ON THE THEORY OF HENSELIAN RINGS

MASAYOSHI NAGATA

Introduction. The notion of Henselian rings was introduced by G. Azumaya [1].[1] We concern ourselves in the present paper mainly with Henselizations of integrally closed integrity domains. Chapter I deals with general integrally closed integrity domains. As a preparation of our studies, we introduce the notion of decomposition rings analogously as in the case of fields (§1). And then we define the notions of (local) Henselian rings and Henselizations of integrally closed integrity domains, and obtain several results concerning characterizations of Henselian rings and the uniqeness of Henselizations (§2).

In Chapter II, we restrict ourselves to the case of valuation rings. First we show that although the definition of Henselian rings are concerned with monic polynomials and the maximal ideal, the Hensel lemma holds also for non-monic polynomials (§3) and even modulo not necessarily prime ideals (with certain conditions) (§5).

Appendix (I) gives a proof of a fundamental lemma concerning extensions of a valuation, which is quoted in §3 and Appendix (II) shows an example of a certain type of Henselian, special, discrete valuation ring.

As for the terms, a ring (or an integrity domain) means always commutative one with identity and a ring which has only one maximal ideal is called quasi-local.

We refer to the notations as $\mathfrak{o}_{\mathfrak{p}}$, where $\mathfrak{o}$ is a ring and $\mathfrak{p}$ is its prime ideal, the ring of quotients of $\mathfrak{p}$ with respect to $\mathfrak{o}$.

Chapter I.

General theory of integrally closed Henselian integrity domains.

1. Decomposition rings.

LEMMA 1. Let $\mathfrak{o}$ be an integrally closed integrity domain with quotient field K. Assume that K' is a normal (algebraic) extension of K and let $\mathfrak{o}'$ be the totality of $\mathfrak{o}$-integers in K'. If $\mathfrak{p}_1'$ and $\mathfrak{p}_2'$ are prime ideals in $\mathfrak{o}'$ such that $\mathfrak{p}_1' \cap \mathfrak{o} = \mathfrak{p}_2' \cap \mathfrak{o}$, then $\mathfrak{p}_1'$ and $\mathfrak{p}_2'$ are conjugate to each other over K.

Proof. When K' is finite over K, our proof is easy,[2] while the general

Received December 4, 1951.

[1] The numbers in brackets refer to bibliography at the end.

[2] Cf. [5, Theorem 5] or the proof of [6, Lemma 1].

case can be proved easily by transfinite induction.

DEFINITION 1. An over-ring $\mathfrak{o}'$ of an integrity domain $\mathfrak{o}$ is called an integral extension of $\mathfrak{o}$ if every element of $\mathfrak{o}'$ is integral over $\mathfrak{o}$ and if $\mathfrak{o}'$ is an integrity domain.

DEFINITION 2. An integral extension $\mathfrak{o}'$ of an integrity domain $\mathfrak{o}$ is said to be almost finite over $\mathfrak{o}$ if the quotient field of $\mathfrak{o}'$ is finite over that of $\mathfrak{o}$.

Now let $\mathfrak{o}$ be an integrally closed integrity domain. Then every integrally closed integral extension $\mathfrak{o}'$ of $\mathfrak{o}$ is the totality of $\mathfrak{o}$-integers in the quotient field of $\mathfrak{o}'$. We may use the terminologies such as normal extensions, Galois groups, decomposition groups and decomposition rings as follows:

DEFINITION 3. An integral extension $\mathfrak{o}'$ of $\mathfrak{o}$ is called a normal extension of $\mathfrak{o}$ if it is integrally closed and if its quotient field K' is normal over the quotient field K of $\mathfrak{o}$; and when this is the case, the Galois group G of K is called the Galois group of $\mathfrak{o}'$ over $\mathfrak{o}$. (It is evident that G is the totality of automorphisms of $\mathfrak{o}'$ over $\mathfrak{o}$.) Further if $\mathfrak{p}'$ is a prime ideal of $\mathfrak{o}'$, the totality H of elements of G which leave $\mathfrak{p}'$ invariant is called the decomposition group of $\mathfrak{p}'$ with respect to $\mathfrak{o}$, which forms a subgroup of G. The decomposition ring of $\mathfrak{p}'$ with respect to $\mathfrak{o}$ is the totality of elements of $\mathfrak{o}'$ which are left invariant under every element of H.

Remark. H is a closed subgroup of G. For a proof, assume that an element σ of G maps $\mathfrak{p}'$ onto another prime ideal $\mathfrak{p}'^{\sigma}$. Let a be an element of $\mathfrak{p}'$ which is not in $\mathfrak{p}'^{\sigma}$, and consider an almost finite normal extension $\mathfrak{o}''$ of $\mathfrak{o}$ containing a and contained in $\mathfrak{o}'$.[8] Then clearly $(\mathfrak{o}'' \cap \mathfrak{p}')^{\sigma} = \mathfrak{o}'' \cap \mathfrak{p}'^{\sigma} \neq \mathfrak{o}'' \cap \mathfrak{p}'$, which shows that σ is not in the closure of H in G and this proves our statement.

LEMMA 2. Let $\mathfrak{o}'$ be an almost finite, separable normal extension of an integrally closed integrity domain $\mathfrak{o}$ with Galois group G. Let $\mathfrak{p}'$ be a prime ideal of $\mathfrak{o}'$ and $\mathfrak{p}'_0 = \mathfrak{p}'$, $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_n$ ($\mathfrak{p}'_i \neq \mathfrak{p}'_j$ if $i \neq j$) be the totality of conjugates of $\mathfrak{p}'$. Let $\tilde{\mathfrak{o}}$ be the decomposition ring of $\mathfrak{p}'$ (with respect to $\mathfrak{o}$). Then every element a of $\tilde{\mathfrak{o}}$ which is not in $\mathfrak{p}'$ and is in every $\mathfrak{p}'_j$ ($n \geqq j \geqq 1$) is a root of an irreducible monic polynomial $f(x)$ such that $f(x) \equiv x^n(x - a_1) \pmod{\mathfrak{p}' \cap \mathfrak{o}}$, $a_1 \in \mathfrak{o}$, $a_1 \equiv a \pmod{\mathfrak{p}' \cap \tilde{\mathfrak{o}}}$.

Proof. Let $G = H + H\sigma_1 + \ldots + H\sigma_n$ ($\sigma_i \in G$), where H is the decomposition group of $\mathfrak{p}'$. Then every conjugate of a is of the form a^{σ_i} or a itself. By our assumption $a^{\sigma_i} \in \mathfrak{p}'$ ($i = 1, \ldots, n$). Therefore the irreducible monic equation $x^{n+1} - a_1 x^n - \ldots - a_{n+1} = 0$ ($a_i \in \mathfrak{o}$) satisfied by a satisfies the following condition: $a_1 \equiv a \pmod{\mathfrak{p}'}$, $a_j \in \mathfrak{p}'$ if $j \geqq 2$. This proves our assertion.

THEOREM 1. *Let $\mathfrak{o}'$ be a separable normal extension of an integrally closed*

integrity domain $\mathfrak{o}$. *Let* $\mathfrak{p}'$ *be a maximal ideal of* $\mathfrak{o}'$ *and set* $\mathfrak{p}=\mathfrak{p}'\cap\mathfrak{o}$. *Let* $\tilde{\mathfrak{o}}$ *be the decomposition ring of* $\mathfrak{p}'$ *and set* $\tilde{\mathfrak{p}}=\mathfrak{p}'\cap\tilde{\mathfrak{o}}$. *Then* (1) $\mathfrak{p}'$ *is the unique maximal ideal of* $\mathfrak{o}'$ *which contains* $\tilde{\mathfrak{p}}$, (2) $\tilde{\mathfrak{p}}$ *is the primary component of* $\mathfrak{p}\tilde{\mathfrak{o}}$ *belonging to* $\tilde{\mathfrak{p}}$ *and* (3) $\tilde{\mathfrak{o}}/\tilde{\mathfrak{p}}=\mathfrak{o}/\mathfrak{p}$.

