目 次

第1章　環とイデアル

1.1　環とその準同型写像

R が環であるとは, まず R は空でない集合であって, その上 R には 2 つの演算が与えられていて, 一方を $+$ (加法), 他方を $\times$(乗法) であらわすとき次の条件 (公理) をみたすことをいう.

(1) $(R,+)$ は an abelian group をなし
(2) $^{\forall}a,b \in R$ に対し $(ab)c = a(bc)$
(3) $^{\forall}a,b \in R$ に対して $a(b+c) = ab+ac$, $(a+b)c = ac+bc$
(4) $^{\exists}1 \in R$; $a1 = 1a = a$, $^{\forall}a \in R$

Lemma 1.1.1. R が環であるとき, 上の定義の条件 (4) をみたす $1 \in R$ は, R 内に唯一である. これを R の単位元 (*the identity*) という.

Proof. 条件 (4) をみたす元 $1' \in R$ をとると, $1' = 11' = 1'1 = 1$. □

最も基本的な環の例を 2 つ挙げておく.

Example 1.1.2.
(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は数の加法と乗法を演算として環をなす.
(2) $n > 0$ として $R = \{A | A$ は n 次の実正方行列 $\}$ とすれば集合 R は行列の和と積を演算にして環をなす.

(1) の例については乗法についての交換法則 ($ab = ba \quad for\ ^{\forall}a,b \in R$) が成立する. このような環を可換環という. (2) の例では, $n \geq 2$ であれば交換法則は一般には成り立たない. このような環を非可換環とよぶ.
次にしばらくの間, R を環とし, 環演算の基本的な性質を論ずることにしよう.

Lemma 1.1.3. 環 R の加法についての単位元は 0 で表し $a \in R$ の逆元は $-a$ で表す. そして, $^{\forall}a,b \in R$ に対して $a-b := a+(-b)$ により減法を定める.

(1) $a0 = 0a = 0$, $^{\forall}a \in R$.
(2) $(-a)b = a(-b) = -ab$, $^{\forall}a,b \in R$.
(3) $-a = (-1)a$, $(-a)(-b) = ab$.
(4) $a(b-c) = ab-ac$, $(a-b)c = ac-bc$.

Proof. $0+0 = 0$. $\therefore a0 = a(0+0) = a0+a0$. $\therefore a0 = 0$. 同様に $0a = (0+0)a = 0a+0a$ より $0a = 0$ を得る. $a(-b)+ab = a\{(-b)+b\} = a0 = 0$. $\therefore a(-b) = -ab$. $(-a)b+ab = \{(-a)+a\}b = 0b = 0$. $\therefore (-a)b = -ab$. $(-a)(-b) = -[a(-b)] = -(-ab) = ab$, $(-1)a = -(1a) = -a$ となる. $a(b-c) = a[b+(-c)] = ab+a(-c) = ab-ac$, $(a-b)c = [a+(-b)]c = ac+(-b)c = ac-bc$. □

このことからわかるように, もし R 内で $1=0$ が成り立つならば ${}^{\forall}a \in R,\ a = a1 = a0 = 0$ となり $R=\{0\}$ となる. よって以下の議論では特に断らないときは,

$$1 \neq 0$$

であると仮定しよう.

R, S を環とし $\varphi : R \to S$ を写像とする. φ が次の条件をみたすとき環の準同型写像であるという.

${}^{\forall}a, b \in R$ に対し
(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$.
(2) $\varphi(ab) = \varphi(a)\varphi(b)$.
(3) $\varphi(1) = 1$.

(1) によると φ は加法については群の準同型写像であるから ${}^{\forall}a, b \in R$ について $\varphi(-a) = -\varphi(a)$, $\varphi(a-b) = \varphi(a) - \varphi(b)$, $\varphi(0) = 0$ である.

Example 1.1.4.

(1) $\mathbb{C}$ は可換環である. 今 $\begin{array}{ccccc} \varphi & : & \mathbb{C} & \longrightarrow & \mathbb{C} \\ & & \cup & & \cup \\ & & a+bi & \longmapsto & a-bi \end{array}$ は環の準同型写像である.

(2) $\begin{array}{ccccc} \varphi & : & \mathbb{R} & \longrightarrow & \mathrm{M}_2(\mathbb{R}) \\ & & \cup & & \cup \\ & & a & \longmapsto & \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \end{array}$ は環の準同型写像である.

Exercise 1. $\varphi : \mathbb{R} \to \mathbb{R}$ が環の準同型写像であれば, φ は恒等写像である.

Proof. $f(1) = 1$ であるから $0 < {}^{\forall}n \in \mathbb{Z},\ f(n) = n.\ \therefore {}^{\forall}r \in \mathbb{Z},\ f(r) = r.$ ここで $f(1) = 1$ であること, ${}^{\forall}q \in \mathbb{Q}$ は $a, b \in \mathbb{Z}$ を $a \neq 0$ にとり $q = \frac{b}{a}$ と表せることから $f(q) = q$ をうる. $0 < {}^{\forall}a \in \mathbb{R},\ a = b^2$ とかくと $f(a) = f(b^2) = f(b)^2$ である. 一方で, $1 = f(1) = f(a\frac{1}{a}) = f(a)f(\frac{1}{a})$ より $f(a) \neq 0.\ \therefore f(a) > 0.$

$$\therefore \quad a, b \in R,\ b > a \Rightarrow f(b) > f(a).$$

さて, ${}^{\forall}a \in R$ をとる. $f(a) = a$ を証明したいので $f(a) \neq a$ としてみよう. このとき $f(a) < a$ であるか, もしくは $f(a) > a$ であるが, もし $f(a) < a$ であれば ${}^{\exists}x \in \mathbb{Q}$ s,t $f(a) < x < a.\ \therefore f(a) < x = f(x) < f(a)$ となり矛盾. 同様にして $f(a) > a$ も矛盾であるので $f(a) = a$ をうる. □

$\varphi : R \to R'$ を環の準同型写像とする. φ に対して

$$\mathrm{Ker}\,\varphi := \{a \in R | \varphi(a) = 0\}$$

とおき φ の Kernel という. $\mathrm{Ker}\,\varphi$ は次の性質をもつ;

(1) $\emptyset \neq \mathrm{Ker}\,\varphi \subseteq R.$ とくに $0 \in \mathrm{Ker}\,\varphi$ である.
(2) ${}^{\forall}x, y \in \mathrm{Ker}\,\varphi,\ {}^{\forall}a \in R$ をとれば $x+y, ax \in \mathrm{Ker}\,\varphi.$

(実のところ $\mathrm{Ker}\,\varphi$ は加法について R の部分群である.)

Lemma 1.1.5. $\varphi : R \to R'$ を環の準同型写像とすると, φ は単射である $\Leftrightarrow \mathrm{Ker}\,\varphi = \{0\}$ である.

Definition 1. 環 R に対し, I が R の *ideal* であるとは,

(1) $\emptyset \neq I \subseteq R$.
(2) $^\forall a \in R$, $^\forall x, y \in I$ について $x+y, ax, xa \in I$.

の 2 つの条件がみたされることをいう. もし R が可換環ならば, (2) は

$$^\forall a \in R,\ ^\forall x, y \in I,\quad x+y, ax \in I$$

となることに注意すること. 集合 $\{0\}$, R は, R の *ideal* である. I が R の *ideal* であれば $(-x = (-1)x)$, $I = R \Leftrightarrow 1 \in I$ であって $I \triangleleft R$ が成り立つ.

Example 1.1.6.
(1) $R = \mathbb{Z}$ のとき. $^\forall a \in \mathbb{Z}$ について $I = \{na | n \in \mathbb{Z}\}$ とおくと, I は $\mathbb{Z}$ の *ideal* である. この I を a で生成された $\mathbb{Z}$ の *ideal* といって (a) と表す.
(2) $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ には $\{0\}$ と R しかない.
(3) n を自然数とし, $R = \mathrm{M}_n(\mathbb{R})$ とすると R 内の *ideal* は $\{0\}$, R だけである.

Proof. (3) のみ. I を $\{0\}$ でない $\mathrm{M}_n(\mathbb{R})$ の ideal とする. $0 \neq {}^\exists A \in I$; $r = \mathrm{rank}\,A$ とおくと, A を基本変形していくことで

$$A = \left(\begin{array}{ccc|c} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ \hline & 0 & & 0 \end{array}\right) \in I. \qquad \therefore \quad \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & 0 \end{array}\right) \in I.$$

よって, $E \in I$ となり $I = \mathrm{M}_n(\mathbb{R})$ をうる. □

環 R 内に, いかなる ideal が含まれているかは, R の環構造の解析 (内部構造論) の重要な手がかり (指標) であると考えられている.

さて, I を環 R の ideal で, $I \neq R$ であるものとすると, $I \triangleleft R$ であるから剰余類群 R/I を考えることができる. このとき, R/I は次の演算によって環となる.

$$\overline{a} \cdot \overline{b} := \overline{ab}.$$

とくに, R が可換であれば R/I も可換である.

Proof. この証明において重要なことは, 積が well-defined であることにある. よって, ここではその事だけを証明して後は読者に委ねることにする. $^\forall \alpha, \beta \in R/I$ をとり, $\alpha = \overline{a} = \overline{a_1}$, $\beta = \overline{b} = \overline{b_1}$ とおく. すると $a - a_1, b - b_1 \in I$ より $a - a_1 = i$, $b - b_1 = j$ ($i, j \in I$) とかくと $ab = (a_1 + i)(b_1 + j) = a_1 b_1 + b_1 i + a_1 j + ij$. $\therefore ab - a_1 b_1 \in I$. □

R/I を, R の I による剰余環という. そして, $\varepsilon : R \to R/I$, $a \mapsto \overline{a}$ を自然な写像という. R/I を考えることは, R から I を経由して新しい環を作る操作であるとみなせる.

Proposition 1.1.7. $\varepsilon : R \to R/I$, $a \mapsto \overline{a}$ は環の準同型写像であって, 全射であり, $\mathrm{Ker}\,\varepsilon = I$ となる.

Corollary 1.1.8. 環 R 内の *ideal* $I \neq R$ は, 全て何かある環の準同型写像の *Kernel* である.

Corollary 1.1.9. $R = \mathrm{M}_n(\mathbb{R})$ とすると, ${}^{\forall}\varphi : R \to R'$ 環の準同型写像は単射である.

Definition 2. S を環とする. R が S の部分環であるとは,

(1) $\emptyset \neq R \subseteq S$
(2) ${}^{\forall}a, b \in R$ について $a \pm b, ab, -a \in R$ かつ
(3) $1 \in R$

が成立することをいう. よって, S は S の部分環である.

Lemma 1.1.10. R が S の部分環ならば, R は S の和と積を演算に環である.

たとえば, $\varphi : R \to S$ を環の準同型写像とすれば, $\varphi(R)$ は S の部分環であって, 従って $\varphi(R)$ はそれ自身で環であり,

$$\begin{array}{ccccc} f & : & R & \longrightarrow & \varphi(R) \\ & & \cup & & \cup \\ & & a & \longmapsto & \varphi(a) \end{array}$$

は環の準同型写像であって全射となる.

Example 1.1.11. $\mathbb{C} \supset R = \{a + b\,i | a, b \in \mathbb{Z}\}$, $S = \{a + b\,i | a, b \in \mathbb{Q}\}$ とおくと, R, S は $\mathbb{C}$ の部分環であってさらに R は S の部分環でもある.
$A = \{a + \sqrt{2}\,b | a, b \in \mathbb{Q}\}$ とおくと A は $\mathbb{R}$ の部分環である.

Example 1.1.12.

$$R = \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} x & y \\ 0 & a \end{pmatrix} \middle| x, y \in \mathbb{Q},\ a \in \mathbb{Z} \right\} \subset \mathrm{M}_2(\mathbb{Q})$$

としよう. R は $\mathrm{M}_2(\mathbb{Q})$ の部分環である. この R は可換環ではない. そして, *Right noetherian* であるが *Left noetherian* ではない.

$$\begin{array}{ccccc} R & \xrightarrow{p_1} & \mathbb{Q} & \qquad R & \xrightarrow{p_2} & \mathbb{Z} \\ \cup & & \cup & \cup & & \cup \\ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} & \longmapsto & a & \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} & \longmapsto & c \end{array}$$

は環の準同型写像で全射となっている. この R も実に奇妙な性質をもつ.

Exercise 2.
(1) $R = \left\{a + b\sqrt{2} | a, b \in \mathbb{Q}\right\}$ とおくと R は数の和と積を演算にして可換環となることを確かめよ.

(2) $R = \{a+bi | a,b \in \mathbb{Q}\}$ とすれば R は数の和と積を演算にして可換環となることを確かめよ．但し，$i = \sqrt{-1}$ を表すものとする．

(3) I が $\mathbb{Z}$ の *ideal* であれば $I = (a)$ となる $a \in \mathbb{Z}$ が存在することを示せ．

(4) n を自然数とし $R = \left\{ \begin{pmatrix} a_{11} & & * \\ & a_{22} & \\ 0 & & \ddots \\ & & & a_{nn} \end{pmatrix} \middle| a_{ij} \in \mathbb{R} \right\}$ とすれば R は行列の加法と積を演算にして環をなすことを確かめよ．

(5) $p \geq 2$ を素数とし $R = \mathbb{Z}/(p)$ とすると，R 内には *ideal* は (0), R のみであることを示せ．

(6) R は可換環とする．$a, b \in R$ に対して $I = \{ax + by | x, y \in R\}$ とおくと I は a, b を含む最小の R の *ideal* であることをたしかめよ．

(7) P を n 次の実正則行列とし $R = \mathrm{M}_n(\mathbb{R})$ とする．
$$\begin{array}{ccccc} \varphi & : & R & \longrightarrow & R \\ & & \cup & & \cup \\ & & A & \longmapsto & P^{-1}AP \end{array}$$
は環の準同型写像である
ことをたしかめよ．また，
$$\begin{array}{ccccc} \varphi & : & R & \longrightarrow & R \\ & & \cup & & \cup \\ & & A & \longmapsto & {}^tA \end{array}$$
は環の同型写像であることをたしかめよ．

1.2 整域と体

以下, R は環とする．

Definition 3. $a \in R$ が, ${}^{\exists}x \in R$ s,t $ax = xa = 1$ をみたすとき, この $a \in R$ を R の単元 (*a unit*) とよび,

$$\mathrm{U}(R) := \{u \in R | u \text{ は } R \text{ の単元 }\}$$

とかくことにする．勿論, 上のような $x \in R$ は, a に対して唯一に定まるので $x = a^{-1}$ とかき, a の逆元という．$1 \in R$ は自明な単元である．

Lemma 1.2.1. $\mathrm{U}(R)$ は R の乗法を演算にして群をなす．

Example 1.2.2.
(1) $\mathrm{U}(\mathbb{Z}) = \{1, -1\}$, $\mathrm{U}(\mathbb{R}) = \mathbb{R}\backslash\{0\}$.
(2) $\mathrm{U}\left(\mathrm{M}_n(\mathbb{R})\right) = \mathrm{GL}_n(\mathbb{R})$.

Lemma 1.2.3. $I \subsetneq R$ は *ideal* とする．$a \in R$ としたとき,

$$\overline{a} \in \mathrm{U}\left(R/I\right) \Leftrightarrow {}^{\exists}x \in R \quad s,t \ 1-ax, 1-xa \in I.$$

Lemma 1.2.4. $\varphi : R \to R'$ を環の準同型写像とする．このとき, ${}^{\forall}a \in \mathrm{U}(R)$ について $\varphi(a) \in \mathrm{U}\left(R'\right)$, $\varphi(a)^{-1} = \varphi(a^{-1})$ である．

Lemma 1.2.5. $a \in \mathrm{U}(R)$ ならば, $x \in R$ について $ax = 0$ であれば $x = 0$. 同様に, $xa = 0$ なら $x = 0$.

さて, 更に R は可換環であるとする.

Definition 4. $a \in R$ が R-*nzd* ($non-zero\ divisor$) であるとは,

$$x \in R \text{ について } ax = 0 \text{ ならば } x = 0 \text{ である}$$

が成り立つことをいう. 従って, ${}^{\forall}u \in \mathrm{U}(R)$ は R-*nzd* である.

一方で, $a \in R$ が R-*zd* であるとは, a は R-*nzd* ではないこと, つまり

$$0 \neq {}^{\exists}x \in R \quad s,t\ ax = 0$$

をみたすものをいう. $\therefore 0 \in R$ は R-*zd* である.

Lemma 1.2.6. $a \in R$ を R-*nzd* にとれば, $\widehat{a} : R \to R$ は単射である. よって, $x, y \in R$ についてもし $ax = ay$ であれば $x = y$ である.

Corollary 1.2.7. $|R| < \infty$ であれば, $a \in R$ について, a が R-*nzd* であれば $a \in \mathrm{U}(R)$ である.

Proof. $\widehat{a} : R \to R$ は単射であるから, $|R| < \infty$ をあわせて, $\widehat{a}$ は bijection になる. $\therefore {}^{\exists}x \in R$ s,t $1 = \widehat{a}(x) = ax$. □

$0 \in R$ は R-zd であった. もし R 内に 0 以外の R-zd が存在しないとき, この R のことを整域とよぶことにしよう. つまり,

Definition 5. 可換環 R が整域であるとは, $a, b \in R$ について $ab = 0$ であれば $a = 0$ か又は $b = 0$, が成立することである. 例えば, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ などは整域であるが, $\mathbb{Z}/(6)$ はそうではない.

そして, $0 \neq {}^{\forall}a \in R$ が R の単元であるとき, R は体であるという. よって, 体は整域であって $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ などは体である.

Corollary 1.2.8.
(1) 整域の任意の部分環は整域である.
(2) 有限整域は体である.

R が体であるとき, $a, b \in R$, $a \neq 0$ について $a^{-1}b$ を $\dfrac{b}{a}$ とかくことにする. すると, $a \cdot \dfrac{b}{a} = \dfrac{b}{a} \cdot a = b$ である. すなわち, $x = \dfrac{b}{a} \in R$ は $ax = xa = b$ をみたす R の元として特徴付けられる. もちろん, $a^{-1} = \dfrac{1}{a}$ となる. さらに次が成立する.

Proposition 1.2.9. R は体であって, $a, b, c, d \in R$, $a, c \neq 0$ とすると,

(1) $\dfrac{b}{a} + \dfrac{d}{c} = \dfrac{cb + ad}{ac}$, $\dfrac{b}{a} \cdot \dfrac{d}{c} = \dfrac{bd}{ac}$.
(2) $\dfrac{bc}{ac} = \dfrac{b}{a} = \dfrac{cb}{ca}$.
(3) $-\dfrac{b}{a} = \dfrac{-b}{a} = \dfrac{b}{-a}$, $\dfrac{0}{a} = 0$, $\dfrac{b}{a} - \dfrac{d}{c} = \dfrac{cb - ad}{ac}$.
(4) $\dfrac{b}{1} = b$.

Proof. (1) の前者を示す. あとは読者に委ねる. $(ac)\left(\dfrac{b}{a}+\dfrac{d}{c}\right)=(ac)\dfrac{b}{a}+(ac)\dfrac{d}{c}=bc+da.$ □

Exercise 3.

(1) $R=\{a+b\,i|a,b\in\mathbb{Z}\}$ を数の加法と乗法によって環とみなすとき, $\mathrm{U}(R)=\{1,-1,i,i\}$ であることを確かめよ.

(2) R を環とすると $^{\forall}u\in\mathrm{U}(R)$ に対して $-u\in\mathrm{U}(R)$ であって, $(-u)^{-1}=-u^{-1}$ であることを確かめよ.

(3) $A\in\mathrm{M}_n(\mathbb{R})$ が, $X\in\mathrm{M}_n(\mathbb{R})$ をとり $XA=0$ ならば $X=0$ である, をみたすならば $A\in\mathrm{U}(\mathrm{M}_n(\mathbb{R}))$ であることを示せ.

(4) $R=\mathbb{Z}$, $2\leq n\in\mathbb{Z}$ とする. $I=(n)$ としたとき, $a\in R$ について

$$\overline{a}\in\mathrm{U}(R/I)\Leftrightarrow(a,n)=1$$

を証明せよ.

(5) $2\leq n\in\mathbb{Z}$ とする. $\mathbb{Z}/(n)$ が整域であることと n は素数であることは同値であることを確かめ, そのとき, $\mathbb{Z}/(n)$ が体であることを証明せよ.

(6) R を環, $0<n\in\mathbb{Z}$ とし, $\mathrm{M}_n(R)=\{(a_{ij})|a_{ij}\in R\}$ とおくと, $\mathrm{M}_n(R)$ は環であることを示せ.

(7) $R=\mathbb{Z}/(11)$ とする. 次を計算せよ.

$$\frac{\overline{3}}{\overline{2}}+\frac{\overline{7}}{\overline{6}}\,,\quad \frac{\overline{5}}{\overline{4}}\cdot\frac{\overline{10}}{\overline{7}}\,,\quad \frac{\overline{6}}{\overline{7}}-\frac{\overline{4}}{\overline{5}}\,,\quad -\frac{\overline{10}}{\overline{9}}.$$

(8) R, R' を環とし, $R\cong R'$ であるとする. R が可換であれば R' も可換であることを確かめよ. 又, R が整域 (*resp*, 体) であれば R' も整域 (*resp*, 体) であることを確かめよ.

(9) R は環とする. $a\in R$ のついて $a^0=1$, $a^1=a$ とし $a^n=a^{n-1}a$ ($^{\forall}n\geq 2$) と定める. このとき次を示せ.

(*i*) $^{\forall}a\in R$, $0\leq{}^{\forall}m,n\in\mathbb{Z}$ について $a^ma^n=a^{m+n}$, $(a^m)^n=a^{mn}$ である.

(*ii*) $a,b\in R$; $ab=ba$ とすれば, $0\leq{}^{\forall}n\in\mathbb{Z}$ について $(ab)^n=a^nb^n$ である.

(10) R は環とする. $n>0$, $a_1,\cdots,a_n\in R$ のとき

$$a_1a_2\cdots a_n:=((\cdots((a_1a_2)\,a_3)\cdots)\,a_{n-1})\,a_n$$

と定めるとき, 次を確かめよ.

(*i*) $(a_1\cdots a_n)(b_1\cdots b_m)=a_1\cdots a_nb_1\cdots b_m$.

(*ii*) R が可換であれば, $^{\forall}\sigma\in\mathfrak{S}_n$ について

$$a_1a_2\cdots a_n=a_{\sigma(1)}a_{\sigma(2)}\cdots a_{\sigma(n)}.$$

但し, $m,n\geq 0$; $a_ib_j\in R$ とする.

(11) $\varphi:R\to S$ を環の準同型写像, $I=\mathrm{Ker}\,\varphi$ とおくと $R/I\cong\varphi(R)$ を証明せよ.

1.3 $\mathbb{Z}$ の基本的性質

ここでは, 整数環 $\mathbb{Z}$ について議論しよう. $\mathbb{Z}$ は代表的な可換環であり, 体ではないが整域である. 次の Lemma が全てを支配する.

Lemma 1.3.1. $0 < n \in \mathbb{Z}$ とすると $^{\forall}m \in \mathbb{Z}$ に対して $^{\exists 1}q, r \in \mathbb{Z}$ *where* $m = qn + r$, $0 \leq r < n$.

Proof. $q \in \mathbb{Z}$ は $\max\{q \in \mathbb{Z} | qn \leq m\}$ をとり, そのとき $m - qn$ を r ととればよい. これにより存在は保証できたので, 唯一であることを示す. (q, r), (q', r') を上のようにとると $m = qn + r = q'n + r'$ であるから $n(q - q') = r' - r$ となり $n | r' - r$ をうるが, これは $r' - r = 0$ を導く. $\therefore q = q'$. □

Corollary 1.3.2. $^{\forall}I \subseteq \mathbb{Z}$; *ideal,* $^{\exists}a \in I$ *s,t* $I = (a)$.

Proof. $I = \{0\}$ ならば $a = 0$, $I = \mathbb{Z}$ ならば $a = 1$ をとればよい. よって $(0) \neq I \subseteq \mathbb{Z}$ としてよい. 今, $a = \min\{a \in I | a > 0\}$ とおく. これから $I = (a)$ を証明する. $(a) \subseteq I$ は自明である. $0 \neq {}^{\forall}x \in I$ をとると $^{\exists 1}q, r \in \mathbb{Z}$ s,t $x = qa + r$, $0 \leq r < a$. $\therefore r = x - qa \in I$ であるが, a の最小性をみて $r = 0$. $\therefore I = (a)$. □

Remark 1.3.3.
(1) $\mathbb{Z}$ の *ideal* I に対して $I = (a)$ となる $a \in \mathbb{Z}$ は, $a \geq 0$ の範囲では唯一つである.
(2) $a, b \in \mathbb{Z}$ について, $a \in (b) \Leftrightarrow b | a$. 従って, $(a) = (b)$ であることと $a = b$ *or* $a = -b$ は同値である.

Proposition 1.3.4. $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ を $\mathbb{Z}$ の *ideals* の列とすれば, $^{\exists}k \leq 1$ *s,t* $I_k = I_{k+1} = \cdots$.

Proof. $I = \bigcup_{i \geq 1} I_i$ とおく. この I は, $^{\forall}i \geq 1$ について I_i が ideal であることと I. が a chain をなすことから, ideal であることが確かめられる. $\therefore {}^{\exists}a \in I$ s,t $I = (a)$. 従って, $^{\exists}k \geq 1$; $a \in I_k$ であるが, $I_r \subseteq I$ $(^{\forall}r)$ であるから $I = I_k$ をうる. □

Corollary 1.3.5. $\mathfrak{S} = \{I | I$ は $\mathbb{Z}$ の *ideal*$\}$ とおくと, $\emptyset \neq {}^{\forall}\mathcal{S} \subseteq \mathfrak{S}$; *a subset* は $^{\exists}I \in \mathcal{S}$ *s,t* $J \in \mathcal{S}$ について $I \subseteq J$ ならば $I = J$.　(i, e　I は $\mathcal{S}$ 内で *maximal* である.)

Proof. maximal element をもたない $\emptyset \neq \mathcal{S} \subseteq \mathfrak{S}$ が存在したとする. $^{\forall}I_1 \in \mathcal{S}$ をとると $^{\exists}I_2 \in \mathcal{S}$ s,t $I_1 \subsetneq I_2$. 同様にして $^{\exists}I_3 \in \mathcal{S}$ s,t $I_2 \subsetneq I_3$.

$$\therefore \quad {}^{\exists}a \textit{ chain}; \quad I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots .$$

しかし, これは上の Proposition に反する. $\therefore {}^{\exists}I \in \mathcal{S}$ s,t I は max in $\mathcal{S}$. □

これら, 2 つの命題については後に Noetherian rings について議論をしているあたりでもう一度, 詳しく触れることにする.

Definition 6. I を $\mathbb{Z}$ の *ideal* とし, $I \neq \mathbb{Z}$ であるものとする. もし *ideal* J が $I \subseteq J \subseteq \mathbb{Z}$ であれば $I = J$ *or* $J = \mathbb{Z}$ である, が成立するとき I は $\mathbb{Z}$ の極大 *ideal* (*maximal ideal*) であるという.

Corollary 1.3.6. $I \neq \mathbb{Z}$ を *ideal* とすれば, $^{\exists}\mathfrak{m} \subsetneq \mathbb{Z}$; *max ideal s,t* $I \subseteq \mathfrak{m}$.
よって, $I = (0)$ とすれば $\mathbb{Z}$ 内には少なくとも一つは *max ideal* が存在することがわかる.

Proof. $\mathcal{S} = \{J | J$ は $\mathbb{Z}$ の *ideal*, $J \neq \mathbb{Z}$, $I \subseteq J\}$ とすればよい. □

Definition 7. $a \in \mathbb{Z}$ について, a が $\mathbb{Z}$ の素元であるとは (a) が $\mathbb{Z}$ の *max ideal* であることとする. 上の *Corollary* により $\mathbb{Z}$ 内には少なくとも一つは *max ideal* $\mathfrak{m}$ が存在して, $\mathfrak{m}$ は $\mathbb{Z}$ の *ideal* であるから $\mathfrak{m} = (x)$ となる $x \in \mathbb{Z}$ をとれば, この $x \in \mathbb{Z}$ は素元である. よって, $\mathbb{Z}$ 内には一つは素元がある.

そこで,

Lemma 1.3.7. $\mathfrak{m}$ が $\mathbb{Z}$ の *max ideal* であれば $\mathbb{Z}/\mathfrak{m}$ は体をなす. 逆に, I を $\mathbb{Z}$ の *ideal* としたとき, もし $\mathbb{Z}/I$ が体であれば I は $\mathbb{Z}$ の *max ideal* である.

Proof. $0 \neq {}^{\forall}\alpha \in \mathbb{Z}/\mathfrak{m}$ をとり $\alpha = \overline{a}$, ($a \in \mathbb{Z}$) と表すと, $\alpha \neq 0$ としていたので $a \notin \mathfrak{m}$. $\therefore J := (a) + \mathfrak{m} = \{ax + y | x \in \mathbb{Z},\ y \in \mathfrak{m}\}$ とおくと, J は $\mathbb{Z}$ の ideal であって $\mathfrak{m} \subsetneq I$ である. $\therefore J = \mathbb{Z}$; i,e ${}^{\exists}x \in \mathbb{Z}$, ${}^{\exists}y \in \mathfrak{m}$ s,t $1 = ax + y$. $\therefore \overline{1} = \overline{ax} + \overline{y} = \overline{a} \cdot \overline{x}$ in $\mathbb{Z}/\mathfrak{m}$.

さて, I を $\mathbb{Z}$ の ideal で, $\mathbb{Z}/I$ が体であるとしよう. $I \neq \mathbb{Z}$ であるから ${}^{\exists}\mathfrak{m}$; max ideal of $\mathbb{Z}$ s,t $I \subseteq \mathfrak{m}$. もし $I \neq \mathfrak{m}$ ならば $\mathfrak{m} \ni {}^{\exists}a \notin I$. $\therefore 0 \neq \overline{a}$ in $\mathbb{Z}/I$. $\therefore {}^{\exists}x \in \mathbb{Z}$ s,t $1 - ax \in I$. よって, $i \in I$ をとり $1 = ax + i$ と表せる. $\therefore 1 = ax + i \in \mathfrak{m}$. (矛盾) □

Definition 8. $a, b \in \mathbb{Z}$ について,

$$a|b \overset{\text{def}}{\Leftrightarrow} a \in (b) \quad \left(\Leftrightarrow\ a = \ell b \ \ {}^{\exists}\ell \in \mathbb{Z} \right)$$

とする.

Corollary 1.3.8. $a \in \mathbb{Z}$ は素元とする. このとき

(1) $a \notin \mathrm{U}(\mathbb{Z})$, $a \neq 0$.
(2) $b, c \in \mathbb{Z}$ について $a|bc \Rightarrow a|b$ *or* $a|c$.
(3) $b \in \mathbb{Z}$ が $b|a$ ならば $b \in \mathrm{U}(R)$ *or* $b = \varepsilon a$ *for some* $\varepsilon \in \mathrm{U}(\mathbb{Z})$.

Proof. $\mathfrak{m} = (a)$ は max ideal of $\mathbb{Z}$ であるから, もし $a = 0$ であれば $(a) = (0) \subsetneq (2) \subsetneq \mathbb{Z}$ となり $a \neq 0$, もし $a \in \mathrm{U}(\mathbb{Z})$ であれば $(a) = \mathbb{Z}$ となり $\mathbb{Z}/I = \{0\}$ をみて $a \notin \mathrm{U}(\mathbb{Z})$. $b, c \in \mathbb{Z}$ を $bc \in (a)$ とする. $\therefore \overline{b}\overline{c} = 0$ in $\mathbb{Z}/(a)$, $\overline{b} = 0$ or $\overline{c} = 0$. よって, $b \in (a)$ であるか又は $c \in (a)$ をうる. $b \in \mathbb{Z}$ が $a \in (b)$ をみたせば, $(b) = (a)$ であるか $(b) = \mathbb{Z}$ である. 今, $(b) = \mathbb{Z}$ であれば $b \in \mathrm{U}(\mathbb{Z})$ であって, $(b) = (a)$ であれば $a \in (b)$ より $a = \ell_1 b$ (${}^{\exists}\ell_1 \in \mathbb{Z}$), $b \in (a)$ より $b = \ell_2 a$ (${}^{\exists}\ell_2 \in \mathbb{Z}$) であるので $a = \ell_1 b = (\ell_1 \ell_2) a$. $\therefore \ell_1, \ell_2 \in \mathrm{U}(\mathbb{Z})$. □

Proposition 1.3.9. $1 \leq a \in \mathbb{Z}$ であれば次は同値である.

(1) a は素元である.
(2) $2 \leq a \in \mathbb{Z}$ であって, $1 \leq d \in \mathbb{Z}$ について $d|a$ であれば $d = 1$ *or* $d = a$.

Proof. (2)⇒(1) のみ. $I = (a)$ とすると, $I \neq \mathbb{Z}$ なので $I \subseteq \mathfrak{m}$ となる $\mathfrak{m} \in \mathrm{Max}\,\mathbb{Z}$ をとると $2 \leq {}^{\exists 1}p \in \mathbb{Z}$ s,t $\mathfrak{m} = (p)$. $a \in (p)$, $p \neq 1$ であるから $a = p$ をうる. □

Theorem 1.3.10. $a \in \mathbb{Z}$ が $a \neq 0$, $a \in \mathrm{U}(\mathbb{Z})$ なら $a = p_1 p_2 \cdots p_n$ ($n > 0$; p_iは $\mathbb{Z}$ の素元) と表せ, この表現は本質的に一意である. つまり $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ ($n > 0$; q_pは $\mathbb{Z}$ の素元) ならば, $n = m$ であって ${}^{\exists}\sigma \in \mathfrak{S}_n$ *s,t* ${}^{\forall}i$ について $p_i = \varepsilon_i q_{\sigma(i)}$ *for some* $\varepsilon_i \in \mathrm{U}(\mathbb{Z})$, をみたしている.

