2023 相原ゼミ (学部) ノート *

(2023 年 6 月 29 日更新)

このノートでは, 2023 年度の相原ゼミ (学部) の補足を簡単にまとめる[*1][*2]. 特に, (♠) については各自で確認されたい.

目次

* 教科書は [ST]

[*1] 筆者の趣味により長くなっている (2023.6.7.). 本編 (楕円曲線論) より付録 (環論) のほうが長い (笑).

[*2] 作成の都合上, 注釈などに重複や順番の前後ができてしまったが, ご容赦願いたい. 大切な議論については, 循環論法が起きないよう心がけている.

1　射影平面

1.1　射影の考え方

射影空間 $\mathbb{P}^n$ とは, ざっくりいうと, 「原点を通る直線を点とみた」ときの空間のことである. (基礎体 K を明示したいときは, $\mathbb{P}^n_K$ とかくこともある. これは数ベクトル空間 K^{n+1} の部分集合 “みたい” なものである[*3].)

- 2 次元ユークリッド空間 $\mathbb{R}^2$ (XY 平面) においては, 原点を通る直線は 1 本 ($Y=0$) を除き, $Y=1$ 上で交わるので, その射影空間をとると,

  $$\text{【}Y=1 \text{ 上の点たち】および【1 点 } (Y=0)\text{】}$$

  と表現できる. これを $\mathbb{P}^1$ ($=\mathbb{P}^1_{\mathbb{R}}$) とかき, 特に, **射影直線**とよぶ. また, 特殊な 1 点 ($Y=0$) を**無限遠点**という.
- 3 次元ユークリッド空間 $\mathbb{R}^3$ (XYZ 空間) においては,
  - XY 平面上にない原点を通る直線は, $Z=1$ 上で交わる;
  - XY 平面上の原点を通る直線は射影直線と同じ.

  よって, 今回の射影空間は,

  $$\text{【}Z=1 \text{ の点たち】および【}Z=0 \text{ かつ } Y=1 \text{ の点たち】および【1 点 } (Z=0=Y)\text{】}$$

  と表せる. これを $\mathbb{P}^2$ ($=\mathbb{P}^2_{\mathbb{R}}$) とかき, 特に, **射影平面**とよぶ. また, 射影直線 ($Z=0$ の点たち) を**無限遠点**という.

補足 1.1. 体 K に対して, 通常の数ベクトル空間 K^n を**アフィン空間**といい, $\mathbb{A}^n$ とかく. このとき, 射影直線および射影平面は次のようにかける:

- 射影直線 $\mathbb{P}^1=\mathbb{A}^1\cup\{\infty\}$
- 射影平面 $\mathbb{P}^2=\mathbb{A}^2\cup\mathbb{P}^1$

1.2　射影空間の定義

さて, 射影空間をきちんと定義しよう. ここでは, なるべく一般的に議論するため, 体 K から出発する. ($K=\mathbb{R},\mathbb{C}$ と思えばだいたい十分.)

[*3] 実際には, 同値関係でわっているため, 真に部分として入っているわけではない.

まず, K^{n+1} に次のように同値関係を定義する (実際に同値関係になることを確認 (♠)):

$$(a_i) \sim (b_i) \quad \overset{\text{def}}{\iff} \quad \text{ある } t\ (\neq 0) \in K \text{ が存在して, 任意の } i \text{ に対して, } b_i = ta_i.$$

(つまり, これら 2 点は, K^n 内で, 原点を通る同一直線上にあるということ.)

このとき, $\mathbb{P}^n := (K^{n+1} \setminus \{ \text{原点} \})/\sim$ を n **次元射影空間**という[*4]. 点 (a_i) を含む同値類を $[a_i]$ で表すことにする.

射影空間では, 元たちはスカラー倍によって同一視されるため, $a_{n+1} = 1$ となる元たち, および, $a_{n+1} = 0$ となる元たちによって大別される. $a_{n+1} = 1$ となる部分を $\mathbb{P}^n$ の**アフィン部分**といい, $\mathbb{A}^n$ で表す. アフィン部分は, K^n と同じ表記になるため, $[a_1, \cdots, a_n, 1]$ を $(a_1, \cdots, a_n)$ と表すこともある. また, $a_{n+1} = 0$ となる元を**無限遠点**とよぶ. これら無限遠点たちは, 1 つ次元の低い射影空間を表している. ゆえに, $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$ とかける.

射影空間を考えるときには, 射影した後のアフィン部分と全体 $\mathbb{P}^n$ を行き来することが多い. このとき, アフィン部分を小文字 $(a_1, \cdots, a_n)$ (例えば, $n = 2$ の場合は (x, y)), 全体 $\mathbb{P}^n$ の元を大文字 $[A_1, \cdots, A_{n+1}]$ (例えば, $n = 2$ の場合は $[X, Y, Z]$) で表す. これらの変換は単に, $a_i = \dfrac{A_i}{A_{n+1}}$ とすればよい. (逆は, $A_{n+1} = 1$ を代入すればよい.)

1.3 射影平面

以下, 簡単のため, 射影平面 $\mathbb{P}^2$ を考える.

$K[x, y]$ を, K の元を係数とする 2 変数 x, y の多項式全体の集合とする (多項式環). このとき, $f(x, y) \in K[x, y]$ をとれば, $f(x, y) = 0$ はアフィン空間 $\mathbb{A}^2$ において, ある曲線 (**代数曲線**) を表している. さらに, $x = \dfrac{X}{Z}$ および $y = \dfrac{Y}{Z}$ とすることで, $F(X, Y, Z) = 0$ は射影平面内のある曲線 (**射影曲線**) を与えている. (Z^d をかけることで, $F(X, Y, Z) \in K[X, Y, Z]$ であり, 各項の次数は一定である. このような多項式を**斉次**な多項式という. $d = \deg f(x, y)$.) ここで, $F(ta, tb, tc) = t^d F(a, b, c)$ が成り立っていることに注意する. (射影平面では, 原点を通る同一直線上の点を同一視したわけだが, この等式によって, 射影平面内の “同じ点” はきちんと同じ曲線上に乗っていることがわかる.)

– 同次化 $f \rightsquigarrow F$: $x = \dfrac{X}{Z}, y = \dfrac{Y}{Z}$; – 非同次化 $F \rightsquigarrow f$: $Z = 1$

(非同次化は, 変数 Z 以外でも可. つまり, $Y = 1$ によって非同次化するときもある.)

[*4] 射影空間はベクトル空間ではない.

1.3.1 ユークリッド幾何学との対比

射影平面における直線は, $f(x,y)=ax+by+c=0$ (ただし, $(a,b,c)\neq(0,0,0)$) と表すことができる. また, $(a,b)=(0,0)$ のときは $Z=0$ を表すが, これも**無限遠直線** (つまり, 無限遠点全体の集合) とよび, 直線とする.

ここでは, ユークリッド幾何学と比較して, 次の 2 つについて確認する:

① 異なる 2 点を通る直線がただ 1 つひける;
② 異なる 2 直線は, 必ずちょうど 1 点で交わる (平行線が存在しない!).

① 異なる 2 点 $\mathcal{P}_1,\mathcal{P}_2$ を通る直線がただ 1 つひける.

(i) 代数的な説明

$\mathcal{P}_1$ および $\mathcal{P}_2$ を通る直線を $F(X,Y,Z)=aX+bY+cZ=0$ とおく. このとき, 文字 3 つ (a,b,c), 式 2 つ ($\mathcal{P}_1,\mathcal{P}_2$ を代入) の連立方程式を得る. $\mathcal{P}_1$ および $\mathcal{P}_2$ は $\mathbb{P}^2$ における異なる点, つまり, K^3 内の同一直線上にはないから, 一次独立である. したがって, この連立方程式の解空間は 1 次元である; つまり, $(a,b,c)=t(a_1,b_1,c_1)$ と表せる. $F(X,Y,Z)=0$ はスカラー倍で同じ直線を表すから, $t=1$ としてよい. ゆえに, ただ 1 つの直線を得る.

(ii) 幾何的な説明

2 点 $\mathcal{P}_1$ および $\mathcal{P}_2$ は, K^3 内では原点を通る異なる直線である. よって, 2 直線を通る平面をただ 1 つとることができ, それは $\mathbb{P}^2$ 内では直線である.

② 異なる 2 直線 $f_1(x,y)=a_1x+b_1y+c_1=0, f_2(x,y)=a_2x+b_2y+c_2=0$ は, 必ずちょうど 1 点で交わる.

(i) 2 直線 $f_1(x,y)=0$ および $f_2(x,y)=0$ がアフィン部分で交わるとする. このとき, その交点は 1 つだが, 特に, $\begin{pmatrix}a_1 & a_2\\ b_1 & b_2\end{pmatrix}$ は正則である[*5]. したがって, $Z=0$ 上での交点は $[0,0,0]$ のみだから, アフィン部分以外での交点はない.

(ii) 2 直線 $f_1(x,y)=0$ および $f_2(x,y)=0$ がアフィン部分で平行とする. このとき, (必要であれば番号付けを取り替えて) ある $t\in K$ によって, $a_2=ta_1, b_2=tb_1$ とかける. ($f_1=0$ および $f_2=0$ は異なる直線だから, $c_2\neq tc_1$ である.) ここで, $(a_1,b_1)=(0,0)$ ならば, $(a_2,b_2)=(0,0)$ となり, $f_1=0$ も $f_2=0$ も無限遠直線となってしまうことに注意する; そこで, $(a_1,b_1)\neq(0,0)$ してよい.

[*5] 横ベクトルを使っているため, 行列はベクトルの右からかける.

$Z=0$ における交点を考える. 連立方程式 $(X,Y)\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} = (0,0)$ の解空間は 1 次元だから, $(X,Y) = t(b_1,-a_1)$ $(t \in K)$ とかける. よって, $F_1 = 0$ および $F_2 = 0$ は無限遠点 $[b_1,-a_1,0]$ でのみ交わる.

1.3.2 接線

射影平面における接線 (接平面) について, 公式を与える.

定理 1.2. 同次多項式 $F_(X,Y,Z)$ に対して, 曲線 $F=0$ の点 $[a,b,c]$ における接線の方程式は, 次で与えられる:

$$F_X(a,b,c)X + F_Y(a,b,c)Y + F_Z(a,b,c)Z = 0.$$

まず, $F(X,Y,Z)$ のそれぞれの偏微分を用いて, 点 $[a,b,c]$ における接平面は次で与えられた (解析学 I, II?):

$$F_X(a,b,c)(X-a) + F_Y(a,b,c)(Y-b) + F_Z(a,b,c)(Z-c) = 0.$$

このとき, $F_X(a,b,c)a + F_Y(a,b,c)b + F_Z(a,b,c)c = 0$ であることを示そう.

それぞれの項だけを考えればよいので, $F(X,Y,Z) = X^iY^jZ^k$ $(i+j+k = \text{一定})$ としてよい. よって,

$$\begin{cases} F_X = iX^{i-1}Y^jZ^k \\ F_Y = jX^iY^{j-1}Z^k \\ F_Z = kX^iY^jZ^{k-1} \end{cases}$$

だから,

$$(\text{与式}) = ia^ib^jc^k + ja^ib^jc^k + ka^ib^jc^k = (i+j+k)F(a,b,c) = 0$$

を得る.

ちなみに, 上では次の一般形を示していることに注意する.

命題 1.3. d 次の斉次多項式 $F(X,Y,Z)$ について, 次が成り立つ:

$$F_X(X,Y,Z)X + F_Y(X,Y,Z)Y + F_Z(X,Y,Z)Z = dF(X,Y,Z).$$

2 ベズーの定理とケーリー・バカラックの定理

教科書 p.20 において, 次のベズーの定理について学んだ. (以下, 3 次曲線はすべて非特異とする.)

定理 2.1 (ベズー)**.** 3 次曲線 C_1 および C_2 が共通部分をもたないならば, その交点数はちょうど 9 点である.

(一般形) m 次曲線 C_1 および n 次曲線 C_2 が共通部分をもたないならば, その交点数はちょうど mn である.

ここで, 曲線 C_1 および C_2 が**共通部分をもつ**とは, $C_1 : F_1(X,Y,Z) = 0$ および $C_2 : F_2(X,Y,Z) = 0$ に対して, F_1 および F_2 を $\mathbb{C}$ 上 3 変数の多項式環 $\mathbb{C}[X,Y,Z]$ (一意分解整域) の元とみたとき, 共通の (定数でない) 因子をもつときにいう.

また, ベズーの定理を理解するためには,

– $\mathbb{C}$ (代数閉体) の中; – 射影平面 (無限遠点); – 重解

を考慮しなければいけないことに注意する.

このベズーの定理を用いて, 次の重要な定理 (系) を学んだ.

定理 2.2 (ケーリー・バカラック)**.** 3 次曲線 C_1 および C_2 が 9 つの点で交わっているとする. このとき, そのうちの 8 点をもつ 3 次曲線 C は, 残りの 1 点も通る.

この定理について, 教科書では感覚的な証明で済ませた. つまり, 8 点をもつ 3 次曲線 $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$ を決定するためには, 8 つの式からなる (a〜j の)10 元 (1 次) 連立方程式を解けばよい. 文字 10 個と式 8 つだから, その解空間は 2 次元 (= 文字数 − rank) であり, 曲線 C_1 および C_2 が与える式 f_1 および f_2 は一次独立 (よって基底) となるから, $f = af_1 + bf_2$ とかけ, 結果的に, f は最後の 9 点目をもつ.

しかし, この 8 つの式が一次独立性を導く (つまり, rank = 8) であることはまったく自明ではない! (教科書付録 A でも, 読者に委ねられているが...) そこで, 以下に証明を与えることにする. (教科書の筆者が念頭においている証明とは異なるかもしれない.)

2.1 ケーリー・バカラックの定理の証明

C_1 および C_2 を (共通部分のない) 3 次曲線とし, それぞれ $F_1(X,Y,Z) = 0$, $F_2(X,Y,Z) = 0$ で表す ($F_1, F_2 \in \mathbb{C}[X,Y,Z]$: 有理的は仮定しない). また, C_1 および C_2 の 9 つの交点を $P_1, \cdots, P_9$ とする.

3 次曲線 $C : F(X,Y,Z) = 0$ が, 9 つの交点のうち, 8 点 $P_1, \cdots, P_8$ をもつとしよう.

以下, 背理法を用いる: 「F は F_1 および F_2 の一次結合ではかけない」と仮定する.

(0) 任意の 2 点 A, B が与えられたとき, A, B を通る非自明な (恒等的に零でない) 3 次曲

線 $G = aF + bF_1 + cF_2 = 0$ が存在する.

文字 3 個, 式 2 つが与えらえるから, 非自明解 (a, b, c) を取ることができる. さらに, これによって $aF + bF_1 + cF_2 = 0$ (恒等的) とすると, 背理法の仮定に反す. (3 次曲線は非零なスカラー倍で同一の曲線を表すことに注意する.)

(1) $P_1, \cdots, P_9$ のうち, 4 点が同一直線上に並ぶことはない.

もし, ある 4 点が同一直線 ℓ 上に並ぶと, ℓ は C_1 および C_2 とそれぞれ 4 つの交点をもつことになる. ℓ および C_1 に対してベズーの定理を適用すると, ℓ (1 次式) は C_1 (F_1) をわり切る. 同様に, ℓ は C_2 もわり切り, 結果的に, C_1 および C_2 が共通部分をもたないことに矛盾する.

(2) $P_1, \cdots, P_9$ のうちの 5 点は, ただ一つの 2 次曲線を決定する.

(存在) 2 次曲線 $g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$ は a〜f (6 文字) を与えることで決定される. よって, 5 点を与えれば, 少なくても一つの非自明解 $(a, \ldots, f)$ を得る.
(一意) $D : g = 0$ および $D' : g' = 0$ を与えられた 5 点を通る 2 次曲線とする. D および D' にベズーの定理を適用すると, D と D' (2 次式) は共通部分をもたなければいけない. それが 1 次式, つまり, 直線 ℓ であるときを考えよう (そうでなければ自動的に $D = D'$). (1) より, 与えられた 5 点のうちの 4 点が同一直線上に並ぶことはないから, ℓ に乗る点は高々 3 点である. したがって, 残りの 2 点は D および D' の ℓ に関する余因子上にあるが, (異なる) 2 点を結ぶ直線は一意的に決まるため, その余因子は等しい; つまり, $D = D'$.

(3) $P_1, \cdots, P_8$ のうち, 3 点が同一直線上に並ぶことはない.

P_1, P_2, P_3 が同一直線 ℓ 上に並んだと仮定しよう; (1) より, 残りの 5 点 $P_4, \cdots, P_8$ は ℓ 上に乗らず, (2) より, それらは 2 次曲線 D を一意的に定める. ここで, ℓ 上の別の点 Q, および, ℓ にも D にもない点 R を取る. (0) より, Q および R をもつ (非自明な) 3 次曲線 $C' : G = aF + bF_1 + cF_2 = 0$ が存在する. このとき, P_1, P_2, P_3, Q は C' 上にも ℓ 上にもあり, ベズーの定理より, ℓ (1 次式) は C' をわり切らなければいけない; 便宜上, $C' = \ell \times D'$ (D' は 2 次曲線) とかくことにしよう. 一方, $P_4, \cdots, P_8$ も C' 上にあるが ℓ 上にはないので, これらは D' 上に乗っている. ゆえに, (2) より,

$D' = D$ を得る; $C' = \ell \times D$. しかし, R は C' 上にあるはずだが, ℓ および D 上にない点として取ったので矛盾する.

(4) $P_1, \cdots, P_8$ のうち, 6 点が同一の 2 次曲線に乗ることはない.

$P_1, \cdots, P_6$ が 2 次曲線 D 上にあると仮定する; (3) より, D は既約である (1 次式に分解されない). また, 残りの 2 点 P_7 および P_8 で決まる唯一の直線を ℓ とする. ここで, Q を D 上の別の点, R を D および ℓ 上にない点として選ぶ. (0) より, Q および R をもつ (非自明な) 3 次曲線 $C' : G = aF + bF_1 + cF_2$ が存在する. このとき, $P_1, \cdots, P_6$ および Q の 7 点は C' 上にあり, ベズーの定理 (D と C') より, D と C' は共通部分をもつ. 一方, D は既約な 2 次曲線より, D が C' をわり切らなければいけない; 便宜上, $C' = D \times m$ (m は直線) とかく.
もし, P_7 と P_8 のうち少なくても 1 つが D 上にあるとすると, D と C_1 は 7 点で交わる. しかし, ベズーの定理より, D および C_1 は共通部分をもつことになり (よって, $D \mid C_1$), 同様に $D \mid C_2$, ゆえに C_1 および C_2 が共通部分をもち矛盾する.
よって, P_7 および P_8 は C' 上にあるが, D 上にはないので m 上にあることになる; したがって, $m = \ell$ を得る. しかし, C' 上のもう一点 R は D および ℓ 以外から取ったので, これに反する.

これで準備が整った (矛盾を導く).

今, P_1 および P_2 で決まる直線を ℓ, (2) のような $P_3, \cdots, P_7$ の 5 点で決まる 2 次曲線を D としよう. (3) より, D は既約である. さらに, (3) および (4) より, P_8 は ℓ 上にも D 上にもない.

ここで, もう 2 点 Q, R を, ℓ 上にあるが D 上にない点として取り, (0) のように Q, R をもつ (非自明な) 3 次曲線を $C' : G = aF + bF_1 + cF_2$ とおく. このとき, P_1, P_2, Q, R の 4 点は C' および ℓ の交点である. ベズーの定理より, C' および ℓ は共通部分をもち, よって, ℓ は C' をわり切る; 便宜上, $C' = \ell \times D'$ とかこう. (3) より, $P_3, \cdots, P_7$ のどの点も ℓ 上にない C' 上の点である. したがって, これらはすべて D' 上に乗る. (2) より, $D' = D$ を得る. しかし, P_8 は C' 上にあるはずだが, ℓ 上にも D 上にもないので矛盾する.

結果的に, F は F_1 および F_2 の一次結合 $F = aF_1 + bF_2$ でかけ, ゆえに, 第 9 の点 P_9 をもつことがわかる.

注意 2.3. 上で, 直線や曲線 $C : F(X, Y, Z) = 0, D : G(X, Y, Z) = 0, E : H(X, Y, Z) = 0$ に対して, しばしば「便宜上」$C = D \times E$ のようにかいた. これは実際には, 多項式で見

た $F = G \times H$ のことであり, 曲線の方で見ると $C = D \cup E$ のことである.

2.2 パップスの定理とパスカルの定理

(工事中)

3 3 次曲線からのワイエルシュトラス標準形

この節では, (有理的で非特異な) 3 次曲線 C

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

から出発し, そのワイエルシュトラスの標準形

$$y^2 = x^3 + Ax^2 + Bx + C$$

を求める手順における注意点を解説する [ST, 1.3 節].

ここで, $f(x,y) = 0$ の有理数解を求めることは, $F(X,Y,Z) = Z^3 f\left(\frac{X}{Z}, \frac{Y}{Z}\right) = 0$ の整数解を求めることと (ほぼ[*6]) 同値であったことを思い出そう. また, $F(X,Y,Z)$ は斉次 (各項の次数が一定) の多項式であることに注意する.

まず, (教科書にあるように) 軸をうまくとれば, 最初の 3 次曲線 $f(x,y) = 0$ は

$$xy^2 + (ax + b)y = cx^2 + dx + e \tag{3.1}$$

のように取り直すことができる. (最初に与えられた a たちとは異なることに注意する.) 実際, $F(X,Y,Z) = 0$ において,

(1) (変曲点[*7]でない[*8]) 有理点 $\mathcal{O}$ を適当に選び, そこでの接線 (接平面) ℓ と C との交点を $\mathcal{P}$ とおく. このとき, ℓ を XY 平面と選び直し, $\mathcal{O} := [1,0,0], \mathcal{P} := [0,1,0]$ とする.
(2) 点 $\mathcal{P}$ における C の接線 (接平面) m をひき, これを YZ 平面と選び直す. (ℓ と m の交差する直線が新しい Y 軸)
(3) 最後に, 点 $\mathcal{O}$ を通る ℓ ではない有理的な直線 (平面) n をとり, それを XZ 平面とする. (ℓ と n の交差が新しい X 軸, m と n の交差が新しい Z 軸)

[*6] 射影的に
[*7] 特異でない, 3 重解をもつ点
[*8] 変曲点の場合は (2) における接線 m を, $\mathcal{O}$ を通らない任意の直線としてとる.

㊟ この変換が**双有理変換** (有理式による操作で移り合う変換, したがって, 有理点の情報がほぼ[*9]遺伝する) であることは後述する (3.2 節).

次に, (教科書にしたがって) 両辺に x をかけてから変換 $xy \rightsquigarrow y$ を施すことで次を得る:

$$y^2 + (ax+b)y = cx^3 + dx^2 + ex. \tag{3.2}$$

これは双有理変換ではあるが, 曲線 (3.1) および曲線 (3.2) の間で有理点の情報がどのくらい変わるのかを観察してみよう.

曲線 (3.1) および曲線 (3.2) 上の有理点全体の集合をそれぞれ, E_1 および E_2 とおく. このとき, 写像 $f : E_1 \setminus \{x=0\} \to E_2 \setminus \{x=0\}$ $((x,y) \mapsto (x, xy)$ が全単射を与えることは容易にわかる. つまり, 両者の有理点の違いは $x=0$ 上で出てくる: $X=0$ を代入して,

$$\begin{aligned} &(3.1) \quad bYZ^2 = eZ^3 \\ &(3.2) \quad Y^2Z + bYZ^2 = 0 \end{aligned}$$

(1) $b \neq 0$ のとき:

- (3.1) の解: $[0,1,0]$ (2 重解), $\left[0, \frac{e}{b}, 1\right]$
- (3.2) の解: $[0,1,0]$, $[0,0,1]$, $[0,-b,1]$

(2) $b = 0$ のとき:

- (3.1) の解: $[0,1,0]$ (3 重解)
- (3.2) の解: $[0,1,0]$ (2 重解), $[0,0,1]$

このように, 多少の違いは見られるが, 点の個数 (特に有限性) については何ら変化がないことがわかる (付随する群についてはこれから勉強?).

さらに, 変換 $(x,y) \rightsquigarrow \left(x, y - \frac{1}{2}(ax+b)\right)$ を施せば,

$$y^2 = \lambda x^3 + \alpha x^2 + \beta x + \gamma \tag{3.3}$$

を得ることができる. (この変換は, 有理数による回転と拡大縮小だから, 有理点の情報が完全に一致することは簡単にわかるだろう.)

最後に, 変換 $(x,y) \rightsquigarrow (\lambda x, \lambda^2 y)$ によって, ワイエルシュトラスの標準形

$$y^2 = x^3 + Ax^2 + Bx + C$$

を得ることができる. (これでも有理点の情報は不変.)

[*9] 有限個の点を除いて

しかしここで, 重要な点を見逃してはいないだろうか? それは, 「$\lambda \neq 0$ か?」ということである. (もちろん, $\lambda = 0$ ならばこの変換で曲線が潰れてしまうし, そもそも (3.3) は 2 次の曲線になってしまう.)

そこで, λ について辿っていくと, λ は (3.1) における c であることがわかる. さらに遡って, 最初の曲線 $f(x, y) = 0$ との関係を知りたいが, (軸の変換は厄介なので) ここでは $c \neq 0$ であることを見ることにする. このとき重要なことは, 「軸の変換で非特異であることは変わらない」という事実である. (特異点とは, いわゆる "尖った点" なので, 軸を取り替えてもその性質が変わらないことは何となくわかるかもしれない.)

今, (3.1) の同次形を (改めて)

$$F(X, Y, Z) = XY^2 + aXYZ + bYZ^2 - cX^2Z - dXZ^2 - eZ^3 = 0$$

とおく. このとき,

$$\begin{cases} F_X(X, Y, Z) = Y^2 + aYZ - 2cXZ - dZ^2 \\ F_Y(X, Y, Z) = 2XY + aXZ + bZ^2 \\ F_Z(X, Y, Z) = aXY + 2bYZ - cX^2 - 2dXZ - 3eZ^2 \end{cases}$$

となるが, $c = 0$ とすると点 $[1, 0, 0]$ は特異点, ゆえに, $c \neq 0$ でなければいけない.

注意 3.1. 有理的という条件を無視すれば, 3 次曲線 $f(x, y) = 0$ を線形な変換のみを用いて, 標準形にすることができる (Dropbox [2023 年度] `weierstrass_form.pdf` を参照).

注意 3.2. 基礎体を $\mathbb{Q}$ から一般の体 K に変えても同様に標準形を得ることができる. このとき, K の標数が $2, 3$ とそれ以外で少し形が異なることに注意が必要である.

3.1 例 $u^3 + v^3 = \alpha$

3 次曲線 $C : u^3 + v^3 = \alpha$ (αは零でない有理数[*10]) を見てみよう. ここで, その同次形を $F(U, V, W) = U^3 + V^3 - \alpha W^3 = 0$ とし, $\mathcal{O} := [1, -1, 0]$ とする. ($\mathcal{O}$ は変曲点であることに注意する.)

まず, それぞれの偏微分を計算しておく:

$$\begin{cases} F_U(U, V, W) = 3U^2 \\ F_V(U, V, W) = 3V^2 \\ F_W(U, V, W) = -3\alpha W^2 \end{cases}$$

[*10] $\alpha = 0$ ならば, 特異点 $[0, 0, 1]$ をもつ.

(1) $\mathcal{O}$ における C の接線 ℓ は $3U+3V=0 \rightsquigarrow U+V=0$ (XY 平面) である.
(2) 直線 m として, $\mathcal{O}$ を通らない直線 $U-V=0$ (YZ 平面) をとる.
(3) 直線 n として, $\mathcal{O}$ を通る直線 $W=0$ (XZ 平面) をとる.

このとき, 新しい軸として,

$$\begin{cases} X \text{ 軸} = [1,-1,0] \ (\ell \text{ と } n \text{ の共通部分}) \\ Y \text{ 軸} = [0,0,1] \ (\ell \text{ と } m \text{ の共通部分}) \\ Z \text{ 軸} = [1,1,0] \ (m \text{ と } n \text{ の共通部分}) \end{cases}$$

がとれるが, それぞれが XYZ 空間で $[1,0,0],[0,1,0],[0,0,1]$ となるので, 対応する基底変換の行列は,

$$\begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \end{pmatrix}$$

で与えられる[*11]. よって, UVW 空間の点 $[U,V,W]$ は XYZ 空間の点

$$[X,Y,Z] = \left[\frac{1}{2}U - \frac{1}{2}V, W, \frac{1}{2}U + \frac{1}{2}V\right]$$

へ移る. したがって, 3 次曲線 $F(U,V,W)$ は,

$$F(X,Y,Z) = 6X^2Z + 2Z^3 - \alpha Y^3$$

と表される. ここで,

① x と y の入れ替え　　② 変換 $x \rightsquigarrow \frac{1}{6}\alpha x,\ y \rightsquigarrow \left(\frac{1}{6}\alpha\right)^2 y$

を施せば, ワイエルシュトラスの標準形

$$y^2 = x^3 - \frac{432}{\alpha^4}$$

を得る. (教科書と少し違う.)

最後に, 微調整して教科書の表記に揃えよう. 次の変換を施す:

$$[X,Y,Z] \rightsquigarrow \left[X, \frac{1}{\alpha}Y, \alpha^2 Z\right].$$

これによって,

$$y^2 = x^3 - 432\alpha^2$$

[*11] 横ベクトルを用いているので, 行列はベクトルの右からかける.

を得ることができる.

さて, この変換を最初から最後まで辿ることで, 実際の変換 $u \rightsquigarrow x, v \rightsquigarrow y$ を観察する.

(1) 軸の変換

$$\begin{cases} X = \dfrac{1}{2}U - \dfrac{1}{2}V \\ Y = W \\ Z = \dfrac{1}{2}U + \dfrac{1}{2}V \end{cases}$$

(2) X と Y の入れ替え

$$\begin{cases} X = W \\ Y = \dfrac{1}{2}U - \dfrac{1}{2}V \\ Z = \dfrac{1}{2}U + \dfrac{1}{2}V \end{cases}$$

(3) x^3 の係数の調整 $\rightsquigarrow$ ワイエルシュトラスの標準形パート 1

$$\begin{cases} \dfrac{1}{6}\alpha X = W \\ \dfrac{1}{36}\alpha^2 Y = \dfrac{1}{2}U - \dfrac{1}{2}V \\ Z = \dfrac{1}{2}U + \dfrac{1}{2}V \end{cases}$$

(4) 定数項の調整 $\rightsquigarrow$ ワイエルシュトラスの標準形パート 2

$$\begin{cases} \dfrac{1}{6}\alpha X = W \\ \dfrac{1}{36}\alpha^2 \cdot \dfrac{1}{\alpha} Y = \dfrac{1}{2}U - \dfrac{1}{2}V \\ \alpha^2 Z = \dfrac{1}{2}U + \dfrac{1}{2}V \end{cases}$$

したがって,

$$\begin{cases} X = \dfrac{6}{\alpha}W \\ Y = \dfrac{18}{\alpha}(U - V) \\ Z = \dfrac{1}{2\alpha^2}(U + V) \end{cases}$$

となるが, 射影して ($W=1$ および $X/Z, Y/Z$)

$$\begin{cases} x = \dfrac{12\alpha}{u+v} \\ y = 36\alpha\dfrac{u-v}{u+v} \end{cases}$$

を得る.

