代数学概論 B 演習

黒木玄 2006 年 6 月 16 日 (月) (教師用)

目 次

3 積閉集合によって定義される分数環 37

4 二次体の整数環 43

5 素元分解整域と一意分解整域 (UFD) 46

研究課題

「研究課題」=「講義とは無関係に単位が欲しい人が解くべき問題」という意味である. 研究課題を解いた人は演習以外の時間に解いてレポートにまとめて提出して欲しい.

積閉集合によって定義される分数環に関する問題演習が足りないような気がするので以下の問題を出すことにする. 講義とは無関係に単位が欲しくない人であっても, 「"$S^{-1}R$" の例を複数挙げよ」「R が整域でない場合の "$S^{-1}R$" の例を挙げよ」のような質問にすぐに答えることができない人は以下の問題をざっと読んで結論だけは確認しておいて欲しい.

さらに二次体の整数環に関する簡単な問題と UFD に関する問題も出しておく. 「UFD の例を複数挙げよ」や「UFD ではない可換整域の例を挙げよ」のような質問にすぐに答えることができない人は後の方の問題をざっと読んで結論だけは確認しておいて欲しい.

将来, 代数系の分野を専攻しようと考えている人は単位とは無関係に以下に出したような基本的な問題を解けるようになっていることが好ましい.

3 積閉集合によって定義される分数環

定義 3.1 (積閉集合) 可換環 R の部分集合 S が**積閉 (部分) 集合 (multiplicatively closed (sub-)set)** であるとは, $1 \in S$ かつ $0 \notin S$ で S が積で閉じていることである. □

[**57**] 以下の集合 S が積閉集合であることを示せ:

1. R が可換環のとき $S = \{\, a \in R \mid a \text{ は } R \text{ の零因子ではない} \,\}$.
2. R が整域のとき $S = R \setminus \{0\}$.
3. R が可換環で P がその素イデアルのとき $S = R \setminus P$. □

定義 3.2 (分数環, 全分数環環, 商体, 素イデアルにおける局所化) R は可換環であり, S はその積閉集合であるとする. 直積集合 $R \times S$ に次のように同値関係を入れる:

$$(a, s) \sim (a', s') \iff \text{ある } t \in S \text{ で } t(s'a - sa') = 0 \text{ を満たすものが存在する.}$$

$S^{-1}R = R \times S/\!\sim$ と置き, (a, s) で代表される $S^{-1}R$ の元を $\dfrac{a}{s}$ と書く. $S^{-1}R$ の和と積を $a/s, a'/s' \in S^{-1}R$ に対して

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'}, \quad \frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}$$

と定めることができる. これによって $S^{-1}R$ は可換環をなす. $S^{-1}R$ を S によって定義された**分数環 (fractional ring)** もしくは**商環 (quotient ring)** もしくは**分数の環 (ring of fractions)** もしくは S による**局所化 (localization)** と呼ぶ. 環準同型

$$i_S : R \to S^{-1}R, \quad i_S(a) = \frac{a}{1} \quad (a \in R)$$

を**自然な環準同型**と呼ぶ. 特に S が R の非零因子全体の集合のとき $S^{-1}R$ を R の**全分数環 (total fractional ring)** もしくは**全商環 (total quotient ring)** と呼ぶ. R が整域で $S = R \setminus \{0\}$ のとき $S^{-1}R$ は体になるので $S^{-1}R$ を R の**商体 (quotient field)** と呼ぶ. R が可換環で P がその素イデアルで $S = R \setminus P$ のとき $S^{-1}R$ を R_P と書き, R の P における**局所化 (localization)** と呼ぶ. □

注意 3.3 上の定義において S が零因子を含まなければ同値関係 $\sim$ は次に等しい:

$$(a, s) \approx (a', s') \iff s'a = sa'.$$

R が整域ならば R の任意の積閉集合は零因子を含まないことに注意せよ. □

[58] (定義の確認) 以下を示せ:

1. 上の定義において $S^{-1}R$ の和と積がうまく定義されている (well-defined である).
2. 写像 i_S は実際に環準同型になっている.
3. $\operatorname{Ker} i_S = \{\, a \in R \mid \text{ある } s \in S \text{ で } sa = 0 \text{ となるものが存在する} \,\}$.
4. S が零因子を含まなければ i_S は単射なので, $a \in R$ と $a/1 \in S^{-1}R$ を同一視して, R を $S^{-1}R$ の部分環とみなせる. □

[59] (分数環の普遍性) R は可換環であり, S はその積閉集合であるとする. $f : R \to R'$ は R から可換環 R' への環準同型であり, 任意の $s \in S$ に対して $f(s)$ は R' の単元であると仮定する. このとき, ある環準同型 $\phi : S^{-1}R \to R'$ で $\phi \circ i_S = f$ をみたすものが唯一存在する. □

定義 3.4 (局所環) 可換環 R が唯一の極大イデアル $\mathfrak{m}$ しか持たないとき $(R, \mathfrak{m})$ もしくは R を**局所環 (local ring)** と呼ぶ. 局所環 $(R, \mathfrak{m})$ に対して体 $R/\mathfrak{m}$ を局所環 R の**剰余体 (residue field)** と呼ぶ. □

[60] 可換環 R が局所環ための必要十分条件は R の非単元全体の集合 $\mathfrak{m} = R \setminus U(R)$ が R のイデアルをなすことである. そのとき $\mathfrak{m}$ は R の唯一の極大イデアルになる. □

[61] (R_P は局所環) 可換環 R の素イデアル P における局所化 R_P が局所環であり, その唯一の極大イデアルは $\mathfrak{m}_P = \{\, p/s \mid p \in P,\ s \in R \setminus P \,\}$ であることを示せ. □

[62] p が素数ならば $\mathbb{Z}$ の単項イデアル (p) は素イデアル (実際には極大イデアル) になる. このとき $\mathbb{Z}$ の (p) における局所化 $\mathbb{Z}_{(p)}$ は 分母が p で割り切れない有理数全体の集合に一致している:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ p \nmid b \right\}.$$

$\mathbb{Z}_{(p)}$ の唯一の極大イデアルは

$$p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z},\ p \mid a,\ p \nmid b \right\}$$

であり, 剰余体は位数 p の有限体 $\mathbb{F}_p$ に等しい. □

[63] $\alpha \in \mathbb{C}$ に対して $\mathbb{C}[x]$ の単項イデアル $(x-\alpha)$ は素イデアル (実際には極大イデアル) になる. このとき $\mathbb{C}[x]$ の $(x-\alpha)$ における局所化 $\mathbb{C}[x]_{(x-\alpha)}$ は $x=\alpha$ に極を持たない複素有理函数全体の集合に一致している:

$$\mathbb{C}[x]_{(x-\alpha)} = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{C}[x],\ g(\alpha) \neq 0 \right\}.$$

$\mathbb{C}[x]_{(x-\alpha)}$ の唯一の極大イデアルは

$$\mathfrak{m} = (x-\alpha)\mathbb{C}[x]_{(x-\alpha)} = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in \mathbb{C}[x],\ f(\alpha) = 0,\ g(\alpha) \neq 0 \right\}$$

であり, 剰余体は $\mathbb{C}$ に同型である:

$$\mathbb{C}[x]_{(x-\alpha)}/\mathfrak{m} \xrightarrow{\sim} \mathbb{C}, \quad \frac{f(x)}{g(x)} \bmod \mathfrak{m} \mapsto \frac{f(\alpha)}{g(\alpha)}. \quad \square$$

参考 3.5 すぐ上の問題はどうして R_P を局所化と呼ぶかを理解するために参考になる. 基本的に R の元が函数とみなせるとき, 函数たちに共通する定義域を縮小する操作が局所化になっている. すぐ上の問題の場合は $\mathbb{C}[x]$ の任意の元は $\mathbb{C}$ 上の函数とみなせるが, 局所化 $\mathbb{C}[x]_{(x-\alpha)}$ の元が定義されている領域の共通部分は α の一点になってしまう. □

