第 1 章　環

環の基礎事項について述べる。

1.1　環

定義 1.1.1 (環). 組 $(A, +, \cdot, 0, 1)$ が**環 (ring)** であるとは、次が成り立つことをいう [1]:

(R1)　$(A, +, 0)$ がアーベル群

(R2)　$(A, \cdot, 1)$ がモノイド

(R3) 分配律　$\forall x, y, z \in A$ に対し次が成り立つ:

$$\begin{cases} x \cdot (y + z) = x \cdot y + x \cdot z \\ (x + y) \cdot z = x \cdot z + y \cdot z \end{cases} \tag{1.1.1}$$

さらに

- 0 を A の**零元 (zero element)** といい、0_A とも書く。
- 1 を A の**単位元 (unit element)** といい、1_A とも書く。

注意 1.1.2. 環の元が乗法に関する左逆元を持つとしても右逆元を持つとは限らない。

例 1.1.3 (可換環の例).

- (零環) 1 点集合 $\{0\}$ には環構造が一意に定まる。これを**零環 (zero ring)** という。環 A が零環であることと $0_A = 1_A$ であることとは同値である。
- (整数環) 有理整数環 $\mathbb{Z}$ や Gauss 整数環 $\mathbb{Z}[i]$ は可換環である。
- (関数環) 位相空間 X 上の $\mathbb{C}$ 値連続関数全体のなす環 $C(X)$ は点ごとの和と積を演算として可換環となる。

例 1.1.4 (非可換環の例).

- (全行列環) 環 A の全行列環 $M_n(A)$ は一般に非可換である。
- (自己準同型環) アーベル群 A (より一般に環上の加群) の自己準同型環 $\mathrm{End}(A)$ は点ごとの和と写像の合成を演算として環となる。これは一般に非可換である。

注意 1.1.5. 一般の環を A、可換環を R で書くことが多い。

例 1.1.6 (測度論との関連). [TODO] ring of sets などの話をしたい

1)　文献によっては環の定義に単位元の存在を仮定しない立場もある。

A. 反転環

反転環を定義する。

定義 1.1.7 (反転環)**.** $(A,+,\cdot)$ を環とする。集合 A^{OP} を $A^{\mathrm{OP}} \coloneqq A$ とおき、アーベル群 $(A^{\mathrm{OP}},+)$ に乗法 $\cdot'$ を

$$a \cdot' b \coloneqq b \cdot a \quad (a,b \in A^{\mathrm{OP}}) \tag{1.1.2}$$

で定めると、$(A^{\mathrm{OP}},+,\cdot')$ は環をなす。この環を A の**反転環 (opposite ring)** という。

例 1.1.8 (反転環の例)**.**

- R を可換環とすると、写像
$$M_n(R) \to M_n(R)^{\mathrm{OP}}, \quad X \mapsto {}^tX \tag{1.1.3}$$
は環同型となる。

B. 零因子と整域

零因子と、零因子を用いて定義される整域の概念を導入する。

定義 1.1.9 (零因子と整域)**.** A を環とする。$a \in A, a \neq 0$ が次をみたすとき、a は A の**零因子 (zero divisor)** であるという:

$$\exists x \in A, x \neq 0 \quad \text{s.t.} \quad ax = 0 \text{ or } xa = 0 \tag{1.1.4}$$

また、A が次のすべてをみたすとき、A を**整域 (integral domain)** という:

(I1) A は零環でない。
(I2) A は可換環である。
(I3) 零因子を持たない。

例 1.1.10 (零因子と整域の例)**.**

- $\mathbb{Z}$ は整域である。
- $\mathbb{Z} \times \mathbb{Z}$ は整域でない ((I1), (I2) をみたすが (I3) をみたさない)。零因子の例のひとつは
$$(1,0) \cdot (0,1) = (0,0) \tag{1.1.5}$$
である。
- Hamilton の四元数環 $\mathbb{H}$ は整域でない ((I1), (I3) をみたすが (I2) をみたさない)。

C. 可除環と体

可除環を定義する。

定義 1.1.11 (乗法群)**.** [TODO]

定義 1.1.12 (可除環). A を環とする。$A^\times = A \setminus \{0\}$ であるとき、A を**可除環 (division ring)** あるいは**斜体 (skew field)** という。可換な可除環を**体 (field)** という。

例 1.1.13 (可除環の例).

- 零環 $A = \{0\}$ は $A^\times = \{0\} \neq \varnothing = A \setminus \{0\}$ より可除環ではない。
- Hamilton の四元数環 $\mathbb{H}$ は可除環である。しかし非可換なので体でも整域でもない。
- $\mathbb{R}$ や $\mathbb{C}$ は可除環である。さらに可換なので体でもある。

可除環に対する次の性質は基本的である。

命題 1.1.14. 可除環は零因子を持たない。

証明　可除環 A が零因子 $x \neq 0$ を持ったとすると、ある $y \in A - \{0\}$ が存在して $xy = 0$ が成り立つ。一方 A は可換環だからある $x' \in A$ が存在して $x'x = 1$ が成り立つ。よって $y = 1y = x'xy = x'0 = 0$ となり $y \neq 0$ に矛盾。したがって A は零因子を持たない。 □

D.　冪等元

定義 1.1.15 (冪等元). A を環とする。$e \in A$ が $e^2 = e$ を満たすとき、e を A の**冪等元 (idempotent)** という。A の中心に属する冪等元をとくに**中心冪等元 (central idempotent)** という。

命題 1.1.16 (中心冪等元により生成される環). A を環とする。$e \in A$ が A の中心冪等元であるとき、Ae は A の両側イデアルとなり、さらに e を単位元とする環となる。

証明　省略 □

定義 1.1.17 (環準同型). [TODO]

1.2　イデアルと商環

イデアルの概念を導入する。

定義 1.2.1 (可換環のイデアル). R を可換環とする。$I \subset R$ が R の**イデアル (ideal)** であるとは、

(I1)　I は R の加法部分群
(I2)　$a \in R$, $b \in I$ ならば $ab \in I$

をみたすことをいう。

一般の環においてはイデアルに左/右/両側の区別がある。

定義 1.2.2 (一般の環のイデアル). A を環とする。$I \subset R$ が R の**左イデアル (left ideal)** であるとは、上の (I1) と

(LI2) $a \in A,\ b \in I$ ならば $ab \in I$

をみたすことをいう。**右イデアル (right ideal)** も同様に定義される。A の左かつ右イデアルを**両側イデアル (two-sided ideal)** という。明らかに可換環のイデアルは左かつ右かつ両側イデアルである。

定義 1.2.3 (固有イデアル). A を環、$I \subset A$ を左/右/両側イデアルとする。I が**固有 (proper)** であるとは、$I \neq A$ であることをいう。

環準同型とイデアルの間には次の関係がある。

定理 1.2.4 (環準同型とイデアル). A, B を環、$f\colon A \to B$ を環準同型とする。

(1) J が B の両側イデアルならば、$f^{-1}(J)$ は A の両側イデアルである。
(2) f が全射で I が A の両側イデアルならば、$f(I)$ は B の両側イデアルである。
(3) $\mathrm{Ker}\, f$ は A の両側イデアルである。
(4) f が全射ならば、$\mathrm{Im}\, f$ は B の両側イデアルである。
(5) $\mathrm{Im}\, f$ は B の部分環である。

証明 (1), (2) [TODO]
(3), (4) (1), (2) の特別な場合である。
(5) [TODO] □

環を両側イデアルで割った商は環をなす。

定義 1.2.5 (商環). [TODO]

環の両側イデアルは商環の両側イデアルと次の定理のように対応する。[TODO] 束の同型？

定理 1.2.6 (両側イデアルの対応原理). A を環、$I \subset A$ を両側イデアルとする。

$$\mathscr{I}_I(A) \coloneqq \{J\colon J \text{ は } I \text{ を含む } A \text{ の両側イデアル}\} \tag{1.2.1}$$
$$\mathscr{I}(A/I) \coloneqq \{J\colon J \text{ は } A/I \text{ の両側イデアル}\} \tag{1.2.2}$$

とおくと、

$$\widetilde{p}\colon \mathscr{I}_I(A) \to \mathscr{I}(A/I), \quad J \mapsto p(J) \tag{1.2.3}$$

は包含関係を保つ全単射であり、$\widetilde{p}$ の逆写像 q は

$$q\colon \mathscr{I}(A/I) \to \mathscr{I}_I(A), \quad J' \mapsto p^{-1}(J') \tag{1.2.4}$$

で与えられる。

注意 1.2.7. 定理より、A/I の両側イデアルは I を含む A の両側イデアル J を用いて J/I の形に一意的に書けて、さらに A の両側イデアル J, J' に関し

$$J' \subset J \quad \Longleftrightarrow \quad J'/I \subset J/I \tag{1.2.5}$$

が成り立つことがわかる。さらに、包含関係を保つことと $JJ'/I = (J/I)(J'/I)$ より、素イデアルは素イデアルと、極大イデアルは極大イデアルとそれぞれ対応することもわかる。

証明 q が well-defined であることを示す。A/I の両側イデアル J' に対し $p^{-1}(J')$ が A の両側イデアルであることは定理 1.2.4 より成り立ち、また $I = p^{-1}(0) \subset p^{-1}(J')$ も成り立つ。よって q は well-defined である。

q が $\widetilde{p}$ の逆写像であることを示す。$J' \in \mathcal{I}(A/I)$ に対し $p(p^{-1}(J')) = J'$ であることは p の全射性より従う。$J \in \mathcal{I}_I(A)$ に対し $p^{-1}(p(J)) = J$ であることを示す。"$\supset$"は集合の一般論より成り立つ。逆に $x \in p^{-1}(p(J))$ とすると、ある $j \in J$ が存在して $p(x) = p(j)$ となる。よって $p(x-j) = 0$ だから $x - j \in p^{-1}(0) = I \subset J$ である。したがって $x = (x-j) + j \in J$ が成り立つから"$\subset$"もいえた。よって q は $\widetilde{p}$ の逆写像である。

$\widetilde{p}$ が包含を保つことは写像による部分集合の像と逆像が包含を保つことから従う。以上で定理の主張が示された。 □

イデアルの演算について述べる。

定義 1.2.8 (加法部分群の和と積)**.** A を環、$I, J \subset A$ を加法部分群とする。

$$I + J \coloneqq \{a + b \mid a \in I,\ b \in J\} \tag{1.2.6}$$

$$IJ \coloneqq \left\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{Z}_{\geq 1},\ a_i \in I,\ b_i \in J \right\} \tag{1.2.7}$$

と書く。

命題 1.2.9 (イデアルの和と積)**.** A を環とする。

(1) A の任意の左 (resp. 右, 両側) イデアル $I, J \subset A$ に対し、$I + J$ は A の左 (resp. 右, 両側) イデアルである。

(2) A の任意の両側イデアル $I, J \subset A$ に対し、$I + J$ は A の両側イデアルである。

証明 [TODO] □

命題 1.2.10. A を環、$I \subset J$ を A の両側イデアルとする。このとき、環の同型

$$\frac{A/I}{J/I} \cong \frac{A}{J} \tag{1.2.8}$$

が成り立つ。

証明　図式

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/I \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ A/J & \xrightarrow[f]{} & \dfrac{A/I}{J/I} \end{array} \tag{1.2.9}$$

を可換にする環の同型が誘導されることを示せばよく、そのためには $J = \operatorname{Ker} q \circ \pi$ をいえばよい。$j \in J$ とすると $j + I \in J + I$ だから $q \circ \pi(j) = q(j + I) = 0$ である。よって $J \subset \operatorname{Ker} q \circ \pi$ である。逆に $q \circ \pi(a) = 0$ $(a \in A)$ とすると $\pi(a) \in J/I$ だから、両側イデアルの対応原理 (定理 1.2.6) より $a \in \pi^{-1}(J/I) = J$ である。したがって $J = \operatorname{Ker} q \circ \pi$ がいえた。準同型定理より上の図式を可換にする環の同型 f が誘導されて証明が完成した。 □

命題 1.2.11 (直積環のイデアル)**.** A, B を環とする。$A \times B$ の任意の左 (resp. 右/両側) イデアル J は A, B のある左 (resp. 右/両側) イデアル J_A, J_B を用いて $J = J_A \times J_B$ の形に書ける。

証明　[TODO] □

部分集合により生成されるイデアルについて述べる。[TODO] Ax とかの記法は？

定義 1.2.12 (生成されたイデアル)**.** R を可換環、$n \in \mathbb{Z}_{\geq 1}$ とする。

- $a_1, \ldots, a_n \in A$ に対し

$$(a_1, \ldots, a_n) \coloneqq \{b_1 a_1 + \cdots + b_n a_n \colon b_1, \ldots, b_n \in R\} \tag{1.2.10}$$

は R のイデアルである。これを $a_1, \ldots, a_n$ で**生成されたイデアル**という。

- イデアル $I \subset R$ が有限個の元により生成されたイデアルであるとき、I は**有限生成 (finitely generated)** であるという。とくに I が 1 個の元により生成されるとき、I を**単項イデアル (principal ideal)** という。

命題 1.2.13 (生成されたイデアルの特徴付け)**.** [TODO]

証明　[TODO] □

1.3　中国剰余定理

中国剰余定理はイデアルの性質に関する定理であり、環論において最も重要かつ基本的な定理のひとつである。

定理 1.3.1 (中国剰余定理)**.** A を環、$I_1, \ldots, I_n$ を A の両側イデアルとする。I_i らは**互いに素**、すなわち $I_i + I_j = A$ $(I \neq j)$ をみたすとする。このとき、準同型定理によって図式

$$\begin{array}{ccc} A & \longrightarrow & A/I_1 \times \cdots \times A/I_n \\ \downarrow & \nearrow & \\ A/(I_1 \cap \cdots \cap I_n) & & \end{array} \tag{1.3.1}$$

の破線部に誘導される環準同型は環の同型を与える。

証明　次のように写像に名前をつける:

$$\begin{array}{ccc} A & \xrightarrow{p=p_1\times\cdots\times p_n} & A/I_1\times\cdots\times A/I_n \\ \downarrow & \nearrow_{\bar{p}} & \\ A/(I_1\cap\cdots\cap I_n) & & \end{array} \tag{1.3.2}$$

$\operatorname{Ker}\bar{p} = I_1\cap\cdots\cap I_n$ より $\bar{p}$ の単射性は明らか。$\bar{p}$ の全射性を n に関する帰納法によって示す。$n=2$ の場合を考える。

$$e_1 \coloneqq (1,0) \in A/I_1\times A/I_2 \tag{1.3.3}$$

$$e_2 \coloneqq (0,1) \in A/I_1\times A/I_2 \tag{1.3.4}$$

とおき、$e_1, e_2 \in \operatorname{Im}\bar{p}$ をいえばよい。I_1, I_2 は互いに素ゆえに $x+y=1$ なる $x\in I_1,\ y\in I_2$ が存在する。このとき

$$p_1(x) = 0 \tag{1.3.5}$$

$$p_2(x) = p_2(1-y) = p_2(1) = 1 \tag{1.3.6}$$

よって

$$p(x) = (p_1(x), p_2(x)) = (0,1) = e_2 \in \operatorname{Im}\bar{p} \tag{1.3.7}$$

が成り立つ。同様に $e_1\in\operatorname{Im}\bar{p}$ も成り立つ。[TODO] □

さらに環が可換の場合は次が成り立つ。

定理 1.3.2. R を可換環とし、$I_1,\dots,I_n$ をイデアルとする。I_i らは互いに素、すなわち $I_i+I_j=A$ $(I\neq j)$ をみたすとする。このとき、

$$I_1\cap\cdots\cap I_n = I_1\cdots I_n \tag{1.3.8}$$

が成り立つ。

証明　cf. 問題 4.31 □

1.4　極大イデアル

極大イデアルを定義する。

定義 1.4.1 (極大イデアル)**.** A を環、$I\subset A$ を左イデアルとする。I が**極大左イデアル (maximal left ideal)** であるとは、I が A の固有左イデアルのうち包含関係に関し極大であることをいう。極大右イデアルおよび極大両側イデアルも同様に定義される。左/右/両側が文脈から明らかな場合は省略して**極大イデアル (maximal ideal)** ということがある。

定理 1.4.2 (Krull の定理)**.** $A\neq 0$ を環、$I\subset A$ を固有両側 (resp. 左, 右) イデアルとする。このとき、I を含む極大両側 (resp. 左, 右) イデアルが存在する。

証明　Zorn の補題を用いる。[TODO]　□

極大イデアルによって定義される環のクラスのうち最も素朴なものが単純環である。単純環については**??** でより詳しく調べる。

定義 1.4.3 (単純環)**.** (0) が極大両側イデアルとなる環を**単純環 (simple ring)** という。

例 1.4.4 (単純環の例)**.**

- division ring は単純環である。
- 単純環の部分環は単純であるとは限らない。例えば、$\mathbb{Z} \subset \mathbb{Q}$ は単純環でないし、$\mathbb{Z}[i,j,k] \subset \mathbb{H}$ も単純環でない。

[TODO] 森田同値の現れ？

定理 1.4.5 (単純環の全行列環は単純環)**.** A が単純環のとき、$M_n(A)$ も単純環である。

証明　[TODO]　□

極大イデアルは商環により特徴付けられる。

定理 1.4.6 (極大イデアルと商環)**.** A を環とする。このとき、A の両側イデアル I に関し I が極大両側イデアルであることと、A/I が単純環であることとは同値である。

証明　両側イデアルの対応原理 (定理 1.2.6) より明らか。　□

極大両側イデアルは極大左/右イデアルとは限らないが、商環が可除となる場合には次のように特徴づけることができる。

定理 1.4.7 (極大イデアルと可除環)**.** A を環とする。A の両側イデアル I に関して次は同値である:

(1)　I は極大左イデアルである。
(2)　I は極大右イデアルである。
(3)　A/I は可除環である。

証明　(1) ⇒(3)　A の両側イデアル I が極大左イデアルであるとする。A/I の零でない元は $a+I$ $(a \in A-I)$ と表せて、A の左イデアル $Aa+I$ は極大左イデアル I を真に含むから $Aa+I=A$ である。よって $(b+I)(a+I)=ba+I=1+I$ なるある $b \in A-I$ が存在する。A の左イデアル $Ab+I$ は極大左イデアル I を真に含むから $Ab+I=A$ である。よって $(c+I)(b+I)=cb+I=1+I$ なるある $c \in A-I$ が存在する。したがって $b+I \in (A/I)^\times$ であり、とくに $a+I$ は $b+I$ の逆元となるから $a+I \in (A/I)^\times$ が従う。いま $a+I$ は A/I の零でない任意の元であったから、A/I は可除環であることがいえた。

(3) ⇒(1)　A/I を可除環とする。$J \supset I$ を左イデアルとする。$I \subsetneq J$ よりある $j \in J - I$ が存在する。いま A/I は可除環だから $1 + I = (a + I)(j + I) = aj + I$ なるある $a \in A$ が存在する。よって $1 - aj = i$ なるある $i \in I \subset J$ が存在する。J が左イデアルゆえに $aj \in J$ であることとあわせて $1 = aj + i \in J$ が従う。よって $J = A$ となり、I が極大左イデアルであることがいえた。

