Bulletin of Tokyo Gakugei University, Division of Natural Sciences, **67**: pp.1 ~ 8, 2015

Product extensions of commutative rings

Yoshimi KITAMURA* and Yoshio TANAKA*

Department of Mathematics

(Received for publication; May 22, 2015)

KITAMURA, Y. and TANAKA, Y.: Product extensions of commutative rings. Bull. Tokyo Gakugei Univ. Div. Nat. Sci., **67**: 1-8 (2015) ISSN 1880-4330

Abstract

We shall investigate a certain product ring $R\times R$ of a commutative ring R which is an extension of R. Such extension rings give useful ring-theoretic constructions or examples. We study these extension rings, and ideals of the rings. Also, we give a characterization of ideals of the rings over principal ideal domains.

Keywords: ring, R-algebra, R-module, product extension, direct product ring, field, integral domain, ideal, principal ideal domain.

Department of Mathematics, Tokyo Gakugei University, 4-1-1 Nukuikita-machi, Koganei-shi, Tokyo 184-8501, Japan

1. Introduction

The symbol $\mathbb{Z}$; $\mathbb{R}$; $\mathbb{C}$ means respectively the ring of integers; the field of real numbers; the field of complex numbers, unless otherwise stated.

As is well-known, the field $\mathbb{C}$ is an extension of $\mathbb{R}$ with the basis $\{1, \sqrt{-1}\}$. We shall generalize the basic field $\mathbb{R}$ to an arbitrary commutative ring R, and then we will consider certain ring operations (addition and multiplication) on the product $R\times R$ as an extension ring of R, containing the field $\mathbb{C}$. In this paper, we shall investigate the ring structure on such extensions of rings.

Let us call such an extension of a ring the product extension. We survey these extensions of fields or integral domains, and their examples. Also, we study ideals in the product extensions. In particular, we characterize ideals of the product extension over a principal ideal domain.

2. Product extensions

Throughout this paper, the symbol R means a non-zero *commutative ring* with the identity element denoted by 1. Unless otherwise stated, a ring is a commutative ring with the identity element, and a subring of a ring contains the same identity

* Tokyo Gakugei University (4-1-1 Nukuikita-machi, Koganei-shi, Tokyo, 184-8501, Japan)

element of the ring. Also, a ring homomorphism is supposed to carry the identity element to the identity element. However, in this section, we assume that a ring is not necessarily commutative.

The symbol $A \times B$ means the product of sets A and B, and $A \times 0$ means $A \times \{0\}$, and similar for $0 \times B$. Let A, B be subsets of R. Define $A + B = \{x + y \mid x \in A, y \in B\}$. Also, for $a \in R$, define $aA = \{ax \mid x \in A\}$.

Recall that a ring A is said to be an R-*algebra*, if there exists a ring homomorphism f of R to A such that the image $f(R)$ is contained in the center $\{a \in A \mid ax = xa$ for all $x \in A\}$ of A.

We will study the product $R \times R$ which is an R-algebra containing a subring isomorphic to R.

Let $P = R \times R$. Let us define addition and scalar multiplication on P by

$$(x, y) + (z, w) = (x + z, y + w),$$
$$r.(x, y) = (rx, ry)$$

for (x, y), $(z, w) \in P$; $r \in R$. Then P is an R-module, that is, the following hold for any $r, r' \in R$; $p, p' \in P$:

$$(r + r').p = r.p + r'.p, \; r.(p + p') = r.p + r.p', \; (rr').p = r.(r'.p), \; 1.p = p.$$

Let $e = (1, 0)$, $u = (0, 1) \in P$. Then e and u form a basis for P over R, that is, every element p of P can be written uniquely as $p = x.e + y.u$ for $x, y \in R$.

Let h be a map of R to P defined by $h(r) = (r, 0)$ for r in R. Evidently, h is an R-module monomorphism with $h(r) = r.e$.

