代数学概論Ｂ演習

教師用　(計算問題の略解付き)

黒木 玄　(東北大学大学院理学研究科数学専攻)

2008 年 4 月 14 日 (月)

目 次

0 この演習のルール

この演習では今までのルールを大幅に変える. ルールの変更点の重要なポイントは太字の大きな文字で書いておいた.

私が渡した文書に誤りを見つけた場合には気軽に指摘して欲しい.

0.1 各演習時間の基本スケジュール

午後 1 時〜1 時半 黒板の前で発表した人はこのあいだに解答を黒板に書く.
この時間にレポートの内容を黒板で説明して欲しい人を指名するかもしれない.

午後 1 時半 自主レポートの提出を受け付け, それが終了したら黒板の前での発表開始.

演習終了後 個人的に数学の質問に答える. 数学の勉強の仕方に関する相談にものる.

0.2 数学をマスターするために必要な勉強法

さて, ある程度以上のレベルの数学をマスターするためには**しっかり書かれた数学の本を丸ごと読む**という勉強が必要になる. そのとき必要なことは

- 証明の理解に論理的ギャップがあってはいけない,
- 数学的な具体例にはどのようなものがあるかをよく調べる,
- 本では説明が省略されている部分を完璧に埋める,
- 本よりも詳しい説明が書かれているノートを作る,
- 最終的には自家製の教科書を完成することを目指す,
- 何よりも重要なのは「数学的本質は何か」について考え続けること

などである. 一冊の本を丸ごと読めない場合には少なくとも章単位で丸ごと読むように努力するのが良い. ノートの作成も重要である. 「教科書を読むよりも君のノートを読んだ方がわかりやすい」と他人に言ってもらえるようなノートを書くことを目指して欲しい.

高校までの数学では問題単位で解き方を習得するような勉強の仕方をしていた人が多いと思う. しかし現在勉強しているような数学を習得するためには「数学の世界がどんな様子をしているか, その本質は何か」を理解するように努力しなければいけない.

私がたくさんの演習問題を渡すのはそれらの問題をすべて解いて欲しいからではない. 演習問題を解く過程でまとまった知識の重要性に気付き, 上に書いたような勉強に進むきっかけを作りたいからである. 演習の時間に「余計なこと」を話そうと努力しているのも同様の理由からである.

以上のような考え方に基づき, この演習では自主レポートとして

私が渡した問題を順番に大量に解いて提出することは禁止

する. 私が渡した問題を大量に解き続ける時間があるなら, 上に書いたような勉強の仕方をした方が良い. 逆に, 上で説明した方法で代数学を勉強しながら,

疑問を質問にまとめてレポートとして提出することは推奨

される. 場合によっては問題を解いたレポートよりも質問のレポートの方を高く評価することもありえる. 自分が理解できていないことを論理的に説明することは自分が理解していることをまとめるよりも圧倒的に難しい. 個人的に数学科の卒業生には「自分の疑問を論理的にまとめる能力」が要求されると思う.

0.3 論理的に口頭で説明できる能力も身に付けよう

ここの数学科の卒業生が身に付けることができる能力は

- 現代の進んだ数学の知識を身に付けること
- 英語で書かれた数学の文献を読めるようになること
- 単に日本語や英語の数学文献を読めるだけではなく,
  その内容を他人に対して口頭で論理的に説明できること

の 3 つだと思う. 4 年生のときのセミナーで英語の文献を読むことになるので, 卒業までにしっかり勉強すれば英語で書かれた数学の文献も読めるようになる. この演習では「数学の知識」だけではなく,「論理的に説明できること」をも身に付けてもらいたいと考えている.

以上の考え方に基づき, この演習では単位取得の必要条件として一回以上黒板の前で発表することを義務として課すことにする.

単位が欲しければ最低でも一回以上黒板の前で発表すること!

(自主) レポートも成績の参考にするが, 単位を取得するためにはそれだけでは足りない. 最終的に救済措置を設ける可能性もあるが, 最初からそう期待しないこと.

しかし, 残念ながら演習の時間は限られているので話す練習を十分にできないだろう. 一人当たり 1〜3 回程度黒板の前に立つだけで終わってしまうと思う. しかし各自が問題の解答をノートにまとめるときに他人に説明するために使えるような書き方を心がけるようにすれば「話す準備の練習」は十分にできるように思われる. 数学の文章 (問題の解答を含む) を書くときには常に口頭での説明を要求されることを前提に書くべきである. 自分が説明するためにさえ使えないようでは書く意味がない.

問題の解答を書いたレポートや質問を書いたレポートを提出した場合には, レポートを見た後 (提出の次週以降になる) に適当に見繕って

レポートの内容を黒板の前で説明することを要求するかもしれない.

特に黒板に書かれた解答が少ない場合はそうするだろう. 主としてレポートを提出していても黒板の前で発表していない人の中から選ぶ予定である.

黒板の前での発表を強制すると嫌われる場合があるのだが, 数学について口頭での発表ができる能力は数学科の卒業生として当然要求されるべき能力だと思うので以上のような方針を採用することにした.

0.4 成績評価の方針

- 黒板の前での発表と自主レポートの内容で成績を評価する.
- 各問題の基本点は 10 点であるが, 易しい問題にはそれ未満の点数が付けられ, 難しい問題には 20 点〜∞点の点数が付けられる. 黒板の前で発表するとその基本点が 5 倍以上になり, 自主レポートで提出した場合には基本点がそのまま付けられる.
- **単位が欲しければ最低でも一回以上黒板の前で発表すること.**
- 救済措置があるかもしれないが, 最初からそう期待しないこと.
- 黒板の前で一回以上発表して最後まで論理的ギャップを埋めれば C 以上で単位を出す.
- 自力で解いた場合には他の人が黒板ですでに解いてしまったのと同じ問題の解答を黒板で発表してよい.
- 黒板の前での自主的な発表には自主レポート提出の 5 倍以上の点数を付ける.
- **自主レポートの内容を黒板の前で発表することを要求するかもしれない.**
- こちらが指名してレポートの内容を黒板の前で説明してもらった場合には「黒板の前での説明一回分」とはみなさない. しかし説明の内容が特別に良ければ例外的に「黒板の前での説明一回分」とみなされ, 5 倍以上の点数が付けられることになる.
- 内容に論理的にギャップがある場合には減点する.
- **自主レポートで問題を大量に解いて提出することは禁止.**
  1 回のレポート提出あたり 2 問以下にして欲しい.
- 一つのテーマについて同じような問題を複数解いてレポートとして提出するのではなく, 複数のテーマに関して複数のレポートを提出するように努力して欲しい.
- 代数学の本を読みながら感じた疑問を質問にまとめてレポートとして提出しても良い. そのようなレポートは高く評価し, 最低でも 30 点以上の点数を付ける. 質問の内容が高度なものであれば 100 点以上の点数を付けてしまうかもしれない. ただし疑問の内容を私が理解できない場合は黒板の前での説明をお願いするかもしれない.
- 現在習っていることよりも進んだ数学について勉強した結果を自主レポートとして提出しても構わない.
- 問題に誤りを見つけた場合には適切に訂正して解こうとすること.

黒板の前で一回以上発表しているという条件を満たしており, 40 点以上なら C, 70 点以上なら B, 100 点以上なら A, 130 点以上なら AA の成績を付ける予定である.

この文書の作成に使ったソフト

数式を含む文書は TEX(テック, テフ) を使って作成することが現在では標準的になっている. 特にマクロセットとして LATEX を使うことが多い. この文書は日本語 LATEX を使って作成されている.

TEX のシステム全体のすべてのソースコードは公開されており, インターネットでバイナリも無料で配布されている. 具体的に TEX を使うにはどうすれば良いのだろうか.

東北大学数学教室の次の場所は非常に役に立つはずである:

- http://www.math.tohoku.ac.jp/tex/index.html

他にも以下の場所は参考になる:

- http://www.ms.u-tokyo.ac.jp/~abenori/tex/
  → http://www.ms.u-tokyo.ac.jp/~abenori/tex/tex0.html
  → http://www.ms.u-tokyo.ac.jp/~abenori/mycreate/#kakuto3
  最新版の「TeX インストーラ」を使うことができれば一番簡単.
  それでダメなら次の場所にアクセスする.

- http://cise.edu.mie-u.ac.jp/~okumura/texwiki/
  → インストール Windows

TEX システム全体と ghostscript と ghostview と dviout がインストールされれば後はメモ帳などで tex ファイルを編集すればすぐにでも日本語 LATEX で文書を作ることができる. しかしメモ帳は使い難い. より優れたエディタをインストールして利用した方が便利である. Linux などの UNIX 系 OS 環境で使える emacs 系エディタに慣れている人 (もしくは慣れたい人) におすすめなのは次の二つである.

- xyzzy と KaTeX を使いたい人は次の場所を見る
  → http://www12.plala.or.jp/ksp/tex/katex/

- Meadow を使いたい人はまず次の場所にアクセスする
  → http://www.meadowy.org/meadow/
  → ダウンロード
  → リリース版の Netinstall packages をダウンロードして実行する
  → 各種設定を行なう.

最近の私は前者の xyzzy と KaTeX を愛用している.

1 復習

この節では環の基礎概念や有限 Abel 群の基本定理の復習を行なう.

1.1 環の定義

定義 1.1 (環, 可換環) 集合 R とその元 $0, 1 \in R$ と演算 $-: R \to R$, $+, \cdot : R \times R \to R$ の組 $(R, \cdot, 1, +, 0, -)$ が**環 (ring)** であるとは以下が成立していることである:

1. $(R, \cdot, 1)$ はモノイド (単位元付き半群) である. すなわち任意の $a, b, c \in R$ について
   (a) $(ab)c = a(bc)$,
   (b) $1a = a1 = a$.
2. $(R, +, 0, -)$ は可換群である. すなわち任意の $a, b, c \in R$ について
   (a) $(a + b) + c = a + (b + c)$,

(b) $a + 0 = 0 + a = a$,

(c) $a + (-a) = (-a) + a = 0$,

(d) $a + b = b + a$.

3. 加法と乗法のあいだに分配法則が成立している. すなわち $a, b, c \in R$ について

(a) $a(b + c) = ab + ac$,

(b) $(a + b)c = ac + bc$.

環 R がさらに次を満たしているとき R は**可換環 (commutative ring)** であるという:

- 乗法は可換である. すなわち $a, b \in R$ に対して $ab = ba$. □

定義 1.2 (自明な環) 零元 0 だけで構成された集合は $1 = 0$ とみなすことによって自然に環をなす. その環を 0 と書き, **自明な環 (trivial ring)** もしくは**零環 (zero ring)** と呼ぶ. 記号 0 が自明な環と零元の二通りの意味で使われることに注意せよ. □

環 R で $1 = 0$ が成立しているならば任意の $a \in R$ に対して $a = 1a = 0a = 0$ より R は自明な環である. したがって環 R が自明であるための必要十分条件は $1 = 0$ が成立することである.

定義 1.3 (斜体, 体) 可換とは限らない自明でない環 R がさらに次を満たしているとき R は**斜体 (skew field)** であるという:

- 任意の 0 でない R の元 a が R の中に乗法に関する逆元 a^{-1} を持つ.

可換な斜体を単に**体 (field)** と呼んだり, 可換性を強調するために**可換体 (commutative field)** と呼んだりする. □

定義 1.4 (環準同型) R, R' は環であるとする. このとき写像 $f : R \to R'$ が**環準同型 (ring homomorphism)** であるとは任意の $a, b \in R$ に対して

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad f(1) = 1$$

が成立していることである. 環準同型は

$$f(0) = 0, \quad f(-a) = -f(a).$$

も満たしている. 環準同型は逆写像を持てばその逆写像も環準同型になる. 2 つの環のあいだに全単射環準同型が存在するとき, それら 2 つの環は環として互いに**同型 (isomorphic)** であるという. □

定義 1.5 (単数, 単元) 環 R の元 a が R の**単数 (単元, unit)** であるとは R の中に乗法に関する逆元 a^{-1} を持つことである. 環 R の単数全体の集合を $U(R)$ もしくは $R^\times$ と書く. $U(R) = R^\times$ は乗法に関して群をなすので, それを R の**単数群 (単元群, unit group)** と呼ぶ. □

環 R が斜体であるための必要十分条件は $U(R) = R \setminus \{0\}$ が成立することである.

