Kangweon–Kyungki Math. Jour. **2** (1994), pp. 35–38

ON THE GROUP OF DIVISIBILITY OF A SUBRING OF $\bar{Z}_P$

GI–IK KIM AND HEUNG–JOON OH

Let T be an R-algebra. An element $u \in T$ is said to be integral over R if u is a root of a monic polynomial with coefficients in R. If every element of T is integral over R we say that T is integral over R. Then the set of elements of T integral over R forms a subring of T and is called the integral closure of R in T. We denote it by $\bar{R}$. Moreover if $R = \bar{R}$, then we say that R is integrally closed in T.

For an integral domain D, K will usually denote its quotient field and $\bar{D}$ the integral closure of D in the quotient field K.

For an integral domain D with quotient field K, a subset A of K is said to be a fractional ideal of D if A is a D-submodule of K such that $dA \subseteq D$ for some non-zero element d of D. Thus each ideal of D is a fractional ideal of D.

If I is a fractional ideal of an integral domain D, we define I^{-1} by $I^{-1} = \{a \in K | aI \subseteq D\}$. If I and J are fractional ideals of D, we define their product $IJ = \{ a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_i \in I, b_j \in J$ for all i and j $\}$. A fractional ideal I is said to be invertible if $II^{-1} = D$. Notice that for any fractional ideal I we have $II^{-1} \subseteq D$. We denote $(I^{-1})^{-1} = I_v$. A fractional ideal I of D is said to be divisorial (or v-ideal) if $I_v = I$. Equivalently, a fractional ideal I is divisorial if and only if I is the intersection of all principal fractional ideals containing I.

An integral domain V is said to be valuation if for any a and b in V either a divides b or b divides a.

The next theorem gives an equivalent condition for a valuation domain (V, M) with M non-principal to have every v-ideal of V principal.

THEOREM 1. *For a valuation domain (V, M) with M non-principal, the following conditions are equivalent.*

(1) *Every v-ideal of V is principal.*

Received January 4, 1994.

(2) *Every non-principal fractional ideal I of V has the form xM where $x \in V_{\{0\}} - \{0\}$.*

Proof. (1) $\Longrightarrow$ (2). Suppose that every v-ideal of V is principal. Let I be a non-principal fractional ideal of V. Since I is not a v-ideal, $I \subset I_v$. So we have $I \subset (x) \subseteq I_v$ where $x \in I_v - I$. Thus $x^{-1}I \subset V$ and so $x^{-1}I \subseteq M$. Thus $I \subseteq xM$. Suppose that $I \subset xM$. Then $I \subset yV \subseteq xM$, where $y \in xM - I$. Then $x \in I_v \subseteq yV \subseteq xM$ and so $xV = xM$, a contradiction. Hence $I = xM$, where $x \in V_{\{0\}} - \{0\}$.

(2) $\Longrightarrow$ (1). It is enough to show that every non-principal ideal is not divisorial. Let I be a non-principal ideal. Then $I = xM$ for some $x \in V_{\{0\}} - \{0\}$. Moreover, $I_v = xM_v = xM$. Hence I is not a v-ideal.

Let D be an integral domain with quotient field K, $K^* = K - \{0\}$, usually considered as a multiplicative group, and $U(D)$ be the multiplicative group of units of D. Then $G(D) = K^*/U(D)$ is called the group of divisibility of D. We write the group operation on the factor group $G(D) = K^*/U(D)$ as addition:

$$aU(D) + bU(D) = abU(D).$$

Let I be an ideal of a ring D and let $\pi : D \longrightarrow D/I$ be the natural homomorphism. Let S be a subring of D/I. Then the subring $\pi^{-1}(S)$ of D is called the composite of D and S over I.

The following two theorems are useful in finding the group of divisibility.

THEOREM 2. *Let D be a semi-quasilocal ring and I an ideal of D. Let S be a subring of D/I and let $R = \pi^{-1}(S)$ where $\pi : D \longrightarrow D/I$ is the natural map. Then $U(D)/U(R) \simeq U(D/I)/U(S)$.*

Proof. See Lemma 2 in [1].

THEOREM 3. *Let D be an integral domain with $G(D)$ finitely generated. Then $G(D) \simeq G(\bar{D}) \oplus U(\bar{D})/U(D)$, where $G(\bar{D})$ is free.*

Proof. Consider the exact sequence

$$0 \longrightarrow U(\bar{D})/U(D) \longrightarrow G(D) \longrightarrow G(\bar{D}) \longrightarrow 0.$$

Then $G(\bar{D})$ is finitely generated and it is also torsion-free since $\bar{D}$ is integrally closed. Hence $G(\bar{D})$ is free. Therefore, the above exact sequence splits. Hence

$$G(D) \simeq G(\bar{D}) \oplus U(\bar{D})/U(D).$$

EXAMPLE 4. *If D is Noetherian, then $\bar{D}$ is Krull and so $G(\bar{D})$ is free. Thus*

$$G(D) \simeq G(\bar{D}) \oplus U(\bar{D})/U(D).$$

EXAMPLE 5. *Let k be a field and K a proper extension field of k. If $D = k + XK[[X]]$ is the ring of a formal power series over K with constant terms in k, then $G(D) = K^*/k^* \oplus \mathbf{Z}$.*

As a concrete example, let $K = GF(p^{nl})$, $k = GF(p^n)$. Then

$$G(D) = \mathbf{Z} \oplus C,$$

where C is the cyclic group of order $\frac{p^{nl}-1}{p^n-1}$.

THEOREM 6. *Let p be a prime. Let $\mathbf{Z}_p$ be the p-adic integers and $\mathbf{Q}_p$ be the field of rational p-adics and L be a finite extension field of $\mathbf{Q}_p$. Let $(\bar{\mathbf{Z}}_p, (\pi))$ be the integral closure of $\mathbf{Z}_p$ in L and $R = \mathbf{Z}_p + \pi^n\bar{\mathbf{Z}}_p$ $(n \geq 1)$. Then $G(R) = \mathbf{Z} \oplus U(\bar{\mathbf{Z}}_p)/U(R)$.*

Proof. It is well-known that $\bar{\mathbf{Z}}_p$ is a complete DVR and the quotient field of R is L. Moreover

$$1 \longrightarrow U(\bar{\mathbf{Z}}_p)/U(R) \longrightarrow L^*/U(R) \longrightarrow L^*/U(\bar{\mathbf{Z}}_p) \longrightarrow 1$$

splits and so

$$G(R) = \mathbf{Z} \oplus U(\bar{\mathbf{Z}}_p)/U(R) .$$

Consider the following diagram

$$\begin{array}{ccc} \bar{\mathbf{Z}}_p & \xrightarrow{\ \pi\ } & \bar{\mathbf{Z}}_p/\pi^n\bar{\mathbf{Z}}_p \\ \uparrow & & \uparrow \\ R = \pi^{-1}(R/\pi^n\bar{\mathbf{Z}}_p) & \longrightarrow & R/\pi^n\bar{\mathbf{Z}}_p \end{array}$$

Thus $U(\bar{\mathbf{Z}}_p)/U(R) \simeq U(\bar{\mathbf{Z}}_p/\pi^n\bar{\mathbf{Z}}_p)/U(R/\pi^n\bar{\mathbf{Z}}_p)$ and $R/\pi^n\mathbf{Z}_p \simeq \mathbf{Z}_p/\mathbf{Z}_p \bigcap \pi^n\bar{\mathbf{Z}}_p$. Let $\bar{\mathbf{Z}}_p = (\bar{\mathbf{Z}}_p, P)$, $\mathbf{Z}_p = (\mathbf{Z}_p, p)$ and $p\bar{\mathbf{Z}}_p = P^e$. Also, let $r = [\ \frac{n+e-1}{e}\ ]$ and $f = [\bar{\mathbf{Z}}_p/P : \mathbf{Z}_p/p]$. Then

$$R/\pi^n\bar{\mathbf{Z}}_p \simeq \mathbf{Z}_p/\mathbf{Z}_p \bigcap \pi^n\bar{\mathbf{Z}}_p \simeq \mathbf{Z}_p/p^r\mathbf{Z}_p \simeq \mathbf{Z}/p^r\mathbf{Z}.$$

Note that

$$U(\mathbf{Z}/p^r\mathbf{Z}) = \begin{cases} C_{p-1} \times C_{p^{r-1}} & (p \neq 2) \\ C_1 & (p = 2,\ r = 1) \\ C_p & (p = 2,\ r = 2) \\ C_p \times C_{p^{r-2}} & (p = 2,\ r \geq 3) \end{cases}$$

where C_q denotes the cyclic group of order q. We have

$$\begin{aligned} |U(\bar{\mathbf{Z}}_p/\pi^n\bar{\mathbf{Z}}_p)| &= |\bar{\mathbf{Z}}_p/\pi^n\bar{\mathbf{Z}}_p| - |\pi\bar{\mathbf{Z}}_p/\pi^n\bar{\mathbf{Z}}_p| \\ &= p^{nf} - p^{(n-1)f} \\ &= p^{(n-1)f}(p^f - 1). \end{aligned}$$

References

[1] D. D. Anderson, *Integral domains with finitely generated groups of divisibility*, Proc. of the A.M.S. **112** (1991), 613–618.

Department of Mathematics
Myongji University
Yongin 449–728, Korea