Proof. (1) follows immediately from Lemma 1 and the remark just above. To prove the others, we first assume that $\mathfrak{o}'$ is almost finite over $\mathfrak{o}$. Let G be the Galois group of $\mathfrak{o}'$ over $\mathfrak{o}$ and let H be the decomposition group of $\mathfrak{p}'$. Denote by $\mathfrak{q}$ the primary component of $\mathfrak{p}\tilde{\mathfrak{o}}$ belonging to $\mathfrak{p}$. Let $G=H+H\sigma_1+\cdots+H\sigma_r$. Then $\mathfrak{p}'$, $\mathfrak{p}'^{\sigma_1}$, $\cdots$, $\mathfrak{p}'^{\sigma_r}$ is the totality of maximal ideals of $\mathfrak{o}'$ containing $\mathfrak{p}$. We show that if an element a of $\tilde{\mathfrak{p}}$ is in none of $\mathfrak{p}_i=\mathfrak{p}'^{\sigma_i}\cap\tilde{\mathfrak{o}}$ $(i=1,\cdots,r)$ then a is in $\mathfrak{q}$. Indeed, $b=\prod_{i=1}^{r}a^{\sigma_i}$ is not in $\tilde{\mathfrak{p}}$, for since a^{σ_i} is in none of $\mathfrak{p}'^{\sigma_1\sigma_i}$, $\cdots$, $\mathfrak{p}'^{\sigma_r\sigma_i}$ and since $\mathfrak{p}'^{\sigma_i}\neq\mathfrak{p}'$ $(i=1,\cdots,r)$ $\mathfrak{p}'$ is one of $\mathfrak{p}'^{\sigma_1\sigma_i},\cdots,\mathfrak{p}'^{\sigma_r\sigma_i}$, we have $a^{\sigma_i}\notin\mathfrak{p}'$ $(i\geqq 1)$. On the other hand, ab is in $\mathfrak{p}$ whence in $\tilde{\mathfrak{p}}$ which shows our statement. This being said, we have $\mathfrak{q}\supseteqq\mathfrak{n}=\bigcap_{i=0}^{r}\tilde{\mathfrak{p}}_i$, where $\tilde{\mathfrak{p}}_0=\tilde{\mathfrak{p}}$: For, let a be as above, and let c be an arbitrary element of $\mathfrak{n}$, then $a+c$ is in $\tilde{\mathfrak{p}}$ and in none of $\tilde{\mathfrak{p}}_j$ $(j\geqq 1)$, whence a, $a+c\in\mathfrak{q}$. Therefore $c\in\mathfrak{q}$. Now we see that $\mathfrak{q}=\tilde{\mathfrak{p}}$ if we observe that $\tilde{\mathfrak{o}}/\mathfrak{n}$ is a direct sum of fields. As for (3), if $r=0$, we see that $\tilde{\mathfrak{o}}=\mathfrak{o}$, whence (3) is evident. Therefore we may assume that $r\geqq 1$. Set $\mathfrak{a}=\bigcap_{i=1}^{r}\tilde{\mathfrak{p}}_i$. Then $\tilde{\mathfrak{p}}+\mathfrak{a}=\tilde{\mathfrak{o}}$. This shows that for every element a of $\tilde{\mathfrak{o}}$ there exists an element a_0 of $\mathfrak{a}$ such that $a_0\equiv a$ (mod. $\tilde{\mathfrak{p}}$). Then there exists an element a_1 of $\mathfrak{o}$ such that $a_1\equiv a$ (mod. $\tilde{\mathfrak{p}}$) by virtue of Lemma 2. The almost finite case being disposed of, we consider the general case. Let a be an element of $\tilde{\mathfrak{o}}$. Let $\mathfrak{o}^*$ be an almost finite normal extension of $\mathfrak{o}$ containing a and contained in $\mathfrak{o}'$. Then there exists an element a_1 of $\mathfrak{o}$ such that $a_1\equiv a$ (mod. $\tilde{\mathfrak{p}}$),[3] which proves (3). If $a\in\tilde{\mathfrak{p}}$, there exists an element b of $\mathfrak{o}^*\cap\tilde{\mathfrak{o}}$ which is not in $\tilde{\mathfrak{p}}$ such that $ab\in\mathfrak{p}(\mathfrak{o}^*\cap\tilde{\mathfrak{o}})$, which proves (2). Thus our proof is complete.

COROLLARY. Let $\mathfrak{o}$ and $\mathfrak{o}'$ be as in Theorem 1. Assume that $\mathfrak{q}'$ is a prime ideal of $\mathfrak{o}'$ and let $\tilde{\mathfrak{o}}$ be the decomposition ring of $\mathfrak{q}'$ with respect to $\mathfrak{o}$. Then we have (1) $\mathfrak{q}'$ is the unique prime ideal of $\mathfrak{o}'$ whose intersection with $\tilde{\mathfrak{o}}$ coincides with $\mathfrak{q}'\cap\tilde{\mathfrak{o}}=\tilde{\mathfrak{q}}$, (2) $\tilde{\mathfrak{q}}$ is the primary component of $(\mathfrak{q}'\cap\mathfrak{o})\tilde{\mathfrak{o}}$ belonging to $\tilde{\mathfrak{q}}$ and (3) the quotient field of $\tilde{\mathfrak{o}}/\tilde{\mathfrak{q}}$ coincides with that of $\mathfrak{o}/(\mathfrak{q}'\cap\mathfrak{o})$.

2. Henselizations.

DEFINITION 4. Let $\mathfrak{o}$ be a ring and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{o}$. $\mathfrak{o}$ is called a locally Henselian ring at $\mathfrak{p}$ if the following condition is satisfied:

If a monic polynomial $f(x)$ with coefficients in $\mathfrak{o}$ factors into a product of monic polynomials $g_0(x)$ and $h_0(x)$ modulo $\mathfrak{p}$ and if the resultant $r(g_0, h_0)$ of

[3] Observe that $\mathfrak{o}^*\cap\tilde{\mathfrak{o}}$ is the decomposition ring of $\mathfrak{p}'\cap\mathfrak{o}^*$ with respect to $\mathfrak{o}$.

$g_0(x)$ and $h_0(x)$ is not in $\mathfrak{p}$ (i.e., $h_0(x)$ and $g_0(x)$ have no common root modulo $\mathfrak{p}$), then $f(x)$ factors into a product of monic polynomials $g(x)$ and $h(x)$ such that $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod. $\mathfrak{p}$).

DEFINITION 5. A ring $\mathfrak{o}$ is called Henselian, if it is quasi-local and if it is locally Henselian at its maximal ideal.

LEMMA 3. Let $\mathfrak{o}$ be an integrally closed integrity domain with unique maximal ideal $\mathfrak{p}$. Then $\mathfrak{o}$ is Henselian if and only if every integral extension of $\mathfrak{o}$ is quasi-local.