定義 1.6 (零因子, 整域) 環 R の元 a が**左零因子 (left zero-divisor)** であるとはある $b \in R$ で $b \neq 0$ かつ $ab = 0$ を満たすものが存在することである. **右零因子 (right zero-divisor)** も同様に定義される. 可換環では左零因子と右零因子の区別を付ける必要はないので単に零因子と呼ぶ. 0 以外の左右零因子を持たない自明でない環を**整域 (domain, integral domain)** と呼ぶ. すなわち 2 つの 0 でない元の積が決して 0 にならないような自明でない環を整域と呼ぶ. □

非可換な場合も含むことを断らない場合は可換な整域のみを考えることにする.

可換環だけを主に扱う場合には可換環, 可換整域, 可換体を単に環, 整域, 体と呼ぶことが多い. 可換環の理論は非可換な場合も含む環の一般論とは違う動機 (特に代数幾何 (algebraic geometry) の基礎付け) に基づいて展開されているので, 非可換環の理論は可換環の理論の一般化だとは考えない方が良い.

例 1.7 $\mathbb{Z}$ は可換環であり, 整域でかつ $U(\mathbb{Z}) = \mathbb{Z}^\times = \{\pm 1\}$ である. □

例 1.8 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は (可換) 体である. □

例 1.9 (行列環) n は 2 以上の自然数であるとする. 実 n 次正方行列全体の集合 $M_n(\mathbb{R})$ は自然に非可換環をなす. $M_n(\mathbb{R})$ の単数群 $U(M_n(\mathbb{R})) = M_n(\mathbb{R})^\times$ は**実一般線形群 (real general linear group)** と呼ばれ, $GL_n(\mathbb{R})$ と書かれる:

$$U(M_n(\mathbb{R})) = M_n(\mathbb{R})^\times = GL_n(\mathbb{R}) = \{\, A \in M_n(\mathbb{R}) \mid A \text{ は逆行列を持つ} \,\}.$$

$M_n(\mathbb{R})$ は整域ではない. 実際 (i, j) 成分だけが 1 で他の成分が 0 であるような行列を E_{ij} と書くと $j \neq k$ のとき $E_{ij}E_{kl} = 0$. □

例 1.10 写像 $f : \mathbb{R} \to M_2(\mathbb{R})$ を $f(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ $(a \in \mathbb{R})$ と定める. このとき f は加法群の準同型でかつ $f(ab) = f(a)f(b)$ を満たしているが, $f(1)$ は単位行列に等しくない. 上の環準同型の定義はこのような写像を排除していることに注意せよ. □

例 1.11 n は 2 以上の自然数であるとする. R は n 次の実対角行列全体集合であるとする. このとき R は可換環であるが整域ではない. □

斜体の最も有名な例は次の問題の Hamilton の四元数体だと思う. Hamilton の四元数体は複素数体をさらに拡張したものである. Hamilton は最初複素数に虚数単位 i とは別の「数」をひとつだけ付け加えることによって「良い環」を構成しようとしたらしい. しかしある日 Hamilton はひとつだけではなく j と k のふたつを付け加えると「非常に良い環」ができることに気付いた。それが Hamilton の四元数体である.

[1] (Hamilton の四元数体) Hamiton の四元数体 $\mathbb{H}$ を定義しよう. 複素数体 $\mathbb{C}$ を拡張して $\mathbb{H}$ を $\mathbb{R}$ 上のベクトル空間として次のように定める:

$$\mathbb{H} = \{\, a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \,\}.$$

1, i, j, k は $\mathbb{H}$ の $\mathbb{R}$ 上の基底になっているとする. $a1$ を以下では単に a と書くことにする. さらに複素数体の虚数単位の計算規則を拡張し, 次のように i, j, k のあいだの積を定める:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

以下を示せ:

1. $\mathbb{H}$ には自然に環構造が入る.

2. 任意の 0 でない $\mathbb{H}$ の元は乗法に関する逆元を持つ.

よって $\mathbb{H}$ は斜体をなす. $\mathbb{H}$ を **Hamilton の四元数体 (Hamiltonian quaternion field)** と呼び, $\mathbb{H}$ の元を**四元数 (quaternion)** と呼ぶ. さらに次を示せ:

3. $p, q, r \in \mathbb{R}$, $p^2 + q^2 + r^2 = 1$ に対して $I = pi + qj + rk$ と置く. このとき $I^2 = -1$ である. よって $\mathbb{C}_I = \{ a + bI \mid a, b \in \mathbb{R} \} \subset \mathbb{H}$ は複素数体と同型な体をなす.

このように Hamilton の四元数体の中には連続的に無限個の複素数体 $\mathbb{C}_I$ が含まれているとみなせる. □

ヒント. 1. 問題は結合律の証明. 直接証明することは少し面倒だが易しい. このヒントでは四元数を行列で表現することによる証明法を紹介しよう. 線形写像 $A : \mathbb{H} \to M_4(\mathbb{R})$ を $\alpha = a + bi + cj + dk \in \mathbb{H}$ に対して

$$A(\alpha) = \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}.$$

と定める. たとえば $A(1)$ は単位行列になり,

$$A(i) = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad A(j) = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad A(k) = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

このとき $\alpha, \beta \in \mathbb{H}$ に対して $A(\alpha\beta) = A(\alpha)A(\beta)$ が成立する. ($\alpha, \beta = i, j, k$ のすべての組み合わせについて確認せよ.) このことと行列の積が結合律を満たすことと $A : \mathbb{H} \to M_4(\mathbb{R})$ が単射であることより, $\mathbb{H}$ の乗法も結合律を満たしていることがわかる.

2 と 3 は次の公式を使えば簡単である. $\alpha = a + bi + cj + dk \in \mathbb{H}$ に対して

$$\overline{\alpha} = a - bi - cj - dk, \quad |\alpha| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

と置くと $\alpha\overline{\alpha} = \overline{\alpha}\alpha = |\alpha|^2$. □

例 1.12 $R = \{ a + bi + cj + dk \in \mathbb{H} \mid a, b, c, d \in \mathbb{Z} \}$ は自然に $\mathbb{H}$ の部分環をなす. R は非可換な整域である. □

[2] 有限整域は体である. □

ヒント. R が整域ならば任意の $a \in R$ に対して写像 $f : R \to R$, $b \mapsto ab$ は単射である. 有限集合からそれ自身への単射は全単射になる. □

定義 1.13 (環の直積) $R_1, \ldots, R_n$ が環であるとき直積集合 $R_1 \times \cdots \times R_n$ に次によって自然に環の構造を入れることができる: $a_i, b_i \in R_i$ のとき

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

$R_1 \times \cdots \times R_n$ の零元と単位元はそれぞれ $(0, \ldots, 0)$, $(1, \ldots, 1)$ になる. これを環 $R_1, \ldots, R_n$ の**直積 (direct product)** と呼ぶ. □

[3] 環 R, R' に対して $U(R \times R') = U(R) \times U(R')$. □

1.2 多項式環の定義

R は環であるとする. (さしあたって可換であると仮定する必要はない.)

定義 1.14 (多項式環) 不定元 (indeterminate) もしくは **変数 (variable)** と呼ばれる文字 x から生成される R **係数の多項式環 (polynomial ring with coefficient in R)** を $R[x]$ と書くことにする. $R[x]$ の元は

$$f(x) = \sum_{i=0}^{m} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m, \quad a_i \in R$$

の形で一意に表わせ, 乗法は次のように定義される:

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k,\ 0\leqq i\leqq m,\ 0\leqq j\leqq n} a_i b_j\right) x^k, \quad a_i, b_j \in R.$$

たとえば, $a \in R$ に対して

$$x^i a = a x^i, \quad x^i x^j = x^{i+j}.$$

実際にはこの 2 つの計算規則さえ知っていれば多項式の積を計算できる. $R[x]$ のことを**一変数多項式環**と呼ぶこともある. 多変数の多項式環 $R[x_1, x_2, \ldots, x_n]$ は

$$R[x_1, x_2, \ldots, x_n] = R[x_1][x_2]\cdots[x_n]$$

と定義することもできるし, 直接に乗法を定義することによっても定義できる. □

参考 1.15 (環の典型的な例) 抽象的な環論を理解するためには前もって環の典型的な例が何であるかについて知識を仕入れておいた方が良い.

可換環の典型的な例はすでに知られている可換環 R を係数とする n 変数多項式環 $R[x_1, \ldots, x_n]$ およびその剰余環, 局所化, 完備化である. (剰余環と局所化については講義の方ですぐに説明されるはずである.) 可換環 R 上有限生成な可換環は R 係数の n 変数多項式環の剰余環に同型になっているので, n 変数多項式環の剰余環はそう特殊な環ではない.

それでは非可換環の典型的な例にはどのようなものがあるのだろうか? まず行列環や四元数環は非可換環の典型的な例である. 他にも**群環 (group algebra)** $k[G]$ や **Lie 代数の普遍展開環 (universal enveloping algebra of a Lie algebra)** $U(\mathfrak{g})$ や **Weyl 代数** (多項式係数の微分作用素環) $\mathbb{C}[x_1, \ldots, x_n, \partial/\partial x_1, \ldots, \partial/\partial x_n]$ も非可換環の典型的な例である. $U(\mathfrak{g})$ や $\mathbb{C}[x_1, \ldots, x_n, \partial/\partial x_1, \ldots, \partial/\partial x_n]$ は非可換な整域の典型例にもなっている. 20 年くらい前からは**量子群 (quantum group)** およびそこから派生する非可換環も重要な例になっている. (これらの非可換環の典型例に関しては谷崎 [2], [3] を参照せよ.) □

定義 1.16 (多項式の次数) $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in R[x]$, $a_m \neq 0$ のとき $f(x)$ の **次数 (degree)** を $\deg f(x) = m$ と定める. $f(x) = 0$ の場合は $\deg f(x) = -\infty$ と定める. □

[4] (整域係数の多項式環も整域 1) 以下を示せ:

1. 任意の $f, g \in R[x]$ に対して

   - $\deg(f+g) \leqq \max(\deg f, \deg g)$,
   - $\deg(fg) \leqq \deg f + \deg g$,
   - $\deg f = -\infty \iff f = 0$.

   さらに R が整域ならば二つ目の不等式で等号が成立する:

   - R が整域 $\implies \deg(fg) = \deg f + \deg g$.

2. 上の結果を用いて R が整域ならば $R[x]$ も整域であることを示せ. □

参考 1.17 (“絶対値” との関係 1) 以下 R は整域であるとする.

実数の絶対値はその実数が「どれだけ 0 から離れているか」を測っているとみなせる. 同じように整域 R を係数とする多項式 $f \in R[x]$ の次数 $\deg f$ は f が「どれだけ 0 から離れているか」を測っているとみなせる. (多項式の次数は $x \to \infty$ で $f(x)$ がどれだけ速く発散するかを測っている.)

この類似は次の定義によってより明瞭になる. $f \in R[x]$ に対して $|f|_\infty = e^{\deg f}$ と置く. ただし自然に $e^{-\infty} = 0$ であると約束しておく. これで写像 $|\cdot|_\infty : R[x] \to \mathbb{R}_{\geqq 0}$ が定まる. このとき R が整域であることより, 任意の $f, g \in R[x]$ に対して

- $|f+g|_\infty \leqq \max(|f|_\infty, |g|_\infty)$,
- $|fg|_\infty = |f|_\infty |g|_\infty$,
- $|f|_\infty = 0 \iff f = 0$

が成立していることがわかる (上の問題の 1 の結果を使う). 最初の不等式から三角不等式 $|f+g|_\infty \leqq |f|_\infty + |g|_\infty$ が導かれることに注意せよ.

このような $|\cdot|_\infty$ は**乗法付値 (multiplicative valuation)** と呼ばれており, 絶対値の概念の直接的一般化になっている.

