環論講義ノート

松本雄也 (matsumoto.yuya.m@gmail.com)

2023 年 03 月 05 日

目次

0 導入

0.1 本講義ノートについて

おおよそ半期分の環論入門の講義ノートです.

1 つ前の半期に行われた想定の群論入門の講義ノート [群論] を参照しています.

各節の末尾には演習問題をつけます．☆はオススメの問題です．多くの問題にはヒントと略解をつける予定ですが，追いついていません.

[※範囲外] とついている部分は（内容が発展的だという理由で，または時間の都合で）試験範囲外です．ま

た，付録（A 節以降）も試験範囲外です．

指定の教科書はありませんが，堀田「代数入門 群と加群」と雪江「代数学 2 環と体とガロア理論」は本講義で扱う内容をだいたいカバーしていると思います．なお，インターネット上で閲覧できる資料等で勉強することも可能ではありますが，内容が正確かどうかの見極めが初心者には難しいかもしれないので，定評のある書籍を 1 冊持っておくのをお勧めします．インターネット上で数学記事を探す場合は，「site:ac.jp」で検索することで大学の講義資料等に当たりやすくするか，または英語版 wikipedia を使うことがお勧めです．

0.2 環論とその関連分野

本講義の主題となる環は，「加法」と「乗法」という 2 つの演算をもつ代数系であり，代数学の広い範囲で活躍する．とくに次のような分野で重要になる．……という話をしたいのですが，環に関する諸概念を導入してからでないと説明が難しい面があります．

- 整数論，とくに代数的整数論では，（代数的）整数とその加法や乗法といった演算が主役となるので，当然ながら環論と関連が深い．
- 代数幾何学で扱う図形である代数多様体は，「可換環のスペクトル」を張り合わせてできるものであり，代数多様体の性質は対応する環と深く関係する．そのため可換環の理論は代数幾何の基盤となっている．
- 環論 ……
- 環の表現論では，環の表現（別名：環上の加群）を扱う．……
- 体論：体は環の特殊な場合（0 以外のすべての元が乗法の逆元をもつ環）であり，体論は環論と相互に関連する．

1 環

1.1 環の定義

復習 1.1 (群)**.** 群の定義（およびそれを述べるために使った諸概念）を復習する．集合 G とその上の 2 項演算 $*$ が次を満たしているとき群というのだった：

- 演算が結合的である：任意の $x, y, z \in G$ に対して $(x * y) * z = x * (y * z)$ が成り立つ．（したがって，曖昧さなくこれを $x * y * z$ と書ける．）
- 単位元が存在する：e が単位元であるとは，任意の $x \in G$ に対して $x * e = e * x = x$ が成り立つことである．（単位元は存在すれば一意であることが証明できる．）
- 各元に対し逆元が存在する：y が x の逆元であるとは，$x * y = y * x = e$ が成り立つことである．（逆元は存在すれば一意であることが証明できる．）

さらに，演算が可換である（任意の $x, y \in G$ に対して $x * y = y * x$ が成り立つ）とき可換群またはアーベル群というのだった． ◊

本講義の主題となる環は，2 つの 2 項演算があり所定の性質を満たすものである．

定義 1.2 (環)**.** 2 つの 2 項演算 $+, \cdot$ をそなえた集合 A が次の条件を満たすとき，A を**環** $(ring)$ という．

(1) $+$ に関して A は可換群をなす．すなわち，
  (a) 任意の $a,b,c \in A$ に対し，$(a+b)+c = a+(b+c)$．（なので，これを単に $a+b+c$ と書く．）
  (b) 0 という元が（一意に）存在し，任意の $a \in A$ に対し，$a+0 = 0+a = a$.
  (c) 任意の $a \in A$ に対し，$x \in A$ が（一意に）存在し，$a+x = x+a = 0$．（この x を $-a$ と書く．）
  (d) 任意の $a,b \in A$ に対し，$a+b = b+a$.
(2) $\cdot$ は結合律を満たし，また $\cdot$ に関する単位元が存在する．すなわち，
  (a) 任意の $a,b,c \in A$ に対し，$(a\cdot b)\cdot c = a\cdot(b\cdot c)$．（なので，これを単に $a\cdot b\cdot c$ と書く．）
  (b) 1 という元が（一意に）存在し，任意の $a \in A$ に対し，$a\cdot 1 = 1\cdot a = a$.
(3) 次の**分配法則** (*distributive law*) が成り立つ：任意の元 $a,b,c \in A$ に対し，$a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ および $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$ が成り立つ．

環 A の加法の単位元を 0（または 0_A）と書き，乗法の単位元を 1（または 1_A）と書く． ◊

注 1.3. 文献によっては，単に環といったら定義 1.2 の条件 (2)(b) を要請せず，この条件を満たす環のことを**単位的** (*unital*) な環とよぶことがある．

本講義では，環にはつねに乗法の単位元の存在を要請する（これを満たすもののみを環とよぶ）． ◊

余談 1.4. フランス語では環を anneau という[*1]．環の記号としては $A,B,C,\dots$ と $R,S,\dots$ がよく用いられる． ◊

補題 1.5. A を環とする．次が成り立つ．

(1) $0_A\cdot a = 0_A$.
(2) $(-1_A)\cdot a = -a$.
(3) $(-a)\cdot b = a\cdot(-b) = -(ab)$, $(-a)\cdot(-b) = ab$. ◊

証明. 分配法則より $(0_A+0_A)\cdot a = 0_A\cdot a + 0_A\cdot a$ であり，$0_A+0_A = 0_A$ より $(0_A+0_A)\cdot a = 0_A\cdot a$ なので，$0_A\cdot a + 0_A\cdot a = 0_A\cdot a$ である．$0_A\cdot a$ の逆元を両辺に足して $0_A\cdot a = 0_A$ を得る．

他も同様に，$(1_A+(-1_A))\cdot a$ や $(a+(-a))\cdot b$ などを 2 通りに計算すればよい．証明は演習問題とする（問題 1.2）． □

注 1.6. 以降，乗法については記号を使わず（$a\cdot b$ のことを ab と書き），乗法と加法が並んだら乗法を先に計算するものとする（例えば $(a\cdot b)+c+(d\cdot e)$ のことを $ab+c+de$ と書く）． ◊

注 1.7. また，$a+(-b)$ のことを $a-b$ と書く．$a-b+c-d$ のように $-$ を含む式では結合性は成り立たないので本来は $((a-b)+c)-d$ のように順番を明示すべきともいえるが，実際には「$+$ と $-$ からなる式については左から計算する」という規則を前提とし括弧を使わずに書くのが普通である． ◊

定義 1.8 (可換環)**.** 環 $A = (A,+,\cdot)$ がさらに次の条件を満たすとき，**可換環** (*commutative ring*) であるという．

(4) 任意の $a,b \in A$ に対し，$a\cdot b = b\cdot a$. ◊

[*1] 読み：あのー

注 1.9. 可換環を主に扱う文献においては，可換環のことを略して単に環とよぶことがある．
本講義では，可換環に制限した話をする場合はその旨を明示する． ◊

定義 1.10 (体)**.** 可換環 $A = (A, +, \cdot)$ が零環（例 1.19）でなく，さらに次の条件を満たすとき，**体** (*field*, ドイツ語 *Körper*) [*2]であるという．

(5) 任意の $a \in A \setminus \{0\}$ に対し，$y \in A$ が（一意に）存在し，$a \cdot y = y \cdot a = 1$．（この y を a^{-1} や $\frac{1}{a}$ と書く．）

可換と限らない環がこの条件を満たすときは，**斜体** (*skew field*) や**可除環** (*division ring*) という．（逆に，体の方を可換性を強調して**可換体** (*commutative field*) とよぶこともある．） ◊

1.2 環の例

以下，$\boldsymbol{C}$ の部分集合については，とくに断らなければ通常の複素数の加法と乗法を考える．

環の例と，環でない例をいくつか挙げる．環でないものには，加法と乗法が定義されているが条件のいくつかを満たさない場合と，そもそも加法と乗法がその集合上の演算になっていない場合がある．後者には例えば，（より大きな集合上で定義された）演算で当該集合が閉じていない場合や，商集合上で well-defined になっていない場合がある．

例 1.11. $\boldsymbol{Z}$ は可換環である．$\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ は体である．
$\boldsymbol{N}$ は（0 を含める流儀でも含めない流儀でも）環でない．0 を含めないならば単位元がなく，含めるならば 0 以外の元が逆元をもたない． ◊

例 1.12. [群論, 8 節] で，加法群 $\boldsymbol{Z}/n\boldsymbol{Z}$ に乗法を $[a] \cdot [b] = [a \cdot b]$ で定めた（これで well-defined になる）．これは可換環である． ◊

注 1.13. 一般に環 A とその加法群としての部分群 $A' \subset A$ に対し，A/A' に乗法を $[a] \cdot [b] = [a \cdot b]$ で定めようとしても，well-defined になるとは限らない．（well-defined になることは A' がイデアルであることと同値である：これについては 4 節で扱う．） ◊

例 1.14. $2\boldsymbol{Z}$ は環にならない．乗法の単位元を含まないので． ◊

例 1.15. 実 n 次正方行列全体 $\mathrm{M}(n, \boldsymbol{R})$ は通常の加法と乗法に関して環をなす．$n \geq 2$ なら非可換である．複素の場合（$\mathrm{M}(n, \boldsymbol{C})$）なども同様である． ◊

例 1.16. $A = C(\boldsymbol{R}, \boldsymbol{R})$ を $\boldsymbol{R}$ から $\boldsymbol{R}$ への連続関数全体の集合とし，加法と乗法を各点で定める（すなわち，$f, g \in C(\boldsymbol{R}, \boldsymbol{R})$ に対し，$(f+g)(x) = f(x) + g(x)$，$(f \cdot g)(x) = f(x)g(x)$ とする）と，可換環になる．0_A は定数関数 0 であり，1_A は定数関数 1 である．
開集合 $U \subset \boldsymbol{R}$ に対し，U から $\boldsymbol{R}$ への連続関数全体の集合 $C(U, \boldsymbol{R})$ も同様に可換環になる．
一般に，位相空間 X から $\boldsymbol{R}$ への連続関数全体の集合 $C(X, \boldsymbol{R})$ も同様に可換環になる． ◊

例 1.17. m を正整数とする．集合 $\{a + b\sqrt{m} \mid a, b \in \boldsymbol{Z}\}$ は，通常の実数の加法と乗法により可換環になる．これを確かめるにあたってのポイントは，この集合が積に関して閉じているかだが，$(a+b\sqrt{m})(a'+b'\sqrt{m}) =$

[*2] 読み：たい

$(aa' + bb'm) + (ab' + a'b)\sqrt{m}$ なので確かに成り立つ.

$\boldsymbol{Z}$ を $\boldsymbol{Q}$ で置き換えた場合も同様に可換環になる（実は体になる）. ◊

例 1.18. x を変数とする（1 変数）実係数多項式環を $\boldsymbol{R}[x]$ で表す．これは可換環である．一般に環 A に対して A 上の（1 変数）多項式環 $A[x]$ を考えることができ，これは環であり，A が可換ならば $A[x]$ も可換である．多項式環については 8 節で詳しく扱う.

（n 変数多項式環 $A[x_1, x_2, \ldots, x_n]$ や，無限個の変数をもつ多項式環を考えることもできる.） ◊

例 1.19. 1 元集合 $A = \{0\}$ に加法と乗法を $0 + 0 = 0 \cdot 0 = 0$ と定めることで環になる．1 元集合である環は実質的にこれだけである．1 元集合である環を**零環** (*zero ring*) とよぶ．この環の加法の単位元は 0 であり，乗法の単位元も 0 である.

加法の単位元と乗法の単位元をそれぞれ $0_A, 1_A$ と書くことにしているので，この環においては $1_A = 0_A$ が成り立つということになる．（環の定義では $1_A \neq 0_A$ とは言っていないことに注意する.）問題 1.5 も参照. ◊

余談 1.20. 環のなかで，零環はいろいろと例外的な性質をもつ．それを理由に零環を環に含めない文献もあるが，空集合を集合に含めない（，空集合を位相空間に含めない）のと同程度に下手な定義だと思っています.

ただ,『零環でないという仮定をしばしば省略する』という文献については，いろいろな命題にいちいち「環 A が零環でない場合」と書くのも面倒だというのは理解できます. ◊

演習問題

問題 1.1 (☆ cf. 例 2.13)**.** (1) $\frac{1}{3}\boldsymbol{Z} := \{\frac{1}{3}n \mid n \in \boldsymbol{Z}\}$ は，（通常の実数の）乗法に関して閉じていないことを示せ．（そのため，これは環にならない.）

(2) $\boldsymbol{Z}[\frac{1}{3}] := \{\frac{n}{3^k} \mid n \in \boldsymbol{Z}, k \in \boldsymbol{N}\}$ は，（通常の実数の）加法と乗法に関して閉じていることを示せ．実は環になる（このことは証明しなくてよい）.

(3) 実 2 次正方行列全体 $\mathrm{M}(2, \boldsymbol{R})$ は通常の加法と乗法に関して環をなす（このことは証明しなくてよい）が，可換ではないことを具体的に元を挙げることで示せ.

問題 1.2 (☆)**.** 補題 1.5 の証明の残りを埋めよ.

問題 1.3. 集合 $\boldsymbol{R}^3$ 上で，加法は通常のベクトルの加法とし，乗法を外積（$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_2y_3 - x_3y_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix}$）

で定めると，環にならないことを示せ.

問題 1.4. $n \geq 2$ とし，実 n 次正方行列全体の集合 $A = \mathrm{M}(n, \boldsymbol{R})$ を考え，加法は通常の加法とする．以下のそれぞれの場合について，A は環にならないことを示せ．ただし以下の式において右辺は通常の加法と通常の乗法とする.

- 乗法を $X \cdot Y := XY - YX$ で定める場合.
- 乗法を $X \cdot Y := XY + YX$ で定める場合.

ただし，環にはならないものの，この演算により A はそれぞれ Lie 代数，Jordan 代数という代数系になる.

問題 1.5. A を環とする．次が同値であることを示せ．

- $|A| = 1$.
- $0_A = 1_A$.
- 0_A が乗法に関する逆元をもつ．

このとき A は零環である（正確には，零環に同型（定義 3.4）である）．

問題 1.6. 集合 A とその上の 2 項演算 $+, \cdot$ が，環の定義（定義 1.2）のうち条件 (1)(d) 以外を満たすと仮定する．このとき条件 (1)(d) も成り立つことを示せ．

2 部分環

2.1 部分環の定義

定義 2.1 (部分環)**.** 環 A の部分集合 B が次を満たすとき，B は A の**部分環** (*subring*) であるという．

(1) 加法に関して A の部分群である．すなわち，加法で閉じていて（$b, b' \in B$ に対して $b + b' \in B$），0_A を含み，逆元についても閉じている（$b \in B$ に対して $-b \in B$）．
(2) 乗法で閉じている（すなわち，$b, b' \in B$ に対して $bb' \in B$）．
(3) 乗法の単位元 1_A を含む．

このとき，A の加法と乗法を制限すると B 上の演算になり，B はこれらの演算に関して環になる． ◊

命題 2.2. A が可換ならば，その部分環も可換である． ◊

証明. 明らか． □

命題 2.3. B が A の部分環で，C が B の部分環ならば，C は A の部分環でもある． ◊

証明. 明らか． □

命題 2.4 (部分環の共通部分と和集合)**.** A を環とし，部分環の族 $(B_\lambda)_{\lambda\in\Lambda}$（各 λ に対し $B_\lambda \subset A$ は部分環）を考える．ただし $\Lambda \neq \emptyset$ とする．

(1) 共通部分 $\bigcap_{\lambda\in\Lambda} B_\lambda$ は部分環である．
(2) この族が包含関係に関して全順序をなせば（すなわち，任意の λ, λ' に対し $B_\lambda \subset B_{\lambda'}$ または $B_\lambda \supset B_{\lambda'}$ が成り立てば），和集合 $\bigcup_{\lambda\in\Lambda} B_\lambda$ も部分環である．
(3) $\Lambda = \{1, 2\}$ で，B_1 と B_2 がどちらも他方を含まないとき，$B_1 \cup B_2$ は部分環でない． ◊

証明. [群論, 補題 3.5（問題 3.2），問題 3.3] と同様である． □

定義 2.5. A を環，$S \subset A$ を部分集合とする．S を含む A の部分環は少なくとも 1 つ存在し（例えば A 自身），それらの部分環すべての共通部分も命題 2.4 より部分環である．明らかに，これは S を含む A の部分環の中で最小のものである．これを S が生成する A の部分環という．

$B \subset A$ が部分環，$S \subset A$ が部分集合のとき，和集合 $B \cup S$ が生成する A の部分環を，B 上 S が生成する

A の部分環といい，$B[S]$ と書く．$S = \{x_1, \ldots, x_n\}$ のときはこれを $B[x_1, \ldots, x_n]$ とも書く． ◊

注 2.6. 8 節で述べるように，この記法（$B[x_1, \ldots, x_n]$）は多項式環の記法と親和的である． ◊

注 2.7. S が生成する部分環の元を（[群論, 命題 3.37] で扱った部分群の場合のように）記述することは可能だが，煩雑（例えば $x_1, \ldots, x_4 \in S$ に対する $1 + x_1x_2 - x_3x_4x_3$ など……）なので省略する． ◊

定義 2.8. 環 A に対し，その部分集合 $\mathrm{Z}(A) := \{b \in A \mid \text{任意の } c \in A \text{ に対して } bc = cb\}$ を A の**中心** (*center*) という．

元 b, c が $bc = cb$ を満たすとき，b と c は**可換** (*commutative*) である，**交換する** (*commute*) という． ◊

命題 2.9. 環 A の中心 $\mathrm{Z}(A)$ は A の可換な部分環である．

より一般に，A の部分集合 S に対して，$\{b \in A \mid \text{任意の } c \in S \text{ に対して } bc = cb\}$ は A の部分環である． ◊

証明. 前半の証明は演習問題とする（問題 2.1）． 後半は前半と同様にできるので省略する． □

注 2.10. 中心 $\mathrm{Z}(A)$ の部分環は当然可換だが，A の可換な部分環が必ず $\mathrm{Z}(A)$ に含まれるわけではない．$\mathrm{Z}(A)$ を真に含む可換な部分環が存在することもある：例えば問題 2.5 を見よ． ◊

注 2.11. 一般に，環が性質 P を満たせばその部分環も性質 P を満たすか？ という形の命題を考えることができるが，一般に成り立たないことが多い．

例えば，整域（定義 7.13）はつねに体の部分環であるが，体は「環論的性質」の多くを満たすのに対し，整域で一般に成り立たない性質はいろいろある． ◊

2.2 部分環の例・中心の例

例 2.12. $\boldsymbol{Z} \subset \boldsymbol{Q} \subset \boldsymbol{R} \subset \boldsymbol{C}$ は部分環の系列である．$\boldsymbol{Z}$ と $\boldsymbol{Q}$ の間にはたくさんの部分環があり（例 2.13 や類似の例），$\boldsymbol{Q}$ と $\boldsymbol{R}$ の間にもたくさんの部分環がある（例 1.17 や類似の例）．$\boldsymbol{R}$ と $\boldsymbol{C}$ の間には他に部分環はない（$\boldsymbol{R}$ 上のベクトル空間としての次元を考えることで分かる）． ◊

例 2.13 (cf. 問題 1.1)**.** $\boldsymbol{Q}$ の部分集合 $\frac{1}{2}\boldsymbol{Z} := \{\frac{1}{2}n \mid n \in \boldsymbol{Z}\}$ は（部分）環にならない．例えば $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ が $\frac{1}{2}\boldsymbol{Z}$ の元でないので，乗法がこの集合上の演算になっていない．

$\boldsymbol{Z}$ 上 $\frac{1}{2}$ が生成する $\boldsymbol{Q}$ の部分環 $\boldsymbol{Z}[\frac{1}{2}]$（定義 2.5 の記法）は $\{\frac{n}{2^k} \mid n \in \boldsymbol{Z}, k \in \boldsymbol{N}\}$ に等しいことを示そう．まず $n, \frac{1}{2} \in \boldsymbol{Z}[\frac{1}{2}]$ なので，k 個の $\frac{1}{2}$ と 1 個の n の積である $\frac{n}{2^k}$ も $\in \boldsymbol{Z}[\frac{1}{2}]$ である．あとは $\{\frac{n}{2^k} \mid n \in \boldsymbol{Z}, k \in \boldsymbol{N}\}$ が $\boldsymbol{Q}$ の部分環であることを確認すればよい．和と積については

$$\frac{n}{2^k} + \frac{n'}{2^{k'}} = \frac{2^{k'}n + 2^k n'}{2^{k+k'}}, \qquad \frac{n}{2^k} \cdot \frac{n'}{2^{k'}} = \frac{nn'}{2^{k+k'}}$$

なのでよく，0，1，加法の逆元についても容易である．2 を他の 3 以上の整数に置き換えても同様である．これは，後に扱う（？）環の局所化の簡単な例である． ◊

例 2.14. $\boldsymbol{R}$ 上の C^∞ 関数全体の集合 $C^\infty(\boldsymbol{R}, \boldsymbol{R})$ は $C(\boldsymbol{R}, \boldsymbol{R})$ の部分環である．

コンパクト台 C^∞ 関数全体の集合は，乗法の単位元すなわち定数関数 1 を含まないので部分環ではない． ◊

例 2.15. 行列環 $\mathrm{M}(n, \boldsymbol{R})$ の中心は $\boldsymbol{R} \cdot E = \{\lambda E \mid \lambda \in \boldsymbol{R}\}$ である．$\boldsymbol{R} \cdot E$ が中心に含まれることは明らかであり，逆向きの包含関係は，例えば各行列単位 E_{ij} と交換するかを見ていくことで示せる．ここで E_{ij} は i 行

j 列成分のみが 1 で他の成分がすべて 0 である行列である．　◊

例 2.16 (四元数環)**.** $\mathrm{M}(2,\boldsymbol{C})$ の元 i,j,k を $i=\begin{pmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{pmatrix}$, $j=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $k=\begin{pmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}$ と定める．$\boldsymbol{R}$ ベクトル空間 $\mathrm{M}(2,\boldsymbol{C})$ の中で E,i,j,k が張る部分ベクトル空間を $\mathbf{H}$ とおくと，$\mathbf{H}$ は非可換な環である．単位元 $1_{\mathbf{H}}$ は E であり，$ij=k=-ji$，$jk=i=-kj$，$ki=j=-ik$ が成り立つ．

$\mathbf{H}$ を（Hamilton の）**四元数環** (*quaternion algebra*) という．

$\boldsymbol{R}\cdot E=\{\lambda E\mid\lambda\in\boldsymbol{R}\}\subset\mathrm{M}(2,\boldsymbol{R})$ は $\mathbf{H}$ の中心 $\mathrm{Z}(\mathbf{H})$ に含まれる．実は $\mathrm{Z}(\mathbf{H})=\boldsymbol{R}\cdot E$ である（問題 2.5）．

さらに，$\mathbf{H}$ は斜体である．実際，0 以外の元 $x=aE+bi+cj+dk\in\mathbf{H}$（$a,b,c,d\in\boldsymbol{R}$）に対し Cayley–Hamilton より $x((\operatorname{tr}x)E-x)=(\det x)E$ であり，$\det x=a^2+b^2+c^2+d^2\in\boldsymbol{R}\setminus\{0\}$ なので，$(\det x)^{-1}((\operatorname{tr}x)E-x)$ が x の逆元である．

ちなみに $\operatorname{tr}x=2a$ であり，$\bar{x}:=aE-bi-cj-dk=(\operatorname{tr}x)E-x$ は x の共役とよばれる．　◊

演習問題

問題 2.1 (☆中心は部分環)**.** 環 A の中心 $\mathrm{Z}(A)$ は A の可換な部分環である．

問題 2.2. $\boldsymbol{R}$ の下記の部分集合は $\boldsymbol{R}$ の部分環か否か判定せよ．また，部分環でない場合は，これが生成する $\boldsymbol{R}$ の部分環を求めよ．

(1) $\{a+b\sqrt[3]{2}\mid a,b\in\boldsymbol{Z}\}$.
(2) $\{a+b\sqrt[3]{2}+c\sqrt[3]{4}\mid a,b,c\in\boldsymbol{Z}\}$.
(3) $\{a+b\sqrt[3]{12}+c\sqrt[3]{18}\mid a,b,c\in\boldsymbol{Z}\}$.
(4) $\{a+b\sqrt{2}+c\sqrt{3}\mid a,b,c\in\boldsymbol{Z}\}$.

なお，$1,\sqrt{2},\sqrt{3}$ などが $\boldsymbol{Q}$ 上 1 次独立であることは使ってよい．

問題 2.3 (☆)**.** $\mathrm{M}(2,\boldsymbol{R})$ の下記の部分集合は部分環か否か判定せよ．また，部分環ならば，可換か否か判定せよ．また，可換でないならば，中心を求めよ．

(1) $\left\{\begin{pmatrix}* & *\\ 0 & *\end{pmatrix}\right\}$（この $*$ は「$\boldsymbol{R}$ の元ならなんでもよい」を意味する．すなわち，これは $(2,1)$ 成分が 0 である行列全体の集合である．以下も同様）.
(2) $\left\{\begin{pmatrix}0 & *\\ * & 0\end{pmatrix}\right\}$.
(3) $\left\{\begin{pmatrix}* & 0\\ 0 & 0\end{pmatrix}\right\}$.
(4) $\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\mid ad-bc\geq 0\right\}$.
(5) $\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\mid a,d\in\boldsymbol{Q},b\in\boldsymbol{R}\right\}$.

問題 2.4. $q\in\boldsymbol{Q}$，$q\neq 0,\pm 1$ とする．$q\boldsymbol{Z}:=\{qn\mid n\in\boldsymbol{Z}\}$ は $\boldsymbol{R}$ の部分環にならないことを示せ．

問題 2.5. Hamilton 四元数環 $\mathbf{H}$（例 2.16）の中心 $\mathrm{Z}(\mathbf{H})$ は $\boldsymbol{R} \cdot E = \{\lambda E \mid \lambda \in \boldsymbol{R}\} \subset \mathrm{M}(2, \boldsymbol{R})$ であることを示せ.

余力があれば：$\mathbf{H}$ の可換な部分環で $\mathrm{Z}(\mathbf{H})$ を真に含むものを 1 つ挙げよ.

3 環の準同型写像と同型写像

3.1 準同型写像と同型写像の定義

定義 3.1 (環準同型写像)**.** A, B を環とし，$f\colon A \to B$ を写像とする．f が次の条件を満たすとき f は**環の準同型写像** (*ring homomorphism*) または単に**準同型写像** (*homomorphism*) という.

(1) $x, y \in A$ に対し $f(x+y) = f(x) + f(y)$.
(2) $x, y \in A$ に対し $f(x \cdot y) = f(x) \cdot f(y)$.
(3) $f(1_A) = 1_B$. ◊

補題 3.2. $f\colon A \to B$ が環準同型ならば，$f(0_A) = 0_B$，$f(-a) = -f(a)$（$a \in A$）が成り立つ. ◊

証明. f は加法群の準同型なので（条件 (1)），主張は [群論, 命題 5.4] そのものである. □

注 3.3. 0 が 0 にうつること（補題 3.2）は条件 (1) から従う一方で，条件 (3) は他の 2 条件からは従わないので別個に要請する必要がある.（[群論, 命題 5.4] の単位元に関する主張の証明でも逆元の存在を使っていたことに注意する.）反例は 3.3 節の命題 3.26 を見よ. ◊

定義 3.4 (環同型写像，環同型)**.** 環 A, B の間の環準同型写像 $f\colon A \to B$ が**環同型写像** (*ring isomorphism*) または環同型（または単に**同型写像** (*isomorphism*)，同型）であるとは，環準同型写像 $h\colon B \to A$ が存在して $h \circ f = \mathrm{id}_A$，$f \circ h = \mathrm{id}_B$ を満たすことをいう.

環 A と B の間に環同型写像が存在するとき，A と B は（環として）**同型** (*isomorphic*) であるという．なお，定義から明らかに，A から B への同型写像が存在することと B から A への同型写像が存在することは同値である.

環 A と B が同型であることを $A \cong B$ と書き，同型でないことを $A \ncong B$ と書く．また，準同型写像 $A \to B$ が同型写像であることを明示するときに $A \xrightarrow{\sim} B$，$A \xrightarrow{\cong} B$ などと書く. ◊

注 3.5. 2 つの環が同型であることと，その間の個々の環準同型写像が同型写像であることは異なる.（環 A と B が同型であっても，A から B への同型写像でない準同型写像は一般に存在する.） ◊

命題 3.6. $f\colon A \to B$ を準同型写像とする．f が同型であることと全単射であることは同値であり，そのとき，定義の h は集合としての逆写像 f^{-1} である．とくに，f が同型のとき，定義 3.4 の h は一意に定まる. ◊

証明. まず f が同型ならば，定義の $h\colon B \to A$ が集合としての逆写像になっているので，f は全単射であり，逆写像の一意性より h は一意に定まる.

逆に f が全単射ならば同型であることを示す．そのためには，逆写像 f^{-1} が準同型であることを示せばよい．例えば，任意の $x', y' \in B$ に対して $f^{-1}(x' \cdot y') = f^{-1}(x') \cdot f^{-1}(y')$ を示す（他の条件も同様）．f が全射なので，$x' = f(x), y' = f(y)$ を満たす $x, y \in A$ が存在する．f が準同型なので $f(x \cdot y) = f(x) \cdot f(y) = x' \cdot y'$ である．これに f^{-1} を適用して $f^{-1}(x') \cdot f^{-1}(y') = f^{-1}(x' \cdot y')$ を得る. □

余談 3.7. ちなみに，定義 3.4，注 3.5，命題 3.6 は [群論, 定義 5.5，注 5.7，命題 5.8] をコピペして適当に書き替えました. ◊

定義 3.8. 準同型 $f\colon A \to B$ の**像** (*image*) とは写像としての像 $f(A) = \{b \in B \mid \exists a \in A, b = f(a)\}$ であり，これを $\operatorname{Im} f$ と書く. ◊

命題 3.9. $f\colon A \to B$ が準同型のとき，像 $\operatorname{Im} f$ は B の部分環である. ◊

証明は演習問題とする（問題 3.1）.

命題 3.10. $f\colon A \to B$ と $g\colon B \to C$ がどちらも環準同型（resp. 環同型）ならば，$g \circ f\colon A \to C$ も環準同型（resp. 環同型）である. ◊

証明. 容易. □

定義 3.11 (自己同型)**.** 環 A から A 自身への環同型写像を環の**自己同型写像** (*automorphism*) という. ◊

A から A 自身への準同型は**自己準同型写像** (*endomorphism*) というが，環の自己同型でない自己準同型は本講義の範囲ではあまり出番がない気がする.

3.2 準同型写像と同型写像の例

例 3.12. A を環とする．恒等写像 $\mathrm{id}_A\colon A \to A$ は（自己）同型写像である. ◊

例 3.13. $A' \subset A$ が部分環ならば，包含写像 $A' \to A$ は単射準同型写像である. ◊

例 3.14. $A' \subset A$ を部分環とする．$f\colon A \to B$ が準同型ならば，f の A' への制限 $f|_{A'}\colon A' \to B$ も準同型である. ◊

例 3.15. 複素共役をとる写像 $c\colon \boldsymbol{C} \to \boldsymbol{C}\colon z = x + y\sqrt{-1} \mapsto \bar{z} = x - y\sqrt{-1}$ は環の同型写像である．$c^2 = \mathrm{id}$ なので c 自身が c の逆である. ◊

例 3.16. m を正整数とし，平方数ではないとする．例 3.15 と同様に，$A = \boldsymbol{Z}[\sqrt{m}] = \{x + y\sqrt{m} \mid x, y \in \boldsymbol{Z}\}$ から A 自身への写像 $f\colon x + y\sqrt{m} \mapsto x - y\sqrt{m}$ は環同型である.

m が平方数のとき，この f（を定義したつもりの式）は well-defined でない：A の元を $x+y\sqrt{m}$ の形に表す方法が一意でないからである．例えば $m = 4$ のとき（$\sqrt{m} = 2$），$1+2\sqrt{m} = 3+1\sqrt{m}$ だが $1-2\sqrt{m} \neq 3-1\sqrt{m}$ である．m が平方数でないならば，1 と $\sqrt{m}$ は $\boldsymbol{Q}$ 上 1 次独立なのでそのような不都合は起こらず，前述の式で f が問題なく定義される. ◊

例 3.17. $A = \mathrm{M}(n, \boldsymbol{C})$ から自身への写像 $f\colon A \to A\colon P \mapsto {}^tP$ は，環準同型の条件 (1) と (3) は満たすものの，(2) を満たさないので環準同型ではない．一方で，$f(PQ) = f(Q)f(P)$ は満たす．条件 (1)(3) とこの条件を満たす写像は**反準同型写像** (*antihomomorphism*) とよばれる.

$g\colon A \to A\colon P \mapsto \overline{{}^tP}$（バーは複素共役）も，準同型ではないが反準同型である.

g を $\mathbf{H} \subset A$ に制限したものも，準同型ではないが反準同型である．例 2.16 の記号を用いると，$g(x) = \bar{x}$ である. ◊

例 3.18. 例 1.16 の記号を用いる．$\boldsymbol{R}$ の開集合 $V \subset U \subset \boldsymbol{R}$ に対し，**制限写像** (*restriction map*) $C(U, \boldsymbol{R}) \to C(V, \boldsymbol{R})\colon f \mapsto f|_V$ は環準同型である．一般には単射でも全射でもない（問題 3.9）． ◊

例 3.19. A を体とする．$A[x]$ を A 上の多項式環とする．

$$f = \frac{d}{dx}\colon A[x] \to A[x]\colon \sum_{n\geq 0} a_n x^n \mapsto \sum_{n\geq 1} n a_n x^{n-1}$$

は，A が零環でなければ，環の準同型でない．1_A の像が 0_A となり 1_A に一致しないので．

（ただし，f は Leibniz 則 $f(rs) = f(r)s + rf(s)$ を満たすので，**導分** (*derivation*) というものにはなっており，これはこれで活躍の場がある．） ◊

例 3.20. A を任意の環とする．$\boldsymbol{Z}$ から A への環準同型 f はただ一つ存在する．（圏論的に言うと，$\boldsymbol{Z}$ は環の圏の始対象である．）f は

$$f(n) = \begin{cases} \overbrace{1_A + 1_A + \cdots + 1_A}^{n\text{ 個}} & (n > 0), \\ 0 & (n = 0), \\ -(\underbrace{1_A + 1_A + \cdots + 1_A}_{-n\text{ 個}}) & (n < 0), \end{cases}$$

で与えられる． ◊

余談 3.21. 例 3.20 の記述で本当に定義になっているのか，また準同型になっているのは明らかなのか，を疑問に思った人のために詳しく述べます．$\boldsymbol{N}$ 上の関数が帰納的に定義できることは認めることにします．f を次のように帰納的に定義する．

$$f(0) = 0_A,$$
$$n \geq 0 \text{ に対し } f(n+1) = f(n) + 1_A,$$
$$n \geq 0 \text{ に対し } f(-n-1) = f(-n) - 1_A.$$

f が準同型であることの証明は次のような方針で示せます．

- $f(1) = 1_A$ を確認する．
- $n \geq 0$ に対して $f(n+1) = f(n) + 1_A$（定義）であり $1_A = f(1)$ なので $f(n+1) = f(n) + f(1)$ である．
- $n \geq 0$ と $m \geq 0$ に対して $f(n+m) = f(n) + f(m)$ であることを m に関する帰納法で示す．(n, m) での成立を仮定すると，$f(n + (m+1)) = f((n+m)+1) = f(n+m) + f(1) = f(n) + f(m) + 1_A = f(n) + f(m+1)$ なので $(n, m+1)$ でも成立する．
- $n, m, n+m$ の符号がそれ以外の場合は省略．
- $f(n \cdot 0) = f(0) = 0_A = f(n) \cdot 0_A = f(n) \cdot f(0)$ である．
- $n \geq 0$ と $m \geq 0$ に対して $f(n \cdot m) = f(n) \cdot f(m)$ であることを m に関する帰納法で示す．(n, m) での成立を仮定すると，$f(n \cdot (m+1)) = f(n \cdot m + n) = f(n \cdot m) + f(n) = f(n) \cdot f(m) + f(n) \cdot 1_A = f(n) \cdot (f(m) + 1_A) = f(n) \cdot f(m+1)(n, m+1)$ でも成立する．
- n, m の符号がそれ以外の場合は省略．

逆に準同型 $g\colon \boldsymbol{Z} \to A$ が f に等しいことは，$g(n \pm 1_{\boldsymbol{Z}}) = g(n) \pm 1_A$ を用いて帰納的に示せます． ◊

例 3.22. A を任意の環とし，n を正整数とする．$\boldsymbol{Z}/n\boldsymbol{Z}$ から A への環準同型は高々一つしかない．

実際，$f, g\colon \boldsymbol{Z}/n\boldsymbol{Z} \to A$ を準同型とすると，$\pi\colon \boldsymbol{Z} \to \boldsymbol{Z}/n\boldsymbol{Z}$ を（唯一の）準同型とするとき例 3.20 より $f \circ \pi = g \circ \pi$ であり，π は全射なので $f = g$ である． ◊

例 3.23. A を任意の環とする．$\boldsymbol{Q}$ から A への環準同型は高々一つしかない．証明は演習問題とする（問題 3.6）． ◊

3.3 直積環

定義 3.24. A_1, A_2 を環とする．直積集合 $A_1 \times A_2$ 上の加法と乗法を成分ごとに定義する．すなわち，

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2), \qquad (a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)$$

と定める．このとき $A_1 \times A_2$ は環になる．これを A_1 と A_2 の**直積環** (*product ring*) という．

$0_{A_1 \times A_2} = (0_{A_1}, 0_{A_2})$，$1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$ である．

同様に，0 個または 1 個または 3 個以上（無限個でもよい）の環の直積環が定義される．単位元の記述も同様である． ◊

注 3.25. 0 個の環の直積は零環（に同型）である． ◊

命題 3.26. A_1, A_2 を環とする．第 1 成分への射影 $\mathrm{pr}_1\colon A_1 \times A_2 \to A_1\colon (a_1, a_2) \mapsto a_1$ および第 2 成分への射影 $\mathrm{pr}_2\colon A_1 \times A_2 \to A_1\colon (a_1, a_2) \mapsto a_2$ は環準同型である．

任意個数の直積環についても同様である．

写像 $i_1\colon A_1 \to A_1 \times A_2\colon a \mapsto (a, 0)$ は，環の準同型写像の条件 (1),(2) を満たすが (3) を満たさない．つまり，加法群の準同型ではあるが，一般に環の準同型ではない． ◊

証明. 射影に関しては容易．

i_1 の方は，A_2 が零環でなければ，$i(1_{A_1}) = (1_{A_1}, 0_{A_2})$ が $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$ に一致しない． □

例 3.27. 環 $\boldsymbol{Z}/15\boldsymbol{Z}$ は直積環 $\boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/5\boldsymbol{Z}$ と同型である．実際, $\boldsymbol{Z}/15\boldsymbol{Z} \to \boldsymbol{Z}/3\boldsymbol{Z} \times \boldsymbol{Z}/5\boldsymbol{Z}\colon [a] \mapsto ([a], [a])$ は環同型写像である．逆は $([i], [j]) \mapsto [10i + 6j]$ で与えられる． ◊

例 3.28. $\boldsymbol{Z}/4\boldsymbol{Z}$ と $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$ は環として同型でない．なぜならば，そもそも加法群として同型でない：位数 4 の元の有無または位数 2 の元の個数を比較せよ． ◊

注 3.29. 加法群としては同型だが環として同型でない場合もある． ◊

演習問題

問題 3.1 (☆準同型の像は部分環)**.** $f\colon A \to B$ が準同型のとき，像 $\mathrm{Im}\, f$ は B の部分環であることを示せ．

問題 3.2 (☆部分環の像・部分環の逆像)**.** A, B を環とし，$f\colon A \to B$ を環準同型とする．

(1) $A' \subset A$ を部分環とする．$f(A')$ は B の部分環であることを示せ．
(2) $B' \subset B$ を部分環とする．$f^{-1}(B')$ は A の部分環であることを示せ．

問題 3.3. A を環，$\sigma\colon A \to A$ を環準同型とする．$A^\sigma := \{a \in A \mid \sigma(a) = a\}$ は A の部分環であることを示せ．

A が $\boldsymbol{C}$ で σ が複素共役の場合，A^σ は何か．

問題 3.4. A, B を環とする．$f, g\colon A \to B$ を環準同型とする．$A' := \{a \in A \mid f(a) = g(a)\}$ は A の部分環であることを示せ．

一般に $(f_\lambda\colon A \to B)_{\lambda\in\Lambda}$ が環準同型の族であるとき，$A' := \{a \in A \mid$ 任意の $\lambda, \mu \in \Lambda$ に対し $f_\lambda(a) = f_\mu(a)\}$ も A の部分環である．

問題 3.5. 互いに同型でない環 A, B で，加法群としては同型であるものの例を挙げよ．

問題 3.6. A を任意の環とする．$\boldsymbol{Q}$ から A への環準同型は高々一つしかないことを示すために，次を順に示せ．$f, g\colon \boldsymbol{Q} \to A$ を環準同型とする．

(1) $f|_{\boldsymbol{Z}} = g|_{\boldsymbol{Z}}$ が成り立つ．
(2) $x \in \boldsymbol{Q} \setminus \{0\}$ に対し，$f(\frac{1}{x})$ は $f(x)$ の（乗法に関する）左逆元かつ右逆元である．g に関しても同様である．
(3) 整数 $n \neq 0$ に対し $f(\frac{1}{n}) = g(\frac{1}{n})$ が成り立つ．
(4) $x = \frac{m}{n} \in \boldsymbol{Q}$（$m, n \in \boldsymbol{Z}, n \neq 0$）に対し $f(x) = g(x)$ が成り立つ．

なお，環 A において b が a の左逆元で c が a の右逆元ならば $b = c$ であることを使ってもよい（[群論, 命題 2.11] と全く同様に示せる）．

問題 3.7. 体から体への準同型写像は単射であることを示せ．

問題 3.8. 特定の環の間の準同型写像の有無・多寡について，次を示せ．

(1) $n \geq 1$ のとき，準同型 $\boldsymbol{Z}/n\boldsymbol{Z} \to \boldsymbol{Z}$ は存在しない．
(2) 準同型 $\boldsymbol{Z}[\sqrt{2}] \to \boldsymbol{Q}$ は存在しない．
(3) 準同型 $\boldsymbol{Z}[\sqrt{2}] \to \boldsymbol{Z}[\sqrt{2}]$ はちょうど 2 つ存在する．
(4) 準同型 $\boldsymbol{R} \to \boldsymbol{R}$ はちょうど 1 つ存在する．

問題 3.9 (環論要素がない……)**.** 位相空間 X とその開集合 $V \subset U \subset X$ に対し，制限写像 $r\colon C(U, \boldsymbol{R}) \to C(V, \boldsymbol{R})\colon f \mapsto f|_V$ を考える．

(1) $X = \boldsymbol{R}$ で，r が全射でない例を挙げよ．
(2) $X = \boldsymbol{R}$ で，r が単射でない例を挙げよ．
(3) $X = \boldsymbol{R}^n$ で，r が全単射ならば，$V = U$ であることを示せ．
(4) $V \subsetneq U$ かつ r が全単射である例を挙げよ．

4 イデアル

4.1 動機

余談 4.1. 環のイデアルにはいろいろな側面があり，イデアルを調べる理由がいろいろある．

まず，（簡単のため可換環で考えるが,）A の元 a に対し単項イデアル (a) が定まり，a が b を割りきることと $b \in (a)$ と $(b) \subset (a)$ が同値である．すなわち，環の元の整除関係に注目して，元を一般化したものと考えられる．

歴史的には代数的整数論に始まる．代数的整数からなる環（典型例は $\boldsymbol{Z}[\sqrt{-5}]$）では $\boldsymbol{Z}$ のような素因数分解の一意性が必ずしも成り立たず，Kummer は通常の数のほかに「理想的（ideal）な数」を導入して素因数分解の一意性を回復できないかと考えた．Dedekind はこれを数そのものではなく数からなる集合として定式化した（これが現在の意味のイデアルである）．

古典的な代数幾何においてはいくつかの（多変数）多項式の共通零点の集合，つまり $\{(x_1, \ldots, x_n) \in \boldsymbol{C}^n \mid f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0\}$ という形の集合が重要である．$f_1, \ldots, f_m$ という有限個の多項式の組を考えるより，それらが生成する $\boldsymbol{C}[x_1, \ldots, x_n]$ のイデアルを考えた方が扱いやすい．現代的には，代数幾何で扱う図形（代数多様体）の点は大雑把にいえば環の素イデアルである．

環の準同型写像の核はイデアルであり，逆にイデアルはある準同型写像の核になる．

環 A 自身を A 上の（左・右）加群と見ることができるが，（左・右）イデアルとはその部分加群に他ならない．　◊

余談 4.2. 日本語ではドイツ語 Ideal の発音に由来した「イデアル」という表記が一般的である（古い文献だと「イデヤル」もある）．英語の発音は「アイディアル」に近い．　◊

4.2　イデアルの定義と例

定義 4.3. 環 A の部分集合 $I \subset A$ に対する次の条件を考える．

(1) I は A の（加法に関する）部分アーベル群である．
(2) 任意の $x \in I$ と $a \in A$ に対し，$ax \in I$ が成り立つ．
(3) 任意の $x \in I$ と $a \in A$ に対し，$xa \in I$ が成り立つ．

条件 (1) と (2) を満たすものを**左イデアル** (*left ideal*) という．条件 (1) と (3) を満たすものを**右イデアル** (*right ideal*) という．条件 (1)(2)(3) を満たすものを**両側イデアル** (*two-sided ideal*) という．

A が可換ならば，(2) と (3) は同値である．このとき左イデアルと右イデアルと両側イデアルはすべて同じ概念になり，単に**イデアル** (*ideal*) という．

（A が可換でなくても，左・右・両側のどれを考えているかが文脈から明らかな場合は，単にイデアルということもある．）

A より真に小さいイデアルを，**真のイデアル** (*proper ideal*) という．　◊

例 4.4. $\{0\}$ および A は A の両側イデアルである．　◊

例 4.5. $a \in A$ が元のとき，$Aa := \{ba \mid b \in A\}$ は左イデアルである（問題 4.1）．同様に，$aA := \{ab \mid b \in A\}$ は右イデアルである．この形に表せるイデアルを**単項イデアル**または**主イデアル** (*principal ideal*) とよぶ（正確には単項左イデアルなどとよぶ）．

$\{0\} = 0A = A0$ と $A = 1A = A1$ は単項イデアルの 2 つの極端な場合である．

A が可換ならば aA と Aa は一致する．これを (a) と書くことも多い．　◊

注 4.6. 集合 $\{xay \mid x, y \in A\}$ は一般に両側イデアルとは限らない．というのは，加法で閉じているとは限らないので（問題 4.4 参照）．◊

一般に，単項（左・右）イデアルとしての表し方は一意ではない．

補題 4.7. A を環とする．

(1) $a, b \in A$ に対し，$Aba \subset Aa$ が成り立つ．
(2) $u \in A$ が左逆元をもつならば，$Aua = Aa$ が成り立つ．

単項右イデアルについても同様のことが成り立つ．◊

証明．(1) Aba の元は cba（$c \in A$）すなわち $(cb)a$ という形をしているので Aa に属する．
(2) まず (1) より $Aua \subset Aa$ は成り立つ．u の左逆元が存在するので，1 つとり v とおくと，再び (1) を用いて $Aa = Avua \subset Aua$ が成り立つ．□

したがって，A が可換な場合には次が言える：$u \in A$ が逆元をもつならば，イデアル (a) と (ua) は一致する．

余談 4.8. A を可換環として，イデアル (a) と (b) が一致するならば $u, v \in A$ で $uv = 1$，$ua = b$，$vb = a$ を満たすものが存在するかというと，例えば A が整域ならば正しいが一般には正しくない（問題 H.12）．◊

例 4.9 (体のイデアル)**.** F を斜体とする[*3]．F の左イデアルは $\{0\}$ と F しかない．これを示す．$I \subset F$ を左イデアルとする．イデアルは加法に関する部分群なので $0 \in I$ である．$I \supsetneq \{0\}$ ならば $I = F$ であることを示す．仮定より $I \setminus \{0\}$ の元 a が存在する．F が斜体なので $ua = 1$ を満たす $u \in F$ が存在し，I が左イデアルなので $1 \in I$ である．したがって任意の $x \in F$ に対して $x = x \cdot 1 \in I$ である．
右イデアルについても同様であり，したがって両側イデアルについても同様である．◊

例 4.10 ($\boldsymbol{Z}$ のイデアル)**.** 環 $\boldsymbol{Z}$ のイデアルをすべて決定しよう．$I \subset \boldsymbol{Z}$ をイデアルとすると，イデアルはとくに（加法に関する）部分群なので，[群論, 例 3.16] で見たように，$n \geq 0$ を用いて $I = n\boldsymbol{Z}$ と表せる．逆に，$n \geq 0$ に対する $I = n\boldsymbol{Z}$ を考えると，これが（単に加法群であるのみならず）イデアルであることが簡単に確かめられる．したがって，$\boldsymbol{Z}$ のイデアルは $n\boldsymbol{Z}$ で尽くされる．◊

例 4.11 ($k[x]$ のイデアル)**.** k を体とし，$A = k[x]$ を k 上の 1 変数多項式環とする．A のイデアルは (0) であるかまたはモニックな多項式 f を用いて (f) と表せて，さらに f は一意に定まる．このことは 8 節で示す．ただし多項式 f が**モニック** (*monic*) であるとは，0 ではなく，かつ最高次の係数が 1 であることをいう．◊

すべてのイデアルが単項イデアルである可換環を**単項イデアル環** (*principal ideal ring*) とよぶ．その中で整域（後述）であるものを**単項イデアル整域** (*principal ideal domain*) または略して *PID* とよぶ．
単項イデアル環はかなり特殊な環であり，一般には単項イデアルでないイデアルがたくさんある．

[*3] 本講義では，斜体は可換なものと可換でないもの両方を含む．

4.3 イデアルの共通部分や和

本小節では，「∗」は「左」「右」「両側」のいずれかとする．∗イデアルの共通部分，生成，和を定義する．なお次小節では（可換環の場合に限定して）積を扱う．

∗イデアルの**共通部分** (*intersection*) とは単に集合としての共通部分である．

命題 4.12 (イデアルの共通部分と和集合，cf. 命題 2.4)**.** A を環とし，∗イデアルの族 $(I_\lambda)_{\lambda\in\Lambda}$（各 λ に対し $I_\lambda \subset A$ は∗イデアル）を考える．ただし $\Lambda \neq \emptyset$ とする．

(1) 共通部分 $\bigcap_{\lambda\in\Lambda} I_\lambda$ は∗イデアルである．
(2) この族が包含関係に関して全順序をなせば（すなわち，任意の λ, λ' に対し $I_\lambda \subset I_{\lambda'}$ または $I_\lambda \supset I_{\lambda'}$ が成り立てば），和集合 $\bigcup_{\lambda\in\Lambda} I_\lambda$ も∗イデアルである．
(3) $\Lambda = \{1, 2\}$ で，I_1 と I_2 がどちらも他方を含まないとき，$I_1 \cup I_2$ は∗イデアルでない． ◊

証明. これも [群論, 補題 3.5（問題 3.2），問題 3.3] と同様である． □

定義 4.13. A を環，$S \subset A$ を部分集合とする．S を含む A の∗イデアルは少なくとも 1 つ存在し（例えば A 自身），それらの∗イデアルすべての共通部分も命題 4.12 より∗イデアルである．明らかに，これは S を含む A の∗イデアルの中で最小のものである．これを S が**生成する** (*generate*) A の∗イデアルという． ◊

命題 4.14. A を環，$S \subset A$ を部分集合とする．

(1) $AS := \{\sum_{i=1}^n a_i s_i \mid n \geq 0, a_i \in A, s_i \in S\}$ は左イデアルである．また，S を含む左イデアルは必ず AS を含む．したがって，これが S が生成する左イデアル（定義 4.13）である．
(2) とくに，S が有限集合 $\{x_1, \ldots, x_m\}$ の場合，AS は $\{\sum_{i=1}^m a_i x_i \mid a_i \in A\}$ に等しい．

右イデアルの場合も同様である（$a_i s_i$ を $s_i a_i$ に置き換える）． ◊

証明. (1) AS が左イデアルであることを示す．和について，$a_1 s_1 + \cdots + a_n s_n + a'_1 s'_1 + \cdots + a'_{n'} s'_{n'}$ は記号をとり直すことで AS に属することが分かる．$0 \in AS$ は $n := 0$ とすれば分かる．逆元については a_i の部分を $-a_i$ にすればよい．スカラー倍については，$c \cdot \sum_{i=1}^n a_i s_i = \sum_{i=1}^n (ca_i) s_i$ である．

I が左イデアルで $S \subset I$ だとして，$AS \subset I$ を示す．AS の元 $\sum_{i=1}^n a_i s_i$ を考えると，まず $s_i \in S \subset I$ であり，I が左からのスカラー倍で閉じているので $a_i s_i \in I$ であり，I が和で閉じているので $\sum_{i=1}^n a_i s_i \in I$ である．

(2) S が有限集合の場合，AS の元の表示において，各 $x_i \in S$ が出てくる項をまとめることで $\sum_{i=1}^m a_i x_i$ の形になる． □

∗イデアル I が集合 S で生成されるとき，S（またはその元を並べた列）を I の生成系という．1 つの元からなる場合はその元を I の**生成元** (*generator*) という．

∗イデアルを生成するのに元が最低いくつ必要か，はイデアル（や環）の複雑さの指標とも考えられる．

A が可換で S が有限集合 $\{x_1, \ldots, x_m\}$ のときは，S が生成するイデアルを $(x_1, \ldots, x_m)$ とも書く．

命題 4.15. I, J を∗イデアルとする．和集合 $I \cup J$ が生成する∗イデアルを $I + J$ と書き，I と J の**和** (*sum*) とよぶ．これは集合として $\{i + j \mid i \in I, j \in J\}$ に一致する．

同様に，有限個 $I_1, \ldots, I_m$ の＊イデアルの和を，それらの和集合が生成する＊イデアルとして定め，$I_1 + \cdots + I_m$ と書く．これは集合として $\{i_1 + \cdots + i_m \mid i_1 \in I_1, \ldots, i_m \in I_m\}$ に一致する．

同様に，（無限個でもよい）＊イデアルの族 $(I_\lambda)_{\lambda\in\Lambda}$ の和を，それらの和集合が生成する＊イデアルとして定め，$\sum_{\lambda\in\Lambda} I_\lambda$ と書く．これは集合として $\{a_{\lambda_1} + \cdots + a_{\lambda_r} \mid r \geq 0, \lambda_i \in \Lambda, a_{\lambda_i} \in I_{\lambda_i}\}$ に一致する．　◊

証明. 「＊」が「左」で，2 個の和集合の場合を示す．まず $S := \{i + j \mid i \in I, j \in J\}$ がイデアルであることを示す．S が加法の部分群であることは I, J がそうなのでよい．元 $i + j \in S$ と $a \in A$ に対して $a(i + j) = ai + aj$ であり，I と J がイデアルなので $ai \in I$，$aj \in J$ であり，したがって $ai + aj \in S$ である．

また，$I \cup J$ を含むイデアルが S を含むことは明らかである．したがって $I \cup J$ が生成するイデアルは S に一致する．

無限個でもよい和集合については，まず加法の部分群であることは [群論, 命題 3.37] から分かり，スカラー倍については 2 個の和集合の場合と同様である．

「＊」がそれ以外の場合も同様である．　□

注 4.16. 和の定義から，＊イデアル K が＊イデアル $I + J$ を含むことは，K が I を含みかつ K が J を含むことと同値である．つまり，イデアルの和はある程度「和集合」と同じように扱える．　◊

命題 4.17. 環の＊イデアルの和について次が成り立つ．$(I + J) + K = I + J + K = I + (J + K)$，$I + J = J + I$，$I + \{0\} = I$，$I + A = A$，$I + I = I$．　◊

略証. 注 4.16 を使って包含関係だけで議論してもよいし，命題 4.15 を使って部分集合としての具体的な表示を用いてもよい．　□

4.4 可換環のイデアルの積

定義 4.18. A を可換環とし，$I, J \subset A$ をイデアルとする．集合 $\{ij \mid i \in I, j \in J\}$ が生成するイデアルを IJ と書き，I と J の**積** (*product*) とよぶ．これは一般に集合 $\{ij \mid i \in I, j \in J\}$ に一致しない（例 4.26 の中にそのような例がある）．

イデアル I と正整数 n に対し**冪乗** (*power*) I^n を，$I^1 = I$，$I^{n+1} = I^n I = II^n$ で帰納的に定義する．　◊

この積および冪乗は，次の意味で環の元の積と冪乗の一般化になっている．

命題 4.19. A を可換環，$a, b \in A$ を元，$n \in \boldsymbol{Z}_{>0}$ を正整数とすると，$(a)(b) = (ab)$，$(a)^n = (a^n)$ が成り立つ．　◊

証明. 積の定義より，$(a)(b)$ とは集合 $S := \{ij \mid i \in (a), j \in (b)\}$ が生成するイデアルである．$i = pa, j = qb$ と書くと $S = \{pqab \mid p, q \in A\}$ であり，明らかに $S \subset (ab)$ であり，一方で（$q = 1$ とすることで）$(ab) \subset S$ でもあるので，$S = (ab)$ である．したがってこれが生成するイデアルである $(a)(b)$ も (ab) に等しい．

冪乗の方は，積の方の結果を使って帰納的に示せる．　□

補題 4.20. 可換環 A の部分集合 S, T に対し，$S \cdot T := \{st \mid s \in S, t \in T\}$ と書くことにする．また，S が生成するイデアルを $\langle S\rangle$ と書くことにする．このとき $\langle S \cdot T\rangle = \langle S\rangle\langle T\rangle$ が成り立つ（右辺はイデアルの積）．　◊

証明. 左辺が右辺に含まれることは容易である：イデアルの積の定義より右辺は $\langle\langle S\rangle \cdot \langle T\rangle\rangle$ であり，$S \subset \langle S\rangle$

と $T \subset \langle T \rangle$ から $\langle S \cdot T \rangle \subset \langle \langle S \rangle \cdot \langle T \rangle \rangle$ なので.

