CONSTRUCTIVE NORMALIZATION OF AN ALGEBRAIC VARIETY

BY GABRIEL STOLZENBERG[1]

1. First let us recall the problem of normalization in the affine case. We are given a prime ideal $\mathfrak{P} = (p_1, \cdots, p_r)$ in a polynomial ring $k[X_1, \cdots, X_n]$ over a field k. We form the quotient ring $R = k[X_1, \cdots, X_n]/\mathfrak{P} = k[x_1, \cdots, x_n]$ and consider its integral closure I in $k(x_1, \cdots, x_n)$. The problem is to represent I as a *finite* R-module $I = Rx_{n+1} + \cdots + Rx_N$, and also as

$$I = k[x_1, \cdots, x_n, x_{n+1}, \cdots, x_N] = k[X_1, \cdots, X_N]/\mathfrak{Q},$$

where $\mathfrak{Q} = (q_1, \cdots, q_s)$ is a *finitely* generated ideal.

The classical solution is nonconstructive in a typical way. One exhibits I as a submodule of a finite R-module and then invokes the Hilbert Basis Theorem, first to assert that I is a finite R-module, and again to assert that $\mathfrak{Q}$ is finitely generated. But the Basis Theorem is, at best, a guarantee that no particular I or $\mathfrak{Q}$ will ever require infinitely many generators. It does not help us to decide whether generators for I and $\mathfrak{Q}$ can actually be constructed or, if they can, how to construct them, how many are needed, and how they depend on the initial data $\mathfrak{P} = (p_1, \cdots, p_r)$.

In this note we will describe a method that treats these questions —in the case that $k(x_1, \cdots, x_n)$ is *separably generated over k*. This restriction and also the requirement that k be a field reflect the limitations of our technique. Also, k must be defined in such a way that the polynomial ring $k[T]$ is constructively a unique factorization domain (or else the class of prime ideals $\mathfrak{P} = (p_1, \cdots, p_r)$ would have to be restricted). A fairly general description of such fields is given in [2], following Kronecker's method of interpolation. Any finitely generated extension of a prime field, or even the algebraic closure of such a field, is allowed. But not the reals nor the complexes nor any p-adic field.

The same methods apply in the projective case, yielding a constructive version of projectively normal normalization and the completeness of the linear system of hypersurface sections of a fixed high degree on a normal projective variety.

2. Serious consideration of a strictly constructive approach to

---

algebra seems to have been initiated by Kronecker and influenced the development of algebraic geometry into the 1920's. Valuable memories of this can be found in the second edition of Van der Waerden's *Modern algebra* [5]. But the most substantial contribution I know of is the 1925 paper [2] of G. Hermann, based on earlier work of K. Hentzelt and E. Noether [1], [3]. I thank S. Kleiman for calling it to my attention. In that paper, starting with an ideal generated by t polynomials of degree at most q in n variables, the author constructs explicit finite sets of generators for the associated primes and for the primary ideals in a certain irredundant primary decomposition. Also exponents are estimated. Explicit bounds $\phi(q, t, n)$ for the number of generators, their degrees, and the number of associated ideals can be derived from the proofs in a routine fashion. However, these bounds are enormous.

Our construction of the normalization is an application of these results.

3. In the course of our proof we will often have to compute the image of a map, in the following sense.

First consider projections. If we are given an ideal $\mathfrak{A} = (f_1, \cdots, f_t)$ in $k[X_1, \cdots, X_n]$ how can we construct a finite set of generators for $\mathfrak{B} = \mathfrak{A} \cap k[X_1, \cdots, X_{n-1}]$? Unless $\mathfrak{A}$ is an intersection of primes, I don't know. But at any rate, via elimination theory, we can write down a finite set of equations whose locus includes the locus of $\mathfrak{B}$ as a union of irreducible components. Then, by [2], we get a finite set of generators for the radical of $\mathfrak{B}$. If $\mathfrak{A}$ is prime so is $\mathfrak{B}$ and the problem is solved in that case.

This generalizes directly to the situation where we are also given $\pi_1, \cdots, \pi_m$ in $k[X_1, \cdots, X_n]$ and $\mathfrak{B}$ is the ideal of all $g(Y_1, \cdots, Y_m)$ for which $g(\pi_1, \cdots, \pi_m)$ is in $\mathfrak{A}$.

