SEMISPRINGING RING ENGAGED BY ALGEBRAIC INTEGERS

DAVID E. DOBBS AND MARCO FONTANA

§1. Introduction. For each algebraic integer $\alpha$, let $\mathbb{Z}_\alpha$ denote the ring of integers of the algebraic number field $\mathbb{Q}(\alpha)$. There has been continuing interest in finding ring-theoretic conditions characterizing when $\mathbb{Z}_\alpha$ coincides with its subring $\mathbb{Z}[\alpha]$ (cf. [15, 18, 1, 13, 12]). One way to extend such work is to consider the intermediate ring $\mathbb{Z}[\alpha]^+$, the seminormalization (in the sense of [17]) of $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_\alpha$. Indeed, if we let $I_\alpha$ denote the conductor $(\mathbb{Z}[\alpha]: \mathbb{Z}_\alpha)$, then it is easy to see (cf. Proposition 3.1) that $\mathbb{Z}[\alpha] = \mathbb{Z}_\alpha$, if, and only if, $\mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha$ and $I_\alpha$ is a radical ideal of $\mathbb{Z}_\alpha$. The condition $\mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha$ seems worthy of separate attention in view of recent results (cf. [3]) that seminormal rings generated by algebraic integers are “often” automatically of the form $\mathbb{Z}_\alpha$. We show in Proposition 3.3 that the condition $\mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha$ is equivalent to several universal properties, including notably that the canonical closed surjection $\text{Spec}(\mathbb{Z}_\alpha) \to \text{Spec}(\mathbb{Z}[\alpha])$ be universally open, be universally going-down, or be a universal homeomorphism.

Quadratic algebraic number fields present a situation in which the condition $\mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha$ may be characterized in terms of elementary number theory. Recall that each quadratic number field $K$ is uniquely of the form $\mathbb{Q}(\sqrt{d})$, for a suitable square-free integer $d$. As usual, let

$$\omega_d = \begin{cases} \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod{4}, \\ \sqrt{d}, & \text{if } d \equiv 2, 3 \pmod{4}. \end{cases}$$

It is well-known that the ring of integers of $K$ (that is, the maximal order of $K$) is $\mathbb{Z}[\omega_d]$, which is a free abelian group on the basis $\{1, \omega_d\}$. Each non-maximal order of $K$ is uniquely of the form $\mathbb{Z}[n\omega_d]$, for a suitable integer $n \geq 2$. For $\alpha = n\omega_d$, the property $\mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha$ is just $\mathbb{Z}[n\omega_d]^+ = \mathbb{Z}[\omega_d]$, and this is characterized in Theorem 3.4 via divisibility and ramification conditions; alternately, via divisibility and congruence conditions on $d$ and $n$.

At the other extreme from the behaviour $\mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha$ is the condition $\mathbb{Z}[\alpha]^+ = \mathbb{Z}[\alpha]$, i.e., the condition that $\mathbb{Z}[\alpha]$ be seminormal. For the quadratic case, $\alpha = n\omega_d$, Corollary 4.5 characterizes this new condition in the above spirit of elementary number theory. This result generalizes some work of Ooishi [16]. Moreover the main result of this paper, Theorem 4.4, identifies $\mathbb{Z}[n\omega_d]^+$ for $d, n$ as above; that is, finds the $m$ so that $(1 \leq m | n)$, $\mathbb{Z}[n\omega_d]^+ = \mathbb{Z}[m\omega_d]$. As $\mathbb{Z}[\omega_d]$ is trivially (semi)normal, this amounts to finding the seminormalization of an arbitrary order in a quadratic algebraic number field.
If one omits universality from the considerations of the first paragraph, one arrives at the condition “Spec \((\mathbb{Z}_\alpha)\to\text{Spec} (\mathbb{Z}[\alpha])\) is a homeomorphism and \(I_\alpha\) is a radical ideal of \(\mathbb{Z}_\alpha\).” It is easy to see (cf. Proposition 2.1) that this is equivalent to “\(\mathbb{Z}[\alpha]\) is a GPVD”. (A GPVD, or globalized pseudo-valuation domain, is a particularly tractable type of seminormal integral domain introduced \textit{via} pullbacks in \([4, 5]\).) Theorem 2.5, which is the principal result in section 2, identifies all the quadratic orders which are GPVD’s. Since all rings of integers are GPVD’s, this amounts to characterizing when \(\mathbb{Z}[n\omega_d]\) is a GPVD; and this is done, in the above spirit of elementary number theory, \textit{via} conditions on divisibility, congruence, and Legendre symbols. These conditions permit effective calculations, yielding for instance (in Remark 3.5(c)) the first known examples in which \(\mathbb{Z}[n\omega_d]\) is seminormal but not a GPVD. In these examples, \(n = 2\). It should be noted that the case \(n = 2\) of Theorem 2.5 is a completion of the work begun in \([5, \text{Example } 4]\), where it had been shown that \(\mathbb{Z}[\sqrt{d}]\) is a GPVD, if, and only if, either \(d = 2, 3 \pmod{4}\) or \(d = 5 \pmod{8}\). As to this paper’s organization, we begin by generalizing this result from \([5]\), and the techniques lead naturally to seminormalization of quadratic orders.

The notations \(\mathbb{Z}_\alpha\), \(I_\alpha\) and \(\omega_d\) will always be used in the senses defined above. For background, the reader is referred to the cited articles on seminormalization, weak normalization, universal properties and GPVD’s; and to standard texts such as \([9, 14, 19]\). The interested reader is invited to replace \(\mathbb{Z}\) wherever possible with a suitable one-dimensional Noetherian (possibly Dedekind) integral domain.

§2. GPVD orders. The main result of this section, Theorem 2.5, determines precisely which of the quadratic orders \(\mathbb{Z}[n\omega_d]\) is a GPVD. In preparation for this, we give two propositions, each of some independent interest.

First, for the sake of completeness, we shall recall some background definitions and facts from \([4]\). An integral domain \(R\) is said to be a pseudo-domain (PVD) in the case when \(R\) has a (necessarily unique) valuation overring \(V\) such that \(\text{Spec} (R) = \text{Spec} (V)\) as sets. PVD’s may be characterized as the pullbacks \(V_{\alpha}K\), where \((V, M)\) is a valuation domain and \(K\) is a subfield of \(k = V/M\). An integral domain \(R\) is said to be a locally pseudo-valuation domain (LPVD) if \(R_M\) is a PVD for each maximal ideal \(M\) of \(R\). Each PVD is an LPVD, as is each Prüfer domain as well. Finally, an integral domain \(R\) is said to be a globalized pseudo-valuation domain (GPVD) if \(R\) has a (canonically associated) Prüfer overring \(T\) such that (a) the canonical contraction map \(\text{Spec} (T)\to\text{Spec} (R)\) is a bijection; and (b) there exists a nonzero radical ideal \(A\) common to \(T\) and \(R\) such that each prime ideal of \(T\) (resp., \(R\)) which contains \(A\) is a maximal ideal of \(T\) (resp., \(R\)). Each Prüfer domain is a GPVD, and each GPVD is an LPVD. However, an LPVD need not be a GPVD, even in the one-dimensional or Noetherian cases. For quasi-local domains, the notions of PVD, LPVD, and GPVD coincide.

**Proposition 2.1.** Let \(\alpha\) be an algebraic integer and \(f: \text{Spec} (\mathbb{Z}_\alpha)\to \text{Spec} (\mathbb{Z}[\alpha])\) the canonical contraction map. Then the following conditions are equivalent.
(1) \( \mathbb{Z}[\alpha] \) is seminormal and \( f \) restricts to a bijection \( \text{Ass}_{\mathbb{Z}_{\alpha}}(I_{\alpha}) \to \text{Ass}_{\mathbb{Z}[\alpha]}(I_{\alpha}) \).

