2章 環 および 可換環

by K. Asai

キーワード: 環，可換環，単数，体，多項式環，全行列環，単数群，一般線形群，
部分環，同型，同型写像，イデアル，単項イデアル，剰余環，$\mathbf{Z}_n$，Euclid の互除法，
Euler の定理，有限体，準同型写像，準同型定理，同型定理，中国の剰余定理，
整域，単項イデアル整域，素イデアル，極大イデアル，局所化，
一意分解整域，Euclid 整域

1.（環の定義）集合 R が，和と積について閉じていて，以下の公理をみたすとき，R を 環 という.（積の記号は通常省略する）

$[R1]$	（加群）	R は加群，すなわち $+$ に関する可換群である.
$[R2{-}1]$	（結合律）	任意の $a,b,c \in R$ に対して，$(ab)c = a(bc)$ がなりたつ.
$[R2{-}2]$	（単位元）	$1 \in R$ が存在し，任意の $a \in R$ に対して， $a1 = 1a = a$ をみたす．この 1 を R の単位元という.
$[R3]$	（分配律）	任意の $a,b,c \in R$ に対して，$a(b+c) = ab + ac$, $(a+b)c = ac + bc$ がなりたつ.

(note) 環 R の加群としての単位元を 0 で表し，0 元という．a の和に関する逆元を a の反元といい，$-a$ とかく．すなわち，

$$a + (-a) = (-a) + a = 0 \tag{1}$$

をみたす元として，$-a$ が定義される．$-(-a) = a$ がなりたつ．なお，$a + (-b) = a - b$ と略記する.

(note) $[R2{-}2]$ の単位元の存在は仮定しないことがある．単位元が存在する環を単位的環という．ここでは特に断らない限り，単位的環を扱う.

(note) 環では和と積それぞれで結合律がみたされるので，1 つの演算の繰り返し: $a_1 + a_2 + \cdots + a_n$ および $a_1 a_2 \ldots a_n$ は括弧の付け方によらない．したがってこのような式では括弧は省略されることが多い.

(Def) 環 R が積に関する交換律: $ab = ba$ $(a,b \in R)$ をみたすとき，R を 可換環 あるいは 可換である という.

(note) 環の特定の元 a,b が $ab = ba$ をみたすとき，a と b は可換であるという.

(ex1) 0 のみからなる環を 0 環または自明な環という．これはもちろん可換環であり，この環では $0 = 1$ である．それ以外の環では，$0 \neq 1$ である.

(ex2) $\mathbf{Z}$，$\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$ は可換環であることを示せ．

(ex3) 環 R において次を示せ． (1) $a0 = 0a = 0$． (2) $(-a)b = a(-b) = -(ab)$，$(-a)(-b) = ab$． (3) $a(b_1 + \cdots + b_n) = ab_1 + \cdots + ab_n$，$(a_1 + \cdots + a_n)b = a_1b + \cdots + a_nb$．

(hint) (1) $a0 + a0 = \cdots$， $0a + 0a = \cdots$ を考えよ． (2) $-a$（a の反元）とは，$a + (-a) = (-a) + a = 0$ をみたす元のこと．それをふまえて，$ab + (-a)b = \cdots$，$(-a)(-b) - ab = \cdots$ 等を考えよ．

環 R の元 a に対して R の元 b が存在し，

$$ab = ba = 1 \tag{2}$$

をみたすとき，a を R の 単数 （または単元，可逆元）といい，b を a の逆元という．すなわち，R の単数とは R の中に逆元が存在する元である．群の場合同様，a の逆元を a^{-1} とかく．a, c を単数とするとき，$(a^{-1})^{-1} = a$，$(ac)^{-1} = c^{-1}a^{-1}$ がなりたつ．

$1 \neq 0$ を含み（すなわち 0 環ではなく），0 以外のすべての元が単数である可換環を 体 と呼ぶ．$\mathbf{Q}$ (有理数体)，$\mathbf{R}$ (実数体)，$\mathbf{C}$ (複素数体) は体の例である．

2.（環の例）整数係数の x の多項式全体の集合を $\mathbf{Z}[x]$ とかく．この中には 0 次の多項式（すなわち 0 でない定数）や 0 も含まれていることに注意する．$\mathbf{Z}[x]$ は可換環である．より一般に，R を可換環として，R の元を係数とする x の多項式全体の集合を $R[x]$ とかく．$R[x]$ は可換環である．たとえば，$\mathbf{Q}[x]$，$\mathbf{R}[x]$，$\mathbf{C}[x]$ は可換環である．$R[x]$ を R 上の 多項式環 といい，その元を R 上の多項式という．さらに，‘変数’ を増やして，R 上の，$x_1, x_2, \ldots, x_n$ の多項式全体の集合を $R[x_1, \ldots, x_n]$ とかく．これは可換環であり，R 上の多変数多項式環と呼ばれる．ここで見たような記号 x あるいは $x_1, \ldots, x_n$ は環 R とは独立な元であり，不定元と呼ばれる．

Ω を $\mathbf{R}$ の適当な部分集合とする．Ω 上の（Ω で定義された）連続な実関数全体のなす集合 $C(\Omega)$ は関数の和と積に関して可換環となる．より一般に Ω を $\mathbf{R}^n$ の部分集合とすれば，Ω 上の連続な n 変数実関数全体の集合 $C(\Omega)$ はまた可換環になる．さらに条件を付けて，Ω 上の C^r 級関数全体の集合 $C^r(\Omega)$ はまた可換環となる．Ω 上の C^∞ 級関数全体の集合 $C^\infty(\Omega)$ も同様である．

R を可換環とする．ある固定された n に対して，R の元を成分とする n 次行列全体の集合 $M_n(R)$ は環である．これを R 上の n 次 全行列環 という．その 0 元は n 次 0 行列 $O_{n,n}$ であり，単位元は n 次単位行列 E_n である．A の反元は $-A$ である．全行列環は，$n \geq 2$ のとき一般に非可換である．これは特に $R = \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ の場合が重要である．R が非単位的な（単位元がない）可換環のときも $M_n(R)$ は同様に定義され，これは非単位的な環になる．

整数 a, b に対して，$a + bi$ を Gauss の整数という．Gauss の整数全体の集合

$$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\} \tag{3}$$

は可換環である．$\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$ などもまた，可換環である．

3.（単数群）環 R のすべての単数からなる集合は乗法群をなす．これを R の 単数群 といい，$R^\times$ で表す．$R^\times$ が乗法群になることを以下に示す．

($\because$) 環の公理より，$R^\times$ は積に関する結合律をみたす．単位元 1 の存在は明らか．$a \in R^\times \Rightarrow a^{-1} \in R^\times$ より，逆元が存在する．最後に，$a, b \in R^\times$ ならば $(ab)^{-1} = b^{-1}a^{-1} \in R$ となって，$ab \in R^\times$．ゆえに，$R^\times$ は積について閉じている． (q.e.d.)

(ex4) (1) $\mathbf{Z}$ の単数群は $\{1, -1\}$ である．(2) $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ の単数群は，それぞれ $\mathbf{Q}^\times$，$\mathbf{R}^\times$，$\mathbf{C}^\times$ である．(3) $\mathbf{Z}[i]$ の単数群は，$\{1, i, -1, -i\}$ である．

R を可換環とする．$M_n(R)$ の単数群を $GL(n, R)$ で表し，これを R 上の n 次 一般線形群 という．K が体であれば，$GL(n, K)$ は $M_n(K)$ の中の正則な行列全体からなる．$GL(n, R)$ の部分群として，（R 上 n 次の）特殊線形群 $SL(n, R)$，直交群 $O(n, R)$，特殊直交群 $SO(n, R)$ が 1 章同様次のように定められる．

$$\begin{array}{l} SL(n,R) = \{X \in GL(n,R) \mid |X| = 1\} \\ O(n,R) = \{T \in GL(n,R) \mid T^t T = {}^t T T = E_n\} \\ SO(n,R) = \{T \in O(n,R) \mid |T| = 1\} \end{array} \tag{4}$$

このとき，1 章 (T16)(i) は，K を可換環 R に置き換えてもなりたつ．(ii) は K が体または整域 (⇒13 節) でなりたつ．その証明は (T16) とほぼ同様である．これを 1 章 (T16') とする．

1 章 (T16'): R を可換環，K を体または整域とするとき，次がなりたつ．

$$\text{(i) } GL(n,R)/SL(n,R) \simeq R^\times. \qquad \text{(ii) } \begin{array}{l} O(n,R)/SO(n,R) \simeq \{x \in R \mid x^2 = 1\}. \\ O(n,K)/SO(n,K) \simeq \{1, -1\}. \end{array} \tag{5}$$

(ex5) $GL(n, \mathbf{Z}) = \{X \in M_n(\mathbf{Z}) \mid |X| = \pm 1\}$ を示せ．

(ex6) 環 R の単数群 $R^\times$ が有限群で，$|R^\times| = n$ のとき，任意の単数 a に対して，$a^n = 1$ である．

($\because$) $|R^\times| = n$，$a \in R^\times$ とする．1 章 (T18) より，a の位数 m は $R^\times$ の位数 n の約数なので，$n = mk$ とかける．ゆえに，

$$a^n = a^{mk} = (a^m)^k = 1^k = 1. \qquad \text{(q.e.d.)} \tag{6}$$

4.（部分環）R を環とする．R の部分集合 S が R と同じ演算に関して環であり，R の単位元 1 を含むとき，S を R の 部分環 という．R 自身は必ず R の部分環になる．これを自明な部分環という．

(ex7) (1) $\mathbf{Z}$ は $\mathbf{Q}$ の部分環である．$\mathbf{Q}$ は $\mathbf{R}$ の部分環である．$\mathbf{R}$ は $\mathbf{C}$ の部分環である．

(2) $\mathbf{Z}$ は $\mathbf{Z}[i]$ の部分環である． (3) $\mathbf{Z}$ の自明でない部分環は存在しない．

(ex8) R を可換環とする．S が R の部分環のとき，$M_n(S)$ は $M_n(R)$ の部分環となる．その具体例をあげよ．

(ex9) R を可換環とする．$i > j \Rightarrow a_{ij} = 0$ をみたす行列 (a_{ij}) を上三角行列といい，$i < j \Rightarrow a_{ij} = 0$ をみたす行列 (a_{ij}) を下三角行列という．$T_n^+(R)$ で，R の元を成分とする n 次上三角行列全体の集合を表し，$T_n^-(R)$ で R の元を成分とする n 次下三角行列全体の集合を表す．$D_n(R)$ で，R の元を成分とする n 次対角行列全体の集合を表す．$D_n(R)$ は $T_n^+(R)$ および $T_n^-(R)$ の部分環であり，$T_n^+(R)$ および $T_n^-(R)$ は $M_n(R)$ の部分環である．

(T1) R を環とする．S が R の部分環になるための必要十分条件は，S が R の部分加群で，単位元を含み，積について閉じていることである．

($\because$) S を R の部分環とする．S が R の部分加群で，単位元を含み，積について閉じていることは定義より明らか．逆にそれがみたされるとする．R が環であることから，S においても結合律，分配律がなりたつことになるので，S は R の部分環になる． (q.e.d.)