この $|\cdot|_\infty$ の値域は $\{0, 1, e, e^2, e^3, \ldots\}$ であり, $\mathbb{R}_{\geqq 0}$ の離散部分集合である. このことより $|\cdot|_\infty$ が自然に定める $R[x]$ の位相は離散位相になることがわかる. □

定義 1.18 (零点の位数) $f(x) = a_m x^m + a_{m+1}x^{m+1} + a_{m+2}x^{m+2} + \cdots$ (有限和), $a_m \neq 0$ のとき $f(x)$ の原点における零点の**位数 (order)** を $\operatorname{ord}_0 f(x) = m$ と定める. すなわち $f(x)$ を割り切る x^m の最大の次数を $\operatorname{ord}_0 f(x)$ と定める. $f(x) = 0$ の場合は $\deg f(x) = \infty$ と定める. □

[5] (整域係数の多項式環も整域 2) 以下を示せ:

1. 任意の $f, g \in R[x]$ に対して

   - $\operatorname{ord}_0(f+g) \geqq \min(\operatorname{ord}_0 f, \operatorname{ord}_0 g)$,
   - $\operatorname{ord}_0(fg) \geqq \operatorname{ord}_0 f + \operatorname{ord}_0 g$,
   - $\operatorname{ord}_0 f = \infty \iff f = 0$.

   さらに R が整域ならば二つ目の不等式で等号が成立する:

- R が整域 $\Longrightarrow \operatorname{ord}_0(fg) = \operatorname{ord}_0 f + \operatorname{ord}_0 g$.

2. 上の結果を用いて R が整域ならば $R[x]$ も整域であることを示せ. □

参考 1.19 (“絶対値” との関係 1) 以下 R は整域であるとする.

$f \in R[x]$ に対して $|f|_0 = e^{-\operatorname{ord}_0 f}$ と置く. ただし自然に $e^{-\infty} = 0$ であると約束しておく. これで写像 $|\cdot|_0 : R[x] \to \mathbb{R}_{\geqq 0}$ が定まる. このとき R が整域であることより, 任意の $f, g \in R[x]$ に対して

- $|f+g|_0 \leqq \max(|f|_0, |g|_0)$,
- $|fg|_0 = |f|_0|g|_0$,
- $|f|_0 = 0 \iff f = 0$

が成立していることがわかる (上の問題の 1 の結果を使う). 最初の不等式から三角不等式 $|f+g|_0 \leqq |f|_0 + |g|_0$ が導かれる.

この $|\cdot|_0$ の値域は $\{0\} \cup \{\ldots, e^{-2}, e^{-1}, 1\}$ である. このことより $|\cdot|_0$ が自然に定める $R[x]$ の位相について $R[x]$ は完備ではない. $|\cdot|_0$ に関する $R[x]$ の完備化は形式べき級数環 $R[[x]]$ になる. □

要約 1.20 多項式の次数や零点の位数によってその多項式が「どれだけ 0 から離れているか」を測ることができる. 次数と零点の位数による「距離」の測り方は異なる. □

以上で説明した概念や結果はどれも易しい. しかしそれらの「数学世界における調和」を認識せずに先に進んでしまいがちである. 「どれだけ 0 から離れているか」を様々な方法で測ることができるということを初めてしったときに, 私は感動したおぼえがある. 数学の世界には他にも感動しなければいけないことはたくさんあるように思われる.

1.3 有限 Abel 群の基本定理

永尾汎著の教科書 [4] では Abel 群を乗法群として扱っているが, この演習では加法群として扱うことにする. その理由は環論との記号の整合性を得るためである.

$\mathbb{Z}/m\mathbb{Z}$ は集合として $\{0, 1, \ldots, m-1\}$ と同一視でき, $a, b = 0, 1, \ldots, m-1$ に対して群の演算の結果としての $a + b \in \mathbb{Z}/m\mathbb{Z}$ は 整数としての a と b の和を m で割った余りとして定義される. $\mathbb{Z}/m\mathbb{Z}$ は 1 から生成される位数 m の巡回群になる.

定理 1.21 (有限 Abel 群の基本定理 1) 任意の有限 Abel 群 M に対して, 2 以上のある整数たち $d_1, d_2, \cdots, d_s$ で群の同型

$$M \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_s\mathbb{Z}), \quad d_1 \mid d_2 \mid \cdots \mid d_s$$

を満たしているものが一意に存在する. □

定理 1.22 (有限 Abel 群の基本定理 2) 任意の有限 Abel 群 M に対して, 素数の正の整数べき $p_1^{f_1}, p_2^{f_2}, \ldots, p_N^{f_N}$ で群の同型

$$M \cong (\mathbb{Z}/p_1^{f_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{f_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_N^{f_N}\mathbb{Z})$$

を満たしているものがそれらを並べる順序の違いを除いて一意に存在する. □

[**6**] 位数 720 の有限 Abel 群 (の同型類) をすべて列挙せよ. □

ヒント. $720 = 2^4 \cdot 3^2 \cdot 5^1$ であり, 指数の 4, 2, 1 の分割の仕方は次のように分類される:

$$4 \to 1+1+1+1 = 1+1+2 = 2+2 = 1+3 = 4, \quad 2 \to 1+1 = 2, \quad 1 \to 1.$$

よって位数 720 の有限 Abel 群の同型類の個数は $5 \times 2 \times 1 = 10$ である. □

以上の見かけ上異なるふたつの有限 Abel 群の基本定理の同値性は本質的に次の**中国式剰余定理 (Chinese Remainder Theorem)** の特殊な場合から導かれる.

補題 1.23 (中国式剰余定理の特殊な場合) $p_1, \ldots, p_n$ が互いに異なる素数であり, $f_1, \ldots, f_n$ が正の整数であるとき, $m = p_1^{f_1} \cdots p_n^{f_n}$ と置くと次の群同型が成立している:

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/p_1^{f_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{f_n}\mathbb{Z}). \quad \square$$

この補題は非常によく使われる. 同型写像は $a \bmod m$ に $(a \bmod p_1^{f_1}, \ldots, a \bmod p_n^{f_n})$ を対応させることによって得られる. この結果は後で環論の枠組みの中で一般化される.

補題 1.23 の証明. 群の準同型 $\phi : \mathbb{Z} \to (\mathbb{Z}/p_1^{f_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{f_n}\mathbb{Z})$ を次のように定める:

$$\phi(a) = (a \bmod p_1^{f_1}, \ldots, a \bmod p_n^{f_n}) \qquad (a \in \mathbb{Z}).$$

$\phi(a) = 0$ という条件は a が $p_1^{f_1}, \ldots, p_n^{f_n}$ のすべてで割り切れることと同値であり, その条件は a が m で割り切れることと同値である. よって $\operatorname{Ker}\phi = m\mathbb{Z}$ である.

$m_i = m/p_i^{f_i}$ $(i = 1, \ldots, n)$ と置くとそれらの最大公約数は 1 なのである整数 $k_1, \ldots, k_n$ で $k_1m_1 + \cdots + k_nm_n = 1$ を満たすものが存在する. このとき $k_im_i \equiv \delta_{ij} \bmod p_j^{f_j}$ である. 整数 $a_1, \ldots, a_n$ に対して $a = k_1m_1a_1 + \cdots + k_nm_na_n$ と置くと $a \equiv a_i \bmod p_i^{f_i}$ となる. よって ϕ は全射である.

したがって準同型定理より補題の同型が得られる. □

[**7**] 補題 1.23 を認めて, 上のふたつの有限 Abel 群の基本定理が互いに同値であることを証明せよ. □

ヒント. まず次の例について考えてから一般的な場合について考えてみよ:

$$(d_1, d_2, d_3, d_4) = (2, 2^2, 2^2 \cdot 3, 2^2 \cdot 3^2 \cdot 5) \leftrightarrow \begin{bmatrix} p_1^{f_1} & p_2^{f_2} & p_3^{f_3} & p_4^{f_4} \\ & & p_5^{f_5} & p_6^{f_6} \\ & & & p_7^{f_7} \end{bmatrix} = \begin{bmatrix} 2 & 2^2 & 2^2 & 2^2 \\ & & 3 & 3^2 \\ & & & 5 \end{bmatrix}.$$

有限 Abel 群の基本定理 1 における e_i たちの存在から有限 Abel 群の基本定理 2 における $p_j^{f_j}$ たちの存在を出すためには各 e_i を素因数分解し, 補題 1.23 を使えばよい. 逆に有限 Abel 群の基本定理 2 における $p_j^{f_j}$ たちの存在から有限 Abel 群の基本定理 1 における e_i たちの存在を出すためにはその逆の操作が可能であることを示せばよい (この部分が本質的). 一意性の同値性に関しても同様の議論で証明可能である.

可能ならば, 上で例示した対応の左辺と右辺の集合を適切に定義し, それらのあいだの自然な一対一対応を構成することによって, 二つの基本定理の同値性を証明せよ. □

次の問題の結果は基本的であり, よく使われる.

[8] 体 K の乗法群 $K^\times$ の有限部分群は巡回群である. □

ヒント. まず一般に次が成立することを示せ:

1. 任意の正の整数 n に対して体 K における方程式 $x^n = 1$ の解の個数は n 以下である.
2. 有限 Abel 群 G が任意の正の整数 n に対して $\sharp\{\, x \in G \mid x^n = 1 \,\} \leqq n$ を満たしているならば G は巡回群である. (ここで $\sharp$ は集合の元の個数を意味している.)

2 の証明は有限 Abel 群の基本定理を使えば易しい. 実際 G が有限 Abel 群であれば有限 Abel 群の基本定理より, 2 以上の整数 $m_1, \ldots, m_s$ で

$$G \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_s\mathbb{Z}), \quad m_1|m_2|\cdots|m_s$$

をみたすものが一意に存在する. 特に $s = 1$ であることと G が巡回群であることは同値である. $m_1|m_2|\cdots|m_s$ より $\{\, x \in G \mid x^{m_s} = 1 \,\} = G$ となる. (群の演算を乗法で書いたり, 加法で書いたりしていることに注意せよ.)

上の二つの結果を $K^\times$ の有限部分群 G に適用すれば G が巡回群であることがただちにわかる. □

Abel 群 M が有限個の元 $v_1, \ldots, v_n \in M$ から生成されるとは M の任意の元が $a_1v_1 + \cdots + a_nv_n$ $(a_i \in \mathbb{Z})$ と表わせることである (表現の一意性は必要ない). 有限 Abel 群の基本定理は有限生成 Abel 群に対して次のように一般化される.

定理 1.24 (有限生成 Abel 群の基本定理 1) 任意の有限生成 Abel 群 M に対して, 0 以上の整数 r と 2 以上のある整数たち $d_1, d_2, \ldots, d_s$ で群の同型

$$M \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_s\mathbb{Z}) \times \mathbb{Z}^r, \quad d_1 \mid d_2 \mid \cdots \mid d_s$$

を満たしているものが一意に存在する. □

定理 1.25 (有限生成 Abel 群の基本定理 2) 任意の有限 Abel 群 M に対して, 0 以上の整数 r と 素数の正の整数べき $p_1^{f_1}, p_2^{f_2}, \ldots, p_N^{f_N}$ で群の同型

$$M \cong (\mathbb{Z}/p_1^{f_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{f_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_N^{f_N}\mathbb{Z}) \times \mathbb{Z}^r$$

を満たしているものが $p_j^{f_j}$ たちを並べる順序の違いを除いて一意に存在する. □

これらの同値性も有限 Abel 群の場合と同様に証明される.

有限生成 Abel 群の基本定理には複数の証明法があり, 環論を積極的に用いた綺麗な証明法がある. 有限生成 Abel 群の基本定理は単項イデアル整域 (PID) 上の有限生成加群の構造論 (単因子論) の特殊な場合になっている. PID 上の有限生成加群の構造論は有限生成 Abel 群の基本定理だけではなく, 行列の Jordan 標準形の理論も含んでいる. PID 上の有限生成加群の理論は環と加群の理論の中では初等的な部分に属するにもかかわらず, かなり強力である. 環と加群の理論がどれだけ強力な理論であるかを納得したければまず最初に PID 上の有限生成加群の理論の理解を目標にするのが良いと思う. (堀田 [6] はおすすめできる副読本である.)

