182. *Finite Automorphism Groups of Restricted Formal Power Series Rings*

By Akira ENDÔ
Department of Mathematics, Shimane University

(Comm. by Kenjiro SHODA, M. J. A., Dec. 12, 1969)

1. A formal power series $f=\sum_{i=0}^{\infty} a_i X^i$ with coefficients in a linearly topological ring A is called a restricted formal power series if the sequence of its coefficients $\{a_i\}$ converges to 0. All of such formal power series forms a subring of the formal power series ring $A[[X]]$, which is called a restricted formal power series ring and denoted by $A\{X\}$.

In [5], Samuel has obtained the following result:

Let A be a Noetherian complete local integral domain, and G a finite group consisting of A-automorphisms of $A[[X]]$. Then there exists a formal power series f such that the G-invariant subring of $A[[X]]$ is $A[[f]]$.

This is a generalization of the result of Lubin [2] which dealt with the case where A is the ring of $\mathfrak{p}$-adic integers and G is given by using a formal group law.

The main purpose of this paper is to prove the following:

Theorem. *Let A be a Noetherian complete integral domain with the maximal ideal $\mathfrak{m}$, and G a finite group consisting of A-automorphisms of $A\{X\}$. If the residue class field $A/\mathfrak{m}$ is perfect, there exists a series $f\in A\{X\}$ such that the G-invariant subring $A\{X\}^G$ of $A\{X\}$ is $A\{f\}$.*

2. At first, we shall show some results concerning $A\{X\}$.

Lemma 1. *Let A be a linearly topological ring whose topology is complete and T_0. Then, $A\{X+a\}=A\{X\}$ for any $a\in A$.*

Proof. For any $f=\sum_{i=0}^{\infty} a_i(X+a)^i\in A\{X+a\}$, we have $f=\sum_{i=0}^{\infty} b_iX^i$ in $A[[X]]$, where $\{b_i\}$ converges to 0. Hence, $f\in A\{X\}$.

If $\mathfrak{a}$ is an ideal of A, by $\mathfrak{a}\{X\}$ we denote the ideal of $A\{X\}$ consisting of all series $\sum_{i=0}^{\infty} a_iX^i$, $a_i\in\mathfrak{a}$.

Lemma 2. *Let A be a linearly topological ring whose topology is complete and T_0. Let $\mathfrak{m}$ be a closed ideal of A such that every $m\in\mathfrak{m}$ is topologically nilpotent. If $f\in A\{X\}$ is a series such that $\bar{f}=f$* mod *$\mathfrak{m}\{X\}$ is a unitary polynomial with the degree $s\geqq 1$, then $A\{X\}$ is the* *finite module over its subring* $A\{f\}$ *with the free base* $\{1, X, \cdots, X^{s-1}\}$.

Proof. Let M be the $A\{f\}$-module with the free base $\{1, X, \cdots, X^{s-1}\}$. Let $\{\mathfrak{m}_\lambda\}$ be a family of ideals which defines the topology in A. Since by Lemma 1 we can assume that $f(0)=0$, we have $f^n\mathfrak{m}_\lambda\{X\}\subset X^n\mathfrak{m}_\lambda\{X\}$ for any n and λ. Therefore $A\{X\}$ is complete and T_0 with respect to the topology defined by $\{f^n\mathfrak{m}_\lambda\{X\}\}$, i.e. $A\{X\} =\varprojlim_{n,\lambda} A\{X\}/f^n\mathfrak{m}_\lambda\{X\}$. M is complete and T_0 with respect to the topology as a finite $A\{f\}$-module, i.e. $M=\varprojlim_{n,\lambda} M/f^n\mathfrak{m}_\lambda\{X\}M$. In [4], Salmon has proved the preparation theorem for $A\{X\}$: For any $g\in A\{X\}$ there exists a unique $h\in A\{X\}$ such that g-fh is a polynomial with the degree at most $s-1$. In its proof it is shown that if $\mathfrak{a}$ is an ideal of A and $g\in\mathfrak{a}\{X\}$ then $h\in\mathfrak{a}\{X\}$. Therefore, for any n and for any pair λ, μ such that $\mathfrak{m}_\lambda\supset\mathfrak{m}_\mu$, $f^n\mathfrak{m}_\lambda\{X\}/f^{n+1}\mathfrak{m}_\lambda\{X\}$ is isomorphic to $f^n\mathfrak{m}_\lambda\{f\}M/f^{n+1}\mathfrak{m}_\mu\{X\}M$ as an $A\{f\}$-module. Hence, it follows from Lemma 2 of [6] (p. 89) that $A\{X\}$ is isomorphic to M.