(T2) R の部分環 S，S' に対して，$S \cap S'$ はまた R の部分環である．

($\because$) (T1) を用いる．S，S' は R の部分加群なので，1 章 (T2) より，$S \cap S'$ は R の部分加群である．$S \cap S'$ が単位元を含むことは明らか．$a, b \in S \cap S'$ を任意に取るとき，S が部分環なので $ab \in S$．同様に，S' が部分環なので $ab \in S'$． $\therefore\ ab \in S \cap S'$．ゆえに，$S \cap S'$ は R の部分環である． (q.e.d.)

3 つ以上の部分群についても (T2) と同様のことがなりたつ．あるいは無限個の部分群についても次のように一般化される．

(T2') R の部分環 S_λ $(\lambda \in \Lambda)$ に対して，$\bigcap_{\lambda\in\Lambda} S_\lambda$ はまた R の部分環である．

5.（環の同型）R, R' を 2 つの環とする．R から R' への 1 対 1 対応 ϕ が存在して次をみたすとき，R と R' は 同型 であるといい，$R \simeq R'$ とかく．

$$\begin{aligned} &\phi(a+b) = \phi(a) + \phi(b) && (a, b \in R) \\ &\phi(ab) = \phi(a)\phi(b) && (a, b \in R) \end{aligned} \tag{7}$$

この ϕ を R から R' への (環) 同型写像 という．

(note) (1) 同型写像は複数個存在することもある． (2) 同型写像を単に環同型，同型ともいう．

(ex10) 同型写像 ϕ に対して，$\phi(0) = 0$，$\phi(1) = 1$ を示せ．

(ex11) R から R' への同型写像 ϕ の逆写像は，R' から R への同型写像になることを示せ．

($\because$) 群の場合と同様なので，省略する．

(note) 群の場合と同様，次がなりたつ．

(i) $R \simeq R$.　(ii) $R \simeq R' \Rightarrow R' \simeq R$.　(iii) $R \simeq R'$，$R' \simeq R'' \Rightarrow R \simeq R''$.

(ex12) R を可換環とする．x, y を不定元とするとき，$R[x] \simeq R[y]$.

($\because$) 写像 $\phi : R[x] \longrightarrow R[y]$ を $\phi(p(x)) = p(y)$ $(p(x) \in R[x])$ で定める．このとき，ϕ は明らかに同型写像である． (q.e.d.)

(ex13) 環 R およびその部分環 S を次で定める．(1) $R \simeq \mathbf{C}$ を示せ． (2) $S \simeq \mathbf{Z}[i]$ を示せ．

$$\begin{aligned} R &= \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbf{R} \right\} \\ S &= \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbf{Z} \right\} \end{aligned} \tag{8}$$

6.（イデアル）R を環とする．R の部分集合 I が次をみたすとき，I を R の **イデアル** という．

$$\begin{aligned} &\text{i:} \quad R \text{ を加群と見たとき，} I \text{ は } R \text{ の部分加群である．} \\ &\text{ii:} \quad r \in R,\ x \in I \ \Rightarrow\ rx, xr \in I. \end{aligned} \tag{9}$$

ii: のところを，ii-l: $r \in R$，$x \in I \Rightarrow rx \in I$ でおきかえるとき，I を左イデアル，
ii-r: $r \in R$，$x \in I \Rightarrow xr \in I$ でおきかえるとき，I を右イデアルという．
このイデアルの定義は，i: を部分加群であるための条件に置き換えて，

$$\text{i':} \quad x, y \in I \ \Rightarrow\ x - y \in I \tag{10}$$

としてもよく，さらにまた R が単位的で $-1 \in R$ であることから，i: を次に代えてもよい．

$$\text{i''}: \quad x, y \in I \ \Rightarrow\ x + y \in I \tag{11}$$

R および，$\{0\}$ はつねに R のイデアルになる．これを自明なイデアルという．可換環においては，イデアル，左イデアル，右イデアルの区別はない．

R の部分集合 S を取る．後に述べる (T4)(iii) により，S を含むすべての R のイデアルの交わり I は，また R のイデアルになる．これを，

$$I = (S) \tag{12}$$

で表し，S で生成された R のイデアルという．I は S を含む R の任意のイデアルに含まれるので，S を含む R の最小のイデアルとなる．

.....

(T3) 環 R の部分集合 S に対して，

$$(S) = \left\{ \sum_{k=1}^{n} r_k g_k r'_k \mid r_k, r'_k \in R,\ g_k \in S\ (k = 1, \ldots, n);\ n = 1, 2, \ldots \right\}. \tag{13}$$

特に R が可換で，$S = \{g_1, \ldots, g_s\}$ のとき，

$$(S) = \{r_1 g_1 + \cdots + r_s g_s \mid r_1, \ldots, r_s \in R\}. \tag{14}$$

.....

($\because$) (14) は (13) から容易に得られるので，(13) を示す．(13) 右辺を J とする．(S) はともかくも S を含む R のイデアルなので，イデアルの定義より，少なくとも J を含ま

なければならない．すなわち $(S) \supset J$ (*)．そこで J が R のイデアルとなることを言う．J の任意の 2 元 x, y を

$$x = \sum_{k=1}^{n} r_k g_k r'_k, \qquad y = \sum_{k=1}^{m} q_k g'_k q'_k \tag{15}$$

とし，任意の $r \in R$ を取るとき，

$$\begin{aligned} x + y &= \sum_{k=1}^{n} r_k g_k r'_k + \sum_{k=1}^{m} q_k g'_k q'_k \in J, \\ rx = \sum_{k=1}^{n} r r_k g_k r'_k \in J, &\qquad xr = \sum_{k=1}^{n} r_k g_k r'_k r \in J. \end{aligned} \tag{16}$$

ゆえに，J は R のイデアルとなる．また明らかに $J \supset S$．ゆえに (S) の最小性より，$(S) \subset J$ (**)．(*),(**) より，$(S) = J$．(q.e.d.)

一般に，環 R の部分集合 A, B に対しては，それらの和，積を群の場合と同様に，

$$\begin{aligned} A + B &= \{a + b \mid a \in A,\, b \in B\} \\ AB &= \{ab \mid a \in A,\, b \in B\} \end{aligned} \tag{17}$$

で定義する．これらはまた R の部分集合となっている．このとき，これらの演算については結合律がなりたつことは，群の場合と同様である．

特に，I, J を R のイデアルとするとき，上述の定義では，一般には IJ はイデアルにはならないので，代りに (IJ)，すなわち IJ で生成されたイデアルを考える．まぎれのないときには，

$$(IJ) = IJ \tag{18}$$

とかくこともあるが，本書では括弧つきで表す．

ただ 1 つの元 a で生成されたイデアル (a) を 単項イデアル または 主イデアル という．(T3) より，次を得る．

.....

(T3') 環 R の元 a に対して，

$$(a) = \left\{ \sum_{k=1}^{n} r_k a r'_k \mid r_k, r'_k \in R,\ (k = 1, \ldots, n);\ n = 1, 2, \ldots \right\}. \tag{19}$$

特に R が可換ならば，

$$\begin{aligned} (a) &= \{ra \mid r \in R\} = Ra \\ &= \{ar \mid r \in R\} = aR. \end{aligned} \tag{20}$$

.....

(ex14) (1) n を正の整数とするとき，$n\mathbf{Z}$ すなわち n のすべての倍数の集合は，$\mathbf{Z}$ のイデアルである．

(2) m, n を正の整数とするとき，$M_n(m\mathbf{Z})$ は $M_n(\mathbf{Z})$ のイデアルである．たとえば，偶数を成分として持つ 2 次行列の集合 $M_2(2\mathbf{Z})$ は，整数を成分として持つ 2 次行列の集合 $M_2(\mathbf{Z})$ のイデアルである．

(3) R を可換環とする．$g(x)$ を R 上の多項式とする．$g(x)$ で割りきれる R 上の多項式を，$g(x)$ の倍元という．$g(x)$ の倍元全体の集合を I とすると，I は $R[x]$ のイデアルになり，$I = (g(x))$.

. . . . . .

(T4) I, J; I_λ $(\lambda \in \Lambda)$ を R のイデアルとするとき，次がなりたつ.

(i) $I + J$ は R のイデアルである． (ii) $I \cap J$ は R のイデアルである． (iii) $\bigcap_{\lambda\in\Lambda} I_\lambda$ は R のイデアルである.

(iv)

$$(IJ) = \left\{ \sum_{k=1}^{n} x_k y_k \mid x_k \in I,\ y_k \in J\ (k = 1, \ldots, n);\ n = 1, 2, \ldots \right\}. \tag{21}$$

. . . . . .

($\because$) I, J を R のイデアルとする.