Proof. If an integral extension of $\mathfrak{o}$ is not quasi-local, we can find an irreducible monic polynomial $x^r + a_1x^{r-1} + \ldots + a_r$ over $\mathfrak{o}$ such that $a_1 \notin \mathfrak{p}$, $a_j \in \mathfrak{p}$ $(j \geqq 2)$, $r \geqq 2$, by virtue of Lemma 2; therefore $\mathfrak{o}$ is not Henselian. Conversely if $\mathfrak{o}$ is not Henselian, there exists an irreducible monic polynomial $f(x)$ which factors into a product of two monic polynomials $g(x)$ and $h(x)$ modulo $\mathfrak{p}$ such that $g(x)$ and $h(x)$ have no common root modulo $\mathfrak{p}$. Then clearly the integral extension of $\mathfrak{o}$ which is obtained by adjoining a root of $f(x)$ is not quasi-local.

THEOREM 2. *An integrally closed integrity domain $\mathfrak{o}$ with a prime ideal $\mathfrak{p}$ is locally Henselian at $\mathfrak{p}$ if and only if $\mathfrak{o}_\mathfrak{p}$ is Henselian.*

THEOREM 3. *An integrally closed integrity domain $\mathfrak{o}$ with a prime ideal $\mathfrak{p}$ is locally Henselian at $\mathfrak{p}$ if and only if every integral extension of $\mathfrak{o}$ has only one prime ideal whose intersection with $\mathfrak{o}$ coincides with $\mathfrak{p}$.*

Proof. By virtue of Lemma 3, Theorems 2 and 3 are equivalent to each other. First we assume that $\mathfrak{o}_\mathfrak{p}$ is Henselian and that a monic polynomial $f(x) \in \mathfrak{o}[x]$ factors into a product of monic polynomials $g_0(x)$ and $h_0(x)$ modulo $\mathfrak{p}$ such that $g_0(x)$ and $h_0(x)$ have no common root modulo $\mathfrak{p}$. Then $f(x)$ factors into a product of two monic polynomials $g(x)$ and $h(x)$ in $\mathfrak{o}_\mathfrak{p}[x]$ such that $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod. $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$). Then since $f(x) = g(x)h(x)$, every coefficient of $g(x)$ and $h(x)$ is integral over $\mathfrak{o}$, and therefore $g(x)$, $h(x) \in \mathfrak{o}[x]$. Therefore $\mathfrak{o}$ is locally Henselian at $\mathfrak{p}$. The converse follows from Lemma 2.

Further we see at the same time, by virtue of Lemma 2, a note-worthy

THEOREM 4. *An integrally closed integrity domain $\mathfrak{o}$ with a prime ideal $\mathfrak{p}$ is locally Henselian at $\mathfrak{p}$ if and only if every monic polynomial $f(x) = x^r + a_1x^{r-1} + \ldots + a_r$ such that $\mathfrak{o} \ni a_1 \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ $(i = 2, \ldots, r)$ has a linear factor $x + a$ with $a \equiv a_1$ (mod. $\mathfrak{p}$).*

DEFINITION 6. Let $\mathfrak{o}$ be an integrally closed integrity domain with a prime ideal $\mathfrak{p}$. Let $\bar{\mathfrak{o}}$ be the totality of separably integral elements over $\mathfrak{o}$ (in an algebraic closure of the quotient field of $\mathfrak{o}$) and let $\bar{\mathfrak{p}}$ be a prime ideal of $\bar{\mathfrak{o}}$ such that $\bar{\mathfrak{p}} \cap \mathfrak{o} = \mathfrak{p}$. Then the decomposition ring $\tilde{\mathfrak{o}}$ of $\mathfrak{p}$ with respect to $\mathfrak{o}$ is called the

local Henselization of $\mathfrak{o}$ at $\mathfrak{p}$. Further $\mathfrak{o}_{\mathfrak{p}\cap\bar{\mathfrak{o}}}$ is called the Henselization of $\mathfrak{o}$ at $\mathfrak{p}$. In case $\mathfrak{p}$ is a unique maximal ideal of $\mathfrak{o}$, the term "at $\mathfrak{p}$" should be omitted in each case.

THEOREM 5. *The local Henselization and the Henselization of an integrally closed integrity domain* $\mathfrak{o}$ *at its prime ideal* $\mathfrak{p}$ *are uniquely determined within isomorphisms over* $\mathfrak{o}$.

Proof. Immediate from Lemma 1.

THEOREM 6. *Let* $\mathfrak{o}^*$ *be the Henselization of an integrally closed integrity domain* $\mathfrak{o}$ *at a prime ideal* $\mathfrak{p}$. *Then* (1) $\mathfrak{o}^*$ *is a Henselian ring,* (2) $\mathfrak{p}\mathfrak{o}^*$ *is the maximal ideal of* $\mathfrak{o}^*$ *and* (3) $\mathfrak{o}^*/\mathfrak{p}\mathfrak{o}^*$ *is the quotient field of* $\mathfrak{o}/\mathfrak{p}$.

Proof. (1) is evident by virtue of Lemma 3 and the corollary to Theorem 1, while the others are immediate consequences of the corollary to Theorem 1.

THEOREM 7. *Let* $\mathfrak{o}$ *be an integrally closed integrity domain with a prime ideal* $\mathfrak{p}$. *If* $\mathfrak{o}'$ *is an integrally closed integrity domain with a prime ideal* $\mathfrak{p}'$ *such that* (1) $\mathfrak{o}'\supseteq\mathfrak{o}$, (2) $\mathfrak{p}'\cap\mathfrak{o}=\mathfrak{p}$ *and* (3) $\mathfrak{o}'$ *is locally Henselian at* $\mathfrak{p}'$, *then* $\mathfrak{o}'$ *contains the local Henselization of* $\mathfrak{o}$ *at* $\mathfrak{p}$ (*up to an isomorphism over* $\mathfrak{o}$).

Proof. Let $\mathfrak{o}''$ be the totality of separably integral elements over $\mathfrak{o}$ in $\mathfrak{o}'$. Then $\mathfrak{o}''$ is locally Henselian at $\mathfrak{p}''=\mathfrak{p}'\cap\mathfrak{o}''$.[4] Let $\bar{\mathfrak{o}}$ be the totality of separably integral elements over $\mathfrak{o}$ (in an algebraic closure which contains $\mathfrak{o}''$) and let $\bar{\mathfrak{p}}$ be a prime ideal of $\bar{\mathfrak{o}}$ such that $\bar{\mathfrak{p}}\cap\mathfrak{o}''=\mathfrak{p}''$. Then since $\mathfrak{o}''$ is locally Henselian at $\mathfrak{p}''$, this $\bar{\mathfrak{p}}$ is uniquely determined. Therefore $\mathfrak{o}''$ contains the decomposition ring of $\bar{\mathfrak{p}}$ with respect to $\mathfrak{o}$, which proves our assertion.

COROLLARY. Under the same assumption as in the preceding theorem, suppose further that $\mathfrak{o}'$ is Henselian and that $\mathfrak{p}'$ is its maximal ideal. Then $\mathfrak{o}'$ contains the Henselization of $\mathfrak{o}$ at $\mathfrak{p}$.

Chapter II.
Henselian valuation rings.

3. Hensel's lemma for Henselian valuation rings.

We cite here

Fundamental lemma on the extensions of valuations.[5] Let $\mathfrak{o}$ be a valuation ring with quotient field K and let a field Z be an algebraic extension of K. Let $\mathfrak{d}$ be the totality of $\mathfrak{o}$-integers in Z. Then, for every maximal ideal $\mathfrak{P}$ of $\mathfrak{d}$, $\mathfrak{d}_{\mathfrak{P}}$ is a valution ring.