(2) ⇔(3)　(1) ⇔(3) の議論と同様。 □

系 1.4.8. 可換環 R と R のイデアル I について、I が極大イデアルであることと、R/I が体であることとは同値である。 □

第 2 章　代数

可換環上の代数の基礎事項について述べる。

2.1　代数

代数とは、和と積とスカラー倍について閉じている代数系のことである。代数の定義にはいくつかのやり方があるが、ここでは特別な環としての定義を採用する。

定義 2.1.1 (代数)**.** A を環、R を可換環とする。

- 環 A と環準同型 $\varphi\colon R \to Z(A)$ の組 (A,φ) を ***R*-代数 (*R*-algebra)** あるいは ***R*-多元環 (*R*-algebra)** という [2)]。記号の濫用で A における $x \in R$ の像も x と書くことがある。
- $(A,\varphi),(B,\psi)$ を R-代数とする。環準同型 $f\colon A \to B$ が図式

$$\begin{array}{ccc} & R & \\ {\scriptstyle\varphi}\swarrow & & \searrow{\scriptstyle\psi} \\ A & \xrightarrow[f]{} & B \end{array} \tag{2.1.1}$$

を可換にするとき、f は ***R*-代数準同型 (*R*-algebra homomorphism)** であるという。

- $A \to B$ なる R-代数準同型全体の集合を $\mathrm{Hom}_R^{\mathrm{al}}(A,B)$ と書く。

例 2.1.2 (代数の例)**.**

- A を環とする。A は環準同型

$$\mathbb{Z} \to A, \quad n \mapsto \underbrace{1+\cdots+1}_{n \text{ times}} \tag{2.1.2}$$

により $\mathbb{Z}$-代数となる。

- 可換環 R 上の n 次正方行列の全体 $M_n(R)$ は、環準同型 $R \to Z(M_n(R)), \lambda \mapsto \lambda I_n$ により R-代数となる。これは非可換な R-代数の例となっている。
- 環 $\mathbb{C}$ は、環準同型 $\mathbb{R} \to \mathbb{C}, x \mapsto x$ により $\mathbb{R}$-代数となる。
- 環 $\mathbb{C}\times\mathbb{C}$ は、環準同型 $\mathbb{C} \to \mathbb{C}\times\mathbb{C}, z \mapsto (z,z)$ により $\mathbb{C}$-代数となる。
- 位相空間 X 上の $\mathbb{C}$ 値連続関数全体のなす環 $C(X)$ は、環準同型 $\mathbb{C} \to C(X)$,

$$\lambda \mapsto (x \mapsto \lambda) \tag{2.1.3}$$

により $\mathbb{C}$-代数となる。

2)　文献によっては代数にスカラー倍の結合性を仮定しない立場もある。翻って本稿における代数の定義では結合性が自動で導かれる。結合性を仮定するという立場を明確にするために**結合的代数 (associative algebra)** と呼ばれることもある。

定義 2.1.3 (R-部分代数)**.** R を可換環、(A, φ) を R-代数とする。A の部分環 B が φ により R-代数となるとき、B を A の ***R*-部分代数 (*R*-subalgebra)** という。

体上の代数には体が埋め込まれているとみなせる。

命題 2.1.4 (代数への体の埋め込み)**.** K を体とする。このとき、0 でない任意の K-代数 (A, φ) に対し φ は単射である。

証明　φ は環準同型 $K \to Z(A)$ だから、K が体であることより $\operatorname{Ker}\varphi = K$ または $\operatorname{Ker}\varphi = 0$ である。$\operatorname{Ker}\varphi = K$ であったとすると $1_A = \varphi(1_K) = 0_A$ より $A = 0$ となり矛盾。したがって $\varphi = 0$、すなわち φ は単射である。 □

2.2　モノイド代数と群環

モノイド代数と群環を定義する。モノイド代数は後で定義する多項式環の一般化である。

定義 2.2.1 (モノイド代数)**.** M をモノイド、$R \neq 0$ を可換環とする。集合 $R[M]$ を

$$R[M] \coloneqq \left\{ \sum_{m \in M}^{\text{finite}} a_m \cdot m \;\middle|\; a_m \in R \right\} \tag{2.2.1}$$

とおく。ただし $\sum^{\text{finite}}$ は**形式的実質的有限和 (formal essential finite sum)** といい、有限個の m を除いて $a_m = 0$ となる和である。$R[M]$ に加法と乗法を

$$\left(\sum_{m \in M}^{\text{finite}} a_m \cdot m \right) + \left(\sum_{m \in M}^{\text{finite}} b_m \cdot m \right) \coloneqq \sum_{m \in M}^{\text{finite}} (a_m + b_m) \cdot m \tag{2.2.2}$$

$$\left(\sum_{m \in M}^{\text{finite}} a_m \cdot m \right) \cdot \left(\sum_{m \in M}^{\text{finite}} b_m \cdot m \right) \coloneqq \sum_{m \in M}^{\text{finite}} \left(\sum_{\substack{x,y \in M \\ xy = m}}^{\text{finite}} a_x b_y \right) \cdot m \tag{2.2.3}$$

で定めると、$\left(R[M], +, \cdot, \sum_{m \in M}^{\text{finite}} 0 \cdot m, 1 \cdot 1_M \right)$ は環となる (このあと示す)。さらに環準同型

$$R \to R[M], \quad r \mapsto r \cdot 1_M \tag{2.2.4}$$

により R-代数の構造が入る (このあと示す)。R-代数 $R[M]$ を R 上の M の**モノイド代数 (monoid algebra)** という。

証明　[TODO] □

定義 2.2.2 (群代数)**.** G を群、$R \neq 0$ を可換環とする。モノイド代数 $R[G]$ を R 上の G の**群代数 (group algebra)** あるいは**群環 (group ring)** という。

R, M から $R[M]$ への自然な埋め込みが次のように定まる。

命題 2.2.3 (モノイド代数への埋め込み)**.** $R \neq 0$ を可換環、M をモノイドとする。このとき、写像

$$M \to R[M], \quad x \mapsto 1_R \cdot x \tag{2.2.5}$$

$$R \to R[M], \quad r \mapsto r \cdot 1_M \tag{2.2.6}$$

$$\tag{2.2.7}$$

はそれぞれ (乗法的) モノイド準同型、R-代数準同型となる。

証明 省略 □

命題 2.2.4 (モノイド代数の加群構造)**.** $R \neq 0$ を可換環、M をモノイドとする。このとき、$R[M]$ は M を基底とする R 上の自由 R-加群である。

証明 [TODO] □

モノイド代数は次の普遍性を持つ。

定理 2.2.5 (モノイド代数の普遍性)**.** $R \neq 0$ を可換環、M をモノイドとする。このとき次が成り立つ:

$$\forall\, A\colon R\text{-代数} \tag{2.2.8}$$

$$\forall\, \varphi\colon M \to A\colon \text{(乗法的) モノイド準同型} \tag{2.2.9}$$

$$\exists!\, \overline{\varphi}\colon R[M] \to A\colon R\text{-代数準同型} \quad \text{s.t.} \tag{2.2.10}$$

$$\begin{array}{ccc} R[M] & \overset{\varphi}{\dashrightarrow} & A \\ \uparrow & \nearrow_{\overline{\varphi}} & \\ M & & \end{array} \tag{2.2.11}$$

証明 φ がモノイド準同型であることより $\overline{\varphi}$ は

$$\overline{\varphi}\left(\sum_{m\in M}^{\text{finite}} a_m \cdot m\right) = \sum_{m\in M}^{\text{finite}} a_m \cdot \varphi(m) \quad (a_m \in R) \tag{2.2.12}$$

をみたさなければならないが、上の命題より M は $R[M]$ の R-加群としての基底だから、このような R-加群準同型 $\overline{\varphi}$ は一意に存在する。あとは $\overline{\varphi}$ が R-代数準同型であることを示せばよい。[TODO] cf. [? , p.5] □

系 2.2.6 (群代数の普遍性)**.** $R \neq 0$ を可換環、G, G' を群、$\varphi\colon G \to G'$ を群準同型とする。このとき、R-代数準同型 $h\colon R[G] \to R[G']$ であって次をみたすものが一意に存在する：

$$h(x) = \varphi(x) \quad (\forall x \in G) \tag{2.2.13}$$

$$h(a) = a \quad (\forall a \in R) \tag{2.2.14}$$

□

2.3 多項式環

多項式環を定義する。多項式環は可換環の重要な例のひとつである。

定義 2.3.1 (多項式環). R を可換環、$X_1, \dots, X_n$ を形式的記号とする。形式的に

$$X_1^{k_1} \dots X_n^{k_n} \quad ((k_1, \dots, k_n) \in \mathbb{Z}_{\geq 0}^n) \tag{2.3.1}$$

というものを考え、これを**単項式 (monomial)** と呼ぶ。ここで集合

$$M_n := \{X_1^{k_1} \dots X_n^{k_n} : (k_1, \dots, k_n) \in \mathbb{Z}_{\geq 0}^n\} \tag{2.3.2}$$

を定め、普通の方法で積を入れて可換モノイドにする。モノイド代数 $R[M_n]$ を $R[X_1, \dots, X_n]$ と書き、***R*-係数 *n* 変数多項式環 (polynomial ring)** と呼ぶ。

定義 2.3.2 (多項式関数). [TODO]

命題 2.3.3 (多項式の表示の一意性). R を可換環とする。$R[X_1, \dots, X_n]$ の元の

$$\sum_{k_1, \dots, k_n \geq 0}^{\text{finite}} a_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n} \tag{2.3.3}$$

の形での表示は一意である。

証明 [TODO] 形式的実質的有限和を写像 $M \to R$ とみれば一意性は明らか？ □

定理 2.3.4 (除法定理). R を可換環とする。このとき、任意の $f \in R[X]$ および最高次係数が単元であるような任意の $g \in R[X]$ に対し

$$\exists! \, q, r \in R[X] \quad \text{s.t.} \quad f = gq + r, \ \deg r < \deg g \tag{2.3.4}$$

が成り立つ。

証明 $m := \deg f$, $n := \deg g \geq 0$ とおく。題意の $q, r \in R[X]$ の存在を m に関する帰納法で示す。$m < n$ ならば $q(X) = 0, r(X) = f(X)$ とおけばよい。$m \geq n$ とし、f, g の最高次係数をそれぞれ a_m, b_n とおく。ここで

$$h(X) := f(X) - g(X) a_m b_n^{-1} X^{m-n} \tag{2.3.5}$$

とおくと $\deg h < \deg f$ であるから、帰納法の仮定より

$$\exists q_1, r_1 \in R[X] \quad \text{s.t.} \quad h = gq_1 + r_1, \ \deg r_1 < \deg g \tag{2.3.6}$$

が成り立つ。そこで

$$q(X) := q_1(X) + a_m b_n^{-1} X^{m-n}, \quad r(X) := r_1(X) \tag{2.3.7}$$

とおけばよい。つぎに一意性を示す。$q^*, r^* \in R[X]$ が

$$f = gq^* + r^*, \ \deg r^* < \deg g \tag{2.3.8}$$

をみたすとする。$f = gq + r$ と差をとって

$$(q^* - q)g = r^* - r \tag{2.3.9}$$

が成り立つ。よって、もし $q^* - q \neq 0$ ならば

$$\deg((q^* - q)g) = \deg(q^* - q) + \deg g \quad (\because\ g \text{ の最高次係数は可逆元}) \tag{2.3.10}$$

$$\geq \deg g \tag{2.3.11}$$

が成り立つが、これは

$$\deg(r^* - r) \leq \max\{\deg r^*, \deg r\} \tag{2.3.12}$$

$$< \deg g \tag{2.3.13}$$

に矛盾する。よって $q^* = q$、したがって $r^* = r$ である。これで一意性がいえた。 □

注意 2.3.5 (除法定理が成り立たない例)**.** 最高次係数が可逆元でない例を考える。$R = \mathbb{Z}$ のとき、$X, 2X \in \mathbb{Z}[X]$ に対し

$$X = 2X \cdot q(X) + r(X),\ \deg r < \deg(2X) = 1 \tag{2.3.14}$$

なる $q, r \in \mathbb{Z}[X]$ は存在しない。

[TODO] 「割り切る」の概念が未定義

系 2.3.6 (剰余定理)**.** R を可換環とし、$\alpha \in R$ とする。このとき

$$\exists!\ q \in R[X] \quad \text{s.t.} \quad f(X) = (X - \alpha)q(X) + f(\alpha) \tag{2.3.15}$$

が成り立つ。とくに

$$X - \alpha \text{ が } f \text{ を割り切る} \quad \Longleftrightarrow \quad f(\alpha) = 0 \tag{2.3.16}$$

が成り立つ。

証明　省略 □

1 変数多項式環においては、次の意味で代入が定義できる。

定理 2.3.7 (1 変数多項式環の普遍性)**.** R を可換環、A を R-代数とする。このとき、任意の $a \in A$ に対し R-代数準同型 $\mathrm{ev}_a \colon R[X] \to A$ であって

$$\mathrm{ev}_a(X) = a \tag{2.3.17}$$

をみたすものがただひとつ存在する。

証明　[TODO] □

多変数多項式環でも代入を定義できるが、多変数の場合は可換性が必要である。

定理 2.3.8 (多変数多項式環の普遍性). R を可換環、A を可換 R-代数とする。このとき、任意の $a_1, \ldots, a_n \in A$ に対し R-代数準同型 $\mathrm{ev}_{(a_1,\ldots,a_n)} \colon R[X_1, \ldots, X_n] \to A$ であって

$$\mathrm{ev}_{(a_1,\ldots,a_n)}(X_i) = a_i \quad (i = 1, \ldots, n) \tag{2.3.18}$$

をみたすものがただひとつ存在する。

証明 [TODO] cf. [雪江 p.16] □

定理 2.3.9 (多項式環の特徴付け). [TODO]

証明 [TODO] □

系 2.3.10 (多変数多項式環の自然な同型).

$$\mathrm{ev}_{(X_1,\ldots,X_n)} \colon R[X_1, \ldots, X_n] \to (R[X_1, \ldots, X_{n-1}])[X_n] \tag{2.3.19}$$

は R-代数の同型である。[TODO]

定義 2.3.11 (次数). [TODO]

多項式環からその係数環への評価準同型は簡単な形の Ker を持っている。

命題 2.3.12 (多項式環の評価準同型の核). R を可換環、$\alpha_1, \ldots, \alpha_n \in R$ とする。このとき、評価準同型 $\mathrm{ev}_{(\alpha_1,\ldots,\alpha_n)} \colon R[X_1, \ldots, X_n] \to R$ の核は

$$\mathrm{Ker}(\mathrm{ev}_{(\alpha_1,\ldots,\alpha_n)}) = (X_1 - \alpha_1, \ldots, X_n - \alpha_n) \tag{2.3.20}$$

の形である。

証明 "⊃"は明らかに成り立つ。"⊂"を n についての帰納法で示す。$n = 1$ のときは剰余定理 (定理2.3.4) からただちに従う。$n \in \mathbb{Z}_{\geq 2}$ とし、$n-1$ で成立を仮定して n での成立を示す。そこで $f(X_1, \ldots, X_n) \in \mathrm{Ker}(\mathrm{ev}_{(\alpha_1,\ldots,\alpha_n)})$ とする。系 2.3.10 より $R[X_1, \ldots, X_n] \cong (R[X_1, \ldots, X_{n-1}])[X_n]$ だから

$$f(X_1, \ldots, X_n) = \sum_{i=0}^{k} f_i(X_1, \ldots, X_{n-1}) X_n^i \tag{2.3.21}$$

$$(f_i \in R[X_1, \ldots, X_{n-1}],\ f_k \neq 0_{R[X_1,\ldots,X_{n-1}]}) \tag{2.3.22}$$

の形に一意に表せる。ここで各 $0 \leq i \leq k$ に対し

$$h_i(X_1, \ldots, X_{n-1}) \coloneqq f_i(X_1, \ldots, X_{n-1}) - f_i(\alpha_1, \ldots, \alpha_{n-1}) \tag{2.3.23}$$

とおくと、定め方から $h_i(\alpha_1, \ldots, \alpha_{n-1}) = 0$ だから、帰納法の仮定より

$$h_i(X_1, \ldots, X_{n-1}) \in \mathrm{Ker}(\mathrm{ev}_{(\alpha_1,\ldots,\alpha_{n-1})}) \tag{2.3.24}$$

$$= (X_1 - \alpha_1, \dots, X_{n-1} - \alpha_{n-1}) \tag{2.3.25}$$

$$\subset (X_1 - \alpha_1, \dots, X_{n-1} - \alpha_{n-1}, X_n - \alpha_n) \tag{2.3.26}$$

となる。また、$\sum_{i=0}^{k} f_i(\alpha_1, \dots, \alpha_{n-1})\alpha_n^i = f(\alpha_1, \dots, \alpha_n) = 0$ と剰余定理 (定理 2.3.4) から $\sum_{i=0}^{k} f_i(\alpha_1, \dots, \alpha_{n-1})X_n^i \in (X_n - \alpha_n)$ が成り立つ。よって

$$f(X_1, \dots, X_n) = \sum_{i=0}^{k} \big(h_i(X_1, \dots, X_{n-1}) + f_i(\alpha_1, \dots, \alpha_{n-1})\big) X_n^i \tag{2.3.27}$$

$$= \underbrace{\sum_{i=0}^{k} h_i(X_1, \dots, X_{n-1})X_n^i}_{\in (X_1 - \alpha_1, \dots, X_n - \alpha_n)} + \underbrace{\sum_{i=0}^{k} f_i(\alpha_1, \dots, \alpha_{n-1})X_n^i}_{\in (X_n - \alpha_n)} \tag{2.3.28}$$

$$\in (X_1 - \alpha_1, \dots, X_n - \alpha_n) \tag{2.3.29}$$

となり、n での成立がいえた。帰納法より命題の主張が示せた。 □

2.4 自由代数

自由代数を定義する。

定義 2.4.1 (自由 R-代数)**.**
S を集合、$R \neq 0$ を可換環とする。S の元 $s_1, \dots, s_n$ を形式的に $s_1 \dots s_n$ と並べた**語 (word)** の全体を

$$W(S) \coloneqq \{S \text{ の元からなる語}\} \cup \{\varnothing\} \tag{2.4.1}$$

と定める。$\varnothing$ を 1 と書き、乗法を

$$(s_1 \dots s_n)(s'_1 \dots s'_m) = s_1 \dots s_n s'_1 \dots s'_m \tag{2.4.2}$$

$$1(s_1 \dots s_n) = (s_1 \dots s_n)1 = s_1 \dots s_n \tag{2.4.3}$$

で定めてモノイド構造を入れる。モノイド代数 $R[W(S)]$ を S により生成される**自由 R-代数 (free R-algebra)** という。

命題 2.4.2 (自由代数の普遍性)**.** [TODO]

