ON A PROBLEM OF ZARISKI

BY

D. Rees

Among the problems posed by D. Hilbert at the Second International Congress of Mathematicians at Paris in 1900, the fourteenth still remains undecided. This problem can be stated as follows:

If S denotes the ring of polynomials in n indeterminates over a field k, and if F is a subfield of the field of fractions of S which contains k, then is the ring $R = S \cap F$ finitely generated over k?

In a paper, [2], published in 1954, O. Zariski posed a problem which generalizes the above problem of Hilbert. Zariski's problem is the following.

Let F be a field finitely generated over a field k, and let S be a finitely generated, normal integral domain[1] over k whose field of fractions F' contains F. Then is the ring $R = S \cap F$ finitely generated over k?

It will be convenient at this point to introduce the following terminology. We shall suppose a field F given. Then if the answer to the above problem is in the affirmative for all choices of S, subject to the conditions stated in the problem, we shall say that F is a Zariski field over k. In the paper already cited, Zariski proved that any field of transcendence degree 1 or 2 over k is a Zariski field over k and posed the conjecture that every finitely generated extension of k is a Zariski field over k.

The next contribution to this problem was made by Nagata in [1]. Nagata's main contribution to the problem lies in the following result.

If F is a finitely generated field extension of k, F is a Zariski field over k if and only if the following is true. Given any finitely generated normal integral domain A over k with F as field of fractions and any ideal $\mathfrak{a}$ of A, the ring $B = \bigcup \mathfrak{a}^{-n}$ is finitely generated over A and therefore k. Here $\mathfrak{a}^{-n}$ denotes the set of elements x of F such that $xa \in A$ whenever $a \in \mathfrak{a}^n$.

It will be convenient to state this result of Nagata in a somewhat different form. We recall that if A is a finitely generated normal integral domain, then with each minimal prime ideal $\mathfrak{p}$ of A we may associate a discrete valuation $v_\mathfrak{p}(x)$ on the field of fractions F of A. The set Σ of valuations thus obtained has the following properties:

(i) $x \in A$ if and only if $v_\mathfrak{p}(x) \geqq 0$ for every valuation $v_\mathfrak{p}(x)$ in Σ,

(ii) if $x \in F$, $v_\mathfrak{p}(x) = 0$ for all save a finite number of valuations in Σ.

It follows from (ii) that, if $\mathfrak{a}$ is any ideal of A, there is only a finite number of valuations $v_\mathfrak{p}(x)$ in Σ such that $v_\mathfrak{p}(x) > 0$ for all elements x of $\mathfrak{a}$. Let $\mathfrak{a}$ be a fixed ideal of A, let these valuations be $v_1(x), \cdots, v_k(x)$, and let e_i be the least value of $v_i(x)$ with x in $\mathfrak{a}$. Then $v_1(x), \cdots, v_k(x)$ are also the only valuations in Σ which are positive on $\mathfrak{a}^n$, and the least value of $v_i(x)$ on $\mathfrak{a}^n$ is

Received August 15, 1957.

[1] A normal integral domain is one integrally closed in its field of fractions.

ne_i. It follows that $x \in \mathfrak{a}^{-n}$ if and only if $v_i(x) \geqq -ne_i$ $(i = 1, \cdots, k)$ and $v_\mathfrak{p}(x) \geqq 0$ for all other valuations $v_\mathfrak{p}(x)$ in Σ. Hence we may characterize B as the ring of all elements x of F such that $v_\mathfrak{p}(x) \geqq 0$ for all valuations $v_\mathfrak{p}(x)$ in Σ save the finite set of valuations $v_i(x)$ $(i = 1, \cdots, k)$. We shall say that A has the Nagata property if, for every finite subset $v_1(x), \cdots, v_k(x)$ of Σ, the ring B constructed in this way is finitely generated over A. Then we can restate Nagata's result in the following form:

A finitely generated extension F of k is a Zariski field over k if and only if every finitely generated normal integral domain A over k having F as field of fractions has the Nagata property.