(2) \( I_{\alpha} \) is a radical ideal of \( \mathbb{Z}_{\alpha} \) and \( f \) is a homeomorphism (with respect to Zariski topology).

(3) \( I_{\alpha} \) is a radical ideal of \( \mathbb{Z}_{\alpha} \) and \( f \) is a bijection.

(4) \( I_{\alpha} \) is a radical ideal of \( \mathbb{Z}_{\alpha} \) and \( f \) induces a bijection

\[ \text{Spec} \left( \mathbb{Z}_{\alpha} / I_{\alpha} \right) \to \text{Spec} \left( \mathbb{Z}[\alpha] / I_{\alpha} \right) . \]

(5) \( \mathbb{Z}[\alpha] \) is a GPVD.

Proof. (1) \( \Rightarrow \) (4). Assume (1). Then \( \mathbb{Z}[\alpha] \) is "seminormal in" \( \mathbb{Z}_{\alpha} \) in the sense of [17], and so [17, Lemma 1.3] yields that \( I_{\alpha} \) is a radical ideal of \( \mathbb{Z}_{\alpha} \). (Cf. also [10, Theorem 1.1].) Of course, \( I_{\alpha} \neq 0 \) since \( \mathbb{Z}_{\alpha} \) is a module-finite overring of \( \mathbb{Z}[\alpha] \). We may assume without loss of generality that \( I_{\alpha} \) is a proper ideal of both \( \mathbb{Z}[\alpha] \) and \( \mathbb{Z}_{\alpha} \). Next, we claim that the induced map

\[ \text{Spec} \left( \mathbb{Z}_{\alpha} / I_{\alpha} \right) \to \text{Spec} \left( \mathbb{Z}[\alpha] / I_{\alpha} \right) \]

is a bijection. For, since \( \mathbb{Z}[\alpha] \) and \( \mathbb{Z}_{\alpha} \) are each one-dimensional Noetherian domains, an associated prime of \( I_{\alpha} \) in \( \mathbb{Z}[\alpha] \) (resp., \( \mathbb{Z}_{\alpha} \)) is just a prime ideal of \( \mathbb{Z}[\alpha] \) (resp., \( \mathbb{Z}_{\alpha} \)) containing \( I_{\alpha} \). As the set of these primes is in canonical one-to-one correspondence with \( \text{Spec} \left( \mathbb{Z}[\alpha] / I_{\alpha} \right) \) (resp., \( \text{Spec} \left( \mathbb{Z}_{\alpha} / I_{\alpha} \right) \)), (4) follows.

(4) \( \Rightarrow \) (3). By the lying-over property for integral extensions (cf. [14, Theorem 44]), \( f \) is surjective in general. Given (4), one need only show that if \( P \in \text{Spec} \left( \mathbb{Z}[\alpha] \right) \) does not contain \( I_{\alpha} \), then at most one \( Q \in \text{Spec} \left( \mathbb{Z}_{\alpha} \right) \) can contract to \( P \). This in turn follows from [14, Exercise 41(b), page 46], for any such \( Q \) satisfies \( \left( \mathbb{Z}_{\alpha} / Q \right) = \left( \mathbb{Z}[\alpha] / P \right) \), whence \( Q = P \left( \mathbb{Z}[\alpha] / P \right) \cap \mathbb{Z}_{\alpha} \).

(3) \( \Rightarrow \) (5). Since \( \mathbb{Z}_{\alpha} \) is a (Dedekind, hence) Prüfer domain, it is a GPVD (cf. [4, p. 156]). Hence we may assume that \( \mathbb{Z}[\alpha] \neq \mathbb{Z}_{\alpha} \) and, in particular, that \( I_{\alpha} \) is a nonzero proper ideal. Since \( \mathbb{Z}[\alpha] \) and \( \mathbb{Z}_{\alpha} \) are each one-dimensional, (3) easily leads to condition (1) in [4, Theorem 3.1] (with \( I_{\alpha} \) playing the role of the common radical ideal \( A \)), yielding (5).

(5) \( \Rightarrow \) (1) and (2). Assume (5). Then, since \( \mathbb{Z}[\alpha] \) is Noetherian, [4, Proposition 3.6] yields that \( \mathbb{Z}_{\alpha} \) is the Prüfer domain associated to (the GPVD) \( \mathbb{Z}[\alpha] \). Then (cf. [4, p. 156]) \( f \) is a homeomorphism. As we have noted via one-dimensionality that the associated primes of \( I_{\alpha} \) are just the prime ideals containing \( I_{\alpha} \), the second assertion in (1) follows easily from the bijectivity of \( f \). Moreover, by [4, p. 156 and Remarks 2.4(a)], (the GPVD) \( \mathbb{Z}[\alpha] \) is an LPVD and, hence, seminormal. Then, as in the above proof that (1) \( \Rightarrow \) (4), we see that \( I_{\alpha} \) is a radical ideal of \( \mathbb{Z}_{\alpha} \).

Finally, since (2) \( \Rightarrow \) (3) trivially, the proof is complete.

As a first step in specializing to the quadratic case, \( \alpha = n \omega_d \), we shall characterize the condition "\( f \) is a bijection" that appeared above.

**Proposition 2.2.** Let \( d \) be a square-free integer and let \( n \geq 2 \) be an integer. Let \( f : \text{Spec} \left( \mathbb{Z}[\omega_d] \right) \to \text{Spec} \left( \mathbb{Z}[n \omega_d] \right) \) be the canonical contraction map. Then the following conditions are equivalent.

(1) \( f \) is a bijection.

(2) \( \mathbb{Z}[n \omega_d] \subset \mathbb{Z}[\omega_d] \) is an \( i \)-extension; i.e., \( f \) is an injection.

(3) \( f \) is a homeomorphism.
(4) If $p$ is a rational prime such that $p \mid n$, then $p$ is not split in $\mathbb{Z}[\omega_d]$.

(5) (a) If $p$ is an odd rational prime such that $p \mid n$ and $p \nmid d$, then $(d/p) = -1$; and

(b) if $d = 1 \pmod{8}$, then $n$ is odd.

Before proving Proposition 2.2, we collect some useful tools.

**Lemma 2.3.** Let $d$ and $n$ be as in Proposition 2.2.

(i) If $p$ is a rational prime such that $p \nmid n$, then $p\mathbb{Z}[\omega_d] \cap \mathbb{Z}[n\omega_d] = p\mathbb{Z}[n\omega_d]$.

(ii) $n\mathbb{Z}[\omega_d] \cap \mathbb{Z}[n\omega_d] = n\mathbb{Z}[\omega_d] = (\mathbb{Z}[n\omega_d]:\mathbb{Z}[\omega_d]) \subseteq n\mathbb{Z}[n\omega_d]$.

(iii) Let $P \in \text{Spec}(\mathbb{Z}[\omega_d])$ be nonzero, with $P \cap \mathbb{Z} = p\mathbb{Z}$. Then $P \supset n\mathbb{Z}[\omega_d]$, if, and only if, $p \mid n$.

(iv) For a rational prime $p$, the following three conditions are equivalent (and make no mention of $n$).

1. $\mathbb{Z}[p\omega_d] \subset \mathbb{Z}[\omega_d]$ is an i-extension.
2. $p$ is not split in $\mathbb{Z}[\omega_d]$.
3. (a) If $p$ is odd and $p \nmid d$, then $(d/p) = -1$; and
   (b) if $d = 1 \pmod{8}$, then $p$ is odd.