注意 3.3. 今回は**たまたま**教科書と同じ標準形を得ることができたが, 軸の取り方によってはもちろん, 異なる標準形が出る. (実際にやってみよう (♠))

3.1.1 変換から軸を見る

上記で実際に変換を一つ一つ与えることで, $u^3+v^3=\alpha$ からワイエスシュトラスの標準形 $y^2=x^3-432\alpha^2$, および, その変換の方法 $(u,v) \rightsquigarrow (x,y) = \left(\dfrac{12\alpha}{u+v}, 36\alpha\dfrac{u-v}{u+v}\right)$ を得ることができた. ここではその逆に, 変換方法から軸の取り換えの様子を観察できることを見てみよう.

変換の方法を同次形で表すと,

$$[X,Y,Z] = \left[\frac{6}{\alpha}W, \frac{18}{\alpha}(U-V), \frac{1}{2\alpha^2}(U+V)\right]$$

となる. このとき, 基底変換の行列 $[U,V,W] \rightsquigarrow [X,Y,Z]$ は

$$\begin{pmatrix} 0 & \dfrac{18}{\alpha} & \dfrac{1}{2\alpha^2} \\ 0 & -\dfrac{18}{\alpha} & \dfrac{1}{2\alpha^2} \\ \dfrac{6}{\alpha} & 0 & 0 \end{pmatrix}$$

となることがわかる. 逆行列を取れば ($[X,Y,Z] \rightsquigarrow [U,V,W]$),

$$\begin{pmatrix} 0 & 0 & \dfrac{\alpha}{6} \\ \dfrac{\alpha}{36} & -\dfrac{\alpha}{36} & 0 \\ \alpha^2 & \alpha^2 & 0 \end{pmatrix}$$

となり, よって, UVW 空間での新しい軸が

$$\begin{cases} X \text{ 軸} = \left[0, 0, \dfrac{\alpha}{6}\right] = [0,0,1] \\ Y \text{ 軸} = \left[\dfrac{\alpha}{36}, -\dfrac{\alpha}{36}, 0\right] = [1,-1,0] \\ Z \text{ 軸} = \left[\alpha^2, \alpha^2, 0\right] = [1,1,0] \end{cases}$$

であることがわかる. (途中で X 軸と Y 軸の入れ替えを行っている関係で, その箇所がひっくり返っているが, 冒頭の軸の取り方と一致している.)

3.1.2 有理数解の変化

ワイエスシュトラスの標準形への変換によって, 楕円曲線上の有理点の情報は変わってしまう. しかし, その変換によって, 有理点の情報が実はほぼ変わっていないことを観察する. ここで, 上で見たように, その変換は有理関数で与えられているため, 対応する点が有理数であること自体は変化していないことに気をつける.

$C := \{(u,v) \in \mathbb{Q}^2 \mid u^3 + v^3 = \alpha\}$ および $D := \{(x,y) \in \mathbb{Q}^2 \mid y^2 = x^3 - 432\alpha^2\}$ とおく. 変換の式は次で与えられている:

$$- \ C \rightsquigarrow D : \ x = \frac{12\alpha}{u+v}, y = 36\alpha\frac{u-v}{u+v}; \qquad - \ D \rightsquigarrow C : \ u = \frac{36\alpha + y}{6x}, v = \frac{36\alpha - y}{6x}$$

したがって, $u + v \neq 0$ および $x \neq 0$ の間では, C と D の間に全単射があることがわかる. よって, さらに関係式 $u + v = 0$ および $x = 0$ をそれぞれ満たす箇所を見てみる:

① $C' = \{(u,v) \in C \mid u + v = 0\}$

$u + v = 0$ は 1 次式だから, ベズーの定理より, C との交点は 3 点である. 実際,

$$C' = \{[1, -1, 0] \ (3 \text{ 重解})\}$$

② $D' := \{(x,y) \in D \mid x = 0\}$

同様に, $x = 0$ (同次形 $X = 0$) と D (同次形 $Y^2Z = X^3 - 432\alpha^2Z^3$) との交点数は 3 である. 実際,

① $[0, \pm 12\sqrt{-3}|\alpha|, 1]$ (複素点 2 つ) ② $[0, 1, 0]$ (無限遠点)

よって,

$$D' = \{[0, 1, 0]\}$$

このように, C および D の間には, 有限個の点を除いて, 有理数解に 1 対 1 の対応がある. (したがって, C および D の有理点たちの情報はほぼ一致し, どちらを眺めてもよいことになる.)

一方, 楕円曲線に付随する加法群については, 和の定義 (直線) が変換の仕方で変わるため, 明らかではない. (が, 一致するということを今後勉強?)

3.1.3 $\alpha = 0$ の場合

$\alpha = 0$ の場合, つまり, $u^3 + v^3 = 0$ について観察してみよう. これは, $(u+v)(u^2 - uv + v^2) = 0$ と因数分解できるため, 有理点を調べるためには $u+v = 0$ および $u^2 - uv + v^2 = 0$ のそれぞれを見ればよい. 特に, 後者の有理点 (さらに実点) は $[0, 0, 1]$ のみである.

3.2 軸の取り換えが双有理変換であること

ここでは, 上でやり残していた問題「軸の取り換えは双有理変換である」ことを確かめる. ポイントは次の 2 点である:

① 変換の際に取った新しい点 $\mathcal{O}, \mathcal{P}$ およびもう 1 点 $\mathcal{Q}$ は, (K^3 内で) 一次独立である;
② それら 3 点は有理点である.

これらにより, $\mathcal{O}, \mathcal{P}, \mathcal{Q}$ は K^3 の基底をなし, 基底変換の行列が有理数成分で与えられることがわかる. よって, 新しい座標 $[X, Y, Z]$ はもとの座標の有理数倍の和で表示できる.

以下, $C : f(x, y) = 0$ を有理的な非特異 3 次曲線とし, C 上の有理点 $\mathcal{O}$ をとる.

3.2.1 点 $\mathcal{O}$ が変曲点でない場合

点 $\mathcal{O}$ が変曲点でないと仮定する.

点 $\mathcal{O}$ における C の接線 ℓ は有理的だから, C との 3 交点 $\mathcal{O}, \mathcal{O}, \mathcal{P}$ もすべて有理的である. ここで, $\mathcal{O}$ は変曲点ではないから, $\mathcal{O} \neq \mathcal{P}$ である. つまり, $\mathcal{O}$ および $\mathcal{P}$ は K^3 内で同一の直線上にはなく, それらは唯一の平面を張る (それが ℓ). また, 点 $\mathcal{P}$ における C の接線 m は ℓ と一致しない (一致したら, 4 交点 $\mathcal{O}, \mathcal{O}, \mathcal{P}, \mathcal{P}$ をもってしまうから). 点 $\mathcal{O}$ を通る ℓ ではない有理的な直線を n とすると, m との交点 $\mathcal{Q}$ もまた, 有理点である.

このとき, $\mathcal{O}, \mathcal{P}, \mathcal{Q}$ が一次独立でないということは, $\mathcal{Q}$ が $\mathcal{O}$ および $\mathcal{P}$ で張られる平面 ℓ に属していることを意味し, それは $\ell = n$ であることを導く. よって, $\mathcal{O}, \mathcal{P}, \mathcal{Q}$ は K^3 で一次独立である.

3.2.2 点 $\mathcal{O}$ が変曲点の場合

上と同様に議論すればよい (♠).

4　特異 3 次曲線

ここでは, 特異 3 次曲線について議論する [ST, 3.7 節, 問題 3.13, 3.14, 3.15].

以下, $C : y^2 = x^3 + ax^2 + bx + c$ $(=: g(x)$[*12]$)$ を有理的な 3 次曲線[*13]とする. (いつものように, $C : f(x, y) = 0$ とも表す.) また, 同次形 $F(X, Y, Z) = Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3$ の偏微分を計算しておく:

$$\begin{cases} F_X(X, Y, Z) = -3X^2 - 2aXZ - bZ^2 \\ F_Y(X, Y, Z) = 2YZ \\ F_Z(X, Y, Z) = Y^2 - aX^2 - 2bXZ - 3cZ^2 \end{cases}$$

(実際には, アフィン部分 $Z = 1$ の特異点[*14]を見るため, $f(x, y)$ の偏微分で十分[*15].)

このとき, 教科書で次を学んだ.

命題 4.1. 点 $\mathcal{P} := (x_0, y_0)$ が C の特異点であることと $x = x_0$ は方程式 $g(x) = 0$ の重解かつ $y_0 = 0$ であることは同値である. さらにこのとき, x_0 は有理数となる.

復習のため, その証明を残す.

証明. 点 $\mathcal{P}$ が C の特異点であると仮定する. このとき, $f_y(x_0, y_0) = 0$ より $y_0 = 0$ を得る; よって, $g(x_0) = 0$. さらに, g の微分 g' は ($\pm$ を無視して) $f_x(x, y)$ と一致することに気をつければ, $g'(x_0) = f_x(x_0, y_0) = 0$ を得る. したがって, $x = x_0$ は $g(x) = 0$ の重解である[*16]. 逆も同様である.

次に, x_0 が有理数であることを示そう. まず, $x = x_0$ は $g'(x) = 3x^2 + 2ax + b = 0$ の解であるから, $x_0 = \dfrac{-a \pm \sqrt{a^2 - 3b}}{3}$ (どちらか一方). 「余りつきわり算 $g(x) \div g'(x)$」を考えると,

$$g(x) = g'(x)p(x) + \left(-\frac{2}{9}a^2 + \frac{2}{3}b\right)x + \left(c - \frac{1}{9}ab\right)$$

となるから, $\left(-\dfrac{2}{9}a^2 + \dfrac{2}{3}b\right)x_0 + \left(c - \dfrac{1}{9}ab\right) = 0$ を得る. $-\dfrac{2}{9}a^2 + \dfrac{2}{3}b \neq 0$ であれば, すぐに x_0 は有理数であることがわかる. 一方, $-\dfrac{2}{9}a^2 + \dfrac{2}{3}b = 0$, つまり, $a^2 - 3b = 0$ で

[*12] 教科書と記号の置き方を変えていることに注意.

[*13] 変換で特異点をもつことは変わらないから, ワイエルシュトラスの標準形を考えれば十分である.

[*14] ワイエルシュトラスの標準形においては, 特異点はあってもアフィン部分にしかない (♠).

[*15] ちなみに, $F(a, b, 1) = F_X(a, b, 1) = F_Y(a, b, 1) = 0$ を満たす (a, b) は, 自動的に $F_Z(a, b, 1) = 0$ を満たす (♠) [ヒント: 命題 1.3].

[*16] 方程式 $g(x) = 0$ において, $x = x_0$ は重解である $\iff$ $g(x_0) = 0 = g'(x_0)$ (♠).

あれば, 上の x_0 の形から $x_0 = -\dfrac{a}{3}$ となり, どちらにしても x_0 は有理数である. □

さて, ここから (この節の最後まで) $\boxed{C \text{ は特異である}}$ と仮定する. 命題 4.1 より, その特異点を $\mathcal{P} = (x_0, 0)$ としよう.

注意 4.2. (教科書 1.2 節で学んだように) 非特異 3 次曲線の【有理点全体の集合】に, (加法の) 群構造 (つまり, アーベル群の構造) を入れることができた. そのときに重要なポイントは, 「すべての点で接線をひくことができる」ことだった. 特異曲線の場合, その特異点で接線をひくことはできないが, 特異点を除いたすべての点で接線をひくことはできる. したがって, 特異曲線の場合も【特異点を除いた有理点全体の集合】に (同じように) 群構造を入れることができる.

(教科書 1.3 節でも学んだように) 特異 3 次曲線は大きく分けて, 2 種類ある ($x_0 = 0$):

① $y^2 = x^3 + x^2$ ($\mathcal{P}$ で 2 重交差をもつ); ② $y^2 = x^3$ ($\mathcal{P}$ で尖点をもつ).

まずは, それぞれの特徴を観察してみよう.

① $C : y^2 = x^3 + x^2$

$x = 0$ 以外の原点を通る直線 $y = rx$ は, C と原点において 2 重に交差し, 他にもう 1 点の交点 $(r^2 - 1, r^3 - r)$ をもつ. また, $x = 0$ と C との 3 交点は, 原点 (2 重解) および $[0, 1, 0]$ (無限遠点) である. よって, C の有理点たちの情報は $\mathbb{Q}$ によって表せる:

$$\{C \text{ の有理点全体 }\} \longleftrightarrow \mathbb{Q}$$

$$(x, y) \longmapsto \begin{cases} \dfrac{y}{x} & (x \neq 0) \\ Z - Y & (x = 0) \end{cases}$$

$$\left.\begin{array}{ll} (r^2 - 1, r^3 - r) & (r \neq -1) \\ [0, 1, 0] & (r = -1) \end{array}\right\} \longmapsto r$$

これらは互いに逆の(ただの) 全単射写像であり, 付随する加法群の間の準同型を与えない! また, 付随する群を構成するためには, 上の左辺から「特異点を除く」必要がある. よって, 上の右辺にも不必要な 1 点がありそうである[*17]. 実は, 両辺から 1 点を取り除き (左辺からは特異点), “うまく” 写像を取り替えると群同型を構成することができる. 教科書では 3.7 節で勉強することだが, ここで紹介しておこう.

[*17] 可算無限集合から 1 点取り除いたところで可算無限だから, この説明は “感覚的” なものに過ぎないが.

特異点を除く 3 次曲線 C の有理点全体の集合を C_{ns} (加法群) で表し, $\mathbb{Q}^{\times} := \mathbb{Q} \setminus \{0\}$ (乗法群) とおく.

定理 4.3. 特異 3 次曲線 $C : y^2 = x^3 + x^2$ に対して, 次で定義される写像 $\phi : C_{\mathrm{ns}} \to \mathbb{Q}^{\times}$ は群の同型を与える:

$$\phi(\mathcal{P}) := \begin{cases} \dfrac{x-y}{x+y} & \mathcal{P} = (x, y); \\ 1 & \mathcal{P} = [0, 1, 0]. \end{cases}$$

さらに, その逆写像 $\psi : \mathbb{Q}^{\times} \to C_{\mathrm{ns}}$ は次で与えられる:

$$\psi(t) = \begin{cases} \left(\dfrac{4t}{(1-t)^2}, \dfrac{4t(1+t)}{(1-t)^3} \right) & t \neq 1; \\ [0, 1, 0] & t = 1. \end{cases}$$

② $y^2 = x^3$

$x = 0$ 以外の原点を通る直線 $y = tx$ は, C と原点において 2 回交わり, 他にもう 1 点の交点 (t^2, t^3) をもつ. また, $x = 0$ と C の交点 (3 つ) は, 原点 (2 重解) および $[0, 1, 0]$ (無限遠点) である. よって, 上の場合と同様に, C の有理点の情報は $\mathbb{Q}$ で表せる:

$$\{C \text{ の有理点全体 }\} \setminus \{(0,0)\} \longleftrightarrow \mathbb{Q}$$

$$(x, y) \longmapsto \begin{cases} \dfrac{y}{x} & (x \neq 0) \\ 0 & (x = 0) \end{cases}$$

$$\left.\begin{array}{ll} (t^2, t^3) & (t \neq 0) \\ [0, 1, 0] & (t = 0) \end{array}\right\} \longmapsto t$$

これらは互いに逆の全単射写像である. さらに実は, C に付随する群 C_{ns} および加法群 $\mathbb{Q}$ の間の同型を与えている. 以下で定理としてまとめておこう.

定理 4.4. 特異 3 次曲線 $C : y^2 = x^3$ に対して, 次で定義される写像 $\phi : C_{\mathrm{ns}} \to \mathbb{Q}$ は群の同型を与える:

$$\phi(\mathcal{P}) := \begin{cases} \dfrac{y}{x} & \mathcal{P} = (x, y); \\ 0 & \mathcal{P} = [0, 1, 0]. \end{cases}$$

さらに, その逆写像 $\psi : \mathbb{Q} \to C_{\mathrm{ns}}$ は次で与えられる:

$$\psi(t) = \begin{cases} (t^2, t^3) & t \neq 0; \\ [0, 1, 0] & t = 0. \end{cases}$$

上のように, 特異 3 次曲線の有理点たちは非常に見つけやすい (解析しやすい) ことがわかるが, 一方で, その付随する群 C_{ns} はどちらも有限生成ではないことに注意する. (非特異 3 次曲線に付随する群は, 有限生成である [モーデルの定理].)

ここで, 加法群 $\mathbb{Q}$ および乗法群 $\mathbb{Q}^\times$ が無限生成であることを実際に確かめておく.

命題 4.5. 加法群 $\mathbb{Q}$ および乗法群 $\mathbb{Q}^\times$ は無限生成である.

証明. (i) 加法群 $\mathbb{Q}$ について

(背理法) $\mathbb{Q} = \langle a_1, \cdots, a_n \rangle$ とし, a_i (有理数) たちの分母の最小公倍数を m とおく. $\dfrac{1}{2m}$ は有理数だから, 生成元 $a_1, \cdots, a_n$ でかける:

$$\frac{1}{2m} = \sum_i m_i a_i \ (m_i \in \mathbb{Z}).$$

ここで, 両辺を m で払うと,

$$\frac{1}{2} = \sum_i m_i (a_i m)$$

となるが, $a_i m$ は整数だから右辺は整数である. 左辺と比べれば, これは明らかに矛盾.

(ii) 乗法群 $\mathbb{Q}^\times$ について

(背理法) $\mathbb{Q}^\times = \left\langle \dfrac{a_1}{b_1}, \cdots, \dfrac{a_n}{b_n} \right\rangle$ $(a_i, b_i \in \mathbb{Z})$ と仮定する. 逆元 (今の場合, 逆数) をとることもできるから, $b_i = 1$ としてよい. このとき, $x := \prod_i a_i + 1$ は a_i たちで生成されることはない.

実際, $x = \prod_i a_i^{m_i}$ とする. m_i は負の整数であることも考慮し, 番号を取り替えて, $1 \leq i \leq \ell$ で m_i は非負, $\ell < i \leq n$ で m_i は負とする. このとき,

$$x \cdot a_{\ell+1}^{-m_{\ell+1}} \cdots a_n^{-m_n} = a_1^{m_1} \cdots a_\ell^{m_\ell}$$

となるが, x はどの a_i でもわることはできないから, $x = \pm 1$ を得る. もし $x = 1$ ならば, a_i のうちどれか 1 つは 0 となり, 矛盾する. もし $x = -1$ ならば, $\mathbb{Q}^\times$ は $-1, \pm 2$ のいずれかで生成されることになるが, これは明らかにおかしい.

(別証明) 上と同様に, $\mathbb{Q}^\times$ は (無限含め) いくつかの整数で生成されているとしてよい. 素因数分解を考えれば, $\mathbb{Q}^\times$ は素数で生成されることがわかる. 素数は無限個あるから, $\mathbb{Q}^\times$ は無限生成である[*18]. □

ここから, 【特異 3 次曲線は大きく 2 種類に分けられる】ことを見てみよう.

[*18] 生成元を変えれば有限個で収められる可能性を否定していないが, すぐにわかる.

(有理的な) 特異 3 次曲線 $C : y^2 = x^3 + ax^2 + bx + c$ $(=: g(x))$ について, $g(x) = 0$ は $x = x_0$ で重解をもったので, $g(x) = (x - x_0)^2(x - \alpha)$ のように因数分解できる. 命題 4.1 より, α も有理数である. そこで, 変換 $x \rightsquigarrow x + x_0$ (平行移動) を施せば,

$$C : y^2 = x^3 + Ax^2 \ (A \in \mathbb{Q})$$

となる. このとき, 付随する有理点の群 C_{ns} は不変であることに気を付けよう.

特異 3 次曲線の【2 種】とは, ① $A \neq 0$ または ② $A = 0$ のことであるが, 前者はさらに 2 つのタイプに分けられる:

(I) $A = B^2$ $(0 \neq B \in \mathbb{Q})$; (II) $\sqrt{A} \notin \mathbb{Q}$.

この分類は, 群 C_{ns} に関するものであるが, 特に, その群は

(I) 乗法群 $\mathbb{Q}^\times$ と同型;
(II) $K^\times$ $(:= K \setminus \{0\})$ のある部分群と同型. ここで, $K = \mathbb{Q}(\sqrt{A})$[*19]である.

となる.

4.1 タイプ (I)

ここでは, 特異 3 次曲線 $C : y^2 = x^3 + Ax^2$ に対して, $A = B^2$ $(0 \neq B \in \mathbb{Q})$ となる場合を考える. 早速, 上で考えたことと同様に, 定理を与える.

定理 4.6. 次の対応は, C_{ns} および $\mathbb{Q}^\times$ の間の互いに逆の群同型を与える:

$$\phi : C_{\mathrm{ns}} \to \mathbb{Q}^\times, \quad \phi(\mathcal{P}) = \begin{cases} \dfrac{y - \sqrt{A}x}{y + \sqrt{A}x} & \mathcal{P} = (x, y); \\ 1 & \mathcal{P} = [0, 1, 0]. \end{cases}$$

$$\psi : \mathbb{Q}^\times \to C_{\mathrm{ns}}, \quad \psi(t) = \begin{cases} \left(\dfrac{4At}{(1-t)^2}, \dfrac{4A\sqrt{A}t(1+t)}{(1-t)^3} \right) & t \neq 1; \\ [0, 1, 0] & t = 1. \end{cases}$$

(ここで, $\sqrt{A} \in \mathbb{Q}$ であることに気を付ける.)

この定理における ϕ および ψ が, 互いに逆の全単射写像になっていることは簡単にわかる. したがって, 証明すべきはこれらの写像が群の準同型であることのみである.

[*19] $\mathbb{Q}(\sqrt{A})$ とは, 有理数体 $\mathbb{Q}$ に $\sqrt{A}$ を添加した体, つまり, 有理数および $\sqrt{A}$ の四則演算すべてで得られる数からなる体である: 有理化を考えれば, $\mathbb{Q}(\sqrt{A}) = \{a + b\sqrt{A} \mid a, b \in \mathbb{Q}\}$.

4.2 タイプ (II)

次に, 特異 3 次曲線 $C : y^2 = x^3 + Ax^2$ に対して, A が有理数の平方でないとする.

準備として, 2 次曲線 (円錐曲線) $H : u^2 - Av^2 = 1$ (非特異) を考える. H の有理点全体の集合も (混乱がない限り) 同様に H で表す. ここで, ($\sqrt{A} \notin \mathbb{Q}$ より) H は無限遠点をもたないことに注意する.

次のように H に積を定義する: $(u_1, v_1), (u_2, v_2) \in H$ に対して,

$$(u_1, v_1) \cdot (u_2, v_2) := (u_1u_2 + Av_1v_2, u_1v_2 + u_2v_1).$$

このとき, H は積で閉じていること, および, $(1, 0)$ を単位元としてもつことは容易にわかる. また, $(u, v)^{-1} = (u, -v)$ である. 最後に, 結合律が成り立つことを確かめて (♠), H が群 (さらに, アーベル群) であることがわかる.

$K := \mathbb{Q}(\sqrt{A})$ とおく. このとき, H を K の言葉で書き直すことができる.

補題 4.7. 対応 $\varphi : (u, v) \mapsto u + \sqrt{A}v$ は, H から $K^\times$ への群の単射準同型を与える. さらに, H は無限生成である.

証明. 前半の主張は明らかである. この対応による $K^\times$ の部分群 $\operatorname{Im}\varphi = \{u+\sqrt{A}v \mid u^2 - Av^2 = 1\}$ も H で表すことにする.

後半の主張を示す. 次のような対応 $\pi : K^\times \to H$ を考える:

$$a + \sqrt{A}b \mapsto \frac{a + \sqrt{A}b}{a - \sqrt{A}b}.$$

この対応の行先が H に属していることはすぐにわかるから, これは写像である. さらに, これが群の準同型であること, および, $\operatorname{Ker}\pi = \mathbb{Q}^\times$ であることも簡単に確かめられる.

次に, π が全射であることを示す. $u + \sqrt{A}v \in H$ とする. このとき, $\pi(a + \sqrt{A}b) = u + \sqrt{A}v$ となる $a, b \in \mathbb{Q}$ を探したい. この式の分母を払ってからまとめることで, a, b に関する連立方程式

$$\begin{pmatrix} u-1 & -Av \\ v & -(u+1) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

を得る. 係数行列の行列式は 0 だから, この連立方程式は非自明解をもつ. それを a, b とすればよい.

最後に, H が無限生成であることを示そう. 準同型定理によって, $K^\times/\mathbb{Q}^\times \simeq H$ を得るが, これによって, H の元は $a + \sqrt{A}b$ $(a, b \in \mathbb{Z})$ によって代表されることがわかる; つ

まり, $K^\times$ の元を有理数倍で同一視する. 特に, それらは K の整数環 R[*20]に属している. (各元 $a+\sqrt{A}b$ の**ノルム** a^2-Ab^2 を考えれば) R の任意の元は, 有限個の既約元の積に分解できる[*21]から, H は R の既約元たちで生成される. しかし, R の既約元は無限個ある[*22]から, H は有限生成ではない[*23]. □

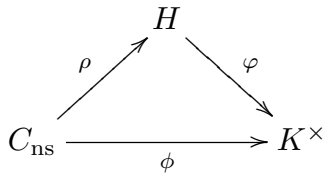
さて, ここから群 C_{ns} の話に戻ろう: $C: y^2=x^3+Ax^2$ ($\sqrt{A}\notin\mathbb{Q}$). 次が主定理である.

定理 4.8. (1) 次の対応は, C_{ns} および H の間の互いに逆の群同型を与える:

$$\rho: C_{\mathrm{ns}}\to H,\quad \rho(\mathcal{P})=\begin{cases}\left(\dfrac{y^2+Ax^2}{x^3},-\dfrac{2y}{x^2}\right) & \mathcal{P}=(x,y);\\ (1,0) & \mathcal{P}=[0,1,0].\end{cases}$$

$$\sigma: H\to C_{\mathrm{ns}},\quad \sigma(u,v)=\begin{cases}\left(\dfrac{2A}{u-1},-\dfrac{2A^2v}{(u-1)^2}\right) & (u,v)\neq(1,0);\\ [0,1,0] & (u,v)=(1,0).\end{cases}$$

(2) 次の可換図式が成り立つ:



ここで, ρ は (1), φ は補題 4.7, ϕ は次で与えられる:

$$\phi(\mathcal{P})=\begin{cases}\dfrac{y-\sqrt{A}x}{y+\sqrt{A}x} & \mathcal{P}=(x,y);\\ 1 & \mathcal{P}=[0,1,0].\end{cases}$$

[*20] ここではあまり深入りしないことにするが, A ($\neq 1$) を平方因子をもたない整数として,

$$\mathbb{Q}(\sqrt{A})\text{ の整数環}=\begin{cases}\mathbb{Z}[\sqrt{A}] & A\equiv 2,3 \pmod 4\\ \mathbb{Z}[\omega] & A\equiv 1 \pmod 4\end{cases}$$

とかける (定理 A.31). ここで, $\omega=\dfrac{1+\sqrt{A}}{2}$ である. また, $\mathbb{Q}(\sqrt{A})$ を変えずに, 平方因子をもたないように A を調整できることに注意する.

[*21] ネーター整域の任意の元は, 有限個の既約元の積に分解できる (定理 A.14). ただし, その分解は (可逆元倍と順序を無視しても) 一意的とは限らない (注意 A.15). 例えば, $\mathbb{Q}(\sqrt{A})$ の整数環はネーター整域である (定理 A.33).

[*22] 素数が無限個あることと同様に確かめられる.

[*23] 生成元を変えれば有限個で収められる可能性を否定していないが, すぐにわかる.

この定理における ρ および σ が, 互いに逆の全単射写像になっていることは容易にわかる. そのため, (2) の可換性を示すことができれば, 残る課題は ϕ の準同型性のみである.

定理 4.8(2) の証明. ガチ計算で示す. $\mathcal{P} = (x, y)$ とする.

$$\varphi\rho(x,y) = \frac{y^2 + Ax^2}{x^3} - \sqrt{A} \cdot \frac{2y}{x^2} = \frac{y^2 + Ax^2 - 2\sqrt{A}xy}{x^3} = \frac{(y - \sqrt{A}x)^2}{y^2 - Ax^2} = \phi(x,y)$$

$\mathcal{P}$ が無限遠点のときは明らか. よって, $\varphi\rho = \phi$ を得る. □

4.3 結論と課題

タイプ (I) および (II) を見比べてみると, (特異点を除いた) 有理点の群 C_{ns} が無限生成であること, および, その $\mathbb{Q}(\sqrt{A})^\times$ への埋め込みが同じように与えられていることがわかる. したがって, 特異 3 次曲線は大きく分けて 2 種類

① $y^2 = x^3 + x^2$ (原点で 2 重交差をもつ); ② $y^2 = x^3$ (原点で尖点をもつ)

しかないことを理解できる.

ただし, 次のことが課題として残っている.

課題 4.9. 上で与えた写像 ϕ はすべて, 群の準同型であることを確認せよ. (このとき, 他のすべての写像も自動的に群の準同型になる.)

付録 A 可換環

この節を通して, R を可換環とする[*24]. また, ここでいう**部分環**は, 単位元が一致しているものを指すことにする.

以降のところどころで, どうしても**加群論**を展開しなければいけない箇所があるため, ここで**簡単に**説明しておくことにする.

R **加群**とは, 体 K 上ベクトル空間の一般化である. ベクトル空間とは, たし算とスカラー (K) 倍ができる集合であった ($+\alpha$ でそれらをうまく扱うための公理がある). R 加

[*24] 以下では, 環論および体論の基礎がどうしても必要になる. できるだけ環論の初歩のみを既知として, 他はフォローするつもりであるが, 代数学特論 AI および AII の知識をもっているほうが望ましい. [雪, 三] を参考文献として挙げておく.