After these preliminaries, we now come to the main purpose of this note. This is to show that a finitely generated extension F of a field k of transcendence degree 3 over k need not be a Zariski field over k. In the counterexample we shall construct, k is the field of complex numbers. We shall now describe how this counterexample is constructed. We start with a nonsingular curve C in the projective plane, with homogeneous generic point (x_0, x_1, x_2) and take a point P on C. Since k is assumed algebraically closed, the prime ideal $\mathfrak{p}$ of $k[x_0, x_1, x_2]$ generated by those forms in x_0, x_1, x_2 which vanish at P may be generated by two linear forms y, z in x_0, x_1, x_2. We now define the ring A' to be $k[x_0, x_1, x_2, ty, tz, t^{-1}]$, where t is an indeterminate over $k(x_0, x_1, x_2)$ and A is to be the integral closure of A in its field of fractions $F = k(x_0, x_1, x_2, t)$. Clearly F has transcendence degree 3 over k. We shall show below that if A has the Nagata property, then, for some integer k, the symbolic power $\mathfrak{p}^{(k)}$ of $\mathfrak{p}$ is a principal ideal of $k[x_0, x_1, x_2]$. Stated in geometrical language, this implies that there is a curve C' in the projective plane which meets C in P counted k times and in no other point. If we assume this result, it is a simple matter to construct the counterexample required. For take C to be a nonsingular elliptic cubic curve. If we now consider the parametrization of C by elliptic functions, then the condition that there should exist a curve meeting C multiply at P and at no other point is that the value of the parameter at P should be a rational multiple of a period. It follows therefore that there are points P on C such that no multiple of P is a complete intersection, and for such points the ring A constructed above does not have the Nagata property. This implies that F is not a Zariski field over k. Notice that F is in this case obtained by adjoining two indeterminates to an extension of k which is of transcendence degree 1 and genus 1.

The rest of this paper will be devoted to the proof of the result assumed above, namely that if A has the Nagata property, then some symbolic power of $\mathfrak{p}$ is a principal ideal.

Before we proceed to the proof of this result, we must make some preliminary remarks. First consider the ring $A' = k[x_0, x_1, x_2, ty, tz, t^{-1}]$. Any element of this ring can be written in the form $\sum_{r=-p}^{q} c_r t^r$ where $c_r \in R = k[x_0, x_1, x_2]$ and, for $r \geqq 0$ we must have $c_r \in \mathfrak{p}^r$. Secondly, R is integrally closed in its field of fractions. This is a consequence of the assumption that C is a nonsingular plane curve and therefore projectively normal, which amounts to saying that R is integrally closed in its field of fractions. It therefore follows that A, the integral closure of A' in its field of fractions, is contained in $R[t, t^{-1}]$, since the latter is a normal integral domain containing A'. Hence every element of A is of the form $\sum_{r=-p}^{q} c_r t^r$ with c_r in R. Further, since A' is a graded ring, that is, $\sum_{r=-p}^{q} c_r t^r$ belongs to A' if and only if each of the terms $c_r t^r$ belongs to A', its integral closure A has the same property, that is, if $\sum_{r=-p}^{q} c_r t^r$ belongs to A, where $c_r \in R$ for each r, then $c_r t^r \in A$. Finally, in the first of our subsidiary lemmas we shall be concerned with the ring B defined as follows. Let $v(x)$ be the valuation defined on $k(x_0, x_1, x_2)$ which is associated with the minimal prime ideal $\mathfrak{p}$ of $R = k[x_0, x_1, x_2]$. Then B is the ring of all finite sums $\sum_{r=-p}^{q} c_r t^r$, where $c_r \in R$ and satisfies $v(c_r) \geqq r$ if $r \geqq 0$.