As corollaries to this lemma, we have the following two theorems:

[4] Cf. the corollary to Lemma 4, § 5.

[5] Cf. [6, Lemma 2]. The proof in that paper makes use of the notion of multiplication rings. Appendix (I) of the present paper gives another proof which does not use that notion.

THEOREM 8. *The Henselization of a valuation ring is also a valuation ring.*

THEOREM 9. *Any integrally closed integral extension of a Henselian valuation ring is also a Henselian valuation ring.*

Further we have the following note-worthy

THEOREM 10. *Let* $\mathfrak{o}$ *be an integrally closed integrity domain which satisfies the following condition: Every prime ideal* $\mathfrak{p}$ *is contained in any principal ideal* $a\mathfrak{o}$ *with* $a \notin \mathfrak{p}$. *If* $\mathfrak{o}$ *is locally Henselian at a prime ideal* $\mathfrak{p}_1$ *and if* $\mathfrak{p}_2$ *is another prime ideal which is contained in* $\mathfrak{p}_1$, *then* $\mathfrak{o}$ *is locally Henselian at* $\mathfrak{p}_2$.

Proof. Any monic polynomial $x^r + a_1x^{r-1} + \ldots + a_r$ with coefficients in $\mathfrak{o}$ such that $a_1 \notin \mathfrak{p}_2$, $a_j \in \mathfrak{p}_2$ $(j \geqq 2)$ has a linear factor $x + a'$ with $a_1 \equiv a' \pmod{\mathfrak{p}_2}$, because $x^r + x^{r-1} + (a_1/a_1^2)x^{r-2} + \ldots + (a^r/a_1^r)$ has a linear factor $x + b$ with $b \equiv 1 \pmod{\mathfrak{p}_1}$, and so $f(x)$ has a linear factor $x + a_1b$ which is not congruent to x modulo $\mathfrak{p}_2$.

COROLLARY.[6] If a valuation ring $\mathfrak{o}$ is locally Henselian at a prime ideal $\mathfrak{p}$, so is also at every prime ideal contained in $\mathfrak{p}$.

Now we prove

THEOREM 11 (*Hensel's lemma*).[7] *Let* $\mathfrak{o}$ *be a locally Henselian valuation ring at its prime ideal* $\mathfrak{p}$. *If* $f(x)$ *is a polynomial of degree* n *with coefficients in* $\mathfrak{o}$ *such that* $f(x) \equiv g_0(x)h_0(x) \pmod{\mathfrak{p}}$, *where* $g_0(x) = x^r + a_1x^{r-1} + \ldots + a^r$ $(n > r > 0)$ *and* $h_0(x)$ *are polynomials in* $\mathfrak{o}$ *which are relatively prime modulo* $\mathfrak{p}$, *then there exist a monic polynomial* $g(x)$ *of degree* r *and a polynomial* $h(x)$ *in* $\mathfrak{o}$ *such that* $f(x) = g(x)h(x)$, $g(x) \equiv g_0(x) \pmod{\mathfrak{p}}$, $h(x) \equiv h_0(x) \pmod{\mathfrak{p}}$.

Proof. First we assume that $\mathfrak{p}$ is the maximal ideal of $\mathfrak{o}$. Let $c_0 \prod_{i=1}^{n}(c_ix - d_i)$ be the factorization of $f(x)$ in a suitable normal extension $\mathfrak{o}'$ of $\mathfrak{o}$, where $c_0 \notin \mathfrak{p}'$ and $c_i = 1$ if $c_i \notin \mathfrak{p}'$, denoting by $\mathfrak{p}'$ the maximal ideal of $\mathfrak{o}'$ (notice Theorem 9). Then we can find r indices, say, $1, \ldots, r$ such that $g_0(x) \equiv \prod_{i=1}^{r}(x - d_i) \pmod{\mathfrak{p}'}$ $(c_1 = \ldots = c_r = 1)$. We may assume without loss of generality that $c_i = 1$ if $i \leqq s$ and that $c_i \in \mathfrak{p}'$ if $i > s$. We set $g(x) = \prod_{i=1}^{r}(x - d_i)$, $k(x) = \prod_{i=r+1}^{s}(x - d_i)$, $f_1(x) = \prod_{i=1}^{s}(x - d_i)$, $h(x) = c_0 \prod_{i=r+1}^{n}(c_ix - d_i)$. Then since every conjugate of d_i is in $\mathfrak{o}'$, we see that $f_1(x)$ whence $g(x)$, $k(x)$ are polynomials in $\mathfrak{o}$. This case being settled, we proceed to the general case. By our above observation,

[6] This corollary may also be proved by our fundamental lemma just above.

[7] This theorem shows that a field with a valuation w is relatively complete with respect to w in the sense of Schilling [9] if and only if the valuation ring determined by w is Henselian.

we see that there exist such $g(x)$ and $h(x)$ in $\mathfrak{o}_\mathfrak{p}[x]$; the modulus being changed to $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$, which is however identical with $\mathfrak{p}$, since $\mathfrak{o}$ is a valuation ring. Therefore we have that $g(x)$ and $h(x)$ are polynomials in $\mathfrak{o}$. Thus the proof is completed.

4. Special valuation rings.

THEOREM 12.[8] *Let $\mathfrak{o}$ be a Henselian special valuation ring and let $\bar{\mathfrak{o}}$ be its completion. Then every elememt a of $\bar{\mathfrak{o}}$ which is separably algebraic over $\mathfrak{o}$ is in $\mathfrak{o}$.*

Proof. It is clear that a is integral over $\mathfrak{o}$, by virtue of Theorem 9. Let a be the limit of the sequence $(c_j = d_0 + \ldots + d_j;\ j = 0, 1, \ldots)$ with $d_i\mathfrak{o} \subset d_j\mathfrak{o}$ if $i > j$ and $\bigcap_{i=0}^{\infty} d_i\mathfrak{o} = (0)$. Let $f(x)$ be the irreducible monic polynomial satisfied by a. If the degree n of $f(x)$ is 1, our assertion is evident. Therefore we may assume that $n > 1$. Let $\alpha_1 = a, \alpha_2, \ldots, \alpha_n$ be the totality of roots of $f(x)$. Then the totality $\mathfrak{o}'$ of $\mathfrak{o}$-integers in $K(\alpha_1, \ldots, \alpha_n)$ is a valuation ring, where K is the quotient field of $\mathfrak{o}$. We see easily that $d_{j+1}\mathfrak{o}' = (\alpha - c_j)\mathfrak{o}' = (a - c_j)\mathfrak{o}'$. This shows that each α_i is the limit of the sequence (c_j) in $\mathfrak{o}$, i.e., $a = \alpha_i$ for each i, which is a contradiction to the fact that a is separable. Therefore $n = 1$ and we have $a \in \mathfrak{o}$.

COROLLARY. Let $\mathfrak{o}$ be a special valuation ring and let $\mathfrak{o}^*$ and $\bar{\mathfrak{o}}$ be respectively its Henselization and completion. Let K be the totality of separably algebraic elements over the quotient field of $\mathfrak{o}$. Then we have $\mathfrak{o}^* = K \cap \bar{\mathfrak{o}}$ (where K is considered as being contained in the algebraic closure of the quotient field of $\bar{\mathfrak{o}}$).

5. Generalized Hensel's lemma.

LEMMA 4. Let $\mathfrak{o}$ be an integrity domain. Assume that a polynomial $f(x)$ over $\mathfrak{o}$ factors into a product of two polynomials $g(x)$ and $h(x)$ with coefficients in an integrity domain which contains $\mathfrak{o}$. If the leading coefficient of $g(x)$ is in the quotient field K of $\mathfrak{o}$ and if $g(x)$ and $h(x)$ have no common root, then every coefficient of $g(x)$ or $h(x)$ is separable with respect to K.