[64] $\alpha, \beta \in \mathbb{C}$ に対して $\mathbb{C}[x,y]$ のイデアル $(x-\alpha, y-\beta)$ は極大イデアルである. $\mathbb{C}[x,y]$ の $(x-\alpha, y-\beta)$ による局所化は x, y の複素有理函数で $(x,y)=(\alpha,\beta)$ でも値が定義されているもの全体の集合に一致している:

$$\mathbb{C}[x,y]_{(x-\alpha,y-\beta)} \left\{ \frac{f(x,y)}{g(x,y)} \,\middle|\, f(x,y), g(x,y) \in \mathbb{C}[x,y],\ g(\alpha,\beta) \neq 0 \right\}.$$

$\mathbb{C}[x,y]_{(x-\alpha,y-\beta)}$ の唯一の極大イデアルは

$$\mathfrak{m} = \left\{ \frac{f(x,y)}{g(x,y)} \,\middle|\, f(x,y), g(x,y) \in \mathbb{C}[x,y],\ f(\alpha,\beta) = 0,\ g(\alpha,\beta) \neq 0 \right\}$$

であり, 剰余体は $\mathbb{C}$ に同型である:

$$\mathbb{C}[x,y]_{(x-\alpha)}/\mathfrak{m} \xrightarrow{\sim} \mathbb{C}, \quad \frac{f(x,y)}{g(x,y)} \bmod \mathfrak{m} \mapsto \frac{f(\alpha,\beta)}{g(\alpha,\beta)}. \quad \square$$

[65] $\alpha \in \mathbb{C}$ に対して $\mathbb{C}[x,y]$ の単項イデアル $(x-\alpha)$ は $\mathbb{C}[x,y]$ の極大ではない素イデアルである. $\mathbb{C}[x,y]$ の $(x-\alpha)$ による局所化は x, y の複素有理函数体 $\mathbb{C}(x,y)$ の部分集合として具体的に次のように表わされる:

$$\mathbb{C}[x,y]_{(x-\alpha)} = \left\{ \frac{f(x,y)}{g(x,y)} \,\middle|\, f(x,y), g(x,y) \in \mathbb{C}[x,y],\ g(\alpha,y) \neq 0 \right\}.$$

$\mathbb{C}[x,y]_{(x-\alpha)}$ の唯一の極大イデアルは

$$\mathfrak{m} = \left\{ \frac{f(x,y)}{g(x,y)} \;\middle|\; f(x,y), g(x,y) \in \mathbb{C}[x,y],\ f(\alpha,y) = 0,\ g(\alpha,y) \neq 0 \right\}$$

であり, 剰余体は $\mathbb{C}(y)$ に同型である:

$$\mathbb{C}[x,y]_{(x-\alpha)}/\mathfrak{m} \xrightarrow{\sim} \mathbb{C}(x), \quad \frac{f(x,y)}{g(x,y)} \bmod \mathfrak{m} \mapsto \frac{f(\alpha,y)}{g(\alpha,y)}. \quad \square$$

参考 3.6 上の問題の $\mathbb{C}[x,y]$ の素イデアル $(x-\alpha)$ は y 軸に平行な直線 $x=\alpha$ に対応している. 直線 $x=\alpha$ 上の有理函数体は $\mathbb{C}(y)$ に同型である. この $\mathbb{C}(y)$ が剰余体になっている.

実は一般の場合も極大でない素イデアルによる局所化の剰余体も同じような感じになっている. この事実を正確に説明するためには代数幾何の初歩の話をしなければいけないのでここでは無理である. 興味のある人は図書室などで代数幾何 (algebraic geometry) の教科書を探して読んで欲しい. $\square$

[66] (整域の商体への埋め込み, 簡単) 可換環 R が整域であるための必要十分条件はある体 K で R を部分環に持つものが存在することである. $\square$

[67] (積閉集合が零元を含むことを許した場合, 簡単) 永尾の教科書 [3] やこの演習では可換環 R の積閉集合 S は $0 \notin S$ を満たすという流儀を採用している. しかし $0 \in S$ を許す流儀も存在する. もしも $0 \in S$ ならば $S^{-1}R = 0$ となってしまうことを示せ. $\square$

注意 3.7 (自明な環) 上の問題の "$S^{-1}R = 0$" の右辺の 0 は零元だけで構成された**自明な環**を意味している. (0 という記号は零元という意味と零元だけで構成された集合という二通りの意味で使われることに注意せよ.) 自明な環では $1 = 0$ が成立していると考える.

整域や体は自明な環ではないとしておかなければいけないことに注意せよ. 整域と体をそのように定義しておかないと, 剰余環が整域もしくは体になるという条件で素イデアルと極大イデアルを特徴付けできなくなってしまう. $\square$

例 3.8 (積閉集合による局所化の最も簡単な例)

1. $R = \mathbb{Z}$, $S = \{1, 2, 2^2, 2^3, \ldots\}$ のとき

$$S^{-1}R = \mathbb{Z}[1/2] = \{\text{ 分母が 2 のべきの有理数全体 }\}.$$

2. $R = \mathbb{C}[x]$, $S = \{1, x, x^2, x^3, \ldots\}$ のとき

$$S^{-1}R = \mathbb{C}[x, x^{-1}] = \{\text{ 変数 } x \text{ の複素係数 Laurent 多項式全体 }\}. \quad \square$$

[68] (積閉集合による局所化の便利な特徴付け) R は可換環であり, S は R の積閉集合であるとする. 可換環 $\widetilde{R}$ と環の準同型 $i : R \to \widetilde{R}$ は以下の条件を満たしていると仮定する:

(i) 任意の $s \in S$ に対して $i(s)$ は $\widetilde{R}$ の単元 (可逆元) である.

(ii) $\widetilde{R} = \{\, i(a)/i(s) \mid s \in S,\ a \in R \,\}$.

(iii) $\mathrm{Ker}\, i = \{\, a \in R \mid$ ある $s \in S$ で $sa = 0$ を満たすものが存在する $\}$.

以上の仮定のもとで $i : R \to \widetilde{R}$ は以下を満たしている:

1. $a, a' \in R$, $s, s' \in S$ に対して

$$\begin{aligned} & i(a)/i(s) = i(a')/i(s') \\ & \iff \text{ある } t \in S \text{ で } t(s'a - sa') = 0 \text{ を満たすものが存在する.} \end{aligned}$$

2. 写像 $\Phi : \widetilde{R} \to S^{-1}R$ を $\Phi(i(a)/i(s)) = a/s$ $(s \in S,\, a \in R)$ と定めることができる. この写像は環の同型写像であり, $\Phi \circ i = i_S$ が成立している. よって Φ を通して $\widetilde{R}$ と $S^{-1}R$ を同一視できる.

3. $f : R \to R'$ は R から可換環 R' への環準同型であり, 任意の $s \in S$ に対して $f(s)$ は R' の単元 (可逆元) であると仮定する. このときある環準同型 $\phi : \widetilde{R} \to R'$ で $\phi \circ i = f$ をみたすものが唯一存在する. (この事実を (i), (ii), (iii) の条件を用いて直接証明せよ. $S^{-1}R$ の普遍性を既知として証明してはいけない.) したがって $i : R \to \widetilde{R}$ を $i_S : R \to S^{-1}R$ で置き換えた同様の結果も成立している ($S^{-1}R$ の普遍性). □

注意 3.9 $i : R \to \widetilde{R}$ が具体的に与えられたとき, 上の問題の条件 (i), (ii), (iii) を確認することによって $\widetilde{R} \cong S^{-1}R$ (環の同型) を証明できる. □

[69] (非整域の分数環の例) $R = \mathbb{C}[x] \times \mathbb{C}[y]$ (可換環の直積) とおく.

1. R は整域ではない.

2. $S_0 = \{\, (x^n, 0) \mid n = 0, 1, 2, \dots \}$ ならば $S_0^{-1}R \cong \mathbb{C}[x, x^{-1}]$.