Proof. $a \in \mathbb{Z}$ は上のようには表せないとする. すると a は素元ではない.

$$\mathcal{S} = \{(a) | 0 \neq a \in \mathbb{Z} \text{ で } a \notin \mathrm{U}(\mathbb{Z}), \text{かつ, 上の分解をもたない}\ \}$$

とすると $\emptyset \neq \mathcal{S}$, $\therefore {}^{\exists}I \in \mathcal{S}$; max elem. このとき $I = (a)$ とかくと, a は素元ではないので $I \notin \mathrm{Max}\,\mathbb{Z}$. よって $\mathfrak{m} \in \mathrm{Max}\,\mathbb{Z}$ を $I \subseteq \mathfrak{m} = (p)$ となるようにとると $a \in (p)$; p は素元であるから $a = pb$ for some $b \in \mathbb{Z}$. $J := (b)$ とすれば $p \notin \mathrm{U}(\mathbb{Z})$ をみて $I \subsetneq J$. $\therefore J \notin \mathcal{S}$; b は分解をもつ. $\therefore b = q_1 \cdots q_m$ と表すと $a = pq_1 \cdots q_m$. (矛盾)

さて, $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$; $n, m > 0$, p_i, q_j は素元, とする. $n = 1$ のときは $a = q_1 q_2 \cdots q_m$, a は素元であるから, もし $m \geq 2$ であれば $q_1 \notin \mathrm{U}(\mathbb{Z})$ より $q_1 = \varepsilon a$ for some $\varepsilon \in \mathrm{U}(\mathbb{Z})$. $\therefore (a\varepsilon) q_2 \cdots q_m = a$, $1 = \varepsilon q_2 \cdots q_m$. (矛盾) $n > 1$ で $n - 1$ 以下までは正しいとする. $q_1 q_2 \cdots q_m \in (p_1)$ であるから $q_i \in (p_1)$ ${}^{\exists}i$. 適当に並べ替えをして $q_1 \in (p_1)$ としてよい. $\therefore q_1$ も素元であるから $q_1 = \varepsilon_1 p_1$ (${}^{\exists}\varepsilon \in \mathrm{U}(\mathbb{Z})$). すると, $p_2 \cdots p_n = (\varepsilon_1 q_2) q_3 \cdots q_m$ となり, induction の仮定から求める結果をうる. □

Corollary 1.3.11. $\mathbb{Z}$ には, 素元は無限に多く存在する.

Proof. 有限個しか存在しないとして, それらを $\{p_1, p_2, \cdots, p_n\}$ と表す. $a = p_1 p_2 \cdots p_n + 1 \in \mathbb{Z}$ をとると, $a \neq p_i$ ${}^{\forall}i$ であるから a は上の分解をもつので $a \in (p_i)$ ${}^{\exists}i$. したがって $a = bp_i$ $b \in \mathbb{Z}$ となるが, $1 = bp_i - p_1 p_2 \cdots p_n \in (p_i)$ という結果を導くので矛盾. □

さて, $a_1, \cdots, a_n \in \mathbb{Z}$ $(n > 0)$ をとり $I = \{r_1 a_1 + \cdots + r_n a_n | r_i \in \mathbb{Z}\}$ とおく. I は $\mathbb{Z}$ の ideal であるから ${}^{\exists}a \in \mathbb{Z}$ s,t $I = (a)$. このとき, ${}^{\forall}i$ について $a_i \in (a)$ であるから $a | a_i$ となり, もし $d \in \mathbb{Z}$ が ${}^{\forall}i$, $d | a_i$ であれば $(a) = (a_1, \cdots, a_n) \subseteq (d)$ であるから $a \in (d)$, つまり $d | a$ が得られる.
このとき, $a \geq 0$ にとっておけば (もし $a \geq 0$ であれば $a' = (-1)a$ を a のかわりにせよ.) a は, まず前者のことから全ての a_i を割っていて, 次に後者のことから $d \in \mathbb{Z}$ が a_i 全てを割るならば d は a も割っている. これは, a が $a_1, \cdots, a_n$ の最大公約数であることを言っていて,

Lemma 1.3.12. $a_1, \cdots, a_n \in \mathbb{Z}$, $(n > 0)$ とする. このとき, $0 \leq {}^{\exists 1}a \in \mathbb{Z}$ *s,t* (1) $a | a_i$ $({}^{\forall}i)$, (2) $d \in \mathbb{Z}$ が $d | a_i$ $({}^{\forall}i)$ であれば $d | a$. この a は, $a = r_1 a_1 + \cdots + r_n a_n$ ${}^{\exists}r_i \in \mathbb{Z}$ となっている. ($a_1, a_2, \cdots, a_n$の最大公約数という.)

Proof. 一意性だけ. 正の整数 a, a' が $(1) \cdot (2)$ をみたすならば, $a \in (a')$ より $a = \varepsilon a'$ であって, $a' \in (a)$ より $a' = \pi a$, 従って $a = \pi \varepsilon a$ から $\pi, \varepsilon \in \mathrm{U}(\mathbb{Z})$. $a, a' > 0$ であるから $\pi = \varepsilon = 1$, $a = a'$. $a = 0$ であれば自明に $a' = 0$ である. □

Corollary 1.3.13. $a, b \in \mathbb{Z}$ とする.

(1) a, b の最大公約数が 0 である $\Rightarrow a = 0$, $b = 0$.
(2) a, b の最大公約数が 1 である $\Rightarrow {}^{\exists}x, y \in \mathbb{Z}$ *s,t* $1 = ax + by$.

Corollary 1.3.14. $a, b \in \mathbb{Z}$ で a, b の最大公約数が 1 である. $c \in \mathbb{Z}$ について, $a | bc$ ならば $a | c$ である.

Proof. $bc = az$ for some $z \in \mathbb{Z}$, 一方で, $x, y \in \mathbb{Z}$ をとり $1 = ax + yb$ とかけるから $c = axc + ybc = axc + yaz = a(xc + yz)$. □

Exercise 4. 以上の議論を, R; 体ではない単項イデアル整域について再度行え.

1.4 埋め込みの原理と Zorn's Lemma

この Lemma を認めて使う.

Lemma 1.4.1. *A を空でない集合とすれば $^{\exists}(B, g)$ where $\emptyset \neq B$; a set, $g; A \to B$ (bijection) s,t $A \cap B = \emptyset$.*

すると,

Lemma 1.4.2. *X, Y を空でない集合とすれば, $^{\exists}(Z, \varphi)$ where Z は空でない集合であって $\varphi : X \to Z$ 全単射, $Y \cap Z = \emptyset$.*

Proof. $V = X \cup Y$ に対して $^{\exists}(W, \psi)$ where $Z \neq \emptyset$; a set であって $\psi : V \to W$ (bijection) s,t $V \cap W = \emptyset$. $X \subseteq V$ より $\psi(X) = Z$ とすると $\emptyset \neq Z \subseteq W$. $\varphi : X \to Z$, $x \mapsto \psi(x)$ とすればよい. □

以下, このノートを通して, R が a ring であるとは,

$$R;\ a\ commutative\ ring;\ R \neq (0)$$

の意味に使うこととする.

Lemma 1.4.3. *R を環とする. X は空でない集合で $f : R \to X$ は全単射とする. このとき, $^{\forall}a, b \in X$ について*

$$\begin{aligned} a + b &:= f\left(f^{-1}(a) + f^{-1}(b)\right) \\ a \cdot b &:= f\left(f^{-1}(a) f^{-1}(b)\right) \end{aligned}$$

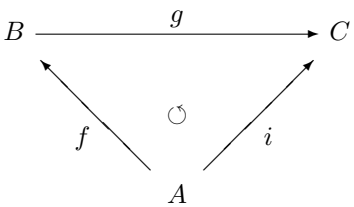
と定めると, この和と積を演算にして X は環になる. このとき, f は環の同型写像であって, もし R が体ならば X も体となる.

証明は *Exercise* としよう.

Exercise 5. 上の *Lemma* を証明せよ.

Theorem 1.4.4. *$f : A \to B$ が環の準同型写像で単射ならば, $^{\exists}(C, g)$ where $g : B \to C$ は環の同型写像であって*

s, t A は C の部分環,



もし, B が体であれば C も体である.

Proof. $B = f(A)$ であれば $C = A$ とするとよい. $B \neq f(A)$ としてよい. $\varphi : B \backslash f(A) \xrightarrow{\sim} X$, $X \cap A = \emptyset$ となる (X, φ) を見つけ g をつくり $C = X \cup A$ に環構造をいれよ. $^{\forall}a \in A$, $g(f(a)) = a = i(a)$, $\therefore A$ は C の部分環である.

$$\begin{array}{ccccc} g & : & B & \longrightarrow & C \\ & & \cup & & \cup \\ & & b & \longmapsto & \begin{cases} a & b = f(a) \in f(A) \\ \varphi(b) & b \notin f(A) \end{cases} \end{array}$$

□

さて, $X \neq \emptyset$; a set とする. 集合 X 上の関係 $\leq$ は次の 3 条件をみたすとき X 上の order であるという.

(1) ${}^{\forall}x \in X,\ x \leq x$.
(2) $x, y \in X$ について $x \leq y$ 且つ $y \leq x$ ならば $x = y$ である.
(3) $x, y, z \in X$ について $x \leq y,\ y \leq z$ ならば $x \leq z$ である.

$X = \{R \text{ の } ideal\}$ とすると, 包含関係 $\subseteq, \supseteq$ はそれぞれ X の order である. 以下, a set X 上には, an order $\leq$ が与えられていると仮定する. このとき,

Definition 9. $\emptyset \neq \mathcal{C} \subseteq X$; *a subset* が *a chain* であるとは, ${}^{\forall}a, b \in \mathcal{C}$ について $a \leq b$ *or* $b \leq a$, をみたすことをいう.

Definition 10. $\emptyset \neq \mathcal{S} \subseteq X$; *a subset* が X 内で上に有界であるとは, ${}^{\exists}x \in X$ *s,t* $s \leq x$ *for all* $s \in \mathcal{S}$, をみたすこととする.

Definition 11. $a \in X$ が *maximal in* X であるとは, もし $x \in X$ について $a \leq x$ であれば $a = x$, をみたすことである.

$\mathbb{Z}$ において I が max ideal であることは, 実は, ideal の包含関係 $\subseteq$ を order $\leq$ としたときの $\{\mathbb{Z} \text{ の } ideal\}$ の maximal であることである. この定義は, 一般の可換環においても全く同じである. つまり,

Definition 12. R を環とし, $I \neq R$ を R の *ideal* とする. I が *maximal ideal* であるとは, J; *an ideal of* R について $I \subsetneq J$ ならば $J = R$ である, をみたすことをいう. そして $\operatorname{Max} R$ によって *a set of maximal ideals of* R を表すことにする.

Corollary 1.4.5. $I \neq R$ を *ideal of* R とする.

$$I \in \operatorname{Max} R \Leftrightarrow R/I \text{ は体である.}$$

Proof. $\mathbb{Z}$ のときと同様にすればよい. □

さて,

Lemma 1.4.6 (Zorn). 全ての *chain in* X が X 内で上に有界であれば, 少なくとも一つの *maximal element* をもつ.

Theorem 1.4.7 (Well ordering theorem). $Y \neq \emptyset$; *a set* 上には少なくとも一つの *well oedering* が定義可能である. 但し, $\leq$ が *well ordering* であるとは, $\emptyset \neq {}^{\forall}\mathcal{S} \subseteq Y$; *a subset* について ${}^{\exists}s \in \mathcal{S}$; *minimal element in* $\mathcal{S}$, を満たすことを言う.

Lemma 1.4.8 (Axiom of choice). $\{X_i\}_{i \in I}$ を $\emptyset \neq I$; *a set* で ${}^{\forall}i \in I$ について $\emptyset \neq X_i$; *a set* とすると, ${}^{\exists}\{x_i\}_{i \in I}$ *where* ${}^{\forall}i \in I$ について $x_i \in X_i$. $\left(i, e;\ \prod_{i \in I} X_i \neq \emptyset. \right)$

この 3 つの主張は同値であることが知られている. (その証明は大変である.) ここでは, 以下, Zorn's Lemma を認め, 自由に扱うこととする. これから Zorn's Lemma の代表的な使用例を 2 述べよう. まず 1 つは,

Theorem 1.4.9. *R を a ring とすれば, $\emptyset \neq \operatorname{Max} R$.*

Proof. $\mathcal{S} = \{I | I$ は *a proper ideal of* $R\}$ とおく. すると, $(0) \in \mathcal{S}\emptyset$ である. 上でも述べたが, 包含関係 $\subseteq$ は $\mathcal{S}$ 上の order である. 今, $^\forall \mathcal{C} \subset \mathcal{S}$; a chain をとる. そして,

$$I := \bigcup_{J \in \mathcal{C}} J$$

とすれば, I は R の ideal で, $I \neq R$ であるから $I\mathcal{S}$. 又, $^\forall J \in \mathcal{C}$, $J \subseteq I$ は定義から自明. $\therefore {}^\exists M \in \mathcal{S}$; a maximal element of $\mathcal{S}$. 今, 私たちは $\mathcal{S}$ の order を, $\subseteq$ によって定義しているからこの $M \in \mathcal{S}$ は $M \in \operatorname{Max} R$ である. □

Corollary 1.4.10. *$I \neq R$; an ideal とすれば, $^\exists M \in \operatorname{Max} R$ s,t $I \subseteq M$.*

P を R の ideal とする. もし, $P \neq R$ であってかつ

$$a, b \in R \text{ について, もし } ab \in P \text{ ならば } a \in P \text{ であるか又は } b \in P \text{ である}$$

をみたすとき, この P を prime ideal という. そして, $\operatorname{Spec} R$ によって a set of prime ideals of R を表すことにする. すると, prime ideal についてはその特殊な性質ゆえに, 次がほとんど自明である.

Lemma 1.4.11. *$P \neq R$ を R の ideal とする.*

$$P \in \operatorname{Spec} R \Leftrightarrow R/P \text{ は } domain \text{ である.}$$

従って, $\operatorname{Max} R \subseteq \operatorname{Spec} R$ をうる.

次の例は, k を体として,

Theorem 1.4.12. *$^\forall M$; $k - vector$ s.p は, (有限, 無限に関係なく) 必ず基底をもつ.*

である. これを証明するには少し準備が必要であろう. 以下, V は an k-vector s.p であるとする.

Definition 13. *$T \subseteq V$; a set とする. $s(T)$ によって an subspace of V generated by T を表すものとする. このとき,*

$$\begin{aligned} s(T) &:= \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; n > 0,\ a_i \in k,\ x_i \in T \right\} \\ &= \bigcap_{\substack{W \subseteq V;\ subspace\ of\ V \\ T \subseteq W}} W \end{aligned}$$

である. つまり $s(T)$ は, 集合 T を含む V の subspace で最小なものを表している.

Lemma 1.4.13. *X, Y を V の subsets とする.*

(S_1) $X \subseteq Y \Rightarrow s(X) \subseteq s(Y)$.
(S_2) $x \in s(X) \Rightarrow {}^\exists X' \subseteq X$ s,t $|X'| < \infty$, $x \in s(X')$.
(S_3) $X \subseteq s(X)$.

(S_4) $s(X) = s(s(X))$.
(S_5) $x \in V$ とする. $y \in s(X,\ x)$ *and* $y \notin s(X) \Rightarrow x \in s(X,\ y)$.

但し, $s(X,\ Y) := s(X \cup Y)$ とする.

Proof. (S_i) $i = 1, 2, 3, 4$ は自明である. $y \in s(X,\ x)$, $y \notin s(X)$ より $y = bx + \xi$ for $0 \neq b \in k$, $\xi \in s(X)$. よって $x = b^{-1}y - b^{-1}\xi \in s(X,\ y)$ である. □

Corollary 1.4.14. $X \subseteq V$; *a subset of* V について, $X = free \Rightarrow Y = free$ *for all* $Y \subseteq X$; *a subset,* が成立する.

Definition 14. $X \subseteq V$; *a subset* とする. X が *a system of generators of* V (これからは, 単に *gen of* V とかく.) であるとは, $V = s(X)$, をみたすことである. 例えば V 自身は *gen of* V である.

X が *Z,S-free* であるとは, $^{\forall}x \in X$ に対して $x \notin s(X\backslash\{x\})$, をみたすことである. この *Z,S-free* の定義は, これまでに私たちが学んできた *free* と同値である. 従って, *Z,S-free* と *free* はこれからは区別なく, 単に *free* とかく. そして $\emptyset$ は *free* であることも自明である.

Lemma 1.4.15. $X \subseteq V$; *a subset,* $y \in V$ とする.

$$X \text{ が } free,\ y \notin s(X) \Rightarrow X \cup \{y\} \text{ も } free.$$

Definition 15. $X \subseteq V$; *a subset* とする. X が V の基底 (*basis*) であるとは, X は *free* かつ *gen of* V である, と定める.

Lemma 1.4.16. $X \subseteq V$; *a subseteq* とする, 次は同値である.

(1) X は *min gen of* V である.
(2) X は *max free* である.
(3) X は *basis of* V である.

Proof. (1)⇒(3) を示す. これは X が min gen of V を仮定して, free であることを云えばよい. X が free でないならば $^{\exists}x \in X$ s,t $x \in s(X\backslash\{x\})$. すると $X\backslash\{x\}$ は, V の generator である. 実際, $^{\forall}v \in V$ をとると $v = \sum_{y \in X} a_y y$, $a_y \in k$ であって $a_y = 0$ for almost all $y \in X$. もし, $a_x = 0$ であれば $v \in s(X\backslash\{x\})$ は自明であって, $a_x \neq 0$ であれば $a_x x \in s(X\backslash\{x\})$ であるから $a_x x$ を $X\backslash\{x\}$ で表現して, v にそれを代入すればよい. $\therefore s(X\backslash\{x\}) = V$, $X\backslash\{x\} \subsetneq X$. (矛盾)
(3)⇒(1) を示す. $^{\exists}Y \subseteq V$; a subset s,t $Y \subsetneq X$, Y は gen of V とすると, $^{\exists}x \in X\backslash Y$. $\therefore Y \subseteq X\backslash\{x\}$, $X\backslash\{x\}$ も gen of V. しかし, $x \in s(X\backslash\{x\})$ となり矛盾.
(2)⇒(3) を示す. もし X が gen of V でないならば, $^{\exists}y \in V$ s,t $y \notin S(X)$. すると $X \cup \{y\}$ も free になることは既に示しているので矛盾.
(3)⇒(2) を示す. もし, $^{\exists}Y \subseteq V$; a subset s,t Y は free, $X \subsetneq Y$ とすれば, $^{\exists}y \in Y\backslash X$. $\therefore X \subseteq Y\backslash\{y\}$. Y は free であるから $y \notin s(Y\backslash\{y\}) = V$. (矛盾) □

Theorem 1.4.17. $^{\exists}W \subseteq V$; *a subset s,t* W は *a basis of* V.

Proof. $\mathcal{R} = \{F \subseteq V | F \text{ は } free\ in\ V\}$ とおく. $\emptyset \in \mathcal{R}$ であるから $\mathcal{R}$ は要素を一つはもつ. $^{\forall}\mathcal{C} \subseteq \mathcal{R}$; a chain をとる. そして $W := \bigcup_{F \in \mathcal{C}} F$ とおく. もし $W \neq free$ であるならば, $^{\exists}v \in W$ s,t $v \in s(W\backslash\{v\})$.
$\therefore {}^{\exists}W' \subseteq W\backslash\{v\}$ s,t $|W'| < \infty$, $v \in s(W')$. $\therefore {}^{\exists}F \in \mathcal{C}$ s,t $W' \subseteq F \ni v$. もともと $v \notin W'$ としていたのだから $W' \subseteq F\backslash\{v\}$. 今, $F = free$ であるから $v \notin s(F\backslash\{v\})$. しかし $v \in s(W') \subseteq s(F\backslash\{v\})$ となり矛盾.
$\therefore W = free$, $W \in \mathcal{R}$. 従って, Zorn's Lemma は maximal free subset in V を保証し, それが V の basis である. □

Theorem 1.4.18 (Zariski-Samuel). *L を a free subset of V, S を a gen of V とすると,*

$$^{\exists}S' \subseteq S;\ a\ subset\ s,t\ \ L \cap S' = \emptyset,\ L \cup S' = basis\ of\ V.$$

Proof. $\mathcal{R} = \{S' | S' \subseteq S,\ L \cap S' = \emptyset,\ S' \cup L = free\ in\ V\}$ とおくと, $\emptyset \in \mathcal{R}$. $\therefore \mathcal{R} \neq \emptyset$. $^{\forall}\mathcal{C} \subseteq \mathcal{R}$; a chain をとり, $C = \bigcup_{S_\alpha \in \mathcal{C}} S_\alpha$ とおく.

Claim 1. $L \cap C = \emptyset$.

proof of Claim 1. もし $^{\exists}y \in L \cap C$ ならば, $y \in L$, $y \in C$ であるから $^{\exists}S_\alpha \in \mathcal{C}$; $y \in S_\alpha$. $\therefore y \in L \cap S_\alpha$. (矛盾) □

Claim 2. $L \cup C$ は *free subset in* V である.

proof of Claim 2. $L \cup C$ が free でないならば $^{\exists}y \in L \cup C$ s,t $y \in s(\{L \cup C\}\backslash\{y\})$. 集合論によって,

$$\Big(L \cup C\Big)\backslash\{y\} = (L\backslash\{y\}) \cup (C\backslash\{y\})$$

であるから, (S_2) によって $^{\exists}X \subseteq L \cup C\backslash\{y\}$; a finite subset s,t $y \in s(X)$. $\therefore {}^{\exists}S_\alpha \in \mathcal{C}$ s,t $X \subseteq L \cup S_\alpha$.
$\therefore {}^{\exists}S_\beta \in \mathcal{C}$ s,t $\{y\} \cup X \subseteq L \cup S_\beta$. 今, $X \subseteq L \cup S_\beta$ については $y \notin X$ より, $X \subseteq \{L \cup S_\beta\}\backslash\{y\}$ であるから $y \in s(\{L \cup S_\beta\}\backslash\{y\})$ であるが, この事実は $L \cup S_\beta$ は free in V であることに反する. □

この Claim 1, Claim 2 によって $C \in \mathcal{R}$ であることが示されたので $^{\exists}S' \subseteq S$; a maximal subset s,t $L \cap S' = \emptyset$, $L \cup S' = free$. よって, $S \subset s(L \cup S')$ だけを示せば十分である. $^{\forall}x \in S$ をとる. $x \notin s(L \cup S')$ であるならば, S" $:= S' \cup \{x\}$ とおくと $x \notin S(L \cup S')$ としていたのだから $x \notin L \cup S'$. このとき $L \cup S$" が free in V であることは以前に示していて, $x \notin L$ であるから $L \cap S$" $= \emptyset$ はほとんど自明である.
$\therefore S' \subsetneq S$" $\in \mathcal{R}$ となりこれは S' の maximality に反する. □

上の 2 つの定理はそれぞれが $^{\forall}V$; k-vector s.p は必ず basis を持つことを保証するが, その濃度については何も触れられてはいない. 次に述べる Lemma は, そのことについて上の事実を補助するものである.

Lemma 1.4.19. 任意の *k-vector s.p* の *basis* の濃度は一定に定まる.

Proof. もし V が有限生成であれば, 線形代数の議論から証明済み. 従って V は有限生成ではないとしてよい. W, W' を a k-vector s.p の basis とする. $^{\forall}x \in V$ に対して $^{\exists}B \subseteq W$ s,t $|B| < \infty$, $x = \sum_{w \in B} a_w w$. ここで, $^{\forall}x \in W$ に対して,

$$\mathcal{F}_x := \{B | B \subseteq W,\ |B| < \infty,\ x \in s(B)\}$$

とおく. すると,

Lemma 1.4.20. $^{\exists 1}$*minimal element in* $\mathcal{F}_x$. (その *min element* を E_xとかく.)

Proof. 有限集合についての議論なので $^{\exists}$minimal element in $\mathcal{F}_x$ は自明であるから, $E_1, E_2 \in \mathcal{F}_x$; minimal elements に対して $E_1 = E_2$ を証明すればよい. $E_1 \neq E_2$ とすると, $^{\exists} y \in E_1 \backslash E_2$. このとき, $D = E_1 \backslash \{y\}$ とおくと $x \notin s(D)$. しかし $x \in s(E_1) = s(D \cup \{y\})$ であるから, (S_5) により, $y \in s(D \cup \{x\})$.
$\therefore x \in s(E_2)$, $y \in s(D \cup E_2)$. この集合 $D \cup E_2$ は $y \notin D \cup E_2$ であって, 集合 $D \cup E_2 \cup \{y\}$ については $\{D \cup E_2 \cup \{y\}\} \subseteq W = free$ より $D \cup E_2 = free$ であるから, $D \cup E_2 \cup \{y\}$ も free in V である. 従って, $y \in s(D \cup E_2)$ は矛盾である. □

よって, $\mathcal{P}(W') := \{E_x | x \in W'\}$ とおき, $W \ni x \mapsto E_x \in \mathcal{P}(W')$ を見るに, $|E_x| < \infty$ であったから集合論の一般論を用いると $|B| \geq |\bigcup_{x \in W'} E_x|$ をうる. $\bigcup_{x \in W'} E_x \supseteq W'$ は自明であるから $|\bigcup_{x \in W'} E_x| \geq |W'|$.
$\therefore |W'| \leq |W|$. 後は, W と W' を入れ替えて $|W| \leq |W'|$ もうるので $|W| = |W'|$. □

よって,

Definition 16. $^{\forall} V \in k - \mathrm{mod}$ の対して $\dim_k V$ を V の *basis* の濃度で定める.

Exercise 6. R は *a ring* とする. $^{\forall} I \subseteq R$; *an ideal* に対して $\mathrm{V}(I) = \{P \in \mathrm{Spec}\, R | I \subseteq P\}$ とおき, $\mathcal{F} := \{\mathrm{V}(I) | I \subseteq R;\ an\ ideal\}$ とすると,

(1) $\mathrm{Spec}\, R, \emptyset \in \mathcal{F}$.
(2) $^{\forall} X_1, X_2 \in \mathcal{F}$, $X_1 \cup X_2 \in \mathcal{F}$.
(3) $\emptyset \neq {}^{\forall} \mathcal{S} \subseteq \mathcal{F}$; *a subset,* $\bigcap_{X \in \mathcal{S}} X \in \mathcal{F}$.

つまり, これにより $\mathrm{Spec}\, R$ には (*the Zariski*) *topology* が定義される.

1.5　商体あるいは局所化

ここでは, A は a ring とする. S が A 内の a multiplicity closed set (これからは, 単に *multi closed* とかく) であるとは, (1) $1 \in S \subseteq R$, (2) $0 \notin S$, (3) $^{\forall} s, t \in S$, $st \in S$, の 3 条件をみたすことをいう.

Example 1.5.1.
(1) $S = \{a \in A | a$ は $A - nzd\}$.
(2) $f \in A$ を $f \notin \sqrt{(0)}$ にとると, $S = \{f^n | n \geq 0\}$ は A 内で *multi closed* である.
(3) $\{P_i \in \mathrm{Spec}\, R\}_{i \in I}$ *where* $I \neq \emptyset$; *a set* とし, $S = A \backslash \bigcup_{i \in I} P_i$ とする. とくに $P \in \mathrm{Spec}\, R$ をとり, $S = A \backslash P$ とする.

これら (1), (2), (3) は非常に大切な multi closed in A の例である. さて, A 内に a multi closed S が与えられているとせよ. $X = S \times A$ とおき, $(s, a), (t, b) \in X$ に対して

$$(s, a) \sim (t, b) \overset{\mathrm{def}}{\Leftrightarrow} u(ta - sb) = 0 \quad for\ some\ u \in S,$$

と定める. この $\sim$ は, 集合 $X = S \times A$ 上の同値関係である.

Proof. (1) $^{\forall}(s,a) \in X$, $1(sa - sa) = 0$. $\therefore (s,a) \sim (s,a)$.
(2) $(s,a) \sim (t,b)$ ならば $^{\exists}u \in S$, $u(ta - sb) = 0$. $\therefore (-1)u(sb - ta) = 0$, $u(sb - ta) = 0$, $(t,b) \sim (s,a)$.
(3) $(s,a) \sim (t,b)$, $(t,b) \sim (u,c)$ なら $^{\exists}v, w \in S$; $v(ta - sb) = 0$, $w(ub - tc) = 0$. ここで $vw \in S$ から v, w を $v \in S$ として十分. すると, $vt(ua - sc) = vtua - vtsc = uvsb - vtsc = vs(ub - tc) = 0$.
$\therefore (s,a) \sim (u,c)$. □

そこで, 商集合 $X/\sim$ を $S^{-1}A$ とかき, $^{\forall}(s,a) \in X$ に対して $\overline{(s,a)}$ を $\dfrac{a}{s}$ と表すことにしたい.

Lemma 1.5.2. $(s,a), (t,b) \in X$ に対して,

(1) $\dfrac{a}{s} = \dfrac{b}{t} \Leftrightarrow {}^{\exists}u \in S$ s,t $u(sb - ta) = 0$.
(2) $^{\forall}t \in S$, $\dfrac{a}{s} = \dfrac{ta}{ts}$.
(3) $^{\forall}s, t \in S$, $\dfrac{0}{s} = \dfrac{0}{t}$, $\dfrac{s}{s} = \dfrac{t}{t}$.
(4) $^{\forall}s, t \in S$, $\dfrac{sa}{s} = \dfrac{ta}{t}$.

Proof. (1) は定義に従う. そして (2), (3), (4) は (1) に従う. □

Theorem 1.5.3. $S^{-1}A$ は次の演算によって環をなす.

$$\frac{a}{s} + \frac{b}{t} := \frac{ta + sb}{st}\ , \quad \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

$S^{-1}A$ を A の S による局所化という.

証明は *Exercise* にしよう.

Exercise 7. 上の定理を証明せよ.

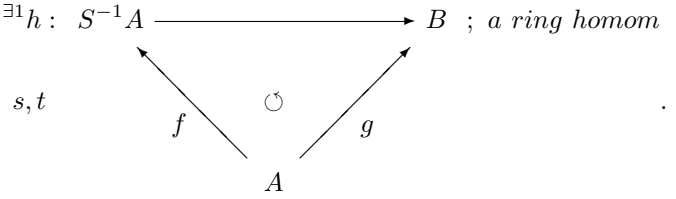
さてそこで, a map $f : A \to S^{-1}A$, $a \mapsto \dfrac{a}{1}$ と定めると,

$$f(a) + f(b) = \frac{a}{1} + \frac{b}{1} = \frac{a+b}{1} = f(a+b)$$
$$f(a)f(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} = f(ab)$$
$$f(1) = \frac{1}{1} = 1$$

を全てみたすので, A から $S^{-1}A$ への環の準同型写像である. そして, 次をみたす.

Lemma 1.5.4.
(1) $^{\forall}s \in S$, $f(s) \in \mathrm{U}(S^{-1}A)$.
(2) $^{\forall}\alpha \in S^{-1}A$, $\alpha = f(a)f(s)^{-1}$ *for some* $a \in A$, $s \in S$.
(3) $\mathrm{Ker}\, f = \{a \in A | sa = 0 \quad for\ some\ s \in S\}$.

Proposition 1.5.5. $g : A \to B$ を環の準同型写像で, $g(S) \subseteq \mathrm{U}(B)$ であるならば,



.

Proof. $^\forall\alpha \in S^{-1}A$ をとり $\alpha = \dfrac{a}{s} = \dfrac{a'}{s'}$ と表すと, $^\exists u \in S;\ u(sa' - s'a) = 0.$ $\therefore g(u)\Big(g(s)g(a') - g(s')g(a)\Big) = 0.$ つまり $g(u) \in \mathrm{U}(B)$ より $g(s)g(a') = g(s')g(a).$ $\therefore g(a)g(s') = g(a')g(s')$ in $B.$ よって $h(\alpha) = g(a)g(s)^{-1}$ と定めると, このとき, $\beta \in S^{-1}A$ をとり, $\beta = \dfrac{b}{t}$ とかくと,

$$
\begin{aligned}
&h(\alpha+\beta) = h\left(\frac{ta+sb}{st}\right) = g(ta+sb)g(st)^{-1} = g(a)g(s)^{-1} + g(b)g(t)^{-1} = h(\alpha) + h(\beta).\\
&h(\alpha\beta) = h\left(\frac{ab}{st}\right) = g(ab)g(st)^{-1} = g(a)g(s)^{-1}\cdot g(b)g(t)^{-1} = h(\alpha)h(\beta)\\
&h(1) = h\left(\frac{1}{1}\right) = g(1)g(1)^{-1} = 1
\end{aligned}
$$

をみて, h は環の準同型写像である. もちろん $a \in A$ について $h \cdot f(a) = h\left(\dfrac{a}{1}\right) = g(a)g(1)^{-1} = g(a)$ である. 以上が, 存在についての議論である.
一意性については, h' という $S^{-1}A$ から B への環の準同型写像で, $h' \cdot f = g$ をみたすとすれば, $^\forall\alpha \in S^{-1}A$ について $\alpha = \dfrac{a}{s}$ と表すと $\alpha = f(a)f(s)^{-1}$ であった.

$$
\therefore \quad h'(\alpha) = h'(f(a)f(s)^{-1}) = h'(f(a))h'(f(s))^{-1} = g(a)g(s)^{-1} = h(\alpha).
$$

よって, $h = h'$ をうる. □

ここで, $S = \{s \in A | s$ は $A - nzd\}$ とおくと, a ring homom $f : A \to S^{-1}A,\ a \mapsto \dfrac{a}{1}$ は単射である. よって埋め込みの原理により $^{\exists 1}(B, g)$ where $B = a\ ring,\ g : S^{-1}A \to B$; a ring homom で且つ bijection s,t (1) $A \subseteq B$, (2) $g \cdot f = i$; the inclusion. この B をよく見ると, まず A は (1),(2) の性質により次の事が分かる.

(a) A は B の部分環であって,
(b) $^\forall s \in S$ に対して $s \in \mathrm{U}(B)$,
(c) $^\forall b \in B$ をとると $b = as^{-1}$ for some $a \in A,\ s \in S.$

Proof. $s = i(s) = g(f(s))$ によって $f(s) \in \mathrm{U}(S^{-1}A)$ より $s = i(s) \in \mathrm{U}(B)$ をうる. $^\forall b \in B,\ b = g(\alpha)$ $^\exists\alpha \in S^{-1}A.$ $\therefore b = g\left(f(a)f(s)^{-1}\right) = as^{-1}.$ □

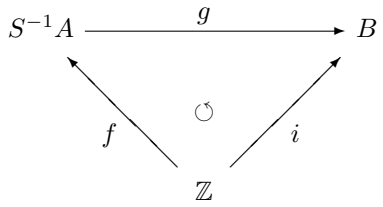
この B を A の全商環といって $\mathbb{Q}(A)$ と書くことにする.

Theorem 1.5.6. *A が an integral domain であれば, A は体の部分環である.*

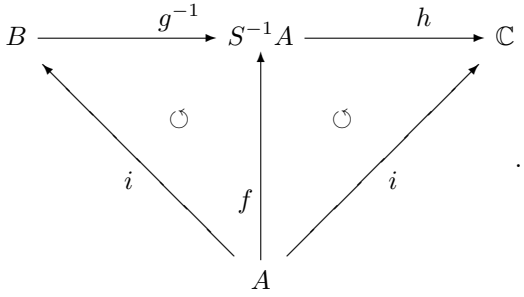
Proof. $\mathbb{Q}(A)$ が体であることを示せば十分. $0 \neq {}^\forall\alpha \in \mathbb{Q}(A)$ をとる. $\alpha = \dfrac{a}{s}$ $(a, s \in A;\ s \neq 0)$ とかくと, $\alpha \neq 0$ より $a \neq 0$ である. $\therefore {}^\exists\beta = \dfrac{s}{a} \in \mathbb{Q}(A),\ \alpha\beta = \dfrac{a}{s}\cdot\dfrac{s}{a} = 1.$ □

A が an integral domain のとき, $\mathbb{Q}(A)$ を商体という.

