

COMPOSITIO MATHEMATICA

E. SNAPPER

Higher-dimensional field theory. I. The integral closure of a module

Compositio Mathematica, tome 13 (1956-1958), p. 1-15

http://www.numdam.org/item?id=CM_1956-1958__13__1_0

© Foundation Compositio Mathematica, 1956-1958, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Higher-Dimensional field Theory

I. The integral closure of a module

by

E. Snapper

Introduction.

Let E/F be a finitely generated field extension, i.e. E and F are commutative fields and there exist a finite number of elements $e_1, \dots, e_n$ in E , such that $E = F(e_1, \dots, e_n)$. If the, necessarily finite, degree of transcendency of E/F is at least 2, we possess only very little coherent theory of E/F , even though many of the theorems of higher-dimensional algebraic geometry can be interpreted in terms of these higher-dimensional field extensions. One of the reasons for this is that the theorems concerning algebraic varieties are formulated and proved by means of models and homogeneous coordinates, while the importance of these theorems for abstract algebra, whenever they have any, can only be detected if they are formulated and proved by means of notions and methods which belong in the style of modern algebra. Think for a moment of Lüroth's theorem, whose geometric importance for curve theory is beautifully brought out, by the use of homogeneous coordinates, in section 5 of Severi's Vorlesungen. Nevertheless, unless we observe that the algebraic content of this theorem is the well-known statement concerning the intermediate fields of a simple transcendental field extension and prove this statement directly by means of some simple argument of modern algebra, we have missed the importance of Lüroth's theorem for field theory.

The purpose of the present three articles, entitled *Higher-Dimensional Field Theory* I, II, III, is to give a start to higher-dimensional field theory, by developing the theory of linear systems of algebraic varieties intrinsically in terms of a finitely generated field extension E/F . Instead of using models and homogeneous coordinates, we use only notions and methods which can properly be regarded as to belong in the style of a modern algebraic treatment of E/F . The articles are consequently self-contained and require no knowledge of algebraic geometry from

the reader. The terms have been chosen in such a way as to conform with the terminology of the underlying geometry. No result, which the author considers as being of only secondary importance, has been labeled „theorem.” We now give a short introduction to each of these articles, listed by subtitle.

I. The integral closure of a module.

(Referred to as *FI*.) The notion of the integral closure of a module was introduced in [1]. (Square brackets refer to the references). The whole field-theoretic approach to linear systems is based on this notion. In order to keep the present articles self-contained, the pertinent material of [1] is reviewed, without proofs, in the first section. The author does not feel happy about the proof of the theorem discussed in [1] and of statement 2.2 of the present paper *FI*. The reason is that the trick of adjoining a variable to E is nothing but a sly way of using homogeneous coordinates and this trick does not belong in the style the author has set for these papers. Probably, both these facts can be proved without the adjunction of a variable to E , but the author possesses no such proofs at this moment. The remainder of the three articles is completely in the style of an intrinsic theory of E/F .

II. Linear systems. (Referred to as *FII*.)

Here we establish the notion of *the divisors of the first kind of a projective class of modules* and then study the connection between the integral closure of a module and the divisors of the first kind of a projective class. This valuation-theoretic treatment of the integral closure of a module gives the correct field-theoretic interpretation of Zariski's theorems on linear systems without base points. These theorems occur in two, as yet unpublished, manuscripts of Zariski, entitled „On Arithmetically Normal Varieties” and „Algebro-geometric interpretations of the 14th problem of Hilbert”; these manuscripts are referred to as respectively Z and ZH .¹⁾

III. Normalization. (Referred to as *FIII*.)

Here we derive, again purely field-theoretically, the principal theorems on normalization which Zariski obtained in [2] and Z .

The author wants to say explicitly that all theorems on linear systems which occur in these articles belong to Professor Zariski;

¹⁾ ZH has appeared in print in “*Bull. Sci. Math.* (2), 78, pp. 155–168 (1954)”.

for each such theorem it is stated where Zariski's formulation and proof can be found. The author also wishes to use this opportunity to thank Professor Zariski for the great help he received from him, several times per week, during 1953–1954.

It is not intended that the present articles convey the idea that algebraic geometry is to be considered as a part of field theory and should be developed without the use of models and homogeneous coordinates. The content of these articles is not geometry, but is higher-dimensional field theory. And although this theory is logically independent of the geometry from which it arose, it could never even have been started if the geometry had not been developed first. On the other hand, it is hoped, that this higher-dimensional field theory may provide further useful tools for geometry.

1. *Review of [1].* Let E/F be as in the introduction. A module $M = (a_1, \dots, a_m)$ of E consists of the linear combinations $c_1 a_1 + \dots + c_m a_m$, where $a_1, \dots, a_m$ are fixed elements of E and $c_1, \dots, c_m$ are arbitrary elements of F . Only this type of modules, i.e. modules which are finitely generated over F , will occur in this paper and hence „module” will always mean „finitely generated module.” The sum $(M_1, \dots, M_h)$ of the modules $M_1, \dots, M_h$ is the module which consists of the sums $b_1 + \dots + b_h$, where $b_j \in M_j$, and the product $M_1 \dots M_h$ is the module which is generated by the products $b_1 \dots b_h$; the product of just two modules M_1 and M_2 is written as $M_1 M_2$ instead of $M_1 \cdot M_2$. Both addition and multiplication are commutative and associative and these operations combine under the law of distributivity. In particular, defining $M^0 = F$ when $M \neq 0$, the powers M^j of a nonzero module are well defined for all nonnegative rational integers j ; of course, when $M = 0$, $M^j = 0$ when $j \geq 1$.

The integral closure $|M|_i$ of a module M is the module which consists of the elements $e \in E$, for which there exists a nonzero module L , such that $eL \subset LM$; the finite generation of $|M|_i$ was proved in [1]. Always, $M \subset |M|_i \subset F\langle M \rangle$, where $F\langle M \rangle$ denotes the ordinary integral closure of the ring $F[M]$ in E . Precisely, $e \in |M|_i$ if and only if e satisfies an equation $x^m + a_1 x^{m-1} + \dots + a_m = 0$, where $m \geq 1$ and $a_j \in M^j$ for $j = 1, \dots, m$. We will often use that for any $a \in E$, $a|M|_i = |aM|_i$, an equality which follows immediately from the definition of $|M|_i$.

