82. Elementary Proof of the Unique Factorization Theorem in Regular Local Rings

By Masao NARITA

International Christian University, Mitaka, Tokyo

(Comm. by Z. SUETUNA, M.J.A., July 12, 1961)

As is well known, the proof of the unique factorization theorem in regular local rings of dimension d is trivial for $d=1, 2$. The case $d\geq 4$ was reduced to the case $d=3$ by Zariski-Nagata [2], and the case $d=3$ was proved by Auslander-Buchsbaum [1]. The proofs in [1], [2] depend on homological method. The author gave an ideal-theoretic proof of the result of [2] in [3]. The purpose of the present paper is to show that also the result of [1] can be proved in an elementary way, without referring to any general theory of homological algebra, along the same idea as in [3].*)

For the convenience of proof, we shall state here the following well-known propositions without any proof.

Proposition 1. Let F be a finite free module over a Noetherian ring, then every submodule of F has a finite base.

Proposition 2. Let M be a finite module over a local ring Q. Let M_0 be a submodule of M, and $\mathfrak{a}$ a proper ideal of Q. If $M\subseteq M_0+\mathfrak{a}M$, then $M=M_0$.

We first prove the following lemmas.

Lemma 1. Let $\mathfrak{q}$ be a primary ideal belonging to the maximal ideal $\mathfrak{m}=Qu+Qv$ of a regular local ring Q of dimension 2. If $\mathfrak{q}$ includes u, then there exists an element b of $\mathfrak{q}$ such that $\mathfrak{q}=Qb+Qu$.

Proof. Since the residue ring $\overline{Q}=Q/Qu$ is a one-dimensional regular local ring, it follows that $\overline{\mathfrak{q}}=\mathfrak{q}/Qu$ is a principal ideal of $\overline{Q}$, whence follows the conclusion.

Lemma 2. Let $\mathfrak{q}$ be a primary ideal belonging to the maximal ideal $\mathfrak{m}$ of a regular local ring Q of dimension 2, and let $\{a_1, a_2, \cdots, a_n\}$ be its minimal base. Let $X_1, X_2, \cdots, X_n$ be indeterminates, and $F=QX_1+QX_2+\cdots+QX_n$ a free module over Q. Let $0\rightarrow R\rightarrow F\underset{\varphi}{\rightarrow}\mathfrak{q}\rightarrow 0$ be an exact sequence, where φ induces the mapping $\varphi(X_i)=a_i; i=1, 2, \cdots, n$. Then R is a free module over Q.

Proof. It is evident that there exists an element u of a minimal base of $\mathfrak{m}$ such that $a_1, a_2, \cdots, a_n \notin Qu$. Let $\mathfrak{a}_1=Qa_2+Qa_3+\cdots+Qa_n$, $\mathfrak{a}_2=Qa_3+Qa_4+\cdots+Qa_n$, $\cdots$, $\mathfrak{a}_{n-2}=Qa_{n-1}+Qa_n$, $\mathfrak{a}_{n-1}=Qa_n$, then $\mathfrak{a}_1+\mathfrak{q}u$,

*) Recently Nagata proved syzygy theory of local rings without using homological algebra. His book including the theory is in press.

$\mathfrak{a}_2+\mathfrak{q}u,\cdots,\mathfrak{a}_{n-2}+\mathfrak{q}u,\mathfrak{a}_{n-1}+\mathfrak{q}u$ are $\mathfrak{m}$-primary ideals. From Lemma 1, it follows that there exist $b_1, b_2, b_3,\cdots, b_{n-1}$ satisfying:

$$\mathfrak{a}_1+\mathfrak{q}u : a_1=Qb_1+Qu$$
$$\mathfrak{a}_2+\mathfrak{q}u : a_2=Qb_2+Qu$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$\mathfrak{a}_{n-1}+\mathfrak{q}u : a_{n-1}=Qb_{n-1}+Qu.$$