証明 [TODO] □

2.5 生成された部分代数

部分集合によって部分代数を生成することができる。

定義 2.5.1 (部分集合により生成された部分代数)**.** $R \neq 0$ を可換環、A を R-代数、$S \subset A$ とする。このとき、標準包含 $\iota\colon S \hookrightarrow A$ により誘導される R-代数準同型 $\bar{\iota}\colon R[W(S)] \to A$ の像 $\operatorname{Im}\bar{\iota}$ を $R\langle S\rangle$ と書き、**S で生成された A の R-部分代数 (R-subalgebra generated by S)** という。とくに S が有限集合ならば、A は R-代数として**有限生**

成 (finitely generated) であるという。

生成された代数は自由代数と同様の普遍性を持つわけではないことに注意すべきである。

注意 2.5.2. $\mathbb{Z}$ 上 $S := \{1/2\}$ により生成された $\mathbb{Q}$ の $\mathbb{Z}$-部分代数 $\mathbb{Z}\langle S\rangle$ を考える。$\mathbb{Z}$ 上 S により生成された $\mathbb{Z}$-部分代数が自由代数の場合と同様の "普遍性" を持ったとすると、写像 $f\colon S \to \mathbb{Z}[X]$, $f(1/2) := X$ に対し

$$\begin{array}{ccc} \mathbb{Z}\langle S\rangle & \overset{g}{\dashrightarrow} & \mathbb{Z}[X] \\ \uparrow & \nearrow_{f} & \\ S & & \end{array} \tag{2.5.1}$$

を可換にする $\mathbb{Z}$-代数準同型 g が一意に存在する。図式の可換性より $g(1/2) = X$ だから $g(1) = g(2 \cdot 1/2) = 2g(1/2) = 2X$ であるが、一方 g は環準同型だから $g(1) = 1 \neq 2X$ であり矛盾を得る。

例 2.5.3 (多項式環は有限生成代数)**.** $R \neq 0$ を可換環とする。R-係数多項式環 $R[X_1, \ldots, X_n]$ は有限集合 $\{X_1, \ldots, X_n\} \subset R[X_1, \ldots, X_n]$ により生成される R-代数だから、R-代数として有限生成である。

生成された部分代数は次のように特徴付けられる。これは生成されたイデアルの特徴付け (命題 1.2.13) の類似である。

命題 2.5.4 (生成された部分代数の特徴付け)**.** $R \neq 0$ を可換環、A を R-代数、$S \subset A$ とする。このとき

$$R\langle S\rangle = \bigcap_{\substack{B \subset A\,:\, R\text{-部分代数} \\ B \supset S}} B \tag{2.5.2}$$

が成り立つ。

証明　$R\langle S\rangle$ は S を含む A の R-部分代数ゆえに右辺の項として現れるから "$\supset$" が成り立つ。

"$\subset$" を示す。そこで $B \subset A$ を S を含む A の R-部分代数とする。また $\Phi\colon S \to R[W(S)]$ を標準射、

$$\iota_S^A\colon S \to A, \quad \iota_S^B\colon S \to B, \quad \iota_B^A\colon B \to A \tag{2.5.3}$$

をそれぞれ標準包含とする。すると R 上 S により生成された自由代数の普遍性より図式

$$\begin{array}{ccc} S & \overset{\iota_S^A}{\hookrightarrow} & A \\ {\scriptstyle\Phi}\downarrow & \nearrow_{\tilde{\iota}_S^A} & \\ R[W(S)] & & \end{array} \qquad \begin{array}{ccc} S & & \\ {\scriptstyle\Phi}\downarrow & \searrow^{\iota_S^B} & \\ R[W(S)] & \overset{\tilde{\iota}_S^B}{\dashrightarrow} & B \end{array} \tag{2.5.4}$$

を可換にする R-代数準同型 $\tilde{\iota}_S^A$, $\tilde{\iota}_S^B$ が一意に存在する。ここで各 $s \in S$ に対し $\iota_B^A \circ \tilde{\iota}_S^B \circ \Phi(s) = \iota_B^A \circ \iota_S^B(s) = \iota_S^A(s) = \tilde{\iota}_S^A \circ \Phi(s)$ が成り立つから、一意性より $\iota_B^A \circ \tilde{\iota}_S^B = \tilde{\iota}_S^A$ である。したがって $R\langle S\rangle = \operatorname{Im} \tilde{\iota}_S^A = \operatorname{Im} \iota_B^A \circ \tilde{\iota}_S^B = \iota_B^A \circ \tilde{\iota}_S^B(R[W(S)]) \subset \iota_B^A(B) = B$ である。よって "$\subset$" が示せた。 □

有限生成可換 R-代数は次のように特徴付けることができる。

命題 2.5.5 (有限生成可換 R-代数の特徴付け)**.** $R \neq 0$ を可換環、A を可換 R-代数、$S \subset A$ とする。このとき、次は同値である:

(1) A は有限生成 R-代数である。
(2) ある $n \in \mathbb{Z}_{\geq 1}$ と全射 R-代数準同型 $f\colon R[X_1, \ldots, X_n] \to A$ が存在する。

証明 [TODO] □

第 3 章　可換環

可換環についてより詳しく調べる。

3.1　素イデアル

素イデアルを定義する。この章では非可換環の素イデアルを扱うことはないが、議論のまとまりのために素イデアルの定義は非可換環の場合も含めて与えておく。

定義 3.1.1 (素イデアル)**.** A を環、P を A の固有両側イデアルとする。

(1)　P が A の**素イデアル (prime ideal)** であるとは、A の任意の固有両側イデアル I, J であって $IJ \subset P$ をみたすものに対して $I \subset P$ または $J \subset P$ が成り立つことをいう。
(2)　P が A の**完全素イデアル (completely prime ideal)** であるとは、任意の $x, y \in A$ であって $xy \in P$ をみたすものに対して $x \in P$ または $y \in P$ が成り立つことをいう。

定義 3.1.2 (素イデアル全体の集合)**.** R を可換環とする。R の素イデアル全体の集合を

$$\mathrm{Spec}(R) \coloneqq \{\mathfrak{p} \subset R : \mathfrak{p} \text{ は素イデアル}\} \tag{3.1.1}$$

と書く。

可換環における素イデアルの特徴付けを与える。

命題 3.1.3 (素イデアルの特徴付け)**.** R を可換環とする。R の固有イデアル $\mathfrak{p} \subset R$ に関し次は同値である:

(1)　$\mathfrak{p}$ は R の素イデアルである。
(2)　$\mathfrak{p}$ は R の完全素イデアルである。
(3)　$R/\mathfrak{p}$ は整域である。

証明　(2) ⇒(1)　cf. 問題 4.36

[TODO]　□

例 3.1.4 (素イデアルの例)**.**

- 素イデアルは極大イデアルとは限らない。実際、$\mathbb{Z} \cong \mathbb{Z}/(0)$ は整域だが体でないので、(0) は $\mathbb{Z}$ の素イデアルだが極大イデアルではない。しかし、可換アルティン環においては素イデアルは極大イデアルとなる (**??**)。

根基と準素イデアルを定義する。これらの概念は冪零元と深い関わりを持つ。

定義 3.1.5 (根基). R を可換環、I を R の固有イデアルとする。このとき

$$\sqrt{I} \coloneqq \{r \in R \mid r^n \in I\ (\exists n \in \mathbb{Z}_{\geq 1})\} \tag{3.1.2}$$

は R の固有イデアルとなり (このあと示す)、$\sqrt{I}$ を I の**根基 (radical)** という。とくに (0) の根基 $\sqrt{(0)}$ を R の**冪零根基 (nilradical)** という。

証明 cf. 問題 4.29 □

命題 3.1.6 (根基の特徴付け). R を可換環、I を R の固有イデアルとする。このとき、$I = \sqrt{I}$ となることは R/I の 0 でない冪零元が存在しないための必要十分条件である。

証明 cf. 問題 4.50 □

定義 3.1.7 (準素イデアル). R を可換環とする。R の固有イデアル I が**準素イデアル (primary ideal)** であるとは、$x, y \in R$ に関し

$$(xy \in I \land x \notin I) \quad \Longrightarrow \quad y \in \sqrt{I} \tag{3.1.3}$$

が成り立つことをいう。

命題 3.1.8 (準素イデアルの特徴付け). R を可換環、I を R の固有イデアルとする。このとき、I が準素イデアルであることは R/I の零因子がすべて冪零元になるための必要十分条件である。

証明 cf. 問題 4.51 □

命題 3.1.9 (準素イデアルの根基). R を可換環、I を R の準素イデアルとする。このとき $\sqrt{I}$ は I を含む最小の素イデアルである。

証明 cf. 問題 4.53 □

3.2 素元と既約元

倍元と約元の概念を定義する。

定義 3.2.1 (倍元と約元). R を可換環、$a, b \in R$ とする。a が b の**倍元 (multiple)**、あるいは b が a の**約元 (divisor)** であるとは、ある $r \in R$ が存在して $a = rb$ が成り立つことをいい、このことを $b \mid a$ と書いて表す。$b \mid a$ であるとき **b は a を割り切る (b divides a)**、あるいは **a は b で割り切れる (a is divisible by b)** という。

定義 3.2.2 (同伴元). R を可換環、$a \in R$ とする。$b \in R$ が $a|b$ かつ $b|a$ をみたすとき、a は b の**同伴元 (associate)** であるという。明らかにこのとき b は a の同伴元である。

定理 3.2.3 (整域における同伴元の特徴付け). R を整域とする。$a,b \in R$ に関し、a,b が互いに同伴元であるための必要十分条件は、ある $u \in R^\times$ が存在して $a = ub$ が成り立つことである。

証明　十分性は明らか。

[TODO]　□

最大公約元の概念を定義する。

定義 3.2.4 (最大公約元). R を可換環、$a_1,\dots,a_n \in R$, $g \in R$ とする。g が $a_1,\dots,a_n$ の**最大公約元 (greatest common divisor)** であるとは、g が次をみたすことをいう:

(1)　g は $a_1,\dots,a_n$ を割り切る。
(2)　$a_1,\dots,a_n$ を割り切る任意の $g' \in R$ に対し g' は g を割り切る。

素元と既約元を定義する。既約元は非自明な分解を持たない元のことである。

定義 3.2.5 (素元と既約元). R を可換環とする。

- $a \in R - \{0\}$ が**素元 (prime element)** であるとは、$(a) \in \mathrm{Spec}(R)$ であることをいう。
- $a \in R - \{0\}$ が**既約元 (irreducible element)** であるとは、
  (1)　$a \notin R^\times$
  (2)　$\forall a,b \in R$ に対し、
  $$a = bc \quad \Longrightarrow \quad (b \in R^\times \vee c \in R^\times) \tag{3.2.1}$$
  をみたすことをいう。

例 3.2.6 (既約元は素元とは限らない). cf. 問題 4.39 [TODO] $\mathbb{Z}[\sqrt{-5}]$ において $6 = 2\cdot 3 = (q+\sqrt{-5})(1-\sqrt{-5})$ を考える。
　ただし、後でみるように UFD では既約元が素元となる。

例 3.2.7 (素元は既約元とは限らない). K を体とし、可換環 $K\times K$ を考える。$(K\times K)/((1,0)) \cong K$ ゆえに $(1,0)$ は素元である。一方、$(1,0) = (1,0)(1,0)$ と可逆でない 2 元の積に書けることから $(1,0)$ は既約元ではない。

整域においては素元は既約元でもある。既約元の判定はしばしば難しく、素元の判定は比較的簡単なことがあるため、この定理は既約元の判定の足がかりとなる。

定理 3.2.8 (整域では素元は既約元). R を整域とする。R の素元は既約元である。

証明　$x \in R - \{0\}$ を素元とする。$x = ab$, $a,b \in R$ とすると x が素元ゆえに (x) が素イデアルであることから $a \in (x)$ または $b \in (x)$ である。$a \in (x)$ の場合を考える。$a = rx$ $(r \in R)$ と表せるからよって $x = rxb = rbx$ である。いま R は整域だから $1 = rb$ が成り立つ。したがって $b \in R^\times$ である。同様に $b \in (x)$ ならば $a \in R^\times$ である。したがって x は R の既約元である。　□

3.3 UFD

UFD を定義する。UFD は既約元分解が次の意味で一意的に存在する整域である。

定義 3.3.1 (UFD)**.** 整域 R が**一意分解整域 (unique factorization domain)**、あるいは略して **UFD** であるとは、R が次をみたすことをいう:

(1) (既約元分解の存在) 0 でも単元でもない $r \in R$ は既約元の積 $r = p_1 \dots p_m$ の形に表せる。各 p_i を r の**素因子 (prime factor)** という。
(2) (既約元分解の一意性) 既約元 $p_1, \dots, p_m, q_1, \dots, q_n \in R$ が $p_1 \dots p_m = q_1 \dots q_n$ をみたすならば、$m = n$ が成り立ち、かつある置換 $\sigma \in S_n$ が存在して p_i と $q_{\sigma(i)}$ は互いに同伴元となる。

異なる概念として定義された素元と既約元だが、整域においては素元は既約元となるのであった。さらに UFD ではこの逆も成り立つ。したがって UFD では既約元分解は素元分解と考えても同じことである。

命題 3.3.2 (UFD の既約元は素元)**.** UFD の既約元は素元である。したがって UFD の零でない元が既約元であることと素元であることは同値である。

証明[3]**.** R を UFD、$p \in R - \{0\}$ を既約元とする。(p) が素イデアルとなることを示せばよい。$ab \in (p)$ とすると $ab = rp$ $(r \in R)$ と表せる。p は既約元だから、左辺の既約元分解には p の同伴元が含まれる。したがって既約元分解の一意性より、a, b の少なくとも一方の既約元分解に p の同伴元が含まれる。よって $a \in (p)$ または $b \in (p)$ が成り立つ。したがって (p) は素イデアルである。よって p は R の素元である。 □

UFD は最大公約元を持つ。

命題 3.3.3 (UFD は最大公約元を持つ)**.** R を UFD とする。任意の $a_1, \dots, a_n \in R$ に対し $a_1, \dots, a_n$ の最大公約元が存在する。

証明 [TODO] cf. [? , p.107] □

上の命題により次の定義が可能となる。

定義 3.3.4 (互いに素)**.** R を UFD、$a_1, \dots, a_n \in R$ とする。$a_1, \dots, a_n$ が**互いに素 (relatively prime)** であるとは、$a_1, \dots, a_n$ の最大公約元が単元のみであることをいう。

命題 3.3.5 (互いに素な元と互いに素なイデアル)**.**

$$(a) + (b) = R \tag{3.3.1}$$

[TODO]

3) PID における別証明は問題 4.40 を参照。

証明 [TODO] 素イデアルが極大イデアルになることや同伴元と単項イデアルの関係を使って示すべき？ □

体上の多項式環は UFD である。

定理 3.3.6. 体上の多項式環は UFD である。

証明 [? , p.111] □

定義 3.3.7 (重複度). $f \in K[X]$ が $f(X) = (X-\alpha)^k g(X)$ (g は α を根に持たない) の形に表せるとき、k を α の**重複度 (multiplicity)** という。

3.4 PID

PID について述べる。PID の概念は**??**で述べる単因子論の基礎となる。

定義 3.4.1 (PID). 任意のイデアルが単項イデアルとなる整域を**単項イデアル整域 (principal ideal domain)** 、あるいは略して **PID** という。

単項イデアルの生成元は次の意味で一意である。

定理 3.4.2 (単項イデアルの生成元の一意性). R を整域とする。$a, b \in R$ に対し次は同値である:

(1) $(a) = (b)$
(2) $\exists r \in A^\times$ s.t. $ra = b$

証明 [TODO] □

定理 3.4.3 (PID の 0 でない素イデアルは極大イデアル). PID の 0 でない素イデアルは極大イデアルである。

証明 $(x) \neq 0$ を素イデアルとし、$(y) \supsetneq (x)$ をイデアルとする。$x \in (y)$ だから $x = yz$ と書ける。よって $yz \in (x)$ である。したがって $y \in (x) \vee z \in (x)$ だが、いま $(y) \supsetneq (x)$ だから $y \notin (x)$、したがって $z \in (x)$ である。よって $z = wx$ と書ける。したがって $x = yz = ywx$ である。よって $1 = yw$ ゆえに y は単元だから $(y) = (1)$ である。 □

命題 3.4.4. PID において、既約元の生成する単項イデアルは極大イデアルである。

証明 [TODO] □

定理 3.4.5. R を PID とする。

(1) R は UFD である。

(2)　$a \in R - R^\times$ に対し $\bigcap_{n\geq 1}(a^n) = 0$ が成り立つ。

証明　(1)　[TODO]

(2)　$a = 0$ の場合は明らかに成り立つ。$a \neq 0$ とすると、R が UFD であることより a は単元と $k_a \in \mathbb{Z}_{\geq 1}$ 個の既約元の積に分解できる。$x \in \bigcap_{n\geq 1}(a^n)$ とする。$x \in R^\times$ であったとすると $x \in (a)$ より a も単元となり矛盾。したがって $x \notin R^\times$ である。$x \neq 0$ と仮定し矛盾を導く。$x \notin R^\times$, $x \neq 0$ より x は単元と $k_x \in \mathbb{Z}_{\geq 1}$ 個の既約元の積に分解できる。$x \in \bigcap_{n\geq 1}(a^n)$ よりすべての $n \in \mathbb{Z}_{\geq 1}$ に対し $x \in (a^n)$ だから $x = r_n a^n$ $(r_n \in R)$ と表せるが、両辺の既約元分解に現れる既約元の個数は左辺にちょうど k_x 個、右辺に nk_a 個以上だから、十分大きな n に対しては等しくなりえず、矛盾が従う。よって $x = 0$ であり、(2) の主張が示された。 □

3.5　Euclid 整域

Euclid 整域について述べる。

定義 3.5.1 (Euclid 整域). R を整域とする。R が **Euclid 整域 (Euclidean domain)** であるとは、次をみたす写像 $\delta\colon R \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ が存在することをいう:

- $\delta(R - \{0\}) \subset \mathbb{Z}_{\geq 0}$
- $\delta(0) = -\infty$
- (割り算原理) $\forall a \in R$ と $\forall h \in R - \{0\}$ に対し

$$\exists q, r \in R \quad \text{s.t.} \quad a = hq + r \quad \text{and} \quad \delta(r) < \delta(h) \tag{3.5.1}$$

Euclid 整域は PID である。

定理 3.5.2. Euclid 整域は PID である。

証明　[TODO] □

体上の 1 変数多項式環は Euclid 整域となる。

定理 3.5.3. 体上の 1 変数多項式環は Euclid 整域である。

証明　cf. 問題 4.20 □

3.6　局所環

極大イデアルによって定義される可換環のクラスのうち最も重要なもののひとつが局所環である。

定義 3.6.1 (局所環). 極大イデアルをただひとつ持つ可換環を**局所環 (local ring)** という。

例 3.6.2 (単純環と局所環の例)**.**

- 可換な単純環は (0) を唯一の極大イデアルとする局所環である。
- 体は単純環かつ局所環である。

局所環 R の極大イデアル $\mathfrak{m}$ は具体的に表せる。すなわち $\mathfrak{m}$ は R の非単元全体の集合である。

定理 3.6.3 (局所環の乗法群による特徴付け)**.** R を可換環とする。次は同値である:

(1) R は局所環である。
(2) $R - R^\times$ は R の極大イデアルである。

証明 (2) ⇒(1) は明らかだから (1) ⇒(2) を示す。$\mathfrak{m}$ を R の唯一の極大イデアルとする。$R^\times \cap \mathfrak{m} = \varnothing$ であることは $\mathfrak{m}$ が固有イデアルであることから明らか。$x \in R - R^\times$ とすると (x) は固有イデアルだから定理 1.4.2 より (x) を含む極大イデアルが存在するが、いま R は局所環だからそれは $\mathfrak{m}$ である。したがって $x \in \mathfrak{m}$ が成り立つ。 □

系 3.6.4. 可換な単純環は体である。 □

3.7 局所化と商体

局所化について述べる。

定義 3.7.1 (局所化)**.** R を可換環とする。

- R の乗法に関する部分モノイドを R の**積閉集合 (multiplicative set)** という。
- $S \subset R$ を R の積閉集合とする。$R \times S$ 上の同値関係 $\sim$ を

$$(r_1, s_1) \sim (r_2, s_2) \quad \Longleftrightarrow \quad \exists\, s \in S \text{ s.t. } (r_1 s_2 - r_2 s_1)s = 0 \tag{3.7.1}$$

で定める (ことができる)。この同値関係による商集合を $S^{-1}R := (R \times S)/\sim$ とおき、(r, s) の属する類を $\dfrac{r}{s}$ と書く。$S^{-1}R$ には自然な加法と乗法が入り、$\dfrac{0}{1}$ を零元、$\dfrac{1}{1}$ を単位元として環となる。$S^{-1}R$ を R の S による**局所化 (localization)** という。

注意 3.7.2 (局所化は局所環とは限らない)**.** 局所化は局所環とは限らない。

局所化は次の普遍性を持つ。

定理 3.7.3 (局所化の普遍性)**.** R を可換環、$S \subset R$ を R の積閉集合、標準射 $R \to S^{-1}R$ を f とおく。このとき、S の元を可換環 B の単元に写すような任意の環準同型 $g\colon R \to B$ に対し、ある環準同型 $h\colon S^{-1}R \to B$ であって

$$\begin{array}{ccc} S^{-1}R & \overset{h}{\dashrightarrow} & B \\ & {\scriptstyle f}\nwarrow \quad \nearrow{\scriptstyle g} & \\ & R & \end{array} \tag{3.7.2}$$

を可換にするものが一意に存在する。

証明 [TODO] □

局所化は次の性質を持つ。局所化によって S の元は分数の分母のところに置けて単元になるというイメージである。

命題 3.7.4 (局所化の性質)**.** (1) $s \in S$ に対し $f(s)$ は $S^{-1}R$ の単元である。
(2) $f(r) = 0$ ならばある $s \in S$ が存在して $rs = 0$ である。
(3) $S^{-1}R$ の任意の元はある $r \in R$ と $s \in S$ により $f(r)f(s)^{-1}$ の形に表せる。
[TODO]

証明 [TODO] □

定義 3.7.5 (saturation)**.** [TODO]

定義 3.7.6 (extension)**.** [TODO]

命題 3.7.7 (局所化のイデアル)**.** [TODO]

証明 [TODO] □

定理 3.7.8 (局所化の素イデアルの対応原理)**.** [TODO]

証明 [TODO] □

第 4 章　基本的な環

4.1　整数

[TODO] 初等整数論を展開する

定理 4.1.1 (Euclid の互除法). [TODO]

証明　[TODO]　□

4.2　有理数

補題 4.2.1 (有理数の表示). 任意の $q \in \mathbb{Q}$ は $q = k/l,\ k \in \mathbb{Z},\ l \in \mathbb{Z}_{\geq 1},\ \gcd(k,l) = 1$ の形に一意的に表せる。

証明　[TODO]　□

4.3　全行列環

4.4　多項式環

4.5　形式的冪級数環

定義 4.5.1. [TODO] $R[[X]]$

命題 4.5.2. K を体とする。$K[[X]]$ のイデアルは

$$(0), (X^d)\ (d \in \mathbb{Z}_{\geq 0}) \tag{4.5.1}$$

で尽くされる。とくに $K[[X]]$ は局所環かつ PID である。

証明　cf. 問題 4.30　□

4.6　Weyl 代数

定義 4.6.1 (Weyl 代数). 商 $\mathbb{C}$-代数

$$\mathbb{C}[x;\partial] \coloneqq \mathbb{C}[W(\{\widetilde{x},\widetilde{\partial}\})] \ /\ (\widetilde{\partial}\widetilde{x} - \widetilde{x}\widetilde{\partial} - 1) \tag{4.6.1}$$

を **Weyl 代数 (Weyl algebra)** という。$\widetilde{x},\widetilde{\partial}$ の像をそれぞれ x,∂ と書く。より一般に

$$\mathbb{C}[x_1,\dots,x_n;\ \partial_1,\dots,\partial_n] \coloneqq \mathbb{C}[W(\{\widetilde{x}_1,\dots,\widetilde{x}_n,\widetilde{\partial}_1,\dots,\widetilde{\partial}_n\})] \ /\ I \tag{4.6.2}$$

も Weyl 代数と呼ぶ。ただし、I は次の元たちから生成されるイデアルである:

$$\begin{cases} \widetilde{\partial}_i \widetilde{x}_j - \widetilde{x}_j \widetilde{\partial}_i - \delta_{ij} \\ \widetilde{x}_i \widetilde{\partial}_j - \widetilde{\partial}_j \widetilde{x}_i \\ \widetilde{\partial}_i \widetilde{\partial}_j - \widetilde{\partial}_j \widetilde{\partial}_i \end{cases} \tag{4.6.3}$$

定義 4.6.2 (標準基底と標準形)**.** cf. 問題 4.47 [TODO]

命題 4.6.3 (次数)**.** [TODO]

命題 4.6.4. Weyl 代数 $\mathbb{C}[x : \partial]$ は単純環である。

証明 cf. 問題 4.48 □

4.7 演習問題

A. Problem set 1

♤ **演習問題 4.1** (代数学 II 1.1)**.** End(ℤ) を求めよ。

演習問題 4.1 の解答. [TODO] □

♤ **演習問題 4.2** (代数学 II 1.2)**.** μ_2 を 2 次巡回群とする。群環 $\mathbb{C}[\mu_2]$ は $\mathbb{C}\times\mathbb{C}$ と $\mathbb{C}$-algebra として同型であることを示せ。

演習問題 4.2 の解答. まず、$\mathbb{C}[\mu_2]$ および $\mathbb{C}\times\mathbb{C}$ はそれぞれ環準同型

$$\varphi\colon \mathbb{C}\to\mathbb{C}[\mu_2],\quad z\mapsto z\bar{0} \tag{4.7.1}$$

$$\psi\colon \mathbb{C}\to\mathbb{C}\times\mathbb{C},\quad z\mapsto (z,z) \tag{4.7.2}$$

により $\mathbb{C}$-alg となっている。写像 $f\colon \mathbb{C}\times\mathbb{C}\to\mathbb{C}[\mu_2]$ を

$$(a,b)\mapsto \frac{a+b}{2}\bar{0}+\frac{a-b}{2}\bar{1} \tag{4.7.3}$$

で定める。f が $\mathbb{C}$-alg 準同型であることを示す。加法について

$$f((a,b)+(a',b')) = f(a+a',b+b') \tag{4.7.4}$$

$$= \frac{a+a'+b+b'}{2}\bar{0}+\frac{a+a'-b-b'}{2}\bar{1} \tag{4.7.5}$$

$$= \frac{a+b}{2}\bar{0}+\frac{a-b}{2}\bar{1}+\frac{a'+b'}{2}\bar{0}+\frac{a'-b'}{2}\bar{1} \tag{4.7.6}$$

$$= f(a,b)+f(a',b') \tag{4.7.7}$$

乗法について

$$f(a,b)\cdot f(a',b') = \left(\frac{a+b}{2}\bar{0}+\frac{a-b}{2}\bar{1}\right)\cdot\left(\frac{a'+b'}{2}\bar{0}+\frac{a'-b'}{2}\bar{1}\right) \tag{4.7.8}$$

$$= \frac{1}{4}\left((a+b)(a'+b')+(a-b)(a'-b')\right)\bar{0} \tag{4.7.9}$$

$$+\frac{1}{4}\left((a-b)(a'+b')+(a+b)(a'-b')\right)\bar{1} \tag{4.7.10}$$

$$= \frac{aa'+bb'}{2}\bar{0}+\frac{aa'-bb'}{2}\bar{1} \tag{4.7.11}$$

$$= f(aa',bb') \tag{4.7.12}$$

$$= f((a,b)\cdot(a',b')) \tag{4.7.13}$$

単位元について

$$f(1,1) = \frac{1+1}{2}\bar{0}+\frac{1-1}{2}\bar{1} = 1\bar{0} \tag{4.7.14}$$

が成り立つから、f は環準同型である。また、図式

$$\begin{array}{ccc} \mathbb{C}\times\mathbb{C} & \xrightarrow{\ f\ } & \mathbb{C}[\mu_2] \\ & {\scriptstyle\psi}\nwarrow \quad \nearrow{\scriptstyle\varphi} & \\ & \mathbb{C} & \end{array} \tag{4.7.15}$$

が可換となることは

$$f \circ \psi(z) = f(z, z) = z\bar{0} = \varphi(z) \tag{4.7.16}$$

よりわかる。したがって f は $\mathbb{C}$-alg 準同型である。f の定義より明らかに $\mathrm{Ker}\, f = 0$ だから、f は単射である。また、再び f の定義から明らかに f は全射である。よって f は全単射、したがって $\mathbb{C}$-alg 同型である。 □

♤ **演習問題 4.3** (代数学 II 1.3)**.** A, B を零環でない環、$f\colon A \to B$ を単射とする。さらに任意の $x, y \in A$ に対して

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y) \tag{4.7.17}$$

が成り立つとする。このとき f は環準同型となるか？

演習問題 4.3 の解答. 反例を挙げる。$A \coloneqq \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in M_2(\mathbb{Z}) \mid a \in \mathbb{Z} \right\}$, $B \coloneqq M_2(\mathbb{Z})$ とおき、写像 $f\colon A \to B$ を

$$f\colon \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mapsto \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \tag{4.7.18}$$

で定める。f は明らかに単射で、また行列の演算の性質から $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ も成り立つ。しかし

$$f\colon 1_A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq 1_B \tag{4.7.19}$$

だから f は環準同型ではない。 □

♤ **演習問題 4.4** (代数学 II 1.4)**.** 可換環の 2 つの冪零元の和は冪零元になることを示せ。また非可換環の場合は同じことが成り立つか？

演習問題 4.4 の解答. a, b が冪零元であるとし、$a^m = 0, b^n = 0$ $(m, n \in \mathbb{Z}_{>0})$ とする。$l = m + n$ とおくと、

$$(a + b)^l = \sum_{k=0}^{l} \binom{l}{k} a^{l-k} b^k = 0 \tag{4.7.20}$$

が成り立つ。ただし、最初の等号では a, b が可換であることを用い、最後の等号では

- $k \geq m$ のとき $a^k = 0$
- $k < m$ のとき $l - k > l - m = n$ より $b^{l-k} = 0$

であることを用いた。したがって $a + b$ も冪零元である。

非可換環の場合の反例として

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \ B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in M_2(\mathbb{Z}) \tag{4.7.21}$$

を考える。

$$A^2 = 0, B^2 = 0 \tag{4.7.22}$$

だからこれらは冪零元である。一方、

$$A + B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4.7.23}$$

ゆえに

$$(A + B)^2 = I_2 \tag{4.7.24}$$

だから、$(A + B)^n = 0$ なる正整数 n があったとすると

$$I_2 = (A + B)^{2n} = 0 \tag{4.7.25}$$

となり矛盾。 □

♤ **演習問題 4.5** (代数学 II 1.5)**.** A を環、$u \in A^\times$ とし、$n \in A$ を冪零元として $un = nu$ であるとする。このとき $u + n \in A^\times$ を示せ。

演習問題 4.5 の解答. $n^{k-1} \neq 0, n^k = 0, k \in \mathbb{Z}_{>0}$ とする。$u + n$ の逆元を発見する手立てとして、等比数列の公式を思い出して形式的に

$$(u + n)^{-1} \overset{?}{=} \frac{1}{u + n} \overset{?}{=} u^{-1} \frac{1}{1 + nu^{-1}} \overset{?}{=} u^{-1} \sum_{i=0}^{\infty} (-nu^{-1})^i \tag{4.7.26}$$

と書いてみると、

$$u^{-1} \sum_{i=0}^{k-1} (-1)^i u^{-i} n^i \tag{4.7.27}$$

が $u + n$ の逆元になりそうだと気づく。そして実際、

$$(u + n)u^{-1} \sum_{i=0}^{k-1} (-1)^i u^{-i} n^i = (u + n) \sum_{i=0}^{k-1} (-1)^i u^{-i-1} n^i \tag{4.7.28}$$

$$= u \sum_{i=0}^{k-1} (-1)^i u^{-i-1} n^i + n \sum_{i=0}^{k-1} (-1)^i u^{-i-1} n^i \tag{4.7.29}$$

$un = nu$ より $u^{-1}n = nu^{-1}$ であることに注意して

$$= \sum_{i=0}^{k-1} (-1)^i u^{-i} n^i + \sum_{i=0}^{k-1} (-1)^i u^{-i-1} n^{i+1} \tag{4.7.30}$$

$$= \sum_{i=0}^{k-1} (-1)^i u^{-i} n^i + \sum_{i=0}^{k-2} (-1)^i u^{-i-1} n^{i+1} \tag{4.7.31}$$

$$= \sum_{i=0}^{k-1} (-1)^i u^{-i} n^i + \sum_{i=1}^{k-1} (-1)^{i-1} u^{-i} n^i \tag{4.7.32}$$

$$= 1 \tag{4.7.33}$$

となる。したがって $u + n \in A^\times$ である。 □

♤ **演習問題 4.6** (代数学 II 1.6). S を index set とし、$\{A_i\}_{i\in S}$ を環の族とする。$(B, \{q_i\colon B \to A_i\}_{i\in S})$ が $\{A_i\}_{i\in S}$ の圏論的直積であるとは、$\{q_i\colon B \to A_i\}_{i\in S}$ は環準同型の族であって任意の環準同型の族 $\{f_i\colon C \to A_i\}_{i\in S}$ に対して図式

$$\begin{array}{ccc} C & \xrightarrow{F} & B \\ & {\scriptstyle f_i}\searrow \quad \swarrow{\scriptstyle q_i} & \\ & A_i & \end{array} \tag{4.7.34}$$

を可換にするような環準同型 $F\colon C \to B$ が一意に存在することをいう。

(a) 直積環 $(\prod_{i\in S} A_i, \{p_i\colon \prod_{i\in S} A_i \to A_i\}_{i\in S})$ は $\{A_i\}_{i\in S}$ の圏論的直積であることを示せ。ここで p_i は標準射影である。

(b) 任意の $\{A_i\}_{i\in S}$ の圏論的直積 $(B, \{q_i\colon B \to A_i\}_{i\in S})$ に対して、

$$\begin{array}{ccc} \prod_{i\in S} A_i & \xrightarrow{\Psi} & B \\ & {\scriptstyle p_i}\searrow \quad \swarrow{\scriptstyle q_i} & \\ & A_i & \end{array} \tag{4.7.35}$$

を可換にするような環の同型写像 $\Psi\colon \prod_{i\in S} A_i \to B$ が一意に存在することを示せ。

演習問題 4.6 の解答. [TODO] □

♤ **演習問題 4.7** (代数学 II 1.7). R を環とする。全行列環 $M_n(R)$ の中心 $Z(M_n(R))$ を求めよ。

演習問題 4.7 の解答. $A = (a_{ij}) \in M_n(R)$ とする。(i, j) 成分が 1 の行列単位を E_{ij} と書くことにする。まず

$$\begin{bmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ a_{i1} & \dots & a_{in} \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{bmatrix} = E_{ii}A = AE_{ii} = \begin{bmatrix} 0 & \dots & a_{1i} & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & a_{ni} & \dots & 0 \end{bmatrix} \tag{4.7.36}$$

より A は対角行列である。つぎに

$$a_{jj}E_{ij} = E_{ij}A = AE_{ij} = a_{ii}E_{ij} \tag{4.7.37}$$

より $a_{jj} = a_{ii}$ であるから、A はスカラー行列である。そこで $A = aI_n, a \in R$ とおく。任意の $b \in R$ に対し

$$abI_n = A(bI_n) = (bI_n)A = baI_n \tag{4.7.38}$$

したがって $ab = ba$ が成り立つ。よって $a \in Z(R)$ である。逆に対角成分が $Z(R)$ の元であるようなスカラー行列は明らかに $Z(M_n(R))$ に属する。したがって $Z(M_n(R))$ は対角成分が $Z(R)$ の元であるようなスカラー行列の全体である。 □

♤ **演習問題 4.8** (代数学 II 1.8)**.** $(A,+,\cdot,0)$ が **nonunital ring** であるとは、

- $(A,+,0)$ がアーベル群かつ
- $(A,\cdot)$ が半群で
- 分配法則をみたすもの

とする。$f\colon A\to B$ が nonunital ring の準同型であるとは、

- 任意の $x,y\in A$ に対して $f(x+y)=f(x)+f(y)$ かつ $f(xy)=f(x)f(y)$ が成り立つこと

とする。さて、任意の nonunital ring A に対して、環 A_1 と nonunital ring の準同型 $\iota\colon A\to A_1$ であって次の条件を満たすものが存在することを示せ:

(条件) 任意の環 B と nonunital ring の準同型 $f\colon A\to B$ に対して図式

$$\begin{array}{ccc} A & \xrightarrow{\iota} & A_1 \\ {\scriptstyle f}\downarrow & \swarrow_{f_1} & \\ B & & \end{array} \tag{4.7.39}$$

を可換にするような環準同型 $f_1\colon A_1\to B$ が一意に存在する。

演習問題 4.8 の解答. [TODO] □

♤ **演習問題 4.9** (代数学 II 1.9)**.** $C(\mathbb{R})$ を $\mathbb{R}$ 上の $\mathbb{C}$ 値連続関数全体のなす $\mathbb{C}$-alg とする。$C(\mathbb{R})$ の零因子を求めよ。

演習問題 4.9 の解答. $f\in C(\mathbb{R})$ が $C(\mathbb{R})$ の零因子であることが次と同値であることを示す:

$$f\neq 0 \quad\text{and}\quad \exists U \overset{\text{open}}{\subset} \mathbb{R} \quad\text{s.t.}\quad \forall x\in U \quad\text{に対し}\quad f(x)=0 \tag{4.7.40}$$