群も同じで, たし算とスカラー (R) 倍ができる集合である[*25][*26]. 例えば, $R = \mathbb{Z}$ のとき, $\mathbb{Z}$ 自身も $\mathbb{Z}$ 加群であり, その直和 $\mathbb{Z}^\ell$ も $\mathbb{Z}$ 加群である[*27] (数ベクトル空間のようなもの). また, R のイデアルは, R 自身を R 加群と見たときの部分 R 加群の典型的な例である.

(体という “ちょー良い” 環の影響で) 任意のベクトル空間は数ベクトル空間 K^ℓ と同型になった (その次元で決まる) が, R 加群ではそうはならない. 例えば, $R = \mathbb{Z}$ の場合, $\mathbb{Z}/n\mathbb{Z}$ も (自然に) $\mathbb{Z}$ 加群となるが, これは自由加群ではない. 実際, $\mathbb{Z}/n\mathbb{Z}$ の任意の元をスカラー n ($\in \mathbb{Z}$) 倍すると零になってしまうが, 自由加群ではそうはならない[*28]. このように, スカラー (R) の変更で, 加群構造はより複雑になる.

ベクトル空間における線型写像に対応する **R 加群としての準同型** *(R 準同型)* についても言及しておこう. これも同様で, たし算とスカラー倍を保存する写像と思えばよい: $f(x+y) = f(x) + f(y), f(\alpha x) = \alpha f(x)$.

もちろん, 加群論を実際に展開するためには, さらに気を付けなければいけないことや勉強しなければいけないことが多数あるが, このノートではこのくらいの認識で話を進めて問題ないだろう. (何かあれば, その都度フォローするつもりである.) 特に気になる読者は [雪] 等を参照されたい.

さて, ここから可換環論に話を戻す. まずは, 既約元および素元の定義を思い出すことから始める.

定義 A.1. $r \in R$ (零でも可逆元でもない) とする.

(1) r が**既約元**であるとは, $r = ab$ $(a, b \in R)$ ならば, a または b が可逆であるときにいう.
(2) r が**素元**であるとは, $r \mid ab$ $(a, b \in R)$ ならば, $r \mid a$ または $r \mid b$ となるときにいう.

簡単な事実を挙げておく (♠).

[*25] 非可換環上の加群を考える場合には, 左加群・右加群の区別が必要である. 可換環上の加群はそれらが一致するため, 単に加群とよぶ場合が多い.

[*26] (ここでは蛇足でしかないが) 小学校算数において, 3×4 か? 4×3 か?という議論がしばしば勃発する. 可換環 $\mathbb{Z}$ における積と思えば, それ ($3 \times 4 = 4 \times 3$) は当たり前なのかもしれないが, よく考えてみるとかけ算導入時には, 実は $\mathbb{Z}$ を (左?右?) $\mathbb{Z}$ 加群として考えている. なぜなら, もし $\mathbb{Z}$ における積として定義するなら, かけられる数およびかける数は同じ土俵 (同じ単位) であるはずだが, 【(1 かたまりの大きさ)×(かたまりの個数)】で定義しているため実際には異なる. しかし, $\mathbb{Z}$ は可換環のため左加群も右加群も一致し, その事実 ($3 \times 4 = 4 \times 3$) は変わらないのだが...

[*27] このような加群 R^ℓ を**自由 R 加群**という. このとき, この非負整数 ℓ をその**階数** *(**ランク**)* という. また, 自由加群の場合は, ベクトル空間と同様に**基底**が取れる (R **基底**とよぶ). $R^n \subseteq R^\ell$ のとき, $n \leq \ell$ となる. 証明は与えないが, 線型数学の延長でどうにかなるだろう. (ちょっと足りないか...)

[*28] 数学で度々使う**自由**という言葉は, 英語の *free* から来るが, “何でも OK” の自由ではなく, (バリアフリーやアルコールフリーのように)“ない” という意味である. 自由加群も, “関係式がない” という意味でフリーである. 自由加群でない $\mathbb{Z}$ 加群 $\mathbb{Z}/n\mathbb{Z}$ には, 関係式 $n = 0$ が入っている.

事実 A.2. (1) 整域における任意の素元は, 既約元である.
(2) 既約元 (素元) の可逆元倍はまた, 既約元 (素元) である.

次に, **素イデアル回避** *(Prime Avoidance)* という可換環論における有名な補題をここで与えておく.

補題 A.3 (素イデアル回避)**.** R のイデアル $\mathfrak{p}_1, \cdots, \mathfrak{p}_\ell$ $(\ell \geq 2)$ のうち, 素イデアルでないものは高々 2 つと仮定する. このとき, R のイデアル I が任意の番号 i で $I \not\subseteq \mathfrak{p}_i$ ならば, $I \not\subseteq \bigcup_i \mathfrak{p}_i$ となる[*29].

証明. $J := \bigcup_i \mathfrak{p}_i$ とおく. ℓ に関する帰納法で示す. $\ell = 2$ とする. 仮定より, $a_i \in I \setminus \mathfrak{p}_i$ となる元が存在する. $a_1 \notin \mathfrak{p}_2$ ならば a_1 が $\mathfrak{p}_1$ も $\mathfrak{p}_2$ も避けている[*30]元である: $a_1 \in I \setminus J$. よって, $a_1 \in \mathfrak{p}_2$ および $a_2 \in \mathfrak{p}_1$ としてよい. このとき, $a_1 + a_2 \in I$ だが $a_1 + a_2 \notin J$ である. 実際, $a_1 + a_2 \in \mathfrak{p}_1$ ($\mathfrak{p}_2$ でも同様) とすると, $a_2 \in \mathfrak{p}_1$ を仮定しているので, $a_1 \in \mathfrak{p}_1$ となってしまうが, これは a_1 の取り方に矛盾する.[*31]

$\ell > 2$ とする. 順番を入れ替えて, $\mathfrak{p}_i$ $(i \geq 3)$ は素イデアルとしてよい. 帰納法の仮定より, 各 i に対して (i 番目の $\mathfrak{p}_i$ を除けば $\ell - 1$ 個), 「$a_i \in I$ だが a_i は $\mathfrak{p}_i$ 以外をすべて避けている」ような元 $a_i \in R$ を取れる. どこかの番号 i で a_i が $\mathfrak{p}_i$ も避けていたら, $a_i \notin J$ となり終了. そこで, 任意の番号 i で $a_i \in \mathfrak{p}_i$ としてよい.

このとき, $a := a_\ell + a_1 \cdots a_{\ell-1}$ は I の元だが (こっちは当たり前), J に属さないことを示す. $1 \sim \ell - 1$ のある番号 i で $a \in \mathfrak{p}_i$ ならば, $a_1 \cdots \overset{\mathfrak{p}_i}{a_i} \cdots a_{\ell-1} \in \mathfrak{p}_i$ より, $a_\ell \in \mathfrak{p}_i$ となりダメ. したがって, $a \notin \mathfrak{p}_i$ $(i = 1, \cdots, \ell - 1)$. そこで, $a \in \mathfrak{p}_\ell$ と仮定しよう (矛盾を導くために). そうすると, $a_1 \cdots\cdots a_{\ell-1} \in \mathfrak{p}_\ell$ で, $\mathfrak{p}_\ell$ は素イデアルより, $1 \sim \ell - 1$ のある番号 i で $a_i \in \mathfrak{p}_\ell$ となるが, これは a_i の取り方からダメ. よって, $a \notin \mathfrak{p}_\ell$ となり, $a \notin J$. □

もう一つ, 可換環論における (ちょー有名で) 重要な事実である**中山の補題**を紹介する.

可換環 R のすべての極大イデアルの共通部分を *(***ヤコブソン***)* **根基**とよび, $\operatorname{rad} R$ で表す (明らかに R のイデアル). また, R の可逆元全体の集合を $R^\times$ とかく. まず, 次を示す.

補題 A.4. $\operatorname{rad} R = \{a \in R \mid$ 任意の $r \in R$ に対して, $1 - ar \in R^\times\}$.

[*29] すべての番号 i で $I \not\subseteq \mathfrak{p}_i$ なら明らかに結論が言えそうな感じもするが,「I がどこかの番号に跨いで入っている可能性」が残されている. 素イデアル回避はそれを否定している. (結構強い結論である.)

[*30] ここでは集合に属さないことを**避けている**と表現しよう.

[*31] ここまででは, 素イデアルという仮定は使っていない. つまり, 2 個までは何も仮定はいらず, これが「素でないイデアルは高々 2 つ」という仮定の意味である.

証明. $a \in \operatorname{rad} R, r \in R$ とする. R の任意の極大イデアル $\mathfrak{m}$ ($\mathfrak{m} \neq R$ に注意) に対して, $ar \in \operatorname{rad} R \subseteq \mathfrak{m}$, ゆえに $1 - ar \notin \mathfrak{m}$ となる. $\mathfrak{m}$ は任意の極大イデアルを取っていたので, 単項イデアル $(1 - ar)$ を含む極大イデアルが存在しないことがわかる. ツォルンの補題から, $(1 - ar) = R$, ゆえに $1 - ar \in R^\times$ を得る.

a を右辺の元とする. (背理法) $a \notin \operatorname{rad} R$ とすると, ある極大イデアル $\mathfrak{m}$ で $a \notin \mathfrak{m}$ となる. このとき, $\mathfrak{m} \subsetneq (a) + \mathfrak{m} \subseteq R$ より, $R = (a) + \mathfrak{m}$, ゆえに $1 = ar + m$ となる $r \in R$ および $m \in \mathfrak{m}$ が存在する. $1 - ar = m \in \mathfrak{m}$ より, $1 - ar$ は可逆でない. これは a の取り方に矛盾する. □

補題 A.5 (中山の補題)**.** I を可換環 R の有限生成イデアルとする. このとき, $I \cdot \operatorname{rad} R = I$ ならば, $I = (0)$ となる.

証明. (背理法) $I \neq (0)$ とする. I は有限生成より, $I = (a_1, \cdots, a_\ell)$ となる $a_i \in R$ を取れる. ここで, いずれかの a_i を抜いたら I にならないと仮定してよい. (不必要なものを除外しておけばよい. $I \neq (0)$ よりすべて抜くことはできない.) 仮定より, $a_\ell \in I = I \cdot \operatorname{rad} R$ だから, $a_\ell = \sum_i a_i x_i$ ($x_i \in \operatorname{rad} R$) とかける. したがって, $(1 - x_\ell) a_\ell = \sum_{j \neq \ell} a_j x_j$ となるが, 前補題より, $1 - x_\ell$ は可逆元であり, $a_\ell \in (a_1, \cdots, a_{\ell-1})$ となってしまう. これは生成元の個数を最小に取ったことに矛盾する. □

A.1 局所化

ここで, 局所化 ($\mathbb{Z} \rightsquigarrow \mathbb{Q}$ の一般化) について簡単にまとめておく. 感覚的には「約分込みの分数」を考えることで, もとの環を含む新しい環を作る操作である. もとの環の多くの性質が局所化で得られる環へ遺伝するので, 局所化を施して議論を帰着させることがよくある.

定義-定理 A.6. (1) 次の条件を満たす R の (ただの) 部分集合 Δ を**乗法的集合**という:

(i) $1 \in \Delta, 0 \notin \Delta$; (ii) $a, b \in \Delta \Rightarrow ab \in \Delta$.

(2) R の乗法的集合 Δ に対して, 直積集合 $R \times \Delta$ に次の関係を定義する:

$$(r, a) \sim (s, b) \overset{\text{def}}{\iff} {}^\exists c \in \Delta \text{ such that } c(rb - as) = 0.$$

これは同値関係になる (♠). この同値関係による商集合 $R \times \Delta / \sim$ を Δ^{-1} とかく. また, (r, a) を含む同値類を $\dfrac{r}{a}$ とかく.

(3) $\frac{r}{a}, \frac{s}{b} \in \Delta^{-1}R$ に対して, 和と積を次のように定義する:

(i) $\frac{r}{a} + \frac{s}{b} := \frac{rb+sa}{ab}$; (ii) $\frac{r}{a} \cdot \frac{s}{b} := \frac{rs}{ab}$.

(通常の分数の和積と同じ.) これは, 代表元の取り方によらず, well-defined な演算である (♠). これによって, $\Delta^{-1}R$ は可換環をなす (♠); 零元 $= \frac{0}{1}$ $\left(= \frac{0}{a}\right)$, 単位元 $= \frac{1}{1}$ $\left(= \frac{a}{a}\right)$[*32]. このような可換環 $\Delta^{-1}R$ を, R の Δ による**局所化**という.

(4) 整域の局所化はまた, 整域である.

(注) 定義から, 集合として厳密には, $R \subseteq \Delta^{-1}R$ ではない. しかし, $\mathbb{Z}$ を $\mathbb{Q}$ の "部分集合" とみなすように, 一般の場合も同様のことがいえる.

(5) 対応 $r \mapsto \frac{r}{1}$ は, 環の準同型 $R \to \Delta^{-1}R$ を与える. この準同型を**自然な準同型**という. さらに, Δ が零因子[*33]を含まなければ, これは単射である.

(注) Δ が零因子を含まない場合, この単射を通して, $R \subseteq \Delta^{-1}R$ とみなす.

以上より, R の Δ による局所化とは, 「Δ の元に (無理矢理) 逆元を作る」操作であり, (いわゆる) 約分も込みで考えている. ざっくり表すと, $\Delta^{-1}R \fallingdotseq \frac{R}{\Delta}$ である[*34].

局所化によって, 整域はいつもある体に含まれることがわかる.

定理 A.7. R を整域とし, $\Delta := R \setminus \{0\}$ とおく. このとき, $\Delta^{-1}R$ は体をなす. この体を R の**商体**という[*35]. R の商体は, R を含む体のうち, 最小の体である; つまり, 体 L が $R \subseteq L$ を満たせば, $K \subseteq L$ となる.

$\mathcal{I}_R$ を環 R のイデアル全体の集合とする.

局所化された環のイデアルも, もとの環から来ることがわかる.

命題 A.8. Δ を R の乗法的集合, $\iota : R \to S := \Delta^{-1}R$ を自然な準同型とする. このとき, 次が成り立つ:

(1) $\iota^{-1} : \mathcal{I}_S \to \mathcal{I}_R$ は写像である;

(2) I を S のイデアルとすると, $I = \left(\iota \circ \iota^{-1}(I)\right) S$ となる;

(3) (1) の写像は単射である.

[*32] 記号を乱用して, $\frac{0}{1}$ も 0, $\frac{1}{1}$ も 1 とかくことにする. (これでも大して混乱はない.)

[*33] $r \in R$: **零因子** $\overset{\text{def}}{\Leftrightarrow} ar = 0$ となる $a\ (\neq 0) \in R$ がある.

[*34] 約分をきちんと意識して, このような形の分数全体と思って差支えない.

[*35] 一般に, 可換環 R に対して, 非零因子全体の集合 Δ は乗法的集合をなす. このときの局所化 $\Delta^{-1}R$ を R の**全商環**という.

証明. (2) のみ示す; 残りも難しくない (♠). “ $\supseteq$ ” は明らか. $x \in I \subseteq S := \Delta^{-1}R \coloneqq \dfrac{R}{\Delta}$ とすると, $x = \dfrac{r}{a}$ $(r \in R, a \in \Delta \subseteq R)$ とかける. $\iota(r) = \dfrac{r}{1} = \dfrac{a}{1} \cdot x \in I$ より, $r \in \iota^{-1}(I)$ である. したがって, $x = \dfrac{r}{1} \cdot \dfrac{1}{a} \in \left(\iota \circ \iota^{-1}(I)\right) S$ を得る. □

可換環の素イデアル $\mathfrak{p}$ に対して, 局所化 $R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}R$ がとても有用である.

命題 A.9. $\mathfrak{p}$ を可換環 R の素イデアルとし, $\Delta := R \setminus \mathfrak{p}$ とおく. このとき, 次が成り立つ.

(1) Δ は乗法的集合である.
(2) 局所化 $R_{\mathfrak{p}} := \Delta^{-1}R$ は, 極大イデアルをただ一つもつ可換環である. 特に, その極大イデアル M は $\dfrac{p}{1}$ $(p \in \mathfrak{p})$ で生成される: $M = \left\{ \dfrac{p}{a} \;\middle|\; p \in \mathfrak{p}, a \in \Delta \right\}$.

ただ一つの極大イデアルをもつ可換環を**局所環**という. (局所化の名前の由来である.) $R_{\mathfrak{p}}$ を $\mathfrak{p}$ における局所環ともいう.

証明. (1) 容易に確認できる.

(2) M を $\dfrac{p}{1}$ $(p \in \mathfrak{p})$ で生成される $R_{\mathfrak{p}}$ のイデアルとする. (最後の主張は明らか.)

(M が極大であること) $M \subsetneq I \subseteq R_{\mathfrak{p}}$ とし, $x := \dfrac{r}{a} \in I \setminus M$ $(r, a \in R, a \notin \mathfrak{p})$ を取る. x は M に属さないから, $r \notin \mathfrak{p}$ である; つまり, $r \in \Delta$. よって, x は $R_{\mathfrak{p}}$ において可逆である; ゆえに, $I = R_{\mathfrak{p}}$.

(ただ一つ) I を $R_{\mathfrak{p}}$ の真のイデアルとすると, I は可逆元を含まないから, I の元の分子は $\mathfrak{p}$ に属さなければいけない. よって, $I \subseteq M$ を得る. □

A.2 可換ネーター環

定義 A.10. R が**ネーター**であるとは, R のイデアルの列 $I_0 \subseteq I_1 \subseteq \cdots$ に対して, ある番号 n で $I_n = I_{n+1} = \cdots$ となるときにいう.

次は, 可換ネーター環の非常に重要な性質である.

定理 A.11. 可換環 R に対して, 次は同値である.

(1) R はネーター環である;
(2) R のすべてのイデアルは有限生成である.

証明. R をネーター環とし, I をそのイデアルとする. 矛盾を導くため, I が無限生成であると仮定する; よって, $I \neq (0)$. $x_1 \in I \setminus (0)$ を取ると, I は無限生成だから $(x_1) \subsetneq I$ であ

る. したがって, さらに $x_2 \in I \setminus (x_1)$ が取れて, $(x_1, x_2) \subsetneq I$ となる. これを繰り返して, $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ となる無限列を取れることになり, R のネーター性に矛盾する.

R の任意のイデアルが有限生成であるとし, R のイデアルの列 $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ を取る. $I := \bigcup_{i=0}^{\infty} I_i$ とおく. このとき, I はイデアルとなる (♠) ので, 仮定より有限生成である: $I = (x_1, \cdots, x_n)$ とかく. そうすると, ある番号 N で, すべての x_i が I_N に含まれる. よって, $I_N \subseteq I = (x_1, \cdots, x_n) \subseteq I_N$ となり, $I_N = I_{N+1} = \cdots = I$ となる. □

この定理によって, 例えば, 単項イデアル整域はネーターであることが従う. また, 本編で扱った**整数環**もネーター整域である (これについては, 次節で紹介することにする).

可換ネーター環の局所化もネーターである.

命題 A.12. Δ を R の乗法的集合とし, $S := \Delta^{-1}R$ とおく. このとき, R がネーター環ならば, S もそうである.

証明. 命題 A.8 より (♠). □

可換環論では, ネーター性がしばしば非常に重要な働きをするが, ネーターでない例を挙げておく. (学部で扱う可換環も, そのほとんどがネーターである[*36].)

例 A.13. $R := \{f(x) \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}$ はネーターでない (整域であることは明らか); 定数項だけ整数の有理数係数多項式全体の集合. このとき, $I := \{xg(x) \mid g(x) \in \mathbb{Q}[x]\}$ (定数項が 0 の多項式全体)[*37]は R のイデアルである (♠) が, 有限生成でない. 実際, 有限生成 $I = (xg_1(x), \cdots, xg_r(x))$ $(g_i(x) \in \mathbb{Q}[x])$ として矛盾を導く. $g_i(0) = \dfrac{a_i}{b_i}$ (既約分数) とする. I に属する任意の多項式 $f(x)$ は, $xg_i(x)$ たちの R 倍の和で表せる: $f(x) = \sum xg_i(x)f_i(x)$ $(f_i(x) \in R)$. このとき, 1 次の項は $g_i(x)$ および $f_i(x)$ の定数項によって表されている. $g_i(x)$ の定数項は $g_i(0) = \dfrac{a_i}{b_i}$ だったため, $f(x)$ の 1 次の項は, それらの (任意の) 整数倍 $f_i(0)$ の和でしかかけないことになる. しかし, I に属す多項式の 1 次の項は, 任意の有理数を取ることができるから, 矛盾する[*38].

次が本編 (補題 4.7) で使った事実である.

[*36] というか, 学部で出てくるネーターでない可換環ってなんだろう...

[*37] R での単項イデアル $(x) = \{xf(x) \mid f(x) \in R\}$ とは異なることに注意.

[*38] 難しい言い方をすれば, $\mathbb{Q}$ が $\mathbb{Z}$ 加群として $\dfrac{a_i}{b_i}$ $(1 \leq i \leq r)$ で生成されることになってしまうが, それはおかしい (命題 4.5).

定理 A.14. ネーター整域 R の任意の元は, 有限個の既約元の積で表せる[*39].

証明. $x := x_0 \in R$ をとる. (x は可逆でないとしてよい.) x_0 が既約元ならばおしまい. x_0 が既約でなければ, 定義より $x_0 = x_1 y_1$ と可逆でない元 $x_1, y_1 \in R$ の積に分解できる.

これを繰り返せばよいわけだが, 問題は

① 有限回のうちに既約元 x_n が出てくるか　② この分解の操作が有限回で終わるか

ということである. (その "有限性" に対してネーターであることが重要.)

① $x_0 = x_1 y_1$ より, 単項イデアルの間に包含関係 $(x_0) \subseteq (x_1)$ が成り立つ. さらに, R は整域より, $(x_0) \neq (x_1)$ である; もし "=" ならば y_1 が可逆元. これを繰り返すと, R のイデアルの列 $(x_0) \subsetneq (x_1) \subseteq (x_2) \subseteq \cdots$ を得るが, R はネーター環なので, ある番号 n で $(x_n) = (x_{n+1}) = \cdots$ となる. これは x_n が既約元であることを意味している.

② (最初の x に戻って) $x =: w_0$ とおく. w_0 が既約元ならばおしまい. w_0 が既約でなければ, ①より, 既約元 z_1 を用いて $w_0 = z_1 w_1$ ($w_1 \in R$) とかける. このとき, 上と同様に $(w_0) \subsetneq (w_1)$ を得る. ①とまったく同じ議論によって, R がネーター環であることを使って, (z_i が可逆元となる前に) $w_{n'}$ が既約元となって終わる.

以上より, 主張を得る. □

注意 A.15. 定理 A.14 における既約元への分解は, (可逆元倍と順序を無視しても) 一意的とは限らない. 実際, $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ を考えよう. この整域の中では, $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{5})$ と因数分解できる. このとき, 2 および $3, 1 \pm \sqrt{-5}$ はすべて既約元であり, (可逆元倍と順序を無視しても) 分解の仕方が一意的でないことが見て取れる.

実際, $1 + \sqrt{-5}$ が既約元であることを確認する; 他の元についても同様に確かめられる. 定義に沿って, $1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$ とおく. 両辺に複素共役をかけてからまとめると, $6 = (a^2 + 5b^2)(c^2 + 5d^2)$ となる. 【ここから通常の整数論】6 の分解は 4 通りあるが, 可換性を考慮すれば, $a^2 + 5b^2 = 1, 2$ のどちらかを考えればよい. 2 の可能性はすぐに否定されるから, $a^2 + 5b^2 = 1$ となるが, このとき $(a, b) = (\pm 1, 0)$ を得る. したがって, $a + b\sqrt{-5}$ が可逆元であることがわかる.

このように, 既約元の分解は一意的とは限らないが, 素元の分解は一意的である.

[*39] 任意の元が有限個の既約元の積で表せる整域を**原子整域** *(atomic domain)* という.

命題 A.16. 整域 R において, 素元分解があれば, それは (可逆元倍と順序を無視して) 一意的である.

証明. $p_1p_2\cdots p_s = q_1\cdots q_t$ を素元分解とする. このとき, 素元 p_1 は右辺をわり切っているので, ある番号 i で $p_1 \mid q_i$ となる; 番号を入れ替えて, $p_1 \mid q_1$ としてよい. そこで, $q_1 = rp_1$ とかけるが, q_1 は素元 (よって, 既約元) だから, r または p_1 は可逆である. p_1 は素元 (可逆でない) から, r が可逆元となり, p_1 と q_1 は可逆元倍の差しかないことがわかる. R は整域なので, $p_2\cdots p_s = rq_2\cdots q_t$ となるが, 同様のことを続ければ, すべての番号 i で p_i と q_i は可逆元倍の違い, かつ, $s = t$ であることがわかる. □

定義 A.17. 任意の元が素元分解をもつ整域を, **一意分解整域** *(UFD)* という. 命題 A.16 より, 素元分解は (自動的に) 一意である. また, この場合, 既約元は素元となる.

定理 A.14 より, 次がわかる.

系 A.18. 任意の既約元が素元となるネーター整域は, 一意分解整域である.

補足 A.19. 整域 R の任意の既約元が素元になるとき, R を *EL* **整域**[*40] という.

ここまでで, 既約元〜素元, およびその分解について議論してきたが, 既約元の分解が存在しない環も紹介しよう.

注意 A.20. 定理 A.14 において, やはり【ネーター】という仮定はとても大切である. つまり, そうでないと有限個の既約元の積に分解できない整域が存在する.

$R := \Omega := \mathbb{C}_{\mathbb{Z}}$ (代数的整数環 $\stackrel{\text{def}}{=} \mathbb{Z}$ 上モニック[*41]な方程式の複素数解全体の集合: 定義 A.24, A.25) を考えてみよう. (明らかに整域.) このとき, 任意の $a \in R$ に対して, $a = b^2$ となる $b \in R$ が存在する. 実際, $b = \pm\sqrt{a}$ とすれば, $b \in \mathbb{C}$ であり, a の ($\mathbb{Z}$ 上) 最小多項式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ に対して, $g(x) = x^{2n} + a_{n-1}x^{2(n-1)} + \cdots + a_0 = 0$ とすれば, これは $x = b$ を解にもつから, b は $\mathbb{Z}$ 上整である. 特に, a が既約元なら b は可逆となり, 結果的に a も可逆で矛盾. つまり, この環 R には既約元が存在しない[*42].

ついでに, 可換ネーター環上の加群の有限生成性について述べておく.

[*40] 有理整数環において, 【素元は既約元】という事実の逆 (**ユークリッドの補題**) をユークリッドが示したことに由来するらしい. つまり, EL=Euclid's Lemma...?

[*41] 最高次の係数が 1

[*42] 体も既約元や素元が存在しないが, ここで議論したことはそれとは意味が異なる. なぜなら, Ω は零でも可逆でもない元を多数もっているが, それを既約元の積で表すことができない, 等の理由である.

命題 A.21. R を可換ネーター環, $N \subseteq M$ を R 加群とする. このとき, M が有限生成ならば, N もそうである.

証明. $M = \langle m_1, \cdots, m_\ell \rangle_R$ とおく. ℓ に関する帰納法で証明する. $\ell = 1$ のとき, 対応 $r \mapsto rm_1$ は R 加群の (全射) 準同型 $f : R \to M$ である. $I := \operatorname{Ker} f$ は R のイデアルである. $J := f^{-1}(N)$ とおくと, R 加群として $J/I \simeq N$ となるが, J は R のイデアルより有限生成 (R がネーター) であるから, N も有限生成である.

$\ell > 1$ とする. $M_1 := \langle m_1, \cdots, m_{\ell-1} \rangle_R$ とおくと, 帰納法の仮定から M_1 の部分加群は有限生成である. そこで, $M_1 \neq M$ としてよい. $N_1 := N \cap M_1, N_2 := \pi(N)$ とおく. ここで, $\pi : M \to M/M_1$ $(= \langle m_\ell \rangle_R \neq 0)$ は自然な全射準同型である. N_1 は M_1 の部分加群, また, N_2 は M/M_1 の部分加群であるから, どちらも有限生成である. したがって, $N_1 = \langle x_1, \cdots, x_m \rangle_R, N_2 = \langle \pi(y_1), \cdots, \pi(y_n) \rangle_R$ $(x_i, y_i \in N)$ とかける.

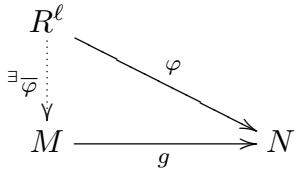
このとき, $N = \langle x_1, \cdots, x_m, y_1, \cdots, y_n \rangle_R$ であることを示そう. "$\supseteq$" は明らか. $n \in N$ とする. $N_2 = \pi(N) \ni \pi(n) = \sum a_i \pi(y_i)$ $(a_i \in R)$ とかける. $n - \sum a_i y_i \in \operatorname{Ker} \pi = M_1$ より, $n - \sum a_i y_i \in N \cap M_1 = N_1$, よって, $n - \sum a_i y_i = \sum b_j x_j$ $(b_j \in R)$ とかける. ゆえに, $n = \sum a_i y_i + \sum b_j x_j \in$ (右辺) となることがわかる. □

(議論は同じだが) 高度な証明を残す (読み飛ばしても問題ない). 以下, R 準同型 (もしくは単に準同型) といったら, R 加群としての準同型を意味する.

R 加群と R 準同型の列 $L \xrightarrow{f} M \xrightarrow{g} N$ に対して, $\operatorname{Im} f = \operatorname{Ker} g$ となるとき, この列は M で**完全である**という. $gf = 0$ であることに注意する. また, $L = 0$ であることと g が単射であること, および, $N = 0$ であることと f が全射であることは, それぞれ同値である.

命題 A.22. R を可換ネーター環, M, N を R 加群とする. このとき, 次が成り立つ.

(1) M が有限生成であることと全射 R 準同型 $R^\ell \to M$ が存在することは同値である.
(2) 任意の全射 R 準同型 $\varphi : M \to R^\ell$ は分裂する; つまり, ある R 準同型 $\psi : R^\ell \to M$ が存在して, $\varphi\psi = \mathsf{id}_{R^\ell}$ (R^ℓ の**射影性**).
(3) R 準同型 $\varphi : R^\ell \to N$ に対して, 次の図式を可換にする R 準同型 $\overline{\varphi} : R^\ell \to M$ が存在する:



さらに, $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ を R 加群の**完全列** (どこでも完全) とする.

(4) L および N が有限生成ならば, M もそうである.
(5) 自由加群 R^ℓ の部分加群は有限生成である.
(6) M が有限生成ならば, L および N もそうである.