(i) $I + J$ が R の部分加群となることは，$x, x' \in I$，$y, y' \in J$ とするとき，$(x + y) - (x' + y') = (x - x') + (y - y') \in I + J$ となることからわかる．また $r \in R$ とするとき，$r(x + y) = rx + ry \in I + J$，$(x + y)r = xr + yr \in I + J$ である．ゆえに $I + J$ は R のイデアルである． (q.e.d.)

(ii) I, J が R の部分加群なので，$I \cap J$ は R の部分加群になる．また $r \in R$，$x \in I \cap J$ とするとき，$x \in I$ なので，$rx \in I$ かつ $xr \in I$．さらに $x \in J$ なので，$rx \in J$ かつ $xr \in J$．ゆえに，$rx \in I \cap J$ かつ $xr \in I \cap J$．ゆえに，$I \cap J$ は R のイデアルである．(q.e.d.)

(iii) (ii) と同様なので省略.

(iv) (T3) において，$S = IJ$ としてやれば,

$$\begin{aligned} (IJ) = &\left\{ \sum_{k=1}^{n} r_k x'_k y'_k r'_k \mid r_k, r'_k \in R,\ x'_k y'_k \in IJ\ (k = 1, \ldots, n);\ n = 1, 2, \ldots \right\} \\ = &\ \text{(21) 右辺.} \qquad \text{(q.e.d.)} \end{aligned} \tag{22}$$

(ex15) $\mathbf{Z}$ のイデアル $I = 2\mathbf{Z}$ および $J = 3\mathbf{Z}$ に対して次を求めよ．(1) $I + J$．(2) $I \cap J$．(3) (IJ).

R のイデアル I, J について，明らかに $IJ \subset I \cap J$ がなりたつ．ここで，$I \cap J$ はイデアルであり，(IJ) は IJ を含む最小のイデアルなので,

$$(IJ) \subset I \cap J \tag{23}$$

がなりたつことになる．また，I, J を共に含むイデアルを I' とすれば，イデアルが加群であることから，明らかに $I + J \subset I'$．ゆえに，$I + J$ は I, J を含む最小のイデアルである．したがって,

$$(I \cup J) = I + J \tag{24}$$

を得る．これらのことは，3 つ以上のイデアルについても同様になりたつ.

次に，$I_1, I_2, \ldots, I_s$ を R のイデアルとする．(T4)(iv) と同様にして，$I_1 I_2 \ldots I_s$ で生成されたイデアル $(I_1 I_2 \ldots I_s)$ を表示できる．また，(IJ) という演算について，結合律がなりたつことがわかる.

以上を定理の形でまとめておく.

(T5) $I_1, I_2, \ldots, I_s$ を R のイデアルとするとき，

$$\begin{gathered}(I_1 \ldots I_s) = \left\{ \sum_{k=1}^{n} x_k \ldots z_k \mid x_k \in I_1, \ldots, z_k \in I_s \ (k = 1, \ldots, n);\ n = 1, 2, \ldots \right\} \\ ((I_1 I_2) I_3) = (I_1 (I_2 I_3)) \\ (I_1 \ldots I_s) \subset I_1 \cap \cdots \cap I_s, \qquad (I_1 \cup \cdots \cup I_s) = I_1 + \cdots + I_s.\end{gathered} \tag{25}$$

7.（剰余環）R を環，I をそのイデアルとする．加群としての剰余群 R/I を考える．

$$R/I = \{I + a \mid a \in R\} \tag{26}$$

であり，その各元 $I + a$ を I に関する（I を法とする）a の剰余類という．簡単のため，$I + a = \overline{a}$ とかくことにする．このとき，剰余群 G/H の演算法則

$$(Hg)(Hg') = H(gg') \tag{27}$$

を R/I の場合にあてはめれば，

$$\begin{gathered}(I + a) + (I + b) = I + (a + b), \quad \text{すなわち,} \\ \overline{a} + \overline{b} = \overline{a + b}\end{gathered} \tag{28}$$

を得る．さらに，$x + a \in \overline{a}$，$y + b \in \overline{b}$ $(x, y \in I)$ を任意に取ると，

$$(x + a)(y + b) = xy + xb + ay + ab = x' + ab \in \overline{ab} \tag{29}$$

となるので，

$$\overline{a}\,\overline{b} \subset \overline{ab} \tag{30}$$

がなりたつ．ここで，新しい積演算として，

$$\overline{a} * \overline{b} = \overline{ab} \tag{31}$$

を定義することができる．このとき，加群としての剰余群 R/I に積演算が追加され，新しい環が生じる．この環を R の I による $\boxed{\text{剰余環}}$，あるいは I を法とする R の剰余環といい，やはり R/I で表す．剰余環 R/I におけるこの積 $*$ の定義は，剰余類の各元を取り出して積を計算したとき，計算した結果が属する剰余類がただ 1 つ決まるので，それを積 $*$ の結果として指定するという演算の方法であって，そのことは R/I における和についても同様である．したがって，R/I における結合律および分配律:

$$\begin{aligned}&(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}), \qquad (\overline{a} * \overline{b}) * \overline{c} = \overline{a} * (\overline{b} * \overline{c}), \\ &\overline{a} * (\overline{b} + \overline{c}) = \overline{a} * \overline{b} + \overline{a} * \overline{c}, \qquad (\overline{a} + \overline{b}) * \overline{c} = \overline{a} * \overline{c} + \overline{b} * \overline{c}\end{aligned} \tag{32}$$

は，もとの R においてそれらの計算法則がなりたっているので，やはりなりたっていると言える．たとえば，

$$\begin{gathered}(\overline{a} * \overline{b}) * \overline{c} = \overline{ab} * \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} * \overline{bc} = \overline{a} * (\overline{b} * \overline{c}), \\ \overline{a} * (\overline{b} + \overline{c}) = \overline{a} * \overline{b + c} = \overline{a(b + c)} \\ = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} * \overline{b} + \overline{a} * \overline{c}.\end{gathered} \tag{33}$$

また，単位元 $\overline{1}$ が存在するので，R/I は確かに環であると言える．R/I における和は (17) と一致するが，積については (17) の定義とは異なることに注意すべきである．通常はまぎれが生じないので，積の記号 $*$ は省略される．

(ex16) 極端な例であるが，環 R に対して，自明なイデアル R，$\{0\}$ を取ると，$R/R \simeq \{0\}$，$R/\{0\} \simeq R$ となる．

8.（$\mathbf{Z}_n$ と Euclid の互除法）n を正の整数とする．環 $\mathbf{Z}$ に対してイデアル $n\mathbf{Z}$ を取る．剰余環 $\mathbf{Z}/n\mathbf{Z}$ を $\mathbf{Z}_n$ とかき，これを n を法とする整数の環という．これは集合としては，

$$\mathbf{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} \tag{34}$$

である．その演算は，modulo n による計算と一致する．まぎれのない場合は，$\overline{x} = x$ とかいて計算してよい．

(ex17) (1) $1 \leq n \leq 12$ に対して，$\mathbf{Z}_n$ の加法表および乗法表をつくれ．(2) $\mathbf{Z}_{19}$ において，7^{-1} を求めよ．(3) $\mathbf{Z}_{19}$ において，$8\cdot 3 + 7\cdot 3 - 8\cdot 15 - 7\cdot 15$ を求めよ．(4) $\mathbf{Z}_{108}$ において，11^{-1} を求めよ．

(ex17) (2),(4) のように，n が大きいとき，$\mathbf{Z}_n$ における x の逆元を求めるのは簡単ではない．これを求めるために，Euclid の互除法を利用する方法がある．Euclid の互除法とは，与えられた整数 r_0, r_1 に対して，

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\cdots\cdots \\ r_{s-1} &= r_s q_s + r_{s+1} \\ r_s &= r_{s+1} q_{s+1} \end{aligned} \tag{35}$$

のように，余りがなくなるまで割り算を続けるアルゴリズムである．このとき，r_{s+1} は r_0 と r_1 の最大公約数となる．

$\mathbf{Z}_n$ において，x^{-1} を求める場合，$r_0 = n$，$r_1 = x$ とおいて，Euclid の互除法を行う．すると，逆元は存在するならば，最終行の 1 つ手前では余りが 1 になる，すなわち $r_{s+1} = 1$ となる．そこで，

$$\begin{aligned} r_0 - r_1 q_1 &= r_2 \\ r_1 - r_2 q_2 &= r_3 \\ &\cdots\cdots \\ r_{s-2} - r_{s-1} q_{s-1} &= r_s \\ r_{s-1} - r_s q_s &= 1 \end{aligned} \tag{36}$$

のように書き換える．最終行から順に r_k を r_{k-1}，r_{k-2} を用いて表していくと，結局，

$$1 = m_1 r_1 + m_0 r_0 = m_1 x + m_0 n \equiv m_1 x \equiv yx \pmod{n} \tag{37}$$

の形の式を得る．ここに，$0 \leq y < n$ である．これより，$\mathbf{Z}_n$ において $yx = xy = 1$ となり，$x^{-1} = y$ と求まる．

$\mathbf{Z}_n$ の単数については次の定理がなりたつ．

(T6) 剰余環 $\mathbf{Z}_n$ において，x が単数（逆元がある元）であるためには，x が n と互いに素（最大公約数が 1）であることが必要十分である．

この定理の証明には，以下の補題が必要となる．（一般的な形であげておく） 整数 $g_1, g_2, \ldots, g_s$ の最大公約数を $\gcd(g_1, \ldots, g_s)$ で表す．（ただし，$s = 2$ のとき $\gcd(g_1, g_2) = (g_1, g_2)$ と略記することがある．） a が b で割りきれるとき，$b \mid a$ とかく．

(L1) $g_1, g_2, \ldots, g_s$ を正の整数とし，$\gcd(g_1, \ldots, g_s) = d$ とするとき，整数 $m_1, m_2, \ldots, m_s$ が存在して，次がなりたつ．

$$m_1 g_1 + m_2 g_2 + \cdots + m_s g_s = d \tag{38}$$

($\because$) 与えられた正の整数 $g_1, g_2, \ldots, g_s$ に対して，整数 $m_1, \ldots, m_s$ が動くとき，(38) 左辺の形で表される値のうちで，もっとも小さい正の整数を a とおく．それを，

$$m_1 g_1 + m_2 g_2 + \cdots + m_s g_s = a \tag{39}$$

とかく．$g_1, \ldots, g_s$ の最大公約数を d とすると，$g_k = dq_k$ とかけるので，

$$\begin{aligned} m_1 g_1 + m_2 g_2 + \cdots + m_s g_s = \quad & d(m_1 q_1 + m_2 q_2 + \cdots + m_s q_s) = a. \\ \therefore \quad & d \mid a. \end{aligned} \tag{40}$$

次に任意の g_k を取り，これを a で割って $g_k = aq + r$ $(0 \le r < a)$ となったとすると，

$$\begin{aligned} r \quad &= g_k - aq = g_k - (m_1 g_1 + \cdots + m_s g_s)q \\ &= -m_1 q g_1 - \cdots + (1 - m_k q) g_k - \cdots - m_s q g_s. \end{aligned} \tag{41}$$

ところが，この式は (38) の左辺と同じ形であり，その正の最小値が $a > r$ であることから，$r = 0$ となる． $\therefore$ $a \mid g_k$．ゆえに，a は $g_1, \ldots, g_s$ の公約数である．ところが d は最大公約数だったので $d \ge a$．これと $d \mid a$ より，$d = a$ となる． (q.e.d.)