($\Leftarrow$) U は $\mathbb{R}$ の開集合だから、或る開区間 $(x_0-\varepsilon,x_0+\varepsilon),\ x_0\in\mathbb{R},\varepsilon>0$ を含む。そこで

$$g(x)\coloneqq\begin{cases} x-(x_0-\varepsilon/2) & x\in(x_0-\varepsilon/2,x_0)\\ -x+(x_0+\varepsilon/2) & x\in(x_0,x_0+\varepsilon/2)\\ 0 & \text{otherwise}\end{cases} \tag{4.7.41}$$

と定めれば $g\in C(\mathbb{R}), g\neq 0$ であり、$f|_U=0$ の仮定から $f\cdot g=0$ が従う。$f\neq 0, g\neq 0$ だから f は $C(\mathbb{R})$ の零因子である。

($\Rightarrow$) f は $C(\mathbb{R})$ の零因子であるとする。零因子の定義から $f\neq 0$ である。背理法のため

$$\forall U \overset{\text{open}}{\subset} \mathbb{R} \quad\text{に対し}\quad \exists x\in U \quad\text{s.t.}\quad f(x)\neq 0 \tag{4.7.42}$$

を仮定する。いま f が $C(\mathbb{R})$ の零因子であることから

$$\exists g\in C(\mathbb{R}), g\neq 0 \quad\text{s.t.}\quad f\cdot g=0 \tag{4.7.43}$$

である。このとき、$g\neq 0$ より

$$\exists x_0\in\mathbb{R} \quad\text{s.t.}\quad g(x_0)\neq 0 \tag{4.7.44}$$

である。このことと g の点 x_0 における連続性より

$$\exists U\colon x_0 \text{ の開近傍} \quad \text{s.t.} \quad \forall x \in U \quad \text{に対し} \quad g(x) \neq 0 \tag{4.7.45}$$

が成り立つ。ここで、この U に対して背理法の仮定を用いると

$$\exists x_1 \in U \quad \text{s.t.} \quad f(x_1) \neq 0 \tag{4.7.46}$$

である。よって

$$(f \cdot g)(x_1) = f(x_1)g(x_1) \neq 0 \tag{4.7.47}$$

が成り立つ。これは $f \cdot g = 0$ に矛盾。 □

♤ **演習問題 4.10** (代数学 II 1.10)**.** A を $1 < \dim_{\mathbb{C}} A < \infty$ なる $\mathbb{C}$-alg とする。このとき A は零因子を持つことを示せ。

演習問題 4.10 の解答. $\dim_{\mathbb{C}} A > 1$ だから $\mathbb{C}$-線型独立な $v_1, v_2 \in A$ がとれる。A が零因子を持たないとして矛盾を導く。$a \in A \setminus \{0\}$ とし、2 つの写像

$$L_a\colon A \to A, \quad x \mapsto ax, \quad R_a\colon A \to A, \quad x \mapsto xa \tag{4.7.48}$$

を考える。これらは明らかに $\mathbb{C}$-線型であり、A が零因子を持たないという仮定から Ker は自明、したがって単射である。$\dim_{\mathbb{C}} < \infty$ であることとあわせて、L_a, R_a の全射性が従う。よって

$$\begin{cases} \exists x \in A \quad \text{s.t.} \quad ax = 1 \\ \exists y \in A \quad \text{s.t.} \quad ya = 1 \end{cases} \tag{4.7.49}$$

であり、逆元の一意性から $x = y$ が従う。よって a は A の可逆元である。さて、$a \in A \setminus \{0\}$ は任意であったから、とくに v_1, v_2 も A の可逆元である。そこで $w \coloneqq v_2 v_1^{-1}$ $(\neq 0)$ とおき、$\mathbb{C}$-線型写像 L_w の特性多項式[1)] を $\Phi(X)$ とおく。Cayley-Hamilton の定理より $\Phi(L_w) = 0$ が成り立つから、

$$0 = (\Phi(L_w))(v_1) = \Phi(w)v_1 \tag{4.7.50}$$

であり、A が零因子を持たないという仮定から $\Phi(w) = 0$ が従う。ここで、$\mathbb{C}$ は代数的閉体だから $\Phi(X)$ は 1 次式の積に分解し

$$\Phi(X) = (X - \mu_1)(X - \mu_2)\cdots(X - \mu_n) \tag{4.7.51}$$

の形に書ける。ただし μ_i らは L_w の固有値である。したがって、$\Phi(w) = 0$ であることと、A が零因子を持たないという仮定をあわせて

$$w - \mu_k \cdot 1_A = 0 \quad (\exists k = 1, \ldots, n) \tag{4.7.52}$$

が成り立ち、w の定義とあわせて

$$v_2 = wv_1 = \mu_k \cdot v_1 \tag{4.7.53}$$

が従う。これは v_1, v_2 の $\mathbb{C}$-線型独立性に矛盾する。よって A が零因子を持たないとした仮定は偽で、題意の主張が示せた。 □

♤ **演習問題 4.11** (代数学 II 1.11)**.** A を環とする。ある零環でない環 B, C が存在して $A \cong B \times C$ となるための必要十分条件は $0, 1 \neq e$ なる冪等元 $e \in Z(A)$ が存在することであることを示せ。

演習問題 4.11 の解答. ($\Rightarrow$)　$B \times C$ において $(1_B, 0) \neq 1_{B\times C}, 0_{B\times C}$ は

$$(1_B, 0)^2 = (1_B, 0) \tag{4.7.54}$$

をみたすから冪等元であり、また明らかに $B \times C$ の中心に属する。そこで、これを同型によって A に写したものが求める e となる。

($\Leftarrow$)　$e, 1-e$ は A の中心冪等元だから、

$$B \coloneqq Ae, \quad C \coloneqq A(1-e) \tag{4.7.55}$$

はそれぞれ $e, 1-e$ を単位元として環をなす。そこで写像 $A \to B \times C$ を

$$x \mapsto (xe, x(1-e)) \tag{4.7.56}$$

で定めれば、これが環同型 $A \cong B \times C$ を与える。定義より B, C は零環でないから、これらが求めるものである。 □

♤ **演習問題 4.12** (代数学 II 1.12 Hamilton's Quaternions)**.** $M_2(\mathbb{C})$ を実ベクトル空間と考え、

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \tag{4.7.57}$$

で生成される 4 次元実部分空間を $\mathbb{H}$ とおく。$\mathbb{H}$ は $M_2(\mathbb{C})$ の部分環となり、さらに division algebra となることを示せ。

演習問題 4.12 の解答. 所与の行列を左から順に $1, I, J, K$ と書くことにする。乗積表は

	1	I	J	K
1	1	I	J	K
I	I	-1	K	$-J$
J	J	$-K$	-1	I
K	K	J	$-I$	-1

となる。よって

$$\begin{aligned}(a1 + bI + cJ + dK)(a'1 + b'I + c'J + d'K) = {} & aa'1 + bb'I + cc'J + dd'K \\ & + ba'I - bb'1 + bc'K - bd'J \\ & + ca'J - cb'K - cc'1 + cd'I \\ & + da'K + db'J - dc'I - dd'1\end{aligned}$$

1)　有限次元線型空間の自己準同型 f に対し、適当な基底による行列表現 B の特性多項式 $\det(XI_n - B)$ を f の**特性多項式 (characteristic polynomial)** という。

である。そこで

$$a' = a, \quad b' = -b, \quad c' = -c, \quad d' = -d \tag{4.7.58}$$

とおけば

$$(a1 + bI + cJ + dK)(a1 - bI - cJ - dK) = (a^2 + b^2 + c^2 + d^2)1 \tag{4.7.59}$$

となる。したがって $a^2 + b^2 + c^2 + d^2 \neq 0$ のとき、すなわち $a1 + bI + cJ + dK \in \mathbb{H} \setminus \{0\}$ のとき $a1 + bI + cJ + dK$ の乗法逆元が

$$\frac{1}{a^2 + b^2 + c^2 + d^2}(a1 - bI - cJ - dK) \tag{4.7.60}$$

で与えられることがわかる。よって $\mathbb{H} \setminus \{0\} \subset \mathbb{H}^\times$ である。逆向きの包含も明らかに成り立つ。よって $\mathbb{H} \setminus \{0\} = \mathbb{H}^\times$、したがって $\mathbb{H}$ は division algebra である。 □

♤ **演習問題 4.13** (代数学 II 1.13). $\{x \in \mathbb{H} \mid x^2 = -1\}$ は無限集合であることを示せ。

演習問題 4.13 の解答. $x = a + bi + cj + dk \in \mathbb{H}$ とおくと

$$\begin{aligned} x^2 &= (a + bi + cj + dk)^2 && (4.7.61)\\ &= aa + abi + acj + adk && (4.7.62)\\ &\quad + bai - bb + bck - bdj && (4.7.63)\\ &\quad + caj - cbk - cc + cdi && (4.7.64)\\ &\quad + dak + dbj - dci - dd && (4.7.65)\\ &= a^2 - b^2 - c^2 - d^2 + 2abi + 2acj + 2adk && (4.7.66) \end{aligned}$$

だから、これが -1 に一致する条件は

$$\begin{cases} a^2 - b^2 - c^2 - d^2 = -1 \\ ab = ac = ad = 0 \end{cases} \tag{4.7.67}$$

すなわち

$$a = 0 \land b^2 + c^2 + d^2 = 1 \tag{4.7.68}$$

である。よって

$$\begin{aligned} \{x \in \mathbb{H} \mid x^2 = -1\} &= \{bi + cj + dk \mid b^2 + c^2 + d^2 = 1\} && (4.7.69)\\ &= \{(\sin\theta_1 \sin\theta_2)i + (\sin\theta_1 \cos\theta_2)j + (\cos\theta_1)k \mid \theta_1, \theta_2 \in \mathbb{R}\} && (4.7.70) \end{aligned}$$

が成り立つ。右辺は無限集合だから、左辺もそうであり、したがって題意の主張が示せた。 □

♤ **演習問題 4.14** (代数学 II 1.14). 非可換 3 次元 $\mathbb{C}$-alg は 0 でない冪零元をもつことを示せ。

演習問題 4.14 の解答. [TODO] 1.10 を使えば零因子の存在はいえるが…？ cf. http://doi.org/10.5169/seals-46956 □

♤ **演習問題 4.15** (代数学 II 1.15). $M_n(\mathbb{C})$ の $\mathbb{C}$-alg としての自己同型写像をすべて求めよ。

演習問題 4.15 の解答. [TODO] □

♤ **演習問題 4.16** (代数学 II 1.16). 任意の巡回群を考えその演算を加法とみなす。すると環の構造を与える乗法が一意に定まることを示せ。

演習問題 4.16 の解答. [TODO] 環同型を除いて？巡回群は $\mathbb{Z}$ あるいは $\mathbb{Z}/n\mathbb{Z}$ に群同型だから、$\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ について考えれば十分。そこで、まず $\mathbb{Z}$ について考える。$\mathbb{Z}$ の通常の加法、乗法をそれぞれ $+, \times$ で表すことにし、さらに $\mathbb{Z}$ に乗法 $\odot$ が与えられたとする。乗法 $\odot$ に関する単位元を e とおく。このとき $e = 0$ なら

$$1 = e \odot 1 \tag{4.7.71}$$
$$= 0 \odot 1 \tag{4.7.72}$$
$$= 0 \tag{4.7.73}$$

となり矛盾だから、$e \neq 0$ である。$e > 0$ の場合

$$1 = e \odot 1 \tag{4.7.74}$$
$$= \underbrace{(1 + \cdots + 1)}_{e \text{ times}} \odot 1 \tag{4.7.75}$$
$$= \underbrace{1 \odot 1 + \cdots + 1 \odot 1}_{e \text{ times}} \tag{4.7.76}$$
$$= e \times (1 \odot 1) \tag{4.7.77}$$

ゆえに e は乗法 $\times$ に関し可逆だから $e = \pm 1$ である。いま $e > 0$ であったから $e = 1$ である。すると $1 \odot 1 = e \odot e = e = 1$ だから、各 $a, b \in \mathbb{Z}$ に対し

$$a \odot b = a \times b \times (1 \odot 1) \tag{4.7.78}$$
$$= a \times b \times 1 \tag{4.7.79}$$
$$= a \times b \tag{4.7.80}$$

が成り立つ。 □

♤ **演習問題 4.17** (代数学 II 1.17). 2 次元 $\mathbb{C}$-alg を同型を除いて分類せよ。

演習問題 4.17 の解答. [TODO] □

♤ **演習問題 4.18** (代数学 II 1.18). $\mathbb{Z}[\sqrt{2}] = \{n + \sqrt{2}m \mid n, m \in \mathbb{Z}\}$ は $\mathbb{C}$ の部分環になることを示せ。また次を示し $\mathbb{Z}[\sqrt{2}]^\times$ が無限群であることを示せ:

$$\mathbb{Z}[\sqrt{2}]^\times = \{n + \sqrt{2}m \mid n, m \in \mathbb{Z}, n^2 - 2m^2 = \pm 1\} \tag{4.7.81}$$

演習問題 4.18 の解答. $\mathbb{Z}[\sqrt{2}]$ が $\mathbb{C}$ の加法部分群であることと 1 を含むことは明らか。乗法について閉じていることは

$$(n+\sqrt{2}m)(a+\sqrt{2}b) = na+2mb+\sqrt{2}(nb+ma) \tag{4.7.82}$$

よりわかる。したがって $\mathbb{Z}[\sqrt{2}]$ は $\mathbb{C}$ の部分環である。乗法群 $\mathbb{Z}[\sqrt{2}]^\times$ が題意のように表されることを示す。"⊂"はモノイド準同型

$$N : \mathbb{Z}[\sqrt{2}]^\times \to \mathbb{Z}, \quad n+\sqrt{2}m \mapsto n^2-2m^2 \tag{4.7.83}$$

を用いて示せる。

∵ $(n+\sqrt{2}m)(a+\sqrt{2}b)=1$ であるとすれば、両辺を N で写して

$$(n^2-2m^2)(a^2-2b^2)=1 \tag{4.7.84}$$

よって $n^2-2m^2=\pm 1$ を得る。 //

"⊃"は、$n^2-2m^2=\pm1$ のとき $n+\sqrt{2}m$ の逆元が $\pm(n-\sqrt{2}m)$ となることから明らか。最後に $\mathbb{Z}[\sqrt{2}]^\times$ が無限群であることは、ひとつの解 $n+\sqrt{2}m$ から新たな解として $(n^2+2m^2)+2\sqrt{2}nm$ を構成できることからわかる。

∵ 実際、

$$(n^2+2m^2)^2-2(2nm)^2 = (n^2-2m^2)^2 \tag{4.7.85}$$

$$= 1 \tag{4.7.86}$$

である。新たな解の実部 n^2+2m^2 はもとの解より大きいから、この構成で得られる無限個の解たちはすべて相異なる。 //

□

B. Problem set 2

♤ **演習問題 4.19** (代数学 II 2.19)**.** 次数が k である n 変数単項式の個数を $d_n(k)$ とおく。

$$\frac{1}{(1-t)^n} = \sum_{k=0}^{\infty} d_n(k)t^k \quad (|t|<1) \tag{4.7.87}$$

を示せ。また $d_n(k)$ を求めよ。

演習問題 4.19 の解答. [TODO] まず $n \in \mathbb{Z}_{\geq 1}, k \in \mathbb{Z}_{\geq 0}$ に対し

$$d_n(k) = \binom{k+n-1}{n-1} \tag{4.7.88}$$

である (区別のある n 個の箱に区別のない k 個の玉を入れることを考える)。つぎに、$n \in \mathbb{Z}_{\geq 0}$ に対し

$$\frac{d^n}{dt^n}\frac{t^n}{1-t} = \frac{d^n}{dt^n}\sum_{k=0}^{\infty} t^{k+n} \tag{4.7.89}$$

$$= \sum_{k=0}^{\infty} \frac{d^n}{dt^n} t^{k+n} \tag{4.7.90}$$

$$= \sum_{k=0}^{\infty} (k+n)\dots(k+1)t^k \tag{4.7.91}$$

が成り立つ。一方、

$$\frac{d^n}{dt^n}\frac{t^n}{1-t} = \frac{d^n}{dt^n}\left(-(t^{n-1}+\dots+t+1)+\frac{1}{1-t}\right) \tag{4.7.92}$$

$$= \frac{d^n}{dt^n}\frac{1}{1-t} \tag{4.7.93}$$

$$= n!\frac{1}{(1-t)^{n+1}} \tag{4.7.94}$$

が成り立つ。したがって

$$\frac{1}{(1-t)^{n+1}} = \frac{1}{n!}\frac{d^n}{dt^n}\frac{t^n}{1-t} \tag{4.7.95}$$

$$= \frac{1}{n!}\sum_{k=0}^{\infty}(k+n)\dots(k+1)t^k \tag{4.7.96}$$

$$= \sum_{k=0}^{\infty}\binom{k+n}{n}t^k \tag{4.7.97}$$

$$= \sum_{k=0}^{\infty} d_{n+1}(k)t^k \tag{4.7.98}$$

である。 □

♤ **演習問題 4.20** (代数学 II 2.20)**.** 体 K 上の 1 変数多項式環 $K[X]$ は Euclid 整域であることを示せ。

演習問題 4.20 の解答. $K[X]$ が Euclid 整域であることを示す。まず $K[X]$ が整域であることは、任意の $f, g \in K[X] - \{0\}$ について

$$f(X) = \sum_{i=0}^{\deg(f)} a_i X^i, \quad a_{\deg(f)} \neq 0 \tag{4.7.99}$$

$$g(X) = \sum_{i=0}^{\deg(g)} b_i X^i, \quad b_{\deg(g)} \neq 0 \tag{4.7.100}$$

と表したときに、これらの積

$$f(X)\cdot g(X) = \sum_{i=0}^{\deg(f)+\deg(g)} \sum_{j=0}^{i} a_j b_{i-j} X^i \tag{4.7.101}$$

の最高次係数 $a_{\deg(f)}b_{\deg(g)}$ が 0 でない ($\because$ K は整域) ことから従う。さらに写像 $\deg\colon K[X] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ は次をみたす:

(1) $\deg(K[X] - \{0\}) \subset \mathbb{Z}_{\geq 0}$

(2) $\deg(0) = -\infty$

(3) $\forall f \in K[X]$ と $\forall g \in K[X] - \{0\}$ に対し、K が体ゆえに g の最高次係数は単元だから、多項式環の除法

定理 (定理 2.3.4) より $\exists q, r \in K[X]$ が存在して

$$f = g \cdot q + r, \quad \deg(r) < \deg(g) \tag{4.7.102}$$

が成り立つ。

したがって $K[X]$ は Euclid 整域である。 □

♤ **演習問題 4.21** (代数学 II 2.21). K を体、$f \in K[X], f \neq 0$ で f の次数を n とする。このとき $\{a \in K : f(a) = 0\}$ の濃度は n 以下であることを示せ。

注意 4.7.1. この問題の主張は K が整域ならば成り立つが、K が division algebra の場合は成り立たない (問題 4.13)。一般的に、可換性を要する命題の証明では、その過程で根の個数の不等式を利用することがよくある。