A-automorphisms of $A\{X\}$ are characterized as follows:

Proposition 1. *Let A be a local integral domain with the maximal ideal $\mathfrak{m}$. If A is complete and T_0, then any A-automorphism ψ of $A\{X\}$ is given as follows;*

$$\begin{cases}\psi X=a_0+a_1X+a_2X^2+a_3X^3+\cdots\in A\{X\},\\ \qquad \textit{where } a_0\in A,\ a_1\in A-\mathfrak{m},\ \textit{and } a_i\in\mathfrak{m}\ \textit{if } i\geqq 2,\\ \textit{and}\\ \psi a=a\ \textit{if } a\in A.\end{cases}$$

Proof. ψ is an A-automorphism of $A\{X\}$ if and only if $A\{\psi X\} =A\{X\}$ since $\psi A\{X\}=A\{\psi X\}$. By Lemma 1 we can assume that $\psi X\notin\mathfrak{m}\{X\}$. Let s be the degree of $\psi X \bmod \mathfrak{m}\{X\}$. If $s=0$, then ψX is inversible in $A\{X\}$ [4]. Then it follows from Lemma 2 that ψ is an A-automorphism if and only if $s=1$.

The following two lemmas will be used to prove Proposition 2.

Lemma 3. *Let R be a Noetherian complete local integral domain with the completion R^*. If R^* is an integrally closed integral domain, then R is also integrally closed.*

Proof. This is a well-known result (for example, see [3], p. 135).

Lemma 4. *Let R be an integrally closed integral domain with the maximal ideal $\mathfrak{m}$, K the quotient field, and k the residue class field of R mod $\mathfrak{m}$: $k=R/\mathfrak{m}$. If $f\in R[X]$ is an irreducible unitary polynomial such that $\bar{f}=f \bmod (\mathfrak{m})\in k[X]$ is irreducible and separable, then $R'=R[X]/(f)$ is the integral closure of R in $L=K[X]/(f)$ and is a local ring with the maximal ideal $\mathfrak{m}R'$.*

Proof. Since the maximal ideal of R' corresponds to the irreducible component of $\bar{f}$, it is obvious that R' is a local ring. If R^*

is the integral closure of R in L, we have $dR^* \subset R' \subset R^*$ where d is the discriminant of f. Since $\bar{f}$ is separable, d is not in $\mathfrak{m}$. Hence, it follows that $R' = R^*$.

Proposition 2. *Let A be a Noetherian integrally closed complete local integral domain with the maximal ideal $\mathfrak{m}$. If the residue class field $k = A/\mathfrak{m}$ is perfect, then $A\{X\}$ is integrally closed*

Proof. Since $\mathfrak{m}\{X\}$ is the Jacobson radical of $A\{X\}$ [4] and $A\{X\}/\mathfrak{m}\{X\} = k[X]$, every maximal ideal $\mathfrak{M}$ of $A\{X\}$ is in the form of $\mathfrak{M} = (\mathfrak{m}, f)A\{X\}$, where $f \in A[X]$ is a unitary polynomial such that $\bar{f} = f \bmod \mathfrak{m}\{X\} \in k[X]$ is irreducible. We have $A\{X\} = \bigcap_f A\{X\}_{(\mathfrak{m}, f)}$, where f runs the set of polynomials in $A[X]$ satisfying the above conditions. $A\{X\}$ is integrally closed if and only if $A\{X\}_{(\mathfrak{m}, f)}$ is integrally closed for all f. If $f = X$, the completion of the local ring $A\{X\}_{(\mathfrak{m}, X)}$ is $A[[X]]$ which is integrally closed. It follows from Lemma 3 that $A\{X\}_{(\mathfrak{m}, X)}$ is integrally closed. If $f = X^s + a_{s-1}X^{s-1} + \cdots + a_1X + a_0$, then by Lemma 2 we have $A\{X\} = A\{f\}[T]/(T^s + a_{s-1}T^{s-1} + \cdots + a_1T + a_0 - f)$. Now, by Lemma 4, $A\{X\}_{(\mathfrak{m}, f)}[T]/(T^s + a_{s-1}T^{s-1} + \cdots + a_1T + a_0 - f)$ is a local ring with the maximal ideal generated by $(\mathfrak{m}, f)$, i.e. $A\{X\}_{(\mathfrak{m}, f)}$. Since $A\{f\}/(\mathfrak{m}, f) = A/\mathfrak{m}$ is perfect, it follows from Lemma 4 that $A\{X\}_{(\mathfrak{m}, X)}$ is integrally closed.