右辺が左辺に含まれることはもう少し頑張る必要がある. $\langle S \rangle \cdot \langle T \rangle \subset \langle S \cdot T \rangle$ を示せばよい. 左辺の元は $\sigma\tau$ ($\sigma \in \langle S \rangle$, $\tau \in \langle T \rangle$) と書ける. 命題 4.14 より, $\sigma = \sum_j b_j s_j$, $\tau = \sum_k c_k t_k$ と書けて ($b_j \in A$, $c_k \in A$, $s_j \in S$, $t_k \in T$), すると $\sigma\tau = \sum_{j,k} b_j c_k s_j t_k$, $b_j c_k \in A$, $s_j t_k \in S \cdot T$ なので $\sigma\tau \in \langle S \cdot T \rangle$ である. □

系 4.21. $(a_1, \ldots, a_n)(b_1, \ldots, b_m) = (a_1 b_1, a_1 b_2, \ldots, a_n b_m)$ が成り立つ (左辺はイデアルの積で, 右辺は nm 個の元で生成されるイデアル). ◊

証明. $S = \{a_1, \ldots, a_n\}$ と $T = \{b_1, \ldots, b_m\}$ に補題 4.20 を適用すればよい. □

命題 4.22. 可換環のイデアルの積について次が成り立つ. $(IJ)K = I(JK)$, $IJ = JI$, $IA = I$, $I(0) = (0)$, $(I + J)K = IK + JK$. ◊

証明. $(IJ)K = I(JK)$ については, 補題 4.20 より, 両辺どちらも集合 $(I \cdot J) \cdot K = I \cdot (J \cdot K) = \{ijk \mid i \in I, j \in J, k \in K\}$ が生成するイデアルに等しい.

$(I + J)K = IK + JK$ を示す. 左辺が右辺に含まれることを示すには, 和の具体的表示 (命題 4.15) と積の定義より, $(i + j)k$ ($i \in I, j \in J, k \in K$) が右辺に含まれることをいえばよいが, $(i + j)k = ik + jk$ で $ik \in IK$, $jk \in JK$ なのでよい. 右辺が左辺に含まれることは, $I \subset I + J$ なので $IK \subset (I + J)K$ であり, 同様に $JK \subset (I + J)K$ なのでよい.

他は簡単である. □

簡単な例として $\boldsymbol{Z}$ のイデアルの和や積を考えたいが, その前にもう少し用語と補題を用意する.

定義 4.23. A を可換環, $a, b \in A$ を元とする. A のある元 c に対して $b = ac$ となるとき, a は b の**約数** (*divisor*) であるといい, b は a の**倍数** (*multiple*) であるという. この関係を $a \mid b$ と書く. ◊

補題 4.24. A を可換環, $a, b \in A$ を元とすると, 次は同値である.

- a は b の約数である. b は a の倍数である.
- $b \in (a)$.
- $(b) \subset (a)$. ◊

証明. 容易. □

例 4.25 ($\boldsymbol{Z}$ のイデアルの和や積)**.** $\boldsymbol{Z}$ のイデアル $(a), (b)$ の和と積を検討する. まず積については命題 4.19 より $(a)(b) = (ab)$ である.

和 $(a) + (b)$ もイデアルなので単項イデアルであり, $(a) + (b) = (g)$ と書ける. この g を**最大公約数** (*greatest common divisor*) といい $\gcd\{a, b\}$ と表す. この g は次の性質を満たす.

- g は a の約数でもあり b の約数でもある (すなわち公約数である). これは $a \in (a) \subset (a) + (b) = (g)$ から分かる (b も同様).
- g は a と b の公約数のうち整除関係に関して最大である, すなわち, h が a と b の公約数ならば g は h の約数である. 実際, h に関する仮定から $(a) \subset (h)$, $(b) \subset (h)$ なので $(g) = (a) + (b) \subset (h)$ である.

ちなみに a と b の最大公約数を (a, b) と書くこともあるが, イデアルの記号と親和している. ◊

一般の環では 2 元の最大公約数が存在するとは限らない.

例 4.26. 4.1 節で述べたように，代数的整数の環は必ずしも素因数分解ができない．これはそれらの環が単項イデアル環と限らないことに由来する．その例として，$A = \boldsymbol{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \boldsymbol{Z}\}$ が単項イデアル環でないことを見よう.

$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ が成り立つ．もし A で素因数分解ができるならば，$2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ の分解を比較することで,

$$2 = pq, \quad 3 = rs, \quad 1 + \sqrt{-5} = pr, \quad 1 + \sqrt{-5} = qs$$

を満たす $p, q, r, s \in A$ が存在するはずである．しかし実際には，$2 = ab$ を満たす (a, b) は $(\pm 1, \pm 2), (\pm 2, \pm 1)$ しかなく，他の元も同様である（問題 4.13(3)）.

ここで次のイデアルを考える：

$$P = Q = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5}), \quad R = (3, 1 + \sqrt{-5}), \quad S = (3, 1 - \sqrt{-5}).$$

このとき，以下のイデアルの等式が成り立つ：

$$(2) = PQ, \quad (3) = RS, \quad (1 + \sqrt{-5}) = PR, \quad (1 - \sqrt{-5}) = QS.$$

$PR = (1 + \sqrt{-5})$ を確かめよう．まず $P = (2, 1 + \sqrt{-5})$，$R = (3, 1 + \sqrt{-5})$ なので，系 4.21 より，

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

であり，この 4 元はすべて $(1+\sqrt{-5})$ に含まれる（$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ を使う）ので $PR \subset (1+\sqrt{-5})$ である．一方で $2 \cdot (1 + \sqrt{-5}), 3 \cdot (1 + \sqrt{-5}) \in PR$ なので $(1 + \sqrt{-5}) = 3 \cdot (1 + \sqrt{-5}) - 2 \cdot (1 + \sqrt{-5}) \in PR$ である．これ以外の 3 つの等式は問題 4.13(4) とする.

$RS = (3)$ だが 3 は R の元と S の元の積にはならないので，定義 4.18 で述べた反例にもなっている（他の組み合わせも同様）.

さらに，A のこれらのイデアルによる剰余環と $\boldsymbol{Z} \to A$ との合成に対して準同型定理（定理 5.17）を適用すると $\boldsymbol{Z}/2\boldsymbol{Z} \cong A/P = A/Q$，$\boldsymbol{Z}/3\boldsymbol{Z} \cong A/R$，$\boldsymbol{Z}/3\boldsymbol{Z} \cong A/S$ を得る（問題 4.13(5)）ため，実は P, Q, R, S は素イデアル（10.1 節）である．すなわち，上記の式が $(2), (3), (1 + \sqrt{-5}), (1 - \sqrt{-5})$ の素イデアル分解を与えている. ◊

注 4.27. この他の演算として，少なくとも可換環の場合に，イデアルの根基（問題 4.8）やイデアル商（問題 4.9）という概念がある．演習問題で扱う. ◊

演習問題

主に 4.2 節に関する問題

問題 4.1 (☆単項イデアル)**.** 環 A とその元 $a \in A$ に対し，$Aa := \{ba \mid b \in A\}$ は左イデアルであることを示せ.（同様に，$aA := \{ab \mid b \in A\}$ は右イデアルである.）

問題 4.2 (部分集合が生成する両側イデアルの具体的表示)**.** A を環，$S \subset A$ を部分集合とする.

(1) $ASA := \{\sum_{i=1}^{n} a_i s_i b_i \mid n \geq 0, a_i \in A, b_i \in A, s_i \in S\}$ は両側イデアルであることを示せ．また，S を含む両側イデアルは必ず ASA を含むことを示せ．したがって，これが S が生成する両側イデアルである．
(2) $ASA = (AS)A = A(SA)$ を示せ．

問題 4.3 (cf. 例 4.9)**.** A が零環でない環で，A の左イデアルは $\{0\}$ と A しかなく，A の右イデアルも $\{0\}$ と A しかないとき，A は斜体であることを示せ．

問題 4.4. （非可換な）環 $A = \mathrm{M}(2, \boldsymbol{R})$ を考える．$I \subset A$ は両側イデアルで，$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$ だとする．$I = A$ であることを示せ．また，集合 $\{xE_{11}y \mid x, y \in A\}$ は A の真部分集合であることを示せ．（したがって，一般に $a \in A$ に対し $\{xay \mid x, y \in A\}$ は両側イデアルとは限らない．）

問題 4.5. m を平方数でない整数とし，$A = \boldsymbol{Z}[\sqrt{m}]$ とする．A の部分群 $I = \{2x + \sqrt{m}y \mid x, y \in \boldsymbol{Z}\}$ と $J = \{2x + (1 + \sqrt{m})y \mid x, y \in \boldsymbol{Z}\}$ がイデアルか否かをそれぞれ判定せよ．必要なら m で場合分けせよ．

主に 4.3,4.4 節に関する問題

問題 4.6 (☆)**.** $I = (6), J = (10) \subset \boldsymbol{Z}$ とする．$I + J$，$I \cap J$，IJ，I^2 を求めよ（(n) の形で表せ）．

問題 4.7 (☆)**.** $I = (x^2), J = (x^2 - x) \subset \boldsymbol{R}[x]$ に対して，問題 4.6 と同じことを行え．

問題 4.8 (イデアルの根基)**.** A を可換環, $I \subset A$ をイデアルとする．$\sqrt{I} := \{a \in A \mid$ ある正整数 n に対し $a^n \in I\}$ を I の**根基** (*radical*) という．I などをイデアルとするとき次を示せ．

(1) $\sqrt{I}$ はイデアルであり，I を含む．
(2) $I' \subset I$ ならば $\sqrt{I'} \subset \sqrt{I}$.
(3) $\sqrt{\sqrt{I}} = \sqrt{I}$.
(4) 正整数 m に対し，$\sqrt{I^m} = \sqrt{I}$.
(5) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

とくに，零イデアル 0 の根基 $\sqrt{0} = \{a \in A \mid$ ある正整数 n に対し $a^n = 0\}$ を**冪零根基** (*nilradical*) という．なお，$\sqrt{I} = I$ を満たすイデアルを**根基イデアル** (*radical ideal*) という．

問題 4.9 (イデアル商)**.** A を可換環，$I, J \subset A$ をイデアルとする．$(I : J) := \{a \in A \mid aJ \subset I\}$ と定める．I などをイデアルとするとき次を示せ．

(1) $(I : J)$ はイデアルである．
(2) $I' \subset I$ ならば $(I' : J) \subset (I : J)$.
(3) $J' \subset J$ ならば $(I : J) \subset (I : J')$.
(4) $((I_1 \cap I_2) : J) = (I_1 : J) \cap (I_2 : J)$.
(5) $(I : (J_1 + J_2)) = (I : J_1) \cap (I : J_2)$.

$(I : J)$ は**イデアル商** (*ideal quotient*) とよばれるが，商と言う名前ではあるものの完全に積の逆演算になっているわけではないことには注意する．例えば，$J \subset (IJ : I)$ だが両辺は一般に一致しない．ちなみに「:」を

「÷」の意味で使う国もあるらしいですね.

問題 4.10. 可換環 A のイデアル I, J が $I + J = A$ を満たすとき，任意の正整数 n, m に対して $I^n + J^m = A$ であることを示せ.

問題 4.11. 可換環のイデアル I, J に対し，$(I \cap J)^2 \subset IJ \subset I \cap J$ が成り立つ.（したがって，冪乗の違いを無視できる文脈では，IJ と $I \cap J$ は同じように扱える.）

問題 4.12. （非可換な）環 $A = \mathrm{M}(2, \boldsymbol{R})$ を考える．A の部分集合 $\{a \in A \mid \text{ある正整数 } n \text{ に対し } a^n = 0\}$ は左イデアルでも右イデアルでもないことを示せ.（したがって，可換と限らない環においては，問題 4.8 のように根基を定めてもイデアルになるとは限らない.）

問題 4.13 (一部 5 節の内容も用いる)**.** $A = \boldsymbol{Z}[\sqrt{-5}]$ とし，写像 $\mathrm{Nm}\colon A \to \boldsymbol{N}$ を $\mathrm{Nm}(x + y\sqrt{-5}) = (x + y\sqrt{-5})\overline{(x + y\sqrt{-5})} = x^2 + 5y^2$ で定める.

(1) $a, b \in A$ に対し $\mathrm{Nm}(ab) = \mathrm{Nm}(a)\,\mathrm{Nm}(b)$ が成り立つことを示せ.
(2) $\mathrm{Nm}(a) = 1$ を満たす $a \in A$ は $a = \pm 1$ のみであることと，$\mathrm{Nm}(a) = 2, 3$ を満たす $a \in A$ は存在しないことを示せ.
(3) $a, b \in A$ が $ab \in \{2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}\}$ を満たすならば a と b の一方は ± 1 に等しいことを示せ.
(4) 例 4.26 で述べたイデアルの等式 $(3) = RS$ 等を示せ.
(5) I を P, Q, R, S のいずれかとし，それに応じて $n = 2, 2, 3, 3$ とする．$\boldsymbol{Z} \to A/I$ は全射であることを示し，その核はそれぞれ $n\boldsymbol{Z}$ であることを示せ．したがって準同型定理から $\boldsymbol{Z}/n\boldsymbol{Z} \cong A/I$ を得る.

5 環準同型とイデアル，剰余環

5.1 準同型によるイデアルの縮約と拡大

引き続き，「∗」は「左」「右」「両側」のいずれかとする.

命題 5.1. $f\colon A \to B$ を環準同型とする．$J \subset B$ が∗イデアルならば，その逆像 $f^{-1}(J) \subset A$ も∗イデアルである. ◊

略証. J は加法の部分群なので，その逆像 $f^{-1}(J)$ が部分群であることは [群論, 問題 5.13(1)] から分かる.

∗＝「左」の場合, $a \in A$ として「$x \in f^{-1}(J)$ ならば $ax \in f^{-1}(J)$」を示したいわけだが, 逆像の定義を使って言い換えると,「$f(x) \in J$ ならば $f(ax) \in J$」を示せばよいことにる．f が準同型なので $f(ax) = f(a)f(x)$ であり，J は左イデアルなので，$f(a) \in B$ と $f(x) \in J$ の積は J に属する．他の条件も同様. □

定義 5.2. この $f^{-1}(J)$ を∗イデアル J の A への**縮約** (*contraction*) または**制限**ともいう．これを $A \cap J$ とも書くことがある（A が B の部分環で f が包含写像ならば普通の記法だが，そうでない場合にも記号を濫用してこう書くことがある)．また，J^{c} と書くこともある. ◊

定義 5.3. A，B を環とする．$I \subset A$ が∗イデアルのとき，$f(I)$ が生成する B の∗イデアルを I の**拡大** (*extension*) という.

A，B が可換な場合は，これを $f(I)B$ または単に IB と書く．また，I^{e} と書くこともある. ◊

像 $f(I) \subset B$ は一般に$*$イデアルではないが，f が全射ならば$*$イデアルになる：

命題 5.4. $f\colon A \to B$ を環の準同型とし，$I \subset A$ を$*$イデアルとする．f が全射ならば，$f(I)$ は B の$*$イデアルである．◊

証明. $f(I)$ が加法の部分群なのは [群論, 問題 5.13(3)] から分かる．$*$＝「左」の場合，$x \in f(I)$ と $b \in B$ に対して $bx \in f(I)$ を言う必要がある．$f(I)$ の定義よりある $w \in I$ に対して $f(w) = x$ であり，また f が全射なのである $a \in A$ に対して $f(a) = b$ である．すると $bx = f(a)f(w) = f(aw)$ で，I が左イデアルで $w \in I$ なので $aw \in I$ であり，よって $bx \in f(I)$ である．他の場合も同様. □

注 5.5. 命題 5.4 において全射性の仮定は必須である．$f\colon A \to B$ を全射でない準同型とし，A の$*$イデアルとして A 自身を考えると，$f(A)$ は B の真部分集合で $f(1_A) = 1_B$ を含むので，$*$イデアルではない．◊

注 5.6. $I \subset A$ が族 $(a_\lambda)_{\lambda\in\Lambda}$ で生成されるとき，$f(I)B \subset B$ は $(f(a_\lambda))_{\lambda\in\Lambda}$ で生成される．とくに，I が有限生成ならば $f(I)B$ も有限生成であり，I が単項ならば $f(I)B$ も単項である．

イデアルの制限に関しては，このような簡単な表示はない．◊

縮約と拡大の関係について述べる．

命題 5.7. $f\colon A \to B$ を可換環の準同型とする．A のイデアル $I \subset A$ と B のイデアル $J \subset B$ に対して，$f(I)B \subset J$ と $I \subset f^{-1}(J)$ は同値である．別の記号で書くと，$I^{\mathrm{e}} \subset J$ と $I \subset J^{\mathrm{c}}$ は同値である．◊

証明. 集合の基本的な議論より，$I \subset f^{-1}(J)$ は $f(I) \subset J$ と同値である．$f(I)B$ は $f(I)$ を含む最小のイデアルなので，イデアルが $f(I)$ を含むことと $f(I)B$ を含むことは同値である. □

系 5.8. $f\colon A \to B$ を可換環の準同型とし，$I \subset A$ と $J \subset B$ をイデアルとすると，次が成り立つ．

(1) $I \subset f^{-1}(f(I)B)$ すなわち $I \subset I^{\mathrm{ec}}$ が成り立つ．
(2) $f(f^{-1}(J))B \subset J$ すなわち $J^{\mathrm{ce}} \subset J$ が成り立つ．
(3) $I^{\mathrm{e}} = I^{\mathrm{ece}}$ が成り立つ．
(4) $J^{\mathrm{c}} = J^{\mathrm{cec}}$ が成り立つ．◊

証明. (1), (2) 定義に戻って直接示すことも当然できる．命題 5.7 を $(I, J) = (I, I^{\mathrm{e}}), (J^{\mathrm{c}}, J)$ に適用しても示せる．

(3) (1) に $(-)^{\mathrm{e}}$ を適用して $I^{\mathrm{e}} \subset I^{\mathrm{ece}}$ を得る．(2) を $J = I^{\mathrm{e}}$ に適用して $I^{\mathrm{ece}} \subset I^{\mathrm{e}}$ を得る．

(4) 同様に (1), (2) をうまいこと適用する. □

注 5.9. 系 5.8 (1), (2) の 2 つの包含関係について，どちらも等号は一般に成立しない．

(1) が真の包含になる例については，問題 5.5 を見よ．
(2) が真の包含になる例については，問題 5.4 を見よ．◊

余談 5.10. 圏論に詳しいまたは興味がある人向けの説明：命題 5.7 は拡大と縮約が随伴関手であることに他ならず，系 5.8 は随伴関手の一般論から直ちに従う．◊

5.2 核

定義 5.11 (核)**.** 環準同型 $f\colon A \to B$ の**核** (*kernel*) とは，$f^{-1}(0) = \{a \in A \mid f(a) = 0\}$ である．これを $\mathrm{Ker}(f)$ と書く． ◊

環準同型の核は両側イデアルである．

命題 5.12. 環準同型 $f\colon A \to B$ の核 $\mathrm{Ker}(f)$ は両側イデアルである． ◊

証明. $\mathrm{Ker}(f)$ は両側イデアル $\{0\} \subset B$ の逆像なので，命題 5.1 から分かる． □

例 5.13. 射影 $\mathrm{pr}_1\colon A \times B \to A$ の核は $\{0\} \times B$ である． ◊

5.3 剰余環

イデアルの重要な性質として，イデアルで割って剰余環を考えることができる．

定義 5.14. A を環，$I \subset A$ を両側イデアルとする．I は加法に関して部分群なので剰余群 A/I が考えられるが，さらに乗法を $[a] \cdot [b] = [ab]$ で定めると well-defined であり，A/I はこの加法と乗法に関して環をなす．これを A の I による**商環** (*quotient ring*) または**剰余環** (*residue class ring*) とよぶ． ◊

$[a]$ のことを $a \bmod I$ や $a + I$ とも書く．また，$a - b \in I$ であることを $a \equiv b \pmod{I}$ とも書く．

乗法が well-defined であることを確認する．$a' - a \in I$ かつ $b' - b \in I$ のとき $a'b' - ab \in I$ であることを確認すればよい．$a' = a + i$，$b' = b + j$ とおくと $a'b' = ab + ib + aj + ij$ であり，$i, j \in I$ で I が両側イデアルなことから $ib + aj + ij \in I$ である．

well-defined であることが分かってしまえば，他の性質は次の意味で明らかである：例えば分配法則 $x(y + z) = xy + xz$ が $x, y, z \in A/I$ について成り立つことを示したいが，$x = [a], y = [b], z = [c]$ を満たす $a, b, c \in A$ をとることができ，$a(b + c)$ と $ab + ac$ は等しく，これらの元の $A \to A/I$ による像が示したい式の左辺と右辺である．

A が可換ならば A/I も可換である（証明は上の分配法則等と同様）．

注 5.15. $I \subset A$ を加法の部分群とするとき，この乗法が well-defined であることは，I が両側イデアルであることと同値である．というのは，well-defined だとしたら，$a \in A$ と $x \in I$ に対して，$[0] = [x]$ なので $[0] = [a \cdot 0] = [a \cdot x]$ となっているはずで，すなわち $a \cdot x \in I$ なので I は左イデアルであり，同様に右イデアルでもある． ◊

命題 5.16. A を環，I を両側イデアルとする．標準的射影 $A \to A/I$ は環準同型であり，全射であり，核は I である． ◊

証明. すべて定義より明らか． □

定理 5.17 (準同型定理)**.** $f\colon A \to B$ が環準同型ならば，A の剰余環 $A/\mathrm{Ker}\, f$ から B の部分環 $\mathrm{Im}\, f$ への準同型 $\bar{f}\colon A/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ が誘導される．$\bar{f}$ は同型である． ◊

証明. 像の定義より $f\colon A \to B$ は $f\colon A \to \operatorname{Im} f$ を誘導する．これを用いて $A/\operatorname{Ker} f$ からの写像を定めたいので，well-defined 性を確かめる．つまり $[a] = [a']$ ならば $f(a) = f(a')$ を確かめたい．$[a] = [a']$ とは $a - a' \in \operatorname{Ker} f$ ということなので，f が準同型であることから $f(a) = f(a - a') + f(a') = 0 + f(a') = f(a')$ である．

$\bar{f}$ が全単射であることを示す．全射性は像の定義から明らか．単射性については，$\bar{f}([a]) = \bar{f}([a'])$ と仮定すると，$f(a) = f(a')$ なので $a - a' \in \operatorname{Ker} f$ となり $[a] = [a']$ が分かる． □

なお，群の準同型定理と基本的に同じ証明です．

命題 5.18 (剰余環のイデアル，cf. [群論, 補題 7.7])**.** I を A の両側イデアルとし，$\pi\colon A \to A/I$ を自然な全射とする．π による像・逆像をとる写像

$$\{J \mid J \text{ は } A \text{ の} * \text{イデアルで } I \text{ を含む}\} \underset{\pi^{-1}(-)}{\overset{\pi(-)}{\rightleftarrows}} \{K \mid K \text{ は } A/I \text{ の} * \text{イデアル}\}$$

は互いに逆写像であり，したがって一対一対応を与える． ◊

証明. 【写像の行先がそれぞれの集合に入っていること】: A/I の$**$イデアルの逆像は$*$イデアルであり（命題 5.1），$\operatorname{Ker}(\pi) = I$ を含む．π が全射なので A の$*$イデアルの像は$*$イデアルである（命題 5.4）．

【互いに逆写像であること】: K が A/I の部分集合のとき，（π が全射なので）$\pi(\pi^{-1}(K)) = K$ である．J が A の部分集合のとき，$\pi^{-1}(\pi(J)) = J + I$ であり，J が I を含む部分群ならばこれは J に等しい． □

注 5.19. 可換環において I を含むイデアルが主に登場する命題は，しばしば，命題 5.18 を用いて A/I のイデアルの話に言い換えることで，$I = 0$ である場合に帰着できる． ◊

演習問題

主に 5.1 節に関する問題

問題 5.1 (☆イデアルの和・共通部分と縮約・拡大)**.** $f\colon A \to B$ を環の準同型とする．$I_1, I_2 \subset A$ を A のイデアルとし，$J_1, J_2 \subset B$ を B のイデアルとする．

(1) $(J_1 \cap A) + (J_2 \cap A) \subset (J_1 + J_2) \cap A$，$(J_1 \cap A) \cap (J_2 \cap A) = (J_1 \cap J_2) \cap A$ を示せ．
(2) A, B は可換とする．$I_1B + I_2B = (I_1 + I_2)B$，$I_1B \cap I_2B \supset (I_1 \cap I_2)B$ を示せ．

問題 5.2 (☆準同型の合成によるイデアルの縮約・拡大)**.** $f\colon A \to B$，$g\colon B \to C$ を環の準同型とする．合成 $g \circ f\colon A \to C$ も準同型である．

(1) C のイデアル J に対し，$A \cap (B \cap J) = A \cap J$ であることを示せ（右辺は $g \circ f$ による縮約である）．
(2) A，B，C は可換とする．A のイデアル I に対し，$(IB)C = IC$ であることを示せ（右辺は $g \circ f$ による拡大である）．

問題 5.3 (☆剰余環のイデアルの縮約の例)**.** $f\colon \boldsymbol{Z} \to B = \boldsymbol{Z}/36\boldsymbol{Z}$ を自然な射影とする．以下に述べる B のイデアルの縮約（f による逆像）を求めよ．(0)，(6)，(30)，(16)，(27)．

問題 5.4 (イデアルの縮約の拡大の例)**.** $f\colon \boldsymbol{Z} \to B = \boldsymbol{Z}[\sqrt{-1}]$ を包含写像とする．J が以下に述べる $\boldsymbol{Z}[\sqrt{-1}]$ のイデアルであるとき，J の縮約 $f^{-1}(J)$ を求めよ．また，その拡大 $f(f^{-1}(J))B$ が J に一致するか否かを

答えよ．(5)，$(2+\sqrt{-1})$，$(2+\sqrt{-1})^2$，$(1+\sqrt{-1})$，$(1+\sqrt{-1})^2$，$(1+\sqrt{-1})^3$.

問題 5.5 (☆イデアルの拡大の縮約の例 1)**.** $f\colon \boldsymbol{Z} \to B = \boldsymbol{Z}[\frac{1}{6}]$ を包含写像とする．I が以下に述べる $\boldsymbol{Z}$ のイデアルのとき，I の拡大の縮約 $f^{-1}(f(I)B)$ を求めよ．また，それが I に一致するか否かを答えよ．(7)，(8)，(9)，(10).

問題 5.6 (☆イデアルの拡大の縮約の例 2)**.** $f\colon \boldsymbol{Z} \to B = \boldsymbol{Z}/6\boldsymbol{Z}$ を自然な射影とするとき，問題 5.5 と同じ問に答えよ.

問題 5.7. 12 以下の各正整数 n に対して，環 $\boldsymbol{Z}/n\boldsymbol{Z}$ のイデアルをすべて挙げよ.

主に 5.3 節に関する問題

問題 5.8 (☆)**.** $I, J \subset A$ を環 A の両側イデアルとする．準同型 $f\colon A \to A/I \times A/J\colon a \mapsto ([a],[a])$ を考える（右辺は A/I と A/J の直積環）．$\operatorname{Ker} f = I \cap J$ を示せ.

問題 5.9 (☆)**.** $f\colon A \to B$ を環準同型とし，$J \subset B$ を両側イデアルとする．標準的射影 $\pi\colon B \to B/J$ と f の合成 $\pi \circ f\colon A \to B/J$ の核 $\operatorname{Ker}(\pi \circ f)$ は $f^{-1}(J)$ であることを示せ.

6 ユークリッド環

本節では環はすべて可換とする．（ただし，ユークリッド環の定義を適当に修正することで，非可換環の左イデアルまたは右イデアルについて定理 6.4 が成り立つようにできる．詳細は省略する.）

正整数 2 つの最大公約数を求める方法としてユークリッドの互除法がある：正整数 $a > b$ に対し，a を b で割った余りを c とすると，$\gcd\{a,b\} = \gcd\{b,c\}$ であり，これを繰り返して小さい数の場合に帰着し，最終的に 2 数の一方が他方を割りきるのでそれが最大公約数になる．ポイントは，「余り」が必ず「割る数」より「小さくなる」ことと，「操作がいつか終了する」ことである．この操作の性質を抽象化したのがユークリッド環であり，ユークリッド環においては（$\boldsymbol{Z}$ の場合と同様に）すべてのイデアルが単項イデアルであることが示せる.

定義 6.1. A が**ユークリッド環** (*Euclidean ring*) であるとは，次を満たす写像 $\phi\colon A \setminus \{0\} \to \boldsymbol{N}$ が存在することをいう.

条件：任意の $a, b \in A \setminus \{0\}$ に対し，ある $q \in A$ が存在し次の一方が成り立つ.

- $a - bq = 0$.
- $a - bq \neq 0$ かつ，$\phi(a-bq) < \phi(b)$.

ユークリッド環かつ整域（定義 7.13）であるとき**ユークリッド整域** (*Euclidean domain*) という． ◊

$a - bq = r$ とおくと，$a = bq + r$ であり，これは b による「余り付き割り算」で q が「商（quotient)」，r が「余り（remainder)」だと思える.

また，イデアルの等式 $(a,b) = (b,r)$ が成り立つことに注意する．($r = a - bq$ なので $r \in (a,b)$ であり，$a = bq + r$ なので $a \in (b,r)$ である.)

注 6.2. 定義には(あまり本質的でない)揺れがある．ϕ の定義域を A 全体にしたうえで, $\phi(a) = 0 \iff a = 0$ を課す流儀もある．また，ϕ の終域を一般の整列集合にしても，定理 6.4 は成立する．

ユークリッド整域のことをユークリッド環とよぶこともあるらしい．本節で紹介する例はすべて整域である． ◊

例 6.3. $\boldsymbol{Z}$ は $\phi(n) = |n|$ によりユークリッド整域になる．実際，$a \in \boldsymbol{Z}$ と $b \in \boldsymbol{Z} \setminus \{0\}$ に対し，q を $\frac{a}{b}$ の整数部分とすると，$b > 0$ のとき $0 \leq a - bq < b$ が成り立ち，$b < 0$ のとき $b < a - bq \leq 0$ が成り立つ．どちらにしても $a - bq = 0$ または $|a - bq| < |b|$ なのでこの q が条件を満たす．(a と b が両方正の場合，通常の正整数の余り付き割り算を行えば，余りは割る数より真に小さいということである.)

なお，$a - bq \neq 0$ の場合，上記の q の代わりに $q + 1$ をとっても条件を満たすので，q の一意性は成立しないが，このことはユークリッド環の文脈では重要でない． ◊

他の例は後で紹介する．

定理 6.4. A がユークリッド環ならば，A は単項イデアル環である（A の任意のイデアルは単項イデアルである).

A がユークリッド整域ならば，A は単項イデアル整域である． ◊

ユークリッドの互除法的議論を明示的に使う証明と，最小元の存在を使って一気に終着点に至るタイプの証明の 2 つを与える．

定理 6.4 の証明その 1（互除法的議論を明示的に行う方法）.

まず 2 元で生成されるイデアル $I = (a_1, a_2)$ を考え，これが単項イデアルであることを示す．$a_2 = 0$ ならば $I = (a_1)$ なのでよい．$a_2 \neq 0$ とする．ユークリッド環なので $a_1 - a_2 q_2 =: a_3$ で $a_3 = 0$ または $\phi(a_3) < \phi(a_2)$ を満たすものが存在する．$a_3 = 0$ ならば $I = (a_2)$ なのでよい．そうでないならば，$I = (a_2, a_3)$ かつ $a_3 \neq 0$ であり，ユークリッド環なので $a_2 - a_3 q_3 =: a_4$ で $a_4 = 0$ または $\phi(a_4) < \phi(a_3)$ を満たすものが存在する．これを繰り返すと，自然数の降下列 $\phi(a_2) > \phi(a_3) > \phi(a_4) > \dots$ が無限に続くことはないので，どこかで $a_k = 0$, $I = (a_{k-1})$ となる．(ユークリッド環の定義で ϕ の終域を一般の整列集合にした場合も，整列集合の元の無限降下列は存在しないことから同じ議論ができる.)

以下で使うためまとめ直すと，$a_2 \neq 0$ かつ $(a_1, a_2) \supsetneq (a_2)$ の場合に，$(a_1, a_2) = (a)$ かつ $\phi(a) < \phi(a_2)$ を満たす a が存在することを示した.

一般のイデアル I が単項イデアルであることを示す．$I = (0)$ ならばよい．そうでないとする．元 $b_0 \in I \setminus \{0\}$ をとる．$I = (b_0)$ ならばよい．そうでないならば, $c_1 \in I \setminus (b_0)$ をとり, 上記の方法で $(c_1, b_0) = (b_1)$ かつ $\phi(b_1) < \phi(b_0)$ を満たす b_1 をとる．これを繰り返すと, 上と同じ理由で降下列 $\phi(b_0) > \phi(b_1) > \phi(b_2) > \dots$ が無限に続くことはないので，どこかで $I = (b_k)$ となる.

有限個の元で生成されているイデアル $I = (c_1, c_2, \dots, c_n)$ については次のようにしてもよい：$d_1 = c_1$ とおく．$(d_1, c_2) = (d_2)$ なる d_2 が存在する．このとき $I = (d_2, c_3, \dots, c_n)$ である．$(d_2, c_3) = (d_3)$ なる d_3 が存在する．以下繰り返して $I = (d_n)$ を得る． □

定理 6.4 の証明その 2（いきなり終着点をとるタイプの議論）.

$I \subset A$ をイデアルとする．$I = (0)$ ならば単項イデアルである．以下 $I \supsetneq (0)$ と仮定する．$\phi\colon A \setminus \{0\} \to \boldsymbol{N}$ をユークリッド環の定義の条件を満たす写像とする．$\phi(I \setminus \{0\}) \subset \boldsymbol{N}$ は空でない部分集合である．その最小元を m とする．(ここでも，ϕ の終域が一般の整列集合だったとしても同じ議論ができる.) $\phi(b) = m$ となる

$b \in I \setminus \{0\}$ を 1 つとる．このとき $I = (b)$ であることを示そう．

$I \supset (b)$ は明らかなので $I \subset (b)$ を示す．$a \in I$ を任意にとる．$a = 0$ なら当然 $a \in (b)$ である．以下 $a \neq 0$ とする．ϕ の性質から，$q \in A$ が存在し，$a - bq = 0$ または，$a - bq \neq 0$ かつ $\phi(a - bq) < \phi(b)$ の一方が成り立つ．後者が成り立つと仮定すると，b が $\phi(I \setminus \{0\})$ の最小元だという仮定に反する．したがって前者が成り立つので，$a = bq \in (b)$ である． □

例 6.5 (8.3 節で詳しく述べる)**.** k を体とし，$k[x] = \{$ 変数 x に関する k 係数の多項式 $\}$ を 1 変数多項式環とする．$k[x]$ がユークリッド環であることを示したい．そのためにまずは多項式の次数を定義する．0 でない多項式 $F \in k[x]$ は $a_0 + a_1 x + \cdots + a_n x^n$，$n \geq 0$，$a_i \in k$，$a_n \neq 0$ の形に一意的に書ける．このとき n を F の**次数** (*degree*) といい，$\deg F$ で表す．

$k[x]$ は $\deg\colon k[x] \setminus \{0\} \to \boldsymbol{N}$ によりユークリッド環であることを示そう．$F, G \in k[x]$ で $G \neq 0$ とするとき，$F - GQ = 0$ または $\deg(F - GQ) < \deg G$ を満たす $Q \in k[x]$ が存在することを示す．$\deg F \geq \deg G$ であるとき，$F = a_0 + \cdots + a_n x^n$，$G = b_0 + \cdots + b_m x^m$ とおくと（$n - m \geq 0$ であり）$F_1 := F - (\frac{a_n}{b_m}) x^{n-m}$ は 0 であるかまたは $\deg F_1 \leq \deg F - 1$ を満たす．これを繰り返すことで求める Q を得られる．

ちなみに，$0 \in k[x]$ の次数は（定義しないままにする手もあるが，定義するなら）形式的に $\deg 0 = -\infty$ とするのが有力である．というのは，こう定めると，「$\deg(FG) = \deg F + \deg G$」と「$\deg(F) \leq n$ と，F が $\sum_{i=0}^{n} a_i x^i$ と書けることが同値」が成り立つので（ユークリッド環の文脈ではこの性質は必要ないが）． ◊

例 6.6. $m \in \{-1, -2\}$ のとき，$A = \boldsymbol{Z}[\sqrt{m}]$ はユークリッド環である．ノルム写像 $\mathrm{Nm}\colon A \to \boldsymbol{N}$ を $\mathrm{Nm}(x + y\sqrt{m}) = (x + y\sqrt{m})\overline{(x + y\sqrt{m})} = x^2 - my^2$ で定めるとき，この写像により A がユークリッド環の定義の条件を満たす（問題 6.1）．証明のポイントは，任意の複素数 $z \in \boldsymbol{C}$ に対しある $q \in A$ が存在して $|z - q| < 1$ を満たすことである．$m \leq -3$ のときはこれが成立しないので同様の議論は成り立たない．

ただし $m \equiv 1 \pmod 4$ に対しては A より少し大きい環 $\boldsymbol{Z}[\frac{1+\sqrt{m}}{2}]$ が自然に登場し，$m = -3, -7, -11$ ならばこれがユークリッド環になる（問題 6.2）． ◊

注 6.7. 定理 6.4 の逆は成り立たない．反例（単項イデアル環だがユークリッド環ではないもの）として $\boldsymbol{Z}[\frac{1+\sqrt{-19}}{2}]$ が有名だが，証明はそこそこ面倒なのでここでは行わない． ◊

演習問題

問題 6.1. m を平方数でない整数とし，$A = \boldsymbol{Z}[\sqrt{m}]$ とする．ノルム写像 $\mathrm{Nm}\colon A \to \boldsymbol{Z}$ を $\mathrm{Nm}(x + y\sqrt{m}) = (x + y\sqrt{m})\overline{(x + y\sqrt{m})} = x^2 - my^2$ で定める．また，$K = \boldsymbol{Q}[\sqrt{m}]$ とし，ノルム写像 $\mathrm{Nm}\colon K \to \boldsymbol{Q}$ を同じ式で定める．Nm は複素数としての絶対値の 2 乗に他ならない．

(1) $a, b \in K$ に対し $\mathrm{Nm}(ab) = \mathrm{Nm}(a)\,\mathrm{Nm}(b)$ が成り立つことを示せ．
(2) K は $\boldsymbol{C}$ の部分環であり，さらに 0 以外の元の逆元をとる操作で閉じていることを示せ．（すなわち，K は $\boldsymbol{C}$ の部分体である．）
(3) 以下では $m \in \{-1, -2\}$ とする．任意の複素数 $z \in \boldsymbol{C}$ に対しある $q \in A$ が存在して $|z - q| < 1$ を満たすことを示せ．
(4) A は Nm によりユークリッド環であることを示せ．（したがって A は単項イデアル環である．）

問題 6.2. m を平方数でない整数とし，$m \equiv 1 \pmod 4$ を満たすとする．$A = \boldsymbol{Z}[\sqrt{m}]$，$B = \boldsymbol{Z}[\frac{1+\sqrt{m}}{2}]$ と

する．

(1) $B = \{x + y\sqrt{m} \mid x, y \in \boldsymbol{Z}$，または，$x - \frac{1}{2}, y - \frac{1}{2} \in \boldsymbol{Z}\}$ であることを示せ．とくに，B は A を部分環として含む．
(2) ノルム写像 $\mathrm{Nm}\colon B \to \boldsymbol{Q}$ を問題 6.1 と同じ式で定めるとき，$\mathrm{Nm}(B) \subset \boldsymbol{Z}$ であることを示せ．
(3) 以下では $m \in \{-3, -7, -11\}$ とする．任意の複素数 $z \in \boldsymbol{C}$ に対しある $q \in B$ が存在して $|z - q| < 1$ を満たすことを示せ．
(4) B は Nm によりユークリッド環であることを示せ．（したがって B は単項イデアル環である．）

余談． なぜこのような B をわざわざ考えるのか疑問になるかもしれない．$m \equiv 1 \pmod 4$ かつ m が平方因子をもたない場合，B は $\boldsymbol{Q}[\sqrt{m}]$ での $\boldsymbol{Z}$ の整閉包とよばれるものになるため，実は A よりも B の方が自然な対象だと考えられる．

問題 6.3. 以下に述べるイデアル $I \subset A$ を単項イデアルとして表せ．なお，単項イデアルとしての表示は複数の可能性があるが，1 つ答えればよい．（ちなみに，A はどれもユークリッド環なのでユークリッドの互除法的議論を使えるが，使っても使わなくてもよい．）

(1) $A = \boldsymbol{Z}$，$I = (1961, 2516)$.
(2) $A = \boldsymbol{Z}[\sqrt{-1}]$，$I = (5, 4 - 2\sqrt{-1})$.
(3) $A = \boldsymbol{Z}[\sqrt{-1}]$，$I = (3 + 4\sqrt{-1}, 3 - 4\sqrt{-1})$.
(4) $A = \boldsymbol{Z}[\sqrt{-1}]$，$I = (8 + \sqrt{-1}, 7 + 4\sqrt{-1})$.
(5) $A = \boldsymbol{Z}[\sqrt{-1}]$，$I = (8 + \sqrt{-1}, 7 - 4\sqrt{-1})$.
(6) $A = \boldsymbol{R}[x]$，$I = (x^3 - x^2, x^3 - x)$.
(7) $A = \boldsymbol{R}[x]$，$I = (x^n - 1, x^m - 1)$，ただし n, m は正整数．必要なら $\gcd\{n, m\}$ で場合分けせよ．
(8) $A = \boldsymbol{R}[x]$，$I = (x^2 + 1, x - a)$，ただし $a \in \boldsymbol{R}$.
(9) $A = \boldsymbol{Z}$，$I = (x^n - 1, x^m - 1)$，ただし x, n, m は 2 以上の整数．必要なら $\gcd\{n, m\}$ で場合分けせよ．

7　単数・零因子，体・整域

本節では環はすべて可換とする．

7.1　単数，単数群

定義 7.1 (可逆元・単数，単数群)**.** 環の元が乗法の逆元をもつとき，その元は**可逆** (*invertible*) である，または**単数**，**単元** (*unit*) であるという．

単数全体は乗法に関して群をなす．これを環の**単数群** (*unit group*) という．環 A の単数群を A^* や $A^\times$ と表す． ◊

注 7.2. A が可換と限らない環のときは，左逆元と右逆元両方をもつ（このときそれらは一意であり一致する）元のことを可逆元とよび，このときも可逆元全体は群をなす． ◊

補題 7.3. $f\colon A \to B$ を環準同型とする．

(1) $a \in A^*$ ならば $f(a) \in B^*$ である．
(2) f の定義域を制限した写像 $f\colon A^* \to B^*$ は群準同型である． ◊

証明. $aa' = 1_A$ ならば $f(a)f(a') = f(aa') = f(1_A) = 1_B$ である．f は環準同型なので積を保つ． □

例 7.4. 任意の環 A において，1 はもちろん単数である．-1 も（$(-1)\cdot(-1) = 1$ なので）単数である．ただし -1 が 1 と異なるとは限らない．
$\boldsymbol{Z}$ の単数は ± 1 のみである． ◊

例 7.5. $m \in \boldsymbol{Z}$ を平方数でない整数とし，$A = \boldsymbol{Z}[\sqrt{m}]$ とする．$m < 0$ のとき，A^* は有限群である（これを求めることを問題 7.6 とする）．
$m > 0$ のとき，A^* は群として $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}$ に同型で，とくに無限群である．証明はそれなりに整数論を頑張る必要がある．$\boldsymbol{Z}[\sqrt{m}]$（$m > 0$）の ± 1 以外の（最も簡単な）単数の例をいくつか挙げると，$(2+\sqrt{5})(-2+\sqrt{5}) = 1$，$(8+3\sqrt{7})(8-3\sqrt{7}) = 1$，$(170+39\sqrt{19})(170-39\sqrt{19}) = 1$ などである． ◊

例 7.6. $\boldsymbol{Z}/n\boldsymbol{Z}$（$1 \le n \le 12$）の単数群の決定は問題 7.2（の一部）とする． ◊

7.2 零因子

$\boldsymbol{Z}$ や $\boldsymbol{C}[x]$ といった環では，0 でない 2 元の積が 0 になることはない．一般の環ではそういうこともありうる．

定義 7.7 (零因子)**.** A を環，$a \in A$ を元とする．a 倍写像 $A \to A\colon x \mapsto ax$ が単射であるとき，a を A の**正則元** (*regular element*) であるといい，そうでないとき，**零因子** (*zero divisor*) であるという． ◊

例 7.8. A が零環でなければ 0 は零因子である．（A が零環ならば 0 は零因子でない．）
$\boldsymbol{Z}$ や $\boldsymbol{C}$ や $\boldsymbol{C}[x]$ などでは 0 以外に零因子は存在しない．
$\boldsymbol{Z}/6\boldsymbol{Z}$ の元 $2, 3$ はそれぞれ 0 ではないが $2\cdot 3 = 0$ なので零因子である．$\boldsymbol{Z}/4\boldsymbol{Z}$ の元 2 は 0 でないが $2\cdot 2 = 0$ なので零因子である．$\boldsymbol{Z}/5\boldsymbol{Z}$ には 0 以外の零因子は存在しない． ◊