**Proof of Lemma 2.3.** (i) One inclusion is clear. Conversely, let $e \in p\mathbb{Z}[\omega_d] \cap \mathbb{Z}[n\omega_d]$. Then $e = p(a + b\omega_d) = a_1 + b_1 n\omega_d$ for suitable $a, b, a_1, b_1 \in \mathbb{Z}$. Then $pa_1 = a_1$, and $pb = b_1 n$. Since $p \nmid n$, the preceding equation yields $p \mid b_1$, say $b_1 = pb_2$, with $b_2 \in \mathbb{Z}$. Then $e = p(a + b_2 n\omega_d) \in p\mathbb{Z}[n\omega_d]$, as desired.

(ii) The second equation follows easily from the fact that $(\omega_d)^2 \in \mathbb{Z} + \mathbb{Z}\omega_d$.

The other assertions are evident.

(iii) Note that $n\mathbb{Z}[\omega_d] \cap \mathbb{Z} = n\mathbb{Z}$. Hence if $P \supset n\mathbb{Z}[\omega_d]$, then intersecting with $\mathbb{Z}$ yields $p\mathbb{Z} = n\mathbb{Z}$, whence $p \mid n$. Conversely, if $p \mid n$, then $n\mathbb{Z}[\omega_d] \subset (p\mathbb{Z})\mathbb{Z}[\omega_d] = p\mathbb{Z}[\omega_d] \subset P$, as desired.

(iv) Consider the function $g: \mathbb{Z}[p\omega_d] \rightarrow \mathbb{Z}/p\mathbb{Z}$ which sends $a + b\omega_d$ to $a + p\mathbb{Z}$ for all $a, b \in \mathbb{Z}$. Since $(\omega_d)^2 \in \mathbb{Z} + \mathbb{Z}\omega_d$, one readily shows that $g$ is a surjective ring-homomorphism, with ker $(g) = p\mathbb{Z}[\omega_d]$. In particular, $p\mathbb{Z}[\omega_d]$ is a prime of $\mathbb{Z}[p\omega_d]$. As (ii) established that $p\mathbb{Z}[\omega_d]$ is the conductor of $\mathbb{Z}[\omega_d]$ in $\mathbb{Z}[p\omega_d]$, one may infer from [14, Exercise 41(b), page 46], the one-dimensionality of these rings and the lying-over property that (1) holds, if, and only if, (at most) one prime ideal of $\mathbb{Z}[\omega_d]$ meets $\mathbb{Z}[p\omega_d]$ in $p\mathbb{Z}[\omega_d]$. By the incomparability property, $p\mathbb{Z}[\omega_d]$ is the only prime of $\mathbb{Z}[p\omega_d]$ that lies over $p\mathbb{Z}$. Thus, (1) holds, if, and only if, (at most) one prime of $\mathbb{Z}[\omega_d]$ lies over $p\mathbb{Z}$. In other words, (1) $\iff$ (2). Finally, (2) $\iff$ (3) by classical facts about $\mathbb{Z}[\omega_d]$ (cf. [19, Chapter 6]). This completes the proof of the lemma.

**Proof of Proposition 2.2.** By integrality, $f$ is surjective; hence, (1) $\iff$ (2). Also by integrality, $f$ is a closed (and continuous) map; hence, (1) $\iff$ (3).

Moreover, since $n$ factors as a nontrivial product of primes in $\mathbb{Z}$, Lemma 2.3(iv) [(2) $\iff$ (3)] easily leads to (4) $\iff$ (5).

Notice also, via Lemma 2.3(ii) and [14, Exercise 41(b), page 46], that $f$ induces a bijection between Spec $(\mathbb{Z}[\omega_d]) \setminus V(n\mathbb{Z}[\omega_d])$ and Spec $(\mathbb{Z}[n\omega_d]) \setminus V(n\mathbb{Z}[\omega_d])$. (As usual, if $I$ is an ideal of a ring $A$, then $V(I)$ denotes the set of prime ideals of $A$ which contain $I$.)
(2) $\Rightarrow$ (4). Assume (2). Then, given $p \mid n$, $\mathbb{Z}[p\omega_d]$ is contained between $\mathbb{Z}[n\omega_d]$ and $\mathbb{Z}[\omega_d]$; then, using (2), we see that $\mathbb{Z}[p\omega_d] \subset \mathbb{Z}[\omega_d]$ is an $i$-extension. Hence, Lemma 2.3(iv) [(1) $\Leftrightarrow$ (2)] yields (4), as desired.

(4) $\Rightarrow$ (2). Let $n = \prod p_j^{e_j}$ be the prime-power factorization of $n$ in $\mathbb{Z}$. Assume (4). Then, by Lemma 2.3(iv), $\mathbb{Z}[p\omega_d] \subset \mathbb{Z}[\omega_d]$ is an $i$-extension for each $j$. Suppose that (2) fails. Then there exist distinct $P_1, P_2 \in \text{Spec}(\mathbb{Z}[\omega_d])$ such that $P_1 \cap \mathbb{Z}[n\omega_d] = P_2 \cap \mathbb{Z}[n\omega_d] = \mathbb{Z}[\omega_d]$, say, $P$; and, by the second paragraph of this proof, $n\mathbb{Z}[\omega_d] \subset P$. Let $p$ be the rational prime such that $P \cap \mathbb{Z} = p\mathbb{Z}$. By Lemma 2.3(iii), $p = p_j$ for some $j$. Hence $P_1 \cap \mathbb{Z}[p\omega_d]$ and $P_2 \cap \mathbb{Z}[p\omega_d]$ are distinct primes of the one-dimensional ring $\mathbb{Z}[p\omega_d]$, each containing $p\mathbb{Z}[\omega_d]$. Since the proof of Lemma 2.3(iv) showed that $p\mathbb{Z}[\omega_d]$ is a (nonzero) prime of $\mathbb{Z}[p\omega_d]$, we have the desired contradiction, and the proof of Proposition 2.2 is complete.

Remark 2.4. (a) It is useful to record what was just proved. Given $d$ and $n = \prod p_j^{e_j}$ as in Proposition 2.2, then $\mathbb{Z}[n\omega_d] \subset \mathbb{Z}[\omega_d]$ is an $i$-extension, if, and only if, $\mathbb{Z}[p\omega_d] \subset \mathbb{Z}[\omega_d]$ is an $i$-extension for each $j$.

(b) Let $p$ be a rational prime and $d$ a square-free integer, and consider positive integers $h < k$. Given the above work, it seems interesting to note that $\mathbb{Z}[p^k\omega_d] \subset \mathbb{Z}[p^h\omega_d]$ is an $i$-extension. We shall now prove this.

To do so, first observe that $(\mathbb{Z}[p^k\omega_d]:\mathbb{Z}[p^h\omega_d]) = p^{k-h}\mathbb{Z}[p^h\omega_d]$. (Cf. the proof of Lemma 2.3(iii).) Call this ideal $I$. Then, by reasoning as in the proof of Proposition 2.2, it will suffice to show that $V(I)$ is a singleton subset of $\text{Spec}(\mathbb{Z}[p^h\omega_d])$. As we saw in the proof of Lemma 2.3(iv), $p\mathbb{Z}[\omega_d]$ is a prime of $\mathbb{Z}[p\omega_d]$; hence, $P = p\mathbb{Z}[\omega_d] \cap \mathbb{Z}[p^h\omega_d]$ is a prime of $\mathbb{Z}[p^h\omega_d]$. As this ring is one-dimensional, it now suffices to show that $P$ is the radical of $I$ (for $\{P\}$ is then the required singleton set). One inclusion is easy since each element of $p\mathbb{Z}[\omega_d]$ has a suitable power in $I$. Conversely, let $\xi \in \text{rad}(I)$. Then $\xi = a + bp^h\omega_d$ for suitable integers $a$ and $b$, and there exists an integer $N \geqslant 1$ such that

$$(a + bp^h\omega_d)^N = \xi^N \in I = p^{k-h}\mathbb{Z} + p^k\mathbb{Z}\omega_d.$$ 

Since $\omega_d^N \in \mathbb{Z} + p\mathbb{Z}\omega_d$, the left-hand side is in $a^N + p\mathbb{Z} + p\mathbb{Z}\omega_d$. Thus $a^N \in p^{k-h}\mathbb{Z} + p\mathbb{Z}$, whence $p \mid a$ and $\xi \in P$. This completes the proof of the remark.