LEMMA 1. *If A has the Nagata property, then B is finitely generated over R.*

Let $u = t^{-1}$. Then if Σ is the set of valuations associated with the minimal prime ideals of A, there is only a finite set of valuations $v_i(x)$ in Σ for which $v_i(u) > 0$. Let these be $v_1(x), \cdots, v_k(x)$. Consider the valuation $v^*(x)$ defined on A by $v^*(\sum_{r=-p}^{q} c_r t^r) = \mathrm{Min}_{r=-p,\cdots,q}(v(c_r) - r)$. Now $v^*(x) \geqq 0$ for all elements in A' and therefore all elements of A. Further $v^*(u) = 1 > 0$. We shall now show that $v^*(x)$ belongs to Σ and therefore to the set $v_1(x), \cdots, v_k(x)$ by showing that the ideal $\mathfrak{p}^*$ of A, consisting of those elements of A such that $v^*(x) > 0$, is a minimal prime ideal of A. Firstly, $\mathfrak{p}^* \cap R = \mathfrak{p}$. Secondly, as $\mathfrak{p}$ contains an element c such that $v(c) = 1$, A' and, a fortiori, A contains an element ct such that $v^*(ct) = 0$ and therefore not belonging to $\mathfrak{p}^*$. From this it follows that $A/\mathfrak{p}^*$ has a field of fractions whose transcendence degree over k is at least 1 greater than that of the field of fractions of $R/\mathfrak{p}$ over k. Since $\mathfrak{p}$ is a minimal prime ideal of R, this implies that the field of fractions of $A/\mathfrak{p}^*$ has transcendence degree at least 2 over k. But the field of fractions of A has transcendence degree 3 over k. Hence $\mathfrak{p}^*$ is a minimal prime ideal of A. Take $v^*(x)$ to be $v_1(x)$ so that $v_1(u) = 1$, and let $v_i(u) = e_i$ $(i = 2, \cdots, k)$. Let $\mathfrak{a}$ be the ideal of A consisting of all elements of A such that $v_i(x) \geqq e_i$ $(i = 2, \cdots, k)$. Then $\mathfrak{a}^{-n}$ consists of all elements of the field of fractions F of A such that $v_i(x) \geqq -ne_i$ $(i = 2, \cdots, k)$ and $v_\mathfrak{p}(x) \geqq 0$ for all other valuations associated with A. But this is the case if and only if $u^n x \in A$ and $v_1(u^n x) \geqq n$. Hence, if $x = \sum_{r=-p}^{q} c_r t^r$, and $n \geqq q$, $x \in \mathfrak{a}^{-n}$ if and only if $v(c_r) \geqq r$ when $r \geqq 0$, and $c_r \in R$ for all r. This implies that $B = \bigcup \mathfrak{a}^{-n}$ and is therefore finitely generated over A and, consequently, finitely generated over over R.

LEMMA 2. *With the same hypothesis as in Lemma 1, there exists an integer k such that, for all n, $(\mathfrak{p}^{(k)})^n = \mathfrak{p}^{(nk)}$.*

The ring B of the last lemma is a graded ring, and therefore the generators of B over R may be chosen to be homogeneous. Since B contains u and, further, every element of B of degree < 0 is of the form cu^r with c in R, we may take these generators to be u and elements $a_i t^{r_i}$ ($i = 1, \cdots, p$) where $r_i > 0$. Let r be the least common multiple of $r_1, \cdots, r_p$, and take $k = pr$. Now $\mathfrak{p}^{(m)}$ is generated by those products $a_1^{s_1} \cdots a_p^{s_p}$ for which $\sum_{i=1}^p r_i s_i \geqq m$, since all elements of the form xt^m with x in $\mathfrak{p}^{(m)}$ belong to B, and conversely, if xt^m ($x \in R$) belongs to B, then $x \in \mathfrak{p}^{(m)}$. If $m \geqq pr$, then at least one of the products $r_i s_i \geqq r$, and hence we can write

$$a_1^{s_1} \cdots a_p^{s_p} = (a_1^{s_1} \cdots a_i^{s_i - t} \cdots a_p^{s_p}) \cdot a_i^t,$$

where $t = r/r_i$ and therefore the first factor belongs to $\mathfrak{p}^{(m-r)}$ and the second to $\mathfrak{p}^{(r)}$. Proceeding in this way, we see that, for any positive integer l

$$\mathfrak{p}^{(k+lr)} \subset \mathfrak{p}^{(k)} \cdot (\mathfrak{p}^{(r)})^l.$$

Since $(\mathfrak{p}^{(r)})^l \subset \mathfrak{p}^{(lr)}$, this implies that, for all $n > 0$, $\mathfrak{p}^{(nk)} \subset (\mathfrak{p}^{(k)})^n$. The reverse inclusion is obvious.