例 7.9. 零因子の倍数は明らかに零因子である．対偶をとると，正則元の約数は正則であることが分かる．
1 は正則元である．上より，単数は正則である． ◊

7.3 体・整域

体の定義を再掲する．

定義 7.10 (体)**.** 零環でなく，0 でない元がすべて可逆である環を**体** (*field*) であるという． ◊

命題 7.11. 環 A が零環であることと，A のイデアルがちょうど 1 つであることは同値である．環 A が体であることと，A のイデアルがちょうど 2 つであることは同値である． ◊

証明. A が零環のときイデアルは $A = (0)$ しかない．零環でないならば A と (0) は相異なるイデアルなのでイデアルは 2 つ以上ある．

A が体のとき，例 4.9 で見たように A のイデアルは (0) と A しかないので，イデアルはちょうど 2 つある．

環 A のイデアルがちょうど 2 つであると仮定する．A は零環ではない．(0) と A は明らかにイデアルであり，両者は相異なるので，イデアルはこの 2 つである．任意の $y \in A \setminus \{0\}$ に対し，y が生成する単項イデアル (y) は，(0) より真に大きいので A に一致する．したがって $1 \in (y)$ であり，すなわち $1 = xy$ となる $x \in A$ が存在する． □

命題 7.12. A が体で，B が零環でない環で，$f\colon A \to B$ が準同型のとき，f は単射である． ◊

証明. A のイデアル $\operatorname{Ker} f$ を考えると，$f(1_A) = 1_B \neq 0_B$ つまり $1_A \notin \operatorname{Ker} f$ なので $\operatorname{Ker} f$ は真のイデアルであり，A のイデアルは (0) と A しかないので $\operatorname{Ker} f = (0)$，すなわち f は単射である． □

定義 7.13 (整域)**.** 零環でない環 A が，条件「$a, b \in A$ が $ab = 0$ を満たすならば，$a = 0$ または $b = 0$」を満たすとき A は**整域** (*integral domain*)（または単に *domain*）であるという． ◊

命題 7.14. A を零環でない環とする．A が整域であることは，A が 0 以外の零因子をもたないことと同値である． ◊

証明. A が整域でないとすると，$a \neq 0, b \neq 0, ab = 0$ を満たす $a, b \in A$ が存在し，この a, b は 0 でない零因子である．

逆に A が 0 以外の零因子 a をもつとすると，零因子の定義より $b \neq 0, ab = 0$ を満たす $b \in A$ が存在し，この a, b が整域の定義の条件の反例になる． □

注 7.15. 整域と体の定義において零環は明示的に排除した．こうすることで，整域において「a が零因子 $\iff a = 0$」，体において「a が可逆でない $\iff a = 0$」という同値が成り立つ．

零環を整域に含めないことが自然である根拠の 1 つは命題 7.16 である． ◊

命題 7.16. 環 A について次は同値である．

(1) A は整域である．
(2) $n \geq 0$ を自然数とし，$a_1, a_2, \ldots, a_n \in A$ とする．$a_1 a_2 \ldots a_n = 0$ ならば，ある $1 \leq i \leq n$ に対して $a_i = 0$ である． ◊

証明. (2) の $n = 0, 2$ の場合の条件について検討する．$n = 0$ の場合の条件は，A が零環でないことと同値である（「$a_1 a_2 \ldots a_n = 0$」は，左辺は 1_A に等しいので，「$1_A = 0_A$」つまり A が零環であることと同値であり，また「ある $1 \leq i \leq n$ に対して $a_i = 0$ である」はつねに偽である）．

$n = 2$ のときは整域の定義に現れる条件「$ab = 0$ ならば $a = 0$ または $b = 0$」そのものである．

したがって，(1) は，(2) が $n = 0, 2$ で成り立つことと同値である．あとは，このとき一般の n に対しても成り立つことを示せばよい．

$n = 1$ の場合の条件はつねに成り立つ．$n \geq 2$ の場合を n に関する帰納法で示す．$n - 1$ での成立を仮定する．$a_1 a_2 \ldots a_n = 0$ ならば，まず $(a_1 a_2 \ldots a_{n-1}) a_n = 0$ なので $a_1 a_2 \ldots a_{n-1} = 0$ または $a_n = 0$ であり，前者の場合帰納法の仮定からある $1 \leq i \leq n - 1$ に対して $a_i = 0$ である． □

命題 7.17. 整域の部分環は整域である． ◊

証明は演習問題とする（問題 7.4）．

注 7.18. 体の部分環は（もちろん整域ではあるが）体とは限らない．例えば $\boldsymbol{Q}$ は体で $\boldsymbol{Z} \subset \boldsymbol{Q}$ は部分環だが体でない． ◊

例 7.19. A, B が零環でない環ならば，直積環 $A \times B$ は整域でない：$(1_A, 0_B)$ と $(0_A, 1_B)$ はどちらも $0_{A\times B} = (0_A, 0_B)$ とは異なるが積は 0 である． ◊

7.4 冪零元

定義 7.20 (冪零元)**.** 環 A の元 $a \in A$ について，$a^n = 0$ を満たす正整数 $n \in \boldsymbol{N}$ が存在するとき a は**冪零** (*nilpotent*) であるという． ◊

補題 7.21. 環の冪零元について次が成り立つ．

- 0 は冪零である．
- $a \neq 0$ が冪零ならば a は零因子である． ◊

証明. 0 が冪零なのは定義より明らか．

$a^n = 0$ を満たす $n \geq 1$ で最小のものをとると，（$a \neq 0$ なので）$n > 1$ である．すると最小性より $a^{n-1} \neq 0$ である．$a^{n-1} \neq 0$ かつ $a \cdot a^{n-1} = 0$ なので a は零因子である． □

注 7.22. 環 A に 0 以外の冪零元が存在すれば，（その元は 0 でない零因子なので，）A は整域でない．この逆は成り立たない：0 以外の冪零元が存在しないが整域でない環も存在する（例えば $\boldsymbol{Z}/6\boldsymbol{Z}$）． ◊

例 7.23. $\boldsymbol{Z}/8\boldsymbol{Z}$ の 2 は冪零であり，零因子である．

$\boldsymbol{Z}/6\boldsymbol{Z}$ の 2 や 3 は冪零でない零因子である．

$\boldsymbol{Z}/n\boldsymbol{Z}$（$1 \leq n \leq 12$）の冪零元や零因子の決定は問題 7.2（の一部）とする． ◊

定義 7.24. 環 A の冪零元全体の集合を $\sqrt{(0)}$ や単に $\sqrt{0}$，または $\operatorname{nil} A$ と表し，これを A の**冪零根基** (*nilradical*) という． ◊

命題 7.25. 冪零根基 $\sqrt{0}$ はイデアルである． ◊

証明は問題 4.8(1) を見よ．

7.5 同伴

定義 7.26. 環の 2 元 $a, b \in A$ が**同伴** (*associate*) であるとは，ある単数 $u \in A^*$ が存在して $a = ub$ となることをいう． ◊

これは同値関係である．証明は演習問題とする（問題 7.5）．

注 7.27. なお，定義 7.26 に現れる u は一意とは限らない．極端な例として，$a = b = 0$ ならば u として任意の単数をとれる．また $A = \boldsymbol{Z}/8\boldsymbol{Z}$ で $a = 2, b = 6$ ならば u として 3 と $7(= -1)$ がとれる． ◊

命題 7.28. A を整域，$a, b \in A$ を元とすると，次は同値である．

(1) a と b は同伴（定義 7.26）である．
(2) $(a) = (b)$ が成り立つ．
(3) a は b を割りきり，b は a を割りきる． ◊

証明. c が d を割りきることは $(d) \subset (c)$ と同値なので，(2) と (3) は同値である．
(1) から (2) や (3) が導けることも明らかである．（ここまでは，整域であることを使っておらず，一般の（可換）環で成り立つ．）
(3) を仮定して (1) を示す．まず $ax = 0$ の場合を考える．b は a で割りきれるので $b = 0$ であり，$b = 1 \cdot a$ なので同伴である．$a \neq 0$ とする．互いに割りきるので，ある $s \in A$ に対し $a = sb$ であり，ある $t \in A$ に対し $b = ta$ である．したがって $a = sb = sta$ すなわち $a(1 - st) = 0$ が分かり，A が整域で $a \neq 0$ なので $1 - st = 0$ すなわち $st = 1$ なので $s \in A^*$ である． □

注 7.29. A が整域でないとき，$(a) = (b)$ でも同伴とは限らない．例は問題 H.12 を見よ． ◊

演習問題

問題 7.1 (☆)**.** $n = 1, 2, \ldots, 12$ に対し，$\boldsymbol{Z}[\frac{1}{n}]$ の単数をすべて求めよ．

問題 7.2 (☆)**.** $n = 1, 2, \ldots, 12$ に対し，$\boldsymbol{Z}/n\boldsymbol{Z}$ の単数，零因子，冪零元をすべて求めよ．また，$\boldsymbol{Z}/n\boldsymbol{Z}$ が体か否か，整域か否かを答えよ．

問題 7.3 (☆)**.** A を環とする．$a \in A$ に対し，$m_a \colon A \to A \colon x \mapsto ax$ を a 倍写像とする．次を示せ．

(1) a が零因子であることは，m_a が単射でないことと同値である．
(2) a が単数であることは，m_a が全射であることと同値である．
(3) A が有限環（有限集合）ならば，a が零因子であることと単数でないことは同値である．

問題 7.4 (☆)**.** 整域の部分環は整域であることを示せ．

問題 7.5. 同伴関係（定義 7.26）は同値関係であることを示せ．

問題 7.6. m を負の整数とする．環 $\boldsymbol{Z}[\sqrt{m}]$ の単数をすべて求めよ．
余裕があれば，$m \equiv 1 \pmod 4$ の場合の環 $\boldsymbol{Z}[\frac{1+\sqrt{m}}{2}]$ の単数も求めてみよ．

問題 7.7. A 上の整除関係（「a は b を割りきる」という 2 項関係）は一般に順序関係でないことを示せ．整序関係は，A を同伴関係で割った商集合上の 2 項関係を定めることを示せ．この（商集合上の）2 項関係は順序関係か？

問題 7.8. $f \colon A \to B$ を環の準同型とし，単数群の方の準同型を区別のため記号を変えて $f^* \colon A^* \to B^*$ で表す．

(1) f が単射（resp. 全射, resp. 全単射）ならば f^* は単射（resp. 全射, resp. 全単射）か？
(2) f^* が単射（resp. 全射, resp. 全単射）ならば f は単射（resp. 全射, resp. 全単射）か？

8 多項式環

本節では環はすべて可換とする．

8.1 環上の代数

例えば $\boldsymbol{C}$ から $\boldsymbol{C}$ への環準同型はたくさんあり，それゆえ多項式環 $\boldsymbol{C}[X]$ から $\boldsymbol{C}[Y]$ への準同型もたくさんある．とはいえ，$\boldsymbol{C}$ の部分では id になっている準同型のみを考えたい場面も多い．以下に定義する A 代数としての準同型（$A = \boldsymbol{C}$ として適用する）とはそのようなものである．

定義 8.1 (環上の代数とその準同型)**.** A, B を（可換）環とし，$f\colon A \to B$ を準同型とする．このとき (B, f) は A 上の代数または A **代数** (A-*algebra*) であるという．

$(B_1, f_1), (B_2, f_2)$ が A 代数のとき，写像 $\phi\colon B_1 \to B_2$ が A 代数の**準同型** (*homomorphism*) であるとは，次の 2 条件を満たすことをいう．

- ϕ は環準同型である．
- $f_2 = \phi \circ f_1$ が成り立つ． ◊

ほとんどの場合，f が何であるかは文脈から明らかなので，単に B を A 代数とよぶ．

例 8.2. 自明な例として，A 自身を（$\mathrm{id}\colon A \to A$ により）A 代数とみなせる． ◊

定義 8.3 (有限生成代数)**.** B を A 代数とする．有限個の元 $b_1, \ldots, b_n$ が存在して B が A の像と $b_1, \ldots, b_n$ で生成されるとき，B は**有限生成** (*finitely generated*) な A 代数であるという．このことは，A 上の（多変数）多項式環からの全射準同型が存在することと同値である（問題 8.7）． ◊

例 8.4. $\boldsymbol{Z}[\sqrt{m}]$，$\boldsymbol{Z}[\frac{1}{m}]$，$\boldsymbol{Z}/m\boldsymbol{Z}$ は有限生成 $\boldsymbol{Z}$ 代数である（n としてそれぞれ $1, 1, 0$ をとれる）．

$\boldsymbol{Q}$ や $\boldsymbol{R}$ は $\boldsymbol{Z}$ 代数として有限生成でない．このことの証明は演習問題とする（問題 8.1）． ◊

注 8.5. 任意の環 A に対し，$\boldsymbol{Z}$ から A への環準同型はただ一つ存在する（例 3.20）ので，任意の環は一意的な方法で $\boldsymbol{Z}$ 代数とみなせる．同じ理由で，$\boldsymbol{Z}$ 代数の間の準同型は環の準同型と同じ概念である．したがって，環と $\boldsymbol{Z}$ 代数は同じ概念である． ◊

8.2 直和加群と，多項式環の形式的な定義

加群（アーベル群）の直積と直和について復習する．

定義 8.6. $(M_i)_{i \in I}$ を加群の族とする．

直積集合 $\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i\}$ に，加法を成分ごとに定義すると加群になる．これを (M_i) の**直積加群** (*direct product*) という．

(M_i) の**直和加群** (*direct sum*) $\bigoplus_{i \in I} M_i$ とは，直積加群の部分加群

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

である（この部分集合が部分加群になることは簡単に確かめられる）. ◊

ちなみに A 節で一般の環 A 上の加群を定義するが，A 加群の直積・直和も同様に定義できる（アーベル群としては同じ構成を行い，A の元によるスカラー倍は成分ごとにスカラー倍することで定める）.

注 8.7. M_i は互いに異ならなくてもよい．極端な場合として，同じ加群（のコピー）をたくさん並べて直積または直和を考えることもできる．同じ加群 M の直積は M^I，直和は $M^{\oplus I}$ と書くこともある. ◊

注 8.8. I が有限集合ならば，直和加群は直積加群と一致する．一般には一致しない. ◊

定義 8.9 (多項式環の形式的な定義)**.** A を環とする．$\boldsymbol{N} = \{0, 1, \dots\}$ で添字づけられた，可算無限個のアーベル群 A の直和 R を考える．すなわち

$$R = \{(a_n)_{n\in\boldsymbol{N}} \mid \text{有限個の } n \text{ を除き } a_n = 0\}$$

である．このアーベル群に，乗法を次のように定義する：

$$(a_n)\cdot(b_n) = (c_n), \qquad c_n := \sum_{k,l\in\boldsymbol{N},\ k+l=n} a_k b_l.$$

すると (c_n) も直和加群 R の元になり，この乗法が結合法則を満たすことが確かめられる．証明は演習問題とする（問題 8.4）． R はその他の条件も満たし環になることが確かめられる.

第 n 成分が 1 で他の成分が 0 である R の元を X^n と書くことにする．$X^n \cdot X^m = x^{n+m}$ が成り立つ．また，A の元 a を第 0 成分が a で他が 0 である R の元と同一視する．R の元 $(a_0, a_1, \dots, a_d, 0, 0, \dots)$ は $a_0 + a_1X + a_2X^2 + \cdots + a_dX^d$ に等しい．この R を A 上の（1 変数）**多項式環** (*polynomial ring*) といい $A[X]$ と表す．$1_R = 1_A = X^0$ である.

X のことを**不定元** (*indeterminate*) とよぶこともある．これを他の文字で書いても差し支えない．多項式環上の多項式環を考える場合などは，むしろ別々の文字を使って区別する方がよい. ◊

帰納的に m 変数多項式環を定義する（$A[X_1, \dots, X_m] := A[X_1, \dots, X_{m-1}][X_m]$）．または，直和の添字および環の定義で $\boldsymbol{N}$ の代わりに直積 $\boldsymbol{N}^m$ を用いることで m 変数多項式環 $A[X_1, X_2, \dots, X_m]$ を定義する.

命題 8.10. A が整域ならば，$A[X]$ も整域で，$A[X]^* = A^*$ が成り立つ. ◊

証明. 証明は演習問題とする（問題 8.6）. □

実のところ A が可換と仮定しなくても多項式環 $A[X]$ を定義できるが，代入写像を考えるときに注意が必要になる．可換と限らない環上の多項式環の中心については次が成り立つ.

命題 8.11. A を（可換と限らない）環とする．$A[X]$ の中心に関して，$\mathrm{Z}(A[X]) = \mathrm{Z}(A)[X]$ が成り立つ. ◊

証明は演習問題とする（問題 8.5）.

8.3 多項式の次数

例 6.5 と一部重複する.

定義 8.12. A を可換環とし，$F \in A[X] \setminus \{0\}$ とする．F は $a_0 + a_1X + \cdots + a_nX^n$, $n \geq 0$, $a_i \in A$, $a_n \neq 0$ の形に一意的に書ける．このとき n を F の**次数** (*degree*) といい，$\deg F$ で表す．また a_nX^n を F の**最高次**

項 (*highest term*) という．a_n を F の最高次係数という．

最高次係数が 1 である多項式を**モニック** (*monic*) な多項式であるという．

$0 \in A[X]$ の次数は $-\infty$ とする．0 の最高次項や最高次係数は考えない． ◊

deg は $A[X]$ から $\boldsymbol{N} \cup \{-\infty\}$ への写像である．$\boldsymbol{N} \cup \{-\infty\}$ 上の加法および大小関係は自然に定義する．

注 8.13. $0 \in A[X]$ の次数はあえて定義しないという流儀もありうる．定義する場合，補題 8.15 や補題 8.17 を成り立たせようとすると $-\infty$ （という名前にするかは別として，加法と順序に関してそのように振る舞う元）にせざるを得ない． ◊

余談 8.14. 多項式を $\mathbb{P}^1 := A \cup \{\infty\}$ 上の有理型関数（cf. 複素解析学）とみなすと，多項式の次数とは有理型関数としての点 ∞ での極の位数に一致する． ◊

補題 8.15. n を整数とする．$A[X]$ の元 F に対して，$F = \sum_{i=0}^{n} a_i X^i$ と書けることと，$\deg F \leq n$ は同値である． ◊

証明. （0 の次数の定義も含めて考えると）明らか. □

注 8.16. 多項式の次数を次のように定義することもできる（定義 8.12 と一致する）．「F の次数が n 以下である」ことを補題 8.15 の条件で定める．「F の次数が n 以下である」が成り立ち，「F の次数が $n-1$ 以下である」が成り立たないときに，F の次数は（ちょうど）n であると定める．任意の整数 n に対して「F の次数が n 以下である」が成り立つとき，F の次数は $-\infty$ であると定める． ◊

補題 8.17. $F, G \in A[X]$ に対し，$\deg(FG) \leq \deg(F) + \deg(G)$ が成り立つ．A が整域であるか，または F と G の一方がモニックならば，等号が成り立つ． ◊

証明. F と G のどちらかが 0 のときの成立は明らか（等号についての主張も含めて）．以下，どちらも 0 でないとする．

$F = a_0 + a_1 X + \cdots + a_n X^n$，$G = b_0 + b_1 X + \cdots + b_m X^m$，$a_n \neq 0$，$b_m \neq 0$ とおくと，$FG = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \cdots + a_n b_m X^{n+m}$ で $n+m$ より高い項はないので，FG の次数は $n+m = \deg F + \deg G$ 以下である．

$a_n b_m \neq 0$ ならば等号が成り立つが，一般の環では $a_n \neq 0, b_m \neq 0$ であっても $a_n b_m \neq 0$ とは限らない．A が整域であるか，a_n と b_m のどちらかが 1 ならば $a_n b_m \neq 0$ が成り立つ. □

多項式の和の次数については次が成り立つ．

補題 8.18. $F, G \in A[X]$ に対し，$\deg(F+G) \leq \max\{\deg(F), \deg(G)\}$ が成り立つ． ◊

証明は，補題 8.15 の言い換えを使うのが簡単である．

8.4 代入写像と因数定理

B を A 代数とし（つまり $\phi_0 \colon A \to B$ を可換環の準同型とし），$b \in B$ を元とする．このとき，写像 $\phi \colon A[X] \to B$ を $\phi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \phi_0(a_i) b^i$ で定めると環準同型である（そうなるように $A[X]$ の演算は定めてあるので，ただし B の可換性は使っている）．さらに A 代数の準同型である．この写像を代入写像とよび，代入写像による像をとることを，X に b を**代入** (*substitute*) する，という．

命題 8.19. B を A 代数とする．写像

$$\{\phi\colon A[X] \to B \mid \phi \text{ は } A \text{ 代数の準同型 }\} \to B$$

を $\phi \mapsto \phi(X)$ で定めると，全単射である． ◊

証明. 全射性は代入写像の存在から明らかである．単射性について考える．ϕ, ψ が左辺の元で，$\phi(X) = \psi(X)$ が成り立つとすると，$A[X]$ の部分集合 $\{t \in A[X] \mid \phi(t) = \psi(t)\}$ は問題 3.4 より $A[X]$ の部分環であり，A と X を含むことから，$A[X]$ 全体に一致する． □

n 変数版である次の命題も同様に示せる（または，命題 8.19 を n 回適用してもよい）．

命題 8.20. B を A 代数とする．写像

$$\{\phi\colon A[X_1, \dots, X_n] \to B \mid \phi \text{ は } A \text{ 代数の準同型 }\} \to B^n$$

を $\phi \mapsto (\phi(X_1), \dots, \phi(X_n))$ で定めると，全単射である． ◊

$\phi\colon A[X_1, \dots, X_n] \to B$ を A 代数の準同型とするとき，$\phi(X_i)$ のことを x_i と書くことがあり，ϕ の像がなす B の部分環は $A[x_1, \dots, x_n] \subset B$ と表される（単に $A[X_1, \dots, X_n] \subset B$ と書くこともある）．

命題 8.19 においてとくに $B = A$（で $\phi_0 = \mathrm{id}_A$）の場合を考えると，$\phi\colon A[X] \to A$ は X にある元 $a \in A$ を代入する写像である．その核は因数定理（命題 8.23）で記述される．

命題 8.21. $F, G \in A[X]$ とし，G はモニックとする．このとき $Q \in A[X]$ で $\deg(F - GQ) < \deg G$ を満たすものが一意に存在する． ◊

証明. まず存在を示す．$\deg F < \deg G$ ならば $Q = 0$ とすればよい．$\deg F = n > \deg G = m$ だとすると，$F = a_0 + a_1 X + \cdots + a_n X^n$，$G = b_0 + b_1 X + \cdots + b_m X^m$ とおくとき $a_n \neq 0$，$b_m = 1$ である．$Q_1 = a_n X^{n-m}$ とおくと，$F - Q_1 G$ は n 次以下であり，n 次の係数が消えるので $n - 1$ 次以下である．これを繰り返すことで最終的に $\deg(F - G(Q_1 + \cdots + Q_k)) < \deg G$ を得る．

一意性：Q_1 と Q_2 が条件を満たしたとすると，$(Q_1 - Q_2)G = (F - GQ_2) - (F - GQ_1)$ の次数は補題 8.15 より $\deg G - 1$ 以下である．補題 8.17 より，$Q_1 - Q_2 = 0$ である． □

系 8.22. k が体ならば，$k[X]$ はユークリッド整域である． ◊

証明. 写像 $\deg\colon k[X] \setminus \{0\} \to \boldsymbol{N}$ がユークリッド環（定義 6.1）の条件を満たすことを示す．$F, G \in k[X]$ で $G \neq 0$ だとする．$G = b_0 + b_1 X + \cdots + b_m X^m$，$b_m \neq 0$ と書ける．F と $b_m^{-1} G$ に対して命題 8.21 を用いることで，$\deg(F - GQ) < \deg G$ を満たす $Q \in k[X]$ が存在することが分かる． □

命題 8.23 (因数定理)**.** A を可換環，$a \in A$ を元とし，$\phi\colon A[X] \to A$ を X に a を代入する写像とする．このとき $\mathrm{Ker}\,\phi = (X - a)$ である．すなわち，a を代入して 0 になることと $X - a$ で割りきれることは同値である． ◊

証明. $(X - a) \subset \mathrm{Ker}\,\phi$ は明らかである．逆向きの包含関係を示す．すなわち，$F \in A[X]$ が $F(a) = 0$ を満たすときに F が $X - a$ の倍数であることを示す．命題 8.21 より，$Q \in A[X]$ で $\deg(F - (X - a)Q) < \deg(X - a) = 1$ を満たすものが存在する．このとき $F - (X - a)Q = b \in A$ である（右辺は定数項しかない多項式）．X に a を代入することで $b = 0$ を得る．すなわち $F = (X - a)Q$ である． □

系 8.24. A を整域とし，$F \in A[X] \setminus \{0\}$ とする．このとき集合 $\{a \in A \mid F(a) = 0\}$ の元の個数は $\deg F$ 以下である．とくに，有限集合である． ◊

証明. 背理法で示す．$\deg F = n$ で，相異なる $n+1$ 個の元 $a_1, \ldots, a_{n+1} \in A$ が $F(a_i) = 0$ を満たすと仮定して矛盾を導く．命題 8.23 より，$F(X) = (X - a_1)F_1(X)$ を満たす $F_1 \in A[X]$ が存在し，補題 8.17 より $\deg F_1 = \deg F - 1$ である．このとき各 $2 \leq i \leq n+1$ に対し $F_1(a_i) = 0$ である．というのは，$F(X) = (X - a_1)F_1(X)$ に $X = a_i$ を代入して $0 = F(a_i) = (a_i - a_1)F_1(a_i)$ であり，$a_i - a_1 \neq 0$ なので A が整域であることから $F_1(a_i) = 0$ である．F_1 と a_2 に対し同じ議論を行い，繰り返すことで，$F(X) = (X - a_1)(X - a_2)\ldots(X - a_n)F_n(X)$，$F_n(a_{n+1}) = 0$，$\deg F_n = \deg F - n$ を満たす F_n を得る．しかし $\deg F_n = \deg F - n = 0$，すなわち F_n は定数でありしかも 0 でないので，$F_n(a_{n+1}) \neq 0$ となり，矛盾である． □

注 8.25. 整域でないほとんどの環 A において，系 8.24 は（モニックという条件を加えても）成立しない．具体例としては，$A = \boldsymbol{Z}/8\boldsymbol{Z}$ において $X^2 - 1 = 0$ や $X^3 = 0$ の解は 4 つ存在する．また，$A = \boldsymbol{Z}/6\boldsymbol{Z}$ において $X^2 - X = 0$ の解は 4 つ存在する． ◊

注 8.26. 非可換環だと，斜体であっても系 8.24 は一般に成り立たない．例えば Hamilton の四元数環 $\mathbf{H}$（例 2.16）は斜体だが，$X^2 + 1 = 0$ の解は $X = \pm i, \pm j, \pm k$ をはじめ無限個ある．系 8.24 の証明は，代入写像が環準同型でない時点で破綻する． ◊

注 8.27. $F \in A[X]$ と $a \in A$ と非負整数 $m \in \boldsymbol{N}$ に対し，F が $(X - a)^m$ で割りきれるとき a は F の重複度 m 以上の解とよぶことにする．また，重複度 m 以上の解であり重複度 $m+1$ 以上の解ではないとき，重複度（ちょうど）m の解とよぶことにする．

このとき，系 8.24 の重複度つきバージョンが成り立つ：$F \in A[X] \setminus \{0\}$ の解の重複度の和は $\deg F$ 以下である．証明は同様である． ◊

系 8.28. A が有限体ならば，A の単数群 A^* は有限巡回群である． ◊

証明. [群論, 命題 8.19] より，有限群が巡回群であるためには，任意の整数 n に対して，位数が n を割りきる元が n 個以下ならばよい．A 係数多項式 $X^n - 1 \in A[X]$ に系 8.24 を適用することで，この条件が成立することが分かる． □

系 8.29. p を素数とすると，法 p の原始根が存在する． ◊

ただし法 p の**原始根** (*primitive root*) とは，p と互いに素な素数 a で，$0 < i < p-1$ ならば $a^i \not\equiv 1 \pmod{p}$ を満たすものである．

証明. a が法 p の原始根であることと，$[a] \in \boldsymbol{Z}/p\boldsymbol{Z}$ が $(\boldsymbol{Z}/p\boldsymbol{Z})^*$ の生成元であることは同値である．p は素数なので $\boldsymbol{Z}/p\boldsymbol{Z}$ は有限体であり，系 8.28 を適用できる． □

8.5 多変数の多項式環

命題 8.10 を繰り返し用いることで次が示せる．

命題 8.30. A が整域ならば，$A[X_1, \ldots, X_n]$ も整域で，$A[X_1, \ldots, X_n]^* = A^*$ が成り立つ． ◊

多変数多項式にも次数が定義できる．

定義 8.31. $F \in A[X_1, \dots, X_m] \setminus \{0\}$ は $a_{i_1,\dots,i_m} X_1^{i_1} \dots X_m^{i^m}$ の形の項有限個の和で書ける．それらの項のうち，$a_{i_1,\dots,i_m} \neq 0$ を満たすもののみを考えて，その中での $i_1 + \dots + i_m$ の最大値を F の**次数** (*degree*) といい，$\deg F$ で表す．$\deg 0 = -\infty$ と定める． ◊

補題 8.17，8.18 と同様に次が示せる．

補題 8.32. $F, G \in A[X_1, \dots, X_m]$ とする．

(1) $\deg(FG) \leq \deg(F) + \deg(G)$ が成り立つ．A が整域ならば，等号が成り立つ．
(2) $\deg(F+G) \leq \max\{\deg(F), \deg(G)\}$ が成り立つ． ◊

なお，これとは別に，特定の変数だけについて考えた次数が有効な場面もある．それと区別したい場合は定義 8.31 の次数のことを**全次数** (*total degree*) とよぶこともある．

体上の 1 変数多項式環の場合（命題 8.21）のように剰余をとることは，多変数の場合一般にはできない．

体上の 1 変数多項式環がユークリッド整域でありしたがって単項イデアル整域であることの証明には，剰余をとる操作を利用していた．変数が 2 つ以上ある場合はこれらは成り立たない．単項イデアルでないイデアルはいくらでもある．

例 8.33. k を体とする．$\mathfrak{m} = (X, Y) \subset A = k[X, Y]$ は単項イデアルでない．もし $\mathfrak{m} = (f)$ と表せたとすると，$A/\mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2 \colon a \mapsto af$ が $A/\mathfrak{m} = k$ 上の代数の全射準同型になり，とくに k 上のベクトル空間の全射線形写像になるが，$\dim_k A/\mathfrak{m} = 1 < \dim_k \mathfrak{m}/\mathfrak{m}^2 = 2$ なので矛盾する．

$\mathfrak{m}^n = (X^n, X^{n-1}Y, \dots, XY^{n-1}, Y^n)$ は生成するのに $n+1$ 個の元を必要とする（証明は略）． ◊

なお，素朴な意味での剰余をとる操作はないが，それに近いことを行う**グレブナー基底** (*Gröbner basis*) の理論がある．

一方で，体上の多変数多項式環は素元分解整域（UFD）にはなる（9.3 節）．

演習問題

問題 8.1. $\boldsymbol{Q}$ や $\boldsymbol{R}$ は $\boldsymbol{Z}$ 代数として有限生成でないことを示せ．（なお，有限生成代数の部分代数は有限生成とは限らないので，$\boldsymbol{Q}$ と $\boldsymbol{R}$ は別個に示す必要がある．）

問題 8.2 (【難しい】)**.** $A \subset B_1 \subset B_2$ を満たす整域 A, B_1, B_2 で，B_1 は A 代数として有限生成でなく，B_2 は A 代数として有限生成なものの例を挙げよ．

問題 8.3. $(M_i)_{i \in I}$ を加群の族とし，N を加群とする．加群 P から Q への準同型全体の集合を $\mathrm{Hom}(P, Q)$ で表す．

(1) $\mathrm{Hom}(N, \prod_{i \in I} M_i) \to \prod_{i \in I} \mathrm{Hom}(N, M_i) \colon f \mapsto (\pi_i \circ f)_{i \in I}$ は全単射であることを示せ．ただし $\pi_i \colon \prod_{i \in I} M_i \to M_i$ は自然な射影（第 i 成分のみをとりだす）を表す．
(2) $\mathrm{Hom}(\bigoplus_{i \in I} M_i, N) \to \prod_{i \in I} \mathrm{Hom}(M_i, N) \colon f \mapsto (f \circ \iota_i)_{i \in I}$ は全単射であることを示せ．ただし $\iota_i \colon M_i \to \bigoplus_{i \in I} M_i$ は自然な包含写像（元 m を，第 i 成分のみが m で他の成分が 0 である元にうつす）を表す．

問題 8.4 (☆)**.** 定義 8.9 で定めた積 (c_n) が R の元であることを確かめよ．また，乗法の結合法則が成り立つことを確かめよ．

問題 8.5. A を（可換と限らない）環とする．$A[X]$ の中心に関して，$\mathrm{Z}(A[X]) = \mathrm{Z}(A)[X]$ が成り立つことを示せ．

問題 8.6 (☆)**.** A が整域ならば，$A[X]$ も整域で，$A[X]^* = A^*$ が成り立つことを示せ．

問題 8.7. A を環とする．A 代数 B が有限生成 A 代数であることと，ある $n \geq 0$ に対して A 代数の全射準同型 $A[X_1, \ldots, X_n] \to B$ が存在することは同値であることを示せ．

問題 8.8. k を体とする．$k[X,Y]$ のイデアルを次で定める：$I_1 = (XY)$, $I_2 = (XY, Y^2)$, $I_3 = (X^2, XY, Y^2)$. $k[X,Y]/I_j$ の零因子，冪零元をすべて求めよ．

問題 8.9. k を体とする．以下の各 f に対して，$\mathrm{Ker}\, f = I$ を示し，また f が全射か否か判定せよ．

(1) $f\colon \boldsymbol{R}[X] \to \boldsymbol{C}\colon X \mapsto \sqrt{-1}$，$I = (X^2+1)$.
(2) $f\colon k[X,Y] \to k[T]\colon X \mapsto T^2 - 1, Y \mapsto T^3 - T$，$I = (Y^2 - X^3 - X^2)$.
(3) $f\colon k[X,Y] \to k[T]\colon X \mapsto T^2, Y \mapsto T^3$，$I = (Y^2 - X^3)$.
(4) $f\colon k[X,Y,Z] \to k[S,T]\colon X \mapsto S^n, Y \mapsto T^n, Z \mapsto ST$，$I = (Z^n - XY)$．ただし n は 1 以上の整数.
(5) $f\colon k[X_0, X_1, X_2, X_3] \to k[S,T]\colon X_i \mapsto S^i T^{3-i}$，$I = (X_1^2 - X_0X_2, X_1X_2 - X_0X_3, X_2^2 - X_1X_3)$.

問題 8.10. A を整域とし，$f \in A[X_1, \ldots, X_n]$ を多項式とする．$S_1, \ldots, S_n$ を A の無限部分集合とする．任意の $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ に対して $f(s_1, \ldots, s_n) = 0$ ならば，$f = 0$ であることを示せ．

9 素元・既約元，素元分解整域

本節では環はすべて可換とする． さらに，整域のみを考える．

9.1 素元・既約元

$\boldsymbol{Z}$ における「素数（の ± 1 倍）」という概念を一般の環で考えたい．一般化する方法が少なくとも 4 つある．2 つをここで紹介し，10.1 節でもう 2 つ紹介する．

定義 9.1 (素元)**.** A は整域で，$a \in A$ は零でも単数でもないとする．a が条件「$x, y \in A$ で，xy が a で割りきれるならば，x または y の少なくとも一方は a で割りきれる」を満たすとき a は**素元** (*prime element*) であるという． ◊

定義 9.2 (既約元)**.** A は整域で，$a \in A$ は零でも単数でもないとする．a が条件「$x, y \in A$ で，$xy = a$ ならば，x または y の少なくとも一方は単数である」を満たすとき a は**既約元** (*irreducible element*) であるという． ◊

例 9.3. 素元（resp. 既約元）に同伴な元もまた素元（resp. 既約元）である． ◊

例 9.4. $A = \boldsymbol{Z}$ のとき，素元と既約元のどちらも「通常の素数の ± 1 倍」と同値である． ◊

命題 9.5. 整域において，素元は既約元である． ◊

証明. a を素元として，$a = xy$ だとする．xy は a の倍数で a は素元なので x と y のどちらかは a の倍数である．一般性を失わず x は a の倍数だとしてよい．$x = aw$ と書くと $a = xy = awy$ なので $a(1 - wy) = 0$ であり，A は整域で $a \neq 0$ なので $1 - wy = 0$ であり y は単数である． □

例 9.6. $A = \boldsymbol{Z}[\sqrt{-5}]$ のとき，$2, 3, 1 \pm \sqrt{-5}$ はどれも既約元だが（問題 4.13(3)），これらのどの 2 つも同伴でないことと，等式 $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ より，これらの元は素元ではないことが分かる．詳しい証明は問題 9.3(1) とする． ◊

注 9.7. $a \in A \setminus \{0\}$ に対して，a が素元であることは (a) が後述の素イデアル（定義 10.1）であることと同値である（問題 10.3）． ◊

9.2 素元分解整域

$\boldsymbol{Z}$ において素因数分解とその一意性が成り立つ：0 以外の整数は有限個の素数と ± 1 の積で書けて，また書き方は順番を除いて一意である（素数に負のものも含める場合は，符号も除けば一意である）．一般の環ではこれは成り立たないが，これが成り立つのが素元分解整域である：

定義 9.8. 整域 A が**素元分解整域**または**一意分解整域** (*unique factorization domain*)，略して UFD であるとは，任意の元 $a \in A \setminus \{0\}$ が有限個（m 個，$m \geq 0$）の素元 $p_1, \ldots, p_m$ と単数 u の積に書けることをいう：$a = up_1p_2 \ldots p_m$. ◊

補題 9.9. 素元 p が素元 q を割りきるならば p と q は同伴である． ◊

証明. $q = ap$ と書くと，q は素元ゆえ既約元なので a と p のどちらかは単数だが，p は素元ゆえ単数でないので，a が単数であり，したがって p と q は同伴である． □

命題 9.10. A が素元分解整域であるとき，素元分解の一意性が次の意味で成り立つ：u, v が単数で，$m, n \geq 0$ で，$p_1, \ldots, p_m, q_1, \ldots, q_n$ が素元で，$up_1p_2 \ldots p_m = vq_1q_2 \ldots q_n$ ならば，$m = n$ であり，さらにある置換 $\sigma \in \mathfrak{S}_n$ に対して p_i と $q_{\sigma(i)}$ は同伴である． ◊

証明. m に関する帰納法で示す．$m = 0$ の場合，左辺は単数であり，素元は単数でないので単数の約数になれないので $n = 0$ であり，この場合は成り立っている．

$m \geq 1$ とする．左辺は p_1 で割りきれるので右辺も p_1 で割りきれる．p_1 は素元なので $v, q_1, \ldots, q_n$ の少なくとも 1 つは p_1 で割りきれる．素元は単数を割りきらないので，ある j が存在して p_1 は q_j を割りきり，したがって p_1 と q_j は同伴である．p_1 と q_j を取り除いて単数を適当に置き換えることにより $m - 1$ の場合に帰着した． □

命題 9.11. 素元分解整域において，既約元であることと素元であることは同値である． ◊

証明. 命題 9.5 で示したように素元ならば既約元である．逆を示す．a を既約元とし，$a = up_1p_2 \ldots p_m$ を素元分解とすると，a は単数でないので $m \neq 0$ であり，$m \geq 2$ だと $a = p_1 \cdot (up_2 \ldots p_m)$ が非自明な分解になって既約性に反するので $m = 1$ である． □

定理 9.12. 単項イデアル整域は素元分解整域である．　◊

証明. A を単項イデアル整域とする．まず A の既約元は素元であることを示す．$a \in A$ を既約元とし，a が bc を割るときに a が b と c のどちらかを割ることを示せばよい．A は単項イデアル環なので $(a,b) = (g)$ と表せて，$a = gh$ となる．a は既約なので g と h のどちらかは単数である．h が単数ならば $g = h^{-1}a$ は a と同伴なので $(a,b) = (g) = (a)$ であり b は a で割れる．g が単数ならば $(a,b) = (g) = (1)$ なので $ax + by = 1$ となる $x, y \in A$ がとれて，このとき $c = (ax + by)c = axc + bcy$ は a で割れる．

この先の証明の気持ちを説明する．A の 0 以外のすべての元が有限個の素元と単数の積に書けることを示したい．$a \in A \setminus \{0\}$ をとる．a が既約ならば素なので話は終わりである．そうでないならば非自明な分解 $a = bc$ をとる．これを続けていって最終的に既約元の積になればよい．そうならないとすると分解が無限に続くことになる．したがって，無限には続かないということを示すのが目標になる．背理法にした方が証明が書きやすい.

$A \setminus \{0\}$ の元で，有限個の素元と単数の積に書けないもの全体の集合を T とする．T が元をもつと仮定して矛盾を導く．$a_0 \in T$ をとる．a_0 が既約元ならば素元なので T の定義に反する．したがって a_0 は既約でないので，$a_0 = a_1 b_1$（$a_1, b_1 \notin A^*$）と書ける．a_1 と b_1 のどちらかは T に属する：そうでないと a_0 が有限個の素元と単数の積に書けてしまう．一般性を失わず $a_1 \in T$ としてよい．このとき $(a_0) \subsetneq (a_1)$ である（真の包含なのは $b_1 \notin A^*$ だから）．a_1 に対して同じ議論を行って $(a_1) \subsetneq (a_2)$ を得る．これを繰り返してイデアルの真の増加列 $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$ を得る．$I := \bigcup_{n \geq 0} (a_n)$ はイデアルの全順序族の和集合なのでイデアルであり（命題 4.12），A が単項イデアル環なので $I = (c)$ と書ける．I の定義から，ある n に対して $c \in (a_n)$ だが，すると $I = (c) \subset (a_n) \subset I$ より $I = (a_n)$ となり，(a_{n+1}) が (a_n) より真に大きいことに矛盾する．　□

注 9.13. 逆は成り立たない．例えば体上の 2 変数以上の多項式環は素元分解整域である（証明は系 9.16）が，単項イデアル整域ではない．　◊

例 9.14. $\boldsymbol{Z}[\sqrt{-5}]$ が単項イデアル整域でないことは既に見た．素元分解整域でもない．素元分解整域ならばすべての既約元は素元になる（命題 9.11）が，$2, 3, 1 \pm \sqrt{-5}$ などは既約だが素元でない．　◊

9.3 素元分解整域上の多項式環 [※範囲外]

本小節では定理 9.15 を証明する．証明には整域の商体を用いるので，性質を簡単に述べておく．（詳しくは 11.1 節を見よ．あるいは，$A = \boldsymbol{Z}$（このとき $\operatorname{Frac} A = \boldsymbol{Q}$）の場合に限定して読んでもよい．）

A を整域とする．$\frac{a}{s}$（$a \in A, s \in A \setminus \{0\}$）の形の分数を考え，$t \in A \setminus \{0\}$ に対し $\frac{a}{s} = \frac{at}{st}$ とみなす（正確にいうと，$A \times (A \setminus \{0\})$ 上のこの同値関係に関する同値類を分数の形で表記している）．加法と乗法が定義されて環になり，$a \neq 0$ ならば $\frac{a}{s}$ の乗法の逆元 $\frac{s}{a}$ が存在するので体になっている．これを A の**商体** (*field of fractions*) といい，$\operatorname{Frac} A$ と表す.

定理 9.15. UFD 上の多項式環は UFD である．　◊

体上の 1 変数多項式環は（ユークリッド環でありしたがって PID であるので）UFD なので，次が成り立つ.

系 9.16. k を体とする．$k[X_1, \dots, X_m]$ は UFD である．　◊

定理 9.15 を証明するための補題を準備する.

補題 9.17. $\pi \in A$ が素元ならば，π は $A[X]$ の元としても素元である．　◊

証明. $F_1 = \sum_i a_i X^i$ と $F_2 = \sum_j b_j X^j$ がどちらも π で割れないとする．a_i が π で割れない i が存在するので，そのような i の最小値を I とおく．同様に J をとる．すると F_1F_2 の X^{I+J} の係数は π で割れないので，F_1F_2 は π で割れない．　□

A を UFD とする．$F \in A[X] \setminus \{0\}$ が A のどの素元でも割れないとき，F を**原始的** (*primitive*) な多項式ということにする．

$F \neq 0$ を $F = \sum_{i=0}^{n} f_i X^i$，$n \geq 0$ と書くとき，F が原始的であることは，$f_0, \ldots, f_n$ すべてを割りきる素元 π が存在しないことと同値である．

$K = \operatorname{Frac} A$ を A の商体とする．

補題 9.18.

(1) 任意の $G \in A[X] \setminus \{0\}$ は，$G = aF$，$a \in A \setminus \{0\}$，$F \in A[X]$ は原始的，の形に書ける．また，a は A の単数倍を除いて一意に定まる．

(2) 任意の $G = K[X] \setminus \{0\}$ は，$G = aF$，$a \in K \setminus \{0\}$，$F \in A[X]$ は原始的，の形に書ける．また，a は A の単数倍を除いて一意に定まる．　◊

証明. (1) $G \in A[X] \setminus \{0\}$ とする．$G = \sum_{i=0}^{n} g_i X^i$，$n \geq 0$，$g_n \neq 0$ と書いて，すべての g_i を割りきる素元があればそれを括りだす，を繰り返せばよい．一意性も分かる．

(2) $G \in K[X] \setminus \{0\}$ とする．分母を払う，すなわち，$cG \in A[X]$ となる $c \in A \setminus \{0\}$ をとると，(1) より $cG = bF$, $b \in A \setminus \{0\}$, $F \in A[X]$ は原始的, と書けて，このとき $G = \frac{b}{c}F$ である．一意性を示す．$aF = a'F'$ とする．$a = \frac{b}{c}$，$a' = \frac{b'}{c'}$ $(b, c, b', c' \in A)$ と書ける．両辺を cc' 倍すると $bc'F = b'cF'$ であり，(1) の一意性から bc' と $b'c$ は単数倍を除き一致する．　□

補題 9.19. $G \in K[X] \setminus \{0\}$ に対し上記の a を対応させる写像を $\phi\colon K[X] \setminus \{0\} \to (K \setminus \{0\})/\sim$ と表す．ただし $\sim$ は同伴関係（定義 7.26）を意味する，すなわち $a \sim b \overset{\text{def}}{\iff}$「ある単数 $u \in A^*$ が存在して $a = ub$ となる」である．このとき $\phi(G_1G_2) = \phi(G_1)\phi(G_2)$ が成り立つ．　◊

証明. 原始的な多項式の積が原始的であることを示せばよく，これは原始的であることの定義と補題 9.17 から分かる．　□

補題 9.20. $P \in A[X]$ が原始的だとする．$Q \in K[X]$ が $PQ \in A[X]$ を満たすならば $Q \in A[X]$ である．　◊

証明. $Q = 0$ ならば明らかに成り立つ．そうでない場合, $\phi(P) = 1$ なので, 補題 9.19 より $\phi(Q) = \phi(PQ) \in A$ である．　□

補題 9.21. $P \in A[X]$ が原始的であり，かつ $K[X]$ の元として素元ならば，$A[X]$ の元としても素元である．◊

証明. $Q, R \in A[X]$ で P が QR を割りきると仮定し，Q または R を割りきることを示す．$K[X]$ ではこれが正しいので，P は $K[X]$ の中で Q または R を割りきる．一般性を失わず $Q = PS$，$S \in K[X]$ としてよい．すると補題 9.20 より $S \in A[X]$ である．　□

$F \in A[X] \setminus \{0\}$ が $A[X]$ の単元と素元の積に分解することを示そう．F の $K[X]$ での分解 $uP_1 \ldots P_m$ を

とる（$u \in K^* = K \setminus \{0\}$，$P_i$ は $K[X]$ の素元）．補題 9.18 を P_i に用いて，$P_i = a_i Q_i$，$a_i \in K \setminus \{0\}$，$Q_i \in A[X]$，$Q_i$ は原始的，と書く．$t := ua_1 \dots a_m$ とおく．すると $F = t \cdot Q_1 \dots Q_m$ であり，補題 9.19 より $\phi(t) = \phi(F) \in (A \setminus \{0\})/\sim$ なので $t \in A \setminus \{0\}$ である．A が UFD なので t を A の単数と素元の積に書ける．Q_i は補題 9.21 より素元である．

以上で定理 9.15 が証明された．

ちなみに，補題 9.18 で G に対応させた a（補題 9.19 で導入した記号を使うと $\phi(G)$）のことを，G の**内容** (*content*) とよぶことがある．また，補題 9.19 の中で示した「原始的な多項式の積は原始的である」や，補題 9.21 を，ガウスの補題とよぶことがある．

演習問題

問題 9.1 ($\boldsymbol{Z}[\sqrt{-1}]$ の素元)**.** 環 $A = \boldsymbol{Z}[\sqrt{-1}]$ の素元について考える．$\mathrm{Nm}\colon A \to \boldsymbol{N}$ を例 6.6 のように定義する．

(1) $a \in A$ とする．$\mathrm{Nm}(a)$ が素数ならば a は A の素元であることを示せ．またこのとき，$\mathrm{Nm}(a) \equiv 1 \pmod 4$ または $\mathrm{Nm}(a) = 2$ であることを示せ．
(2) $q \in \boldsymbol{Z}$ が $q > 0$ かつ $q \equiv 3 \pmod 4$ を満たす素数ならば，q は A の素元であることを示せ．
(3) A の素元は (1) と (2) のどちらかを満たすものと同伴であることを示せ．

(3) では，「$p \in \boldsymbol{Z}$ が $p > 0$ かつ $p \equiv 1 \pmod 4$ を満たす素数のとき，p は 2 つの平方数の和で書ける」を用いてもよい（このことの証明はいろいろあるが，例えば [群論, 問題 8.8] を参照）．

問題 9.2. $B = \boldsymbol{Z}[\sqrt{-1}]/(3)$ は問題 9.1 より体である．単数群 B^* の生成元を 1 つ求めよ．（定理 F.6 で，有限体の乗法群は巡回群であることを示す．これを使ってもよい．）

問題 9.3 (素元でない既約元の例)**.** 以下の元は既約元であり素元ではないことを示せ．k は体とする．

(1) $2, 3, 1 \pm \sqrt{-5} \in \boldsymbol{Z}[\sqrt{-5}]$.
(2) $3, 5, \sqrt{15} \in \boldsymbol{Z}[\sqrt{15}]$.
(3) $X, Y \in k[X, Y]/(Y^2 - X^3)$.
(4) $X, X + 1, Y \in k[X, Y]/(Y^2 - X^3 - X^2)$.
(5) $X, Y, Z \in k[X, Y, Z]/(XY - Z^n)$，ただし n は 2 以上の整数.