Proof is easy.

COROLLARY. If moreover $f(x)$, $g(x)$, $h(x)$ are monic, then all coefficients of $g(x)$ and $h(x)$ are separably integral over $\mathfrak{o}$.

THEOREM 13 (*Generalized Hensel's lemma*). *Let $f(x)$ be a primitive polynomial of degree $r+s$ with coefficients in a Henselian valuation ring $\mathfrak{o}$. If there exist two polynomials $g_0(x)$ and $h_0(x)$ in $\mathfrak{o}[x]$ with respective degrees r*

[8] Cf. the example in Appendix (II).

https://doi.org/10.1017/S0027763000015439 Published online by Cambridge University Press

and s such that $g_0(x)$ is a monic polynomial and (1) $f(x)$ and $g_0(x)h_0(x)$ have the same leading coefficient, (2) $f(x) \equiv g_0(x)h_0(x)$ modulo an ideal $\mathfrak{a}$ of $\mathfrak{o}$, which is contained in $a^2b\mathfrak{o}$ where $a \neq 0$ is the resultant of $g_0(x)$ and $h_0(x)$ and b is an element of $\mathfrak{o}$ which is nilpotent modulo $a\mathfrak{o}$, then there exist two polynomials $g(x)$ and $h(x)$ in $\mathfrak{o}[x]$ such that (I) $g(x)$ and $h(x)$ have the respective degrees r and s, (II) $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod. $abc^{-1}\mathfrak{o}$) and $g(x)$ is a monic polynomial, where c is an arbitrary non-zero element which is nilpotent modulo $a\mathfrak{o}$, but c may be 1 if $a\mathfrak{o}$ is a primary ideal belonging to the maximal ideal of $\mathfrak{o}$, (III) $f(x) = g(x)h(x)$.

Proof. We first consider the case where $\mathfrak{o}$ is a special valuation ring. Let $\bar{\mathfrak{o}}$ be the completion of $\mathfrak{o}$. Then, as is well known,[9] we can find such $g(x)$ and $h(x)$ with coefficients in $\bar{\mathfrak{o}}$, and in this case, we can set $c = 1$. Then by Lemma 4 and Theorem 12, all coefficients of $g(x)$ and $h(x)$ are in $\mathfrak{o}$, which proves our assertion.

Now we prove the general case. Let $\mathfrak{p}_1$ be the minimal prime over-ideal of $a\mathfrak{o}$, and let $\mathfrak{p}_2$ be the largest prime ideal contained in $a\mathfrak{o}$. Then we see easily that $\mathfrak{o}_{\mathfrak{p}_1}/\mathfrak{p}_2\mathfrak{o}_{\mathfrak{p}_1}$ is a Henselian special valuation ring. Therefore, there exist two polynomials $g_1(x)$ and $h_1(x)$ with coefficients in $\mathfrak{o}_{\mathfrak{p}_1}$ such that (i) $g_1(x)$ and $h_1(x)$ have the respective degrees r and s, (ii) $g_1(x) \equiv g_0(x)$, $h_1(x) \equiv h_0(x)$ (mod. $ab\mathfrak{o}_{\mathfrak{p}_1}$) and $g_1(x)$ is a monic polynomial, (iii) $f(x) \equiv g_1(x)h_1(x)$ (mod. $\mathfrak{p}_2\mathfrak{o}_{\mathfrak{p}_1}$). Since $\mathfrak{o}_{\mathfrak{p}_1}$ is locally Henselian at $\mathfrak{p}_2\mathfrak{o}_{\mathfrak{p}_1}$ by virtue of the corollary to Theorem 10, there exist polynomials $g(x)$ and $h(x)$ with coefficients in $\mathfrak{o}_{\mathfrak{p}_1}$ such that (I) is satisfied and that (II)′ $g(x) \equiv g_1(x) \equiv g_0(x)$, $h(x) \equiv h_1(x) \equiv h_0(x)$ (mod. $ab\mathfrak{o}_{\mathfrak{p}_1}$), $g(x)$ is monic, (III)′ $f(x) = g(x)h(x)$.

Since $ab\mathfrak{o}_{\mathfrak{p}_1}$ is an ideal of $\mathfrak{o}$ contained in $abc^{-1}\mathfrak{o}$, we see that $g(x)$ and $h(x)$ are polynomials in $\mathfrak{o}$. This $g(x)$ and $h(x)$ are required polynomials.

Remark. Theorem 13 holds even if $\mathfrak{o}$ is a valuation ring which is locally Henselian at a prime ideal $\mathfrak{p}$ (not necessarily maximal) which contains the resultant a of $g_0(x)$ and $h_0(x)$.

6. Some remarks on the Henselizations of valuation rings.

LEMMA 5. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be prime ideals of a ring $\mathfrak{o}$ such that $\mathfrak{p}_1 \supset \mathfrak{p}_2$. If $\mathfrak{o}$ is locally Henselian at $\mathfrak{p}_2$ and if $\mathfrak{o}/\mathfrak{p}_2$ is locally Henselian at $\mathfrak{p}_1/\mathfrak{p}_2$, then $\mathfrak{o}$ is locally Henselian at $\mathfrak{p}_1$.

Proof is easy.

LEMMA 6. Let $\mathfrak{p}$ be a prime ideal of a valuation ring $\mathfrak{o}$ with quotient field K. Let there be an element a which is a root of an irreducible monic polynomial $f(x)$ of degree n such that $f(x)$ modulo $\mathfrak{p}$ is also irreducible over $\mathfrak{o}/\mathfrak{p}$.

[9] Cf. [8, § 11]. Virtually it is the same as that in [3, p. 71].

If $\mathfrak{v}$ is a valuation ring which contains $\mathfrak{o}/\mathfrak{p}$ and a modulo $\mathfrak{p}$, then there exists a valuation ring $\mathfrak{o}'$ such that (1) the quotient field of $\mathfrak{o}'$ is $Z=K(a)$, (2) $\mathfrak{o}'\cap K=\mathfrak{o}$ and therefore there exists a prime ideal $\mathfrak{p}'$ of $\mathfrak{o}'$ such that $\mathfrak{p}'\cap\mathfrak{o}=\mathfrak{p}$, (3) $\mathfrak{o}'\ni a$ (4) if we consider a modulo $\mathfrak{p}$ as a modulo $\mathfrak{p}'$ of $\mathfrak{o}'/\mathfrak{p}'$, the quotient field of $\mathfrak{o}'/\mathfrak{p}'$ is generated by a modulo $\mathfrak{p}$ over that of $\mathfrak{o}/\mathfrak{p}$ and further $\mathfrak{o}'/\mathfrak{p}'\subseteqq\mathfrak{v}$.