Adding to b_i some quantity which belongs to Qu if necessary, we can assume that those $b_1, b_2, b_3,\cdots, b_{n-1}$ satisfy the following equations:

$$b_1a_1+c_{12}a_2+c_{13}a_3+\cdots+c_{1n-1}a_{n-1}+c_{1n}a_n=0$$
$$uc_{21}a_1+b_2a_2+c_{23}a_3+\cdots+c_{2n-1}a_{n-1}+c_{2n}a_n=0$$
$$uc_{31}a_1+uc_{32}a_2+b_3a_3+\cdots+c_{3n-1}a_{n-1}+c_{3n}a_n=0$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$uc_{n-11}a_1+uc_{n-12}a_2+uc_{n-13}a_3+\cdots+b_{n-1}a_{n-1}+c_{n-1n}a_n=0.$$

Let $\alpha_1,\alpha_2,\alpha_3,\cdots,\alpha_{n-1}$ be elements of F such that

$$\alpha_1=b_1X_1 + c_{12}X_2 + c_{13}X_3+\cdots+c_{1n-1}X_{n-1}+c_{1n}X_n$$
$$\alpha_2=uc_{21}X_1+b_2X_2 + c_{23}X_3+\cdots+c_{2n-1}X_{n-1}+c_{2n}X_n$$
$$\alpha_3=uc_{31}X_1+uc_{32}X_2+b_3X_3+\cdots+c_{3n-1}X_{n-1}+c_{3n}X_n$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$\alpha_{n-1}=uc_{n-11}X_1+uc_{n-12}X_2+uc_{n-13}X_3+\cdots+b_{n-1}X_{n-1}+c_{n-1n}X_n$$

then it is clear that these $\alpha_1,\alpha_2,\cdots,\alpha_{n-1}$ belong to R.

We shall prove that $\{\alpha_1,\alpha_2,\cdots,\alpha_{n-1}\}$ is a free basis of R. In fact, it is obvious from the definition that

$$R\subseteq Q\alpha_1+R\cap(QuX_1+QX_2+\cdots+QX_{n-1}+QX_n)$$
$$R\cap(QuX_1+QX_2+\cdots+QX_n)$$
$$\subseteq Q\alpha_2+R\cap(QuX_1+QuX_2+QX_3+\cdots+QX_n)$$
$$R\cap(QuX_1+QuX_2+QuX_3+\cdots+QX_n)$$
$$\subseteq Q\alpha_3+R\cap(QuX_1+QuX_2+QuX_3+QX_4+\cdots+QX_n)$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$R\cap(QuX_1+\cdots+QuX_{n-2}+QX_{n-1}+QX_n)$$
$$\subseteq Q\alpha_{n-1}+R\cap(QuX_1+\cdots+QuX_{n-2}+QuX_{n-1}+QX_n).$$

Moreover, it is clear that

$$R\cap(QuX_1+\cdots+QuX_{n-1}+QX_n)$$
$$\subseteq R\cap(QuX_1+\cdots+QuX_{n-1}+QuX_n)=R\cap uF=uR.$$

Hence we have $R\subseteq Q\alpha_1+Q\alpha_2+\cdots+Q\alpha_{n-1}+uR$.

From Proposition 2, it follows that $R=Q\alpha_1+Q\alpha_2+\cdots+Q\alpha_{n-1}$.

In order to prove that $\{\alpha_1,\alpha_2,\cdots,\alpha_{n-1}\}$ is free, we shall consider the following equation:

$$x_1\alpha_1+x_2\alpha_2+\cdots+x_{n-1}\alpha_{n-1}=0\,;\ x_i\in Q.$$

Comparing the coefficients of X_1, we have $x_1\in Qu$. Using this result and comparing the coefficients of X_2, we have $x_2 \in Qu$, and so on. Thus we have $x_i = y_i u$; $i=1, 2, \cdots, n-1$. Therefore we have

$$y_1\alpha_1 + y_2\alpha_2 + \cdots + y_{n-1}\alpha_{n-1} = 0;\ y_i \in Q.$$

Repeating this procedure, we have $y_i \in Qu$, $x_i \in Qu^2$, and so on. Therefore we see easily that $x_i \in \bigcap_{k=1}^{\infty} Qu^k = 0$. Hence R is a free module.