なお問題 8.9 や問題 10.3 の結果を使ってもよい．

10 素イデアルと極大イデアル

本節では環はすべて可換とする．

10.1 素イデアルと極大イデアル

これらも $\boldsymbol{Z}$ の素数の一般化である．

定義 10.1 (素イデアル)**.** 環 A の真のイデアル $\mathfrak{p} \subsetneq A$ が次を満たすとき**素イデアル** (*prime ideal*) であると

いう：$a, b \in A$ が $ab \in \mathfrak{p}$ を満たすならば $a \in \mathfrak{p}$ と $b \in \mathfrak{p}$ のどちらかが成立する．◊

定義 10.2 (極大イデアル)**.** 環 A の真のイデアル $\mathfrak{m} \subsetneq A$ が，真のイデアルのうちで包含関係に関して極大であるとき（すなわち，$\mathfrak{m} \subsetneq I \subsetneq A$ を満たすイデアル I が存在しないとき）**極大イデアル** (*maximal ideal*) であるという．◊

命題 10.3. A を環とし，$\mathfrak{p}$ や $\mathfrak{m}$ は A のイデアルとする．

(1) $\mathfrak{p}$ が素イデアルであることと，$A/\mathfrak{p}$ が整域であることは同値である．
(2) $\mathfrak{m}$ が極大イデアルであることと，$A/\mathfrak{m}$ が体であることは同値である．◊

証明は演習問題とする（問題 10.2）．

注 10.4. 素イデアルについてなぜ真のイデアルという条件を課すかというと，$\boldsymbol{Z}$ で ± 1 は素数とよばない（乗法に関して素数よりも極端な性質をもつので素数とは別に扱うのが妥当と考える）のと同様である．こうすることで命題 7.16 とも整合する．◊

例 10.5. 体の真のイデアルは (0) のみであり，これは唯一の極大イデアルであり唯一の素イデアルである．◊

例 10.6. $\boldsymbol{Z}$ のイデアルはすべて単項なので，イデアルが素イデアルか否かの判定は素数かどうかとほぼ同義になる．すなわち，$\boldsymbol{Z}$ の素イデアルは各素数 p に対する (p) と，もう 1 つ (0) がある．(0) 以外の素イデアルは極大イデアルである．

体でない単項イデアル整域でも全く同様に，素イデアルは (0) と，各素元 π に対する (π) であり，後者は極大である．ただし $\boldsymbol{Z}$ の場合より同伴関係が複雑な点には注意する．◊

素イデアルのきわめて重要な性質として次がある．

命題 10.7. $\phi\colon A \to B$ を環準同型とし，$\mathfrak{p} \subset B$ を素イデアルとする．このとき $\mathfrak{p}$ の縮約 $\phi^{-1}(\mathfrak{p}) \subset A$ も素イデアルである．◊

証明. 命題 10.3 の言い換えを使う．ϕ は単射環準同型 $A/\phi^{-1}(\mathfrak{p}) \to B/\mathfrak{p}$ を誘導する．$B/\mathfrak{p}$ が整域なので $A/\phi^{-1}(\mathfrak{p})$ も整域である．□

注 10.8. 命題 10.7 の状況で，$\mathfrak{p}$ が極大イデアルだとしても $\phi^{-1}(\mathfrak{p})$ は極大イデアルとは限らない．証明を真似しようとすると体の部分環は（整域ではあるが）一般に体にならないところで破綻する．具体例としては $\boldsymbol{Z} \to \boldsymbol{Q}$ による $\boldsymbol{Q}$ の極大イデアル $(0) \subset \boldsymbol{Q}$ の縮約は $(0) \subset \boldsymbol{Z}$ でありこれは明らかに極大でない．◊

余談 10.9. A の素イデアル全体の集合を A の**スペクトル** (*spectrum*) とよび，$\operatorname{Spec} A$ と書く．また A の極大イデアル全体の集合を A の**極大スペクトル** (*maximal spectrum*) とよび，$\operatorname{Specm} A$ などと書く．命題 10.7 より，環準同型 $\phi\colon A \to B$ は写像 $\phi^{-1}\colon \operatorname{Spec} B \to \operatorname{Spec} A$ を誘導する（$\operatorname{Specm} B$ の像は一般に $\operatorname{Specm} A$ に含まれない）．

（現代的な）代数幾何学の第一歩は，この集合 $\operatorname{Spec} A$ に**ザリスキ位相** (*Zariski topology*) という位相を入れて位相空間にし，ϕ^{-1} が連続写像であることを示し（問題 10.9 参照），さらに $\operatorname{Spec} A$ に環の層を乗せて局所環付き空間であることを示し，ϕ^{-1} が局所環付き空間の射であることを示し，環の圏から局所環付き空間の圏への関手 Spec が忠実充満であることを示すことである．$\operatorname{Spec} A$ の形の空間（これを**アフィンスキーム** (*affine scheme*) という）が代数幾何学の基本的な空間である．◊

定理 10.10. $\sqrt{0}$ は A のすべての素イデアルの共通部分に等しい. ◊

証明. 任意の素イデアル $\mathfrak{p} \subset A$ に対して $\sqrt{0} \subset \mathfrak{p}$ であることは難しくない（問題 10.5）. したがって $\sqrt{0} \subset \bigcap_{\mathfrak{p}} \mathfrak{p}$（$\bigcap$ はすべての素イデアル $\mathfrak{p}$ をわたる）である.

逆向きの包含関係は後日命題 11.24 で示す. □

10.2 素イデアルの例

10.2.1 体上の 1 変数多項式環の場合

k を体とし，$A = k[X]$ とする.

A は整域なので (0) は素イデアルである．ここで，(0) 以外の A の素イデアルは極大イデアルであることを示そう．$\mathfrak{p} \supsetneq (0)$ を A の (0) 以外の素イデアルとすると，0 でない元 $f \in \mathfrak{p}$ をもち，$f \notin A^* = k^*$ なので $\deg f \geq 1$ である．すると $(f) \subset \mathfrak{p}$ より $A/\mathfrak{p}$ は $A/(f)$ の剰余環であり，$A/(f)$ は k ベクトル空間として $\deg f$ 次元，とくに有限次元であり，したがって $A/\mathfrak{p}$ も有限次元であり，命題 F.7 より $A/\mathfrak{p}$ は体である．すなわち $\mathfrak{p}$ は極大イデアルである．また，$k[X]$ は単項イデアル整域なので $\mathfrak{p}$ は 1 つの多項式で生成される.

$a \in k$ に対し，$A/(X-a) \cong k$ なので，$(X-a)$ は極大イデアルである．一般には，素イデアルはこの形に書けるとは限らない．例えば $\boldsymbol{R}[X]/(X^2+1) \cong \boldsymbol{C}$（参考：問題 8.9）は体なので，$(X^2+1) \subset \boldsymbol{R}[X]$ は極大イデアルである.

k が代数閉体（詳細は体論の講義を参照）の場合，$f \in \mathfrak{p} \setminus \{0\}$ とすると $f = b(X-a_1)\dots(X-a_n)$ ($b \in k^*$, $a_i \in k$）と書けて，$\mathfrak{p}$ は素イデアルなのである i に対して $X - a_i \in \mathfrak{p}$ である．$(X-a_i) \subset \mathfrak{p}$ だが $(X-a_i)$ は極大イデアルなので $\mathfrak{p}$ に一致する．ということは結局 $n=1$ であり $\mathfrak{p} = (X-a_1)$ と書ける.

10.2.2 二次体の整数環の場合

m を平方数でない整数とし，$A = \boldsymbol{Z}[\sqrt{m}]$ とする．$A \cong \boldsymbol{Z}[X]/(X^2-m)$ と書けることに注意する．（m によってはこれは「二次体の整数環」ではなくその部分環にすぎないのだが，そのことはここでの話にはあまり影響しないので気にしないことにする.）

A は整域なので (0) は素イデアルである．ここで，(0) 以外の A の素イデアルは極大イデアルであることを示そう．$\mathfrak{p} \supsetneq (0)$ を A の (0) 以外の素イデアルとすると，0 でない元 $x + y\sqrt{m} \in \mathfrak{p}$（$x, y \in \boldsymbol{Z}$）をもつことから，0 でない元 $f := x^2 - my^2 = (x+y\sqrt{m})(x-y\sqrt{m}) \in \mathfrak{p} \cap \boldsymbol{Z}$ をもつ．すると $(f) \subset \mathfrak{p}$ より $A/\mathfrak{p}$ は $A/(f)$ の剰余環であり，$A/(f) = (\boldsymbol{Z}/f\boldsymbol{Z})[X]/(X^2-m)$ は有限集合なので $A/\mathfrak{p}$ は有限整域であり，したがって命題 F.5 より $A/\mathfrak{p}$ は体である．すなわち $\mathfrak{p}$ は極大イデアルである.

$A = \boldsymbol{Z}[\sqrt{m}]$ の (0) 以外の素イデアル $\mathfrak{p}$ を考える（前述のように，$\mathfrak{p}$ は極大イデアルである）．$\mathfrak{p} \cap \boldsymbol{Z}$ を考えると，これは $\boldsymbol{Z}$ の素イデアルであり，前述の議論から (0) より真に大きいので，ある素数 p を用いて $\mathfrak{p} \cap \boldsymbol{Z} = p\boldsymbol{Z}$ と表せる．言い換えると，$p \in \mathfrak{p}$ である．$|A/(p)| = p^2$ なので，次のいずれかが成り立つ（cf. 濃度 p^2 の環の分類（問題 H.17））.

- $\mathfrak{p} = (p)$ であり，$A/\mathfrak{p}$ は位数 p^2 の体である． p を含む A の素イデアルは $\mathfrak{p}$ のみである.
- $(p) \subsetneq \mathfrak{p}$ であり，指数は p であり，$A/\mathfrak{p}$ は位数 p の体である．$A/(p)$ は整域でない.
  この場合，さらに次の 2 つの場合がある.
  - $A/(p)$ は $\boldsymbol{F}_p \times \boldsymbol{F}_p$ に同型であり，p を含む A の素イデアルは $\mathfrak{p}$ を含めてちょうど 2 つ存在する.
  - $A/(p)$ は $\boldsymbol{F}_p[Y]/(Y^2)$ に同型であり，p を含む A の素イデアルは $\mathfrak{p}$ のみである.

どの場合が発生するかは m と p によって決まる．詳細は二次体の整数論を勉強してください．

10.3 Eisenstein の既約性判定法 [※範囲外]

定理 10.11 (Eisenstein の既約性判定法)．A を整域，$\mathfrak{p} \subset A$ を素イデアルとする．n 次モニック多項式 $F = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$（$n \geq 1$）が次を満たすとする．

(1) $a_{n-1}, \ldots, a_0 \in \mathfrak{p}$.
(2) $a_0 \notin \mathfrak{p}^2$.

このとき F は既約である．　◊

証明. F が n 次モニックで，条件 (1) を満たし，既約でないと仮定して，$a_0 \in \mathfrak{p}^2$ を示せばよい．n 次未満のモニック多項式 G, H を用いて $F = GH$ と書けたとする．$A/\mathfrak{p}$ は整域なので，$A[X] \to (A/\mathfrak{p})[X]$ による F の像 X^n の n 次未満のモニック多項式 2 つの積への分解は $X^s \cdot X^t$（$s+t=n$，$s,t>0$）しかない．したがって G, H の像はこのように書ける．言い換えると，$G = X^s + b_{s-1}X^{s-1} + \cdots + b_0$, $H = X^t + c_{t-1}X^{t-1} + \cdots + c_0$ で，$b_i, c_j \in \mathfrak{p}$ である．$s,t>0$ なので $b_0, c_0 \in \mathfrak{p}$ であり，$a_0 = b_0c_0 \in \mathfrak{p}^2$ である．　□

注 10.12. 証明から分かるように，条件 (2) はもう少し弱い条件「$a_0 \notin \{fg \mid f, g \in \mathfrak{p}\}$」に置き換えることができる．$\mathfrak{p}$ が単項イデアルの場合は同値だが．　◊

例 10.13. $A = \boldsymbol{Z}$ で $\mathfrak{p}$ が素数 p で生成される場合が有名である．例えば，$m \neq \pm 1, 0$ が素数の 2 乗で割れない整数ならば，$X^n - m$ は既約であることがこの判定法から分かる．　◊

例 10.14. p を素数とする．p 番目の円分多項式とは $\Phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + 1$ である．これが $\boldsymbol{Z}$ 上既約であることを示そう．$\Phi_p(X)$ は定数項が 1 なので直接判定法を用いることはできないが，同型写像 $\boldsymbol{Z}[X] \to \boldsymbol{Z}[Y]\colon X \mapsto Y+1$ でうつすことで適用できるようになる．この同型写像による $\Phi_p(X)$ の像は $\frac{(Y+1)^p-1}{Y} = \sum_{1\leq k\leq p} \binom{p}{k} Y^{k-1} = \sum_{0\leq i\leq p-1} \binom{p}{i+1} Y^i$ であり，Y^{p-1} の係数は 1 なのでモニックであり，それ以外の係数は 2 項係数の性質から p で割り切れ，定数項は $\binom{p}{1} = p$ なので p^2 で割り切れない．したがってこの多項式は既約であり，ゆえに $\Phi_p(X)$ も既約である．

素数以外の一般の正整数に対する円分多項式も定義され（E 節参照，もう少し複雑な形になる），既約になるが，ここでは触れない．　◊

10.4 極大イデアルの存在

定理 10.15. A が零環でない（単位的で可換な）環ならば，A は極大イデアルをもつ．　◊

余談 10.16. 実は定理 10.15 は（ZF 公理系の下で）選択公理と同値な命題である．　◊

証明. $\mathcal{F}$ を A の真のイデアル全体の集合とする．$\mathcal{F}$ は包含関係により順序集合をなす．$\mathcal{F}$ が帰納的順序集合ならば，Zorn の補題より $\mathcal{F}$ は極大元をもち，それは A の極大イデアルに他ならない．

$\mathcal{F}$ が帰納的順序集合であることを示そう．すなわち，$S \subset \mathcal{F}$ が全順序部分集合ならば S は（$\mathcal{F}$ の中に）上界をもつことを示す．$S' := \{(0)\} \cup S$ も $\mathcal{F}$ の全順序部分集合であり（A が零環でないので），S' は空でない．$I := \bigcup_{J\in S'} J$ はイデアルの空でない全順序族の和集合なので，命題 4.12 よりイデアルである．明らかに S の

任意の元は I の部分集合である．あとは I が A の真のイデアルであることを示せばよい．$I = A$ だとすると $1 \in I$ だが，I の定義より，S のある元 J が $1 \in J$ を満たすことになり，これは J が（$J \in S \subset \mathcal{F}$ ゆえ）真のイデアルであるという仮定に反する．したがって $I \subsetneq A$ である． □

系 10.17. A が環で，$a \in A$ が単数でない元ならば，A の極大イデアルで a を含むものが存在する． ◊

証明. a が単数でないので，$A/(a)$ は零環でない．定理 10.15 より $A/(a)$ は極大イデアルをもち，これは A の極大イデアルで a を含むものに対応する（命題 5.18，問題 10.4）．

別証明として，A の真のイデアルで a を含むもの全体の集合を考えて，定理 10.15 の証明と同様の議論を行ってもよい． □

極大イデアルは素イデアルなので，当然次も成り立つ．

系 10.18. A が零環でない（単位的で可換な）環ならば，A は素イデアルをもつ． ◊

余談 10.19. 系 10.18 は（ZF 公理系の下で）選択公理より真に弱い命題であることが知られている． ◊

系 10.20. 環 A の単数群 A^* は，どの極大イデアルにも属さない元全体の集合に等しい． ◊

証明. $s \in A$ が単数ならば $(s) = A$ なので s が極大イデアルに属することはない．s が単数でないならば，系 10.17 より s を含む極大イデアルが存在する． □

定義 10.21. 極大イデアルをちょうど 1 つもつ環を**局所環** (*local ring*) という．局所環とその極大イデアルの組 $(A, \mathfrak{m})$ を「局所環」とよぶこともある． ◊

例 10.22. 体は局所環である． ◊

他には，系 11.23 で得られるものが典型的である．

系 10.20 より直ちに次を得る．

系 10.23. $(A, \mathfrak{m})$ が局所環ならば，A は集合として A^* と $\mathfrak{m}$ の非交差和である． ◊

演習問題

問題 10.1. (0) でも極大イデアルでもない素イデアルの例を挙げよ．

問題 10.2 (☆)**.** $\mathfrak{p} \subset A$ が素イデアルであることと，$A/\mathfrak{p}$ が整域であることは同値であることを示せ．$\mathfrak{m} \subset A$ が極大イデアルであることと，$A/\mathfrak{m}$ が体であることは同値であることを示せ．

問題 10.3 (☆)**.** A を環，$a \in A$ を 0 でない元とする．a が素元であること，(a) が素イデアルであること，$A/(a)$ が整域であること，はすべて同値であることを示せ．

問題 10.4 (☆)**.** $I \subset A$ をイデアルとする．命題 5.18 より，A/I のイデアルは，A のイデアルで I を含むものと一対一に対応する．この対応で，素イデアルは素イデアルと対応し，極大イデアルは極大イデアルと対応することを示せ．

問題 10.5. A を環，$\mathfrak{p} \subset A$ を素イデアルとする．$\sqrt{0} \subset \mathfrak{p}$ を示せ．

問題 10.6. A を環とし，$I, J, \mathfrak{p}$ をイデアルとし，$\mathfrak{p}$ は素イデアルだとする．$IJ \subset \mathfrak{p}$ ならば $I \subset \mathfrak{p}$ または $J \subset \mathfrak{p}$ であることを示せ．$I \cap J \subset \mathfrak{p}$ ならば $I \subset \mathfrak{p}$ または $J \subset \mathfrak{p}$ であることを示せ．

問題 10.7 (☆いわゆる「prime avoidance」)**.** A を環，I をイデアルとし，$\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ を（有限個の）素イデアルとする．各 $1 \leq i \leq n$ に対して $I \not\subset \mathfrak{p}_i$ と仮定する．このとき $I \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$ を示せ．（この結果・議論は可換環論において頻出である．）

問題 10.8 (prime avoidance の別形)**.** A を環，I をイデアルとし，$\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ および $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ を（有限個の）素イデアルとする．どの i, j に対しても $\mathfrak{q}_j \not\subset \mathfrak{p}_i$ だと仮定する．このとき $x \in I$ で，どの i に対しても $x \notin \mathfrak{p}_i$ かつ，どの j に対しても $x \in \mathfrak{q}_j$ を満たすものが存在することを示せ．

問題 10.9 (ザリスキ位相)**.** 環 A に対し，A の素イデアル全体の集合を $\operatorname{Spec} A$ と表す．A のイデアル $I \subset A$ に対し，$V(I) := \{\mathfrak{p} \in \operatorname{Spec} A \mid I \subset \mathfrak{p}\} \subset \operatorname{Spec} A$ と定める．

(1) $\operatorname{Spec} A$ の部分集合族 $\{V(I) \mid I \subset A\}$ は閉集合系の公理を満たすことを確かめよ．これが定める位相を $\operatorname{Spec} A$ の**ザリスキ位相** (*Zariski topology*) という．
(2) $\phi\colon A \to B$ を環準同型とし，$\phi^{-1}\colon \operatorname{Spec} B \to \operatorname{Spec} A$ をイデアルの縮約が定める写像とする．ϕ^{-1} は（ザリスキ位相に関して）連続写像であることを示せ．

11 環の局所化

本節では環はすべて可換とする．

11.1 整域の商体

整数だけを知っている状態で有理数を構成することを考える．

まず $\frac{n}{m}$ という記号（分数）を用意する．ただし $n, m \in \boldsymbol{Z}$ で，$m \neq 0$ とする．$\frac{n}{m} = \frac{n'}{m'}$ となるための条件を定める（$nm' = n'm$）．さらに整数 n と分数 $\frac{n}{1}$ も等しいものとする．$m\frac{n}{m} = n$ が成り立つように演算を定める．具体的には，$\frac{n}{m} + \frac{n'}{m'} = \frac{nm'}{mm'} + \frac{n'm}{mm'} = \frac{nm'+n'm}{mm'}$ および $\frac{n}{m} \cdot \frac{n'}{m'}$ と定める．well-defined 性の確認もする．

以上の構成は一般の整域に適用でき，そうして得られる体が商体である．

定義 11.1. A を整域とする．A の**商体** (*field of fractions*)　(*quotient field*, *fraction field* などともいう) $\operatorname{Frac} A$（$Q(A)$ などとも書く）は以下で定義される．

まず集合としては $\operatorname{Frac} A$ は直積集合の商集合 $(A \times (A \setminus \{0\}))/\approx$ である．ここで $A \times (A \setminus \{0\})$ 上の同値関係 $\approx$ は次で定義される：

$$(a_1, s_1) \approx (a_2, s_2) \overset{\text{def}}{\iff} a_1 s_2 - a_2 s_1 = 0.$$

(a, s) の同値類を $\frac{a}{s}$ と書く．次に $\operatorname{Frac} A$ 上の加法と乗法を定める：

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}, \qquad \frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}.$$

A が整域なので分母は確かに非零である．これは well-defined になる．最後に写像 $\phi\colon A \to \operatorname{Frac} A$ を $\phi(A) = \frac{a}{1_A}$ で定める． ◊

命題 11.2. 商体について次が成り立つ.

(1) $A \times (A \setminus \{0\})$ 上の 2 項関係 $\approx$ は同値関係である.
(2) $\mathrm{Frac}\, A$ 上の加法と乗法は well-defined である.
(3) $\mathrm{Frac}\, A$ はこの加法と乗法に関して可換環をなす. $0_{\mathrm{Frac}\, A} = \frac{0_A}{1_A}, 1_{\mathrm{Frac}\, A} = \frac{1_A}{1_A}$, $-\frac{a}{s} = \frac{-a}{s}$ である.
(4) $\phi\colon A \to \mathrm{Frac}\, A$ は環準同型であり, 単射である.
(5) $\mathrm{Frac}\, A$ は体である. 0 でない元 $\frac{a}{s} \in \mathrm{Frac}\, A$ に対し $a \neq 0$ であり, $(\frac{a}{s})^{-1} = \frac{s}{a}$ である. ◊

証明は演習問題とする（問題 11.1）.

例 11.3. $\boldsymbol{Z}$ の商体は $\boldsymbol{Q}$ である. ◊

例 11.4. 体の商体は自分自身である. 正確には, k が体ならば上述の準同型 $\phi\colon k \to \mathrm{Frac}\, k$ は同型であり, 基本的にこの同型写像を通じて k と $\mathrm{Frac}\, k$ を同一視する. ◊

例 11.5. k が体で $A \subset k$ が部分環（したがって整域）ならば, $\mathrm{Frac}\, A$ も k の部分環（部分体）とみなせる. $\mathrm{Frac}\, A$ は k に一致することもしないこともある.

B が整域で $A \subset B$ が部分環（したがって整域）ならば, $\mathrm{Frac}\, A$ も $\mathrm{Frac}\, B$ の部分環（部分体）とみなせる. $\mathrm{Frac}\, A$ は $\mathrm{Frac}\, B$ に一致することもしないこともある. ◊

例 11.6. $k[X_1, \ldots, X_n]$ の商体を $k(X_1, \ldots, X_n)$ と書き, k 上の n 変数**有理関数体** (*field of rational functions*) とよぶ. ◊

11.2 環の積閉集合と局所化

11.1 節で整域の商体の構成を見たが, $\boldsymbol{Z}$ からの例えば $\boldsymbol{Z}[\frac{1}{2}]$ の構成（分母として 2 の冪乗だけを考えると得られる）などを含めた形で, また整域と限らない環に適用可能な形で一般化することを考える.

分母として許す元全体の集合としてはどのようなものを考えるかが最初のポイントになる. それが次の積閉集合である. 分数 $\frac{a}{s}$ と $\frac{b}{t}$ を含む環を考えるならそれらの積 $\frac{ab}{st}$ をも含めないといけないので, 条件 (2) は自然である. (1) は, 2 個以上の積を考えるなら 0 個の積も考えましょうというよくある考え方である.

定義 11.7. $S \subset A$ を環の部分集合とする. S が次の条件を満たすとき S は A の**積閉集合** (*multiplicatively closed set*) であるという.

(1) $1 \in S$.
(2) $s, t \in S$ ならば $st \in S$. ◊

例 11.8. $S = \{1\}$ と $S = A$ がそれぞれ A の最小と最大の積閉集合である.
$f \in A$ に対し, $\{f^n \mid n \in \boldsymbol{N}\} = \{1, f, f^2, f^3, \ldots\}$ は積閉集合である.
A が整域ならば $A \setminus \{0\}$ は積閉である. ◊

$\boldsymbol{Z}$ とその積閉集合 $\boldsymbol{Z} \setminus \{0\}$ からの有理数の構成や, 積閉集合 $\{1, m, m^2, \ldots\}$ からの $\boldsymbol{Z}[\frac{1}{m}]$ の構成を一般化したのが次の局所化という操作である.

定義 11.9. A が環で $S \subset A$ が積閉集合のとき, A の S での**局所化** (*localization*) は $S^{-1}A$ や A_S と表され,

次で定義される．まず集合としては A_S は直積集合の商集合 $(A \times S)/\sim$ である．ここで $A \times S$ 上の同値関係 $\sim$ は次で定義される：

$$(a_1, s_1) \sim (a_2, s_2) \overset{\text{def}}{\iff} \text{ある } t \in S \text{ に対して } (a_1 s_2 - a_2 s_1)t = 0.$$

（この 2 項関係が同値関係であることは後で確認する．）(a, s) の同値類を $\frac{a}{s}$ と書く．次に A_S 上の加法と乗法を定める：

$$\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}, \qquad \frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}.$$

S が積閉なので分母は確かに S の元である．これは well-defined になる．最後に写像 $\phi\colon A \to A_S$ を $\phi(a) = \frac{a}{1_A}$ で定める． ◊

命題 11.10. 局所化について次が成り立つ．

(1) $A \times S$ 上の 2 項関係 $\sim$ は同値関係である．
(2) A_S 上の加法と乗法は well-defined である．
(3) A_S はこの加法と乗法に関して可換環をなす．$0_{A_S} = \frac{0_A}{1_A}, 1_{A_S} = \frac{1_A}{1_A}$，$-\frac{a}{s} = \frac{-a}{s}$ である．
(4) $\phi\colon A \to A_S$ は環準同型である．
(5) S の像 $\phi(S)$ は $(A_S)^*$ に含まれる．$s \in S$ に対し，$\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$ である．
(6) $\phi\colon A \to A_S$ が同型であることと，$S \subset A^*$ は同値である． ◊

証明. (1) 反射律と対称律は明らかである．推移律の証明は演習問題とする（問題 11.2）．

(2), (3)（S が零因子を含まない場合は，経験的には明らかである．）定義に沿って示せばよい．well-defined 性については，$\frac{a_1}{s_1} = \frac{a_2}{s_2}$ のとき $\frac{a_1}{s_1} + \frac{a'}{s'} = \frac{a_2}{s_2} + \frac{a'}{s'}$，$\frac{a_1}{s_1} \cdot \frac{a'}{s'} = \frac{a_2}{s_2} \cdot \frac{a'}{s'}$ が成り立つことを示せば実質的には十分である．

(4), (5) これも難しくない．

(6) 同型ならば，A_S に行って単元になる A の元はもとから単元である．したがって (5) から $S \subset A^*$ を得る．$S \subset A^*$ ならば逆写像を $\frac{a}{s} \mapsto as^{-1}$ で定めると well-defined になる． □

注 11.11. 定義 11.9 で使った同値関係 $\sim$ は少しややこしいので，定義 11.1 で使った $\approx$ で代用できないか，というのは素朴な疑問である：

$$(a_1, s_1) \approx (a_2, s_2) \overset{\text{def}}{\iff} a_1 s_2 - a_2 s_1 = 0.$$

これは一般に同値関係にならない．$(a_1, s_1) \approx (a_2, s_2) \approx (a_3, s_3)$ から $(a_1, s_1) \approx (a_3, s_3)$ を示そうとすると，$a_1 s_3 - a_3 s_1 = 0$ をいいたいのだが，せいぜい $s_2(a_1 s_3 - a_3 s_1) = 0$ しかいえない（s_2 が零因子かもしれないので，ここから $a_1 s_3 - a_3 s_1 = 0$ はいえない）．

一方で，S が零因子を含まない積閉集合の場合は，$\sim$ と $\approx$ は一致する．例えば A が整域で S が 0 を含まない場合はそうである． ◊

例 11.12. $0_A \in S$ であることと A_S が零環であることは同値である．（A_S が零環であることと $1_{A_S} = 0_{A_S}$ は同値であり，$1_{A_S} = 0_{A_S}$ を同値関係の定義にしたがって変形すれば分かる．） ◊

注 11.13. まったく推奨しないが，零環を嫌う（または，環に含めない）文献では積閉集合の定義に $0_A \notin S$ を含めることがある． ◊

例 11.14. $S = \{f^n \mid n \in \boldsymbol{N}\}$ による局所化を A_f と書く．A が整域で $f \neq 0$ ならば，これは $\operatorname{Frac} A$ の部分環 $A[\frac{1}{f}]$ に等しい．
$A = k[x]$ で $f = x$ のときは $k[x]_x$ を $k[x, x^{-1}]$ や $k[x^{\pm 1}]$ とも書く．◊

例 11.15. $\mathfrak{p} \subset A$ を素イデアルとすると，$S := A \setminus \mathfrak{p}$ は積閉集合である．これによる局所化を $A_{\mathfrak{p}}$ と書く．
整域の素イデアル (0) での局所化は商体に他ならない．◊

余談 11.16. $A_{\mathfrak{p}}$ が $A_{A\setminus\mathfrak{p}}$ を表すのでなかなか怪しい記法だが，広く用いられており，慣れれば混乱はない．一応以下の点には注意しよう．

- $f \in A$ が素元のとき $(f) \subset A$ は素イデアルである．このとき A_f と $A_{(f)}$ は異なる．
- $p \in \boldsymbol{Z}$ が素数のとき，（どちらの局所化とも異なる）p 進整数環を $\boldsymbol{Z}_p$ で表すのが一般的である．では p の冪からなる積閉集合による局所化はどう表すのかというと，$\boldsymbol{Z}[\frac{1}{p}]$ でしょうかね．◊

例 11.17. 整域の場合，0 を含まない積閉集合による局所化の中では商体が最大である．つまり，A が整域で，$S \subset A$ が 0 を含まない積閉集合ならば，$A \to A_S$ および $A_S \to \operatorname{Frac} A$ は単射であり，A_S は $\operatorname{Frac} A$ の部分環とみなせる．◊

A が整域でない場合，$A \setminus \{0\}$ は積閉集合でない．整域と限らない環への一般化として次がある．

定義 11.18. 環 A の非零因子全体の集合 S は積閉である．この S による A の局所化を A の**全商環** (*total ring of fractions*) という．*total quotient ring* ともいう．$Q(A)$ などと書く．◊

整域の全商環は商体である．
積閉集合 S による局所化 A_S は一般に有限生成 A 代数にならないが，次は成り立つ．

命題 11.19. A_f は $A[X]/(fX - 1)$ に同型である．とくに，A_f は有限生成 A 代数である．◊

証明は演習問題とする（問題 11.7）．

11.3 局所化のイデアルや素イデアル [※範囲外]

命題 11.20. $\phi\colon A \to A_S$ を環の局所化に伴う環準同型とし，$-^{\mathrm{e}}, -^{\mathrm{c}}$ をイデアルの拡大，縮約（5.1 節）とする．

(1) イデアル $J \subset A_S$ に対し，$J^{\mathrm{ce}} = J$（別の記法で書くと $\phi(J \cap A)A_S = J$）である（一般の環準同型では $\subset$ が成立するのだった（系 5.8(1))）．
(2) イデアル $J, J' \subset A_S$ に対し，$J \subset J'$ と $J^{\mathrm{c}} \subset J'^{\mathrm{c}}$ は同値である．
(3) イデアルの縮約をとる写像 $-^{\mathrm{c}}\colon \{A_S \text{ のイデアル }\} \to \{A \text{ のイデアル }\}\colon J \mapsto J^{\mathrm{c}}$ は単射である．◊

証明. (1) $\frac{a}{s} \in J$ とすると $a \in J \cap A$ なので $\frac{a}{s} = \phi(a) \cdot \frac{1}{s} \in (J \cap A)A_S$ である．
(2) 縮約と拡大が包含関係を保つことと (1) から直ちに分かる．
(3) (1) から直ちに分かる．□

命題 11.21. $\phi\colon A \to A_S$ を環の局所化に伴う環準同型とすると，ϕ によるイデアルの縮約をとる写像

$$\{A_S \text{ の素イデアル }\} \to \{A \text{ の素イデアル }\}$$

は単射であり，像は S と交わらない素イデアル全体の集合である． ◊

証明. 単射性は命題 11.20(3) から分かる．$\mathfrak{q} \subset A_S$ が素イデアルのとき $(A_S)^* \cap \mathfrak{q} = \emptyset$ であり，$\phi(S) \subset (A_S)^*$ なので，$S \cap \phi^{-1}(\mathfrak{q}) = \emptyset$ である．ここで次を示す．

主張．$\mathfrak{p}$ を S と交わらない素イデアルとする．$n \geq 0$ で，$a_1, \ldots, a_n \in A$, $s_1, \ldots, s_n \in S$ が $\prod_{i=1}^n \frac{a_i}{s_i} \in \mathfrak{p}A_S$ を満たすなら，ある $1 \leq i \leq n$ に対して $a_i \in \mathfrak{p}$ である．

主張の証明．そのとき，$x_1, \ldots, x_m \in \mathfrak{p}$ と $\frac{c_1}{u_1}, \ldots, \frac{c_m}{u_m} \in A_S$ が存在して $\prod_{i=1}^n \frac{a_i}{s_i} = \sum_{j=1}^n x_j \frac{c_j}{u_j}$ が成り立つが，右辺を通分して $\frac{x}{u}$（$x \in \mathfrak{p}$，$u \in S$）と書ける．これは A での等式 $vu \prod_{i=1}^n a_i = vx \prod_{i=1}^n s_i$（$v \in S$）を意味する．右辺は $\mathfrak{p}$ の元であり，$v, u \in S$ は $\mathfrak{p}$ に属さないので，$\mathfrak{p}$ が素イデアルであることから，ある i に対して $a_i \in \mathfrak{p}$ が成り立つ．以上で主張が示された．

$\mathfrak{p} \subset A$ が素イデアルで $\mathfrak{p} \cap S = \emptyset$ のとき，$\mathfrak{p}A_S$ が素イデアルで $\mathfrak{p}A_S \cap A = \mathfrak{p}$ を満たすことを示そう．$\frac{a}{s}, \frac{b}{t} \in A_S$ が $\frac{a}{s}\frac{b}{t} \in \mathfrak{p}A_S$ を満たすとすると，主張より $a \in \mathfrak{p}$ または $b \in \mathfrak{p}$ なので，$\frac{a}{s} \in \mathfrak{p}A_S$ または $\frac{b}{t} \in \mathfrak{p}A_S$ である．2 個でなく一般の個数の元の積についても同様なので，$\mathfrak{p}A_S$ は素イデアルである．

$\mathfrak{p}A_S \cap A \subset \mathfrak{p}$ を示す．これは 1 個の元 $\frac{a}{1}$ の積に主張を適用すればよい． □

積閉集合 S として $\{a^n \mid n \in \boldsymbol{N}\}$ および $A \setminus \mathfrak{p}$ を考えることで，次の 2 つの系を得る．

系 11.22. $a \in A$ を元とすると，$\{A_a$ の素イデアル $\}$ と $\{A$ の素イデアルで a を含まないもの $\}$ の間に一対一対応がある． ◊

証明. 任意の $n \geq 1$ に対して，$a^n \notin \mathfrak{p}$ は $a \notin \mathfrak{p}$ と同値である． □

系 11.23. $\mathfrak{p} \subset A$ を素イデアルとすると，$\{A_\mathfrak{p}$ の素イデアル $\}$ と $\{A$ の素イデアルで $\mathfrak{p}$ に含まれるもの $\}$ の間に一対一対応がある．とくに，$A_\mathfrak{p}$ は局所環である． ◊

証明. A の部分集合が $A \setminus \mathfrak{p}$ と交わらないことは，$\mathfrak{p}$ に含まれることと同値である．$\mathfrak{p}$ に含まれる素イデアルの中で明らかに $\mathfrak{p}$ が最大なので，$A_\mathfrak{p}$ の極大イデアルは（$\mathfrak{p} \subset A$ に対応する）$\mathfrak{p}A_\mathfrak{p}$ のみである． □

命題 11.24 (定理 10.10 の残り)**.** A を環とする．$a \in A$ が A の任意の素イデアルに含まれるならば，a は冪零である． ◊

証明. 仮定と系 11.22 より，A_a は素イデアルをもたない．定理 10.15 より，A_a は零環である．例 11.12 より，今回使った積閉集合 $\{a^n \mid n \in \boldsymbol{N}\}$ は 0 を含む．すなわち a は冪零である． □

11.4 何が局所なのか [※範囲外]

X を実 C^∞ 多様体または複素正則多様体，$x \in X$ を点，$A = \mathcal{O}(X)$ を X 上の実 C^∞ 関数または複素正則関数全体がなす環とする．$\mathfrak{p} \subset A$ を x を零点にもつ関数全体がなすイデアルとすると，$A/\mathfrak{p}$ は $\boldsymbol{R}$ または $\boldsymbol{C}$ に同型なので $\mathfrak{p}$ は極大イデアルである．積閉集合 $A \setminus \mathfrak{p}$ の元は x の近傍で可逆なので，$A_\mathfrak{p}$ は，x のある近傍で定義されている C^∞ 関数または正則関数全体ということになる．また $f \in A$ に対し A_f は，f の零点集合の補集合（開集合）上の関数全体となる．

$X = \operatorname{Spec} A$ とし A を X 上の関数の環とみなした場合も同様に $A_\mathfrak{p}$ は $\mathfrak{p} \in \operatorname{Spec} A$ の近傍で定義されている関数全体の環と思える（ただし $A/\mathfrak{p}$ は一般には整域でしかない）．A_f なども同様である．

このように関数の定義域が狭まっていることが局所化の名前の由来である．たぶん．

演習問題

問題 11.1 (☆ cf. 命題 11.10)**.** 命題 11.2 を示せ.

問題 11.2 (☆)**.** 定義 11.9 の 2 項関係 $\sim$ が推移律を満たすことを示せ.

問題 11.3. 問題 8.9 の各 $f\colon A \to B$ に対して，$\mathrm{Frac}(\mathrm{Im}(f)) \subset \mathrm{Frac}(B)$ が一致するかを答えよ.

問題 11.4. m を平方数でない整数とする．$\mathrm{Frac}(\boldsymbol{Z}[\sqrt{m}])$ は $\boldsymbol{Q}[\sqrt{m}]$ と同型であることを示せ.

問題 11.5. A を環，$S \subset A$ を積閉集合，$\phi\colon A \to A_S$ を局所化とする．$f\colon A \to B$ を A 代数とする．次が同値であることを示せ.

- $f(S) \subset B^*$.
- A 代数の準同型 $A_S \to B$ が存在する.

さらに，このとき A 代数の準同型 $A_S \to B$ は一意であることを示せ．したがって，全単射

$$\mathrm{Hom}(A_S, B) \to \{f \in \mathrm{Hom}(A, B) \mid f(S) \subset B^*\}\colon g \mapsto g \circ \phi$$

を得る（Hom は環準同型全体の集合を表す）.

問題 11.6 (☆)**.** $\boldsymbol{Q}$ の任意の部分環 B は，$\boldsymbol{Z}$ の積閉集合 S を用いて $\boldsymbol{Z}_S$ の形に書けることを示せ.
なお，$\boldsymbol{Z}$ を一般の整域にして $\boldsymbol{Q}$ をその商体にすると成立しない（問題 H.18）.

問題 11.7 (cf. 命題 11.19)**.** A_f は $A[X]/(fX-1)$ に同型であることを示せ.

問題 11.8. A を環，$S \subset A$ を積閉集合とする．B を，S で添字づけられた不定元の族 $(X_s)_{s\in S}$ を使った A 上の多項式環 $A[X_s \mid s \in S]$ とし，$I \subset B$ を集合 $\{sX_s - 1 \mid s \in S\}$ で生成されるイデアルとする．A_S は B/I と同型であることを示せ.

問題 11.9. A を整域とし，$S \subset A \setminus \{0\}$ を積閉集合とし，$\phi\colon A \to A_S$ を局所化とする．$\pi \in A$ が素元ならば，$\phi(\pi)$ は単元または素元であることを示せ.

問題 11.10. A を整域とし，$S \subset A \setminus \{0\}$ を積閉集合とする．A が PID ならば A_S も PID であることを示せ．A が UFD ならば A_S も UFD であることを示せ.

問題 11.11. A を環とする.

(1) $f \in A$ を元，$k \geq 1$ を正整数とする．A_f と A_{f^k} は同型であることを示せ.
(2) $f, g \in A$ を元とする．次の 3 つは同型であることを示せ.
   - A の積閉集合 $\{f^n g^m \mid n, m \in \boldsymbol{N}\}$ による局所化,
   - A の局所化 A_f の積閉集合 $\{(\frac{g}{1})^m \mid m \in \boldsymbol{N}\}$ による局所化,
   - A_{fg}.

問題 11.12. A を環，$S \subset A$ を積閉集合，$T \subset A_S$ を積閉集合とする．$T' := \{b \in A \mid \frac{b}{1}$ はある T の元を割りきる $\}$ と定めると，T' は積閉集合であり，$A_{T'}$ と $(A_S)_T$ は同型であることを

示せ.

12 ネーター環 [※範囲外]

本節では環はすべて可換とする. ただし，非可換環においても例えば左ネーター環（左イデアルに関する昇鎖律を満たす環）などを考えることはできる.

12.1 ネーター環の定義

ある種の有限性を満たす環としてネーター環，アルティン環がある.

定義 12.1. 一般に順序集合 $X = (X, \leq)$ において，$x_1 \leq x_2 \leq x_3 \leq \ldots$ を満たす列を**昇鎖** (*ascending chain*) や**増大列**といい，ある $N \in \boldsymbol{N}$ が存在して任意の $n \geq N$ に対して $x_n = x_N$ であるときこの列は**停止する** (*eventually stabilize*) または *stationary* であるという．任意の昇鎖が停止するときこの順序集合は**昇鎖律** (*ascending chain condition*) または昇鎖条件を満たすという．長さ無限の真の増大列（不等号がすべて $<$ であるもの）が存在しないと言い換えてもよい.

$x_1 \geq x_2 \geq x_3 \geq \ldots$ を満たす列を**降鎖** (*descending chain*) や**減少列**といい，任意の降鎖が停止するときこの順序集合は**降鎖律** (*descending chain condition*) または降鎖条件を満たすという．長さ無限の真の減少列（不等号がすべて $>$ であるもの）が存在しないと言い換えてもよい. ◊

定義 12.2. 環 A が**ネーター環** (*Noetherian ring*) [*4] [*5]であるとは，その環のイデアル全体が包含関係に関してなす順序集合が昇鎖律を満たすことをいう.

環 A が**アルティン環** (*Artinian ring*) [*6]であるとは，その環のイデアル全体が包含関係に関してなす順序集合が降鎖律を満たすことをいう. ◊

例 12.3. $\boldsymbol{Z}$ はネーター環である．$I_0 \subsetneq I_1$ を $\boldsymbol{Z}$ のイデアルとすると I_1 は 0 でない元 a を含み，したがって $\boldsymbol{Z}/I_1$ は $\boldsymbol{Z}/(a)$ の剰余環なので有限集合であり，ゆえに $\boldsymbol{Z}/I_1$ のイデアルは有限個しかなく，すなわち I_1 を含む $\boldsymbol{Z}$ のイデアルも有限個しかないので，真の増大列 $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$ は有限個で止まる.

一方，$\boldsymbol{Z}$ はアルティン環ではない．実際，例えば降鎖 $(1) \supset (2) \supset (4) \supset (8) \supset \cdots \supset (2^n) \supset \ldots$ は停止しない. ◊

例 12.4. イデアルが有限個しかない環は明らかにネーター環かつアルティン環である．これを満たす例として，体（イデアルは (0) と (1) しかない）や，有限環がある.

A が体 k 上の代数で，（このとき k 上のベクトル空間にもなるので次元が定義できるが）有限次元だとする．このとき A のイデアルも k 上のベクトル空間であり，増大列・減少列において次元の不等式が成り立つので，A はネーター環かつアルティン環である. ◊

昇鎖律・降鎖律は任意の順序集合で考えることができるが，イデアルの昇鎖律については次の言い換えがある.

[*4] 数学者 Emmy Noether にちなむ.
[*5] 「ネータ」「ネター」という綴りも見かける.
[*6] 数学者 Emil Artin にちなむ.

命題 12.5. 環 A に対して次は同値である．

(1) ネーター環である（イデアルの昇鎖律を満たす）．
(2) A の任意のイデアルは有限生成である． ◊

証明. （(2) $\implies$ (1)）：$I_1 \subset I_2 \subset \cdots \subset I_n \subset \ldots$ をイデアルの昇鎖とする．和集合 $I := \bigcup_{n\geq 1} I_n$ もイデアルである（命題 4.12）ので，仮定より有限個の元 $a_1, \ldots, a_k \in I$ で生成される．I の定義より，各 $1 \leq j \leq k$ に対して，番号 n_j が存在し $a_j \in I_{n_j}$ である．すべての j に対し $N \geq n_j$ となる N をとる（$k \geq 1$ ならば $N = \max\{n_1, \ldots, n_k\}$ とすればよく，$k = 0$ なら N はなんでもよい）．すると $I_{n_j} \subset I_N$ なので，$a_1, \ldots, a_k \in I_N$ であり，したがって $I \subset I_N$ である．一方で明らかに $I_N \subset I$ なので，$I = I_N$ である．任意の $n \geq N$ に対し，$I_N \subset I_n \subset I = I_N$ なので $I_n = I_N$ である．すなわちこの列は停止する．

（$\neg$(2) $\implies$ $\neg$(1)）：I を有限生成でないイデアルとする．I に含まれる有限生成イデアルの真の増大列 $I_0 \subsetneq I_1 \subsetneq \ldots$ を帰納的に構成する．$I_0 = (0)$ とする．I_n までできたとする．I_n は有限生成で I は有限生成でないので $I_n \subsetneq I$ である．言い換えると，$a \in I$ かつ $a \notin I_n$ を満たす元が存在する．$I_{n+1} = I_n + (a)$ とおく．構成より，I_{n+1} も有限生成であり，$I_n \subsetneq I_{n+1}$ である． □

余談 12.6. （$\neg$(2) $\implies$ $\neg$(1)）の構成で暗に選択公理を使ったわけですが（無限個の $I \setminus I_n$ から元をとったので），ZF 上では (1) と (2) は同値ではないらしいです． ◊

12.2 ネーター環の例

この小節で証明する命題 12.7 の前半と命題 12.8 から，ネーター環上有限生成な環はネーターである．ここからたくさんのネーター環の例を作れる．

ネーターでない環の例は 12.4 節で挙げる．

命題 12.7. A を環，$I \subset A$ をイデアルとする．A がネーター環（resp. アルティン環）ならば剰余環 A/I もそうである．

A を環，$S \subset A$ を積閉集合とする．A がネーター環（resp. アルティン環）ならば局所化 $S^{-1}A$ もそうである． ◊

証明. 剰余環 A/I については命題 5.18 から，局所化 A_S については命題 11.20 から，イデアル全体が包含関係に関してなす順序集合は A のそれの部分集合であることが分かる．したがって，A においてイデアルの昇鎖律（resp. 降鎖律）が成り立つならば剰余環や局所化においても成り立つ． □

命題 12.8. A がネーター環ならば，A 上の（1 変数）多項式環 $A[X]$ もネーター環である． ◊

命題 12.8 は**ヒルベルトの基底定理** (*Hilbert's basis theorem*) ともよばれる．これを繰り返し使うことで，任意の n に対して，n 変数多項式環 $A[X_1, \ldots, X_n]$ もネーター環であることが分かる．

証明. $I \subset A[X]$ をイデアルとする．これが有限生成であることを示したい．各 $n \in \boldsymbol{N}$ に対し，集合 I_n を

$$I_n = \{a \in A \mid \text{ある } f \in I \text{ が存在し，} \deg f \leq n \text{ かつ，} f \text{ の } X^n \text{ の係数は } a\}$$

と定めると，I_n は A のイデアルであり，$\cdots \subset I_n \subset I_{n+1} \subset \ldots$ が成り立つ．A がネーターなので，ある N が存在し $I_N = I_{N+1} = \ldots$ が成り立つ．$n \in \boldsymbol{N}$，$n \leq N$ に対し，I_n は有限個の元 $a_{n,1}, \ldots, a_{n,k_n}$ で生成さ

れる．これらを実現する（n 次以下の）多項式 $f_{n,1},\dots,f_{n,k_n}\in I$ をとる．

このとき I は $(f_{n,j})_{n\le N,1\le j\le k_n}$ で生成されることを示そう．これらの元で生成するイデアルを I' とおく．$I'\subset I$ は明らかなので，$I\subset I'$ を示せばよい．$g\in I$, $g\neq 0$ とする．$n=\deg g$ とおく．g の X^n の係数 g_n は I_n に属する．$n>N$ ならば $m:=N$, $n\le N$ ならば $m:=n$ とおくと，(前者の場合 $I_n=I_N$ なので) $g_n\in I_m$ であり，ある $b_1,\dots,b_{k_N}\in A$ に対して $g_n=\sum_j b_j a_{m,j}$ である．すると $g':=g-\sum_j b_j X^{n-m}f_{m,j}\in I$ であり，$\deg g'<n$ である．$g-g'\in I'$ なので，$g\in I'$ は $g'\in I'$ と同値である．この操作を繰り返すことで最終的に 0 に到達し，g は I' の元であることが分かる． □

12.3 ネーター環の性質

ネーター環はある種の「有限性」を意味しており，そこからさまざまな「良い」性質が導かれる．本講義で説明しきることは不可能だが，いくつか有名なものを挙げる．

ネーター環上の 0 でない加群は**素因子** (*associated prime*) を 1 つ以上もつことが証明でき（問題 A.5），この事実をもとに素因子の理論がうまく機能する．詳しくは例えば [松村 80, 6 節] を参照せよ．

定理 12.9 (クルルの交差定理)**.** A をネーター局所環またはネーター整域，$I\subsetneq A$ を真のイデアルとすると，$\bigcap_{n\in\boldsymbol{N}} I^n=0$ である． ◊

証明は例えば [松村 80, 定理 8.10] を見よ．

定理 12.10 (クルルの単項イデアル定理・クルルの標高定理)**.** A をネーター局所環，$I\subset A$ を $r\ge 0$ 個の元で生成されるイデアルとし，$\mathfrak{p}$ を I を含む素イデアルの中で極小なものとすると，その高さ $\operatorname{ht}\mathfrak{p}$ は r 以下である． ◊

$r=1$ の場合が単項イデアル定理とよばれる．証明は例えば [松村 80, 定理 13.5] を見よ．

定義 12.11. 素イデアル $\mathfrak{p}\subset A$ の**高さ** (*height*) とは，$\mathfrak{p}_0\subsetneq\mathfrak{p}_1\subsetneq\cdots\subsetneq\mathfrak{p}_d=\mathfrak{p}$ の形の A の素イデアルの包含列の長さ d の上限（0 以上の整数または無限大）である．$\mathfrak{p}$ の高さを $\operatorname{ht}\mathfrak{p}$ で表す． ◊

12.4 ネーターでない環の例

12.2 節で述べたことから，ネーター環（とくに $\boldsymbol{Z}$ や体）上有限生成な環やその局所化はネーター環である．したがって，ネーターでない環の典型的な作り方は，無限個の生成元を使うことである．

例 12.12. A を零環でない環とする．A 上の（可算）無限個の変数の多項式環 $B=A[X_n\mid n\in\boldsymbol{N}]=A[X_0,X_1,X_2,\dots]$ を考える．（なお，可算無限個の変数の多項式環は定義していない気もするが，$B_m:=A[X_0,X_1,\dots,X_m]$ とおいて $\bigcup_{m\in\boldsymbol{N}}B_m$ だと思えばよい．）B はネーターでない．実際，$m\in\boldsymbol{N}$ に対してイデアル $I_m=(X_0,X_1,\dots,X_m)\subset B$ を考えると，昇鎖 (I_m) は停止しない．別の言い方をすると，イデアル $(X_0,X_1,\dots,X_m,\dots)$ は有限生成でない． ◊

例 12.13. A を零環でない環とする．p を 2 以上の整数とする．$m\in\boldsymbol{N}$ に対して，$B_m=A[X^{1/p^m}]$ を 1 変数の多項式環とし，$X^{1/p^m}=(X^{1/p^{m+1}})^p$ により $B_m\subset B_{m+1}$ とみなす．$B:=\bigcup_{m\in\boldsymbol{N}}B_m$ とおくと B はネーターでない．実際，$m\in\boldsymbol{N}$ に対してイデアル $I_m=(X^{1/p^m})\subset B$ を考えると，昇鎖 (I_m) は停止しない．

$I = \bigcup_{m \in \boldsymbol{N}} I_m$ とおくと，任意の $n \geq 1$ に対して $I^n = I$ なので，クルルの交差定理（定理 12.9）への反例になっている．

ちなみにこの環は UFD でもない．簡単にいうと，X をいくらでも細かく分解できてしまうので． ◊

例 12.14. k を体とし，$B = k[x][x^n y \mid n \in \boldsymbol{Z}] \subset k[x^{\pm 1}, y]$ とする．$\mathfrak{p} = (x^n y \mid n \in \boldsymbol{Z})$，$\mathfrak{m} = (x)$ とすると，$(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$ は素イデアルの包含列である．

$\bigcap_{n \geq 0} \mathfrak{m}^n = \mathfrak{p} \supsetneq (0)$ であり，単項イデアル (x) はこれ自身を含む極小素イデアルで高さ 2 なので，クルルの交差定理（定理 12.9）や単項イデアル定理（定理 12.10）への反例になっている． ◊

少し風味の違う例としては次がある．

命題 12.15. $\boldsymbol{Q}[X]$ の部分環 A を，$A = \{f \in \boldsymbol{Q}[X] \mid$ 任意の $n \in \boldsymbol{Z}$ に対して $f(n) \in \boldsymbol{Z}\}$ で定める．すると A はネーターでない． ◊

証明は演習問題とする（問題 12.3）．

注 12.16. 例 12.14 や命題 12.15，あるいは問題 12.5 から分かるように，ネーター環の部分環は一般にネーター環とは限らない．このことのもっと極端な例として，A をネーターでない整域とすると，$\mathrm{Frac}\, A$ は体なのでネーターであり A はその部分環である． ◊

B 節ではさらにいろいろな環の作り方を紹介する．

12.5 アルティン環はネーター環である

一般の順序集合においては，昇鎖律と降鎖律の間に特段の関係はない（一方が成り立つと仮定して，他方は成り立つかもしれないし成り立たないかもしれない）．ところが，環のネーター性とアルティン性に関しては次が成り立つ．

命題 12.17. A がアルティン環ならば，A はネーター環である． ◊

証明は本講義では行わない．例えば [AM69, 定理 8.5] または [松村 80, 定理 3.2] を参照してください．

演習問題

問題 12.1. PID はネーター環であることを示せ．

問題 12.2. ネーター環でない UFD の例を挙げよ．

問題 12.3. 命題 12.15 の環 $A = \{f \in \boldsymbol{Q}[X] \mid$ 任意の $m \in \boldsymbol{Z}$ に対して $f(m) \in \boldsymbol{Z}\}$ を考える．

(1) $n \geq 0$ に対し，

$$f_n(X) := \binom{X}{n} = \frac{X(X-1)(X-2)...(X-(n-1))}{n!} \in \boldsymbol{Q}[X]$$

とおく．$f_n \in A$ を示せ．

(2) p を素数とする．$1 \leq n < p$ ならば $f_n(p) \in p\boldsymbol{Z}$ であり，$n = p$ ならば $f_n(p) \notin p\boldsymbol{Z}$ であることを示せ．

(3) $I_n = (f_1, f_2, f_3, ..., f_n) \subset A$ とすると昇鎖 $\cdots \subset I_n \subset I_{n+1} \subset \ldots$ は停止しないことを示せ．したがっ

て A はネーターでない.