証明. (1) $M = \langle m_1, \cdots, m_\ell \rangle_R$ とする. このとき, 対応 $(r_i) \mapsto \sum_i r_i m_i$ は R 加群としての全射準同型である. 逆も同様である. (与えられた全射準同型に対して, 単位ベクトルに対応する M の元を m_i とすればよい.)

(2) φ は全射より, R^ℓ の各単位ベクトルに対応する M の元を m_i とおく (1 つ取って固定). このとき, $\psi : (r_i) \mapsto \sum r_i m_i$ とすればよい.

(3) $\psi := (\varphi\ g) : R^\ell \oplus M \to N$ とおく (g が全射より, ψ もそう). また, $L := \operatorname{Ker} \psi$[*43] から $R^\ell \oplus M$ への射を $\binom{\alpha}{-\beta}$ とおく. まず, α が全射であることを示す. $\pi\alpha = 0$ を満たす準同型 $\pi : R^\ell \to X$ を取る[*44]. このとき, $(\pi\ 0)\binom{\alpha}{-\beta} = 0$ より, 余核 $N = \operatorname{Coker}\binom{\alpha}{-\beta}$ の性質[*45]から, $\rho : N \to X$ で $(\pi\ 0) = \rho\psi$ となるものが存在する:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\binom{\alpha}{-\beta}} & R^\ell \oplus M & \xrightarrow{(\varphi\ g)} & N & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle (\pi\ 0)} & \swarrow{\scriptstyle \exists \rho} & & & \\ & & & & X & & & & \end{array}$$

$\rho g = 0$ で g は全射より, $\rho = 0$, よって, $\pi = \rho\varphi = 0$ を得る. ゆえに, α は全射である.

(2) より, $\alpha\gamma = \mathsf{id}_{R^\ell}$ となる $\gamma : R^\ell \to L$ が存在する. そこで, $\overline{\varphi} := \beta\gamma : R^\ell \to M$ とおく. $(\varphi\ g)\binom{\alpha}{-\beta} = 0$, つまり, $g\beta = \varphi\alpha$ であることに気を付けて,

$$g\overline{\varphi} = g\beta\gamma = \varphi\alpha\gamma = \varphi$$

となる. このように, 図式を可換にする準同型 $\overline{\varphi} : R^\ell \to M$ の存在がわかる.

(4) (1) より, R 加群の全射準同型 $\pi_L : R^{\ell_1} \to L$ および $\pi_N : R^{\ell_2} \to N$ がとれる. また, (3) のような $\overline{\pi_N} : R^{\ell_2} \to M$ が存在する. このとき, 次のような完全列の間の可換図式を作れる:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^{\ell_1} & \xrightarrow{\binom{1}{0}} & R^{\ell_1+\ell_2} & \xrightarrow{(0\ 1)} & R^{\ell_2} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi_L} & & \downarrow{\scriptstyle (f\pi_L\ \overline{\pi_N})} & & \downarrow{\scriptstyle \pi_N} & & \\ 0 & \longrightarrow & L & \xrightarrow[f]{} & M & \xrightarrow[g]{} & N & \longrightarrow & 0 \end{array}$$

[*43] このような L を $R^\ell \to N \leftarrow M$ の**引き戻し** *(Pull Back)* という.
[*44] $f : M \to N$ が全射 $\overset{\text{def}}{\Leftrightarrow} gf = 0$ となる $g : N \to L$ は零 (圏論的定義) $\Leftrightarrow$ いつもの全射 (集合論的定義)
[*45] 圏論における定義だが, ここでは書ききれないので興味をもった読者は是非調べてほしい. (**アーベル圏**)

蛇の補題[*46]より, $\begin{pmatrix} f\pi_L & \overline{\pi_N} \end{pmatrix}$ は全射となり, (1) より, M は有限生成である.

(5) X を R^ℓ の部分加群とする. ℓ に関する帰納法で示す. $\ell = 1$ のとき, X は R のイデアルだから, OK (R はネーター). $\ell > 1$ とする. $R^\ell = R \oplus R^{\ell-1}$ とみて, $Y := X \cap R$ とおくと, 完全列 $0 \to Y \to X \to X/Y \to 0$ がとれる. $Y \subseteq R$, また, 第 2 同型定理より, $X/Y \simeq (X+R)/R \subseteq R^\ell/R \simeq R^{\ell-1}$ となるから, 帰納法の仮定からどちらも有限生成である. よって, (4) より, X も有限生成である.

(6) (1) より, 全射準同型 $\pi_M : R^\ell \to M$ がとれる. また, 全射準同型 $R^\ell \xrightarrow{\pi_M} M \xrightarrow{f} N$ が存在するから, N も有限生成である. さらに, 次のような完全列の間の可換図式がある:

$$\begin{array}{ccccccccc}
 & & & & & & L & & \\
 & & & & & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & X & \longrightarrow & R^\ell & \xrightarrow{\pi_M} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle h} & & \| & & \downarrow{\scriptstyle g} & & \\
0 & \longrightarrow & Y & \longrightarrow & R^\ell & \xrightarrow[g\pi_M]{} & N & \longrightarrow & 0
\end{array}$$

(5) より, Y は有限生成であり, その全射の像 $\operatorname{Coker} h$ ($:= Y/\operatorname{Im} h$) も有限生成である. 蛇の補題より, $L \simeq \operatorname{Coker} h$ だから, L も有限生成である. □

補足 A.23. 上の証明では, 対象 (R 加群) の元を (ほぼ) 取ることなく, その間の射 (R 準同型) のみで議論を行っている. 特に, 有限生成性および射影性をそれぞれ (1)(2) で再定義すると, それ以降は射のみの議論で済む. そうすると, 「可換ネーター環 R」でなくても[*47]同様の話ができることになり, 汎用性が非常に高い. このような手法を**圏**[*48]**論**的手

[*46] 完全列の間の可換図式

$$\begin{array}{ccccccccc}
 & & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & &
\end{array}$$

に対して, 完全列 $\operatorname{Ker} f \to \operatorname{Ker} g \to \operatorname{Ker} h \xrightarrow{\delta} \operatorname{Coker} f \to \operatorname{Coker} g \to \operatorname{Coker} h$ が存在する. δ を**連結射**とよぶ. 証明はそれほど難しくないので, 是非挑戦してほしい. (ただし, 圏論的に証明しようとするとかなり大変... だった気がする.)

[*47] 例えば, (可換非可換問わずただの) 環やもっと一般の “何か”(**関手**とか). ネーター性は帰納法における $\ell = 1$ のとき (イデアルが有限生成) にしか使っていない.

[*48] **圏** = 対象とその間の射のペア. 例えば, **集合の圏** Set は, 集合 (対象) 全体の集まりとその間の写像 (射) 全体のことであり, 環 R に対して, *(**右**)*R **加群の圏** $\mathsf{Mod}\, R$ は, (右)R 加群 (対象) 全体の集まりと R 準同型 (射) 全体のことである. これらは異なる圏構造をもっているが, 後者に対してさらに, **有限表示** (右)R 加群の圏 $\mathsf{fp}\, R$ を考えると, 命題 A.22 と同様の議論が展開できる (**アーベル圏**). ちなみに, 命題

法といい, 圏論は近年, 数学の様々な分野で重要な役割を果たしている.

A.3 整数環

(この節では, 証明を後回しにして, 整数環の重要事項をまとめる.)

いわゆる**整数**とは, $\cdots, -1, 0, 1, 2, \cdots$ のような数のことであるが, 方程式の観点から見ると, これらは (**モニック**な[*49]) 整数係数「1 次方程式」の解たちのことである. このとき,「2 次以上の方程式では？」と考えるのは自然なことである. 実は, そのような数たちも整数と似たような振る舞いをすることが知られている. 以下で正確な定義を述べよう.

定義-定理 A.24. $f(x) \in \mathbb{Z}[x]$ をモニックな多項式とする. このとき, 方程式 $f(x) = 0$ の解 $(\in \mathbb{C})$ を**代数的整数**[*50][*51]という. 代数的整数全体の集合を Ω で表し, これは環をなす.

例えば, $\sqrt{2}$ や (高校で扱う) ω $\left(:= \frac{-1+\sqrt{-3}}{2}\right)$, $\sqrt[3]{2}, \sqrt{-1}$ などは代数的整数である. 一方, $\frac{2}{3}$ は代数的整数ではない. また, $\Omega \subset \overline{\mathbb{Q}}$ ($\mathbb{Q}$ の代数閉包[*52]) である.

以降のため, もう少し一般的な定義を与える.

定義 A.25. (1) $R \subseteq S$ を可換環とする.

(i) S の元が R 上**整**であるとは, あるモニックなR 係数方程式 $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ の解となるときにいう.

(ii) S の元がすべて R 上整のとき, S は R 上**整**, または, S は R の**整拡大**という.

(2) R を整域, K をその商体[*53]とする.

A.22 では, 有限ランク ℓ しか考えなかったが, (それを無視すれば) $\mathsf{Mod}\, R$ でも議論でき, これもアーベル圏の構造をもつ. (さらに込み入った話になるが) 一般に, 有限生成 (右)R 加群の圏 $\mathsf{mod}\, R$ では不十分であり, R にネーター性を課すと $\mathsf{fp}\, R = \mathsf{mod}\, R$ となる. (一般に, $\mathsf{fp}\, R \subseteq \mathsf{mod}\, R \subseteq \mathsf{Mod}\, R$)

[*49] 最高次の係数が 1

[*50] モニックという仮定を外したとき, 方程式 $f(x) = 0$ の解 $(\in \mathbb{C})$ を**代数的数**という. 代数的でない数のことを**超越数**とよぶ. 例えば, 円周率 π やネイピア数 e などは超越数である.

[*51] 代数的整数と区別して, 通常の整数を**有理整数**とよぶこともある.

[*52] $K \subseteq L$ を体の拡大とする.

- L が K の**代数拡大** $\overset{\text{def}}{\Leftrightarrow}$ L の任意の元は, K 係数方程式の解である.
- L が K の**有限次拡大** $\overset{\text{def}}{\Leftrightarrow}$ $[L : K] := \dim_K L < \infty \Leftrightarrow$ 有限生成な代数拡大
- **代数閉体** $L \overset{\text{def}}{\Leftrightarrow}$ 定数でない L 係数の方程式が L の中で必ず解をもつ.
- L が K の**代数閉包** $(L = \overline{K}) \overset{\text{def}}{\Leftrightarrow} K \subseteq L$ が代数拡大, かつ, L が代数閉体.

代数閉包は必ず存在し, 一意的である. 例えば, $\overline{\mathbb{R}} = \mathbb{C}$ である. 一方, $\overline{\mathbb{Q}}$ は $\mathbb{C}$ ではない (代数拡大でない).

[*53] $\mathbb{Z}$ に対する $\mathbb{Q}$ の一般化. ラフな言い方をすれば, 約分込みの R の分数 $\frac{a}{b}$ $(a, b \in R, b \neq 0)$ 全体のことであり, R を含む (最小の) 体となる. 整域に対して必ず存在する. (A.1 節参照)

(i) L を R を含む体とする．このとき, $L_R := \{a \in L \mid a \text{ は } R \text{ 上整 }\}$ $(\supseteq R)$ を R の L における**整閉包**という．(例えば, $\mathbb{C}_{\mathbb{Z}} = \Omega$.)

(ii) $K_R = R$ となるとき, R を**正規環**, または, **整閉整域**という．

定義からは明らかではないが, 整閉包はきちんと環をなす．

定理 A.26. 整域 R の体 L における整閉包 L_R は, 環をなす．(特に, $\overline{L}$ の部分環である.)

例 A.27. 有理整数環 $\mathbb{Z}$ は正規環である．($\mathbb{Z}$ の商体は $\mathbb{Q}$.) 実際, $\mathbb{Z} \subseteq \mathbb{Q}_{\mathbb{Z}}$ であるが, 反対に $\frac{a}{b} \in \mathbb{Q}$ が $\mathbb{Z}$ 上整とすると, これはある $\mathbb{Z}$ 係数の方程式 $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ の解となる．整数係数方程式の有理数解の可能性としては, $\pm\frac{\text{定数項の約数}}{\text{最高次の係数の約数}}$ しかないが, モニックを仮定しているので, それは整数である．ゆえに, $\frac{a}{b} \in \mathbb{Z}$ を得る．

さらに一般に, 次が成り立つ．(証明は $\mathbb{Z}$ の場合と同様.)

命題 A.28. 一意分解整域は正規環である．

有理数体 $\mathbb{Q}$ の有限次拡大 K を**代数体**という．特に, $[K : \mathbb{Q}] = d$ のとき, K を d **次体**とよぶ．例えば, (本編で扱った) $\mathbb{Q}(\sqrt{A})$ $(\sqrt{A} \notin \mathbb{Q})$ などは 2 次体である．また, 代数体は $\overline{\mathbb{Q}}$ $(\subset \mathbb{C})$ の部分体である．

(ここでやっと) 整数環の定義を述べる (定理 A.26 参照).

定義 A.29. K を代数体とする．このとき, $K_{\mathbb{Z}}$ を K の**整数環**という．(どの代数体 K に対しても, $\mathbb{Z}$ 上整なものを取っていることは変わらないので, $\mathcal{O}_K$ とかくこともある.)

例 A.30. (1) $K = \mathbb{Q}(\sqrt{2})$ の整数環は, $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ である．実際, $\mathcal{O}_K := \mathbb{Q}(\sqrt{2})_{\mathbb{Z}} \supseteq \mathbb{Z}[\sqrt{2}]$ はすぐにわかる．反対に, $\frac{a}{b} + \frac{c}{d}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ が $\mathbb{Z}$ 上整とする．これは, (整数係数最小の) 2 次方程式 $b^2d^2x^2 - 2adx + (a^2d^2 - 2b^2c^2) = 0$ の解であるが, モニックである必要があるので, $b = d = \pm 1$ とならなければいけない．

(2) $K = \mathbb{Q}(\sqrt{-3})$ の整数環は, $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}$[*54] である (♠)．ここで, $\omega := \frac{-1 + \sqrt{-3}}{2}$[*55].

このように, 2 次体の整数環については (その生成元が) よくわかる．

[*54] $\omega^2 = -1 - \omega$ であることに注意.

[*55] $\omega = \frac{1 + \sqrt{-3}}{2}$ と取っても同じ.

定理 A.31. A $(\neq 1)$ を平方因子をもたない整数として,

$$\mathbb{Q}(\sqrt{A}) \text{ の整数環} = \begin{cases} \mathbb{Z}[\sqrt{A}] & A \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\omega] & A \equiv 1 \pmod 4 \end{cases} \xrightarrow{\mathbb{Z} \text{ 基底}} \begin{cases} \{1, \sqrt{A}\} \\ \{1, \omega\} \end{cases}$$

とかける. ここで, $\omega = \dfrac{1+\sqrt{A}}{2}$ である. 特に, 2 次体の整数環は, $\mathbb{Z}$ 加群として[*56] $\mathbb{Z}^2$ と同型である.

さらに一般に, d 次体についても次のことがわかる.

定理 A.32. d 次体 K の整数環 $\mathcal{O}_K$ は, $\mathbb{Z}$ 加群として $\mathbb{Z}^d$ と同型である.

本編でも扱った代数体の整数環に関する重要事項をまとめる.

定理 A.33. K を代数体とし, $R := \mathcal{O}_K$ とおく.

(1) R はネーター整域である;
(2) I を零でない R のイデアルとすると, 剰余環 R/I は有限集合である;
(3) R は (体でない) 正規環である;
(4) R の零でない素イデアルはすべて, 極大イデアルである;
(5) R が一意分解整域ならば, それは単項イデアル整域である.

注意 A.34. 一般に, 可換環 R に対して, 定理 A.33(2) $\Rightarrow$ (4) が成り立つ (♠).

A.3.1 証明

上において, 証明を残しているものは次であるが, それぞれに包含関係がある:

1 定理 A.24 $\Leftarrow$ 定理 A.26;
2 定理 A.31;
3 定理 A.32 $\Rightarrow$ 定理 A.33(2)(3);
4 定理 A.33(1)(5);

なるべく準備が簡単なものから示していく (循環論法になっていないことを願う[*57]). 方針としては,

[*56] (体上) ベクトル空間の一般化. 可換環 R に対して, たし算とスカラー (R) 倍ができる集合を R **加群**という. 例えば, $\mathbb{Z}^d$ や $\mathbb{Z}/n\mathbb{Z}$ (有限生成), $\mathbb{Q}, \mathbb{R}$ (無限生成) は $\mathbb{Z}$ 加群である.
[*57] 気付いたことがあれば著者へ連絡してほしい.

(a) 定理 A.26 (よって, 定理 A.24)
(b) 定理 A.32 を認めて, 定理 A.33(2)(3)
(c) 定理 A.33(1)(3)(4) を認めて, 定理 A.33(5)
    - 定理 A.32 を認めれば, 定理 A.32 $\overset{\text{(b)}}{\Longrightarrow}$ 定理 A.33(2) $\overset{\text{A.34}}{\Longrightarrow}$ 定理 A.33(4)
(d) 定理 A.32 (ついでに定理 A.31) および定理 A.33(1)

という順番で証明を与えていく.

A.3.1.1 定理 A.26

ここでは, 【整閉包 L_R が和差積で閉じていること】を示したい. つまり, L の元で R 上整なもの同士の和差積はまた, R 上整であることを言いたい. (L の元であることは明らか.) しかし, それら和差積を解にもつ方程式を探すのはなかなか困難である.

そこで, 「R 上整」を次のように言い換えよう.

命題 A.35. $R \subseteq S$ を可換環の拡大とし, $s \in S$ とする. このとき, 次は同値である:

(1) s は R 上整である;
(2) $R[s] := \{f(s) \mid f(x) \in R[x]\} \subseteq T \subseteq S$ となる S の部分環 T で, R 加群として有限生成[*58]なものが存在する.

証明. s が R 上整と仮定する. このとき, R 上モニックな多項式 $f(x) = \sum_{i=0}^{n} c_i x^i$ が存在して, $f(s) = 0$ となる. $R[x]/(f(x)) \to R[s]$ $(g(x) \mapsto g(s))$ は環の全射準同型[*59]であるが, R 加群 ($\fallingdotseq R$ 上 "ベクトル空間") としての全射準同型でもある. 左辺 $R[x]/(f(x))$ は $\{1, x, \cdots, x^{n-1}\}$ を基底[*60]とする有限生成 R 加群である. よって, 右辺 $R[s]$ も有限生成であるから, $T := R[s]$ とおけばよい.

条件 (2) を仮定する. (このとき, $x = s$ を解にもつ R 上モニックな方程式 $f(x) = 0$ を作りたい.) T の R 加群としての生成元を $t_1, \cdots, t_\ell$ とする. $s \in R[s] \subseteq T$ より, 各 st_i も T の元だから, $t_1, \cdots, t_\ell$ の一次結合でかける: $st_i := a_{11}t_1 + \cdots + a_{1\ell}t_\ell$ $(a_{ij} \in R)$. $A := (a_{ij}), \mathbf{t} := (t_i)$ (縦ベクトル) とおく. このとき, $A\mathbf{t} = s\mathbf{t}$ となるから, s は行列 A の固有値である ($\mathbf{t}$ は対応する A の固有ベクトル). したがって, s は固有方程式 $f(x) := \det(xE - A) = 0$ の解である. ここで, E は ℓ 次単位行列. 固有多項式 $f(x)$ は R

[*58] つまり, T は R 上の有限次元ベクトル空間 "のような" ものである.
[*59] $(f(x)) \subseteq \mathrm{Ker}$ だが, 逆があやしい. ($f(x)$ の最小性?)
[*60] $f(x)$ がモニックであることが大事.

上モニックなので, 希望する多項式が取れたことになる. □

可換環の拡大列 $R_i \subseteq R_{i+1}$ において, 各 R_{i+1} が R_i 上有限生成ならば, R_{i+2} も R_i 上有限生成となるから, (定理 A.26 より強い) 次の定理を得る.

定理 A.36. $R \subseteq S$ を可換環の拡大とし, $s, s' \in S$ を R 上整な元とする. このとき, $s \pm s', ss'$ も R 上整である.

証明. $R =: R_0 \subseteq R_1 := R_0[s] \subseteq R_2 := R_1[s'] = R_0[s, s'] \subseteq S$ とおく. s は R 上整だから, 命題 A.35 より R_1 は R 上有限生成である. s' も R 上整だから, 明らかに R_1 上整である (R 上モニック多項式を取れて $R \subseteq R_1$). したがって, 命題 A.35 より, R_2 は R_1 上有限生成である. このように, R_2 は R 上有限生成である.

任意に $t \in R_2$ を取ると, $R[t] \subseteq R_2 \subseteq S$ で R_2 は R 上有限生成だから, 命題 A.35 より, t は R 上整である. もちろん, $s \pm s', ss' \in R_2$ だから, 主張が成り立つ. □

これで, 定理 A.24 および定理 A.26 の証明が終わった.

A.3.1.2 局所化と整閉包

ここで, 今後のため, 局所化と整閉包についてまとめておく.

補題 A.37. R を整域とする.

(1) S を R の整拡大とし, 整域であるとする.
   (i) S が体であることと R がそうであることは同値である.
   (ii) Δ を R の乗法的集合とする (よって, S の乗法的集合でもある). このとき, $\Delta^{-1}S$ も $\Delta^{-1}R$ の整拡大である.

(2) K を R の商体, $K \subseteq L$ を体の有限次拡大, $S := L_R$ を R の L における整閉包とする. また, Δ を R の乗法的集合とする.
   (i) $\Delta^{-1}R$ の L における整閉包は, $\Delta^{-1}S$ である.
   (ii) R が正規環ならば, $\Delta^{-1}R$ もそうである.
   (iii) S の商体は L である.

証明. (1)(i) R を体とする. $s\ (\neq 0) \in S$ とすると, R 上モニックな多項式 $f(x)$ が存在し, $f(s) = 0$ である; つまり, $s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0\ (a_i \in R)$. $a_0 = 0$ ならば, 上の式を s でくくって, $s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1) = 0$ となる. 後半の式に同じことを繰り返して, $a_0 \neq 0$ としてよい (S は整域だから, どこかで $a_i \neq 0$ が出てくるはず). このと

き, $s(s^{n-1}+a_{n-1}s^{n-2}+\cdots+a_1)=-a_0\ (\neq 0)\in R$ だから, s の逆元が見つかる.

S を体とする. $r\ (\neq 0)\in R$ とすると, $r\in S$ でもあるから, r の逆元が S の中で取れる: $r^{-1}\in S$. S は R の整拡大だから, $r^{-1}\in S$ に対して, R 上モニックな多項式 $f(x)$ が存在して $f(r^{-1})=0$ となる: $(r^{-1})^n+a_{n-1}(r^{-1})^{n-1}+\cdots+a_0=0\ (a_i\in R)$. r^n を両辺にかけて, $1+a_{n-1}r+a_{n-2}r^2+\cdots+a_0r^n=0$ を得る. よって, $1=-r(a_{n-1}+a_{n-2}r+\cdots+a_0r^{n-1})$ となるが, 後半の因子は R の元なので, r の R における逆元が見つかる.

(ii) $\dfrac{s}{a}\in\Delta^{-1}S\coloneqq\dfrac{S}{\Delta}\ (s\in S, a\in\Delta)$ とする. $s\in S$ は R 上整より, $R[s]$ は $s_1,\cdots,s_\ell$ によって R 上生成される (命題 A.35). よって, $\left(\Delta^{-1}R\right)\left[\dfrac{s}{a}\right]$ は $s_1,\cdots,s_\ell$ によって $\Delta^{-1}R$ 上生成される (分母はすべて係数の $\Delta^{-1}R$ に押し付ける) から, もう一度命題 A.35 を適用して, $\dfrac{s}{a}$ は $\Delta^{-1}R$ 上整である.

(2) R,S は整域より, $R\subseteq\Delta^{-1}R\subseteq K:=(R\setminus\{0\})^{-1}R\subseteq L$ および $S\subseteq\Delta^{-1}S\subseteq L$ であることに注意する.

(i) $L_{\Delta^{-1}R}=\Delta^{-1}S$ を示す. (1)(ii) より, " $\supseteq$ " が成り立つ. 逆に, $t\in L$ を $\Delta^{-1}R$ 上整とする: $t^n+\dfrac{r_{n-1}}{a_{n-1}}t^{n-1}+\cdots+\dfrac{r_0}{a_0}=0\ (r_i\in R, a_i\in\Delta\subseteq R)$. $n-1$ 次以下の項の分母を払って整理すると, $t^n+\dfrac{1}{a}(s_{n-1}t^{n-1}+s_{n-2}t^{n-2}+\cdots+s_0)=0\ (a\in\Delta, s_i\in R)$ とかける. さらに, 両辺に a^n をかけると,

$$(at)^n+s_{n-1}(at)^{n-1}+as_{n-2}(at)^{n-2}+\cdots+a^{n-1}s_0=0$$

となるから, $at\in L$ は R 上整であり, $at\in S$ を得る. ゆえに, $t=\dfrac{at}{a}\in\Delta^{-1}S$ がわかる.

(ii) $\Delta^{-1}R$ の商体を K' とおくと, R の商体 K の最小性より, $K\subseteq K'$ となる. 一方, $\Delta^{-1}R\subseteq K$ であるから, $\Delta^{-1}R$ の商体 K' の最小性より, $K'\subseteq K$ を得る. ゆえに, $K'=K$ である.

このとき, (2)(i) を $L\rightsquigarrow K$ として適用すると, $S:=L_R\rightsquigarrow K_R=R$ より, $\Delta^{-1}R$ の K における整閉包 $K_{\Delta^{-1}R}$ は, $\Delta^{-1}R$ 自身となるから, $\Delta^{-1}R$ は正規環である.

(iii) $S\subseteq L$ なので, S の商体 L' の最小性より, $L'\subseteq L$ である. 一方, (2)(i) を $\Delta\rightsquigarrow R\setminus\{0\}$ で適用すると, $\Delta^{-1}R\rightsquigarrow K$ となるから, K の L における整閉包 $L_K\overset{(\spadesuit)}{=}L$ は $(R\setminus\{0\})^{-1}S$ である. よって, $L=(R\setminus\{0\})^{-1}S\subseteq(S\setminus\{0\})^{-1}S=:L'$ を得る. 結果的に, $L'=L$ であることがわかる. □

これによって, $\overset{\text{整域}}{R}\subseteq\underbrace{\overset{\text{商体}}{K}\subseteq L}_{\text{有限次拡大}}\supseteq S:=L_R$ の状況において, L の任意の元を適当に S 倍すると, S に落ちる. 例えば, これには次のような使い方がある.

補題 A.38. 上の状況において, L の K 上ベクトル空間としての基底を S から選ぶことができる.

証明. $\{t_1, \cdots, t_d\}$ を L の K 基底とする. L は S の商体より, ある $s\ (\neq 0) \in S$ が取れて, (任意の番号 i で) $st_i \in S$ とできる. このとき, $\{st_1, \cdots, st_d\}$ もまた, L の K 基底である. 実際, $\alpha_1(st_1) + \cdots + \alpha_d(st_d) = 0$ $(\alpha_i \in K)$ とおく. このとき, $s(\alpha_1 t_1 + \cdots + \alpha_d t_d) = 0$ であり, $s \neq 0$ より, $\alpha_1 t_1 + \cdots + \alpha_d t_d = 0$ である. $t_1, \cdots, t_d$ は一次独立より, $\alpha_i = 0$ を得る. $d = \dim_K L$ より, $\{st_1, \cdots, st_d\}$ も L の K 基底をなす. □

A.3.1.3 定理 A.33(2)(3)

最初に, 定理 A.32 を認めて, 定理 A.33(3) を示す.

定理 A.33(3) の証明. 補題 A.37 より, $\mathcal{O}_K$ の商体は K だから, 示したいことは, $\mathcal{O}_K\ (:= K_{\mathbb{Z}}) = K_{\mathcal{O}_K}$ である. " $\subseteq$ " は明らか. $t \in K_{\mathcal{O}_K}$ ($\mathcal{O}_K$ 上整な K の元) とする. このとき, $\mathbb{Z}[t] \subseteq \mathcal{O}_K[t] \subseteq K$ となるが, 定理 A.32 より, $\mathcal{O}_K$ は $\mathbb{Z}$ 上有限生成である. さらに, 命題 A.35 より, $\mathcal{O}_K[t]$ は $\mathcal{O}_K$ 上有限生成である. したがって, $\mathcal{O}_K[t]$ は $\mathbb{Z}$ 上有限生成である. もう一度, 命題 A.35 を適用すれば, t は $\mathbb{Z}$ 上整であることを得る: $t \in K_{\mathbb{Z}} =: \mathcal{O}_K$. □

ここから, 定理 A.32 から定理 A.33(2) を導くために, **ノルム**の概念を導入する.

R, S, k を可換環とし, $R \supseteq k \subseteq S$ を満たしているとする. k の元を保存する R から S への環準同型写像 (k 多元環の準同型写像) 全体の集合を $\mathrm{Hom}_k^{\mathrm{alg}}(R, S)$ とかく.

(ガロア理論を知っている読者のために補足すると) $\mathbb{Q} \subseteq K$ がガロア拡大のとき, $\mathrm{Hom}_{\mathbb{Q}}^{\mathrm{alg}}(K, \overline{K})$ がまさにガロア群 $\mathsf{Gal}(K/\mathbb{Q})$ を与える.

次もガロア理論を学ぶ上で, 非常に重要な事実である.

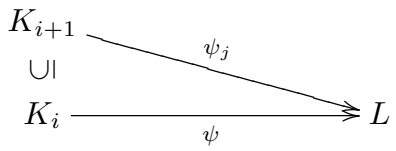
補題 A.39. $K \subseteq L$ を標数零の体の有限次拡大とする. このとき, $|\mathrm{Hom}_K^{\mathrm{alg}}(L, \overline{K})| = [L : K]$ が成り立つ.

証明. $K \subseteq L$ が有限次の拡大 ($\Leftrightarrow$ 有限生成な代数拡大) より, $L = K(a_1, \cdots, a_n)$ となる $a_i \in L$ たちが存在する. そのため, 体の拡大列

$$K \subseteq K(a_1) \subseteq K(a_1, a_2) \subseteq \cdots \subseteq K(a_1, \cdots, a_n) = L$$

を取ることができる: $K_i := K(a_1, \cdots, a_i)$.