2 環と加群の理論

2.1 イデアル

[9] $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$ の単数全体の集合とイデアル全体の集合を求めよ. □

環論のひとつの考え方はイデアルたちの性質によって環の様々な性質を特徴付けることである.

[10] (斜体のイデアルを用いた特徴付け) (可換とは限らない) 環 R が斜体であるための必要十分条件は R が自明でない左イデアルを持たないことである. □

ヒント. R が環であるとき, R が斜体であることと R の 0 でない左イデアルが常に R に等しいことが同値であることを示せばよい. 前者から後者が導かれることの証明は易しい. 問題は後者から後者を導くことである. そのとき以下の事実を証明して利用せよ.

- R の左イデアル I について $I = R$ と $1 \in I$ は同値である.
- $0 \neq a \in R$ のとき $Ra = \{ ra \mid r \in R \}$ は R の 0 でない左イデアルである.
- $a, a', a'' \in R$ のとき $a'a = 1$ かつ $a''a' = 1$ ならば $a'' = a$ となるので a' は a の逆元である. □

解. R が斜体であることと R の 0 でない左イデアルが常に R に等しいことが同値であることを示せばよい.

R は斜体であり, I は R の 0 でない左イデアルであるとする. $I \neq 0$ なので I は 0 でない元 a を含む. R は斜体なので a の逆元 $a^{-1} \in R$ が存在する. I は左イデアルなので $1 = a^{-1}a \in I$ である. よって $I = R$.

R の 0 でない左イデアルは常に R に等しいと仮定し, 0 でない R の元 a を任意に取る. R の左イデアル Ra は 0 でないので R に等しい. よって $1 \in Ra$ である. すなわちある $a' \in R$ が存在して $a'a = 1$ となる. $a' \neq 0$ なので同様にしてある $a'' \in R$ が存在して $a''a' = 1$ となる. 乗法の結合律より $a'' = a''1 = a''(a'a) = (a''a')a = 1a = a$ である. よって $aa' = a''a' = 1$ となり, a' は a の逆元であることがわかる. したがって R は斜体である. □

[11] R は (可換とは限らない) 環であり, I, J はその両側イデアルであるとし, $I + J = \{ a + b \mid a \in I,\ b \in J \}$ と置く. $I + J$ と $I \cap J$ も R の両側イデアルである. □

一般の可換環のイデアルは「数」の類似物だとみなせる. 実際次のように $\mathbb{Z}$ のイデアルは非負の整数と一対一に対応している.

[12] ($\mathbb{Z}$ のイデアル) 有理整数環 $\mathbb{Z}$ について以下を示せ.

1. $\mathbb{Z}$ は PID である.
2. $\mathbb{Z}$ のイデアルは $(0), (1), (2), \ldots$ のどれかに等しい.
3. 0 以上の整数 a, b について $(a) \supset (b)$ と $a \mid b$ は同値である.

4. 0 以上の整数 a, b の最大公約数 (greatest common divisor) と最小公倍数 (least common multiple) をそれぞれ g, l と書くと, $(a)+(b)=(g)$, $(a)\cap(b)=(l)$.

(0 は任意の数で割り切れる. 0 と a の最大公約数は a であり, 0 と a の最小公倍数は 0 とみなす.) □

$\mathbb{Z}$ は単項イデアル整域 (principal ideal domain, PID) なのでイデアルと数の対応は直接的である. PID 以外の可換環であってもイデアルを「数」の類似物をみなすという発想はイデアル＝理想数のアイデアの源泉であった.

低次元の整域を扱う場合にはイデアルを「数」の類似物とみなす発想は非常にうまく行く (Dedekind 整域＝次元 1 の正規 Noether 整域の理論). 後で説明するように, 体 k 上の多項式環のイデアルは「代数方程式」であるとみなせる. イデアルの理論は「数」や「代数方程式」の理論の一般化になっている.

[13] (Euclid 環の例) 有理整数環 $\mathbb{Z}$, 体 K 上の一変数多項式環 $K[x]$, Gauss の整数環 $\mathbb{Z}[\sqrt{-1}]$ が Euclid 環であることを示せ. □

[14] (PID ではない整域の例) 有理整数環上の一変数多項式環 $\mathbb{Z}[x]$ と体 K 上の二変数多項式環 $K[x,y]$ が PID ではないことを示せ. □

ヒント. 2 以上の整数 m に対して $(m,x)\subset\mathbb{Z}[x]$ が単項イデアルでないことと, $(x,y)\subset K[x,y]$ が単項イデアルではないことを示せ. □

2.2 剰余環

正の整数 n の Euler の函数 $\varphi(n)$ を次のように定義する:

$$\varphi(n)=(1,2,\dots,n-1 \text{ に含まれる } n \text{ と互いに素な数の個数}).$$

たとえば $\varphi(1)=0$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$, $\varphi(8)=4$, $\varphi(9)=6$ である. 素数のべき p^f に対して $\varphi(p^f)=p^f-p^{f-1}$ が成立する.

[15] ($\mathbb{Z}$ の剰余環の単数群の位数) 正の整数 n に関して以下を示せ.

1. $\mathbb{Z}/(n)$ の単数群 $U(\mathbb{Z}/(n))$ の位数は $\varphi(n)$ に等しい.
2. **(Fermat の小定理)** n と互いに素な $a\in\mathbb{Z}$ に対して $a^{\varphi(n)}\equiv 1 \bmod n$.
3. n の素因数分解を $n=p_1^{f_1}\cdots p_s^{f_s}$ と表わすと, 可換環としての同型

$$\mathbb{Z}/(n)\cong\mathbb{Z}/(p_1^{f_1})\times\cdots\times\mathbb{Z}/(p_s^{f_s}).$$

が成立しているので, 次の群の同型が成立している:

$$U(\mathbb{Z}/(n))\cong U(\mathbb{Z}/(p_1^{f_1}))\times\cdots\times U(\mathbb{Z}/(p_s^{f_s})).$$

4. Euler の函数は次の表示を持つ:

$$\varphi(n)=\prod_{i=1}^{s}(p_i^{f_i}-p_i^{f_i-1})=n\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right).$$

5. $\mathbb{Z}/(n)$ が体になるための必要十分条件は n が素数であることである. □

上の問題の結果より $U(\mathbb{Z}/(n))$ の構造の決定は n が素数べき p^f に等しい場合に帰着する.

[16] ($U(\mathbb{Z}/(p^f))$ の構造の決定, 20 点) 次を示せ:

1. p が奇素数のとき $U(\mathbb{Z}/(p^f))$ は位数が $\varphi(p^f) = p^f - p^{f-1} = (p-1)p^{f-1}$ の巡回群である.

2. $p = 2$ のとき

   (a) $U(\mathbb{Z}/(2)) = 1$ (単位元しか持たない群).

   (b) $U(\mathbb{Z}/(2^2)) = \langle -\bar{1} \rangle$ (位数 2 の巡回群).

   (c) $f \geqq 3$ ならば $U(\mathbb{Z}/(p^f)) = \langle -\bar{1} \rangle \times \langle \bar{5} \rangle$ である.
   ここで $\langle -\bar{1} \rangle$ の位数は 2 であり, $\langle \bar{5} \rangle$ の位数は 2^{f-2} である. □

参考 2.1 上の問題の結果の証明は実質的に p 進整数環 $\mathbb{Z}_p = \operatorname{proj}\lim_{f\to\infty} \mathbb{Z}/(p^f)$ の単数群 $U(\mathbb{Z}_p)$ の構造を求めたことになっている. 数論に興味のある人は解いておいた方が良いだろう. 結果だけを [1] の pp.77-79 から抜き出しおこう:

1. p が奇素数のとき $U(\mathbb{Z}_p) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.

2. $p = 2$ のとき $U(\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

なお永尾 [4] では $\mathbb{Z}/(n)$ を $\mathbb{Z}_n$ と書いてしまっているが, $\mathbb{Z}_p$ という記号は p 進整数環の意味で用いることが多い. そこでこの演習では $\mathbb{Z}/(n)$ のことを $\mathbb{Z}_n$ とは書かないことにした. □

[17] (Wilson の定理) p が素数ならば $(p-1)! \equiv -1 \pmod{p}$ である. □

ヒント. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は体でかつ $\mathbb{F}_p^\times$ は位数 $p-1$ の巡回群になる. よって $\mathbb{F}_p[x]$ において $x^{p-1} - 1 = (x - \bar{1}) \dots (x - (\overline{p-1}))$.
$\mathbb{F}_p[x]$ において公式 $x^{p-1} - 1 = (x - \bar{1}) \dots (x - (\overline{p-1}))$ が成立することさえ示せれば後は容易である. その公式は $\mathbb{F}_p^\times$ が位数 $p-1$ の有限群であることさえ知っていれば示せる (どうやって示すかについては自分で考えよ). 一般に位数 N の有限群 G の任意の元 $a \in G$ は $a^n = 1$ を満たしている (たとえば [4] p.24 系 8.5). これより $\mathbb{F}_p^\times$ の任意の元 a は $a^{p-1} = 1$ を満たしている. この事実と高校のときに習った剰余定理を使えば上の公式を容易に示せるはずである. □

2.3 環の準同型定理

[18] (環の準同型定理) R, R' は (可換とは限らない) 環であるとし, $f : R \to R'$ は環の準同型であるとする. このとき $\operatorname{Im} f$ は R' の部分環になり, $\operatorname{Ker} f$ は R の両側イデアルになり, f は環同型 $R/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$ を誘導する. 特に f が全射ならば $R/\operatorname{Ker} f \cong R'$ である. □

例 2.2 問題 [1] のヒントの $A : \mathbb{H} \to M_4(\mathbb{R})$ は環の単射準同型写像である. よって環として $\mathbb{H} \cong \operatorname{Im} A$. □

[19] (両側イデアルの対応) R, R' は (可換とは限らない) 環であるとし, $f : R \to R'$ は環の全射準同型であるとする. 以下を示せ:

1. R' の両側イデアル I' に対して, $I = f^{-1}(I')$ は $\operatorname{Ker} f$ を含む R の両側イデアルであり, $f(I) = I'$ が成立する.
2. R の両側イデアル I に対して, $I' = f(I)$ は R' の両側イデアルであり, $f^{-1}(I') = I + \operatorname{Ker} f$ が成立する.
3. 以上の対応によって R' の両側イデアルと $\operatorname{Ker} f$ を含む R の両側イデアルは一対一に対応する.
4. 互いに対応する R' の両側イデアル I' と $\operatorname{Ker} f$ を含む R の両側イデアル I' が与えられたとき, f は自然な環同型 $R/I \xrightarrow{\sim} R'/I'$ を誘導する. □

[20] (カスプ, 20 点) 体 K 係数の一変数多項式環 $K[t]$ の部分環 R' を

$$R' = \{\, a_0 + a_2 t^2 + a_3 t^3 + \cdots (\text{有限和}) \mid a_i \in K \,\}$$

と定める. R' は t を含まないので $K[t]$ よりも真に小さい. これとは別に二変数多項式環 $K[x, y]$ を考える. 環の準同型定理を用いて $K[x, y]/(y^2 - x^3) \cong R'$ を証明せよ. □

ヒント. K 上の環準同型 $\phi : K[x, y] \to R'$ を $\phi(x) = t^2$, $\phi(y) = t^3$ という条件で定める. このとき ϕ が全射でかつ $(y^2 - x^3) \subset \operatorname{Ker} \phi$ であることは易しい. $(y^2 - x^3) \supset \operatorname{Ker} \phi$ を示すためには y の多項式とみなした $y^2 - x^3$ による割り算 (商と余りを求める計算) を考えよ. □

参考 2.3 $x = t^2$, $y = t^3$ は曲線 $y^2 = x^3$ のパラメーター表示になっている. 曲線 $y^2 = x^3$ のグラフを描くと点 $(x, y) = (0, 0)$ でとがっている. 曲線 $y^2 = x^3$ における $(x, y) = (0, 0)$ のような特異点を**カスプ (cusp)** と呼ぶ[1]. $K[x, y]/(y^2 - x^3) = K[t^2, t^3]$ はカスプを持つ曲線 $y^2 = x^3$ の上の多項式函数のなす環である. それに t を加えて $K[t]$ という特異点のない直線上の函数環を構成する操作は特異点解消 (resolution of singularities) の最も簡単な場合である. (ただしこの場合は 1 次元なので**正規化 (normalization)** という操作で特異点が解消されてしまう. 特異点解消が難しいのは高次元の場合である.) 広中平祐 (1931–) は標数が 0 の場合には任意の次元において特異点が常に解消可能であることを証明し, 1970 年に Fields 賞 (Fields medal prize) を受賞している. 広中の特異点解消定理は代数幾何学だけに限らず様々な分野に応用を持つ大定理である. □

2.4 素イデアルと極大イデアル

この節では環はすべて可換であると仮定する。

[1] cusp は「とがった先端」という意味の名詞である.