演習問題 4.21 の解答. n に関する帰納法で示す。$n = 0$ の場合は f の根は存在しないから主張が成り立つ。$n \geq 1$ とし、すべての $k = 0, 1, \ldots, n-1$ に対し主張の成立を仮定する。f が根を持たなければただちに主張が成り立つから、f は少なくとも 1 つの根 $\alpha_0 \in K$ を持つとする。剰余定理より

$$\exists g \in K[X] \quad \text{s.t.} \quad f(X) = (X - \alpha_0) g(X) \tag{4.7.103}$$

が成り立つ。いま K は体、とくに整域だから α_0 以外の f の根は g の根でもある。さらに $\deg g = \deg f - 1 = n - 1$ であることとあわせて、帰納法の仮定より

$$\begin{aligned} |\{a \in K : f(a) = 0\}| &\leq |\{a \in K : g(a) = 0\} \cup \{\alpha_0\}| && (4.7.104)\\ &\leq |\{a \in K : g(a) = 0\}| + 1 && (4.7.105)\\ &\leq n && (4.7.106) \end{aligned}$$

が成り立つ。 □

♤ **演習問題 4.22** (代数学 II 2.22). K を体とする。乗法群 $K^\times$ の任意の有限部分群は巡回群になることを示せ。

演習問題 4.22 の解答. [TODO] トーシェント関数についてどこかに書きたい

Euler のトーシェント関数を φ とおく。すなわち

$$\varphi(n) = (n \text{ と互いに素な } n \text{ 以下の正整数の個数}) \quad (n \in \mathbb{Z}_{\geq 1}) \tag{4.7.107}$$

とおく。一般に、任意の巡回群 G に対し

$$\sharp\{x \in G : x \text{ は } G \text{ の生成元}\} = \varphi(|G|) \tag{4.7.108}$$

が成り立つ。

(∵) $d = |G|$ とおき、G の生成元 g_0 をひとつ固定する。$g \in G$ を G の生成元とすると、ある $1 \leq d' \leq d$ がただひとつ存在して $g = g_0^{d'}$ が成り立つ。このとき $\gcd(d', d) = 1$ である。実際、g が生

成元であることより、ある $1 \leq k \leq d$ が存在して

$$g_0 = g^k = g_0^{d'k} \tag{4.7.109}$$

が成り立つ。よって、ある $l \in \mathbb{Z}$ が存在して

$$1 = d'k + dl \tag{4.7.110}$$

が成り立つ。よって $\gcd(d', d) = 1$ である。逆に $1 \leq d'' \leq d$ が $\gcd(d'', d) = 1$ をみたすとすればある $k', l' \in \mathbb{Z}$ が存在して

$$1 = d''k' + dl' \tag{4.7.111}$$

が成り立つから、

$$g_0 = g_0^{d''k'} \tag{4.7.112}$$

となり、したがって $g_0^{d''}$ は G の生成元である。以上より全単射

$$\{x \in G \colon x \text{ は } G \text{ の生成元}\} \leftrightarrow \{k \in \{1, \dots, d\} \colon \gcd(k, d) = 1\} \tag{4.7.113}$$

が存在するから、求める主張が従う。 //

また、一般に任意の正整数 n に対し

$$n = \sum_{d|n} \varphi(d) \tag{4.7.114}$$

が成り立つ。

$\because$ 巡回群 $\mathbb{Z}/n\mathbb{Z}$ を考える。各 $d \in \mathbb{Z}_{\geq 1},\ d|n$ に対し、$\mathbb{Z}/n\mathbb{Z}$ の位数 d の巡回部分群 H_d はただひとつ存在する (ちなみにそれは $H_d = \left\langle \frac{n}{d} + n\mathbb{Z} \right\rangle$ である) から、

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \{x \in \mathbb{Z}/n\mathbb{Z} \colon x \text{ の位数は } d\} \tag{4.7.115}$$

$$= \bigsqcup_{d|n} \{x \in \mathbb{Z}/n\mathbb{Z} \colon x \text{ は } H_d \text{ の生成元}\} \tag{4.7.116}$$

が成り立つ。よって

$$n = \sum_{d|n} \sharp\{x \in \mathbb{Z}/n\mathbb{Z} \colon x \text{ は } H_d \text{ の生成元}\} \tag{4.7.117}$$

$$= \sum_{d|n} \varphi(d) \tag{4.7.118}$$

である。 //

さて、$H \subset K^\times$ を有限部分群とし、H が巡回群であることを示す。$n := |H|$ とおくと

$$H = \bigsqcup_{d|n} \{x \in H \colon x \text{ の位数は } d\} \tag{4.7.119}$$

が成り立つ。$d \in \mathbb{Z}_{\geq 1},\ d|n$ とし、H の位数 d の元 x_0 が存在したとする。すると

$$\langle x_0 \rangle \subset \{x \in H \colon x^d = 1\} \tag{4.7.120}$$

が成り立つが、いま H は体 K の部分集合であったから右辺の集合の濃度は d 以下である (問題 4.21)。このことと、左辺の集合の濃度が d であることをあわせて

$$\langle x_0 \rangle = \{x \in H \colon x^d = 1\} \tag{4.7.121}$$

が成り立つ。よって x_0 は巡回群 $\{x \in H \colon x^d = 1\}$ の生成元である。したがって、各 $d \in \mathbb{Z}_{\geq 1}$, $d|n$ に対し

$$H_d \coloneqq \{x \in H \colon x^d = 1\} \tag{4.7.122}$$

とおけば

$$\{x \in H \colon x \text{ の位数は } d\} = \begin{cases} \{x \in H \colon x \text{ は } H_d \text{ の生成元}\} & (H \text{ が位数 } d \text{ の元をもつ}) \\ \varnothing & (\text{otherwise}) \end{cases} \tag{4.7.123}$$

が成り立つ。したがって

$$\begin{aligned} n &= |H| && (4.7.124)\\ &= \sum_{d|n} \sharp\{x \in H \colon x \text{ の位数は } d\} && (4.7.125)\\ &\leq \sum_{d|n} \sharp\{x \in H \colon x \text{ は } H_d \text{ の生成元}\} && (4.7.126)\\ &= \sum_{d|n} \varphi(d) \quad (\because (4.7.108)) && (4.7.127)\\ &= n \quad (\because (4.7.114)) && (4.7.128) \end{aligned}$$

が成り立つ。よってとくに集合 $\{x \in H \colon x \text{ の位数は } d\}$ は空でなく、H は位数 n の元をもつ。したがって H は巡回群である。 □

♤ **演習問題 4.23** (代数学 II 2.23)**.** Gauss 整数環 $\mathbb{Z}[i] = \{m + ni \colon m, n \in \mathbb{Z}\}$ は Euclid 整域であることを示せ。

演習問題 4.23 の解答. 写像 $N \colon \mathbb{Z}[i] \to \mathbb{Z}$ を

$$N(m + ni) \coloneqq m^2 + n^2 \tag{4.7.129}$$

で定める。$\mathbb{C}$ における絶対値の性質から明らかに

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad (\forall \alpha, \beta \in \mathbb{Z}[i]) \tag{4.7.130}$$

が成り立つ。さて、$\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ に対し

$$\exists \gamma, \delta \in \mathbb{Z}[i] \quad \text{s.t.} \quad \alpha = \beta\gamma + \delta, \quad N(\delta) < N(\beta) \tag{4.7.131}$$

を示す。目標の式から逆算して形式的に変形してみると

$$\frac{\alpha}{\beta} - \gamma = \frac{\delta}{\beta} \tag{4.7.132}$$

を得る。右辺の絶対値をできるだけ小さくすればうまくいきそうである。そこで α/β に最も近い Gauss 整数のひとつを $\gamma \in \mathbb{Z}[i]$ とおき、$\delta \coloneqq \alpha - \beta\gamma \in \mathbb{Z}[i]$ とおく。あとは $N(\delta) < N(\beta)$ を示せばよい。γ の定め方から

明らかに

$$\left|\gamma - \frac{\alpha}{\beta}\right| < 1 \tag{4.7.133}$$

なので

$$1 > N\left(\frac{\delta}{\beta}\right) = \frac{N(\delta)}{N(\beta)} \tag{4.7.134}$$

よって $N(\delta) < N(\beta)$ が成り立つ。そこで写像 $N' \colon \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ を

$$N'(\alpha) \coloneqq \begin{cases} N(\alpha) - 1 & (\alpha \neq 0) \\ -\infty & (\alpha = 0) \end{cases} \tag{4.7.135}$$

と定めれば N' は

(1) $N'(\mathbb{Z}[i] - \{0\}) \subset \mathbb{Z}_{\geq 0}$
(2) $N'(0) = -\infty$
(3) $\forall \alpha \in \mathbb{Z}[i]$ と $\beta \in \mathbb{Z}[i] - \{0\}$ に対し、$\exists \gamma, \delta \in \mathbb{Z}[i]$ が存在して

$$\alpha = \beta\gamma + \delta, \quad N'(r) < N'(g) \tag{4.7.136}$$

が成り立つ (除法定理)。

をみたすから、$\mathbb{Z}[i]$ は Euclid 整域である。 □

♤ **演習問題 4.24** (代数学 II 2.24)**.** K を無限個の元を持つ体とする。このとき $\mathrm{Map}(K^n, K)$ で K^n から K への写像全体のなす集合とする。K 上の n 変数多項式環 $K[X_1, \ldots, X_n]$ から $\mathrm{Map}(K^n, K)$ への写像 F を $K[X_1, \ldots, X_n]$ の元を対応する多項式関数に写すことで与える。このとき F は単射であることを示せ。

演習問題 4.24 の解答. 各 $n \in \mathbb{Z}_{\geq 1}$ に対し F を F_n と書くことにし、$\mathrm{Map}(K^n, K)$ には K 上の和と積から自然に環構造を入れる。すると各 F_n は環準同型である。よって、F_n の単射性を示すには $\mathrm{Ker}\, F_n = \{0_{K[X_1,\ldots,K_n]}\}$ を示せばよい。これを n に関する数学的帰納法で示す。

[1] $\mathrm{Ker}\, F_1 \subset \{0_{K[X_1]}\}$ を示す。そこで $f \in K[X_1]$ について $f \neq 0_{K[X_1]}$ とすると、K が体であることから f の根は有限個である。一方、問題の仮定より K は無限個の元を持つから、或る $b_1 \in K$ が存在して $f(b_1) \neq 0$ が成り立つ。よって $F_1(f) \neq 0_{\mathrm{Map}(K^1,K)}$ である。したがって $\mathrm{Ker}\, F_1 \subset \{0_{K[X_1]}\}$ である。逆の包含は明らかだから $\mathrm{Ker}\, F_1 = \{0_{K[X_1]}\}$ が成り立つ。

[2] $n-1$ のとき成立を仮定し、$\mathrm{Ker}\, F_n \subset \{0_{K[X_1,\ldots,X_n]}\}$ を示す。そこで $f \in K[X_1, \ldots, X_n]$ とする。f は

$$f = \sum_{\substack{0 \leq i_1 \leq d_1 \\ \cdots \\ 0 \leq i_n \leq d_n}} a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n} \quad (a_{i_1 \ldots i_n} \in K) \tag{4.7.137}$$

と表せる。ここで $f \neq 0_{K[X_1,\ldots,X_n]}$ とすると、或る $0 \leq \exists k_j \leq d_j$ $(j = 1, \ldots, n)$ が存在して

$$a_{k_1 \ldots k_n} \neq 0 \tag{4.7.138}$$

が成り立つ。さて、$F_n(f) \neq 0_{\mathrm{Map}(K^n,K)}$ を示したい。ここで $(K[X_1,\dots,X_{n-1}])[X_n]$ の元

$$\sum_{i_n}\left(\sum_{i_1,\dots,i_{n-1}} a_{i_1\dots i_n} X_1^{i_1}\cdots X_{n-1}^{i_{n-1}}\right) X_n^{i_n} \tag{4.7.139}$$

を考えると、$a_{k_1\dots k_n} \neq 0$ より k_n 次の係数は

$$\sum_{i_1,\dots,i_{n-1}} a_{i_1\dots i_{n-1}k_n} X_1^{i_1}\cdots X_{n-1}^{i_{n-1}} \neq 0_{K[X_1,\dots,X_{n-1}]} \tag{4.7.140}$$

をみたす。したがって帰納法の仮定より

$$F_{n-1}\left(\sum_{i_1,\dots,i_{n-1}} a_{i_1\dots i_{n-1}k_n} X_1^{i_1}\cdots X_{n-1}^{i_{n-1}}\right) \neq 0_{\mathrm{Map}(K^{n-1},K)} \tag{4.7.141}$$

である。よって、或る $(b_1,\dots,b_{n-1}) \in K^{n-1}$ が存在して

$$\sum_{i_1,\dots,i_{n-1}} a_{i_1\dots i_{n-1}k_n} b_1^{i_1}\cdots b_{n-1}^{i_{n-1}} \neq 0 \tag{4.7.142}$$

が成り立つ。そこで $K[X_n]$ の元

$$\sum_{i_n}\left(\sum_{i_1,\dots,i_{n-1}} a_{i_1\dots i_n} b_1^{i_1}\cdots b_{n-1}^{i_{n-1}}\right) X_n^{i_n} \tag{4.7.143}$$

を考えると、これは k_n 次の係数が 0 でないから $\neq 0_{K[X_n]}$ となる。よって、$n=1$ の場合と同様の議論により、或る $b_n \in K$ が存在して

$$\sum_{i_n}\left(\sum_{i_1,\dots,i_{n-1}} a_{i_1\dots i_n} b_1^{i_1}\cdots b_{n-1}^{i_{n-1}}\right) b_n^{i_n} \neq 0 \tag{4.7.144}$$

が成り立つ。よって

$$F_n(f)(b_1,\dots,b_n) = \sum_{i_1,\dots,i_n} a_{i_1\dots i_n} b_1^{i_1}\cdots b_n^{i_n} \tag{4.7.145}$$

$$= \sum_{i_n}\left(\sum_{i_1,\dots,i_{n-1}} a_{i_1\dots i_n} b_1^{i_1}\cdots b_{n-1}^{i_{n-1}}\right) b_n^{i_n} \tag{4.7.146}$$

$$\neq 0 \tag{4.7.147}$$

である。したがって

$$F_n(f) \neq 0_{\mathrm{Map}(K^n,K)} \tag{4.7.148}$$

である。これで $\mathrm{Ker}\, F_n \subset \{0_{K[X_1,\dots,X_n]}\}$ がいえた。逆の包含は明らかだから $\mathrm{Ker}\, F_n = \{0_{K[X_1,\dots,X_n]}\}$、したがって F_n は単射である。帰納法より、すべての $n \in \mathbb{Z}_{\geq 1}$ に対して F_n が単射であることが示せた。 □

♤ **演習問題 4.25** (代数学 II 2.25). K を有限個の元からなる体とする。問題 4.24 のような写像 $F\colon K[X_1,\dots,X_n] \to \mathrm{Map}(K^n,K)$ を考えると F は全射であることを示せ。

演習問題 4.25 の解答. 各 $(a_1,\dots,a_n)\in K^n$ に対し、多項式 $\delta_{a_1\dots a_n}$ を

$$\delta_{a_1\dots a_n}(X_1,\dots,X_n):=\prod_{i=1}^{n}\prod_{\substack{t\in K\\ t\neq a_i}}(a_i-t)^{-1}(X_i-t) \tag{4.7.149}$$

で定めると、K が有限個の元からなることから右辺は有限積となり $\delta_{a_1\dots a_n}$ は well-defined である。$\delta_{a_1\dots a_n}$ は $(t_1,\dots,t_n)\in K^n$ に対し

$$\delta_{a_1\dots a_n}(t_1,\dots,t_n)=\begin{cases}1 & (t_1,\dots,t_n)=(a_1,\dots,a_n)\\ 0 & \text{otherwise}\end{cases} \tag{4.7.150}$$

をみたす。そこで $f\in \mathrm{Map}(K^n,K)$ に対し多項式 $g\in K[X_1,\dots,X_n]$ を

$$g(X_1,\dots,X_n):=\sum_{(a_1,\dots,a_n)\in K^n} f(a_1,\dots,a_n)\delta_{a_1\dots a_n}(X_1,\dots,X_n) \tag{4.7.151}$$

で定めると、K、したがって K^n が有限個の元からなることから右辺は有限和となり g は well-defined である。g は $(t_1,\dots,t_n)\in K^n$ に対し

$$F(g)(t_1,\dots,t_n)=f(t_1,\dots,t_n) \tag{4.7.152}$$

をみたす。よって F は全射である。 □

♤ **演習問題 4.26** (代数学 II 2.26)**.** 加法群が巡回群になるような環を同型を除いてすべて決定せよ。

演習問題 4.26 の解答. [TODO] □

♤ **演習問題 4.27** (代数学 II 2.27)**.** 1 つの元で $\mathbb{C}$ 上生成される $\mathbb{C}$-代数で零因子を持たないものを同型を除いてすべて決定せよ。

演習問題 4.27 の解答. A を 1 つの元 $s\in A$ で $\mathbb{C}$ 上生成される $\mathbb{C}$-代数とする。このとき評価準同型 $\mathrm{ev}_s\colon \mathbb{C}[X]\to A$ は全射だから、準同型定理より $A\cong \mathbb{C}[X]/\mathrm{Ker}\,\mathrm{ev}_s$ が成り立つ。ここで $\mathbb{C}[X]$ のイデアルは $(0),(1),(X^m)$ $(m\in\mathbb{Z}_{\geq 1})$ で尽くされるから $\mathrm{Ker}\,\mathrm{ev}_s$ はこれらのいずれかに一致する。$\mathrm{Ker}\,\mathrm{ev}_s=(0)$ なら $A\cong\mathbb{C}[X]/(0)\cong\mathbb{C}[X]$ であり、これは整域だから零因子をもたない。$\mathrm{Ker}\,\mathrm{ev}_s=(1)$ なら $A\cong\mathbb{C}[X]/(1)=0$ であり、これは零因子をもたない。$\mathrm{Ker}\,\mathrm{ev}_s=(X)$ なら $A\cong\mathbb{C}[X]/(X)$ であり、(X) は素イデアルだから $\mathbb{C}[X]/(X)$ は整域で零因子をもたない。$\mathrm{Ker}\,\mathrm{ev}_s=(X^m)$ $(m\in\mathbb{Z}_{\geq 2})$ なら $A\cong\mathbb{C}[X]/(X^m)$ は $s\neq 0$, $s^m=0$ となり s が零因子となる。よって A は $(0),\mathbb{C}[X],\mathbb{C}[X]/(X)$ のいずれかであり、逆にこれらはそれぞれ $0,X,X+(X)$ により $\mathbb{C}$ 上生成される $\mathbb{C}$-代数で零因子を持たない。したがって求めるものは $(0),\mathbb{C}[X],\mathbb{C}[X]/(X)$ である。 □

♤ **演習問題 4.28** (代数学 II 2.28)**.** $\mathbb{C}[X]^\times\cong\mathbb{C}^\times$ および $(\mathbb{C}[X]/(X^{n+1}))^\times\cong\mathbb{C}^\times\times\mathbb{C}^n$ を示せ。ただし $\mathbb{C}^n$ は $\mathbb{C}$ を加法群とみたものの n 個のコピーの直積である。