なお，$A = \boldsymbol{Z}[f_n \mid n \geq 0]$ が成り立つ.

問題 12.4. $T \subset \boldsymbol{N} = \{0, 1, 2, \dots\}$ を部分集合とする．$k[X^t \mid t \in T] \subset k[X]$ はネーター環か？

問題 12.5. 次がネーター環になるか答えよ.

(1) k を体とし，$t \in \boldsymbol{R}$ を実数とするとき，$A_1 = k[x][x^i y^j \mid j > 0, i + tj > 0] \subset k[x^{\pm 1}, y^{\pm 1}]$ と，$A_2 = k[x][x^i y^j \mid i + tj > 0] \subset k[x^{\pm 1}, y^{\pm 1}]$.
(2) k を標数が 2 でない体とするとき，$A_3 = \{f \in k[X, Y] \mid f(1, 0) = f(-1, 0)\}$.
(3) k を体とするとき，$A_5 = \{f \in k[X, Y] \mid f(X, 0) = 0\}$.
(4) $A_4 = \boldsymbol{Z}[X][\frac{X^n}{n!} \mid n \in \boldsymbol{N}] \subset \boldsymbol{Q}[X]$.

13 中国剰余定理 [※範囲外]

本節では環はすべて可換とする.

$\boldsymbol{Z}$ の剰余群に関する中国剰余定理（[群論, 命題 8.5]）と同様にして次が示せる.

定理 13.1 (中国剰余定理)**.** A を環，$I_1, \dots, I_n \subset A$ をイデアルとし，$i \neq j$ に対し $I_i + I_j = A$ が成り立つとする．このとき，$[a]$ を $([a], [a], \dots, [a])$ にうつす環の同型写像 $A/I_1 I_2 \dots I_n \cong A/I_1 \times A/I_2 \times \dots A/I_n$ が存在する. ◊

証明. まず $n = 2$ の場合を示す．$I_1 + I_2 = A$ なので，$e_1 + e_2 = 1$ を満たす $e_1 \in I_1$ と $e_2 \in I_2$ をとれる．このとき,

$$\begin{aligned} \alpha\colon A/I_1 I_2 \to A/I_1 \times A/I_2\colon &\qquad [a] \mapsto ([a], [a]), \\ \beta\colon A/I_1 \times A/I_2 \to A/I_1 I_2\colon &\qquad ([b_1], [b_2]) \mapsto [b_1 e_2 + b_2 e_1] \end{aligned}$$

が well-defined であり，アーベル群の準同型であり，互いに逆であることが確かめられる．さらに α は明らかに積を保つので，環同型写像である.

一般の n に対しては，$I_i + I_j = A$ かつ $I_i + I_k = A$ ならば $I_i + I_j I_k = A$ なので，$n = 2$ の場合を繰り返し用いればよい. □

なお，（$i \neq j$ に対し $I_i + I_j = A$ が成り立つという）仮定の下で $I_1 I_2 \dots I_n = I_1 \cap I_2 \cap \dots \cap I_n$ なので，共通部分の形で定理を述べることもある.

参考文献

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. 新妻弘（訳）, 可換代数入門, 共立出版, 2006.

[松村 80] 松村 英之, 可換環論, 共立出版, 1980.

[群論] 松本 雄也, 群論講義ノート (2022). 近日公開予定.

ここ以降は意欲のある人向けの付録なので講義では扱いません.

A 環上の加群

線形代数学で扱った体上のベクトル空間の一般化として，環上の加群というものを導入する.
可換と限らない環上の加群も重要だが，A.2 節以降では可換環上の加群のみ考える.

A.1 環上の加群の定義

定義 A.1 (左加群)**.** A が環，M が加群，$\cdot$ が写像 $A \times M \to M$ で，(この写像による (a, m) の像を $a \cdot m$ と書き,) これが次の条件を満たすとき M を**左 A 加群** (*left A-module*) であるという.

(1) 任意の $a, b \in A$ と $m \in M$ に対し，$(a + b) \cdot m = a \cdot m + b \cdot m$.
(2) 任意の $a \in A$ と $m, n \in M$ に対し，$a \cdot (m + n) = a \cdot m + a \cdot n$.
(3) 任意の $a, b \in A$ と $m \in M$ に対し，$(a \cdot b) \cdot m = a \cdot (b \cdot m)$.
(4) 任意の $m \in M$ に対し，$1_A \cdot m = m$. ◊

補題 A.2. M が A 加群のとき，次が成り立つ.

- $m \in M$ に対し，$0_A \cdot m = 0_M$.
- $m \in M$ に対し，$(-1_A) \cdot m = -m$. (なお，左辺の -1_A は A の乗法の単位元 1_A の加法に関する逆元であり，右辺の $-$ は M の加法に関する逆元である.) ◊

証明. 環での $0 \cdot a = 0$ や $(-1) \cdot a = -a$ の証明と同様にできる. □

定義 A.3 (右加群)**.** A が環，M が加群，$\cdot$ が写像 $M \times A \to M$ で，(この写像による (m, a) の像を $m \cdot a$ と書き,) これが次の条件を満たすとき M を**右 A 加群** (*right A-module*) であるという.

(1) 任意の $a, b \in A$ と $m \in M$ に対し，$m \cdot (a + b) = m \cdot a + m \cdot b$.
(2) 任意の $a \in A$ と $m, n \in M$ に対し，$(m + n) \cdot a = m \cdot a + n \cdot a$.
(3) 任意の $a, b \in A$ と $m \in M$ に対し，$m \cdot (a \cdot b) = (m \cdot a) \cdot b$.
(4) 任意の $m \in M$ に対し，$1_A \cdot m = m$. ◊

注 A.4. 左加群と右加群の定義において本質的な違いは定義 A.1 の条件 (3) と定義 A.3 の条件 (3) で，A の元 a と b を続けて作用させた結果が ab の作用になるか ba の作用になるかである.
A が可換ならば，左 A 加群と右 A 加群の概念は一致し，これを単に **A 加群** (*A-module*) という. ◊

注 A.5. k が可換体ならば，k 加群とは k ベクトル空間のことに他ならない. ◊

例 A.6. A を環とする．A 自身は自然な方法（環の乗法をそのまま使う）で左 A 加群かつ右 A 加群になる.
A の左イデアルとは，左 A 加群 A の部分左 A 加群に他ならない．右イデアルについても同様である. ◊

命題 A.7. アーベル群には一意的に $\boldsymbol{Z}$ 加群の構造が定まる. ◊

証明. M をアーベル群とする．$n \in \boldsymbol{Z}$ と $x \in M$ に対し，

$$n \cdot x := \begin{cases} \overbrace{x + \cdots + x}^{n\text{ 個}} & (n > 0), \\ 0_M & (n = 0), \\ \underbrace{(-x) + \cdots + (-x)}_{-n\text{ 個}} & (n < 0), \end{cases}$$

と定めると，$\boldsymbol{Z}$ 加群になる（詳細は省略）．

逆に，M が $\boldsymbol{Z}$ 加群のとき，$n \cdot x$ が上に一致する：$n = 1, 0, -1$ のときは明らか，$n \geq 1$ や $n \leq -1$ のときは帰納法を用いる． □

注 A.8. $a \neq 0$ かつ $m \neq 0$ でも $am = 0$ となりうる（体上のベクトル空間との相違点の 1 つ）． ◊

以下本節の終わりまで，簡単のため可換環 A 上の加群のみを考える．

A.2 A 加群に関する基本的概念

アーベル群（$= \boldsymbol{Z}$ 加群）に関するさまざまな概念は A 加群に対して一般化される．

部分アーベル群 $M' \subset M$ が A 作用で閉じているとき**部分 A 加群** (A-*submodule*) という．

$M' \subset M$ が部分加群であるとき，剰余アーベル群 M/M' に自然に A 作用が定まる．これを**剰余加群**または**商加群** (*quotient module*) という．

イデアルの場合と同様に，いくつかの部分 A 加群の共通部分や和も部分 A 加群になり，また，部分集合が生成する部分 A 加群も同様に定義される．

A 加群 M と A のイデアル I に対して，IM は部分集合 $\{am \mid a \in I, m \in M\}$ が生成する部分 A 加群である．

A 加群 M_1, M_2 の間の（アーベル群としての）準同型 $f\colon M_1 \to M_2$ が，任意の $a \in A$ と $m \in M_1$ に対して $f(a \cdot m) = a \cdot f(m)$ を満たすとき，A 加群としての準同型写像，または短く A **準同型** (A-*homomorphism*) という．A **線形** (A-*linear*) であるともいう．

全単射である A 準同型写像を A 同型写像といい，そのとき逆写像も A 準同型である．

A 準同型の核，像はアーベル群の準同型としてのそれだが，自動的に A 部分加群になる．準同型定理も同様に成り立つ．

A 加群の族の直和加群，直積加群もアーベル群の場合と同様に定義され，添字集合が有限ならば直和と直積は一致する．

M, N が A 加群のとき，M から N への A 準同型全体の集合 $\mathrm{Hom}_A(M, N)$ には自然に A 加群の構造が入る：$a \in A$ と $f \in \mathrm{Hom}_A(M, N)$ に対して $(af)(m) := af(m) = f(am)$ とする．（なお，これは A が可換であることを使っており，非可換環 A 上の例えば左加群の間の Hom には左右どちらの A 加群構造も入らない．）

$\mathrm{End}_A(M) := \mathrm{Hom}_A(M, M)$ も A 加群であり，A 準同型写像の合成により自然に（一般に非可換な）環の構造が入る．

A 準同型 $f\colon N_1 \to N_2$ と合成するという写像 $f \circ -\colon \mathrm{Hom}_A(M, N_1) \to \mathrm{Hom}_A(M, N_2)\colon \phi \mapsto f \circ \phi$ は A 準同型である．

A 準同型 $g\colon M_1 \to M_2$ と合成するという写像 $- \circ g\colon \mathrm{Hom}_A(M_2, N) \to \mathrm{Hom}_A(M_1, N)\colon \phi \mapsto \phi \circ g$ は A 準同型である．

A.3 A 加群に関する基本的概念・続き

定義 A.9. A 加群 M に対して $\{a \in A \mid aM = 0\}$ はイデアルである．これを M の**零化イデアル** (*annihilator*) とよび，$\mathrm{Ann}(M)$ と表す．

より一般に A 加群 M の部分集合 S に対しても $\mathrm{Ann}(S) = \{a \in A \mid s \in S \text{ ならば } as = 0\}$ と定めることができる． ◊

例 A.10. （A が可換ならば）$\mathrm{Ann}(A/I) = I$ である． ◊

定義 A.11. $\mathrm{Ann}(M) = 0$ である加群 M を**忠実加群** (*faithful module*) という． ◊

定義 A.12. いくつか（無限個でもよい）の A 加群 A の直和に同型な加群を**自由 A 加群** (*free A-module*) という．r 個の直和に同型なとき，その**階数** (*rank*) が r であるという． ◊

注 A.13. A が体のときは，A 加群すなわち A ベクトル空間はつねに基底をもち，自由加群であった．A が体でないときは，自由でない加群が大量に存在する．例えば 0 でも A でもないイデアル I に対する A/I はそうである． ◊

注 A.14. A が零環でない場合，自由加群 M の階数は（無限である場合も含めて）一意に定まる．証明にはテンソル積（A.5 節）を用いる．$A^{\oplus r}$ と $A^{\oplus r'}$ が同型ならば，A の極大イデアル $\mathfrak{m}$ をとって $k := A/\mathfrak{m}$ とし，$A^{\oplus r} \cong A^{\oplus r'}$ の両辺に $\otimes_A k$ することにより $k^{\oplus r} \cong k^{\oplus r'}$ を得る．ベクトル空間の次元の一意性より $r = r'$ である． ◊

A.4 ネーター加群，アルティン加群

定義 A.15. A を環とする．A 加群 M が**ネーター加群** (*Noetherian module*)　(resp. **アルティン加群** (*Artinian module*)) であるとは，その加群の部分加群全体が包含関係に関してなす順序集合が昇鎖律（resp. 降鎖律）を満たすことをいう． ◊

例 A.16. A 加群 A がネーター（resp. アルティン）加群であることは，A が（左）ネーター環であることと同値である．というのは，（左）A 加群としての A の部分加群とは A の（左）イデアルに他ならないので． ◊

例 A.17. $M_n = \frac{1}{2^n}\boldsymbol{Z} \subset \boldsymbol{Q}$ とし，$M = \bigcup_{n \in \boldsymbol{N}} M_n$ とし，$L_n = M_n/\boldsymbol{Z}$，$L = M/\boldsymbol{Z}$ とすると，L の部分 $\boldsymbol{Z}$ 加群は L および L_n しかないので，L はアルティン $\boldsymbol{Z}$ 加群である．ネーター $\boldsymbol{Z}$ 加群ではない． ◊

注 A.18. ネーター加群であることと任意の部分加群が有限生成であることは同値である．このことは命題 12.5 と全く同様に証明できる． ◊

命題 A.19. ネーター（resp. アルティン）加群の部分加群や剰余加群はまたネーター（resp. アルティン）である． ◊

略証. 部分加群または剰余加群の部分加群全体のなす順序集合は，もとの加群の部分加群全体のなす順序集合の部分集合である． □

命題 A.20. M が A 加群，$M' \subset M$ が部分加群で，M' と M/M' がネーター（resp. アルティン）ならば，M もネーター（resp. アルティン）である． ◊

証明. (N_n) が M の部分加群の昇鎖（resp. 降鎖）だとする．$(N_n \cap M')$ と $((N_n + M')/M')$ はそれぞれ M' と M/M' の昇鎖（resp. 降鎖）なので仮定より停止する．両方が停止したら (N_n) も停止することが $(N_n/(N_n \cap M') \cong (N_n + M')/M'$ を使うと）分かる． □

命題 A.21. A がネーター（resp. アルティン）環ならば，有限生成 A 加群はネーター（resp. アルティン）である． ◊

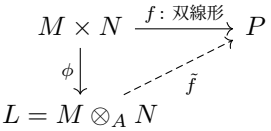
証明. A 加群 A は仮定よりネーター（resp. アルティン）である．$A^{\oplus r+1}/A^{\oplus r} \cong A$ なので，命題 A.20 から帰納的に $A^{\oplus r}$ もネーター（resp. アルティン）である．有限生成加群は $A^{\oplus r}$ の剰余加群なので，再び命題 A.20 よりネーター（resp. アルティン）である． □

A.5 テンソル積

言及したい場面があるので最低限の定義だけ書いておきます．詳細は環上の加群の適当な教科書を参照してください．

A を環とし，M, N, P を A 加群とする．写像 $f\colon M \times N \to P$ が A **双線形** (*bilinear*) であるとは，任意の m に対して $N \to P\colon n \mapsto f(m,n)$ が A 準同型であり，かつ任意の n に対して $M \to P\colon m \mapsto f(m,n)$ が A 準同型であることをいう．

命題 A.22. A を環とし, M, N を A 加群とする．このとき次を満たす A 加群 L と A 双線形写像 $\phi\colon M \times N \to L$ が存在する：任意の A 双線形写像 $f\colon M \times N \to P$ に対し，A 線形写像 $\tilde{f}\colon L \to P$ が一意に存在し $f = \tilde{f} \circ \phi$ を満たす．すなわち，任意の A 加群 P に対し写像 $\mathrm{Hom}_A(L,P) \to \mathrm{Bil}_A(M \times N, P)\colon \tilde{f} \mapsto \tilde{f} \circ \phi$ は全単射である．ただし Bil は双線形写像全体の集合を表す．（この条件を，テンソル積の普遍性という．）



さらに，(L, ϕ) は一意的な同型を除いて一意に定まる（すなわち，(L,ϕ) と (L',ϕ') がどちらも条件を満たすならば，同型写像 $\psi\colon L \to L'$ が一意に存在し $\psi \circ \phi = \phi'$ を満たす）．L のことを $M \otimes_A N$ と書き，M と N の**テンソル積** (*tensor product*) とよぶ．また，$L = M \otimes_A N$ の元 $\phi(m,n)$ を $m \otimes n$ と書く． ◊

存在の証明は省略する（適当な環上の加群の教科書を参照せよ）．一意性の部分はテンソル積の普遍性から分かる．

M，N がそれぞれ $(m_i)_{i \in I}$ と $(n_j)_{j \in J}$ を基底とする自由 A 加群のときは，$M \otimes N$ は $(m_i \otimes n_j)_{(i,j) \in I \times J}$ を基底とする自由 A 加群である．A が体ならばつねにこの形で表せる．

一般の加群のテンソル積の記述はもっと複雑だが，A 加群 $M \otimes N$ が部分集合 $\{m \otimes n \mid m \in M, n \in N\}$ で生成されることはいえるので，テンソル積の元について何かを定めたり何かが成り立つことを示す際にこの形の元を考えれば十分であることが多い．

定義 A.23. A を環，M を A 加群，B を A 代数とすると，$M \otimes_A B$ には自然に B 加群構造が入る $(b \cdot (m \otimes b') := m \otimes bb')$．この B 加群 $M \otimes_A B$ を A 加群 M の**係数拡大** (*extension of scalars*) という．$\Diamond$

定義 A.24. A を環，B と C を A 代数とすると，$B \otimes_A C$ には自然に A 代数（および B 代数，C 代数）の構造が入る（積は $(b \otimes c) \cdot (b' \otimes c') := bb' \otimes cc'$）．$\Diamond$

例 A.25. k を体，$k' \supset k$ を拡大体，$P(X) \in k[X]$ を多項式とするとき，$k[X] \otimes_k k'$ は $k'[X]$ と自然に同型であり，$k[X]/(P(X)) \otimes_k k'$ は $k'[X]/(P(X))$ と自然に同型である．$P(X)$ が $k[X]$ の既約多項式であり $k'[X]$ の元としては既約多項式でない場合，整域と体のテンソル積が整域でない例になる．$\Diamond$

A.6 複体，完全列，ホモロジー代数

この小節についても，詳細は適当な環上の加群の教科書を参照してください．

A 加群と A 準同型からなる列

$$\cdots \to C^{n-1} \xrightarrow{f^{n-1}} C^n \xrightarrow{f^n} C^{n+1} \to \dots$$

を考える．この列のことを $C^\bullet$ と表す．なお，添字が減る方向の列 $C_\bullet \colon \cdots \to C_n \xrightarrow{f_n} C_{n-1} \to \dots$ を考えることもあり，その場合は添字を右上でなく右下につけることが多い．また，左または右または両方が有限個で止まるものも考える．

この列が A 加群の**コチェイン複体** (*cochain complex*)（または単に**複体** (*complex*)）であるとは，各 n に対して $f^n \circ f^{n-1} \colon C^{n-1} \to C^{n+1}$ が 0 であることをいう．これは $\mathrm{Im}(f^{n-1}) \subset \mathrm{Ker}(f^n)$ と同値である．$H^n(C^\bullet) := \mathrm{Ker}(f^n)/\mathrm{Im}(f^{n-1})$ をこの複体の**コホモロジー** (*cohomology*) という．

添字が減る方向の場合は，各 n に対し $f_n \circ f_{n+1} \colon C_{n+1} \to C_{n-1}$ が 0 であるとき**チェイン複体** (*chain complex*)（または単に複体）といい，$H_n(C_\bullet) := \mathrm{Ker}(f_n)/\mathrm{Im}(f_{n+1})$ を**ホモロジー** (*homology*) という．

複体がさらに $\mathrm{Im}(f^{n-1}) = \mathrm{Ker}(f^n)$（チェイン複体の場合は $\mathrm{Im}(f_{n+1}) = \mathrm{Ker}(f_n)$）を満たすとき，**完全列** (*exact sequence*) であるという．

複体にさまざまな関手（$\mathrm{Hom}_A(-, N)$，$\mathrm{Hom}_A(M, -)$，$- \otimes_A N$ など）を施すと新たな複体が得られる．もとの複体が完全であっても，新しい複体が完全とは限らない．完全にどれだけ近い・遠いかを調べるのがホモロジー代数（の一部）である．

演習問題

問題 A.1 を除き，環 A, B は可換だと仮定する．

問題 A.1.（この問題は A の可換性を仮定しない．）$f \colon A \to A$ が左 A 加群としての準同型ならば，ある $x \in A$ が存在して $f(y) = yx$ であることを示せ．

問題 A.2. M を A 加群とする．$A \to \mathrm{End}_A(M)$ を $a \mapsto (m \mapsto a \cdot m)$ で定めると環準同型であることを示せ．$\mathrm{Ann}(M) = \mathrm{Ker}(A \to \mathrm{End}_A(M))$ を示せ．

問題 A.3. 次を示せ．$\mathrm{Ann}(A/I) = I$．$\mathrm{Ann}(A/I \oplus A/J) = I \cap J$．$\mathrm{Ann}((I+J)/I) = (I : J)$．

問題 A.4. A を環，$I \subset A$ をイデアルとし，M, N を A/I 加群とする．M, N は自然に A 加群とみなせるこ

とを示せ．写像 $f\colon M \to N$ が A/I 線形であることと A 線形であることは同値であることを示せ．

問題 A.5. A がネーター環で M が 0 でない A 加群ならば，$\mathrm{Ann}(x) \subset A$ が素イデアルである $x \in M$ が存在することを示せ．
余談. $\mathrm{Ann}(x)$（$x \in M$）の形に表せる A の素イデアルを，A 加群 M の**素因子** (*associated prime*) という．素因子全体の集合を $\mathrm{Ass}(M)$ と表す．この問題より，ネーター環上の 0 でない加群は素因子をもつ（Ass は空でない）．

問題 A.6. 次のそれぞれに対して，条件を満たす環 A と A 加群の完全列 $0 \to M_1 \to M_2 \to M_3 \to 0$ と A 加群 N の例を与えよ．

- $0 \to \mathrm{Hom}_A(N, M_1) \to \mathrm{Hom}_A(N, M_2) \to \mathrm{Hom}_A(N, M_3) \to 0$ は完全でない．
- $0 \to \mathrm{Hom}_A(M_3, N) \to \mathrm{Hom}_A(M_2, N) \to \mathrm{Hom}_A(M_1, N) \to 0$ は完全でない．
- $0 \to M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N \to 0$ は完全でない．

問題 A.7. A 加群 M, N, P に対して次の同型を示せ：$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$．

問題 A.8. B を A 代数とする．B 加群 N に対して，N を A 加群とみなしたものを $N|_A$ とおく．A 加群 M と B 加群 N に対して次の同型を示せ：$\mathrm{Hom}_B(M \otimes_A B, N) \cong \mathrm{Hom}_A(M, N|_A)$．

問題 A.9. M を A 加群とし，$x \in M$ を元とする．A の部分集合 $O(x)$ を，$O(x) = \{f(x) \mid f \in \mathrm{Hom}_A(M, A)\}$ で定める．

(1) $\mathrm{ev}_x\colon \mathrm{Hom}_A(M, A) \to A$ を，$\mathrm{ev}_x(f) = f(x)$ で定める（すなわち，x を代入するという操作である）．ev_x は A 加群の準同型であることを示せ．
(2) $O(x)$ は A のイデアルであることを示せ．

余談. この $O(x)$ の形に表せるイデアルは *order ideal* とよばれる．

B 環の例

B.1 多項式環の亜種：モノイド環，群環

モノイドについては [群論, B 節] を参照してください．群でないモノイドの基本的な例は自然数全体の集合 $\boldsymbol{N}$ が加法に関してなすモノイドです．

定義 B.1. A を環，M をモノイドとする．M の演算は乗法で書く．直和アーベル群 $A[M] := \bigoplus_{m \in M} A = \{(a_m) \in A^M \mid \text{有限個の } m \text{ を除き } a_m = 0\}$ に対し，多項式環と同様に加法と乗法を定める：すなわち，加法は m ごとに和をとり，乗法は，$(a_m), (b_m) \in A[M]$ に対し，$c_m := \sum_{p,q \in M, pq=m} a_p b_q$ とし（これは有限和である[*7]），$(a_m) \cdot (b_m) := (c_m)$ とする．これを**モノイド環** (*monoid ring*) という．M が群のときは**群環** (*group ring*) ともいう．

[*7] $(p, q) \in M^2$ で $pq = m$ を満たすものは無限個存在しうるが（無限個の元の和は定義されないが），それらのうち $a_p b_q \neq 0$ なものは有限個しかないので，0 でない有限個の和と解すればよく，問題なく定義される．というのが「有限和である」の意味するところである．

$m \in M$ に対し，m 番目のみが 1 でそれ以外は 0 である $A[M]$ の元を例えば $[m]$ と書く．（誤解がなさそうなら $[m]$ を単に m と書くこともあるかもしれない．）すると $A[M]$ は $[m]$（$m \in M$）を基底とする自由 A 加群であり，$[m] \cdot [m'] = [mm']$ を満たす．$(a_m) \in A[M]$ のことを $\sum_{m \in M} a_m[m]$ と書く．これは有限和である．

A と M の両方が可換ならば $A[M]$ も可換である．

M が可換で演算を加法で書くときは，$[m]$ の代わりに例えば X^m と書く（$X^m \cdot X^{m'} = X^{m+m'}$ を満たす）．この場合，不定元を明示するために $A[M]$ の代わりに $A[X; M]$ などと書く． ◊

例 B.2. $M = \boldsymbol{N}$ が自然数全体のモノイドならば $A[X; \boldsymbol{N}]$ は通常の多項式環 $A[X]$ に自然に同型である．もう少し一般に，$A[X; \boldsymbol{N}^d]$ は通常の d 変数多項式環 $A[X_1, \dots, X_d]$ に自然に同型である（第 i 成分のみが 1 で他の成分のみが 0 である $\boldsymbol{N}^d$ の元 e_i に対して，X^{e_i} と X_i を対応させる）． ◊

例 B.3. $M = \boldsymbol{N}^{\oplus \boldsymbol{N}}$ を $\boldsymbol{N}$ で添字づけられた可算無限個の $\boldsymbol{N}$ の直和，すなわち

$$M = \{(m_i)_{i \in \boldsymbol{N}} \in \prod_{i \in \boldsymbol{N}} \boldsymbol{N} \mid \text{有限個の } i \text{ を除き } m_i = 0\}$$

とすると，$A[X; M]$ は例 12.12 で見た無限変数多項式環である． ◊

例 B.4. M が $\boldsymbol{N}$ の部分モノイド $\boldsymbol{N} \setminus \{1\} = \{0, 2, 3, 4, 5, \dots\}$ のとき，$A[X; M] = A[X^2, X^3]$ であり，A を体 k とするとこれは問題 9.3(3) に登場した環と同型である．

$n \geq 2$ が整数で，M が $\boldsymbol{N}^2$ の部分モノイド $\{(i, j) \in \boldsymbol{N}^2 \mid i - j \equiv 0 \pmod{n}\}$ のとき，$A[X; M]$ は A を体 k とすると問題 9.3(5) に登場した環と同型である． ◊

注 B.5. $A = k$ が標数 0 の体で G が有限群のとき，群環 $k[G]$ は半単純環（定義は省略）になることが知られており，半単純環は斜体上の行列環の直積に書けることが知られている（Wedderburn–Artin の定理）．問題 H.13 も見よ． ◊

B.2 形式冪級数環と収束冪級数環

本小節では環は可換とする．

B.2.1 形式冪級数環

定義 B.6. A を環とする．直積集合 $A[[X]] := A^{\boldsymbol{N}}$ に対し，多項式環と同様に加法と乗法を定める：すなわち，加法は n ごとに和をとり，乗法は，$(a_n), (b_n) \in A[[X]]$ に対し，$c_n := \sum_{p,q \in \boldsymbol{N}, p+q=n} a_p b_q$ とし，$(a_n) \cdot (b_n) := (c_n)$ とする．どの n に対しても，$p + q = n$ を満たす $(p, q) \in \boldsymbol{N}^2$ は有限個しかないため，これは有限和である[*8]．この加法と乗法により $A[[X]]$ が環になることは簡単に確かめられる．乗法の単位元は $(1, 0, 0, \dots)$ である．$(a_n) \in A[X]$ のことを $\sum_{n \geq 0} a_n X^n$ と書く．多項式の場合と異なり，これは有限和ではなく形式的な記号である．この環を A 上の 1 変数の**形式冪級数環** (*formal power series ring*) という． ◊

$\boldsymbol{N}$ の代わりに $\boldsymbol{N}^d$ を考えることで，d 変数の形式冪級数環も考えられる．これは形式冪級数環をとる操作を d 回繰り返しても得られる（問題 B.1(1) を見よ）．

[*8] 「有限和である」は，有限か否かが明らかでなかった添字集合 $\{(p, q) \in \boldsymbol{N}^2 \mid p + q = n\}$ が実は有限である，という意味で使っている．

注 B.7. $A[X]$ は $A[[X]]$ の部分環とみなせる．多変数の場合も同様である．なお，複数の変数があり [] と [[]] が混ざっていると話はややこしい．例えば問題 B.1(2) を見よ． ◊

注 B.8. ただのアーベル群の無限個の元の和は一般には定義されないが，アーベル群に位相が導入されていれば収束する無限和を考えることもできる．

$A[[X]]$ の位相を，$f \in A[[X]]$ に対し f の基本近傍系を $(f + X^n A[[X]])_{n\in \boldsymbol{N}}$ とすることで定める．ただし $f + X^n A[[X]] = \{f + g \mid g \in X^n A[[X]]\}$ である．このとき $\sum_{n\geq 0} a_n X^n$ は収束する無限和である．なお，この位相に関して，$A[[X]]$ は単に環でありかつ位相空間であるだけでなく，位相環になりしかも完備である（位相環の詳細は G.2 節を見よ）． ◊

注 B.9. 多項式環の場合と異なり，形式冪級数環の不定元には任意の元を代入できるわけではない．例えば $1 + X + X^2 + \ldots$ に $X = 1$ を代入するのはいかにもまずそうである．しかし，冪零な元ならば代入することができる．というのは，x が冪零ならば $\sum_{n\in \boldsymbol{N}} a_n x^n$ は有限和になるからである．この代入写像は環準同型になることも確認できる．もう少し一般に，A が完備な位相環のとき A の位相的冪零な元を代入することはできる．詳細は省略する． ◊

命題 B.10 (cf. 命題 12.8)**.** A がネーター環ならば，A 上の（1 変数）形式冪級数環 $A[[X]]$ もネーター環である． ◊

したがって，n 変数形式冪級数環もネーター環である．

証明. $I \subset A[[X]]$ をイデアルとする．これが有限生成であることを示したい．各 $n \in \boldsymbol{N}$ に対し，集合 I_n を

$$I_n = \{a \in A \mid \text{ある } f \in I \text{ が存在し，} f \text{ の } X^n \text{ の係数は } a \text{ で，} m < n \text{ ならば } X^m \text{ の係数は } 0\}$$

と定めると，I_n は A のイデアルであり，$\cdots \subset I_n \subset I_{n+1} \subset \ldots$ が成り立つ．A がネーターなので，ある N が存在し $I_N = I_{N+1} = \ldots$ が成り立つ．$n \in \boldsymbol{N}$，$n \leq N$ に対し，I_n は有限個の元 $a_{n,1}, \ldots, a_{n,k_n}$ で生成される．これらを実現する（n 次未満の係数が 0 である）元 $f_{n,1}, \ldots, f_{n,k_n} \in I$ をとる．

このとき I は $(f_{n,j})_{n\leq N, 1\leq j\leq k_n}$ で生成されることを示そう．これらの元で生成するイデアルを I' とおく．$I' \subset I$ は明らかなので，$I \subset I'$ を示せばよい．$g \in I$ とする．$g^{(i)} \in I \cap X^i A[[X]]$（$i = 0, 1, \ldots$）を次で帰納的に定義する．$g^{(0)} = g$ とする．$g^{(i)}$ が定義されたとして $g^{(i+1)}$ を定める．$g^{(i)}$ の X^i の係数 c_i は I_i の元である．$i > N$ ならば $m := N$，$i \leq N$ ならば $m := i$ とおくと，（前者の場合 $I_i = I_N$ なので）$c_i \in I_m$ であり，ある $b_1^{(i)}, \ldots, b_{k_m}^{(i)} \in A$ に対して $c_i = \sum_{j=1}^{k_m} b_j^{(i)} a_{m,j}$ である．$g^{(i+1)} := g^{(i)} - \sum_{j=1}^{k_m} b_j^{(i)} X^{i-m} f_{m,j}$ と定める．

構成より，各 i に対して $g^{(i)} - g^{(i+1)} \in I'$ であり，また $g^{(N)} = \sum_{j=1}^{k_N} (\sum_{i\geq N} b_j^{(i)} X^{i-N}) f_{N,j}$ も（$f_{N,j} \in I'$ と $A[[X]]$ の元の積の有限和なので）I' の元なので，$g = \sum_{0\leq i<N} (g^{(i)} - g^{(i+1)}) + g^{(N)} \in I'$ である． □

$A((X)) := A[[X]][X^{-1}]$ は形式冪級数に有限個の負冪の項を加えた級数からなる環であり，1 元 X による局所化でもある．この環の元を**形式ローラン級数** (*formal Laurent power series*) という．A が体ならば $A((X)) = \operatorname{Frac} A[[X]]$ でありこれは体である．

B.2.2 収束冪級数環

A に適切な構造が入っていれば，冪級数の収束や収束半径を考えることができる．ここでは $A = \boldsymbol{C}$ の場合のみ考える．$\boldsymbol{C}$ の原点上の近傍での正則関数を考えると，その Taylor 展開が考えられ，収束半径は正の実数または無限大である．$r > 0$ に対し，$B_r := \{\sum_{n\geq 0} a_n z^n \mid \text{収束半径は } r \text{ 以上である}\}$ とする（条件を言い換

えると，$\limsup_{n\to\infty}(a_n)^{1/n} \le \frac{1}{r}$ である）．B_r は $\boldsymbol{C}[[z]]$ の（真の）部分環であり，$r < r'$ のとき $B_r \supsetneq B_{r'}$ である．また，$r \ge 0$ に対し，$B_{r+} := \bigcup_{s>r} B_s$ とおくと，B_{r+} も $\boldsymbol{C}[[z]]$ の（真の）部分環であり，$r > 0$ に対し $B_r \supsetneq B_{r+}$ である．

これらの環の元に有限個の負冪の項を加えた級数からなる環も考えられる（形式ローラン級数の場合と同様に，1 元 z による局所化でもある）．

$0 < r_1 < r_2$ を正の実数として，円環 $\{z \in \boldsymbol{C} \mid r_1 < |z| < r_2\}$ で収束する冪級数からなる環 $B_{(r_1,r_2)}$ を考えることもできる．$B_{(r_1,r_2)}$ の元は，正の方向と負の方向それぞれに無限である（かもしれない）級数 $\sum_{n\in\boldsymbol{Z}} a_n z^n$ であって，$\sum_{n\ge 0} a_n z^n$ は $|z| < r_2$ で収束し，$\sum_{n\le 0} a_n z^n$ は $|z| > r_1$ で収束するものである．条件を言い換えると，$\limsup_{n\to\infty}(a_n)^{1/n} < \frac{1}{r_2}$ かつ $\liminf_{n\to-\infty}(a_n)^{-1/n} > \frac{1}{r_1}$ である．$\sum_{n\in\boldsymbol{Z}} a_n z^n$ と $\sum_{n\in\boldsymbol{Z}} b_n z^n$ の積は $\sum_{n\in\boldsymbol{Z}} c_n z^n$，ただし $c_n := \sum_{k\in\boldsymbol{Z}} a_k b_{n-k}$，と定める．$c_n$ を定義する和が絶対収束し $\sum_{n\in\boldsymbol{Z}} c_n z^n$ が再び $B_{(r_1,r_2)}$ の元となることの証明は演習問題とする（問題 B.2）． この環の元を**ローラン級数** (*Laurent series*) という．

B.3 非可換な環の例

例 B.11 (非可換多項式環)**.** 自由群と同様に自由モノイドを定義できる．例えば，2 元 X, Y が生成する自由モノイド $\langle X, Y\rangle$ の元は，X と Y を 0 個以上有限個並べた語である．A を可換環とし，自由モノイド $\langle X, Y\rangle$ に対するモノイド環を考え，これを非可換多項式環とよび $A\langle X, Y\rangle$ などと表す．（$A \ne 0$ ならば）$XY \ne YX$ である． ◊

例 B.12 (Dieudonné 環)**.** 非可換多項式環とは逆に，不定元同士は可換だが係数と可換でない環を考えることもある．A を可換な環，$\sigma\colon A \to A$ を環の自己同型として，A 加群 $R = \bigoplus_{n\in\boldsymbol{N}} AT^n$ に積を $T \cdot a = \sigma(a) \cdot T$ が成り立つように定めると，（$\sigma \ne \mathrm{id}$ ならば）非可換な環になる．

W を所定の可換環，$\sigma\colon W \to W$ を所定の自己同型として，W 加群として 2 変数多項式環 $W[F, V]$ を用意し，乗法を $Fw = \sigma(w)F$，$wV = V\sigma(w)$（$w \in W$）が成り立つように定め，さらに関係式 $FV = VF = p$ で割ったものが Dieudonné 環である． ◊

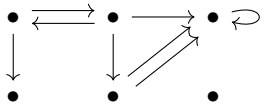
例 B.13. k を体とし $A = k[x]$ とする．$\mathrm{End}_k(A)$ を k ベクトル空間 A から自身への k 線形写像全体とすると環である．A の元 $f \in A$ は $g \mapsto f \cdot g$ という $\mathrm{End}_k(A)$ の元を定め，$A \to \mathrm{End}_k(A)$ は環準同型である．A の像と $\frac{d}{dx}$ が生成する $\mathrm{End}_k(A)$ の部分環を $k\langle x, \frac{d}{dx}\rangle$ と書く．これは非可換環であり，交換子 $[\frac{d}{dx}, x]$ は 1 に等しい．$k\langle x, \frac{d}{dx}\rangle$ は $k\langle X, Y\rangle/(XY - YX - 1)$ に同型である（たぶん）． ◊

B.4 箙代数

モノイドでは任意の 2 元に対して積が定義されるが，限られた場合にのみ積を定義する代数系も考えられる．例えば，不特定の集合間の写像からなる集合では，2 つの写像の合成が定義できるのは 1 つめの終域と 2 つめの定義域が一致している場合（あるいは考え方によっては，前者が後者に含まれる場合）に限られる．

定義 B.14 (箙)**.** **箙** (*quiver*) または**有向グラフ** (*directed graph*)（または *oriented graph*）とは，形式的には，2 つの集合 V, E と 2 つの写像 $s, t\colon E \to V$ の組である．V の元を**頂点** (*vertex*) とよび，E の元を**辺** (*edge*) とよび，$e \in E$ に対し $s(e), t(e) \in V$ をそれぞれ e の**始点** (*source*)，**終点** (*target*) などとよぶ．頂点

を丸，辺を矢印とした図で表すことが多い．



上図は（多重辺，ループ，閉路，孤立点を含む）箙の例である． ◊

定義 B.15 (箙代数)**.** 箙 $\Gamma = (V, E, s, t)$ に対し，*path* とは，列 $v_0, e_0, v_1, e_1, \ldots, e_{n-1}, v_n$（$n \geq 0$）であって，各 $0 \leq i < n$ に対して $s(e_i) = v_i$，$t(e_i) = v_{i+1}$ を満たすものである．

Γ を箙，A を可換環とするとき，**箙代数** (*quiver algebra*) $A[\Gamma]$ を次で定める．A 加群としては path を基底とする自由 A 加群とし，積は，path $(v_0, e_0, \ldots, e_{n-1}, v_n), (w_0, f_0, \ldots, f_{m-1}, w_m)$ に対し，

$$(v_0, e_0, \ldots, e_{n-1}, v_n) \cdot (w_0, f_0, \ldots, f_{m-1}, w_m) = \begin{cases} (v_0, e_0, \ldots, e_{n-1}, v_n, f_0, \ldots, f_{m-1}, w_m) & (v_n = w_0), \\ 0 & (v_n \neq w_0) \end{cases}$$

と定める．この乗法が結合的であることは容易に分かる．

V が有限集合ならば，各 $v \in V$ を始点とする長さ 0 の path（すなわち，列 v）の和が $A[\Gamma]$ の単位元となる．V が無限集合ならば，（A が零環でない限り）$A[\Gamma]$ は単位元をもたない． ◊

命題 B.16 (箙の表現)**.** A を可換環とする．箙 $\Gamma = (V, E, s, t)$ の（A 係数の）**表現** (*representation*) とは，各頂点 $v \in V$ に対する A 加群の族 $(M_v)_{v \in V}$ と，各辺 $e \in E$ に対する A 準同型の族 $(f_e \colon M_{s(e)} \to M_{t(e)})_{e \in E}$ の組である．

これは箙代数 $A[\Gamma]$ 上の加群と同じことである． ◊

注 B.17. グラフ (*graph*) は離散数学や情報科学などでも広く使われる概念である．（「関数のグラフ」とはあまり関係がない．）目的に応じて，多少異なった概念も用いられる．2 つの写像 $s, t \colon E \to V$ の代わりに，E から V の 2 元部分集合（resp. 1 または 2 元部分集合）全体の集合への写像を考えるのは，ループを許容しない（resp. 許容する）**無向グラフ** (*undirected graph*) である．この写像に単射性を要求するのは多重辺を許容しないことに相当する．s, t が定める有向グラフに対し，写像 $e \mapsto \{s(e), t(e)\}$ が定める無向グラフはもとの有向のグラフの向きを忘れたものと考えられる． ◊

演習問題

問題 B.1. 多変数の形式冪級数環を考える．A は零環でない可換環とする．

(1) $A[[X]][[Y]]$ と $A[[X, Y]]$ が環として同型であることを確認せよ．
(2) $A[[X]][Y]$ と $A[Y][[X]]$ はどちらも $A[[X, Y]]$ の部分環とみなせるが，両者は一致しないことを示せ．包含関係はどうか？

問題 B.2 (ローラン級数)**.** $0 < r_1 < r_2$ を正の実数として，B.2.2 節の環 $B_{(r_1, r_2)}$ を考える．同小々節の記号を用いる．c_n を定義する和が絶対収束し，$\sum_{n \in \boldsymbol{Z}} c_n z^n$ が再び $B_{(r_1, r_2)}$ の元となることを示せ．

問題 B.3. 非可換な環 R で，右イデアルがすべて両側イデアルであり左イデアルもすべて両側イデアルであるものの例を挙げよ．

C　ヒルベルトの零点定理

本節では環はすべて可換とする．

命題 C.1. $k \to k'$ が体拡大で，かつ k' が有限生成 k 代数ならば，k' は k の有限次拡大（すなわち，k 加群すなわち k ベクトル空間としての次元が有限）である． ◊

証明はここでは省略する．例えば [AM69, 系 5.24 または演習問題 5.18 または命題 7.9] を見てください．

系 C.2 (ヒルベルトの弱零点定理)**.** k を代数閉体とする．A が有限生成 k 代数で，$\mathfrak{m} \subset A$ が極大イデアルならば，$A/\mathfrak{m}$ は k に同型である． ◊

証明. $A/\mathfrak{m}$ に命題 C.1 を適用する． □

次の**ヒルベルトの零点定理** (*Hilbert's Nullstellensatz*) を述べるために記法を導入する：$a = (a_1, \ldots, a_n) \in k^n$ と $f \in k[X_1, \ldots, X_n]$ に対し，$f(a) = f(a_1, \ldots, a_n)$ と書く．

定理 C.3 (ヒルベルトの零点定理)**.** k を代数閉体とし，n を非負整数とする．イデアル $J \subset k[X_1, \ldots, X_n]$ に対し，集合 $V(J) \subset k^n$ を

$$V(J) := \{a \in k^n \mid \text{任意の } f \in J \text{ に対して } f(a) = 0\}$$

で定める．また，集合 $V \subset k^n$ に対し，イデアル $I(V) \subset k[X_1, \ldots, X_n]$ を

$$I(V) := \{f \in k[X_1, \ldots, X_n] \mid \text{任意の } a \in V \text{ に対して } f(a) = 0\}$$

で定める．

このとき，任意のイデアル $J \subset k[X_1, \ldots, X_n]$ に対し $I(V(J)) = \sqrt{J}$ が成り立つ． ◊

証明. $\sqrt{J} \subset I(V(J))$ を示す．まず定義から明らかに $J \subset I(V(J))$ は成り立つ．$f \in \sqrt{J}$ とすると $f^m \in J$ を満たす m が存在する．$a \in V(J)$ に対し $f(a) = 0$ を示せばよいが，仮定より $f(a)^m = f^m(a) = 0$ が成り立つので，（k の冪零元は 0 しかないので）$f(a) = 0$ である．

$I(V(J)) \subset \sqrt{J}$ を示す．$g \notin \sqrt{J}$ ならば $g \notin I(V(J))$ であることを示す，$A = k[X_1, \ldots, X_n]$，$B = k[X_1, \ldots, X_n]/J$ とおく．g（の像）は環 B において冪零でないので，命題 11.24 より B_g は零環でなく，極大イデアル $\mathfrak{m} \subset B_g$ をもつ．命題 11.19 より $B_g/\mathfrak{m}$ は有限生成 k 代数なので，弱零点定理（系 C.2）より $B_g/\mathfrak{m}$ は k の有限次拡大体であり，k が代数閉体なので $B_g/\mathfrak{m} \cong k$ である．$\mathfrak{n} := \mathrm{Ker}(A \to B \to B_g \to B_g/\mathfrak{m}) \subset A$ とおくと，合成 $k \to A/\mathfrak{n} \hookrightarrow B_g/\mathfrak{m} \cong k$ が同型なことから $A/\mathfrak{n}$ も k に同型である．（極大イデアルの縮約は一般に極大イデアルとは限らないが，この場合には成り立っている．）$A = k[X_1, \ldots, X_n] \to A/\mathfrak{n} \cong k$ は各 $X_1, \ldots, X_n$ にある k^n の元 $a = (a_1, \ldots, a_n)$ を代入する写像である．構成より $g \notin \mathfrak{n}$ と $J \subset \mathfrak{n}$ が成り立つので $g(a) \neq 0$ と $a \in V(J)$ が成り立つ．すなわち $g \notin I(V(J))$ である． □

イデアル J を用いて $V(J)$ の形に書ける k^n の部分集合を**代数的集合** (*algebraic subset*) とよぶ．定理 C.3 から直ちに次の対応が得られる．

系 C.4. 写像 I と V は，k^n の代数的集合全体の集合と $k[X_1, \ldots, X_n]$ の根基イデアル（問題 4.8）全体の集合の間に全単射を与える．さらに，これらの写像は包含関係を逆転させる（すなわち，V_1 と J_1，V_2 と J_2 が

対応するとき，$V_1 \subset V_2$ と $J_1 \supset J_2$ は同値である）．◊

注 C.5. 定理 C.3 は k が代数閉体でないと成り立たない．反例は例えば問題 C.1 を見よ．◊

余談 C.6. Nullstellensatz[*9]はドイツ語だが，しばしば英語の文章でもドイツ語のまま用いられる．ドイツ語で Null は零，Stelle（複数形 Stellen）は場所，Nullstelle は零点，Satz は定理を表す．なお，ドイツ語では名詞はつねに大文字で始め，また単語を合成する際にはスペースやハイフンを用いず直につなげる．◊

演習問題

問題 C.1. 定理 C.3 の $V(-)$ および $I(-)$ を，k が代数閉体でない場合にも使うことにする．$\boldsymbol{R}[X,Y]$ のイデアル $J_1 = (X^2+Y^2)$ および $J_2 = (X^2+Y^2+1)$ に対し，$V(J_i)$ および $I(V(J_i))$ を求め，$I(V(J_i)) = J_i$ が成り立つかどうか確かめよ．

問題 C.2. k を体とし，$\mathfrak{m} \subset A = k[X_1,\dots,X_n]$ を極大イデアルとすると，次を満たす $f_1,\dots,f_n \in A$ が存在することを示せ．

- $f_i \in k[X_1,\dots,X_i]$ である．
- $\mathfrak{m} \cap k[X_1,\dots,X_i] = (f_1,\dots,f_i)$ である．

D　可換環の次元

本節では環はすべて可換とする．

素イデアルの真の包含列 $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$ に対しその長さを d とおく．

定義 D.1. A を環とする．A の**クルル次元** (*Krull dimension*) を，A の素イデアルの真の包含列の長さの上限として定める．これを $\dim A$ と書く．

なお，A が素イデアルをもたないとき（定理 10.15 より，A が零環の場合に限る）は，$\dim A = -\infty$ と定める．◊

例 D.2. 体は素イデアルを 1 つしかもたないので，体の次元は 0 である．

$\boldsymbol{Z}$ の素イデアルは (0) と素数に対する (p) のみであり，素イデアルの間の真の包含関係は $(0) \subsetneq (p)$ しかないので，$\boldsymbol{Z}$ の次元は 1 である．◊