We can prove as follows that $F\langle M \rangle$ is always Noetherian, a fact which we omitted to observe in [1]. If $F(M)$ denotes the

field of quotients of $F[M]$ and A the algebraic closure of $F(M)$ in E , $F\langle M \rangle$ is also the integral closure of $F[M]$ in A . The field extension $A/F(M)$ is, as an intermediate extension of a finitely generated field extension, itself finitely generated and hence has a finite field degree. Consequently, according to a classical theorem, $F\langle M \rangle$ has a finite number of generators when considered as a module over $F[M]$, which proves the assertion.

2. *Adjunction of a variable to E .* Consider the field extension $E(x)/F$, where x is transcendental with respect to E . When M is a module in E , M is also a module in $E(x)$ and, since E is algebraically closed in $E(x)$, the integral closure $|M|_i$ of M in E is identical with the integral closure of M in $E(x)$; consequently, when forming integral closures, we can completely forget about E and consider only $E(x)$. Furthermore, xM is a module of $E(x)$ and we denote again by $F\langle xM \rangle$ the ordinary integral closure of the ring $F[xM]$ in $E(x)$.

STATEMENT 2.1. *Let M be a module of E and e an element of E . Then, for any $h \geq 0$, $e \in |M^h|_i$ if and only if $x^h e \in F\langle xM \rangle$.*

PROOF. If $e \in |M^h|_i$, $x^h e \in x^h |M^h|_i = |(xM)^h|_i \subset F\langle (xM)^h \rangle$, where $F\langle (xM)^h \rangle$ denotes of course the integral closure of the ring $F[(xM)^h]$ in $E(x)$. Now $F[(xM)^h] \subset F[xM]$ and every element of xM is integral with respect to the ring $F[(xM)^h]$, which shows that $F\langle (xM)^h \rangle = F\langle xM \rangle$; hence $x^h e \in F\langle xM \rangle$. Conversely, let $x^h e \in F\langle xM \rangle$, say $(x^h e)^n + a_1(x^h e)^{n-1} + \dots + a_n = 0$, where $a_j \in F[xM]$. Then, each a_j is a polynomial $c_0 + c_1 x + \dots + c_s x^s$ with $c_u \in M^u$, and if we equate the coefficient of x^{hn} in this equation to zero, we find that $e^n + b_1 e^{n-1} + \dots + b_n = 0$ where $b_j \in M^{hj}$; hence $e \in |M^h|_i$ and we are done.

Since $F[xM] \subset E[x]$ and $E[x]$ is integrally closed in $E(x)$, $F\langle xM \rangle \subset E[x]$. Let $f = e_0 + e_1 x + \dots + e_n x^n$ be a polynomial of $E[x]$ which lies in $F\langle xM \rangle$. We can prove, by means of the following argument of Zariski, that then each individual term $e_j x^j$ belongs to $F\langle xM \rangle$. (See footnote 24 of [2].) If c is a nonzero element of F , the substitution $x \rightarrow cx$ gives rise to an automorphism S_c of $E[x]$ which maps $F\langle xM \rangle$ onto itself and hence $S_c(f) \in F\langle xM \rangle$. If F contains $n+1$ distinct, nonzero elements $c_0, \dots, c_n$, we conclude from $S_{c_0}(f), \dots, S_{c_n}(f) \in F\langle xM \rangle$ that each $e_j x^j \in F\langle xM \rangle$. Otherwise, we go over to the algebraic closure F^* of F , which is contained in an extension field E^* of E and we consider the tower $F^*[xM] \subset F^*\langle xM \rangle \subset E^*[x]$, where $F^*\langle xM \rangle$ denotes the integral closure of the ring $F^*[xM]$ in $E^*(x)$. Since F^* has infinitely many

elements and our $f \in F^*\langle xM \rangle$, each $e_j x^j \in F^*\langle xM \rangle$. Furthermore, every element of $F^*[xM]$ depends integrally on $F[xM]$, and hence $e_j x^j \in F\langle xM \rangle$, which proves the assertion.

Consider the contraction in $F\langle xM \rangle$ of the prime ideal (x) of $E[x]$; i.e., we consider the prime ideal $\mathfrak{p}$ of $F\langle xM \rangle$, which consists of the polynomials of $F\langle xM \rangle$ with zero constant term. Since $E(x)/F$ is still finitely generated, $F\langle xM \rangle$ is again Noetherian and hence $\mathfrak{p}$ has a finite ideal basis, say $\mathfrak{p} = (f_1, \dots, f_n)$ where $f_j \in F\langle xM \rangle$. According to the just completed argument, each term of each polynomial f_j belongs to $\mathfrak{p}$ and hence we can use these terms also as an ideal basis for $\mathfrak{p}$. In other words, $\mathfrak{p}$ possesses an ideal basis whose elements are of the form $e_j x^j$, where $j \geq 1$ and $e_j \in |M^j|_i$.

It is only for the proof of the following statement, that the variable x was adjoined to E .

STATEMENT 2.2. *Let M be a module of E . There exist a finite number of rational integers $u_1, \dots, u_n$, where each $u_j \geq 1$, such that for all $h \geq 1$, $|M^h|_i = (|M^{h-u_1}|_i |M^{u_1}|_i, \dots, |M^{h-u_n}|_i |M^{u_n}|_i)$. Only those terms $|M^{h-u_j}|_i |M^{u_j}|_i$ are written down on the right hand side for which $h \geq u_j$.*

PROOF. Let $e_1 x^{u_1}, \dots, e_n x^{u_n}$, where $e_j \in |M^{u_j}|_i$ and $u_j \geq 1$, be an ideal basis for $\mathfrak{p}$. We will show that these integers $u_1, \dots, u_n$ satisfy the requirement of statement 2.2. If $L_1, \dots, L_h$ are any h modules of E , it follows immediately from the definition of the integral closure of a module, that the following rule holds for products: $|L_1|_i \cdot \dots \cdot |L_h|_i \subset |L_1 \cdot \dots \cdot L_h|_i$. Consequently, each term $|M^{h-u_j}|_i |M^{u_j}|_i \subset |M^h|_i$ and all we have to show is that $|M^h|_i \subset (|M^{h-u_1}|_i |M^{u_1}|_i, \dots, |M^{h-u_n}|_i |M^{u_n}|_i)$. If $e \in |M^h|_i$, $x^h e \in F\langle xM \rangle$ and since $h \geq 1$, $x^h e = f_1 e_1 x^{u_1} + \dots + f_n e_n x^{u_n}$, where f_j is a polynomial of $F\langle xM \rangle$. Since $e, e_1, \dots, e_n$ and the coefficients of each f_j all belong to E , we may assume that $f_j = d_j x^{h-u_j}$, where $d_j \in |M^{h-u_j}|_i$ and where we consider only those terms for which $h \geq u_j$. We cancel x^h at both sides and obtain that $e = d_1 e_1 + \dots + d_n e_n$ and we are done.

