

Title	On prime ideals of a Witt ring over a local ring
Author(s)	Kanzaki, Teruo; Kitamura, Kazuo
Citation	Osaka Journal of Mathematics. 9(2) P.225-P.229
Issue Date	1972
Text Version	publisher
URL	https://doi.org/10.18910/7379
DOI	10.18910/7379
rights	
Note	

Osaka University Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

Osaka University

ON PRIME IDEALS OF A WITT RING OVER A LOCAL RING

TERUO KANZAKI AND KAZUO KITAMURA

(Received August 9, 1971)

In this note, we consider commutative local rings with invertible element 2, and give a relation between an ordered local ring and a prime ideal of Witt ring over it which is a generalization of the results of Lorenz and Leicht [3] related to prime ideals of Witt ring over a field. By [5], any non-degenerate and finitely generated projective quadratic module (V, q) over a local ring R can be written as a form $(V, q) = \langle a_1 \rangle \perp \langle a_2 \rangle \perp \cdots \perp \langle a_r \rangle$, where a_i is in the unit group $U(R)$ of R and $\langle a_i \rangle$ denotes a rank one free quadratic submodule $(Rv_i, q|_{Rv_i})$ such that $q(v_i) = \frac{a_i}{2}$. If, for any element a in $U(R)$, the element having the representative $\langle a \rangle$ in the Witt ring $W(R)$ is denoted by a , then any element of $W(R)$ can be written as a sum of elements of $U(R)$. We use \perp , \top and \otimes for the notations of sum, difference and product in $W(R)$. In §1, we have essentially same argument for Witt ring over a local ring as one in [3]. In §2, we study about an ordered local ring R which is an ordered ring such that every unit in R is either >0 or <0 , and give a generalization of Sylvester's theorem. In §3, we give an one to one correspondence between such orderings on R and prime ideals \mathfrak{P} of $W(R)$ such that $W(R)/\mathfrak{P} \approx \mathbb{Z}$. Throughout this paper, we assume that the ring R is commutative local ring with invertible element 2, and every R -module is unitary.

1. Let R be a local ring with the maximal ideal \mathfrak{m} and the unit group $U(R)$. Since $\langle a \rangle \otimes_R \langle b \rangle \approx \langle ab \rangle$ for $a, b \in U(R)$, we have $(a \perp 1) \otimes (a \top 1) = a^2 \top 1 = 1 \perp (-1) = 0$ in $W(R)$ for any a in $U(R)$. Therefore, we have the following analogous argument on local ring R to [3]. If \mathfrak{P} is any prime ideal of $W(R)$, then any element a in $U(R)$ is either $a \equiv 1 \pmod{\mathfrak{P}}$ or $a \equiv -1 \pmod{\mathfrak{P}}$. We denote $\varepsilon_{\mathfrak{P}}(a) = 1$ or -1 , if $a \equiv 1 \pmod{\mathfrak{P}}$ or $a \equiv -1 \pmod{\mathfrak{P}}$, respectively. Then for any element $\alpha \in W(R)$, say $\alpha = a_1 \perp a_2 \perp \cdots \perp a_n$ for $a_i \in U(R)$, we have $\alpha \equiv \varepsilon_{\mathfrak{P}}(a_1) \perp \varepsilon_{\mathfrak{P}}(a_2) \perp \cdots \perp \varepsilon_{\mathfrak{P}}(a_n) \pmod{\mathfrak{P}}$, therefore there exists an epimorphism $Z \rightarrow W(R)/\mathfrak{P}$, and so $W(R)/\mathfrak{P} \approx \mathbb{Z}$ or $\approx \mathbb{Z}/(p)$ for some prime number p in the integers \mathbb{Z} . Accordingly, we have

(1.1) $W(R)/\mathfrak{P} \approx Z$ if and only if \mathfrak{P} is a minimal prime ideal of $W(R)$ which is not maximal.

(1.2) $W(R)/\mathfrak{P} \approx Z/(p)$ for some prime number p if and only if \mathfrak{P} is a maximal ideal of $W(R)$.

(1.3) $W(R)$ is a Jacobson ring, i.e. every prime ideal is an intersection of maximal ideals.

There is an epimorphism $W(R) \rightarrow Z/(2)$ such that if $\alpha = a_1 \perp a_2 \perp \cdots \perp a_n$ is in $W(R)$ for $a_i \in U(R)$ then α corresponds to $n \pmod{2}$. Then we denote $\ker(W(R) \rightarrow Z/(2))$ by \mathfrak{M} .

(1.4) A prime ideal \mathfrak{P} is $\mathfrak{P} \neq \mathfrak{M}$ if and only if $1 \not\equiv -1 \pmod{\mathfrak{P}}$.

(1.5) Any minimal prime ideal \mathfrak{P} of $W(R)$ is contained in \mathfrak{M} .

