ON THE STRUCTURE OF COMPLETE LOCAL RINGS

MASAYOSHI NAGATA

The concept of a local ring was introduced by Krull [2],[0] who defined it as a Noetherian ring R (we say that a commutative ring R is Noetherian if every ideal in R has a finite basis and if R contains the identity) which has only one maximal ideal $\mathfrak{m}$. If the powers of $\mathfrak{m}$ are defined as a system of neighbourhoods of zero, then R becomes a topological ring satisfying the first axiom of countability. And the notion was studied recently by C. Chevalley and I. S. Cohen. Cohen [1] proved the structure theorem for complete rings besides other properties of local rings.

The main purpose of the present paper is to show that the structure theorem holds for rings satisfying somewhat weaker condition; for local rings in the sense of this paper (cf. Definition 1).

Appendix (1) shows some other properties of local rings; they may be considered as generalizations of Lemma 1 and Theorems 4, 7 and 8 in Part I, [1]. Further, Appendix (2) is to show an example of non-Noetherian local ring whose maximal ideal has a finite basis (non-Noetherian generalized local ring in the sense of Cohen [1]).

As for terminology, a ring means, throughout this paper, a commutative ring with identity. Under a subring we mean a subring having the same identity element.

DEFINITION 1. A local ring R is a ring in which (1) the set $\mathfrak{m}$ of non-units form an ideal and (2) $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$.

In any local ring R a topology can be introduced by taking ideals $\mathfrak{m}, \mathfrak{m}^2, \ldots$ to be neighbourhoods of zero. This is the natural topology of a local ring.

DEFINITION 2. An absolutely unramified local ring is a local ring with the maximal ideal (p) where p is zero or a prime number.

DEFINITION 3. If R and R' are two local rings such as (1) R is a subring of R' and (2) non-units in R are non-units in R', then we say that R is a special subring of R'.

LEMMA 1. Any local ring contains at least one absolutely unramified local

Received December 21, 1949.

[0] The number in brackets refers to the bibliography at the end.

ring as a special subring.

Proof. The special subring which is generated by the identity is an absolutely unramified local ring.

LEMMA 2. If a local ring R_0 with the maximal ideal xR_0 is a special subring of a local ring R, then R_0 is a subspace of R.

Proof. We can prove this by the same way as the proof of Theorem 6, [1].

From now on, we shall denote by $\mathfrak{m}$ the maximal ideal in a local ring R. The maximal ideal in an absolutely unramified local ring is denoted by (p), p being 0 or a prime number.

PROPOSITION 1.[1] Let R be a complete local ring and R_0 an absolutely unramified local ring which is a special subring of R. If a^* of $R/\mathfrak{m}$ is separably algebraic or transcendental over $R_0/(p)$, then R contains an absolutely unramified local ring R_0' such as $R_0 \subseteqq R_0'$ and $R_0'/(p) = R/(p)\cdot(a^*)$. [3, Proposition 3, § III] [1, p. 73]

Proof. When a^* is transcendental over $R_0/(p)$ the assertion is evident. If a^* is separably algebraic over $R_0/(p)$, let $F^*(z) = z^n + a_1^* z^{n-1} + \ldots + a_n^*$ be an irreducible polynomial over $R_0/(p)$ such that $F^*(a^*) = 0$. Then $dF^*/dz(a^*) \not\equiv 0$. Let a_i be representatives of a_i^* in R_0 and put $F(z) = z^n + a_1 z^{n-1} \ldots + a_n$. We have $F(\theta) \equiv 0(\mathfrak{m})$ and $dF/dz(\theta) \not\equiv 0(\mathfrak{m})$ for any $\theta \in a^*$. $dF/dz(\theta)$ has an inverse in R, say $a(\theta)$.

If we set $\theta_2 = \theta - a(\theta)F(\theta)$, we have $\theta_2 \in a^*$ and $F(\theta_2) \equiv F(\theta) - a(\theta)F(\theta)dF/dz(\theta) \equiv 0$ (mod. $(F(\theta)^2)$).

Therefore we can construct a convergent sequence (θ_n) such that $\theta_n \in a^*$, $F(\theta_n) \in \mathfrak{m}^n$. Let ζ be its limit. Then $F(\zeta) = 0$ and the special subring generated by R_0 and ζ is the required ring.