これより，次の系を得る．

(L2) $g_1, g_2, \ldots, g_s$ を正の整数とする．$\gcd(g_1, \ldots, g_s) = 1$ であるための必要十分条件は，整数 $m_1, m_2, \ldots, m_s$ が存在して，次がなりたつことである．

$$m_1 g_1 + m_2 g_2 + \cdots + m_s g_s = 1 \tag{42}$$

($\because$) $\gcd(g_1, \ldots, g_s) = 1$ とする．(L1) より，(42) がなりたつ．

逆に，(42) がなりたつとする．$\gcd(g_1, \ldots, g_s) = d$ とすると，$d \mid g_k$ $(k = 1, \ldots, s)$ なので，(42) より，$d \mid 1$． $\therefore$ $d = 1$． (q.e.d.)

(L1)，(L2) は $s = 2$ の場合によく用いる．特に，(L2) の $s = 2$ の場合をかいておく．

(L2') $(g, g') = 1 \iff mg + m'g' = 1$ となる整数 m, m' が存在する．

これを用いて，(T6) を証明できる．

($\because$) (T6) $\mathbf{Z}_n$ において，x が単数とすると，$xy = 1$ となる $y \in \mathbf{Z}_n$ が存在する．したがって，通常の計算では $xy + mn = 1$ となる．(L2') より，これは $(x, n) = 1$ を示す．

逆に，$x \in \mathbf{Z}$ が $(x, n) = 1$ をみたすとすると，(L2') より $mx + m'n = 1$ となる整数 m, m' が存在する．ここで $m = nq + r$ $(0 \leq r < n)$ となる r を取れる．このとき，

$$rx = (m - nq)x = mx - nqx = 1 - m'n - nqx \equiv 1 \pmod{n}. \tag{43}$$

これは，$\mathbf{Z}_n$ において，$rx = xr = 1$ を示す．ゆえに x は単数である． (q.e.d.)

$\mathbf{Z}_n$ の単数群 $\mathbf{Z}_n^\times$ については，(T6) より，

$$\mathbf{Z}_n^\times = \{x \in \{0, 1, \ldots, n-1\} \mid (x, n) = 1\} \tag{44}$$

と表される．ここで $|\mathbf{Z}_n^\times| = \varphi(n)$ とおく．$\varphi(n)$ は n と互いに素な n 以下の正の整数の数であり，この関数 φ を Euler の関数と呼ぶ．そこで (ex6) を用いると，$x \in \mathbf{Z}_n^\times$ ならば，$x^{\varphi(n)} = 1$ がなりたつことがわかる．ゆえに，次を得る．

(T7) (Euler の定理) n を正の整数とし，整数 a が $(a, n) = 1$ をみたすならば，$a^{\varphi(n)} \equiv 1 \pmod{n}$.

p を素数とする．(T6) より，$\mathbf{Z}_p$ の 0 以外のすべての元は，p と互いに素なので，必ず単数になる．$n > 1$ が素数でないとき，$\mathbf{Z}_n$ のある 0 でない元は，n と互いに素ではないので，単数にならない．$\mathbf{Z}_1$ は 0 のみからなる 0 環なので，体ではない．以上をまとめると，次を得る．

(T8) $\mathbf{Z}_p$ が体 $\iff$ p が素数.

素数 p に対して $\mathbf{Z}_p$ は p 個の元を持つ体であり，これは有限個の元からなる体，すなわち 有限体 の一種である．体は可換なので，$ab^{-1} = b^{-1}a = \frac{a}{b}$ とかくことが多い．これを a の b による商という．

(ex18) (1) $1 \leq n \leq 12$ について，$\mathbf{Z}_n^\times$ を決定し，各元の逆元を求めよ．

(2) $\mathbf{Z}_7$ において，$\frac{1+2+3+6}{1-2-3+6}$ を求めよ．また，$\frac{1^{-1}+2^{-1}+3^{-1}+6^{-1}}{1^{-1}-2^{-1}-3^{-1}+6^{-1}}$ を求めよ．

(3) $\mathbf{Z}_n$ において $(n-1)^{-1} = n-1$ を示せ．また，n が 3 以上の奇数のとき，$\mathbf{Z}_n$ において $1 + 2 + \cdots + (n-1) = 0$ を示せ．

(ex19) (1) $R = M_2(\mathbf{Z})$ とする．$I = M_2(2\mathbf{Z})$ は R のイデアルである．このとき剰余環 R/I はどのような環になるか？ またこの環の加法表と乗法表をつくれ．

(2) $R = M_n(\mathbf{Z})$，$I = M_n(m\mathbf{Z})$ のとき，R/I を求めよ．

(3) $R = \mathbf{Z}[x]$ とする．$g(x) = x^2+2$ とおく．剰余環 $R/(g(x))$ において，$(x+3)(x-1)(x-5)$ を求めよ．

(4) $R = \mathbf{Z}_3[x]$ とする．$g(x) = x^2 + 1$ とおく．剰余環 $R/(g(x))$ の加法表と乗法表を作れ．この環は体か？

9.（環の準同型定理）R, R' を 2 つの環とする．写像 $\phi : R \longrightarrow R'$ が

$$\begin{array}{ll} \phi(a+b) = \phi(a) + \phi(b) & (a, b \in R) \\ \phi(ab) = \phi(a)\phi(b) & (a, b \in R) \\ \phi(1) = 1 & \end{array} \tag{45}$$

をみたすとき，ϕ を R から R' への $\boxed{\text{(環) 準同型写像}}$ あるいは (環) 準同型という．ϕ がさらに全射であれば，全準同型 (写像) といい，ϕ が単射であれば，単準同型 (写像) という．もし ϕ が 1 対 1 対応であれば，(環) 同型写像と呼ぶことはすでに [5.] で述べた．

$\phi : R \longrightarrow R'$ を準同型とする．群の場合と同様，R の部分集合 A に対して，

$$\phi(A) = \{\phi(a) \mid a \in A\} \tag{46}$$

と定め，これを ϕ による A の像という．特に，$\phi(R) = \mathrm{Im}\,\phi$ を ϕ の像という．また，R' の部分集合 A' に対して，

$$\phi^{-1}(A') = \{a \in R \mid \phi(a) \in A'\} \tag{47}$$

と定め，これを ϕ による A' の逆像という．特に，

$$\phi^{-1}(0) = \{a \in R \mid \phi(a) = 0\} = \mathrm{Ker}\,\phi \tag{48}$$

を ϕ の核という．

(ex20) 準同型 $\phi : R \longrightarrow R'$ に対して次を示せ．(1) $\phi(0) = 0$．(2) $\phi(-a) = -\phi(a)$．(3) $\phi(a_1 + \cdots + a_s) = \phi(a_1) + \cdots + \phi(a_s)$．(4) $\phi(a_1 \ldots a_s) = \phi(a_1) \ldots \phi(a_s)$．

次がなりたつ．

. . . . . .

(T9) $\phi : R \longrightarrow R'$ を準同型とする．(i) $\mathrm{Ker}\,\phi$ は R のイデアルである．(ii) $\mathrm{Im}\,\phi$ は R' の部分環である．(iii) ϕ が単準同型 $\iff \mathrm{Ker}\,\phi = \{0\}$．

. . . . . .

($\because$) (i) ϕ を加群としての準同型とみれば，1 章 (T8) より，$\mathrm{Ker}\,\phi$ は R の部分加群である．さらに，$x \in \mathrm{Ker}\,\phi$，$r \in R$ とすると，$\phi(rx) = \phi(r)\phi(x) = 0$．$\therefore\ rx \in \mathrm{Ker}\,\phi$．$\phi(xr) = \phi(x)\phi(r) = 0$．$\therefore\ xr \in \mathrm{Ker}\,\phi$．ゆえに，$\mathrm{Ker}\,\phi$ は R のイデアルである．(q.e.d.)

($\because$) (ii) ϕ を加群としての準同型とみれば，1 章 (T8) より，$\mathrm{Im}\,\phi$ は R' の部分加群である．また，$\phi(1) = 1 \in \mathrm{Im}\,\phi$．さらに，$a', b' \in \mathrm{Im}\,\phi$ のとき，$\phi(a) = a'$，$\phi(b) = b'$ となる $a, b \in R$ が存在し，

$$a'b' = \phi(a)\phi(b) = \phi(ab) \in \mathrm{Im}\,\phi \tag{49}$$

となるので，$\mathrm{Im}\,\phi$ は R' の部分環である．(q.e.d.)

($\because$) (iii) R を加群と見ると，1 章 (T9) より明らか．(q.e.d.)