It is well-known that any Noetherian complete local integral domain has the following property:

Let R be an integral domain, K the quotient field of R, and L a finite extention of K. If R' is the integral closure of R in L, then R' is a finite R-module.

Next, we shall show that $A\{X_1, \cdots, X_n\}$ has this property.

Proposition 3. *Let A be a Noetherian complete local integral domain with the maximal ideal $\mathfrak{m}$. Let K be the quotient field of $R = A\{X_1, \cdots, X_n\}$, and L a finite extention of K. Then the integral closure R' of R in L is a finite R-module.*

Proof. Let p be the characteristic of K. If $p = 0$, our assertion is trivial since R is Noetherian [4] and L is separable over K. Hence we need only to prove this proposition in the case of $p \neq 0$. There exists a regular local subring B of A such that A is a finite B-module. Let $\mathfrak{n}$ be the maximal ideal of B. Since the topology of A coincides with that of A as a finite B-module by Theorem (16.8) in [3], there exists $h > 0$ such that $\mathfrak{m}^h \subset \mathfrak{n}A \subset \mathfrak{m}$. Hence it follows that $A\{X\}$ is a finite $B\{X\}$-module. Since R' is the integral closure of $B\{X\}$, we need only to prove this proposition in the case of that A is regular. In this case A is isomorphic to $k[[T_1, \cdots, T_r]]$, $k = A/\mathfrak{m}$ by Cohen's structure theorem. Then we have $A\{X_1, \cdots, X_n\} \cong k[X_1, \cdots, X_n][[T_1, \cdots, T_r]]$. Now, Proposition 3 follows from (0, 23.1.4) of [1].

The following lemma will be used to prove the theorem.

Lemma 5. *Let A be a Noetherian complete local integral domain with the maximal ideal $\mathfrak{m}$, and A' the integral closure in the quotient field of A. If $f \in A\{X\}$ is a series such that $f \notin \mathfrak{m}\{X\}$ and $f(0) \in \mathfrak{m}$, then $A'\{f\} \cap A\{X\} = A\{f\}$.*

Proof. In [5], it is proved that $A'[[f]] \cap A[[X]] = A[[f]]$. Since $f \in A\{X\}$, $A'\{f\} \cap A[[X]] \subset A\{X\}$. Then we have $A'\{f\} \cap A\{X\} = A'\{f\} \cap A[[X]] = A'\{f\} \cap A'[[f]] \cap A[[X]] = A'\{f\} \cap A[[f]] = A\{f\}$.

3. Proof of the theorem. Put $f = \prod_{\psi \in G} \psi X$. The degree of $f \bmod \mathfrak{m}\{X\}$ is equal to the order of G. We have $A\{f\} \subset A\{X\}^G \subset A\{X\}$. It follows from Lemma 2 that $A\{X\}^G$ is integral over $A\{f\}$ and $A\{X\}^G$ has the same quotient field of $A\{f\}$. If A is integrally closed, then $A\{f\}$ is also integrally closed by Proposition 2, and hence $A\{X\}^G = A\{f\}$. In the general case, if A' is the integral closure of A, A' satisfies conditions of Proposition 2. Then we have $A'\{X\}^G = A'\{f\}$. Since $f(0) = 0$, it follows from Lemma 5 that $A\{X\}^G = A'\{X\}^G \cap A\{X\} = A'\{f\} \cap A\{X\} = A\{f\}$.

As was shown above, it seems that the essential part in the proof of the theorem is to show that $A\{X\}$ is integrally closed (Proposition 2). It is not an essential condition that $A/\mathfrak{m}$ is perfect. For example, if A is a complete regular local ring, the theorem is true since $A\{X\}$ is a regular ring [4], and hence it is an integrally closed ring.

References

[1] Grothendieck, A.: Eléments de géométrie algébrique. IV (première partie). Pub. Math., **20**, I.H.E.S. (1964).
[2] Lubin, J.: Finite subgroups and isogenies of one-parameter formal Lie group. Ann. of Math., **85**, 296–302 (1967).
[3] Nagata, M.: Local Rings. Interscience Pub. (1960).
[4] Salmon, P.: Sur les séries formelles restreintes. Bull. Soc. Math. France, **92**, 385–410 (1964).
[5] Samuel, P.: Groupes fini d'automorphisms des anneaux de séries formelles. Bull. Sci. Math., **90**, 97–101 (1966).
[6] Serre, J. P.: Corps locaux. Hermann (1962).