2. We call that local ring R is an *ordered local ring* if R is an ordered ring such that every unit is either positive element or negative element (R is not necessarily total ordered). For ordered local ring R , we call that the set of positive units in $U(R)$ is the *positive units part* of R .

(2.1) **Proposition.** A local ring R is an ordered local ring if and only if there exists a subset P satisfying the following conditions

$$(1) \quad P \cup -P = U(R)$$

$$(2) \quad P \cap -P = \phi$$

$$(3) \quad P \cdot P \subset P$$

$$(4) \quad (P+P) \cap U(R) \subset P.$$

Proof. Let P be a subset of $U(R)$ satisfying the conditions. We set $m_+ = \{x \in m; \text{there exists } a \in P \text{ such that } x - a \in P\}$, and $Q = P \cup m_+$. Then we have the following properties:

1) $m_+ \cap -m_+ = \phi$. Because, if there exists an element x in $m_+ \cap -m_+$, then there exists a, b in P such that $x - a$ and $-x - b$ are in P , and so $-(a+b) = (x-a) + (-x-b) \in P+P$. If $a+b$ is in $U(R)$, it is impossible by 4) and 2). Therefore, $a+b \in m$ and $a-b = (a+b) - 2b \in U(R)$. If $a-b \in P$, then $x-b = (x-a) + (a-b) \in P$ and so $-2b = (x-b) + (-x-b) \in P$, it is a contradiction to (2). If $b-a$ is in P , then similarly we have contradiction $-2a = (x-a) + (-x-a) \in P$.

Analogously, we have easily

$$2) \quad (P+P) \cap m \subset m_+.$$

$$3) \quad (P+m_+) \subset P.$$

$$4) \quad m_+ + m_+ \subset m_+.$$

- 5) $P \cdot m_+ \subset m_+$.
- 6) $m_+ \cdot m_+ \subset m_+$.

Therefore Q has the properties (I) $Q \cap -Q = \phi$, (II) $Q \cdot Q \subset Q$ and (III) $Q + Q \subset Q$. By the set Q , we can make R an ordered ring which has positive part Q . The converse is clear.

We denote by $k = R/m$ the residue field of R and $\varphi: R \rightarrow k$ the canonical homomorphism.

(2.2) Proposition. *Let R be an ordered local ring with positive units part P . Then it satisfies $P + P \subset P$ if and only if k is a total ordered field such that $\varphi(P)$ is the positive part, i.e. k is a formal real field.*

Proof. If $k = R/m$ is a total ordered field such that $\varphi(P)$ is the positive part, then $\varphi(P) + \varphi(P) \subset \varphi(P)$ and $0 \notin \varphi(P)$, therefore we have $P + P \subset P$. Conversely, if $P + P \subset P$, then we have $\varphi(P) \cap -\varphi(P) = \phi$. Therefore, we obtain easily that k is total ordered field with positive part $\varphi(P)$.

Let P be any subset of local ring R satisfying the conditions in (2.1) and $Q = P \cup m_+$, where $m_+ = \{x \in m; \exists a \in P; x - a \in P\}$.

(2.3) *For any x, y in R , $x + y \in Q$ implies $x \in Q$ or $y \in Q$.*

Proof. Let $x + y \in Q$. If $x + y \in P$, then $x \in U(R)$ or $y \in U(R)$. If x and y are in $U(R)$, then $x \in P$ or $y \in P$. If $x \in U(R)$ and $y \in m$, then $x \in P$ or $y \in m_+$. If $x + y$ is in m_+ , there exists $a \in P$ such that $x + y - a \in P$. Since $x + y - a = (x - \frac{a}{2}) + (y - \frac{a}{2})$, we have $x - \frac{a}{2} \in P$ or $y - \frac{a}{2} \in P$, accordingly $x \in m_+$ or $y \in m_+$.

(2.4) Proposition. *Let P and Q be as above. Then $\mathfrak{p} = \{x \in R; x \notin Q \cup -Q\}$ is a prime ideal of R .*

Proof. From (2.3), we have $\mathfrak{p} + \mathfrak{p} \subset \mathfrak{p}$. We shall show that for any $r \in R$ and $x \in \mathfrak{p}$ we have $rx \in \mathfrak{p}$. We assume $rx \notin \mathfrak{p}$. Then we may assume $rx \in Q$. It is considered in the three cases; 1) If $r \in U(R)$, then it is impossible that $rx \in Q \cup -Q$. 2) If $r \in m_+$, then there exists $a \in P$ such that $r - a = c \in P$, and from (2.3) $xa + xc = xr \in Q$ implies $xa \in Q$ or $xc \in Q$, it is impossible from the first case. 3) If $r \in \mathfrak{p}$, then $xr \in m_+$ and so there exists $a \in P$ such that $xr - a \in P$. Since $r(x - a) + a(r - 1) = xr - a \in Q$, we have $r(x - a) \in Q$ or $a(r - 1) \in Q$. But $a(r - 1) \in Q$ is impossible. Therefore, it must be $r(x - a) \in Q$. But, it is also impossible from the first case. Accordingly, $rx \in \mathfrak{p}$, and \mathfrak{p} is an ideal of R . Since $(Q \cup -Q)(Q \cup -Q) \subset Q \cup -Q$, \mathfrak{p} is a prime ideal.