Example 1.5.7. $A=\mathbb{Z}$ とし $B=\mathbb{Q}(\mathbb{Z})$ をつくる. 私たちの作り方によると, $S=\mathbb{Z}\backslash\{0\}$ で



であった. $S\subseteq \mathrm{U}(\mathbb{C})=\mathbb{C}\backslash\{0\}$ より ${}^{\exists 1}h: S^{-1}A\to\mathbb{C}$; *a ring homom s,t* $i=h\cdot f$. この h は $h\left(\frac{a}{s}\right)=as^{-1}$ で定義されていたので, $h\left(\frac{a}{s}\right)=0$ であれば $as^{-1}=0$ となるが, $s\neq 0$ より $a=0$. $\therefore \frac{a}{s}=0$, h は *injection.*



今, 上の可換図において $\varphi=h\cdot g^{-1}$ とおくと, φ は *a ring homom, injection* である. つまり, ${}^{\forall}a\in\mathbb{Z}$, $\varphi(a)=a$. とくに $\mathrm{Im}\,\varphi=\mathbb{Q}$. これは ${}^{\forall}b\in B$, $b=as^{-1}$ $(a,s\in A=\mathbb{Z};\ s\neq 0)$ とかくとき, $\varphi(b)=\varphi(as^{-1})=\varphi(a)\varphi(s)^{-1}=as^{-1}\in\mathbb{Q}$ *in* $\mathbb{C}$. ${}^{\forall}x\in\mathbb{Q}$, $x=\frac{a}{s}$ とかくと $x=as^{-1}$ である. $\therefore x=\varphi(as^{-1})$.
$\therefore \mathbb{Q}=\mathrm{Im}\,\varphi$.

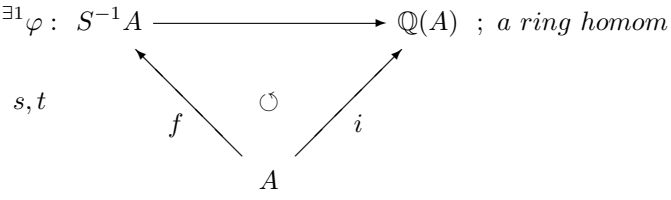
実のところは, $\mathbb{Q}$ は上のようにして $\mathbb{Q}(\mathbb{Z})$ (i,e $\mathbb{Z}$ の商体) として構成され, $\mathbb{R}$, $\mathbb{C}$ は $\mathbb{Q}$ をもとに構成されたものである.

Exercise 8.
(1) *Proposition 5.5* において, *a ring homom* h が単射あるいは全射になるための必要十分条件を求めよ.
(2) $\mathbb{Q}(A)$ は, $(a),(b)$ の性質のみで同型の範囲で唯一通りであることを証明せよ.

proof of (2). $\mathbb{Q}(A)$ は環であって

(i) $A\subseteq\mathbb{Q}(A)$,
(ii) the inclusion map $i: A\to\mathbb{Q}(A)$ は a ring homom,
(iii) ${}^{\forall}s\in S=\{u\in A|u$ は $A-nzd\}$, $s\in \mathrm{U}(\mathbb{Q}(A))$,
(iv) ${}^{\forall}\alpha\in\mathbb{Q}(A)$, $\alpha=as^{-1}$ for some $a\in A$, $s\in S$,

をみたす. このとき, (i),(ii),(iii) により



をうる. この φ は $a \in A$, $s \in S$ について $\varphi\left(\frac{a}{s}\right) = as^{-1}$ となるから, (iv) より φ が全射であることが求まる. 又, $\varphi\left(\frac{a}{s}\right) = 0$ in $\mathbb{Q}(A)$ とすると, $as^{-1} = 0$; $s \in \mathrm{U}(\mathbb{Q}(A))$ より $a = 0$. $\therefore \frac{a}{s} = 0$ in $S^{-1}A$, φ は単射. 従って, φ は同型写像であるから, $\mathbb{Q}(A)$ は (i) —(iv) の性質で定まることがわかる. □

1.6　多項式環

A は a ring とする. A に対して $C = \left\{(a_0, a_1, a_2, \cdots) | a_i \in A \ \ for\ all\ {}^{\forall} i \geq 0\right\}$ とおき ${}^{\forall} f \in C$ について f_n によって f の第 n 成分を表す. (勿論, $n \geq 0$ である.) C は次の演算により a ring となる.

$$f + g := (\cdots, f_n + g_n, \cdots)$$

$$f \cdot g := \left(\cdots, \sum_{i+j=n} f_i g_j, \cdots\right)$$

証明は *Exercise* としよう.

Exercise 9. *C が a ring であることを証明せよ.*

次に $Y = (0, 1, 0, 0, \cdots) \in C$ とおく. もちろん $Y_n = \delta_{n,1}$ $({}^{\forall} n \geq 0)$ である. このとき, $Y^2 = (0, 0 \cdot 1 + 1 \cdot 0, 1 \cdot 1, 0, 0, \cdots) = (0, 0, 1, 0, 0, \cdots)$ である. これは一般に, $n = 0$ のときは $Y^0 = 1 = (1, 0, 0, \cdots)$ であると定めると, ${}^{\forall} n \geq 0$ に対して $Y^n = (0, \cdots, \overset{(n)}{1}, 0, \cdots)$ であることが n についての induction から従う. そこで, $B = \left\{f \in C | {}^{\exists} N \geq 0\ s,t\ f_n = 0 \ \ for\ all\ {}^{\forall} n \geq N\right\}$ とおく.

Lemma 1.6.1. *B は C の部分環である.*

A map $\varphi : A \to B$ を $\varphi(a) = (a, 0, 0, \cdots)$ と定めるとこの φ は環の準同型写像であって単射である. よって埋め込みの原理により ${}^{\exists}(D, \rho)$ where D は環, $\rho : B \to D$ は環の準同型写像で bijection であって次の条件 (1),(2) を満たす.

(1) $A \subseteq D$.
(2) $\rho \cdot \varphi$ は A から D への the inclusion map.

そこで, このような a pair (D, ρ) を一組とり $X = \rho(Y)$ とおくと, $X \in D$ であって

Theorem 1.6.2. $\left\{X^i\right\}_{i \geq 0}$ は D の *an A-free basis* をなす.

Proof. ${}^{\forall} f \in D$ をとると $f = \rho(g)$ for some $g \in B$. 今, $g = (g_0, g_1, g_2, \cdots)$ であって ${}^{\exists} N \geq 0$ s,t $g_i = 0$ for ${}^{\forall} i \geq N$. $n \geq 0$ を $g = (g_0, g_1, \cdots, g_n, 0, 0, \cdots)$ にとると

$$g = \sum_{i=0}^{n} \varphi(g_i) Y^i$$

であるから,

$$\therefore \quad f = \sum_{i=0}^{n} \rho(\varphi(g_i)) X^i = \sum_{i=0}^{n} g_i X^i.$$

$\therefore {}^{\exists}(n \geq 0;\ a_0, a_1, \cdots, a_n \in A)$ s,t $f = a_0 + a_1X + \cdots + a_nX^n$. 逆に, $n \geq 0$ と $a_0, a_1, \cdots, a_n \in A$ を与えるとき $g = (a_0, a_1, \cdots, a_n, 0, 0, \cdots) \in B$ である. そして, $g = \sum_{i=0}^{n} \varphi(a_i)Y^i$ であって, $\rho(g) = \sum_{i=0}^{n} a_iX^i$ であるので,

$$\sum_{i=0}^{n} a_iX^i = 0 \Leftrightarrow g = 0 \Leftrightarrow a_i = 0,\ 0 \leq {}^{\forall}i \leq n,$$

をうる. よって, 今, $0 \neq f \in D$ に対して $f = a_0 + a_1X + \cdots + a_nX^n$ となる $n \geq 0$ と $a_i \in A$ を $a_n \neq 0$ にとれるが, この表現は f に対して唯一通りである. 実際, $f = \sum_{i=0}^{m} b_iX^i$ ($m \geq 0$; $b_i \in A$ であって $b_m \neq 0$) としたとき, $m \leq n$ としてよくて,

$$f = \sum_{i=0}^{n} a_iX^i = \sum_{i=0}^{m} b_iX^i \Rightarrow \sum_{i=0}^{m} (a_i - b_i)X^i + \sum_{i=m+1}^{n} a_iX^i = 0$$

をみればほとんど明らかであろう. これからは, この n を $\deg f$ とかき, もし必要であれば $f = 0$ については $\deg f = -\infty$ と定める. □

Definition 17. 上の D を $A[X]$ と書き, A 上 1 変数多項式環という.

Theorem 1.6.3 (代入原理). *E を a ring, $\xi : A \to E$ を環の準同型写像とする. このとき ${}^{\forall}\alpha \in E$ について ${}^{\exists 1}\sigma : A[X] \to E$ a ring homom s,t $\sigma(X) = \alpha$ であって ${}^{\forall}a \in A$ については $\sigma(a) = \xi(a)$. (各 $f \in A[X]$ に対して, $\sigma(f)$ を $f(\alpha)$ とかくことにする.)*

Proof.
(uniqueness) σ, σ' が上の性質を持つなら ${}^{\forall}f \in A[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$ ($n \geq 0$; $a_i \in A$) と表したとき

$$\sigma'(f) = \sum_{i=0}^{n} \sigma'(a_i)\sigma'(X)^i = \sum_{i=0}^{n} \xi(a_i)\alpha^i = \sigma(f).$$

$\therefore \sigma = \sigma'$.
(existance) $f \in A[X]$ をとり $f = \sum_{i=0}^{n} a_iX^i$ ($n \geq 0$; $a_i \in A$) とかく. 私たちは,

$$\sigma(f) = \sum_{i=0}^{n} \xi(a_i)\alpha^i$$

と定めたい. σ が well-defined であることは, $f = b_0 + b_1X + \cdots + b_mX^m$ ($m \geq 0$; $b_j \in A$) と表したとき, $m \geq n$ とすると,

$$\sum_{i=0}^{n} (b_i - a_i)X^i + \sum_{i=n+1}^{m} b_iX^i = 0$$

より $b_i - a_i = 0$ ($0 \leq {}^{\forall}i \leq n$), $b_j = 0$ ($n + 1 \leq {}^{\forall}j \leq m$). $\therefore \sum_{i=0}^{n} \xi(b_i - a_i)\alpha^i + \sum_{i=n+1}^{m} b_i\alpha^i = 0$. つまり σ は well-defined である. 後は, σ が環の準同型写像であることをいえばよい. $1 \in A[X]$ は $1 \in A$ であるから

$\sigma(1)=\xi(1)=1$ は明らか. ${}^{\forall}f,g\in A[X]$ をとり $f=a_0+a_1X+\cdots+a_nX^n$, $g=b_0+b_1X+\cdots+b_nX^n$ となる $n\geq 0$; $a_i,b_j\in A$ をとる. すると

$$\sigma(f+g)=\sigma\left(\sum_{i=0}^{n}(a_i+b_i)X^i\right)=\sum_{i=0}^{n}\xi(a_i+b_i)\alpha^i=\sigma(f)+\sigma(g)$$
$$\sigma(fg)=\sigma\left(\sum_{i,j}(a_ib_j)X^{i+j}\right)=\sum_{i,j}\xi(a_ib_j)\alpha^{i+j}\ \sigma(f)\sigma(g)$$

をみて σ が環の準同型写像であることをうる. □

Corollary 1.6.4. *F を a ring とし, $A\subseteq F$; a subring of A であり ${}^{\exists}Z\in F$ s,t (1) ${}^{\forall}f\in F$ は $f=a_0+a_1Z+\cdots+a_nZ^n$ for some $n\geq 0$; $a_i\in A$ と表せる, (2) $n\geq 0$ で $a_i\in A$ について, $\sum_{i=0}^{n}a_iZ^i=0$ ならば $a_i=0$ for ${}^{\forall}i$ をみたす,* とする. このとき ${}^{\exists}\sigma:A[X]\to F$ *a ring homom s,t σ は bijection* であって $\sigma(X)=Z$, $\sigma(a)=a$ ${}^{\forall}a\in A$.

つまり多項式環は, 同型の範囲で唯一つである.

Lemma 1.6.5. *A が an integral domain ならば, $A[X]$ も an integral dimain* である.

Proof. $f,g\in A[X]$ を $f\neq 0$, $g\neq 0$ にとる. すると $f=a_0+a_1X+\cdots+a_nX^n$ ($n\geq 0$; $a_i\in A$, $a_n\neq 0$), $g=b_0+b_1X+\cdots+b_mX^m$ ($m\geq 0$; $b_j\in A$, $b_m\neq 0$) と表せられる. よって, $fg=(a_nb_m)X^{n+m}+$ (*lower terms*) $\neq 0$ となり, $\deg(fg)=n+m$ である. □

Example 1.6.6. *k を体として $k[X]$ をつくると, $k[X]$ は整域であるから $\mathbb{Q}(k[X])$ をつくれる. これを $k(X)$ と表すことにしよう. つまり $k=\mathbb{R}$ のときをみるに ${}^{\forall}\xi\in\mathbb{R}(X)$, $\xi=\dfrac{f}{g}$ for some $f,g\in\mathbb{R}[X]$, $g\neq 0$,* となる. つまり, これまで私たちが自由に扱ってきた $\dfrac{1}{X-1}$, $\dfrac{X+1}{X^2}$ などは全て, この意味で考えていたのである.

Remark 1.6.7. *$p\geq 2$ を素数とし, $k=\mathbb{Z}/(p)$ とする. k は $|k|=p$ となるような体である. よって $k[X]$ 内で $f=\prod_{\alpha\in k}(X-\alpha)$ をとると $f\neq 0$, しかし ${}^{\forall}\alpha\in k$ に対して $f(\alpha)=0$* である. これより, 多項式は函数そのものではないことがわかる.

1.7　UFD について

この節では, A は整域とする. $a,b\in A$ について $a|b$ とは $b\in(a)$ なること, すなわち $b=ax$ ${}^{\exists}x\in A$ であることをいう. 従って, $(a)=(b)\Leftrightarrow a=\varepsilon b$ ${}^{\exists}\varepsilon\in\mathrm{U}(A)$ である.

Definition 18. *$a\in A$ について, $a\neq 0$ であって $(a)\in\operatorname{Spec}A$ であるとき, a は素元であるという.*

Definition 19. *$a\in A$ について, $a\neq 0$ かつ $a\notin\mathrm{U}(A)$ であってさらに $a=bc$ であるならば $b\in\mathrm{U}(A)$ or $c\in\mathrm{U}(A)$ であるとき, a は an irreducible element* という.

Lemma 1.7.1. 全ての素元は *irreducible* である.

Proof. $a \in A$ を素元とする. $a \neq 0$, $a \notin \mathrm{U}(A)$ は自明. $a = bc$ とすると $bc \in (a)$ であるから $b \in (a)$ or $c \in (a)$. $b \in (a)$ としてよい. $\therefore b = da$ for some $d \in A$, $a = (da)c = a(dc)$. A は整域であるから $dc = 1$ となり $c \in \mathrm{U}(A)$ をうる. □

Lemma 1.7.2. $p_1, \cdots, p_n, q_1, \cdots, q_m \in A$ $(m, n \geq 1)$ は全て素元とする. このとき $p_1 \cdots p_n = q_1 \cdots q_m$ ならば, $n = m$ であって且つ, 適当に並び替えをして $^{\forall}i$; $(p_i) = (q_i)$ をみたす.

Proof. $n = 1$ ならば $p_1 = q_1 \cdots q_m$. p_1 は irreducible であるから $n = 1$, $p_1 = q_1$. $m > 1$ で $m - 1$ 以下で正しいとする. もちろん, $n > 1$ で $q_1 \cdots q_n \in (p_1)$ より $q_1 \in (p_1)$ としてよい. このとき, $q_1 = \varepsilon_1 p_1$ と表すと $p_1 \notin \mathrm{U}(A)$ であるから $\varepsilon_1 \in \mathrm{U}(A)$. $\therefore (p_1) = (q_1)$, $p_2 \cdots p_n = \varepsilon_1 q_2 \cdots q_m$. ここで n についての induction を用いればよい. □

Definition 20. A が体であるか, もしくは A は体ではないが $a \in A$ が $a \neq 0$, $a \notin \mathrm{U}(A)$ について $a = p_1 \cdots p_n$ $(n \geq 1;\ p_i \in A$ は素元$)$ と表せるとき, A は *UFD* (*Unique Factorisation Domain*) という.

Lemma 1.7.3. A が *UFD* であれば $a \in A$ について, a が素元であることの必要十分条件は, a は *irreducible,* である.

Proof. A は体ではないとしてよい. $\Leftarrow$ のみ. $a \neq 0$, $a \notin \mathrm{U}(A)$ より $a = p_1 \cdots p_n$ $(n \geq 0;\ p_i$ は A の素元$)$ とかくと, a は irreducible であるから $n = 1$ であることは自明であろう. □

Lemma 1.7.4. *PID* は *UFD* である.

Proof. A を体でない PID とせよ. もし A が UFD でないならば $^{\exists}a \in A$ s,t $a \neq 0$, $a \notin \mathrm{U}(A)$ であって且つ a は有限個の素元の積では表せない. よって,

$$\mathcal{S} := \{(a) | a \neq 0,\ a \notin \mathrm{U}(A) \text{であって且つ} a \text{は有限個の素元の積では表せない}\}$$

とおくと $\emptyset \neq \mathcal{S}$ である. $I_1, I_2 \in \mathcal{S}$ に対して $I_1 \leq I_2$ を $I_1 \subseteq I_2$ で定めると $(\mathcal{S}, \leq)$ は inductive set になるから $^{\exists}I \in \mathcal{S}$; max element. $I = (a)$ とかく. $\mathcal{S}$ の取り方から $^{\exists}b, c \in A$ s,t $b, c \neq 0$, $b, c \notin \mathrm{U}(A)$ であって $a = bc$. このとき $(a) \subsetneq (b)$, $(a) \subsetneq (c)$ であるから $(b), (c) \notin \mathcal{S}$. $\therefore b = p_1 \cdots p_n$, $c = q_1 \cdots q_m$ $(m, n \geq 1;$ $p_i, q_j \in A$ は素元$)$ と表せるので $a = p_1 \cdots p_n q_1 \cdots q_m$ となり矛盾である. □

Definition 21. A が *Euclidean* であるとは, 次の条件 (1), (2) をみたす写像 $\varphi : A\backslash\{0\} =: A^* \to \mathbb{Z}$ が存在することである.

(1) $\varphi(a) \geq 0$ *for* $^{\forall}a \in A^*$,
(2) $a, b \in A$ で $a \neq 0$ について $^{\exists}q, r \in A$ *where* $b = qa + r$ であって, もし $r \neq 0$ ならば $\varphi(r) < \varphi(a)$.

Example 1.7.5.
(1) $\mathbb{Z}$ は, *a map* $\varphi : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}$, $a \mapsto |a|$ によって *Euclidean* である.
(2) k を体とし, $A = k[X]$ とする. A は, $\varphi : A\backslash\{0\} \to \mathbb{Z}$, $f \mapsto \deg f$ によって *Euclidean* である.

Proposition 1.7.6. *Euclidean* は *PID* である.

Proof. $I \subseteq A$; ideal をとる. $I = (a)$ for some $a \in A$ を示したい. $I \neq (0)$ としてよい. $0 \neq f \in I$ を $\varphi(f)$ が最小になるようにとる. A は Euclidean であるから, $^\forall g \in I$ に対して $^\exists q, r \in A$ where $g = qf + r$. もし $r \neq 0$ ならば, $r = g - qf \in I$ となるが $\varphi(r) < \varphi(f)$ であるが, これは $\varphi(f)$ の最小性に反する.
$\therefore g = qf \in (f)$, $I = (f)$. □

Corollary 1.7.7. *k を体, $A = k[X]$ とするとき,*

(1) *$f \in A$ について, $f \in \mathrm{U}(A) \Leftrightarrow f \in k\backslash\{0\}$.*
(2) *$f \in A$, $f \notin \mathrm{U}(A)$ なら, $f = f_1 \cdots f_n$ $(n \geq 1;$ f_iは irreducible in $A)$.*

Example 1.7.8. $\mathbb{Z}[i] = \{a + b\,i | a, b \in \mathbb{Z}\}$ は $\mathbb{C}$ の部分環であって *Euclidean* である.

Proof. $^\forall \alpha \in \mathbb{C}$, $|\alpha| := \sqrt{a^2 + b^2}$ where $\alpha = a + b\,i$, $a, b \in \mathbb{R}$ とおく. $A = \mathbb{Z}[i]$ とすると, $\varphi : A\backslash\{0\} \to \mathbb{Z}$ を $\varphi(\alpha) := |\alpha|^2$ で定めたい. まず, $0 \neq {}^\forall\alpha \in A$, $\alpha = a + b\,i$ に対して $\left|\sqrt{a^2 + b^2}\right|^2 = a^2 + b^2$, $0 \leq a^2 + b^2 \in \mathbb{Z}$ は明らか. $^\forall \alpha, \beta \in A$, $\alpha \neq 0$ をとる. $\dfrac{\beta}{\alpha} \in \mathbb{C}$ に対して, 複素数体の一般論 ($\mathbb{C}$ 内で $\mathbb{Z}[i]$ のなす lattice をみよ.) によって $^\exists(\gamma, \lambda)$ where $\gamma \in \mathbb{Z}[i]$, $\lambda \in \mathbb{C}$, $\dfrac{\beta}{\alpha} - \gamma = \lambda$ であって, さらに $|\lambda| < 1$. $\therefore \beta = \gamma\alpha + \lambda\alpha$. $\delta = \lambda\alpha$ とおくと $\delta \in A$ は自明. そして $|\delta| \leq |\lambda| \cdot |\alpha| \leq |\alpha|$ もほとんど明らか. □

次にしばらくの間, A は a UFD で体ではないとしよう. $K = \mathbb{Q}(A) \supseteq A$ を A の商体とする.

Lemma 1.7.9. *$a_1, \cdots, a_n \in A$ $(n > 0)$ とすれば $^\exists d \in A$ s,t*

(1) *$d | a_i$ for $^\forall i$,*
(2) *$e \in A$ で $e | a_i$ $(^\forall i)$ なら $e | d$.*

このような d は単元の違いを除いて唯一つに定まる.

Proof. (existance) まず $a_i = 0$ $(^\forall i)$ のときは $d = 0$ とすればよい. 次に $a_i \neq 0$ $(^\exists i)$ とする. もし $a_i \in \mathrm{U}(A)$ $^\exists i$ ならば $d = 1$ ととるとよいので, $a_i \neq 0$ $^\exists i$ であって, さらに $a_i \neq 0$ については $a_i \notin \mathrm{U}(A)$ としてよい. そこで, $I = \{i | 1 \leq i \leq n;\ 0 \neq a_i \notin \mathrm{U}(A)\}$ とおく. もし, $^\forall i \in I$ について $p | a_i$ となる $p \in A$; prime element が存在しないならば $d = 1$ とすればよい. 従って $^\exists p \in A$; a prime element s,t $^\forall i \in I$ に対して $p | a_i$ としてよい. このときは $a_i = a_i' p$ となる $\{a_i'\}_{i \in I}$ について上と同じ操作を繰り返せばよい. そしてこの操作は有限回でとまる. 一意性は, $d | d'$, $d' | d$ による. □

$0 \neq f \in A[X]$ が primitive であるとは, $f = a_0 + a_1 X + \cdots + a_n X^n$ と表したとき $(a_0, a_1, \cdots, a_n) = A$ in A であること, (i,e a_i の A 内の最大公約数が 1 である.) ことをいう.

Lemma 1.7.10. *$p \in A$ が素元ならば, $p \in A[X]$ も素元である.*

Proof. $P = (p)$ in A とおき, $\varphi : A[X] \to (A/P)[X]$ を $\varphi(a_0 + a_1 X + \cdots + a_n X^n) = \overline{a_0} + \overline{a_1} X + \cdots + \overline{a_n} X^n$ とおく. このとき, $\operatorname{Ker}\varphi = \{f \in A[X] | f$ の係数は全て P の元である $\} = pA[X]$ であって, $(A/P)[X] \cong A[X]/\operatorname{Ker}\varphi$, $(A/P)[X]$ は整域であること全てを合せると, $pA[X] \in \operatorname{Spec} A[X]$ をうる. □

Proposition 1.7.11.
(1) *$f, g \in A[X]$ は primitive である $\Rightarrow$ $fg \in A[X]$ は primitive である.*

(2) $f \in A[X]$ は *primitive* とせよ. $g \in A[X]$ について, $f|g$ *in* $K[X] \Rightarrow f|g$ *in* $A[X]$.

Proof. (1) $fg \neq$ *primitive* とすると $^{\exists}p \in A$; prime element of A s,t p は fg の係数の全てを A 内で割る. つまり, $fg \in pA[X]$, $pA[X] \in \operatorname{Spec} A[X]$ であるから $f \in pA[X]$ or $g \in pA[X]$. (矛盾)
(2) $g \neq 0$ として十分. $g = \varphi f$ in $K[X]$ for some $0 \neq \varphi \in K[X]$ であるから φ の係数の共通分母 $d \in A$ をとり, $d\varphi = ch$ ($c \in A$, $h \in A[X]$; primitive) と表すと, $dg = d(\varphi f) = (ch)f$. (1) により fh は primitive であるから $g = \alpha\xi$ ($\alpha \in A$, $\xi \in A[X]$; primitive) と表すと $c(fh) = dg = d\alpha\xi$ より $d\alpha = c\varepsilon$ $^{\exists}\varepsilon \in \mathrm{U}(A)$.
$\therefore dg = d\alpha\varepsilon^{-1}(fh)$ より $g = \alpha\varepsilon^{-1}(fh)$, $f|g$ in $A[X]$. □

さて次を示そう.

Theorem 1.7.12. *A が a UFD ならば $A[X]$ も a UFD である.*

Proof. A は体でないとして十分. $f \in A[X]$ をとり $f \neq 0$, $f \notin \mathrm{U}(A[X])$ として $\deg f = n$ とする. $n = 0$ ならば $f \in A$ であるから A 内での積をとればよい. $n > 0$ とせよ. $f = \varphi_1 \cdots \varphi_\ell$ を $K[X]$ 内での素元分解とする. $0 \neq d_i \in A$ を φ_i の共通分母にとり $d_i\varphi_i \in A[X]$ として, 更に $d_i\varphi_i = c_i g_i$ ($c_i \in A$, $g_i \in A[X]$; primitive) と表すと, $d = d_1 \cdots d_\ell$ について $df = (c_1 \cdots c_\ell)(g_1 \cdots g_\ell)$ より $d = \varepsilon(c_1 \cdots c_\ell)$ $^{\exists}\varepsilon \in \mathrm{U}(A)$.
$\therefore f = \tau g_1 \cdots g_\ell$ $^{\exists}\tau \in \mathrm{U}(A)$. $^{\forall}g_i$ は $A[X]$ 内の素元である. これは, $\alpha, \beta \in A[X]$; $\alpha\beta \in (g_i)$ in $A[X]$ とすると, $c_i \in \mathrm{U}(K[X])$ より $\alpha\beta \in (d_i\varphi_i)$ in $K[X]$ である. $\varphi_i \in K[X]$ は素元, $d_i \in \mathrm{U}(K[X])$ であるから $(d_i\varphi_i) \in \operatorname{Spec} K[X]$. $\therefore \alpha \in (d_i\varphi_i) \subseteq (g_i)$ or $\beta \in (d_i\varphi_i) \subseteq (g_i)$ in $K[X]$. $g_i =$ *primitive* in $A[X]$ より $\alpha \in (g_i)$ or $\beta \in (g_i)$ in $A[X]$ となり, $(g_i) \in \operatorname{Spec} A[X]$ をうる. □

さて A を a ring として, $0 < n \in \mathbb{Z}$ とする. A 上 $X_1, \cdots, X_n$ を変数とする多項式環を

$$A[X_1, \cdots, X_{n-1}, X_n] := \Big(A[X_1, \cdots, X_{n-1}]\Big)[X_n] \quad (\ n \geq 2\ )$$

によって定める. $I = \{(\alpha_1, \cdots, \alpha_n) | 0 \leq \alpha_i \in \mathbb{Z}\}$ とし, $^{\forall}\alpha \in I$ に対して $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in B = A[X_1, \cdots, X_n]$ と定める. $\{a_\alpha\}_{\alpha \in I}$ を A の元の族とする. $a_\alpha = 0$ for almost all $\alpha \in I$ とは, $\emptyset \neq {}^{\exists}\Lambda \subseteq I$; a finite subset s,t $\alpha \in I$ についてもし $\alpha \notin \Lambda$ ならば $a_\alpha = 0$, であることをいう. このとき $\displaystyle\sum_{\alpha \in \Lambda} a_\alpha X^\alpha \in B$ は, Λ の取り方によらない. これを, $\displaystyle\sum_{\alpha \in I} a_\alpha X^\alpha$ とかく.

Lemma 1.7.13. $^{\forall}f \in B$, $^{\exists 1}\{a_\alpha\}_{\alpha \in I}$ *where* $a_\alpha \in A$, $a_\alpha = 0$ *for almost all* $\alpha \in I$ *s,t* $f = \displaystyle\sum_{\alpha \in I} a_\alpha X^\alpha$.

Proof. n についての induction で証明する. $n = 1$ は証明済み. $n > 1$ として $n - 1$ 以下で正しいとする. $C = A[X_1, \cdots, X_{n-1}] \subseteq B = C[X_n]$ とするとき, $^{\forall}f \in B$, $f = c0 + c_1X_n + \cdots + c_\ell X_n^\ell$ ($\ell \geq 0$; $c_i \in C$) とかくと $0 \leq {}^{\forall}i \leq \ell$, $c_i = \displaystyle\sum_{\beta \in J} a_\beta^i X_\beta$ where $J = \{\beta = (\beta_1, \cdots, \beta_{n-1}) | 0 \leq \beta_j \in \mathbb{Z}\}$ であり $a_\beta^i \in A$, $a_\beta^i = 0$ for almost all $\beta \in J$.

$$\therefore \quad f = \sum_{i=0}^{\ell} c_i X_n^i = \sum_{i=0}^{\ell} \left(\sum_{\beta \in J} a_\beta^i X^\beta \right) X_n^i = \sum_{0 \leq i \leq \ell} \left(\sum_{\beta \in J} a_\beta^i X_1^{\beta_1} \cdots X_{n-1}^{\beta_{n-1}} \right) X_n^i.$$

さて, $f = \displaystyle\sum_{\alpha \in I} a_\alpha X^\alpha = \sum_{\alpha \in I} b_\alpha X^\alpha$ なら $\displaystyle\sum_{\alpha \in I} (a_\alpha - b_\alpha) X^\alpha = 0$ より $f = 0$ としてよい. $\emptyset \neq \Lambda \subseteq I$; a finite subset を $a_\alpha = 0$ if $\alpha \in I \backslash \Lambda$ にとる. すると, $\displaystyle\sum_{\alpha \in \Lambda} a_\alpha X^\alpha = 0$ を X_n について整理して induction による. □

Theorem 1.7.14. $n \geq 1$ とする. $\varphi : A \to B$ を *a ring homomorphism,* $Z_1, \cdots, Z_n \in B$ とするとき, ${}^{\exists 1}\sigma : A[X_1, \cdots, X_n] \to B$ *a ring homom s,t* $\sigma(a) = \varphi(a)$ *for* ${}^{\forall}a \in A$, $\sigma(X_i) = Z_i$ $({}^{\forall}i)$.

Proof. $f \in A[X_1, \cdots, X_n]$ について $f = \sum_{\alpha \in I} a_\alpha X^\alpha$ と表したとき $\sigma(f) = \sum_{\alpha \in I} \varphi(a_\alpha) Z^\alpha$ と定めよ. □

Corollary 1.7.15. $A[X_1, \cdots, X_n]$ は同型の範囲で唯一つに定まる.

Theorem 1.7.16. *A が a UFD ならば* $A[X_1, \cdots, X_n]$ *も a UFD である.*

Proof. n についての induction に従う. □

1.8 Ideals の operations

A を a ring とし, $\mathcal{F} := \{I | I$ は *an ideal of* $A\}$ とする. $(0), A \in \mathcal{F} \neq \emptyset$ である. この $\mathcal{F}$ 上に 4 つの演算を与えよう. ${}^{\forall}I, J \in \mathcal{F}$ に対して

$$
\begin{aligned}
&I + J := \{a + b | a \in I,\ b \in J\} \\
&I \cdot J := \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n > 0;\ a_i \in I,\ b_i \in J \right\} \\
&I \cap j := \{a \in A | a \in I,\ a \in J\} \\
&I \underset{A}{:} J := \left\{a \in A | ab \in I \ \ {}^{\forall}b \in J\right\}
\end{aligned}
$$

これらは全て A の ideal である.

Exercise 10. $I + J$, $I \cdot J$, $I \cap J$, $I \underset{A}{:} J$ が A の *ideal* であることを確かめよ.

ここで注目すべきは, $I \cup J \subseteq I + J$, $ab \in I \cdot J$ $({}^{\forall}a \in I, {}^{\forall}b \in J)$, しかも $I \cdot J \subseteq I \cap J$ であり, $I \subseteq I \underset{A}{:} J$ となっていることである. もし, $J \subseteq I$ なら $I + J = I$ である.

Lemma 1.8.1. $(\mathcal{F}, +)$ と $(\mathcal{F}, \times)$ はそれぞれ (0), A を単位元にもつような *commutative semigroup* である.

従って $I_1, \cdots, I_n \in \mathcal{F}$ $(n > 0)$ に対して, $\sum_{i=1}^{n} I_i$ と $\prod_{i=1}^{n} I_i$ が自然に定義される. ideal の冪について復習しておくと $I \in \mathcal{F}$, $n \geq 0$ のときは

$$
I^n = \begin{cases} A & n = 0 \\ I & n = 1 \\ I^{n-1} \cdot I & n \geq 2 \end{cases}
$$

である. この記号の下に

Lemma 1.8.2. $I^n \cdot I^m = I^{n+m}$, $(I^n)^m = I^{nm}$, $(I \cdot J)^n = I^n \cdot J^n$ *where* $I, J \in \mathcal{F}$, $n, m \geq 0$ が成立する.

Lemma 1.8.3. $(I + J)^n = \sum_{i+j=n} I^i \cdot J^j$ *where* $I, J \in \mathcal{F}$, $n \geq 0$.

この補題の証明には

Lemma 1.8.4. *$I\cdot(J+K)=I\cdot J+I\cdot K$, $(I+J)\cdot K=I\cdot K+J\cdot K$ where $I,J,K\in\mathcal{F}$.*

を用いる.

次に ideal の生成系について考えよう. $\emptyset\neq S\subseteq A$; a subset of A に対して,

$$(S):=\{a_1s_1+\cdots+a_ns_n|n>0;\ a_i\in A,\ s_i\in S\}$$

と定め, (もし $S=\emptyset$ ならば $(S)=(0)$ と定義する.) これを S で生成された A の ideal という. すると,

Lemma 1.8.5.
(1) (S) は A の *ideal* で, $S\subseteq(S)$.
(2) $I\in\mathcal{F}$ について, $S\subseteq I\Leftrightarrow(S)\subseteq I$.
(3) $(S)=\bigcap_{\substack{I\in\mathcal{F}\\ S\subseteq I}} I$.