By Proposition 1 and Zorn's Lemma, we have: "Let R be a complete local ring. If $R/\mathfrak{m}$ is of characteristic zero, R contains a field K_0 which form a complete set of representatives of R modulo $\mathfrak{m}$. Moreover, if K is a field contained in R as a subring, then we can take K_0 such as $K_0 \supseteqq K$".

Now, we consider the case $R/\mathfrak{m}$ of characteristic $p \not\equiv 0$ (R being also complete)

DEFINITION 4. If $b^* \in R/\mathfrak{m}$, a multiplicative representative of b^* is an element b in R such as $b \in b^*$ and b has a p^k-th root in R for every positive integer k, [4, p. 154]; the terminology will be justified in Lemma 4.

[1] This can be proved also by Hensel's Lemma. Hensel's Lemma holds for complete local rings (cf. Proposition 5, Appendix (1)).

LEMMA 3. Let K be the maximal perfect field contained in $R/\mathfrak{m}$. Then every element of K has one and only one multiplicative representative. [4, p. 154] (The notation K will be used below as the same).

Proof. Let b^* be an element of K. Let b_n' be an element of b^{*1/p^n}. Then the sequence $(b_n) = (b_n'^{p^n})$ is convergent. For, if $a \equiv b \pmod{\mathfrak{m}^h}$, $a = b + c$, $c \in \mathfrak{m}^h$, then $a^p = b^p + pb^{p-1}c + \ldots + c^p \equiv b \pmod{\mathfrak{m}^{h+1}}$, and therefore $b_n = b_n'^{p^n} \equiv b'^{p^{n+1}}_{n+1} = b_{n+1} \pmod{\mathfrak{m}^n}$. Let b be its limit. Then b is a multiplicative representative of b^*. On the other hand if b' is a multiplicative representative of b^*, b' is the limit of the sequence $((b'^{1/p^n})^{p^n})$. Hence $b = b'$.

LEMME 4. Let a and b be the multiplicative representatives of a^* and b^* of K respectively. Then ab is the multiplicative representative of a^*b^*. [4, p. 154]

Proof. Trivial.

LEMMA 5. We can define polynomials $h_0(x,y), h_1(x,y), \ldots$ whose coeficients are rational integers such as

$$x^{p^n} + y^{p^n} = h_0^{p^n} + ph_1^{p^{n-1}} + \ldots + p^{n-1}h_{n-1}^p + p^n h_n, \quad (n = 0,1,\ldots).$$

[4, p. 156]

Proof. Let $h_0(x,y) = x + y$. Assume further that $h_0, \ldots, h_{n-1}$ are defined; $x^{p^n} + y^{p^n} = h_0(x^p, y^p)^{p^{n-1}} + \ldots + p^{n-1}h_{n-1}(x^p, y^p)$. On the other hand, $h_i(x,y)^p \equiv h_i(x^p, y^p) \pmod{p}$ $(i = 1,2,\ldots,n-1)$, whence $p^i h_i(x,y)^{p^{n-1}} \equiv p^i h_i(x^p, y^p)^{p^{n-1-i}} \pmod{p^n}$ $(i = 1,2,\ldots,n-1)$. Therefore $x^{p^n} + y^{p^n} - \sum_{i=0}^{n-1} p^i h_i^{p^{n-i}} \equiv 0 \pmod{p^n}$; we can define h_n by $h_n = (x^{p^n} + y^{p^n} - \sum_{i=0}^{n-1} p^i h_i^{p^{n-i}})/p^n$. Now the lemma is proved by induction.

LEMMA 6. Let a^* and b^* be two element of K with multiplicative representatives a and b respectively. Let $c_n^*(a,b)$ be an element with multiplicative representative $c_n(a,b)$ such as $c_n^{*p^n} = h_n(a^*, b^*)$ with h_i in Lemma 5. Then