In terms of R-algebras, it is natural to ask the following question: What is multiplication $*$ on the above R-module P which makes the map h a ring homomorphism satisfying condition (h): $r.p = h(r) * p = p * h(r)$ for all $r \in R$ and all $p \in P$? (Here, we can replace (h) by "$r.u = h(r) * u = u * h(r)$ for all $r \in R$", noting that $\{e, u\}$ is a basis for the R-module P with $e = h(1)$). The following gives an answer to this question.

Proposition 2.1. *Let $P = R \times R$. Let $e = (1, 0)$, $u = (0, 1) \in P$. If the R-module P is a ring under component-wise addition, and multiplication $*$, and if the map h: $R \to P$ is a ring homomorphism satisfying the condition (h), then, putting $u * u = (a, b) \in P$, the multiplication $*$ is given by*

(1) $$(x, y) * (z, w) = (xz + ayw, xw + yz + byw)$$

for (x, y), $(z, w) \in P$, hence P is a commutative R-algebra. Conversely, for each $(a, b) \in P$, define multiplication $*$ on the R-module P by (1). Then *P is a commutative R-algebra such that the map h is a ring homomorphism satisfying condition (h).*

Proof. For the first half, we have obviously

$$e * e = e, \quad e * u = u * e = u, \quad u * u = a.e + b.u.$$

Also, we have the following by the condition (h).

$$(r.p) * (r'.p') = (rr').(p * p') \; (r, r' \in R; p, p' \in P).$$

Thus, we have

$$\begin{aligned}(x.e + y.u) * (z.e + w.u) &= xz.(e * e) + xw.(e * u) + yz.(u * e) + yw.(u * u) \\ &= (xz + ayw).e + (xw + yz + byw).u\end{aligned}$$

for all $x, y, z, w \in R$, which shows that (1) holds, and hence P is a commutative R-algebra. For the latter part, assume (1). Recalling R is a commutative ring and $\{e, u\}$ is a basis for the R-module P, it is routinely shown that multiplication $*$ on P given by (1) makes the R-module P a commutative ring with the identity element e, and that the map h: $R \to P$ is a ring homomorphism satisfying condition (h), hence P is a commutative R-algebra. □

In view of Proposition 2.1, let us recall the following extension ring on the product set $P = R \times R$.

Definition 2.2. Let $P = R \times R$. For $(a, b) \in P$, let $(R \ltimes R; a, b)$ be a commutative ring $(P, +, *)$ defined by the following addition $+$ and multiplication $*$: For (x, y), $(z, w) \in P$, let

$$(x, y) + (z, w) = (x + z, y + w),$$
$$(x, y) * (z, w) = (xz + ayw, xw + yz + byw).$$

Then $e = (1, 0)$ is the identity element, and for $u = (0, 1)$, $u * u = (a, b)$, and $(x, y) = (x, 0) * e + (y, 0) * u$ in $(R \ltimes R; a, b)$. We note that the ring $(R \ltimes R; a, b)$ is a commutative R-algebra having $\{e, u\}$ as a basis over R. Evidently, it contains a subring isomorphic to R by the map h: $R \to (R \ltimes R; a, b)$, $h(r) = (r, 0)$.

For $R = \mathbb{R}$, the ring $(R \ltimes R; -1, 0)$ is isomorphic to the field $\mathbb{C}$ as a ring. The ring $(R \ltimes R; 0, 0)$ is called the *trivial extension* of R by itself (see [3], etc.).

Let us call the ring $(R \ltimes R; a, b)$ the *product extension* of R. Also, we denote $(R \ltimes R; 0, 0)$ by $R \ltimes R$.

For $a \in R$, the symbol (a) means the ideal of R generated by a.