We are now able to interpret the conditions in Proposition 2.1 for an arbitrary quadratic order.

**Theorem 2.5.** Let $d$ be a square-free integer and let $n \geqslant 2$ be an integer. Then the following four conditions are equivalent.

(1) $\mathbb{Z}[n\omega_d]$ is a GPVD.

(2) $\mathbb{Z}[n\omega_d] \subset \mathbb{Z}[\omega_d]$ is an $i$-extension and $n\mathbb{Z}[\omega_d]$ is a radical ideal of $\mathbb{Z}[\omega_d]$.

(3) $n$ is square-free and, for each rational prime $p$ such that $p \mid n$, $p$ is inert in $\mathbb{Z}[\omega_d]$.
(4) \( n \) is square-free. In addition, if \( n \) is even, then \( d \equiv 5 \pmod{8} \). If \( p \) is an odd rational prime such that \( p \mid n \), then \( (p \nmid d \text{ and}) \)
\[ \left(\frac{d}{p}\right) = -1. \]

Moreover, if the above conditions hold, then \( \mathbb{Z}[\omega_d] \) is the Prüfer domain canonically associated to the GPVD, \( \mathbb{Z}[n\omega_d] \).

Proof. \((1) \Rightarrow (2)\). In view of Lemma 2.3(ii) and integrality, this equivalence is the special case \( \alpha = n\omega_d \) of Proposition 2.1 \((5) \Leftrightarrow (3)\).

\((2) \Rightarrow (3)\). Assume (2). If \( n \) were not square-free, \( q^2 \mid n \) for some rational prime \( q \), and it would follow that \( q \in \text{rad} \left( n\mathbb{Z}[\omega_d] \right) = n\mathbb{Z}\omega_d \); then \( q \in q^2\mathbb{Z} \), a contradiction. Hence, \( n \) is square-free. Next, let \( p \) be a rational prime dividing \( n \). By Lemma 2.3(iv) and Remark 2.4(a), \( p \) is not split in \( \mathbb{Z}[\omega_d] \). If \( p \) is not inert, then \( p \) ramifies: \( p\mathbb{Z}[\omega_d] = P^2 \), with \( P \in \text{Spec} (\mathbb{Z}[\omega_d]) \). Then \( n\mathbb{Z}[\omega_d] = (np^{-1})P^2 \), which has a unique factorization as a product of prime ideals in the Dedekind domain \( \mathbb{Z}[\omega_d] \), cannot be a radical ideal, a contradiction. Hence, \( p \) is inert in \( \mathbb{Z}[\omega_d] \).

\((3) \Leftrightarrow (4)\). This follows from classical quadratic theory, as in [19, Chapter 6].

The final assertion follows from the Noetherianness of \( \mathbb{Z}[n\omega_d] \) (cf. [4, Proposition 3.6]). The proof is complete.

Remark 2.6. Let \( d \) be a square-free integer, \( d \equiv 1 \pmod{4} \). By Theorem 2.5, \( \mathbb{Z}[\sqrt{d}](=\mathbb{Z}[2\omega_d]) \) is a GPVD, if, and only if, \( d \equiv 5 \pmod{8} \). Thus Theorem 2.5 recovers the motivating result, [5, Example 4].

§3. When the seminormalization is the ring of integers. A sufficient condition for the property studied in Proposition 2.1 is that \( \mathbb{Z}[\alpha] = \mathbb{Z}_\alpha \). This condition has been of recurring interest (cf. [15, 18, 1, 13, 12]). We next give a fresh characterization of this condition in terms of seminormalization and other concepts which figured in Section 2.

Proposition 3.1. For an algebraic integer \( \alpha \), the following conditions are equivalent.

1. \( \mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha \) and \( I_\alpha \) is a radical ideal of \( \mathbb{Z}_\alpha \).
2. \( \mathbb{Z}[\alpha] = \mathbb{Z}_\alpha \).

Proof. \((2) \Rightarrow (1)\) trivially. \((1) \Rightarrow (2)\) directly via a result of Traverso [17, Corollary 1.8] but, for the sake of completeness, we offer the following alternate proof. It will be convenient to write \( R = \mathbb{Z}[\alpha] \) and \( T = \mathbb{Z}_\alpha \). Assume (1). Without loss of generality, \( R \neq T \), and so \( I_\alpha \) is a (nonzero) proper ideal. For
each prime ideal \( P \) of \( R \) containing \( I \), the seminormalization hypothesis gives a unique \( Q \in \text{Spec} \langle T \rangle \) contracting to \( P \), and the canonical map \( R/\overline{P} \to T/\overline{Q} \) is an isomorphism. One then has a commutative diagram

\[
\begin{array}{ccc}
R/\overline{P} & \longrightarrow & \Pi R/P \\
\downarrow & & \downarrow \\
T/\overline{Q} & \longrightarrow & \Pi T/Q
\end{array}
\]

in which the horizontal maps are isomorphisms given by the Chinese Remainder Theorem; and the right-vertical map is (an isomorphism) given coordinate-wise by the above isomorphisms \( R/\overline{P} \to T/\overline{Q} \). Then the left-vertical map is also an isomorphism. Hence \( T = R + \overline{Q} = R + \text{rad}_T \langle I \rangle = R + I = R \), completing the proof.

**Remark 3.2.** (a) As noted by Ooishi [16, Example 1], \( \mathbb{Z}[\sqrt{-4}]^+ = \mathbb{Z}[i] \). (Another proof of this would follow from Theorem 3.4 below.) Thus, by taking \( \alpha = \sqrt{-4} = 2\sqrt{-1} \), we see that the "radical" hypothesis on \( I \) cannot be deleted from condition (1) of Proposition 3.1.

(b) Of course, the "\( \mathbb{Z}[\alpha] = \mathbb{Z}_\alpha \)" condition also cannot be deleted. To illustrate this, consider \( \alpha = \sqrt{5} \). Then (cf. [5, Example 4] and Proposition 2.1) \( I \) is radical, although \( \mathbb{Z}[\alpha] = \mathbb{Z}[\alpha] \neq \mathbb{Z}_\alpha \). The (not necessarily GPVD) seminormal quadratic orders are characterized in Theorem 4.1 below.

(c) If \( \mathbb{Z}[\alpha] = \mathbb{Z}_\alpha \), then \( \mathbb{Z}[\alpha] \) is a (Dedekind domain, hence a) GPVD. Another way to see this is to relate condition (1) of Proposition 3.1 and condition (2) of Proposition 2.1: in this case, the homeomorphic nature of \( f \) is explained naturally via seminormalization.

In view of Proposition 3.1, we focus next on characterizing the condition, "\( \mathbb{Z}[\alpha] = \mathbb{Z}_\alpha \)." In fact, we shall relate this condition to many of the universal properties in [11, p. 240], [2, 8, 6, and 7]. (See these references as needed for background information. In particular, \((-)^*\) denotes weak normalization in the sense of [2].)