例 D.3. A/I を A の剰余環とすると，自然な埋め込み $\operatorname{Spec} A/I \subset \operatorname{Spec} A$ は順序を保つので，$\dim A/I \leq \dim A$ である．

A_S を A の局所化とすると，自然な埋め込み $\operatorname{Spec} A_S \subset \operatorname{Spec} A$ は順序を保つので，$\dim A_S \leq \dim A$ である．◊

注 D.4. A がネーター環ならば，長さ無限の真の増大列 $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots$ は存在しない．しかしクルル次元が無限になることはある（永田の反例が有名である）．◊

[*9] 読み：ぬるしゅてれんざっつ

定理 D.5. A を環，$A[x]$ を A 上の 1 変数多項式環とすると，$\dim A + 1 \leq \dim A[x] \leq 2\dim A + 1$ が成り立つ． ◊

証明. $I \subset A$ がイデアルであるとき，$I[X] := \{\sum_{i=0}^{n} a_i X^i \in A[X] \mid a_i \in I\} \subset A[X]$ と書く．$\mathfrak{p} \subset A$ が素イデアルならば，$A[X]/\mathfrak{p}[X] \cong (A/\mathfrak{p})[X]$ なので $\mathfrak{p}[X] \subset A[X]$ も素イデアルである．

$\dim A = -\infty$（すなわち A が零環）ならば主張は自明なので，$\dim A \geq 0$ とする．

A の素イデアルの包含列 $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ を 1 つとると $\mathfrak{p}_0[X] \subsetneq \cdots \subsetneq \mathfrak{p}_n[X] \subsetneq \mathfrak{p}_n[X] + (X)$ は $A[X]$ の素イデアルの包含列なので，$\dim A[X] \geq \dim A + 1$ である．

$\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ が $A[X]$ の素イデアルの包含列ならば $\mathfrak{q}_0 \cap A \subset \cdots \subset \mathfrak{q}_n \cap A$ も A の素イデアルの包含列だが，こちらは真の包含とは限らない．$\mathfrak{p} \subset A$ が素イデアルのとき，$\{\mathfrak{q} \in \operatorname{Spec} A[X] \mid \mathfrak{q} \cap A = \mathfrak{p}\}$ は $\operatorname{Spec} \kappa(\mathfrak{p})[X]$ と一対一対応する（問題 D.1）ので，列 $\mathfrak{q}_i \cap A$ の中に同じ素イデアルは高々 2 回しか現れない．ここから $\dim A[X] + 1 \leq 2(\dim A + 1)$ を得る． □

ネーター環ならば $\dim A[X]$ は $\dim A$ のみから定まる：

定理 D.6. A がネーター環ならば $\dim A[x] = \dim A + 1$ が成り立つ． ◊

証明は例えば [AM69, 演習問題 11.7] を見よ．

注 D.7. ネーター環という仮定を外すと定理 D.6 は一般に成り立たない．問題 D.2 は $\dim A = 1$ で $\dim A[X] = 3$ となる例を与える．これを一般化して $\dim A = n$ で $\dim A[X] = 2n + 1$ となる例を作れる． ◊

系 D.8. 体上有限生成な環や $\boldsymbol{Z}$ 上有限生成な環の次元は有限である． ◊

証明. 定理 D.6 と，剰余環の次元に関する不等式（例 D.3）から分かる． □

体上有限生成な環の次元については次が知られている．なお，**超越次数** (*transcendence degree*) の定義は体論の教科書を参照してください．

定理 D.9. k を体とし，A を有限生成 k 代数で整域だとする．このとき $\dim A$ は $\operatorname{Frac}(A)$ の k 上の超越次数 $\operatorname{trdeg}_k \operatorname{Frac}(A)$ に等しい． ◊

証明は例えば [AM69, 定理 11.25] を見よ．

簡単な例として $A = k[X_1, \ldots, X_d]$ のとき $\dim A = \operatorname{trdeg}_k k(X_1, \ldots, X_d) = d$ である．

演習問題

問題 D.1. $\mathfrak{p} \in \operatorname{Spec} A$ に対し，$\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ とおく．$\operatorname{Spec} A[X] \to \operatorname{Spec} A$ による $\mathfrak{p}$ の逆像は $\operatorname{Spec} \kappa(\mathfrak{p})[X]$ と一対一対応することを示せ．（一般に，$\operatorname{Spec} B \to \operatorname{Spec} A$ による $\mathfrak{p}$ の逆像は，テンソル積 $B \otimes_A \kappa(\mathfrak{p})$ のスペクトル $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ と一対一対応する．））

問題 D.2. （この例は `https://math.stackexchange.com/questions/1267419/` を参考にしました．）k

を体，$k(t)$ を k 上の 1 変数有理関数体とする．$B = k(t)[[Y]]$ とし，その部分環 $B_0 \subset B_1 \subset B$ を

$$B_1 = \{\sum_{i\geq 0} a_i Y^i \in B \mid a_0 \in k[t]\},$$
$$B_0 = \{\sum_{i\geq 0} a_i Y^i \in B \mid a_0 \in k\}$$

で定める．また $\mathfrak{p} = YB$ とし，$\mathfrak{p}_1 = \mathfrak{p} \cap B_1$，$\mathfrak{p}_0 = \mathfrak{p} \cap B_0$ とする．$\dim B_0[X] > \dim B_0 + 1$ であることを以下の手順で示せ．

(1) $\operatorname{Spec} B_0 = \{(0), \mathfrak{p}_0\}$ を示せ．したがって $\dim B_0 = 1$ である．
(2) $\mathfrak{p}_1$ は極大イデアルでないことを示せ．したがって $\dim B_1 \geq 2$ である．
(3) $B_0[X]$ から B_1 への同型でない全射が存在することを示せ．したがって $\dim B_0[X] \geq \dim B_1 + 1 > \dim B_0 + 1$ である．

E 円分多項式

定義 E.1. 正整数 d に対し，d 番目の**円分多項式** (*cyclotomic polynomial*) $\Phi_d(X) \in \boldsymbol{Z}[X]$ を，正整数 n に対して $\prod_{d|n} \Phi_d(X) = X^n - 1$ が成り立つように定める． ◊

ただし $\prod_{d|n}$ は「d は n の正の約数全体をわたる」を意味する．

命題 E.2. 定義 E.1 の条件を満たす多項式 $\Phi_d(X) \in \boldsymbol{Z}[X]$ の族が一意に存在する．$d \neq d'$ ならば $\Phi_d(X)$ と $\Phi_{d'}(X)$ は（$\boldsymbol{Z}[X]$ の単数以外の）共通因子をもたない． ◊

証明. $\prod_{d|n} \Phi_d(X) = X^n - 1$ が成り立つように $\Phi_d(X) \in \operatorname{Frac}(\boldsymbol{Z}[X]) = \boldsymbol{Q}(X)$ をとれることおよび一意性は明らかである．$\Phi_d(X) \in \boldsymbol{Z}[X]$ であることを示したい．

「$\Phi_d(X) \in \boldsymbol{Z}[X]$ であり，$d' < d$ に対し $\Phi_d(X)$ と $\Phi_{d'}(X)$ は共通因子をもたない」が成り立つことを d に関する帰納法で示す．

$$\Phi_d(X) = \frac{X^d - 1}{\prod_{e|d, e\neq d} \Phi_e(X)}$$

である．分母の各 e に対して，$\Phi_e(X) \mid (X^e - 1) \mid (X^d - 1)$ なので，分母の各因子は $X^d - 1$ を割りきる．$\boldsymbol{Z}[X]$ は UFD（定理 9.15）なので，$e \neq e'$ に対し $\Phi_e(X)$ と $\Phi_{e'}(X)$ が共通因子をもたないこと（帰納法の仮定）から，分母は $X^d - 1$ を割りきる．すなわち $\Phi_d(X) \in \boldsymbol{Z}[X]$ である．

$\Phi_d(X)$ と $\Phi_{d'}(X)$（$d' < d$）が共通の素元 P で割れたと仮定して矛盾を導く．$\Phi_d(X)$ はモニックなので，P は次数が 1 以上である．P は $X^{d'} - 1$ と $X^d - 1$ を割るので，$g := \gcd\{d', d\}$ として $X^g - 1$ をも割り（問題 6.3(7)），ある g の約数 d'' に対して $\Phi_{d''}(X)$ をも割る．$g < d$ なので，帰納法の仮定より $d'' = d'$ であり，したがって d' は d を割る．すると（P が Φ_d と $\Phi_{d'}$ を割るので）P^2 が $X^d - 1$ を割ることになる．このとき P は $\frac{d}{dX}(X^d - 1) = dX^{d-1}$ を割るはずだが，$\boldsymbol{Q}[X]$ で dX^{d-1} と $X^d - 1$ は互いに素なので，矛盾した． □

例 E.3. 最初のいくつかを具体的に書くと，$\Phi_1(X) = X - 1$，$\Phi_2(X) = X + 1$，$\Phi_3(X) = X^2 + X + 1$，$\Phi_4(X) = X^2 + 1$，$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$，$\Phi_6(X) = X^2 - X + 1$ である． ◊

命題 E.4. d を正整数とする．$S_d \subset \boldsymbol{C}^*$ を 1 の原始 d 乗根（すなわち，$\boldsymbol{C}^*$ の位数 d の元）全体の集合とすると，$\Phi_d(X) = \prod_{z \in S_d}(X - z)$ である． ◊

証明. これを Φ_d としたとき $\prod_{d|n} \Phi_d(X) = X^n - 1$ が成り立つことを確かめればよく，容易である． □

系 E.5. $\phi(d) = |(\boldsymbol{Z}/d\boldsymbol{Z})^*|$ とおくと，$\deg \Phi_d = \phi(d)$ である． ◊

注 E.6. 命題 E.4 を円分多項式の定義にしてもよいのだが，整数係数であることが見えづらい． ◊

注 E.7. d が素数のとき Φ_d が既約であることは Eisenstein の既約性判定法を用いて示した（例 10.14）．一般の d でも既約になるのだが，ここでは証明しない． ◊

F　正標数の体

ここでは正標数の体について少し述べて，有限体は必ず可換になること（定理 F.6）を示す．
本節では環を可換と仮定しない．

F.1　体の標数

定義 F.1. k を環とする．（唯一の）環準同型 $f\colon \boldsymbol{Z} \to k$ の核は $\boldsymbol{Z}$ のイデアルなので，$\operatorname{Ker} f = (n)$ となる $n \geq 0$ がただ一つ存在する．この n を k の**標数** (*characteristic*) とよび，$\operatorname{char} k$ と書く． ◊

注 F.2. 一般の環の場合（つまり，体と限らない場合），すべての素イデアルでの剰余体が標数 p であるときに限り標数 p とよび，そうでない場合（剰余体によって標数が異なる場合）に**混標数** (*mixed characteristic*) であるということもある． ◊

命題 F.3. 体の標数は 0 または素数である． ◊

証明. $(0) \subset k$ は素イデアルなのでその逆像も素イデアルであり，$\boldsymbol{Z}$ の素イデアルは (0) であるかまたはある素数 p に対する (p) である．
（よく考えると，素イデアルは可換環に対してしか定義していないが，上の議論を適切に言い直せば非可換環にも通用する．） □

命題 F.4. k を有限体とする．このとき，k の標数は素数 p であり，$\boldsymbol{Z} \to k$ の像は位数 p の有限体であり，k の位数は p の冪乗である． ◊

証明. 標数が 0 だとすると $\boldsymbol{Z} \to k$ が単射になるが，$\boldsymbol{Z}$ は無限集合なので有限集合への単射は存在しない．したがって $\operatorname{char} k = p$ は素数である．$\boldsymbol{Z} \to k$ の像 k' は準同型定理より $\boldsymbol{Z}/(p)$ に同型なので体である．k は k' ベクトル空間なので，次元を $d = \dim_{k'} k$ とおくと $|k| = |k'|^d$ である． □

F.2　有限体

命題 F.5. 有限整域は体である．（ここでは，整域と体のどちらも可換性を仮定していない．） ◊

証明. A を有限整域とする．$a \in A \setminus \{0\}$ とし，これが逆元をもつことを示す．A が整域なので，a 倍写像

$A \to A\colon x \mapsto ax$ は単射である（$ax = ay$ ならば $a(x-y) = 0$ なので $x - y = 0$ である）．A が有限集合なので，この写像は全射でもある．したがって $ax = 1$ を満たす $x \in A$ が存在する．a の左逆元についても同様. □

定理 F.6. 有限体は可換である．さらに，その乗法群は巡回群である. ◊

証明. k を（可換と仮定されていない）有限体とする．k の中心 $\mathrm{Z}(k)$ も有限体である．$q = |\mathrm{Z}(k)|$ とおき，$q^d = |k|$ とおく．乗法群 k^* の中心は $\mathrm{Z}(k)^*$ である．中心に属さない k^* の元の共役類を $C_1, \dots, C_n$ とおく．C_i の代表元 x_i をとり，その中心化環 $\mathrm{Z}_k(x_i)$ を k_i とおくと，k_i は $\mathrm{Z}(k)$ を部分体として含む体である．$q^{e_i} = |k_i|$ とおく．中心に属さない元の軌道を考えているので $e_i < d$ である．類等式 [群論, 命題 14.2] から

$$q^d - 1 = q - 1 + \sum_{i=1}^{n} \frac{q^d - 1}{q^{e_i} - 1}$$

を得る．ここで $q^d - 1$ および $\frac{q^d-1}{q^{e_i}-1}$ は $\Phi_d(q)$ の倍数である（Φ_d は d 番目の円分多項式（定義 E.1））．したがって $q - 1$ も $\Phi_d(q)$ の倍数でなければならない．k が可換でないとすると $d > 1$ であり，このとき，命題 E.4 の記号で $S_d \subset \boldsymbol{C}^*$ を 1 の原始 d 乗根全体の集合とすると任意の $z \in S_d$ に対して $|q - z| > |q - 1|$ なので，

$$0 < q - 1 \leq (q-1)^{\deg \Phi_d} < \prod_{z \in S_d} |q - z| = |\Phi_d(q)|$$

となり矛盾する. □

有限体とは直接関係ないが，命題 F.5 と同様の議論で次が示せる．

命題 F.7. A を整域とする．A が体 k を（部分環として）含み，A が k ベクトル空間として有限次元ならば，A は体である. ◊

証明. $a \in A \setminus \{0\}$ とし，これが逆元をもつことを示す．A が整域なので，a 倍写像 $A \to A\colon x \mapsto ax$ は単射である（$ax = ay$ ならば $a(x-y) = 0$ なので $x - y = 0$ である）．また，k 線形写像でもある．A が有限次元 k ベクトル空間なので，この線形写像は全射でもある．以下命題 F.5 の証明と同様. □

F.3 位数 q の有限体の存在と一意性

本小節では環はすべて可換とする．

命題 F.8. k が有限体で $|k| = q$ ならば，任意の $a \in k$ に対し $a^q = a$ が成り立つ. ◊

証明. $a = 0$ ならば明らか．$a \neq 0$ ならば $a \in k^*$ であり，k^* は位数 $q - 1$ の群なので $a^{q-1} = 1$ が成り立ち，したがって $a^q = a$ である. □

系 F.9. k が有限体で $|k| = q$ ならば，多項式 $X^q - X$ は $\prod_{a \in k}(X - a)$ に等しい. ◊

証明. 任意の $a \in k$ が $X^q - X$ の根なので，因数定理を繰り返し用いることで，$X^q - X = g(X) \prod_{a \in k}(X - a)$ を得る（g は k 係数多項式）．次数と最高次の係数を比較して $g(X) = 1$ を得る. □

系 F.10. k が有限体で，多項式 $F(X) \in \boldsymbol{F}_p[X]$ が任意の $a \in k$ に対して $F(a) = 0$ を満たすならば，$F(X)$ は $X^{|k|} - X$ で割りきれる. ◊

定理 F.11. q を素数の冪乗とすると，位数 q の有限体は同型を除いてただ一つ存在する． ◊

証明. 一意性を示す．k, k' を位数 $q = p^e$（p は素数）の有限体とする．次を満たす環 $A = k \otimes_{\boldsymbol{Z}} k'$（$k$ と k' の $\boldsymbol{Z}$ 上のテンソル積）が存在することを認める．

- 環準同型 $k \to A$ および $k' \to A$ が存在する．
- A は零環でない.

すると，A の極大イデアルを 1 つとり $\mathfrak{m}$ とおくと，$k \to A/\mathfrak{m}$ および $k' \to A/\mathfrak{m}$ は単射である（問題 3.7）．このとき，$K := A/\mathfrak{m}$ とおくと，k と k' のどちらの像も集合 $\{a \in K \mid a^q - a = 0\}$ に含まれ，この集合の元の個数は高々 q 個であることから，k と k' は K の部分集合として一致する．

存在を示す．p を素数とし $q = p^e$ とする．$\boldsymbol{F}_p$ 上の多項式 $X^q - X$ の分解体 K をとる：すなわち，$K[X]$ で $X^q - X$ は 1 次式の積 $\prod_{i=1}^{q}(X - a_i)$（$a_i \in K$）に分解する（分解体の存在については体論の教科書を参照）．$X^q - X$ は分離的なので $a_1, \ldots, a_q$ はどの 2 つも相異なる（体論の教科書を参照）．$F\colon K \to K\colon a \mapsto a^q$ は自己準同型（命題 F.14）なので，$K' := \{a \in K \mid a^q - a = 0\}$ は K の部分体であり，K のとり方と系 8.24 から $|K'| = q$ である． □

注 F.12. $\boldsymbol{F}_q/\boldsymbol{F}_p$ は有限次分離拡大なので単拡大であり（体論の教科書を参照），すなわちある e 次既約多項式 $Q(X) \in \boldsymbol{F}_p[X]$ を用いて $\boldsymbol{F}_q = \boldsymbol{F}_p[X]/Q(X)$ と書ける．

逆に e 次既約多項式の存在を示せば $q = p^e$ 個の元からなる体の存在がいえるわけだが，ちなみにこれを直接示すこともできる：$\boldsymbol{F}_p[X]$ での $X^q - X$ の既約モニック多項式への分解を $X^q - X = \prod_i P_i(X)$ とする．$X^q - X$ と $\frac{d}{dX}(X^q - X)$ の最大公約数が 1 なので，P_i はどの 2 つも相異なる（問題 F.6）．$d_i = \deg P_i(X)$ とおくと，$\boldsymbol{F}_p[X]/(P_i(X))$ は位数 p^{d_i} の体である．d_i が e の約数であることが示せる．d_i がすべて e より真に小さいと仮定すると，e の約数 $d < e$ に対する d 次既約モニック多項式の個数を評価すると（d 次モニック多項式の個数以下である）$\sum \deg P_i < q$ となって矛盾を得る．詳細は省略する． ◊

F.4 フロベニウス写像と完全体

本小節では環はすべて可換とする．

定義 F.13. k を標数 $p > 0$ の可換環とする．写像 $k \to k\colon a \mapsto a^p$ を**フロベニウス写像** (*Frobenius map*) という． ◊

命題 F.14. フロベニウス写像は環準同型であり，k が整域ならば単射である． ◊

証明. 積および 1 を保つのは明らか．和に関しては，2 項定理 $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$ において，$0 < i < p$ のとき $\binom{p}{i}$ は p の倍数なので k の元としては 0 になり，右辺は $a^p + b^p$ のみが残る．

$a^p = b^p$ ならば $(a-b)^p = 0$ であり，k が整域ならば冪零元は 0 しかないので $a = b$ である． □

定義 F.15. 正標数の体は，フロベニウス写像が全射であるとき**完全体** (*perfect field*) という． ◊

注 F.16. 本来は任意の標数の体に適用可能な定義を述べて，この性質と同値であることをいうべきなのだが，詳しいことは体論の講義にお任せする． ◊

例 F.17. 有限体は完全体である．実際，有限集合から自分自身への単射は必ず全射である． ◊

例 F.18. 代数閉体は完全体である．実際，k が代数閉体ならば，$a \in k$ に対し，$X^p - a = 0$ が k に属する解をもつ． ◊

例 F.19. 完全体でない体の例としては，例えば k を標数 $p > 0$ の体として，有理関数体 $k(X) = \mathrm{Frac}(k[X])$ が挙げられる．p 乗して X になる元は存在しない． ◊

演習問題

問題 F.1. k を標数 p の体とする．$a \in k$ の p 乗根は k の中に高々 1 つしか存在しないことを示せ．

問題 F.2. A が標数 p の環（resp. 整域，resp. 体）ならば，A の部分集合 $A^p := \{a^p \mid a \in A\}$ は部分環（resp. 部分整域，resp. 部分体）であることを示せ．

問題 F.3. A を標数 p の環とし，$I \subset A$ をイデアルとする．$I^{[p]}$ を $\{a^p \mid a \in I\}$ が生成するイデアルとする．$I = (a_1, \ldots, a_n)$ ならば $I^{[p]} = (a_1^p, \ldots, a_n^p)$ であることを示せ．（無限個の生成元の場合も同様である．）また，一般に $I^{[p]} \neq I^p$ であることを示せ．

問題 F.4. A を有限環とする．

(1) $\mathrm{char}\, A$ は $|A|$ を割りきることを示せ．
(2) ある整数 N に対して，$|A|$ は $(\mathrm{char}\, A)^N$ を割りきることを示せ．

なお，$|A|$ が $\mathrm{char}\, A$ の冪乗になるとは限らない．

問題 F.5. A_1, A_2 を環とする．A_1 から A_2 への環準同型が存在するならば，$\mathrm{char}\, A_2$ は $\mathrm{char}\, A_1$ を割りきることを示せ．

k_1, k_2 を体とする．k_1 から k_2 への環準同型が存在するならば，$\mathrm{char}\, k_2 = \mathrm{char}\, k_1$ であることを示せ．

問題 F.6. k を体とし，$P, Q \in k[X]$ とする．P は既約だとする．

(1) P^2 が Q を割るならば, P は Q と Q' の両方を割ることを示せ．ただし Q' は $\frac{d}{dX}Q$ を表す（$\frac{d}{dX} : k[X] \to k[X]$ とは $\frac{d}{dX}(X^n) = nX^{n-1}$ を満たす k 線形写像である）．
(2) $(Q, Q') = (1)$ ならば Q は定数でない多項式の 2 乗で割れないことを示せ．
(3) k が完全体ならば，前 2 項の逆も成り立つことを示せ．
(4) k が完全体と仮定しない場合，逆は一般に成り立たないことを示せ．

多項式 Q に対する条件 $(Q, Q') = 1$ は，Q が**分離的** (*separable*) であることと同値である．

G　環の完備化

これまでに環の構成法として，剰余環，多項式環（や一般にモノイド環），局所化を紹介した．もう一つ重要な構成法として完備化がある．構成のための準備として環などの射影系と射影極限を導入し，また位相環の概念を導入する．

G.1 射影系と射影極限

G.1.1 射影系

定義 G.1. 集合の**逆系** (*inverse system*) または**射影系** (*projective system*) とは，$\boldsymbol{N}$ で添字づけられた集合族 $(M_n)_{n\in\boldsymbol{N}}$ と，写像の族 $(f_{n+1}\colon M_{n+1}\to M_n)_{n\in\boldsymbol{N}}$ の組である．

f_n のことを射影系の**推移写像** (*transition map*) などとよぶ． ◊

射影系を $((M_n),(f_n))$ または，推移写像が明らかな場合は単に (M_n) などと書く．

定義 G.2. M_n がすべて群（resp. 加群，A 加群，環，A 代数）であり f_{n+1} がすべて群（resp. ……）の準同型であるとき，群（resp. ……）の射影系という． ◊

命題 G.3. 射影系は，次の条件を満たす組とも思える：$\boldsymbol{N}$ で添字づけられた集合族 $(M_n)_{n\in\boldsymbol{N}}$ と，$\{(n,m)\in \boldsymbol{N}\times\boldsymbol{N}\mid n\le m\}$ で添字づけられた写像の族 $(f_{n,m}\colon M_m\to M_n)_{n\le m}$ との組であって，$f_{n,n}=\mathrm{id}_{M_n}$ および（$n\le m\le l$ に対し）$f_{n,m}\circ f_{m,l}=f_{n,l}$ を満たすもの．群（resp. ……）の射影系についても同様である． ◊

略証. 定義 G.2 の意味の射影系が与えられたとき，$f_{n,m}$ を $f_{n+1}\circ f_{n+2}\circ\cdots\circ f_{m-1}\circ f_m$ とすればよい． □

G.1.2 射影極限

定義 G.4. 射影系 $((M_n),(f_n))$ の**逆極限** (*inverse limit*) または**射影極限** (*projective limit*) を，

$$M:=\varprojlim_n M_n:=\{(x_n)\in\prod_{n\in\boldsymbol{N}}M_n\mid \text{各 } n\in\boldsymbol{N} \text{ に対して } f_{n+1}(x_{n+1})=x_n\}$$

で定める．また，写像 $\phi_n\colon M\to M_n$ を直積集合からの射影とする． ◊

命題 G.5. $((M_n),(f_n))$ が群（resp. 加群，A 加群，環，A 代数）の射影系（定義 G.2）であるとき，射影極限 $\varprojlim_n M_n$ にも自然に群（resp. ……）の構造が入り，また ϕ_n は群（resp. ……）の準同型である． ◊

証明は難しくない．

また，次のバージョンもある．

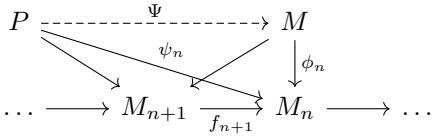
命題 G.6. $((A_n),(f_n))$ が環（または B 代数）の射影系，$((M_n),(g_n))$ がアーベル群の射影系であり，各 n に対し M_n は A_n 加群であり，作用が整合的だとする，すなわち次の図式が可換だとする：

$$\begin{array}{ccc} A_{n+1}\times M_{n+1} & \longrightarrow & M_{n+1} \\ {\scriptstyle f_{n+1}\times g_{n+1}}\downarrow & & \downarrow{\scriptstyle g_{n+1}} \\ A_n\times M_n & \longrightarrow & M_n. \end{array}$$

ただし横の写像は環の加群への作用である．このとき，$M:=\varprojlim_n M_n$ は $A:=\varprojlim_n A_n$ 上の加群であり，$A\times M\to M$ と $A_n\times M_n\to M_n$ も上と同様の意味で整合的である． ◊

射影極限 $M=\varprojlim_n M_n$ と付随する写像 $\phi_n\colon M\to M_n$ は $\phi_n=f_{n+1}\circ\phi_{n+1}$ を満たすが，さらに次の普遍性をもつ．

命題 G.7. $((M_n),(f_n))$ を集合の射影系，$M := \varprojlim_n M_n$ をその射影極限とする．P を集合，$(\psi_n\colon P \to M_n)_{n\in\boldsymbol{N}}$ を写像の族とし，各 n に対し $\psi_n = f_{n+1}\circ\psi_{n+1}$ が成り立つと仮定する．このとき写像 $\Psi\colon P\to M$ で，各 n に対し $\psi_n = \phi_n\circ\Psi$ を満たすものがただ一つ存在する．



すなわち，$\mathrm{Map}(P,M)$ から集合 $\{(\psi_n)\in\prod_{n\in\boldsymbol{N}}\mathrm{Map}(P,M_n)\mid f_n = f_{n+1}\circ\psi_{n+1}\}$ への写像 $\Psi\mapsto(\phi_n\circ\Psi)$ は全単射である． ◊

証明. $x\in P$ に対し $(\psi_n(x))_{n\in\boldsymbol{N}}\in M=\varprojlim_n M_n$ を対応させればよい／させるよりない． □

命題 G.8. 命題 G.7 において $((M_n),(f_n))$ が群（resp. ……）の射影系であり，N も群（resp. ……）であり，各 ψ_n も群（resp. ……）の準同型だとする．そのとき Ψ も群（resp. ……）の準同型になる．すなわち，命題 G.7 の後段の全単射は Map を Hom にしても成り立つ． ◊

G.2 位相環

定義 G.9. 環（resp. 加群すなわちアーベル群）A が位相空間であり，写像 (1), (2), (3) （resp. (1), (2)）がすべて連続であるとき，A を**位相環** (*topological ring*) （resp. **位相加群** (*topological module*) という．

(1) $A\times A\to A\colon (a,b)\mapsto a+b$.
(2) $A\to A\colon a\mapsto -a$.
(3) $A\times A\to A\colon (a,b)\mapsto ab$.

ただし $A\times A$ には直積位相を入れる．

A が位相環で，M が A 加群かつ位相加群で，さらに写像

(4) $A\times M\to M\colon (a,x)\mapsto ax$

も連続であるとき，M は位相 A 加群であるという． ◊

なお位相加群の定義とあわせるため位相環に (2) の連続性も課したが，実はこれは残り 2 つの条件から導かれるので不要である．

本節では主に部分加群の族で定義される位相を考える．

定義 G.10. M が A 加群で，$(M_n)_{n\in\boldsymbol{N}}$ が部分 A 加群の減少列だとする（真の減少列でなくてもよい）．M の位相を，$x\in M$ の基本近傍系を $(x+M_n)_{n\in\boldsymbol{N}}$ とすることで定める．ただし $x+M_n := \{x+y\mid y\in M_n\}$ である． ◊

とくに，$I\subset A$ をイデアルとして，$M_n = I^nM$ とした場合を I **進位相** (I-*adic topology*) という．

次が簡単に確認できる．

命題 G.11. A，M，$(M_n)_{n\in\boldsymbol{N}}$，および M の位相を定義 G.10 の通りとする．次は同値である．

- M の位相は T_1 である．すなわち，すべての 1 点集合は閉集合である．
- M の位相はハウスドルフである．
- $\bigcap_{n\in\boldsymbol{N}} M_n = 0$. ◊

注 G.12. 異なる加群列が同じ位相を定めることもある．例えば，k が正整数のとき，I 進位相と I^k 進位相は一致する．位相が一致するための条件については問題 G.3 を見よ． ◊

G.3 環の完備化

定義 G.13. 環 A のイデアル I による**完備化** (*completion*) とは $\hat{A} := \varprojlim_n A/I^n$ である． ◊

命題 G.14. A がネーター環ならば，$\hat{A}$ はネーターかつ $I\hat{A}$ 進位相に関して完備であり，$\hat{A}/I^n\hat{A} \cong A/I^n$ が成り立つ． ◊

証明は例えば [AM69, 10 章] を見よ．

例 G.15. 素数 p に対する (p) 進位相を単に p 進位相という．

$\boldsymbol{Z}$ の p 進位相による完備化を $\boldsymbol{Z}_p := \varprojlim_n \boldsymbol{Z}/p^n\boldsymbol{Z}$ と表す．$\boldsymbol{Z}_p$ を p **進整数環** (*ring of p-adic integers*) とよぶ．$\boldsymbol{Q}_p := \operatorname{Frac}\boldsymbol{Z}_p$ を p **進数体** (*field of p-adic numbers*) とよぶ． ◊

例 G.16. k を体とし $A = k[X]$ とする．A の (X) 進位相による完備化 $\hat{A} = \varprojlim_n k[X]/(X^n)$ は $k[[X]]$ に同型である．同型写像は $k[[X]] \to \hat{A}\colon \sum_{i\geq 0} a_iX^i \mapsto (\overline{\sum_{i=0}^{n-1} a_iX^i})$ で与えられる． ◊

A が局所ネーター整域だとしても $\hat{A}$ が整域になるとは限らない（問題 G.4 や問題 H.23）が，一方で次元（定義 D.1）や深さ（定義はしない）といった量は保たれることが知られている．また，次の例でみるように正則局所環の完備化は分かりやすい形をしている．

例 G.17. （用語の定義はしない．）X が代数閉体 k 上定義された d 次元代数多様体で $x \in X$ を閉点とする．このとき，x が正則点（非特異点ともいう）であることと，局所環 $\mathcal{O}_{X,x}$ の完備化 $\hat{\mathcal{O}}_{X,x}$ が d 変数形式冪級数環 $k[[T_1,\ldots,T_d]]$ に同型になることは同値である． ◊

G.4 コーシー列を用いて定める完備化との関係

本小節を通して，M の位相が部分加群の減少列 $(M_n)_{n\in\boldsymbol{N}}$ から定まっているとする．

定義 G.18. M の点列 $(x_k)_{k\in\boldsymbol{N}}$ が**コーシー列** (*Cauchy sequence*) であるとは，任意の n に対しある k_0 が存在し，$k, k' \geq k_0$ ならば $x_k - x_{k'} \in M_n$ が成り立つことをいう．また，点列 $(x_k)_{k\in\boldsymbol{N}}$ が $x \in M$ に**収束** (*converge*) するとは，任意の n に対しある k_0 が存在し，$k \geq k_0$ ならば $x_k - x \in M_n$ が成り立つことをいう．

コーシー列 $(x_k), (y_k)$ が**同値** (*equivalent*) であるとは，任意の n に対しある k_0 が存在し，$k \geq k_0$ ならば $x_k - y_k \in M_n$ が成り立つことをいう． ◊

収束列ならばコーシー列である．収束列に同値なコーシー列も収束列である．

注 G.19. $0 < c < 1$ を実数とし，M の元 $x, y \in M$ に対し $x - y \in M_n$ を満たす最大の n を $n_0(x, y)$ とし

て $d(x,y) = c^{n_0(x,y)}$ と定め，ただし任意の n に対し $x - y \in M_n$ である場合には $d(x,y) = 0$ と定めると，$d\colon M \times M \to \boldsymbol{R}$ は擬距離関数（距離関数の公理のうち「$d(x,y) = 0$ ならば $x = y$」を除いたもの）になり，コーシー列や収束の定義はこの擬距離に関するものと一致する．$\bigcap_n M_n = 0$ ならば，d は距離関数になる．$\Diamond$

命題 G.20. M の完備化 $\hat{M}$ は，コーシー列の同値類全体の集合に自然に同型である．　$\Diamond$

略証. (x_k) がコーシー列のとき $\hat{M}$ の元 (y_n) を次のように定める：各 n に対し十分大きい k に対しては $\bar{x_k} \in M/M_n$ は定数列になるので，それを y_n とおく．　□

演習問題

問題 G.1. $((M_n),(f_n))$ を空でない集合の射影系とし，$M = \varprojlim_n M_n$ を射影極限とする．すべての n に対して f_n が全射ならば，M も空でないことを示せ．

問題 G.2. $((M_n),(f_n))$ を集合の射影系とし，$M = \varprojlim_n M_n$ を射影極限とする．M が空でないための十分条件を考えたい．

(1) 各 n に対し $M'_n := \bigcap_{m \geq n} \mathrm{Im}(f_{n,m})$ とおくと，$f_{n+1}(M'_{n+1}) \subset M'_n$ であることを示せ．したがって，$f_{n+1}\colon M_{n+1} \to M_n$ の制限は写像 $f'_{n+1}\colon M'_{n+1} \to M'_n$ を定め，(M'_n) も射影系になる．
(2) $\varprojlim_n M'_n \to \varprojlim_n M_n$ は全単射であることを示せ．

命題 G.3 で与えられる写像を $f_{n,m}\colon M_m \to M_n$ とおく．次が成り立つとき，この射影系は**ミッタク・レフラー条件** (*Mittag-Leffler condition*) を満たすという：各 n に対して，M_n の部分集合の減少列 $(\mathrm{Im}(f_{n,m}))_{m \geq n}$ は停止する（定義 12.1 参照）．

(3) (M_n) がミッタク・レフラー条件を満たすならば，$f'_{n+1}\colon M'_{n+1} \to M'_n$ は全射であることを示せ．
(4) (M_n) がミッタク・レフラー条件を満たし，各 M_n が空でないならば，$\varprojlim_n M_n$ も空でないことを示せ．
(5) (M_n) が空でない有限集合からなる射影系ならば，$\varprojlim_n M_n$ も空でないことを示せ．

問題 G.3. $M = M'$ が A 加群で，$(M_n)_{n \in \boldsymbol{N}}$ と $(M'_n)_{n \in \boldsymbol{N}}$ がそれぞれ部分 A 加群の減少列だとする．M と M' にそれぞれ加群列が定める位相を入れる．このとき，次が同値であることを示せ．

(1) $\mathrm{id}\colon M \to M'$ が連続である．
(2) 任意の n に対してある k が存在し $M_k \subset M'_n$ が成り立つ．

したがって，2 つの位相が一致することは，(2) の条件および M と M' を入れ替えた条件の両方が成り立つことと同値である．

問題 G.4. k を標数が 2 でない体とする．$A := k[X,Y]/(Y^2 - X^2 - X^3)$ は整域だが，その極大イデアル (X,Y) での完備化 $\hat{A} = k[[X,Y]]/(Y^2 - X^2 - X^3)$ は極小素イデアルを 2 つもち，したがって整域でないことを示せ．

余談. 集合 $V = \{(x,y) \in \boldsymbol{R}^2 \mid y^2 - x^2 - x^3 = 0\}$ を考える（この集合は $k = \boldsymbol{R}$ のときの $\{\mathfrak{m} \subset A \mid A/\mathfrak{m} \cong \boldsymbol{R}\}$ と自然に対応する）．V を描いてみると原点の（ユークリッド）近傍では 2 本の「曲線」になっている．一方でザリスキ位相では V を原点の近傍に制限しても 2 つの真の閉部分集合の和集合で表すことはできず（雰囲気としては，「2 本」のように見えて遠くでつながっていることが原因），これは A が整域であることと対応す

る．ところが原点で完備化することで遠くの情報は失われて 2 本の曲線の和集合とみなせるようになる．これは $\hat{A}$ が極小素イデアルを 2 つもつことと対応する．

問題 G.5. k を体とする．A は k 代数で，イデアル $I \subset A$ に対する I 進位相で完備だとし，$x \in I$ を元とする．

(1) $\operatorname{char} k = 0$ とする．任意の $\alpha \in A$ に対して，

$$(1+x)^\alpha := \sum_{i \geq 0} \binom{\alpha}{i} x^i$$

と定める．ただし，（α が整数と限らなくても）2 項係数は

$$\binom{\alpha}{i} := \frac{\alpha(\alpha-1)\dots(\alpha-(i-1))}{i!}$$

で定める．このとき次が成り立つことを示せ．

- $\alpha \in \boldsymbol{Z}$ ならば，通常の冪乗に一致する．
- 任意の $\alpha, \beta \in A$ に対して $(1+x)^\alpha (1+x)^\beta = (1+x)^{\alpha+\beta}$ が成り立つ．

(2) p を素数とし，$\boldsymbol{Z}_{(p)}$ を $\boldsymbol{Z}$ の素イデアル (p) での局所化とする．$\alpha \in \boldsymbol{Z}_{(p)}$ と $i \in \boldsymbol{N}$ に対して，(1) で定めた $\binom{\alpha}{i}$ も $\boldsymbol{Z}_{(p)}$ の元であることを示せ．

(3) $\operatorname{char} k = p > 0$ とする．$\alpha \in \boldsymbol{Z}_{(p)}$ に対して，$(1+x)^\alpha$ を (1) と同じ式で定める（ただし 2 項係数は (2) で定めた値の，（唯一の）環準同型 $\boldsymbol{Z}_{(p)} \to k$ による像とする）．このとき，$\alpha, \beta \in \boldsymbol{Z}_{(p)}$ に対して (1) と同じ主張が成り立つことを示せ．

したがって，m が標数で割れない正整数のとき，$1+x$ の m 乗根が必ず存在する．

H　チャレンジ問題

本講義の水準を度外視した演習問題をいくつか入れておきます．力試しにどうぞ．ほとんどはこの講義ノートで解説した内容だけで解くことが一応可能です．

（[群論] のチャレンジ問題よりは難易度が控えめだと思いますが，私の専門分野の関係で難易度判定がおかしくなっている可能性もあります．）

問題 H.1. 環とその真部分環 $A \subsetneq B$ で，環として同型であるものを挙げよ．（もちろん，その同型写像は包含写像とは異なる．）

問題 H.2. 可換環 A とそのイデアル I, J で，$IJ \supsetneq \{ij \mid i \in I, j \in J\}$ を満たす例を挙げよ．

問題 H.3. 非可換な環だが，左イデアルと右イデアルがすべて両側イデアルであるものを挙げよ．

問題 H.4. $\boldsymbol{Q}$ の部分加群をすべて求めよ．

問題 H.5. $\boldsymbol{Q}$ の部分環をすべて求めよ．

問題 H.6. I，J が有限生成イデアルならば $I \cap J$ もそうか？

問題 H.7. 環の乗法群が可換ならばもとの環も可換か？

問題 H.8. 環準同型 $A \to B$ であって，$A[[x]] \otimes_A B \to B[[x]]$ が全射でない例・単射でない例をそれぞれ挙げよ．

問題 H.9. A は 1 次元ネーター整域で，任意のイデアル $I \neq 0$ に対して $|A/I| < \infty$ だとする．このとき $|A/IJ| = |A/I| \cdot |A/J|$ か？

問題 H.10. k を体とする．$k[t]$ の極大イデアル (t) での局所化を A とする．A のイデアル全体の集合が積に関してなすモノイドの構造を求めよ．分数イデアルで同じことをせよ．$k[t^2, t^3]$ の極大イデアル (t^2, t^3) での局所化を B とする．B で同じことをせよ．

ここで整域 C の**分数イデアル** (*fractional ideal*) とは，$\operatorname{Frac} C$ の部分 C 加群 I であって，ある $c \in C \setminus \{0\}$ に対して $cI \subset C$ を満たすものである．

問題 H.11. 環準同型 $A \to B$ で，同型ではないが，誘導されるスペクトルの間の写像 $\operatorname{Spec} B \to \operatorname{Spec} A$ は全単射であるものを挙げよ．

問題 H.12. $A = \boldsymbol{Z}[a, b, s, t]/(a - sb, b - ta)$ とする．この環において $(a) = (b)$ だが a と b は同伴でないことを示せ．

問題 H.13. $G = \boldsymbol{Z}/n\boldsymbol{Z}$ および $G = \mathfrak{S}_3$ に対し，群環 $\boldsymbol{C}[G]$ を $\boldsymbol{C}$ 上の行列環の直積として表せ．（なお，$\boldsymbol{C} = \mathrm{M}(1, \boldsymbol{C})$ も $\boldsymbol{C}$ 上の行列環である．）

問題 H.14. A は整域でなく零環でもない（可換な）環であり，次の条件を満たす：任意のモニック多項式 $F \in A[x]$ に対し，集合 $\{a \in A \mid F(a) = 0\}$ の元の個数は $\deg F$ 以下である．このような環 A（の同型類）をすべて求めよ．

問題 H.15. 次の環が UFD か否か判定せよ．k は体とする．$k[X, Y]/(XY - 1)$，$\boldsymbol{Q}[X, Y]/(X^2 + Y^2 - 1)$，$\boldsymbol{Q}(\sqrt{-1})[X, Y]/(X^2 + Y^2 - 1)$.

問題 H.16 (参考：問題 8.6)**.** 環 A は 0 以外に冪零元をもたないとする（そのような環は**被約** (*reduced*) であるという）．このとき $A[X]^* = A^*$ が成り立つことを示せ．

問題 H.17. p を素数とする．位数 p^2 の環を分類せよ（同型類をすべて挙げよ）．

問題 H.18. $A \subset B \subset \operatorname{Frac} A$ を満たす整域 A, B で，どの積閉集合 $S \subset A$ に対しても B が A_S と一致しないものの例を挙げよ．

問題 H.19. X をコンパクトでない位相空間とし，$C_0(X, \boldsymbol{R})$ を X 上のコンパクト台実数値連続関数全体の集合とし，加法と乗法を各点ごとに定めると，これは環の公理のうち乗法の単位元の存在以外を満たすが，乗法の単位元は存在しない．真か偽か？

問題 H.20. A をアーベル群 $\boldsymbol{Z}$ とする．A に入りうる（単位的可換）環構造をすべて決定せよ．

問題 H.21. 本問においては環に単位的であることを要請せず，環の準同型に乗法の単位元を保つことを要請しない．前者を要請するときは単位的環，後者を要請するときは単位的環準同型ということにする．

(1) A を環とする．A の元 $a \in A$ と整数 $n \in \boldsymbol{Z}$ に対し，$n \cdot a \in A$ を

$$n \cdot a := \begin{cases} \overbrace{a + \cdots + a}^{n} & (n > 0), \\ 0 & (n = 0), \\ -((-n) \cdot a) & (n < 0) \end{cases}$$

で定める．このとき，$(n+n') \cdot a = n \cdot a + n' \cdot a$，$n \cdot (a+a') = n \cdot a + n \cdot a'$, $n \cdot (n' \cdot a) = (nn') \cdot a$ が成り立つことを確認せよ．

(2) A を環とする．直和アーベル群 $\boldsymbol{Z} \oplus A$ を B とおき，B に演算 $*$ を $(n,a) * (n',a') := (nn', n \cdot a' + n' \cdot a + aa')$ で定める．ただし $n \cdot a$ などは上で定めたもので，aa' は A の乗法である．B は単位的環になることを示せ．

(3) A が単位的ならば，B は直積環 $\boldsymbol{Z} \times A$ に同型であることを示せ．

(4) A が単位的でないならば，B は直積環 $\boldsymbol{Z} \times A$ に同型でないことを示せ．

(5) 自然な埋め込み $A \to \boldsymbol{Z} \oplus A = B$ を i とおく．C を単位的環とする．$f \mapsto f \circ i$ が，B から C への単位的環準同型全体の集合から A から C への環準同型全体の集合への全単射であることを示せ．（環 A からの単位的環 B の構成はこの意味で “自然” である．）

問題 H.22. UFD ではないが「既約元は素元」を満たす整域の例を挙げよ．

問題 H.23. k を標数 $p > 0$ の体とする．R_0 を $k[X]$ の (X) での局所化とし，R をその X 進完備化 $k[[X]]$ とする．$F \in k[[X]]$ を $k(X)$ 上超越的な元（定義は省略）とし，$G = F^p$ とし，$L = k(X)(G)$ ($k(X)$ 上 G が生成する体）とし，$R_1 = L \cap k[[X]]$ とする．$S = R_1[Y]/(Y^p - G)$ とする．$\mathfrak{m}_1 = XR_1 \subset R_1$, $\mathfrak{n} = XS + YS \subset S$ とし，R_1 と S のそれぞれ $\mathfrak{m}_1, \mathfrak{n}$ での完備化を $\hat{R}_1$，$\hat{S}$ と書く．このとき次を示せ．

- R_1 および S は整域である．
- $\hat{R}_1 = k[[X]]$.
- $\hat{S} \cong \hat{R}_1[Y]/(Y^p - G) \cong k[[X]][Y]/(Y^p - G)$.
- $\hat{S}$ は被約でない（0 以外の冪零元をもつ）.

余談. ネーター局所環 A が優秀環（定義は省略）ならば完備化は被約性を保ってしまい，単純な構成の環は大抵優秀になってしまうので，完備化が被約性を保たない例はそこそこ複雑にならざるを得ない．なお，標数 0 の体上の例も存在する．

問題 H.24. A を p 進完備な環（すなわち，A のイデアルの族 (p^n) による完備化から A への準同型が同型である）とする．$A/(p)$ のフロベニウス準同型 $\phi\colon A/(p) \to A/(p)\colon x \mapsto x^p$ が同型だとする．このとき，$A/(p)$ から A への写像 $[-]$ を次で定める：$x \in A/(p)$ に対し，各 $n \in \boldsymbol{N}$ に対して $\phi^{-n}(x)$ のリフト y_n をとり，$[x] := \lim_{n\to\infty} {y_n}^{p^n}$ とする．ただし $A \to A/(p)$ による逆像に属する元のことをリフトとよぶ．

- 列 ${y_n}^{p^n}$ が収束することと，極限は y_n の選び方に依存しないことを示せ．
- $x, x' \in A/(p)$ に対して $[x][x'] = [xx']$ が成り立つことを示せ．

この $[-]$ を**タイヒミュラーリフト** (*Teichmüller lift*) とよぶ．なお，$[x] + [x'] = [x + x']$ は基本的に成り立たないので，$[-]$ は環準同型ではない．

問題 H.25. $A = \boldsymbol{Z}[p^{1/p^n} \mid n \in \boldsymbol{N}]$ とおく．ただし p^{1/p^n} とは, $(p^{1/p})^p = p$, $(p^{1/p^{n+1}})^p = p^{1/p^n}$ を満たす元の

族とする．各 $n \in \boldsymbol{N}$ に対して $B_n = A/(p)$ とし, 推移写像をフロベニウス準同型 $f_{n+1}\colon B_{n+1} \to B_n\colon x \mapsto x^p$ とする射影系 $(B_n, f_{n+1})_{n\in\boldsymbol{N}}$ を考え，その射影極限を $A^\flat := \varprojlim_n B_n$ とおく．$A^\flat$ は $\boldsymbol{F}_p[T^{1/p^n} \mid n \in \boldsymbol{N}]$ の T 進完備化に同型であることを示せ．ただし T^{1/p^n} とは，$(T^{1/p})^p = T$，$(T^{1/p^{n+1}})^p = T^{1/p^n}$ を満たす元の族とする．

余談. A の p 進完備化 $\hat{A}$ は**パーフェクトイド環** (*perfectoid ring*) とよばれる種の環になり，$A^\flat$ はその**傾化** (*tilt*) とよばれる．一般にパーフェクトイド環とその傾化 $A^\flat$ は，前者は標数 0（混標数）かもしれない一方後者は標数 p であるという違いにもかかわらず，密接な関係がある．

問題 H.26. 環論の講義について……《この問題は解答を用意していません.》

- 環論の講義の演習問題を作ってみよう.
- 環論の講義の試験問題を作ってみよう.
- 環論の講義の講義ノートを作ってみよう.
- 環論の講義を行ってみよう.

問題 H.27. 環論に関する新しい定理を見つけよう．または，環論を用いて新しい定理を見つけよう.《この問題は解答を用意していません.》

演習問題のヒント

ヒント 1.6 2 通りの順番で $(1_A + 1_A)(a + b)$ を（分配法則を使って）展開する．

ヒント 2.1 例えば $\mathrm{Z}(A)$ が積で閉じていることを示す，すなわち，「A の任意の元と可換である」という性質をもつ 2 元をとり，その積も同じ性質をもつことを示す．

ヒント 2.4 1 を含まないか，または積で閉じていないことを示す．

ヒント 2.5 例 2.16 の基底 E, i, j, k を用いて（これらの線形結合として表して）計算するとよい．

ヒント 3.1 例えば $x, x' \in \mathrm{Im}\, f$ に対して $x + x' \in \mathrm{Im}\, f$ であることを示したいが，$\mathrm{Im}\, f$ の定義より $a, a' \in A$ で $x = f(a), x' = f(a')$ なるものをとれる．これと準同型の定義（の中の適切な条件）を用いる．

ヒント 3.3 0_A や 1_A が A^σ に含まれることや，$x, y \in A^\sigma$ のとき $-x, x + y, xy \in A^\sigma$ であることを示す．示すために σ が環準同型であることを用いる．

ヒント 3.4 示すべきことは問題 3.3 と同様で，示すために f, g が環準同型であることを用いる．

ヒント 3.5 例えば加法群として $\boldsymbol{Z} \times \boldsymbol{Z}$ に同型であるものが無限個ある．

ヒント 3.6 例 3.20 より $\boldsymbol{Z}$ への制限は一致する．$f(x \cdot \frac{1}{x})$ や $f(\frac{1}{x} \cdot x)$ を考える．

ヒント 3.8 準同型を f とおく．(1)：$n \cdot 1$ の像を考える．(2)，(3)：$f(\sqrt{2})$ は $f(\sqrt{2})^2 = 2$ を満たすことに注目する．(4)：$\boldsymbol{R}$ の元 x, y に対して，「$x \geq y$」は「ある $z \in \boldsymbol{R}$ に対して $x = y + z^2$」と同値であることに注目する．また，$\boldsymbol{Q}$ に制限して得られる準同型 $\boldsymbol{Q} \to \boldsymbol{R}$ の一意性も使える（例 3.23）．

ヒント 4.4 適当に行列要素をかけることで，$E_{22} \in I$ を示す．後半はランクを検討する．

ヒント 4.5 積で閉じているか否かが焦点で，I の生成元（I なら $2, \sqrt{m}$）と A の元の積を考えれば十分である．

ヒント 4.8 (1) イデアルであること：$a, b \in \sqrt{I}$ に対して $a + b \in \sqrt{I}$ であること：a, b に対して条件を満たす n, m をとり，これに応じて十分大きい N をとる．他（スカラー倍で閉じていることなど）は容易．$I \subset \sqrt{I}$ は，$n = 1$ をとればよい．

ヒント 4.9 イデアルであること：$(I : J)$ が和で閉じていることを，元をとって定義に則って示す．他は容易．
(4),(5) は，$a \in A$ が左辺に属することと右辺に属することの同値を形式的変形で示せる．

ヒント 4.10 イデアルが A 全体に一致することと 1 を含むことは同値である．1 を I の元と J の元の和で書いたうえでなんとかする．

ヒント 4.12 和で閉じていないことを示してもよいし，スカラー倍で閉じていないことを示してもよい．

ヒント 5.3 命題 5.18 を用いる．また，$\boldsymbol{Z}$ の場合 n を含むイデアルとはすなわち n の約数で生成されるイデアルである．
例えば $(30) \subset B = \boldsymbol{Z}/36\boldsymbol{Z}$ の場合，$(30) = (6)$ であることが分かる（30 と 36 の最大公約数を求める）．

ヒント 5.5 2 や 3 と素でない場合が怪しい.