3. Proof of the principal theorem. It is easy to draw the following consequence from statement 2.2.

STATEMENT 3.1. *Let M be a module of E and let the integers $u_1, \dots, u_n$ be as in statement 2.2. Then, if $h \geq t \text{Max}(u_1, \dots, u_n)$ where t is a positive rational integer, $|M^h|_i = \sum |M^{h-j_1 u_1 - \dots - j_n u_n}|_i (|M^{u_1}|_i)^{j_1} \cdot \dots \cdot (|M^{u_n}|_i)^{j_n}$, where the sum is extended over all nonnegative rational integers $j_1, \dots, j_n$ for which $j_1 + \dots + j_n = t$.*

PROOF. When $t = 1$, statements 3.1 and 2.2 coincide, since then $h \geq u_j$ for $j = 1, \dots, n$ and hence all the terms on the right hand side of the expression for $|M^h|_i$, given in statement 2.2, occur. Suppose then that the present statement has been proved for $t = 1, 2, \dots, t_0 - 1$ and that $h \geq t_0 \text{Max}(u_1, \dots, u_n)$. Then, certainly $h \geq (t_0 - 1)\text{Max}(u_1, \dots, u_n)$ and hence

$$|M^h|_i = \Sigma |M^{h-j_1 u_1 - \dots - j_n u_n}|_i (|M^{u_1}|_i)^{j_1} \dots (|M^{u_n}|_i)^{j_n},$$

where $j_1 + \dots + j_n = t_0 - 1$. Furthermore, $h - j_1 u_1 - \dots - j_n u_n \geq h - (t_0 - 1)\text{Max}(u_1, \dots, u_n) \geq \text{Max}(u_1, \dots, u_n)$. Hence each coefficient $|M^{h-j_1 u_1 - \dots - j_n u_n}|_i$ in this expansion for $|M^h|_i$ can itself be expanded according to the case $t = 1$ and we are done.

We now introduce a new fact concerning integral closures of modules.

STATEMENT 3.2. *Let M be a module of E . Then there exists a nonnegative rational integer h_0 , such that, if $h \geq h_0$, $(|M|_i)^{h+s} = (|M|_i)^h M^s$ for all $s \geq 0$.*

PROOF. All we have to show is that, when $h \geq h_0$, $(|M|_i)^{h+1} = (|M|_i)^h M$. Namely, this means that our statement has been proved for $s = 0, 1$. We can then assume that it has been proved for $s = 0, 1, \dots, s_0 - 1$ and conclude that $(|M|_i)^{h+s_0} = (|M|_i)^{(h+1)+(s_0-1)} = (|M|_i)^{h+1} M^{s_0-1} = (|M|_i)^h M M^{s_0-1} = (|M|_i)^h M^{s_0}$. The inclusion $(|M|_i)^h M \subset (|M|_i)^{h+1}$ is trivial since, for any $h \geq 0$, $(|M|_i)^h M \subset (|M|_i)^h |M|_i = (|M|_i)^{h+1}$. In order to show that $(|M|_i)^{h+1} \subset (|M|_i)^h M$, when h is large enough, let $e \in |M|_i$. Then $e^n + a_1 e^{n-1} + \dots + a_n = 0$, where $n \geq 1$ and $a_j \in M^j$. It follows that, when $j \geq 1$, $a_j e^{n-j} \in M^j (|M|_i)^{n-j} = M M^{j-1} (|M|_i)^{n-j} \subset M (|M|_i)^{j-1} (|M|_i)^{n-j} = M (|M|_i)^{n-1}$, which shows that $e^n \in M (|M|_i)^{n-1}$. Let $|M|_i = (a_1, \dots, a_k)$, where $a_j^{n_j} \in M (|M|_i)^{n_j-1}$ and $m = \text{Max}(n_1, \dots, n_k)$. Then $a_j^m \in M (|M|_i)^{m-1}$ for $j = 1, \dots, k$, since $a_j^m = a_j^{n_j} a_j^{m-n_j} \in M (|M|_i)^{n_j-1} (|M|_i)^{m-n_j} = M (|M|_i)^{m-1}$. For any $h \geq 0$, the monomials $a_1^{q_1} \dots a_k^{q_k}$, where $q_1 + \dots + q_k = h$, generate $(|M|_i)^h$. There exists of course an h_0 such that, when $h \geq h_0$, each one of these monomials factors out at least one a_j^m for some $1 \leq j \leq k$; we now show that this h_0 has the required property. Namely, if $h \geq h_0$, $a_1^{q_1} \dots a_k^{q_k} = a_j^{a_1^{q_1} \dots a_j^{q_j-m} \dots a_k^{q_k}} \in M (|M|_i)^{m-1} (|M|_i)^{q_1} \dots (|M|_i)^{q_j-m} \dots (|M|_i)^{q_k} = M (|M|_i)^{h-1}$ and consequently, $(|M|_i)^h \subset M (|M|_i)^{h-1}$. We multiply this last inclusion on both sides with $|M|_i$ and we are done.

We now prove the principal theorem concerning integral closures of modules.

THEOREM 3.1 *Let M be a module of E . Then there exists a non-*

negative rational integer k_0 , such that, if $k \geq k_0$, $|M^{k+s}|_i = |M^k|_i M^s$ for all $s \geq 0$.