3. $S_1 = \{\, (x^n, 1) \mid n = 0, 1, 2, \dots \}$ ならば $S_1^{-1}R \cong \mathbb{C}[x, x^{-1}] \times \mathbb{C}[y]$. □

ヒント. 1. 容易.
2. $i_0 : R \to \mathbb{C}[x, x^{-1}]$ を $i_0(f(x), g(y)) = f(x)$ $((f(x), g(y)) \in R)$ と定め, これが **[68]** の条件を満たしていることを示せ.
3. $i_1 : R \to \mathbb{C}[x, x^{-1}] \times \mathbb{C}[y]$ を $i_1(f(x), g(y)) = (f(x), g(y))$ $((f(x), g(y)) \in R)$ と定め, これが **[68]** の条件を満たしていることを示せ. □

[70] R は可換環であり, S はその積閉集合であるとする. $i : R \to S^{-1}R$ は R から分数環への自然な環準同型であるとする. $\overline{R} = R/\mathrm{Ker}\, i_S$ と置き, S の $\overline{R}$ での像を $\overline{S}$ と書くことにする. このとき $\overline{S}$ は $\overline{R}$ の積閉集合である. $\overline{i} : \overline{R} \to \overline{S}^{-1}\overline{R}$ は $\overline{R}$ から分数環への自然な環準同型であるとする. 写像 $\Phi : \overline{S}^{-1}\overline{R} \to S^{-1}R$ を $\Phi(\overline{a}/\overline{s}) = a/s$ ($a \in R$, $s \in S$, $^-$ は R から $\overline{R}$ への自然な射影) と定めることができ, Φ は環の同型写像であり, $\Phi \circ \overline{i} = i$ を満たしている. □

ヒント. 問題 **[68]** の結果を使う. 問題 **[70]** の 2 のヒントの議論の一般化. □

注意 3.10 一般に集合の集合 $\mathcal{A}$, $\mathcal{B}$ のあいだの写像 $f : \mathcal{A} \to \mathcal{B}$, $g : \mathcal{B} \to \mathcal{A}$ が $I \in \mathcal{A}$, $J \in \mathcal{B}$ に対して $g(f(I)) \supset I$, $f(g(J)) \subset J$ を満たしているならば $f(g(f(I))) = f(I)$, $g(f(g(J))) = g(J)$ が成立する. よって $f(I)$ 全体の集合と $g(J)$ 全体の集合は f, g によって一対一に対応する.

[71] (環準同型によるイデアルの対応, 簡単だが基本的) A, B は可換環であり, $\phi : A \to B$ は環準同型であるとする. A, B のイデアル全体の集合 $\mathrm{Ideal}(A)$, $\mathrm{Ideal}(B)$ のあいだには自然に次の二つの写像を構成できる:

$$\mathrm{Ideal}(B) \to \mathrm{Ideal}(A), \quad J \mapsto \phi^{-1}(J),$$
$$\mathrm{Ideal}(A) \to \mathrm{Ideal}(B), \quad I \mapsto B\phi(I) = (\phi(I) \text{ で生成される } B \text{ のイデアル}).$$

これらの写像は次の二つの部分集合のあいだの一対一対応を定める:

(a) $\{\, \phi^{-1}(J) \mid J \text{ は } B \text{ のイデアル} \,\} \subset \mathrm{Ideal}(A)$,

(b) $\{\, B\phi(I) \mid I \text{ は } A \text{ のイデアル} \,\} \subset \mathrm{Ideal}(B)$. □

ヒント. I を A のイデアル, J を B のイデアルとする. (1) $\phi^{-1}(B\phi(I)) \supset I$, (2) $B\phi(\phi^{-1}J) \subset J$ は容易に示される. (1) より $B\phi(\phi^{-1}(B\phi(I))) \supset B\phi(I)$ であり, (2) より逆の包含関係が成立するので, 等号が成立する. 同様に (2) より $\phi^{-1}(B\phi(\phi^{-1}J)) \subset \phi^{-1}(J)$ であり, (1) より逆の包含関係が成立するので, 等号が成立する. □

注意 3.11 上の問題において ϕ が全射ならば

(a') $\{\, \phi^{-1}(J) \mid J \text{ は } B \text{ のイデアル} \,\} = \{\, I \in \mathrm{Ideal}(A) \mid \mathrm{Ker}\,\phi \subset I \,\}$,

(b') $\{\, B\phi(I) \mid I \text{ は } A \text{ のイデアル} \,\} = \mathrm{Ideal}(B)$.

よって上の問題の結果は全射環準同型によるイデアルの対応の一般化になっている.

後で可換環 R の分数環のイデアル全体の集合を R のイデアルの集合の一対一対応を構成するとき ([**72**]) に上の問題の結果が使われる. □

[72] (分数環のイデアル, 20 点) R は可換環であり, S はその積閉集合 (で 0 を含まないもの) であり, $i : R \to S^{-1}R$ は R から分数環への自然な環準同型であるとする. このとき以下が成立する:

1. R のイデアル I に対して I_S を

$$I_S = \{\, a \in R \mid \text{ある } s \in S \text{ で } sa \in I \text{ を満たすものが存在する} \,\}.$$

と定めると I_S も R のイデアルであり, $(I_S)_S = I_S$.

2. R の素イデアル P に対して $P_S = P$ と $P \cap S = \emptyset$ は同値である.

3. I が R のイデアルならば, $i(I)$ から生成される $S^{-1}R$ のイデアルは

$$S^{-1}I := S^{-1}R\, i(I) = \{\, a/s \mid a \in I,\ s \in S \,\}.$$

と表わされる.

4. R のイデアル I に対して $i^{-1}(S^{-1}I) = I_S$.

5. $S^{-1}R$ のイデアル J に対して $S^{-1}\phi^{-1}(J) = J$.

6. R が PID (単項イデアル整域) ならば $S^{-1}R$ もそうである.

7. $S^{-1}R$ のイデアル J 全体の集合と R のイデアル I で $I_S = I$ を満たすもの全体の集合は対応 $J \mapsto i^{-1}(J)$ とその逆対応 $I \mapsto S^{-1}I$ によって一対一に対応する.

8. この対応によって $S^{-1}R$ の素イデアル全体の集合と R の素イデアル P で S と交わりを持たないもの全体の集合は一対一に対応している. □

ヒント. たとえばリード [7] pp.98–99, 第 6.3 節や松村 [6] pp.26–27 を見よ.

1, 2, 3. 容易.

4. I を R のイデアルとする. $a \in I_S$ すなわちある $t \in S$ が存在して $ta \in I$ とすると $i(a) = a/1 = (ta)/t \in S^{-1}I$ なので $a \in i^{-1}(S^{-1}I)$. 逆に $a \in i^{-1}(S^{-1}I)$ すなわち $i(a) \in S^{-1}I$ とすると 3 より $i(a)$ は $i(a) = b/s$, $b \in I$, $s \in S$ と表わされる. そのとき $i(sa) = i(s)i(a) = i(b)$ なのである $s' \in S$ で $s'sa = b \in I$ を満たすものが存在する. よって $a \in I_S$.

5. J を $S^{-1}R$ のイデアルとする. $S^{-1}i^{-1}(J) \subset J$ は容易. 逆に $b = a/s \in J$, $a \in R$, $s \in S$ とすると $i(a) = i(s)b \in J$ すなわち $a \in i^{-1}(J)$ なので $b = i(s)^{-1}i(a) \in S^{-1}Ri(i^{-1}(J)) = S^{-1}i^{-1}(J)$. これで逆の包含関係が示され, $S^{-1}i^{-1}(J) = J$ が成立することがわかった.

6. 5 からただちに導かれる.

7. 問題 **[71]** の結果に 4, 5 を適用せよ.

8. 2 と 7 からただちに導かれる. □

[73] (20 点) 体 K 上の n 変数形式べき級数環 $K[[x_1, \ldots, x_n]]$ は局所環である. □

ヒント. $\mathfrak{m} = (x_1, \ldots, x_n) = \{ f \in K[[x_1, \ldots, x_n]] \mid f(0, \ldots, 0) = 0 \}$ が唯一の極大イデアルになる. □

4 二次体の整数環

[74] $m \in \mathbb{Z}$ かつ $\sqrt{m}$ は有理数ではないと仮定する. 一般に $\mathbb{Z}$ と $\alpha \in \mathbb{C}$ を含む $\mathbb{C}$ の最小の部分環を $\mathbb{Z}[\alpha]$ と書く. 以下を証明せよ.

1. $\mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \mathbb{Z}\sqrt{m}$,

2. $\mathbb{Z}[x]/(x^2 - m) \cong \mathbb{Z}[\sqrt{m}]$.

ヒント. 1. $\mathbb{Z}$ と $\sqrt{m}$ を含む $\mathbb{C}$ の任意の部分環が $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ を含むことは容易に確かめられる. $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ は $\mathbb{C}$ の部分環であることも容易に確かめられる.