$I\in\mathcal{F}$ について $I=(S)$ となる $S\subseteq A$; a subset を I の生成系という. もちろん, I は I の生成系である. $a_1,a_2,\cdots,a_n\in A$ $(n>0)$ について $S=\{a_1,a_2,\cdots,a_n\}$ とおき, (S) のことを

$$(a_1,a_2,\cdots,a_n)$$

とかく.

Lemma 1.8.6. $(a_1,a_2,\cdots,a_n)=\left\{\sum_{i=1}^{n}x_ia_i\ \middle|\ x_i\in A\right\}$.

Lemma 1.8.7. *$I\cdot J=(S)$ where $S=\{ab|a\in I,\ b\in J\}$.*

Example 1.8.8. *k を体とし, $A=k[X,Y,Z]$, $B=k[t]$ とおく. $\varphi:A\to B$ the k-algebra map s,t $\varphi(X)=t^3$, $\varphi(Y)=t^4$, $\varphi(Z)=t^5$ と定めるとき $I=\operatorname{Ker}\varphi$ は A の prime ideal である. そして I の生成系のうちなるべく単純なものを求めてみると*

$$I=(X^3-YZ,\ Y^2-XZ,\ Z^2-X^2Y)$$

となる.

Proof. $J=(X^3-YZ,\ Y^2-XZ,\ Z^2-X^2Y)$ とおく. $X^3-YZ,\ Y^2-XZ,\ Z^2-X^2Y\in\operatorname{Ker}\varphi=I$ は明らか. $\therefore I\supseteq J$. $^\forall n\in\mathbb{Z}$ について $\Lambda_n=\{(\alpha,\beta,\gamma)|0\leq\alpha,\beta,\gamma\in\mathbb{Z};\ 3\alpha+4\beta+5\gamma=n\}$ とおく. もし $\Lambda_n\neq\emptyset$ であるときは, $A_n:=\left\{\sum_{\lambda\in\Lambda_n}c_\lambda X^\alpha Y^\beta Z^\gamma\ \middle|\ c_\lambda\in k,\ (\alpha,\beta,\gamma)\in\Lambda_n\right\}$, $\Lambda_n=\emptyset$ であれば $A_n=(0)$ と定めると, $\{A_n\}_{n\in\mathbb{Z}}$ は A の additive subgroup の族であって, $A=\bigoplus_{n\in\mathbb{Z}}A_n$; $A_0=k$, $A_nA_m\subseteq A_{n+m}$ for $^\forall n,m\in\mathbb{Z}$, となる. $f\in A$ をとり $f=\sum_{0\leq n\in\mathbb{Z}}f_n$ where $f_n\in A_n$ と表すと $\varphi(f)=\sum_{0\leq n\in\mathbb{Z}}\varphi(f_n)$ であって, $0\leq n\in\mathbb{Z}$ について $\varphi(f_n)=c_nt^n$ $(c_n\in k)$ であるので, $\varphi(f_n)=c_nt^n=0$ $(^\forall n)\Leftrightarrow\varphi(f)=0$. つまり, $I=\sum_{n\geq0}(I\cap A_n)$

となる. 従って, $^{\forall}n \geq 0$, $I \cap A_n \subseteq J$ を示せばよい. そこで, $^{\exists}n \geq 0$; $I \cap A_n \not\subseteq J$ として, このような n を最小にとり $f \in I \cap A_n$, $f \notin J$ とする. 今,

$$f = \sum_{\lambda \in \Lambda_n} c_\lambda X^\alpha Y^\beta Z^\gamma$$

where $\Lambda_n = \{(\alpha, \beta, \gamma) | 0 \leq \alpha, \beta, \gamma \in \mathbb{Z},\ 3\alpha + 4\beta + 5\gamma = n\}$ であって $c_\lambda \in k$, $^{\forall}\lambda \in \Lambda_n$ とかく. すると,

$$0 = \varphi(f) = \left(\sum_{\lambda \in \Lambda_n} c_\lambda \right) t^n$$

より, $\sum_{\lambda \in \Lambda_n} c_\lambda = 0$ in k. $\therefore (\alpha', \beta', \gamma') = \mu \in \Lambda_n$ を一つとると

$$f = f - \left(\sum_{\lambda \in \Lambda_n} c_\lambda \right) X^{\alpha'} Y^{\beta'} Z^{\gamma'} = \sum_{\lambda \in \Lambda_n} c_\lambda \left(X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'} \right) \notin J$$

であるから $^{\exists}\lambda = (\alpha, \beta, \gamma) \in \Lambda_n$ s,t $X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'} \notin J$. よって, $g = X^\alpha Y^\beta Z^\gamma - X^{\alpha'} Y^{\beta'} Z^{\gamma'}$ とすると $g \in I \cap A_n$, $g \notin J$. つまり, 矛盾を導くにはこのような g が存在しないことを示せばよい.

もし $\gamma' \geq 2$ ならば $X^{\alpha'} Y^{\beta'} Z^{\gamma'} \underset{J}{\equiv} X^{\alpha'} Y^{\beta'} Z^{\gamma'-2}(X^2 Y)$. よって, 一般性を失うことなく $\gamma = \gamma' = 0$ か又は $\gamma = 1, \gamma' = 0$ のときを見ればよい. $\gamma = \gamma' = 0$ なら $g = X^\alpha - Y^\beta$ のはずで, もちろん $\alpha, \beta \geq 1$, $3\alpha = 4\beta$. よって $\alpha = 4\ell$, $\beta = 3\ell$ $(\ell \geq 1)$ と表すと, $g = (X^4)^\ell - (Y^3)^\ell \underset{J}{\equiv} (XYZ)^\ell - (XYZ)^\ell = 0$ となる. よって $\gamma = \gamma' = 0$ となる g は存在しない. 次に, $\gamma = 1, \gamma' = 0$ とする. つまり $g = X^\alpha Y^\beta Z - X^{\alpha'} Y^{\beta'}$ とする. $\alpha > 0$ のとき, $\alpha' = 0$, $\beta = 0$ となり, $g = X^\alpha Z - Y^{\beta'}$ $(3\alpha + 5 = 4\beta')$ である. 今, $X^\alpha Z = X^{\alpha-1} XZ \underset{J}{\equiv} Y^2 X^{\alpha-1}$ によると $g \underset{J}{\equiv} Y^2 X^{\alpha-1} - Y^{\beta'}$ となるが, $\beta' > 0$ ならば $Y(YX^{\alpha-1} - Y^{\beta'-1})$ であって $YX^{\alpha-1} - Y^{\beta'-1} \in I \backslash J$ となるが, これは g の次数の最小性に反する. $\therefore \beta' = 0$ となるが, これは $0 < 3\alpha + 5 = 4\beta' = 0$ を導くので矛盾である. よって $\alpha = 0$ である. すると $g = Y^\beta Z - X^{\alpha'} Y^{\beta'}$ となる. もし $\beta > 0$ ならば $Y^\beta Z \equiv X^3 Y^{\beta-1}$ であるから $\alpha' = 0$, $\beta' > 0$. これも g の最小性に反する. $\therefore \beta = 0$ であるが, このときは $5 = 3\alpha' + 4\beta'$ を $0 \leq \alpha', \beta' \in \mathbb{Z}$ が満たさなければならないので, 矛盾である. □

$\emptyset \neq \Lambda$; a set で $\{I_\lambda\}_{\lambda \in \Lambda}$ が A の ideals の族とするとき,

$$\sum_{\lambda \in \Lambda} I_\lambda = \left\{ \sum_{\lambda \in \Lambda} a_\lambda \ \middle|\ ^{\forall}\lambda \in \Lambda,\ a_\lambda \in I_\lambda \text{かつ } a_\lambda = 0 \ for\ almost\ all\ \lambda \in \Lambda \right\}$$

と定める. $\sum_{\lambda \in \Lambda} I_\lambda$ は $\bigcup_{\lambda \in \Lambda} I_\lambda$ で生成された A の ideal である. もちろん $\bigcap_{\lambda \in \Lambda} I_\lambda$ も A の ideal となっている.

Definition 22. $I \in \mathcal{F}$ に対して $\mathrm{V}(I) := \{P \in \operatorname{Spec} A | I \subseteq P\}$ とおく. $I \neq A$ なら $\mathrm{V}(I) \neq \emptyset$ である.

Definition 23. $I \in \mathcal{F}$ について $\sqrt{I} = \{a \in A | a^n \in I \ \ for\ some\ n > 0\}$ とおき I の *radical* という. 従って, $P \in \operatorname{Spec} A$ については $\sqrt{P} = P$ である.

Lemma 1.8.9. $\sqrt{I}$ は A の *ideal* である.

Proof. $I \subseteq \sqrt{I}$. $\therefore x, y \in \sqrt{I}$, $a \in A$ とすると $^{\exists}m, n > 0$ s,t $x^m, y^n \in I$. すると, $(ax)^m = a^m x^m \in I$, $(x+y)^{m+n-1} \in I$ である. □

Proposition 1.8.10. *$I \neq A$ を ideal とせよ. このとき $\sqrt{I} = \bigcap_{P \in \mathrm{V}(I)} P$ をみたす.*

Proof. $P \in \operatorname{Spec} A$ について, $I \subseteq P \Leftrightarrow \sqrt{I} \subseteq P$, であるから $(\subseteq)$ は自明であろう. $\sqrt{I} \subsetneq \bigcap_{P \in \mathrm{V}(I)} P$ とせよ. $\therefore {}^{\exists} f \in P$ for all $P \in \mathrm{V}(I)$ s,t $f \notin \sqrt{I}$. よって, ${}^{\forall}\ell \geq 0$, $f^{\ell} \neq 0$ である. $S = \left\{ f^{\ell} \,\middle|\, \ell \geq 0 \right\}$ とおき, $B = S^{-1}A$ をみると, $\varphi : A \to B$ を $a \mapsto \dfrac{a}{1}$ とおいて, $J = IB$ は $J \neq B$ である. 実際, $J = B$ ならば $1 \in J$ であるから $1 = \dfrac{a}{f^n}$ $(a \in I, n > 0)$ と表せるので $f^{\ell}(1f^n - 1a) = 0$ for some $\ell > 0$ である. これを整理すると, $f^{\ell} f^n = f^{\ell+n} = f^{\ell} a \in I$ であるが, これは f の取り方に反する. $\therefore {}^{\exists} M \in \operatorname{Max} B$ s,t $J \subseteq M$. 今, $P = M \cap A$ とおくと $P \in \operatorname{Spec} A$, $I \subseteq P$ である. 従って, $f \in P$ であるが, これは $\dfrac{f}{1} = \varphi(f) \in M$, つまり $M = B$ を導くので $\sqrt{I} \neq \bigcap_{p \in \mathrm{V}(I)} P$ は有り得ない. $\therefore \sqrt{I} = \bigcap_{p \in \mathrm{V}(I)} P$. □

Definition 24. $\sqrt{(0)}$ を *the nilradical* といい, $\bigcap_{M \in \operatorname{Max} A} M$ を A の *the Jacobson ideal* とよび $\mathrm{J}(A)$ と表す. そして A が, $\sqrt{(0)} = (0)$ をみたすとき, A は *reduced* であるという.

Lemma 1.8.11. *$\sqrt{I}$ が有限生成ならば ${}^{\exists}\ell \gg 0$ s,t $\sqrt{I} \subseteq I$.*

Proof. $\sqrt{I} = (a_1, \cdots, a_n)$ とおく. ${}^{\forall} i$ について ${}^{\exists} n_i > 0$ s,t $a_i^{n_i} \in I$. よって $\ell \gg 0$ にとると $a_1^{\alpha_1} \cdots a_n^{\alpha_n} \in I$ where $0 < \alpha_i \in \mathbb{Z}$, $\alpha_1 + \cdots + \alpha_n = \ell$ は殆ど明らかであろう. $\therefore \sqrt{I}^{\ell} \subseteq I$. □

Lemma 1.8.12 (Prime adoivance). *I, J, K を A の ideal, $n \geq 0$; $P_1, \cdots, P_n$ を A の prime ideal とする. このとき.*

$$I \subseteq J \cup K \cup \bigcup_{i=1}^{n} P_i \Rightarrow I \subseteq J, \text{ or } I \subseteq K, \text{ もしくは } I \subseteq P_i \ {}^{\exists} i.$$

Lemma 1.8.13 (modular low). *I, J, K を A の ideal で $J \subseteq I$ としたとき,*

$$I \cap (J + K) = J + (I \cap K)$$

が成立する.

上の 2 つの命題は *Exercise* としよう.

Exercise 11. *Prime avoidance* と *modular low* を証明せよ.

さてしばらくの間, $\varphi : A \to B$ を環の準同型写像とする. ${}^{\forall} I \subseteq A$; an ideal に対して $\varphi(I)$ で生成された B の ideal を IB とかく. すなわち,

$$IB = \left\{ \sum_{i=1}^{\ell} \varphi(a_i) b_i \,\middle|\, \ell > 0,\ a_i \in I,\ b_i \in B \right\}$$

である. もし I が有限生成ならば IB も有限生成である. このとき, 次が正しい.

Lemma 1.8.14.
(1) $(I + J)B = IB + JB$,

(2) $(IJ)B = (IB)(JB)$.

Proof. (1) ($\supseteq$) は自明. $^\forall x \in I+J$, $x = i+j$ $(i \in I,\ j \in J)$ と表すと $\varphi(x) = \varphi(i) + \varphi(j) \in IB + JB$.
$\therefore (I+J)B = IB + JB$.
(2) $i \in I,\ j \in J$ について $\varphi(ij) = \varphi(i)\varphi(j)$ である. 従って, $(IJ)B \subseteq (IB)(JB)$ は明らか. そして $\alpha = (\varphi(i)b_1)(\varphi(j)b_2) \in (IB)(JB)$ $(i \in I,\ j \in J,\ b_1, b_2 \in B)$ をとる. $\therefore \alpha = (b_1b_2)(\varphi(i)\varphi(j)) = (b_1b_2)\varphi(ij) \in (IJ)B$. □

逆に, $^\forall J \subseteq B$; an ideal に対して $\varphi^{-1}(J)$ を

$$J \cap A = \{a \in A | \varphi(a) \in J\}$$

とかき, J の A への制限という. $J \cap A$ は A の ideal であって, $(J \cap A)B \subseteq J$ が成立する. 又, I が A の ideal ならば, $IB \cap A \supseteq I$ である. $Q \operatorname{Spec} B \Rightarrow Q \cap A \in \operatorname{Spec} A$ も成り立つ.

次に, S を A の multi closed とし $\varphi : A \to S^{-1}A$, $a \mapsto \dfrac{a}{1}$ を自然な写像とする. すると,

Lemma 1.8.15.
(1) $^\forall J \subseteq S^{-1}A$; *an ideal* に対して $^\exists I \subseteq A$; *an ideal s,t* $J = IS^{-1}A$. *この* I *は,* $I = J \cap A$ *で与えられる.*
(2) $^\forall I \subseteq A$; *an ideal* に対して

$$IS^{-1}A = \left\{ \frac{a}{s} \,\middle|\, a \in I,\ s \in S \right\}, \quad IS^{-1}A \cap A = \{a \in A | as \in I \ \ \textit{for some } s \in S\}$$

である.

Proof. (1) $\dfrac{a}{s} \in J$ としたとき $\dfrac{a}{s} = \dfrac{a}{1} \cdot \dfrac{1}{s} = \varphi(a)\dfrac{1}{s} \in J$ である. $\therefore \dfrac{1}{s} \in \mathrm{U}(S^{-1}A)$, $\varphi(a) \in J$.
$\therefore J \subseteq (J \cap A)S^{-1}A$. 逆包含は自明であるから $J = (J \cap A)S^{-1}A$ をうる.
(2) まず, $IS^{-1}A = \left\{ \dfrac{a}{s} \,\middle|\, a \in I,\ s \in S \right\}$ を示す. $^\forall \alpha \in IS^{-1}A$, $\alpha = \displaystyle\sum_{i=1}^{n} \varphi(a_i)\frac{b_i}{s_i} = \sum_{i=1}^{n} \frac{a_ib_i}{s_i}$ where $n > 0$; $a_i \in I$, $b_i \in A$, $s_i \in S$. 今, $a_ib_i \in I$ であるからこれを改めて a_i とかき, $s = s_1 \cdots s_n$, $t_i = s_1 \cdots s_{i-1}s_{i+1} \cdots s_n$ とおくと,

$$\alpha = \sum_{i=1}^{n} \frac{a_i}{s_i} = \sum_{i=1}^{n} \frac{a_it_i}{s} = \frac{\sum_{i=1}^{n} a_it_i}{s},$$

である. $\therefore \displaystyle\sum_{i=1}^{n} a_it_i \in I$, $\alpha \in$ (右辺). 逆に, $a \in I$, $s \in S$ をとると $\dfrac{a}{s} = \varphi(a)\dfrac{1}{s} \in IS^{-1}A$ である.
次に, $IS^{-1}A \cap A = \{a \in A | as \in I \ \ \textit{for some } s \in S\}$ を示す. $^\forall a \in IS^{-1}A \cap A$ をとると $\varphi(a) = \dfrac{a}{1} \in IS^{-1}A$ であるから $^\exists i \in I$, $t \in S$ s,t $\dfrac{a}{1} = \dfrac{i}{t}$, つまり $u(at - 1i) = 0$ for some $u \in S$ となる. 従って, $(ut)a = i \in I$ となる. $a \in A$ を $as \in I$ for some $s \in S$ となるようにとると, $\varphi(a) = \dfrac{a}{1} = \dfrac{as}{s} \in IS^{-1}A$ であることから自明. □

Corollary 1.8.16. $I \subseteq A$; *an ideal* について, $IS^{-1}A = S^{-1}A \Leftrightarrow I \cap S \neq \emptyset$, である.

Lemma 1.8.17. $P \in \operatorname{Spec} A$ を $P \cap S = \emptyset$ にとれば $PS^{-1}A \in \operatorname{Spec} S^{-1}A$ であって, 実は次のような全単射が存在する.

$$\begin{array}{ccc} \operatorname{Spec} S^{-1}A & \longrightarrow & \{P \in \operatorname{Spec} A | P \cap S = \emptyset\} \\ \cup & & \cup \\ Q & \longmapsto & Q \cap A \end{array}$$

Proof. $^\forall Q \in \operatorname{Spec} S^{-1}A$ に対して $P := Q \cap A \in \operatorname{Spec} A$ とおく. $Q = PS^{-1}A$ であるから $P \cap S = \emptyset$ である. よって, 後は $P \in \operatorname{Spec} A$, $P \cap S = \emptyset$ について $P = PS^{-1}A \cap A$ だけをしめせば十分. $P \cap S = \emptyset$ であるから, $a \in A$, $s \in S$ について $as \in P \Leftrightarrow a \in P$ をみよ. □

Lemma 1.8.18. $^\forall I, J \subseteq A$; *ideals of* A について $(I \cap J)S^{-1}A = IS^{-1}A \cap JS^{-1}A$.

Proof. ($\supseteq$) のみ. $^\forall \alpha \in IS^{-1}A \cap JS^{-1}A$ をとる. $\alpha \in IS^{-1}A$, $\alpha \in JS^{-1}A$ であるから $^\exists s, t \in S$, $a \in I$, $b \in J$ s,t $\alpha = \dfrac{a}{s} = \dfrac{b}{t}$. $\therefore {}^\exists u \in S$ s,t $u(sb - at) = 0$. よって, $\alpha = \dfrac{a}{s} = \dfrac{uta}{uts} = \dfrac{usb}{ust}$ をみればよい. □

次に $P \in \operatorname{Spec} A$ とし $S = A \backslash P$ としよう. このときは $S^{-1}A$ を A_P で表すことにする.

Definition 25. *A ring* A が *maximal ideal* を唯一つしか持たないとき, この A は *a local ring* であるという.

Proposition 1.8.19. A_P は PA_P を *maximal ideal* にもつ *a local ring* である.

証明は上の全単射から直ちに従う.

Lemma 1.8.20. A は *a local ring* とせよ. I, J を A の *ideal* としたとき, $I + J = A \Rightarrow I = A$ *or* $J = A$, をみたす.

Proof. $I \neq A$, $J \neq A$ であれば $I + J \subseteq \mathfrak{m}$ where $\mathfrak{m}$ は A の the maximal ideal. $\therefore A = I + J \subseteq \mathfrak{m} \subsetneq A$. (矛盾) □

Exercise 12. A を *a ring* とする. 次を証明せよ.

(1) $I, J \subseteq A$; *ideals* について, $I + J = A \Rightarrow I \cap J = IJ$.

(2) $n > 0$ とする. I_i は A の *ideal*, $I_i \neq A$ であって更に $I_i + I_j = A$ *for* $i \neq j$ ならば $\varphi : A \to \prod_{i=1}^{n} A/I_i$, $a \mapsto (\overline{a}, \cdots, \overline{a})$ は環の準同型写像で全射である. そして $\operatorname{Ker} \varphi = \prod_{i=1}^{n} I_i$ である.

(2) は *Chainese Remainder Theorem* とよばれる重要な定理である. これは, よく用いられるので必ず証明するように.

第2章　環の次元

2.1 Noether 環

A は a ring とせよ.

Definition 26. *A が Noetherian であるとは, 全ての ideal in A が有限生成でることをいう.*

$\mathcal{I} = \{I | I$ は A の *ideal*$\}$ とせよ.

Lemma 2.1.1. 次の 3 条件は同値である.

(1) A は *Noetherian* である.
(2) $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_i \subseteq \cdots$ が A の *ideal* の *chain* とすれば $^{\exists}N > 0$ *s,t* $I_N = I_{N+1} = \cdots$.
(3) $\emptyset \neq {}^{\forall}\mathcal{S} \subseteq \mathcal{I}$, $^{\exists}I \in \mathcal{S}$ *s,t* I は *maximal in* $\mathcal{S}$.

Proof. (1)⇒(2) $I = \bigcup_{\ell \geq 1} I_\ell$ は A の ideal であるから $I = (a_1, \cdots, a_m)$ とかける. $\therefore {}^{\exists}N \gg 0$ s,t $a_i \in I_N$ for $^{\forall}i$. $\therefore I_N = I_{N+1} = \cdots$.
(2)⇒(3) ほとんど自明.
(3)⇒(1) A 内で有限生成ではない ideal I が存在したとせよ. そして,

$$\mathcal{S} = \{J | J \text{ は } A \text{ の } ideal,\ J \text{ は有限生成},\ J \subseteq I\}$$

とおく. $(0) \in \mathcal{S}$ より $\mathcal{S} \neq \emptyset$ である. $\therefore {}^{\exists}J \in \mathcal{S}$ s,t J は maximal in $\mathcal{S}$. $J \subsetneq I$ は自明であろう. $a \in A$ を $a \in I$, $a \notin J$ にとると $J \subsetneq J + (a) \subseteq I$ であるから $J + (a) \notin \mathcal{S}$, つまり, $J + (a)$ は有限生成ではないという結果をうるがこれは明らかに矛盾である. □

Corollary 2.1.2. *$I \neq A$ を ideal とする. A が Noetherian ならば A/I も Noetherian である.*

Proof. K を A/I の ideal とすれば $K = \overline{J}$ for some $J \subseteq A$; an ideal であるから殆ど自明である. □

Corollary 2.1.3. *A が Noetherian ならば $S^{-1}A$ も Noetherian である.*

Proof. $^{\forall}J \subseteq S^{-1}A$; an ideal について $J = (J \cap A)S^{-1}A$ であることから明らか. □

Theorem 2.1.4 (Hilbert). *A が Noetherian ならば $A[X]$ も Noetherian である.*

Proof. $I_0 \subseteq I_1 \subseteq \cdots$ を $A[X]$ の ideals の chain とせよ. $^{\forall}j$ に対して

$$\mathfrak{a}_{i,j} := \left\{a \in A | a \neq 0,\ f = aX^j + (lower\ terms)\ \ for\ some\ f \in I_i\right\} \cup \{0\}$$

とおく. $I_i \subseteq I_{i+1}$ は $\mathfrak{a}_{i,j} \subseteq \mathfrak{a}_{i+1,j}$ for $^\forall j$ を導き, $^\forall f \in I_i$ に対して $Xf \in I_i$ は $\mathfrak{a}_{i,j} \subseteq \mathfrak{a}_{i,j+1}$ を導く. そして, $I_i = I_{i+1}$ であるための必要十分条件は $^\forall j$; $\mathfrak{a}_{i,j} = \mathfrak{a}_{i+1,j}$ である. 従って, $^\exists N \gg 0$ s,t $\mathfrak{a}_{N,j} = \mathfrak{a}_{N+1,j}$ for $^\forall j$ を示せば十分. 今,

$$\begin{array}{ccccccccc}
\vdots & & \vdots & & \vdots & & & & \vdots & \\
\cup\!| & & \cup\!| & & \cup\!| & & & & \cup\!| & \\
\mathfrak{a}_{0,i} & \subseteq & \mathfrak{a}_{1,i} & \subseteq & \mathfrak{a}_{2,i} & \subseteq & \cdots & \subseteq & \mathfrak{a}_{n,i} & \subseteq \cdots \\
\cup\!| & & \cup\!| & & \cup\!| & & & & \cup\!| & \\
\vdots & & \vdots & & \vdots & & & & \vdots & \\
\cup\!| & & \cup\!| & & \cup\!| & & & & \cup\!| & \\
\mathfrak{a}_{0,1} & \subseteq & \mathfrak{a}_{1,1} & \subseteq & \mathfrak{a}_{2,1} & \subseteq & \cdots & \subseteq & \mathfrak{a}_{n,1} & \subseteq \cdots \\
\cup\!| & & \cup\!| & & \cup\!| & & & & \cup\!| & \\
\mathfrak{a}_{0,0} & \subseteq & \mathfrak{a}_{1,0} & \subseteq & \mathfrak{a}_{2,0} & \subseteq & \cdots & \subseteq & \mathfrak{a}_{n,0} & \subseteq \cdots
\end{array}$$

を, まず対角線にみて $\mathfrak{a}_{0,0} \subseteq \mathfrak{a}_{1,1} \subseteq \cdots$ であることから $^\exists \ell \geq 0$ s,t $\mathfrak{a}_{\ell,\ell} = \mathfrak{a}_{\ell+1,\ell+1} = \cdots$. $\therefore {}^\forall i, j \geq \ell$ に対して $\mathfrak{a}_{i,j} = \mathfrak{a}_{\ell,\ell}$ である. そして, $^\forall j \leq \ell - 1$ については $\mathfrak{a}_{0,j} \subseteq \mathfrak{a}_{1,j} \subseteq \mathfrak{a}_{2,j} \subseteq \cdots \subseteq \mathfrak{a}_{n,j} \subseteq \cdots$ であるから $^\exists \alpha_j \geq 0$ s,t $\mathfrak{a}_{\alpha_j,j} = \mathfrak{a}_{\alpha_j+1,j} = \cdots$. $\therefore N = \max\{\alpha_1, \cdots, \alpha_{\ell-1}, \ell\}$ が求める数である. □

Corollary 2.1.5. *A が Noetherian ならば $A[X_1, \cdots, X_n]$ も Noetherian である.*

Corollary 2.1.6. *A が Noetherian ならば, $I \subsetneq A[X_1, \cdots, X_n]$; an ideal に対して $A[X_1, \cdots, X_n]/I$ も Noetherian である. とくに $\mathbb{C}[X_1, \cdots, X_n]/I$ は Noetherian である.*

Theorem 2.1.7 (Cohen). 次は同値である.

(1) *A は Noetherian である.*
(2) $^\forall P \in \operatorname{Spec} A$ は有限生成である.

Proof. (2)⇒(1) のみ. $\mathcal{S} = \{I | I$ は A の *ideal*, $I \neq f, gen\}$ とおく. もし $\mathcal{S} \neq \emptyset$ ならば $\mathcal{C} \subseteq \mathcal{S}$; a chain に対して $I = \bigcup_{J \in \mathcal{S}} J$ とおく. $I = f, gen \Rightarrow {}^\exists x_1, \cdots, x_n \in I$; generator. $\therefore x_i \in J$ for some $J \in \mathcal{C}$, $J = (x_1, \cdots, x_n)$. (矛盾) $\therefore I\mathcal{S}$ であるから Zorn's Lemma より $^\exists$maximal element in $\mathcal{S}$. これを I とかく. $I \neq A$ は自明. もし $I \notin \operatorname{Spec} A$ ならば $^\exists x, y \in A$ s,t $x, y \notin I$ であって且つ $xy \in I$. $I \subsetneq I + (x)$ より $I + (x)$ は有限生成である. $\therefore I + (x) = (a_1 + r_1 x, \cdots, a_n + r_n x)$ where $a_i \in I$, $r_i \in A$. 今, $J = I : x$ とおく. $I \subsetneq I + (y) \subseteq J$ であるから J も有限生成であるから $J = (z_1, \cdots, z_m)$ と表す. $^\forall \alpha \in I$ をとると $\alpha \in I + (x)$ であるので

$$\alpha = \sum_{i=1}^n s_i(a_i + r_i x) = \sum_{i=1}^n s_i a_i + \sum_{i=1}^n s_i(r_i x) \quad (s_i \in A).$$

$$\therefore I \ni \alpha - \sum_{i=1}^n s_i a_i = \sum_{i=1}^n (s_i r_i)x,\ \sum_{i=1}^n s_i r_i \in J. \therefore \alpha \in (a_1, \cdots, a_n, xz_1, \cdots, xz_m).$$

$$\therefore \quad I = (a_1, \cdots, a_n, xz_1, \cdots, xz_m).$$

よって, $\mathcal{S} = \emptyset$ となり, A は Noetherian である. □

2.2 Primary decomposition

A は a ring とせよ.

Definition 27. *I が A の primary ideal であるとは,*

(1) *$I \subsetneq A$; an ideal of A,*
(2) *$a, b \in A$ について, $ab \in I \Rightarrow a \in I$ or $b \in \sqrt{I}$,*

という 2 条件をみたすことをいう. 勿論, *$P \operatorname{Spec} A$ は primary ideal* である. また $^\forall M \in \operatorname{Max} A$, $^\forall \ell > 0$ に対して M^ℓ も *primary ideal* である.

Lemma 2.2.1. *I が A の primary ideal* であれば $\sqrt{I} \in \operatorname{Spec} A$ である.

Proof. $a, b \in A$ をとり $ab \in \sqrt{I}$, $a \notin \sqrt{I}$ とする. $(ab)^\ell = a^\ell b^\ell \in I$ for $\ell \geq 1$, $a^\ell \notin I$ であるから $(b^\ell)^\alpha = b^{\ell\alpha} \in I$. $\therefore b \in \sqrt{I}$. □

Definition 28. *I を A の primary ideal, $P \in \operatorname{Spec} A$* とせよ. $\sqrt{I} = P$ であるとき, *I は P-primary* であるという.

Lemma 2.2.2. *I_1, I_2 が P-primary* ならば *$I_1 \cap I_2$ も P-primary* である.

Proof. $\sqrt{I_1 \cap I_2} = P$ である. $ab \in I_1 \cap I_2$ で $b \notin P$ ならば $a \in I_1$, $a \in I_2$ による. □

Definition 29. *$I \subsetneq A$; an ideal of A* のとき *I が A* 内で *a primary decomposition* をもつとは

$$^\exists Q_1, \cdots, Q_n \ (n > 0) \text{ primary ideals of } A \quad s,t \ I = Q_1 \cap \cdots \cap Q_n$$

なることをいう. *I が A* 内で *a primary decomposition* をもつとき, この *decomposition* が *reduced* (無駄のない分解) であるとは

(1) *$\sqrt{Q_i}$* は互いに全て異なる,
(2) *$n = 1$* であるか, 又は *$\bigcap_{j \neq i} Q_j \not\subseteq Q_i$ for $^\forall i$,*

が成立することをいう. そして一度 *I が primary decomposition* をもつことが分かれば, 上の補題によってそれを *reduced* にすることができる.

Theorem 2.2.3 (Laker-Noether). *A が Noetherian* であれば *$^\forall I \subsetneq A$; an ideal は a primary decomposition* をもつ.

Definition 30. *$I \subseteq A$; an ideal* について,

(1) *$I \neq A$,*
(2) *$J, K \subseteq A$; ideals* について, *$I = J \cap K \Rightarrow I = J$ or $I = K$,*

をみたすとき, *I は an irreducible ideal* であるという.

まず A を Noetherian としよう．もし $^{\exists}I \subsetneq A$; an ideal s,t I は irreducible decomposition (i,e; $I = Q_1 \cap \cdots \cap Q_n$, Q_i は irreducible ideal in A) を持たない, を仮定する．$\mathcal{S}$ を上のような A の ideal の集合とおくと $I \in \mathcal{S} \neq \emptyset$. A の極大条件により $\mathcal{S}$ 内には極大元が存在し, それを I とおくと, I は irreducible ideal ではないので $^{\exists}J, K$; proper ideals of A s,t $I = J \cap K$. $J, K \notin \mathcal{S}$ であるから J, K は irreducible decomposition をもち, それらを合せたものが I の irreducible decomposition になる．従って A が Noetherian であれば, $^{\forall}I \subsetneq A$; an ideal は irreducible decomposition をもつことがわかる．よって, 上の定理の証明は次の補題をいえば十分である．

Lemma 2.2.4. *A が Noetherian ならば, irreducible ideal は primary ideal である．*

Proof. $\sqrt{I} \subsetneq A$ である．$a, b \in A$ について $ab \in I$, $b \notin \sqrt{I}$ とせよ．$^{\forall}n > 0$ について $b^n \notin I$. そこで,

$$I \underset{A}{:} b \subseteq I \underset{A}{:} b^2 \subseteq \cdots \subseteq I \underset{A}{:} b^n \subseteq \cdots$$

をつくる．すると $^{\exists}n > 0$ s,t $I \underset{A}{:} b^n = I \underset{A}{:} b^{n+1} = \cdots$. 次を示そう．

Claim 3. $\left(I \underset{A}{:} b\right) \cap [I + (b^n)] = I$.

proof of Claim. $x \in A$ が $bx \in I$, $x = i + yb^n$ であれば $bx = bi + yb^{n+1}$. $\therefore y \in I :_A b^{n+1} = I \underset{A}{:} b^n$.
$\therefore x \in I$. □

定理の証明にもどると $I = irreducible$, $b^n \notin I$ より $I :_A b = I$ である．$\therefore a \in I \underset{A}{:} b = I$. □

以下, A は Noetherian, $I \subsetneq A$; an ideal of A として $I = Q_1 \cap \cdots \cap Q_n$; a reduced primary decomposition, $P_i = \sqrt{Q_i}$ とおく．

Theorem 2.2.5. $\{P_1, \cdots, P_n\} = \{P \in \operatorname{Spec} A | P = I : x \quad for\ some\ x \in A\}$.