PROOF. Again, all we have to show is that, when $k \geq k_0$, $|M^{k+1}|_i = |M^k|_i M$. Namely then we can, as in the proof of statement 3.2, assume that our theorem has been proved for $s = 0, 1, \dots, s_0 - 1$ and conclude that $|M^{k+s_0}|_i = |M^{(k+1)+(s_0-1)}|_i = |M^{k+1}|_i M^{s_0-1} = |M^k|_i M M^{s_0-1} = |M^k|_i M^{s_0}$. Furthermore, $|M^{k+1}|_i = |M^k|_i M$ is proved, as soon as we have shown that there exists some module N such that $|M^{k+1}|_i = NM$. Namely then, using the definition of $|M^{k+1}|_i$ together with the fact that NM is finitely generated, we first conclude that there exists a module L such that $NML \subset LM^{k+1} = LMM^k$; then, using the definition of $|M^k|_i$, we see that $N \subset |M^k|_i$ and hence that $|M^{k+1}|_i \subset |M^k|_i M$. The inverse inclusion is trivial, since for any $k \geq 0$, always $|M^k|_i M \subset |M^k|_i |M|_i$, and, using the rule for products expressed in the proof of statement 2.2, $|M^k|_i |M|_i \subset |M^{k+1}|_i$. We now return to the modules $|M^{u_1}|_i, \dots, |M^{u_n}|_i$ of statement 3.1, in order to show that there exists an integer k_0 , such that when $k \geq k_0$, $|M^{k+1}|_i$ factors out M . Using M^{u_j} as the module M of statement 3.2, we denote by $h_0^{(j)}$ the integer which this last statement associates to M^{u_j} ; let $h_0 = \text{Max}(h_0^{(1)}, \dots, h_0^{(n)})$. We then choose an integer t_0 , such that when $j_1 + \dots + j_n = t_0$ where $j_1, \dots, j_n$ are nonnegative rational integers, at least one $j_m \geq h_0 + 1$. We will show that $k_0 = t_0 \text{Max}(u_1, \dots, u_n)$ has the required property. Namely, according to statement 3.1, when $k \geq k_0$, $|M^k|_i$ can be written as a sum of terms each one of which factors out $(|M^{u_1}|_i)^{j_1} \cdot \dots \cdot (|M^{u_n}|_i)^{j_n}$ with $j_1 + \dots + j_n = t_0$; hence, each of these terms factors out at least one $(|M^{u_j}|_i)^{h_0+1} = (|M^{u_j}|_i)^{h_0} M^{u_j}$. Since $u_j \geq 1$, this shows that $|M^k|_i$ factors out M ; of course, if $k \geq k_0$, also $k+1 \geq k_0$, and hence $|M^{k+1}|_i$ also factors out M and we are done.

4. *The dimension of $|M^h|_i$.* Let M be a module of E . The dimension of M is of course the maximum number of elements of M which are linearly independent with respect to F . If $M = (a_1, \dots, a_m)$ and $\mathfrak{p}$ is the prime ideal of the polynomial ring $F[x_1, \dots, x_m]$ which consists of the polynomials which vanish for $x_j = a_j$, $j = 1, \dots, m$, the residueclass ring $F[x_1, \dots, x_m]/\mathfrak{p}$ is F -isomorphic with the ring $F[M]$. Hence, the maximum number of polynomials of $F[x_1, \dots, x_m]$ of degree at most s , which are linearly independent modulo $\mathfrak{p}$, is equal to the dimension of the module $(M^0, M, M^2, \dots, M^s)$. We assume momentarily that $1 \in M$, which implies that $M^h \subset M^k$ when $h \leq k$, and hence that

$(M^0, M, M^2, \dots, M^s) = M^s$. We can then conclude from the theory of the Hilbert characteristic function of $\mathfrak{p}$ that there exists a polynomial $f(x)$ with rational coefficients, whose degree d is equal to the degree of transcendency of the field extension $F(M)/F$, and which is such that $\dim(M^s) = f(s)$, when s is large enough. Since $M^s \subset M^{s+1}$, $f(s)$ is a nondecreasing function for large s and hence its leading coefficient c_0 must be positive. Furthermore, $f(x)$ is a polynomial which takes on integral values for all large integral values of x . Consequently, when we write this polynomial as $f(x) = a_0 \binom{x}{d} + a_1 \binom{x}{d-1} + \dots + a_{d-1} \binom{x}{1} + a_d$, where $\binom{x}{j}$ is the usual binomial coefficient $x!/j!(x-j)!$, the coefficients $a_0, \dots, a_d$ are all rational integers; this general property of polynomials can be proved in a few lines by induction on d , as observed by Zariski in *Z*. Clearly $c_0 = a_0/d!$ and hence also $a_0 > 0$. We call a_0 the degree of M and $f(x)$ the Hilbert characteristic function of M . If $1 \notin M$ but $M \neq 0$ (i.e., M does not consist of only the zero element of E), we choose any nonzero element $a \in M$ and apply the above reasoning to the module $(1/a)M$; this is permitted since $1 \in (1/a)M$. Furthermore, because $((1/a)M)^s = (1/a^s)M^s$, we see that $\dim((1/a)M)^s = \dim(M^s)$, and hence the Hilbert characteristic function of $(1/a)M$ gives the dimension of M^s for large values of s . It follows in particular that this polynomial is independent of the choice of a , which is further clarified by the observation that the field $F((1/a)M)$ is evidently independent of a . Since clearly, $F(M) = F(a, (1/a)M)$, the degree of transcendency of $F(M)/F$ is either equal to that of $F((1/a)M)/F$ or exceeds it by unity. We have now arrived at the following formulation of the classical theorem concerning the Hilbert characteristic function.

