Journal of the Mathematical Society of Japan Vol. 3, No. 1, May, 1951.

A Note on Finite Ring Extensions

Emil ARTIN and John T. TATE

Let $R \subset S$ be two commutative rings. We shall say that S is a modul finite extension of R if a finite number of elements $\omega_1, \omega_2, \cdots \omega_n$ of S can be found such that

$$S=R\omega_1+R\omega_2+\cdots+R\omega_n.$$

This modul finite extension has to be distinguished from what we shall call a ring finite extension

$$S=R[\xi_1, \xi_2, \cdots \xi_n],$$

in which every element of S can be written as polynomial in the generators $\xi_1, \xi_2, \cdots \xi_n$ with coefficients in R. If we call S' the ring of all polynomials in the indeterminates $x_1, x_2, \cdots x_n$ with coefficients in R then S is a homomorphic image of S' and the following well known lemma is immediate:

Lemma 1. If R is a Noetherian ring[1] with unit element and $S=R[\xi_1, \xi_2, \cdots \xi_n]$ a ring finite extension of R then S is Noetherian.

Lemma 2. Let R be a Noetherian ring with unit element and $S=R\omega_1+R\omega_2+\cdots+R\omega_n$ a modul finite extension of R. Then any intermediate ring T: $R\subset T\subset S$ is also a modul finite extension of R.

The proof is simple and also well known. We consider S as an R-space. The R-subspaces of S—and T is one of them—satisfy the ascending chain condition. T is therefore a modul finite extension of R.

The main result of our note is:

Theorem 1. Let R be a Noetherian ring with unit element, $S=R[\xi_1, \xi_2, \cdots \xi_n]$ a ring finite extension and T an intermediate ring such that S is a modul finite extension of T: $S=T\omega_1+T\omega_2+\cdots+T\omega_m$. Then T is a ring finite extension of R.

Proof: There exist expressions of the form:

$$(1) \qquad \xi_i=\sum_{\nu=1}^{m} a_{i\nu}\omega_\nu\,; \quad i=1, 2, \cdots n\,; \qquad a_{i\nu}\in T$$

1) i.e. a ring with ascending chain condition for ideals.

$$(2) \qquad \omega_i\omega_j = \sum_{\nu=1}^{m} b_{ij\nu}\omega_\nu\,; \quad i, j = 1, 2, \cdots m\,; \quad b_{ij\nu} \in T.$$

Let T_0 be the ring finite extension of R generated by the $a_{i\nu}$ and the $b_{ij\nu}$. Lemma 1 shows that T_0 is Noetherian. Trivially $T_0 \subset T \subset S$.

An element of S is a polynomial in the ξ_i with coefficients in R. Substituting (1) and making repeated use of (2) shows that

$$S = T_0\omega_1 + T_0\omega_2 + \cdots + T_0\omega_m,$$

so that S is a modul finite extension of T_0. Because of lemma 2 our ring T is also a modul finite extension of T_0, say by elements $\alpha_1, \alpha_2, \cdots \alpha_p$ of T. Therefore T is a ring finite extension of R by the elements $a_{i\nu}$, $b_{ij\nu}$ and α_ν.

As an application we prove the following theorem of Zariski.[2)]

Theorem 2. Let k be a field and assume that the ring finite extension $E = k[\xi_1, \xi_2, \cdots \xi_n]$ is a field. Then E/k is algebraic and consequently modul finite.

Proof: Suppose E/k is transcendental. Let $\xi_1, \xi_2, \cdots \xi_r$ be algebraically independent, all other ξ_ν algebraically dependent on $\xi_1, \xi_2, \cdots \xi_r$. Call F the field $k(\xi_1, \xi_2, \cdots \xi_r)$ of all rational functions of $\xi_1, \xi_2, \cdots \xi_r$. Then $k \subset F \subset E$ and E is a modul finite extension of F (being a finite algebraic extension of F). Because of theorem 1 F would be a ring finite extension $k[\eta_1, \eta_2, \cdots \eta_m]$ of k. Each η_i is a rational function of $\xi_1, \xi_2, \cdots \xi_r$. Let M be the set of all denominators of the η_i. In the polynomial domain $k[\xi_1, \xi_2, \cdots \xi_r]$ there are infinitely many irreducible polynomials. (One can make a uniform proof for all fields k which is similar to Euclid's proof for the existence of infinitely many primes.) Let f be irreducible and assume f divides none of the polynomials of M. The element $\frac{1}{f}$ of F could not be a polynomial in $\eta_1, \eta_2, \cdots \eta_m$. This is a contradiction.

Zariski uses theorem 2 for a short proof of Hilbert's Nullstellensatz. He concludes as follows:

Let $\mathfrak{a} \neq \mathfrak{o}$ be an ideal in the domain of polynomials $\mathfrak{o} = k[x_1, x_2, \cdots x_n]$ in indeterminates x_ν. Let $\mathfrak{p} \supset \mathfrak{a}$ be a maximal ideal above $\mathfrak{a}$. Then $\mathfrak{o}/\mathfrak{p}$ is a field on one hand and a ring finite extension of k by the residue

2) Oscar Zariski, A new proof of Hilbert's Nullstellensatz. Bull. Amer. Math. Soc. **53** (1947).

classes $\mu_1, \mu_2, \cdots \mu_n$ of $x_1, x_2, \cdots x_n$ on the other. Therefore each μ_i is algebraic over k. If $f(x_1, x_2, \cdots x_n) \epsilon \mathfrak{p}$ then $f(\mu_1, \mu_2, \cdots \mu_n)=0$. Therefore $\mathfrak{p}$ has an algebraic zero and a fortiori $\mathfrak{a}$.