**Proposition 3.3.** Let \( \alpha \) be an algebraic integer, \( i: \mathbb{Z}[\alpha] \to \mathbb{Z}_\alpha \) the inclusion (map), and \( f: \text{Spec}(\mathbb{Z}_\alpha) \to \text{Spec}(\mathbb{Z}[\alpha]) \) the induced contraction map. Then the following conditions are equivalent.

1. \( i \) is universally going-down.
2. \( i \) is UGD.
3. \( i \) is radiciel.
4. \( i \) is universally mated.
5. \( f \) is universally open.
6. \( f \) is a universal homeomorphism.
7. \( \mathbb{Z}[\alpha]^* = \mathbb{Z}_\alpha \).
8. \( \mathbb{Z}[\alpha]^+ = \mathbb{Z}_\alpha \).

**Proof.** (8) \( \Leftrightarrow \) (3). (3) holds, if, and only if, (the surjective map) \( f \) is an injection and the extensions of residue class fields induced by \( f \) are all (algebraic) purely inseparable. As the residue class fields of \( R \) are all perfect,
(3) is thus equivalent to requiring that \( f \) is a bijection and each of the extensions of residue class fields induced by \( f \) is an isomorphism. In view of the characterization of seminormalization in [17], the assertion follows.

(3) \( \iff \) (4). By [6, Theorems 2.1 and 2.5], (3) holds, if, and only if, \( f_i : \text{Spec} (\mathbb{Z}_a[X]) \to \text{Spec} (\mathbb{Z}[\alpha][X]) \) is an injection; and (4) holds, if, and only if, \( \mathbb{Z}[\alpha][X] \to \mathbb{Z}_a[X] \) is mated. However, each of these conditions is equivalent to \( f_i \) being a bijection (and so the assertion follows). The point is that \( f_i \) is surjective since \( i \) is (universally) integral.

(4) \( \Rightarrow \) (2). One-dimensionality assures that \( i \) satisfies going-down. Accordingly, [6, Proposition 3.14] yields the assertion.

(2) \( \Rightarrow \) (7). [6, Remark 3.6] yields this assertion.

(7) \( \Rightarrow \) (6). By [2, Theorema 1], \( \text{Spec} (\mathbb{Z}[\alpha]^* \to \text{Spec} (\mathbb{Z}[\alpha]) \) is a universal homeomorphism. The assertion follows.

(6) \( \Rightarrow \) (5). Trivial.

(5) \( \Rightarrow \) (1). It suffices to recall that "open" implies "going-down" [11]. ( Cf. also [8].)

(1) \( \Rightarrow \) (2). Apply [6, Corollary 3.20].

(2) \( \Rightarrow \) (4). Apply [6, Corollary 3.12(b)].

The proof is complete.

We next use some of the material in Section 2 to interpret the condition "\( \mathbb{Z}[\alpha]^* = \mathbb{Z}_a \)" for a typical quadratic order, with \( \alpha = n \omega_d \).

**Theorem 3.4.** Let \( d \) be a square-free integer and let \( n \geq 2 \) be an integer. Then the following conditions are equivalent.

1. \( \mathbb{Z}[n \omega_d]^* = \mathbb{Z}[\omega_d] \).
2. Each rational prime \( p \) such that \( p | n \) is ramified in \( \mathbb{Z}[\omega_d] \).
3. If \( d \equiv 1 \pmod{4} \), then \( n \) is odd. In addition, \( d \) is divisible by each odd prime divisor of \( n \).

**Proof.** By [17], (1) holds, if, and only if, both the following conditions hold: \( \mathbb{Z}[n \omega_d] \subset \mathbb{Z}[\omega_d] \) is an \( \mathbb{z} \)-extension, and \( k(P \cap \mathbb{Z}[n \omega_d]) \cong k(P) \) for each \( P \in \text{Spec} (\mathbb{Z}[\omega_d]) \). As in the proof of Proposition 2.2, these conditions need only be checked in case \( P \) contains the conductor, \( n \mathbb{Z}[\omega_d] \); that is, by Lemma 2.3(iii), in case \( P \cap \mathbb{Z} = p \mathbb{Z} \) with \( p | n \). Set \( P_1 = P \cap \mathbb{Z}[p \omega_d] \) and \( P_2 = P \cap \mathbb{Z}[n \omega_d] \). By incomparability, \( P_1 = p \mathbb{Z}[\omega_d] \) and \( P_2 = p \mathbb{Z}[\omega_d] \cap \mathbb{Z}[n \omega_d] \). Consider the field extensions

\[ \mathbb{Z}/p \mathbb{Z} \hookrightarrow k(P_2) \hookrightarrow k(P_1) \hookrightarrow k(P). \]

As noted in the proof of Lemma 2.3(iv), \( \mathbb{Z}/p \mathbb{Z} \cong k(P_i) \). Thus \( \mathbb{Z}/p \mathbb{Z} \cong k(P_2) \). Hence, using quadratic ramification theory (concerning \( \sum e_i f_i \)), we have the following assertions. If \( p \) is ramified in \( \mathbb{Z}[\omega_d] \), then \( k(P_2) \cong k(P) \); if \( p \) is inert in \( \mathbb{Z}[\omega_d] \), then \( k(P_2) \hookrightarrow k(P) \) is two-dimensional. By combining Proposition 2.2 [(2) \( \iff \) (4)] with the above consequence of [17], we can now conclude that (1) \( \iff \) (2). Finally, (2) \( \iff \) (3) by classical quadratic theory [19, Chapter 6]. The proof is complete.

**Remark 3.5.** (a) The conditions in Theorems 2.5 and 3.4 cannot hold simultaneously: ramified primes are not inert! This is to be expected since
each GPVD is (equal to its own) seminormal (ization), while \( n \equiv 2 \) forces \( \mathbb{Z}[n\omega_d] \neq \mathbb{Z}[\omega_d] \).

(b) Let \( d \) be a square-free integer. Then either \( d = 2, 3 \pmod{4} \) or \( d = 1 \pmod{4} \). We could use condition (3) in Theorem 3.4 to develop examples showing that this congruence information alone does not determine whether \( \mathbb{Z}[3\omega_d]^+ \) and \( \mathbb{Z}[\omega_d] \) coincide. However, it is enough to observe via this condition that \( \mathbb{Z}[3\omega_d]^+ = \mathbb{Z}[\omega_d] \), if, and only if, \( 3 \mid d \).

(c) The case \( n = 2 \) deserves separate treatment. Let \( d \) be a square-free integer. If \( d = 2, 3 \pmod{4} \), then \( \mathbb{Z}[2\omega_d] = \mathbb{Z}[2\sqrt{d}] \) is not seminormal, since \( \mathbb{Z}[2\omega_d]^+ = \mathbb{Z}[\omega_d] = \mathbb{Z}[^{\sqrt{d}}] \) in this case. However, if \( d = 1 \pmod{4} \), then we see as above that \( \mathbb{Z}[2\omega_d]^+ \neq \mathbb{Z}[\omega_d] \); since \( \mathbb{Z}[2\omega_d] \subset \mathbb{Z}[2\omega_d]^+ \subset \mathbb{Z}[\omega_d] \), we have \( \mathbb{Z}[2\omega_d]^+ = \mathbb{Z}[2\omega_d] \) in this case. In other words, if \( d = 1 \pmod{4} \), then \( \mathbb{Z}[2\omega_d] = \mathbb{Z}[\sqrt{d}] \) is seminormal. Thus, by Theorem 2.5, \( \mathbb{Z}[2\omega_1] = \mathbb{Z}[\sqrt{7}] \) is an example of a seminormal quadratic order which is not a GPVD; for a “complex” example, consider \( \mathbb{Z}[\sqrt{-7}] \).

By extending this sort of reasoning, we shall determine all seminormal quadratic orders in section 4. More generally, we shall identify the seminormalization of each quadratic order.