$\psi \in \mathrm{Hom}_K^{\mathrm{alg}}(K_i, \overline{K})$ を一つ固定したとき, 可換図式



を満たす $\psi_j \in \mathrm{Hom}_K^{\mathrm{alg}}(K_{i+1}, \overline{K})$ (ψ の K_{i+1} への**延長**という) をちょうど $[K_{i+1} : K_i]$ 個取ることができれば, $\mathrm{Hom}_K^{\mathrm{alg}}(K, \overline{K})$ の唯一の元である恒等射 ($= \mathsf{id}_K$) から出発して,

$$|\mathrm{Hom}_K^{\mathrm{alg}}(L, \overline{K})| = \mathsf{id}_K \text{ の } L \text{ への延長の個数} = [K_n : K_{n-1}] \cdots \underbrace{[K_2 : K_1]}_{K_2 \text{ へ延長}} \underbrace{[K_1 : K]}_{K_1 \text{ へ延長}} = [L : K]$$

を得ることができる.

そこで, 記号を取り替えて, $K \subseteq M \subseteq M(a) =: L$ とし, 【$\psi \in \mathrm{Hom}_K^{\mathrm{alg}}(M, \overline{K})$ の延長の個数が $[L : M]$ である】ことを示す. a の M 上最小多項式を $g(x)$[*61] とする. また, $h(x) \in M[x]$ の各係数に ψ を施した新しい多項式を $h^\psi(x) \in \overline{K}[x]$ とかくことにする.

まず, $[L : M]$ を次のように言い直したい:

$$[L : M] = \deg g(x) = \deg g^\psi(x)^{*62} \overset{(*)}{=} \text{「}g^\psi(x) = 0 \text{ の解の個数」}.$$

$(*)$ のために, 方程式 $g^\psi(x) = 0$ は重解をもたないことを示そう. $f(x)$ を a の K 上最小多項式とする. $f(x) \in M[x]$ でもあるから, a の M 上の最小多項式 $g(x)$ は $f(x)$ をわりきる: $g(x) \mid f(x)$. よって, $g^\psi(x) \mid f^\psi(x) = f(x)^{*63}$ (in $\overline{K}[x]$) を得る. 標数零より, 方程式 $f(x) = 0$ は重解をもたないから, $g^\psi(x) = 0$ も重解をもたない.

したがって, 【「ψ の L への延長の個数」$= [L : M]$】を得るためには, ψ の延長と方程式 $g^\psi(x) = 0$ の解が一対一に対応することを証明すればよい. ここで, $\overbrace{K \subseteq \underbrace{\psi(M)}_{\text{代数拡大}} \subseteq \overline{K}}^{\text{代数拡大}}$ より, $\psi(M)$ の代数閉包は $\overline{K}$ と一致することに注意する; よって, $g^\psi(x)$ は $\overline{K}$ 上で一次式の積に分解され, ゆえに $g^\psi(x) = 0$ の解はすべて $\overline{K}$ の中でとれる.

(i) $\xi : L \to \overline{K}$ を ψ の延長とする. このとき, $g(x) = \sum c_i x^i$ とおくと,

$$g^\psi(\xi(a)) = \sum \psi(c_i)\xi(a)^i = \sum \xi(c_i)\xi(a^i) = \xi\left(\sum c_i a^i\right) = \xi(g(a)) = 0.$$

[*61] 標数零より, 方程式 $g(x) = 0$ は重解をもたない.

[*62] M は体より, ψ は単射であることに注意.

[*63] ψ は K の元を保存する.

2 つ目の等号は, ξ が ψ の延長より, M 上で 2 つの写像が一致していることから来る. したがって, $\xi(a)$ は $g^{\psi}(x)=0$ の解である.

(ii) b を方程式 $g^{\psi}(x)=0$ の解 ($\in \overline{K}$) とする. このとき,

$$\begin{array}{ccccccc} \xi_b : L := M(a) & \xleftarrow{\simeq} & M[x]/(g(x)) & \longrightarrow & \overline{K}[x]/(g^{\psi}(x)) & \longrightarrow & \overline{K} \\ h(a) & \longleftarrow & h(x) & \longmapsto & h^{\psi}(x) & \longmapsto & h^{\psi}(b) \end{array}$$

は well-defined な環の準同型であり, K の元を保存する (K 多元環の準同型). さらに, M 上では ψ と一致する. このように, ψ の L への延長 ξ_b を得ることができる.

(i) および (ii) の対応は, 互いに逆の写像を与えることは容易に確かめられる. よって, ψ の L への延長, および, 方程式 $g^{\psi}(x)=0$ の解が一対一に対応していることがわかる. □

そこで, ノルムの定義を与える.

定義 A.40. $K \subseteq L$ を標数零の体の d 次拡大とし, $\mathrm{Hom}_K^{\mathrm{alg}}(L, \overline{K}) = \{\sigma_1, \cdots, \sigma_d\}$ (補題 A.39) とおく. このとき, $a \in L$ に対して,

$$\mathrm{N}_{L/K}(a) := \prod_{i=1}^{d} \sigma_i(a)$$

を a の**ノルム**という.

例 A.41. 2 次体 $\mathbb{Q}(\sqrt{A}) := \{a+b\sqrt{A} \mid a, b \in \mathbb{Q}\}$ を考えよう. $\mathrm{Hom}_{\mathbb{Q}}^{\mathrm{alg}}(\mathbb{Q}(\sqrt{A}), \overline{\mathbb{Q}})$ の元は $\sqrt{A}$ の行先で決まり, それは 2 乗して A となる数でなければいけないから, $\sqrt{A} \mapsto \pm\sqrt{A}$ (+ の場合は恒等射) の 2 つしかない. よって, $\mathrm{N}_{\mathbb{Q}(\sqrt{A})/\mathbb{Q}}(a+b\sqrt{A}) = a^2 - Ab^2$ となる.

ノルムの基本性質を示す.

命題 A.42. 定義 A.40 の状況で, $\mathrm{N}_{L/K} : L \to K$ は K を保存する環の単射準同型である.

証明. 主張は $\mathrm{N}_{L/K}(a) \in K$ のみである; このとき, 環の準同型であること, および, 単射であることは明らかである.

$\widetilde{L}$ を L の K 上のガロア閉包[*64]とする. $\sigma_i(a)$ も a の K 上最小多項式 $=0$ の解だから, $\sigma_i(a) \in \widetilde{L}$ となる: $\mathrm{Hom}_K^{\mathrm{alg}}(L, \overline{K}) = \mathrm{Hom}_K^{\mathrm{alg}}(L, \widetilde{L})$. よって, $\mathrm{N}_{L/K}(a) \in \widetilde{L}$ である. ガロ

[*64] L を含む K の最小のガロア拡大. 有限次拡大に対して, 必ず存在する. 実際に, L のすべての元に対して, その最小多項式 $=0$ の $\overline{K}$ における解をすべて添加すればよい. (有限次拡大だから, 高々有限回のステップで済む.)

アの基本定理によって, これが $\mathsf{Gal}(\widetilde{L}/K) := \{\sigma \in \mathrm{Hom}_K^{\mathrm{alg}}(\widetilde{L}, \widetilde{L}) \mid \sigma$は全単射 $\}$ の任意の元 σ で止まっている (すなわち, $\sigma(\mathrm{N}_{L/K}(a)) = \mathrm{N}_{L/K}(a)$) ことを示せばよい.

上のように, $\sigma_i \in \mathrm{Hom}_K^{\mathrm{alg}}(L, \widetilde{L})$ だから $\sigma\sigma_i \in \mathrm{Hom}_K^{\mathrm{alg}}(L, \widetilde{L})$ であり, σ は全単射なので, この対応は $\{\sigma_1, \cdots, \sigma_d\}$ 上の置換を引き起こす. したがって,

$$\sigma(\mathrm{N}_{L/K}(a)) = \sigma\left(\prod_{i=1}^{d} \sigma_i(a)\right) = \prod_{i=1}^{d} \sigma\sigma_i(a) = \prod_{i=1}^{d} \sigma_i(a) = \mathrm{N}_{L/K}(a)$$

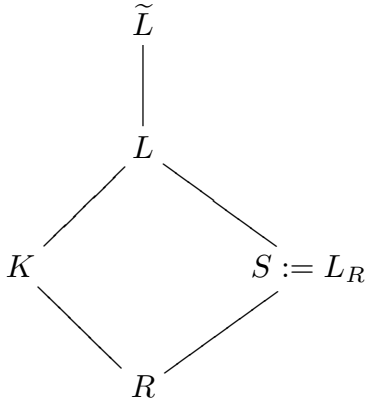
となる. □

定理 A.33(2) を示すためのキーとなる命題を与える.

命題 A.43. R を正規環, K をその商体, $K \subseteq L$ を標数零の体の有限次拡大とする. また, $S := L_R$ を R の L における整閉包とする. このとき, 次が成り立つ.

(1) $s\ (\neq 0) \in S$ ならば, $\dfrac{\mathrm{N}_{L/K}(s)}{s} \in S$;
(2) I を零でない S のイデアルとし, $s \in I \setminus \{0\}$ をとると, $\mathrm{N}_{L/K}(s) \in I \cap R$ となる. 特に, $I \cap R \neq (0)$ である.

証明. $\widetilde{L}$ を L の K 上のガロア閉包とし, $\mathrm{Hom}_K^{\mathrm{alg}}(L, \overline{K}) = \mathrm{Hom}_K^{\mathrm{alg}}(L, \widetilde{L}) = \{\sigma_1, \cdots, \sigma_d\}$ (恒等射はあるから, $\sigma_1 := \mathsf{id}$) とおく.



命題 A.42 より, $t := \mathrm{N}_{L/K}(s) \in K$ である; よって, $\dfrac{t}{s} \in L$. $s \in S := L_R$ より, R 上モニックな多項式 $f(x) = \sum c_i x^i$ が存在して, $f(s) = 0$ となる. 各 j に対して, $\sigma_j(s) \in \widetilde{L}$ であるが,

$$f(\sigma_j(s)) = \sum c_i \sigma_j(s)^i = \sum \sigma_j(c_i)\sigma_j(s^i) = \sigma_j\left(\sum c_i s^i\right) = \sigma_j(f(s)) = 0,$$

つまり, R 上整なので $\sigma_i(s) \in \widetilde{L}_R$ となる; よって, $t, \dfrac{t}{s} \in \widetilde{L}_R$.

(1) $\frac{t}{s} \in L$ かつ R 上整なので, $\frac{t}{s} \in L_R = S$ を得る.

(2) $t \in K$ かつ R 上整なので, $t \in K_R = R$ (R は正規環). さらに, $s \in I$ かつ $\frac{t}{s} \in S$ より, $t = s \cdot \frac{t}{s} \in I$ (I は S のイデアル). したがって, $t \in I \cap R$ を得る. □

これで, 定理 A.32 から定理 A.33(2) を導く準備が整った.

定理 A.33(2) の証明. I ($\neq (0)$) を $\mathcal{O}_K$ のイデアルとする. 任意に I の元 a ($\neq 0$) を取る. 命題 A.43 を次のように適用する:

$$R \rightsquigarrow \mathbb{Z}\ (K \rightsquigarrow \mathbb{Q}),\ L \rightsquigarrow K\ (S \rightsquigarrow \mathcal{O}_K).$$

このとき, $b := \mathrm{N}_{K/\mathbb{Q}}(a) \in I \cap \mathbb{Z}$ である. よって, $(b) \subseteq I$ となるから, 環の全射準同型 $\mathcal{O}_K/(b) \to \mathcal{O}_K/I$ が存在する. $\mathcal{O}_K/(b)$ が有限集合ならば, $\mathcal{O}_K/I$ もそうだから, $\mathcal{O}_K/(b)$ が有限集合であることを示す.

定理 A.32[*65] より, $\mathbb{Z}$ 加群としての同型[*66] $\varphi : \mathcal{O}_K \to \mathbb{Z}^d$ が存在する. $b \in \mathbb{Z}$ より,

$$\varphi((b)) = \varphi(b\mathcal{O}_K) = b\varphi(\mathcal{O}_K) = (b\mathbb{Z})^d$$

となるから, $\mathcal{O}_K/(b) \simeq (\mathbb{Z}/b\mathbb{Z})^d$ (有限集合) であることがわかる. □

A.3.1.4 デデキント環と定理 A.33(5)

一般に, 定理 A.33(1)(3)(4) を満たす環を**デデキント環**という.

定義 A.44. R が**デデキント環**であるとは, 次の 3 条件を満たすときにいう:
(i) ネーター環; (ii) (体でない[*67]) 正規環; (iii) 非零な素イデアルは極大イデアル.
(特に, 整域であることに注意.)

定理 A.33(5) はデデキント環に対して議論できる. そのため, この節では R がデデキント環であることのみを仮定する. (この節はデデキント環についてのお話, 他とは独立して読めるはず.) とりあえず, 今後も R は可換環とする.

次がこの節の主定理である.

定理 A.45 (定理 A.33(5))**.** デデキント環が一意分解整域ならば, それは単項イデアル整域である.

[*65] 命題 A.43 では不要であるが, 定理 A.32 を適用するときに, R がネーターであることが必要である.
[*66] (体上) ベクトル空間における線型写像と同様に, たし算とスカラー ($\mathbb{Z}$) 倍を保存する.
[*67] 体をデデキント環のクラスに含めるかどうかは流儀による.

証明を与えるため, その準備をする.

可換環 R のイデアル I, J に対して, xy $(x \in I, y \in J)$ で生成されるイデアルを IJ とかき, I と J の**積**という: $IJ = \{\sum xy \text{ (有限和)} \mid x \in I, y \in J\}$[*68]. いつもと同じように, I^n $(n \geq 0)$ を定義する: $I^0 = R$.

素イデアルがイデアルの積を含むと, いつものようにどちらかを含むことがわかる (♠).

事実 A.46. I, J を R のイデアルとし, $\mathfrak{p}$ を素イデアルとする. このとき, $IJ \subseteq \mathfrak{p}$ ならば, $I \subseteq \mathfrak{p}$ または $J \subseteq \mathfrak{p}$ となる. 特に, R のイデアル $I_1, \cdots, I_\ell$ に対して, $\bigcap_i I_i = \mathfrak{p}$ ならば, ある番号 i で $I_i = \mathfrak{p}$ となる.

単項イデアルの積は容易に書き換えられ, それ自体が単項イデアルになる (♠).

事実 A.47. $I = (x), J = (y)$ ならば, $IJ = (xy)$ である. 特に, $I^n = (x^n)$ である.

次の定理が重要である.

定理 A.48. デデキント環の任意のイデアルは, 有限個の素イデアルの積に分解できる (**素イデアル分解**). さらに, その分解は順序を無視して一意的である.

これを認めて, 先に定理 A.45 を示そう. (素イデアル分解の例も後で与える.)

定理 A.45 の証明. I を R の零でないイデアルとする. 定理 A.48 より, $I = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_\ell$ ($\mathfrak{p}_i$ は素イデアル) とかけるから, 任意の素イデアルが単項であることが示せればよい.

I を素イデアルとする (よって, $I \neq R$). x $(\neq 0) \in I$ とすると, 仮定より R は一意分解整域だから, $x = p_1p_2\cdots p_t$ と素元分解ができる. I は素イデアルだから, ある番号 i で $p_i \in I$ となる. このとき, $(p_i) \subseteq I \subsetneq R$ となるが, R はデデキント環 (定理 A.33(4)) より, 素イデアル (p_i) は極大イデアルとなる. したがって, $I = (p_i)$ を得る. □

ここから, 定理 A.48 を証明するための準備に入る.

最初に, ネーター性のもう一つの重要な同値条件を与える.

定理 A.49. 次は同値である:

(1) R はネーター環である;
(2) R のイデアルの任意の(空でない) 集合に, (包含関係に関して) 極大なものが存在する (**極大条件**).

[*68] $IJ = \{xy \mid x \in I, y \in J\}$ だとダメ. (たし算で閉じていないから, イデアルにならない.)

証明. (1)⇒(2): $\mathcal{M}$ ($\neq \emptyset$) を R の (ある) イデアルの集合とする. (背理法) $I_1 \in \mathcal{M}$ とすると, 背理法の仮定からこれは極大ではない. つまり, $I_2 \in \mathcal{M}$ が取れて, $I_1 \subsetneq I_2$ とできる. I_2 に対しても同じことができるから, これを続けて, R のイデアルの昇鎖列 $I_1 \subsetneq I_2 \subsetneq \cdots$ ができるが, これは R がネーターであることに矛盾する.

(2)⇒(1): R のイデアルの昇鎖列 $I_1 \subseteq I_2 \subseteq \cdots$ を取り, $\mathcal{M} := \{I_i \mid i \geq 1\}$ とおく. 仮定より, $\mathcal{M}$ は極大元 I をもつ: ある番号 n で $I = I_n$ とかける. このとき, I の極大性から, $I = I_n = I_{n+1} = \cdots$ が従う. □

次に, 新しい "イデアル" の概念を導入する; 今までの環 R のイデアルの概念よりも広く, (R が整域の場合) その商体 K のある部分集合も R の "イデアル" とよぶことにする.

定義 A.50. R を整域, K をその商体とする.

(1) $X \subseteq K$ とする. X が R の**分数イデアル**であるとは, 次の 2 条件を満たすときにいう:
(i) X は R 加群である; (ii) $rX \subseteq R$ となる r ($\neq 0$) $\in R$ が存在する.
(K の部分集合だけどそれほど大きいものではなく, 高々 R 倍で R に落ちる.)

(2) R の通常の意味でのイデアルを**整イデアル**といい, 分数イデアルと区別する[*69]. 明らかに, 整イデアルは分数イデアルである.

(3) R の零でないイデアル I に対して,

$$I^{-1} := \{x \in K \mid xI \subseteq R\}$$

とおき, I の**逆イデアル**とよぶ. これは明らかに R の分数イデアルであり, $II^{-1} \subseteq R$ が成り立つ. ただし, $II^{-1} = R$ となるとは限らない. (下の例を参照)

例 A.51. (1) $R = \mathbb{Z}$ とする ($K = \mathbb{Q}$). このとき, $X := \frac{1}{3}\mathbb{Z} := \left\{ \frac{1}{3}n \;\middle|\; n \in \mathbb{Z} \right\}$ は R の分数イデアルだが, 整イデアルではない. また, $I := 3\mathbb{Z} \subseteq \mathbb{Z}$ とおくと, $I^{-1} = X$ である. この場合, $II^{-1} = R$ となる.

(2) $R = \mathbb{Q}[x, y]$ とし, R の (極大) イデアル $I = (x, y)$ を考える ($K = \mathbb{Q}(x, y)$ 有理関数体). このとき, $I^{-1} = R$ (実際, I^{-1} の元は x にかけても y にかけても R に入らないといけない) であり, $II^{-1} = I \neq R$ となる.

イデアルに関する補題を 2 つ用意する.

補題 A.52. 可換ネーター環 R の零でない任意のイデアル I に対して, ある零でない素イデアル $\mathfrak{p}_1, \cdots, \mathfrak{p}_\ell$ が存在して, $\mathfrak{p}_1 \cdots \mathfrak{p}_\ell \subseteq I$ とできる.

[*69] 何もないときの "イデアル" は, だいたい通常の意味でのイデアル.

証明. R のイデアルの集合 $\mathcal{M}$ を次のように定義する:

$$\mathcal{M} := \{I\ (\neq 0) \mid {}^{\forall}\ell > 0, {}^{\nexists}\mathfrak{p}_1, \cdots, \mathfrak{p}_\ell : \text{素イデアル}\ (\neq 0)\ \text{s.t.}\ \mathfrak{p}_1 \cdots \mathfrak{p}_\ell \subseteq I\}.$$

このとき, $\mathcal{M} = \emptyset$ を示したい. (背理法) R はネーターであるから, $\mathcal{M}$ は極大元 J をもつ. $\mathcal{M}$ の取り方から, J は素イデアルでない. よって, $I_1 I_2 \subseteq J,\ I_1, I_2 \nsubseteq J$ となる R のイデアル $I_1, I_2\ (\neq 0)$ が取れる. そこで, $J_1 := J + I_1,\ J_2 := J + I_2\ (\neq 0)$ とおくと, $J_1 J_2 \subseteq J,\ J \subsetneq J_1, J_2$ となる. J の極大性より, $J_1, J_2 \notin \mathcal{M}$ であるから, J_1 も J_2 も有限個の (零でない) 素イデアルの積を含む. これにより, $J \in \mathcal{M}$ も有限個の (零でない) 素イデアルの積を含むことになるから, 矛盾である. □

補題 A.53. デデキント環 R の任意の (零でない) 素イデアル $\mathfrak{p}$ は, $\mathfrak{p}\mathfrak{p}^{-1} = R$ を満たす.

証明. 分数イデアルの定義から, $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R$ である. さらに, デデキント環の定義から, $\mathfrak{p}$ は極大イデアルである. そこで, $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ を否定したい. (背理法) $\mathfrak{p}$ の各元 $p\ (\neq 0)$ に対して, 前補題を適用して, $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_\ell \subseteq (p) \subseteq \mathfrak{p}$ となる (零でない) 素イデアル $\mathfrak{p}_i$ を取る. $\mathfrak{p}_1, \cdots, \mathfrak{p}_\ell$ のうちの $\ell - 1$ 個の積で (p) に含まれるなら, 最初からその個数を ℓ とすればよいので, どの $\ell - 1$ 個の積も (p) に含まれないと仮定してよい.

$\ell = 1$ ならば, デデキント環の定義から $\mathfrak{p}_1$ も極大イデアルだから, $\mathfrak{p}_1 = (p) = \mathfrak{p}$ となる. このとき, $\mathfrak{p}^{-1} = \dfrac{1}{p}R$ となり, $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1} = R$ でダメ. したがって, $\ell \geq 2$ である. $\mathfrak{p}$ は素イデアルより, ある番号 i で $\mathfrak{p}_i \subseteq \mathfrak{p}$ となる: $i = 1$ としてよい. $\mathfrak{p}_1$ も極大イデアルだから, $\mathfrak{p}_1 = \mathfrak{p}$ である. 仮定によって, $\mathfrak{p}_2 \cdots \mathfrak{p}_\ell \nsubseteq (p)$ だから, $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_\ell$ だが $a \notin (p)$ となる元が取れる. このとき,

$$\frac{a}{p}\mathfrak{p}_1 \subseteq \frac{1}{p}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_\ell \subseteq \frac{1}{p}(p) = R$$

より, $t := \dfrac{a}{p} \in \mathfrak{p}_1^{-1} = \mathfrak{p}^{-1}$ である (t は K の元). したがって, $t\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ となる.

ゆえに, $t^n\mathfrak{p} \subseteq t^{n-1}\mathfrak{p} \subseteq \cdots \subseteq \mathfrak{p}$ を得る. つまり, 任意の元 $s\ (\neq 0) \in \mathfrak{p}$ に対して, $st^n \in \mathfrak{p} \subseteq R$. よって, R のイデアルの昇鎖列

$$(st) \subseteq (st, st^2) \subseteq (st, st^2, st^3) \subseteq \cdots$$

を取れるが, R はネーターより, ある番号 n で $(st, \cdots, st^{n-1}) = (st, \cdots, st^{n-1}, st^n)$ となる. 特に, $st^n = \sum_{i=1}^{n-1} r_i(st^i)\ (r_i \in R)$ とかける. R は整域なので両辺を s でわって, $t \in K$ は R 上整, つまり $t \in K_R$ を得る. R はデデキント環 (よって正規環) なので, $R = K_R \ni t = \dfrac{a}{p}$.

しかし, このとき $p \mid a$, つまり $a \in (p)$ となり, a の取り方に矛盾する. □

これで (やっと) 定理 A.48 を証明する準備が整った.

定理 A.48 の証明. (存在) R のイデアルの集合 $\mathcal{M}$ を次で定義する:

$$\mathcal{M} := \{\ \text{有限個の素イデアルの積で表されない } R \text{ の真のイデアル全体}\ \}.$$

$\mathcal{M} \neq \emptyset$ を示したい. (背理法) R はネーターより, $\mathcal{M}$ は極大元 I をもつ. $\mathfrak{p}$ を I を含む極大イデアルとする (ネーター性に関係なく必ず存在する【ツォルンの補題[*70]】). 補題 A.53 より, $I \subseteq I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \overset{\text{A.53}}{=\!=} R \subseteq \mathfrak{p}^{-1}$ となる.

$I = I\mathfrak{p}^{-1}$ と仮定する. もし $R = \mathfrak{p}^{-1}$ ならば, $R = \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p} \neq R$ よりダメ. よって, $R \subsetneq \mathfrak{p}^{-1}$ である: $^{\exists}t \in \mathfrak{p}^{-1} \setminus R$ (t は K の元). 仮定より, $tI \subseteq I\mathfrak{p}^{-1} = I$ となる.

(補題 A.53 証明枠内と同じ議論) なので, $R = K_R \ni t$.

これは t の取り方に矛盾する.

このように, $I \subsetneq I\mathfrak{p}^{-1}$ であることがわかった. I の極大性より, $I\mathfrak{p}^{-1} \notin \mathcal{M}$ である. よって, $I\mathfrak{p}^{-1} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_\ell$ ($\mathfrak{p}_i$: R の素イデアル) とかける[*71]. 補題 A.53 より, 両辺に $\mathfrak{p}$ をかけて, $I = \mathfrak{p}\mathfrak{p}_1\cdots\mathfrak{p}_\ell$ を得る. これは I の取り方に矛盾し, $\mathcal{M} = \emptyset$ となる.

(一意性) 事実 A.46 および補題 A.53 を用いて, 命題 A.16 と同様の議論で示せる[*72]. □

[*70] 選択公理と同値

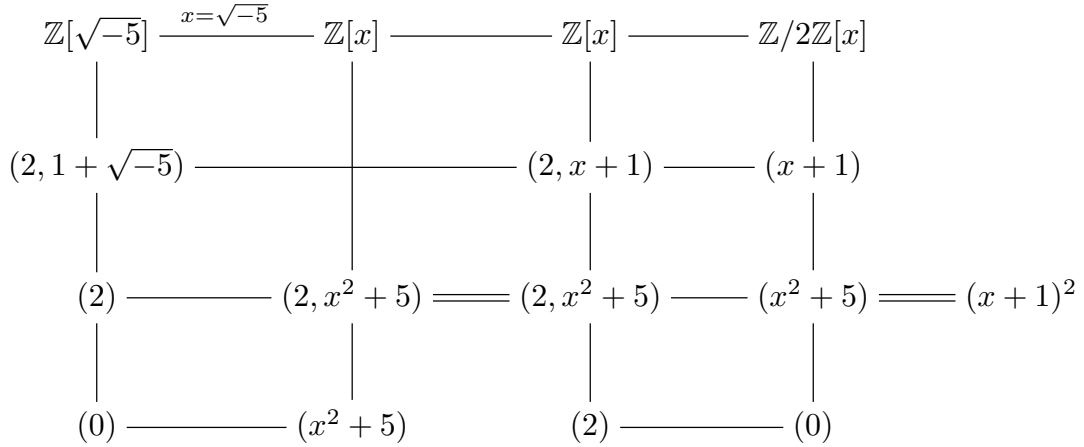
[*71] $I\mathfrak{p}^{-1}$ が R 自身になることもあるが, それも可.

[*72] 命題 A.16 における元の整除 $a \mid b$ ($(a) \supseteq (b)$) を, イデアルの包含 $\mathfrak{a} \supseteq \mathfrak{b}$ に置き換えればよい. このとき, イデアル $\mathfrak{a}$ は $\mathfrak{b}$ を**わり切る**ということもある.

ここで, 素イデアル分解の例を与えよう. (特に整数環の例を与えるが, この場合, 一意分解整域ならば単項イデアル整域[*73]なので, そうでない例を挙げる.)

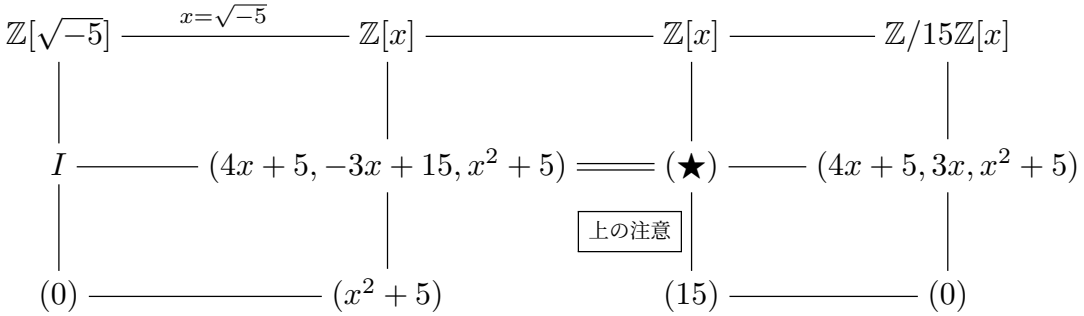
例 A.54. $R = \mathbb{Z}[\sqrt{-5}]$ とする ($K = \mathbb{Q}(\sqrt{-5})$)[*74].

(1) $I = (2)$: 次のように環を (同型を使って) 書き換える:



したがって, $(2) = (2, 1+\sqrt{-5})^2$ である. さらに, $(\mathbb{Z}/2\mathbb{Z}[x])/(x+1) \simeq \mathbb{Z}/2\mathbb{Z}$ より, $(2, 1+\sqrt{-5}) \subseteq \mathbb{Z}[\sqrt{-5}]$ は極大イデアル (よって素イデアル) であることがわかる.

(2) $I = (5+4\sqrt{-5}, 15-3\sqrt{-5})$: 同様に, 環の書き換えを行うが, 少し大変. 命題 A.43(2) より, $\mathrm{N}_{K/\mathbb{Q}}(5+4\sqrt{-5}) = 105, \mathrm{N}_{K/\mathbb{Q}}(15-3\sqrt{-5}) = 270 \in I$, ゆえに $\gcd(105, 270) = 15 \in I$ であることに気をつける.



もう少し書き換えたい. $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ より, $\mathbb{Z}/15\mathbb{Z}[x] \simeq \mathbb{Z}/3\mathbb{Z}[x] \oplus \mathbb{Z}/5\mathbb{Z}[x]$

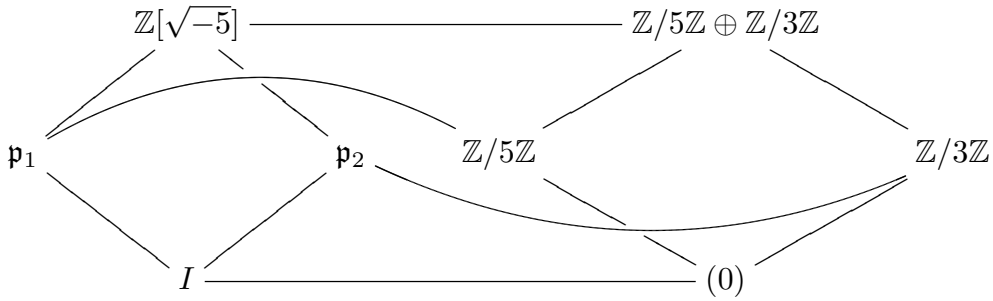
[*73] 素イデアル分解が素元分解から来てしまう.