まず, S は A の multi closed, $I \cap S = \emptyset$ とすると,

$$IS^{-1}A = \bigcap_{P_i \cap S = \emptyset} Q_i S^{-1} A$$

は, $IS^{-1}A$ の $S^{-1}A$ 内での reduced primary decomposition であることに注目しよう．実際, $I \cap S = \emptyset$ を仮定しているので $IS^{-1}A \subsetneq S^{-1}A$ である．ここで,

$$I \cap S \neq \emptyset \Leftrightarrow \sqrt{I} \cap S \neq \emptyset$$

であることから $Q_i \cap S = \emptyset$ であることは $P_i \cap S = \emptyset$ と同値である．これから $Q_i S^{-1}A$ が $P_i S^{-1}A$-primary であることを示そう．これは $\sqrt{Q_i S^{-1}A} = P_i S^{-1}A$ であって, $\alpha\beta \in Q_i S^{-1}A$ とすると $\alpha = \dfrac{a}{s}$, $\beta = \dfrac{b}{t}$ と表したとき $\alpha\beta = \dfrac{ab}{st} \in Q_i S^{-1}A$ であるから $^{\exists}u \in S$ s,t $u(ab) \in Q_i$. $\therefore ua \in Q_i$ or $b \in P_i$, $\alpha = \dfrac{ua}{us} \in Q_i S^{-1}A$ or $\beta = \dfrac{b}{t} \in P_i S^{-1}A$. 勿論, $\left\{P_i S^{-1}A\right\}_{P_i \cap S = \emptyset}$ は distinct であるし, 又 $Q_i \cap S = \emptyset$ であるとき, もし $Q_i S^{-1}A \supseteq \bigcap_{j \neq i} Q_j S^{-1}A$ ならば $Q_i \supseteq \bigcap_{\substack{j \neq i \\ P_j \cap S = \emptyset}} Q_j$ であるから $Q_i S^{-1}A \not\supseteq \bigcap_{j \neq i} Q_j S^{-1}A$ である．よって, 以上のことから reduced であることが分かる．

proof of theorem. まず $S = A\backslash P_i$ ととるとき $IA_{P_i} = \bigcap_{P_j \subseteq P_i} Q_j A_{P_i}$ は reduced primary decomposition of IA_{P_i} in A_{P_i} である. もし $^{\exists}y \in A_{P_i}$ s,t $IA_{P_i} : y = P_i A P_i$ ならば $y = \dfrac{x}{s}$ とかくとき $IA_{P_i} : \dfrac{x}{1} = P_i A_{P_i}$ である. よって $\dfrac{x}{1} P_i A_{P_i} \subseteq IA_{P_i}$ より $^{\exists}t \in S$; $txP_i \subseteq I$. $a \in A$ について $atx \in I$ ならば $\dfrac{a}{1} \cdot \dfrac{x}{1} \in IA_{P_i}$ より $\dfrac{a}{1} \in P_i A_{P_i}$ で, 従って $a \in P_i$. つまり,

$$I \underset{A}{:} tx = P_i$$

をうる. 逆に, $P \in \operatorname{Spec} A$ について $^{\exists}x \in A$ s,t $P = I : x$ であれば $I \subseteq P$ より $S = A\backslash P$ として $IA_P : \dfrac{x}{1} = PA_P$, $IA_P = \bigcap_{P_i \subseteq P} Q_i A_P$ という a reduced primary decpmposition を通してみれば $(A, \mathfrak{m})$ local ring に帰着できる.

そこで以下, $(A, \mathfrak{m})$ は a Noetherian local ring とする.

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_n$$

は reduced primary decpmposition で, $\sqrt{Q_1} = \mathfrak{m}$ とすると $^{\exists}x \notin Q_1$, $x \in \bigcap_{i \geq 2} Q_i$ であって $xQ_1 \subseteq I$.
$\therefore Q_1 \subseteq I : x$ で $^{\exists}\ell > 0$; $\mathfrak{m}^\ell \subseteq Q_1$. よって $\mathfrak{m}^\ell x \subseteq I$. このような ℓ を最小にとると $\mathfrak{m}^\ell x \subseteq I$, $\mathfrak{m}^{\ell-1} x \not\subseteq I$.
$\therefore y \in \mathfrak{m}^{\ell-1} x$, $y \notin I$. もちろん, $\mathfrak{m} y \subseteq I$ であるから $\mathfrak{m} \subseteq I : y \subsetneq A$ をみて $\mathfrak{m} = I : y$ である.
逆に $^{\exists}x \in A$; $\mathfrak{m} = I : x$ なら, $x\mathfrak{m} \subseteq I$. ここで $x \notin I$ であることから $^{\exists}i$; $x \notin Q_i$. ゆえに $x\mathfrak{m} \subseteq Q_i$ より $\mathfrak{m} \subseteq P_i$. $\therefore P_i = \mathfrak{m}$. □

Theorem 2.2.6. *P_i が $P_1, \cdots, P_n$ 内で minimal であれば*

$$Q_i = IA_{P_i} \cap A$$

である. 従って Q_i は分解の仕方によらない.

Proof. $IA_{P_i} = Q_i A_{P_i}$ であって $Q_i A_{P_i} \cap A = Q_i$ であることに従う. □

Definition 31. *$^{\forall}I \subsetneq A$; an ideal に対して*

$$\operatorname{Ass}_A A/I = \{P \in \operatorname{Spec} A | P = I : x \quad for\ some\ x \in A\}$$

とおき, I の the associated prime ideals という.

Corollary 2.2.7. *A が Noetherian で, $I \subseteq A$; an ideal のとき $|\operatorname{Ass}_A A/I| < \infty$ であって, $\operatorname{Ass}_A A/I = \emptyset \Leftrightarrow I = A$ である.*

Corollary 2.2.8. *A が Noetherian で, $I \subsetneq A$; an ideal のとき*

$$\bigcup_{P \in \operatorname{Ass}_A A/I} P = \{a \in A | a \text{ は } A/I - zd \text{ である }\}.$$

Proof. $x \in A$ が $^{\exists}y \in A\backslash I$; $xy \in I$ のときは $xy \in Q_i$ ($^{\forall}i$). 一方で, $y \notin Q_i$ ($^{\exists}i$) であるから $x \in P_i$. 逆に, $P \in \operatorname{Ass}_A A/I$ をとり $x \in P$ について $P = I : a$ ($^{\exists}a \in A$) であったので $ax \in I$. $a \notin I$ であるから x は $A/I - zd$ である. □

Corollary 2.2.9. *A が Noetherian のとき,*

$$\bigcup_{P\in \operatorname{Ass} A/(0)} P = \{a \in A | a \text{ は } A - zd\}.$$

Corollary 2.2.10. *A が Noetherian* $\Rightarrow |\{P \in \operatorname{Spec} A | P \text{ は } minimal\ in\ \operatorname{Spec} A\}| < \infty$.

Definition 32.

$$\operatorname{Ass} A := \{P \in \operatorname{Spec} A | P = (0) : x \quad for\ some\ x \in A\}\ ,$$
$$\operatorname{Min} A := \{P \in \operatorname{Spec} A | P \text{ は } minimal\ in\ \operatorname{Spec} A\}\ ,$$

とおく.

もちろん,

Corollary 2.2.11. *A が Noetherian* ならば $\operatorname{Min} A \subseteq \operatorname{Ass} A$, $\sqrt{(0)} = \bigcap_{P\in \operatorname{Min} A} P$ である.

Proposition 2.2.12. $(A, \mathfrak{m})$ を *a Noetherian local ring* とするとき次は同値である.

(1) $\mathfrak{m} \in \operatorname{Ass} A$.
(2) $^{\forall} x \in \mathfrak{m}$ は $A - zd$ である.

Proof. (2)⇒(1) のみ. これは $\mathfrak{m} \subseteq \bigcup_{P\in \operatorname{Ass} A} P$ による. □

Proposition 2.2.13. $(A, \mathfrak{m})$ を *a Noetherian local ring* とするとき次は同値である.

(1) $\operatorname{Spec} A = \{\mathfrak{m}\}$.
(2) $^{\exists}\ell > 0$; $\mathfrak{m}^{\ell} = (0)$.

2.3　次元論, まず Artinian rings から

ここでは, A は a Noetherian ring とする. $I \subseteq A$; an ideal に対して

$$\operatorname{Ass}_A A/I = \{P \in \operatorname{Spec} A | P = I : x \quad for\ some\ x \in A\}$$

とおき, I の the associated prime ideal という. 前回に示したように,

(1) $|\operatorname{Ass}_A A/I| < \infty$,
(2) $\operatorname{Ass}_A A/I \neq \emptyset \Leftrightarrow I \neq A$,
(3) $I \subsetneq A$ であれば $I = \bigcap_{P\in \operatorname{Ass}_A A/I} I(P)$ となるような $\{I(P)\}_{P\in \operatorname{Ass}_A A/I}$ where $I(P)$ は P-primary ideal in A が存在する,
(4) $I \subsetneq A$ のときは $\bigcup_{P\in \operatorname{Ass}_A A/I} P = \{a \in A | a \text{ は } A/I - zd\}$,

が成立していた. とくに, $\mathrm{Ass}_A\, A/(0) = \mathrm{Ass}\, A$ とかくと

$$\bigcup_{P\in \mathrm{Ass}_A\, A} P = \{a \in A | a \text{ は } A - zd\}$$

となる. $\mathrm{Min}\, A = \{P \in \mathrm{Spec}\, A | P \text{ は } \textit{minimal in } \mathrm{Spec}\, A\}$ と定めると, $\emptyset \neq \mathrm{Min}\, A \subseteq \mathrm{Ass}\, A$ である. この記号の下に, $^\forall P \in \mathrm{Spec}\, A$, $^\exists Q \in \mathrm{Min}\, A$ s,t $Q \subseteq P$ である.

さて, これからは A は a ring としておく.

Lemma 2.3.1 (Krull-東屋). *I を A の a f,g ideal とするとき, $I = JI$ ならば $I = (0)$ である.*

Proof. $I \neq (0)$ として $I = (x_1, \cdots, x_n)$ となる $x_i \in A$ を $n > 0$ が最小になるようにとる. すると, $x_i \in JI$ であるから $x_i = \sum_{j=1}^{n} a_{ij}x_j$ $^\exists a_{ij} \in \mathrm{J}(A)$. よって $(1 - a_{nn})x_n = \sum_{j=1}^{n-1} a_{jn}x_j$ であるから $1 - a_{nn} \in \mathrm{U}(A)$ に注目すると $I = (x_1, \cdots, x_{n-1})$ となり, これは n の最小性に反する. $\therefore I = (0)$. □

Definition 33. *A が Artinian であるとは, $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$ が A の ideal の列であれば $^\exists n > 0$ s,t $I_n = I_{n+1} = \cdots$, をみたすことをいう.*

Lemma 2.3.2. *$(A, \mathfrak{m})$ local ring, $^\exists \ell > 0$ s,t $\mathfrak{m}^\ell = (0)$ とせよ. もし $\mathfrak{m}$ が有限生成ならば A は Artinian である.*

Proof. ℓ についての induction で示す. $\ell = 1$ のときは A は体である. $\ell > 0$ として $\ell - 1$ 以下で正しいとせよ. すると,

$$0 \longrightarrow \mathfrak{m}^{\ell-1} \xrightarrow{\ i\ } A \xrightarrow{\ \varphi\ } \frac{A}{\mathfrak{m}^{\ell-1}} \longrightarrow 0$$

をみるに $L := \mathfrak{m}^{\ell-1} \in \underline{\underline{\mathrm{M}}}(A/\mathfrak{m})$ であるから A は DDC をみたす. これをまじめにすると次のようになる. $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$; ideals of A をとると $^\exists n > 0$ s,t $\varphi(I_n) = \varphi(I_{n+1}) = \cdots$. 一方で, $^\exists \ell > 0$ s,t $L \cap I_\ell = L \cap I_{\ell+1} = \cdots$. $N = \max\{n, \ell\}$ とおくと, $I_N = I_{N+1} = \cdots$ をみたすであろう. □

Lemma 2.3.3. *A が Artinian であれば $|\mathrm{Max}\, A| < \infty$ である.*

Proof. $\mathrm{Max}\, A = \{\mathfrak{m}_i | i > 0,\ \mathfrak{m}_i \text{は } \textit{distinct}\}$ とおくと,

$$^\exists a\ \textit{chain};\ \ \mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supsetneq \cdots$$

である. □

Lemma 2.3.4. *A が Artinian domain ならば A は体である.*

Proof. $0 \neq {}^\forall a \in A$, $^\exists n > 0$ s,t $(a^n) = (a^{n+1})$. $\therefore a^n = xa^{n+1}$ より $1 = ax$. □

Corollary 2.3.5. *A が Artinian ならば $\mathrm{Spec}\, A = \mathrm{Max}\, A$ である.*

Proposition 2.3.6. 次は同値である.

(1) *A は Artinian である.*

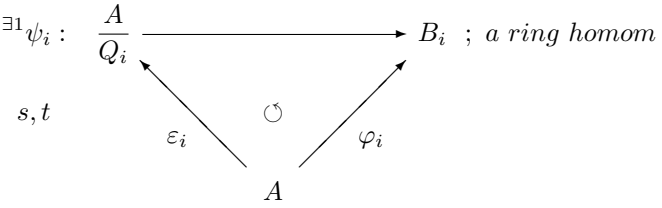
(2) A は *Noetherian* であって $\operatorname{Spec} A = \operatorname{Max} A$ である.

Proof. (1)⇒(2) $\operatorname{Max} A$ は finite set, $^{\forall}M \in \operatorname{Max} A$ に対して A_M は Artinian である. $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$; ideals of A をとる. もし $^{\forall}M \in \operatorname{Max} A$, A_M が Noetherian であれば $^{\exists}n > 0$ s,t $I_nA_M = I_{n+1}A_M = \cdots$. よって, $^{\exists}N > 0$ s,t $^{\forall}M \in \operatorname{Max} A$ に対して $I_NA_M = I_{N+1}A_M = \cdots$. 今, $^{\forall}i \geq N$ について $^{\forall}x \in I_{i+1}$ は $\dfrac{x}{1} \in I_iA_M$ for all $M \in \operatorname{Max} A$. $\therefore {}^{\exists}s \in A\backslash M$ s,t $sx \in I_N$. もし $^{\exists}\mathfrak{m} \in \operatorname{Max} A$ s,t $I_i : x \subseteq \mathfrak{m}$ であれば, $a \in A$ について $ax \in I_i \Rightarrow a \in \mathfrak{m}$ であるがこれは $M = \mathfrak{m}$ としたときの $s \in A\backslash\mathfrak{m}$ の存在に反する.
$\therefore I_i : x = A$. よって $x \in I_i$ で $I_i = I_{i+1}$. 従って, $(A, \mathfrak{m})$ local としたとき A が Noetherian であることを示せば十分. 今, $\mathfrak{m}$ が有限生成であることは A が Artinian であることから直ちに従う. $\therefore \operatorname{Spec} A = \operatorname{Max} A = \{\mathfrak{m}\}$ をみて A は Noetherian である.
(2)⇒(1) $^{\forall}M \in \operatorname{Max} A$, A_M が Artinian を示せば十分. よって $(A, \mathfrak{m})$ local としてよい. $^{\exists}\ell > 0$; $\mathfrak{m}^{\ell} = (0)$ より A は DDC をみたす. □

Corollary 2.3.7. *A が Artinian ならば $\mathrm{J}(A)^{\ell} = (0)$ for $\ell \gg 0$.*

Theorem 2.3.8 (構造定理). *A が Artinian とする. $\varphi : A \to \prod_{M \in \operatorname{Max} A} A_M$, $a \mapsto \left(\dfrac{a}{1}\right)$ とすれば, この φ は環の同型射である.*

Proof. $n = |\operatorname{Max} A|$ とし $\operatorname{Max} A = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\}$ とかく. (0) の a reduced primary decomposition を $Q_1 \cap \cdots \cap Q_n$ where $\sqrt{Q_i} = \mathfrak{m}_i$ として, それぞれの自然な写像を $\varphi_i : A \to B_i$, $\varepsilon : A \to A/Q_i$ とおく. $^{\forall}a \in A\backslash\mathfrak{m}_i$ をとると, A/Q_i は $\mathfrak{m}_i/Q_i$ を maximal ideal にもつような local ring であるから $\varepsilon(a) = \overline{a} \in \mathrm{U}(A/Q_i)$. 従って, 次のような可換図を得られる.



局所化の性質により $\operatorname{Ker}\varphi_i = \{a \in A | as \in Q_i \ \ for\ some\ s \in A\backslash\mathfrak{m}_i\}$ であったがこれは primary ideal の定義そのものである, つまり $Q_i = \ker\varphi_i$ である. 一方で, $^{\forall}\alpha \in A/Q_i$ は $\alpha = \overline{a} = \varepsilon(a)$ と表せる.
$\therefore \alpha = \varepsilon(a)\varepsilon(1)^{-1}$, $A/Q_i \cong A_{\mathfrak{m}_i}$. □

2.4　次元論

以下, A は a Noetherian ring とする.

Lemma 2.4.1. *$(A, \mathfrak{m})$ local で $f \in \mathfrak{m}$ とする. $Q \in \operatorname{Spec} A$ とせよ. もし $\mathfrak{m} = \sqrt{(f)}$ でかつ $Q \subsetneq \mathfrak{m}$ であれば $Q \in \operatorname{Min} A$.*

Proof. $^{\forall}\ell > 0$, $Q^{(\ell)} = \left\{a \in A | as \in Q^{\ell} \ \ for\ some\ s \in A\backslash Q\right\}$ とおく. つまり $Q^{(\ell)} = Q^{\ell}A_Q \cap A$ である. この $Q^{(\ell)}$ は Q-primary, $Q^{\ell} \subseteq Q^{(\ell)}$ である. 更に, $Q^{(\ell+1)} \subseteq Q^{(\ell)}$ が成立する. よって, $(f) \subseteq (f) + Q^{(\ell+1)} \subseteq (f) + Q^{(\ell)} \subseteq A$ をうる. 一方で, $A/(f)$ は Artinian であるから $^{\exists}\ell > 0$ s,t $(f) + Q^{(\ell+1)} = (f) + Q^{(\ell)}$.

$f \notin Q$ であるから $Q^{(\ell)} = (f) \cap Q^{(\ell)} + Q^{(\ell+1)} = fQ^{(\ell)} + Q^{(\ell+1)}$. $\therefore Q^{(\ell)} = Q^{(\ell+1)}$. ここで A_Q を考えると $Q^\ell A_Q = (0)$, つまり $(QA_Q)^\ell = (0)$ であるから $Q \in MinA$ をうる. □

Definition 34. $^\forall P \in \operatorname{Spec} A$ に対して

$$\operatorname{ht}_A P = \sup\left\{0 \leq n \in \mathbb{Z} | {}^\exists P = P_n \supsetneq P_{n-1} \supsetneq \cdots \supsetneq P_1 \supsetneq P_0 \ \ in\ \operatorname{Spec} A\right\}$$

と定める.

この記号によれば

Corollary 2.4.2. $(A, \mathfrak{m})$ *local* で $^\exists f \in \mathfrak{m}$ *s,t* $\mathfrak{m} = \sqrt{(f)}$ ならば $\operatorname{ht}_A \mathfrak{m} \leq 1$ である.

Theorem 2.4.3. $P \in \operatorname{Spec} A$ とする. $f_1, \cdots, f_n \in A$ $(n \geq 0)$ で $I = (f_1, \cdots, f_n)$ としたとき, $P \in \operatorname{Min} A/I$ ならば $\operatorname{ht}_A P \leq n$ である.

Proof. $(A, \mathfrak{m})$ local で $\mathfrak{m} \in \operatorname{Min} A/I$ として十分. n についての induction で証明する. $n \leq 1$ については証明済み. よって $n \geq 2$ として $n-1$ 以下まで正しいとせよ. もし $\operatorname{ht}_A \mathfrak{m} \geq n+1$ なら $^\exists$a chain in $\operatorname{Spec} A$; $\mathfrak{m} = P_{n+1} \supsetneq P_n \supsetneq \cdots \supsetneq P_1 \supsetneq P_0$. 今, $0 \leq {}^\forall i \leq n$, $I_i = (f_1, \cdots, f_i)$ とし $Q = P_n$ とおく. すると,

$$Q + I_n \supseteq Q + I_{n-1} \supseteq \cdots \supseteq Q + I_1 \supseteq Q + I_0 = Q \subsetneq \mathfrak{m}\ ,$$

$Q+I_n$; $\mathfrak{m}-primary$ より $\sqrt{Q+I_i} = \mathfrak{m}$ となる i を最小にとる. すると, $^\exists P \in \operatorname{Spec} A$ s,t $Q+I_{i-1} \subsetneq P \subsetneq \mathfrak{m}$. ところで $Q + I_i \subseteq P + (f_i) \subseteq \mathfrak{m}$ より $^\exists \ell > 0$; $\mathfrak{m}^\ell \subseteq P + (f_i)$.

$(i = n)$ のとき. このときは $I_{n-1} \subseteq P \subsetneq \mathfrak{m}$ で $I_{n-1} + (f_n) \underset{min}{\subsetneq} \mathfrak{m}$ より A/I_{n-1} を通すと $I_{n-1} \subseteq P$ は minimal. よって n についての induction により $\operatorname{ht}_A P \leq n-1$. $\therefore \operatorname{ht}_A Q \leq n$. (矛盾)

$(i < n)$ のとき. このときは $i+1 \leq {}^\forall j \leq n$, ${f_j}^\ell \in P + (f_i)$ より ${f_j}^\ell = p_j + a_j f_i$ ($^\exists p_j \in P$, $^\exists a_j \in A$). すると $J = I_{i-1} + (p_j | i < j \leq n)$ とすると ${f_j}^\ell \in J + (f_i) \subseteq P$ $(i < {}^\forall j \leq n)$. $\therefore I \subseteq \sqrt{J + (f_i)}$. よって,

$$\begin{array}{l} \mathfrak{m} \underset{min}{\supsetneq} J + (f_i) \\ \mathfrak{m} \supsetneq P \supseteq J \end{array}$$

より A/J を通すと $P \in \operatorname{Min} A/J$ のはずである. n についての induction により $\operatorname{ht}_A P \leq (i-1)+(n-i) = n-1$. $\therefore \operatorname{ht}_A Q \leq n-1$. (矛盾) □

Corollary 2.4.4. $^\forall P \in \operatorname{Spec} A$, $\operatorname{ht}_A P < \infty$.

Definition 35.

$$\dim A := \sup_{P \in \operatorname{Spec} A} \operatorname{ht}_A P = \sup\left\{0 \leq n \in \mathbb{Z} | {}^\exists P_n \supsetneq \cdots \supsetneq P_0 \ \ in\ \operatorname{Spec} A\right\}.$$

これを A の *Krull* 次元 (単に, 次元) という.

Corollary 2.4.5. $(A, \mathfrak{m})$ を *local* とし, $d = \dim A$ とすると,

(1) $0 \leq d < \infty$.

(2) $d = \mathrm{ht}_A\,\mathfrak{m}$.
(3) $d > 0$ ならば $^{\exists}f_1, \cdots, f_d \in \mathfrak{m}$ *s,t* $\sqrt{(f_1, \cdots, f_d)} = \mathfrak{m}$.

(3) の証明は次の補題をみよ.

Lemma 2.4.6. $I \subsetneq A$; *an ideal* に対して $n = \mathrm{ht}_A I := \min_{P \in \mathrm{V}(I)} \mathrm{ht}_A P$ と定めるとき, $n > 0$ ならば $^{\exists}f_1, \cdots, f_n \in I$ *s,t* $\mathrm{ht}_A(f_1, \cdots, f_i) = i$ *for* $0 \leq {}^{\forall}i \leq n$.

Proof. $n = 0$ なら自明. $n \geq 1$ とせよ. $^{\forall}Q \in \mathrm{Min}\, A/I$, $I \not\subseteq Q$. $\therefore {}^{\exists}f = f_1 \in I$ s,t $f \notin Q$ for $^{\forall}Q \in \mathrm{Min}\, A$. $\therefore \mathrm{ht}_A(f_1) = 1$. よって $1 \leq i < n$ で $f_1, \cdots, f_i$ まで取れているものとせよ. すると $(f_1, \cdots, f_i) \subseteq Q$ で $\mathrm{ht}_A Q = i$ となるものは $I \not\subseteq Q$. $^{\exists}f_{i+1} \in I$ s,t $^{\forall}Q \in \mathcal{F} := \{P \in \mathrm{V}(f_1, \cdots, f_i) | \mathrm{ht}_A P = i\}$, $f_{i+1} \notin Q$. もちろん $\mathrm{ht}_A(f_1, \cdots, f_{i+1}) = i + 1$. □

Definition 36. $(A, \mathfrak{m})$ が *a Noetherian local,* $d = \dim A$ とおくと $d > 0$ のときは

$$^{\exists}f_1, \cdots, f_d \in \mathfrak{m}\ s,t\ \ell_A(A/(f_1, \cdots, f_d)) < \infty \Leftrightarrow \sqrt{(f_1, \cdots, f_d)} = \mathfrak{m}$$

このような $\{f_1, \cdots, f_d\}$ を A の *an sop* という. もし $d = 0$ ならば *sop of* A は考えないかもしくは $\emptyset$ をとることにする.

Definition 37. $d = \dim A$ とおく.

$$\mathrm{Min}\, A := \{Q \in \mathrm{Spec}\, A | Q \text{ は } \textit{minimal in } \mathrm{Spec}\, A\}$$
$$\mathrm{Assh}\, A := \{Q \in \mathrm{Spec}\, A | \dim R/Q = d\}$$

とおく.

もちろん $\mathrm{Spec}\, A$ 内には $^{\exists}Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ であるから $Q_0 \in \mathrm{Assh}\, A \neq \emptyset$ である. $^{\forall}Q \in \mathrm{Assh}\, A$ は $\mathrm{Spec}\, A$ の極小元なので $Q \in \mathrm{Ass}\, A$ である.

$$\therefore \quad \emptyset \neq \mathrm{Assh}\, A \subseteq \mathrm{Min}\, A \subseteq \mathrm{Ass}\, A \subseteq \mathrm{Spec}\, A, \quad |\mathrm{Ass}\, A| < \infty.$$

$^{\forall}f \in \mathfrak{m}$ について $A/fA \neq (0)$ であって, さらに

(1) $d \geq \dim A/fA \geq d - 1$.
(2) $\dim A/fA = d - 1 \Leftrightarrow f \notin Q$ *for* $^{\forall}Q \in \mathrm{Assh}\, A$.

をみたす.

Proof. (1) もし $\dim A/fA \leq d - 2$ とすると $\mathrm{Spec}\, A/fA = \left\{\overline{P} | P \in \mathrm{V}(f)\right\}$. $\therefore {}^{\exists}g_1, \cdots, g_{d-2} \in \mathfrak{m}$ s,t $\ell_A\left(\dfrac{A/fA}{(\overline{g_1}, \cdots, \overline{g_{d-2}})}\right) < \infty$. よって $^{\exists}f, g_1, \cdots, g_{d-2} \in \mathfrak{m}$ s,t $\sqrt{(f, g_1, \cdots, g_{d-2})} = \mathfrak{m}$. (矛盾)
(2) $\dim A/fA = d - 1 \Rightarrow {}^{\forall}Q \in \mathrm{Assh}\, A$, $Q \not\supseteq (f)$. $\therefore f \notin Q$. $^{\forall}Q \in \mathrm{Assh}\, A$, $f \notin Q \Rightarrow \dim A/fA \neq d$. □

Corollary 2.4.7. $(A, \mathfrak{m})$ *local* で $f \in \mathfrak{m}$; A*-nzd* $\Rightarrow \dim A/fA = d - 1$.

第3章　加群の定義

3.1　加群と準同型写像

以下, R は可換環とする. M が an R-module であるとは, まず M は加法群 ($+$ について abel 群) であって, その上 a map $\mu : R \times M \to M$ が与えられて $\mu((a,x)) = ax$ (ax を $a \rightharpoonup x$ と表すこともある.) とかくことにすれば次の条件 (公理) をみたすことをいう.

(1) $(a+b)x = ax + bx$,
(2) $a(x+y) = ax + ay$,
(3) $a(bx) = (ab)x$,
(4) $1x = x$,

where $a, b \in R$, $x, y \in M$. 上の定義において, μ の存在は $\alpha : R \to \mathrm{Hom}(M,M)$ a unitary ring homom が与えられることと同値である. 但し, $\mathrm{Hom}(M,M)$ は $\{f | f : M \to M \ \ a\ group\ homom\}$ を表しているものとする.

Definition 38. *L, M; R-modules であるとき, $\varphi : L \to M$ が準同型写像であるとは, $^\forall x, y \in L$, $^\forall a \in R$ に対して (1) $\varphi(x+y) = \varphi(x) + \varphi(y)$, (2) $\varphi(ax) = a\varphi(x)$, をみたすことをいう. これからは, R-加群の準同型写像のことを an R-linear map とかく.*

Example 3.1.1.
(1) *R は an R-module である.*
(2) *$^\forall I \subseteq R$; an ideal は R-module である.*
(3) *$n > 0$ について R^n は自然に R-module となる.*
(4) *$\varphi : R \to S$ を環の準同型写像とせよ. $a \rightharpoonup s := \varphi(a)s$ と定めると S は an R-module である.*
(5) *k を体とすれば, $^\forall V$; k-vector s,p は k-module である.*
(6) アーベル群は *$\mathbb{Z}$-module* である.

Lemma 3.1.2. *M が R-module ならば,*

(1) $a0 = 0x = 0$.
(2) $a(-x) = (-a)x = -ax$.
(3) $a(x-y) = ax - ay$, $(a-b)x = ax - bx$.

Definition 39. *M を an R-module とせよ. このとき N が M の R-submodule であるとは,*

(1) $\emptyset \neq N \subseteq M$,
(2) $^\forall x, y \in N$, $^\forall a \in R$ について $x+y, ax \in N$,

をみたすことをいう. このとき, N は *an R-module* である. これは ${}^{\forall}x \in N$ に対して $-x = (-1)x \in N$ であることによる.

Lemma 3.1.3. *M を R-module, $N \subseteq M$ を R-submodule とせよ. このとき M/N は, ${}^{\forall}a \in R$ に対して $a \rightharpoonup \overline{x} := \overline{ax}$ と作用を定義することにより R-module になる.*

Lemma 3.1.4. *$\varphi : L \to M$ を an R-linear map とせよ. すると $\mathrm{Ker}\,\varphi$ は L の R-submodule であって, $\mathrm{Im}\,\varphi$ は M の R-submodule である.*

Definition 40. *L, M を R-modules とする. $L \cong M$ as R-modules であるとは, ${}^{\exists}\varphi : L \to M$ an R-linear map s,t φ は bijection をみたすことである. このとき, L と M は本質的には同じ加群と思ってよい.*

Lemma 3.1.5. *$\varphi : L \to M$ を an R-linear map とせよ. すると $\mathrm{Im}\,\varphi \cong L/\mathrm{Ker}\,\varphi$ である.*

Theorem 3.1.6 (対応定理). *M を an R-module, $N \subseteq M$ を M の R-submodule とせよ. そして $\varepsilon : M \to M/N$ an R-linear map とするとき, ${}^{\exists}\Phi : \{X | X \text{ は } M \text{ の } R-submodule,\ N \subseteq X\} \to \{Y | Y \text{ は } M/N \text{ の } R-submodule\}$, $X \mapsto \varepsilon(X)$ s,t Φ は包含関係を保つような全単射である.*

次に, M は an R-module とし, $x_1, \cdots, x_n \in M$ $(n > 0)$ をとる.

$$N = \{a_1x_1 + \cdots + a_nx_n | a_i \in R\}$$

とおくと N は M の R-submodule である. この N を $x_1, \cdots, x_n$ で生成された M の R-submodule という. そして, $L \subseteq M$ を M の R-submodule としたとき, $x_i \in L$ $({}^{\forall}i) \Leftrightarrow N \subseteq L$ である. よって N は $x_1, \cdots, x_n$ を含む M の R-submodule の内で最小な部分加群であることがわかる. この N を,

$$N = Rx_1 + \cdots + Rx_n$$

とかく.

より, 一般には ${}^{\forall}S \subseteq M$ を M の部分集合としたとき $(S) = \bigcap_{\substack{N \text{ は } M \text{ の } R-submodule \\ S \subseteq N}}$ N は S で生成された M の R-submodule という. $S = \emptyset$ ならば $(S) = (0)$ であるし, $S \neq \emptyset$ ならば,

$$(S) = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; n > 0,\ a_i \in R,\ x_i \in S \right\}$$

である.

Example 3.1.7. *$n > 0$, $M = R^n$ とする. $1 \leq {}^{\forall}i \leq n$, e_i を $[e_i]_j = \delta_{ij}$ とせよ. すると $e_1, \cdots, e_n \in M$ であって $M = Re_1 + \cdots + Re_n$ である. 又, ${}^{\forall}f_1, \cdots, f_\ell \in M$ $({}^{\forall}\ell > 0)$, $N = Rf_1 + \cdots + Rf_\ell$ は M の R-submodule であって, $\overline{M} := M/N$ は an R-module であり, $\{R - modules\}$ は大きな class であるであることがわかる.*

Lemma 3.1.8. *$n > 0$, $\ell > 0$ とし $\varphi : R^\ell \to R^n$ が an R-linear map であれば $\varphi(e_j) = \sum_{i=1}^{n} a_{ij}e_i$ によって, 行列 $A = [a_{ij}] \in \mathrm{M}_{n\ell}(R)$ を定めると ${}^{\forall}x \in R^\ell$ について $\varphi(x) = Ax$ が成立する. 逆に, 行列 $A \in \mathrm{M}_{n\ell}(R)$ に対して $\psi(x) = Ax$ for ${}^{\forall}x \in R^\ell$ は an R-linear map である. 従って, 行列 $A \in \mathrm{M}_{n\ell}(R)$ と an R-linear map $\varphi : R^\ell \to R^n$ は 1 対 1 対応となっている.*

3.2 Submodules の operations

An R-module L を 1 つ固定する.

Lemma 3.2.1. $\Lambda \neq \emptyset$; *a set* とし $\{M_\lambda\}_{\lambda\in\Lambda}$ が L の *R-submodule* の族であるとき,

$$\bigcap_{\lambda\in\Lambda} M_\lambda\ ,\quad \sum_{\lambda} M_\lambda := \left\{ \sum_{\lambda\in\Lambda} x_\lambda \;\middle|\; x_\lambda \in M_\lambda\ ({}^\forall\lambda),\ \ x_\lambda = 0\ \ for\ almost\ all\ \lambda\in\Lambda \right\}$$

は L の *R-submodule* である. 例えば, M, N が L の *R-submodules* であるとき $M\cap N$, $M+N$ は L の *R-submodule* である.

Definition 41. $I \subseteq R$; *an ideal* について

$$IL := \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; n>0,\ a_i\in I,\ x_i \in L \right\}$$

は L の *R-submodule* である. とくに $I=(a)$ であるときは $IL = \{ax | x\in L\}$ を aL とかく.

Theorem 3.2.2.
(1) M, N が L の *R-submodule* であるとき,

$$\frac{M+N}{N} \cong \frac{M}{M\cap N} \quad as\ R-modules$$

である.
(2) $N\subseteq M$ が L の *R-submodules* であれば M/N は L/N の *R-submodule* であって, $\dfrac{L/N}{M/N} \cong L/N$ である.