§4. The seminormal quadratic orders. The rings mentioned in this section's title will be characterized in Corollary 4.5, as a consequence of this section's main result, Theorem 4.4. The latter result computes the seminormalization of an arbitrary quadratic order \( \mathbb{Z}[m\omega_d] \); that is, computes the positive integer \( m \) such that \( \mathbb{Z}[n\omega_d]^+ = \mathbb{Z}[m\omega_d] \). To prepare the way, we next generalize some of the earlier sections' material concerning the inclusion \( \mathbb{Z}[n\omega_d] \subset \mathbb{Z}[\omega_d] \) to the context \( \mathbb{Z}[n\omega_d] \subset \mathbb{Z}[m\omega_d] \).

**Lemma 4.1.** Let \( d \) be a square-free integer and let \( m, n \) be positive integers.

(i) If \( m \mid n \), then

\[
(n/m)\mathbb{Z}[m\omega_d] \cap \mathbb{Z}[n\omega_d] = (n/m)\mathbb{Z}[m\omega_d] = (\mathbb{Z}[n\omega_d] : \mathbb{Z}[m\omega_d]).
\]

(ii) If \( p \) is a rational prime, then \( p\mathbb{Z}[m\omega_d] \) is a prime ideal of \( \mathbb{Z}[pm\omega_d] \).

**Proof.** (i) As in the proof of Lemma 2.3(ii), this follows easily from the fact that \( \{1, k\omega_d\} \) is a \( \mathbb{Z} \)-basis of \( \mathbb{Z}[k\omega_d] \), for each integer \( k \geq 1 \).

(ii) Consider the function \( g : \mathbb{Z}[pm\omega_d] \to \mathbb{Z}/p\mathbb{Z} \) which sends \( a + bpm\omega_d \) to \( a + p\mathbb{Z} \) for all \( a, b \in \mathbb{Z} \). As in the proof of Lemma 2.3(iv), \( g \) is a surjective ring-homomorphism, with \( \ker (g) = p\mathbb{Z}[m\omega_d] \), and the assertion is immediate.

**Lemma 4.2.** Let \( d, m, n \) be as in Lemma 4.1, with \( m \mid n \). Then the following three conditions are equivalent.

(1) \( \mathbb{Z}[n\omega_d] \subset \mathbb{Z}[m\omega_d] \) is an i-extension.

(2) If \( p \) is a rational prime such that \( p \mid (n/m) \) and \( p \nmid m \), then \( p \) is not split in \( \mathbb{Z}[\omega_d] \).

(3) Let \( n = p_1^{s_1} \cdots p_r^{s_r} \) and \( m = p_1^{s_1} \cdots p_r^{s_r} \) be the prime-power decompositions of \( n \) and \( m \) (with \( s \leq r \) and \( 1 \leq g_i \leq e_i \) for \( i \leq s \)). Let \( p = p_j \) for some \( s + 1 \leq j \leq r \).
If $d = 1 \pmod{8}$, then $p$ is odd. Moreover, if $p$ is odd and $p \not| d$, then

\[ \left( \frac{d}{p} \right) = -1. \]

Proof. By Proposition 2.2, we may assume $m \neq 1$.

(1) $\Rightarrow$ (2). Deny this. Then there exists a rational prime $p$ such that $p | (n/m)$, $p \not| m$, and $p\mathbb{Z}[\omega_d] = P_1 P_2$, where $P_1$ and $P_2$ are distinct prime ideals of $\mathbb{Z}[\omega_d]$. Put $Q_i = P_i \cap \mathbb{Z}[\omega_d]$. As $P_i \cap \mathbb{Z} = p\mathbb{Z}$, so also $Q_i \cap \mathbb{Z} = p\mathbb{Z}$. If $Q_i$ contains $(\mathbb{Z}[\omega_d]:\mathbb{Z}[\omega_d]) = m\mathbb{Z}[\omega_d]$, then intersecting with $\mathbb{Z}$ leads to $p\mathbb{Z} \supset m\mathbb{Z}[\omega_d] \cap \mathbb{Z}$, contradicting $p \not| m$. Thus $Q_i$ does not contain the conductor, and so (cf. [14, Exercise 41(b), p. 46]) the fact that $P_1 \neq P_2$ assures that $Q_1 \neq Q_2$. By (1) and the condition $p | (n/m)$, $Q_1 \cap \mathbb{Z}[pm\omega_d] \neq Q_2 \cap \mathbb{Z}[pm\omega_d]$. However, we also have equality (and thus the desired contradiction): $p\mathbb{Z}[pm\omega_d] \subset Q_i \cap \mathbb{Z}[pm\omega_d]$ are primes of $\mathbb{Z}[pm\omega_d]$ each lying over $p\mathbb{Z}$, whence equality follows via incomparability.

(2) $\Rightarrow$ (1). Deny this. Then there exist distinct $Q_1$, $Q_2$ in $\text{Spec} (\mathbb{Z}[m\omega_d])$ such that $Q_1 \cap \mathbb{Z}[m\omega_d] = Q_2 \cap \mathbb{Z}[m\omega_d]$, say, $P$. Let $p$ be the rational prime such that $P \cap \mathbb{Z} = p\mathbb{Z}$. As $P$ must contain $(\mathbb{Z}[m\omega_d]:\mathbb{Z}[m\omega_d])$, Lemma 4.1(i) readily yields $p | (n/m)$. Next, choose (distinct) $P_1, P_2 \in \text{Spec} (\mathbb{Z}[\omega_d])$ such that $P_1 \cap \mathbb{Z}[m\omega_d] = Q_1$. One can now see that $p \not| m$. Indeed, if $p | m$, then incomparability would force the inclusion $p\mathbb{Z}[\omega_d] \subset P_i \cap \mathbb{Z}[m\omega_d]$ to be an equality, so that intersecting with $\mathbb{Z}[m\omega_d]$ would lead to $Q_i = Q_j$, an absurdity. By (2), only one prime ideal of $\mathbb{Z}[\omega_d]$ lies over $p\mathbb{Z}$. Hence $P_1 = P_2$, the desired contradiction.

(2) $\Rightarrow$ (3). Notice that \( \{ p_i : s+1 \leq i \leq r \} \) is the set of all rational primes $p$ such that $p | (n/m)$ and $p \not| m$. Accordingly, (2) $\Leftrightarrow$ (3) follows from classical facts about $\mathbb{Z}[\omega_d]$ (cf. [19, Ch. 6]). The proof of Lemma 4.2 is complete.

It should be noted that, aside from some trivial set-theoretic and topological observations, setting $m = 1$ in Lemma 4.2 recovers Proposition 2.2.

Lemma 4.3. Let $d$, $m$, $n$ be as in Lemma 4.1, with $m | n$, and suppose that $\mathbb{Z}[n\omega_d] \subset \mathbb{Z}[m\omega_d]$ is an $i$-extension.

(i) Let $P \in \text{Spec}(\mathbb{Z}[n\omega_d])$ be nonzero, let $p$ be the rational prime such that $P \cap \mathbb{Z} = p\mathbb{Z}$, and let $Q \in \text{Spec}(\mathbb{Z}[\omega_d])$ such that $Q \cap \mathbb{Z}[m\omega_d] = P$. Suppose that $p | (n/m)$. If $p | m$, then $k(P \cap \mathbb{Z}[n\omega_d]) \sim k(P) \equiv \mathbb{Z}/p\mathbb{Z}$. If $p \not| m$, then the following four conditions are equivalent.