Proof. Let $\mathfrak{o}''$ be the totality of $\mathfrak{o}$-integers in $Z=K(a)$. Let $\mathfrak{p}''$ be a prime ideal of $\mathfrak{o}''$ such that $\mathfrak{p}''\cap\mathfrak{o}=\mathfrak{p}$. We want to show that the quotient field of $\mathfrak{o}''/\mathfrak{p}''$ is generated by a (modulo $\mathfrak{p}$) over the quotient field $\bar{K}$ of $\mathfrak{o}/\mathfrak{p}$. Indeed, every element of $\mathfrak{o}''$ is of a form $(c_{1,0}/c_{2,0})+(c_{1,1}/c_{2,1})a+\ldots+(c_{1,n-1}/c_{2,n-1})a^{n-1}$ with $c_{i,j}\in\mathfrak{o}$ $(i=1, 2 : j=0, \ldots, n-1)$. Since $\mathfrak{o}$ is a valuation ring, we may assume that $c_{2,j}=1$ unless $c_{1,j}=1$. Then since $1, a, \ldots, a^{n-1}$ are linearly independent over $\mathfrak{o}/\mathfrak{p}$, we have $c_{2,j}\notin\mathfrak{p}$ for every $j=1, \ldots, n-1$, and this shows our statement. Now let $\mathfrak{q}''$ be a maximal ideal of $\mathfrak{o}''$ such that $\mathfrak{q}''\supseteqq\mathfrak{p}''$ and $\mathfrak{q}''/\mathfrak{p}''$ contains the intersection of maximal ideal of $\mathfrak{v}$ with $\bar{K}$ [a modulo $\mathfrak{p}$]. Then we see easily that $\mathfrak{o}'=\mathfrak{o}''_{\mathfrak{q}''}$ is a required ring.

THEOREM 14. *Let $\mathfrak{p}$ be a prime ideal of a valuation ring $\mathfrak{o}$ and let $\mathfrak{o}^*$ be the Henselization of $\mathfrak{o}$. Then there exists a prime ideal $\mathfrak{p}^*$ of $\mathfrak{o}^*$ such that $\mathfrak{p}^*\cap\mathfrak{o}=\mathfrak{p}$; and for this $\mathfrak{p}^*$, $\mathfrak{o}^*/\mathfrak{p}^*$ is the Henselization of $\mathfrak{o}/\mathfrak{p}$.*

Proof. The existence of $\mathfrak{p}^*$ is evident. Since $\mathfrak{o}^*/\mathfrak{p}^*$ is Henselian, it contains the Henselization of $\mathfrak{o}/\mathfrak{p}$. As for the converse, we observe that since $\mathfrak{o}^*$ is locally Henselian at $\mathfrak{p}^*$, $\mathfrak{o}^*$ contains the local Henselization $\tilde{\mathfrak{o}}$ of $\mathfrak{o}$ at $\mathfrak{p}$. Denote by $\mathfrak{o}_1$ the valuation ring $\tilde{\mathfrak{o}}_{\tilde{\mathfrak{q}}}$, where $\tilde{\mathfrak{q}}$ is the intersection of the maximal ideal of $\mathfrak{o}^*$ with $\tilde{\mathfrak{o}}$. Then, by Theorem 6, $\mathfrak{o}_1/\mathfrak{p}_1=\mathfrak{o}/\mathfrak{p}$, where $\mathfrak{p}_1$ is the prime ideal of $\mathfrak{o}_1$ such that $\mathfrak{p}_1\cap\mathfrak{o}=\mathfrak{p}$. Since $\mathfrak{o}_1$ is locally Henselian at $\mathfrak{p}_1$, we see easily by virtue of Lemma 6 that there exists a valuation ring $\mathfrak{o}'$ such that (1) $\mathfrak{o}_1\subseteqq\mathfrak{o}'\subseteqq\mathfrak{o}^*$ and therefore there exists a prime ideal $\mathfrak{p}'$ of $\mathfrak{o}'$ such that $\mathfrak{p}'\cap\mathfrak{o}_1=\mathfrak{p}_1$ and (2) $\mathfrak{o}'/\mathfrak{p}'$ is the Henselization of $\mathfrak{o}_1/\mathfrak{p}_1=\mathfrak{o}/\mathfrak{p}$. Further it is easy to see that $\mathfrak{o}'$ is locally Henselian at $\mathfrak{p}'$. Now, by virtue fo Lemma 5, $\mathfrak{o}'$ is Henselian, whence $\mathfrak{o}'\supseteqq\mathfrak{o}^*$. Thus our proof is complete.

THEOREM 15.[10] *Let $\mathfrak{o}$ be a valuation ring and let $\mathfrak{o}^*$ be its Henselization. Then every principal ideal of $\mathfrak{o}^*$ is generated by an element of $\mathfrak{o}$.*

Proof. It is sufficient to show that if $\mathfrak{o}\neq\mathfrak{o}^*$, there exists a valuation ring $\mathfrak{o}'$ $(\mathfrak{o}\subset\mathfrak{o}'\subseteqq\mathfrak{o}^*)$ such that every principal ideal of $\mathfrak{o}'$ is generated by an element of $\mathfrak{o}$. Let $\mathfrak{i}$ be a minimal integrally closed integral extension of $\mathfrak{o}$ contained in $\mathfrak{o}^*$. Then we can find two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathfrak{o}$ such that (1) there exist at least two prime ideals in $\mathfrak{i}$ whose intersection with $\mathfrak{o}$ coincides with $\mathfrak{p}_1$, (2) there

[10] If we make use of the results concerning maximally complete valuation rings due to Krull [4], this result is evident by virtue of the corollary to Theorem 7.

exists unique prime ideal in $\mathfrak{i}$ whose intersection with $\mathfrak{o}$ coincides with $\mathfrak{p}_2$, (3) there exists no prime ideal $\mathfrak{p}$ such that $\mathfrak{p}_1 \supset \mathfrak{p} \supset \mathfrak{p}_2$. Let $\mathfrak{p}_1^*$ and $\mathfrak{p}_2^*$ be prime ideals of $\mathfrak{o}^*$ such that $\mathfrak{p}_i^* \cap \mathfrak{o} = \mathfrak{p}_i$ $(i = 1, 2)$ and set $\mathfrak{q} = \mathfrak{p}_1^* \cap \mathfrak{i}$. Let K' be the quotient field of $\mathfrak{i}$ and set $\mathfrak{o}' = \mathfrak{o}^* \cap K'$. Then we have $\mathfrak{o}'/\mathfrak{p}_1^* \cap \mathfrak{o}' = \mathfrak{i}/\mathfrak{q} = \mathfrak{o}/\mathfrak{p}$ by virtue of the corollary to Theorem 1. Therefore we may assume that $\mathfrak{p}_1$ is maximal. Let $\mathfrak{a}$ be the intersection of all maximal ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of $\mathfrak{i}$ other than $\mathfrak{q}$ and let a be an element of $\mathfrak{q}$ which is not in $\mathfrak{a}$. Let $\mathfrak{b}$ be a principal ideal of $\mathfrak{o}'$. (I) When $\mathfrak{b} \nsubseteq \mathfrak{p}_2^* \cap \mathfrak{o}'$: It is evident that $\mathfrak{b}$ is generated by an element b of $\mathfrak{a}$. We can find natural numbers s and t such that $c = b + a^s(1 + a + \ldots + a^{t-1}) \notin \mathfrak{q}_i$ $(1 \leqq i \leqq r)$, $\mathfrak{b} = c\mathfrak{o}'$. Then evidently $\mathfrak{b}$ is generated by the norm of c with respect to $\mathfrak{o}$. (II) When $\mathfrak{b} \subseteq \mathfrak{p}_2^* \cap \mathfrak{o}'$: That $\mathfrak{b}$ is generated by an element of $\mathfrak{o}$ is evident because every element of $\mathfrak{i}$ is of a form $(a_{1,0}/a_{2,0}) + (a_{1,1}/a_{2,1})a + \ldots + (a_{1,n}/a_{2,n})a^n$ $(a_{i,j} \in \mathfrak{o},\ a_{2,j} \notin \mathfrak{p}_2)$, where $n+1$ is the degree of a with respect to $\mathfrak{o}$.