環においても，準同型の合成はまた準同型になることなどは，群の場合と全く同様に示される．すなわち，

(T10) R, R', R'' を環とする．$\phi : R \longrightarrow R'$，$\psi : R' \longrightarrow R''$ を 2 つの準同型とするとき，その合成 $\psi \circ \phi : R \longrightarrow R''$ はまた準同型である．さらに，同型の合成はまた同型であり，全準同型の合成はまた全準同型であり，単準同型の合成はまた単準同型である．

R を環，S をその部分環とする．S から R への写像 m を

$$m(x) = x \qquad (x \in S) \tag{50}$$

で定めるとき，m を標準的単射という．これは単準同型である．次に，I を R のイデアルとする．R から R/I への写像 p を

$$p(a) = \overline{a} \qquad (a \in R) \tag{51}$$

で定めるとき，p を標準的全射という．これは全準同型である．

(ex21) (1) m が単準同型であることを示せ．(2) p が全準同型であることを示せ．

環においても，群と同様の準同型定理がなりたつ．

(T11)（準同型定理）R から R' への全準同型 ϕ に対して，$\mathrm{Ker}\,\phi = I$ とおく．R から R/I への標準的全射を p とおく．このとき，R/I から R' への同型写像 $\overline{\phi}$ であって，$\phi = \overline{\phi} \circ p$ をみたすものがただ 1 つ存在する．これにより，

$$R/I \simeq R' \tag{52}$$

を得る．

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R' \\ {\scriptstyle p}\downarrow & \overline{\phi}\nearrow & \\ R/I & & \end{array} \tag{53}$$

ϕ が準同型のときは，$R/I \simeq \mathrm{Im}\,\phi$ がなりたつ．

($\because$) 加群の準同型定理より，$\phi = \overline{\phi} \circ p$ をみたす加群としての同型写像 $\overline{\phi} : R/I \longrightarrow R'$ がただ 1 つ存在し，それは

$$\overline{\phi}(\overline{a}) = \phi(a) \qquad (a \in R) \tag{54}$$

で定められることがわかる．あとは，積についての準同型の式を確かめればよい．

$$\overline{\phi}(\overline{a}\,\overline{b}) = \overline{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(\overline{a})\,\overline{\phi}(\overline{b}). \tag{55}$$

ϕ が準同型のときは，ϕ を R から $\mathrm{Im}\,\phi$ への全準同型とみなせばよい．(q.e.d.)

10.（環の同型定理）群の場合と同様，環においても同型定理がなりたつ．これらは準同型定理を用いて導かれる．まず同型定理に関連する定理をあげておく．

(T12) R, R' を環，$\phi : R \longrightarrow R'$ を準同型とする．S を R の部分環，I を R のイデアルとし，S' を $\mathrm{Im}\,\phi$ の（R' の）部分環，I' を $\mathrm{Im}\,\phi$ の（R' の）イデアルとする．このとき，(i) $\phi(S)$ は $\mathrm{Im}\,\phi$ の部分環，$\phi(I)$ は $\mathrm{Im}\,\phi$ のイデアルである．(ii) $\phi^{-1}(S')$ は R の部分環，$\phi^{-1}(I')$ は R のイデアルである．

($\because$) (i) $\phi(I)$ が $\mathrm{Im}\,\phi$ のイデアルになることを示す．1 章 (T12) より $\phi(I)$ は加群になる．$r' \in \mathrm{Im}\,\phi$，$x' \in \phi(I)$ とすると，$r \in R$，$x \in I$ が存在して $r' = \phi(r)$，$x' = \phi(x)$ となるので，$r'x' = \phi(r)\phi(x) = \phi(rx) = \phi(y) \in \phi(I)$ $(y \in I)$．同様に，$x'r' \in \phi(I)$．(q.e.d.)

($\because$) (ii) $\phi^{-1}(I')$ が R のイデアルになることを示す．1 章 (T12) より $\phi^{-1}(I')$ は加群になる．$r \in R$，$x \in \phi^{-1}(I')$ とすると，$\phi(rx) = \phi(r)\phi(x) = r'x' \in I'$ $(r' \in \mathrm{Im}\,\phi,\, x' \in I')$．$\therefore$ $rx \in \phi^{-1}(I')$．同様に，$xr \in \phi^{-1}(I')$．(q.e.d.)

(T12') R, R' を環，$\phi : R \longrightarrow R'$ を準同型とする．$\mathrm{Ker}\,\phi$ を含む R のイデアル全体の集合 $\mathbf{S}$ から，$\mathrm{Im}\,\phi$ のイデアル全体の集合 $\mathbf{S}'$ への 1 対 1 対応 $\tilde{\phi}$ が，$\tilde{\phi}(I) = \phi(I)$ $(\tilde{\phi}^{-1}(I') = \phi^{-1}(I'))$ で得られる．この定理は，“イデアル” を “部分環” に置き換えてもなりたつ．

($\because$) 1 章 (T12') により，$\mathrm{Ker}\,\phi$ を含む部分加群の集合から $\mathrm{Im}\,\phi$ の部分加群の集合への 1 対 1 対応が $\tilde{\phi}(I) = \phi(I)$ で得られる．ところが，(T12) より，$\tilde{\phi}$ の定義域を $\mathbf{S}$ へ制限すると，$\mathbf{S}$ から $\mathbf{S}'$ への 1 対 1 対応が得られる．(q.e.d.)

(T13)（同型定理）

(i) R, R' を環，$\phi : R \longrightarrow R'$ を全準同型とし，I' を R' のイデアルとする．$\phi^{-1}(I') = I$ とおくと，I は R のイデアルとなり，

$$R/I \simeq R'/I'. \tag{56}$$

(ii) R を環，I を R のイデアルとし，S を R の部分環とする．このとき，

$$S/(S \cap I) \simeq (S + I)/I. \tag{57}$$

(iii) R を環，I, J を R のイデアルとし，$I \supset J$ とするとき，

$$R/I \simeq (R/J)/(I/J). \tag{58}$$

($\because$) (i) 全準同型の合成:

$$R \xrightarrow{\phi} R' \xrightarrow{p} R'/I' \tag{59}$$

（p は標準的全射）を考えると，$p \circ \phi : R \longrightarrow R'/I'$ を得るが，それは (T10) より全準同型になる．そして，

$$\mathrm{Ker}(p \circ \phi) = (p \circ \phi)^{-1}(I') = \phi^{-1} \circ p^{-1}(I') = \phi^{-1}(I') = I \tag{60}$$

となる．そこで，$p \circ \phi$ に準同型定理を適用して，$R/I \simeq R'/I'$ を得る．(q.e.d.)

($\because$) (ii) 準同型の合成:

$$S \xrightarrow{m} (S+I) \xrightarrow{p} (S+I)/I \tag{61}$$

（m は標準的単射）を考えると，$p \circ m : S \longrightarrow (S+I)/I$ を得るが，それは (T10) より準同型になる．さらに $p \circ m$ が全射であることを示す．$(S+I)/I$ の任意の元は $I+(s+x) = I+s$ $(x \in I,\, s \in S)$ の形で表され，その s に対して $p \circ m(s) = I+s$ となるので，$p \circ m$ は全射である．こうして $p \circ m$ は全準同型だと言える．また，

$$\mathrm{Ker}(p \circ m) = (p \circ m)^{-1}(I) = m^{-1}(p^{-1}(I)) = m^{-1}(I) = S \cap I. \tag{62}$$

そこで，$p \circ m$ に準同型定理を適用して，$S/(S \cap I) \simeq (S+I)/I$ を得る． (q.e.d.)

($\because$) (iii) まず，I/J が R/J のイデアルになることを示す．R, I, J を加群としてみるとき，1 章 (ex38) より I/J は R/J の部分加群となる．そこで $\overline{a} \in R/J$，$\overline{x} \in I/J$ とするとき，

$$\overline{a}\,\overline{x} = \overline{ax} \in I/J, \qquad \overline{x}\,\overline{a} = \overline{xa} \in I/J \tag{63}$$

となるので，I/J は R/J のイデアルとなる．

次に準同型の合成:

$$R \xrightarrow{p} R/J \xrightarrow{\tilde{p}} (R/J)/(I/J) \tag{64}$$

を考える．これは標準的全射の合成なので，(T10) より全準同型である．また，

$$\mathrm{Ker}(\tilde{p} \circ p) = (\tilde{p} \circ p)^{-1}(I/J) = p^{-1}(\tilde{p}^{-1}(I/J)) = p^{-1}(I/J) = I. \tag{65}$$

そこで，$\tilde{p} \circ p$ に準同型定理を適用して，$R/I \simeq (R/J)/(I/J)$ を得る． (q.e.d.)