ヒント 5.6 逆に 2 や 3 と素な部分がなくなる.

ヒント 5.7 命題 5.18 を用いる．また，$\boldsymbol{Z}$ の場合 n を含むイデアルとはすなわち n の約数で生成されるイデアルである.

ヒント 6.1 (4)： $\mathrm{Nm}(a-bq) < \mathrm{Nm}(b)$ は $\mathrm{Nm}(\frac{a}{b}-q) < \mathrm{Nm}(1) = 1$ と同値である.

ヒント 6.3 $(x^n-1, x^m-1) \subset \boldsymbol{R}[x]$ について：通常の正整数の余り付き割り算で n を m で割った余りが r であるとき，ある $q \in \boldsymbol{R}[x]$ に対して $x^n-1 = (x^m-1)q + x^r - 1$ となる．したがってこの操作は n と m の最大公約数をユークリッドの互除法で求める操作と平行に進む.

ヒント 7.6 ノルム写像 $\mathrm{Nm}\colon A \to \boldsymbol{N}$ を $\mathrm{Nm}(x+y\sqrt{m}) = (x+y\sqrt{m})\overline{(x+y\sqrt{m})} = x^2 + (-m)y^2$ で定める．$a, b \in A$ に対し $\mathrm{Nm}(ab) = \mathrm{Nm}(a)\,\mathrm{Nm}(b)$ が成り立つことを示し，$\mathrm{Nm}(a) = \pm 1 \iff a \in A^*$ であることを示す.

ヒント 7.7 順序関係の公理のうち反対称律が焦点である.

ヒント 8.1 $\boldsymbol{R}$ は濃度を考える．$\boldsymbol{Q}$ については，有限個の元 $\frac{m_1}{n_1}, \ldots, \frac{m_k}{n_k}$（$m_i \in \boldsymbol{Z}, n_i \in \boldsymbol{Z} \setminus \{0\}$）で生成されたとして，$n_1, \ldots, n_k$ のどれも割らない素数を考える.

ヒント 8.3 [群論] での群やアーベル群での議論を思い出す.

ヒント 8.5 $\mathrm{Z}(A[X])$ の元をとり A の任意の元とかけてみる.

ヒント 8.6 2 元の積が 1 だとして,

ヒント 8.9 $I \subset \mathrm{Ker}\, f$ は計算すれば分かる．$\mathrm{Ker}\, f$ が I より真に大きいとすると，$\mathrm{Ker}\, f$ は簡単な形の元（(1) なら $a + bX$ の形の元）を 0 以外にもつことになるが，その元の像が 0 でないことは比較的簡単に確かめられる.

ヒント 8.10 系 8.24 と帰納法を使う.

ヒント 9.1 $\boldsymbol{Z}[\sqrt{-1}]$ は単項イデアル整域ゆえ素元分解整域であり，したがって既約元は素元である．また，$\boldsymbol{Z}[\sqrt{-1}]$ の元のノルム $\mathrm{Nm}(x+y\sqrt{-1}) = x^2 + y^2$ は 0 以上であり，かつ $0, 1, 2 \pmod 4$ のどれかであることに注意する.

ヒント 9.2 1 つ 1 つ元の位数を計算してもいいが，この体の場合は逆に生成元でない（位数が小さすぎる）元がすべて簡単に求まる.

ヒント 9.3 既約性を示すには，代数的整数の場合はノルムが使える場合があり，多項式環の部分環の場合は多項式環での素元分解が使える場合がある.

ヒント 10.3 素元と素イデアルの定義を見比べる．問題 10.2 を使う.

ヒント 10.4 それぞれで剰余環を考える.

ヒント 10.6 対偶を示すのがやりやすい.

ヒント 10.7 任意の $i \neq j$ に対して $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ だと仮定できる．各 i に対し，$\mathfrak{p}_i$ には属さず他の $n-1$ 個には属する元をみつけることを考える．

別解：n に関する帰納法を使うとよいかもしれない．I の元について，n 個の素イデアルに属する・属さないのパターンとして何が可能か書いてみるとよいかもしれない．

ヒント 11.2 $(a_1, s_1) \sim (a_2, s_2) \sim (a_3, s_3)$ と仮定し，ここから得られる A での等式 2 つから a_2 を消去する．

ヒント 11.4 0 以外の $\boldsymbol{Z}[\sqrt{m}$ の元 $a + b\sqrt{m}$ は，$\boldsymbol{Q}[\sqrt{m}]$ で逆元をもつことを示せばよい．

ヒント 11.5 $\frac{a}{s}$ の行先が何であるべきか考える．

ヒント 11.6 S として $\{n \in \boldsymbol{Z} \setminus \{0\} \mid \frac{1}{n} \in B\}$ を考える．

ヒント 11.7 $A_f \to A[X]/(fX-1)$ を定めるには $\frac{1}{f}$ の行先を適切に定めればよく，$A[X]/(fX-1) \to A_f$ を定めるには X の行先を適切に定めればよい．

ヒント 11.8 まず両方向にそれらしい写像を作ることを考える．

ヒント 11.9 問題 10.3 を使う．

ヒント 11.10 命題 11.20 や問題 11.9 を使う．

ヒント 11.11 これらの環の間に自然な準同型を作ればよい（互いに逆であることは構成から明らかになるように）．

ヒント 12.2 12 節で挙げた環の例の中にある．

ヒント A.1 $f(y) = f(y \cdot 1_A)$ である．

ヒント A.5 $M \setminus \{0\}$ の元の列で，Ann が単調に増加するものをとり，止まったところで素イデアルであることを示す．

ヒント A.6 $A = \boldsymbol{Z}$ とし，完全列として $0 \to \boldsymbol{Z} \xrightarrow{[2]} \boldsymbol{Z} \xrightarrow{\pi} \boldsymbol{Z}/2\boldsymbol{Z} \to 0$ を考えると 3 つ全部倒せる．ただし [2] は 2 倍写像 $x \mapsto 2x$ で，π は標準的射影とする．

ヒント D.2 (1) $\mathfrak{p}_0 = \{\sum_{i \geq 0} a_i Y^i \in B \mid a_0 = 0\}$ に注意する．$\mathfrak{p}_0$ は極大イデアルなので，あとは，$(0) \subsetneq \mathfrak{q} \in \operatorname{Spec} B_0$ ならば $\mathfrak{q} \supset \mathfrak{p}_0$ であることを示せばよい．$f \in \mathfrak{q} \setminus \{0\}$，$g \in \mathfrak{p}_0$ とし，n を $f \in Y^n B$（※ $Y^n B_0$ ではない）なる最大の整数とするとき，f は g^{n+1} を割りきることを示せ．

ヒント F.1 フロベニウス写像は単射準同型である．

ヒント F.2 準同型（フロベニウス写像）の像なので．

ヒント F.3 前半：$a \in I$ のとき $a^p \in (a_1^p, \ldots, a_n^p)$ であることを示せばよい．後半：単項生成だと一致してしまう．

ヒント F.6 $\frac{d}{dX}$ は Leibniz 則 $(PQ)' = P'Q + PQ'$ を満たす．

ヒント G.1 M_0 の元をとりその逆像をとり……

ヒント G.5 (2) 問題 12.3 の略解で使った議論をまねる．
(1), (3) x^n の係数を比較する．$\alpha, \beta \in \boldsymbol{N}$ ならば成り立つことを用いる．

ヒント H.4 各素数 p に対し，p^n（$n \in \boldsymbol{Z}$）のうちどれを含むかを考える．

ヒント H.5 実は問題 11.6 で解決している．

ヒント H.6 一般には成り立たない．

ヒント H.9 ちなみにデデキント整域（定義は省略）だとつねに等式が成り立つので，反例はそうでない 1 次元ネーター整域から探す必要がある．

ヒント H.10 A のイデアルは (0) と (t^n)（$n \in \boldsymbol{N}$）で尽くされる．B のイデアルについては例えば $(t^2 + at^3)$（$a \in k$）と (t^2, t^3) がありこれらはどの 2 つも相異なる．

ヒント H.13 $G = \boldsymbol{Z}/n\boldsymbol{Z}$ の場合：$\boldsymbol{C}[G]$ から $\boldsymbol{C}$ への環準同型をすべて求めてみよ（ヒント：G の生成元を 1 つとりその行先を考える）．
$G = \mathfrak{S}_3$ の場合，$\boldsymbol{C}[G]$ 加群 $\boldsymbol{C}^3$ の既約加群への分解を考えよ．

ヒント H.15 問題 11.10 を使う．例えば X が既約元や素元であるか考える．

ヒント H.16 定理 10.10 は冪零元と素イデアルの関係を与える．

ヒント H.20 $\boldsymbol{Z}$ の生成元を 1 つとり 1 と書くが，これは A の乗法の単位元とは限らないことに注意する．双線形写像を決めるには $(1, 1)$ の像だけ決めればよい．
別のヒント：A の乗法の単位元 e が A の元 a の正整数倍 $e = na$ と書けたら $n = 1$ であることを示せ．

ヒント H.24 $n \geq 1$ で $y \equiv y' \pmod{p^n}$ ならば $y^p \equiv y'^p \pmod{p^{n+1}}$ が成り立つことを用いる．

ヒント H.25 $A^\flat$ の元 $(p, p^{1/p}, p^{1/p^2}, \dots)$ を t とおく．

演習問題の略解

略解 1.6 ヒントの続き：すると $a+a+b+b = a+b+a+b$ を得る．a の逆元を左から，b の逆元を右から加えることで $a + b = b + a$ が分かる．

略解 2.1 $1_A \in \mathrm{Z}(A)$ は明らか．$0_A \in \mathrm{Z}(A)$ は補題 1.5(1) から分かる．$b_1, b_2 \in \mathrm{Z}(A)$ に対して $-b_1, b_1 + b_2, b_1 b_2 \in \mathrm{Z}(A)$ を示そう．任意の $c \in A$ に対して，補題 1.5(2) や結合法則や分配法則より $(-b_1)c = -(b_1 c) = -(cb_1) = c(-b_1)$，$(b_1 + b_2)c = b_1 c + b_2 c = cb_1 + cb_2 = c(b_1 + b_2)$，$b_1 b_2 c = b_1 c b_2 = c b_1 b_2$ が成り立つので，$-b_1, b_1 + b_2, b_1 b_2$ も任意の $c \in A$ と可換であり，すなわち $\mathrm{Z}(A)$ の元である．

略解 2.2 (2) と (3) は部分環．(1)：$\sqrt[3]{2}^2$ を含まないので部分環でない．これが生成する部分環は (2) の環．(4)：$\sqrt{2} \cdot \sqrt{3}$ を含まないので部分環でない．これが生成する部分環は「$+d\sqrt{6}$（$d \in \boldsymbol{Z}$）」を書き加えたもの．

略解 2.4 問題の集合を A とおく．部分環であるためには $1 \in A$ でないといけないので，$q = \frac{1}{n}$，$n \in \boldsymbol{Z} \setminus \{0\}$ の形でないといけない．$q \neq \pm 1$ という仮定より $n \neq \pm 1$ である．このとき，$\frac{1}{n} \in A$ だが，$\frac{1}{n} \cdot \frac{1}{n} = \frac{1}{n^2} \notin A$ な

ので，A は乗法について閉じていない．

略解 2.5 単位行列およびそのスカラー倍が他の行列と可換なのは明らか．逆を示す．$x = aE + bi + cj + dk \in \mathrm{Z}(\mathbf{H})$（$a, b, c, d \in \boldsymbol{R}$）とする．$xi = ix$ の両辺を計算して E, i, j, k の $\boldsymbol{R}$ 線形結合で表し，j, k の係数を比較すると $c = d = 0$ を得る．同様に $xj = jx$ から $b = d = 0$ を得る．（同様に $xk = kx$ から $b = c = 0$ を得る．）したがって $x = aE$ である．

なお，成分表示を用いて（≒ 行列単位 $E_{11}, E_{12}, E_{21}, E_{22}$ という行列環の基底の線形結合で表して）計算することもできるが，基底 E, i, j, k を用いた方がたぶん楽である．

なお，$\mathbf{H}$ の任意の元と可換であるという仮定から，$\mathrm{M}(2, \boldsymbol{R})$ や $\mathrm{M}(2, \boldsymbol{C})$ の任意の元と可換であるとはいえない（結果的には正しいが）．

$\{aE + bi \mid a, b \in \boldsymbol{R}\} \subset \mathbf{H}$ は $\mathrm{Z}(\mathbf{H})$ を含み可換な部分環である．実は，$\boldsymbol{R}$ 部分ベクトル空間 $A \subset \mathbf{H}$ で $\boldsymbol{R} \cdot E$ を含み $\dim_{\boldsymbol{R}} A = 2$ であるものはすべて条件を満たし，逆に条件を満たす部分環はすべてこの形である．実際，A が条件を満たすとすると，$x \in A$ で $x \notin \boldsymbol{R} \cdot E$ を満たすものが存在するが，A は可換なのでとくに x と可換な元からなり，つまり $A \subset \{y \in \mathbf{H} \mid xy = yx\}$ であり，成分表示を用いて計算すると右辺の $\boldsymbol{R}$ 上の次元が 2 であることが分かる．

略解 3.1 まず加法に関して部分群であることを示す．$x, x' \in \operatorname{Im} f$ とする．（$x + x' \in \operatorname{Im} f$ を示したい．）$\operatorname{Im} f$ の定義より $a, a' \in A$ で $x = f(a), x' = f(a')$ なるものをとれる．f は準同型なので $x + x' = f(a) + f(a') = f(a + a')$ であり，$a + a' \in A$ なので $x + x' \in \operatorname{Im} f$ である．単位元 0_B と逆元 $-x$ については補題 3.2 を使って同様にできる．$x \cdot x' \in \operatorname{Im} f$ も和と同様にできる．$1_B \in \operatorname{Im} f$ は準同型の定義より $1_B = f(1_A)$ であることから従う．

略解 3.3（示すべきことについてはヒントを参照.）$x, y \in A^\sigma$ のとき $\sigma(x + y) = \sigma(x) + \sigma(y) = x + y$ が成り立つ．他も同様.

$\boldsymbol{C}^\sigma$ は $\boldsymbol{R}$.

なお，本問は問題 3.4 の特殊な場合（$B = A, f = \mathrm{id}, g = \sigma$）でもある．

略解 3.4（示すべきことについてはヒントを参照.）$x, y \in A'$ のとき $f(x + y) = f(x) + f(y) = g(x) + g(y) = g(x + y)$ が成り立つ．他も同様.

一般の場合も同様にできる．または，$\lambda, \mu \in \Lambda$ に対し $A'_{\lambda,\mu} := \{a \in A \mid f_\lambda(a) = f_\mu(a)\}$ を考え（これは前半より部分環である），$A' = \bigcap_{(\lambda,\mu)\in\Lambda^2} A'_{\lambda,\mu}$ を確認しこれに命題 2.4 を適用してもよい．

略解 3.5 直積環 $A = \boldsymbol{Z} \times \boldsymbol{Z}$ および，平方数でない相異なる整数 m, m' に対する $B = \boldsymbol{Z}[\sqrt{m}]$，$B' = \boldsymbol{Z}[\sqrt{m'}]$ を考えると，これらはどれも同型でない．まず A は 0 でない 2 元の積が 0 になることがあり（例えば $(0, 1) \cdot (1, 0) = (0, 0)$），$B, B'$ はそうではない（成分計算で確かめられる）ので，A は B, B' と同型でない．また，集合 $S = \boldsymbol{Z} \cap \{\beta^2 \mid \beta \in B\}$ は $\{mk^2 \mid k \in \boldsymbol{Z}\}$ に等しいことが成分計算で確かめられ，この集合は m ごとに異なるので，B と B' も同型でない．

略解 3.6 $1_A = f(1_{\boldsymbol{Q}}) = f(x \cdot \frac{1}{x}) = f(x) \cdot f(\frac{1}{x})$ など．$f(n)$ と $g(n)$ が等しいので，それらの左かつ右逆元である $f(\frac{1}{n})$ と $g(\frac{1}{n})$ も等しい．最後は $f(m) = g(m)$ と $f(\frac{1}{m}) = g(\frac{1}{n})$ から従う．

略解 3.7 $f\colon k_1 \to k_2$ を体の間の準同型とする．$a \in k_1 \setminus \{0\}$ とすると，k_1 は体なので $ab = 1_{k_1}$ を満たす $b \in k_1$ が存在する．このとき $f(a)f(b) = f(1_{k_1}) = 1_{k_2}$ であり，k_2 は零環でないので $1_{k_2} \neq 0_{k_2}$ である．し

たがって $f(a)$ も 0 でない.

別解：後に定義する素イデアルを用いる．$(0) \subset k_2$ は素イデアルであり，その縮約 $f^{-1}(0) \subset k_1$ も素イデアルである（命題 10.7）．体の素イデアルは (0) しかないので，$f^{-1}(0) = (0)$ が成り立つ.

略解 3.8 (1)：$\boldsymbol{Z}/n\boldsymbol{Z}$ では $n \cdot 1_{\boldsymbol{Z}/n\boldsymbol{Z}}$（$n$ 個の $1_{\boldsymbol{Z}/n\boldsymbol{Z}}$ の和）は $0_{\boldsymbol{Z}/n\boldsymbol{Z}}$ だが，$\boldsymbol{Z}$ では $n \cdot 1_{\boldsymbol{Z}} \neq 0_{\boldsymbol{Z}}$ なので，環の準同型は存在しない.

(2) 準同型 f に対して $f(\sqrt{2})^2 = f(\sqrt{2}^2) = 2$ となるが，$\boldsymbol{Q}$ に $x^2 = 2$ を満たす元は存在しない.

(3) 前項と同じ議論で，$f(\sqrt{2})$ は $\sqrt{2}$ または $-\sqrt{2}$ である．どちらの場合も，$\sqrt{2}$ の像と 1 の像が決まったことで f は一意的に定まる．また，前者の場合（id）は明らかとして，後者の場合の $x + y\sqrt{2} \mapsto x - y\sqrt{2}$ が準同型であることも簡単に確認できる.

(4) $f\colon \boldsymbol{R} \to \boldsymbol{R}$ を準同型とする．ヒントの後半から $f|_{\boldsymbol{Q}} = \mathrm{id}_{\boldsymbol{Q}}$ である．ヒントの前半から，$x \geq y$ を満たす任意の $x, y \in \boldsymbol{R}$ に対して，$x + z^2 = y$ を満たす z がとれて，このとき $f(x) + f(z)^2 = f(y)$ なので $f(x) \geq f(y)$ である．x または y として有理数をとることで，任意の $x \in \boldsymbol{R}$ に対し $f(x) = x$ であることが分かる（もし $x < f(x)$ だとすると，$x < y < f(x)$ を満たす $y \in \boldsymbol{Q}$ を考えることで矛盾し，$x > f(x)$ の場合も同様に矛盾する）.

略解 3.9 $\boldsymbol{R}$ から $\boldsymbol{R} \setminus \{0\}$ に制限するとき全射でない．例えば $C(\boldsymbol{R} \setminus \{0\}, \boldsymbol{R})$ の元 $\mathrm{sgn}(x)$ や $1/x$ は像に属さない.

$\boldsymbol{R} \setminus \{0\}$ から $\boldsymbol{R}_{>0}$ に制限するとき単射でない．例えば 1（定数写像）と $\mathrm{sgn}(x)$ の像が一致する.

$V \subsetneq U$ として r が全単射でないことを示す．$y \in U \setminus V$ をとる．y が V の閉包に属するならば，$1/|x - y|$ は像に属さないので全射でない．y が V の閉包に属さないならば，y を中心とする適当な半径 $\varepsilon > 0$ の開球は V と交わらず，この開球の外で 0 であり恒等的には 0 でない U 上の連続写像が存在し，その V への制限は 0 なので単射でない.

最後の例については密着でも離散でもない 2 点位相空間を考えればよい.

略解 4.1 加法群であること：和で閉じていることは $ba + b'a = (b + b')a$，0 は $0 = 0a$，逆元は $-(ba) = (-b)a$．左からのスカラー倍で閉じていること：$c(ba) = (cb)a$.

略解 4.3 $a \in A \setminus \{0\}$ とする．Aa は左イデアルであり（問題 4.1），明らかに $\{0\}$ でないので仮定より $Aa = A$ である．すなわち，a の乗法の左逆元 y が存在する．同様に，a の乗法の右逆元 z が存在する．そしてこのとき $y = yaz = z$ なので $y = z$ なので，A は斜体の定義の条件（定義 1.10）を満たす.

略解 4.4 I が両側イデアルなので，$E_{22} = E_{21}E_{11}E_{12} \in I$ である．したがって $E = E_{11} + E_{22} \in I$ なので，$I = A$ である.

$x, y \in A$ に対し $\operatorname{rank} xE_{11}y \leq \operatorname{rank} E_{11} = 1$ であり，一方で $\operatorname{rank} E = 2$ なので，E は集合 $\{xE_{11}y \mid x, y \in A\}$ に属さない.

略解 4.5 I：m が奇数ならば，$\sqrt{m} \in I$ と $\sqrt{m} \in A$ の積 m が属さないのでイデアルでない．m が偶数ならばイデアルである.

J：m が偶数ならば，$1 + \sqrt{m} \in I$ と $\sqrt{m} \in A$ の積 $(m - 1) + (1 + \sqrt{m})$ が属さないのでイデアルでない．m が奇数ならばイデアルである.

略解 4.6 順に (2)，(30)，(60)，(36)．$\boldsymbol{Z}$ のイデアル（すべて単項イデアルである）の場合，イデアルの和と共

通部分は整数の最大公約数と最小公約数に対応し，積や累乗は整数のそれと対応する．

略解 4.7 順に (x)，(x^3-x^2)，(x^4-x^3)，(x^4)．

略解 4.8 (1) $a,b\in\sqrt{I}$ とすると，ある正整数 n,m に対して $a^n,b^m\in I$ である．このとき，2 項定理を用いた展開 $(a+b)^{n+m-1}=\sum_{i+j=n+m-1}\binom{*}{*}a^ib^j$（2 項係数の中身はどうでもいい）において，各 (i,j) に対し，$i\geq n$ と $j\geq m$ の少なくとも一方が成り立つ．a^n と b^m で括ることで $(a+b)^{n+m-1}=a^nx+b^my$ $(x,y\in A)$ と書けて，右辺は明らかに I に属する．

(3) $a\in\sqrt{\sqrt{I}}$ ならば，ある正整数 n に対して $a^n\in\sqrt{I}$ であり，このときある正整数 m に対して $(a^n)^m\in I$ であり，$(a^n)^m=a^{nm}$ である．

(4) $a^n\in I$ ならば $a^{nm}\in I^m$ である．

略解 4.9 $a_1,a_2\in(I:J)$ のとき $a_1+a_2\in(I:J)$ であることを示す．$j\in J$ に対して $(a_1+a_2)j\in I$ であることを示せばよく，$a_1j,a_2j\in I$ なのでよい．

$a\in((I_1\cap I_2):J)\iff aJ\subset I_1\cap I_2\iff aJ\subset I_1,aJ\subset I_2\iff a\in(I_1:J)\cap(I_2:J)$.

$a\in(I:(J_1+J_2))\iff a(J_1+J_2)\subset I\iff aJ_1,aJ_2\subset I\iff a\in(I:J_1)\cap(I:J_2)$.

略解 4.10 イデアルが A 全体に一致することと 1 を含むことは同値である．和の定義より $a\in I,b\in J$ で $a+b=1$ を満たすものをとれる．2 項定理を用いた展開 $1=1^{n+m-1}=\sum_{i+j=n+m-1}\binom{*}{*}a^ib^j$（2 項係数の中身はどうでもいい）において，各 (i,j) に対し，$i\geq n$ と $j\geq m$ の少なくとも一方が成り立つ．a^n と b^m で括ることで $1=a^nx+b^my$（$x,y\in A$）と書けて，右辺は明らかに I^n+J^m に属する．

別証明：$K=I^n+J^m$ とし，$\sqrt{K}=\{a\in A\mid$ ある正整数 t に対し $a^t\in K\}$ を考える（問題 4.8 より，これはイデアルである）．$\{b^n\mid b\in I\}\subset I^n\subset K$ より $I\subset\sqrt{K}$ であり，同様に $J\subset\sqrt{K}$ である．すると $1\in I+J\subset\sqrt{K}$ よりある正整数 t に対し $1=1^t\in K$ である．（なお，引用した問題 4.8 では実のところ本問の最初の解答と同じようなことを行う．）

略解 4.11 イデアルの積をとる操作が包含関係を保つ（$I'\subset I$ かつ $J'\subset J$ ならば $I'J'\subset IJ$ を満たす）ことは定義から明らかである．

ひとつめの包含関係は，$I\cap J\subset I$ と $I\cap J\subset J$ から分かる．$IJ\subset I$ と $IJ\subset J$ は明らかに成り立つので，ふたつめの包含関係も分かる．

略解 4.12 問題の集合を S とおくと，$E_{12},E_{21}\in S$ だが，$E_{12}+E_{21}$ は 2 乗が単位行列なので $E_{12}+E_{21}\notin S$ である．すなわち，S は和で閉じていない．また，$E_{21}E_{12}=E_{11}$ は 2 乗が自分自身なので $E_{21}E_{12}\notin S$ である．すなわち，S は左からのスカラー倍でも右からのスカラー倍でも閉じていない．

略解 4.13 Nm が積を保つことは直接計算で分かる．

方程式 $x^2+5y^2\in\{1,2,3\}$ の整数解は，整数の平方のとりうる値が $0,1,4,\ldots$ であることから，簡単に列挙できる．

(3) は以上のことから分かる．（例えば $ab=2$ なら $\mathrm{Nm}(a)\,\mathrm{Nm}(b)=\mathrm{Nm}(ab)=\mathrm{Nm}(2)=4$ だが，$(\mathrm{Nm}(a),\mathrm{Nm}(b))=(2,2)$ は不可能であり，$(\mathrm{Nm}(a),\mathrm{Nm}(b))=(1,4)$ と $(\mathrm{Nm}(a),\mathrm{Nm}(b))=(4,1)$ のときはそれぞれ $a=\pm1$，$b=\pm1$ である．）

(4) 系 4.21 より，$RS=(3\cdot3,3\cdot(1-\sqrt{-5}),(1+\sqrt{-5})\cdot3,(1+\sqrt{-5})\cdot(1-\sqrt{-5}))$ である．まず $RS\subset(3)$ を示す．RS を生成する 4 元のうち最初の 3 個が (3) に属するのは明らかであり，4 個目も

$(1+\sqrt{-5})\cdot(1-\sqrt{-5})=3\cdot 2$ なので属する．次に $RS\supset(3)$ を示す．$RS\ni 3\cdot 3,(1+\sqrt{-5})\cdot(1-\sqrt{-5})$ なので，$RS\ni 3\cdot 3-(1+\sqrt{-5})\cdot(1-\sqrt{-5})=3$ であり，したがって $RS\supset(3)$ である．$PQ=(2)$ と $QS=(1-\sqrt{-5})$ も同様にできる．

略解 5.3 (36)，(6)，(6)，(4)，(9).

略解 5.4 (5)，(5)，(25)，(2)，(2)，(4)．一致するのは J が (5) と $(1+\sqrt{-1})^2$ の場合のみ（なお後者は (2) に等しい）.

略解 5.5 (7)，(1)，(1)，(5).

略解 5.6 (1)，(2)，(3)，(2).

略解 5.7 例えば $n=12$ の場合，(1)，(2)，(3)，(4)，(6)，(12)．ただし $i\in\boldsymbol{Z}$ の剰余類のことも i と書いた.

略解 6.2 $-m\geq 1$ のとき，$|z-q|\leq\frac{1}{4}(\sqrt{-m}+\frac{1}{\sqrt{-m}})$ にできて，$1\leq -m<(2+\sqrt{3})^2\approx 13.9$ のとき右辺は <1 である.

略解 6.3 (37), $(2-\sqrt{-1})$, (1)，$(2-\sqrt{-1})$, $(3+2\sqrt{-1})$, (x^2-x), $(x^{\gcd\{n,m\}}-1)$, (1)，$(x^{\gcd\{n,m\}}-1)$,

ちなみに $\boldsymbol{Z}[\sqrt{-1}]$ における各元の素因数分解は $4-2\sqrt{-1}=-\sqrt{-1}(1+\sqrt{-1})^2(2-\sqrt{-1}),\ 3\pm 4\sqrt{-1}=(2\pm\sqrt{-1})^2,\ 5=(2+\sqrt{-1})(2-\sqrt{-1}),\ 8+\sqrt{-1}=(2-\sqrt{-1})(3+2\sqrt{-1}),\ 7+4\sqrt{-1}=\sqrt{-1}(2-\sqrt{-1})(3-2\sqrt{-1}),\ 7-4\sqrt{-1}=-\sqrt{-1}(2+\sqrt{-1})(3+2\sqrt{-1})$，となり，$\pm\sqrt{-1}$ は可逆な元なのでイデアルを考えるにあたっては無視できる.

略解 7.3 (3) は，有限集合から自身への写像について単射と全射が同値であることを用いる．なお，有限でない環ではほとんどの場合に成り立たない.

略解 7.5 $a=1a$．$a=ub$ ならば $b=u^{-1}a$．$a=ub$ かつ $b=vc$ ならば $a=uvc$.

略解 7.6 $m=-1$ のとき $\{\pm 1,\pm\sqrt{-1}\}$ で，$m<-1$ のとき $\{\pm 1\}$.

後半：$m=-3$ のとき $\{\pm 1,\frac{\pm 1+\sqrt{-3}}{2}\}$ で，それ以外のとき $\{\pm 1\}$.

略解 7.7（整除関係は反射律および推移律を満たす.）A が 1 以外の単元 u をもつとき，1 と u はお互いを割りきるが等しくないので，A 上の整除関係は反対称律を満たさず，したがって順序関係でない．そのような A, u の例としては $A=\boldsymbol{Z}$，$u=-1$ がある.

同伴関係を $\sim$ と書き，それによる商集合を $A/\!\sim$ と書く．$a\mid b$（a は b を割りきることをこの記号で表す）かつ $a\sim a'$，$b\sim b'$ ならば $a'\mid b'$ であることを確認する（これにより順序関係が $A/\!\sim$ 上の well-defined な 2 項関係を定めることが分かる）．同伴と整序の定義より $b=ca$，$a'=ua$，$b'=vb$ なる $c\in A$ と $u,v\in A^*$ が存在し，すると $b'=vcu^{-1}a'$ である.

$A/\!\sim$ 上の整除関係が順序関係であることは，「$a\mid b$ かつ $b\mid a$ ならば単数 $u\in A^*$ が存在して $a=ub$」を満たすことと同値であるが，例えば問題 H.12 の環はこの条件を満たさないので，一般には順序関係にならない.

略解 7.8 f が単射ならば部分集合においてもそうなので f^* も単射である.

f が全単射ならばすなわち環の同型写像なので当然 f^* も同型であり全単射である.

$f\colon\boldsymbol{Z}\to\boldsymbol{Z}/5\boldsymbol{Z}$ は全射だが，$\boldsymbol{Z}^*=\{\pm 1\}$ から $(\boldsymbol{Z}/5\boldsymbol{Z})^*=\{[1],[2],[3],[4]\}$ へは全射でない.

A を整域とすると $A[X]^*=A^*$ が成り立つ（命題 8.10）．したがって，$f\colon\boldsymbol{Z}\to\boldsymbol{Z}[X]$ は f^* が全単射だが

f は全射でない例であり，$f\colon \boldsymbol{Z}[X] \to \boldsymbol{Z}\colon X \mapsto 0$ は f^* が全単射だが f は単射でない例である．

略解 8.1 環 A 上有限生成な代数の濃度は $|A| \cdot |\boldsymbol{N}|$ 以下であることが示せる．$|\boldsymbol{Z}| \cdot |\boldsymbol{N}| = |\boldsymbol{N}| < |\boldsymbol{R}|$ なので $\boldsymbol{R}$ は $\boldsymbol{Z}$ 上有限生成でない．

$\boldsymbol{Q}$ の有限生成な部分 $\boldsymbol{Z}$ 代数 $B = \frac{m_1}{n_1}, \dots, \frac{m_k}{n_k}$（$m_i \in \boldsymbol{Z}, n_i \in \boldsymbol{Z} \setminus \{0\}$）を考える．$p$ を $n_1 \dots n_k$ を割らない素数とすると，$\boldsymbol{Z}[\frac{m_1}{n_1}, \dots, \frac{m_k}{n_k}]$ は $\boldsymbol{Q}$ の真部分環 $\{\frac{m}{n} \mid m, n \in \boldsymbol{Z}, n \notin p\boldsymbol{Z}\}$ に含まれるので，$\boldsymbol{Q}$ より真に小さい．したがって $\boldsymbol{Q}$ は $\boldsymbol{Z}$ 代数として有限生成でない．

略解 8.2 例えば，$A = k[x, xy] \subset B_1 = k[x, xy^n \mid n \in \boldsymbol{N}] \subset B_2 = k[x, y]$ とすると，$B_2 = A[y]$ は A 代数として有限生成であり，B_1 は有限生成でない．B_1 が有限生成でないことの証明：有限個の元 $f_1, \dots, f_m \in B_1$ に対し，ある $N \in \boldsymbol{N}$ が存在し，$f_1, \dots, f_m \subset k[x, xy^n \mid 1 \leq n \leq N] \subsetneq B_1$ となるので，$A[f_1, \dots, f_m] \subsetneq B_1$ である．

略解 8.3 (1) は [群論, 命題 11.4] と同様．(2) は [群論, 命題 12.2] と同様．

略解 8.5 $f = \sum_{i=0}^{n} a_i X^i \in \mathrm{Z}(A[X])$ とすると，任意の $b \in A \subset A[X]$ に対して $bf = fb$ であることから任意の $b \in A$ に対して $ba_i = a_i b$ であり，すなわち $a_i \in \mathrm{Z}(A)$ である．$\mathrm{Z}(A)[X] \subset \mathrm{Z}(A[X])$ は明らか．

略解 8.6 $A[X]$ が零環でないことは明らか．$f, g \in A[X] \setminus \{0\}$ として，$f = \sum_{i=0}^{n} a_i X^i$，$g = \sum_{j=0}^{m} b_j X^j$（$a_n, b_m \neq 0$）と書く．このとき fg は $n+m$ 次の係数が 0 でないので $fg \neq 0$ である．次に，$fg = 1$ を満たすならば，$n+m$ 次の係数を比べることで $n = m = 0$ であり，$a_0 b_0 = 1$ より $a_0, b_0 \in A^*$ である．$A^* \subset A[X]^*$ は明らか．

略解 8.7 $x_1, \dots, x_n \in B$ で生成されるとき，$A[X_1, \dots, X_n] \to B$ を $X_i \mapsto x_i$ で定めればよい．

略解 8.8 I_1：冪零元は 0 のみ，零因子全体の集合は $Xk[X, Y]/I_1 \cup Yk[X, Y]/I_1$．

I_2：冪零元全体の集合は kY，零因子全体の集合はイデアル (X, Y)（これは $\mathrm{Ann}(Y)$ に等しい）．

I_3：冪零元全体の集合と零因子全体の集合どちらも唯一の極大イデアル (X, Y) に等しい．

略解 8.9 (1) $\mathrm{Ker}\, f$ が I より真に大きいとすると $a + bX$ の形の元を 0 以外に含むことになるが，$1, \sqrt{-1} \in \boldsymbol{C}$ は $\boldsymbol{R}$ 上 1 次独立なのでそのようなことは起こらない．逆に $a + b\sqrt{-1} \in \boldsymbol{C}$ は $a + bX$ の像なので全射である．

(2) $\mathrm{Ker}\, f$ が I より真に大きいとすると $a + bY$（$a, b \in k[X]$）の形の元を 0 以外に含むことになるが，$f(a+bY) = a(T^2-1)+(T^3-T)b(T^2-1)$ の偶数次部分と奇数次部分を見ることで $a(T^2-1) = b(T^2-1) = 0$ となり，したがって $a = b = 0$ となり矛盾する．

f と $k[T] \to k[T]/(T^2-1)$ との合成の像は k なので全射でない．したがって f も全射でない．

(3) $\mathrm{Ker}\, f = I$ は前項と同様．非全射性は $k[T] \to k[T]/(T^2)$ を使って前項と同様．

(4) $\mathrm{Ker}\, f = I$ は前項と同様（$a_0 + a_1 Z + \cdots + a_{n-1} Z^{n-1}$，$a_i \in k[X, Y]$ の形の元を考える）．$n = 1$ ならば明らかに全射である．$n \geq 2$ ならば，$k[S, T] \to k[S, T]/(S^n, ST, T^n)$ を使って前項と同様に議論する．

(5) 略．

略解 8.10 $n = 0$ のときは明らかである．一般の n の場合を帰納法で示す．f を $f = \sum_{i=0}^{d} f_i X_n^i$（$f_i \in A[X_1, \dots, X_{n-1}]$）と書く．$(s_1, \dots, s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$ とする．$\sum_{i=0}^{d} f_i(s_1, \dots, s_{n-1}) X_n^i \in A[X_n]$ は X_n に無限集合 S_n のどの元を代入しても 0 になるので，系 8.24 より $f_i(s_1, \dots, s_{n-1}) = 0$ である．$n-1$ の場合より，$f_i = 0$ であり，したがって $f = 0$ である．

略解 9.1 Nm が ± 1 の元は単元であることに注意すると，$\mathrm{Nm}(a)$ が素数ならば a は A の既約元であり，このときヒントの内容から $\mathrm{Nm}(a) = 2$ または $\mathrm{Nm}(a) \equiv 1 \pmod 4$ である．

逆に素数 $p > 0$ が $p = 2$ または $p \equiv 1 \pmod 4$ を満たせば $p = \mathrm{Nm}(\pi) = \pi\bar{\pi}$ と書けて，このとき π と $\bar{\pi}$ は素元である．

$q > 0$ が $q \equiv 3 \pmod 4$ を満たす素数ならば既約元であることを示す．$ab = q$ ならば $\mathrm{Nm}(a)\,\mathrm{Nm}(b) = q^2$ であり，ノルムは 0 上かつ $0, 1, 2 \pmod 4$ であることから，$\mathrm{Nm}(a) = 1$ または $\mathrm{Nm}(b) = 1$ である．

$a \in A$ が素元だとする．$\mathrm{Nm}(a)$ が $p = 2$ または $p \equiv 1 \pmod 4$ を満たす素数 $p > 0$ で割れるならば，$p = \pi\bar{\pi}$ と書いて，$\pi\bar{\pi}$ が $a\bar{a}$ を割るので π または $\bar{\pi}$ が a を割りきり，よって a は π または $\bar{\pi}$ と同伴である．$\mathrm{Nm}(a)$ が $q \equiv 3 \pmod 4$ を満たす素数 $q > 0$ で割れるならば，$a = x + y\sqrt{-1}$ と書くとき x も y も q で割れるので a は q で割れる．よって a は q と同伴である．そのような p も q も存在しないならば $\mathrm{Nm}(a) = 1$ だがこの場合 a は単元となり矛盾する．

略解 9.2 $|B| = 3^2 = 9$, $|B^*| = |B| - 1 = 8$ である．したがって定理 F.6 より B^* は位数 8 の巡回群であり，4 乗して 1 になる元をちょうど 4 つもち，残りの元は生成元である．$\pm 1, \pm\sqrt{-1}$ はどれも 4 乗すると 1 になり，また（剰余環 B の元として）どの 2 つも等しくない．したがってこれら以外の元 $\pm 1 \pm \sqrt{-1}$ はすべて B^* の生成元である．

$(1 \pm \sqrt{-1})^2 = \mp\sqrt{-1}$ を直接計算で確かめてもよい．

略解 9.3 (1) で既約元であること，素元でないこと：問題 4.13(3) 周辺で述べたノルムの性質から分かる．(2) で既約元であること：同様にノルムを使って示せるが，例えば $x^2 - 15y^2 = \pm 3$ が整数解をもたないことを示す必要がある（詳細略）．素元でないことは $3 \cdot 5 = \sqrt{15}^2$ から．

(3) 以降で，既約元であること：(3) で説明する．問題 8.9 の準同型により $k[T]$ の部分環とみなす．$k[X,Y]/(Y^2 - X^3)$ での分解 $X = FG$ をとる．$k[T]$ の元として $F = aT^i$, $G = bT^j$, $i + j = 2$, $a, b \in k[T]^* = k^*$（最後の等号は命題 8.10）となる．$(i, j) = (1, 1)$ だとすると $k[X,Y]/(Y^2 - X^3)$ の像に入らないので矛盾する．$i = 0$ または $j = 0$ の場合それぞれ F または G は k^* の元なので $k[X,Y]/(Y^2 - X^3)$ の単元である．他の場合も同様．

素元であること：$k[X,Y]/(Y^2 - X^3)$ を X が生成するイデアルで割ると $k[Y]/(Y^2)$ に同型であり，この環は 0 でない零因子を含むので整域でない．言い換えると，X は $k[X,Y]/(Y^2 - X^3)$ の素元でない．他の場合も同様．

略解 10.1 体上の多変数多項式環ならいくらでも例がある．$(X) \subset k[X,Y]$ など．または $\boldsymbol{Z}$ 上の 1 変数多項式環でもよい．$(p), (X - 1) \subset \boldsymbol{Z}[X]$ など．

略解 10.2 $I \subset A$ が真のイデアルであることと $A/I \neq 0$ は同値である．

A における「$xy \in \mathfrak{p}$ ならば $x \in \mathfrak{p}$ ならば $y \in \mathfrak{p}$」は $A/\mathfrak{p}$ における「$x'y' = 0$ ならば $x' = 0$ または $y' = 0$」と同値である．

$\mathfrak{m} \subset A$ が極大イデアルだと仮定して $A/\mathfrak{m}$ が体であることを示す．$x' \in A/\mathfrak{m}$ が 0 でないと仮定して逆元の存在を示す．商写像を $\pi\colon A \to A/\mathfrak{m}$ と書く．$\pi(x) = x'$ を満たす $x \in A$ をとる．$x' \neq 0$ なので $x \notin \mathfrak{m}$ であり，したがって $\mathfrak{m} + (x)$ は $\mathfrak{m}$ より真に大きいイデアルである．$\mathfrak{m}$ は極大なので，$\mathfrak{m} + (x) = A$ である．したがって $t \in \mathfrak{m}$ と $a \in A$ を用いて $t + ax = 1_A$ と書ける．これを π で送ると $\pi(a) \cdot x' = 1_{A/\mathfrak{m}}$ を得る．

$A/\mathfrak{m}$ が体ならば，$A/\mathfrak{m}$ のイデアルは (0) と $A/\mathfrak{m}$ しかなく，A のイデアルで $\mathfrak{m}$ を含むものは（命題 5.18 より $A/\mathfrak{m}$ のイデアルと一対一対応するので）$\mathfrak{m}$ と A しかない．すなわち $\mathfrak{m}$ は極大である．

略解 10.4 I を含む A のイデアル J と対応するのは, A/I のイデアル J/I である．剰余環 A/J と $(A/I)/(J/I)$ は環として同型であり，イデアルが素イデアル（resp. 極大イデアル）か否かは剰余環が整域（resp. 体）か否かで判定できる（問題 10.2）ので，J が素イデアル（resp. 極大イデアル）であることは J/I がそうであることと同値である．

略解 10.5 $a \in \sqrt{0}$ とすると，ある $n > 0$ に対して $a^n = 0 \in \mathfrak{p}$ であり，素イデアルの定義から，$a \in \mathfrak{p}$ が分かる．

略解 10.6 対偶を示す．$I \not\subset \mathfrak{p}$ かつ $J \not\subset \mathfrak{p}$ だとすると，$x \in I \setminus \mathfrak{p}$ を満たす x と $y \in J \setminus \mathfrak{p}$ を満たす y がとれる．このとき $\mathfrak{p}$ は素イデアルゆえ $xy \notin \mathfrak{p}$ であり，また $xy \in IJ \subset I \cap J$ なので，$IJ \not\subset \mathfrak{p}$，$I \cap J \not\subset \mathfrak{p}$ である．

略解 10.7 任意の $i \neq j$ に対して $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ だと仮定してよい（もし $\mathfrak{p}_j \subset \mathfrak{p}_i$ ならこの $\mathfrak{p}_j$ を除いた $n-1$ 個に対して成り立てばもとの n 個でも成り立つので）．各 $i \neq j$ に対し，$\mathfrak{p}_j \not\subset \mathfrak{p}_i$ なので，元 $a_{ij} \in \mathfrak{p}_j \setminus \mathfrak{p}_j$ をとれる．すると $b_i := \prod_{j \neq i} a_{ij}$ は $\mathfrak{p}_i$ には属さず他の $n-1$ 個には属する．また各 i に対し，$I \not\subset \mathfrak{p}_i$ なので，元 $c_i \in I \setminus \mathfrak{p}_i$ をとれる．$x_i := b_i c_i$ とおくと，$x_i \in I$，$x_i \in \mathfrak{p}_j$ $(j \neq i)$，$x_i \notin \mathfrak{p}_i$ である．$y := \sum_{i=1}^n x_i$ とおくと，$y \in I$，$y \notin \mathfrak{p}_i$ である．

別解：$n \leq 1$ のときは明らかである．n に関する帰納法で示す．$n-1$ の場合に成立することから，各 $1 \leq i \leq n$ に対し，$\mathfrak{p}_i$ 以外の $n-1$ 個のどれにも属さない I の元 z_i をとれる．$1 \leq i \leq n$ で $z_i \notin \mathfrak{p}_i$ を満たすものが存在すれば，その z_i が条件を満たす．そうでないと仮定する．各 $1 \leq i \leq n$ に対し，x_i を $z_1, \ldots, z_n$ のうち z_i 以外の積とすると，$x_i \in I$ であり，$x_i \notin \mathfrak{p}_i$ であり，$j \neq i$ ならば $x_i \in \mathfrak{p}_j$ である．$x_1 + \cdots + x_n$ が条件を満たす．

略解 10.8 問題 10.7 を仮定する場合，$I' := I \cap \bigcap_{j=1}^m \mathfrak{q}_j$ とおくと $I' \not\subset \mathfrak{p}_i$（問題 10.6）なので，$I'$ と $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ に対して問題 10.7 を適用すればよい．

略解 10.9 $\operatorname{Spec} A = V((0))$，$\emptyset = V((1))$，$V(I) \cup V(J) = V(IJ) = V(I \cap J)$，$\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda)$.