STATEMENT 4.1. *Let M be a nonzero module of E . The Hilbert characteristic function of M is the rational polynomial $f(x) = a_0 \binom{x}{d} + a_1 \binom{x}{d-1} + \dots + a_d$, which is such that $\dim(M^s) = f(s)$, when $s \geq s_0$; here, s_0 is some rational integer associated with M . The degree d of $f(x)$ is the degree of transcendency of the field extension $F((1/a)M)/F$, for any nonzero $a \in M$. The coefficients $a_0, \dots, a_d$ are rational integers and the positive integer a_0 is called the degree of M .*

In order to prove theorem 4.1, we have to consider a slight generalization of statement 4.1, since we have to deal with the

dimension of $M^s N$, where both M and N are nonzero modules of E . Let $M = (a_1, \dots, a_m)$, $N = (b_1, \dots, b_n)$ and let $\mathfrak{p}$ denote the prime ideal of the polynomial ring $F[x_1, \dots, x_m, y_1, \dots, y_n]$ which consists of the polynomials which vanish for $x_j = a_j$, $y_k = b_k$, where $j = 1, \dots, m$ and $k = 1, \dots, n$. Clearly, the residueclass ring $F[x_1, \dots, x_m, y_1, \dots, y_n]/\mathfrak{p}$ is F -isomorphic with the ring $F[M, N]$ and hence the maximum number of polynomials of $F[x_1, \dots, x_m, y_1, \dots, y_n]$ of degree at most s in $x_1, \dots, x_m$ and at most one in $y_1, \dots, y_n$, which are linearly independent modulo $\mathfrak{p}$, is the dimension of the module $(M^0, M, M^2, \dots, M^s)(N^0, N)$. We assume again momentarily that $1 \in M$ and $1 \in N$, which implies that $(M^0, M, M^2, \dots, M^s)(N^0, N) = M^s N$. Any derivation of the classical theorem on the Hilbert characteristic function can also be used to prove the existence of a rational polynomial $f(x)$ which is such that, when s is large enough, $f(s)$ is the maximum number of polynomials of $F[x_1, \dots, x_m, y_1, \dots, y_n]$ of degree at most s in $x_1, \dots, x_m$ and at most one in $y_1, \dots, y_n$ which are linearly independent modulo $\mathfrak{p}$. (The author must warn the reader that this is not the same as to quote the well-known fact that the theory of the Hilbert characteristic function can be worked out for two sets of variables $x_1, \dots, x_m$ and $y_1, \dots, y_n$. In the latter case, we vary the degree of both the variables $x_1, \dots, x_m$ and the variables $y_1, \dots, y_n$ freely but, in our case, we only vary the degree of the variables $x_1, \dots, x_m$ freely while keeping the degree of the variables $y_1, \dots, y_n$ bounded by one.) Again, the degree d of $f(x)$ is the degree of transcendency of the field extension $F(M)/F$ and, since $f(x)$ has again the property of assuming integral values for all large integral values of x , we obtain again an integral polynomial when $f(x)$ is expressed, as before, in terms of binomial coefficients. The fact that the leading coefficient of $f(x)$ is positive now follows from the observation that $M^s N \subset M^{s+1} N$. Finally, if M and N are arbitrary nonzero modules of E , we apply this reasoning to the modules $(1/a)M$ and $(1/b)N$, where a and b are any nonzero elements of respectively M and N . We observe that $((1/a)M)^s((1/b)N) = (1/a^s b)M^s N$ and hence that $\dim((1/a)M)^s((1/b)N) = \dim(M^s N)$ and we have arrived at the following formulation of the classical theorem on the Hilbert characteristic function, which is general enough for our purpose.

STATEMENT 4.2. *Let M and N be nonzero modules of E . There exists a rational polynomial $f(x) = a_0 \binom{x}{d} + a_1 \binom{x}{d-1} + \dots + a_d$,*

which is such that $\dim(M^s N) = f(s)$, when $s \geq s_0$; here, s_0 is some rational integer associated with M and N . The degree d of $f(x)$ is the degree of transcendency of the field extension $F((1/a)M)/F$, for any nonzero $a \in M$. The coefficients $a_0, \dots, a_d$ are rational integers and a_0 is positive.

We now return to theorem 3.1 and to the integer k_0 which occurs there. By using the module $|M^{k_0}|_i$ as the module N of statement 4.2, we see that there exists a rational polynomial $f'(x)$, which is such that $\dim(|M^{k_0+s}|_i) = f'(s)$, when $s \geq s_0$. We rewrite the polynomial $f'(x)$ as $f(x - k_0)$ and have obtained the following theorem.

THEOREM 4.1. *Let M be a nonzero module of E . There exists a rational polynomial $f(x) = a_0 \binom{x}{d} + a_1 \binom{x}{d-1} + \dots + a_d$, which is such that $\dim(|M^s|_i) = f(s)$, when $s \geq s_0$; here, s_0 is some rational integer associated with M . The degree d of $f(x)$ is the degree of transcendency of the field extension $F((1/a)M)/F$, for any nonzero $a \in M$. The coefficients $a_0, \dots, a_d$ are rational integers and a_0 is positive.*

The polynomials of both statement 4.1 and theorem 4.1 are invariantly associated with the module M . The author believes that the polynomial of theorem 4.1 will turn out to be the important one.

5. Further relations between $|M|_i$ and $F\langle M \rangle$. The two statements of this section are auxiliary results which are needed for *FII* and *FIII*. They are derived here, because they belong in the part of the theory which is independent of the valuation theory of our field E .

Let M be a module of E and let us denote by N_s the module $(M^0, M, M^2, \dots, M^s)$, for any $s \geq 0$. Clearly, the set-theoretic union $\bigcup_{s=0}^{\infty} N_s$ of these modules is the ring $F[M]$ and $F[M] = F[N_s]$, for $s \geq 1$. We now derive the corresponding result for the ring $F\langle M \rangle$ and the set-theoretic union $\bigcup_{s=0}^{\infty} |N_s|_i$ of the integral closures $|N_s|_i$. As always, $F\langle M \rangle$ denotes the ordinary integral closure in E of the ring $F[M]$.

STATEMENT 5.1. $F\langle M \rangle = \bigcup_{s=0}^{\infty} |N_s|_i$ and there exists a rational integer s_0 , such that for all $s \geq s_0$, $F\langle M \rangle = F[|N_s|_i]$.