[21] (極大イデアルと剰余体) 可換環 R のイデアル I が極大イデアルであるための必要十分条件は R/I が体になることである. 特に可換環の極大イデアルは素イデアルである. I が極大イデアルのとき R/I を**剰余体 (residue field)** と呼ぶ. $\mathbb{Z}$ のイデアル $(n) = n\mathbb{Z}$ (n は 0 以上の整数) が極大イデアルになるための必要十分条件は n が素数であることを示せ. □

定義 2.4 (素元) 可換環 R の 0 でない元 p が**素元 (prime element)** であるとは, 単項イデアル $(p) = Rp$ が素イデアルになることである. □

定義 2.5 (既約元) 可換環 R の元 p が**既約元 (irreducible element)** であるとは, p が単元ではなく, $a, b \in R$, $p = ab$ ならば a または b が単元になることである. たとえば 0, 1 は既約元ではない. □

注意 2.6 上の意味での既約元のことを素元と呼んでいる本もあるので注意せよ. 例えば永尾 [4] はそういう流儀を採用している. しかし素元と素イデアルを対応させたければ上の意味での素元を既約元と呼ぶ流儀を採用した方が良い. □

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

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

注意 2.7 上の問題の逆は PID や UFD ではが成立するが, 一般の整域では成立しない. □

[23] (PID の既約元) R が PID ならば 0 でない $p \in R$ に対して以下の条件は互いに同値になる:

(a) (p) は R の極大イデアルである.

(b) (p) は R の素イデアルである. すなわち p は R の素元である.

(c) p は R の既約元である. □

[24] (極大ではない素イデアルの例) K は体であるとする. 以下を示せ:

1. $\mathbb{Z}$ のイデアル (0) は素イデアルだが極大イデアルではない.
2. $\mathbb{Z}[x]$ のイデアル (x) は 0 でない素イデアルだが極大イデアルではない.
3. 素数 p に対して $\mathbb{Z}[x]$ のイデアル (p, x) は極大イデアルである.
4. $K[x]$ のイデアル (0) は素イデアルだが極大イデアルではない.
5. $K[x, y]$ のイデアル (y) は 0 でない素イデアルだが極大イデアルではない.
6. $K[x, y]$ のイデアル (x, y) は極大であるである. □

定義 2.8 (既約多項式) 整域 R 上の一変数多項式環 $R[x]$ について考える. $f \in R[x]$ が $R[x]$ において**既約 (irreducible)** であるとは, $f \notin R$ であり, $g, h \in R[x]$, $f = gh$ ならば g または h が R の元になることである.

特に K が体ならば $K[x]$ の既約多項式の全体の集合は $K[x]$ の既約元の集合に等しい. □

[25] (Eisenstein の判定法) p は素数であるとする. このとき

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

の係数 $a_i \in \mathbb{Z}$ が条件

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

を満たしているならば f は $\mathbb{Z}[x]$ において既約である. たとえば $x^n + p$ や $x^n + px + p$ は $\mathbb{Z}[x]$ において既約である. □

注意 2.9 実は $\mathbb{Z}[x]$ において既約ならば $\mathbb{Q}[x]$ においても既約である. このことは UFD に関する Gauss の定理の証明のところでずっと一般的に証明されることになる. □

3 環と加群の理論

3.5 イデアルとは何か

「イデアルとは何か」を理解するためには「環をイデアルで割ること」を理解しなければいけない. 「環をイデアルで割ること」は「加法群を加法部分群で割ること」の特殊な場合なので最初に後者について説明することにする.

3.5.1 加法群を加法部分群で割ること (商加法群)

加法群 M とその加法部分加群 N が与えられたとする. (たとえば環は加法群とみなせるし, 体上のベクトル空間や環上の加群も加法群とみなせる.) そのとき「M の中で N の元をすべて 0 とみなしてできる加法群」を M/N と書く習慣になっている:

$$M/N = (M \text{ の中で } N \text{ の元をすべて } 0 \text{ とみなしてできる加法群}).$$

たとえば $M = \mathbb{Z}$, $N = 3\mathbb{Z}$ のとき $M/N = \mathbb{Z}/3\mathbb{Z}$ は $\mathbb{Z}$ の中で 3 の倍数をすべて 0 とみなしてできる加法群である. $\mathbb{Z}/3\mathbb{Z}$ の中では 3 は 0 とみなされるので $\overline{5} = \overline{2} + \overline{3} = \overline{2}$ という計算が成立していなければいけない.

上の説明の仕方は直観的過ぎて論理的厳密性の観点からは不十分である. 商加法群 M/N の論理的に厳密な構成法は次の通り:

$$M/N = \{\, a + N \mid a \in M \,\}, \quad (a + N) + (b + N) = (a + b) + N \ \ (a, b \in M).$$

M の部分集合 $a + N = \{\, a + n \mid n \in N \,\}$ を M/N の元とみなすとき, それを次のように書くことがある:

$$a + N = a \bmod N = [a] = \overline{a} \in M/N.$$

論理的に厳密な商加法群 M/N の構成法が実際に「M の中で N の元をすべて 0 とみなしてできる加法群」を与えていることを確認しよう.

補題 3.1 $a, b \in M$ に対して以下の条件は互いに同値である:

(a) $a + N = b + N$,

(b) $b \in a + N$,

(c) $a \in b + N$,

(d) $b - a \in N$. □

証明. (a) から (b) が出ること. $a + N = b + N$ ならば $b \in b + N = a + N$ である.

(b) と (c) が同値であること. $b \in a + N$ のとき, ある $n \in N$ で $b = a + n$ となるものが存在するので $a = b - n = b + (-n) \in b + N$ である. 逆に $a \in b + N$ のとき, ある $n \in N$ で $a = b + n$ となるものが存在するので $b = a - n = a + (-n) \in a + N$ である.

(b) と (d) が同値であること. $b \in a + N$ のとき, ある $n \in N$ で $b = a + n$ となるものが存在するので $b - a = n \in N$ である. 逆に $n := b - a \in N$ のとき $b = a + n \in a + N$ である.

(d) から (a) が出ること. $n := b - a \in N$ と仮定する. そのとき $a = b - n$ かつ $b = a + n$ である. よって任意に $a + n' \in a + N$ $(n' \in N)$ を取ると $a + n' = b + (n' - n) \in m' + N$ であるから $a + N \subset b + N$ であり, 任意に $b + n'' \in b + N$ $(n'' \in N)$ を取ると $b + n'' = a + (n + n'') \in a + N$ であるから $b + N \subset a + N$ である. したがって $a + N = b + N$ である. □

[26] 以下の数学的対象の図を描け:

1. $M = \mathbb{R}$ の中の $N = \mathbb{Z}$, $0.3 + N$, $-0.3 + N$, $-1.7 + N$.
2. $M = \mathbb{Z}^2$ の中の $N = \{\, (a, -a) \mid a \in \mathbb{Z} \,\}$, $(1, 2) + N$, $(2, -2) + N$.
3. $M = \mathbb{Z}$ の中の $N = 6\mathbb{Z}$, $1 + N$, $2 + N$, $3 + N$, $4 + N$, $5 + N$, $6 + N$. □

上の補題より M/N の元たちは M の元たちを N の差を無視して同一視することによって得られたと考えることができる. M/N が M の部分集合の集合であるという考え方にこだわる限り, このような考え方はできないので注意して欲しい.

補題 3.2 $a_1, a_2, b_1, b_2 \in M$ のとき $a_1 + N = a_2 + N$ かつ $b_1 + N = b_2 + N$ ならば $(a_1 + b_1) + N = (a_2 + b_2) + N$ である. □

証明. 補題 3.1 よりある $n, n' \in N$ で $a_1 = a_2 + n$, $b_1 = b_2 + n'$ となるものが存在する. そのとき $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = n + n' \in N$ である. よって補題 3.1 より $(a_1 + b_1) + N = (a_2 + b_2) + N$ である. □

この補題より M/N における加法が well-defined であること (矛盾なくうまく定義されていること) がわかる.

補題 3.3 $(M/N, +)$ は加法群である. □

証明. 記号の簡単のため $a + N$ を $[a]$ と書くことにする. M/N における加法の定義は $[a] + [b] = [a + b]$ である. 以下を示せばよい: 任意の $[a], [b], [c] \in M\mathbb{N}$ に対して

1. $([a]+[b])+[c]=[a]+([b]+[c])$,
2. $[a]+[0]=[0]+[a]=[a]$,
3. $[a]+[-a]=[-a]+[a]=[0]$.

2 番目と 3 番目が成立することは M/N の加法の定義より明らかである. 1 番目の M/N における加法の結合律は M における加法の結合律から導かれる. 実際

$$\begin{aligned}([a]+[b])+[c]&=[a+b]+[c]=[(a+b)+c]\\&=[a+(b+c)]=[a]+[b+c]=[a]+([b]+[c]).\quad\square\end{aligned}$$

このように M/N が加法群になることの証明は簡単である. 加法群になることそのものの証明よりも加法の定義が well-defined であることの証明の方が面倒である. こういうことはよくある. こういう議論に慣れないうちは必要な well-definedness の証明を省略してはいけない.

3.5.2 両側イデアルの導入

R は (可換とは限らない) 環であり, I は R の加法部分群であるとする. 商加法群

$$R/I=\{\,[a]=a+I\mid a\in R\,\},\quad [a]+[b]=[a+b]\ \ (a,b\in R)$$

に乗法を

$$[a][b]=[ab]\quad (a,b\in R)$$

によって定めることができるためには, 任意の $a\in R$, $f\in I$ に対して $af, fa\in I$ が成立していることが必要である.

実際 $f\in I$ と $f \bmod I = 0 \bmod I$ は同値であり, 上の式によって乗法がうまく定義されているとすれば $f\in I$ のとき

$$[af]=[a][f]=[a][0]=[a0]=[0]=I$$

より $af\in I$ でなければいけない. 同様にして $fa\in I$ でなければいけないこともわかる.

このような性質を持つ R の加法部分群に名前を付けておこう.

定義 3.4 (両側イデアル, イデアル) 環 R の加法部分群 I が R の元による左右からの積で閉じているとき (すなわち $a\in R$, $f\in I$ に対して $af, fa\in I$ であるとき), I を R の**両側イデアル (two-sided ideal)** と呼ぶ. 環 R が可換な場合には単に**イデアル (ideal)** と呼ぶことにする. $\square$

逆に I が環 R の両側イデアルであれば R/I に自然に環の構造が入ることを示せる. もしもこれを示せなければ上の定義は失敗に終わったということになる. 論理的にはどのような定義も許されるが, 「数学的にうまい仕組みに名前を付けること」という意味での定義はその「うまい仕組み」が証明されるまで正しい定義であるかどうかわからない.

定理 3.5 (剰余環) I が環 R の両側イデアルであるとき商加法群 R/I には

$$[a][b] = [ab] \quad (a, b \in R)$$

によって環構造を入れることができる. このとき環 R/I を**剰余環 (residue ring)** もしくは**剰余類環 (residue-class ring)** もしくは**商環 (factor ring, quotient ring)** と呼ぶ.