1. $k(P \cap \mathbb{Z}[n\omega_d]) \sim k(P)$
2. $[k(Q):\mathbb{Z}/p\mathbb{Z}] = 1$
3. $p$ is ramified in $\mathbb{Z}[\omega_d]$.
4. If $d = 1 \pmod{4}$, then $p$ is odd. In addition, if $p$ is odd, then $p | d$.

(ii) Let $n = p_1^{e_1} \ldots p_s^{e_s}$ and $m = p_1^{g_1} \ldots p_s^{g_s}$ be the prime-power decompositions of $n$ and $m$ (with $s \leq r$ and $1 \leq g_i \leq e_i$ for $i \leq s$). Then the following four conditions are equivalent (with (4) vacuously satisfied if $s = r$).

1. $\mathbb{Z}[m\omega_d]$ is the seminormalization of $\mathbb{Z}[n\omega_d]$ in $\mathbb{Z}[m\omega_d]$.
2. $k(P \cap \mathbb{Z}[n\omega_d]) \sim k(P)$ for each $P \in \text{Spec}(\mathbb{Z}[m\omega_d])$.
3. If $p$ is a rational prime such that $p | (n/m)$ and $p \not| m$, then $p$ is ramified in $\mathbb{Z}[\omega_d]$. 


(4) Let \( p = p_i \) for some \( s + 1 \leq i \leq r \). If \( d = 1 \pmod{4} \), then \( p \) is odd. In addition, if \( p \) is odd, then \( p \mid d \).

Proof. (i) It is well known that \((3) \iff (4)\) (cf. [19, Ch. 6]). Next, note that \( p\mathbb{Z}[\omega_d] \subset Q \cap \mathbb{Z}[\omega_d] \) are prime ideals of \( \mathbb{Z}[\omega_d] \) (cf. Lemma 4.1(ii)), each of which lies over \( p\mathbb{Z} \). Thus, by incomparability, \( p\mathbb{Z}[\omega_d] = Q \cap \mathbb{Z}[\omega_d] \); moreover, \( \mathbb{Z}/p\mathbb{Z} \rightarrow k(p\mathbb{Z}[\omega_d]) \) by the proof of Lemma 2.3(iv).

Suppose \( p \mid m \). Then we have the tower of fields

\[
\mathbb{Z}/p\mathbb{Z} \rightarrow k(P \cap \mathbb{Z}[n\omega_d]) \rightarrow k(P) \rightarrow k(p\mathbb{Z}[\omega_d]).
\]

By the above remarks, \( \mathbb{Z}/p\mathbb{Z} \rightarrow k(P) \), and so the first assertion holds.

Suppose \( p \not\mid m \). Then, by Lemma 4.2 \((1) \implies (2)\), only one prime of \( \mathbb{Z}[\omega_d] \) (namely, \( Q \)) lies over \( p\mathbb{Z} \). By the fundamental equation of ramification theory, \((2) \iff (3)\). Next, notice that \( k(P) \rightarrow k(Q) \) since the condition \( p \not\mid m \) assures that \( P \) does not contain \( m\mathbb{Z}[\omega_d] = (\mathbb{Z}[m\omega_d]:\mathbb{Z}[\omega_d]) \). In view of the tower of fields

\[
\mathbb{Z}/p\mathbb{Z} \rightarrow k(P \cap \mathbb{Z}[n\omega_d]) \rightarrow k(Q \cap \mathbb{Z}[(n/m)\omega_d]) \rightarrow k(Q \cap \mathbb{Z}[p\omega_d])
\]

and the above remarks, \((2) \iff (1)\).

(ii) Since \( \mathbb{Z}[n\omega_d] \subset \mathbb{Z}[m\omega_d] \) is assumed to be an \( i \)-extension, the characterisation of seminormalization in [17] immediately yields \((1) \iff (2)\). It is easy to see that the remaining equivalences follows from (i). (For some of these, one is given \( p \), and then uses lying-over to arrange a \( P \) to which (i) applies.) The proof is complete.

We next present the main result of this section.

Theorem 4.4. Let \( d \) be a square-free integer and let \( m \leq n \) be positive integers. Then the following four conditions are equivalent.

1. \( \mathbb{Z}[n\omega_d]^+ = \mathbb{Z}[m\omega_d] \).
2. \( m \) is minimal among positive integers with respect to these three properties:
   \( m \mid n, \mathbb{Z}[n\omega_d] \subset \mathbb{Z}[m\omega_d] \) is an \( i \)-extension, and \( k(P \cap \mathbb{Z}[n\omega_d]) \rightarrow k(P) \) for each \( P \in \text{Spec} (\mathbb{Z}[m\omega_d]) \).
3. \( m = \{ p : \text{p is a rational prime, } p \mid n, \text{ and } p \not\mid d \text{ if } p \text{ is odd, and } d = 1 \pmod{4} \text{ if } p = 2 \} \).
4. \( m = \{ p : \text{p is a rational prime, } p \mid n, p \not\mid d \text{ if } p \text{ is odd, and } d = 1 \pmod{4} \text{ if } p = 2 \} \).

Proof. (1) \( \iff (2) \). Apply the characterization of semi-normalization in [17].

(2) \( \iff (3) \). If \( m \mid n, p \) is a rational prime such that \( p \not\mid (n/m) \), and \( P \in \text{Spec} (\mathbb{Z}[m\omega_d]) \) satisfies \( P \cap \mathbb{Z} = p\mathbb{Z} \), then \( k(P \cap \mathbb{Z}[n\omega_d]) \rightarrow k(P) \). (The point is that \( P \) does not contain \( (\mathbb{Z}[n\omega_d]:\mathbb{Z}[m\omega_d]) = (n/m)\mathbb{Z}[m\omega_d] \). Hence, by combining Lemma 4.2 with Lemma 4.3(i) (or by applying Lemma 4.3(ii)), we see that (2) is equivalent to \( m \) being minimal among divisors of \( n \) such that: whenever \( p \) is a rational prime such that \( p \mid (n/m) \) and \( p \not\mid m \), then \( p \) is ramified in \( \mathbb{Z}[\omega_d] \). Using a prime-power decomposition of \( n \), one readily shows that this latter condition is equivalent to (3).
\( (3) \Leftrightarrow (4) \). Apply the classical facts about ramification of rational primes in quadratic number fields (cf. [19, Chapter 6]). The proof is complete.

**Corollary 4.5.** Let \( d \) be a square-free integer and \( n \geq 2 \) an integer. Then the following three conditions are equivalent.

1. \( \mathbb{Z}[\omega_d] \) is seminormal, that is, \( \mathbb{Z}[\omega_d]^+ = \mathbb{Z}[\omega_d] \).
2. \( n \) is square-free and no rational prime factor of \( n \) is ramified in \( \mathbb{Z}[\omega_d] \).
3. \( n \) is square-free. If \( n \) is even, then \( d = 1 \pmod{4} \). The greatest common divisor of \( d \) and \( n \) is (either 1 or) an integral power of 2.

**Proof.** Interpret \( m = n \) for conditions (3) and (4) in the statement of Theorem 4.4.

**Remark 4.6** (a) It is conventional to interpret a product of integers indexed by the empty set to be 1. Thus, taking \( m = 1 \), we see that Theorem 4.4 subsumes Theorem 3.4. Note that the above convention also renders Theorem 4.4 valid in case \( n = 1 \) (= \( m \)), since \( \mathbb{Z}[\omega_d] \) is (semi)normal.

(b) The examples in Remark 3.5(c) are illuminated by the following result. Let \( d \) be a square-free integer and \( n \geq 2 \) an integer. Then \( \mathbb{Z}[\omega_d] \) is a GPVD, if, and only if, \( \mathbb{Z}[\omega_d] \) is seminormal such that \( \mathbb{Z}[\omega_d] \subset \mathbb{Z}[\omega_d] \) is an \( i \)-extension. The easiest proof of this result is via the elementary number-theoretic criteria in Theorem 2.5(4), Corollary 4.5(3), and Proposition 2.2(5). Since each GPVD is seminormal, another proof follows from Proposition 2.1 \( (5) \Leftrightarrow (3) \) and [17, Lemma 1.3].