PROOF. Let $a \in \bigcup_{s=0}^{\infty} |N_s|_i$ i.e., $a \in |N_s|_i$ for some fixed $s \geq 0$; then, according to section 1, $a \in F\langle N_s \rangle$. If $s \geq 1$, $F[M] = F[N_s]$ and

hence $F\langle M \rangle = F\langle N_s \rangle$; if $s = 0$, $F[N_0] = F$ and hence $F\langle N_0 \rangle$ is then the algebraic closure of F in E , which shows that in this case $F\langle N_0 \rangle \subset F\langle M \rangle$. Consequently, in both cases, $a \in F\langle M \rangle$. Conversely, if $a \in F\langle M \rangle$, $a^n + c_1 a^{n-1} + \dots + c_n = 0$, where $n \geq 1$ and $c_j \in F[M]$ for $j = 1, \dots, n$. Since $F[M] = \bigcup_{s=0}^{\infty} N_s$ and $N_h \subset N_k$ when $h \leq k$, there exists a fixed m such that $c_j \in N_m$ for $j = 1, \dots, n$. We then conclude from $a^n = -c_1 a^{n-1} - c_2 a^{n-2} - \dots - c_n$ that $a^n \in (a^{n-1}N_m, a^{n-2}N_m, \dots, N_m) = (a^{n-1}, a^{n-2}, \dots, 1)N_m$. Furthermore, $1 \in N_m$ and hence $(a^{n-1}, a^{n-2}, \dots, 1) \subset (a^{n-1}, a^{n-2}, \dots, 1)N_m$, so that we can conclude that $(a^n, a^{n-1}, \dots, 1) \subset (a^{n-1}, a^{n-2}, \dots, 1)N_m$. Clearly, for any $j \geq 0$, $(a^j, a^{j-1}, \dots, 1) = (a, 1)^j$ and hence we have that $(a, 1)^n \subset (a, 1)^{n-1}N_m$ i.e., since $n \geq 1$, that $(a, 1)(a, 1)^{n-1} \subset (a, 1)^{n-1}N_m$. It now follows from the definition of $|N_m|_i$ that $(a, 1) \subset |N_m|_i$ and hence that $a \in |N_m|_i$; this finishes the proof that $F\langle M \rangle = \bigcup_{s=0}^{\infty} |N_s|_i$. Since $|N_h|_i \subset |N_k|_i$, when $h \leq k$, the sequence $F[|N_1|_i] \subset F[|N_2|_i] \subset \dots \subset F[|N_s|_i] \subset \dots$ is an increasing sequence of $F[M]$ -modules of $F\langle M \rangle$. We have seen in section 1 that $F\langle M \rangle$ has a finite number of generators, when considered as a module over $F[M]$, and consequently there exists an s_0 such that $F[|N_{s_0}|_i] = F[|N_s|_i]$, when $s \geq s_0$. Since $F\langle M \rangle = \bigcup_{s=0}^{\infty} |N_s|_i$, certainly $F\langle M \rangle = \bigcup_{s=0}^{\infty} F[|N_s|_i]$, which shows that $F\langle M \rangle = F[|N_s|_i]$ when $s \geq s_0$; done.

REMARK 5.1. In many cases, $F\langle M \rangle = \bigcup_{s=0}^{\infty} |M^s|_i$. For example, in most of our applications $1 \in M$, which implies that $N_s = M^s$ and hence that statement 5.1 is then valid with N_s replaced by M^s . In the case of the ring $F\langle xM \rangle$ of section 2, $F\langle xM \rangle$ is not equal to $\bigcup_{s=0}^{\infty} |(xM)^s|_i$ and, no matter how large we choose s , also not equal to $F[|(xM)^s|_i]$. However, $F\langle xM \rangle$ is equal to the infinite sum $\sum_{s=0}^{\infty} |(xM)^s|_i$ of the modules $|(xM)^s|_i$, which follows from statement 2.1 together with the assertion, proved in section 2, that if $e_0 + e_1 x + \dots + e_n x^n \in F\langle xM \rangle \cap E[x]$, each $e_j x^j \in F\langle xM \rangle$. In general, although always $F[M] = \sum_{s=0}^{\infty} M^s$ (this is equivalent to the assertion that $F[M] = \bigcup_{s=0}^{\infty} N_s$), $F\langle M \rangle$ is not equal to $\sum_{s=0}^{\infty} |M^s|_i$, as the following example demonstrates. Let $E = F(t)$, where t is transcendental over F , and let $M = (t^2)$. Then, $F[M] = F[t^2]$ and $F\langle M \rangle = F[t]$. Furthermore, $M^s = (t^{2s}) = t^{2s}(1)$, from which it follows that $|M^s|_i = t^{2s}|(1)|_i = (t^{2s})$. ($|(1)|_i$ is always the algebraic closure of F in E which, in our case, is F itself). Hence $\sum_{s=0}^{\infty} |M^s|_i = F[t^2]$, which is not equal to $F[t]$.

We now go over to the second statement of this section. If M is a nonzero module of E and h a nonnegative rational integer, we denote by $Q(M; h)$ the module of E which consists of the elements e of E which are such that $eM^s \subset M^{s+h}$ for some $s \geq 0$. It is clear that $Q(M; h)$ is closed under multiplication by elements of F while, if $eM^s \subset M^{s+h}$ and $e'M^{s'} \subset M^{s'+h}$ where say $s \geq s'$, also $e'M^s \subset M^{s+h}$ and hence $(e \pm e')M^s \subset M^{s+h}$. Moreover, since $M^{s+h} = M^s M^h$, it follows from the definition of $|M^h|_i$ and the fact that $M \neq 0$, that $Q(M; h) \subset |M^h|_i$; this shows that $Q(M; h)$ is finitely generated and hence that $Q(M; h)$ is indeed a module. We also observe, by choosing $s = 0$, that $M^h \subset Q(M; h)$. The importance of the module $Q(M; h)$ is minor as compared to that of $|M^h|_i$. Even so, these two modules have similar properties, as the following statement, which is needed for *FIII*, indicates.

We denote by G a finite or infinite generating system of M . For example, all elements of M form a G or if, in our notation, $M = (a_1, \dots, a_m)$, the elements $a_1, \dots, a_m$ also form a G .