Appendix (I)

LEMMA 7. Let $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$ be valuation rings with common quotient field K. Let a be an element of K. Then there exists a natural number s such that both $a/(1 + a + \ldots + a^{s-1})$ and $1/(1 + a + \ldots + a^{s-1})$ are in the intersection $\mathfrak{d}$ of $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$. If t is any given natural number, we can select s such that $(t, s) = 1$.

Proof. It is clear that there exists a natural number $s \geqq 2$ such that $(s, t) = 1$ and that $1 + a + \ldots + a^{s-1}$ is not in the maximal ideal $\mathfrak{p}$ of $\mathfrak{o}$ for every i $(1 \leqq i \leqq n)$. This s is a required number: For, when $a \in \mathfrak{o}$, it is clear that $(1 + a + \ldots + a^{s-1})$ is a unit in $\mathfrak{o}_i$, and therefore $a/(1 + a + \ldots + a^{s-1})$, $1/(1 + a + \ldots + a^{s-1}) \in \mathfrak{o}_i$; when $a \notin \mathfrak{o}_i$, we see easily that these elements are in $\mathfrak{o}_i$, if we observe that $0 = w_i(1) > w_i(a) \geqq w_i(1 + a + \ldots + a^{s-1})$, w_i being a valuation given by $\mathfrak{o}_i$.

Theorem of independency of valuations.[11] *Let $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$ be valuation rings with common quotient field K. Assume that $\mathfrak{o}_i \nsubseteq \mathfrak{o}_j$ if $i \neq j$ $(1 \leqq i, j \leqq n)$. Set $\mathfrak{d} = \mathfrak{o}_1 \cap \ldots \cap \mathfrak{o}_n$ and let $\mathfrak{p}_i$ be the maximal ideal of $\mathfrak{o}_i$ for each i. Then (1) every $\mathfrak{q}_i = \mathfrak{p}_i \cap \mathfrak{d}$ $(1 \leqq i \leqq n)$ is a maximal ideal of $\mathfrak{d}$ and conversely every maximal ideal of $\mathfrak{d}$ is one of $\mathfrak{q}_i$. Further (2) $\mathfrak{d}_{\mathfrak{q}_i} = \mathfrak{o}_i$.*[12]

Proof. First we prove (2). Let a be an element of $\mathfrak{o}_i$. Then there exists a natural number s such that $a/(1 + a + \ldots + a^{s-1})$, $1/(1 + a + \ldots + a^{s-1})$ are in $\mathfrak{d}$ by Lemma 7. Then it is evident that $1/(1 + a + \ldots + a^{s-1}) \notin \mathfrak{p}_i$, whence

[11] This is a refinement of a Krull's result [4, Theorem 18].

[12] This last assertion (2) holds without the assumpion that $\mathfrak{o}_i \nsubseteq \mathfrak{o}_j$ if $i \neq j$, as is seen in the proof.

$a \in \mathfrak{d}_{q_i}$. Therefore $\mathfrak{d}_{q_i} \geqq \mathfrak{o}_i$. Since $\mathfrak{o}_i \geqq \mathfrak{d}$, $q_i = \mathfrak{p}_i \cap \mathfrak{d}$, we have $\mathfrak{o}_i \geqq \mathfrak{d}_{q_i}$, hence $\mathfrak{d}_{q_i} = \mathfrak{o}_i$. This shows, by our assumption on $\mathfrak{o}_i$, that $q_i \not\subseteq q_j$ if $i \neq j$. There exists therefore an element e_i of $\mathfrak{d}$ such that e_i is a unit in $\mathfrak{o}_i$ and is a non-unit in other $\mathfrak{o}_j$ for each i.[13] Now we prove (1). For this purpose, it is sufficient to show that every ideal of $\mathfrak{d}$ is contained in one of q_i, i.e., if an ideal $\mathfrak{a}$ of $\mathfrak{d}$ contains elements $a_1, \ldots, a_n$ such that a_i is a unit in $\mathfrak{o}_i$ for each i, then $\mathfrak{a} = \mathfrak{d}$. Now, $\mathfrak{a}$ contains $a_i e_i$, which is a unit in $\mathfrak{o}_i$ and is a non-unit in other $\mathfrak{o}_j$. Therefore $e = \sum_{i=1}^{n} a_i e_i$ is in $\mathfrak{a}$. It is evident that e is a unit in every $\mathfrak{o}_i$, whence e is a unit in $\mathfrak{d}$. Therefore $\mathfrak{a} = \mathfrak{d}$. Thus our theorem is proved.

COROLLARY 1. Let $\mathfrak{d}, \mathfrak{o}_1, \ldots, \mathfrak{o}_n$ be the same as in the preceding theorem. Let $\mathfrak{a}_i$ be an ideal in $\mathfrak{o}_i$ and let $\mathfrak{p}_i'$ be the minimal prime over-ideal of $\mathfrak{a}_i$ for each i. If $\mathfrak{p}_i' \not\subseteq \mathfrak{p}_j'$ for every pair i, j $(i \neq j)$, then $\mathfrak{d}/\bigcap_{i=1}^{n} \mathfrak{a}_i$ is the direct sum of $\mathfrak{o}_1/\mathfrak{a}_1, \ldots, \mathfrak{o}_n/\mathfrak{a}_n$.

Proof. If we observe the fact that if $\mathfrak{p}$ is a prime ideal of a valuation ring $\mathfrak{o}$, $\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$ coincides with $\mathfrak{p}$ set-theoretically, then we can see in virtue of the above theorem that $(\mathfrak{a}_i \cap \mathfrak{d}) + (\mathfrak{a}_j \cap \mathfrak{d}) = \mathfrak{d}$ if $i \neq j$: Indeed, if we consider the ring $\mathfrak{d}_{\mathfrak{p}_i' \cap \mathfrak{d}}$, then this ring is the valuation ring $\mathfrak{o}_{i\mathfrak{p}_i'}$, which has the maximal ideal $\mathfrak{p}'\mathfrak{o}_{i\mathfrak{p}_i'} = \mathfrak{p}_i'$. If there exists a maximal ideal $q_j = \mathfrak{p}_j \cap \mathfrak{d}$ such that $j \neq i$, $q_j \geqq \mathfrak{p}_i' \cap \mathfrak{d}$, then $\mathfrak{d}_{\mathfrak{p}_i' \cap \mathfrak{d}}$ is a valuation ring of type $\mathfrak{o}_{j_q}$ with a suitable prime ideal $\mathfrak{q}$ of $\mathfrak{o}_j$. Since the maximal ideal of $\mathfrak{o}_{i_q}$ is $\mathfrak{q}\mathfrak{o}_{j_q} = \mathfrak{q}$, we have $\mathfrak{p}_i' = \mathfrak{q} \subseteq \mathfrak{o}_j$. Therefore $\mathfrak{p}_i' \subseteq \mathfrak{p}_j'$ or $\mathfrak{p}_j' \subseteq \mathfrak{p}_i'$, contrary to our assumption. Thus q_i is the unique maximal ideal of $\mathfrak{d}$ containing $\mathfrak{p}_i' \cap \mathfrak{d}$ whence $\mathfrak{a}_i \cap \mathfrak{d}$. Thus we see that $\mathfrak{d}/\bigcap_{i=1}^{n} \mathfrak{a}_i$ is the direct sum of $\mathfrak{d}/\mathfrak{a}_1 \cap \mathfrak{d}, \ldots, \mathfrak{d}/\mathfrak{a}_n \cap \mathfrak{d}$. That $\mathfrak{d}/\mathfrak{a}_i \cap \mathfrak{d} = \mathfrak{o}_i/\mathfrak{a}_i$ is evident because $\mathfrak{d}_{q_i} = \mathfrak{o}_i$.