(2.5) Theorem. *Let R be an ordered local ring with the positive units part P , and let Q and \mathfrak{p} be as (2.4). Then the localization $R_{\mathfrak{p}} = Q^{-1}R$ of R by prime ideal*

\mathfrak{p} is also an ordered local ring such that $\hat{Q} = Q^{-1}Q$ is the positive units part and $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is a formal real field. Let \mathfrak{R} be the real closure of $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Then there exists a ring homomorphism $f: R \rightarrow \mathfrak{R}$ such that f induces the epimorphism $\bar{f}: W(R) \rightarrow W(\mathfrak{R}) \approx Z$, and $f(P)$ is contained in the positive part of \mathfrak{R} , furthermore $\ker \bar{f}$ is generated by $\{x \top 1; x \in P\}$.

Proof. It is obvious that $\hat{Q} \cup -\hat{Q} = U(R_{\mathfrak{p}})$, $\hat{Q} \cap -\hat{Q} = \phi$, $\hat{Q}\hat{Q} \subset \hat{Q}$ and $\hat{Q} + \hat{Q} \subset \hat{Q}$. Therefore, by (2.2) the canonical homomorphism $\varphi': R_{\mathfrak{p}} \rightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ induces a total ordering on $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Therefore, $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is a formal real field. Let \mathfrak{R} be the real closure of $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Then $W(\mathfrak{R}) \approx Z$. Let $f: R \rightarrow \mathfrak{R}$ be the composition of ring homomorphisms $R \rightarrow R_{\mathfrak{p}} \xrightarrow{\varphi'} R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \rightarrow \mathfrak{R}$. The positive units part of R is sent to the positive part of \mathfrak{R} . Therefore, f induces the ring epimorphism $\bar{f}: W(R) \rightarrow W(\mathfrak{R})$, and $\ker \bar{f}$ is generated by $\{x \top 1; x \in P\}$. Because, if α is any element in $\ker \bar{f}$ and $\alpha = a_1 \perp a_2 \perp \dots \perp a_n$, then we have $\varepsilon_{\mathfrak{p}}(a_1) \perp \varepsilon_{\mathfrak{p}}(a_2) \perp \dots \perp \varepsilon_{\mathfrak{p}}(a_n) = 0$, in $W(\mathfrak{R})$, also in $W(R)$, where $\varepsilon_{\mathfrak{p}}a() = \begin{cases} 1: a \in P \\ -1: a \in -P \end{cases}$. Since $\varepsilon_{\mathfrak{p}}(a_i)a_i$ is in P for $i=1, 2, \dots, n$, we have $\alpha = a_1 \perp a_2 \perp \dots \perp a_n \perp (\varepsilon_{\mathfrak{p}}(a_1) \perp \dots \perp \varepsilon_{\mathfrak{p}}(a_n)) = \varepsilon_{\mathfrak{p}}(a_1) \otimes (\varepsilon_{\mathfrak{p}}(a_1)a_1 \top 1) \perp \dots \perp \varepsilon_{\mathfrak{p}}(a_n) \otimes (\varepsilon_{\mathfrak{p}}(a_n)a_n \top 1)$ in $W(R)$. Therefore we have $\ker \bar{f} \subset (\{x \top 1; x \in P\})$. $\ker \bar{f} \supset \{x \top 1; x \in P\}$ is clear.

We have the following Sylvester's theorem for ordered local ring.

(2.6) Corollary. *Let R be an ordered local ring, and (V, q) a non-degenerate and finitely generated projective quadratic R -module. If $(V, q) \approx \langle a_1 \rangle \perp \langle a_2 \rangle \perp \dots \perp \langle a_r \rangle \perp \langle -b_1 \rangle \perp \langle -b_2 \rangle \perp \dots \perp \langle -b_s \rangle$ for positive units a_1, a_2, \dots, a_r and b_1, b_2, \dots, b_s in R , then the integer $r-s$ is uniquely determined by (V, q) .*