If consequently $\mathfrak{a}$ is an ideal without algebraic zeros then $\mathfrak{a}=\mathfrak{o}$. The full Nullstellensatz is an easy consequence of this statement.[3]

Now let R be a Noetherian integral domain with unit element 1 and quotient field F.

Theorem 3. R has a ring finite extension $S=R[\xi_1, \xi_2, \cdots, \xi_n]$ which is a field, if and only if F is itself a ring finite extension of R. If this is the case the fields of type S are simply all modul finite extension fields of F.

Proof: If S is a field, then $R \subset F \subset S$ and $S=F[\xi_1, \xi_2, \cdots \xi_n]$. According to theorem 2 S is a modul finite extension of F. From theorem 1 it follows that F is s ring finite extension of R. Conversely, if F is a ring finite extension, then any modul finite extension of F is obviously a ring finite extension of R.

Our next theorem gives necessary and sufficient conditions for F to be a ring finite extension of R.

Theorem 4. The following four statements about R are equivalent:

(A) F is a ring finite extension of R.

(B) There exists an element $a \neq 0$ of R which is contained in all prime ideals of R.

(C) There are only a finite number of minimal prime ideals of R.

(D) There are only a finite number of prime ideals in R, and every one of them is maximal.

(By ideal we always mean a "proper" ideal, different from $\{0\}$ and R.)

Proof:

(A)→(B): Let $F=R[\eta_1, \eta_2, \cdots, \eta_n]$. Let $a \in R$ be a common denominator of the η_i. Then for any element $f=f(\eta_1, \eta_2, \cdots, \eta_n) \epsilon F$ we have $a^\nu f \epsilon R$ for some ν. Given any prime ideal $\mathfrak{p}$ of R, let $b \neq 0$ be an element of $\mathfrak{p}$. Then we have $a^\nu \frac{1}{b} \epsilon R$; hence $a^\nu \epsilon\, bR \subset \mathfrak{p}$ and therefore $a \epsilon \mathfrak{p}$.

(B)→(C): Let $aR=\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_r$, each $\mathfrak{q}_i$ primary belonging to $\mathfrak{p}_i$. For a sufficiently high m we have $\mathfrak{p}_i^m \subset \mathfrak{q}_i$ for all i. Let $\mathfrak{p}$ be any prime ideal. Then

3) See for instance: van der Waerden, Moderne Algebra, vol. 2 (1931), p. 11.

$$\mathfrak{p}_1^m\mathfrak{p}_2^m\cdots\mathfrak{p}_r^m \subset \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_r \subset \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_r = aR \subset \mathfrak{p},$$

and therefore $\mathfrak{p}_i \subset \mathfrak{p}$ for some i. It follows that the minimal primes must be among the primes $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$.

(C)$\rightarrow$(D) : We shall use the fact that any element $c \in R$ which is not a unit is contained in some minimal prime. This follows directly from a theorem of Krull[4] which states that any prime ideal which is minimal among the primes containing a principal ideal cR is minimal in R.

Let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_s$ be the minimal primes of R. For each i, there exists an element $a_i \notin \mathfrak{p}_i$ such that $a_i \in \mathfrak{p}_j$ for $j \neq i$. Otherwise we would have $\mathfrak{p}_i \supset \cap_{j \neq i}\mathfrak{p}_j \supset \Pi_{j \neq i}\mathfrak{p}_j$, and therefore $\mathfrak{p}_i \supset \mathfrak{p}_j$ for some $j \neq i$, contradicting the minimality of $\mathfrak{p}_i$. Take now any element $b \notin \mathfrak{p}_1$. The element

$$b' = b + \sum_{i;\, b \in \mathfrak{p}_i} a_i \equiv b \pmod{\mathfrak{p}_1}$$

is clearly contained in none of the minimal primes $\mathfrak{p}_i$ and is therefore a unit. It follows that $\mathfrak{p}_1$, and similarly any $\mathfrak{p}_i$, is maximal.

(D)$\rightarrow$(C) : Trivially.

(C)$\rightarrow$(B) : Take an $a \neq 0$ in the product of the minimal primes.

(B)$\rightarrow$(A) : Take $b \neq 0$ in R. Write $bR = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_r$, each $\mathfrak{q}_i$ primary belonging to $\mathfrak{p}_i$. From $a \in \mathfrak{p}_i$ we conclude some power of a is in all the $\mathfrak{q}_i$, therefore in bR: $a^m = bc$. Then $\frac{1}{b} = \frac{c}{a^m}$ shows that $F = R\left[\frac{1}{a}\right]$.

The question whether a field $E \supset R$ can be imbedded in a ring finite extension $S = R[\xi_1, \xi_2, \cdots, \xi_n]$ of R can be answered immediately. Let $\mathfrak{p}$ be a maximal ideal of S. The residue class field $S/\mathfrak{p}$ still contains E and $S/\mathfrak{p} = R[\eta_1, \eta_2, \cdots, \eta_n]$ where η_i is the residue class of ξ_i. According to theorem 3 R has to satisfy the condition stated in this theorem and $S/\mathfrak{p}$ is a modul finite extension of F. Therefore E is a modul finite extension of F.

Princeton University.

---

4) W. Krull, Dimensionstheorie in Stellenringen, Journal für die reine und angewandte Mathematik, vol. 179, p. 221 (1938).