$$a + b = \sum_{n=0}^{\infty} c_n(a,b)p^n. \quad [4, \text{p. } 156]$$

Proof. We can write $a^{p^k} + b^{p^k} = \sum_{i=0}^{k} p^i h_i(a,b)^{p^{k-i}}$. On the other hand $h_i(a,b) \equiv c_i(a,b)^{p^i} \pmod{p}$, and therefore $h_i(a,b)^{p^{k-i}} \equiv c_i(a,b)^{p^k} \pmod{p^{k+1-i}}$. Since $c_i(a,b)$ is the multiplicative representative of $h_i(a^*, b^*)^{1/p^n}$, $c_i(a,b)^{p^k}$ is the multiplicative representative of $h_i(a^{*p^k}, b^{*p^k})^{1/p^n}$. Therefore $a^{p^k} + b^{p^k} \equiv \sum_{i=0}^{k} p^i c_i(a^{p^k}, b^{p^k}) \pmod{p^{k+1}}$, i.e., $a + b \equiv \sum_{i=0}^{k} p^i c_i(a,b) \pmod{p^{k+1}}$ for any two $a^*, b^* \in K$. Hence $a + b = \sum_{n=0}^{\infty} p^n c_n(a,b)$.

Note: If $[K]$ is the set of multiplicative representatives of K, we can construct, by virtue of this lemma, a ring $R' = \left\{\sum_{n=0}^{\infty} a_n p^n;\ a_n \in [K]\right\}$; R' is an absolutely unramified local ring of characteristic 0, and furthermore, R' is complete and the special subring R'' generated by $[K]$ in R is a homomorphic image of R', where R'' is of characteristic $p^n (\neq 0)$; otherwise, the completion of R'' is R': i.e., the completion $\overline{R''}$ of R'' is a special subring of R and a homomorphic image of R'.

DEFINITION 5. A p-basis of $R/\mathfrak{m}$ is a set M of elements in $R/\mathfrak{m}$ such that [4, p. 158]:

(1) $[R/\mathfrak{m}(a_1^{*1/p}, \ldots, a_r^{*1/p}) : R/\mathfrak{m}] = p^r$ for any r and for any r distinct elements $a_1^*, \ldots, a_r^* \in M$,

(2) $(R/\mathfrak{m})^p(M) = R/\mathfrak{m}$.

(Existence of M can be proved by Zorn's Lemma).

Let $\mathfrak{M}$ be a system of representatives of p-basis M of $R/\mathfrak{m}$. Since M is a transcendental basis of $R/\mathfrak{m}$ over K, the special subring R_0 generated by $\overline{R''}$ and $\mathfrak{M}$ is an absolutely unramified local ring and $R_0/(p) = R/\mathfrak{m}$. Furthermore, R_0 is a homomorphic image of the ring $\mathfrak{S}$ of quotients of $pR'[\mathfrak{M}]$ with respect to $R'[\mathfrak{M}]$,[2] and the completion $\overline{R_0}$ of R_0 is again an absolutely unramified local ring and a special subring of R. Thus we have

PROPOSITION 2. Let R be a complete local with maximal ideal. Then R contains a complete, absolutely unramified local ring $\overline{R_0}$ such that $\overline{R_0}/(p) = R/\mathfrak{m}$. Therefore R is a homomorphic image of the ring of power series $\overline{R_0}[[x_\lambda;\ \lambda \in \Lambda]]$ in indeterminates $x_\lambda, \lambda \in \Lambda$ with coefficients in $\overline{R_0}$, where $\{x_\lambda, \lambda \in \Lambda\}$ is a basis of the maximal ideal $\mathfrak{m}$ of R. [1, Theorems 9, 11 and 12]

COROLLARY. If the maximal ideal of a complete local ring R has a finite basis, then R is Noetherian. [1, Theorem 3]

Proof. This follows immediately from our proposition and Lemma 8, § 11, [3].

Furthermore, if we observe the fact that any absolutely unramified local ring of characteristic 0 is a valuation ring of the field of quotients of the ring, we have

PROPOSITION 3. An absolutely unramified local ring is a field or a valuation ring or a homomorphic image of a valuation ring. [1, Corollary 3 to Theorem 11]

COROLLARY. A complete, absolutely unramified local ring $\overline{R_0}$ is uniquely de-

[2] As for the notion of the ring of quotients of a prime ideal, see § 1, [3].

termined (up to an isomorphism) when the residue field $\overline{R}_0/(\bar{p})$ and the characteristic of $\overline{R}_0$ are given.