Lemma 3. Let $\mathfrak{a}$ be any ideal ($\mathfrak{m}$-primary or not) of a regular local ring Q of dimension 2. Then the same result as Lemma 2 holds.

Proof. It is enough to prove the lemma when the rank of $\mathfrak{a}$ is one. The regular local ring Q of dimension 2 is a unique factorization ring. Since we assumed that $\mathfrak{a}$ is of rank 1, it follows that there exists the greatest common measure c of $a_1, a_2, \cdots, a_n$, where $\{a_1, a_2, \cdots, a_n\}$ is a minimal base of $\mathfrak{a}$. Therefore we have $\mathfrak{a} = \mathfrak{q}c$, where $\mathfrak{q} = Qb_1 + Qb_2 + \cdots + Qb_n$; $a_i = b_i c$. It is clear that this $\mathfrak{q}$ is an $\mathfrak{m}$-primary ideal or Q itself. (When $\mathfrak{a}$ is principal, $\mathfrak{q}$ is Q itself.) The rest of proof follows from the above Lemma 2.

Lemma 4. Let Q be a regular local ring of dimension 3, and $\mathfrak{m}$ its maximal ideal. Let $\mathfrak{a}$ be an ideal of Q such that $\mathfrak{a} : \mathfrak{m} = \mathfrak{a}$. (Clearly the rank of $\mathfrak{a}$ is one or two at most.) Let $\{a_1, a_2, \cdots, a_n\}$ be a minimal base of $\mathfrak{a}$. Let $X_1, X_2, \cdots, X_n$ be indeterminates, and $F = QX_1 + QX_2 + \cdots + QX_n$ a free module over Q. Let $0 \to R \to F \underset{\varphi}{\to} \mathfrak{a} \to 0$ be an exact sequence, where φ induces the mapping $\varphi(X_i) = a_i$. Then R is a free module over Q.

Proof. If $n=1$, then the lemma is trivial. Now we shall assume that $n \geqq 2$. Let u be an element of a minimal base of the maximal ideal $\mathfrak{m}$ of Q such that $\mathfrak{a} : u = \mathfrak{a}$. Let ψ be a natural homomorphism of Q onto $\overline{Q} = Q/Qu$, and let $\overline{a}_i = \psi(a_i)$. Then $\{\overline{a}_1, \overline{a}_2, \cdots, \overline{a}_n\}$ is a minimal base of $\overline{\mathfrak{a}} = \psi(\mathfrak{a})$. Let $Y_1, Y_2, \cdots, Y_n$ be indeterminates, and $\overline{F} = \overline{Q}Y_1 + \overline{Q}Y_2 + \cdots + \overline{Q}Y_n$ be a free module over $\overline{Q}$. Let $0 \to \overline{R} \to \overline{F} \underset{\overline{\varphi}}{\to} \overline{\mathfrak{a}} \to 0$ be an exact sequence, where $\overline{\varphi}$ induces $\overline{\varphi}\ (Y_i) = \overline{a}_i$. From Lemma 3, it follows that $\overline{R}$ has a free basis. Let $\{\overline{\alpha}_1, \overline{\alpha}_2, \cdots, \overline{\alpha}_{n-1}\}$ be the free basis of $\overline{R}$. It is clear that we can extend naturally the homomorphism $\psi: Q \to \overline{Q}$ to the homomorphism of the Q-module F onto the $\overline{Q}$-module $\overline{F}$, i.e. $\psi(\Sigma c_i X_i) = \Sigma \psi(c_i) Y_i$.