(c) Corollary 4.5 recovers all the facts implicit in Remark 3.5(c); for instance, \( \mathbb{Z}[\sqrt{d}] \) is seminormal, for each square-free integer \( d \). A far-reaching generalization of this, originally discovered by Ooishi, is given in Corollary 4.7 below.

(d) We have seen that if \( d \) is a square-free integer, then \( A = \mathbb{Z}[\sqrt{d}] \) is seminormal. This is due to a variety of deep reasons. If \( d = 2, 3 \pmod{4} \), \( A \) is actually normal. If \( d = 5 \pmod{8} \), then \( A \) is a GPVD [5, Example 4], note, however, in this case that \( A \) is not root-closed [3, Proposition]. Finally, if \( d = 1 \pmod{8} \), the above references show that \( A \) is root-closed, but not a GPVD. Thus, \( A \) is both root-closed and a GPVD, if, and only if, \( d = 2, 3 \pmod{4} \); that is, if, and only if, \( A \) is the maximal order of \( \mathbb{Q}(\sqrt{d}) \).

More generally, if \( n \) is any positive integer and \( d \) is as above, then \( B = \mathbb{Z}[\omega_d] \) is both root-closed and a GPVD, if, and only if, \( n = 1 \). This is a consequence of the following result. Let \( R \) be an LPVD (for instance, a GPVD) whose quotient field \( K \) is an algebraic number field. Suppose that \( R \) is contained in the ring of integers \( D \) of \( K \). Then \( R \) is integrally closed (that is, \( R = D \)) if (and only if) \( R \) is root-closed.

For a proof, note first, by the Krull–Akizuki theorem, that \( R \) is a one-dimensional Noetherian integral domain. Accordingly, by localizing and applying a result of Angermüller [3, Theorem 1], we have the desired assertion, unless \( D \) has some residue field \( D/N \cong \mathbb{Z}/2\mathbb{Z} \). In this remaining case, one need only show that \( M = N \cap R \) is such that (the PVD) \( R_M \) is integrally closed. This, in turn, follows from the \( (L)PVD \) condition, as the isomorphism \( R/M \to D/N \cong \mathbb{Z}/2\mathbb{Z} \) leads to \( R_M \cong D_{N/(D/M)} R/M \cong D_N \); an integrally closed (DVR) integral domain.
The "Noetherian" hypothesis is essential above, for one may construct a one-dimensional root-closed PVD which is not integrally closed.

(e) Theorem 4.4(4) permits easy calculation of seminormalizations of quadratic orders, significantly extending Remark 3.5(b). We next list several additional applications.

\[ \mathbb{Z}[3\sqrt{2}]^* = \mathbb{Z}[3\omega_2]^* = \mathbb{Z}[3\omega_2] = \mathbb{Z}[3\sqrt{2}], \]
\[ \mathbb{Z}[3\sqrt{3}]^* = \mathbb{Z}[3\omega_3]^* = \mathbb{Z}[1\omega_3] = \mathbb{Z}[\sqrt{3}], \]
\[ \mathbb{Z}[4\sqrt{2}]^* = \mathbb{Z}[2\sqrt{2}]^* = \mathbb{Z}[\sqrt{2}], \]
\[ \mathbb{Z}[4\sqrt{3}]^* = \mathbb{Z}[2\sqrt{3}]^* = \mathbb{Z}[\sqrt{3}], \]
\[ \mathbb{Z}[4\omega_3]^* = \mathbb{Z}[2\omega_3] = \mathbb{Z}[\sqrt{5}] \neq \mathbb{Z}[\omega_3], \]
\[ \mathbb{Z}[4\sqrt{6}]^* = \mathbb{Z}[2\sqrt{6}]^* = \mathbb{Z}[\sqrt{6}], \]
\[ \mathbb{Z}[18i]^* = \mathbb{Z}[6i]^* = \mathbb{Z}[3\omega_{-1}] = \mathbb{Z}[3i]. \]

In [16, Example 1, page 7], Ooishi characterized the non-square integers \( N \) such that \( \mathbb{Z}[^{\sqrt{N}}] \) is seminormal. We next recover this, as our final result.

**Corollary 4.7.** Let \( N \) be a nonsquare integer. Write \( N = n^2d \), with prime-power decompositions \( n = 2^{e_0}p_1^{e_1} \cdots p_r^{e_r} \) and \( d = \pm 2^{g_0}p_{+1}p_{+2} \cdots p_s \). (Here, \( \{p_1, \ldots, p_r\} \) and \( \{p_{+1}, \ldots, p_s\} \) are each sets of pairwise distinct odd primes, \( f_0 \geq 0, f_i \geq 1 \) for all \( 1 \leq i \leq s \), and \( g_0 \leq 1 \). If \( s = r, d = \pm 2^{g_0} \).) Then \( \mathbb{Z}[^{\sqrt{N}}] \) is seminormal, if, and only if, \( N = \pm 2^{h_0}p_1^{h_1} \cdots p_{+1}^{h_{+1}}p_{+2}^{h_{+2}} \cdots p_s^{h_s} \), with \( h_0 \leq 1 \) and \( p_i \neq p_j \) whenever \( 1 \leq i \leq s \) and \( s + 1 \leq j \leq r \).

**Proof.** As \( N \) is not a perfect square, \( d \neq 1 \). Thus, \( d \) is square-free. By Remark 4.6(c) and the convention regarding products indexed by the empty set, the assertion is verified if \( n = 1 \). Assume henceforth that \( n \neq 1 \). There are two cases.

Suppose \( d = 2, 3 \mod 4 \). Then \( \mathbb{Z}[\sqrt{N}] = \mathbb{Z}[\sqrt{n}] = \mathbb{Z}[\sqrt{n}]. \) By Corollary 4.5 [(1) \( \iff \) (3)], \( \mathbb{Z}[\sqrt{N}] \) is seminormal, if, and only if, \( n = p_1 \cdots p_s (\neq 1) \) and \( (d, n) = 1 \). The assertion is evidently verified in this case.

Finally, suppose \( d \equiv 1 \mod 4 \). Then \( \mathbb{Z}[\sqrt{N}] = \mathbb{Z}[2n]. \) By another appeal to Corollary 4.5, \( \mathbb{Z}[\sqrt{N}] \) is seminormal, if, and only if, \( 2n \) is square-free and \( (d, 2n) \) is (either 1 or) an integral power of 2; that is, if, and only if, \( f_0 = 0, f_1 = \ldots = f_s = 1, \) and \( \{p_1, \ldots, p_r\} \cap \{p_{+1}, \ldots, p_s\} = \emptyset \). The assertion clearly holds in this case, completing the proof.

**Acknowledgments.** The authors gratefully acknowledge partial support from each other's institution and from a NATO Collaborative Research grant. The second author worked under the auspices of the GNSAGA of the Consiglio Nazionale delle Ricerche.

**References**

SEMINORMAL RINGS GENERATED BY ALGEBRAIC INTEGERS


Professor D. E. Dobbs, 12A25: *ALGEBRAIC NUMBER THEORY; Algebraic number theory; global fields; Quadratic fields*

Department of Mathematics,
University of Tennessee,
Knoxville, Tennessee 37996-1300
U.S.A.

Professor M. Fontana,
Dipartimento di Matematica,
Università di Roma, “La Sapienza”
00185 Roma,
Italia.

Received on the 11th of November, 1986.