Proof. When $\overline{R}_0$ is a field, our assertion is trivial. Therefore it is sufficient to prove the uniqueness of such a ring R when $p \neq 0$ and the characteristic of R is 0. If the case is so, our assertion follows from the above construction of $\overline{R}_0$ (in the proof of Proposition 2).

Appendix (1)

Proposition 4[3]. Let R be a ring with the intersection $\mathfrak{m}$ of all maximal ideals. Let M be a finite R-module. Then if $M\mathfrak{m} = M$, $M = (0)$.

Proof. Let $M = (u_1, \ldots, u_n)$. Then we have $u_i = \sum_{j=1}^{n} a_{ij}u_j$, $a_{ij} \in \mathfrak{m}$ $(1 \leqq i \leqq n)$. Let d be the determinant $|\delta_{ij} - a_{ij}|$. Then $d \equiv 1 \pmod{\mathfrak{m}}$. Therefore d is a unit in R. On the other hand $du_j = 0$ for each j. Therefore $u_j = 0$ for each j.

Corollary. Let R and $\mathfrak{m}$ be the same as above. Let M be a finite R-module. If N is a sub-R-module of M such as $N + M\mathfrak{m} = M$, then $M = N$. [1, Lemma 1, Part I]

Proof. Let $\overline{M} = M/N$. Then $\overline{M}\,\mathfrak{m} = \overline{M}$ and M is a finite R-module. Therefore $\overline{M} = (0)$, i.e., $M = N$.

Proposition 5.[4] Let R be a comolete local ring with the maximal ideal $\mathfrak{m}$. Let $f(z)$ be a polynomial of degree n in $R[z]$. If there exist polynomials $g_0(z)$ and $h_0(z)$ such that

(1) $f(z) \equiv g_0(z)h_0(z) \pmod{\mathfrak{m}}$,

(2) $g_0(z) = a_0z^r + a_1z^{r-1} + \ldots + a_r$, where $a_0 \notin \mathfrak{m}$, and $h_0(z)$ is of degree not greater than $n - r$,

(3) $(g_0(z), h_0(z), \mathfrak{m}) = R$,

then there exist $g(z)$ and $h(z)$ in $R[z]$ such as

(1) $f(z) = g(z)h(z)$,

(2) $g(z) = a_0z^r + a_1'z^{r-1} + \ldots + a_r'$, $h(z)$ is of degree not greater than $n - r$, and

(3) $g(z) \equiv g_0(z) \pmod{\mathfrak{m}}$, $h(z) \equiv h_0(z) \pmod{\mathfrak{m}}$.

---

[3] This holds for non-commutative rings too, if we denote by $\mathfrak{m}$ the radical of R in the sense of Jacobson, as was communicated by Prof. G. Azumaya.

[4] This can be generalized for generalized semi-local rings in the sense of Nagata [5]; and further for non-commutative case. The latter was communicated to me by Prof. G. Azumaya.

Proof. Starting with $g_0(z)$ and $h_0(z)$, we construct two sequences $(g_k(z))$ and $(h_k(z))$ such as

(a) $g_{k+1}(z) \equiv g_k(z) \pmod{\mathfrak{m}^{k+1}}$, $h_{k+1}(z) \equiv h_k(z) \pmod{\mathfrak{m}^{k+1}}$ and $f(z) \equiv g_k(z)h_k(z) \pmod{\mathfrak{m}^k}$, and

(b) $g_k(z) = a_0z^r + a_{1,k}z^{r+1} + \ldots + a_{r,k}$, degree of $h_k(z) \leqq n - r$.

If $g_0, \ldots, g_k$ and $h_0, \ldots, h_k$ are already defined then we write

$$f(z) - g_k(z)h_k(z) = \sum_{i=0}^{n} \alpha_i z^i, \quad \alpha_i \in \mathfrak{m}^k.$$

We can fined $r_i(z)$ and $s_i(z)$ in $R[z]$ such as $z^i \equiv r_ih_0 + s_ig_0 \pmod{\mathfrak{m}}$ $(0 \leqq i \leqq n)$. Since a_0 is a unit in R, we can take r_i such as the degree of $r_i < r$; then the degree of $s_i \leqq n - r$.

Let $g_{k+1}(z) = g_k(z) + \sum_{i=0}^{n} \alpha_i r_i(z)$, $h_{k+1}(z) = h_k(z) + \sum_{i=1}^{n} \alpha_i s_i(z)$.