2. 環準同型 $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{m}]$ を $\phi(f(x)) = f(\sqrt{m})$ $(f \in \mathbb{Z}[x])$ と定めることができる. ϕ は全射であることが簡単にわかる. よって環の準同型定理より $\mathbb{Z}[x]/\mathrm{Ker}\,\phi \cong \mathbb{Z}[\sqrt{m}]$ である. したがって $\mathrm{Ker}\,\phi = (x^2 - m)$ を示せばよい. $\phi(x^2 - m) = \sqrt{m}^2 - m = 0$ より $x^2 - m \in \mathrm{Ker}\,\phi$ であるから $(x^2 - m) \subset \mathrm{Ker}\,\phi$ である. 任意に $f(x) \in \mathrm{Ker}\,\phi$ を取る. $x^2 - m$ による割り算によって $f(x)$ を $f(x) = g(x)(x^2 - m) + ax + b$ $(g(x) \in \mathbb{Z}[x], a, b \in \mathbb{Z})$ と表わせる. その等式の両辺に $x = \sqrt{m}$ を代入すると $a\sqrt{m} + b = 0$ が得られる. $\sqrt{m}$ は有理数ではないと仮定したので $a = b = 0$ である. したがって $f(x) = g(x)(x^2 - m) \in (x^2 - m)$ である. これで示すべきことが示された. □

定義 4.1 (素元) 可換環 R の 0 でない元 p が**素元 (prime element)** であるとは, 単項イデアル $(p) = Rp$ が素イデアルになることである. □

定義 4.2 (既約元) 可換環 R の元 p が**既約元 (irreducible element)** であるとは, p が単元ではなく, $a, b \in R$, $p = ab$ ならば a または b が単元になることである. たとえば 0, 1 は既約元ではない. □

注意 4.3 上の意味での既約元のことを素元と呼んでいる本もあるので注意せよ. 例えば永尾 [3] はそういう流儀を採用している. しかし素元と素イデアルを対応させたければ上の意味での素元を既約元と呼ぶ流儀を採用した方が良い. □

[75] (任意の整域において素元は既約元, 簡単) 任意の整域において素元は既約元である. □

ヒント. R は整域であるとし, p はその素元であるとする. 素元の定義より単項イデアル (p) は 0 でない素イデアルである. $a, b \in R$, $p = ab$ と仮定する. このとき $ab \in (p)$ なので $a \in (p)$ または $b \in (p)$ である. $b \in (p)$ と仮定してよい. そのとき b は $b = a'p$, $a' \in R$ と表わされる. よって $p = ab = aa'p$ である. R は整域なので $1 = aa'$ となるので a は R の単元である. □

注意 4.4 上の問題の逆は PID や UFD では成立するが, 一般の整域では成立しない. □

参考 4.5 (二次体の整数環) 上の問題の $\mathbb{Z}[\sqrt{m}]$ の商体 $\mathbb{Q}(\sqrt{m})$ は**二次体 (quadratic field)** と呼ばれている. 二次体 K は平方因子を含まない 0 でも 1 でも有理整数 m によって $K = \mathbb{Q}(\sqrt{m})$ と一意に表わされる. $m > 0$ のとき $\mathbb{Q}(\sqrt{m})$ は**実二次体 (real quadratic field)** と呼ばれ, $m < 0$ のとき $\mathbb{Q}(\sqrt{m})$ は**虚二次体 (imaginary quadratic field)** と呼ばれている.

$\alpha \in \mathbb{C}$ が**代数的整数 (algebraic integer)** であるとはあるモニックな $f \in \mathbb{Z}[x]$ で $f(\alpha) = 0$ を満たすものが存在することである.

$\omega \in \mathbb{Q}(\sqrt{m})$ を次のように定める:

$$\omega = \begin{cases} \sqrt{m} & (m \equiv 2, 3 \bmod 4) \\ (1 + \sqrt{m})/2 & (m \equiv 1 \bmod 4). \end{cases}$$

このとき $\mathbb{Z}[\omega] = \mathbb{Z} + \mathbb{Z}\omega$ であり, $\mathbb{Z}[\omega]$ は非常に良い性質を持っていることが知られている:

1. $\mathbb{Q}(\sqrt{m})$ に含まれる代数的整数の全体は $\mathbb{Z}[\omega]$ に一致する. ($\mathbb{Z}[\omega]$ は二次体の整数環と呼ばれる.)

2. $\mathbb{Z}[\omega]$ は Dedekind 整域である. 特に $\mathbb{Z}[\omega]$ では任意の 0 でないイデアルが素イデアルの積に一意的に分解される (素イデアル分解の一意存在).

詳しくは代数的整数論の教科書を見よ. たとえば, 1 の結果の証明は [2] p.119 問 3 の解答 (pp.146-147) に書いてあり, Dedekind 整域の一般論は [5] 第 5 章にある.

さらに以下が成立していることに注意しなければいけない:

- $m \equiv 1 \bmod 4$ のとき $\mathbb{Z}[\sqrt{m}]$ では「素イデアル分解の一意存在」が成立していない.

- $\mathbb{Z}[\omega]$ で「既約元の積への分解の一意存在」(後で整域において「素元分解の存在」と同値であることを示す) が成立しているとは限らない.

たとえば $m=-1.-2.-3,2$ のとき $\mathbb{Z}[\omega]$ で「既約元の積への分解の一意存在」が成立しているが, $m=-5,-26,10$ のとき $\mathbb{Z}[\omega]=\mathbb{Z}[\sqrt{m}]$ ではそうではない.

有理整数環 $\mathbb{Z}$ の整数論では「素因数分解の一意存在」が基本的であった. しかし二次体の整数環ではそれに対応する「既約元の積への分解の一意存在」が成立しないことがある. しかし「数」のレベルではなく「イデアル」のレベルでは素なモノへの分解の一意存在が成立しているのである.

これがイデアル＝理想数のアイデアの出発点である. イデアルの概念は「イデアル＝理想数」という出発点の発想をはるかに超えた有用性を持っていることがわかっている.

以上のような込み入った事情の説明を読めば, 代数学の講義や演習でイデアルが歴史的に導入された動機の説明をすることが難しいことがわかると思う. 可換環 R のイデアルとは R 自身の部分 R 加群のことであるという簡単な定義があることは非常にありがたいことである. □

[76] $\mathbb{Z}[\sqrt{-26}]$ における数の計算に関して以下が成立していることを示せ:

1. $U(\mathbb{Z}[\sqrt{-26}])=\{\pm 1\}$ である.
2. $3,1\pm\sqrt{-26}$ は $\mathbb{Z}[\sqrt{-26}]$ の既約元である.
3. しかし $27=3^3=(1+\sqrt{-26})(1-\sqrt{-26})$ が成立している. $\mathbb{Z}[\sqrt{-26}]$ では 27 の既約元の積への分解の一意性が成立していない. □

ヒント. $N:\mathbb{Z}[\sqrt{-26}]\to\mathbb{Z}$ を $N(m+n\sqrt{-26})=(m+n\sqrt{-26})(m-n\sqrt{-26})=m^2+26n^2$ と定める. このとき $N(ab)=N(a)N(b)$ が成立する.