STATEMENT 5.2. *Let M be a nonzero module of E and G any finite or infinite generating system of M , where $0 \notin G$. Then, for all $h \geq 0$, $|M^h|_i = \bigcap_{a \in G} a^h F \langle (1/a)M \rangle$ and $Q(M; h) = \bigcap_{a \in G} a^h F[(1/a)M]$.*

PROOF. If $e \in |M^h|_i$ and a is any nonzero element of E , $e/a^h \in (1/a^h)|M^h|_i = |((1/a)M)^h|_i \subset F \langle ((1/a)M)^h \rangle = F \langle (1/a)M \rangle$. (The fact that for any module N whatsoever, always $F \langle N^h \rangle = F \langle N \rangle$, is explained in the second sentence of the proof of statement 2.1.) This shows that $e \in \bigcap_{a \in G} a^h F \langle (1/a)M \rangle$ and hence certainly that $e \in \bigcap_{a \in G} a^h F \langle (1/a)M \rangle$. Conversely, let $e \in \bigcap_{a \in G} a^h F \langle (1/a)M \rangle$. Then, for any $a \in G$, $e/a^h \in F \langle (1/a)M \rangle$. Since $a \in M$, $1 \in (1/a)M$, which enables us to conclude, according to remark 5.1, that $F \langle (1/a)M \rangle = \bigcup_{s=0}^{\infty} |((1/a)M)^s|_i$. Hence there exists an s_0 such that, if $s \geq s_0$, $e/a^h \in |((1/a)M)^s|_i = (1/a)^s |M^s|_i$. It follows that $ea^s \in a^h |M^s|_i$ and therefore, since $a^h |M^s|_i \subset M^h |M^s|_i \subset |M^h|_i |M^s|_i \subset |M^{h+s}|_i$, that $ea^s \in |M^{h+s}|_i$. Since M is finitely generated, G contains a finite generating system $a_1, \dots, a_m$ of M ; let $s_0^{(1)}, \dots, s_0^{(m)}$ be the rational integers which are associated, in the above way, to respectively $a_1, \dots, a_m$ and let $t = \text{Max}(s_0^{(1)}, \dots, s_0^{(m)})$. The module M^u is generated by the monomials $a_1^{q_1} \dots a_m^{q_m}$, where $q_1 + \dots + q_m = u$, and we assume that u has been chosen so large that each of these monomials factors out at least one a_j^t for some $1 \leq j \leq m$. We then have that $ea_1^{q_1} \dots a_m^{q_m} = (ea_j^t) a_1^{q_1} \dots a_j^{q_j-t} \dots a_m^{q_m} \in |M^{h+t}|_i M^{q_1+\dots+q_m-t} \subset |M^{h+t+a_1+\dots+a_m-t}|_i = |M^{h+u}|_i$ and hence

that $eM^u \subset |M^{h+u}|_i$. Using the definition of $|M^{h+u}|_i$ and the fact that eM^u is finitely generated, we conclude that there exists a nonzero module L such that $eM^u L \subset LM^{h+u} = LM^u M^h$ and hence that $e \in |M^h|_i$; the first equality of statement 5.2 has now been established. If $e \in Q(M; h)$, $eM^s \subset M^{s+h}$ for some $s \geq 0$. Consequently, if a is a nonzero element of M , we conclude from $ea^s \in M^{s+h}$ that $e \in a^h((1/a)M)^{s+h} \subset a^h F[(1/a)M]$. This shows that $Q(M; h) \subset \bigcap_a a^h F[(1/a)M]$, where a runs through all the nonzero elements of M , and hence certainly that $Q(M; h) \subset \bigcap_{a \in G} a^h F[(1/a)M]$. Conversely, let $e \in \bigcap_{a \in G} a^h F[(1/a)M]$. Then, for any $a \in G$, $e/a^h \in F[(1/a)M]$ and therefore, when s is large enough, $e/a^h \in ((1/a)M)^s = (1/a^s)M^s$; this implies that $ea^s \in a^h M^s \subset M^h M^s = M^{h+s}$. In the proof of the previous equality we concluded from $ea^s \in |M^{h+s}|_i$ for large s , that $eM^u \subset |M^{h+u}|_i$ for large u . We use precisely the same reasoning here to conclude from $ea^s \in M^{h+s}$ for large s , that $eM^u \subset M^{h+u}$ for large u . This proves that $e \in Q(M; h)$ and we are done.

Observe that section 1 contains two characterizations of the integral closure of a module and that statement 2.1 contains a third one. Statement 5.2 gives, if $M \neq 0$, as fourth characterization that $|M|_i = \bigcap_{a \in G} aF\langle(1/a)M\rangle$. In FII, section 3, we will find a fifth one in terms of the valuations of E .

6. *Extension to several modules.* We mention here that each previous statement and theorem, together with its proof, can be extended easily to several modules, because this generalization is necessary whenever one has to use the field-theoretic equivalent of the graph of algebraic correspondences. *Since the present section is used nowhere in FII and FIII*, we discuss only very briefly the extension to several modules of the most important facts of this paper, which however will be enough so that anyone can carry out this generalization in full detail.

Let $M_1, \dots, M_n$ be modules of E and consider the field-extension $E(x_1, \dots, x_n)/F$, where $x_1, \dots, x_n$ are algebraically independent over E . An element e of E is contained in $|M_1^{h_1} \cdots M_n^{h_n}|_i$ if and only if $ex_1^{h_1} \cdots x_n^{h_n} \in F\langle x_1 M_1, \dots, x_n M_n \rangle$, where $F\langle x_1 M_1, \dots, x_n M_n \rangle$ denotes the ordinary integral closure in $E(x_1, \dots, x_n)$ of the ring $F[x_1, \dots, x_n]$; here, $h_1, \dots, h_n$ are arbitrary nonnegative rational integers. (Analogue of statement 2.1.) This should make it clear how all of sections 2 and 3 can be extended to the set of modules $M_1, \dots, M_n$ and how we arrive at the following analogue of theorem 3.1.

THEOREM 6.1. *Let $M_1, \dots, M_n$ and L be modules of E . Then there exist nonnegative rational integers $k_0^{(1)}, \dots, k_0^{(n)}$, such that, if $k_j \geq k_0^{(j)}$, $|M_1^{k_1+s_1} \dots M_n^{k_n+s_n} L|_i = |M_1^{k_1} \dots M_n^{k_n} L|_i M_1^{s_1} \dots M_n^{s_n}$ for all $s_j \geq 0$; here $j = 1, \dots, n$. Of course, L may not be present.*