Definition 42. $(0) :_R M := \left\{ a\in R | ax = 0\ \ for\ {}^\forall x\in M \right\}$ と定め, M の *the annihilator* とよび, $\mathrm{Ann}_R M$ と表すこともある. $\mathrm{Ann}_R M$ は R の *ideal* であって, $\mathrm{Ann}_R M = R \Leftrightarrow M = (0)$ である. もし I *an ideal of* R が $I\subseteq \mathrm{Ann}_R M$ であれば ${}^\forall\alpha\in R/I$, $\alpha = \overline{a}$ をとると, $\alpha \rightharpoonup x := ax$; ${}^\forall x\in M$ と作用を定義することによって M は R/I-*module* とみなせる.

Remark 3.2.3. $\varphi : R\to S$ が環の準同型写像であれば, ${}^\forall X\in S-\mathrm{mod}$ は R-*module* であり, $\alpha : X\to Y$ *an* S-*linear map* は R-*linear* でもある.

3.3 Exact sequences

R-modules の列,

$$\cdots \longrightarrow M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \longrightarrow \cdots$$

は $({}^\forall i)\ \mathrm{Im}\, f_{i+1} = \mathrm{Ker}\, f_i$ をみたすとき *exact* であるという. 完全列 $0\to X \longrightarrow X \longrightarrow Y \longrightarrow Z \to 0$ を a short exact sequence という. 全ての完全列は short exact sequence に分解可能である.

$\varphi : L \to M$ を an R-linear map とする. The map $i : \operatorname{Ker}\varphi \hookrightarrow L$ を自然な埋め込み (the inclusion) と呼び, $\operatorname{Coker}\varphi := M/\operatorname{Im}\varphi$ と表す. すると,

$$\begin{cases} 0 \to \operatorname{Ker}\varphi \to L \xrightarrow{\varphi} M \to \operatorname{Coker}\varphi \to 0 \\ 0 \to \operatorname{Ker}\varphi \to L \to \operatorname{Im}\varphi \to 0 \\ 0 \to \operatorname{Im}\varphi \to M \to \operatorname{Coker}\varphi \to 0 \end{cases}$$

は *exact* である.

Lemma 3.3.1. *$\varphi : L \to M$, $\psi : M \to X$ R-linear maps* とする. もし $\psi\varphi = 0$ ならば $^{\exists 1}\xi : \operatorname{Coker}\varphi \to X$ *an R-linear map s,t $\psi = \xi\varepsilon$,* ただし $\varepsilon : M \to \operatorname{Coker}\varphi$ *an R-linear map* である. つまり,

$$\begin{array}{ccc} L & \xrightarrow{\varphi} & M \\ & \searrow^{0} & \downarrow{\scriptstyle \psi} \\ & & X \end{array} \quad \Rightarrow \quad \begin{array}{ccc} M & \xrightarrow{\varepsilon} & \operatorname{Coker}\varphi \\ \downarrow{\scriptstyle \psi} & \swarrow_{^{\exists 1}\xi} & \\ X & & \end{array}$$

ということである.

Exercise 13 (Snake lemma). 次の可換図,

$$\begin{array}{ccccccccc} & & L_1 & \longrightarrow & M_1 & \longrightarrow & N_1 & \longrightarrow & 0 \quad \textit{exact} \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L_1 & \longrightarrow & M_1 & \longrightarrow & N_1 & & \textit{exact} \end{array}$$

を与えると $^{\exists}$*a exact sequence*; $\operatorname{Ker} f \to \operatorname{Ker} g \to \operatorname{Ker} h \xrightarrow{\Delta} \operatorname{Coker} f \to \operatorname{Coker} g \to \operatorname{Coker} h$.

3.4　直和と直積

$\{M_\lambda\}_{\lambda\in\Lambda}$ where $\Lambda \neq \emptyset$; a set, M_λ は R-module for $^{\forall}\lambda \in \Lambda$, とせよ. このとき,

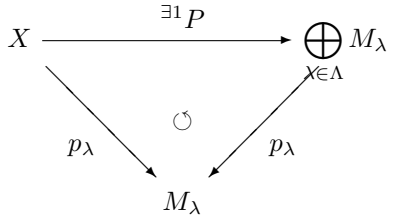
$$\prod_{\lambda\in\Lambda} M_\lambda := \left\{ (x_\lambda)_{\lambda\in\Lambda} \mid x_\lambda \in M_\lambda \quad for\ ^{\forall}\lambda \in \Lambda \right\}$$
$$\bigoplus_{\lambda\in\Lambda} M_\lambda := \left\{ (x_\lambda)_{\lambda\in\Lambda} \mid x_\lambda \in M_\lambda\ (^{\forall}\lambda),\ x_\lambda = 0 \quad for\ almost\ all\ \lambda \in \Lambda \right\} \subseteq \prod_{\lambda\in\Lambda} M_\lambda$$

と定め, それぞれ $\{M_\lambda\}_{\lambda\in\Lambda}$ の直積, 直和という.

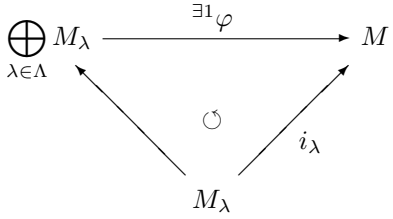
Lemma 3.4.1. *$X \in R-\operatorname{mod}$ をとり $^{\forall}\lambda \in \Lambda$, $f_\lambda : M_\lambda \to X$ an R-linear map* ならば

$$\begin{array}{ccc} \bigoplus_{\lambda\in\Lambda} M_\lambda & \xrightarrow{^{\exists 1}\Phi} & X \\ & \nwarrow^{\varphi_\lambda} \quad \circlearrowleft \quad \nearrow_{f_\lambda} & \\ & M_\lambda & \end{array}$$

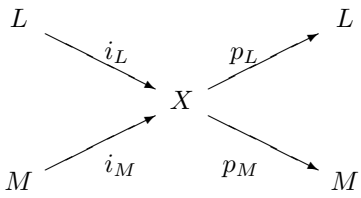
Lemma 3.4.2. $X \in R-\mathrm{mod}$ をとり ${}^{\forall}\lambda \in \Lambda$, $p_\lambda : X \to M_\lambda$ *an R-linear map* ならば



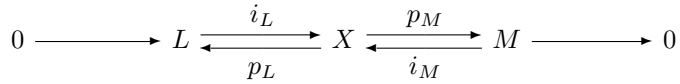
Remark 3.4.3. とくに $M_\lambda \subseteq M$ $({}^{\forall}\lambda \in \Lambda)$ のとき



この φ が単射であるとき $\{M_\lambda\}_{\lambda\in\Lambda}$ は M 内で直和をなす, という. この条件は $\sum_{\lambda\in\Lambda} x_\lambda = 0 \Rightarrow x_\lambda = 0$ *for* ${}^{\forall}\lambda \in \Lambda$, と同値であり, $M_\lambda \cap \sum_{\mu\neq\lambda} M_\mu = (0)$ $({}^{\forall}\lambda \in \Lambda)$ とも表せる. もし, この φ が同型射であるとき M は $\{M_\lambda\}_{\lambda\in\Lambda}$ の直和に分解するという. $|\Lambda| = 2$ のときを例にとる. $L, M \in R-\mathrm{mod}$, $X = L \oplus M$ とおく.



であるから



は *exact* であって, $p_L i_L = 1_L$, $p_M i_M = 1_M$ である.

Lemma 3.4.4. 完全列 $0 \to X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z \to 0$ について次は同値であり, このとき $Y \cong X \oplus Z$ となっていて, 完全列は *split* するという.

(1) ${}^{\exists}f : Y \to X$ *an R-linear map s,t* $f\alpha = 1_X$.
(2) ${}^{\exists}g : Z \to Y$ *an R-linear map s,t* $\beta g = 1_Z$.

Proof. (1)⇒(2) ${}^{\forall}y \in Y$, $y - \alpha(f(y)) \in \mathrm{Ker}\, f$. $\therefore Y = \mathrm{Ker}\, f \oplus \mathrm{Im}\, \alpha$. $\sigma : \mathrm{Ker}\, f \hookrightarrow X = \mathrm{Ker}\, f \oplus \mathrm{Im}\, \alpha \xrightarrow{\beta} Z$ は同型射である. $\therefore g : \xrightarrow{\sigma^{-1}} \mathrm{Ker}\, f \hookrightarrow X$ ととればよい.
(2)⇒(1) ${}^{\forall}y \in Y$, $y - g(\beta(y)) \in \mathrm{Ker}\, \beta$. $\therefore Y = \mathrm{Ker}\, \beta \oplus \mathrm{Im}\, g$. よって $f : Y \xrightarrow{p} \mathrm{Ker}\, \beta = \mathrm{Im}\, \alpha \xrightarrow{\sim} X$ とすればよい. □

第4章　Appendix

4.1　Appendix I (Tensor product)

R を a ring として M, N を R-modules とする.

Definition 43. *P を an R-module, $f : M \times N \to P$ を写像とする. f が an R-bilinear map であるとは,*

(1) $f(x + x', y) = f(x, y) + f(x', y)$,
(2) $f(x, y + y') = f(x, y) + f(x, y')$,
(3) $f(ax, y) = f(x, ay) = af(x, y)$,

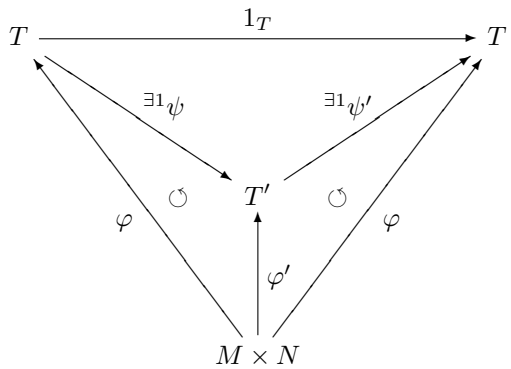
を全てみたすことをいう. 但し, $x, x' \in M$, $y, y' \in N$, $a \in R$ とする.

Theorem 4.1.1. *次に挙げる条件をすべてみたす a pair (T, φ) が同型を除いて唯一通りに存在する.*

(1) *T は an R-module.*
(2) *$\varphi : M \times N \to T$ は an R-bilinear map.*
(3) *P は R-module, $g : M \times N \to P$ は an R-bilinear map であるような任意の組 (P, g) に対して ${}^{\exists}\psi : T \to P$ an R-linear map s,t $g = \psi\varphi$.*

このような T を the tensor product of M and N とよび, $M \otimes_R N$ と表す.

Proof. (uniqueness) (T, φ), (T', φ') が上の条件をみたすとすれば,



をみて, $\psi'\psi = 1_T$ をうる. 同様にして $\psi\psi' = 1_{T'}$ をみたすことが示されるので, このような条件をみたす組は全て同型でることがわかる.

(existance) F を $\left\{e_{(x,y)}\right\}_{(x,y)\in M\times N}$ を R-free basis にもつ R-module とせよ. そして C を

$$\left\{\left.\begin{array}{c} e_{(x+x',y)}-e_{(x,y)}-e_{(x',y)} \\ e_{(x,y+y')}-e_{(x,y)}-e_{(x,y')} \\ e_{(ax,y)}-ae_{(x,y)} \\ e_{(x,ay)}-ae_{(x,y)} \end{array}\right| x,x'\in M,\quad y,y'\in N,\quad a\in R\right\}$$

で生成される F の R-submodule とせよ. そして $T:=F/C$ とおき, $\overline{e_{(x,y)}}:=x\otimes_R y$ とかくことにする. すると, 定義より ${}^\forall x,x'\in M$, ${}^\forall y,y'\in N$, ${}^\forall a\in R$ に対して

$$\begin{aligned}(x+x')\otimes_R y&=x\otimes_R y+x'\otimes_R y\\ x\otimes_R(y+y')&=x\otimes_R y+x\otimes_R y'\\ (ax)\otimes_R y&=x\otimes_R(ay)=a(x\otimes_R y)\end{aligned}$$

をみたす. 写像 $\varphi:M\times N\to T$, $(x,y)\mapsto x\otimes_R y$ は C の取り方から an R-bilinear であることは殆ど自明であって, P は R-module, $g:M\times N\to P$ は an R-bilinear map であるような組 (P,g) に対して ${}^{\exists 1}\alpha:F\to P$, $e_{(x,y)}\mapsto g((x,y))$ an R-linear map. 今, g を bilinear にとっている以上 $C\subseteq\operatorname{Ker}\alpha$ は明らか. $\therefore {}^{\exists 1}\psi:T\to P$ an R-linear s,t $g=\psi\varphi$. □

$M\otimes_R N$ は, その構成の仕方からみて ${}^\forall\alpha\in M\otimes_R N$ は,

$$\alpha=\sum_{i=1}^{n}x_i\otimes_R y_i\quad n>0;\ x_i\in M,\ y_i\in N$$

と書き出せる. もし $M'\subseteq M$; an R-submodule, $N'\subseteq N$; an R-submodule としたとき $M'\otimes_R N'$ を $M\otimes_R N$ の R-submodule として構成することができる. 今, $R=\mathbb{Z}$, $M=\mathbb{Z}$, $N=\mathbb{Z}/(2)$ として $M'=2\mathbb{Z}$ としよう. ${}^\forall x\in N$ に対して $2\otimes x\neq 0$ in $M'\otimes_R N$ ではあるが $2\otimes x=1\otimes 2x=0$ in $M\otimes_R N$ となる. つまり, $\alpha\neq 0$ in $M'\otimes_R N$ であっても $\alpha=0$ in $M\otimes_R N$ となるような例は簡単につくることができる.

Corollary 4.1.2. *$x_i\in M$, $y_i\in N$ を $\sum x_i\otimes_R y_i=0$ in $M\otimes_R N$ となるようにとれば, ${}^\exists M'\subseteq M$; an R-submodule of M, ${}^\exists N'\subseteq N$; an R-submodule of N s,t $\sum x_i\otimes_R y_i=0$ in $M'\otimes_R N'$.*

Proof. $\sum x_i\otimes_R y_i=0$ in $M\otimes_R N$ であるということは, $\sum e_{(x_i,y_i)}\in C$ である. 従って, $\sum e_{(x_i,y_i)}$ を表現するときに現れる第 1 成分すべての集合を $X\subset M$, $\sum e_{(x_i,y_i)}$ を表現するときに現れる第 2 成分すべての集合を $Y\subset N$, として $M'=RX$, $N'=RY$ とすればよい. □

Definition 44. *$n>0$, $M_1,\cdots,M_n$, P を R-modules とする. $f:M_1\times\cdots\times M_n\to P$ が an R-multi-linear* であるとは,

(1) $1\leq{}^\forall i\leq n$ に対して $f((x_1,\cdots,x_i+x_i',\cdots,x_n))=f((x_1,\cdots,x_i,\cdots,x_n))+f((x_1,\cdots,x_i',\cdots,x_n))$.
(2) $1\leq{}^\forall i\leq n$ に対して $f((x_1,\cdots,ax_i,\cdots,x_n))=af((x_1,\cdots,x_i,\cdots,x_n))$.

をみたすことをいう. 但し, $x_i\in M_i$ (${}^\forall i$), ${}^\forall a\in R$ である.

すると, この multi R-linear についても上のような Universal proparty が存在する. それは,

Theorem 4.1.3. 次に挙げる条件をすべてみたす *a pair (T,φ)* が同型を除いて唯一通りに存在する.

(1) T は *an R-module.*
(2) $\varphi : M_1 \times \cdots \times M_n \to T$ は *an R-multilinear map.*
(3) P は *R-module,* $g : M_1 \times \cdots \times M_n \to P$ は *an R-multilinear map* であるような任意の組 (P, g) に対して $^{\exists}\psi : T \to P$ *an R-linear map s,t* $g = \psi\varphi$.

このような T を *the tensor product of* $M_1, \cdots, M_{n-1}$ *and* M_n とよび, $M_1 \otimes_R \cdots \otimes_R M_n$ と表す.

Exercise 14. 次の *R-linear maps* は全て自然な同型写像であることを示せ.

$$(1)\quad \begin{array}{ccc} M \otimes_R N & \longrightarrow & N \otimes_R M \\ \cup & & \cup \\ m \otimes n & \longmapsto & n \otimes m \end{array} .$$

$$(2)\quad \begin{array}{ccccc} (L \otimes_R M) \otimes_R N & \longrightarrow & L \otimes_R M \otimes_R N & \longrightarrow & L \otimes_R (M \otimes_R N) \\ \cup & & \cup & & \cup \\ (\ell \otimes m) \otimes n & \longmapsto & \ell \otimes m \otimes n & \longmapsto & \ell \otimes (m \otimes n) \end{array} .$$

$$(3)\quad \begin{array}{ccc} \left(\bigoplus_{i\in I} M_i\right) \otimes_R N & \longrightarrow & \bigoplus_{i\in I}(M_i \otimes_R N) \\ \cup & & \cup \\ (m_i)_{i\in I} \otimes n & \longmapsto & (m_i \otimes n)_{i\in I} \end{array} .$$

$$(4)\quad \begin{array}{ccc} R \otimes_R M & \longrightarrow & M \\ \cup & & \cup \\ r \otimes m & \longmapsto & rm \end{array} .$$

さて, A a ring とする. N が *an (R, A) – bimodule* であるとは

(1) $N \in R - \mathrm{mod}$ かつ $N \in A - \mathrm{mod}$.
(2) $a(rn) = r(an)$ for all $r \in R$, $a \in A$, $n \in N$.

を満たすことをいう. 今, $M \in R - \mathrm{mod}$, $X \in A - \mathrm{mod}$ としたとき $M \otimes_R N$, $N \otimes_A X$ に自然に (R, A)-bimodule の構造が定まる. 更に次の $(R, A) - bimodule$ としての自然な同型

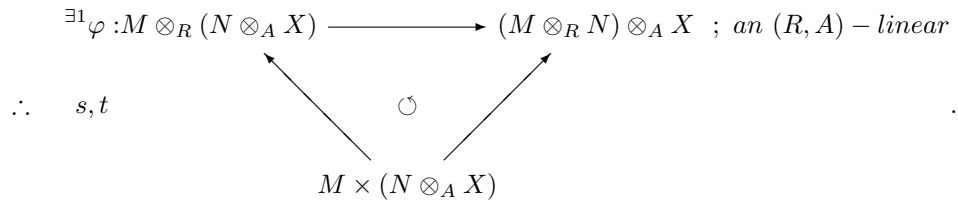
$$(M \otimes_R N) \otimes_A X \cong M \otimes_R (N \otimes_A X)$$

が存在する. これは次のように示される. $^{\forall}m \in M$ (fixed) をとり $f_m : N \times X \to (M \otimes_R N) \otimes_A X$, $(n, x) \mapsto (m \otimes n) \otimes x$ とおく. この f_m は an A-bilinear map であるから

$$\begin{array}{ccc} {}^{\exists 1}g_m : N \otimes_A X & \longrightarrow & (M \otimes_R N) \otimes_A X \ ;\ an\ A - linear \\ & \nwarrow \quad \circlearrowleft \quad \nearrow & \\ s, t & & \\ & N \times X & \end{array}$$

をうる. この g_m を用いると次のような an R-bilear map をとることができる.

$$\begin{array}{ccccc} h & : & M \times (N \otimes_A X) & \longrightarrow & (M \otimes_R N) \otimes_A X \\ & & \cup & & \cup \\ & & (m, \alpha) & \longmapsto & g_m(\alpha) \end{array} .$$



一方で, これと全く同様にして φ の逆写像となる an (R, A)-linear map $\psi : (M \otimes_R N) \otimes_A X \to M \otimes_R (N \otimes_A X)$, $(m \otimes n) \otimes x \mapsto m \otimes (n \otimes x)$ をつくることができる. よって上の同型をうる.

これより $f : R \to A$ は環の準同型写像とする. $^{\forall}X \in A - \mathrm{mod}$ に対して $r \rightharpoonup x := f(r)x$ とおくことによって X 上に自然に R-module の構造が定まる.

Proposition 4.1.4. *A は a f,g R-module, X は a f,g A-module であるならば $X \in fgMod(R)$ である.*

Proof. $\{a_i\}_{1 \le i \le n}$ を A の R-generator, $\{x_j\}_{1 \le j \le m}$ を X の A-generator としたとき $\{a_i x_j\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ をとればよい. □

$M \in R - \mathrm{mod}$, $X \in A - \mathrm{mod}$ として加法群の写像 $\varphi : M \to X$ をとる. この φ が $^{\forall}r \in R$, $\varphi(rm) = f(r)\varphi(m)$ をみたすとき $f - linear$ であるということにする. このとき,

Lemma 4.1.5 (Base change). *$^{\forall}$a pair (X, φ) where $X \in A - \mathrm{mod}$, $\varphi : M \to X$ an $f - linear$ に対して $^{\exists 1}\psi : A \otimes_R M \to X$ an A-linear map s,t $\varphi = \psi\varepsilon$.* ただし $\varepsilon : M \to A \otimes_R M$, $m \mapsto 1 \otimes m$ とする.

$M, N \in R - \mathrm{mod}$, $P \in R - \mathrm{mod}$ として

$$\mathcal{S} = \{f | f : M \times N \to P \ \ an\ R - bilinear\ map\}$$

とおく. $^{\forall}f, g \in \mathcal{S}$, $^{\forall}r \in R$ に対して $\alpha \in M \times N$ をとり,

$$\begin{aligned} (f+g)(\alpha) &:= f(\alpha) + g(\alpha) \\ (r \rightharpoonup f)(\alpha) &:= rf(\alpha) \end{aligned}$$

と定めることによって $\mathcal{S}$ は an R-module になる. そして,

Lemma 4.1.6.

$$\mathcal{S} \underset{canon}{\cong} \mathrm{Hom}_R(M \otimes_R N, P) \quad in \quad R - \mathrm{mod}.$$

これは, tensor の universal property をみれば自明である. 一方で, 次のような自然な同型も存在する.

Lemma 4.1.7.

$$\mathcal{S} \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

Exercise 15. 上の補題を証明せよ.

従って, $\mathrm{Hom}_R(M \otimes_R N, P) \underset{canon}{\cong} \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$ をうる.

Proposition 4.1.8. *$N \in R - \mathrm{mod}$ とする. 次は同値である.*

(1) $^{\forall}$*exact in* $R-\mathrm{mod}$; $0\to M_1\xrightarrow{f}M_2\xrightarrow{g}M_3\to 0$ に対して $0\to N\otimes_R M_1\xrightarrow{N\otimes f}N\otimes_R M_2\xrightarrow{N\otimes g}N\otimes_R M_3\to 0$ は *exact* である.
(2) $^{\forall}$*exact in* $R-\mathrm{mod}$; $0\to M_1\xrightarrow{f}M_2$ に対して $0\to N\otimes_R M_1\xrightarrow{N\otimes f}N\otimes_R M_2$ は *exact* である.
(3) $^{\forall}$*exact in* $\underline{\underline{\mathrm{M}}}(R)$; $0\to M_1\xrightarrow{f}M_2$ に対して $0\to N\otimes_R M_1\xrightarrow{N\otimes f}N\otimes_R M_2$ は *exact* である.

このような N を *a flat R-module* という.

証明は (3) $\Rightarrow$ (2) だけを言えばよいのだが, これは $^{\forall}\alpha\in\mathrm{Ker}\,N\otimes f$ に対して $\alpha=\sum x_i\otimes y_i$ where $x_i\in N$, $y_i\in M_1$ と表したとき $M_1'=\sum Ry_i\subseteq M_1$ と, $N\otimes f(\alpha)=\sum x_i\otimes f(y_i)=0$ in $N\otimes_R M_2$ について $\sum x_i\otimes f(y_i)=0$ in $N\otimes_R M_2'$ となる $M_2'\subseteq M_2$; a f,g R-submodule of M_2 をとり, $0\to M_1'\to M_2'$ に制限して考えればよい.

Exercise 16. $f:R\to A$ を *a ring homom* とせよ. M が *a flat R-module* ならば $A\otimes_R M$ は *a flat A-module* であることを証明せよ.

R を a ring とする. A が環であって a ring homom $f:R\to A$ が一つ指定されているとき, A は *an* $R-$*algebra* であるといって f はその構造射であるという. そして今, A, B を R-algebra としてその構造射を f, g とする. このとき, 環の準同型写像 $h:A\to B$ が *an* $R-$*algrbra map* であるとは $g=hf$ をみたすことをいう.

4.2 Appendix II (Integral dependence と Valuation rings)

さて, しばらくは $R\subseteq A$; rings とする. $x\in A$ が *integral over* R であるとは, $a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n=0$ for some $n>0$; $a_i\in R$ であることをいう. 従って $^{\forall}r\in R$ が integral over R であることは自明である.

Proposition 4.2.1. 次は同値である.

(1) $x\in A$ は *integral over R.*
(2) $R[x]$ は *a* f,g *R-module.*
(3) $^{\exists}B\subseteq A$; *subring s,t* $R[x]\subseteq B$, B は *a* f,g *R-module.*
(4) $^{\exists}M$; *a faithfull* $R[x]$*-module s,t* M は *an R-module.*

ただし, M が *faithfull* $R[x]$*-module* であるとは, $(0)\underset{R[x]}{:}M=(0)$ をみたすことをいう.

Proof. (1)$\Rightarrow$(2) $R[x]=R+Rx+\cdots+Rx^{n-1}$ と表せる.
(2)$\Rightarrow$(3) $B=R[x]$ とすればよい.
(3)$\Rightarrow$(4) $M=B$ とすればよい.
(4)$\Rightarrow$(1) $\widehat{x}:M\to M$ をみる. $M\in\underline{\underline{\mathrm{M}}}(R)$ であるから $\widehat{x}^n+a_{n-1}\widehat{x}^{n-1}+\cdots+a_0=0$ ($n>0$; $a_i\in R$) をうる. $\therefore{}^{\forall}m\in M$, $0=\left(\widehat{x}^n+a_{n-1}\widehat{x}^{n-1}+\cdots+a_0\right)(m)=(x^n+a_{n-1}x^{n-1}+\cdots+a_0)m$. 今, M は $R[x]-faithfull$ であったので $x^n+a_{n-1}x^{n-1}+\cdots+a_0=0$ をうる. □

Corollary 4.2.2. $x_1,\cdots,x_n\in A$ が *integral over* R であれば $R[x_1,\cdots,x_n]$ は *a f,g R-module* である.

Corollary 4.2.3. $\overline{R} := \{x \in A | x$ は *integral over* $R\}$ とすると, $\overline{R}$ は R を部分環に含むような A の部分環である. この $\overline{R}$ を *the integral closure of* R *in* A という. 今もし, $R = \overline{R}$ であれば R を *integrally closed in* A, $\overline{R} = A$ であれば A を *integral over* R, という. これからは, R が *integrally closed in* A であるとき $R = \overline{R}$ (どこで整拡大かを表に出したいときは $R = \overline{R}^A$とかく.), A が *integral over* R であるとき A/R; *integral*, とそれぞれ表すこともある.

Proof. $x, y \in \overline{R}$ をとる. すると, $R[x, y]$ は a f,g R-module であって $R[x \pm y], R[xy] \subseteq R[x, y]$ であるから $x \pm y, xy \in \overline{R}$. □

Proposition 4.2.4. $R \subseteq AsubseteqB$; *rings* とする. A/R, B/A が *integral* ならば B/R も *integral* である.

Proposition 4.2.5. $\overline{R}$ は *integrally closed in* A.

Proof. B を the integral closure of $\overline{R}$ in A とすれば, $B/\overline{R}$, $\overline{R}/R$ は integral なので B/R は integral.
$\therefore B = \overline{R}$. □

Proposition 4.2.6. A/R; *integral* とする.

(1) $I \subsetneq A$; *an ideal of* $A \Rightarrow A/I$ は *integral over* $R/(I \cap R)$.
(2) $S \subseteq R$; *multi closed of* $R \Rightarrow S^{-1}A$ は *integral over* $S^{-1}R$.

Proof. (1) $^\forall\alpha \in A/I$ をとり, $\alpha = \bar{a}$ とかく. A/R; integral であるから, $^\exists f \in R[X]$ s,t f は monic であって $f(a) = 0$. すると $0 = \overline{f(a)} = \overline{f}(\alpha)$ in $(R/I \cap R)$. 今, $\overline{f} \in \dfrac{R}{I \cap R}\left[\overline{X}\right]$ は monic polynomial である.
(2) $^\forall\alpha \in S^{-1}A$ をとる. すると, $^\exists s \in S$ s,t $s\alpha \in A$ であるから $^\exists f \in R[X]$ s,t f は monic であって $f(s\alpha) = 0$. $f(X) = X^n + r_1X^{n-1} + \cdots + r_n$ と表すと

$$0 = (s\alpha)^n + r_1(s\alpha)^{n-1} + \cdots + r_n = \frac{1}{s^n}\left\{\alpha^n + \frac{r_1}{s^n}\alpha + \cdots + \frac{r_n}{s^n}\right\}$$

をうる. □

Lemma 4.2.7. A は *domain*, A/R; *integral* とする. このとき, A が体であるための必要十分条件は R が体である.

Proof. A が体を仮定する. $0 \neq {}^\forall x \in R$ をとる. $x \neq 0$ in A であるから $^\exists x^{-1} \in A$, $^\exists f = X^n + r_1X^{n-1} + \cdots + r_n \in R[X]$ s,t $f(x^{-1}) = 0$. よって, $x^{-n} = -\left(r_1x^{-n+1} + \cdots + r_n\right)$ となるが, 両辺を x^n 倍すれば, $1 = (-1)x(r_1 + \cdots + r_nx^{n-1})$ をうる. 逆に, R が体を仮定しよう. $0 \neq {}^\forall x \in A$ をとる. $x \notin R$ としてよい.
$\therefore {}^\exists f = X^n + r_1X^{n-1} + \cdots + r_n \in R[X]$ s,t $n > 1$ であって $f(x) = 0$. この f は $r_n \neq 0$ にとれるので, $1 = r_nr_n^{-1} = -r_n^{-1}\left(x^{n-1} + r_1x^{n-2} + \cdots + r_{n-1}\right)x$ をうる. □

Corollary 4.2.8. A/R; *integral*, $P \in \operatorname{Spec} A$ とする. $P \in \operatorname{Max} A$ であるための必要十分条件は $\mathfrak{p} := P \cap R \in \operatorname{Max} R$ である.

Corollary 4.2.9. A/R; *integral*, $P_1, P_2 \in \operatorname{Spec} A$ とする. もし, $P_1 \subseteq P_2$ かつ $P_1 \cap R = P_2 \cap R$ ならば $P_1 = P_2$ である.

Proof. $\mathfrak{p} = P_1 \cap R = P_2 \cap R$ とおく. すると, $A_\mathfrak{p}/R_\mathfrak{p}$; integral である. このとき $P_1 A_\mathfrak{p} \subseteq P_2 A_\mathfrak{p}$, $P_1 A_\mathfrak{p} \cap R_\mathfrak{p} = P_2 A_\mathfrak{p} \cap R_\mathfrak{p} = \mathfrak{p} R_\mathfrak{p}$ をみたす. $\therefore P_1 A_\mathfrak{p}, P_2 A_\mathfrak{p} \in \operatorname{Max} A_\mathfrak{p}$. $\therefore P_1 = P_2$. □

Theorem 4.2.10 (Lying over theorem). *A/R; integral とする. $^\forall\mathfrak{p} \in \operatorname{Spec} R$ に対して $^\exists P \in \operatorname{Spec} A$ s,t $\mathfrak{p} = P \cap R$.*

Proof. $A_\mathfrak{p}/R_\mathfrak{p}$; integral である. 今, $\mathfrak{m} \in \operatorname{Max} A_\mathfrak{p}$ をとると $\mathfrak{m} \cap R_\mathfrak{p} \in \operatorname{Max} R_\mathfrak{p}$. $\therefore \mathfrak{m} \cap R_\mathfrak{p} = \mathfrak{p} R_\mathfrak{p}$ となり $(\mathfrak{m} \cap R_\mathfrak{p}) \cap R = \mathfrak{p} R_\mathfrak{p} \cap R = \mathfrak{p}$ である. 一方で, $(\mathfrak{m} \cap R_\mathfrak{p}) \cap R = (\mathfrak{m} \cap A) \cap R = \mathfrak{p}$, $\mathfrak{m} \cap A \in \operatorname{Spec} A$ も明らか. この $\mathfrak{m} \cap A$ が求める A の prime ideal である. □

Proposition 4.2.11 (Going-up). *A/R; integral とする. $P_1 \in \operatorname{Spec} A$, $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} R$ が $\mathfrak{p}_1 = P_1 \cap R$, $\mathfrak{p}_1 \subseteq fkp_2$ であるならば $^\exists P_2 \in \operatorname{Spec} A$ s,t $P_1 \subseteq P_2$, $\mathfrak{p}_2 = P_2 \cap R$.*

Proof. A_{P_1} は $R_{\mathfrak{p}_1}$ 上 integral であった. $\therefore \mathfrak{p}_2/\mathfrak{p}_1 \in \operatorname{Spec} R/\mathfrak{p}_1$ に対して $^\exists Q \in \operatorname{Spec} A/P_1$ s,t $Q \cap R/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. そして, Q に対して $^\exists P \in \operatorname{Spec} A$ s,t $Q = P/P_1$. この P が求める prime ideal である. □

これまでと同じように $R \subseteq A$ rings としよう.

Proposition 4.2.12. *S を R の multi closed としたとき,*

$$S^{-1}\left(\overline{R}^A\right) = \overline{S^{-1}R}^{S^{-1}A}$$

が成り立つ.

Proof. $\overline{R}^A$ は R 上 integral であるから $S^{-1}\left(\overline{R}^A\right)$; integral, $\therefore S^{-1}\left(\overline{R}^A\right) \subseteq \overline{S^{-1}R}^{S^{-1}A}$. $^\forall\alpha \in \overline{S^{-1}R}^{S^{-1}A}$ をとると, その定義から $S^{-1}R[X]$ の monic polynomial で α を代入して 0 になるものが存在し, それを

$$\alpha^n + \frac{r_1}{s}\alpha^{n-1} + \cdots + \frac{r_n}{s} = 0 \quad for\ some\ r_i \in R,\ s \in S$$

と表す. もともと $\alpha \in S^{-1}A$ であるから $^\exists u \in S$ s,t $u\alpha \in A$, $\dfrac{ur_i}{s} = \dfrac{r_i'}{1}$. この r_i' を改めて r_i とおく. よって,

$$\begin{aligned} 0 &= \frac{u^n}{1}\left\{\alpha^n + \frac{r_1}{s}\alpha^{n-1} + \cdots + \frac{r_n}{s}\right\} \\ &= \left(\frac{u\alpha}{1}\right)^n + \frac{ur_1}{s}\left(\frac{u\alpha}{1}\right)^{n-1} + \cdots + \frac{u^n r_n}{s} \\ &= \left(\frac{u\alpha}{1}\right)^n + \frac{r_1}{1}\left(\frac{u\alpha}{1}\right)^{n-1} + \cdots + \frac{u^{n-1} r_n}{1} \\ &= \frac{(u\alpha)^n + r_1(u\alpha)^{n-1} + \cdots + r_n u^{n-1}}{1} \end{aligned}$$

$\therefore {}^\exists v \in S$ s,t $0 = v^n\left\{(u\alpha)^n + r_1(u\alpha)^{n-1} + \cdots + r_n u^{n-1}\right\} = (vu\alpha)^n + vr_1(vu\alpha)^{n-1} + \cdots + r_n u^{n-1} v^n$.
$\therefore uv\alpha \in \overline{R}^A$. $\therefore \alpha = \dfrac{uv\alpha}{uv} \in S^{-1}\left(\overline{R}^A\right)$. $\therefore S^{-1}\left(\overline{R}^A\right) = \overline{S^{-1}R}^{S^{-1}A}$. □

ここで, 言葉を一つ定義しよう.