1. $a=k+l\sqrt{-26}, b=m+n\sqrt{-26}\in\mathbb{Z}[\sqrt{-26}]$, $1=ab$ のとき $1=N(a)N(b)=(k^2+26l^2)(m^2+26n^2)$ である. これより $k=\pm 1$, $l=0$ であることがわかる.
2. 3 が $\mathbb{Z}[\sqrt{-26}]$ の既約元であるとは $a,b\in\mathbb{Z}[\sqrt{-26}]$, $3=ab$ ならば a または b が $\mathbb{Z}[\sqrt{-26}]$ の単元になることである. $a=k+l\sqrt{-26}, b=m+n\sqrt{-26}\in\mathbb{Z}[\sqrt{-26}]$. $3=ab$ のとき $9=N(a)N(b)=(k^2+26l^2)(m^2+26n^2)$ である. よってもしも a も b も単元でないとすれば $k^2+26l^2=3$ でなければいけない. しかしこれは不可能である. したがって 3 は既約元である. $1\pm\sqrt{-26}$ も同様の議論で既約元であることを示せる.
3. 容易. □

[77] (20 点以上) $\mathbb{Z}[\sqrt{-26}]$ におけるイデアルの計算に関して以下が成立していることを示せ:

1. $\mathbb{Z}[\sqrt{-26}]$ のイデアル $I=(3,1+\sqrt{-26})$, $J=(3,1-\sqrt{-26})$ は $\mathbb{Z}[\sqrt{-26}]$ の素イデアルである.
2. $(3)=IJ$, $(1+\sqrt{-26})=I^3$, $(1-\sqrt{-26})=J^3$.
3. イデアル (27) の 2 通りの素イデアル分解 $(27)=(3^3)=(3)^3=(IJ)^3=I^3J^3$, $(27)=((1+\sqrt{-26})(1+\sqrt{-26}))=(1+\sqrt{-26})(1+\sqrt{-26})=I^3.J^3$ の結果は一致している. (注意: 一般論によってこの一致は当然.) □

参考 4.6 数学的に深くて応用的にも有用な結果を出すためには扱う数学的対象に何らかの有限性の条件を課しておいた方が良い. 可換環に関する体 K 上有限生成や $\mathbb{Z}$ 上有限生成という条件はその意味で非常に良い条件である. □

参考 4.7 以上においては主として可換環のイデアルのイメージについて説明した. 非可換環のイデアルのイメージは可換環の場合とは異なる場合がある. □

5 素元分解整域と一意分解整域 (UFD)

定義 5.1 (素元) 可換環 R の 0 でない元 p が**素元 (prime element)** であるとは, 単項イデアル $(p) = Rp$ が素イデアルになることである. たとえば単元は素元ではない. □

[78] (素元の定義の確認, 簡単) 可換環 R の 0 でない元 p について次の二つの条件は互いに同値である:

(a) p は R の素元である.

(b) $a, b \in R$, $p \mid ab$ ならば $p \mid a$ または $p \mid b$.

定義 5.2 (既約元) 可換環 R の元 p が**既約元 (irreducible element)** であるとは, p が単元ではなく, $a, b \in R$, $p = ab$ ならば a または b が単元になることである. たとえば 0, 1 は既約元ではない. □

[79] (単項イデアルの言葉による既約元の特徴づけ, 簡単) R は整域であるとし, $0 \neq p \in R$ であるとする. このとき p が R の既約元であるための必要十分条件は R と一致しない R の単項イデアル全体の集合の中で (p) が包含関係に関する極大元になっていることである. □

定義 5.3 (素元分解整域) 整域 R が**素元分解整域 (factorial domain)** であるとは R の 0 でない任意の元が R の素元の積で表わされることである. (単元は 0 個の素元の積であるとみなす.) つまり「素元分解の存在」で素元分解整域を定義する. □

定義 5.4 (一意分解整域) 整域 R が**一意分解整域 (UFD, unique factorization domain)** であるとは R の 0 でない任意の元が R の既約元の積で表わされ, しかもその表示の仕方が積の順序と単元倍を除いて一意的であることである. (単元は 0 の既約元の積であるとみなす.) つまり「既約元の積への分解の一意存在」で一意分解整域を定義する. □

注意 5.5 (用語法に関する注意) 既約元のことを素元と呼ぶ流儀もあることを再度注意しておく. 上の定義の意味での素元分解整域をも一意分解整域 (UFD) と呼ぶ流儀もある. しかし結果的に上の意味での素元分解整域と一意分解整域は同じものになり, 素元分解整域=一意分解整域において素元と既約元は同じものになるので論理的には問題が生じない.

上の意味での一意分解整域の定義は永尾の教科書 [3] の定義と一致している. □

定義 5.6 (同値関係 $\approx$, 素元の完全代表系) R は整域であるとし, K はその商体であるとする.

K における同値関係 $\approx$ を次のように定める:

$$a \approx b \iff R \text{ の単元 } u \text{ で } ua = b \text{ を満たすものが存在する.}$$

すなわち K の元 a, b が R の単元倍の違いしかないとき $a \approx b$ と書く.

R の素元全体の集合の同値関係 $a \approx b$ に関する商集合の完全代表系を R の**素元の完全代表系**と呼ぶ. すなわち R の素元の集合 $\mathcal{P}$ が素元の完全代表系であるとは R の任意の素元 p に対してある $p' \in \mathcal{P}$ で $p \approx p'$ を満たすものが一意に存在することである. □

[80] ($\approx$ の特徴付け, 簡単) R は整域であるとし, K はその商体であるとする. $a, b \in K$ に対して $a \approx b$ と $Ra = Rb$ は同値である. □

参考 5.7 R は整域であるとし, K はその商体であるとする.

$a \in K$ に対する $Ra \subset K$ をも (a) と書き, R の**単項 (分数) イデアル (principal (fractional) ideal)** と呼ぶことがある. 特に代数体の整数環ではそのように呼ぶ. 一般に K の R 部分加群 I で $sI \subset R$ を満たす $s \in R \setminus \{0\}$ を持つものを R の**分数イデアル (fractional ideal)** と呼ぶ. このとき R のイデアルは**整イデアル (integranl ideal)** と呼ばれる.

二つの分数イデアル I, J の積 IJ が整イデアルの積と同様に定義され, 結合律を満たし, 可換である. さらに $R = (1)$ はその積に関する単位元になり, $a, b \in K$ に対して $(a)(b) = (ab)$ が成立し, $a \neq 0$ ならば $(a)(a^{-1}) = (1)$ であることがわかる. よって 0 でない単項 (分数) イデアル全体の集合は自然に Abel 群をなす.

可逆な分数イデアル全体の集合も Abel 群をなす. 可逆な分数イデアル全体のなす群を単項 (分数) イデアル全体のなす群で割ってできる剰余群は**イデアル類群 (ideal class group)** と呼ばれている.

このような構成は数論的にも代数幾何的に重要な意味を持っている. □

[81] (R における $\approx$, 超簡単) R が整域で $a, b \in R$ であるとき, $a \approx b$ が成立することと $a \mid b$ かつ $b \mid a$ が成立することは同値である. □

[82] (素元分解の約数, 簡単) R は整域であるとし, $p_1, \ldots, p_n$ はその素元であるとする. このとき $a \in R$ が $a \mid p_1 \cdots p_n$ を満たしているならばある $1 \leqq i_1 < \cdots < i_r \leqq n$ で $a \approx p_{i_1} \cdots p_{i_r}$ を満たすものが存在する. □

ヒント. n に関する帰納法. $n = 1$ の場合は明らか. $n - 1$ まで成立していると仮定する (帰納法の仮定). $a \mid p_1 \cdots p_n$ ならばある $b \in R$ で $ab = p_1 \cdots p_n$ を満たすものが存在する. p_n は素元なので $p_n \mid ab$ より $p_n \mid a$ または $p_n \mid b$. $p_n \mid a$ のとき $a' \in R$, $a = p_n a'$, $b' = b$ とし, $p_n \mid b$ のとき $a' = a$, $b' \in R$, $b = p_n b'$ とする. このとき R は整域なので $a'b' = p_1 \cdots p_{n-1}$. 帰納法の仮定より a' は $a' = p_{i_1} \cdots p_{i_s}$, $1 \leqq i_1 < \cdots < i_s \leqq n - 1$ と表わされる. これより n の場合も成立することがわかる. □

次の問題は **[75]** の再掲である.