Remark 2.3. *Let $R[X]$ be the polynomial ring over R, and let $I = (X^2 - a - bX)$. Then the ring $(R \ltimes R; a, b)$ is isomorphic to the residue class ring $R[X]/I$ (by a map $(x, y) \mapsto [x + yX]$). Obviously, $(R \ltimes R; a, b)$ is isomorphic to $(R \ltimes R; a, -b)$ as rings (by a map $(x, y) \mapsto (x, -y)$).*

As is well-known, the product $P = R \times R$ is a ring *under component-wise addition and multiplication* (i.e., for (x, y), $(z, w) \in R \times R$, $(x, y) + (z, w) = (x + z, y + w)$, and $(x, y) \cdot (z, w) = (xz, yw)$). This canonical ring P is a commutative ring which contains a subring isomorphic to R by f: $R \to R \times R$, $f(r) = (r, r)$, but P is not an integral domain. Let us denote such a ring P by $R \otimes R$, and call it the *direct product ring* of R (see [2] for order structures on the rings $R \otimes R$ and $R \ltimes R$). We have the following analogue to Proposition 2.1.

Remark 2.4. *Let $P = R \times R$. Let $e = (1, 0)$, $u = (0, 1) \in P$. If the R-module P is a ring under component-wise addition,* and multiplication $\circ$ *with $u \circ u = (0, 1)$, and if the map f: $R \to P$ defined by $f(r) = (r, r)$ is a ring homomorphism satisfying condition (f): $r.p = f(r) \circ p = p \circ f(r)$ for all $r \in R$ and all $p \in P$, then the multiplication $\circ$ is given by*

(2) $$(x, y) \circ (z, w) = (xz, yw)$$

for (x, y), $(z, w) \in P$, and hence $(P, +, \circ) = R \otimes R$ is a commutative R-algebra. (We can replace the condition (f) by "$r.u = f(r) \circ u = u \circ f(r)$ for all $r \in R$", as in the condition (h)). Conversely, if multiplication $\circ$ on the R-module P is defined by (2), then *$(P, +, \circ) = R \otimes R$ is a commutative R-algebra such that $u \circ u = (0, 1)$ and the map f: $R \to P$ is a ring homomorphism satisfying condition (f).*

Indeed, for the first half, $e + u = (1, 1) = f(1)$ and $u^2 = u$, hence $e^2 = e$, $e \circ u = u \circ e = 0$. Recall that $(x, y) = x.e + y.u$. Thus we have (2). Hence $(P, +, \circ) = R \otimes R$ is a commutative R-algebra. The parenthetic part holds, noting that $r.u = f(r) \circ u = u \circ f(r)$ implies $r.e = f(r) \circ e = e \circ f(r)$. The latter part is obvious.

Let us survey ring structure on $(R \ltimes R; a, b)$.

Proposition 2.5. *Let $P = R \times R$, and $(a, b) \in P$. Let $f(X, Y) = X^2 + bXY - aY^2 \in R[X, Y]$. Then the following hold.*

(1) *Let R be a field. Then $(R \ltimes R; a, b)$ is a field if $f(X, Y)$ has no zero points in P except $(0, 0)$. Also, $(R \ltimes R; a, b)$ is not an integral domain if $f(X, Y)$ has a zero point in P except $(0, 0)$.*

(2) *Let R be an integral domain. Then $(R \ltimes R; a, b)$ is an integral domain iff $f(X, Y)$ has no zero points in P except $(0, 0)$.*

Proof. (1) Obviously, the relation $(x, y) * (z, w) = (0, 0)$ in $(R \ltimes R; a, b)$ is equivalent to

$$xz + ayw = 0, yz + (x + by)w = 0.$$

Let $d = \det \begin{bmatrix} x & ay \\ y & x + by \end{bmatrix} = x^2 + bxy - ay^2$.

In case $f(X, Y)$ has no zero points in P except $(0, 0)$, let $(x, y) * (z, w) = (0, 0)$ and $(x, y) \neq (0, 0)$. Then $dz = dw = 0$. Since $d = f(x, y) \neq 0$, we have $(z, w) = (0, 0)$. Hence $(R \ltimes R; a, b)$ is an integral domain with the identity element e. Further, for every $(x, y) \neq (0, 0)$, there exists $(z, w) \in P$ such that $(x, y) * (z, w) = e$ (indeed, $z = (x + by) f(x, y)^{-1}$, $w = -yf(x, y)^{-1}$). Thus $(R \ltimes R; a, b)$ is a field.