証明. 乗法の well-definedness を示すためには次を示さなければいけない:

$$a_1, a_2, b_1, b_2 \in R \text{ のとき } [a_1] = [a_2] \text{ かつ } [b_1] = [b_2] \text{ ならば } [a_1b_1] = [a_2b_2].$$

$a_1, a_2, b_1, b_2 \in R$, $[a_1] = [a_2]$, $[b_1] = [b_2]$ と仮定する. 補題 3.1 より, ある $f, g \in I$ で $a_1 = a_2 + f$, $b_1 = b_2 + g$ を満たすものが存在する. そのとき

$$a_1b_1 = (a_2 + f)(b_2 + g) = a_2b_2 + a_2g + fb_2 + fg.$$

I は両側イデアルなので $a_2g, fb_2, fg \in I$ である. よって $a_1b_1 \in a_2b_2 + I = [a_2b_2]$ であることがわかる. 補題 3.1 より $[a_1b_1] = [a_2b_2]$ である.

あとは以下を示せば十分である: $a, b, c \in R$ に対して

1. $([a][b])[c] = [a]([b][c])$,
2. $[1][a] = [a][1] = [a]$,
3. $[a]([b] + [c]) = [a][b] + [a][c]$,
4. $([a] + [b])[c] = [a][c] + [b][c]$.

これらが成立していることは R/I の加法と乗法の定義と R が環であることから容易に確かめられる. しかし読者は自分のノートに実際にその証明を一生に一度以上は省略せずに書いてみなければいけない. □

3.5.3 代数方程式のイデアルによる表現

現代の代数学では代数方程式の代わりに対応するイデアルや剰余環を扱うことがある.

K は任意の体であるとする (たとえば $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ や有限体など).

簡単のため二つの多項式 $F, G \in K[x, y]$ を用いて書き下された連立方程式

$$F(x, y) = 0, \quad G(x, y) = 0 \tag{$*$}$$

を多項式環 $K[x]$ のイデアルとして表現する方法を説明しよう.

連立方程式 $(*)$ に対応するイデアルは F, G から生成される $K[x, y]$ のイデアル

$$(F, G) = K[x, y]F(x, y) + K[x, y]G(x, y)$$

である. たとえば有理数係数の連立代数方程式

$$x^2 + y^2 = 1, \quad x = y \tag{1}$$

に対応する $\mathbb{Q}[x, y]$ のイデアルは $(x^2 + y^2 - 1, x - y)$ になる.

体 K を含む可換環 R が任意に与えられたとき, 連立代数方程式 $(*)$ の R における解とは R の元の組 $(\alpha,\beta)\in R^2$ で

$$F(\alpha,\beta)=0,\quad G(\alpha,\beta)=0 \tag{$**$}$$

をみたすもののことである. たとえば有理数係数の連立方程式 (1) の有理数解は存在しないが, 実数解 $(\pm 1/\sqrt{2},\pm 1/\sqrt{2})$ は存在する.

[**27**] 以下を示せ:

1. $\mathbb{Q}[x,y]$ のイデアル $(x^2+y^2-1,x-y)$, $(2x^2-1,x-y)$ は互いに等しい.
2. $\mathbb{Q}[x]$ のイデアル (x^6-1,x^4-1) , (x^2-1) は互いに等しい.
3. $\mathbb{Q}[x]$ のイデアル (x), (x^2) は互いに等しくない. □

ヒント. 1. $x^2+y^2-1+(x+y)(x-y)=2x^2-1$. (注意: 1 の結果は有理数係数の連立方程式 (1) と次の連立方程式

$$2x^2=1,\quad x=y. \tag{2}$$

が同値であることのイデアル版である.)

2. $x^6-1,x^4-1\in(x^2-1)$ でかつ $x^6-1-x^2(x^4-1)=x^2-1$. (注意: 2 の結果は $x^6=1$ と $x^4=1$ の共通解は $x^2=1$ の解に等しいという結果のイデアル版である.)

3. $x\notin(x^2)$ を示せ. (注意： $x=0$ は方程式 $x=0$ の単根だが, 方程式 $x^2=0$ の重根である. イデアルによる代数方程式の表現によっても単根と重根が区別される.) □

方程式の解をイデアルの言葉を用いて特徴付けられることを説明しよう.

R は体 K を含む任意の可換環であるとする.

任意に $(\alpha,\beta)\in R^2$ を取ると環準同型 $\phi_{\alpha,\beta}:K[x,y]\to R$ を

$$\phi_{\alpha,\beta}(f(x,y))=f(\alpha,\beta)\quad(f\in K[x,y])$$

によって定めることができる. このとき次が成立している:

$$(\alpha,\beta)\text{ は方程式 }(*)\text{ の解である}\iff(F,G)\subset\operatorname{Ker}\phi_{\alpha,\beta}.$$

実際, (α,β) が方程式 $(*)$ の解であることの定義は $F(\alpha,\beta)=G(\alpha,\beta)=0$ が成立することであり, $\phi_{\alpha,\beta}$ の定義より $F(\alpha,\beta)=G(\alpha,\beta)=0$ と $F,G\in\operatorname{Ker}\phi_{\alpha,\beta}$ は同値であり, (F,G) は F,G を含む $K[x,y]$ の最小のイデアルなので $F,G\in\operatorname{Ker}\phi_{\alpha,\beta}$ と $(F,G)\subset\operatorname{Ker}\phi_{\alpha,\beta}$ は同値である.

さらに剰余環 $K[x,y]/(F,G)$ を使えば可換環 R における方程式 $(*)$ の解全体の集合を環の準同型写像の集合で表現できる.

K を含む二つの可換環 R_1 から R_2 への環準同型 ϕ が K 上の環準同型であるとは任意の $a\in K$ に対して $\phi(a)=a$ が成立することである. R_1 から R_2 への K 上の環準同型全体の集合を次のように書くことにする:

$$\operatorname{Hom}_{K\text{-ring}}(R_1,R_2)=\{\,\phi:R_1\to R_2\mid\phi\text{ は }K\text{ 上の環準同型}\,\}.$$

定理 3.6 次の自然な一対一対応が存在する:

$$\mathrm{Hom}_{K\text{-ring}}\left(K[x,y]/(F,G),R\right) \cong \left\{\,(\alpha,\beta)\in R^2 \mid F(\alpha,\beta)=G(\alpha,\beta)=0\,\right\}. \quad \square$$

略証. K 上の環準同型 $\phi : K[x,y]/(F,G) \to R$ に対して $(\alpha,\beta) = (\phi([x]),\phi([y])) \in R^2$ と置くと $F(\alpha,\beta) = G(\alpha,\beta) = 0$ である.

逆に $(\alpha,\beta) \in R^2$ が $F(\alpha,\beta) = G(\alpha,\beta) = 0$ を満たしていれば, K 上の環準同型 $\phi : K[x,y]/(F,G) \to R$ を $\phi([f(x,y)]) = f(\alpha,\beta)$ $(f \in K[x,y])$ によって定めることができる (well-definedness の証明が必要).

これらの対応は互いに逆写像になっている. $\square$

[28] (20 点) すぐ上の略証で省略されている部分を完全に埋めよ. $\square$

後で次の定理を学ぶことになる.

定理 3.7 (体上の Hilbert の基定理) 体 K 上の n 変数多項式環 $K[x_1,\ldots,x_n]$ の任意のイデアル I はある $F_1,\ldots,F_r \in K[x_1,\ldots,x_n]$ によって $I = (F_1,\ldots,F_r)$ と表現できる. $\square$

実際には **Hilbert 基定理 (Hilbert's basis theorem)** は K が体よりもずっと一般な Noether 環の場合にも成立している. 証明については永尾 [4] pp.121–122 や堀田 [5] p.145 などを見よ. ほとんどの代数学の教科書に証明が書いてある.

上の方の議論から体 K 係数の連立代数方程式には $K[x_1,\ldots,x_n]$ のイデアルを対応させることができる. 逆に Hilbert の基定理は $K[x_1,\ldots,x_n]$ の任意のイデアル I はある連立代数方程式

$$F_i(x_1,\ldots,x_n) = 0 \quad (i = 1,\ldots,r)$$

に対応していることを主張している.

以上によって $K[x_1,\ldots,x_n]$ のイデアルは K 係数の連立代数方程式の抽象化になっていることがわかった.

3.5.4 体上有限生成な可換環

前節では体 K 上の多項式環のイデアルが代数方程式に対応していることを説明した. それではもっと一般的な可換環のイデアルはどのように解釈可能なのだろうか?

体 K 上有限生成な可換環のイデアルであれば前節と同様に代数方程式に対応していると解釈できる.

定義 3.8 (体 K 上有限生成) 体 K を含む可換環 R が K **上有限生成 (finitely generated over K)** であるとは, ある有限個の元 $a_1,\ldots,a_n \in R$ が存在して, R の任意の元が $a_1,\ldots,a_n$ の K 係数多項式で表わされることである. このとき $a_1,\ldots,a_n$ は R の K **上での生成元 (generators over K)** であるという. $\square$

補題 3.9 体 K 上有限生成な可換環は体 K 上の n 変数多項式環の剰余環に環として同型である. $\square$

証明. R は体 K 上有限生成な可換環であるとし, $a_1, \ldots, a_n \in R$ は R の K 上での生成元であるとする. このとき環準同型 $\phi : K[x_1, \ldots, x_n] \to R$ を

$$\phi(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n) \quad (f \in K[x_1, \ldots, x_n])$$

と定めることができる. R のすべての元は $a_1, \ldots, a_n$ の K 係数多項式 $f(a_1, \ldots, a_n)$ で表わされるので ϕ は全射である. したがって環の準同型定理より, 環の同型

$$K[x_1, \ldots, x_n]/\mathrm{Ker}\,\phi \cong R, \quad [f(x_1, \ldots, x_n)] \mapsto f(a_1, \ldots, a_n).$$

が成立する. □

したがって体 K 上有限生成な可換環 R の構造について調べるときには

$$R = K[x_1, \ldots, x_n]/I, \quad I \text{ は } K[x_1, \ldots, x_n] \text{ のあるイデアル}$$

であると仮定してよい. 問題 **[19]** の結果より, R のイデアル J と $K[x_1, \ldots, x_n]$ の I を含むイデアル J' は自然に一対一に対応しており, 剰余環のあいだにも自然な同型

$$R/J \cong K[x_1, \ldots, x_n]/J'$$

が成立している. このことより R のイデアルによる剰余環の構造を調べるためには, $K[x_1, \ldots, x_n]$ の I を含むイデアルによる剰余環の構造を調べればよいことがわかる. さらに Hilbert の基定理より $K[x_1, \ldots, x_n]$ の任意のイデアルはある連立代数方程式に対応しているのであった. 以上を合わせれば, 体 K 上有限生成な可換環およびその剰余環の理論もまたある連立代数方程式に対応していると考えることができる.

以上によって体 K 上有限生成な可換環の理論は K 係数の連立代数方程式の理論の抽象化であると考えて構わないことがわかった.

3.5.5 $\mathbb{Z}$ 上有限生成な可換環

応用上重要な可換環の中には体上有限生成な可換環ではないものが存在する. それは有理整数環 $\mathbb{Z}$ 上有限生成な可換環である. たとえば $\mathbb{Z}$ 自身は体上有限生成ではないが, $\mathbb{Z}$ 上有限生成である. $\mathbb{Z}$ は可換環として明らかに基本的でかつ重要である. 同様に $\mathbb{Z}$ 上の n 変数多項式環 $\mathbb{Z}[x_1, \ldots, x_n]$ も体上有限生成ではないが, $\mathbb{Z}$ 上有限生成である.

$\mathbb{Z}$ 上有限生成な可換環は**数論における基本的な研究対象**である.

定義 3.10 (体 K 上有限生成) 可換環 R が $\mathbb{Z}$ **上有限生成 (finitely generated over $\mathbb{Z}$)** であるとは, ある有限個の元 $a_1, \ldots, a_n \in R$ が存在して, R の任意の元が $a_1, \ldots, a_n$ の有理整数係数多項式で表わされることである. □

注意 3.11 可換環の任意の元の有理整数倍が自然に定義される. しかし有限体のように標数が正の場合には有理整数倍の結果が 0 になるかもしれない. □

Hilbert の基定理は一般の Noether 環上で成立しているので当然 $\mathbb{Z}$ 上でも成立しており, 次の結果が得られる.