[83] (任意の整域において素元は既約元, 簡単) 任意の整域において素元は既約元である. □

ヒント. R は整域であるとし, p はその素元であるとする. 素元の定義より単項イデアル (p) は 0 でない素イデアルである. $a, b \in R$, $p = ab$ と仮定する. このとき $ab \in (p)$ なので $a \in (p)$ または $b \in (p)$ である. $b \in (p)$ と仮定してよい. そのとき b は $b = a'p$, $a' \in R$ と表わされる. よって $p = ab = aa'p$ である. R は整域なので $1 = aa'$ となるので a は R の単元である. □

注意 5.8 UFD においては上の問題の逆が成立しているが ([**84**], [**85**]), 一般には成立していない ([**95**], [**96**]). □

[**84**] **(簡単)** 素元分解整域において既約元は素元になる. (任意の整域で素元は既約元になる ([**75**]) ので, 素元分解整域において素元と既約元は一致する.) □

ヒント. 既約元 p の素元分解を $p = p_1 \cdots p_r$ とする. もしも $r > 1$ ならば $p_2 \cdots p_r$ が単元になり矛盾する. □

[**85**] 一意分解整域において既約元は素元になる. (任意の整域で素元は既約元になる ([**75**]) ので, 一意分解整域において素元と既約元は一致する.) □

ヒント. p は R の既約元であるとし, $(p) = Rp$ が素イデアルになることを示せばよい. $a, b \in R$, $a, b \neq 0$, $ab \in (p)$ であるとする. R は一意分解整域なので a, b は $a \approx p_1 \cdots p_r$, $b \approx q_1 \cdots q_s$ (u, v は R の既約元, p_i, q_j は R の素元) の形に積の順序と単元倍の違いを除いて一意に分解される. $ab \in (p)$ より $p \mid p_1 \cdots p_r q_1 \cdots q_s$. 既約元の積への分解の一意性より p は p_i, q_j のどれかと単元倍の違いを除いて等しい. 必要があれば a, b の立場を交換し, 積の順序を並び換えることによって $p \approx p_1$ であるとしてよい. そのとき $a \in (p)$ である. これで (p) が素イデアルになることがわかった. □

[**86**] **(整域における素元分解の一意性)** 整域 R において 0 でない元の素元分解は積の順序と単元倍を除いて一意的である. すなわち

$$p_1 \cdots p_r \approx q_1 \cdots q_s, \quad p_i, q_j \text{ は } R \text{ の素元}$$

とすると $r = s$ でかつ適当に番号を付け変えれば $p_i \approx q_i$ $(i = 1, \ldots, r)$ となる. □

ヒント. $r \leqq s$ と仮定してよい. r に関する数学的帰納法. $r = 0$ のときすなわち $q_1 \cdots q_s$ が単元のとき $s = 0$ とならなければいけないことはすぐにわかる (なぜか?). $r > 0$ のとき (p_1) は素イデアルなのである i について $q_i \in (p_1)$ となる (なぜか?). 番号を付け変えて $i = 1$ と仮定し, $q_1 \in (p_1)$ であるとしてよい. 素元 q_1 は既約元 ([**75**]) なので $p_1 \approx q_1$ であることがわかる (なぜか?). したがって R のある単元 u', v' が存在して $p_2 \cdots p_r \approx q_2 \cdots q_s$. 帰納法の仮定より $r = s$ で $p_i \approx q_i$ $(i = 2, \ldots, r)$. □

[**87**] 可換環 R が素元分解整域であることと一意分解整域であることは同値である. □

ヒント. 以上の問題の結果をまとめれば容易に証明される.

R は素元分解整域であるとする. 問題 [**83**], [**84**] の結果より R において素元と既約元は一致している. よって, 素元分解の存在は既約元の積への分解の存在を意味し, 素元分解の一意性 ([**86**]) は既約元の積への分解の一意性を意味している. よって R は一意分解整域である.

R は一意分解整域であるとする. 問題 [**85**] の結果より R において既約元は素元である. よって既約元の積への分解の存在から素元分解の存在が導かれる. よって R は素元分解整域である. □

問題 [87] の結果より素元分解整域と一意分解整域 (UFD) は同じものである．これ以後, 素元分解整域と一意分解整域を明確に区別せずに総称して UFD と呼ぶことにする．

[88] **(簡単)** R は UFD であるとする．$a_1, \ldots, a_n \in R$ の最大公約元と最小公倍元の定義を説明し, それらが互いに素であることの定義を述べよ．□

[89] **(体は UFD, 超簡単)** 体は UFD である．□

[90] **(PID ならば UFD)** PID は UFD である．したがって $\mathbb{Z}$ や体 K 上の一変数多項式環 $K[x]$ は UFD である．□

ヒント． 教科書を見よ．たとえば永尾 [3] p.103 や堀田 [4] pp.47-48．□

[91] **(UFD の分数環も UFD)** R が UFD であり, K はその商環であるとし, $\mathcal{P}$ は R の素元の完全代表系であるとする．集合 X に対して $\mathbb{Z}^{\oplus X}$, $\mathbb{Z}_{\geqq 0}^{\oplus X}$ を次のように定める:

$$\mathbb{Z}^{\oplus X} = \{\, (e_p)_{p\in X} \mid e_p \in \mathbb{Z},\ \text{有限個を除いて } e_p = 0 \,\},$$
$$\mathbb{Z}_{\geqq 0}^{\oplus X} = \{\, (e_p)_{p\in X} \mid e_p \in \mathbb{Z}_{\geqq 0},\ \text{有限個を除いて } e_p = 0 \,\}.$$

このとき以下が成立する:

1. K の 0 でない元 a は
$$a = u \prod_{p\in\mathcal{P}} p^{e_p}, \quad (e_p)_{p\in\mathcal{P}} \in \mathbb{Z}^{\oplus\mathcal{P}}, \quad u \in U(R)$$
と一意に表わされる (K における素元分解の一意存在)．有限個を除いて $e_p = 0$ なので右辺の積は有限積になることに注意せよ．

2. 次の二つの集合は互いに等しい:
   (a) $\mathcal{P}$ の部分集合 $\mathcal{F}$ から生成された積閉集合 (すなわち $\mathcal{F}$ を含む最小の積閉集合) S による R の局所化 $S^{-1}R$ 全体の集合,
   (b) R の積閉集合 S (0 を含まないもの) による局所化 $S^{-1}R$ 全体の集合．

3. $\mathcal{P}$ の部分集合 $\mathcal{F}$ から生成される積閉集合を S と書き, $\mathcal{F}$ の $\mathcal{P}$ における補集合を $\mathcal{F}^c$ と書くことにする．このとき $S^{-1}R$ の単元 v は
$$v = u \prod_{p\in\mathcal{F}} p^{e_p}, \quad (e_p)_{p\in\mathcal{F}} \in \mathbb{Z}^{\oplus\mathcal{F}}, \quad u \in U(R)$$
と一意に表わされ, $S^{-1}R$ の 0 でない元 a は
$$a = v \prod_{p\in\mathcal{F}^c} p^{e_p}, \quad (e_p)_{p\in\mathcal{F}^c} \in \mathbb{Z}_{\geqq 0}^{\oplus\mathcal{F}^c}, \quad v \in U(S^{-1}R)$$
と一意に表わされる．

4. このことから $S^{-1}R$ は UFD であり, $S^{-1}R$ の素元の完全代表系として $\mathcal{F}$ の $\mathcal{P}$ における補集合 $\mathcal{F}^c$ が取れることがわかる．□

[92] R は UFD であるとし, p はその素元であるとする. R の (p) における局所化 $R_{(p)}$ も UFD であり, その素元の完全代表系として $\{p\}$ が取れ, $pR_{(p)}$ は局所環 $R_{(p)}$ の唯一の極大イデアルである. □

ヒント. p を含む R の素元の完全代表系を $\mathcal{P}$ とし, S は $\mathcal{P} \setminus \{p\}$ から生成される積閉集合であるとすると $R_{(p)} = S^{-1}R$. □

[93] $\mathbb{Z}[1/300]$ は UFD であり, その素元の完全代表系として $2, 3, 5$ 以外の素数全体の集合が取れる. □

ヒント. S を $2, 3, 5$ から生成される $\mathbb{Z}$ の積閉集合とすると $\mathbb{Z}[1/300] = S^{-1}\mathbb{Z}$. □

[94] $\mathbb{C}[x, x^{-1}, (x-1)^{-1}]$ は UFD であり, その素元の完全代表系として $0, 1$ 以外の $\alpha \in \mathbb{C}$ に対する $x - \alpha$ 全体の集合が取れる. □

ヒント. S を $x, x-1$ から生成される $\mathbb{C}[x]$ の積閉集合とすると $\mathbb{C}[x, x^{-1}, (x-1)^{-1}] = S^{-1}\mathbb{C}[x]$. □

[95] (カスプ) $\mathbb{C}[x, y]/(y^2 - x^3)$ は UFD ではなく, 素元ではない既約元を持つ. □

ヒント. $R = \mathbb{C}[x, y]/(y^2 - x^3)$ における x, y の像 $\bar{x}, \bar{y}$ は R の既約元だが素元ではない. $U(R) = \mathbb{C}^\times$ である. **[86]** の結果と $\bar{y}^2 = \bar{x}^3$ から, R が UFD ではないことと $\bar{x}, \bar{y}$ が素元ではないことがわかる. □