11.（環の直積）R_1, R_2 を 2 つの環とするとき，

$$R_1 \times R_2 = \{(a_1, a_2) \mid a_1 \in R_1,\, a_2 \in R_2\} \tag{66}$$

を R_1 と R_2 の直積という．$R_1 \times R_2$ には，次のように演算が定義される．

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &= (a_1 + b_1,\, a_2 + b_2) \\ (a_1, a_2)(b_1, b_2) &= (a_1 b_1,\, a_2 b_2) \end{aligned} \tag{67}$$

$R_1 \times R_2$ はこの演算に関して環になる．この環の 0 元は $(0,0)$，単位元は $(1,1)$ である．a_1, a_2 がそれぞれ R_1, R_2 の単数ならば，(a_1, a_2) は $R_1 \times R_2$ の単数であり，逆もなりたつ．このとき，$(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$ である．

3 つ以上の環の直積 $R_1 \times \cdots \times R_n$ も同様に，

$$R_1 \times \cdots \times R_n = \{(a_1, \ldots, a_n) \mid a_1 \in R_1, \ldots, a_n \in R_n\} \tag{68}$$

で定義され，次の演算に関して環になる．(0 元は $(0, \ldots, 0)$，単位元は $(1, \ldots, 1)$)

$$\begin{aligned} (a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 + b_1, \ldots, a_n + b_n) \\ (a_1, \ldots, a_n)(b_1, \ldots, b_n) &= (a_1 b_1, \ldots, a_n b_n) \end{aligned} \tag{69}$$

単数についても 2 つの環の直積の場合と同様で，単数 $a_i \in R_i$ $(i = 1, \ldots, n)$ に対して，$(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$ がなりたつ．

$i = 1, \ldots, n$ に対して，I_i を R_i のイデアルとするとき，イデアルの直積 $I_1 \times \cdots \times I_n$ も環の直積と同様に定義する．これは (T14) で述べるように，環の直積 $R_1 \times \cdots \times R_n$ のイデアルになる．

(ex22) R_1, R_2 を 2 つの環とするとき，$R_1 \times R_2$ が環になることを示せ．

($\because$) $R_1 \times R_2$ が加群であることは加群の直積が加群であることから従う．次に (a_1, a_2), $(b_1, b_2), (c_1, c_2) \in R_1 \times R_2$ のとき，

$$\begin{aligned}((a_1, a_2)(b_1, b_2))(c_1, c_2) &= (a_1b_1, a_2b_2)(c_1, c_2) = ((a_1b_1)c_1, (a_2b_2)c_2) \\ &= (a_1(b_1c_1), a_2(b_2c_2)) = (a_1, a_2)(b_1c_1, b_2c_2) \\ &= (a_1, a_2)((b_1, b_2)(c_1, c_2))\end{aligned} \tag{70}$$

より結合律がなりたつ．また，単位元 $(1, 1)$ が存在する．最後に分配律については，

$$\begin{aligned}&(a_1, a_2)((b_1, b_2) + (c_1, c_2)) = (a_1, a_2)(b_1 + c_1, b_2 + c_2) \\ &= (a_1(b_1 + c_1), a_2(b_2 + c_2)) = (a_1b_1 + a_1c_1, a_2b_2 + a_2c_2) \\ &= (a_1b_1, a_2b_2) + (a_1c_1, a_2c_2) \\ &= (a_1, a_2)(b_1, b_2) + (a_1, a_2)(c_1, c_2).\end{aligned} \tag{71}$$

同様に

$$((a_1, a_2) + (b_1, b_2))(c_1, c_2) = (a_1, a_2)(c_1, c_2) + (b_1, b_2)(c_1, c_2) \tag{72}$$

もなりたつ．ゆえに $R_1 \times R_2$ は環である．

.....

(T14) (i) S_i が R_i の部分環のとき，$S_1 \times S_2$ は $R_1 \times R_2$ の部分環である．(ii) I_i が R_i のイデアルのとき，$I_1 \times I_2$ は $R_1 \times R_2$ のイデアルである．3 つ以上の直積でも同様のことがなりたつ．

.....

($\because$) (i) S_i は R_i の部分加群なので，1 章 (T7) より，$S_1 \times S_2$ は $R_1 \times R_2$ の部分加群．$S_1 \times S_2$ は単位元 $(1, 1)$ を含む．$(a_1, a_2), (b_1, b_2) \in S_1 \times S_2$ とすると，$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2) \in S_1 \times S_2$．ゆえに $S_1 \times S_2$ は $R_1 \times R_2$ の部分環である． (q.e.d.)

($\because$) (ii) I_i は R_i の部分加群なので，(i) 同様，$I_1 \times I_2$ は $R_1 \times R_2$ の部分加群．$(x_1, x_2) \in I_1 \times I_2$，$(r_1, r_2) \in (R_1 \times R_2)$ とすると，

$$\begin{aligned}(r_1, r_2)(x_1, x_2) &= (r_1x_1, r_2x_2) \in I_1 \times I_2 \\ (x_1, x_2)(r_1, r_2) &= (x_1r_1, x_2r_2) \in I_1 \times I_2.\end{aligned} \tag{73}$$

ゆえに $I_1 \times I_2$ は $R_1 \times R_2$ のイデアルである． (q.e.d.)

(ex23) 加群としての同型 $\mathbf{R} \times \mathbf{R} \simeq \mathbf{C}$ はなりたつが，環としての同型 $\mathbf{R} \times \mathbf{R} \simeq \mathbf{C}$ はなりたたない．たとえば，$\phi : \mathbf{R} \times \mathbf{R} \longrightarrow \mathbf{C}$ として $\phi(x, y) = x + yi$ を取ったとき，これは同型写像ではないことを示せ．

12.（中国の剰余定理）中国の剰余定理 (Chinese remainder theorem) は，中国の古い算術書『孫子算経』に由来する定理で，孫子の定理ともいう．これは元来整数の剰余に関する定理であるが，現代では環論の言葉でより一般化した形で述べられることが多い．

はじめに素朴な形の定理として述べる．

(T15)（中国の剰余定理）$m_1, \ldots, m_n$ をどの 2 つも互いに素であるような正の整数とする．このとき，任意の整数 $a_1, \ldots, a_n$ に対して，

$$\begin{cases} x \equiv a_1 & (\mathrm{mod}\, m_1) \\ x \equiv a_2 & (\mathrm{mod}\, m_2) \\ \qquad \cdots\cdots & \\ x \equiv a_n & (\mathrm{mod}\, m_n) \end{cases} \tag{74}$$

をみたす x が $m_1 \ldots m_n$ を法として一意的に存在する．

(note) m を法として一意的に存在するとは，x, x' が共に題意をみたすならば，必ず $x \equiv x' \ (\mathrm{mod}\, m)$ をみたすということである．

(ex24) 3 で割ると 2 余り，5 で割ると 3 余り，7 で割ると 2 余る数を求めよ．($x \equiv 23 \ (\mathrm{mod}\, 105)$)

次に，一般化した形の定理を述べる．

(T15') R を環，$I_1, \ldots, I_n$ をそのイデアルとし，異なる j, k に対しては，$I_j + I_k = R$ をみたすとする．$I_1 \cap \cdots \cap I_n = I$ とおく．

(i)

$$I_j + \bigcap_{k \neq j} I_k = R. \qquad (j = 1, \ldots, n) \tag{75}$$

(ii)（中国の剰余定理）任意の $a_1, a_2, \ldots, a_n \in R$ に対して，$a - a_j \in I_j$ $(j = 1, \ldots, n)$ をみたす $a \in R$ が I を法として一意的に存在する．

(iii)（中国の剰余定理）

$$R/I \simeq R/I_1 \times \cdots \times R/I_n. \tag{76}$$

(note) I を法として一意的に存在するとは，a, a' が共に題意をみたすならば，必ず $a - a' \in I$ をみたすということである．

(note) $a - a' \in I$ であることを，$a \equiv a' \ (\mathrm{mod}\, I)$ ともかく．

($\because$) (i) 異なる j, k に対して，$I_j + I_k = R$ より，$x_k + y_k = 1$ をみたす $x_k \in I_j$，$y_k \in I_k$ が存在する．ここで j を固定して，$k(\neq j)$ を動かすと，

$$x_k + y_k = 1 \qquad (x_k \in I_j,\, y_k \in I_k;\ k = 1, \ldots, \hat{j}, \ldots, n) \tag{77}$$

を得る．($\hat{j}$ は j を除くことを示す除外記号）これらの式を辺々掛けると

$$(x_1, \ldots, x_n \text{ のうち少なくとも 1 つを含む項の和}) + y_1 \ldots \hat{y}_j \ldots y_n = u_j + v_j = 1 \tag{78}$$

を得る．ここに，$u_j \in I_j$，$v_j \in \bigcap_{k\neq j} I_k$ である．そこで R の任意の元 r を取ると，

$$ru_j + rv_j = r \qquad (ru_j \in I_j,\ rv_j \in \bigcap_{k\neq j} I_k) \tag{79}$$

となるので，(75) を得る． (q.e.d.)

($\because$) (ii) 任意の $a_1, a_2, \ldots, a_n \in R$ に対して，$a - a_j \in I_j$ $(j = 1, \ldots, n)$ をみたす $a \in R$ が存在することを示す．一意性については (iii) の後に示す．

(i) の証明における $v_1, \ldots, v_n$ を用いて，$a \in R$ を

$$a = a_1v_1 + a_2v_2 + \cdots + a_nv_n \tag{80}$$

と定める．$j = 1, \ldots, n$ に対して，

$$\begin{aligned} a - a_j &= a_1v_1 + \cdots + a_j(v_j - 1) + \cdots + a_nv_n \\ &= a_1v_1 + \cdots - a_ju_j + \cdots + a_nv_n \in I_j. \end{aligned} \tag{81}$$

なぜならば，$k \neq j$ のとき，$v_k \in I_j$ であり，$u_j \in I_j$ だから． (q.e.d.)

($\because$) (iii) R から R/I_j への標準的全射を p_j とするとき，写像 $\phi : R \longrightarrow R/I_1 \times \cdots \times R/I_n$ を

$$\phi(a) = (p_1(a), \ldots, p_n(a)) \tag{82}$$

で定める．このとき，ϕ が全準同型であることを示す．まず，

$$\begin{aligned} \phi(a+b) &= (p_1(a+b), \ldots, p_n(a+b)) = (p_1(a) + p_1(b), \ldots, p_n(a) + p_n(b)) \\ &= (p_1(a), \ldots, p_n(a)) + (p_1(b), \ldots, p_n(b)) \\ &= \phi(a) + \phi(b) \end{aligned} \tag{83}$$

であり，同様に，

$$\phi(ab) = \phi(a)\phi(b) \tag{84}$$

もなりたつ．また (ii) より，任意の $\overline{a_1} \in R/I_1, \ldots, \overline{a_n} \in R/I_n$ に対して，a が存在して，$a - a_j \in I_j$ すなわち，$a \in I_j + a_j = \overline{a_j}$．ゆえに，

$$p_j(a) = \overline{a_j} \qquad (j = 1, \ldots, n). \tag{85}$$

これは，ϕ が全射であることを示す．ゆえに ϕ は全準同型である．

ここで，

$$\mathrm{Ker}\,\phi = \phi^{-1}(I_1, \ldots, I_n) = I_1 \cap \ldots \cap I_n = I \tag{86}$$

であることがわかるので，ϕ に準同型定理を適用すれば，(76) を得る． (q.e.d.)