Let $M_j = (a_1^{(j)}, \dots, a_{m_j}^{(j)})$ for $j = 1, \dots, n$ and consider, in the polynomial ring $R = F[x_1^{(1)}, \dots, x_{m_1}^{(1)}, \dots, x_1^{(n)}, \dots, x_{m_n}^{(n)}]$, the prime ideal $\mathfrak{p}$ which consists of the polynomials of R which vanish for $x_h^{(j)} = a_h^{(j)}$, where $j = 1, \dots, n$ and $h = 1, \dots, m_j$. The residue-class ring $R/\mathfrak{p}$ is F -isomorphic with the ring $F[M_1, \dots, M_n]$ and hence the maximum number of polynomials of R , of degree at most s_j in the variables $x_1^{(j)}, \dots, x_{m_j}^{(j)}$ for $j = 1, \dots, n$, and which are linearly independent modulo $\mathfrak{p}$, is the dimension of the module $(M_1^0, M_1, M_1^2, \dots, M_1^{s_1}) \dots (M_n^0, M_n, M_n^2, \dots, M_n^{s_n})$; if we assume momentarily that $1 \in M_j$ for $j = 1, \dots, n$, this module becomes $M_1^{s_1} \dots M_n^{s_n}$. Hence, when we repeat the arguments of section 4, using the theory of the Hilbert characteristic function for n sets of variables $x_1^{(1)}, \dots, x_{m_1}^{(1)}, \dots, x_1^{(n)}, \dots, x_{m_n}^{(n)}$ (see [3]), we arrive at the following analogue of statements 4.1 and 4.2.

STATEMENT 6.1. *Let $M_1, \dots, M_n$ and N be nonzero modules of E . There exists a rational polynomial $f(x_1, \dots, x_n) = \sum a_{j_1, \dots, j_n} \binom{x_1}{j_1} \dots \binom{x_n}{j_n}$, where we sum over all $j_1 + \dots + j_n \leq d$, which is such that $\dim(M_1^{s_1} \dots M_n^{s_n} N) = f(s_1, \dots, s_n)$ when $s_j \geq s_0^{(j)}$ for $j = 1, \dots, n$; $\binom{x_1}{j_1}, \dots, \binom{x_n}{j_n}$ denote again the usual binomial coefficients and $s_0^{(1)}, \dots, s_0^{(n)}$ are rational integers which are associated with the set of modules $M_1, \dots, M_n, N$. The degree d of this polynomial is the degree of transcendency of the field extension $F((1/a_1)M_1, \dots, (1/a_n)M_n)/F$, where a_j is any nonzero element of M_j for $j = 1, \dots, n$. The coefficients $a_{j_1, \dots, j_n}$ are rational integers, and those coefficients $a_{j_1, \dots, j_n}$ for which $j_1 + \dots + j_n = d$ are nonnegative. If the module N is not present, we refer to these nonnegative coefficients $a_{j_1, \dots, j_n}$ with $j_1 + \dots + j_n = d$, as the degrees of the set of modules $M_1, \dots, M_n$ and to the polynomial $f(x_1, \dots, x_n)$ as the Hilbert characteristic function of these modules.*

We now return to the integers $k_0^{(1)}, \dots, k_0^{(n)}$ of theorem 6.1 and use the module $|M_1^{k_1^{(1)}} \dots M_n^{k_n^{(n)}} L|_i$ as the module N of statement 6.1. We then easily derive the following analogue of theorem 4.1.

THEOREM 6.2. *Let $M_1, \dots, M_n$ and L be nonzero modules of E . There exists a rational polynomial $f(x_1, \dots, x_n) = \sum a_{j_1, \dots, j_n} \binom{x_1}{j_1} \dots \binom{x_n}{j_n}$, where we sum over all $j_1 + \dots + j_n \leq d$, which*

is such that $\dim (|M_1^{s_1} \cdot \dots \cdot M_n^{s_n} L|_i) = f(s_1, \dots, s_n)$ when $s_j \geq s_0^{(j)}$ for $j = 1, \dots, n$; here, $s_0^{(1)}, \dots, s_0^{(n)}$ are rational integers which are associated with the set of modules $M_1, \dots, M_n, L$. The degree d of this polynomial is the degree of transcendency of the field extension $F((1/a_1)M_1, \dots, (1/a_n)M_n)/F$, where a_j is any nonzero element of M_j for $j = 1, \dots, n$. The coefficients $a_{j_1, \dots, j_n}$ are rational integers and those coefficients $a_{j_1, \dots, j_n}$ for which $j_1 + \dots + j_n = d$ are nonnegative. The module L may of course be absent.

When $M_1, \dots, M_n$ are nonzero modules of E and $h_1, \dots, h_n$ are nonnegative rational integers, we denote by $Q(M_1, \dots, M_n; h_1, \dots, h_n)$ the module of E which consists of the elements e of E which are such that $eM_1^{s_1} \cdot \dots \cdot M_n^{s_n} \subset M_1^{s_1+h_1} \cdot \dots \cdot M_n^{s_n+h_n}$, for some set of nonnegative rational integers $s_1, \dots, s_n$. Then again, $M_1^{h_1} \cdot \dots \cdot M_n^{h_n} \subset Q(M_1, \dots, M_n; h_1, \dots, h_n) \subset |M_1^{h_1} \cdot \dots \cdot M_n^{h_n}|_i$, and the following analogue of statement 5.2 holds.

STATEMENT 6.2. Let $M_1, \dots, M_n$ be nonzero modules of E and let G_j be any finite or infinite generating system of M_j , not containing 0, for $j = 1, \dots, n$. Then, when $h_1, \dots, h_n$ are any nonnegative rational integers,

$$|M_1^{h_1} \cdot \dots \cdot M_n^{h_n}|_i = \bigcap_{a_j \in G_j} a_1^{h_1} \cdot \dots \cdot a_n^{h_n} F \langle (1/a_1)M_1, \dots, (1/a_n)M_n \rangle$$

and

$$Q(M_1, \dots, M_n; h_1, \dots, h_n) = \bigcap_{a_j \in G_j} a_1^{h_1} \cdot \dots \cdot a_n^{h_n} F [(1/a_1)M_1, \dots, (1/a_n)M_n].$$

REFERENCES

E. SNAPPER

- [1] *Integral closure of modules and complete linear systems*, to be published in the Princeton Symposium Volume in honor of Professor S. Lefschetz.

O. ZARISKI

- [2] *Some results in the arithmetic theory of algebraic varieties*, American Journal of Mathematics Vol. 61 (1939) pp. 249—294.

B. L. VAN DER WAERDEN

- [3] *On Hilbert's function, series of composition of ideals and a generalization of the theorem of Bézout*, Neder. Akad. Wetensch. Vol 31 (1928) pp. 749—770.

Miami University, Ohio.

(Oblatum 7-5-55).