[96] (楕円曲線) $R = \mathbb{C}[x, y]/(y^2 - x^3 + 1)$ は UFD ではなく, 素元ではない既約元を持つ. □

ヒント. $R = \mathbb{C}[x, y]/(y^2 - x^3 + 1)$ における x, y の像を $\bar{x}, \bar{y}$ と書き, $\omega = \exp(2\pi i/3)$ とおくと, $\bar{y}$, $\bar{x} - 1$, $\bar{x} - \omega$, $\bar{x} - \omega^2$ は R の既約元である. 後は問題 **[95]** と同じ. □

参考 5.9 (楕円曲線) 方程式 $y^2 = (x$ の 3 次式$)$ で定義される曲線は楕円曲線と呼ばれる (大雑把な説明). 楕円 $(x^2/a^2 + y^2/b^2 = 1)$ と楕円曲線 $(y^2 = (x$ の 3 次式$))$ は異なる曲線なので区別しなければいけない. 混同しないように注意して欲しい. □

[97] ($\mathbb{Z}[\sqrt{-5}]$ は一意分解整域ではない) $\mathbb{Z}$ と $\alpha \in \mathbb{C}$ に対して $\mathbb{Z}$ と α を含む $\mathbb{C}$ の最小の部分環を $\mathbb{Z}[\alpha]$ と書く. このとき以下が成立することを示せ:

1. $\mathbb{Z}[\sqrt{-5}] = \{\, m + n\sqrt{-5} \mid m, n \in \mathbb{Z} \,\}$.
2. $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$.
3. 2, 3, $1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ の既約元である.
4. $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ より $\mathbb{Z}[\sqrt{-5}]$ は一意分解整域ではないことがわかる.
5. 複素平面上に $\mathbb{Z}[\sqrt{-5}]$ とそのイデアル (2), (3), $A = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$, $B = (3, 1 + \sqrt{-5})$, $C = (3, 1 - \sqrt{-5})$ がどのような集合であるかをわかり易く図示せよ.

6. $1 \pm \sqrt{-5}$ は $\bmod 2$ でも $\bmod 3$ でも 0 ではないが, $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$ は $\bmod 2$ でも $\bmod 3$ でも 0 になる. このことより 2, 3 は $\mathbb{Z}[\sqrt{-5}]$ の素元でないことがわかる.

7. A, B, C は $\mathbb{Z}[\sqrt{-5}]$ の素イデアルである (実際には極大イデアルになる).

8. $(2) = A^2$, $(3) = BC$ であるから, $(6) = A^2BC$ である. □

ヒント. 1. $\mathbb{Z}[\alpha]$ は $\mathbb{Z}$ と $\sqrt{-5}$ を含み加法と乗法で閉じているので $\mathbb{Z}[\alpha]$ は右辺を含まなければいけない. その右辺は $\mathbb{C}$ の部分環をなすので等号が成立する.

2. $\mathbb{Z}[\sqrt{-5}]$ の絶対値が 1 未満の元は 0 に限る. よって $\mathbb{Z}[\sqrt{-5}]$ の元が単元であるためにはその絶対値が 1 であることが必要である. 複素平面上に $\mathbb{Z}[\sqrt{-5}]$ の図を描いてみれば明らかなようにそのような元は ± 1 しかない. よって $\mathbb{Z}[\sqrt{-5}] = \{\pm 1\}$ である.

3. $\mathbb{Z}[\sqrt{-5}]$ の $0, \pm 1$ 以外の元の絶対値は 2 以上である. よって $\mathbb{Z}[\sqrt{-5}]$ の 0 でも単元でもない 2 個以上の元の積の絶対値は 4 以上になる. このことから 2, 3, $1 \pm \sqrt{-5}$ が $\mathbb{Z}[\sqrt{-5}]$ の既約元であることがわかる.

4. $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ は 6 の既約元の積への二種類の分解であり, $1 \pm \sqrt{-5} \not\sim 2, 3$ である. よって $\mathbb{Z}[\sqrt{-5}]$ は一意分解整域ではない.

5. $A = \mathbb{Z}2 + \mathbb{Z}(1+\sqrt{-5}) = \mathbb{Z}2 + \mathbb{Z}(1-\sqrt{-5})$, $B = \mathbb{Z}3 + \mathbb{Z}(1+\sqrt{-5})$, $C = \mathbb{Z}3 + \mathbb{Z}(1-\sqrt{-5}) = \mathbb{Z}3 + \mathbb{Z}(1+2\sqrt{-5})$.

7. $\mathbb{Z}[\sqrt{-5}]/A \cong \mathbb{F}_2$, $\mathbb{Z}[\sqrt{-5}]/B \cong \mathbb{Z}[\sqrt{-5}]/C \cong \mathbb{F}_3$.

8. $2 = -2 \cdot 2 + (1+\sqrt{-5})(1-\sqrt{-5}) \in A^2$ であるから $(2) \subset A^2$ である. 逆に $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5} \in (2)$ であるから $A^2 \subset (2)$ であることもわかる. よって $(2) = A^2$ である. 同様にして $(3) = BC$ も確かめられる. □

参考 5.10 上の問題の結果は E. Kummner (1810–1893) による理想数 (ideal number) としてのイデアルのアイデアを説明するためによく使われる. たとえば高木 [8] 第 5 章第 41 節 273–274 頁を見よ. $\mathbb{Z}[\sqrt{-5}]$ では数の既約元の積への分解の一意性も成立していないし, 数の素元の積への分解も存在するとは限らない. しかし, イデアルの素イデアルの積への一意分解可能性は成立している. 数の世界では成立していない素因数分解の一意存在がイデアル (理想数) の世界では成立しているのである. この事実を抽象化することによって **Dedekind 整域 (Dedekind domain)** の理論が構築され, 代数的整数論の基礎になっている. □

参考 5.11 実は一般に UFD でない Noether 整域は素元ではない既約元を持つ. たとえば松村 [6] p.199 の注 1 を見よ. □

定義 5.12 (原始多項式) R 上の一変数多項式環

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$$

について, 係数 $a_0, a_1, \ldots, a_n$ が互いに素なとき $f(x)$ を**原始多項式 (primitive polynomial)** と呼ぶ. □

[98] (内容) R は UFD であり, K はその商体であるとする.

1. 任意の $f(x) \in K[x]$ に対してある原始多項式 $f_0(x) \in R[x]$ と $c \in K$ で $f(x) = cf_0(x)$ を満たすものが存在する. このような $f_0(x)$, c は R の単元倍を除いて一意に定まる. c を $I(f)$ と書き, $f(x) \in K[x]$ の**内容 (content)** と呼ぶ.

2. $f(x) \in R[x]$ となるための必要十分条件は $I(f) \in R$ が成立することである.

3. $f(x)$ が $R[x]$ の原始多項式であるための必要十分条件は $I(f) \approx 1$ が成立することである.

4. たとえば $R = \mathbb{Z}$ のとき $f(x) = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{3}{4}x + \frac{2}{3}$ ならば $I(f) \approx \frac{1}{12}$ である. □

ヒント. 教科書を見よ. □

[99] (Gauss の補題) R は UFD であり, K はその商体であるとする.

1. $R[x]$ において原始多項式の積は原始多項式である.

