<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>On prime ideals of a Witt ring over a local ring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Kanzaki, Teruo; Kitamura, Kazuo</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 9(2) P.225-P.229</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1972</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/7379">https://doi.org/10.18910/7379</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/7379</td>
</tr>
</tbody>
</table>
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 $\perp$, $\uparrow$ 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 $W(R)/\mathfrak{P} \cong \mathbb{Z}$. 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 $m$ 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 $(a \perp 1) \otimes (a \uparrow 1) = a^2 \uparrow 1 = 1 \perp (-1) = 0$ 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 $e_{\mathfrak{P}}(a) = 1$ or $-1$, if $a \equiv 1 \pmod{\mathfrak{P}}$ or $a \equiv -1 \pmod{\mathfrak{P}}$, respectively. Then for any element $a \in W(R)$, say $\alpha = a_1 \perp a_2 \perp \cdots \perp a_n$ for $a_i \in U(R)$, we have $\alpha \equiv e_{\mathfrak{P}}(a_1) \perp e_{\mathfrak{P}}(a_2) \perp \cdots \perp e_{\mathfrak{P}}(a_n) \pmod{\mathfrak{P}}$, therefore there exists an epimorphism $\mathbb{Z} \rightarrow W(R)/\mathfrak{P}$, 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) \( W(R)/\mathfrak{P} = \mathbb{Z} \) if and only if \( \mathfrak{P} \) is a minimal prime ideal of \( W(R) \) which is not maximal.

(1.2) \( W(R)/\mathfrak{P} = \mathbb{Z}/(p) \) 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 \( W(R) \to \mathbb{Z}/(2) \) 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 \( \alpha \) corresponds to \( n \mod 2 \). Then we denote \( \ker (W(R) \to \mathbb{Z}/(2)) \) by \( \mathfrak{M} \).

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

(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

\begin{align*}
(1) & \quad P \cup -P = U(R) \\
(2) & \quad P \cap -P = \phi \\
(3) & \quad P \cdot P \subseteq P \\
(4) & \quad (P + P) \cap U(R) \subseteq P.
\end{align*}

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, \( a+b \equiv m \) and \( a-b = (a+b) - 2b \equiv U(R) \). If \( a-b \in P \), then \( x-b = (x-a)+(x-b) \in P \) 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) \( (P+P) \cap m \subseteq m_+ \).
3) \( (P+m_+) \subseteq P \).
4) \( m_+ + m_+ \subseteq m_+ \).
5) $P \cdot m_+ \subseteq m_+.$
6) $m_+ \cdot m_+ \subseteq m_+.$

Therefore $Q$ has the properties (I) $Q \cap -Q = \emptyset,$ (II) $Q \cdot Q \subseteq Q$ and (III) $Q + Q \subseteq Q.$ 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 $\varphi: R \to k$ the canonical homomorphism.

(2.2) Proposition. Let $R$ be an ordered local ring with positive units part $P.$ Then it satisfies $P + P \subseteq P$ 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 $\varphi(P) + \varphi(P) \subseteq \varphi(P)$ and $0 \notin \varphi(P),$ therefore we have $P + P \subseteq P.$ Conversely, if $P + P \subseteq P,$ then we have $\varphi(P) \cap -\varphi(P) = \emptyset.$ 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 $x + y - a = (x - a) + (y - a),$ we have $x - a \in P$ or $y - a \in P,$ accordingly $x \in m_+$ or $y \in m_+.$

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

Proof. From (2.3), we have $\wp + \wp \subseteq \wp.$ We shall show that for any $r \in R$ and $x \in \wp$ we have $rx \in \wp.$ We assume $rx \notin \wp.$ 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 $r \in \wp,$ 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, $rx \in \wp,$ and $\wp$ is an ideal of $R.$ Since $(Q \cup -Q) (Q \cup -Q) \subseteq Q \cup -Q,$ $\wp$ is a prime ideal.