Definition 45. *R は domain とする. R が integrally closed in $\mathbb{Q}(R)$ であるときは, 単に R は integrally closed である, ということにする.* (本によっては *normal domain* と呼ぶものもある.) *例えば, $\mathbb{Z}$ は integrally closed の代表的な例である.*

Exercise 17. $\mathbb{Z}$ が *integrally closed* であることを証明せよ.

Lemma 4.2.13. R は *domain* とせよ. 次は同値である.

(1) R は *integrally closed.*
(2) $^\forall\mathfrak{p} \in \operatorname{Spec} R$ に対して $R_\mathfrak{p}$ は *integrally closed.*
(3) $^\forall\mathfrak{m} \in \operatorname{Max} R$ に対して $R_\mathfrak{m}$ は *integrally closed.*

Proof. (1)⇒(2) は少し考えると殆ど自明であって, (2)⇒(3) は自明. よって (3)⇒(1) のみ. $f : R \to \left(\overline{R}\right)$ とする. 上の補題より, $\left(\overline{R}\right)_\mathfrak{m} = \overline{R_\mathfrak{m}}$ であって, 一方で仮定より $f_\mathfrak{m}$ は identity. $\therefore f$ は identity. □

$I \subseteq R$; an ideal of R とする. $x \in A$ が *integral over* I であるとは, $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some $n > 0$; $a_i \in I$, をみたすことをいう. さらに, $\{x \in A | x$ は *integral over* $I\}$ のことを *integral closure of* I *in* A という. これが I を含むことは自明であろう.

Lemma 4.2.14. $I \subseteq R$; *an ideal of* R とするとき,

$$\sqrt{I \cdot \overline{R}^A} = \{x \in A | x \text{ は } integral\ over\ I\}$$

が成り立つ.

Proof. $x \in A$ を integral over I にとる. すると, $x \in \overline{R}^A$ であって $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some $n > 0$; $a_i \in I$, をみたす. $\therefore x^n = -(a_1x^{n-1} + \cdots + a_n) \in I \cdot \overline{R}^A$, $x \in \sqrt{I \cdot \overline{R}^A}$.
$^\forall x \in \sqrt{I \cdot \overline{R}^A}$ をとる. $x^\ell \in I \cdot \overline{R}^A$ $(\ell > 0)$ より $x^\ell = \sum_{i=1}^{m} a_ix_i$ $(a_i \in I,\ x_i \in \overline{R}^A)$ と表すと, $x_i \in \overline{R}^A$ であるから $R[x_1, \cdots, x_m]$ は R 上有限生成加群である. 今, $\widehat{x^\ell} : R[x_1, \cdots, x_m] \to R[x_1, \cdots, x_m]$ をみると $\operatorname{Im} \widehat{x^\ell} \subseteq I \cdot R[x_1, \cdots, x_m]$. $\therefore {}^\exists zero-map;\ \widehat{x^\ell}^r + b_1\widehat{x^\ell}^{r-1} + \cdots + b_r$ for some $r > 0$. これに $1 \in R[x_1, \cdots, x_m]$ を代入すれば求める結果をうる. □

Definition 46. $K \subseteq L$ を体の拡大とせよ. $x \in L$; *algebraic over* K をとり, $f_x : K[X] \to K[x]$ *the* K*-algebra map* としたとき $g \in K[X]$ が x の *the minimal polynomial* であるとは, $\operatorname{Ker} f_x = (g)$ を満たすことをいう. 従って, $K[X]$ が *PID* であったことから, 上のことは $h \in K[X]$ の元で $h(x) = 0$ をみたすものの内で最小の次数のものであることと同値である.

Lemma 4.2.15. A は *domain,* R は *integrally closed,* $I \subseteq R$; *an ideal* として $x \in A$ を *integral over* I にとる.

(1) x は *algebraic over* $\mathbb{Q}(R)$.
(2) x の $\mathbb{Q}(R)$ 上の *the minimal polynomial* を $t^n + a_1t^{n-1} + \cdots + a_n$ とすると $a_1, \cdots, a_n \in \sqrt{I}$.

Proof. (1) は自明. (2) を示す. $x_1, \cdots, x_n$ を x の共役元として L を $x_1, \cdots, x_n \in L$ となる $\mathbb{Q}(R)$ の拡大体とする. すると, $x_1, \cdots, x_n$ は integral over I であり, $a_1 = -(x_1 + \cdots + x_n), \cdots, a_n = (-1)^n x_1 \cdots x_n$ であるから $a_1, \cdots, a_n \in \{a \in \mathbb{Q}(R) | a$ は *integral over* $I\} = \sqrt{I \cdot \overline{R}} = \sqrt{I}$. □

Proposition 4.2.16 (Going-down). A は *domain,* A/R; *integral,* R は *integrally closed* とせよ. $P_1 \in \operatorname{Spec} A$, $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec} R$ が $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$, $\mathfrak{p}_1 = P_1 \cap R$ であるならば ${}^\exists P_2 \in \operatorname{Spec} A$ *s,t* $\mathfrak{p}_2 = P_2 \cap R$, $P_2 \subseteq P_1$.

Proof. 今, $\mathfrak{p}_2 A_{P_1} \cap R = \mathfrak{p}_2$ が成り立つとする. このとき $^{\exists}Q \in \operatorname{Spec} A_{P_1}$ s,t $Q \cap R = \mathfrak{p}_2$. 又, Q は次を満たす.

$$(1)\ Q \cap A \in \operatorname{Spec} A, \quad (2)\ (Q \cap A) \cap R = \mathfrak{p}_2, \quad (3)\ Q \cap A \subseteq P_1.$$

このことから $P_2 = Q \cap A$ とすればよい. 従って, $\mathfrak{p}_2 A_{P_1} \cap R = \mathfrak{p}_2$ だけを示せば十分. $\mathfrak{p}_2 A_{P_1} \cap R \supseteq \mathfrak{p}_2$ は自明である. $0 \neq {}^{\forall}x \in \mathfrak{p}_2 A_{P_1} \cap R$ をとる. $x \in \mathfrak{p}_2 A_{P_1} \subseteq \mathbb{Q}(A)$ より $x = \dfrac{a}{s}$ where $a \in \mathfrak{p}_2 A$, $s \in A \backslash P_1$ とかく. このとき, a は integral over $\mathfrak{p}_2$ であるから a の $\mathbb{Q}(A)$ 上の the minimal polynomial

$$f(t) = t^n + u_1 t^{n-1} + \cdots + u_n \quad u_i \in \mathbb{Q}(A)$$

をとる. 上の補題から $u_i \in \mathfrak{p}_2$ である. ここで, $s = \dfrac{a}{x}$ より $g = \dfrac{f}{x^n}$ は s の $\mathbb{Q}(A)$ 上の the minimal polymnomial になる. $\therefore v_i = \dfrac{u_i}{x^i} \in R$. よって, $x^i, v_i \in R$ であって $\mathfrak{p}_2 \ni u_i = x^i v_i$ より $x \in \mathfrak{p}_2$ or $v_i \in \mathfrak{p}_2$ である. もし, $x \notin \mathfrak{p}_2$ ならば $v_i \in \mathfrak{p}_2$ であるから $s \in P_1$. (矛盾) $\therefore x \in \mathfrak{p}_2$. □

Proposition 4.2.17. *R は integrally closed, $K = \mathbb{Q}(R)$ とする. さらに L; K の finite algebraic separable extension としたとき, $^{\exists}v_1, \cdots, v_n$; L の K-basis s,t $\overline{R}^L \subseteq \sum_{i=1}^{n} Rv_i$.*

これは, ここでは証明の筋道だけを紹介することにしよう. まず, $L = \mathbb{Q}\left(\overline{R}^L\right)$ を示すことから始まる. 次に L の K-basis $\{v_1, \cdots, v_n\}$ をとるのだが, これは $v_i \in \overline{R}^L$ としてよい. ここで, $f : L \times L \to K$, $(x, y) \mapsto Tr(xy)$ と定めると,

(1) f は K-bilinear map である.
(2) f は non-degenerated である.

を満たすので, $\{v_1, \cdots, v_n\}$ の K-dual basis $\{w_1, \cdots, w_n\}$ をとり, この $\{w_1, \cdots, w_n\}$ が $\overline{R}^L \subseteq \sum_{i=1}^{n} Rw_i$ をみたしていることを言えばよい.

以下, R は domain であって $K = \mathbb{Q}(R)$ とする.

Definition 47. *$0 \neq {}^{\forall}x \in K$ に対して, $x \in R$ か又は $x^{-1} \in R$ であるとき, R は a valuation ring であるという.*

Lemma 4.2.18. *R は a valuation ring とする.*

(1) *R は a local ring である.*
(2) *R' が R を含むような K の部分環であれば R' も a valuation ring である.*
(3) *R は integrally closed である.*

Proof. (2) は自明である. $I = R \backslash \mathrm{U}(R)$ とおく. $^{\forall}x, y \in I$, $^{\forall}a \in R$ をとる. 今, $x, y \neq 0$ としてよい. $ax \notin I$ ならば $^{\exists}u \in \mathrm{U}(R)$ s,t $u(ax) = 1$. $\therefore (ua)x = 1$, $x \in \mathrm{U}(R)$ となり矛盾であるから $ax \in I$ である. 一方で, $0 \neq xy^{-1} \in K$ であったので $xy^{-1} \in R$ or $x^{-1}y \in R$. $xy^{-1} \in R$ ならば $x + y = y(xy^{-1} + 1)$ となるからすぐ上のことから $x + y \in I$ をうる. 同様にして $x^{-1}y \in R$ のときも $x + y \in I$ をみたす. よっ

て, R は local ring である. 次に $\overline{R}^K = R$ を示す. $0 \neq {}^\forall x \in K$ をとる. $x \in R$ or $x^{-1} \in R$ であるから, もし $x \in R$ ならば十分である. よって $x^{-1} \in R$ としてみよう. $x \in K$ は R 上 integral であるから $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ for some $n > 0$; $a_i \in R$ である. $\therefore x^n = -(a_1 x^{n-1} + \cdots + a_n)$ より $x = x^n \cdot x^{-n+1} = -(a_1 x^{n-1} + \cdots + a_n)x^{-n+1} = -(a_1 + \cdots + a_n x^{-n+1}) \in R$. □

上のことから, a valuation ring の大まかな性質は分かったと思ってここからは, その存在について議論をしよう. Ω を an algebraic closed field, $\varphi : R \to \Omega$ a ring homom を与えて,

$$\mathcal{S} := \left\{ (A, f) \,\middle|\, \begin{array}{l} A \text{ は } R \text{ を含む } K \text{ の部分環, } f : A \to \Omega \text{ 環の準同型写像,} \\ i : R \hookrightarrow A \text{ ; } \textit{the inclusion map} \text{ としたとき} \varphi = fi \end{array} \right\}$$

とおく. この $\mathcal{S}$ に次のような順序を定義しよう.

$$(A, f) \leq (B, g) \overset{\text{def}}{\Leftrightarrow} {}^\exists i : A \hookrightarrow B \;\; \textit{the inclusion } s, t \;\; f = gi$$

Exercise 18. $(\mathcal{S}, \leq)$ は順序集合であることを示せ. そして $\mathcal{S}$ は *an inductive set* であることを示せ.

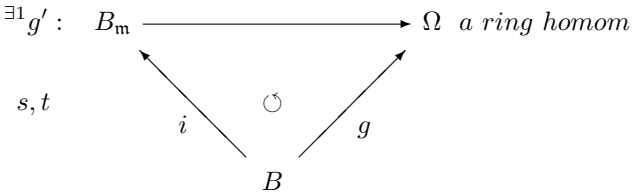
従って, *Zorn's Lemma* から ${}^\exists (B, g) \in \mathcal{S}$; maximal element をうる. 以下, (B, g) は $\mathcal{S}$ の a maximal element とせよ. これから私たちが証明したいことは

$$B \text{ は } \textit{a valuation ring} \text{ である,}$$

という事実で, これをいうために少し補題を用意しよう.

Lemma 4.2.19. $\mathfrak{m} = \operatorname{Ker} g$ とおくと, $(B, \mathfrak{m})$ は *local ring* である.

Proof. $B/\mathfrak{m} \cong g(B) \subseteq \Omega$ より $\mathfrak{m} \in \operatorname{Spec} B$ をうる. ${}^\forall s \in B \backslash \mathfrak{m}$ に対して $g(s) \neq 0$ より



$B_\mathfrak{m} \subseteq K$ であるから $(B_\mathfrak{m}, g') = (B, g)$. $\therefore (B, \mathfrak{m})$ は local ring である. □

Lemma 4.2.20. $0 \neq {}^\forall x \in K$, $\mathfrak{m}B[x] \neq B[x]$ *or* $\mathfrak{m}B[x^{-1}] \neq B[x^{-1}]$.

Proof. $\mathfrak{m}B[x] = B[x]$ かつ $\mathfrak{m}B[x^{-1}] = B[x^{-1}]$ であるとせよ. このとき

$$\begin{cases} 1 = u_0 x^\ell + u_1 x^{\ell-1} + \cdots + u_{\ell-1} x + u_\ell & \ell > 0;\ u_i \in \mathfrak{m} \\ 1 = v_0 x^{-n} + v_1 x^{-n+1} + \cdots + v_{n-1} x^{-1} + v_n & n > 0;\ v_i \in \mathfrak{m} \end{cases}$$

と ℓ, n がそれぞれ最小になるように表せる. $\ell \geq n$ とせよ. すると $x^n = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ より $x^n = v_0' + v_1 x + \cdots + v_{n-1}' x^{n-1}$ where $v_i' = v_i(1 - v_n)^{-1}$. $\therefore x^\ell = x^{\ell-n} x^n = x^{\ell-n}(v_0' + v_1 x + \cdots + v_{n-1}' x^{n-1}) = v_0' x^{\ell-n} + v_1 x^{\ell-n+1} + \cdots + v_{n-1}' x^{\ell-1}$. となり n の最小性に反する. $n \geq \ell$ のときは上と同様にして ℓ の最小性に反することがわかる. □

Theorem 4.2.21. B は *a valuation ring* である.

Proof. $0 \neq {}^{\forall}x \in K$ をとる. このとき $\mathfrak{m}B[x] \neq B[x]$ or $\mathfrak{m}B[x^{-1}] \neq B[x^{-1}]$ であるが, 実は, $\mathfrak{m}B[x] \neq B[x]$ として $x \in B$ を示せば十分である. よって $\mathfrak{m}B[x] \neq B[x]$ を仮定する. ${}^{\exists}M \in \operatorname{Max} B[x]$ s,t $\mathfrak{m}B[x] \subseteq M$. まず $M \cap B = \mathfrak{m}$ を確かめよう. $M \cap B \neq B$ より $M \cap B \subseteq \mathfrak{m}$ は明らか. そして $M \cap B \supseteq \mathfrak{m}B[x] \cap B \supseteq \mathfrak{m}$ より $M \cap B = \mathfrak{m}$ をうる. よって,

$$\begin{array}{ccccc} B/\mathfrak{m} & \longrightarrow & B[x]/M & \ni & \overline{x} \\ \uparrow{\scriptstyle \varepsilon} & \circlearrowleft & \uparrow{\scriptstyle \varepsilon} & & \uparrow \\ B & \longrightarrow & B[x] & \ni & x \end{array}$$

となる. このとき $B[x]/M = (B/\mathfrak{m})[\overline{x}]$ であるから $\overline{x}$ は $B/\mathfrak{m}$ 上代数的である. また,

$$\begin{array}{ccccc} 0 & \longrightarrow & B/\mathfrak{m} & \xrightarrow{{}^{\exists}\overline{g}} & \Omega \ \ a\ ring\ hom \\ & & \uparrow{\scriptstyle i} & \nearrow{\scriptstyle g} & \\ & & B & & \end{array}$$

である. よって,

$$\begin{array}{ccccc} 0 & \longrightarrow & B/\mathfrak{m}[\overline{x}] & \xrightarrow{{}^{\exists}\overline{g}'} & \Omega \ \ a\ ring\ hom \\ & & \uparrow{\scriptstyle i} & \nearrow{\scriptstyle \overline{g}} & \\ & & B/\mathfrak{m} & & \end{array}$$

となるから,

$$\begin{array}{ccccc} B[x] & \xrightarrow{\varepsilon} & (B/\mathfrak{m})[\overline{x}] & \xrightarrow{\overline{g}'} & \Omega \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} & \nearrow{\scriptstyle \overline{g}} & \\ B & \xrightarrow[\varepsilon]{} & B/\mathfrak{m} & & \end{array}$$

をみて $B = B[x]$. $\therefore x \in B$. □

Corollary 4.2.22. $\overline{R}^K = \bigcap_{\substack{B\ は\ valuation\ ring\ of\ K \\ R \subseteq B}} B.$

Proof. $R \subseteq B \Rightarrow \overline{R}^K \subseteq \overline{B}^K = B$. $\therefore \overline{R}^K \subseteq \bigcap B$ は明らか. ${}^{\exists}x \in \bigcap B \backslash \overline{R}$ とすれば $x \notin R[x^{-1}]$ であるから $x^{-1} \notin \mathrm{U}(R[x^{-1}])$. $\therefore {}^{\exists}M \in \operatorname{Max} R[x^{-1}]$ s,t $x^{-1} \in M$. ここで, $\Omega = \overline{R[x^{-1}]/M}$ として $f : R[x^{-1}] \to R[x^{-1}]/\mathfrak{m} \hookrightarrow \Omega$ とする. すると, ${}^{\exists}(B, g) \in \mathcal{S}$; maximal element s,t $(R[x^{-1}], f) \leq (B, g)$. すると, $g(x^{-1}) \neq 0$ であるが $f(x^{-1}) = 0$ であるから矛盾. □

Proposition 4.2.23. *A は domain, finitely generated R-algebra で $i : R \hookrightarrow A$ を the inclusion map とする. $0 \neq v \in A$ に対して $0 \neq {}^{\exists}u \in R$ with this condition*

$$f : R \to \Omega \text{ は } f(u) \neq 0 \text{ であるような環の準同型写像を与えると}$$
$${}^{\exists}g : A \to \Omega \quad s,t\ g(v) \neq 0 \text{ であって } f = g \cdot i \text{ である.}$$

Proof. One generator のときだけを示せばよい. それを x とおく. x が R 上超越的であるとする. 次は認めよう.

(1) D を domain, $|D| = \infty$ として $f \in D[t]$ とする. もし ${}^{\forall}a \in D$ に対して $f(a) = 0$ ならば $f = 0$ である.
(2) 代数閉体は無限体である.

今, $v = a_0x^n + \cdots + a_n$ where $n \geq 0$; $a_i \in R$ であって $a_0 \neq 0$, とおく. $v \in R[x]$ である. 仮定より $v \neq 0$ である. この v に対して $u = a_0$ とおき, 環の準同型写像 $f : R \to \Omega$ を $f(u) \neq 0$ となるようにとる. すると, ${}^{\exists}\alpha \in \Omega$ s,t $f(a_0)\alpha^n + \cdots + f(a_n) \neq 0$ for $n \geq 0$. 実際, $n = 0$ ならば自明に正しく $n > 0$ について, もし ${}^{\forall}\alpha \in \Omega$ に対して $f(a_0)\alpha^n + \cdots + f(a_n) = 0$ ならば $f(a_i) = 0$ $({}^{\forall}i)$ であるから矛盾. よって, 上のような $\alpha \in \Omega$ は確かに存在する. このときは, $g : A \to \Omega$ は, $r \in R$ については $g(r) := f(r)$, x については $g(x) = \alpha$, という代入射をとればよい.
次に x は R 上代数的であるとしよう. a は K 上でも代数的であるから $K[x]/K$ は integral である.
$\therefore K[x]$ は体である. ここで $v = r_0x^s + \cdots + r_s$ $(r_i \in R)$ とすると $v \in K[x]$ であって $v \in A$ でもある. $v \neq 0$ とすれば ${}^{\exists}v^{-1} \in K[x]$. 今, v は K 上代数的であるから $\alpha_0v^n + \cdots + \alpha_n = 0$ for $n > 0$, $\alpha_i \in K$. ここで α_i の分母をはらって

$$a_0v^n + \cdots + a_n = 0 \quad (\ n > 0;\ a_i \in R,\ a_n \neq 0\ )$$

と表せる. 一方で, $v^{-1} \in K[x]$ であったので $a_nv^{-1} + \cdots + a_0 = 0$. x が K 上代数的であるから $\beta_0x^m + \cdots + \beta_m = 0$. これも分母をはらって $b_0x^m + \cdots + b_m = 0$ $(m > 0;\ b_i \in R,\ b_0 \neq 0)$ とかく. $a_0b_0 \neq 0$ である. よって $0 \neq u = a_0b_0 \in R$ とおく. そして a ring homom $f : R \to \Omega$ を $f(u) \neq 0$ となるようにとる. このとき

(1) $u^{-1} \in K$ は R 上代数的である.
(2) ${}^{\exists 1}f' : R[u^{-1}] \to \Omega$ a ring homom s,t the inclusion map $R \hookrightarrow R[u^{-1}]$ を i とおくと $f'i = f$ である. このとき $f'(u^{-1}) = f'(u)^{-1} = f(u)^{-1}$ である.

ここで $\mathcal{S}$ の maximal element (B, g) を $(R[u^{-1}], f') \leq (B, g)$ となるようにとる. すると x は $R[u^{-1}]$ 上 integral であるから $x \in B$ である. $\therefore A \subseteq B$, $v \in B$. 一方, v^{-1} も $R[u^{-1}]$ 上 integral なので $v^{-1} \in B$.
$\therefore g(v) \neq 0$. 従って, 私たちがもとめる写像は $g|_A$ をとればよい. □

Corollary 4.2.24. *k は体として, A を a finite generated k-algebra とせよ. A が体ならば A は k 上有限次代数拡大である.*

Proof. $\Omega = \overline{k}$, $v = 1$ とせよ. $f : k \hookrightarrow \overline{k}$ に対して $i : k \hookrightarrow A$ を the inclusion map とすれば上の補題から ${}^{\exists}g : A \to \Omega$ a ring homom s,t $f = gi$. よって g は単射であるから $g(A)$ は k の代数拡大である. さらに仮定から $g(A)$ は有限次代数拡大であるから A もそうである. □

さて, これから次のようなことをして上の Corollary 4.2.24 考えてみよう. これは, 一般に "*Zariski* の補題" といわれる重要なものである. まずは, 次を見ることにする.

Proposition 4.2.25. $R \subseteq A \subseteq B$ は環の拡大で R は *Noetherian* とせよ. そして B は *a f,g R-algebra* とする. このとき,

(1) B は *a f,g A-module* である.
(2) B/A は *integral* である.

のいずれかをみたすならば, A は *a f,g R-algebra* である.

Proof. はじめに, (1) と (2) が同値であることを示そう. (1) を仮定して, $^{\forall}x \in B$ をとると $A[x] \subseteq B$ であって B は a f,g A-module なので x は A 上 integral である. 一方で, (2) を仮定すると $B = R[x_1, \cdots, x_n]$ for some $n > 0$; $x_i \in B$ と表せていて $^{\forall}i$ について x_i は A 上 integral なので $A[x_1, \cdots, x_n]$ は a f,g A-module である. よって $B \subseteq R[x_1, \cdots, x_n] \subseteq A[x_1, \cdots, x_n] \subseteq B$ より B は a f,g A-module である. よって, (1) と (2) は同値であることが示されたのでこれからは (1) を仮定する. すると B は次のように表すことができる.

$$B = R[x_1, \cdots, x_n] \quad as\ R - algebra,$$
$$B = Ay_1 + \cdots + Ay_m \quad as\ A - module,$$

今, $^{\forall}\alpha \in B$ をとる. すると $\alpha = \sum_{r_1, \cdots, r_n} \alpha_{r_1, \cdots, r_n} x_1^{r_1} \cdots x_n^{r_n}$ とかく. $x_i \in Ay_1 + \cdots + Ay_m$ であるから $x_i = \sum_{j=1} a_{ij} y_j$ $(a_{ij} \in A)$ とすると

$$\alpha = \sum_{r_1, \cdots, r_n} \alpha_{r_1, \cdots, r_n} \left\{ \prod_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} x_j \right)^{r_i} \right\},$$

となる. しかし, $1 \leq {}^{\forall}u, v \leq m$ に対して $y_u y_v = \sum_{w=1}^{m} a_{ijw} y_w$ $(a_{ijw} \in A)$ となるので $b_1, \cdots, b_m$ を $\{a_{ij},\ a_{uvw} | 1 \leq i \leq n,\ 1 \leq j, u, v, w \leq m\}$ の多項式の中からうまくとると,

$$\alpha = \sum_{r_1, \cdots, r_n} \alpha_{r_1, \cdots, r_n} (b_1 y_1 + \cdots + b_m y_m) = \sum_{r_1, \cdots, r_n} \{ (\alpha_{r_1, \cdots, r_n} b_1) y_1 + \cdots + (\alpha_{r_1, \cdots, r_n} b_m) y_m \}$$

となる. $\therefore \alpha \in \sum_{k=1}^{m} R[a_{ij},\ a_{uvw} | 1 \leq i \leq n,\ 1 \leq j, u, v, w \leq m] \cdot y_k$. ここで $A_0 = R[a_{ij},\ a_{uvw} | 1 \leq i \leq n,\ 1 \leq j, u, v, w \leq m]$ とおくと次をみたすことがわかる.

(1) $R \subseteq A_0 \subseteq A$.
(2) A_0 は a f,g R-algebra である. 従って A_0 は a Noetherian ring である.
(3) B は a finite A_0-algebra である.

このとき (2),(3) をみるに B は a Noetherian A_0-module である.

$$\begin{aligned}\therefore \quad A &= A_0a_1 + \cdots + A_0a_k \qquad for\ some\ a_i \in A \\ &= A_0[a_1, \cdots, a_k] \\ &= \Big(R[a_ij,\ a_{uvw} | 1 \leq i \leq n,\ 1 \leq u, v, w \leq m]\Big)[a_1, \cdots, a_k] \\ &= R[a_\ell,\ a_ij,\ a_{uvw} | 1 \leq i \leq n,\ 1 \leq u, v, w \leq m,\ 1 \leq \ell \leq k].\end{aligned}$$

$\therefore A$ は a f,g R-algebra である. □

Proposition 4.2.26. *k を体として, $K = k[x_1, \cdots, x_n]$ where $n > 0$; $x_i \in K$ とする. このとき K が体ならば $x_1, \cdots, x_n$ はすべて k 上代数的である.*

Proof. n についての induction で証明する. $n = 1$ のとき $x = x_1$ とおくと $K = k[x]$ である. K は体なのだから $^{\exists}x^{-1} \in K$; $x^{-1} = a_0x^m + \cdots + a_m$. $\therefore a_0x^{m+1} + \cdots + a_mx - 1 = 0$, x は k 上代数的である.
$n > 1$ として $n - 1$ 以下で正しいとせよ. 今は, $x_2, \cdots, x_n$ が k 上代数的であるとする. $x = x_1$ とおいて $F = k(x)$ とすると, $K = f[x_2, \cdots, x_s]$ である. このとき K/F は代数拡大であるから Proposition 4.2.25 より F は a f,g $k[x]$-algebra である. $\therefore F = \Big(k[x]\Big)[y_1, \cdots, y_s]$ where $y_i = \dfrac{g_i}{f}$ $f, g_i \in k[x]$, $f \neq 0$. もし x が *trancsendental* ならば f は $^{\forall}p$; irreducible polynomial に対して $f \in (p)$ であるが,

$$\bigcap_{p:\ irreducible} (p) = (0)$$

であるから $f = 0$ となり矛盾である. $\therefore x$ は k 上代数的である. □

4.3 Appendix III (Direct limit)

A は a ring とする. この節は基本的に大まかに記すことにする.

Definition 48. *$I \neq \emptyset$; an ordered set とする. もし $^{\forall}\alpha, \beta \in I$ に対して $^{\exists}\gamma \in I$ s,t $\alpha \leq \gamma$ かつ $\beta \leq \gamma$ であるとき, この I を a direct set という.*

Definition 49. *$\{M_i\}_{i \in I}$ を A-module の族, $^{\forall}(i \leq j)$ where $i, j \in I$ に対して $f_{ij} : M_i \to M_j$ を an A-linear map とする. $\mathcal{F} = \{M_i, f_{ij}\}_{i \in I}$ が a direct system であるとは,*

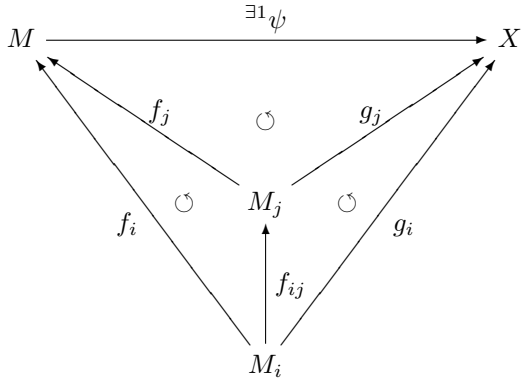
(1) $^{\forall}i \in I$ に対して $f_{ii} = 1_{M_i}$.
(2) $i, j, k \in I$, $i \leq j$, $j \leq k$ ならば $f_{ik} = f_{jk} \cdot f_{ij}$.

をみたすことをいう. 今, X を an A-module としたとき $\{X, 1_X\}$ は direct system である.

Proposition 4.3.1. 次の条件をみたすような *a pair $(M, \{f_i\})$* が $\mathcal{F} = \{M_i, f_{ij}\}_{i \in I}$ に対して同型を除いて唯一通りに存在する.

(1) M は *an A-module.*
(2) $^{\forall}i \in I$, $f_i : M_i \to M$ *an A-linear map* であって, $i \leq j$ ならば $f_i = f_jf_{ij}$.

(3) $(X, \{g_i\})$ を (1), (2) をみたすようにとると,



そしてこの M を $\mathcal{F}$ の *the direct limit* とよび, $\varinjlim M_i$ とかく.

存在は次のようにすればよい. まず $C = \bigoplus_{i\in I} M_i$ とおき, $^\forall i \in I$ に対して a map $\lambda_i : M_i \to C$ を第 i 成分への埋め込みとし,

$$\left\{\lambda_i(x_i) - \lambda_j\left(f_{ij}(x_i)\right) \,\middle|\, i,j \in I,\ i \le j \text{であって } x_i \in M_i \ \ for\ ^\forall i \in I\right\}$$

で生成される C の A-submodule を D とおく. このとき, 求める A-module は C/D であって, $\{f_i\}$ については $^\forall i \in I$ に対して $f_i : M_i \xrightarrow{\lambda_i} C \to C/D$ とすればよい.

Proposition 4.3.2. $\{M_i, f_{ij}\}$ を *a direct system* とする.

(1) $^\forall x \in \varinjlim M_i$ に対して $^\exists\gamma \in I$, $^\exists m_\gamma \in M_\gamma$ *s,t* $x = f_\gamma(x_\gamma)$.
(2) $\gamma \in I$ とする. $f_\gamma(m_\gamma) = 0 \Leftrightarrow {}^\exists\delta \ge \gamma$ *s,t* $f_{\gamma\delta}(m_\gamma) = 0$.

Proof. (1) については

$$x = \overline{(m_\alpha)_{\alpha\in I}} = \sum_{\alpha\in I} \lambda_\alpha(m_\alpha)$$

と表せるから, $\Lambda_x = \{\alpha \in I | m_\alpha \neq 0\}$ とおくと定義から $|\Lambda_x| < \infty$ である. そして I は a direct set であったから $^\exists\beta \in I$ s,t $^\forall\alpha \in \Lambda_x$ に対して $\alpha \le \beta$. この $\beta \in I$ に $m_\alpha \in M_\alpha$ を写せばよい.
(2) は $\Rightarrow$ だけを示せばよい. $\rho \in I$ について $f_\rho(m_\rho) = 0$ とする. これは $\lambda_\rho(m_\rho) \in D$ と同値であるから $^\exists\ell > 0$, $\alpha_i \le \beta_i$ where $\alpha_i, \beta_i \in I$, $^\exists\{y_i\}$ s,t

$$\begin{aligned}
\lambda_\rho(m_\rho) &= \sum_{i=1}^{\ell} \left(\lambda_{\beta_i}\left(f_{\alpha_i\beta_i}(y_{\alpha_i})\right) - \lambda_{\alpha_i}(y_{\alpha_i})\right) \\
&= \sum_{i=1}^{\ell} \lambda_{\beta_i}\left(f_{\alpha_i\beta_i}(y_{\alpha_i})\right) - \sum_{i=1}^{\ell} \lambda_{\alpha_i}(y_{\alpha_i}) \\
&= \left(\sum_{\rho=\beta_i} \lambda_{\beta_i}\left(f_{\alpha_i\beta_i}\left(y_{\alpha_i}\right)\right) + \sum_{\rho\neq\beta_i} \lambda_{\beta_i}\left(f_{\alpha_i\beta_i}\left(y_{\alpha_i}\right)\right)\right) - \left(\sum_{\alpha_i\neq\rho} \lambda_{\alpha_i}(y_{\alpha_i}) + \sum_{\alpha_i=\rho} \lambda_{\alpha_i}(y_{\alpha_i})\right).
\end{aligned}$$

よって,

$$\begin{cases} x = \sum_{\rho=\beta_i} \lambda_{\beta_i}\left(f_{\alpha_i\beta_i}\left(y_{\alpha_i}\right)\right) - \sum_{\alpha_i=\rho} \lambda_{\alpha_i}(y_{\alpha_i}) \\ 0 = \sum_{\xi=\beta_i} \lambda_{\beta_i}\left(f_{\alpha_i\beta_i}\left(y_{\alpha_i}\right)\right) - \sum_{\alpha_i=\xi} \lambda_{\alpha_i}(y_{\alpha_i}) \quad \xi \in I,\ \xi \neq \rho \end{cases}$$

とかける. $\therefore {}^{\exists}\delta \in I$ s,t $\alpha_i \leq \delta$, $\beta_i \leq \delta$. 従って,

$$\begin{aligned} f_{\rho\delta}(m_\rho) &= f_{\rho\delta}\left(\sum_{\rho=\beta_i} f_{\alpha_i\beta_i}\left(f_{\alpha_i\beta_i}\left(y_{\alpha_i}\right)\right) - \sum_{\alpha_i=\rho} f_{\alpha_i\delta}(y_{\alpha_i})\right) + \sum_{\substack{\xi\in I\\ \xi\neq\rho}} f_{\xi\delta}(0) \\ &= \sum_{\rho=\beta_i} f_{\rho\delta}\left(f_{\alpha_i\beta_i}\left(y_{\alpha_i}\right)\right) - \sum_{\alpha_i=\rho} f_{\rho\delta}(y_{\alpha_i}) + \left(\sum_{\beta_i\neq\rho} f_{\beta_i\delta}\left(f_{\alpha_i\beta_i}(y_{\alpha_i})\right) - \sum_{\alpha_i\neq\rho} f_{\alpha_i\delta}(y_{\alpha_i})\right) \\ &= \sum_{i=1}^{\ell} f_{\beta_i\delta}\left(f_{\alpha_i\beta_i}(y_{\alpha_i})\right) - \sum_{i=1}^{\ell} f_{\alpha_i\delta}(y_{\alpha_i}) \\ &= \sum_{i=1}^{\ell} \left(f_{\beta_i\delta}\left(f_{\alpha_i\beta_i}(y_{\alpha_i})\right) - f_{\alpha_i\delta}(y_{\alpha_i})\right) \\ &= 0 \end{aligned}$$

となる. □

これから述べる命題は上の補題と Universal property を用いて証明することができる. それらは, 複雑ではあるが定義をしっかりと理解していれば難しくはないので全て *Exercise* にする.