Then $f(z) - g_{k+1}(z)h_{k+1}(z) \equiv f(z) - g_k(z)h_k(z) - \sum_{i=1}^{u} \alpha_i(r_i(z)h_k(z) + s_i(z)g_k(z))$ $\equiv 0 \pmod{\mathfrak{m}^{k+1}}$. The other condition in (a) and (b) are clearly satisfied.

Let $g(z)$ and $h(z)$ be the limits of $(g_k(z))$ and $(h_k(z))$ respectively, then they are the required polynomials.

PROPOSITION 6. Let R be a complete local ring with maximal ideal $\mathfrak{m}$ and R' an integral domain containing R (from this assumption, it follows that R is a subring of R'). If R' is integrally dependent on R[5], then the non-units in R' form an ideal. If R' is a finite R-module, then R' is a complete local ring. [1, Theorem 7]

Proof. When the first assertion is proved, the second part follows immediately from Proposition 9, Chapter II, [5]. So we will prove the first part.

By Lemma 2, Chapter II, [5], $\mathfrak{m}R' \neq R'$. Let $\mathfrak{m}'$ be the radical of the ideal $\mathfrak{m}R'$. We will show that $\mathfrak{m}'$ contains all non-units in R'. Let u be a non-unit in R'. Then there exists $f(z) = z^m + a_1z^{m-1} + \ldots + a_m, a_i \in R$, such that $f(u) = 0$; where we can assume that u does not satisfy any monic equation of lower degree. Since u is a non-unit, a_m is a non-unit, hence $a_m \in \mathfrak{m}$. If $a_r \notin \mathfrak{m}$, $a_j \in \mathfrak{m}$ for $m \geqq j > r$ $(0 < r \leqq m)$, $f(z) \equiv z^{n-r}(z^r + \ldots + a_r) \pmod{\mathfrak{m}}$ and these factors are relatively prime modulo $\mathfrak{m}$. Proposition 5 (Hensel's Lemma) implies that $f(z)$ factors into monic polynomials of respective degree r and $m - r$. But this implies that u satisfies a monic equation of degree lower than m, contrary to our assumption. Therefore $a_i \in \mathfrak{m}$, $(i = 1, 2, \ldots, m)$. This shows $u^m \in \mathfrak{m}R'$, i.e., $u \in \mathfrak{m}'$.

LEMMA 7. Let K be a field contained in a Noetherian primary ring R with

[5] We say that R' is integrally dependent on R, if every element of R' satisfies a suitable monic equation with coefficients in R.

maximal ideel $\mathfrak{m}$. If $[R/\mathfrak{m} : K] = \mu < \infty$, then R has a K-basis of $\lambda\mu$ elements, where λ is the length of zero-ideal in R.

Proof. This is a special case of Theorem 8, [1].

PROPOSITION 7. Let R be a complete local ring with maximal ideal $\mathfrak{m}$. Let R' be a local ring with maximal ideal $\mathfrak{m}'$ which contains R as a subring. Then R' is a finite R-module if and only if $R'/\mathfrak{m}'$ is a finite algebraic extension over $R/\mathfrak{m}$ and $\mathfrak{m}R'$ is a primary ideal of a finite length belonging to $\mathfrak{m}'$. With these conditions are satisfied, R' is complete and has an R-basis of $\lambda\mu$ elements, where $\mu = [R'/\mathfrak{m}' : R/\mathfrak{m}]$ and λ is the length of $\mathfrak{m}R'$.

Proof. It is clear that if R' is a finite R-module, $\mathfrak{m}R' \neq R'$ and $R'/\mathfrak{m}R'$ is a finite $R/\mathfrak{m}$-module by Proposition 9, Chapter II, [5]. Then $R'/\mathfrak{m}R'$ is a primary ring. Since $R/\mathfrak{m}$ is a field and $R'/\mathfrak{m}R'$ is finite over $R/\mathfrak{m}$, $R'/\mathfrak{m}R'$ satisfies the maximal, therefore also minimal, condition for ideels. Therefore $\mathfrak{m}R'$ is a primary ideal having a finite length.

