p \mid I(g)$ となるが，これに応じて，$p \mid f(X)$ または $p \mid g(X)$ となり，p は $R[X]$ の素元である．

2. $f(X) \mid g(X)h(X)$, $g(X), h(X) \in R[X]$ とする．K を R の全商体として，この約数関係を $K[X]$ で考える．$f(X)$ の $K[X]$ で既約性 (命題 D.2) と $K[X]$ が UFD であることより，$f(X)$ は $K[X]$ で素元である (命題 2.6)．よって，$K[X]$ で $f(X) \mid g(X)$ または $f(X) \mid h(X)$ が成立する．例えば，$f(X) | g(X)$ であるとし，$g(X) = f(X)q(X)$, $q(X) \in K[X]$ とする．両辺の内容を考えると，$I(g) = \varepsilon I(f)I(q)$, $\varepsilon \in R^\times$ となるが，f が原始的なので，$I(f) = 1$ であり，$g \in R[X]$ より，$I(g) \in R$ となる．よって，$I(q) \in R$ となるので $q(X) \in R[X]$ となり，$R[X]$ で $f(X) \mid g(X)$ となる．$f(X) \mid h(X)$ の場合も同様なので，結局 $R[X]$ で $f(X) \mid g(X)$ または $f(X) \mid h(X)$ が成立し，f は素元である．

定理 D.2 の証明. $f(X) \in R[X]$ が素元の積に書けることを示す．$f(X) = I(f)f_0(X)$ で，$f_0(X) \in R[X]$ は原始的である．R は UFD で $I(f) \in R$ だから，R の素元 $p_1, \ldots, p_r$ が存在して，$I(f) = p_1 \cdots p_r$ となる．K を R の全商体とするすると，$K[X]$ は UFD である．$f_0(X) \in K[X]$ と見て素元分解すると，$K[X]$ の既約な多項式 $q_1, \ldots, q_s$ が存在して，$f_0(X) = q_1(X) \cdots q_s(X)$ となる．両辺の内容を考えると，

$$I(f_0) = 1 = I(q_1) \cdots I(q_s), \qquad I(q_i) \in K \ (i = 1, \ldots, s)$$

を得る．内容の定義から，$\dfrac{q_i(X)}{I(q_i)} \in R[X]$ で，かつこの多項式は原始的でさらに既約である．すなわち，これらは $R[X]$ の素元である．上の式から，

$$f(X) = I(f)f_0(X) = p_1 \cdots p_r \frac{q_1(X)}{I(q_1)} \cdots \frac{q_s(X)}{I(q_s)}$$

は $f(X)$ の $R[X]$ での素元分解を与える．

上の証明から，次の系を得る．

系 D.2 R を UFD とすると，$R[X]$ の素元は R の素元 p もしくは，既約かつ原始的な多項式の 2 種類に限られる．

参考文献

[1] 小林正典, 寺尾宏明著, 線形代数講義と演習, 培風館.
[2] 砂田利一著, 行列と行列式 (現代数学への入門), 岩波書店.
[3] 佐武一郎著, 線型代数学 (新装版), 数学選書 1, 裳華房.
[4] 齋藤正彦著, 線型代数入門, 東京大学出版会.
[5] 松坂和夫著, 線型代数, 入門数学入門シリーズ 2, 岩波書店.
[6] 雪江明彦著, 代数学: 環と体と Galois 理論, 日本評論社.
[7] 森田康夫著, 代数概論, 裳華房.
[8] 堀田良之著, 可換環と体, 岩波書店.
[9] 堀田良之著, 代数入門（新装版） –群と加群–, 裳華房.
[10] 堀田良之著, 加群十話, 朝倉書店.

この講義ノートを作るにあたって参考にした書籍, および本文内で参照した書籍である. これら以外にも, 良書は沢山ある.