定理 3.12 ($\mathbb{Z}$ 上の Hilbert の基定理) 有理整数環 $\mathbb{Z}$ 上の n 変数多項式環 $\mathbb{Z}[x_1,\ldots,x_n]$ の任意のイデアル I はある $F_1,\ldots,F_r \in \mathbb{Z}[x_1,\ldots,x_n]$ によって $I=(F_1,\ldots,F_r)$ と表現できる. □

補題 3.9 と完全に同様の議論によって次を証明できる.

補題 3.13 $\mathbb{Z}$ 上有限生成な可換環は $\mathbb{Z}$ 上の n 変数多項式環のある剰余環に環として同型である. □

[29] 実際に補題 3.13 の証明を書き下せ. □

以上の 定理 3.12, 補題 3.13 の結果より, $\mathbb{Z}$ 上有限生成な可換環もまた連立代数方程式に対応しているとみなせる. ただし $\mathbb{Z}[x_1,\ldots,x_n]$ には (24) のような数で生成されるイデアルが存在し, $\mathbb{Z}[x_1,\ldots,x_n]/(24)$ の中で数 24 は 0 とみなされる. このように $\mathbb{Z}$ 上有限生成な可換環の場合には 1 次以上の多項式を 0 と置くような代数方程式を考えるだけではなく, 24 のような数をも 0 とみなすことがある点が体上有限生成な可換環を扱った場合とは違っている.

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

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

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

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

注意 3.14 上の問題の結果より $\sqrt{m}$ のような数の研究も $\mathbb{Z}$ 上有限生成な可換環の研究に含まれていることがわかる. □

参考 3.15 (二次体の整数環) 上の問題の $\mathbb{Z}[\sqrt{m}]$ の商体 $\mathbb{Q}(\sqrt{m})$ は**二次体 (quadratic field)** と呼ばれている. 二次体 K は平方因子を含まない 0 でも 1 でも有理整数 m によって $K=\mathbb{Q}(\sqrt{m})$ と一意に表わされる. $m>0$ のとき $\mathbb{Q}(\sqrt{m})$ は**実二次体 (real quadratic field)** と呼ばれ, $m<0$ のとき $\mathbb{Q}(\sqrt{m})$ は**虚二次体 (imaginary quadratic field)** と呼ばれている.

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

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

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

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

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

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

詳しくは代数的整数論の教科書を見よ. たとえば, 1 の結果の証明は [1] p.119 問 3 の解答 (pp.146-147) に書いてあり, Dedekind 整域の一般論は [7] 第 5 章にある.

さらに以下が成立していることに注意しなければいけない:

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

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

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

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

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

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

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

1. $U(\mathbb{Z}[\sqrt{-26}]) = \{\pm 1\}$ である.

2. $3, 1 \pm \sqrt{-26}$ は $\mathbb{Z}[\sqrt{-26}]$ の既約元である.

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

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

1. $a = k + l\sqrt{-26}, b = m + n\sqrt{-26} \in \mathbb{Z}[\sqrt{-26}]$, $1 = ab$ のとき $1 = N(a)N(b) = (k^2+26l^2)(m^2+26n^2)$ である. これより $k = \pm 1$, $l = 0$ であることがわかる.

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

3. 容易. □

[32] (20 点以上) $\mathbb{Z}[\sqrt{-26}]$ におけるイデアルの計算に関して以下が成立していることを示せ:

1. $\mathbb{Z}[\sqrt{-26}]$ のイデアル $I = (3, 1 + \sqrt{-26})$, $J = (3, 1 - \sqrt{-26})$ は $\mathbb{Z}[\sqrt{-26}]$ の素イデアルである.

2. $(3) = IJ$, $(1 + \sqrt{-26}) = I^3$, $(1 - \sqrt{-26}) = J^3$.

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

参考 3.16 数学的に深くて応用的にも有用な結果を出すためには扱う数学的対象に何らかの有限性の条件を課しておいた方が良い. 可換環に関する体 K 上有限生成や $\mathbb{Z}$ 上有限生成という条件はその意味で非常に良い条件である. □

参考 3.17 以上においては主として可換環のイデアルのイメージについて説明した. 非可換環のイデアルのイメージは可換環の場合とは異なる場合がある. □

3.6 素イデアルと極大イデアル

[33] (素イデアルと極大イデアルの定義) R は可換環であり, I はそのイデアルであり, $I \neq R$ であるとする. 以下を示せ.

1. 以下の条件は互いに同値である:

   (a) 剰余環 R/I は整域である.

   (b) $a, b \in R$ のとき $a \notin I$ かつ $b \notin I$ ならば $ab \notin I$.

   (c) $a, b \in R$ のとき $ab \in I$ ならば $a \in I$ または $b \in I$.

   (d) $a, b \in R$ のとき $a \notin I$ かつ $ab \in I$ ならば $b \in I$.

   これらの条件が成立するとき I は R の**素イデアル (prime ideal)** であると言う.

2. 次の二つの条件は互いに同値である:

   (a) 剰余環 R/I は体である.

   (b) R の I を真に含むイデアルは R 以外に存在しない.

   これらの条件が成立するとき I は R の**極大イデアル (maximal ideal)** であると言い, 剰余環 R/I は体になるので**剰余体 (residue field)** と呼ばれる. □

[34] (極大イデアルの存在定理) R は可換環であるとし, I は R のイデアルであり, $I \neq R$ であるとする. このとき I を含む R の極大イデアルが存在する. □

ヒント. Zorn の補題の決まり切った使い方で証明できる. ほとんどの代数学の教科書の証明が書いてある. □

[35] ($\mathbb{C}[x]$ の極大イデアル) 以下を示せ.

1. $\alpha \in \mathbb{C}$ に対して環の準同型写像 $\phi_\alpha : \mathbb{C}[x] \to \mathbb{C}$ を $\phi_\alpha(f(x)) = f(\alpha)$ と定める. このとき ϕ_α は環の同型 $\bar{\phi}_\alpha : \mathbb{C}[x]/(x-\alpha) \xrightarrow{\sim} \mathbb{C}$, $f(x) \bmod (x-\alpha) \mapsto f(\alpha)$ を誘導する.
2. $\mathbb{C}[x]$ の極大イデアルはどれも $(x-\alpha)$ $(\alpha \in \mathbb{C})$ の形をしている.
3. $f(x) \in \mathbb{C}[x]$ について $f(x) \notin (x-\alpha)$ と $f(\alpha) \neq 0$ は同値である.
4. $f(x) \in \mathbb{C}[x]$ が $\mathbb{C}[x]$ の単元であるための必要十分条件は任意の $\alpha \in \mathbb{C}$ に対して $f(\alpha) \neq 0$ が成立することである. □

ヒント. 1. 環の準同型定理を使う.
2. $\mathbb{C}[x]$ は単項イデアル整域なので $\mathbb{C}[x]$ の極大イデアルは $\mathbb{C}[x]$ のあるモニックな既約多項式 $f(x)$ で生成される単項イデアルに等しい. $\mathbb{C}$ の代数閉体なので $\mathbb{C}[x]$ の多項式は一次式の積に分解される.
3. 剰余定理を使う.
4. $\mathbb{C}[x]$ の多項式は一次式の積に分解される. □

注意 3.18 上の問題 **[35]** について以下を注意しておく.

1. $\mathbb{C}[x]$ の極大イデアル全体の集合は $\mathbb{C}$ と同一視できる.
2. $\alpha \in \mathbb{C}$ に対応する極大イデアル $(x-\alpha)$ で割った $\mathbb{C}[x]$ の剰余環 $\mathbb{C}[x]/(x-\alpha)$ を考えるということは $\mathbb{C}[x]$ の多項式 $f(x)$ の $x = \alpha$ での値を考えることに等しい.
3. $\mathbb{C}[x]$ の単元はどこでも 0 にならない多項式と一致するいう結果は極大イデアルによる単元の特徴付けだとみなすことができる. □

[36] (極大イデアルによる単元の特徴付け) R は可換環であるとし, $f \in R$ を任意に取る. 以下の条件が互いに同値であることを示せ:

(a) f は R の単元である.

(b) R の任意の極大イデアル I に対して $f \notin I$. □

ヒント. f が R の単元であることと $(f) = R$ は同値である.
R のイデアル I が f を含むことと (f) を含むことは同値である.
f が R の単元ならば $(f) = R$ であり, 極大イデアルは定義より R に等しくないので (f) を含む極大イデアルは存在しない.
f が R の単元でないならば $(f) \neq R$ なので, 極大イデアルの存在定理より (f) を含む極大イデアル I が存在する. □

[**37**] **(素イデアルの引き戻し)** R, R' は可換環であり, $\phi : R \to R'$ は環の準同型であるとする. このとき以下が成立していることを示せ:

1. I' が R' の素イデアルならば $\phi^{-1}(I')$ も R の素イデアルである.
2. ϕ が全射のとき, I' が R' の極大イデアルならば $\phi^{-1}(I')$ も R の極大イデアルである.
3. しかし一般の場合には I' が R' の極大イデアルでも $\phi^{-1}(I')$ は R の極大イデアルになるとは限らない. (反例を具体的に示せ.) □

ヒント. 1, 2. まず環の準同型定理を用いて ϕ が環の単射準同型 $\tilde{\phi} : R/\phi^{-1}(I') \hookrightarrow R'/I'$ を誘導することを示せ. 整域の部分環は整域である. ϕ が全射ならば $\tilde{\phi}$ は同型になる.

3. 体の部分環は体とは限らない. たとえば $R = \mathbb{Z}$, $R' = \mathbb{Q}$, $I' = 0$. (他にも面白い例を見つけてみよ.) □

参考 3.19 ($\operatorname{Spec} R$) 上の問題の結果は Grothendieck が発展させた**概型 (scheme)** の理論の出発点になる. 空間があればその上の体に値を持つ函数たちは自然に可換環をなす. 逆に概型の理論を使えば任意の可換環があたかも函数の環であるかのように考えることができる.

そのとき任意の可換環に対応する空間 (多様体) を構成しなければいけない. 極大イデアルはまさに直観的な意味での点に対応しているので, 可換環の極大イデアル全体の集合に適当に位相を入れて幾何学を建設できないかと考えることもできる. しかし可換環のあいだの環準同型に空間のあいだの写像を自然に対応させるためには極大イデアルだけではなく, 素イデアルをも「点」とみなした方が自然である.

実際上の問題より, 可換環 R の素イデアル全体の集合を

$$\operatorname{Spec} R = \{\, I \subset R \mid I \text{ は } R \text{ の素イデアル} \,\}$$

と書くと, 可換環のあいだの任意の環準同型 $\phi : R \to R'$ に対して写像

$$\operatorname{Spec} R' \leftarrow \operatorname{Spec} R, \quad I' \leftarrow \phi^{-1}(I')$$

が得られることがわかる. 可換環のあいだの準同型の向きと, それらの Spec のあいだの対応する写像の向きは互いに逆になる. この結果を次の問題と比較せよ. □

[**38**] **(C^∞ 多様体)** 以下を示せ:

1. M が C^∞ 多様体のとき, M 上の実数値函数全体の集合を $C^\infty(M)$ と書くと, $C^\infty(M)$ は自然に可換環をなす.
2. $\psi : M \to N$ は C^∞ 多様体のあいだの C^∞ 写像であるとする. このとき次の環準同型が自然に得られる:

$$\psi^* : C^\infty(N) \to C^\infty(M), \quad f \mapsto \psi^*(f) = f \circ \psi.$$

多様体のあいだの写像の向きとそれに対応する可換環のあいだの写像の向きは互いに逆になる. □

[39] K は体であるとする. $K[x]\times K[y]$ の部分環 R を次のように定める:

$$R=\{\,(f(x),g(y))\in K[x]\times K[y]\mid f(0)=g(0)\,\}.$$

このとき次の環同型が存在する:

$$K[x,y]/(xy)\xrightarrow{\sim} R,\quad F(x,y)\bmod(xy)\mapsto(F(x,0),F(0,y)).$$

$K[x,y]/(xy)\cong R$ は整域ではないので (xy) は素イデアルではない. □

ヒント. $\phi: K[x,y]\to R,\ F(x,y)\mapsto(F(x,0),F(0,y))$ に環の準同型定理を適用せよ. □

参考 3.20 (上の問題の幾何学的意味) 一変数多項式環 $K[x]$ は x 直線上の函数のなす環であり, 一変数多項式環 $K[y]$ は y 直線上の函数のなす環であるとみなせる. 直積環 $K[x]\times K[y]$ は x 直線と y 直線の非連結和の上の函数のなす環とみなせる. したがって $R=\{\,(f(x),g(y))\in K[x]\times K[y]\mid f(0)=g(0)\,\}$ は x 直線の原点と y 直線の原点を貼り合わせて作った空間上の函数のなす環とみなせる. (x 直線上の函数 $f(x)$ と y 直線上の函数 $g(y)$ の原点における値が一致していなければ x 直線と y 直線の原点を貼り合わせて作った空間上の函数とはみなせない.)