Conversely, if $[R'/\mathfrak{m}' : R/\mathfrak{m}] = \mu$ and $\mathfrak{m}R'$ is a primary ideal of length λ belonging to $\mathfrak{m}'$, $R'/\mathfrak{m}R'$ has an $R/\mathfrak{m}$-basis of $\lambda\mu$ elements, by Lemma 7. By Proposition 10, Chapter II, [5], R' has an R-basis of $\lambda\mu$ elements. The completeness of R' follows from Proposition 9, Chapter II, [5].

APPENDIX (2): An example of non-Noetherian local ring whose maximal ideal has a finite basis.

Let K be a field and x and y two indeterminates. Let R be the special subring of the ring of power series $K(\!(x,y)\!)$ which is generatated by $K[x,y]$ and $xK(\!(x,y)\!)$. Then:

(1) R is a local ring with the maximal ideal $(x,y)R$.

Proof. Let u_1 be a non-unit in R. Then there exists an unit α in R such as $u = \alpha u_1 \in K[x,y] + xK(\!(x,y)\!)$: $u = fy + x\sum_{i=0,j=0}^{\infty} \alpha_{ij}x^iy^j$, $\alpha_{ij} \in K$, $f \in K[x,y]$: $u \equiv x\sum_{i,j} \alpha_{ij}x^iy^j \pmod{yR}$, $x\sum_{i,j} \alpha_{ij}x^iy^j = x(x\sum_{i=1,j=0}^{\infty} \alpha_{ij}x^{i-1}y^j) + \alpha_{00}x + y(\sum_{j=1}^{\infty}\alpha_{0j}y^{j-1}) \in (x,y)R$.

(2) R is a subspace of $K(\!(x,y)\!)$.

Proof. Let $u(\in R)$ be an element of $(x,y)^kK(\!(x,y)\!)$. We will show that $u \in (x,y)^kR$, by induction.

We can assume without loss of generality that $u \in K[x,y] + xK(\!(x,y)\!)$. Further, we can assume that our assertion holds for $k-1$, by virtue of (1) above. Then: $u = fy^k + x\sum_{i+j\geqq k-1} \alpha_{ij}x^iy^j$, $f \in K[x,y]$, $\alpha_{ij} \in K$. $u \equiv x\sum_{i+j\geqq k-1, j<k} \alpha_{ij}x^iy^j \equiv x^k\sum_{i\geqq k-1} \alpha_{i0}x^{i-k+1} + x^{k-1}y\sum_{i\geqq k-2} \alpha_{i1}x^{i-k+2} + \cdots + xy^{k-1}\sum_{i\geqq 0} \alpha_{ik-1}x^i \equiv x^k(x\sum_{i\geqq k} \alpha_{i0}x^{i-k})$

$$+ x^{k-1}y(x\sum_{i\geqq k-1}\alpha_{i1}x^{i-k+1}) + \cdots + xy^{k-1}(x\sum_{i\geqq 1}\alpha_{i,k-1}x^{i-1}) \equiv 0 \pmod{(x,y)^kR}.$$

(3) $R \neq K[\![x,y]\!]$; the completion of R is $K[\![x,y]\!]$.

Proof. There exists at least one element Y such as $Y \in K[\![y]\!]$ and $Y \notin R$ because the ring of quotients of $yK[y]$ with respect to $K[y]$ is not complete. The else is evident.

(4) R is not Noetherian.

Proof. The ideal xR does not contain xY, if $Y \in K[\![y]\!]$ and $Y \notin R$. Therefore xR is not closed in R.

Bibliography

[1] I. S. Cohen; On the structure and ideal theory of complete local rings, Trans. Amer. Math. Soc. Vol. **59**, No. 1, pp. 54-106 (1946).

[2] W. Krull; Dimensionstheorie in Stellenringen, J. Reine Angew. Math. Vol. **179**, pp. 204-226 (1938).

[3] C. Chevalley; On the theory of local rings, Ann. of Math. Vol. **44**, pp. 690-708 (1943).

[4] O. Teichmüller; Über die Struktur diskrete bewerteter perfect Körper, Ges. d. Wiss. Nachrichten Math. -Phys. Kl. Fachgr. I.N.F. Vol. **1**, No. 10, pp. 151-161 (1936).

[5] M. Nagata; On the theory of semi-local rings, forthcoming.

Nagoya University