LEMMA 3. *If k is the integer found in the last lemma, $\mathfrak{p}^{(k)}$ is a principal ideal.*

We shall write $\mathfrak{a}$ for the ideal $\mathfrak{p}^{(k)}$ and let $a_1, \cdots, a_m$ be a basis of $\mathfrak{a}$. Let P be the ring $R[a_1 t, \cdots, a_m t, t^{-1}]$. Then P is finitely generated over R and hence over the base field k. Further P is integrally closed in its field of fractions F. For, since R is normal, the same applies to $R[t, t^{-1}]$. Hence the integral closure of P is contained in $R[t, t^{-1}]$. On the other hand, if $v(x)$ is the valuation on $k(x_0, x_1, x_2)$ associated with $\mathfrak{p}$, $\mathfrak{a}^n = \mathfrak{p}^{(nk)}$ is the set of elements of R which satisfy $v(x) \geqq nk$. Hence, if $v^*(x)$ is the valuation on F determined by defining $v^*(at^r) = v(a) - rk$, $a \in R$, $v^*(x) \geqq 0$ on P, and, if r is positive, $v^*(at^r) \geqq 0$ implies that $a \in \mathfrak{a}^r$ i.e. $at^r \in P$. Hence P is integrally closed in F.

Let $u = t^{-1}$, and consider the ideal uP of P. This is a rank 1 ideal and consists of those elements of P which satisfy $v^*(x) \geqq k$. Hence it is a primary ideal whose radical $\mathfrak{p}^*$ consists of those elements of P which satisfy $v^*(x) > 0$ and meets R in $\mathfrak{p}$. Let $\mathfrak{m}$ denote the maximal homogeneous ideal (x_0, x_1, x_2). Since $\mathfrak{m} \not\subset \mathfrak{p}$, $\mathfrak{m}P + uP$ is of rank at least 2, and therefore the ring $P' = P/(\mathfrak{m}P + uP)$ has transcendence degree at most 1 over k. Now the base field k is infinite. Hence there exists an element a' of degree 1 in P' such that P' is a finite $k[a']$-module. If a is an element of $\mathfrak{a}$ such that a' is the residue of at modulo $\mathfrak{m}P + uP$, it then follows that, for n sufficiently large, $\mathfrak{a}^{n+1} = a\mathfrak{a}^n + \mathfrak{m}\mathfrak{a}^{n+1}$, which, since $\mathfrak{m}$ is the maximal homogeneous ideal of R, implies that $\mathfrak{a}^{n+1} = a\mathfrak{a}^n$. Now let $b_1, \cdots, b_q$ be a basis of $\mathfrak{a}^n$, and let b be any element of $\mathfrak{a}$. Then bb_i belongs to $\mathfrak{a}^{n+1}$ for each i, and hence we can write

$$bb_i = a \sum_{j=1}^{q} c_{ij} b_j \qquad \text{where } c_{ij} \in R \text{ and } i = 1, \cdots, q.$$

This implies that

$$|\, c_{ij} - (b/a)\delta_{ij} \,| = 0$$

and therefore that b/a is integrally dependent on R. Since the latter is integrally closed, it follows that $b/a \in R$ and finally that $\mathfrak{a} = aR$, that is, $\mathfrak{a}$ is a principal ideal.

The author is greatly indebted to Dr. J. A. Todd for assistance in the geometrical part of the construction of the above counterexample.

References

1. M. NAGATA, *A treatise on the 14th problem of Hilbert*, Mem. Coll. Sci. Univ. Kyoto Ser. A. Math., vol. 30 (1956), pp. 57–70.
2. O. ZARISKI, *Interprétations algébrico-géométrique de quatorzième problème de Hilbert*, Bull. Sci. Math., vol. 78 (1954), pp. 155–168.

DOWNING COLLEGE
CAMBRIDGE, ENGLAND