演習問題 4.28 の解答. [TODO] □

♤ **演習問題 4.29** (代数学 II 2.29)**.** R を可換環、I を R の固有イデアルとする。このとき

$$\sqrt{I} \coloneqq \{a \in R \colon a^n \in I \ (\exists n \in \mathbb{Z}_{\geq 1})\} \tag{4.7.153}$$

とおくと、$\sqrt{I}$ は R の固有イデアルとなることを示せ。

演習問題 4.29 の解答. $\sqrt{I}$ が R のイデアルであるとは

(1) $\sqrt{I}$ は R の加法部分群である。
(2) $p \in R,\ q \in \sqrt{I}$ ならば $pq \in \sqrt{I}$ である。

が成り立つことであった。

まず (1) を示す。$a, b \in \sqrt{I}$ をとる。$a+b \in \sqrt{I}$ を示す。このとき

$$\exists\, m, n \geq 1 \quad \text{s.t.} \quad a^m \in I,\ b^n \in I \tag{4.7.154}$$

が成り立つ。このとき

$$(a+b)^{m+n} = \underbrace{a^{m+n}}_{\in I} + \binom{m+n}{1} \underbrace{a^{m+n-1}b}_{\in I} + \cdots + \binom{m+n}{m+n-1} \underbrace{ab^{m+n-1}}_{\in I} + \underbrace{b^{m+n}}_{\in I} \tag{4.7.155}$$

となる。よって $a+b \in \sqrt{I}$ となる。よって $\sqrt{I}$ は加法について閉じている。また、$\sqrt{I}$ は加法の単位元 0 を含む。なぜなら $0 = 0^1 \in I$ だからである。つぎに $a \in \sqrt{I}$ をとる。$-a \in \sqrt{I}$ を示す。$a \in \sqrt{I}$ より

$$\exists\, m \geq 1 \quad \text{s.t.} \quad a^m \in I \tag{4.7.156}$$

である。このとき $(-1)^m a^m \in I$ なので、R が可換であることより $(-a)^m \in I$ である。したがって $-a \in \sqrt{I}$ となる。以上より $\sqrt{I}$ は R の加法部分群である。

(2) を示す。$p \in R,\ q \in \sqrt{I}$ をとる。$pq \in \sqrt{I}$ を示す。$q \in \sqrt{I}$ より

$$\exists\, m \geq 1 \quad \text{s.t.} \quad q^m \in I \tag{4.7.157}$$

となる。これと $p^m \in R$ より $p^m q^m \in I$ となる。R が可換であることより $(pq)^m \in I$ である。よって $pq \in \sqrt{I}$ となる。 □

♤ **演習問題 4.30** (代数学 II 2.30)**.** 体 K 上の 1 変数形式的べき級数環 $K[[X]]$ のイデアルをすべて求め $K[[X]]$ が局所環かつ PID であることを示せ。

演習問題 4.30 の解答. $K[[X]]$ のイデアルが

$$(0), (X^d)\ (d \in \mathbb{Z}_{\geq 0}) \tag{4.7.158}$$

で尽くされることを示せばよく、このときイデアルの形から明らかに $K[[X]]$ は局所環かつ PID である。各 $f = \sum_{i \in \mathbb{Z}_{\geq 0}} a_i X^i \in K[[X]]$ に対し、係数が単元である次数の最小値を $\deg^-(f)$ と表すことにする。すなわち、

$$\deg^-(f) \coloneqq \min(\{i \in \mathbb{Z}_{\geq 0} \colon a_i \in K^\times\} \cup \{\infty\}) \tag{4.7.159}$$

とおく。$I \subset K[[X]]$ を $I \neq (0)$ なるイデアルとする。ここで

$$d \coloneqq \min\{\deg^-(f) \colon f \in I\} \tag{4.7.160}$$

とおくと、$I \neq (0)$ より $d \in \mathbb{Z}_{\geq 0}$ である。$I = (X^d)$ を示せばよい。ここで、d の定め方から $\deg^-(f_0) = d$ なる $f_0 \in I$ が存在し、$\deg^-$ の定義から

$$\exists g = \sum_{i \in \mathbb{Z}_{\geq 0}} a_i X^i \in K[[X]] \quad \text{s.t.} \quad a_0 \in K^\times,\ f_0(X) = g(X)X^d \tag{4.7.161}$$

が成り立つ。このとき、$a_0 \in K^\times$ より $g \in K[[X]]^\times$ である。

$\because$ $a_0 \in K^\times$ より

$$g(X) = a_0\Bigg(1 - \underbrace{\Bigg(-\sum_{i \in \mathbb{Z}_{\geq 0}} a_0^{-1} a_{i+1} X^i\Bigg)}_{=:h(X)} X\Bigg) = a_0(1 - h(X)X) \tag{4.7.162}$$

であり、

$$(1 - h(X)X) \sum_{i \in \mathbb{Z}_{\geq 0}} h(X)^i X^i = 1 \tag{4.7.163}$$

より

$$g(X)a_0^{-1} \sum_{i \in \mathbb{Z}_{\geq 0}} h(X)^i X^i = 1 \tag{4.7.164}$$

が成り立つ。よって $g \in K[[X]]^\times$ である。 //

したがって

$$X^d = g(X)^{-1} f_0(X) \in I \tag{4.7.165}$$

より $(X^d) \subset I$ である。また、d の定め方から逆向きの包含も成り立つ。したがって $I = (X^d)$ である。これが示したいことであった。 □

♤ **演習問題 4.31** (代数学 II 2.31)**.** (**中国剰余定理 (Chinese Remainder Theorem)**) R を可換環とし、$I_1, \ldots, I_n$ をその固有イデアルとする。さらに $i \neq j$ なる $1 \leq i, j \leq n$ に対し $I_i + I_j = R$ をみたすとする。このとき、

$$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n \tag{4.7.166}$$

となることを示せ。

演習問題 4.31 の解答. $(\supset)$ は明らかだから $(\subset)$ を示す。n に関する帰納法で示す。$n = 1$ のときは明らかだから、$n \geq 2$ とし、$a \in I_1 \cap \cdots \cap I_n$ とする。ここで、各 $i = 1, \ldots, n$ に対し或る $c_i \in I_i$ と $d_i \in \bigcap_{j \neq i} I_j$ が存在して

$$c_i + d_i = 1 \tag{4.7.167}$$

が成り立つ。

(∵) $R = I_i + \bigcap_{j\neq i} I_j$ を示せばよい。各 $j \neq i$ に対し、問題の仮定 $I_i + I_j = R$ より或る $a_j \in I_i$ と $b_j \in I_j$ が存在して

$$a_j + b_j = 1 \tag{4.7.168}$$

が成り立つ。このとき $\prod_{j\neq i}(a_j + b_j) = 1$ であり、左辺を展開すると $a_j \in I_i$ $(j \neq i)$ を含む項と $\prod_{j\neq i} b_j \in \bigcap_{j\neq i} I_j$ との和の形になるから、整理して

$$1 - \prod_{j\neq i} b_j \in I_i \tag{4.7.169}$$

を得る。よって

$$1 = \left(1 - \prod_{j\neq i} b_j\right) + \prod_{j\neq i} b_j \tag{4.7.170}$$

$$\in I_i + \bigcap_{j\neq i} I_j \tag{4.7.171}$$

が成り立つ。したがって $R = I_i + \bigcap_{j\neq i} I_j$ がいえた。 //

このとき

$$\prod_{i=1}^{n}(c_i + d_i) = 1 \quad \therefore \quad a\prod_{i=1}^{n}(c_i + d_i) = a \tag{4.7.172}$$

が成り立つ。左辺は

$$ad_i \in I_i \bigcap_{j\neq i} I_j \overbrace{=}^{\text{帰納法の仮定}} I_1 \cdots I_n \quad (i = 1, \ldots, n) \tag{4.7.173}$$

を含む項と

$$a\prod_{i=1}^{n} c_i \in I_1 \cdots I_n \tag{4.7.174}$$

との和の形になるから $a \in I_1 \cdots I_n$ である。よって $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ がいえた。 □

♤ **演習問題 4.32** (代数学 II 2.32). (**Frobenius 準同型**) R を可換環、p を素数とする。さらに $\iota\colon \mathbb{Z} \to R$ を一意的にきまる環準同型とし $\mathrm{Ker}(\iota) = (p)$ であると仮定する。このとき写像 $F\colon R \to R$ を $F(x) = x^p$ で定めるとこれは環準同型になることを示せ。

演習問題 4.32 の解答. 二項係数 $\binom{p}{i}$ $(1 \leq \forall i \leq p-1)$ は p で割り切れるから、$x, y \in R$ に対し

$$F(x + y) = (x + y)^p \tag{4.7.175}$$

$$= \sum_{i=0}^{p}\binom{p}{i}x^i y^{p-i} \quad (\because\ R \text{ は可換環}) \tag{4.7.176}$$

$$= x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} \tag{4.7.177}$$

$$= x^p + y^p + \sum_{i=1}^{p-1} \iota\left(\binom{p}{i}\right) x^i y^{p-i} \tag{4.7.178}$$

$$= x^p + y^p \quad (\because \operatorname{Ker}(\iota) = (p)) \tag{4.7.179}$$

$$= F(x) + F(y) \tag{4.7.180}$$

が成り立つ。また

$$F(xy) = (xy)^p \tag{4.7.181}$$

$$= x^p y^p \quad (\because R \text{ は可換環}) \tag{4.7.182}$$

$$= F(x)F(y) \tag{4.7.183}$$

と

$$F(1_R) = 1_R^p = 1_R \tag{4.7.184}$$

も成り立つ。よって F は環準同型である。 □

♤ **演習問題 4.33** (代数学 II 2.33). $\mathbb{Z}$ を加法群とみたときの群環 $\mathbb{C}[\mathbb{Z}]$ のイデアルおよび素イデアルをすべて求めよ。

演習問題 4.33 の解答. [TODO] □

♤ **演習問題 4.34** (代数学 II 2.34). p を素数とするとき $\mathbb{Z}/(p^{k+1})$ の乗法群を求めよ。

演習問題 4.34 の解答. [TODO] □

♤ **演習問題 4.35** (代数学 II 2.35). 極大両側イデアルは素イデアルになることを示せ。

演習問題 4.35 の解答. [TODO] □

♤ **演習問題 4.36** (代数学 II 2.36). 完全素イデアルは素イデアルになることを示せ。また、逆は成り立つか？

演習問題 4.36 の解答. A を環とし、$P \subset A$ を完全素イデアルとする。A の固有両側イデアル I, J が $IJ \subset P$ をみたすとし、さらに $I \not\subset P$ を仮定する。仮定より或る $i_0 \in I \setminus P$ が存在する。このとき、任意の $j \in J$ に対し $j \in P$ が成り立つ。実際、$i_0 j \in IJ \subset P$ だから P が完全素イデアルであることより $i_0 \in P$ または $j \in P$ であるが、いま $i_0 \notin P$ であったから $j \in P$ である。したがって $J \subset P$ である。よって P は素イデアルである。

逆が成り立たないことを反例によって示す。$\mathbb{R}$ 上の 2 次の全行列環 $M_2(\mathbb{R})$ と、その零イデアル (0) を考える。まず、(0) は素イデアルであることを示したい。そのために $M_2(\mathbb{R})$ の両側イデアルが自明なものしかない

ことを示しておく。$I \subset M_2(\mathbb{R})$ を $I \neq (0)$ なる両側イデアルとする。$I \neq (0)$ より或る $B_0 \in I, B_0 \neq 0$ が存在する。このとき $\operatorname{rank} B_0 > 0$ だから、或る正則行列 $Q, R \in M_2(\mathbb{R})$ が存在して

$$QB_0R = \begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix} \tag{4.7.185}$$

が成り立つ。I は両側イデアルであったから

$$\begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix} \in I \tag{4.7.186}$$

が成り立つ。さらに

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I, \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in I \tag{4.7.187}$$

も成り立つ。よって

$$1_{M_2(\mathbb{R})} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I \tag{4.7.188}$$

である。したがって $I = M_2(\mathbb{R})$ となる。よって $M_2(\mathbb{R})$ の両側イデアルは自明なものしかないことがいえた。よって、明らかに (0) は素イデアルである。ところが、(0) は完全素イデアルではない。実際、$M_2(\mathbb{R})/(0) \cong M_2(\mathbb{R})$ は零因子を持つ。 □

♤ **演習問題 4.37** (代数学 II 期末問題候補)**.** R を可換環、A を R-alg とし、$S \subset A$ とする。

$$\mathcal{S}_S := \{B \subset A : B \text{ は } R\text{-subalg かつ } S \subset B\} \tag{4.7.189}$$

とおくとき

$$R\langle S \rangle = \bigcap_{B \in \mathcal{S}_S} B \tag{4.7.190}$$

となることを示せ。

演習問題 4.37 の解答. [TODO] □

C. Problem set 3

♤ **演習問題 4.38** (代数学 II 3.37)**.** [TODO]

演習問題 4.38 の解答. [TODO] □

♤ **演習問題 4.39** (代数学 II 3.38)**.** k を正整数、X, Y を不定元として $A = \mathbb{C}[X, Y]/(X^2 - Y^{2k+1})$ とおく。$x \in A$ を標準射影による X の像としたとき、x は既約元であるが素元ではないことを示せ。

演習問題 4.39 の解答. Z を不定元とする多項式環 $\mathbb{C}[Z]$ を考える。部分集合 $\{Z^{2k+1}, Z^2\} \subset \mathbb{C}[Z]$ により $\mathbb{C}$ 上生成される $\mathbb{C}[Z]$ の部分 $\mathbb{C}$-代数 $\mathbb{C}\langle\{Z^{2k+1}, Z^2\}\rangle$ を B とおく。A は B と $\mathbb{C}$-代数として同型であることを示す。多項式環の普遍性より、$\mathbb{C}$-代数準同型 $\varphi\colon \mathbb{C}[X,Y] \to \mathbb{C}[Z]$ であって

$$X \mapsto Z^{2k+1}, \quad Y \mapsto Z^2 \tag{4.7.191}$$

をみたすものが存在する。このとき、$\operatorname{Im}\varphi = B$ である。

(∵) 両辺とも $Z^{2k+1}, Z^2 \in \mathbb{C}[Z]$ の和、積および $\mathbb{C}$ の元によるスカラー倍の有限回の組み合わせで表せる元全体の集合だから、たしかに一致する。 //

また、$\operatorname{Ker}\varphi = (X^2 - Y^{2k+1})$ である。

(∵) ($\supset$) は φ の定義より明らかだから、($\subset$) を示す。$f \in \operatorname{Ker}\varphi$ とする。f と $X^2 - Y^{2k+1}$ を ($\mathbb{C}$-代数としての) 同型 $\mathbb{C}[X,Y] \cong (\mathbb{C}[Y])[X]$ により $(\mathbb{C}[Y])[X]$ の元とみなすと、$X^2 - Y^{2k+1}$ の最高次係数 1 は $\mathbb{C}[X,Y]$ の単元だから、除法定理より或る $g(X,Y) \in (\mathbb{C}[Y])[X]$ と $r_1, r_0 \in \mathbb{C}[Y]$ が存在して

$$f(X,Y) = (X^2 - Y^{2k+1})g(X,Y) + r_1(Y)X + r_0(Y) \tag{4.7.192}$$

が成り立つ。いま $f \in \operatorname{Ker}\varphi$ ゆえに $f(Z^{2k+1}, Z^2) = 0$ だから

$$r_1(Z^2)Z^{2k+1} + r_0(Z^2) = 0 \tag{4.7.193}$$

である。左辺の第 1 項は奇数次の項しかなく、第 2 項は偶数次の項しかないから、右辺と係数を比較して $r_1 = 0, r_0 = 0$ となる。よって

$$f(X,Y) = (X^2 - Y^{2k+1})g(X,Y) \in (X^2 - Y^{2k+1}) \tag{4.7.194}$$

が成り立つから $\operatorname{Ker}\varphi \subset (X^2 - Y^{2k+1})$ である。したがって $\operatorname{Ker}\varphi = (X^2 - Y^{2k+1})$ である。 //

したがって、準同型定理より $\mathbb{C}$-代数の同型 $\overline{\varphi}\colon B \to A$ が誘導される。$\overline{\varphi}$ により $x \in A$ と対応する元は $Z^{2k+1} \in B$ だから、Z^{2k+1} が B の既約元であって素元でないことを示せばよい。まず、Z^{2k+1} は B の既約元である。

(∵) 背理法を用いる。すなわち Z^{2k+1} が B の既約元でないと仮定して矛盾を導く。まず $\deg Z^{2k+1} \neq 0$ より Z^{2k+1} は B の単元でない。よって、背理法の仮定から Z^{2k+1} は B の単元でない 2 元 f, g の積で $Z^{2k+1} = f(Z)g(Z)$ と表せる。すると $\mathbb{C}[Z]$ が整域であることとあわせて

$$\deg f \geq 1, \quad \deg g \geq 1, \quad \deg f + \deg g = 2k+1 \tag{4.7.195}$$

が成り立ち、とくに

$$1 \leq \deg f \leq 2k, \quad 1 \leq \deg g \leq 2k \tag{4.7.196}$$

が成り立つ。このことと $f, g \in B$ であることから、f, g は Z^2 の和、積および $\mathbb{C}$ の元によるスカラー倍の有限回の組み合わせで表せる。よって f, g の次数は偶数であり、$\deg f + \deg g = 2k+1$ に矛盾する。背理法より Z^{2k+1} は B の既約元である。 //

さらに、Z^{2k+1} は B の素元でない。

(∵) Z^{2k+1} により生成される B の単項イデアルを J とおく ($\mathbb{C}[Z]$ でなく B のイデアルだから、たとえば Z^{2k+2} は J には属さない)。すると

$$Z^{4k}Z^2 = (Z^{2k+1})^2 \in J, \quad Z^{4k}, Z^2 \notin J \tag{4.7.197}$$

だから J は B の素イデアルでない。よって Z^{2k+1} は B の素元でない。 //

以上より、x は A の既約元だが素元ではないことが示せた。 □

♤ **演習問題 4.40** (代数学 II 3.39)**.** PID において既約元は素元になることを示せ。

演習問題 4.40 の解答. R を PID とし、$r \in R$ が既約元であるとする。まず (r) は極大イデアルである。

(∵) (r) を含む任意の固有イデアルは、R が PID であることからある $a \in R$ を用いて (a) の形に書ける。すると $r \in (r) \subset (a)$ より $r = ab$ $(\exists b \in R)$ と書ける。いま (a) は固有イデアルゆえに a は単元でないから、r が既約元であることとあわせて b は単元となる。よって $a = rb^{-1} \in (r)$ だから $(a) \subset (r)$ である。よって $(r) = (a)$ である。したがって (r) は極大イデアルである。 //

極大イデアルは素イデアルだから (r) は素イデアルである。よって r は素元である。 □

♤ **演習問題 4.41** (代数学 II 3.40)**.** A を可換 $\mathbb{C}$-代数で $d = \dim_{\mathbb{C}} A$ としたとき $0 < d < \infty$ であるとする。このとき A は高々 d 個しか極大イデアルを持たないことを示せ。