[*74] これはどの本でも扱われる典型的な例で, 一意分解整域でない整数環の例である.

とできる (係数をわけて考えるだけ). したがって, (係数もそれぞれで簡略化)

$$\begin{aligned}
&(\mathbb{Z}/15\mathbb{Z}[x])\,/(4x+5, 3x, x^2+5)\\
&\simeq (\mathbb{Z}/5\mathbb{Z}[x])\,/(x, x, x^2) \oplus (\mathbb{Z}/3\mathbb{Z}[x])\,/(x+2, x^2+2)\\
&\qquad\quad \boxed{x=0 \text{ を代入}} \qquad\qquad \boxed{x=1 \text{ を代入}}\\
&\simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.
\end{aligned}$$

このように, R/I は次のような構造をもつ:



あとは頑張って, この同型を遡れば, $\mathfrak{p}_1, \mathfrak{p}_2$ がわかる. $\mathbb{Z}[x]$ からの全射を追うと,

$$\begin{array}{ccccccc}
\mathbb{Z}[x] & \longrightarrow & \mathbb{Z}/15\mathbb{Z}[x] & \longrightarrow & \mathbb{Z}/5\mathbb{Z}[x] \oplus \mathbb{Z}/3\mathbb{Z}[x] & \longrightarrow & \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}\\
f(x) & \longmapsto & \overline{f}(x) & \longmapsto & (\overline{f}(x), \overline{f}(x)) & \longmapsto & (\overline{f}(0), \overline{f}(1))
\end{array}$$

である. ここで, $\overline{f}$ はそれぞれで係数をわった多項式を表す. $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ における第一項 $\mathbb{Z}/5\mathbb{Z}$ のみを残すためには, 「$x=1$ して 0」または「係数が 3 の倍数」になればよいので, $\mathfrak{q}_1 = (3, x-1)$ が対応する. 一方, 第二項 $\mathbb{Z}/3\mathbb{Z}$ のみを残すためには, 「$x=0$ して 0」または「係数が 5 の倍数」となればよいので, $\mathfrak{q}_2 = (5, x)$ が対応する. (ちなみに, これらはどちらも, きちんと $\mathbb{Z}[x]$ のイデアル (★) を含んでいる.)
したがって, 最後の $x = \sqrt{-5}$ の対応で戻せば, $\mathfrak{p}_1 = (3, -1+\sqrt{-5})$ および $\mathfrak{p}_2 = (5, \sqrt{-5}) = (\sqrt{-5})$ を得る. (対応を考えれば) $\mathfrak{p}_1$ も $\mathfrak{p}_2$ も素イデアルであり, $I = \mathfrak{p}_1\mathfrak{p}_2$ となっている. 実際に,

$$\mathfrak{p}_1\mathfrak{p}_2 = (3\sqrt{-5}, 5+\sqrt{-5}) \overset{\text{(i)}}{=\!=} (5+4\sqrt{-5}, 3\sqrt{-5}) \overset{\text{(ii)}}{=\!=} (5+4\sqrt{-5}, 15-3\sqrt{-5}) = I$$

(i) $5+4\sqrt{-5} = 3\sqrt{-5} + (5+\sqrt{-5})$; (ii) $15 \in$ (両辺).
(このように, ガチ計算で素イデアルの積を理解することはできるが, 環の書き換えなしにこのような素イデアルが取れるとはとても思えない...)

A.3.1.5 定理 A.32 (ついでに定理 A.31) および定理 A.33(1)

次の定理を示すことが目標である.

定理 A.55. R をネーター正規環, K をその商体, $K \subseteq L$ を標数零の体の有限次拡大とする. また, $S := L_R$ を R の L における整閉包とする. このとき, 次が成り立つ.

(1) S は有限生成 R 加群である;
(2) S もネーター環である;
(3) R が単項イデアル整域ならば, $S \simeq R^d$ (R 加群として) である. ここで, $d := [L : K]$.

これを使って, 定理 A.32 および定理 A.33(1) を先に示そう.

定理 A.32 および定理 A.33(1) の証明. 定理 A.55 を次のように適用すればよい:

$$R \rightsquigarrow \mathbb{Z}\ (K \rightsquigarrow \mathbb{Q}),\ L \rightsquigarrow K\ (S \rightsquigarrow \mathcal{O}_K).$$

このとき, 定理 A.32 = 定理 A.55(3), および, 定理 A.33(1) = 定理 A.55(2) となる. □

注意 A.56. 定理 A.55 において, R がネーターであることが必要である.

定理 A.31 の後半の主張は, 定理 A.32 における $d = 2$ の場合である. $\mathbb{Q}(\sqrt{A})$ の整数環が決定されれば, その $\mathbb{Z}$ 基底を求めることは容易であるから, $\mathbb{Q}(\sqrt{A})$ の整数環を求める.

まず, トレースの定義と事実を述べる. 以下はそれぞれ, 定義 A.40, 例 A.41, 命題 A.42, 命題 A.43 に対応して, 証明も同様に与えられる.

定義 A.57. $K \subseteq L$ を標数零の体の d 次拡大とし, $\mathrm{Hom}_K^{\mathrm{alg}}(L, \overline{K}) = \{\sigma_1, \cdots, \sigma_d\}$ とおく. このとき, $a \in L$ に対して,

$$\mathrm{Tr}_{L/K}(a) := \sum_{i=1}^{d} \sigma_i(a)$$

を a の**トレース**という.

例 A.58. 2 次体 $\mathbb{Q}(\sqrt{A})$ において, $\mathrm{Tr}_{L/K}(a + b\sqrt{A}) = (a + b\sqrt{A}) + (a - b\sqrt{A}) = 2a$.

命題 A.59. 定義 A.57 の状況で, $\mathrm{Tr}_{L/K} : L \to K$ は K 線型写像である.

命題 A.60. R を正規環, K をその商体, $K \subseteq L$ を標数零の体の有限次拡大とする. また, $S := L_R$ を R の L における整閉包とする. このとき, $s \in S$ ならば, $\mathrm{Tr}_{L/K}(s) \in R$.

そこで, 定理 A.31 を示す.

定理 A.31 の証明. 例 A.41, A.58 のように, $t := a + b\sqrt{A} \in \mathcal{O}_{\mathbb{Q}(\sqrt{A})}$ に対して,

$$\mathrm{N}_{L/K}(t) = a^2 - Ab^2,\ \mathrm{Tr}_{L/K}(t) = 2a \in \mathbb{Z} \text{ (命題 A.43, A.60)}$$

である. よって, $a = \dfrac{a'}{2}$ $(a' \in \mathbb{Z})$ となる. さらに,

$$4\mathbb{Z} \ni 4\,\mathrm{N}_{L/K}(t) = 4(a^2 - Ab^2) = a'^2 - 4Ab^2$$

より, $4Ab^2 \in \mathbb{Z}$ を得る. A は平方因子をもたない整数なので, b の分母は 1 か 2 である. (± は分子に任せる.) そこで, $b = \dfrac{b'}{2}$ $(b' \in \mathbb{Z})$ とかく. (b' が偶数ならば b の分母は 1.)

(i) b' が偶数ならば $b \in \mathbb{Z}$ であり, $\mathbb{Z} \ni \mathrm{N}_{L/K}(t) = a^2 - Ab^2$ より, $a^2 \in \mathbb{Z}$, つまり $a \in \mathbb{Z}$.

(ii) b' が奇数ならば, $a'^2 - Ab'^2 \in 4\mathbb{Z}$ であるが, $b' \equiv 1 \pmod 4$ より, $A \equiv a'^2 \equiv 0, 1 \pmod 4$ となる. A は平方因子をもたないから, 結果的に, $A \equiv 1 \pmod 4$ とならなければいけない. (したがって, a' も奇数でなければいけない.)

(1) $A \equiv 2, 3 \pmod 4$ と仮定する. このとき, (ii) は起こらず (i) のみが起こる. よって, $t = a + b\sqrt{A} \in \mathbb{Z}[\sqrt{A}]$. 逆の包含は明らかだから, $\mathcal{O}_{\mathbb{Q}(\sqrt{A})} = \mathbb{Z}[\sqrt{A}]$ であることがわかる.

(2) $A \equiv 1 \pmod 4$ と仮定する. (このとき, (i) も (ii) も起こる.) $\omega := \dfrac{1 + \sqrt{A}}{2}$ は $x^2 - x + \underbrace{\dfrac{1 - A}{4}}_{\mathbb{Z}} = 0$ の解となるから, $\omega \in \mathcal{O}_{\mathbb{Q}(\sqrt{A})}$ である; ゆえに, $\mathcal{O}_{\mathbb{Q}(\sqrt{A})} \supseteq \mathbb{Z}[\omega]$.

逆に,

$$t = a + b\sqrt{A} = \left\{ \begin{array}{ll} (a - b) + 2b\omega & \text{(i) } a, b \in \mathbb{Z}; \\ \dfrac{a' - b'}{2} + b'\omega & \text{(ii) } a', b' \text{ 奇数} \end{array} \right\} \in \mathbb{Z}[\omega]$$

となるから, $\mathcal{O}_{\mathbb{Q}(\sqrt{A})} = \mathbb{Z}[\omega]$ を得る. □

注意 A.61. $R := \mathbb{Z}[\sqrt{A}]$ $(A \equiv 2, 3 \pmod 4)$; $\mathbb{Z}[\omega]$ $(A \equiv 1 \pmod 4)$ とおいたとき, 上の証明において, $R \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{A})}$ であることを確かめることは難しくないので, 逆の包含を示すことが肝心であった. ここで, $\mathbb{Z}$ 加群として $R \simeq \mathbb{Z}^2$ であることを確かめることも難しくないが, 定理 A.32 を先に示しているので, $\mathbb{Z}$ 加群として $\mathcal{O}_{\mathbb{Q}(\sqrt{A})}$ も $\mathbb{Z}^2$ と同型であることがわかっている. ゆえに, $\mathbb{Z}$ 加群としての単射 $\mathbb{Z}^2 \to \mathbb{Z}^2$ があることがわかるが, しかし! これをすぐに同型としてはいけない. (これが体上ベクトル空間と $\mathbb{Z}$ 加群の大きな違いの一つ.) 例えばもっと極端に ("1 次元" の場合), $\mathbb{Z} \to \mathbb{Z}$ $(n \mapsto 2n)$ は $\mathbb{Z}$ 加群の間の単射であるが, 全射ではない. (ベクトル空間では, 次元が等しいベクトル空間の間の単射線型写像は自動的に全射になる.)

(♢) さて, ここから目標である定理 A.55 の証明に話を戻そう. まずは, 設定を思い出す:
① R : ネーター正規環; ② K : R の商体 (標数零); ③ L : K の d 次拡大体;
④ $S := L_R$: R の L における整閉包.
さらに, 上の設定から次のように記号をおく:

- $\{x_1, \cdots, x_d\} \subseteq L$: L の K 基底; − $\widetilde{L}$: L の K 上のガロア閉包 (命題 A.42);
- $\mathrm{Hom}_K^{\mathrm{alg}}(L, \overline{K}) := \{\sigma_1, \cdots, \sigma_d\} = \mathrm{Hom}_K^{\mathrm{alg}}(L, \widetilde{L})$ (補題 A.39 および命題 A.42);
- 各 σ_i は $\mathrm{Hom}_K^{\mathrm{alg}}(\widetilde{L}, \widetilde{L})$ $(:= \mathsf{Gal}(\widetilde{L}/K))$ の元に延長できる[*75](補題 A.39).

証明の方針は次である:

(1) S を含む有限生成 R 加群を構成する $\overset{A.21}{\rightsquigarrow}$ (R がネーターより) S も有限生成 R 加群.
(2) I を S のイデアルとする. R 加群としても $I \subseteq S$ だから, (1) および命題 A.21 より, I も有限生成 R 加群である. $R \subseteq S$ より, I は有限生成 S 加群[*76]でもあり, つまり, イデアルとして有限生成である. よって, S がネーター環であることがわかる.
(3) いろいろ準備が必要 (**単因子論**).

まずは, (1) から確認しよう.
$U := (\sigma_i(x_j))_{ij}$ ($\widetilde{L}$ 上 d 次正方行列) とおく. 最初の主張は次.

主張. 正方行列 U は正則である.

証明. 各行ベクトル $\boldsymbol{u}_i$ が ($\widetilde{L}$ 上) 一次独立であることを示せばよい. $\sum_{i=1}^d a_i \boldsymbol{u}_i = 0$ ($a_i \in \widetilde{L}$) とおく. 第 j 成分に注目して (縦にたして), 各 j で $\sum_i a_i \sigma_i(x_j) = 0$ を得る. 任意の L の元は $x_1, \cdots, x_d$ の一次結合でかけるから, $\sum_i a_i \sigma_i$ は写像 $L \to \widetilde{L}$ として零である. 写像 $L \to \widetilde{L}$ 全体の集合は, $\widetilde{L}$ 上のベクトル空間をなし, 積を保つ相異なる元たちは一次独立になる[*77]から, $\sum_i a_i \sigma_i = 0$ より, $a_i = 0$ を得る. ■

以下, 補題 A.38 より, $\{x_1, \cdots, x_d\} \subseteq S$ となるように取る. このとき, $\sigma_i(x_j)$ も R 上整であり, 行列式の定義 (成分の和差積) から, $u := |U|$ も R 上整な $\widetilde{L}$ の元である. また, 上の主張から $u \neq 0$.

次が重要な主張である.

[*75] 延長も同じ σ_i で表す.

[*76] (加群論を使ってちょっと高度に) 全射な R 準同型 $R^\ell \twoheadrightarrow M$ があるから, ($- \otimes_R S$ を施して) 全射な S 準同型 $S^\ell \twoheadrightarrow M \otimes_R S \twoheadrightarrow M$ がある.

[*77] (ベクトル空間になること) 終域が体だから. (一次独立について) 数学的帰納法を適用し, 一次独立を確かめるための式 $\sum_i a_i \chi_i = 0$ に対して, 写像に x を代入したものの全体に $\chi_1(\alpha)$ をかけたもの, および, 写像に $x\alpha$ を代入したものを比較せよ. ここで, α は, $\chi_1 \neq \chi_2$ より, $\chi_1(\alpha) \neq \chi_2(\alpha)$ となる定義域の元とする.

主張. [*78] 次が成り立つ:

(1) $u^2 \in R$;
(2) $a_i \in K$ で $x := \sum_i a_i x_i \in S$ ならば, すべての番号 i で $u^2 a_i \in R$.

証明. $\sigma \in \mathsf{Gal}(\widetilde{L}/K)$ とする. 行列式の定義から $\sigma(u) = \det(\sigma\sigma_i(x_j))_{ij}$ となるが, σ は $\sigma_1, \cdots, \sigma_d$ の置換を引き起こすから, 行列 $(\sigma\sigma_i(a))_{ij}$ は U に対して行の入れ替えを行っただけの行列である; ゆえに, $\sigma(u) = \det(\sigma\sigma_i(x_j)) = \pm u$. よって, $\sigma(u^2) = u^2$, ガロアの基本定理より $u^2 \in K$ である. u^2 は R 上整だから, $u^2 \in K_R = R$ (R は正規環) を得る.

$y_i := \sigma_i(x) \in \widetilde{L}$ ($x \in S$ より, これらも R 上整) とおき, 仮定で与えられた式を行列で書き直すと,

$$U \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} \sum_i a_i \sigma_1(x_i) \\ \vdots \\ \sum_i a_i \sigma_d(x_i) \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix}$$

となる. U の余因子行列 $\widetilde{U}$ はまた, R 上整な $\widetilde{L}$ の元を成分にもち[*79], $U^{-1} = u^{-1}\widetilde{U}$. したがって, $a_i = u^{-1} \cdot (R$ 上整な $\widetilde{L}$ の元の和差積) となるから,

$$K \ni u^2 a_i = u \cdot (R \text{ 上整な } \widetilde{L} \text{ の元の和差積}) : R \text{ 上整},$$

よって, $u^2 a_i \in K_R = R$ を得る. ■

定理 A.55(1)(2) の証明を与えよう.

定理 A.55(1)(2) の証明. 上で行った考察 (方針) から, $S \subseteq M$ となる有限生成 R 加群を構成すればよい. そこで, $M := \langle u^{-2}x_1, \cdots, u^{-2}x_d \rangle_R = \left\{ \sum r_i (u^{-2}x_i) \;\middle|\; r_i \in R \right\}$ ($\subseteq L$) とおく. (前主張より $u^2 \in R$ だから, $u^{-2} \in K$ である.) また, S ($\subseteq L$) の任意の元は $x_1, \cdots, x_d$ の K 上一次結合でかけるから, (無理矢理 u^{-2} でくくれば) $S \subseteq M$ であることがわかる. □

次に, 定理 A.55(3) を示したい. しかし, 長くなりそうなので, この部分節はここで一旦切って次の節にぶん投げる.

[*78] この主張には, R のネーター性は必要ない.

[*79] 余因子行列の定義より, $\widetilde{U}$ は U の各 i 行 j 列を引っこ抜いて行列式を取ってからの全体の転置. どの操作でも R 上整な $\widetilde{L}$ の元の和差積.

A.3.1.6 単因子論

定理 A.55(3) の証明において, 最も大切な理論が次に挙げる**単因子論**である (代数学特論 BI)[*80] . それは, **有限生成アーベル群の基本定理** (代数学 II) の一般化である ($R = \mathbb{Z}$).

定理 A.62 (単因子論)**.** 単項イデアル整域 R 上の任意の有限生成 R 加群 M は,

$$R^{\ell} \oplus R/(a_1) \oplus \cdots \oplus R/(a_n) \quad (\text{ただし}, (a_{i+1}) \supseteq (a_i))$$

と同型である. さらに, ℓ および $a_i \in R$ は (M によって) 一意的に決まる[*81].

$R = \mathbb{Z}$ の場合の単因子論が次である.

系 A.63 (有限生成アーベル群の基本定理)**.** 任意の有限生成アーベル群は, (群として) $\mathbb{Z}^{\ell} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z}$ (ただし, $n_{i+1} \mid n_i$) と同型である. 特に, (加法群を自然に $\mathbb{Z}$ 加群とみて) それは $\mathbb{Z}$ 加群としての同型でもある.

注意 A.64. 定理 A.32 を証明するだけであれば, 定理 A.55(1) と有限生成アーベル群の基本定理で十分である ($\mathcal{O}_K$ が整域であることも注意). ここでは, せっかく定理 A.55 まで一般化したので, それを証明することにする.

定理 A.62 の直和分解 $M \simeq R^{\ell} \oplus \bigoplus R/(a_i)$ における $\bigoplus R/(a_i)$ を M の**ねじれ部分**という. これはつまり, $am = 0$ となる a ($\neq 0$) $\in R$ が存在するような $m \in M$ (**ねじれ元**) たちのことである. M のねじれ元全体の集合を M_{tor} とかくと, これは M の部分 R 加群をなす. また, $(M/M_{\mathrm{tor}})_{\mathrm{tor}} = \{0\}$ となる. 有限生成加群に対しては, このねじれ部分があるかどうかが自由加群 R^{ℓ} かどうかを決める.

定理 A.65. R を, イデアルがすべて自由加群となるネーター整域とする. このとき, 有限生成 R 加群 M に対して, 次は同値である:

(1) M は自由加群である;
(2) M はある自由 R 加群の部分加群である;
(3) $M_{\mathrm{tor}} = 0$.

証明. (1) $\overset{\text{自明}}{\Longrightarrow}$ (2) $\overset{\text{整域}}{\Longrightarrow}$ (3). そこで, $M_{\mathrm{tor}} = 0$ と仮定する ($M \neq 0$ としてよい). M の生成元を $\{m_1, \cdots, m_{\ell}\}$ とし, (必要なら順番を入れ替えて) そのうち一次独立となる最大の

[*80] この節では, どうしても加群論を扱うことになる.
[*81] $(a_i) = (b_i)$ の意味で.

部分集合を $\{m_1, \cdots, m_{\ell'}\}$ とする ($M_{\mathrm{tor}} = 0$ より一つは残る): $N := \langle m_1, \cdots, m_{\ell'} \rangle_R \simeq R^{\ell'}$ とおく. 最大性より, $\ell'+1 \leq i \leq \ell$ に対して, $a_i m_i = \sum_{j=1}^{\ell'} b_j m_j$ となる a_i ($\neq 0$) $\in R$ が取れる. M の任意の元 m は $m_1, \cdots, m_\ell$ の R 上一次結合でかけるから, ($a = \prod a_i$ とでもおけば) $am \in N$ とできる (R は整域より $a \neq 0$). このとき, $M \to N$ ($m \mapsto am$) は, $M_{\mathrm{tor}} = 0$ より単射 R 準同型である (2).

(簡単のため記号を取り直して) $M \subseteq R^\ell$ とする. このとき, M も自由加群であることをランク ℓ に関する帰納法で示す. $\ell = 1$ のとき, M は R のイデアルを意味するから, 仮定より従う. $\ell > 0$ とする. R 準同型 $\varphi : M \subseteq R^\ell \xrightarrow{\text{第一成分}} R$ を考える. $\mathrm{Im}\,\varphi$ は R の部分加群, つまりイデアルだから, 仮定より自由加群になる. 命題 A.22(2) より, $M \overset{\varphi}{\twoheadrightarrow} \mathrm{Im}\,\varphi \simeq R^{k}$[*82]は分裂する: $M \simeq R^k \oplus \mathrm{Ker}\,\varphi$. R はネーターより $\mathrm{Ker}\,\varphi$ も有限生成で, $\mathrm{Ker}\,\varphi = M \cap \underset{\text{第 } 2\sim\ell \text{ 成分}}{R^{\ell-1}} \subseteq R^{\ell-1}$ より, 帰納法の仮定を適用して, $\mathrm{Ker}\,\varphi$ は自由加群 R^{n}[*83]となる. よって, $M \simeq R^{k+n}$ であることがわかる. □

注意 A.66. 上の定理において, R は「イデアルがすべて自由加群となる」ネーター整域と仮定した. これは結局, 「単項イデアル整域」と同値である. ここでは, ネーター性を外して, 【有限生成イデアルがすべて自由加群 $\Leftrightarrow$ 有限生成イデアルは単項イデアル[*84]】を確認しよう.

証明. I ($\neq 0$) を R のイデアルで $I = (a)$ とする. このとき, $R \simeq I$ ($r \mapsto ar$) を得る.

逆に, R の有限生成イデアル I ($\neq 0$) は自由加群とする; $I \subseteq R$ より $I \simeq R$. このとき, $1 \in R$ に対応する I の元を a とおけば, $I = (a)$ となることを簡単に確認できる. ■

以下, R を可換ネーター環とする.

単因子論で何を行っているかを説明する.

R 加群 M, N に対して, R 準同型全体の集合を $\mathrm{Hom}_R(M, N)$ とかくことにする. このとき, R 加群として $\mathrm{Mat}_{\ell_2 \times \ell_1}(R) \simeq \mathrm{Hom}_R(R^{\ell_1}, R^{\ell_2})$ ($A \mapsto A \times -$) となる[*85].

有限生成 R 加群 M に対して, 全射 R 準同型 $R^{\ell_2} \twoheadrightarrow M$ があるが, (R のネーター性よ

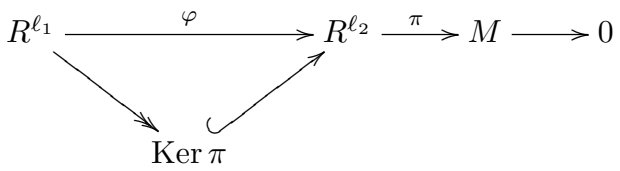
[*82] 実際には, $R^k \subseteq R$ より, $k = 1$ となる ($\varphi \neq 0$).

[*83] これについても $n \leq \ell - 1$.

[*84] このような整域を**ベズー整域**という.

[*85] 縦ベクトルを使う. 証明は線型数学 (R が体のとき) と同じ.

り) これの核も有限生成であるから, もう一つ全射 R 準同型が伸びる:



このとき, φ は R 上の行列 A と対応している ($\varphi(x) = Ax$). (線型数学のときと同じように) 行列の基本変形はいくつかの基本行列の積 (正則行列) をかけることにより得られる. 正則行列は同型写像と対応しているから, 同型を通して次のように書き換えられる:

$$\begin{array}{ccccccc} R^{\ell_1} & \xrightarrow{A} & R^{\ell_2} & \longrightarrow & M & \longrightarrow & 0 \\ {\scriptstyle X}\downarrow{\scriptstyle \simeq} & & {\scriptstyle \simeq}\downarrow{\scriptstyle Y} & & \downarrow{\scriptstyle \simeq} & & \\ R^{\ell_1} & \xrightarrow[A']{} & R^{\ell_2} & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

ここで, A', X, Y は R 上の行列で, $A' = YAX^{-1}$ となる[*86].

このとき, **うまく基本変形を取ることができれば**,

$$A' = \left(\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & 0 \\ & & a_n & \\ \hline & & & 0 \\ & 0 & & \ddots \\ & & & & 0 \end{array}\right) \tag{A.1}$$

とできて, A' の余核 (商) を取ることで, $M \simeq M' \simeq R/(a_1) \oplus \cdots \oplus R/(a_n) \oplus \underbrace{R \oplus \cdots \oplus R}_{\ell}$ (ここで, ℓ は A' の右下の零ブロックのサイズ) を得られるはずである. このときに A' の対角線に出てくる $a_1, \cdots, a_n, 0, \cdots, 0$ を A の**単因子**という.

このように, 準同型に対応する行列 A に基本変形を施すことで, 「どのくらい良い行列に変形できるか」が (線型数学と同様に) 重要である. R が体 (普通の線型数学) の場合は, 基礎環が【体】であることから, どの行列に対しても $a_1 = \cdots = a_n = 1$ とすることが可能だった (逆元, もっと言えば, 分数が使えた). しかし, 普通はうまくいかないことは明白だろう (R の元の和差積しか使えない).

[*86] 線型数学での表現行列を思い出そう. X と Y は基底変換の行列に対応する.

単因子論では, (R が単項イデアル整域であれば) このような基本変形が可能であり, さらに, a_i たちの間に約・倍の関係まであることを主張している. 百聞は一見に如かずなのだが, ただの行列の基本変形のため, 練習問題として読者に委ねる.

練習問題 A.67. $R = \mathbb{Z}, \mathbb{Z}[\sqrt{-1}], \mathbb{Q}[x]$ (どれもユークリッド整域, ゆえに単項イデアル整域) のそれぞれに対して, R を成分にもつ適当な $\ell_2 \times \ell_1$ 行列を取って, 単因子を求めよ.

さて, これを考慮に入れて, 定理 A.62 を証明しよう.

定理 A.62 の証明. $L := \operatorname{Im}\varphi = \operatorname{Im}(A \times -) = \operatorname{Ker}\pi \subseteq R^{\ell_2}$ とおく. 定理 A.65 より, L は自由加群であり, 命題 A.22(2) より, 全射 $R^{\ell_1} \twoheadrightarrow L$ は分裂する: $R^{\ell_1} \simeq L \oplus \operatorname{Ker}\varphi$. ここまでの行列 A の変換 A' を同型を無視して $(A.1)$ のように書き直すと,

$$A' = \left(\begin{array}{c|c} L & 0 \\ \hline 0 & 0 \end{array}\right)$$

のようになっている. なお, 右下の零行列は $\operatorname{Ker}\varphi$ に対応している.

したがって, 残りでは $R^n \simeq L \subseteq R^{\ell_2}$ に対して, (同型を通して) R^n の各因子が R^{ℓ_2} の各因子に対応していることを示せばよい. 定理 A.65 の証明より, L の自由加群としての分解は, $L \subseteq R^{\ell_2}$ の各成分への射影で得ることができた. さらに, その合成 $L \subseteq R^{\ell_2} \xrightarrow{\text{第 } i \text{ 成分}} R$ の像 L_i は R のイデアルであり, R は単項イデアル整域だから, $L_i = (a_i)$ となる $a_i \in R$ が存在する. これはつまり, (同型を通して[*87]) $L \simeq \bigoplus_i L_i = \bigoplus_i (a_i) \underset{\text{各成分}}{\subseteq} R^{\ell_2}$ となることを意味している. したがって, 上の A' は同型を無視して,

$$A' = \left(\begin{array}{ccc|c} a_1 & & & \\ & \ddots & & 0 \\ & & a_n & \\ & & & 0 \\ \hline & 0 & & 0 \end{array}\right)$$

と変形できることがわかる; ここまでの変形で, $M \simeq \bigoplus_i R/(a_i) \oplus R^{\ell}$ を得られる.

(ここまででは, 最初の行列 A に対しての a_i たちの一意性はまだあやしい[*88]. ただし,

[*87] 順番も変えている.

[*88] 例えば, $R = \mathbb{Z}$ において, $A_1 = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$ は $A_2 = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$ と同型の加群 M を与える. 単因子論では, A_2 の見方での一意性を主張している. (この例を見れば, この後何をしたいか・すべきかがわかるかも.)

a_i はイデアル L_i で決まる.)

中国式剰余定理 (補題 A.75[*89]) を繰り返し使えば, a_i たちに約・倍の関係 $(a_i) \supseteq (a_{i+1})$ を入れることができる[*90][*91].

一意性を示すことが残っている. 有限生成 R 加群 M と N が同型ならば, その同型射は $M_{\mathrm{tor}} \simeq N_{\mathrm{tor}}$ を誘導するから, 自由部分とねじれ部分のそれぞれで一意性を確認すればよい. 自由部分についてはランクの一意性からよいだろう; つまり, ℓ は一意的に定まる.

ねじれ部分について, (上でおこなったように) 中国式剰余定理を適用して, 素元べきで並べれば,

$$M_{\mathrm{tor}} \simeq \bigoplus_p \Big(R/(p^{e_{1_p}}) \oplus \cdots \oplus R/(p^{e_{k_p}}) \Big) \quad (\text{ただし, } e_{1_p} \geq \cdots \geq e_{k_p} \text{ とする.})$$

とできる. (ここで, $M := M_{\mathrm{tor}}$ とかき直す.) さらに, 素元 $p \neq q$ ならば, $(p^{e_{1_p}})$ と (q^e) は互いに素だから, $M/p^{e_{1_p}}M$ は p 部分だけを残す:

$$M/p^{e_{1_p}}M \simeq R/(p^{e_{1_p}}) \oplus \cdots \oplus R/(p^{e_{k_p}}).$$

これも同型で不変だから, 改めて $M := M/p^{e_{k_p}}M$ とおき直す. (e_{i_p} も単に e_i とかこう.)