(2.5) Theorem. Let $R$ be an ordered local ring with the positive units part $P,$ and let $Q$ and $\wp$ be as (2.4). Then the localization $R_\wp = Q^{-1}R$ of $R$ by prime ideal
Proof. It is obvious that $\hat{Q} \cup -\hat{Q} = U(R_p)$, $\hat{Q} \cap -\hat{Q} = \emptyset$, $\hat{Q} \hat{Q} \subset \hat{Q}$ and $\hat{Q} + \hat{Q} \subset \hat{Q}$. Therefore, by (2.2) the canonical homomorphism $\varphi^r: R_p \to R_p/\varphi R_p$ induces a total ordering on $R_p/\varphi R_p$. Therefore, $R_p/\varphi R_p$ is a formal real field. Let $W^S_\mathfrak{a}$ be the real closure of $R_p/\varphi R_p$. Then $W(R) \approx Z$. Let $f: R \to W^S_\mathfrak{a}$ be the composition of ring homomorphisms $R \to R_p \xrightarrow{\nu} R_p/\varphi R_p \to W^S_\mathfrak{a}$. The positive units part of $R$ is sent to the positive part of $W^S_\mathfrak{a}$. Therefore, $f$ induces the ring epimorphism $f^R: W(R) \to W(R)$. Furthermore, $\ker f^R$ is generated by $\{a_i a_j; 1 \leq i, j \leq n\}$. Because, if $a$ is any element in $\ker f^R$ and $a = a_1 \perp a_2 \perp \cdots \perp a_n \in W(R)$, then $\epsilon_\mathfrak{a}(a) = 1: a \in P$. Since $\epsilon_\mathfrak{a}(a_i) a_i$ is in $P$ for $i = 1, 2, \ldots, n$, we have $a = a_1 \perp a_2 \perp \cdots \perp a_n \perp a_i \epsilon_\mathfrak{a}(a_i) \perp \cdots \perp a_n \perp a_i \epsilon_\mathfrak{a}(a_i) \perp \cdots \perp a_n \perp a_i \epsilon_\mathfrak{a}(a_i)$ in $W(R)$. Therefore we have $\ker f^R \subset \{x + T; x \in P\}$. Because, $\ker f^R$ is a real closed field $W(R)$.

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 $(V, q) \approx (a_i) \perp (a_i) \perp \cdots \perp (a_i) \perp (-b_1) \perp (-b_2) \perp \cdots \perp (-b_s)$ for positive units $a_1, a_2, \ldots, a_r$ and $b_1, b_2, \ldots, b_s$ in $R$, then the integer $r - s$ is uniquely determined by $(V, q)$.

Proof. From (2.5), there exists a real closed field $\mathfrak{a}$ and a ring homomorphism $f: R \to \mathfrak{a}$ such that the positive units part of $R$ is sent to the positive part of $\mathfrak{a}$. If $(V, q) \approx (a_i) \perp \cdots \perp (a_i) \perp (-b_1) \perp (-b_2) \perp \cdots \perp (-b_s) \approx (a_i) \perp \cdots \perp (a_i) \perp (-b_1) \perp \cdots \perp (-b_s)$, then $(\sum_{i=1}^{r^1} a_i \perp b_i) \perp (\sum_{i=1}^{r^1} a_i \perp b_i) \perp (\sum_{i=1}^{r^1} a_i \perp b_i) \perp \cdots \perp (\sum_{i=1}^{r^1} a_i \perp b_i)$ in $W(R)$, and by the ring homomorphism $f^R: W(R) \to W(R) \approx Z$ 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 $\mathfrak{p} \neq \mathfrak{a}$ 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 $\mathfrak{B}$ be a prime ideal of $W(R)$ such that $\mathfrak{B} \neq \mathfrak{M}$, and put $P(\mathfrak{B}) = \{x \in U(R): x \equiv 1 \pmod{\mathfrak{B}}\}$. Then $P(\mathfrak{B})$ satisfies the conditions (1), (2), (3) and (4) in (2.1). Therefore $R$ is an ordered local ring with positive part $Q(\mathfrak{B}) = \mathfrak{B}(\mathfrak{B}) \cup \{x \in m: \exists a \in P(\mathfrak{B}); x - a \in P(\mathfrak{B})\}$. If $\mathfrak{B}(P(\mathfrak{B}))$ denotes the ideal of $W(R)$ generated by $\{x \in P(\mathfrak{B})\}$, then $\mathfrak{B}(P(\mathfrak{B}))$ is a minimal prime ideal of $W(R)$ such that $\mathfrak{B} \supset \mathfrak{B}(P(\mathfrak{B}))$. Therefore, if $\mathfrak{B}$ is a minimal prime ideal of $W(R)$, then $\mathfrak{B} = \mathfrak{B}(P(\mathfrak{B}))$.

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 $P(\mathfrak{B}(P)) = P$.

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

(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.

References