二変数多項式環 $K[x,y]$ は xy 平面上の函数のなす環とみなせる. 剰余環 $K[x,y]/(xy)$ は二変数多項式環 $K[x,y]$ の中で xy を 0 とみなしてできる環である. したがって $K[x,y]/(xy)$ は方程式 $xy=0$ の解空間すなわち原点で交わる x 軸と y 軸の和集合の上の函数のなす環とみなせる.

以上のように考えると R と $K[x,y]/(xy)$ は本質的に同じ空間上の函数のなす環であることがわかる. 実際にそれらの環が同型であることが証明できるということが上の問題の内容である.

このように可換環に関する操作は幾何学的な意味を持っていることが多い. 曖昧に感じられる幾何学的直観が可換環の議論によって明確になることも少なくない. □

2 環と加群の理論

2.6 中国式剰余定理 (Chinese remainder theorem)

[40] R は (可換とは限らない) 環であるとし, I は R の左イデアルであり, J は R の空でない部分集合であるとする. IJ を次のように定める:

$$IJ=\left\{\left.\sum_{i=1}^{s}f_ig_i\,\right|\,f_i\in I,\ g_i\in J\right\}.$$

このとき IJ は R の左イデアルである. □

[41] (易しい) 可換環 R の単項イデアル (a), (b) に対して $(a)(b)=(ab)$ である. □

[42] (可換とは限らない環に関する中国式剰余定理) R は可換とは限らない環であるとし, $I_1,\dots,I_n$ はその両側イデアルであるとする. このときもしも $I_i+\bigcap_{j(\neq i)}I_j=R$ $(i=1,\dots,n)$ ならば次の環同型が得られる:

$$R/(I_1\cap\cdots\cap I_n)\xrightarrow{\sim} R/I_1\times\cdots\times R/I_n,\quad a\bmod I\mapsto(a\bmod I_1,\dots,a\bmod I_n).$$ □

ヒント. 環の準同型 $\phi : R \to R/I_1 \times \cdots \times R/I_n$ を $\phi(a) = (a \bmod I_1, \ldots, a \bmod I_n)$ $(a \in R)$ と定める. $\mathrm{Ker}\,\phi = I_1 \cap \cdots \cap I_n$ であることは容易にわかる. 仮定よりある $f_i \in I_i$ と $g_i \in \bigcap_{j(\neq i)} I_j$ で $f_i + g_i = 1$ を満たすものが存在する. そのとき $a_1, \ldots, a_n \in R$ に対して $\phi(a_1 g_1 + \cdots + a_n g_n) = (a_1 \bmod I_1, \ldots, a_n \bmod I_n)$ である. よって ϕ は全射である. したがって環の準同型定理より目的の環同型が得られる. □

[43] R は (可換とは限らない) 環であるとし, $J_1, \ldots, J_n$ は R のイデアルであり, $R = J_1 \oplus \cdots \oplus J_n$ (加法群としての直和) になっているとする. このとき $I_i = J_1 \oplus \cdots \oplus \widehat{J_i} \oplus \cdots \oplus J_n$ ($\widehat{\ }$ は取り除くという意味) と置くと, 次の環同型が得られる:

$$R/\bigcap_{i=1}^{n} I_i \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_n, \quad a \bmod I \mapsto (a \bmod I_1, \ldots, a \bmod I_n). \quad \square$$

定義 2.1 (互いに素) 可換環 R のイデアル I, J が $I + J = R$ を満たしているとき, I と J は**互いに素 (coprime)** であると言う. □

[44] (易しい) $\mathbb{Z}$ のイデアル $(a), (b)$ が互いに素であるための必要十分条件は a, b の最大公約数が 1 に等しいことである. したがってイデアルが互いに素であることの定義は整数が互いに素であることの定義の一般化になっている. □

[45] (易しい) 可換環 R の相異なる 2 つの極大イデアル I, J は互いに素である. □

[46] (中国式剰余定理, Chinese remainder theorem) R は可換環であるとし, $I_1, \ldots, I_n$ はその両側イデアルであるとする. このときもしも $I_1, \ldots, I_n$ の任意の二つの組み合わせが互いに素であるならば次の環同型が得られる:

$$R/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_n, \quad a \bmod I \mapsto (a \bmod I_1, \ldots, a \bmod I_n). \quad \square$$

ヒント. 可換とは限らない環の中国式剰余定理より, R が可換環のとき, $I_1, \ldots, I_n$ の中の任意の二つの組み合わせが互いに素であるならば 任意の $i = 1, \ldots, n$ に対して I_i と $\bigcap_{j(\neq i)} I_j$ が互いに素になることを示せば十分である. 実際には I_1 と $I_2 \cap \cdots \cap I_n$ が互いに素であることだけを示せば十分である. (他の場合は番号の付け替えで証明される.) そのことは以下のような方針で示される:

1. 一般に可換環 R のイデアル I, J が互いに素ならば $I \cap J = IJ$. ($\supset$ は明らかなので $\subset$ のみを示せば良い. $I + J = R$ よりある $f \in I, g \in J$ で $f + g = 1$ となるものが存在する. このとき $a \in I \cap J$ ならば $a = af + ag$ で $af, ag \in IJ$ なので $a \in IJ$.)

2. $i = 2, \ldots, n$ に対して I_1 と I_i が互いに素ならば I_1 と $I_2 \cdots I_n$ は互いに素である. (一般の n で直接示せる. $i = 2, \ldots, n$ のとき $I_1 + I_i = R$ なのである $a_i \in I_1$ と $b_i \in I_i$ で $a_i + b_i = 1$ となるものが存在する. このとき $1 = (a_2 + b_2) \cdots (a_n + b_n)$ は $a_2 \cdots a_n \in I_2 \cdots I_n$ と I_1 の元の和の形になっている. よって $I_1 + I_2 \cdots I_n = R$ である.)

3. $I_2, \ldots, I_n$ のどの二つの組み合わせも互いに素であるならば $I_2 \cap \cdots \cap I_n = I_2 \cdots I_n$ となる. (上の二つの事実を使えば n に関する帰納法で示せる. $n = 2$ の場合は明らかであり, $n = 3$ の場合は実質的に上の 1 の結果そのものである. 上の 2 の結果より $I_2 \cdots I_{n-1}$ と I_n は互いに素になるので, $I_2 \cap \cdots \cap I_{n-1} = I_2 \cdots I_{n-1}$ ならば上の 1 の結果より $I_2 \cap \cdots \cap I_{n-1} \cap I_n = I_2 \cdots I_{n-1} \cap I_n = I_2 \cdots I_{n-1} I_n$ となる.)

4. 以上の 2 と 3 より I_1 と $I_2 \cap \cdots \cap I_n = I_2 \cdots I_n$ が互いに素であることがわかる. □

注意 2.2 可換環の中国式剰余定理について.

1. 上のヒントの 3 より, 可換環 R のイデアル $I_1, \ldots, I_n$ のどの二つの組み合わせも互いに素ならば, $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ となることもわかる. したがって上の問題の環同型を次のように書くこともできる:

$$R/(I_1 \cap \cdots \cap I_n) = R/I_1 \cdots I_n \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_n.$$

   問題 [**47**] も見よ.

2. 可換とは限らない一般の環でも $I_i + \bigcap_{j(\neq i)} I_j = R$ $(i = 1, \ldots, n)$ と仮定すれば中国式剰余定理が成立する. その条件は各 i ごとに n 個のイデアルのすべてが登場する条件になっているので使いにくい. しかし, 可換環では $I_1, \ldots, I_n$ のどの二つの組み合わせも互いに素であればその条件が成立していることがわかる. これが可換環での中国式剰余定理である. □

[**47**] 以下の環同型の存在を中国式剰余定理の応用として証明せよ:

1. n は正の整数であり, その素因数分解を $n = p_1^{e_1} \cdots p_s^{e_s}$ と書くと

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p^{e_1}) \times \cdots \times \mathbb{Z}/(p_s^{e_s}).$$

2. $\alpha_1, \ldots, \alpha_s \in \mathbb{C}$ は互いに異なるとし, $e_1, \ldots, e_s$ は正の整数であるとし,

$$f(x) = (x - \alpha_1)^{e_1} \cdots (x - \alpha_s)^{e_s}$$

   と置く. このとき

$$\mathbb{C}[x]/(f(x)) \cong \mathbb{C}[x]/((x - \alpha_1)^{e_1}) \times \cdots \times \mathbb{C}[x]/((x - \alpha_s)^{e_s}). \quad \square$$

注意 2.3 上の問題の小問 1 は有限生成 Abel 群の基本定理と関係が深く, 小問 2 は線形代数における Jordan 標準形の理論と関係が深い. □

2.7 積閉集合によって定義される分数環と素イデアルによる局所化

定義 2.4 (積閉集合) 可換環 R の部分集合 S が**積閉 (部分) 集合 (multiplicatively closed (sub-)set)** であるとは, $1 \in S$ かつ $0 \notin S$ で S が積で閉じていることである. □

[**48**] 以下の集合 S が積閉集合であることを示せ:

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

定義 2.5 (分数環, 全分数環環, 商体, 素イデアルにおける局所化) R は可換環であり, S はその積閉集合であるとする. 直積集合 $R \times S$ に次のように同値関係を入れる:

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

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

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

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

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

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

注意 2.6 上の定義において S が零因子を含まなければ同値関係 $\sim$ は次に等しい:

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

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

[49] **(定義の確認)** 以下を示せ:

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

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

定義 2.7 (局所環) 可換環 R が唯一の極大イデアル $\mathfrak{m}$ しか持たないとき $(R, \mathfrak{m})$ もしくは R を**局所環 (local ring)** と呼ぶ. 局所環 $(R, \mathfrak{m})$ に対して体 $R/\mathfrak{m}$ を局所環 R の**剰余体 (residue field)** と呼ぶ. □

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

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

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

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

$\mathbb{Z}_{(p)}$ の唯一の極大イデアルは

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

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

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

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

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

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

であり, 剰余体は $\mathbb{C}$ に同型である:

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

参考 2.8 すぐ上の問題はどうして R_P を局所化と呼ぶかを理解するために参考になる. 基本的に R の元が函数とみなせるとき, 函数たちに共通する定義域を縮小する操作が局所化になっている. すぐ上の問題の場合は $\mathbb{C}[x]$ の任意の元は $\mathbb{C}$ 上の函数とみなせるが, 局所化 $\mathbb{C}[x]_{(x-\alpha)}$ の元が定義されている領域の共通部分は α の一点になってしまう. □

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

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

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

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

であり, 剰余体は $\mathbb{C}$ に同型である:

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

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

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

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

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

であり, 剰余体は $\mathbb{C}(y)$ に同型である:

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

参考 2.9 上の問題の $\mathbb{C}[x,y]$ の素イデアル $(x-\alpha)$ は y 軸に平行な直線 $x=\alpha$ に対応している. 直線 $x=\alpha$ 上の有理函数体は $\mathbb{C}(y)$ に同型である. この $\mathbb{C}(y)$ が剰余体になっている.

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

参考文献

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

[2] 谷崎俊之, 環と体 3—非可換環論, 岩波講座 現代数学の基礎 17, 岩波書店, 1998

[3] 谷崎俊之, リー代数と量子群, 共立出版株式会社, 2002

[4] 永尾汎, 代数学, 新数学講座 4, 朝倉書店, 1983

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

[6] 堀田良之, 加群十話—代数学入門, すうがくぶっくす 3, 朝倉書店, 1988

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