($\because$) (ii)（一意性）a, a' が共に (ii) の条件をみたすとする．(iii) の議論より，(85) および，

$$p_j(a') = \overline{a_j} \qquad (j = 1, \ldots, n) \tag{87}$$

がなりたつ．

$$\begin{aligned} &\therefore\ \phi(a - a') = (p_1(a - a'), \ldots, p_n(a - a')) = (I_1, \ldots, I_n). \\ &\therefore\ a - a' \in \mathrm{Ker}\,\phi = I. \qquad \text{(q.e.d.)} \end{aligned} \tag{88}$$

($\because$) (T15) $R=\mathbf{Z}$, $I_j=m_j\mathbf{Z}$ とおく．$m_1,\ldots,m_n$ はどの 2 つも互いに素なので，$I_j+I_k=R$ をみたすことがわかる．これに (T15')(ii) を適用すれば，(T15) を得る． (q.e.d.)

(T15)，(T15')(ii) は，ある種の方程式の解の存在を述べているが，解を明示的に表したものではない．ただ，(T15')(i-ii) の証明で現れた v_j を用いれば，解 a は (80) で表される．これを (ex23) に当てはめてみよう．Euclid の互除法または暗算で，

$$\begin{aligned} 3\cdot 12-35\cdot 1&=1\\ -5\cdot 4+21\cdot 1&=1\\ -7\cdot 2+15\cdot 1&=1 \end{aligned} \tag{89}$$

が得られる．ゆえに，$v_1=-35$，$v_2=21$，$v_3=15$ となる．これより，

$$a=2\cdot(-35)+3\cdot 21+2\cdot 15=23 \tag{90}$$

が得られ，これは $3\cdot 5\cdot 7=105$ を法として一意的となる．

(ex25) 9 で割ると 4 余り，8 で割ると 1 余り，7 で割ると 5 余る数を求めよ．($a\equiv 481 \pmod{504}$)

13.（整域と単項イデアル整域）R を環とする．0 でない R の元 a,b が $ab=0$ をみたすとき，a を左 0 因子，b を右 0 因子という．K を体とする．$n\geq 2$ のとき，全行列環 $M_n(K)$ においては，左右の 0 因子が存在する．それは 0 行列でない非正則な行列に他ならない．なぜならば，A をそのような行列とすれば，A の列ベクトルおよび行ベクトルが線形従属になるので，$B,C\neq O$ が存在して

$$AB=CA=O \tag{91}$$

をみたすからである．n が合成数のとき，$\mathbf{Z}_n$ には 0 因子が存在する．それは，$kl\equiv 0 \pmod{n}$ $(0<k,l<n)$ をみたす k,l であり，それはすなわち $\mathbf{Z}_n$ の 0 でない非単数（n と互いに素ではない元）に他ならない．可換環のときは，左右の 0 因子に区別はない．

R を自明でない（すなわち $1\neq 0$ の）可換環とする．R に 0 因子が存在しないとき，R を 整域 という．$\mathbf{Z}$ は整域の典型例である．また，明らかに体には 0 因子が存在しないので，体は整域である．さらに，R を整域とするとき，多項式環 $R[x]$ は整域になる．より一般に，多変数多項式環 $R[x_1,\ldots,x_n]$ も整域になる．

整域でない可換環の例としては，上に述べた合成数 n に対する $\mathbf{Z}_n$ の他に，関数のなす環などがある．適当な集合 Ω で定義された連続な実関数全体の集合 $C(\Omega)$ や $C^r(\Omega)$，$C^\infty(\Omega)$ などは整域でない可換環の例である．

(ex26) (1) $M_2(\mathbf{Z})$ の 0 因子をいくつかあげよ． (2) $\mathbf{Z}_{12}$ の 0 因子をすべて求めよ．
(3) $C(\mathbf{R})$ の 0 因子の例をあげよ．

. . . . . .

(T16) 整域上の（多変数）多項式環は整域である．

. . . . . .

($\because$) R を整域とし，多項式環 $R_1=R[x_1]$ を考える．R_1 の 0 でない任意の 2 元

$$\begin{aligned} f(x)&=a_0x^m+a_1x^{m-1}+\cdots+a_m \qquad (a_0\neq 0)\\ g(x)&=b_0x^n+b_1x^{n-1}+\cdots+b_n \qquad (b_0\neq 0) \end{aligned} \tag{92}$$

を取ると，R が整域なので，$f(x)g(x)$ の最高次の係数 $= a_0b_0 \neq 0$．　$\therefore$　$f(x)g(x) \neq 0$．ゆえに，R_1 は整域である．したがってまた，$R_2 = R_1[x_2]$ も整域である．以下帰納的に，$R_n = R_{n-1}[x_n]$ は整域になる．ところで，明らかに

$$R_n \simeq R[x_1, \ldots, x_n] \tag{93}$$

なので，多変数多項式環 $R[x_1, \ldots, x_n]$ は整域である．(q.e.d.)

R を整域とする．R の元 a, b, c について，$a = bc$ とかけるとき，a は b (c) で割りきれるといい，$b \mid a$　$(c \mid a)$ とかく．このとき，b (c) を a の約元または因子，a を b (c) の倍元という．

幾らかの元の共通の約元をそれらの公約元あるいは共通因子という．$a_1, \ldots, a_s$ の公約元のうちで，他のすべての $a_1, \ldots, a_s$ の公約元の倍元となっているものを最大公約元といい，

$$\gcd(a_1, \ldots, a_s) \tag{94}$$

で表す．幾らかの元の共通の倍元をそれらの公倍元という．$a_1, \ldots, a_s$ の公倍元のうちで，他のすべての $a_1, \ldots, a_s$ の公倍元の約元となっているものを最小公倍元といい，

$$\mathrm{lcm}\,(a_1, \ldots, a_s) \tag{95}$$

で表す．2 つの元 a, b について，$\gcd(a, b) = (a, b)$ ともかく．$(a, b) = 1$ のとき，a, b は互いに素であるという．

体の上の多項式環 $K[x]$ における最大公約元や最小公倍元は，定数倍を除けば 1 通りに決まる．1 変数多項式 $g(x)$ の次数を $\deg(g(x))$ で表す．これはもちろん，係数が 0 でない項の中の最高次数のことである．0 以外の定数の次数は 0 だが，0 の次数は $-\infty$ とする．

. . . . . .

(L3) K を体，$g_1(x), \ldots, g_s(x)$ を K 上の 1 変数多項式とする．

(i) $\gcd(g_1(x), \ldots, g_s(x)) = d(x)$ とするとき，K 上の 1 変数多項式 $m_1(x), \ldots, m_s(x)$ が存在して，次がなりたつ．

$$m_1(x)g_1(x) + \cdots + m_s(x)g_s(x) = d(x) \tag{96}$$

(ii) $\gcd(g_1(x), \ldots, g_s(x)) = 1$ であるための必要十分条件は，K 上の 1 変数多項式 $m_1(x)$, $\ldots, m_s(x)$ が存在して，次をみたすことである．

$$m_1(x)g_1(x) + \cdots + m_s(x)g_s(x) = 1 \tag{97}$$

. . . . . .

($\because$) この証明は，(L1),(L2) の証明を少し修正すればできるので省略する．

整域 R の任意のイデアルが単項イデアルとなるとき，R を 単項イデアル整域 という．身近な可換環でこの性質を持つものとして，$\mathbf{Z}$ や 1 変数多項式環がある．

. . . . . .

(T17) (i) $\mathbf{Z}$ は単項イデアル整域である．(ii) K を体とするとき，多項式環 $K[x]$ は単項イデアル整域である．

. . . . . .

($\because$) (i) $\mathbf{Z}$ の任意のイデアル I を取る．I には明らかに正の元が含まれる．I の中で最小の正の元を g とする．I の任意の元 g' に対して，(L1) より $m, m' \in \mathbf{Z}$ が存在して，最大公約数 (g, g') が

$$(g, g') = mg + m'g' \tag{98}$$

とかける．ところで I はイデアルで，$g, g' \in I$ なので，$(g, g') = mg + ng' \in I$．すなわち，$(g, g') \geq g$．これより，$g \mid g'$．g' は任意だったので，$I = (g)$．(q.e.d.)

($\because$) (ii) $K[x]$ の任意のイデアル I を取る．I の中で次数が最小の元を 1 つ取り，それを $g_1(x)$ とおく．I の任意の元 $g_2(x)$ に対して，(L3) より $m_1(x), m_2(x) \in K[x]$ が存在して，最大公約元 $\gcd(g_1(x), g_2(x)) = d(x)$ が

$$d(x) = m_1(x)g_1(x) + m_2(x)g_2(x) \tag{99}$$

とかける．ここで I はイデアルで，$g_1(x), g_2(x) \in I$ なので，$d(x) \in I$．すなわち，$\deg(d(x)) \geq \deg(g_1(x))$．これより，$g_1(x) \mid g_2(x)$．$g_2(x)$ は任意だったので，$I = (g_1(x))$．(q.e.d.)

(note) 多変数多項式環は，単項イデアル整域ではない．

.....

(T18) K を体，$R = \mathbf{Z}$ または $K[x]$ とするとき，$S = \{g_1, \ldots, g_s\}$ で生成された R のイデアル $I = (S)$ について，

$$I = (\gcd(g_1, \ldots, g_s)). \tag{100}$$

.....

($\because$) (T3) より，

$$I = \{r_1 g_1 + \cdots + r_s g_s \mid r_1, \ldots, r_s \in R\} \tag{101}$$

とかける．ここで，$\gcd(g_1, \ldots, g_s) = d$ とおくと，(L1),(L3) より，$m_1, \ldots, m_s \in R$ を用いて

$$d = m_1 g_1 + \cdots + m_s g_s \tag{102}$$

とかけるので，$d \in I$．また，$d \mid g_k$ $(k = 1, \ldots, s)$ なので，任意の $r_1, \ldots, r_s \in R$ に対して，

$$d \mid r_1 g_1 + \cdots + r_s g_s. \tag{103}$$

ゆえに，任意の $x \in I$ に対して，$r \in R$ を用いて $x = rd$ とかける．$\therefore I = (d)$．(q.e.d.)