COROLLARY 2.[14] Let $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$ and K be the same as in the above and let $w_1, \ldots, w_n$ be the valuations of K given by $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$ respectively. Let $a_1, \ldots, a_n$ be elements of $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$ respectively such that the respective minimal prime over-ideals $\mathfrak{p}_1', \ldots, \mathfrak{p}_n'$ of $a_1\mathfrak{o}_1, \ldots, a_n\mathfrak{o}_n$ in $\mathfrak{o}_1, \ldots, \mathfrak{o}_n$ have no inclusion relation. If $d_1, \ldots, d_n$ is a given system of elements of K such that $w_i(a_i d_i) \geqq 0$ for each i, then we can find an element d of K such that $w_i(d - d_i) \geqq w_i(a_i)$.

Proof. Set $\mathfrak{d} = \mathfrak{o}_1 \cap \ldots \cap \mathfrak{o}_n$ as above. Then by Corollary 1 $\mathfrak{d}/\bigcap_{i=1}^{n} a_i^2\mathfrak{o}_i = \mathfrak{o}_1/a_1^2\mathfrak{o}_1 + \ldots + \mathfrak{o}_n/a_n^2\mathfrak{o}_n$ (direct sum). There exists therefore an element e of $\mathfrak{d}$ such that $w_i(a_i) = w_i(e)$ for every i. Further we see that there exists an element f of $\mathfrak{d}$ such that $w_i(f - ed_i) \geqq w_i(a_i^2)$. Then evidently $d = f/e$ is a required element.

[13] Take an element of $\bigcap_{j \neq i} q_j$ which is not in q_i.

[14] This is a generalization of Krull's result [4, Theorem 15].

https://doi.org/10.1017/S0027763000015439 Published online by Cambridge University Press

Now we come to the fundamental lemma concerning the extensions of valuations, which is quoted in § 3. But, before proving this, we prove a well known

LEMMA 8. Let $\mathfrak{o}$ be a valuation ring with quotient field K. Assume that a field Z is an algebraic normal extension of K with Galois group G. If $\mathfrak{o}'$ is a valuation ring with quotient field Z such that $\mathfrak{o}' \cap K = \mathfrak{o}$,[15] then the intersection $\mathfrak{d} = \bigcap_{\sigma \in G} \mathfrak{o}'^{\sigma}$ is the totality of $\mathfrak{o}$-integers in Z.

Proof. Let $\mathfrak{d}'$ be the totality of $\mathfrak{o}$-integers in Z. Since $\mathfrak{d}$ is integrally closed, it is clear that $\mathfrak{d} \supseteq \mathfrak{d}'$. Conversely, if a is an element of $\mathfrak{d}$, a power of the fundamental symmetric formulas of all distinct conjugates of a is in $\mathfrak{o}$. This shows that a is integral over $\mathfrak{o}$, i.e., $a \in \mathfrak{d}'$. Therefore $\mathfrak{d} = \mathfrak{d}'$.

Proof of the fundamental lemma. First we assume that Z is finite normal over K. Then the theorem of independency of valuations, combined with Lemma 8, shows the validity of our assertion. As for the general case, it is sufficient to show that if $0 \neq a \in Z$ then $a \in \mathfrak{d}_{\mathfrak{p}}$ or $a^{-1} \in \mathfrak{d}_{\mathfrak{p}}$. But this can easily be seen if we consider a finite normal extension of K containing a and contained in Z,[16] since we may assume that Z is normal over K.

Appendix (II)

Here we show an example of Henselian, special, discrete valuation ring $\mathfrak{o}$ such that (1) $\mathfrak{o}$ is not complete, (2) the completion $\bar{\mathfrak{o}}$ of $\mathfrak{o}$ is an almost finite integral extension of $\mathfrak{o}$.

Example. Let $\mathfrak{k}$ be a perfect field of characteristic p ($\neq 0$) and let $z, x_1, \ldots, x_n, \ldots$ be indeterminates. Let $\bar{\mathfrak{o}}$ be the ring of power series of z over $k(x_1, \ldots, x_n, \ldots)$, which is a discrete complete special valuation ring. Let $\bar{K}$ be the quotient field of $\bar{\mathfrak{o}}$. We set $K_0 = \bar{K}^p(z, x_1, \ldots, x_n, \ldots)$.

Then the element $c = \sum_{i=1}^{\infty} x_i z^i$ of $\bar{K}$ is not contained in K_0. Let K be a maximal subfield of $\bar{K}$ among those which contain K_0 and do not contain c. Since the p-th power of an arbitrary element of $\bar{K}$ is in K_0, $\bar{K}$ must be $K(c)$. Now set $\mathfrak{o} = \bar{\mathfrak{o}} \cap K$. Then $\mathfrak{o}$ is evidently a valuation ring and $\bar{\mathfrak{o}}$ is its completion. Thus $\mathfrak{o}$ is a required example.

Remark 1. $\bar{\mathfrak{o}}$ is not finite over $\mathfrak{o}$. For, if $\bar{\mathfrak{o}}$ is finite over $\mathfrak{o}$, $\mathfrak{o}$ must be complete.

Remark 2. The completion of such a valuation ring $\mathfrak{o}$ that is required here is purely inseparable integral extension of $\mathfrak{o}$.

---

[15] This relation means that the valuation given by $\mathfrak{o}'$ is an extension of that given by $\mathfrak{o}$.

[16] Observe [6, Lemma 1].

Bibliography

[1] G. Azumaya, On maximally central algebras, Nagoya Math. Journ. **2** (1950), pp. 119-150.
[2] I. S. Cohen--A. Seidenberg, Prime ideals and integral dependence, Bull. Amer. Math. Soc. **52** (1946), pp. 252-261.
[3] K. Hensel, Theorie der algebraischen Zahlen I, Teubner (1908).
[4] W. Krull, Allgemeine Bewertungstheorie, Jour. reine angew. Math. **167** (1932), pp. 160-196.
[5] W. Krull, Beiträge zur Arithmetik kommutativer Integritätsbereiche III, Math. Zeit. **42** (1936-37), pp. 745-766.
[6] M. Nagata, On Krull's conjecture concerning valuation rings, Nagoya Math. Journ. **4** (1952), pp. 29-33.
[7] A. Ostrowski, Untersuchungen zur arithmetischen Theorie der Körper I, Math. Zeit. **39** (1935), pp. 261-320.
[8] K. Rychilik, Zur Bewertungstheorie der algebraischen Körper, Journ. reine angew. Math. **153** (1924), pp. 94-107.
[9] O. F. G. Schilling, Normal extensions of relatively complete fields, Amer. Journ. Math. **65** (1934), pp. 309-334.

Mathematical Institute,
Nagoya University

Added in Proof. The corollary to Theorem 7 can be generalized as follows:

"Let $\mathfrak{o}$ be an integrally closed quasi-local integrity domain with maximal ideal $\mathfrak{p}$. If $\mathfrak{o}'$ is a Henselian integrity domain with maximal ideal $\mathfrak{p}'$ such that $\mathfrak{o}' \supseteq \mathfrak{o}$ and $\mathfrak{p}' \cap \mathfrak{o} = \mathfrak{p}$, then $\mathfrak{o}'$ contains the Henselization of $\mathfrak{o}$ up to an isomorphism over $\mathfrak{o}$."

This will be proved in a later paper.

https://doi.org/10.1017/S0027763000015439 Published online by Cambridge University Press