From the definition of the submodule R and $\overline{R}$ of F and $\overline{F}$, it follows evidently that $\psi(R) \subseteq \overline{R}$. We first show that $\psi(R) = \overline{R}$. In fact, if $\overline{\alpha} = \overline{c}_1 Y_1 + \overline{c}_2 Y_2 + \cdots + \overline{c}_n Y_n$ belongs to $\overline{R}$, i.e. $\overline{c}_1\overline{a}_1 + \overline{c}_2\overline{a}_2 + \cdots + \overline{c}_n\overline{a}_n = 0$, then there exists an element β of F such that $\beta = c_1 X_1 + c_2 X_2 + \cdots + c_n X_n$, where $\psi(c_i) = \overline{c}_i$. Obviously we have $\psi(\beta) = \overline{\alpha}$. Since $\psi(c_1 a_1 + c_2 a_2 + \cdots + c_n a_n) = 0$, it follows that $c_1 a_1 + c_2 a_2 + \cdots + c_n a_n \in Qu \cap \mathfrak{a} = \mathfrak{a}u$. Therefore there exist elements $d_1, d_2, \cdots, d_n$ such that $(c_1$

$+ud_1)a_1+(c_2+ud_2)a_2+\cdots+(c_n+ud_n)a_n=0$. Let $\alpha=(c_1+ud_1)X_1+(c_2+ud_2)X_2+\cdots+(c_n+ud_n)X_n$, then obviously $\alpha\in R$ and $\psi(\alpha)=\psi(\beta)=\bar{\alpha}$. Thus we conclude that the mapping of R into $\bar{R}$ is surjective.

Let $\{\bar{\alpha}_1,\bar{\alpha}_2,\cdots,\bar{\alpha}_{n-1}\}$ be a free basis of $\bar{R}$, and let $\{\alpha_1,\alpha_2,\cdots,\alpha_{n-1}\}$ be a set of elements of R such that $\psi(\alpha_i)=\bar{\alpha}_i$. We first show that those $\alpha_1,\alpha_2,\cdots,\alpha_{n-1}$ generate R. Since $\psi(R)=\bar{R}=\bar{Q}\bar{\alpha}_1+\bar{Q}\bar{\alpha}_2+\cdots+\bar{Q}\bar{\alpha}_{n-1}$, we have $\psi(R)=\psi(Q\alpha_1+Q\alpha_2+\cdots+Q\alpha_{n-1})$, therefore $R\subseteq Q\alpha_1+Q\alpha_2+\cdots+Q\alpha_{n-1}+R\cap uF=Q\alpha_1+Q\alpha_2+\cdots+Q\alpha_{n-1}+uR$. From Proposition 2, it follows that $R=Q\alpha_1+Q\alpha_2+\cdots+Q\alpha_{n-1}$. Now we shall show that $\{\alpha_1,\alpha_2,\cdots,\alpha_{n-1}\}$ is a free basis of R. For the purpose, we shall consider the equation: $x_1\alpha_1+x_2\alpha_2+\cdots+x_{n-1}\alpha_{n-1}=0;\ x_i\in Q$. Since $\{\bar{\alpha}_1,\bar{\alpha}_2,\cdots,\bar{\alpha}_{n-1}\}$ is a free basis of $\bar{R}=\psi(R)$, it follows that $\bar{x}_1=\bar{x}_2=\cdots=\bar{x}_{n-1}=0$. Hence we have $x_i\in Qu$. Let $x_i=y_iu;\ y_i\in Q$, then we have $y_1\alpha_1+y_2\alpha_2+\cdots+y_{n-1}\alpha_{n-1}=0$. By the same procedure, we conclude that $y_i\in Qu$, i.e. $x_i\in Qu^2$. Repeating this procedure, we can easily see that $x_i\in\bigcap_{k=1}^{\infty}Qu^k=0$. Therefore $\{\alpha_1,\alpha_2,\cdots,\alpha_{n-1}\}$ is a free basis of R. Thus the lemma is proved.

From Lemma 4, the following theorem follows immediately. (See [1].)

Theorem (Auslander-Buchsbaum). A regular local ring of dimension 3 is a unique factorization ring.

References

[1] A. Auslander and D. A. Buchsbaum: Unique factorization in regular local rings, Proc. Nat. Acad. Sci., U.S.A., **45**, 733–734 (1959).

[2] M. Nagata: A general theory of algebraic geometry over Dedekind domains, II, Amer. J. Math., **80**, 382–420 (1958).

[3] M. Narita: On the unique factorization theorem in regular local rings, Proc. Japan Acad., **35**, 329–331 (1959).