このとき, 各 j で $p^{e_j-1}M/p^{e_j}M$ を考えると,

$$p^{e_j-1}M/p^{e_j}M \simeq \bigoplus_{i=1} (p^{e_j-1})/(p^{e_j}) \oplus \cdots \oplus \bigoplus_{i=j} (p^{e_j-1})/(p^{e_j}).$$

これは $R/(p)$ (体) 加群 (よってベクトル空間) としての分解でもあるから, 因子の個数は一意的に決まる. つまり, $e_1 \geq \cdots \geq e_k$ の並びがただ一つに定まることを意味している. このように, ねじれ部分も一意的に決まることがわかる. □

(有限生成)R 加群 M が**直既約**であるとは, $M \simeq M_1 \oplus M_2$ と分解できれば $M_1 = 0$ または $M_2 = 0$ が成り立つときにいう.

事実 A.68. 単項イデアル整域 R に対して, $R/(p^n)$ (p は素元または零) は有限生成直既約加群全体を表す.

[*89] 前後が逆になったが, この節が重くなるため, このままにしようと思っている...

[*90] 主張の包含 $(a_i) \subseteq (a_{i+1})$ と逆になっているが, 証明内では右下に 0 を書きたい, つまり, 左上に行くほど約元を出したかったので, このように書いている. 最後に番号を取り替えてひっくり返せばよいだろう.

[*91] もう少し詳しく述べると, 互いに素となるイデアルでくっつけたり, 分けたりすればよい. 実際には, 各 a_i を素元分解 (PID より UFD) して, 素元べきで並べてから適切にくっつければよい. この操作で, 因子 $R/(a_i)$ の個数 n も変わる可能性はある.

証明. 定理 A.62 の一意性の証明と同様の議論をすればよい. ($p = 0$ なら定理 A.65 とランクの比較, $p \neq 0$ ならば p でわってベクトル空間に持ち込む.) ■

補足 A.69 (vs. **クルル–シュミット性** (B.1 節))**.** 数における素因数分解の存在と一意性のように, (有限生成) 加群に対しても直既約加群 (有限個) の分解の存在と一意性がほしい. 単因子論では, 単項イデアル整域に対してそれを保証しているわけだが, 一般には (既約元と素元のように) 直既約加群での分解では一意性が担保されない. そればかりか, 様々なところで "良くない (都合が悪い)" ことが起こる. それらを一気に解決してくれる性質が**クルル–シュミット性**である. これによって, ある種の「最小性」を様々なところで取ることができる. 例えば, 有限生成 R 加群 M に対して, 自然な全射 $R^\ell \twoheadrightarrow M$ が取れたが, これを '最小' に取りたい. (R^ℓ のうちの '無駄' を取り除きたい[*92].) クルル–シュミット性を満たすとそれが可能であり, そのような「最小」の射影加群を M の**射影被覆**[*93]という.

注意 A.70. 有理整数環 $\mathbb{Z}$ (PID) の有限生成加群たち (加群圏 $\mathsf{mod}\,\mathbb{Z}$) は, (アーベル圏だが) クルル–シュミット性を満たさない. 例えば, $\mathbb{Z}$ 上の加群 $\mathbb{Z}/6\mathbb{Z}$ を考えてみると, (中国式剰余定理より) $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ となるが, 左辺で見ると $\mathbb{Z}$, 右辺で見ると $\mathbb{Z} \oplus \mathbb{Z}$ を "射影被覆" として取りたくなる. しかし, この場合どちらを M の "射影被覆" としてよいのか (同型を通してみないと) わからない[*94]

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/6\mathbb{Z} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\simeq} \\ \mathbb{Z} \oplus \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \end{array}$$

実際には, 上の φ は分裂するから, 左辺で見たときのランク 1 の自由加群 $\mathbb{Z}$ が一番小さい.

注意 A.71. 定理 A.62 の証明の第一段落では, 単項イデアル整域ほど強くなくてもよい. 具体的には, 【自由加群の部分加群が射影的である】くらいの仮定で十分である. このような環を**遺伝的**という. 例えば, デデキント環が良い例である (A.4.4 節).

これで (やっと) 定理 A.55(3) を証明する準備が整った.

定理 A.55(3) の証明. 定理 A.55(1) より, S は有限生成 R 加群である. また, S は整域だ

[*92] R^ℓ のうちの無駄 $= M$ に影響を与えない R^ℓ の直和因子 (つまり, 射影加群)

[*93] M によって一意に定まる.

[*94] 同型で "射影被覆" の取り方が変わる. また, 直和因子のそれぞれの "射影被覆" の直和が, もとの "射影被覆" にならない. だから, "射影被覆" を考えられない.

からねじれ部分は零となる．今, 仮定から R は単項イデアル整域だから, 単因子論を発動させて, $S \simeq R^{\ell}$ を得る．

最後に, S のランク ℓ を求めよう; $\ell = d$ を示したい．前節の最後 ((♢) 以降) を思い出すと, S の中で L の K 基底 $\{x_1, \cdots, x_d\}$ を取り, さらに, S を含む自由加群 M を得た．このとき, $\underset{\text{ランク } d}{\langle x_1, \cdots, x_d \rangle_R} \subseteq \underset{\text{ランク } \ell}{S} \subseteq \underset{\text{ランク } d}{M}$ となるから, $d \leq \ell \leq d$ より, $\ell = d$ である． □

単因子論をせっかくやったので, **ジョルダン標準形**との関係を話したくなるが, また今度 (A.6 節)

A.3.1.7 まとめ (感想) と注意

これでようやく, この節の冒頭で挙げた事実をすべて証明することができた．かなりの知識と積み重ねが必要だったが, とても興味深く勉強になることが多かった．もちろん, 整数環についての理論は多岐にわたり, その研究もまだまだ続いているため, これらは整数環の初歩に過ぎないと思うが, 非常に奥が深い理論を学ぶことができたと感じている．

今後も整数環に関する面白い事実が出てきたら, その都度更新していこうと思っている．

注意 A.72. 証明の所々で, 【体の標数は零】という仮定が出てきた．(整数環を考えるだけであれば, この仮定を課してもなんら問題ない.) この仮定は, (埋もれがちだが) 補題 A.39 で重要な役割を果たしている．その証明を見てみるとわかるが, 「方程式が重解をもたない」という箇所でこの仮定が効いている．(証明では, 拡大次数とある方程式の解の個数を比べている.)

そのため, 「重解をもたないような体の代数拡大」であれば, 同様の議論が働くわけだが, そのような拡大を**分離拡大**[*95]という．標数が零であれば, 代数拡大はいつでも分離拡大となる．また, 例えば $K := \mathbb{Z}/3\mathbb{Z}$ 上の既約多項式 $f(x) = x^6 + x^3 - 1$ を考えると, ($\overline{K}$ で) $f(x) = (x-\alpha)^3(x-\beta)^3$ と因数分解できるため, $K(\alpha)$ は K の分離拡大ではない[*96].

[*95] (もう少し正確に) 代数拡大 $K \subseteq L$ が**分離拡大**とは, L の任意の元が ($\overline{K}$ で) 重解をもたない K 上最小多項式をもつときにいう．重解をもたない (もつ) 既約多項式を *(非)* **分離的**という:

- $f(x) \in K[x]$ が非分離多項式 $\Leftrightarrow f'(x) = 0$ (多項式として)
- $\operatorname{char} K = p$ ($\neq 0$); $f(x)$ が非分離 $\Leftrightarrow f(x) = f_s(x^{p^e})$ となる K 上既約な分離多項式 $f_s(x)$ がある．上の既約分離多項式 $f_s(x)$ を $f(x)$ の**被約多項式**, 被約多項式が一次式となる非分離多項式 $f(x)$ を**純非分離多項式**という．

[*96] この場合, $f(x)$ の被約多項式は $f_s(x) = x^2 + x - 1$.

A.3.2 整数環のイデアル類群

A.4.5 節参照.

A.3.3 整数環の話題

A.4 デデキント環

A.3.1.4 節において, デデキント環を勉強していたら面白くなったので, もう少し深く追及してみることにする.

A.4.1 イデアル群

補題 A.53 では, 「$\mathfrak{p}$ が逆元 $\mathfrak{p}^{-1}$ をもつ」ことを示唆している. これを念頭におくと, ある群の存在が浮かび上がる. つまり, デデキント環 R に対して, R の零でない分数イデアル全体の集合を $\mathcal{X}_R$ とおくと, これに群の構造が入る.

定理 A.73. デデキント環 R に対して, $\mathcal{X}_R$ は (分数) イデアルの積に関してアーベル群をなす (R の**イデアル群**). さらに, これは素イデアルで生成される自由 $\mathbb{Z}$ 加群である[*97].

証明. $\mathcal{X}_R$ において, 積が演算になること, および, 結合律が成り立つこと, 単位元 R が存在することは明らかである. また, $\mathcal{X}_R$ が群をなせば, それはアーベルであることも明らかである. そのため, 次を示せばよい:
(i) 逆元の存在; (ii) 素イデアルで生成される; (iii) 自由加群.

(i)(ii) $X \in \mathcal{X}_R$ とする. 分数イデアルの定義より, ある $r \in R$ が存在して, $rX \subseteq R$ は整イデアルとなる. 定理 A.48 より, $rX = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell$ となる素イデアル $\mathfrak{p}_i$ が取れる. さらに, $(r) \subseteq R$ にも適用して, $(r) = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ となる素イデアル $\mathfrak{q}_i$ が存在する. 補題 A.53 より, $X = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_m^{-1}$ となるから, $Y := \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_\ell^{-1} \mathfrak{q}_1 \cdots \mathfrak{q}_m$ は X の逆元である.

(iii) (有限個の) 素イデアルを取ったとき, それが $\mathbb{Z}$ 上一次独立になることを示す. 異なる素イデアル $\mathfrak{p}_1, \cdots, \mathfrak{p}_\ell$ に対して, $R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\ell^{e_\ell}$ $(e_i \in \mathbb{Z})$ とする[*98]. 適当に順番を入れ替えて, ある番号 m で $e_i \geq 0$ $(i \leq m)$ かつ $e_i < 0$ $(i > m)$ としてよい. 補題 A.53 より,

---

[*97] 任意のアーベル群は, ある加法群に同型である (この群の演算をたし算でかいても気持ち悪くない). 加法群においては, (乗法群の n 乗の代わりに) n 倍を考えるので, 自然に $\mathbb{Z}$ 加群の構造が入る.

[*98] 演算 (乗法 vs. 加法) と単位元 (1 vs. 0) に注意する.

$\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}=\mathfrak{p}_{m+1}^{-e_{m+1}}\cdots\mathfrak{p}_\ell^{-e_\ell}$ となるが, これは整イデアルの素イデアル分解である. $\mathfrak{p}_i$ はすべて異なるので, 素イデアル分解の一意性より, $e_i=0$ でなければいけない. □

まず, イデアル群が有限生成, つまり R の素イデアルが有限個になるのはどのような場合かが気になる. 次が知られている.

命題 A.74. デデキント環 R の素イデアルが有限個ならば, R は単項イデアル整域である.

これを示すために, (非常に有名な) **中国式剰余定理**を与える.

補題 A.75 (中国式剰余定理)**.** $I_1,\cdots,I_\ell$ を R のイデアルとし, どの i,j $(i\neq j)$ に対しても $I_i+I_j=R$ と仮定する (このような I_i,I_j を**互いに素**という). このとき, $R/\bigcap_i I_i\simeq\bigoplus_i R/I_i$ が成り立つ.

証明. $\varphi:R\to\bigoplus_i R/I_i$ を $r\mapsto(r)_i$ で定義する (それぞれの剰余環で剰余する). 明らかに, これは環の準同型であるから, 全射および $\operatorname{Ker}\varphi=\bigcap_i I_i$ を示す. (後者は明らか.)

全射を証明するために, 各番号 i に対して, $R=I_i+\prod_{j\neq i}I_j$ が成り立つことを示そう. $1=\underset{I_i}{\bigcirc}+\underset{\prod I_j}{\triangle}$ となることを示せばよい. 各番号 j に対して, $R=I_i+I_j$ より, $1=x_j+y_j$ $(x_j\in I_i,\ y_j\in I_j)$ とかける. よって, $1=\prod_{j\neq i}(x_j+y_j)$ となるが, この右辺を展開すれば, 希望の等式を得ることができる.

φ が全射であることを示す. $(r_i)_i\in\bigoplus_i R/I_i$ とする. $(r_i\in R$ とみて) 各番号 i で $r_i=a_i+b_i$ $(a_i\in I_i,\ b_i\in\prod_{j\neq i}I_j)$ とかけるから, $r=\sum_i b_i$ とおく. $r_i\equiv b_i\pmod{I_i}$ $(r_i=b_i$ in $R/I_i)$ かつ $b_h\equiv 0\pmod{I_i}$ $(b_h=0$ in $R/I_i,\ h\neq i)$ だから, $\varphi(r)=(r)_i=(r_i)_i$ となる. □

命題 A.74 を証明しよう.

命題 A.74 の証明. 仮定より, $\mathfrak{p}_1,\cdots.\mathfrak{p}_\ell$ をすべての (異なる零でない) 素イデアルとする. (定理 A.45 の証明のように) 素イデアル分解を考えれば, 任意の素イデアルが単項であることを示せばよい. ここでは, $\mathfrak{p}_1$ が単項イデアルであることを証明しよう.

補題 A.53 より, 任意の (零でない) 素イデアル $\mathfrak{p}$ に対して, $\mathfrak{p}^2\neq\mathfrak{p}$ である. そこで, $a\in\mathfrak{p}_1\setminus\mathfrak{p}_1^2$ を取る. また, R はデデキント環より, 零でない素イデアルはすべて極大イデアルである. よって, $\mathfrak{p}_1^2,\mathfrak{p}_2,\cdots,\mathfrak{p}_\ell$ はどの 2 つも互いに素である. 中国式剰余定理を発動させて, $(a,1,\cdots,1)\in R/\mathfrak{p}_1^2\oplus\bigoplus_{i\geq 2}R/\mathfrak{p}_i$ に対応する $b\in R$ を取る:

$$b\equiv\begin{cases}a & (\mathrm{mod}\ \mathfrak{p}_1^2);\\ 1 & (\mathrm{mod}\ \mathfrak{p}_i)\ (i\geq 2),\end{cases}$$

特に $b \notin \mathfrak{p}_1^2$ かつ $b \notin \mathfrak{p}_i$ $(i \geq 2)$ である．ここで, 単項イデアル (b) の素イデアル分解 $(b) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_\ell^{e_\ell}$ を考えると, $b \notin \mathfrak{p}_i$ $(i \geq 2)$ より, $e_i = 0$ $(i \geq 2)$ であり, $b \in \mathfrak{p}_1$ かつ $b \notin \mathfrak{p}_1^2$ より, $e_1 = 1$ である．つまり, $(b) = \mathfrak{p}_1$ を得る． □

A.4.1.1 命題 A.74 の証明の考察 I

定理 A.45 でも A.74 でも, 証明の流れとしては【整域が『素イデアル分解をもつ (デデキント環)[*99]かつ任意の**素イデアル**が単項イデアルとなる』ならば『単項イデアル整域である』】だった．しかし, 実は本質はそこではない．面白いことに, 【整域の『任意の**素イデアル**が単項イデアル』ならば『単項イデアル整域』】ということがいえてしまう．

次は, この事実について議論していく．最もキーになる定理から始めよう．

定理 A.76. 可換環 R の任意の素イデアルが有限生成ならば, R はネーター環である．

(定理 A.11 より, 逆はわかっている.)

R のイデアル I, J に対して,

$$I : J := \{r \in R \mid \text{すべての } a \in J \text{ に対して, } ar \in I\}$$

($I \div J$ 的な意味で) I と J の**商**といい, 簡単に R のイデアルであることが確認できる．

定理 A.76 の証明. (背理法) R をネーターでないとし, 有限生成でないイデアル全体の集合を $\mathcal{M}$ とおく (包含関係によって, 半順序集合である)．背理法の仮定より, $\mathcal{M} \neq \emptyset$．$\mathcal{M}$ の空でない全順序部分集合 $\mathcal{C}$ を取り, $I' := \bigcup_{J\in\mathcal{C}} J$ とおくと, I' は有限生成でない[*100]: $I' \in \mathcal{M}$．よって, これは $\mathcal{C}$ の ($\mathcal{M}$ 内の) 上界を与えている．ツォルンの補題[*101]より, $\mathcal{M}$ の極大元 I が取れる: $I \neq R$ (R は有限生成な R のイデアル)．仮定より, I は素イデアルでないから, $a, b \in R$ で $ab \in I$ かつ $a, b \notin I$ となるような元が取れる．$I \subsetneq I + (a)$ より, I の極大性から $I + (a)$ は有限生成である．また, $J := I : (a)$ とおくと, $I \subsetneq I + (b) \subseteq J$ より, J も有限生成である．

そこで, $I + (a) = (a_1 + ar_1, \cdots, a_\ell + ar_\ell)$ $(a_i \in I,\ r_i \in R)$, および, $J = (c_1, \cdots, c_m)$ とおく．このとき, $x \in I \subsetneq I + (a)$ を取ると, $x = \sum_i s_i(a_i + ar_i)$ $(s_i \in R)$ とかける．よって, $I \ni x - \sum_i s_i a_i = a\sum_i s_i r_i$ より, $\sum_i s_i r_i \in I : (a) = J$ を得る: $\sum_i s_i r_i =$

[*99] 【デデキント環 ⇒ 素イデアル分解をもつ】という事実は上で示した．実は逆も成り立つ．(A.4.3 節)

[*100] 有限生成なら, 生成元が有限個の J に属してしまい, どこかの J で有限生成になってしまう．

[*101] 集合論バージョン．選択公理と同値．

$\sum_i t_i c_i$ $(t_i \in R)$. したがって, $x = \sum_i s_i a_i + a\sum_i t_i c_i \in (a_1, \cdots, a_\ell) + (ac_1, \cdots, ac_m)$: $I \subseteq \underset{I}{(a_1, \cdots, a_\ell)} + \underset{ac_i \in I}{(ac_1, \cdots, ac_m)} \subseteq I$. このように, $I \in \mathcal{M}$ が有限生成となり, 矛盾. □

我々の (現在の) 目標を達成しよう.

定理 A.77. 整域 R の任意の素イデアルが一元生成ならば, R は単項イデアル整域である.

証明. R は体でないとしてよい.

① 定理 A.76 より, R はネーター整域である.

② よって, 定理 A.14 より, R の任意の元は有限個の既約元の積で表せる. ここで, a を既約元としよう; 特に, $(a) \neq R$. ツォルンの補題から, 単項イデアル (a) を含む極大イデアル $\mathfrak{p}$ (特に素イデアル) が存在する. 仮定より, $\mathfrak{p} = (p)$ となる $p \in R$ が取れる. このとき, $(a) \subseteq \mathfrak{p} = (p)$ より, a は p 倍である $(a = pc,\ c \in R)$ が, a は既約元としたので, c は可逆, ゆえに $\mathfrak{p} = (p) = (a)$ となり, a が素元であることがわかる. したがって, R は一意分解整域である; 特に, 正規環 (命題 A.28).

③ ② とまったく同じ議論で, R の零でないすべての素イデアルは極大イデアルであることがわかる.

以上のことから, R はデデキント環である. ② および定理 A.45 より, R は単項イデアル整域であることがわかる. □

補足 A.78. つまり, 整域における『すべての**素イデアル**が単項イデアル』という条件だけで, その整域は自動的にデデキント環になってしまう. (定理 A.76 と合わせて, やはりネーター性が偉大.)

局所環の極大イデアルが一元生成でも似たようなことがいえる.

命題 A.79. 可換ネーター局所環 R の (ただ一つの) 極大イデアル $\mathfrak{m}$ が単項イデアルと仮定する: $\mathfrak{m} = (m)$. このとき, 次が成り立つ.

(1) R の素イデアルは, $\mathfrak{m}$ または (0) の高々 2 つである.

(2) 次は同値である:
  (i) R は体でない整域である;
  (ii) R が $\mathfrak{m}$ と異なる素イデアルをもつ;
  (iii) R は単項イデアル整域である;
  (iv) R は体でない正規環である.

(3) R が整域でないならば, R はアルチン環である.

証明. (1) $\mathfrak{p}$ を R の素イデアルとし, $\mathfrak{p} \neq (0)$ と仮定する. R は局所環より, $\mathfrak{p} \subseteq \mathfrak{m}$ となる. R のネーター性より, $\mathfrak{p} = (p_1, \cdots, p_\ell)$ とかけるが, 各 i で $p_i \in \mathfrak{m} = (m)$ となるから, $\mathfrak{p} \ni p_i = mq_i$. $\mathfrak{p}$ は素イデアルより, $m \in \mathfrak{p}$ または $q_i \in \mathfrak{p}$ が成り立つ. 一つでも前者となる番号 i が存在したら, $\mathfrak{p} = \mathfrak{m}$ となる. すべての番号 i で $q_i \in \mathfrak{p}$ とすると,

$$\mathfrak{pm} \subseteq \mathfrak{p} = (p_1, \cdots, p_\ell) = (mq_1, \cdots, m\mathfrak{q}_\ell) = (q_1, \cdots, q_\ell)(m) \subseteq \mathfrak{pm}$$

となるから, $\mathfrak{pm} = \mathfrak{p}$ を得る. $\mathfrak{m} = \operatorname{rad} R$ より, 中山の補題を適用すれば $\mathfrak{p} = (0)$ であることがわかる.

(2) (i) $\Rightarrow$ (ii): R は整域より, (0) は R の素イデアルである. もし $\mathfrak{m} = (0)$ ならば R は体となるから, $\mathfrak{m} \neq (0)$.

(ii) $\Rightarrow$ (iii): (1) より, R の異なる素イデアルは $\mathfrak{m}$ および (0) のみ. (0) を素イデアルにもつから, R は整域である. さらに, 素イデアルがすべて単項イデアルだから, 定理 A.77 より, R は単項イデアル整域である.

(iii) $\Rightarrow$ (iv): 単項イデアル整域だから一意分解整域である. よって, 正規環である.

(iv) $\Rightarrow$ (i): 正規環の定義より.

(3) (1) より, R の素イデアルは $\mathfrak{m}$ のみである. アルチン環についてはまた今度 □

補足 A.80. 体でない単項イデアル局所整域 (命題 A.79(2)) を**離散付値環** *(DVR)* という. これは, 局所デデキント環であることと同値である (命題 A.74). デデキント環の零でない素イデアル (よって極大イデアル) における局所環は離散付値環である.

A.4.1.2 命題 A.74 の証明の考察 II

命題 A.74 の証明において, ある箇所に下線を引いた. 気になっている読者もいると思うが, これについて言及したい. (証明を見ればわかるが, 素イデアルの生成元を取るために, この事実が大切だった.)

下線部【任意の (零でない) 素イデアル $\mathfrak{p}$ に対して, $\mathfrak{p}^2 \neq \mathfrak{p}$ である】という事実について, 命題 A.74 の証明内ではデデキント環であること (任意の非零素イデアルは可逆であること: 命題 A.53) を用いた. しかし, この事実に対してもデデキント環であることが重要なのではなく, そのネーター性がキーになる. 次を示そう.

命題 A.81. ネーター整域 R の零でない素イデアル $\mathfrak{p}$ に対して, $\mathfrak{p}^2 \neq \mathfrak{p}$ が成り立つ.

証明. (背理法) $\mathfrak{p}$ における局所環 $R_{\mathfrak{p}}$ を考える: $M := \left\{ \dfrac{p}{a} \;\middle|\; p \in \mathfrak{p}, a \in R \setminus \mathfrak{p} \right\}$ (唯一の極大イデアル: $\operatorname{rad} R_{\mathfrak{p}} = M$). $R_{\mathfrak{p}}$ もネーター環であり, M は有限生成である. 背理法の仮定より $M^2 = M$ となるから, 中山の補題を発動させて, $M = (0)$ を得る. よって, 任意の $p \in \mathfrak{p}$ に対して, $\dfrac{p}{1} = 0$ (in $R_{\mathfrak{p}}$), ゆえに $p = 0$. このように, $\mathfrak{p} = (0)$ となり, 矛盾. □

疑問. 上の命題で, R が整域であるという仮定を外すと, (証明の最後の段階で) $\mathfrak{p}$ の任意の元が零因子である (特に, $^{\forall}p \in \mathfrak{p}$ に対して, $^{\exists}c \in R \setminus \mathfrak{p}$ s.t. $pc = 0$) というところで止まる. このとき, これ以上のことが言えるか?

A.4.2 イデアル群の存在の逆

定理 A.73 において, 【デデキント環 $\Rightarrow$ $\mathcal{X}_R$ は群をなす】という事実を示した. このとき, 「逆は?」という問いは自然である. 実はこれも成り立つ. 特に, 『分数イデアルの積で演算』, 『結合律』, 『単位元 R』はいつも成り立っているから, 『逆元の存在』が問題である. そこで, 次を示すことが目標である; これによって, 【デデキント環 $\Leftrightarrow$ $\mathcal{X}_R$ は群】.

定理 A.82. (体でない) 整域 R の零でない任意の分数イデアルが ($\mathcal{X}_R$ で) 可逆であるならば, R はデデキント環である.

以下, (特に断りがない限り) R を (体でない) 整域, K をその商体とする.
まずは, R の整イデアルの ($\mathcal{X}_R$ における) 逆元を記述しよう.

主張. R の可逆なイデアル I の $\mathcal{X}_R$ における逆元は, I^{-1} (逆イデアル) である.

証明. I の逆元を X ($\subseteq K$) とおく: $IX = R$. 明らかに $X \subseteq I^{-1}$ となるから, $R = IX \subseteq II^{-1} \subseteq R$, ゆえに $R = IX = II^{-1}$. 単位元の一意性より, $X = I^{-1}$ である. ■

R がネーター環であることを見るため, 次を確認する.

主張 A.83. R の可逆な (整) イデアル I は有限生成である[*102].

証明. $R = II^{-1}$ より, $1 = \sum_{i=1}^{\ell} a_i x_i$ ($a_i \in I, x_i \in I^{-1}$) とかける: $(a_1, \cdots, a_\ell) \subseteq I$. このとき, 任意の $a \in I$ に対して,

$$a = \sum_i a_i \underset{R}{(ax_i)} \in (a_1, \cdots, a_\ell)$$

を得る. したがって, $I = (a_1, \cdots, a_\ell)$ となり, I は有限生成であることがわかる. ■

[*102] 分数イデアル X に対して, $r \in R$ とすると $rX \subseteq R$ である. R 加群として $X \simeq rX$ ($\subseteq R$).

次は正規環であることを確かめるための準備.

(零因子を含まない) 任意の積閉集合[*103]Δ による局所化 $\Delta^{-1}R$ に対して, (環の単射準同型 $R \to \Delta^{-1}R$ が存在するから) $R \subseteq \Delta^{-1}R$ とみなす. また, 素イデアル $\mathfrak{p}$ に対して, ($R \setminus \mathfrak{p} \subseteq R \setminus \{0\}$ より) $R \subseteq R_{\mathfrak{p}} \subseteq K$ とみなす. $R_{\mathfrak{p}}$ の商体も K である.

命題 A.84. $R = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ が成り立つ. ただし, $\mathfrak{m}$ は R の極大イデアル全体を走る.

証明. " $\subseteq$ " は明らか. $x \in K$ に対して, $I_x := \{r \in R \mid rx \in R\}$ は R のイデアルである. このとき, R の素イデアル $\mathfrak{p}$ に対して, $x \in R_{\mathfrak{p}} \Leftrightarrow I_x \nsubseteq \mathfrak{p}$. よって, $x \in \bigcap R_{\mathfrak{m}}$ とすると, $I_x \nsubseteq \mathfrak{m}$ ($^\forall\mathfrak{m}$) となるから, ツォルンの補題より $I_x = R \ni 1$; ゆえに, $x = 1x \in R$. □

系 A.85. 次は同値である:

(1) R は正規環である;
(2) 任意の素イデアル $\mathfrak{p}$ における局所環 $R_{\mathfrak{p}}$ は正規環である;
(3) すべての極大イデアル $\mathfrak{m}$ における局所環 $R_{\mathfrak{m}}$ は正規環である.

証明. (1) $\Rightarrow$ (2): 補題 A.37.

(2) $\Rightarrow$ (3): 明らか.

(3) $\Rightarrow$ (1): $x \in K_R$ (R 上整な K の元) とする. 極大イデアル $\mathfrak{m}$ に対して $R \subseteq R_{\mathfrak{m}}$ より, x は $R_{\mathfrak{m}}$ 上整である. 仮定より, $x \in K_{R_{\mathfrak{m}}} \overset{(3)}{=\!=} R_{\mathfrak{m}}$ ($R_{\mathfrak{m}}$ の商体は K). したがって, 命題 A.84 より, $x \in R$, ゆえに $K_R = R$ を得る. □

最後に, (零でない) 素イデアルが極大イデアルであることを調べるための準備を与える.

命題 A.86. ネーター整域 R とその可逆な素イデアル $\mathfrak{p}$ に対して, 次が成り立つ.

(1) 局所環 $R_{\mathfrak{p}}$ の (ただ一つの) 極大イデアルは単項イデアルである.
(2) $\mathfrak{p}$ は非自明な素イデアルを含まない.

証明. (1) $R = \mathfrak{p}\mathfrak{p}^{-1}$ より, $1 = \sum_{i=1}^{\ell} p_i x_i$ ($p_i \in \mathfrak{p}, x_i \in \mathfrak{p}^{-1}$) とかける. 各 i に対して, $a_i := p_i x_i \in R$ とおく: $1 = \sum_i a_i$. すべての a_i が $\mathfrak{p}$ に属すことはない ($\mathfrak{p} \neq R$) から, ある番号 i で $a_i \notin \mathfrak{p}$ となる. ここで, $R_{\mathfrak{p}}$ の (ただ一つの) 極大イデアルを M とおく: $M = \left(\frac{p}{1} \;\middle|\; p \in \mathfrak{p} \right) = \left\{ \frac{p}{s} \;\middle|\; p \in \mathfrak{p}, s \in R \setminus \mathfrak{p} \right\}$. このとき, $M = \left(\frac{p_i}{1} \right)$ であることを示

[*103] 今は R を整域と仮定しているため, すべての積閉集合でよい.