In case $f(X, Y)$ has a zero point in P except $(0, 0)$, let $(x, y) \in P$ with $f(x, y) = 0$ and $(x, y) \neq (0, 0)$. Then, since $d = f(x, y) = 0$, there exists a non-zero point (z, w) in P such that $xz + ayw = 0$, $yz + (x + by)w = 0$. Thus $(x, y) * (z, w) = (0, 0)$, which implies that $(R \ltimes R; a, b)$ is not an integral domain.

(2) Let K be the quotient field of the integral domain R. Then it is easy to see that $f(X, Y)$ has a zero point in P except $(0, 0)$ iff $f(X, Y)$ has the same property in $K \times K$. Hence, (2) follows from (1). □

Corollary 2.6. *Let K be a field. For $a, b \in K$, the following are equivalent.*
(1) $(K \ltimes K; a, b)$ *is a field.*
(2) $(K \ltimes K; a, b)$ *is an integral domain.*
(3) $f(X, Y) = X^2 + bXY - aY^2 \in K[X, Y]$ *has no zero points in $K \times K$ except* $(0, 0)$.

Remark 2.7. *An R-module M satisfying the descending (resp. ascending) chain condition is said to be artinian (resp. noetherian). A ring R is said to be artinian; noetherian if it is so as an R-module, respectively. (For these, see* [1], [3], *etc.). We recall that every artinian integral domain is precisely a field.*

For the ring $(R \ltimes R; a, b)$, it is artinian (resp. noetherian) iff R is artinian (resp. noetherian). In particular, for R being a field, $(R \ltimes R; a, b)$ is artinian and noetherian.

Indeed, for the if part, the R-module $(R \ltimes R; a, b)$ has a basis $\{e, u\}$, then it is an artinian R-module (see [1, Corollary 6.4], etc.). But, every ideal of $(R \ltimes R; a, b)$ is evidently an R-submodule of $(R \ltimes R; a, b)$. Thus the ring $(R \ltimes R; a, b)$ is artinian. For the only if part, to see R is artinian, let $I_1 \supset I_2 \supset \cdots$ be a descending chain on ideals in R. Then $I_1 \times I_1 \supset I_2 \times I_2 \supset \cdots$ is a descending chain on ideals in $(R \ltimes R; a, b)$. Thus $I_n \times I_n = I_{n+1} \times I_{n+1} = \cdots$ for some n, which yields $I_n = I_{n+1} = \cdots$. Similarly, the parenthetic part holds.

In view of Proposition 2.5, we have Example 2.8 and Remark 2.9 below.

Example 2.8. (1) Let $f(X, Y) = X^2 + Y^2 \in \mathbb{R}[X, Y]$. Then $f(X, Y)$ has no zero point except $(0, 0)$ in $\mathbb{R} \times \mathbb{R}$. Thus $(\mathbb{R} \ltimes \mathbb{R}; -1, 0)$ is a field isomorphic to the field $\mathbb{C}$.

(2) Let $f(X, Y) = X^2 - Y^2 \in \mathbb{R}[X, Y]$. Then $f(X, Y)$ has a zero point in $\mathbb{R} \times \mathbb{R}$ except $(0, 0)$. Thus $(\mathbb{R} \ltimes \mathbb{R}; 1, 0)$ is not an integral domain (actually, $(1, 1) * (-1, 1) = (0, 0)$).

(3) Let $f(X, Y) = X^2 + Y^2 \in \mathbb{C}[X, Y]$. Then $f(X, Y)$ has a zero point $(1, i) \neq (0, 0)$ in $\mathbb{C} \times \mathbb{C}$, where $i = \sqrt{-1}$. Thus $(\mathbb{C} \ltimes \mathbb{C}; -1, 0)$ is not an integral domain (actually, $(1, i) * (-1, i) = (0, 0)$).

Remark 2.9. (1) *Let $f(X) = X^2 + bXY \in R[X, Y]$ $(b \in R)$. Then $f(X, Y)$ has a zero point in $R \times R$ except* $(0, 0)$. *Thus $(R \ltimes R; 0, b)$ is not an integral domain (actually,* $(0, 1) * (-b, 1) = (0, 0)$*).*

(2) *Let $(R, \leq)$ be an ordered integral domain with $a < 0$. Let $f(X, Y) = X^2 - aY^2 \in R[X, Y]$. Then $f(X, Y)$ has no zero points except* $(0, 0)$ *in $R \times R$. Hence $(R \ltimes R; a, 0)$ is an integral domain. Especially,* for *R being an ordered field with $a < 0$, $(R \ltimes R; a, 0)$ is a field.*

3. Ideals

Let p_1, p_2: $R \times R \to R$ be the projections defined by $p_1(x, y) = x$, and $p_2(x, y) = y$.

For $R \times R$ being the direct product ring $R \otimes R$, p_1, p_2 are obviously ring homomorphisms, and the following routinely hold:

(a) For ideals I and J of R, $I\times J$ is an ideal of $R\otimes R$.

(b) For an ideal I of $R\otimes R$, (i) $p_1(I)$ and $p_2(I)$ are ideals of R, and (ii) $I=p_1(I)\times p_2(I)$.

For $R\times R$ being the product extension $(R\ltimes R;a,b)$, however, p_1 need not be a ring homomorphism (p_2 is never a ring homomorphism), and (b)(i) holds, but (a) need not hold, and similar for (b)(ii); see Corollary 3.2, Remark 3.3 and Corollary 3.4 below.

Proposition 3.1. *For a subset $A=A_1\times A_2$ of $R\times R$, A is an ideal of $(R\ltimes R;a,b)$ iff $aA_2\subset A_1\subset A_2$ with A_1, A_2 ideals of R.*

Proof. Note that $(x,y)*(a_1,a_2)=(xa_1+aya_2, xa_2+ya_1+bya_2)$ $(x,y\in R; a_1\in A_1, a_2\in A_2)$. Then the if part is obvious. For the only if part, A_1 and A_2 are evidently ideals of R. Since $(0,1)*(a_1,a_2)=(aa_2, a_1+ba_2)$ $(a_1\in A_1, a_2\in A_2)$, we have $aA_2\subset A_1\subset A_2$. □

Corollary 3.2. *Let I, J be ideals of R. For $a\in I$, $I\times J$ is an ideal of $(R\ltimes R;a,b)$ iff $I\subset J$. Also, $0\times J$ is an ideal iff $aJ=0$ (but, $I\times 0$ is never an ideal if $I\neq 0$). Further, $I\times I$ is an ideal.*

For elements a, b in an integral domain R, the symbol $a\mid b$ (resp. $a\sim b$) means that $b=ar$ for some element (resp. unit) r in R.

Remark 3.3. *Let R be an integral domain. For $m,n\in R$ with $n\mid m$, the following hold.*

(1) *$mR\times nR$ is a principal ideal of $R\ltimes R$ iff $m=0$ or $m\sim n$.*

(2) *If $m\neq 0$ and $n\nsim m$, then for an ideal $I=((m,n))$ of $R\ltimes R$, $I\neq p_1(I)\times p_2(I)$.*

Indeed, for (1), note that $A=mR\times nR$ is an ideal of $R\ltimes R$ by Corollary 3.2. The if part is obvious. To see the only if part, assume that A is principal and $m\neq 0$. Put $A=((p,q))=\{(px, qx+py)\mid x,y\in R\}$. Then $pR=mR$, thus $p\sim m$. While, $(0,n)=(px,qx+py)$ for some $x,y\in R$. Then $px=0$, so $x=0$. Thus, $n=py$, so $m\mid n$. But $n\mid m$, hence $n\sim m$.

For (2), let $m=rn$ for some $r\in R$. Then $I=\{(mx, n(x+ry))\mid x,y\in R\}$, which yields $p_1(I)\times p_2(I)=mR\times nR$. Hence $p_1(I)\times p_2(I)$ is not principal by (1). Thus $I\neq p_1(I)\times p_2(I)$.

The following holds (in view of the proof of Proposition 3.1).

Corollary 3.4. *For an ideal I of $(R\ltimes R;a,b)$, $p_1(I)$, $p_2(I)$ are ideals of R, and $p_1(I)\times p_2(I)$ is an ideal of $(R\ltimes R;a,b)$.*

Remark 3.5. *Let I be an ideal of $(R\ltimes R;a,b)$. Then an ideal $J=p_1(I)\times p_2(I)$ contains I, but $J=I$ need hold (Remark 3.3 (2)). While, obviously the following holds.*

$I=p_1(I)\times p_2(I)$ iff $p_1(I)\times 0\subset I$ and $0\times p_2(I)\subset I$. Especially, $I=0\times p_2(I)$ iff $p_1(I)=0$. Thus, for I being a non-zero and proper in $R\ltimes R$, if R is a field, $I=0\times R$. Here, an ideal is called proper if it is not the whole ring.

Remark 3.6. (1) *For a subset A of $(R\ltimes R;a,b)$, that $p_1(A)\times p_2(A)$ is an ideal of $(R\ltimes R;a,b)$ need not imply A is an ideal of $(R\ltimes R;a,b)$.*

(2) *For a subring R' of R, define a ring $R'\ltimes R$ and the projections p_1, p_2 by the same way as $R\ltimes R$. Then we have the following analogue to Corollary 3.4.*

Let I be an ideal of $R'\ltimes R$. Then $p_1(I)$ is an ideal of R', $p_2(I)$ is an R'-submodule of R, and $p_1(I)\subset p_2(I)$. Also, $p_1(I)\times p_2(I)$ is an ideal of $R'\ltimes R$, but $p_2(I)$ need not be an ideal of R.

Indeed, for (1), consider $A=(2\mathbb{Z}\times 0)\cup(0\times 2\mathbb{Z})$ of $(\mathbb{Z}\ltimes\mathbb{Z};a,b)$. For (2), let $r'\in R'$ and $r\in R$, and $(x,y)\in I$. Then

$$(r',r)*(x,y)=(r'x, rx+r'y)\in I,$$

which yields (i) $(r', 0) * (x, y) = (r'x, r'y) \in I$ and (ii) $(0, r) * (x, y) = (0, rx) \in I$. Thus, obviously $p_1(I)$ is an ideal of R' and $p_2(I)$ is an R'-submodule of R by (i), and $p_1(I) \subset p_2(I)$ by (ii). Also, $p_1(I) \times p_2(I)$ is an ideal of $R' \ltimes R$ in view of (i) and (ii). To see $p_2(I)$ need not be an ideal of R, let $R' = \mathbb{Z}$, $R = \mathbb{R}$. Then, for an ideal $I = 0 \times \mathbb{Z}$ of $R' \ltimes R$, $p_2(I)$ is not an ideal of R.

Remark 3.7. (1) *For any proper ideal I of $R \ltimes R$, $p_1(I) \neq R$, which implies that an ideal $p_1(I) \times p_2(I)$ is proper in $R \ltimes R$, but possibly, $p_2(I) = R$.*

(2) *For any proper ideal I of $\mathbb{Z} \ltimes \mathbb{Z}$, $I' = p_1(I) \times p_2(I)$ is proper by (1). However, for each $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $(a, b) \neq (0, 0)$, there exists a proper ideal I of $(\mathbb{Z} \ltimes \mathbb{Z}; a, b)$ such that $p_1(I) \times p_2(I) = (\mathbb{Z} \ltimes \mathbb{Z}; a, b)$.*

Indeed, for (1), suppose $p_1(I) = R$, and take $(1, y) \in I$. Then $(1, 0) = (1, y) * (1, -y) \in I$, which implies $I = R \ltimes R$, a contradiction. For (2), let p be an odd prime number with $p > |b|$. Let $I = ((1, p))$ $(= \{(x + yap, xp + y(1 + bp)) \mid x, y \in \mathbb{Z}\})$. Then (a) $I \not\ni (1, 0)$, but (b) $p_1(I) \ni 1$, $p_2(I) \ni 1$, which shows that the ideal I is a desired one. To see (a), suppose $I \ni (1, 0)$. Then $x + yap = 1$, $xp + y(1 + bp) = 0$ for some x, $y \in \mathbb{Z}$. Thus $(-ap^2 + 1 + bp)y = -p$, which yields (i) $|-ap^2 + 1 + bp| = 1$, or (ii) $|-ap^2 + 1 + bp| = p$ holds. (i) implies $|b| = |a|p \geq p$ or $p \mid 2$, a contradiction. (ii) implies $(ap - b + 1)p = 1$ or $(ap - b - 1)p = 1$, a contradiction. Hence, $I \not\ni (1, 0)$. For (b), $p_1(I) \ni 1$ by $(1 - ap) + ap = 1$, and $p_2(I) \ni 1$ by $-bp + (1 + bp) = 1$.

Proposition 3.8. *Let R be a principal ideal ring. Let I be an ideal of $(R \ltimes R; a, b)$. Then there exist $(m, t) \in I$ and $n \in R$ such that $I = (m, t) * (R \times 0) + (0, n) * (R \times 0)$ and $I \cap (0 \times R) = 0 \times nR$.*

Proof. Since R is a principal ideal ring, $I \cap (0 \times R) = 0 \times nR$ for some $n \in R$. If $p_1(I) = 0$, then $I \subset 0 \times R$, so $I = 0 \times nR = (0, n) * (R \times 0)$. So, let $p_1(I) \neq 0$. Since $p_1(I)$ is an ideal of R, $p_1(I) = mR$ for some $m \in R$ with $m \neq 0$. Let $(m, t) \in I$. Let (c, d) be any element of I. Then $c = mq$ for some $q \in R$. Since $(c, d) - (m, t) * (q, 0) = (0, d - qt) \in I \cap (0 \times R)$, there exists $j \in R$ such that $(c, d) - (m, t) * (q, 0) = (0, jn)$. Hence $(c, d) = (m, t) * (q, 0) + (0, n) * (j, 0)$. Thus

$$I = (m, t) * (R \times 0) + (0, n) * (R \times 0). \qquad \square$$

Remark 3.9. (1) *For a non-zero ideal I of $(R \ltimes R; a, b)$, let us consider* (*) *$I \cap (0 \times R) \neq 0$. We may assume that I contains (m, t) with $m \neq 0$. Then* (*) *holds if (i) $a = 0$ with $m + bt \neq 0$, or (ii) $m^2 + mbt - at^2 \neq 0$.*

(2) *For $R = \mathbb{Z}$, there exist uniquely m, $n \in R$ with $m \geq 0$, $n \geq 0$ in Proposition 3.8. Also, if $n > 0$, there exists uniquely $t \in \mathbb{Z}$ such that $(m, t) \in I$ and $0 \leq t < n$.*

Indeed, for (1), consider $(m, t) * (0, 1) = (at, m + bt) \in I$ for (i), or $(m, t) * (-at, m) = (0, m^2 + mbt - at^2) \in I$ for (ii). For (2), the first half is obvious. For the latter part, if $(m, i) \in I$, $i = nq + t$ $(0 \leq t < n)$ for some q, $t \in R$, thus $(m, i) - (0, n) * (q, 0) = (m, t) \in I$, which suggests the latter part.

The following is routinely shown.

Lemma 3.10. *For a subset $A = \sum_{i=1}^{k} (p_i, q_i) * (R \times 0)$ of $(R \ltimes R; a, b)$ with $(p_i, q_i) \in (R \ltimes R; a, b)$, A is an ideal of $(R \ltimes R; a, b)$ iff $(p_i, q_i) * (0, 1) \in A$ for $i = 1, \cdots, k$.*

Proposition 3.11. *Let R be an integral domain. Let $A = (m, t) * (R \times 0) + (0, n) * (R \times 0)$ be a subset of $(R \ltimes R; a, b)$. Then A is an ideal of $(R \ltimes R; a, b)$ iff (i) $m \mid at$, (ii) $m \mid an$, and (iii) $mn \mid (m^2 + mbt - at^2)$.*

Proof. Note that $A = \{(xm, xt + yn) \mid x, y \in R\}$. For $A = 0$ (that is, $m = t = n = 0$), the result holds. So, assume $A \neq 0$. For $m = 0$, $A = \{(0, xt + yn) \mid x, y \in R\}$. By Lemma 3.10, A is an ideal iff $(0, t) * (0, 1)$, $(0, n) * (0, 1) \in A$, that is, $at = an = 0$. Thus, for $m = 0$, the result holds. Hence, we assume $m \neq 0$.

Case $n \neq 0$: Assume A is an ideal of $(R \ltimes R; a, b)$. Since $(0, n) * (0, 1) = (an, bn) \in A$, there are x_0, $y_0 \in R$ such that

$x_0m = an$, $x_0t + y_0n = bn$. Thus $(b - y_0)mn = atn$, hence $(b - y_0)m = at$. Thus (i) and (ii) hold. Also, noting $(m, t) * (0, 1) \in A$, there are $x_1, y_1 \in R$ such that $at = x_1m$, $m + bt = x_1t + y_1n$. Then $y_1mn = m^2 + mbt - at^2$. Thus (iii) holds. Conversely, assume (i), (ii) and (iii) hold. Then, by (i) and (ii), there are $x_0, y_0 \in R$ such that $x_0m = an$ and $y_0m = at$. Put $x = x_0$, $y = b - y_0 \in R$. Then $ym = bm - at$, and so $m(xt + yn - bn) = 0$, which yields $bn = xt + yn$. Hence $(0, n) * (0, 1) = (xm, xt + yn) \in A$. Also, by (i) and (iii), there are x_1, $y_1 \in R$ such that $x_1m = at$, $y_1mn = m^2 + mbt - at^2$. Then $(m, t) * (0, 1) = (x_1m, x_1t + y_1n) \in A$. Thus A is an ideal of $(R \ltimes R; a, b)$ by Lemma 3.10.

Case $n = 0$: $A = (m, t) * (R \times 0)$, and the result also holds in view the above proof. □

For a principal ideal domain R, Propositions 3.8 and 3.11 yield the following characterization for a subset of $(R \ltimes R; a, b)$ to be an ideal.

Theorem 3.12. *Let R be a principal ideal domain,* and *A be a subset of $(R \ltimes R; a, b)$. Then A is an ideal of $(R \ltimes R; a, b)$ iff $A = (m, t) * (R \times 0) + (0, n) * (R \times 0)$ for some $m, t, n \in R$ satisfying (i), (ii), and (iii) in Proposition 3.11. In particular, A is an ideal of $R \ltimes R$ iff $A = (m, t) * (R \times 0) + (0, n) * (R \times 0)$ for some $m, t, n \in R$ with $n \mid m$.*

Remark 3.13. *Let $A = (m, t) * (R \times 0) + (0, n) * (R \times 0)$ in $(R \ltimes R; a, b)$. Then $A \ni (1, 0)$ iff $(*)$ m is a unit in R and $n \mid t$. In particular, for A being an ideal of $(R \ltimes R; a, b)$, $A = (R \ltimes R; a, b)$ iff $(*)$ holds.*

References

[1] M. F. Atiyah and L. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, 1969.

[2] Y. Kitamura and Y. Tanaka, Partially ordered rings II, to appear in Tsukuba J. Math.

[3] T. Y. Lam, Lectures on modules and rings, Graduate Texts in Mathematics, 189, Springer, 1998.

可換環の積拡大

北　村　　　好・田　中　祥　雄

数学分野

要　　旨

可換環 R の直積 $R\times R$ において，R の拡大環であるような或る種の環を研究する。このような拡大環は環論的に有用な種々の構造と例を与える。これらの拡大環とそのイデアルを考察し，単項イデアル整域上の拡大環についてそのイデアルの特徴付けを与える。

キーワード：環，R-代数，R-加群，積拡大，直積環，体，整域，イデアル，単項イデアル整域