(ex27) (1) $R = \mathbf{Z}$ とする．次の各 S に対して，R のイデアル (S) を単項イデアル (a) の形に表せ．(i) $S = \{18, 24\}$．(ii) $S = \{10, 15, 25\}$．

(2) $R = \mathbf{Q}[x]$ として，(1) と同じ問いを解け．(i) $S = \{x^2 - 1, x^2 + 2x + 1\}$．(ii) $S = \{x^4 - 1, x^6 + 1\}$．

14.（整域と素イデアル）R を可換環とする．R のイデアル I について，R/I が整域になるとき，I を R の素イデアルという．次がなりたつ．

(T19) I が素イデアル $\iff xy \in I \Rightarrow x \in I$ または $y \in I$.

($\because$) ($\Rightarrow$) R を可換環，I を R の素イデアルとする．$xy \in I$ とする．$\overline{x}, \overline{y} \in R/I$ を考える．

$$\overline{x}\,\overline{y} = \overline{xy} = \overline{0} \tag{104}$$

である．ここで，仮定より R/I は整域なので，$\overline{x} = \overline{0}$ または $\overline{y} = \overline{0}$ がなりたつ．これはすなわち，$x \in I$ または $y \in I$ を意味する． (q.e.d.)

($\because$) ($\Leftarrow$) 可換環 R のイデアル I について，$xy \in I \Rightarrow x \in I$ または $y \in I$ がなりたつとする．$\overline{x}, \overline{y} \in R/I$ が (104) をみたすならば，$xy \in I$ であり，仮定より，$x \in I$ または $y \in I$ となる．これは，$\overline{x} = \overline{0}$ または $\overline{y} = \overline{0}$ を意味する．ゆえに，

$$\overline{x}\,\overline{y} = \overline{0} \;\Rightarrow\; \overline{x} = \overline{0} \text{ または } \overline{y} = \overline{0}. \tag{105}$$

これは，R/I が整域であることを意味する． (q.e.d.)

(ex28) (1) 素数 p について，$p\mathbf{Z}$ は環 $\mathbf{Z}$ の素イデアルであることを示せ． (2) 合成数 n について，$n\mathbf{Z}$ は環 $\mathbf{Z}$ の素イデアルではないことを示せ．

次に，R を環とする．R の自明でないイデアル I に対して，$I \subset I'$ かつ $I \neq I'$ をみたす R のイデアル I' が存在しないとき，I を R の極大イデアルという．

(T20) R を可換環とするとき，I が R の極大イデアル $\iff R/I$ が体．

($\because$) ($\Rightarrow$) I を R の極大イデアルとする．R/I が可換環であることは明らかで，I が自明でないことから，R/I は 0 環ではない．よって，R/I の任意の $\overline{0}$ でない元が単数であることを示せばよい．$\overline{x} \in R/I$，$\overline{x} \neq \overline{0}$ とするとき，$x \notin I$ となる．ここでイデアル:

$$(x) + I = \{rx + I \mid r \in R\} \tag{106}$$

を考えると，I が極大イデアルなので，$(x) + I = R$．これより，ある $r \in R$，$y \in I$ が存在して，$rx + y = 1$． $\therefore\ rx \in 1 + I$． $\therefore\ \overline{r}\,\overline{x} = \overline{rx} = \overline{1}$． $\therefore\ \overline{r} = \overline{x}^{-1}$． (q.e.d.)

($\because$) ($\Leftarrow$) R/I が体であるとする．$x \in R - I$ を任意に取る．x と I を含む最小のイデアルは (106) であり，これが自明になることを示せば I は極大イデアルになる．R/I が体であり，$\overline{x} \neq \overline{0}$ なので，$\overline{r} \in R/I$ が存在して，$\overline{r}\,\overline{x} = \overline{rx} = \overline{1}$． $\therefore\ rx + I = 1 + I$． $\therefore$ $(x) + I = (1) = R$． (q.e.d.)

(ex29) (1) 素数 p について，$p\mathbf{Z}$ は環 $\mathbf{Z}$ の極大イデアルであることを示せ． (2) 合成数 n について，$n\mathbf{Z}$ は環 $\mathbf{Z}$ の極大イデアルではないことを示せ． (3) 可換環 R の極大イデアルは素イデアルであることを示せ．

15.（可換環の局所化）R を可換環とする．R の局所化とは，R のいくらかの元の逆元を R に追加する一般的な方法のことである．たとえば，$\mathbf{Z}$ に分数を追加して，$\mathbf{Q}$ を構成することはその一例である．R の部分集合 S が積について閉じていて，$1 \in S$，$0 \notin S$ をみたすとき，S を R の積閉集合という．このとき，直積 $R \times S$ を考え，$R \times S$ における和と積を次のように定める．

$$\begin{array}{l}(r,s)+(r',s')=(rs'+r's,ss')\\(r,s)(r',s')=(rr',ss')\end{array} \tag{107}$$

これは，$(r,s)=r/s$ と考えて演算を定義したのである．すなわち，S の元を分母とするような分数を作ろうとしている．しかしきちんとした分数にするためには，約分を可能にする必要がある．そこで，

$$(r,s)\sim(r_1,s_1) \iff s_0 \in S \text{ が存在して,} s_0(rs_1-r_1s)=0 \tag{108}$$

によって同値関係 $\sim$ を定める．この関係により $R \times S$ はいくらかの同値類に分割されるが，同じ同値類に属する元たちをすべて同じ分数と見做す，すなわち同一視することにする．これで，約分が可能となる．ここで問題になるのは，この同一視が (107) と両立するかどうかということである．そこで，$(r,s)\sim(r_1,s_1)$，$(r',s')\sim(r_1',s_1')$ とするとき，次を示す．

$$\begin{array}{c}(r,s)+(r',s')\sim(r_1,s_1)+(r_1',s_1')\\(r,s)(r',s')\sim(r_1,s_1)(r_1',s_1')\end{array} \tag{109}$$

($\because$) (第 1 式) $(r,s)+(r',s')=(rs'+r's,ss')$，$(r_1,s_1)+(r_1',s_1')=(r_1s_1'+r_1's_1,s_1s_1')$ ゆえ，$(rs'+r's,ss')\sim(r_1s_1'+r_1's_1,s_1s_1')$ を示せばよい．仮定より，ある $s_0,s_0' \in S$ が存在して，$s_0(rs_1-r_1s)=0$，$s_0'(r's_1'-r_1's')=0$．ゆえに，

$$\begin{array}{l}s_0s_0'\left[(rs'+r's)(s_1s_1')-(r_1s_1'+r_1's_1)ss'\right]\\=s_0s_0'\left(rs's_1s_1'-r_1s_1'ss'+r'ss_1s_1'-r_1's_1ss'\right)\\=s_0's's_1's_0(rs_1-r_1s)+s_0ss_1s_0'(r's_1'-r_1's')=0. \qquad \text{(q.e.d.)}\end{array} \tag{110}$$

($\because$) (第 2 式) $(r,s)(r',s')=(rr',ss')$，$(r_1,s_1)(r_1',s_1')=(r_1r_1',s_1s_1')$ ゆえ，$(rr',ss')\sim(r_1r_1',s_1s_1')$ を示せばよい．

$$\begin{array}{l}s_0s_0'\left(rr's_1s_1'-r_1r_1'ss'\right)=s_0s_0'\left(rr's_1s_1'-r_1r'ss_1'+r_1r'ss_1'-r_1r_1'ss'\right)\\=s_0'r's_1's_0(rs_1-r_1s)+s_0r_1ss_0'(r's_1'-r_1's')=0. \qquad \text{(q.e.d.)}\end{array} \tag{111}$$

このようにして，$\sim$ による同一視と演算 (107) が矛盾なく行われる．そこで，(r,s) が属する同値類を r/s で表し，同値類全体がなす集合を新たな環と見做すことができる．これを S による R の局所化または商環といい，$S^{-1}R$ または R_S で表す．

(ex30) (1) $\sim$ が同値関係であることを示せ．(2) $S^{-1}R$ が環の公理をみたすことを示せ．

16.（一意分解整域）$\mathbf{Z}$ の任意の元は素因数の積に一意的に分解される．このような性質を抽象化して定義されるのが一意分解整域である．

R を整域とする．$a \in R$ が 既約元 であるとは，$a \neq 0$ かつ，

$$a = bc \ \Rightarrow \ b \text{ または } c \text{ が単数} \tag{112}$$

をみたすことをいう．特に，多項式環における既約元を既約多項式という．

次に $a \in R$ が 素元 であるとは，a が 0 でも単数でもなく，かつ，

$$a \mid bc \ \Rightarrow \ a \mid b \text{ または } a \mid c \tag{113}$$

をみたすことをいう．$R = \mathbf{Z}$ のときは，素元とは素数に符号を付けたものになる．R の元 a, b がある単数 c に対して $a = bc$ をみたすとき，a, b は単数の違いを持つという．

整域 R が次の条件をみたすとき，一意分解整域 と呼ばれる．

[$U1$]（一意分解性）　R の 0 でも単数でもない任意の元は，既約元の積で，順序と単数の違いを除いて一意的に表される．

(T21) 単項イデアル整域は，一意分解整域である．

($\because$) . (q.e.d.)

(T22) R が一意分解整域ならば，$R[x]$ もまた一意分解整域である．

($\because$) . (q.e.d.)

(T22) より，R が一意分解整域 $\Rightarrow R_1 = R[x_1]$ が一意分解整域 $\Rightarrow R_2 = R_1[x_2]$ が一意分解整域 ... となるので，帰納的に次を得る．

(T22') R が一意分解整域ならば，$R[x_1, \ldots, x_n]$ もまた一意分解整域である．