Proof. From (2.5), there exists a real closed field \mathfrak{R} and a ring homomorphism $f: R \rightarrow \mathfrak{R}$ such that the positive units part of R is sent to the positive part of \mathfrak{R} . If $(V, q) \approx \langle a_1 \rangle \perp \dots \perp \langle a_r \rangle \perp \langle \perp b_1 \rangle \perp \dots \perp \langle -b_s \rangle \approx \langle a_1' \rangle \perp \dots \perp \langle a_r' \rangle \perp \langle -b_1' \rangle \perp \dots \perp \langle -b_s' \rangle$, then $(\sum_{i=1}^r \perp a_i) \top (\sum_{i=1}^s \perp b_i) = (\sum_{i=1}^{r'} \perp a_i') \top (\sum_{i=1}^{s'} \perp b_i')$ in $W(R)$, and by the ring homomorphism $\bar{f}: W(R) \rightarrow W(\mathfrak{R}) \approx Z$ induced by f , it is sent to $r-s = r'-s'$.

3. We shall show the following main theorem.

(3.1) Theorem. *For any local ring R with invertible 2, there exists an one to one correspondence between the set of minimal prime ideals \mathfrak{P} of $W(R)$ such that $\mathfrak{P} \neq \mathfrak{M}$ and the set of subsets P of $U(R)$ satisfying the conditions (1), (2), (3) and (4) in (2.1), i.e. the set of minimal orderings on R such that R makes ordered local ring.*

This theorem is obtained from the following arguments.

(3.2) Let \mathfrak{P} be a prime ideal of $W(R)$ such that $\mathfrak{P} \neq \mathfrak{M}$, and put $P(\mathfrak{P}) = \{x \in U(R) : x \equiv 1 \pmod{\mathfrak{P}}\}$. Then $P(\mathfrak{P})$ satisfies the conditions (1), (2), (3) and (4) in (2.1). Therefore R is an ordered local ring with positive part $Q(\mathfrak{P}) = \mathfrak{P}(\mathfrak{P}) \cup \{x \in \mathfrak{m} : \exists a \in P(\mathfrak{P}) ; x - a \in P(\mathfrak{P})\}$. If $\mathfrak{P}(P(\mathfrak{P}))$ denotes the ideal of $W(R)$ generated by $\{x \top 1 : x \in P(\mathfrak{P})\}$, then $\mathfrak{P}(P(\mathfrak{P}))$ is a minimal prime ideal of $W(R)$ such that $\mathfrak{P} \supset \mathfrak{P}(P(\mathfrak{P}))$. Therefore, if \mathfrak{P} is a minimal prime ideal of $W(R)$, then $\mathfrak{P} = \mathfrak{P}(P(\mathfrak{P}))$.

Proof. The proof of conditions (1), (2), (3), and (4) is obtained similarly to the case over field (cf. [4]). The other part is obvious.

(3.3) Let P be a subset of R satisfying the conditions (1), (2), (3) and (4) in (2.1). Then we have $P(\mathfrak{P}(P)) = P$.

Proof. Since $\mathfrak{P}(P) = \{x \top 1 ; x \in P\}$, $P(\mathfrak{P}(P)) \supset P$ is obvious. If there exists an element x in $P(\mathfrak{P}(P))$ such that $x \notin P$, then $x \in -P$, and so $-x \top 1 \in \mathfrak{P}(P)$. Therefore, we have $1 \equiv x \equiv -1 \pmod{\mathfrak{P}(P)}$, it is contradiction to $\mathfrak{P}(P) \neq \mathfrak{M}$. Accordingly, we have $P(\mathfrak{P}(P)) = P$.

(3.4) Corollary. For any local ring R with invertible 2, the Witt ring $W(R)$ is either a local ring with the maximal ideal \mathfrak{M} such that \mathfrak{M} is nil ideal and $W(R)\mathfrak{M} \approx Z/(2)$, or a Jacobson ring such that every maximal ideal has height 1 and every minimal prime ideal has a residue ring isomorphic to Z .

(3.5) Corollary. If R is a local domain with altitude 1 and an ordered local ring, then R is a total ordered ring, or the residue field is a formal real field.

OSAKA CITY UNIVERSITY
OSAKA KYOIKU DAIGAKU

References

- [1] S. Bruno et T. Kanzaki: *Sur l'anneau de Witt d'un anneau local*, C.R. Acad. Sci. Paris Ser. A-B. **272** (1971), 1691–1694.
- [2] T. Kanzaki: *On bilinear module and Witt ring over a commutative ring*, Osaka J. Math. **8** (1971), 485–496.
- [3] F. Lorenz und J. Leicht: *Die primideal des Wittschen Ringes*, Invent. Math. **10** (1970), 82–88.
- [4] F. Lorenz: *Quadratische Formen über Körpern*, Lecture Notes in Math. 130, Springer-Verlag, 1970.
- [5] A. Micali et O. Villamayor: *Sur les algèbres de Clifford*, Ann. Sci. Ecole Norm. Sup. **1** (1968), 271–304.