For $\mathfrak{A}$ prime we generalize further to consider a rational map. Namely, set $k[X_1, \cdots, X_n]/\mathfrak{A} = k[x_1, \cdots, x_n]$ and choose $\phi_1, \cdots, \phi_m$ in the function field $k(x_1, \cdots, x_n)$. We seek a finite set of generators for the ideal $\mathfrak{B}$ that is defined by $k[\phi_1, \cdots, \phi_m] = k[Y_1, \cdots, Y_m]/\mathfrak{B}$. Each ϕ_i has a representative g_i/h_i in $k(X_1, \cdots, X_n)$, with h_i not in $\mathfrak{A}$. Then the ideal $(\mathfrak{A}, h_1 Y_1 - g_1, \cdots, h_m Y_m - g_m)$ has exactly one associated isolated prime $\mathfrak{J}$ not containing any $h_1, \cdots, h_m$. Generators for $\mathfrak{J}$ are constructed by [2], and $\mathfrak{B}$ is just the projection $\mathfrak{J} \cap k[Y_1, \cdots, Y_m]$.

4. We will now discuss our proof of affine normalization. We have $\mathfrak{P} = (p_1, \cdots, p_r)$ prime in $k[X_1, \cdots, X_n]$, and the function field $k(x_1, \cdots, x_n)$ is separably generated over k.

The first step, following the classical proof, is to represent the integral closure I explicitly as a submodule of a finite module over the coordinate ring. The dimension q can be computed by elimination theory, and we may as well assume that it is positive. The separability condition will lead to a shuffling of the indices and a construction of polynomials F_j in $\mathfrak{P} \cap k[X_1, \cdots, X_q, X_j], j = q+1, \cdots, n$, for which $\partial F_j/\partial X_j$ is not in $\mathfrak{P}$. Using §3 the constructivization of Noether Normalization is routine and leads to a coordinate change $k[X_1, \cdots, X_n]$ $= k[Y_1, \cdots, Y_n]$, with $k[Y_1, \cdots, Y_n]/\mathfrak{P} = k[y_1, \cdots, y_n]$ integral and separable over $k[y_1, \cdots, y_q]$, and $\mathfrak{P} \cap k[Y_1, \cdots, Y_q] = (0)$. Let A be the polynomial ring $k[y_1, \cdots, y_q]$ and K its function field $k(y_1, \cdots, y_q)$. Then, routine constructivization of the Primitive Element Theorem produces a y in $k[y_1, \cdots, y_n]$ for which $k(y_1, \cdots, y_n)$ $= K(y)$. The minimal polynomial $f(Y)$ of y over K is constructed along with y. It is separable, lies in $A[Y]$, and has a certain explicit degree d and a nonzero discriminant D in A. In this setting I is necessarily a submodule of the finite A-module generated by $1/D$, y/D, $\cdots$, y^{d-1}/D.

The second step is to normalize in codimension one. Let E be an irreducible factor of D appearing with exponent e. Then the localization at E, A_E, is a discrete valuation ring whose integral closure I_E in $K(y)$ is a submodule of the A_E-module generated by $1/E^e$, $\cdots$, y^{d-1}/E^e. In this case (see [4]) if we can find $z_1, \cdots, z_e$ integral over A such that, setting $y = z_0$, each z_i does not belong to $A_E[z_0, \cdots, z_{i-1}]$, then $I_E = A_E[z_0, \cdots, z_e]$.

So the problem here is, given $z_0, \cdots, z_c$ integral over A, to find a method which either proves that $A_E[z_0, \cdots, z_c]$ is integrally closed or else produces a *new* integral element z_{c+1} not in it.

Now $B = A_E[z_0, \cdots, z_c]$ is a semilocal ring which will be integrally closed exactly when its localization at each maximal ideal is principal. The maximal ideals of B are induced from the finitely many isolated primes of the ideal generated by E in $k[y_1, \cdots, y_q, z_0, \cdots, z_c]$. Hence we can construct a finite set of generators for each by the methods of §3 and [2]. At this point we have to make a separate argument for the case of a *curve over a finite field* and we will not pursue that any further here. Ruling out that case, we can construct an infinite sequence $\{u_i\}$ of elements of A which are units in A_E and for which each $u_i - u_j$ is also a unit so long as $i \neq j$. Say B has m maximal ideals. Let $\mathfrak{M}$ be one of them and let a and b be two nonzero members of our explicitly constructed generating set for $\mathfrak{M}$. Then it can be shown that one of $a/(ub+a)$ for $u = u_1, \cdots, u_{m+1}$ must be integral over A_E (and in each case we can check yes or no by examining the

characteristic polynomial). It can also be checked whether or not this element is in B. If it is not we have produced a new integral element (clearing a denominator to make it integral over A). If this element $x = a/(ub+a)$ does belong to B then, either x is a unit in the local ring $B_{\mathfrak{M}}$ in which case $b = x^{-1}(1-x)u^{-1}a$ is a multiple of a in $B_{\mathfrak{M}}$; or $1-x$ is a unit in $B_{\mathfrak{M}}$, in which case $a = xu(1-x)^{-1}b$ is a multiple of b.