2. $f, g \in K[x]$ に対して $I(fg) \approx I(f)I(g)$. □

ヒント. 教科書を見よ. □

[100] R は UFD であり, K はその商体であるとする. $f(x), g(x) \in R[x]$ で $g(x)$ を原始多項式とするとき, $f(x) = g(x)h(x)$, $h(x) \in K[x]$ ならば $h(x) \in R[x]$. □

ヒント. $I(f) = I(gh) \approx I(g)I(h)$ などを使う. □

[101] (UFD 係数の既約多項式は商体上でも既約) R は UFD であり, K はその商体であるとする. $R[x]$ の既約多項式は $K[x]$ においても既約多項式である. □

ヒント. 教科書を見よ. □

[102] (Eisenstein の判定法) R は UFD であるとし, K はその商体であるとする. p は R の素元であるとする. このとき

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$$

の係数 $a_i \in R$ が条件

$$p \nmid a_n, \quad p \mid a_{n-1}, \ \ldots, \ p \mid a_1, \ p \mid a_0, \quad p^2 \nmid a_0.$$

を満たしているならば f は $R[x]$ において既約である. したがって問題 **[101]** の結果より f は $K[x]$ においても既約である. たとえば k が体で $R = k[t]$ のとき, $K = k(t)$ であり, $x^2 - t$, $x^3 + tx + t \in R[x]$ は $K[x]$ の既約多項式である. □

[103] p が素数のとき $x^p + x^{p-1} + \cdots + x + 1$ が $\mathbb{Q}[x]$ の既約多項式になることを示せ. □

ヒント. x に $x+1$ を代入して Eisenstein の判定法を使え. x に $x+1$ を代入する操作は多項式環の自己同型なので代入結果の既約性を判定すれば必要十分である. □

[104] (UFD 係数の一変数多項式環の既約元) R は UFD であるとする．$R[x]$ の既約元は R の既約元か $R[x]$ の既約原始多項式のどちらかである．□

ヒント. たとえば永尾 [3], p.106, 例題 26.11. □

[105] (UFD 上の多項式環も UFD) UFD R 上の n 変数多項式環 $R[x_1, \ldots, x_n]$ もまた UFD である．特に体 K 上の n 変数多項式環 $K[x_1, \ldots, x_n]$ は UFD である．□

ヒント. 教科書を見よ．□

[106] ($\mathbb{Z}[x]$ の素イデアルの分類) $\mathbb{Z}$ 係数一変数多項式環 $\mathbb{Z}[x]$ の素イデアル P は次のどれかに等しい:

$$0, \quad (p), \quad (f(x)), \quad (p, f(x)).$$

ここで p は $\mathbb{Z}$ の素数で $f(x)$ は $\mathbb{Z}[x]$ の既約原始多項式である．□

ヒント. $P \neq 0$, $P \cap \mathbb{Z} = 0$ のとき．0 でない P の元を素元分解すると, P は素イデアルなのでその素因子のどれかは P に含まれる．$P \cap \mathbb{Z} = 0$ なのでその素因子は $\mathbb{Z}[x]$ のある既約原始多項式 $f(x)$ である．$f(x)$ で割り切れない P の元が存在すると仮定して矛盾を導こう．その元を素元分解することによって同様にしてある既約原始多項式 $g(x) \in P$ で $g(x) \not\approx f(x)$ となるものが存在することがわかる．そのときある $\tilde{a}(x), \tilde{b}(x) \in \mathbb{Q}[x]$ で $\tilde{a}(x)f(x) + \tilde{b}(x)g(x) = 1$ を満たすものが存在する．分母の整数 $d \neq 0$ をその両辺にかけることによって $a(x)f(x) + b(x)g(x) = d$, $a(x), b(x) \in \mathbb{Z}[x]$ を得る．このとき $0 \neq d \in P \cap \mathbb{Z}$ となって矛盾.

$P \neq 0$, $P \cap \mathbb{Z} \neq 0$ のとき．$P \cap \mathbb{Z}$ は $\mathbb{Z}$ の 0 でない素イデアルなのである素数 p が存在して $P \cap \mathbb{Z} = p\mathbb{Z}$. よって $p\mathbb{Z}[x] \subset P$ である．自然な同型 $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x]$ より, P は $(\mathbb{Z}/p\mathbb{Z})[x]$ の素イデアルに対応している．$\mathbb{Z}/p\mathbb{Z}$ は有限体になるので $(\mathbb{Z}/p\mathbb{Z})[x]$ の素イデアルは 0 または $(\mathbb{Z}/p\mathbb{Z})[x]$ の既約多項式 $\bar{g}(x)$ から生成される単項イデアルである．前者の場合には $P = p\mathbb{Z}[x] = (p)$ となる．後者の場合にはある 0 でない多項式 $g(x) \in P$ で $\bar{g}(x)$ を像に持つものが存在して $P = (p, g(x))$ となる．P は素イデアルなので $g(x)$ の素因子のどれかが P に含まれる．その素因子が素数 p' ならば上の方の $g(x)$ に関する議論と同様にして $p' = p$ でなければいけないことがわかる．しかしそのとき $\bar{g}(x) = 0$ になってしまうので矛盾する．よって $g(x)$ の素因子で P に含まれるものはある既約原始多項式 $f(x)$ でなければいけない．そのとき $P = (p, f(x))$ となる．□

[107] ($k[x, y]$ の素イデアルの分類) 体 k 上の二変数多項式環 $R = k[x, y]$ の素イデアル P は次のどれかに等しい:

$$0, \quad (f(x)), \quad (g(x, y)), \quad (f(x), g(x, y)).$$

ここで $f(x)$ は $k[x]$ の既約多項式で $g(x, y)$ は $k[x]$ 係数の y に関する既約原始多項式である．□

ヒント. [106] のヒントと同様．□

[108] (UFD の別の特徴付け) R は整域であるとする．R が UFD であるための必要十分条件は次の二つの条件が成立することである:

(a) R において既約元は素元である.

(b) R の単項イデアルで構成された空でない集合は包含関係に関する極大元を持つ (単項イデアルに関する極大条件). □

ヒント. 必要性. R は UFD であるとする. 問題 [**84**] (または [**85**]) の結果より (a) が成立する. (b) を背理法で示そう. (b) の否定を仮定する. すなわち R の単項イデアルで構成された空でない集合で極大元を持たないものが存在すると仮定する. このとき R の単項イデアルの無限列 $(a_0), (a_1), (a_2), \ldots$ で $(a_0) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots$ を満たすものが存在する. そのとき a_0 の素元分解を $a_0 = p_1 \cdots p_n$ と書くと $\{1, \ldots, n\}$ の部分集合の無限減少列 $Q_0 \supsetneqq Q_1 \supsetneqq Q_2 \supsetneqq \cdots$ で $a_k \approx \prod_{i \in Q_k} p_i$ を満たすものが存在しなければいけない. しかしこれは不可能である. よって (b) が成立しなければいけない.

十分性. (a) と (b) を仮定する. $a_0 \in R$, $a_0 \neq 0$, $a_0 \not\approx 1$ と仮定する. このとき (b) より (a) を含む R でない単項イデアル全体の集合は極大元 (p_1) を持つ. (p_1) の極大性より p_1 は R の既約元になる. (a) より p_1 は素元である. このとき $a = p_1 a_1$, $a_1 \in R$, $a_1 \neq 0$ である. もしも $a_1 \approx 1$ ならば $a \approx p_1$ である. もしも $a_1 \not\approx 1$ ならば同様に続けて $a_1 = p_2 a_2$, $a_2 = p_3 a_3$, $\ldots$ (p_i は素元, $a_i \in R$, $a_i \neq 0$) とできる. もしもどこまで続けても $a_i \approx 1$ とならなければ 極大元を持たない単項イデアルの上昇列 $\{(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots\}$ が得られるので (b) に矛盾する. よってある $i = n$ で $a_n \approx 1$ となる. そのとき $a \approx p_1 \cdots p_n$ と a は素元分解されている. したがって R は UFD である. □

参考 5.13 UFD に関するさらに進んだ結果についてはたとえば松村 [6] 第 7 章 §20 を参照せよ. UFD は代数幾何学的にも重要な概念である (Mumford [1] III §7 も参照せよ).

代数体の整数環のように (一般に UFD ではないが) イデアルの素イデアル分解の一意存在が成立する重要なクラスの整域 (Dedekind 整域) が存在する. Dedekind 整域についてはたとえば松村 [6] 第 4 章 §11 を参照せよ. □

参考文献

[1] Mumford, D., The Red Book of Varieties abd Schemes, Lecture Notes in Math., Vol. 1358, 1988

[2] 加藤和也, 黒川信重, 斎藤毅, 数論 1—Fermat の夢, 岩波講座現代数学の基礎 18, 岩波書店 1996

[3] 永尾汎, 代数学, 新数学講座 4, 朝倉書店, 1983

[4] 堀田良之, 代数入門—群と加群, 数学シリーズ, 裳華房, 1987

[5] 堀田良之, 環と体 1—可換環論, 岩波講座 現代数学の基礎 15, 岩波書店, 1997

[6] 松村英之, 可換環論, 共立出版, 1980, 2000

[7] リード, M., 可換環論入門, 伊藤由佳里訳, 岩波書店, 原書 1995, 翻訳 2000

[8] 高木貞治, 初等整数論講義, 第 2 版, 共立出版, 1971