Lemma 4.3.3. *Direct limit* をとる操作は *an exact functor* である.

Lemma 4.3.4. $\{M_i, f_{ij}\}_{i\in I}$ を *a direct system, N* を *an A-module* とせよ. このとき,

$$\left(\varinjlim M_i\right) \otimes_A N \underset{canon}{\cong} \varinjlim (M_i \otimes_A N)$$

が成立する.

Lemma 4.3.5. $\Omega \neq \emptyset$; *a set,* ${}^{\forall}\alpha \in \Omega$ に対して $\{X_i^\alpha, f_{ij}^\alpha\}$ は *a direct system* であるとせよ. このとき,

$$\bigoplus_{\alpha\in\Omega} \varinjlim X_i^\alpha \underset{canon}{\cong} \varinjlim \left(\bigoplus_{\alpha\in\Omega} X_i^\alpha\right)$$

が成立する.

4.4 Appendix IV (Topology and Complition)

しばらくは, G は加法群とする. もし, G 上にある位相 $\mathcal{O}_G$ が定義されていて $\sigma : G\times G \to G, (x, y) \mapsto x+y$ と $\varepsilon : G \to G, x \mapsto -x$ という 2 つの写像が連続であるとき $(G, \mathcal{O}_G)$ は *a topological abel group* という. これからは単に, G は *a topological abel group* である, と表すことにするが実は, 表記上表には現れていないが

G 上の位相 $\mathcal{O}_G$ も常に組にして考えていてることに注意する必要があると思われる. そして, $^\forall x \in G$ に対して $\mathcal{U}(x) := \{U \in \mathcal{O}_G | x \in U\}$, つまり $x \in G$ の開近傍系を表すことにする. とくに $x = 0$ のときは $\mathcal{U}(x) = \mathcal{U}$ とかくことにする. この $\mathcal{U}(x)$ $(x \in G)$ は $\mathcal{U}$ によって定まっていること ($i, e; \mathcal{U}(x) = \{x + U | U \in \mathcal{U}\}$,) が知られている. そして, σ と ε の連続性から次のことが殆ど自明に成立する.

Lemma 4.4.1.
(1) $x, y \in G$ とする. $U \in \mathcal{O}_G$ がもし $U \in \mathcal{U}(x+y)$ であるならば $^\exists V \in \mathcal{U}(x)$, $^\exists W \in \mathcal{U}(y)$ s,t $V + W \subseteq U$.
(2) $x \in G$ とする. $U \in \mathcal{O}_G$ がもし $U \in \mathcal{U}(-x)$ であれば $^\exists V \in \mathcal{U}(x)$ s,t $-V \subseteq U$.

さて, $\Delta : G \to G \times G$ を $\Delta(x) = (x, x)$ とするとき, この Δ については, $\Delta(G)$ が $G \times G$ 内で閉集合であることと G が *Hausdorff* 空間であることは同値である. 実際, まずは $\Delta(G)$ が閉集合であるとしよう. $x, y \in G$; $x \neq y$ をとると $(x, y) \notin \Delta(G)$ であるから $^\exists V \in \mathcal{U}(x)$, $^\exists V \in \mathcal{U}(y)$ s,t $V \times W \cap \Delta(G) = \emptyset$. このとき $V \cap W = \emptyset$ をみたしている. 逆に, G が *Hausdorff* 空間であるとして $\Delta(G)^c := G \times G \backslash \Delta(G)$ が開集合であることを示す. $^\forall (x, y) \in \Delta(G)$ をとると, $x \neq y$ であるから $^\exists V \in \mathcal{U}(x)$, $^\exists W \in \mathcal{U}(y)$ s,t $V \cap W = \emptyset$. すると $V \times W \cap \Delta(G)^c = \emptyset$ をみたすので $(x, y) \in {}^\exists V \times W \subseteq \Delta(G)^c$; an open set. よって $\Delta(G)^c$ は開集合の定義をみたすので $\Delta(G)$ は閉集合である.

一方で, $\varphi : G \times G \to G$ を $\varphi((x, y)) = x - y$ とおく. この φ は連続であって $\mathrm{Ker}\,\varphi = \Delta(G)$ である. これらのことを踏まえて,

Lemma 4.4.2. *H はすべての 0 の開近傍の共通集合, つまり $H = \bigcap_{U \in \mathcal{U}} U$ とする.*

(1) H は $\{0\}$ の閉包である.
(2) H は G の部分群である.
(3) $\{0\}$ の閉包は自分自身であることと, G が *Hausdorff* 空間であることは同値である.

Proof. $\overline{\{0\}}$ によって $\{0\}$ の閉包を表すことにする. (1) を証明しよう. $^\exists x \in H$ s,t $x \notin \overline{\{0\}}$ を仮定すれば $^\exists V \in \mathcal{U}(x)$ s,t $V \cap \{0\} = \emptyset$. $V = x + U$ for some $U \in \mathcal{U}$ と表せていたので $-x \notin U$. $\therefore x \notin \varepsilon(U)$. しかし ε は連続な写像だから $x \in H$ に反する. よって $H \subseteq \overline{\{0\}}$ をうる. 次に, $^\exists x \in \overline{\{0\}}$ s,t $x \notin H$ とすれば $x \notin U$ となる $U\mathcal{U}$ が存在する. この U については $0 \notin x + \varepsilon(U)$ であるから $V = x + \varepsilon(U)$ とおくと $V \in \mathcal{U}(x)$ であって $\{0\} \cap V = \emptyset$ となるが, これは $x \in \overline{\{0\}}$ に反する. よって, これらのことから $H = \overline{\{0\}}$ をうる.
(2) を証明しよう. $0 \in H$ であるから $H \neq \emptyset$ は明らか. $x \in H$ とする. もし $-x \notin H$ であれば, (1) から H は閉集合なので $\varepsilon^{-1}(H)$ も閉集合である. $x \notin \varepsilon^{-1}(H)$ より $^\exists V \in \mathcal{U}(x)$ s,t $V \cap \varepsilon^{-1}(H) = \emptyset$. $\varepsilon(0) = 0 \in H$ であるからこの V は $\{0\}$ との共通をもたないが一方で, $x \in H = \overline{\{0\}}$ としているので $V \cap \{0\} \neq \emptyset$ であるから $-x \notin H$ は矛盾であることがわかる. $\therefore -x \in H$ for $^\forall x \in H$.
$x, y \in H$ とする. このとき $x + y \notin H$ であることと $(x, y) \notin \varsigma^{-1}(H)$ は同値であって, もし $x + y \notin H$ であれば $\varsigma^{-1}(H)$ は閉集合なので $^\exists V \in \mathcal{U}(x)$, $^\exists W \in \mathcal{U}(y)$ s,t $V \times W \cap \sigma^{-1}(G) = \emptyset$. しかしながら, 上でも述べたことだが $0 \in V$, $0 \in W$ であるから $(0, 0) \in V \times W \cap \sigma^{-1}(H) \neq \emptyset$ をうる. よって $x + y \in H$ for all $x, y \in H$ である.
(3) を証明しよう. $\{0\} = \overline{\{0\}}$ を仮定すれば $\Delta(G) = \mathrm{Ker}\,\varphi = \varphi^{-1}\left(\overline{\{0\}}\right)$ であるから $\Delta(G)$ は閉集合であることがわかるので G は *Hausdorff* 空間である. 逆に, G が *Hausdorff* 空間であるとしよう. もし, $\{0\} \neq \overline{\{0\}}$ ならば $0 \neq {}^\exists x \in \overline{\{0\}}$ であるから $U \cap V = \emptyset$ となる $U \in \mathcal{U}$, $V \in \mathcal{U}(x)$ が存在する. 従って $x \notin U$ であるがこれは $x \in \overline{\{0\}}$ に矛盾する. □

以下, G の点列 $\{x_i\}_{i\geq 1}$ のことを $\{x_i\}$ とかくことにする.

Definition 50. $x \in G$ とする. G の点列 $\{x_i\}$ がもし, ${}^{\forall}U \in \mathcal{U}$ に対して ${}^{\exists}N_U \geq 1$ *s,t* $x - x_i \in U$ *for* ${}^{\forall}i \geq N_U$ をみたすとき, $\{x_i\}$ は x に収束するといい, ここでは $x_i \to x$ とかくことにする.

Lemma 4.4.3. $x, y \in G$ として, $\{x_i\}, \{y_i\}$ を G の点列とする.

(1) $\{x_i + y_i\}$ は $x + y$ に収束する G の点列である.
(2) $\{-x_i\}$ は $-x$ に収束する G の点列である.

Proof. (2) は (1) と同様にして証明できるのでここでは (1) だけを示す. ${}^{\forall}U \in \mathcal{U}$ をとる. $0 = 0 + 0$ とみることによって ${}^{\exists}V, W \in \mathcal{U}$ s,t $V + W \subseteq U$. このとき

$$V \in \mathcal{U} \text{ に対して} {}^{\exists}N_V \geq 1 \ s,t \ x - x_i \in V \quad for \ i \geq N_V \ ,$$
$$W \in \mathcal{U} \text{ に対して} {}^{\exists}N_W \geq 1 \ s,t \ y - y_j \in W \quad for \ j \geq N_W \ ,$$

となる. 今, $N_U = \max\{N_V, N_W\}$ とおく. すると ${}^{\forall}k \geq N_U$ について $(x+y)-(x_k+y_k) = (x-x_k)+(y-y_k) \in V + W \subseteq U$ をうる. □

Lemma 4.4.4. G は *Hausdorff* 空間とする. もし点列が収束するならばその極限は点列に対して唯一に定まる.

Proof. $\{x_i\}$ を G の点列, $x, x' \in G$ として $x_i \to x$, $x_i \to x'$ とする. もし $x \neq x'$ ならば ${}^{\exists}V \in \mathcal{U}(x)$, ${}^{\exists}V' \in \mathcal{U}(x')$ s,t $V \cap V' = \emptyset$. このとき

$$x_i \to x \text{ より } V \in \mathcal{U}(x) \text{ に対して} {}^{\exists}N_V \geq 1 \ s,t \ x_i \in V \quad for \ i \geq N_V \ ,$$
$$x_i \to x' \text{より } V' \in \mathcal{U}(x') \text{ に対して} {}^{\exists}N_{V'} \geq 1 \ s,t \ x_j \in V' \quad for \ j \geq N_{V'} \ ,$$

よって ${}^{\forall}k \geq \max\{N_V, N_{V'}\}$ をとれば $x_k \in V \cap V' \neq \emptyset$ である. □

これから *Cauchy* 列を用いて G の *completion* $\widehat{G}$ を定義しよう. よって, まずは *Cauchy* 列と *complete* 空間の定義を述べておく.

Definition 51. $\{x_i\}$ を G の点列とする. $\{x_i\}$ が ${}^{\forall}U \in \mathcal{U}$ に対して ${}^{\exists}N_U \geq 1$ *s,t* $x_i - x_j \in U$ *for* ${}^{\forall}i, j \geq N_U$ をみたすとき, この $\{x_i\}$ を G の *a Cauchy* 列という. そして, G の任意の *Cauchy* 列がそれぞれある一点に収束するとき G は *complete* であるという.

以下, $\mathrm{C}(G)$ によって G の a Cauchy 列の集合を表すことにする. ${}^{\forall}x \in G$ に対して $\{x, x, \cdots\}$ という点列は明らかに G の a Cauchy 列であるから $\mathrm{C}(G) \neq \emptyset$ をうる. 今, $\{x_i\}, \{y_i\} \in \mathrm{C}(G)$ として, $\{x_i\}$ と $\{y_i\}$ との和を $\{x_i\} + \{y_i\} := \{x_i + y_i\}$ によって定義する. (この和の well-defined, つまり $\{x_i + y_i\} \in \mathrm{C}(G)$ を証明することは *Exercise* とする.) このとき $(\mathrm{C}(G), +)$ は $\{0, 0, \cdots\}$ を単位元にもつ加法群をなすことがわかる. さらに $\mathrm{C}_0(G) = \{\{x_i\} \in \mathrm{C}(G) | x_i \to 0\}$ とおくと, この $\mathrm{C}_0(G)$ は $\mathrm{C}(G)$ の部分群になる.

次に ${}^{\forall}U \in \mathcal{U} \subseteq \mathcal{O}_G$ に対して $U_C := \left\{x = \{x_i\} \in \mathrm{C}(G) | {}^{\exists}N_x \geq 1 \ s,t \ x_i \in U \quad for \ {}^{\forall}i \geq N_x\right\}$ とおく. もし $U = \emptyset$ ならば $U_C = \emptyset$ であって, $U = G$ ならば $U_C = \mathrm{C}(G)$ である. そして $\mathcal{X} = \{U_C | U \in \mathcal{O}_G\}$ として

$$\mathcal{O}_{\mathrm{C}(G)} := \left\{ \bigcup_{U_C \in \Lambda} U_C \ \middle| \Lambda \subseteq \mathcal{X} \right\}$$

とおくと $\mathcal{O}_{\mathrm{C}(G)}$ は $\mathrm{C}(G)$ 上の位相となる. しかし一般には, $(\mathrm{C}(G), \mathcal{O}_{\mathrm{C}(G)})$ が a topological abel group であるとは限らない. 以降, $\mathrm{C}(G)/\mathrm{C}_0(G)$ のことを $\widehat{G}$ と表し, $\varphi_G : G \to \widehat{G}$, $x \mapsto \overline{\{x\}}$ と定める. この φ_G は群の準同型写像であることは殆ど自明であって, 次をみたしている.

(1) φ_G は連続である.
(2) $\mathrm{Ker}\,\varphi_G = \bigcap_{U \in \mathcal{U}} U$.
(3) φ_G が全射であることの必要十分条件は任意の Cauchy 列がそれぞれに収束することである.

従って, G が complete であることと φ_G が同型写像であることは同値である.

H を a topological abel group, $f : G \to H$ を群の準同型写像で連続なものとする. そして, $^\forall y \in H$ に対して $\mathcal{U}(y) \subseteq \mathcal{O}_H$ のことを $\mathcal{O}_G$ と区別するために $\mathcal{U}_H(y)$ と表し, とくに $\mathcal{U}_H(0)$ は $\mathcal{U}_H$ とする.

Lemma 4.4.5. $\{f(x_i)\}$ を G の *a Cauchy* 列とすれば $\{f(x_i)\}$ は H の *a Cauchy* 列である.

Proof. $^\forall U \in \mathcal{U}_H$ をとる. f は連続としていたので $f^{-1}(U) \in \mathcal{U}$ である. $\therefore {}^\exists N_{f^{-1}(U)} \geq 1$ s,t $x_i - x_j \in f^{-1}(U)$ for $^\forall i, j \geq N_{f^{-1}(U)}$. よって, $^\forall i, j \geq N_{f^{-1}(U)}$ について $f(x_i) - f(x_j) = f(x_i - x_j) \in U$ となる. □

Corollary 4.4.6. $\{x_i\} \in \mathrm{C}(G)$ がもし $\mathrm{C}_0(G)$ に含まれているならば $\{f(x_i)\}$ は $\mathrm{C}_0(H)$ の元である.

よって, $f : G \to H$ は $\widehat{f} : \widehat{G} \to \widehat{H}$, $\overline{\{x_i\}} \to \overline{\{f(x_i)\}}$ を induce する. そして, その写り方から $\widehat{f}$ は群の準同型写像であって $\widehat{f} \cdot \varphi_G = \varphi_H \cdot f$ をみたすことは自明である. よって, $\widehat{f}$ も連続写像である.

これまでは, 一般の位相についての議論であった. しかし, 位相をある方法で正しく定義することによってよりよい議論になることがわかっている. これからの議論はそのことについて述べていくことにしよう.

まず, G は加法群とせよ. そして $\{G_n\}_{n \in \mathbb{Z}}$ where G_n は G の部分群であって $G_0 = G$, $^\forall i \in \mathbb{Z}$ に対して $G_i \supseteq G_{i+1}$ である, という G の部分群の族を一つとる. (これを G の *a filtration* という.) このとき, $\mathcal{X} = \{x + G_n | x \in G,\ n \in \mathbb{Z}\}$ とおき

$$\mathcal{O}_G = \left\{ \bigcup_{U \in \Lambda} U \;\middle|\; \Lambda \subseteq \mathcal{X} \right\}$$

とすると, $\mathcal{O}_G$ は G 上に位相を定める. これは次のことだけを示せば十分である.

Lemma 4.4.7. $a, b \in G$ として $\ell, m \in \mathbb{Z}$ とする. そして $X = (a + G_\ell) \cap (b + G_m)$ とする. もし $X \neq \emptyset$ でなければ $X \in \mathcal{X}$ をみたす.

Proof. $\ell \geq m$ ならば $a + G_\ell \subseteq a + G_m$ である. よって $(a + G_m) \cap (b + G_m) \neq \emptyset$ となるが, これは G_m で G を分割したものとしてみれば $a + G_m = b + G_m$ となる. $\therefore X = (a + G_\ell) \cap (b + G_m) = (a + G_\ell) \cap (a + G_m) = a + G_\ell \in \mathcal{X}$. $\ell \leq m$ ならば $X = b + G_m \in \mathcal{X}$ である. □

そして,

Lemma 4.4.8. $(G, \mathcal{O}_G)$ は *a topological abel group* である.

Proof. $^{\forall}x, y \in G$ をとる. $^{\forall}U \in \mathcal{U}(x+y)$ に対して $^{\exists}n \in \mathbb{Z}$ s,t $(x+y)+G_n \subseteq U$. このとき, $(x+G_n)+(y+G_n)=(x+y)+G_n$ をみればよい. 同様にして $^{\forall}U \in \mathcal{U}(-x)$ についても証明すればよい. □

次に $\widehat{G}$ の部分集合 $\widehat{G}_n$ を,

$$\widehat{G}_n := \left\{\overline{x} | x = \{x_i\} \in \mathrm{C}(G),\ {}^{\exists}N_x \geq 1\ s,t\ {}^{\forall}i \geq N_x \text{に対して } x_i \in G_n\right\} \quad \left(= \overline{(G_n)_C}\ in\ \mathrm{C}(G)/\mathrm{C}_0(G) \right)$$

によって定めることにしよう. すると, (1) $\widehat{G}_n$ は $\widehat{G}$ の部分群であって, (2) $\widehat{G}_n \supseteq \widehat{G}_{n+1}$, をみたしている. すると上の補題は $\widehat{G}$ 上に $\left\{\widehat{G}_n\right\}$ から定まる位相 $\mathcal{O}_{\widehat{G}}$ を定義できて, $\left(\widehat{G}, \mathcal{O}_{\widehat{G}}\right)$ は a topological abel group をなすことがわかる. しかも, $\varphi_G : G \to \widehat{G}$ は連続で, その核は一般論では $\bigcap_{U\in\mathcal{U}} U$ で与えられていたが, G の位相の定め方から $\operatorname{Ker}\varphi_G = \bigcap_{n\in\mathbb{Z}} G_n$ であることがわかる. そして, 次は証明したい定理のうちの一つである.

Theorem 4.4.9. $\widehat{G}$ は *a complete abel group* である. そしてこの $\widehat{G}$ を G の $\{G_n\}$*-adic completion* という.

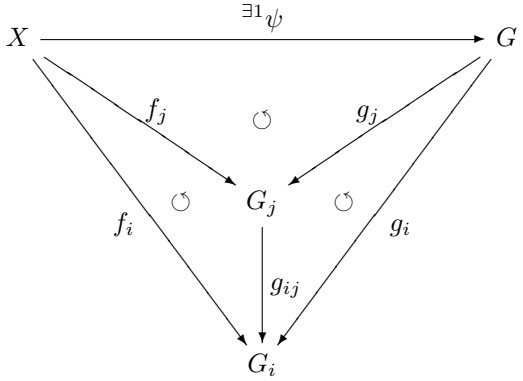
まずは少し一般論から始める.

Definition 52. $\{G_i, g_{ij}\}$ *where* G_i は加法群で $^{\forall}(i \leq j)$; $0 \leq i, j \in \mathbb{Z}$ に対して $g_{ij} : G_j \to G_i$ は群の準同型写像, とする. もし (1) $g_{ii} = 1_{G_i}$ ($^{\forall}i \in \mathbb{Z}$), (2) $i \leq j \leq k$ ならば $g_{ik} = g_{ij}g_{jk}$, をみたすときこの $\{G_i, g_{ij}\}$ は *an inverse system* であるという.

$\{G_i, g_{ij}\}$, $\{G'_i, g'_{ij}\}$ を inverse systems とする. $\varphi = \{\varphi_i\}$ where $\varphi_i : G_i \to G'_i$ $(^{\forall}i)$ は群の準同型写像であって $^{\forall}(i \leq j)$ について $\varphi_i g_{ij} = g'_{ij}\varphi_i$ をみたすとき, この $\varphi = \{\varphi_i\}$ のことを *a map of inverse systems* という. このとき,

Proposition 4.4.10. 次の条件をみたすような *a pair* $(G, \{g_i\})$ が $\{G_i, g_{ij}\}$ に対して同型を除いて唯一通りに存在する.

(1) G は加法群.
(2) $^{\forall}i$, $g_i : G \to G_i$ は群の準同型写像であって, $i \leq j$ ならば $g_j = g_i g_{ij}$.
(3) $(X, \{f_i\})$ を (1), (2) をみたすようにとると,



そしてこの G を $\{G_i, g_{ij}\}$ の *the inverse limit* とよび, $\varprojlim G_i$ とかく.

Proof. G としては

$$G = \left\{ (x_i) \in \prod_{i \geq 0} G_i \;\middle|\; 0 \leq i, j \in \mathbb{Z} \text{ について } i \leq j \text{ ならば } x_i = g_{ij}(x_j) \right\}$$

をとり $\{g_i\}$ はそれぞれの projection をとればよい. あとは読者に委ねることとしよう. □

Proposition 4.4.11. $\{G_i\} = \{G_i, g_{ij}\}$ と $\{G'_i\} = \{G'_i, g'_{ij}\}$ を *inverse systems* として $\varphi = \{\varphi_i\} : \{G_i\} \to \{G'_i\}$ を *a map of inverse systems* とすると, $^{\exists 1}\Phi : \varprojlim G_i \to \varprojlim G'_i$ *an group homomorphism s,t* $^{\forall} i$ に対して $\varphi_i g_i = g'_i \Phi$. この Φ のことを $\varprojlim \varphi_i$ と表すこともある.

Proof. Φ として $(x_i) \mapsto (\varphi_i(x_i))$ とすればよい. □

ここで $\{A_i\} = \{A_i, \alpha_{ij}\}$, $\{B_i\} = \{B_i, \beta_{ij}\}$, $\{C_i\} = \{C_i, \gamma_{ij}\}$ を inverse systems とする. そして $f = \{f_i\} : \{A_i\} \to \{B_i\}$, $g = \{g_i\} : \{B_i\} \to \{C_i\}$ を maps of inverse systems とする. このとき,

$$0 \longrightarrow \{A_i\} \xrightarrow{f} \{B_i\} \xrightarrow{g} \{C_i\} \longrightarrow 0$$

が *exact of systems* であるとは $^{\forall} i$ に対して

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{i+1} & \xrightarrow{f_{i+1}} & B_{i+1} & \xrightarrow{g_{i+1}} & C_{i+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_{ii+1}} & & \downarrow{\scriptstyle \beta_{ii+1}} & & \downarrow{\scriptstyle \gamma_{ii+1}} & & \\ 0 & \longrightarrow & A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i & \longrightarrow & 0 \end{array}$$

が可換であることをいう. また, $\{A_i\}$ が *surjective* であるとは $^{\forall}\alpha_{ij}$ が全射であることをいう.

Lemma 4.4.12. もし $0 \to \{A_i\} \xrightarrow{\{f_i\}} \{B_i\} \xrightarrow{\{g_i\}} \{C_i\} \to 0$ が *exact of systems* であれば

$$exact; \quad 0 \to \varprojlim A_i \xrightarrow{f} \varprojlim B_i \xrightarrow{g} \varprojlim C_i \ ,$$

である. そして, もし $\{A_i\}$ が *surjective* であるならば g は全射である.

Proof. $A = \prod A_i$, $B = \prod B_i$, $C = \prod C_i$ として $d^A(a_i) = a_i - \alpha_{ii+1}(a_{i+1})$ と定め, d^B と d^C も同様にとる. すると $\operatorname{Ker} d^A = \varprojlim A_i$ であるから

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\ 0 & \longrightarrow & A_i & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \end{array}$$

をみて, Snake Lemma より

$$exact; \quad 0 \to \operatorname{Ker} d^A \to \operatorname{Ker} d^B \to \operatorname{Ker} d^C \to \operatorname{Coker} d^A \to \operatorname{Coker} d^B \to \operatorname{Coker} d^C \to 0$$

をうる. よって殆ど明らかとなる. □

ここで定理の証明に戻る. $0 \leq n, m \in \mathbb{Z}$; $m \leq n$ とする. このとき

$$\{G/G_m,\ g_{mn}\} \quad where \ \ g_{mn} : G/G_m \to G/G_n,\ \overline{x} \mapsto \overline{x},$$

は surjective な an inverse system である.

Lemma 4.4.13. $^\forall n \geq 0$ に対して $p_n : \varprojlim G/G_n \to G/G_n$ を *projection* とせよ. このとき $\{\mathrm{Ker}\, p_n\}$ は $\varprojlim G/G_n$ の *a filtration* をなす.
従って $\varprojlim G/G_n$ は $\{\mathrm{Ker}\, p_n\}$ によって定義される位相について *a topological abel group* をなす.

Proof. $^\forall n \leq 0$ をとり, $\mathrm{Ker}\, p_n \supseteq \mathrm{Ker}\, p_{n+1}$ をいえばよい. $^\forall (x_i) \in \mathrm{Ker}\, p_{n+1}$ をとる. $p_n((x_i)) = g_{nn+1}(p_{n+1}((x_i))) = 0$ となる. □

Proposition 4.4.14. 位相も含めて $\widehat{G}$ と $\varprojlim G/G_n$ は群として同型である.

Proof. $^\forall n \geq 0$ をとる. そして $\alpha_n : \widehat{G} \to G/G_n$ を次のように定める. $^\forall \overline{\{x_i\}} \in \widehat{G}$ をとる. このとき n に対して $^\exists N_n \geq 1$ s,t $^\forall i, j \geq N_n$ に対して $x_i - x_j \in G_i$. よって $\{x_{N_n}, \cdots, x_{N_n}, x_{n+1}, x_{n+2}, \cdots\} \in \mathrm{C}(G)$ であって, この Cauchy 列は $\overline{\{x_i\}}$ の代表元ととれるので $^\forall j \geq n$ については $x_n - x_j \in G_n$ としてよい. ここで α_n は $\overline{\{x_i\}} \mapsto \overline{x_n}$ としよう. すると, $g_{nn+1}(\overline{x_{n+1}}) = \overline{x_{n+1}}$ となるが $x_n - x_{n+1} \in G_n$ をみて $g_{nn+1}(\overline{x_{n+1}}) = \overline{x_{n+1}} = \overline{x_n}$. これは $\alpha_n = g_{nn+1}\alpha_{n+1}$ が成り立つことを示している. よって, $^{\exists 1}\alpha : \widehat{G} \to \varprojlim G/G_n$ a group homom s,t $^\forall n$ に対して $\alpha_n = p_n\alpha$. これから次のことを示そう.

(1) α は全射である.
(2) α は単射である.
(3) $^\forall n$ に対して $\alpha\left(\widehat{G}_n\right) = \mathrm{Ker}\, p_n$ である.

$^\forall(\overline{x_1}, \overline{x_2}, \cdots) \in \varprojlim G/G_n$ をとる. $^\forall i$ について $\overline{x_i} - g_{ii+1}(\overline{x_i + 1}) = 0$ だから $x_i - x_{i+1} \in G_i$ である. よって $\{x_1, x_2, \cdots, x_n, \cdots\} \in \mathrm{C}(G)$ をみたし α の全射が確かめられた. 次に $\overline{(x_1, x_2, \cdots)} \in \mathrm{Ker}\, \alpha$ をとる. $0 = \alpha(((x_1, x_2, \cdots)) = (\overline{x_1}, \overline{x_2}, \cdots)$ であるから $x_i \in G_i$ $(^\forall i)$ となる. よって α は単射である. そして (3) については $\widehat{G}_n$ の定義にもどれば殆ど自明である. □

Lemma 4.4.15. $0 \to G' \xrightarrow{\xi} G \xrightarrow{\pi} G'' \to 0$ を群の *exact* とせよ. そして G' の *a filtration* $\{\xi^{-1}(G_n)\}$ と, G'' の *a filtration* $\{\pi(G_n)\}$ をとると, それぞれの *filtration* が定める位相について

$$0 \longrightarrow \widehat{G'} \xrightarrow{\widehat{\xi}} \widehat{G} \xrightarrow{\widehat{\pi}} \widehat{G''} \longrightarrow 0$$

は完全列をなす.

Proof. まず $^\forall n$ について $\xi^{-1}(G_n) \to G_n \to \pi(G_n) \to 0$ は完全列であることに注意しよう. すると

$$\begin{array}{ccccccccc} & & \xi^{-1}(G_n) & \longrightarrow & G_n & \longrightarrow & \pi(G_n) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \end{array}$$

という可換図をうることができ, ここで Snake Lemma を用いて $^\forall n$ に対して次の完全列が得られる.

$$0 \longrightarrow \frac{G'}{\xi^{-1}(G_n)} \longrightarrow \frac{G}{G_n} \longrightarrow \frac{G''}{\pi(G_n)} \longrightarrow 0.$$

しかもこの完全列は inverse system の完全列

$$0 \longrightarrow \left\{\frac{G'}{\xi^{-1}(G_n)}\right\}_{n\geq 0} \longrightarrow \left\{\frac{G}{G_n}\right\}_{n\geq 0} \longrightarrow \left\{\frac{G''}{\pi(G_n)}\right\}_{n\geq 0} \longrightarrow 0$$

を導く. □

Corollary 4.4.16. $^\forall n \geq 0$ に対して

$$\frac{G}{G_n} \cong \frac{\widehat{G}}{\widehat{G}_n}$$

が成り立つ. 従って, *a map of inverse systems* $\varphi = \{\varphi_n\} : \left\{\dfrac{G}{G_n}\right\} \to \left\{\dfrac{\widehat{G}}{\widehat{G}_n}\right\}$ をとれば $\varprojlim \varphi_i$ は同型写となる.

Proof. G/G_n ($^\forall n$) について $\pi^{-1}(\{0\}) = G_n$ であるので $\{0\} \in \mathcal{U}_{G/G_n}$ である. よって G/G_n は complete である. ここで

$$0 \longrightarrow G_n \longrightarrow G \longrightarrow G/G_n \longrightarrow 0$$

から次の完全列が得られる.

$$0 \longrightarrow \widehat{G_n} \longrightarrow \widehat{G} \longrightarrow \widehat{G/G_n} \longrightarrow 0\cdot$$

$$\therefore \quad \frac{\widehat{G}}{\widehat{G_n}} \cong \frac{\widehat{G}}{G_n} = \frac{G}{G_n}.$$

よって, 後は $\xi(\widehat{G_n}) = \widehat{G}_n$ を示せば十分. しかしこれは定義にもどれば殆ど明らか. □

これまでの議論から $\varprojlim G/G_n \cong \varprojlim \widehat{G}/\widehat{G}_n$ が確かめられた. 従って後は,

$$\begin{array}{ccc} \widehat{G} & \xrightarrow{\varphi_{\widehat{G}}} & \widehat{\widehat{G}} \\ \downarrow & \circlearrowleft & \downarrow \\ \varprojlim G/G_n & \xrightarrow{\sim} & \varprojlim \widehat{G}/\widehat{G}_n \end{array}$$

を確かめれば定理の証明が終わる. 実際, $\overline{x} = \overline{\{x_i\}} \in \widehat{G}$ をとると

$$\begin{array}{ccccc} \overline{x} & \longmapsto & \overline{(\overline{x}, \overline{x}, \cdots)} & & \\ \downarrow & & & \searrow & \\ (\overline{x_1}, \overline{x_2}, \cdots) & \longmapsto & \left(\overline{\varphi(x_1)}, \overline{\varphi(x_2)}, \cdots\right) & & (\overline{x}, \overline{x}, \cdots) \end{array}$$

となるが $^\forall i$ について

$$\begin{aligned} \overline{x} - \overline{\varphi(x_i)} = 0 \quad &\Leftrightarrow \quad x - \varphi(x_i) \in \mathrm{C}_0\left(\widehat{G}\right) \\ &\Leftrightarrow \quad \overline{(x_1 - x_i, x_2 - x_i, \cdots, x_i - x_i, x_{i+1} - x_i, \cdots)} \in \widehat{G}_i \end{aligned}$$

であって, この 3 つのうちどれかをみたせばよい. しかし $^{\forall}j \geq i$ に対しては $x_i - x_j \in G_i$ ととれていた. よって, 上の diagram は可換である.

Exercise 19.

(1) A を環, $I \subsetneq A$; *an ideal* とせよ. このとき $G = A$, $G_n = I^n$ とすることによって *a topological abel group* $\mathrm{C}(A)$ を得られるが, この $\mathrm{C}(A)$ は積を $\{x_i\} \cdot \{y_i\} := \{x_i y_i\}$ によって定めると環となることを証明せよ.

(2) A を環として, M を *an A-module* とせよ. 今, $\{M_i\}$ *where* M_i は M の *an A-submodule* で $M_0 = M$ として $^{\forall}n \in \mathbb{Z}$ に対して $M_n \supseteq M_{n+1}$, とすると *a topological abel group* $\mathrm{C}(M)$ を得られるが, $^{\forall}a \in A$, $^{\forall}\{x_i\} \in \mathrm{C}(M)$ に対して $a \rightharpoonup \{x_i\} := \{ax_i\}$ という作用を定義することによって $\mathrm{C}(M)$ は *an A-module* であることを証明せよ.