This shows that if for each pair of generators a, b in each maximal ideal $\mathfrak{M}$ the constructed integral element $a/(ub+a)$ lies in B then each localization $B_{\mathfrak{M}}$ is principal and, hence, B is integrally closed.

Consequently, in at most e steps we get $A_E[z_0, \cdots, z_e]$ integrally closed. Doing this for each prime factor E of D gives altogether at most degree (D) elements $v_1, \cdots, v_\delta$ integral over A such that each $A_E[y, v_1, \cdots, v_\delta]$ is integrally closed. This is normalization in codimension one.

The third and last step is the key one. Relabel $y_1, \cdots, y_q, y$, $v_1, \cdots, v_\delta$ as $w_1, \cdots, w_t$ and set $S = k[w_1, \cdots, w_t]$. The effect of normalization in codimension one is that if s is in S then s/D is integral over S (and therefore over A) if and only if it is regular in codimension one—equivalently, if and only if it is in the localization of S at each isolated prime of the ideal generated by D in S. This leads to the following characterization of the integral closure I.

Let $\mathfrak{A}$ be the intersection of the isolated primary components of the ideal generated by D in S. Then $I = \mathfrak{A}/D$.

A finite set of generators for $\mathfrak{A}$ can be constructed by the methods of [2] and §3. We express S as $k[W_1, \cdots, W_t]/\mathfrak{J}$, get generators for $\mathfrak{J}$ as in §3, then get generators for the intersection of the isolated primary components of $(D, \mathfrak{J})$ by [2], and finally reduce modulo $\mathfrak{J}$.

This gives I as a finite S-module and essentially completes the proof. For S is a finite A-module, generated by the products of the w_j^i for $j = q+1, \cdots, t$ and $i < d$; so combining expressions gives generators for I as a finite A-module, with A contained in $R = k[x_1, \cdots, x_n]$. Thus we have the desired representation

$$I = Rx_{n+1} + \cdots + Rx_N = k[x_1, \cdots, x_N] = k[X_1, \cdots, X_N]/\mathfrak{Q}$$

where generators for $\mathfrak{Q}$ can be got as in §3.

We heartily thank M. Artin and P. Deligne for very useful and pleasant discussions about these matters.

REFERENCES

1. K. Hentzelt, *Zur Theorie der Polynomideale und Resultanten. Bearbeitet von E. Noether*, Math. Ann. 88 (1922), 53–79.

   2. G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynom-ideale*, Math. Ann. 95 (1925), 736–788.
   3. E. Noether, *Eliminationstheorie und allgemeine Idealtheorie*, Math. Ann. 90 (1923), 229–261.
   4. J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.
   5. B. L. Van der Waerden, *Modern algebra*. Vols. I, II, 2nd ed., Ungar, New York, 1937–1940.

INSTITUT DES HAUTES ETUDES SCIENTIFIQUES, FRANCE AND BROWN UNIVERSITY

VARIETIES OF GROUPS AND BURNSIDE'S PROBLEM

BY L. G. KOVÁCS

If $\mathfrak{B}$ is a variety of groups and d is a positive integer, $\mathfrak{B}^{(d)}$ denotes the variety consisting of the groups whose d-generator subgroups are all in $\mathfrak{B}$. In a recent paper [3], B. H. Neumann formulated the Extended Burnside Problem:

Problem 7. Let $\mathfrak{B}$ be a locally finite variety and $d \geq 1$ an integer. Is $\mathfrak{B}^{(d)}$ locally finite?

He went on to ask two related questions:

Problem 8. Is there, to each locally finite variety $\mathfrak{B}$, an integer $d = d(\mathfrak{B})$ such that $\mathfrak{B}^{(d)}$ is locally finite?

Problem 9. Do the locally finite groups in $\mathfrak{B}^{(d)}$, where $\mathfrak{B}$ is a locally finite variety, form a variety?

Neumann called the latter the Restricted Extended Burnside Problem. One might derive from it, like Problem 8 from Problem 7, the following:

Problem N. Is there, to each locally finite variety $\mathfrak{B}$, an integer $n = n(\mathfrak{B})$ such that the locally finite groups in $\mathfrak{B}^{(n)}$ form a variety?

The purpose of this note is to present reduction theorems for Problem 8 and Problem N, similar to the Hall-Higman reduction theorems [1] for the classical forms of Burnside's Problem.

THEOREM 1. *If $\mathfrak{B}$ is a locally finite and locally soluble variety, $\mathfrak{B}_{LN}$ is the variety consisting of the locally nilpotent groups of $\mathfrak{B}$, and $\mathfrak{B}_{LN}^{(d)}$ is locally finite for some integer d, then $\mathfrak{B}^{(d^*)}$ is locally finite for some integer d^*.*

This is a direct consequence of (c) of the forthcoming paper [2]. Theorem 2 will be derived from the following part of (b) of [2]: