

ON THE GROUP OF DIVISIBILITY OF A SUBRING OF Z_p

GI-IL 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 $I^{-1} = \{a \in K \mid aI \subseteq D\}$. If I and J are fractional ideals of D , we define their product $IJ = \{a_1b_1 + a_2b_2 + \dots + a_nb_n \mid a_i \in I, b_j \in J \text{ for all } i \text{ and } j\}$. 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) $\Rightarrow$ (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) $\Rightarrow$ (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 $\pi : D \rightarrow D/I$ 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 $\pi : D \rightarrow D/I$ 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

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

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

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

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 $G(D) = K^*/k^* \oplus \mathbb{Z}$.

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

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

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

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

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

$$1 \rightarrow U(\mathbb{Z}_p)/U(R) \rightarrow L^*/U(R) \rightarrow L^*/U(\mathbb{Z}_p) \rightarrow 1$$

splits and so

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

Consider the following diagram

$$\begin{array}{ccc} \mathbb{Z}_p & & R = \pi^{-1}(R/\pi^n \mathbb{Z}_p) \\ \downarrow & & \downarrow \\ \mathbb{Z}_p/\pi^n \mathbb{Z}_p & \xrightarrow{\pi} & R/\pi^n \mathbb{Z}_p \end{array}$$

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

$$R/\pi^n \mathbb{Z}_p \simeq \mathbb{Z}_p/\mathbb{Z}_p \cup \pi^n \mathbb{Z}_p \simeq \mathbb{Z}_p^{(p)}/P^r \mathbb{Z}_p^{(p)} \simeq \mathbb{Z}_p^{(p)}/P^f \mathbb{Z}_p^{(p)} \simeq \mathbb{Z}_p^{(p)}/P^e \mathbb{Z}_p^{(p)}.$$

Note that

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

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

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

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
Myeungji University
Yongin 449-728, Korea