演習問題 4.41 の解答. [TODO] 可換性いつ使う？A の相異なる $r > d$ 個の極大イデアル $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ がとれたとして矛盾を導く。CRT より

$$\begin{array}{ccc} A & \longrightarrow & A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_r = A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_r \\ \downarrow & \overset{\cong}{\nearrow} & \\ A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r) & & \end{array} \tag{4.7.198}$$

を可換にする環の同型が誘導されるから、図式の上側の射 (これは $\mathbb{C}$-代数準同型である) は全射である。よって

$$\dim_C A \geq \dim_C (A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_r) \geq r > d \tag{4.7.199}$$

となり矛盾が従う。

(∵) 各 $A/\mathfrak{m}_i$ は 0 でない $\mathbb{C}$-代数だから $\mathbb{C}$ 上の次元が 1 以上の $\mathbb{C}$-ベクトル空間である。よって

$$\dim_C (A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_r) \geq r \tag{4.7.200}$$

である。 //

よって A の極大イデアルは d 個以下である。 □

♤ **演習問題 4.42** (代数学 II 3.41). A を可換 $\mathbb{C}$-代数で $d = \dim_{\mathbb{C}} A$ としたとき $0 < d < \infty$ であるとする。A が 0 でない冪零元を持たないならば、A は d 個の複素数体の直積と同型になることを示せ。

演習問題 4.42 の解答. 問題 4.41 より A の極大イデアルは d 個以下である。そこで A の相異なる極大イデアルのすべてを

$$\mathfrak{m}_1, \dots, \mathfrak{m}_r \quad (1 \leq r \leq d) \tag{4.7.201}$$

とおく。すると CRT より

$$\begin{array}{ccc} A & \longrightarrow & A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_r = A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_r \\ \downarrow & \overset{\cong}{\nearrow} & \\ A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r) & & \end{array} \tag{4.7.202}$$

を可換にする環の同型が誘導される。ここで各 $A/\mathfrak{m}_i$ は極大イデアルによる商だから体であり、また $\mathbb{C}$ 上の次元は d 以下である。よって Dixmier の定理より $A/\mathfrak{m}_i \cong \mathbb{C}$ が成り立ち、上の図式より

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{C}^r \\ \downarrow & \overset{\cong}{\nearrow} & \\ A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r) & & \end{array} \tag{4.7.203}$$

が成り立つ。さて、A は 0 でない冪零元を持たないとする。いま A は可換アルティン環だから、[TODO] アルティンとは仮定されてない A の素イデアルは極大イデアルでもある。よって $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ は A の素イデアル全部の交わり、すなわち A の冪零根基である。いま A は 0 でない冪零元を持たないから $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = 0$ である。よって図式から $A \cong \mathbb{C}^r$ が従う。$\mathbb{C}$ 上の次元を比較して $r = d$ でなければならず、$A \cong \mathbb{C}^d$ がいえた。[TODO] 初等的に示せるか？ □

定義 4.7.2 (derivation). K を体、A を K-代数とする。K-線型写像 $D\colon A \to A$ が A 上の **derivation** であるとは、任意の $a, b \in A$ に対して

$$D(ab) = D(a)b + aD(b) \tag{4.7.204}$$

が成り立つことをいう。

♤ **演習問題 4.43** (代数学 II 3.43). 複素数体上の n 変数多項式環 $\mathbb{C}[X_1, \dots, X_n]$ 上の derivation をすべて求めよ。

演習問題 4.43 の解答. [TODO] monomial について議論すればよい □

定義 4.7.3 (G-gradation). G を加法群、K を体、A を K-代数とする。A の **G-gradation** とは、G を添字集合とする A の K-部分ベクトル空間の族による A の K-ベクトル空間としての直和分解

$$A = \bigoplus_{g \in G} A(g) \tag{4.7.205}$$

であって、任意の $x, y \in G$, $a \in A(x)$, $b \in A(y)$ に対して $ab \in A(x+y)$ をみたすものをいう。

♤ **演習問題 4.44** (代数学 II 3.44)**.** K を体、A を K-代数とする。K を加法群とみなしたときの A の K-gradation

$$A = \bigoplus_{z \in K} A(z) \tag{4.7.206}$$

が与えられていたとする。このとき K-線型写像 $D\colon A \to A$ を $z \in K$, $a \in A(z)$ に対して $D(a) = za$ となるように定める。このとき D は derivation になることを示せ。

演習問題 4.44 の解答. $a, b \in A$ とする。A は所与の K-gradation のような直和分解を持つから、或る $x, y \in K$ が存在して

$$a \in A(x), \quad b \in A(y) \tag{4.7.207}$$

が成り立つ。このとき、K-gradation の定義より $ab \in A(x+y)$ だから $D(ab) = (x+y)ab$ である。よって

$$\begin{aligned} D(a)b + aD(b) &= (xa)b + a(yb) && (4.7.208)\\ &= xab + yab && (4.7.209)\\ &= (x+y)ab && (4.7.210)\\ &= D(ab) && (4.7.211) \end{aligned}$$

が成り立つ。したがって D は A 上の derivation である。 □

♤ **演習問題 4.45** (代数学 II 3.46)**.** 単純環の中心は体になることを示せ。

注意 4.7.4. 単純環の部分環が単純であるとは限らないことに注意せよ (例 1.4.4)。

演習問題 4.45 の解答. A を単純環とし、$Z(A)$ が体であることを示す。中心の定義から $Z(A)$ が可換環であることは明らかだから、あとは $Z(A)$ の 0 でない任意の元が $Z(A)$ に逆元を持つことを示せばよい。$x \in Z(A)$, $x \neq 0$ とすると、Ax は A の左イデアルであり、(0) を真に含む。いま A は単純環ゆえに (0) は A の極大イデアルなので、$A = Ax$ である。よって、或る $x' \in A$ が存在して

$$\begin{aligned} 1 &= x'x \quad (\because A = Ax) && (4.7.212)\\ &= xx' \quad (\because x \in Z(A)) && (4.7.213) \end{aligned}$$

が成り立つ。このとき

$$x'y = x'yxx' = x'xyx' = yx' \quad (\forall y \in A) \tag{4.7.214}$$

が成り立つから $x' \in Z(A)$ である。よって、x は $Z(A)$ の可逆元である。したがって $Z(A)$ は体である。 □

♤ **演習問題 4.46** (代数学 II 3.47)**.** 有限体の元の個数はある素数の冪になることを示せ。

証明 cf. **??** □

♤ **演習問題 4.47** (代数学 II 3.49)**.** Weyl 代数 $\mathbb{C}[x:\partial]$ は $\mathbb{C}$-ベクトル空間としての基底 $\{x^i\partial^j \mid i,j \in \mathbb{Z}_{\geq 0}$ をもつことを示せ。

証明 [TODO] □

♤ **演習問題 4.48** (代数学 II 3.50)**.** Weyl 代数 $\mathbb{C}[x:\partial]$ は単純環であることを示せ。

証明 [TODO] □

D. Problem set 5

♤ **演習問題 4.49** (代数学 II 5.64)**.** R を可換環、n を正整数、$\mathfrak{m}$ を R の極大イデアルとする。このとき $R/\mathfrak{m}^n$ は局所環であることを示せ。

演習問題 4.49 の解答. イデアルの対応原理より、$\mathfrak{m}/\mathfrak{m}^n$ は $R/\mathfrak{m}^n$ の極大イデアルである。これが唯一の極大イデアルであることを示せばよい。そこで $J/\mathfrak{m}^n$ を $R/\mathfrak{m}^n$ の極大イデアルとする。すると J は R の極大イデアルであって $\mathfrak{m}^n$ を含む。ここで J は R の素イデアルでもあるから、J は $\mathfrak{m}$ を含む。よって、$\mathfrak{m}$ が R の極大イデアルであることより $J=\mathfrak{m}$ である。したがって $J/\mathfrak{m}^n = \mathfrak{m}/\mathfrak{m}^n$ である。これで唯一性がいえた。 □

♤ **演習問題 4.50** (代数学 II 5.65)**.** R を可換環、I を R の固有イデアルとする。このとき $I=\sqrt{I}$ となることは R/I の 0 でない冪零元が存在しないための必要十分条件であることを示せ。

演習問題 4.50 の解答. R/I の 0 でない冪零元 $a+I$ $(a \in R-I)$ が存在したとすると、ある $n \in \mathbb{Z}_{\geq 1}$ が存在して $a^n+I=(a+I)^n=0+I$ より $a^n \in I$、したがって $a \in \sqrt{I}$ が成り立つ。よって $I \neq \sqrt{I}$ である。逆に $I \neq \sqrt{I}$ とすると $I \subsetneq \sqrt{I}$ であるから、ある $b \in \sqrt{I}-I$ がとれる。このとき

- $b \in \sqrt{I}$ よりある $n \in \mathbb{Z}_{\geq 1}$ が存在して $(b+I)^n = b^n+I=0+I$
- $b \notin I$ より $b+I \neq 0+I$

したがって $b+I$ は R/I の 0 でない冪零元である。 □

♤ **演習問題 4.51** (代数学 II 5.66)**.** R を可換環、I を R の固有イデアルとする。このとき I が準素イデアルであることは R/I の零因子がすべて冪零元になるための必要十分条件であることを示せ。

演習問題 4.51 の解答. I を準素イデアルであるとする。$r+I \in R/I$ を零因子とすると

$$(s+I)(r+I)=0+I \quad (\exists s \in R-I) \tag{4.7.215}$$

が成り立つ。よって

$$sr \in I, \quad s \notin I \tag{4.7.216}$$

だから、I が準素イデアルであることより $r \in \sqrt{I}$ である。よって $r+I$ は R/I の冪零元である。逆に、R/I の零因子はすべて冪零元であるとする。$x, y \in R$ について、$xy \in I$ かつ $x \neq I$ であるとする。$y \in I$ の場合は $y \in I \subset \sqrt{I}$ である。$y \notin I$ の場合は

$$(x+I)(y+I) = xy + I = 0 + I \tag{4.7.217}$$

$$x + I \neq 0 + I, \quad y + I \neq 0 + I \tag{4.7.218}$$

より $y+I$ は零因子、したがって冪零元だから $y \in \sqrt{I}$ が成り立つ。よって I は準素イデアルである。 □

♤ **演習問題 4.52** (代数学 II 5.67). R を可換環、$\mathfrak{p}$ を R の素イデアル、n を正整数とする。このとき $\mathfrak{p}^n$ は準素イデアルであることを示せ。また、任意の準素イデアルはこのような形に書けるか？正しければ証明を、誤りならば反例を与えよ。

演習問題 4.52 の解答. [TODO] 問題の前半は誤植。反例がある。https://math.stackexchange.com/questions/93478/is-each-power-of-a-prime-ideal-a-primary-ideal

$\mathbb{C}[X,Y]$ のイデアル $I = (X, Y^2)$ を考える。準素イデアルの特徴付け (命題 3.1.8) を用いて I が $\mathbb{C}[X,Y]$ の準素イデアルであることを示す。ここで $\mathbb{C}[X,Y]/I \cong \mathbb{C}[Y]/(Y^2)$ である。$f+(Y^2),\ g+(Y^2) \neq 0+(Y^2),\ fg+(Y^2) = 0+(Y^2)$ とすると、f, g は Y の倍元でなければならないから $f^2+(Y^2) = 0+(Y^2),\ g^2+(Y^2) = 0+(Y^2)$ である。したがって $\mathbb{C}[X,Y]/I \cong \mathbb{C}[Y]/(Y^2)$ の零因子はすべて冪零元である。特徴付けより I は準素イデアルである。

一方、I は素イデアルの冪でないことを示す。I は準素イデアルだから、命題3.1.9 より $\sqrt{I}$ は I を含む最小の素イデアルである。ここで I が素イデアルの冪 $I = \mathfrak{p}^n$ の形に表せたとする。すると $I = \mathfrak{p}^n \subset \mathfrak{p}$ だから $\sqrt{I}$ の最小性より $\mathfrak{p}^n = I \subset \sqrt{I} \subset \mathfrak{p}$ が成り立つ。さらに $\sqrt{I}$ は素イデアルだから $\mathfrak{p}^n \subset \sqrt{I}$ より $\mathfrak{p} \subset \sqrt{I}$ が成り立つ。よって $\mathfrak{p} \subset \sqrt{I} \subset \mathfrak{p}$、したがって $\sqrt{I} = \mathfrak{p}$ が従う。$\sqrt{I}$ を具体的に求める。同型 $\mathbb{C}[X,Y]/I \cong \mathbb{C}[Y]/(Y^2)$ を再び用いる。$\mathbb{C}[Y]$ が PID ゆえに $\mathbb{C}[Y]$ の素イデアルは極大イデアルでもあることに注意すると、問題 4.49 より $\mathbb{C}[Y]/(Y^2)$ の素イデアルは $(Y)/(Y^2)$ ただひとつであるから、同型で写して $\mathbb{C}[X,Y]/I$ の素イデアルは $(X,Y)/I$ ただひとつである。したがって $\mathbb{C}[X,Y]$ の I を含む素イデアルは (X,Y) ただひとつであり、$\mathfrak{p} = \sqrt{I} = (X,Y)$ が従う。すると $\mathfrak{p}^2 = (X,Y)^2 \subsetneq I = (X,Y^2) \subsetneq (X,Y) = \mathfrak{p}$ が成り立つ (左の不等号は $X \notin (X,Y)^2$ より従い、右の不等号は $Y \notin (X,Y^2)$ より従う)。これは $I = \mathfrak{p}^n$ に矛盾。したがって I は素イデアルの冪でない。 □

E. Problem set 6

♤ **演習問題 4.53** (代数学 II 6.78). R を可換環、I を R の準素イデアルとすると $\sqrt{I}$ は I を含む最小の素イデアルであることを示せ。

演習問題 4.53 の解答. $\sqrt{I}$ が素イデアルであることを示す。$ab \in \sqrt{I},\ (a, b \in R),\ a \notin \sqrt{I}$ とし、$b \in \sqrt{I}$ を示す。$ab \in \sqrt{I}$ より、ある $n \in \mathbb{Z}_{\geq 1}$ が存在して $a^n b^n \in I$ が成り立つ。このとき $a \notin \sqrt{I}$ より $a^n \notin I$ だから、I が準素イデアルであることよりある $m \in \mathbb{Z}_{\geq 1}$ が存在して $b^{nm} \in I$ が成り立つ。したがって $b \in \sqrt{I}$ である。よって $\sqrt{I}$ は素イデアルである。[TODO] 冪零根基の特徴付けを使うべき？

$\mathfrak{p}$ を I を含む素イデアルとし、$\sqrt{I} \subset \mathfrak{p}$ を示す。$x \in \sqrt{I}$ とすると、ある $n \in \mathbb{Z}_{\geq 1}$ が存在して $x^n \in I$ が成り立つ。このとき $x^n \in I \subset \mathfrak{p}$ だから、$\mathfrak{p}$ が素イデアルであることより $x \in \mathfrak{p}$ となる。したがって $\sqrt{I} \subset \mathfrak{p}$ である。

□

F. Problem set 12

♤ **演習問題 4.54** (代数学 II 12.151)**.** $\mathbb{C}[X,Y,Z]/(XYZ-1)$ は PID でないことを示せ。

演習問題 4.54 の解答. $R \coloneqq \mathbb{C}[X,Y]$ とおき、R の部分集合 S を $S \coloneqq \{X^kY^k \mid k \in \mathbb{Z}_{\geq 0}\}$ で定めると S は R の積閉集合であり、環の同型 $\mathbb{C}[X,Y,Z]/(XYZ-1) \cong S^{-1}R$ が成り立つ。

∵ [TODO] //

そこで $S^{-1}R$ が PID でないことを示せばよい。$S^{-1}R$ のイデアル $\left(\frac{X-1}{1}, \frac{Y-1}{1}\right)$ を J とおく。J が単項イデアルでないことを示す。背理法のため、ある $f \in R$ が存在して $\left(\frac{f}{1}\right) = J$ と表せたとする。このとき $J = S^{-1}R$ である。

∵ $f/1 \in J$ よりある $g,h \in R$ および $m,n \in \mathbb{Z}_{\geq 0}$ が存在して

$$\begin{cases} \dfrac{X-1}{1} &= \dfrac{g}{X^mY^m}\dfrac{f}{1} \\ \dfrac{Y-1}{1} &= \dfrac{h}{X^nY^n}\dfrac{f}{1} \end{cases} \tag{4.7.219}$$

が成り立つ。必要ならば g,h をそれぞれ gX^nY^n, hX^mY^m に置き換えることで $m = n$ であるとしてよい。R は整域かつ $S \not\ni 0$ だから通分して

$$\begin{cases} X^mY^m(X-1) &= fg \\ X^mY^m(Y-1) &= fh \end{cases} \tag{4.7.220}$$

が成り立つ。よって $X^mY^m(X-1)h = fgh = X^mY^m(Y-1)g$ であり、X^mY^m を払って $(X-1)h = (Y-1)g$ が成り立つ。$X-1, Y-1$ は互いに素だから、[TODO] 説明不足 R が体上の多項式環ゆえに UFD であることよりある $g' \in R$ が存在して $g = g'(X-1)$ と表せる。したがって (4.7.220) の第 1 式より

$$X^mY^m(X-1) = fg'(X-1) \quad \therefore \quad X^mY^m = fg' \tag{4.7.221}$$

を得る。よって $\frac{1}{1} = \frac{g'}{X^mY^m}\frac{f}{1} \in \left(\frac{f}{1}\right) = J$ だから $J = S^{-1}R$ がいえた。 //

よって $(X-1, Y-1) \cap S \neq \varnothing$ である。

∵ $I \coloneqq (X-1, Y-1)$ とおき、標準射 $R \to S^{-1}R,\ r \mapsto r/1$ を φ とおく。明らかに $J = \left(\frac{X-1}{1}, \frac{Y-1}{1}\right) = S^{-1}\varphi(I)$ であることに注意する。いま $J = S^{-1}R$ だから $\varphi^{-1}(J) = \varphi^{-1}(S^{-1}R) = R$ である。よって $1 \in \varphi^{-1}(J) = \varphi^{-1}(S^{-1}\varphi(I))$ だから、ある $i \in I,\ s \in S$ が存在して $\frac{1}{1} = \frac{i}{s}$ と表せる。通分して $s = i$ だから $I \cap S \neq \varnothing$ がいえた。 //

よってある $m \in \mathbb{Z}_{\geq 0}$ が存在して $X^mY^m \in (X-1, Y-1)$、したがって

$$X^mY^m = u(X-1) + v(Y-1) \quad (\exists u, v \in R) \tag{4.7.222}$$

となるが、両辺に $X = 1, Y = 1$ を代入すると $1 = 0$ となり矛盾が従う。背理法より J は単項イデアルでない。したがって $S^{-1}R$、ひいては $\mathbb{C}[X, Y, Z]/(XYZ - 1)$ が PID でないことが示せた。 □