す. “ $\supseteq$ ” は明らか. 逆に, 各 $\dfrac{p}{1}$ $(p \in \mathfrak{p})$ が右辺に入ればよい:

$$\frac{p}{1} = \frac{pa_i}{a_i} \underset{a_i \notin \mathfrak{p}}{} = \overbrace{\frac{p_i}{1} \cdot \frac{px_i}{a_i}}^{a_i = p_i x_i} \underset{px_i \in R}{} \in \left(\frac{p_i}{1}\right).$$

(2) $(0) \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ ($\mathfrak{q}$ は素イデアル) とする. 局所化によって, $(0) \subseteq \mathfrak{q}R_\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p} = M$ $(\neq (0))$ となるが, (1) および命題 A.79(2) ($R_\mathfrak{p}$ は体でない整域) より, $\mathfrak{q}R_\mathfrak{p} = (0)$ または $\mathfrak{q}R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p} = M$. 前者なら $\mathfrak{q} = (0)$, 後者なら $\mathfrak{q} = \mathfrak{p}$ であることが容易に確認できる. □

これですべての準備が整った.

定理 A.82 の証明. R を, 任意の分数イデアルが可逆である (体でない) 整域とする.

(ネーター) 主張 A.83 より.

(正規) $\mathfrak{m}$ を R の極大イデアルとする. (R は体でないから $\mathfrak{m} \neq (0)$.) 命題 A.86(1) より, 局所環 $R_\mathfrak{m}$ の (ただ一つの) 極大イデアルは単項イデアルである. 命題 A.79(2) より, $R_\mathfrak{m}$ は (体でない) 正規環である. よって, 系 A.85 より, R も正規環である.

(1 次元[*104]) $\mathfrak{p}$ を零でない R の素イデアルとする. ツォルンの補題より, $\mathfrak{p}$ はある極大イデアル $\mathfrak{m}$ に含まれる. $\mathfrak{m}$ も素イデアルだが, 命題 A.86(2) より, $\mathfrak{m}$ は非自明な素イデアルを含まない. よって, $\mathfrak{p} = \mathfrak{m}$ を得る. □

注意 A.87. 上の証明を見てもわかるように, 定理 A.82 の主張は (「任意の分数イデアルが可逆」ではなく) 「任意の素イデアルが可逆」という条件で十分成り立つ. つまり, (体でない) 整域に対して, 補題 A.53 の逆が成り立つ. (ただし, 定理 A.76 は必要.)

A.4.3 素イデアル分解の存在の逆

工事中

A.4.4 遺伝的整域

可換 (ネーター) 環 R に対して, 任意の全射 R 準同型 $M \to P$ が分裂するとき, P を**射影加群**[*105]という (命題 A.22 参照). (有限生成) 加群 P が射影的であることと P が (有限) 自由加群の直和因子であることは同値である. また, R が単項イデアル整域ならば, 射影加群と自由加群は一致する.

[*104] 零でない任意の素イデアルが極大イデアルとなる整域を *(**クルル**) **次元** 1* をもつ整域という.

[*105] (少し高度に) $\mathrm{Ext}^1_R(P, -) = 0$

(有限) 自由加群の部分加群がすべて射影的であるとき, R は**遺伝的**であるという.
この節の目標は, 遺伝的 (ネーター) 整域を分類することだが, 実は次がいえる.

命題 A.88. R を (体でないネーター) 整域とする. このとき, R が遺伝的であることと R がデデキント環であることは同値である.

次を示せばよい.

主張. R を (ネーター) 整域とする. このとき, R の (整) イデアル I が射影 R 加群であることと I が可逆であることは同値である.

証明. I が可逆とすると, $II^{-1} = R$ である: $1 = \sum_{i=1}^{\ell} x_i y_i$ $(x_i \in I, y_i \in I^{-1})$. (主張 A.83 のように) I は x_i たちで生成される. そこで, $\pi : R^\ell \to I$ を自然な全射とし, 逆に, $\varphi : X \to I^\ell$ $(x \mapsto (xy_i)_i)$ とおくと,

$$\pi\varphi(x) = \sum_i (xy_i)x_i = x$$

となるから, $\pi\varphi = \mathsf{id}_I$. ゆえに, π は分裂し, I は R^ℓ の直和因子である.

I を射影的なイデアル (R 加群) とする; R のネーター性から I は有限生成. I は射影的だから, 自然な全射 $\pi : R^\ell \to I$ は分裂する. そこで, $\pi\iota = \mathsf{id}_I$ となる R 準同型 $\iota : I \to R^\ell$ を取り, 各成分に対して $\iota = {}^t(\,\iota_1 \cdots \iota_\ell\,)$ $(\iota_i \in \mathrm{Hom}_R(I, R))$ とかく. ただし, ${}^t(-)$ は行列の転置を表す. 任意の R 準同型 $\varphi : I \to R$ は K の元による定数倍写像である. 実際, x, y $(\neq 0) \in I$ とすると, $y\varphi(x) = \varphi(xy) = x\varphi(y)$ より, $\alpha := \dfrac{\varphi(x)}{x} \in K$ は常に一定である: $\varphi(x) = \alpha x$[*106]. そこで, 各番号 i で $\iota_i(x) = y_i x$ $(y_i \in K)$ とおくと,

$$\begin{aligned} x &= \pi\iota(x) = \textstyle\sum_i (y_i x)x_i = x\sum x_i y_i \quad \rightsquigarrow \quad 1 = \sum x_i y_i \\ I^{-1} &:= \{\alpha \in K \mid \alpha I \subseteq R\} = \langle y_1, \cdots, y_\ell \rangle_R \end{aligned}$$

となるから, $II^{-1} = R$; ゆえに, I は可逆である. ■

注意 A.89. 上では, 有限生成 (ネーター) にこだわって証明したが, いらない. また, 整イデアルに限定していたが, これもいらない. 一方, 自由加群の任意の有限生成部分加群が射影的となる環を**半遺伝的**という. (そのため, 上では半遺伝的とまでしか示していないが, このへんで切り上げよう.)

[*106] ここでは, 元を取って示したが, ホモロジカル (圏論) 的には何を意味しているか?

A.4.5 イデアル類群

定理 A.73 で示したように, デデキント環 R に対して, 分数イデアル全体の集合 $\mathcal{X}_R$ は群をなす. また, R の商体 K とその元 α に対して, $\alpha R := \{\alpha r \mid r \in R\}$ も分数イデアルとなるが, これを**単項分数イデアル**という. 単項分数イデアル同士の積および単項分数イデアルの逆元もまた, 単項分数イデアルなので, 単項分数イデアル全体の集合 $\mathcal{Y}_R$ は $\mathcal{X}_R$ の部分群をなす; $\mathcal{X}_R$ はアーベル群なので, $\mathcal{Y}_R$ は特に正規部分群. このとき, 剰余群 $\mathcal{X}_R/\mathcal{Y}_R$ を R の**イデアル類群**といい, その位数を R の**類数**という. 次のことが知られている.

定理 A.90. 代数体 K の整数環 $\mathcal{O}_K$ のイデアル類群は有限 (アーベル) 群である.

類数を求めることも難しいが, 知られている公式を与えておく.

定理 A.91. 平方因子をもたない整数 d に対して,

$$D := \begin{cases} d & d \equiv 1 \pmod 4; \\ 4d & d \equiv 2, 3 \pmod 4; \end{cases}$$

とおき, $K := \mathbb{Q}(\sqrt{d})$ とする: $R := \mathcal{O}_K$. このとき, $d < 0$ ならば, R のイデアル類群の代表元および類数を次のステップにより求めることができる:

Step 1 : $|b| \leq \sqrt{\dfrac{|D|}{3}}$ である $b \in Z$ に対して, $4ac = b^2 - D,\ a \leq c,\ c > 0$ となる $a, c \in \mathbb{Z}$ を求める. ただし, $D \neq -3$ ならば, $|b| < \sqrt{\dfrac{|D|}{3}}$ としてよい.

Step 2 : Step 1 の (a, b, c) のうち, $\gcd(a, b, c) = 1$ で,

(i) $-a < b \leq a < c$ (ii) $0 \leq b \leq a = c$

のどちらかを満たすものを求める.

このとき, R の類数は (a, b, c) の個数と一致する. さらに, $\left(a, \dfrac{-b + \sqrt{D}}{2}\right)_R$ となる全体が R のイデアル類群の代表元となる.

両定理とも証明はとても大変なので, ここでは与えない. (またいつか...?)

例 A.92. K を代数体とし, $R := \mathcal{O}_K$ とおく.

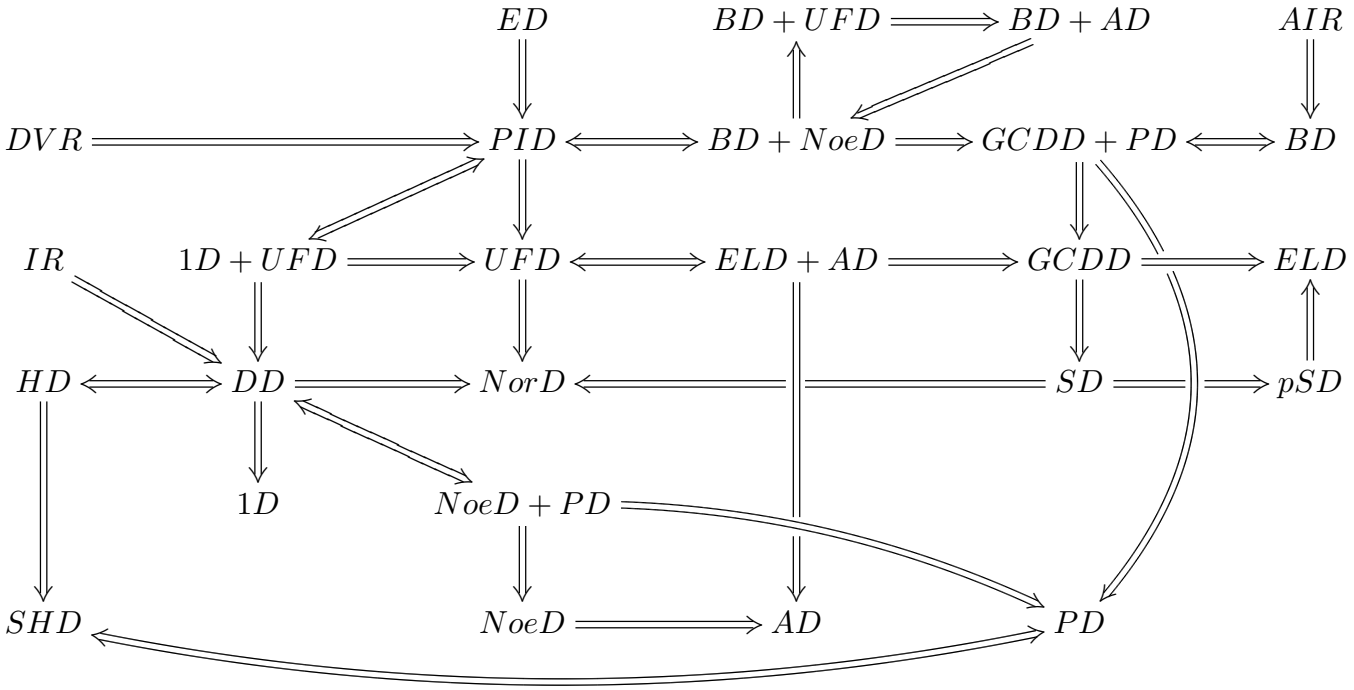
(1) R が一意分解整域なら単項イデアル整域なので, R の類数は 1 である.

(2) $K = \mathbb{Q}(\sqrt{-5})$ とする: $R := \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. このとき, R の類数は 2 であり, そのイデアル類群は $I := (2, -1 + \sqrt{-5})_R$ で生成される: $\mathcal{X}_R/\mathcal{Y}_R = \langle I \rangle \simeq C_2$.

A.4.6 デデキント環の話題

A.5 地図

この節に出てきた (体でない) 整域の強弱について, 「地図」を残しておく:



- ED := ユークリッド整域 $\overset{\text{def}}{\Leftrightarrow}$ 余りつきわり算ができる
- PID := 単項イデアル整域 $\overset{\text{def}}{\Leftrightarrow}$ すべてのイデアルが単項イデアル
- UFD := 一意分解整域 $\overset{\text{def}}{\Leftrightarrow}$ 素元分解が存在 (自動的に一意)
- AIR := 代数的整数環 $\overset{\text{def}}{\Leftrightarrow}$ 代数的整数全体
- IR := 代数体の整数環 $\overset{\text{def}}{\Leftrightarrow}$ $\mathbb{Z}$ の代数体における整閉包
- DD := デデキント環 $\overset{\text{def}}{\Leftrightarrow}$ (体でない) 1 次元ネーター正規環 $\Leftrightarrow$ 一意的な素イデアル分解が存在 $\Leftrightarrow$ 分数イデアル全体が群
- NoeD := ネーター整域 (ネーター) $\overset{\text{def}}{\Leftrightarrow}$ 昇鎖律を満たす $\Leftrightarrow$ イデアルが有限生成 $\Leftrightarrow$ 極大条件を満たす $\Leftrightarrow$ 素イデアルが有限生成
- NorD := 正規環 $\overset{\text{def}}{\Leftrightarrow}$ 商体における整閉包と一致
- 1D := 1 次元整域 $\overset{\text{def}}{\Leftrightarrow}$ 零でない素イデアルが極大イデアル

- AD := 原子整域 $\overset{\text{def}}{\Leftrightarrow}$ 既約元分解が存在
- ELD := EL 整域 $\overset{\text{def}}{\Leftrightarrow}$ 既約元が素元
- DVR := 離散付値環 $\overset{\text{def}}{\Leftrightarrow}$ (体でない) 単項イデアル局所整域 $\Leftrightarrow$ 局所デデキント環
- HD := 遺伝的整域 $\overset{\text{def}}{\Leftrightarrow}$ 自由加群の部分加群が射影的
- SHD := 半遺伝的整域 $\overset{\text{def}}{\Leftrightarrow}$ 自由加群の有限生成部分加群が射影的
- BD := ベズー整域 $\overset{\text{def}}{\Leftrightarrow}$ 有限生成イデアルが単項イデアル $\Leftrightarrow$ 2 元生成イデアルが単項イデアル
- GCDD := GCD 整域 $\overset{\text{def}}{\Leftrightarrow}$ 任意の 2 元に次の意味での**最大公約元** d が存在する: (公約元の中で "最大") r が公約元ならば $r \mid d$[*107].
- PD := プリューファー整域 $\overset{\text{def}}{\Leftrightarrow}$ 有限生成イデアルが可逆 $\Leftrightarrow$ SHD
- SD := シュライアー整域 $\overset{\text{def}}{\Leftrightarrow}$ 正規環かつ非零元がプライマル (primal)[*108]
- pSD := 前シュライアー整域 $\overset{\text{def}}{\Leftrightarrow}$ 非零元がプライマル

このノートで証明していない非自明な包含について確認しておく.

命題 A.93. $BD + AD \Rightarrow BD + NoeD$

証明. R をベズー原子整域とし, $\mathfrak{p}$ $(\neq 0)$ をその素イデアルとする. $\mathfrak{p}$ は零でない元をもつが, その元を既約分解 (AD) して素イデアルということを使えば, $p \in \mathfrak{p}$ となる既約元 p が取れる: $(p) \subseteq \mathfrak{p}$. $q \in \mathfrak{p}$ とすると, R がベズー整域ということから, $(p, q) = (r)$ $(\subseteq \mathfrak{p})$ となる r が取れる. このとき, $(p) \subseteq (r)$ より $p = ra$ となるが, p は既約元だから r または a は可逆元である. 前者ならば $\mathfrak{p} \supseteq (r) = R$ となりダメ. よって, a が可逆だが, そのとき $(p) = (r) = (p, q) \ni q$ より, $\mathfrak{p} = (p)$ を得る. このように, R の素イデアルが一元生成 (有限生成) より, R は単項イデアル整域 (ネーター) であることがわかる. □

命題 A.94. $AIR \Rightarrow BD$ (AIR はネーターでない.)

証明. $\Omega := \mathbb{C}_{\mathbb{Z}}$ とし, J を Ω の有限 (2 元) 生成イデアルとする: $J = (s, t)_\Omega$. 代数体 $K := \mathbb{Q}(s, t)$ およびその整数環 $R := \mathcal{O}_K$ $(= K_{\mathbb{Z}})$ を考える: $s, t \in R$. また, $I := (s, t)_R$ を R の (整) イデアルとする[*109]. このとき, 定理 A.90 より, ある正の整数 ℓ で, I^ℓ は R の単項 (分数) イデアルとなる: $I^\ell = (r)$ $(r \in R)$. $u := \sqrt[\ell]{r} \in \mathbb{C}$ とおくと, これは $\mathbb{Z}$ 上整

[*107] ただし, イデアルでいうと最小 $(r) \supseteq (d)$.

[*108] a がプライマル $\overset{\text{def}}{\Leftrightarrow}$ 「$a \mid bc \Rightarrow a = a_1 a_2,\ a_1 \mid b,\ a_2 \mid c$ $(^\exists a_1, a_2)$」

[*109] I と J は一致しない. 例えば, $J := (\sqrt{-2})_\Omega$ を取ったとき, $\sqrt{2} \in J$ だが, $I = (\sqrt{-2})_R \not\ni \sqrt{2}$.

である: $u \in \Omega$. $L := K(u) = \mathbb{Q}(s,t,u)$ とおき, $S := \mathcal{O}_L$ $(= L_{\mathbb{Z}})$ とすると,

$$(s,t)_S^\ell = (r)_S = (u)_S^\ell.$$

S における素イデアル分解の一意性より, $(s,t)_S = (u)_S$, 特に $J = (s,t)_\Omega = (u)_\Omega$.

(ネーターでないこと) $J := (\sqrt[\ell]{2} \mid \ell > 0)$ は Ω の無限生成イデアルとなる. □

注意 A.95. 上のことから $AIR \Rightarrow ELD$ だが, AIR には既約元はない (注意 A.20).

例 A.96. $\Omega \supseteq (2, -1+\sqrt{-5})_\Omega$ を単項イデアルで表してみよう. $K := \mathbb{Q}(\sqrt{-5})$ とし, $R := \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ を考える. $I := (2, -1+\sqrt{-5})_R \subseteq R$ とすると, $I^2 = (2)_R$ となる (例 A.92(2)). このとき, $(2, -1+\sqrt{-5})_\Omega = (\sqrt{2})_\Omega$ を得る: 実際に, $u := \sqrt{2}$ として,

- $2 = \underset{\Omega}{\sqrt{2}}\, u,\ -1+\sqrt{-5} = \underbrace{\dfrac{-1+\sqrt{-5}}{\sqrt{2}}}_{s \text{ とおく}} \cdot u$
  - s の $\mathbb{Z}$ 上最小多項式は $x^4 + 4x^2 + 9$ (モニック) より, $s \in \Omega$.
- $\sqrt{2} = -2\underset{\Omega}{\sqrt{2}} + (-1+\sqrt{-5}) \cdot \underbrace{\dfrac{-1-\sqrt{-5}}{\sqrt{2}}}_{t \text{ とおく}}$
  - t の $\mathbb{Z}$ 上最小多項式も $x^4 + 4x^2 + 9$ (モニック) より, $t \in \Omega$.

(注) どちらも $\mathbb{Q}(\sqrt{-5}, \sqrt{2})$ の整数環 S の中で表せている: $(2, -1+\sqrt{-5})_S = (\sqrt{2})_S$.

(注) $(2, -1+\sqrt{-5})_R$ は R の単項イデアルではない.

命題 A.97. $pSD \Rightarrow ELD$

証明. 練習問題 □

A.5.1GCD 整域

上で GCD 整域を出したので, その周辺の事実についてまとめる. ($UFD \Rightarrow GCDD$ は明らかだろう.) まずは, 簡単な (しかし初等整数論でも有用な) 事実から確認しよう.

補題 A.98. GCD 整域 R の元 a, b, c について, 次が成り立つ[*110]:

(1) $a = \gcd(a,b) \cdot s,\ b = \gcd(a,b) \cdot t$ としたとき, $\gcd(s,t) = 1$;

(2) $\gcd(a,b) \cdot c = \gcd(ac, bc)$;

[*110] a と b の最大公約元 $\gcd(a,b)$ は可逆元倍を除いて一意的に決まる (♠). 以下, 最大公約元も「$=$」を使って表すが, 可逆元倍で "揺れ" があることに注意する.

(3) $a \mid bc$ かつ $\gcd(a,b)=1$ ならば, $a \mid c$;

証明. (1) 簡単. ((2) の証明のどこかに現れている.)

(2) $d := \gcd(a,b)$ とおくと, $a = dr,\ b = ds$ となるから, $ac = (dc)r,\ bc = (dc)s$ より, dc は ac と bc の公約元である: $dc \mid \gcd(ac,bc) =: e$. よって,

$$\begin{cases} ac = et \\ bc = eu \\ e = (dc)v \end{cases} \rightsquigarrow \begin{cases} a = dtv \\ b = duv \end{cases} \rightsquigarrow \begin{cases} dv \mid a \\ dv \mid b \end{cases} \rightsquigarrow dv \mid \gcd(a,b) = d$$

したがって, v は可逆元であり, $e = (dc)v$ より e と dc は可逆元倍の違いで等しい.

(3) $c = \gcd(a,b)\cdot c = \gcd(ac,bc)$ となり, a は ac と bc の公約元だから $a \mid c$. □

命題 A.99. 次が成り立つ:

$$\begin{array}{ccccc} BD & \overset{(1)}{\Longleftrightarrow} & GCDD + PD & & \\ & & \Downarrow & & \\ SD & \underset{(3)}{\Longleftarrow} & GCDD & \underset{(2)}{\Longrightarrow} & ELD \end{array}$$

証明. (1) “ $\Rightarrow$ ” R をベズー整域とする.

(GCDD) $a, b \in R$ とする. 仮定より, $(a,b) = (d)$ となる $d \in R$ が存在する. このとき, d が a と b の最大公約元になることは容易にわかる.

(PD) I $(\neq (0))$ を有限生成イデアルとする. R はベズー整域より, I は単項イデアル, ゆえに射影的である. よって, R は半遺伝的であり, プリューファー整域である.

“ $\Leftarrow$ ” R をプリューファー GCD 整域とし, I をその有限 (2 元) 生成イデアルとする: $I = (a,b)$. $d := \gcd(a,b)$ (GCD) とおき, $I = (d)$ を示す. K を R の商体とする. $R = II^{-1}$ (PD) より, $I^{-1} := \{x \in K \mid xI \subseteq R\} = \dfrac{1}{d}R$ を示せばよい. “ $\supseteq$ ” は明らか. $x = \dfrac{r}{s} \in I^{-1}$ とする; $\gcd(r,s) = 1$ としてよい. $ax \in R$ より, $s \mid ar$, 特に $s \mid a$ を得る; 同様に, $s \mid b$. したがって, $s \mid d$ となる: $d = st$. このとき, $x = \dfrac{r}{s} = \dfrac{rt}{st} = \dfrac{1}{d}\cdot tr \in \dfrac{1}{d}R$.

(2) R を GCD 整域とし, その既約元 p が $p \mid ab$ を満たすとする. $d := \gcd(p,a)$ とおくと, $d \mid p,\ d \mid a$ より, $p = dr,\ a = ds$ とかける. p は既約元だから, d または r は可逆となる. 後者ならば, (簡単な式変形で) $p \mid a$ を得る. そこで, d が可逆と仮定する. このとき, $db = \gcd(p,a)\cdot b = \gcd(pb,ab)$ であり, p は pb と ab の公約元だから, $p \mid db$ を得る. d は可逆だから, $p \mid b$ となる. このように, p が素元であることがわかる.

(3) R を GCD 整域とし, K をその商体とする.

(正規環) $\frac{r}{s} \in K_R$ とする; $\gcd(r,s)=1$ としてよい. さらに, $\frac{r}{s}$ は, ある R 上の方程式 $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ の解である. 代入し分母を払って, $r^n + sa_{n-1}r^{n-1} + \cdots + a_0 s^n = 0$; ゆえに, $r \mid a_0 s^n$. 上の補題 (3) を n 回使えば, $r \mid a_0$ を得る: $a_0 = rb_0$. このとき, $x^{n-1} + a_{n-1}x^{n-2} + \cdots + b_0 = 0$ は $x = \frac{r}{s}$ を解にもつ. これを繰り返せば, $\frac{r}{s}$ は R 上 1 次方程式の解となる[*111]から, $\frac{r}{s} \in R$, よって $K_R = R$ となる.

(プライマル) $a \mid bc$ とする: $ar = bc$. $a_1 := \gcd(a,b)$ とおくと,

$$\begin{cases} a = a_1 a_2 \\ b = a_1 s \\ \gcd(a_2, s) = 1 \end{cases} \quad \rightsquigarrow \quad a_1 a_2 r = a_1 sc \quad \rightsquigarrow \quad a_2 \mid sc \quad \rightsquigarrow \quad a_2 \mid c$$

よって, a はプライマルである. □

次も GCD 整域の有用な言い換えである.

命題 A.100. 整域 R に対して, 次は同値である:

(1) R は GCD 整域である;
(2) 任意の 2 元 a, b に対して, 次の意味での**最小公倍元** $\ell := \mathrm{lcm}(a,b)$ が存在する: r が公倍元ならば $\ell \mid r$[*112];

証明. (1)⇒(2): $d := \gcd(a,b)$ とおき, $a = ds, b = dt$ とかいたとき, $\mathrm{lcm}(a,b) = dst$ となることを確かめればよい. 逆も同様 ($+\alpha$ 上で確かめた事実の最小公倍元バージョン). □

(有理) 整数のときと同様, GCD 整域でも次が成り立つ (上の証明から直ちにわかる).

命題 A.101. GCD 整域の任意の元 a, b に対して, $ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$ となる[*113].

最大公約元, 最小公倍元をイデアルで書き表してみよう.

命題 A.102. GCD 整域 R の 2 元 a, b に対して, 次が成り立つ.

(1) $(a) \cap (b) = (\mathrm{lcm}(a,b))$.
(2) $(a) + (b) = (a,b) \subseteq (\gcd(a,b))$. ただし, 等号が成立するとは限らない[*114].

[*111] もう一回同じことを繰り返してもよい. そのときは, s が (R で) 可逆となり, $\frac{r}{s} = rs^{-1} \in R$.
[*112] イデアルでいうと最大 $(\ell) \supseteq (r)$.
[*113] 可逆元倍は無視して (再確認)
[*114] ベズー整域との差

この命題では, 最後の主張だけが気になる (ベズーでない GCD 整域). 一般に, 環 R に対して, その一変数多項式環 $R[x]$ を取る操作は, 可換, 整域, UFD (代数学特論 AI), および, ネーター (**ヒルベルトの基底定理**, 代数学特論 BII) という性質を保存することが知られている. また, UFD の証明と同様に (まったく同じように議論できる[*115]), GCD 性も保存されることがわかる. 一方, PID やベズーといった性質は保存されないことがすぐにわかる. そのため, 原始的でない GCD 整域 R を取れば, $R[x]$ は非 UFD 非ベズー非ネーターな GCD 整域となる:

- $R[x]$ が UFD $\Rightarrow$ R が UFD $\Rightarrow$ R が AD.
- $R[x]$ がベズー $\Rightarrow$ (x, r) $(^\forall r\ (\neq 0) \in R)$ は単項イデアル $\Rightarrow$ r は可逆, よって R は体.
- $R[x]$ がネーター $\Rightarrow$ $R[x]$ がネーター ELD, よって UFD.

例えば, 代数的整数環 Ω は BD (よって GCDD) だが AD ではない (PID でない). よって, $\Omega[x]$ はベズーでない GCD 整域の例である.

A.5.2 様々な整域

上で挙げた整域の他にも, 様々な整域がある. すべてを扱うことはできないが, (知りうる限り, 知ったら) ここに列挙し, 機会があれば詳しく扱うつもりである. (体は無視)

- 局所環 : 任意の可換環は, 素イデアルで局所化[*116]すると局所環になり, 局所化は様々な性質を遺伝させる. そのため, 重要な局所環がいろいろある. (例えば DVR.)
  - VR := 付値環 $\overset{\text{def}}{\Leftrightarrow}$ **付値**をもった整域 (自動的に局所環) $\Leftrightarrow$ 局所ベズー整域 $\Leftrightarrow$ イデアル全体が (包含関係で) 全順序 $\Leftrightarrow$ 素イデアル全体が (包含関係で) 全順序 $\Leftrightarrow$ 商体の元 x に対して, x かその逆元はもとの整域に入る
    - 付値環に対して, ネーター $\Leftrightarrow$ PID $\Leftrightarrow$ DVR ($\overset{\text{def}}{\Leftrightarrow}$ 局所 PID)
    - 任意の素イデアルにおける局所化が付値環 $\Leftrightarrow$ PD
  - RLR := 正則局所環 $\overset{\text{def}}{\Leftrightarrow}$ ネーター局所環で, その (唯一の) 極大イデアルの生成元の最小個数が**クルル次元**と一致 (自動的に整域) $\Leftrightarrow$ ネーター局所環で, その**大域次元**が有限 (このとき, それはクルル次元と一致)
    - RLR $\Rightarrow$ UFD

[*115] そのため, とりあえずここではやらない.

[*116] 可換環 R の乗法的集合 Δ に対して, $\Delta^{-1}R$ を Δ における局所化とよんだので, 「素イデアル $\mathfrak{p}$ における局所化 $R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}R$」という言い回しは実際には語弊がある. しかし, しばしばこのような言い方を使う.

- 正則局所環の素イデアルでの局所化もまた, 正則局所環
- 任意の素イデアルでの局所化が正則局所環となる可換ネーター環を**正則環**という. (一般に, 整域とは限らない.) 正則環であることとその大域次元が有限であることも同値. (このとき, 大域次元はクルル次元と一致する.)
- 一変数多項式環を取る操作で正則性は保たれる.

•

工事中

A.6　単因子論とジョルダン標準形

工事中

A.7　可換環論の話題

付録 B　環の表現論 (加群論)

B.1　クルル–シュミット性

工事中

参考文献について

(大変失礼なことに) このノートに載っているすべての結果について, その参考文献を挙げることはできそうにない. ただ, できるだけ読者が自分で調べられる (参考文献を得られる) ように, その痕跡を残すように心がけるつもりである.

参考文献

[ST] J. H. Silverman and J. T. Tate, 楕円曲線論入門 (日本語版, 訳: 足立恒雄, 木田雅成, 小松啓一, 田谷久雄). 丸善出版 (1992, 2015).

[後] 後藤四郎, 可換環論の勘どころ. 数学のかんどころ **32**, 共立出版 (2017).

[三] 三宅敏恒, 入門代数学. 培風館 (1999).

[雪] 雪江明彦, 初等整数論から p 進数へ. 日本評論社 (2013).