$I \subset A$ をイデアルとし $\mathfrak{p} \in \operatorname{Spec} B$ とすると，$I \subset \phi^{-1}(\mathfrak{p})$ と $\phi(I) \subset \mathfrak{p}$ と $\phi(I)A \subset \mathfrak{p}$ は同値なので，$(\phi^{-1})^{-1}(V(I)) = V(\phi(I)A)$ である．

略解 11.1 (1) 反射律と対称律は明らか．推移律を示す．$(a_1, s_1) \approx (a_2, s_2) \approx (a_3, s_3)$ と仮定すると，$a_1 s_2 - a_2 s_1$ と $a_2 s_3 - a_3 s_2$ が 0 なので，$(a_1 s_2 - a_2 s_1)s_3 + (a_2 s_3 - a_3 s_2)s_1 = s_2(a_1 s_3 - a_3 s_1)$ も 0 であり，$s_2 \neq 0$ なので $a_1 s_3 - a_3 s_1 = 0$ すなわち $(a_1, s_1) \approx (a_3, s_3)$ が成り立つ．

(2) $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ のとき $\frac{a_1}{s_1} + \frac{a'}{s'} = \frac{a_2}{s_2} + \frac{a'}{s'}$，$\frac{a_1}{s_1} \cdot \frac{a'}{s'} = \frac{a_2}{s_2} \cdot \frac{a'}{s'}$ が成り立つことを示せば十分である．というのは，まったく同様に $\frac{a'}{s'}$ を取り換えたときの等式も示せて，2 つを組み合わせれば一般の場合がいえるからである．というわけで，$\frac{a_1}{s_1} = \frac{a_2}{s_2}$ を仮定する．すなわち $a_1 s_2 - a_2 s_1 = 0$ である．このとき，$(a_1 s' + a' s_1)(s_2 s') - (a_2 s' + a' s_2)(s_1 s') = (a_1 s_2 - a_2 s_1)s'^2$ と $(a_1 a')(s_2 s') - (a_2 a')(s_1 s') = (a_1 s_2 - a_2 s_1)a' s'$ も 0 なので，$\frac{a_1 s' + a' s_1}{s_1 s'} = \frac{a_2 s' + a' s_2}{s_2 s'}$ と $\frac{a_1 a'}{s_1 s'} = \frac{a_2 a'}{s_2 s'}$ が成り立つ．

(3) （経験上は明らかであり,）やればできる．

それ以降も明らか．

略解 11.2 $(a_1, s_1) \sim (a_2, s_2) \sim (a_3, s_3)$ と仮定する．定義より $t_1, t_2 \in S$ が存在して $(a_1 s_2 - a_2 s_1)t_1 = 0$，$(a_2 s_3 - a_3 s_2)t_2 = 0$ が成り立つ．1 つめの式の $t_2 s_3$ 倍と 2 つめの式の $t_1 s_1$ 倍を比べることで a_2 を消去すると $(a_1 s_3 - a_3 s_1)t_1 t_2 s_2 = 0$ を得る．S は積閉ゆえ $t_1 t_2 s_2 \in S$ なので $(a_1, s_1) \sim (a_3, s_3)$ が成り立つ．

略解 11.3 $\mathrm{Im}(f) = B$ の場合は当然一致する（$\boldsymbol{C}$ の場合がそう）．$\mathrm{Frac}(k[T^2-1, T^3-T])$ は $T = \frac{T^3-T}{T^2-1}$ を含み，$\mathrm{Frac}(k[T^2, T^3])$ は $T = \frac{T^3}{T^2}$ を含むので，これらの場合も一致する．

(4) で $n \geq 2$ の場合は一致しない：像には S^iT^j（$i + j \equiv 0 \pmod{n}$）の形の多項式しか現れず，像の Frac もこれらの形の多項式の商で書ける有理式しか含まない．(5) も S^iT^j（$i - j \equiv 0 \pmod{3}$）で同様のことが成り立つ．

略解 11.4 $a + b\sqrt{m} \in \boldsymbol{Z}[\sqrt{m}] \setminus \{0\}$（すなわち $(a, b) \neq (0, 0)$）のとき，$(a + b\sqrt{m})^{-1} = \frac{a-b\sqrt{m}}{a^2-b^2m} = \frac{a}{a^2-b^2m} + \frac{-b}{a^2-b^2m}\sqrt{m} \in \boldsymbol{Q}[\sqrt{m}]$ なので $\mathrm{Frac}(\boldsymbol{Z}[\sqrt{m}]) \subset \boldsymbol{Q}[\sqrt{m}]$ である．逆向きの包含関係は明らか．

略解 11.5 A 代数の準同型 $g\colon A_S \to B$ があれば，$s \in S$ に対し $f(s)g(\frac{1}{s}) = g(\frac{s}{1}\frac{1}{s}) = g(1) = 1$ なので $f(s) \in B^*$ である．逆に $f(S) \subset B^*$ ならば，$\frac{g}{A_S}B$ を $g(\frac{a}{s}) = f(a)f(s)^{-1}$ と定めると well-defined であり，こう定めるよりない．

略解 11.6 $S = \{n \in \boldsymbol{Z} \setminus \{0\} \mid \frac{1}{n} \in B\}$ とおくと $\boldsymbol{Z}_S = B$ であることを示す．問題 11.5 より $\boldsymbol{Z}_S \subset B$ である．B の元 b をとり既約分数 $\frac{m}{n}$ で表す．既約なので $\gcd\{m, n\} = 1$ であり，すなわち $mx + ny = 1$ を満たす $x, y \in \boldsymbol{Z}$ が存在する．すると $B \ni xb + y = \frac{1}{n}$ なので $n \in S$ であり $\frac{m}{n} \in \boldsymbol{Z}_S$ である．

略解 11.7 $A_f \to A[X]/(fX - 1)$ を $\frac{a}{f^n} \mapsto aX^n$ で定めると well-defined であり，$A[X]/(fX - 1) \to A_f$ を $X \mapsto \frac{1}{f}$ で定めると well-defined であり，互いに逆を与えることは簡単に確かめられる．

略解 11.8 準同型 $B/I \to A_S$ を与える．各 X_s の行先を $\frac{1}{s}$ と指定することで準同型 $B \to A_S$ が定まり（命題 8.20 の無限変数版），このとき I の生成元 $sX_s - 1$ の行先は 0 なので $B/I \to A_S$ が定まる．

写像 $A_S \to B/I$ を $\frac{a}{s} \mapsto aX_s$ で定めると well-defined になることを示す．$\frac{a}{s} = \frac{b}{t}$ ならばある $u \in S$ に対して $(at - bs)u = 0$ であり，これに $X_sX_tX_u$ をかけて $aX_s = bX_t$ を得る．すなわち上の写像は well-defined である．この写像が $B/I \to A_S$ の逆写像になっているので，同型である．

略解 11.9 問題 10.3 の同値（π が素元であることと $A/\pi A$ が整域であることは同値）を使う．$\pi \in A$ が素元なので $A/\pi A$ は整域であり，したがって $A_S/\phi(\pi)A_S = (A/\pi A)_S$ は整域の局所化なので整域または零環である．これが整域ならば $\phi(\pi) \in A_S$ は素元であり，零環ならば $\phi(\pi) \in A_S$ は単元である．

略解 11.10 $\phi\colon A \to A_S$ とおく．整域の 0 を含まない積閉集合による局所化なので A_S は整域である．

PID：$J \subset A_S$ をイデアルとする．命題 11.20(1) より，$J = \phi(\phi^{-1}(J))$ である．A が PID なので $\phi^{-1}(J) = (a)$ と書ける．このとき $J = \phi(\phi^{-1}(J)) = \phi((a)) = (\phi(a))$ なので単項である．

UFD：A_S の任意の元 $\frac{a}{s}$ が有限個の素元と有限個の単元の積で書けることをいえばよい．A が UFD なので $a \in A$ は有限個の A の素元と有限個の A の単元の積で書ける．問題 11.9 より，$\phi(a)$ も有限個の素元と有限個の単元の積である．$\frac{a}{s} = \phi(a) \cdot \frac{1}{s}$ であり，$\frac{1}{s}$ は単元なので，有限個の素元と有限個の単元の積で書けることが示された．

略解 11.11 $\frac{a/f^n}{(g/1)^m} \mapsto \frac{a}{f^ng^m}$，$\frac{a}{f^ng^m} \mapsto \frac{af^mg^n}{(fg)^{n+m}}$ などとする．

略解 11.12 $(A_S)_T \to A_{T'}$ を $\frac{a/s}{c/u} \mapsto \frac{au}{cs}$ で定める．なお $\frac{cs}{1} \cdot \frac{1}{su} = \frac{c}{u} \in T$ なので $cs \in T'$ である．

b が $\frac{b}{1} \cdot \frac{d}{v} = \frac{e}{w} \in T$ を満たす（したがって $b \in T'$ である）とき，$\frac{a}{b} \mapsto \frac{ad/v}{e/w}$ とすることで $A_{T'} \to (A_S)_T$ を定める．

この 2 つが well-defined で準同型で互いに逆であることを確かめればよい（略）．

略解 12.1 任意のイデアルが単項生成なのでとくに有限生成である．

略解 12.2 体上の無限変数多項式環(例 12.12)は UFD であることを示す．k を体とし，$B_m = k[X_0, \dots, X_m]$ とし，$B = \bigcup_{m \in \boldsymbol{N}} B_m$ とおく．まず $\pi \in k[X_0, \dots, X_m]$ が素元ならば B の元としても素元であることを確認する．問題 10.3 より，π が素元であることと (π) による商が整域であることは同値である．$k[X_0, \dots, X_m]/(\pi)$ が整域なので $B/(\pi) \cong (k[X_0, \dots, X_m]/(\pi))[X_{m+1}, \dots]$ も整域である．

任意の $f \in B \setminus \{0\}$ が単元と有限個の素元の積で書けることを示す．ある m に対して $f \in B_m$ であり B_m が UFD なので f は B_m の単元と有限個の素元の積に書けるが，それらは B の単元と素元でもある．

略解 12.3 (1) アーベル群の準同型 $\Delta\colon \boldsymbol{Q}[X] \to \boldsymbol{Q}[X]$ を $\Delta(f(X)) = f(X+1) - f(X)$ で定める．まず，$f \in \boldsymbol{Q}[X]$ に対して，$f \in A$ であることと，$f(0) \in \boldsymbol{Z}$ かつ $\Delta(f) \in A$ であることの同値性が容易に確認できる．$f_n(X) \in A$ を n に関する帰納法で示す．$f_0(X) = 1 \in A$ は明らかである．$n \geq 1$ のとき，$f_n(0) = 0 \in \boldsymbol{Z}$ は明らかに成り立ち，$\Delta(f_n) = f_{n-1}$ は帰納法の仮定から A に属する．

別解 1：$m \geq n$ のとき $f_n(m)$ が整数なのは 2 項係数の組合せ論的解釈から明らかである．一般の $m \in \boldsymbol{Z}$ に対しては，$m' := m + n!t \geq n$ なる $t \in \boldsymbol{Z}$ をとると，$n!f_n(X) \in \boldsymbol{Z}[X]$ なので $n!f_n(m) \equiv n!f_n(m') \equiv 0 \pmod{n!}$ であり，したがって $f_n(m) - f_n(m') \in \boldsymbol{Z}$ である．

別解 2：整数 k と素数 p に対し，$\mathrm{ord}_p(k) = \max\{e \in \boldsymbol{N} \mid p^e \text{ は } k \text{ を割る }\}$ と定める．ただし $\mathrm{ord}_p(0) = \infty$ とおく．任意の整数 m に対して，

$$\begin{aligned}\mathrm{ord}_p\, m(m-1)\dots(m-(n-1)) &= \sum_{e \geq 1} |\{k \in \{m, \dots, m-(n-1)\} \mid p^e \text{ は } k \text{ を割る }\}| \\ &\geq \sum_{e \geq 1} \lfloor \frac{n}{p^e} \rfloor = \mathrm{ord}_p\, n!\end{aligned}$$

である．任意の素数 p に対してこれが成り立つので，$f_n(m)$ は整数である．(なお，「$1, 2, \dots, n$ の倍数が分子の因子にそれぞれ 1 つ以上存在する」という言い方だと怪しい．$3, 4, 5, 7$ の中には $1, 2, 3, 4$ の倍数がそれぞれ 1 つ以上存在するが，$3 \cdot 4 \cdot 5 \cdot 7$ は $4!$ で割れない．)

(2) $1 \leq n < p$ のとき，$f_n(p)$ を定義するときに使った分数表記の分子は p の倍数であり分母は p の倍数でない．$n = p$ のとき，どちらも p でちょうど 1 回割れる．(そもそも明らかに $f_n(p) = 1$ である．)

(3) p を素数として，$A \to \boldsymbol{Z}\colon f \mapsto f(p)$ による $p\boldsymbol{Z}$ の逆像を $J_p \subset A$ とすると，$I_{p-1} \subset J_p$，$I_p \subsetneq J_p$ なので，$I_{p-1} \subsetneq I_p$ である．

略解 12.5 A_2 のイデアル $I = (x^i y^j \mid i + tj > 0)$ を考え，これの有限生成部分イデアル J を考える．$J \subsetneq I$ を示せばよい．J は単項式 $x^{i_n} y^{j_n}$ $(1 \leq n \leq N)$ $(N > 0)$ で生成されているとしてよい．$c := \min_{1 \leq n \leq N}(i_n + tj_n)$ とおく．$0 < i' + tj' \leq c$ なる (i', j') で，どの (i_n, j_n) とも異なるものが存在する（詳細略）．このとき $x^{i'} y^{j'}$ は I に属するが J に属さない（詳細略）．A_1 も同様にできる．

$A_3 = k + (X^2 - 1)k[X, Y] + Yk[X, Y]$ である(k 代数として)．A_3 は k 代数として $X^2 - 1, X(X^2 - 1), Y, YX$ で生成されるので，ネーターである．

$A_5 = k[x^n y \mid n \in \boldsymbol{N}]$ である．$I = (x^n y \mid n \in \boldsymbol{N})$ とおくと，I は有限生成でない（例えば I/I^2 がこれらの元を基底とする無限次元 k ベクトル空間であることから分かる)．

A_4：写像 $\mathrm{ord}_p\colon \boldsymbol{Z} \to \boldsymbol{N} \cup \{\infty\}$ を，$\mathrm{ord}_p(\frac{a}{s}) = \mathrm{ord}_p(a) - \mathrm{ord}_p(s)$ により $\mathrm{ord}_p\colon \boldsymbol{Q} \to \boldsymbol{Z} \cup \{\infty\}$ に拡張する．

$$(p-1)\,\mathrm{ord}_p(\frac{1}{n!}) + n \begin{cases} = 0 & (n = 0) \\ = 1 & (n = p^e, e \in \boldsymbol{N}) \\ \geq 2 & (\text{otherwise}) \end{cases}$$

が成り立つ．$k = 1, 2$ に対して $J_k = \{\sum_{i=0}^{m} a_i X^i \in A_4 \mid (p-1)\,\mathrm{ord}_p(a_i) + i \geq k\}$ とおき，A_4/J_2 での $\frac{X^n}{n!}$ の像を Y_n とおくと，$p > 2$ の場合，J_1/J_2 は Y_{p^e}（$e \in \boldsymbol{N}$）を基底とする無限次元 $\boldsymbol{F}_p$ ベクトル空間であり，とくに有限生成でない．$p = 2$ の場合も Y_{p^e}（$e \in \boldsymbol{N}$）と p を基底として同様．したがって A_4/J_2 はネーター環でなく，A_4 もネーター環でない．

略解 A.1 $y \in A$ に対して $f(y \cdot 1_A) = f(y) \cdot f(1_A)$ なので，$x = f(1_A)$ とすればよい．

略解 A.5 $x_0 \in M \setminus \{0\}$ とし，$I_0 := \mathrm{Ann}(x_0) \subsetneq A$ とする．I_n が素イデアルでなければ次のように $x_{n+1} \in M$ と $I_{n+1} \subset A$ をとる：$I_n \subsetneq A$ が素イデアルでないため，$s_n, t_n \in A$ で $s_n t_n \in I_n$ だが $s_n, t_n \notin I_n$ であるものが存在するので 1 組とり，$x_{n+1} := s_n x_n$ とおき $I_{n+1} := \mathrm{Ann}(x_{n+1})$ とおく．$I_n \subsetneq I_{n+1} \subsetneq A$ である（真の包含なのはそれぞれ $t_n \in I_{n+1} \setminus I_n$ と $s_n x_n \neq 0$ から）．A はネーター環なのでこの操作が無限回続くことはなく，したがってある n に対して $I_n = \mathrm{Ann}(x_n)$ が素イデアルになる．

略解 A.6 A および完全列はヒントの通りとする．$N = \boldsymbol{Z}/2\boldsymbol{Z}$ として $\mathrm{Hom}_A(N, -)$ すると，$\mathrm{Hom}_{\boldsymbol{Z}}(\boldsymbol{Z}/2\boldsymbol{Z}, \boldsymbol{Z}) = 0$，$\mathrm{Hom}_{\boldsymbol{Z}}(\boldsymbol{Z}/2\boldsymbol{Z}, \boldsymbol{Z}/2\boldsymbol{Z}) = \boldsymbol{Z}/2\boldsymbol{Z} \neq 0$ なので，$\mathrm{Hom}_A(N, M_2) \to \mathrm{Hom}_A(N, M_3)$ 右側の準同型が全射にならず，完全でない．

$N = \boldsymbol{Z}$ として $\mathrm{Hom}_A(-, N)$ すると，$\mathrm{Hom}_{\boldsymbol{Z}}(\boldsymbol{Z}, \boldsymbol{Z}) = \boldsymbol{Z}$ で，$[2]$ が誘導する準同型は $[2]\colon \boldsymbol{Z} \to \boldsymbol{Z}$ なので全射でなく，完全でない．

$N = \boldsymbol{Z}/2\boldsymbol{Z}$ として $\otimes_A N$ すると，$\boldsymbol{Z} \otimes_{\boldsymbol{Z}} \boldsymbol{Z}/2\boldsymbol{Z} = \boldsymbol{Z}/2\boldsymbol{Z}$ であり，$[2]$ が誘導する準同型は $[2] = [0]\colon \boldsymbol{Z}/2\boldsymbol{Z} \to \boldsymbol{Z}/2\boldsymbol{Z}$ なので単射でなく，完全でない．

略解 A.7 右辺の $f\colon M \to \mathrm{Hom}_A(N, P)$ に対して左辺の元を $m \otimes n \mapsto f(m)(n)$ で定める．

略解 A.8 右辺の $f\colon M \to N|_A$ に対して左辺の元を $m \otimes b \mapsto bf(m)$ で定める．

略解 A.9 ev_x が A 準同型なことは簡単．すると $O(x)$ は ev_x の像なので部分加群であり，すなわちイデアルである．

略解 B.1 $A[Y][[X]]$ は $A[[X]]$ と Y を含むので $A[[X]][Y]$ を含む．$\sum_{n \geq 0} X^n Y^n$ は $A[Y][[X]]$ には属するが $A[[X]][Y]$ には属さない．

略解 B.3 R が斜体ならば 0 以外の元が単元なので，左イデアルも右イデアルも両側イデアルも (0) と R しかない．

k を $2 \neq 0$ を満たす（可換な）体とし，V を 2 次元 k ベクトル空間とし，$R = \bigwedge V = k \oplus V \oplus \bigwedge^2 V$ を外積代数とすると，左・右・両側イデアルは次のいずれかである：R 自身；V の各部分ベクトル空間 $0 \subset W \subset V$ に対する $W \oplus \bigwedge^2 V$；(0).

k を（可換な）体，$\sigma\colon k \to k$ を非自明な自己同型として，$R = k \oplus k\varepsilon$ に乗法を $\varepsilon a = \sigma(a)\varepsilon$ $(a \in k)$，$\varepsilon^2 = 0$ で定めると，左・右・両側イデアルは $(1), (\varepsilon), (0)$ のみ．これは行列環 $\mathrm{M}(2, k)$ の部分環 $\left\{ \begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix} \mid a, b \in k \right\}$

と同型である（この元が $a+b\varepsilon$ に対応する）.

略解 C.1 $V(J_1)=\{(0,0)\}$, $I(V(J_1))=(X,Y)$ であり，$V(J_2)=\emptyset$, $I(V(J_2))=(1)=\boldsymbol{R}[X,Y]$ である．どちらの場合も $I(V(J_i))\supsetneq\sqrt{J_i}$ である.

略解 C.2 $A_i=k[X_1,\dots,X_i]$, $\mathfrak{m}_i=\mathfrak{m}\cap A_i$ とし，$k_i=A_i/\mathfrak{m}_i$ とおく．準同型の列 $k=k_0\to k_1\to\cdots\to k_n=A/\mathfrak{m}$ があり，弱零点定理（系 C.2）より $A/\mathfrak{m}$ は k の有限次拡大体なので，命題 F.7 より各 i に対し k_i も体である.

$(f_1,\dots,f_j)=\mathfrak{m}_j$ であるとき，$(f_1,\dots,f_j,f_{j+1})=\mathfrak{m}_{j+1}$ が成り立つことは，$(A_j/\mathfrak{m}_j)[X_{j+1}]$ のイデアル $\mathfrak{m}_{j+1}/\mathfrak{m}_j$ を f_{j+1} の像 $\bar{f}_{j+1}$ が生成することと同値である．$(A_j/\mathfrak{m}_j)[X_{j+1}]$ は体上の 1 変数多項式環なので PID であり，したがって $\mathfrak{m}_{j+1}/\mathfrak{m}_j$ を生成する元が存在する．その逆像を 1 つとり f_{j+1} とすると $(f_1,\dots,f_j,f_{j+1})=\mathfrak{m}_{j+1}$ が成り立つ．これを繰り返して求める $f_1,\dots,f_n$ を得る.

略解 D.1 $\mathfrak{q}\in\operatorname{Spec}A[X]$ に対し，$\mathfrak{q}\cap A$ が $\mathfrak{p}$ を含むことは $\mathfrak{q}$ が $\mathfrak{p}[X]$ を含むことと同値であり，そのような $\mathfrak{q}$ 全体は $A[X]/\mathfrak{p}[X]=(A/\mathfrak{p})[X]$ のスペクトルと一対一対応する．$\bar{A}:=A/\mathfrak{p}$ とおき，以下 $\mathfrak{q}$ を $\bar{A}[X]$ の素イデアルと同一視する．このとき $\mathfrak{q}\cap\bar{A}=(0)$ であることは，$S:=\bar{A}\setminus\{0\}$ と交わらないことと同値であり，したがって局所化 $\bar{A}[X]_S=\bar{A}_S[X]$ の素イデアルと対応する．$\bar{A}_S\cong\kappa(\mathfrak{p})$ である.

略解 D.2 (1) ヒントの続き：B の 0 以外の元は Y の非負整数乗と単数の積で書けることに注意する．$fh=g^{n+1}$ を満たす $h\in YB$ が存在するが，$YB=\mathfrak{p}_0\subset B_0$ なので B_0 においても g^{n+1} は f を割りきる．すなわち $g\in\sqrt{(f)}\subset\sqrt{\mathfrak{q}}=\mathfrak{q}$ である.

(2) $B_1/\mathfrak{p}_1\cong k[t]$.

(3) $B_0[X]\to B_1$ を $X\mapsto t$ で定めると，全射であり，$YX-tY\in B_0[X]$ は核の元なので単射でない．なお，$X-t$ は B_0 の元でないことに注意する.

略解 F.1 α,α' が a の p 乗根ならば，$(\alpha-\alpha')^p=\alpha^p-\alpha'^p=a-a=0$ であり，フロベニウス写像（p 乗写像）が単射なので $\alpha-\alpha'=0$ である.

略解 F.2 環：準同型（フロベニウス写像）の像なので部分環である．整域（resp. 体）：フロベニウス写像が単射なので，$A\to A^p$ は同型であり，したがって A^p も整域（resp. 体）である.

略解 F.3 前半：$a\in I$ のとき $a^p\in(a_1^p,\dots,a_n^p)$ であることを示せばよいが，$a=b_1a_1+\cdots+b_na_n$ の両辺を p 乗すればよい.

後半：$I=(X,Y)\subset k[X,Y]$ とすると，$X^{p-1}Y\in I^p$ だが $X^{p-1}Y\notin I^{[p]}=(X^p,Y^p)$ である.

略解 F.4 $\boldsymbol{Z}\to A$ の像は A の部分群なので，位数 $\operatorname{char}A$ は A の位数を割りきる.

A のアーベル群としての生成系 $x_1,\dots,x_N$ をとる．すなわちアーベル群の全射 $\boldsymbol{Z}^N\to A$ を得るが，$(\operatorname{char}A)\cdot x_i=0$ なので，この写像はアーベル群の全射 $(\boldsymbol{Z}/(\operatorname{char}A)\boldsymbol{Z})^N\to A$ を誘導する．位数を比較して $|A|$ が $(\operatorname{char}A)^N$ を割りきることが分かる.

略解 F.5 $(\operatorname{char}A_1)1_{A_1}=0_{A_1}$ の像をとって $(\operatorname{char}A_1)1_{A_2}=0_{A_2}$ を得る．標数の定義より，$\operatorname{char}A_2$ は $\operatorname{char}A_1$ を割りきる.

k_1 が体のとき，$(\operatorname{char}k_2)\cdot1_{k_1}$ の像は 0_{k_2} であり，とくに非単元なので，$(\operatorname{char}k_2)\cdot1_{k_1}$ も非単元であり，したがって 0_{k_1} に等しい.

略解 F.6 $Q = P^2R$ ならば $Q' = 2PP'R + P^2R'$ は P で割れる（このことは P が既約でなくても成り立つ）．

k が完全だと仮定して，既約多項式 P が Q と Q' を割るならば P^2 が Q を割ることを示そう．$Q = PR$ と書けて，これを微分して $Q' = PR' + P'R \equiv P'R \pmod{(P)}$ を得る．一旦 $P' \neq 0$ と仮定すると，微分の定義から $0 \leq \deg P' < \deg P$ なので，P' は P で割れず，P は素元なので，P が Q' を割るという仮定から P が R を割ることが分かる．$P' = 0$ だとすると，P は定数ではないので，微分の定義から，$\operatorname{char} k = p > 0$ かつ $P = \sum_{i=0}^{m} a_i X^{ip}$ と書ける．しかし k は完全なので $b_i^p = a_i$ を満たす $b_i \in k$ が存在し，$P = (\sum_{i=0}^{m} b_i X^i)^p$ となり既約性に反する．したがって $P' = 0$ となることはない．

k が完全でない場合，$a \in k \setminus k^p$ が存在する．このとき $P := X^p - a$ は既約であり，$Q = P$ とおくと，P は Q および $Q' = 0$ を割るが，P^2 は Q を割らない．

略解 G.1 M_0 は空でないので元 $x_0 \in M_0$ を 1 つとれる．$f_1^{-1}(x_0) \subset M_1$ も空でないので元 x_1 を 1 つとれる．これを繰り返して x_n をとると (x_n) は射影極限 M の元である．

略解 G.2 (2) 単射は明らか．(x_n) が右辺の元ならば $x_n \in M_n'$ なので (x_n) は左辺に属する．

(3) $\operatorname{Im}(f_{n+1,m})$ が停止するので，$M'_{n+1} = \operatorname{Im}(f_{n+1,m_0})$ を満たす m_0 をとれる．$x \in M_n'$ をとる．定義より $y \in M_{m_0}$ で $f_{n,m_0}(y) = x$ を満たすものが存在する．$z := f_{n+1,m_0}(y)$ とおくと $f_{n+1}(z) = x$ であり，$z \in \operatorname{Im}(f_{n+1,m_0}) \subset M'_{n+1}$ である．

(4) 各 n に対して，M_n' はある $m \geq n$ に対する $\operatorname{Im}(f_{n,m})$ に一致するので，空でない．(3) と問題 G.1 より $\varprojlim_n M_n'$ は空でなく，(2) より $\varprojlim_n M_n$ はこれに等しい．

(5) 有限集合の部分集合の減少列は停止するので，ミッタク・レフラー条件を満たす．

略解 G.3 位相の連続性を基本近傍系を用いて述べる方法を思い出す．

略解 G.4 $f \in k[[X]]$ を $f^2 = 1 + X$ を満たすようにとる：具体的には $f = \sum_{i \geq 0} \binom{1/2}{i} X^i$ とすればよい（問題 G.5）．ここで $i \geq 0$ に対し，t が整数でなくても $\binom{t}{i} := t(t-1)\dots(t-(i-1))/i!$ としている．

すると $Y^2 - X^2 - X^3 = (Y - Xf)(Y + Xf)$ なので，$\hat{A}$ はこれに対応する 2 つの極小素イデアルをもつ．

略解 G.5 (2) 分子の ord_p を問題 12.3 の別解 2 と同様に評価する．

(1), (3) 示すべき式 $(1+x)^\alpha (1+x)^\beta = (1+x)^{\alpha+\beta}$ の両辺を無限和（の積）で書いて，x^n の係数を比較した等式

$$\sum_{i+j=n} \binom{\alpha}{i}\binom{\beta}{j} = \binom{\alpha+\beta}{n}$$

が任意の α, β に対して成り立つことを示せばよい．2 変数多項式環 $\boldsymbol{Q}[\alpha, \beta]$ での等式だと思って示せばよい．(α, β) に $\boldsymbol{N} \times \boldsymbol{N}$ の元を代入すると等式は組合せ論的解釈（α 人いる A 組から i 人，β 人いる B 組から j 人，合計 n 人の委員を選出する）から成り立つので，問題 8.10 から一般の場合も成り立つ．

略解 H.1 例えば $n \geq 2$ を整数としたときの $A[T^n] \subsetneq A[T]$（T^n を T にうつすことで同型になる）．

略解 H.2 $\boldsymbol{Z}[\sqrt{-5}]$ で (2) や (3) や $(1 + \sqrt{-5})$ や $(1 - \sqrt{-5})$ を 2 つの素イデアルの積で書いたものは条件を満たす．

略解 H.3 斜体はそう．その他に $\boldsymbol{F}_4\langle x \rangle / (ax - xa^2 (a \in \boldsymbol{F}_4))$ なども．

略解 H.4 $\{0\}$ 以外の部分加群 $M \subset \boldsymbol{Q}$ を考える．p を素数とし，集合 $N_p := \{\operatorname{ord}_p(x) \mid x \in M \setminus \{0\}\}$

を考える．$n \in N_p$ ならば $n+1 \in N_p$ であることと，$N_p \neq \emptyset$ であることから，$N_p = \boldsymbol{Z}$ であるか，またはある（一意に定まる）整数 $n_p \in \boldsymbol{Z}$ に対して $N_p = \{n \in \boldsymbol{Z} \mid n \geq n_p\}$ であるかのいずれかである．前者の場合 $n_p := -\infty$ とおくことで，この場合も $N_p = \{n \in \boldsymbol{Z} \mid n \geq n_p\}$ が成り立つ．このとき，$M' := \{x \in \boldsymbol{Q} \mid$ すべての素数 p に対して $\mathrm{ord}_p(x) \geq n_p\}$ とおくと，$M = M'$ であることを示す．$M \subset M'$ は明らかである．$x \in M'$ として $x \in M$ を示そう．$\boldsymbol{Z}$ の部分集合 $J = \{k \in \boldsymbol{Z} \mid kx \in M\}$ を考えると，これはイデアルであり，(0) より真に大きい．$J = (1)$ であることを示す．任意の素数 p に対して，J が (p) に含まれないことを示す（これが言えれば $J = (1)$ が従う）．n_p の定義より，$\mathrm{ord}_p(x) = \mathrm{ord}_p(y)$ を満たす $y \in M$ が存在する．このとき $ax = by$ および $p \nmid a, b$ を満たす整数 $a, b \in \boldsymbol{Z}$ が存在し，$a \in J$ なので，$J \not\subset (p)$ である．

以上の構成をまとめると，写像 $\{M \subset \boldsymbol{Q} \mid M \supsetneq \{0\}\} \underset{g}{\overset{f}{\rightleftarrows}} (\boldsymbol{Z} \cup \{-\infty\})^P$ で，$g \circ f = \mathrm{id}$ であるものを構成した．ただし P で素数全体の集合を表す．あとは f の像を決定すればよい．

$S = \{(n_p)_{p \in P} \in (\boldsymbol{Z} \cup \{-\infty\})^P \mid n_p > 0$ を満たす p は高々有限個 $\}$ とおく．S が f の像であることを示す．まず $0 \subsetneq M \subset \boldsymbol{Q}$ に対して，$x \in M \setminus \{0\}$ をとると，$\mathrm{ord}_p(x) > 0$ なる p は有限個しかないので，$n_p > 0$ なる p も有限個しかない．すなわち f の像は S に含まれる．逆に任意の $(n_p) \in S$ をとり，これを実現する部分加群を構成する．すべての素数 p に対して $\mathrm{ord}_p(x) = \max\{0, n_p\}$ なる x をとる（例えば $n_p > 0$ を満たす素数 p（有限個）に関する p^{n_p} の積をとればよい）．集合 $\{p^m x \mid p \in P, m \in \boldsymbol{Z}, \mathrm{ord}_p(p^m x) \geq n_p\}$ が生成する $\boldsymbol{Q}$ の部分加群が条件を満たす．

略解 H.5 問題 11.6 より，$\boldsymbol{Z}$ の積閉集合 S を用いて $\boldsymbol{Z}_S$ と表せる．さらに，同問題の証明より，S は「S の元の約数も S に属する」を満たすようにとれる．このとき，素数からなる集合 T が存在して，S は $\{n \in \boldsymbol{Z} \setminus \{0\} \mid n$ は単元（± 1）と T に属する素数有限個の積 $\}$ と表せる．

略解 H.6 反例を挙げる．$A = k[x, y, z_n, w_n \mid n \in \boldsymbol{N}]$ とし，$K_1 \subset A$ を，不定元 2 つの積の形の元のうち xz_n（$n \in \boldsymbol{N}$）と yw_n（$n \in \boldsymbol{N}$）でもないもの全体の集合が生成するイデアルとし，$K_2 \subset A$ を $\{xz_n - yw_n \mid n \in \boldsymbol{N}\}$ が生成するイデアルとし，$B = A/(K_1 + K_2)$ とし，B のイデアルを $I = (x)$，$J = (y)$ で定めると，$I \cap J = (xz_n \mid n \in \boldsymbol{N}) = (yw_n \mid n \in \boldsymbol{N})$ は有限生成でない．

略解 H.7 $\left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \subset \mathrm{GL}(2, \boldsymbol{F}_2)$ が反例．

略解 H.8 A が 0 環でなく $B = A[T]$ のとき，$A[[x]] \otimes_A A[T] = A[[x]][T] \to A[T][[x]]$ は全射でない（問題 B.1(2)）．

$I = (a_0, a_1, \dots) \subset A$ が可算生成であり有限生成でないイデアルで $B = A/I$ のとき単射でない：$f = \sum_{n \geq 0} a_n x^n \otimes 1 \in A[[x]] \otimes_A A/I$ とおくと，f の像は 0 だが，$f = 0$ だとするとある n に対する有限生成イデアル $(a_0, a_1, \dots, a_n)$ で割った時点で消えていることになり（※），I が有限生成でないことに反する．※の証明はテンソル積の構成を追うか，右随伴関手をもつ関手が余極限を保つことを使ってください．

略解 H.9 $A_1 = \boldsymbol{Z}[\sqrt{-4}]$，$I = J = (2, \sqrt{-4})$ とすると，$|A_1/IJ| = 8 > |A_1/I| \cdot |A_1/J| = 4$ である．$k = \boldsymbol{F}_q$ を位数 q の有限体とし $A_2 = k[t^2, t^3]$，$I = J = (t^2, t^3)$ とすると，$|A_2/IJ| = q^3 > |A_2/I| \cdot |A_2/J| = q^2$ である．

一般に，$\mathfrak{m} \subset A$ が極大イデアルで，$\mathfrak{m}A_{\mathfrak{m}} \subset A_{\mathfrak{m}}$ が単項生成でないならば，$d := \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \geq 2$ であり，$|A/\mathfrak{m}| = q < \infty$ という仮定を付ければ $I = J = \mathfrak{m}$ が反例になる：$|A/IJ| = |A/\mathfrak{m}| \cdot |\mathfrak{m}/\mathfrak{m}^2| = q \cdot q^d > |A/\mathfrak{m}|^2 = q^2$ である．上の A_1, A_2 はこの形である．

一方で，逆向きの不等号が成立する場合もある：$k = \boldsymbol{F}_q$ を位数 q の有限体とし $A = k[t^4, t^5, t^6, t^7]$, $I = (t^4, t^5)$, $J = (t^4, t^6)$ とすると，$IJ = (t^8, t^9, t^{10}, t^{11})$ であり，$|A/IJ| = q^5 < |A/I| \cdot |A/J| = q^3 \cdot q^3$ である．

略解 H.10 A のイデアル（resp. 分数イデアル）は (0) と (t^n)（$n \in \boldsymbol{N}$（resp. $n \in \boldsymbol{Z}$））で尽くされ，積は（(0) に関するものは明らかなので省略して）$(t^n)(t^{n'}) = (t^{n+n'})$ で与えられる．

イデアルがこれで尽くされることの証明の方針：A および $\operatorname{Frac} A$ を $k[t]$ の局所化と見て，元を分数 $\frac{a}{s}$ の形で書いたときに $\operatorname{ord}_t(\frac{a}{s}) := \operatorname{ord}_t(a) - \operatorname{ord}_t(s)$ が well-defined であることに注意する（A の場合は $\operatorname{ord}_t(s) = 0$ である）．$I \subset A$ が (0) より真に大きいイデアルだとして，$\{\operatorname{ord}_t(f) \mid f \in I \setminus \{0\}\}$ の最小値を n とすると，$f \in I$ に対して（$f = \frac{a}{s}$ と書いたとき $t^{-n}a \in k[t] \setminus (t)$ なので），$t^{-n}f \in A$ となり，したがって $f = (t^n)$ である．

B のイデアルは

- (0),
- (1)（これは下の記号でいう $I_{0,0}$ に等しい），
- $I_{n,a} := (t^n + at^{n+1})$（$n \in \boldsymbol{Z}_{\geq 2}, a \in k$），
- $J_n := (t^n, t^{n+1})$（$n \in \boldsymbol{Z}_{\geq 2}$）

で尽くされ（これらはどの 2 つも相異なり），積は（(0) と (1) に関するものは明らかなので省略して）

$$I_{n,a}I_{n',a'} = I_{n+n',a+a'}, \quad I_{n,a}J_{n'} = J_{n+n'}, \quad J_nJ_{n'} = J_{n+n'},$$

で与えられる．B の分数イデアルについては，上の表示で n の動く範囲を $\boldsymbol{Z}$ にした形で与えられる．

イデアルがこれで尽くされることの証明の方針：$I \subsetneq B$ が (0) より真に大きいイデアルだとして，$IA = (t^n)$（$n \geq 2$）と書けて，$\operatorname{ord}_t(f) = n$ を実現する $f \in I$ をとり $f = \frac{b}{s}$，$b = b_0t^n + b_1t^{n+1} + t^{n+2}Q \in k[t^2, t^3]$, $b_0 \in k^*$, $Q \in k[t]$ と書く．b_0^{-1} をかけることで $b_0 = 1$ としてよい．このとき b は $b' := t^n + b_1t^{n+1}$ と同伴である．なぜならば，$(1+b_1t+t^2Q)b' = (1+b_1t)b$ の両辺に $1-b_1t$ をかけて $(1-b_1^2t^2+t^2Q-b_1t^3Q)b' = (1-b_1^2t^2)b$ であり，両辺の括弧内は $k[t^2, t^3] \setminus (t^2, t^3)$ の元である．

略解 H.11 解答例 0：体の拡大．

解答例 1：$B = A[X]/(X^2)$.

解答例 2：k は標数 $p > 0$ の体，$A = k[X_1, \ldots, X_n]$，$B = k[X_1^p, \ldots, X_n^p]$.

解答例 3：k は体，$A = k[X, Y]/(Y^2 - X^3)$，$B = k[T]$，$X \mapsto T^2, Y \mapsto T^3$.

解答例 4：A は素イデアルを $\mathfrak{p} \subsetneq \mathfrak{m}$ のちょうど 2 つもつ環（たとえば $\boldsymbol{Z}_{(p)}$）とし，$B = \kappa(\mathfrak{p}) \times \kappa(\mathfrak{m})$ とする．ただし一般に素イデアル $\mathfrak{p}$ に対し $\kappa(\mathfrak{p}) := A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ はその素イデアルでの剰余体である．なお，この例では $\operatorname{Spec} B \to \operatorname{Spec} A$ は全単射だが同相ではない（ザリスキ位相に関して）．

略解 H.12 $(a) = (b)$ は明らか（$a = sb \in (b)$，$b = ta \in (a)$ である）．

a を消去して $A = \boldsymbol{Z}[b, s, t]/(b(1 - st))$ と書く．$u, v \in A$ が $uv = 1$ を満たすとき $ub \neq sb$ であることを示せばよい．$u = \sum_{i=0}^m u_ib^i, v = \sum_{j=0}^n v_jb^j$, $u_i, v_j \in \boldsymbol{Z}[s, t]$ と書ける．剰余環 $A/(b) \cong \boldsymbol{Z}[s, t]$ においても $uv = 1$ なので $u_0v_0 = 1$ であり，したがって $u_0, v_0 \in \{\pm 1\}$ である．すると $ub = \sum_{i=0}^m u_ib^{i+1}$ の b^1 の係数は ± 1 であり，$\boldsymbol{Z}[s, t]/(1 - st)$ において s に一致しない．

略解 H.13 $G = \boldsymbol{Z}/n\boldsymbol{Z}$ の場合．$G^\vee$ を G から $\boldsymbol{C}^*$ への群準同型全体の集合とする：$\boldsymbol{Z}/n\boldsymbol{Z}$ の生成元 1 の行先

を $\boldsymbol{C}^*$ の 1 のどの n 乗根にうつすかで n 通りある．$G^\vee$ の各元が環準同型 $\boldsymbol{C}[G] \to \boldsymbol{C}$ を誘導する．これらの環準同型が定める写像 $\boldsymbol{C}[G] \to \prod_{G^\vee} \boldsymbol{C}$ は同型である．（表現の言葉でいうと，有限次既約表現は 1 次元のもの（n 個）しかない．）

$G = \mathfrak{S}_3$ の場合．G の元 g を $1 \in \boldsymbol{C}$（resp. $\mathrm{sgn}(g) \in \boldsymbol{C}$）にうつす環準同型を $f_1 \colon \boldsymbol{C}[G] \to \boldsymbol{C}$（resp. f_2）とおく．2 次元ベクトル空間 $V := \langle e_1, e_2, e_3\rangle / \langle e_1 + e_2 + e_3\rangle$ に自然に G が作用するので，環準同型 $f_3 \colon \boldsymbol{C}[G] \to \mathrm{M}(2, \boldsymbol{C})$ を得る．$(f_1, f_2, f_3) \colon \boldsymbol{C}[G] \to \boldsymbol{C} \times \boldsymbol{C} \times \mathrm{M}(2, \boldsymbol{C})$ は同型である．（有限次既約表現は 3 つあり次元は $1, 1, 2$ である．）

略解 H.14 答えは $\boldsymbol{Z}/4\boldsymbol{Z}$ と $\boldsymbol{F}_2[x]/(x^2)$ である．

A がこの 2 つのどちらかであるとき条件を満たすことを示す．$f \in A[x]$ をモニック多項式とする．$d = \deg(f)$ ごとに，根が高々 d 個であることを示す．$d = 0, 1$ のとき：明らか．$d \geq 4$ のとき，根の個数は高々 $|A| = 4$ である．$d = 2, 3$ で，根を $d+1$ 個以上もつと仮定する．平行移動により $0, 1$ が根だとしてよい．このとき $f(x) = x(x-1)h(x)$ と書ける．$d = 2$ のとき，$h = 1$ であり，f は他に根をもたない．$d = 3$ のとき，$h = x - b$ であり，b と極大イデアル（(2) または (t)）を法として合同でなく $0, 1$ と異なる元 $c \in A$ が存在し，c は f の根でない（$h(c)$ は単数で $c(c-1) \neq 0$ なので）．

A は零環でも整域でもない環で，モニック多項式の根の個数に関する条件を満たすと仮定し，A が上記の 2 つのどちらか（に同型）であることを示す．A は零環でも整域でもないので，零因子 $a \neq 0$ が存在する．すなわち，$I := \mathrm{Ann}(a)$ は (0) でも (1) でもない．ここで，I が 0 でも a でもない元 b を含むと，$f = (x-a)(x-b)$ が少なくとも 3 つの根 $0, a, b$ をもち条件に反する．したがって $I \subset \{0, a\}$ である．したがって $I = (a) = \{0, a\}$ である．すると任意の $c \in A$ に対し，$ca \in (a) = \{0, a\}$ なので $ca = 0$ または $ca = a$ であり，したがって $c \in \mathrm{Ann}(a) = \{0, a\}$ または $c - 1 \in \mathrm{Ann}(a) = \{0, a\}$ である．ということは $A \subset \{0, a, 1, 1+a\}$ である．右辺のどの 2 元も異なることは簡単に分かるので，$|A| = 4$ であり $A = \{0, a, 1, 1+a\}$ であり $a^2 = 0$ である．2（$:= 1 + 1$）が a か 0 かに応じて $A \cong \boldsymbol{Z}/4\boldsymbol{Z}$ または $A \cong (\boldsymbol{Z}/2\boldsymbol{Z})[t]/(t^2)$ である．

略解 H.15 $k[X, Y]/(XY - 1) = k[X]_X$ であり，$k[X]$ は UFD なので，問題 11.10 より $k[X]_X$ も UFD である．

$\boldsymbol{Q}(\sqrt{-1})[X, Y]/(X^2 + Y^2 - 1)$ は $Z = X + \sqrt{-1}Y, W = X - \sqrt{-1}Y$ を用いて $\boldsymbol{Q}(\sqrt{-1})[Z, W]/(ZW - 1)$ と書けるので，これも UFD である．

$A = \boldsymbol{Q}[X, Y]/(X^2 + Y^2 - 1)$ が UFD でないことを示す．X が既約元であり素元ではないことを示す．

A の元は $p + qY$，ただし $p, q \in \boldsymbol{Q}[X]$，と一意的に書けることに注意する．$X$ が 2 元の積 $X = (a_0 + a_1Y)(b_0 + b_1Y)$（$a_i, b_i \in \boldsymbol{Q}[X]$）と書けたとすると，$a_0b_0 + a_1b_1(1 - X^2) = X$ かつ $a_0b_1 + a_1b_0 = 0$ と書ける．後者の式と UFD $\boldsymbol{Q}[X]$ における素元分解から，$a_0 = pq, a_1 = pr, b_0 = qs, b_1 = -rs$（$p, q, r, s \in \boldsymbol{Q}[x]$）と書ける．前者の式にこれを代入して $ps(q^2 + r^2(X^2 - 1)) = X$ を得る．$q^2 + r^2(X^2 - 1)$ の次数は $\max\{2\deg q, 2 + 2\deg r\}$ に等しい：もしそうでないとすると q^2 と $r^2(X^2 - 1)$ の次数が等しくかつ最高次の係数でキャンセルが起こっていることになるが，2 つの 0 でない有理数の平方の和は決して 0 にならない．これと $\deg(q^2 + r^2(X^2 - 1)) \leq \deg X = 1$ より，$r = 0$ であり，$a_0 + a_1Y = a_0$ と $b_0 + b_1Y = b_0$ のどちらかが定数でどちらかが X の定数倍である．以上より X が既約元であることと $A^* = \boldsymbol{Q}^*$ が分かった．同様の議論より $Y \pm 1$ も既約元であり，また X はこれらの元を割らない．一方で X は $(Y - 1)(Y + 1) = -X^2$ を割るので，X は素元でない．

略解 H.16 $F = \sum_{i=0}^{n} a_i X^i \in A[X]^*$ だとする．各素イデアル $\mathfrak{p} \subset A$ に対し，$A/\mathfrak{p}$ は整域なので問題 8.6 より

$(A/\mathfrak{p})[X]^* = (A/\mathfrak{p})^*$ である．したがって，F を法 $\mathfrak{p}$ で考えることで，$i > 0$ に対して $a_i \in \mathfrak{p}$ が分かる．定理 10.10 よりすべての素イデアルの共通部分は A の冪零根基 $\sqrt{0}$ に等しいが，仮定よりそれは (0) である．したがって $i > 0$ に対して $a_i \in \bigcap_{\mathfrak{p}} \mathfrak{p} = (0)$ なので $F \in A$ であり．定数項を考えて $F \in A^*$ である．（最後の部分は，すべての素イデアル $\mathfrak{p}$ に対して $a_0 \notin \mathfrak{p}$ なので $a_0 \in A^*$ である，としてもよい．）

略解 H.17 A を $|A| = p^2$ を満たす環とする．A の標数は p または p^2 である．p^2 ならば，$\boldsymbol{Z}/p^2\boldsymbol{Z} \to A$ が同型である．以下標数は p だとする．$\boldsymbol{Z} \to A$ の像を $\boldsymbol{F}_p$ とみなす．A は $\boldsymbol{F}_p$ 加群（ベクトル空間）として 2 次元なので基底 $1, x$ をとれる．A の可換性も分かる．$x^2 \in A$ なのである 2 次モニック多項式 $Q \in \boldsymbol{F}_p[X]$ が存在して $Q(x) = 0$ であり，$\boldsymbol{F}_p[X]/(Q) \to A\colon X \mapsto x$ は同型である．

Q が相異なる 2 つの $\boldsymbol{F}_p$ 係数モニック 1 次式 Q_1, Q_2 の積に分解する場合，中国剰余定理より $A \cong \boldsymbol{F}_p[X]/(Q_1) \times \boldsymbol{F}_p[X]/(Q_2) \cong \boldsymbol{F}_p \times \boldsymbol{F}_p$ である．

Q が $\boldsymbol{F}_p$ 係数モニック 1 次式 R の 2 乗である場合，X を $X - a$ で置き換えることで $R = X$ としてよく，$A \cong \boldsymbol{F}_p[X]/(X^2)$ である．

Q が既約の場合，$A \cong \boldsymbol{F}_p[X]/(Q)$ は体であり，したがって $\boldsymbol{F}_{p^2}$ に同型である．

略解 H.18 $S \subset A_S^* \cap A$ がつねに成り立つ．また，$S \subset A^*$ ならば $A_S = A$ である．したがって，$A \subsetneq B$ かつ $B^* \cap A = A^*$ なる A, B を見つければ反例になる．

k を体とし，$A = k[X, Y] \subset B = k[X, \frac{Y}{X}]$ とおくと，問題 8.6 より $A^* = k^*$ であり，B も（A との関係を忘れれば）k 上の 2 変数多項式環 $k[X, Z]$ と k 代数として同型なので $B^* = k^*$ である．

略解 H.19 自然数全体の集合 $\boldsymbol{N}$ に通常の順序を入れ，左順序位相を入れる（開集合は各 $n \in \boldsymbol{N}$ に対する $\{x \mid x < n\}$（空集合含む）と全体集合である）．$\boldsymbol{N}$ から $\boldsymbol{R}$（ユークリッド位相）への連続関数は定数関数しかない．コンパクト台連続関数は 0 しかない．したがって $C_0(X, \boldsymbol{R})$ は零環であり乗法の単位元をもつ．

順序数に慣れた人相手なら，底集合 ω に開集合系 $\omega + 1$ を入れる，と簡潔に説明できます．

略解 H.20 $\boldsymbol{Z}$ の生成元を 1 つとり 1 と書くが，これは A の乗法の単位元とは限らないことに注意する．2 元の積を与える写像 $\times\colon A \times A \to A$ は $\boldsymbol{Z}$ 双線形写像なので，$(1, 1)$ での値 $a \in A$ を決めれば定まる．さて環 A の単位元を $n1$ とすると $n = n^2 a$ であり，$n \neq 0$ なので $a \in \{\pm 1\}$ でなければならない．$a = 1$ ならば通常の環構造である．$a = -1$ ならば，-1 のことを改めて 1 と書くことにすると通常の環構造である．

略解 H.21 (3) $B = \boldsymbol{Z} \oplus A \to \boldsymbol{Z} \times A\colon (n, a) \mapsto (n, a + n \cdot 1_A)$ が同型射を与える．

(4) B は単位的であり $\boldsymbol{Z} \times A$ は単位的でない．

(5) 環準同型 $\phi\colon A \to C$ に対し，単位的環準同型 $\boldsymbol{Z} \oplus A \to C\colon (n, a) \mapsto n \cdot 1_C + \phi(a)$ を対応させる写像が逆を与える．

略解 H.22 $B_1 \subset B_2 \subset \ldots$ が UFD の包含列で，$n \geq m$ のとき $B_n^* \cap B_m = B_m^*$ が成り立つならば，$B := \bigcup_{m \geq 1} B_m$ も「既約元は素元」を満たすことを示す．対偶を示す．$f \in B$ は素元でないとする．$f \mid gh$，$f \nmid g$，$f \nmid h$ を満たす $g, h \in B$ が存在する．$f, g, h \in B_m$ を満たす m をとると，f は B_m の素元でない．B_m は UFD なので f は B_m の既約元でなく，すなわち $f = pq$，$p, q \notin B_m^*$ という分解をもつ．仮定より $p, q \notin B^*$ である．

例 12.13 において A を体 k とすると，環 $B = \bigcup_{m \in \boldsymbol{N}} k[X^{1/p^m}]$ は条件を満たす：X はいくらでも大きい個数の非単元の積に書ける（$X = (X^{1/p^m})^{p^m}$）ので UFD でない．または $B = \bigcup_{m \in \boldsymbol{N}} k[[X^{1/p^m}]]$ でもよい（この環には既約元・素元は 1 つもない）．

略解 H.23 R_1 が整域なのは整域の部分環なのでよい．$S = R_1[Y]/(Y^p - G)$ が整域であるためには G が R_1 の元の p 乗になっていなければよいが，もしなっていたとすると $G^{1/p} = F \in L = k(X)(G)$ ということになり，F が $k(X)$ 上超越的という仮定に反する．

R_1 の元が X^n で割れることと $k[[X]]$ において X^n で割れることは同値なので，$R_1/\mathfrak{m}_1^n = k[[X]]/(X^n)$ である．S は階数 p の自由 R_1 加群で，$\mathfrak{n}$ 進位相は $\mathfrak{m}_1$ 進位相と一致するので，$\hat{S}$ は $\hat{R}_1[Y]/(Y^p - G)$ に等しい．さて $\hat{R}_1[Y]/(Y^p - G) = k[[X]][Y]/(Y^p - G)$ において $(Y - F)^p = Y^p - G = 0$ なのでこの環は被約でない．

略解 H.24 まずヒントの主張の証明は，$y' = y + p^n z$ とおくとき $y'^p - y^p = \sum_{k=1}^{p} \binom{p}{k} y^{n-k} p^{kn} z^k$ であり，$0 < k < p$ に対しては 2 項係数が p で割れて $k = p$ に対しては p^{kn} が p^{n+1} で割れることから．

ヒントの主張から列 ${y_n}^{p^n}$ が p 進コーシー列であることが分かり，p 進完備なので極限が存在する．z_n を別のリフトの族とすると，${y_n}^{p^n} \equiv {z_n}^{p^n} \pmod{p^{n+1}}$ なので 2 つのコーシー列の極限は一致する．

左辺の x，x' に対するリフトの列として y_n，y'_n をとり，右辺の xx' に対するリフトの列として $y_n y'_n$ を採用すれば，極限が等しいのは明らかである．

略解 H.25 $n \in \boldsymbol{N}$ に対し，$A^\flat$ の元 $(p^{1/p^n}, p^{1/p^{n+1}}, p^{1/p^{n+2}}, \dots)$ を t^{1/p^n} とおくと，$(t^{1/p^{n+1}})^p = t^{1/p^n}$ が成立する．C を $\boldsymbol{F}_p[T^{1/p^n} \mid n \in \boldsymbol{N}]$ の T 進完備化とし，$f_n \colon C/(T^{p^n}) \to B_n \colon T^{1/p^m} \mapsto p^{1/p^{n+m}}$ とおくと，f_n は同型であり，かつ推移写像と可換なので，これが誘導する $C = \varprojlim_n C/(T^{p^n}) \to A^\flat = \varprojlim_n B_n$ も同型である．

索引