ALGEBRAIC RINGS(1)

BY

MARVIN J. GREENBERG

Introduction. The notion of *algebraic ring* has appeared recently in the literature (cf. [5; 9; 10]), a structure which is a blend of algebraic geometry and ring theory. In this paper we consider some foundational results for *ring varieties* (§1). The chief results are: (1) the underlying ring must be Artinian (2.2); (2) the underlying additive group variety must be unipotent (4.3); (3) the equivalence in characteristic 0 with the theory of finite dimensional algebras (5.1); (4) the fact that the units form an open subvariety with induced structure of group variety (6.1); (5) a structure theorem for commutative ring varieties in characteristic $p > 0$ (8.2). Some of the proofs rely heavily on the established structure theory of group varieties (cf. [1; 6; 7]); others are elementary. Many problems for further research are mentioned throughout the paper.

1. **Definitions.** We use the terminology of [1], working over an algebraically closed ground field k.

In the broadest definition, an *algebraic ring* should be a "ring in the category of algebraic spaces," i.e., an algebraic space R such that the functor $\mathrm{Reg}(X,R)$ (= all regular mappings $X \to R$) in the variable algebraic space X takes its values in the category of rings; equivalently, R should be a commutative algebraic group under addition endowed with a biadditive regular mapping $m: R \times R \to R$ (multiplication). This definition would include as examples all finite-dimensional algebras over k, associative or not.

For our purposes we add the following restrictions: (1) *Multiplication is associative and admits an identity element* $1 \neq 0$. (2) *The underlying space* $|R|$ *of* R *is irreducible.* The resulting structure will be called a *ring variety*. (Note: this definition is less restrictive than the noncategorical one given in [5].) Similarly, a *module variety* over the ring variety R is a commutative group variety M endowed with a regular mapping $R \times M \to M$ making M into a (unitary) module over the ring R. If in addition R is commutative and M is itself a ring variety in such a way that the underlying ring $|M|$ is an algebra over $|R|$, we call M an *algebra variety* over R; it is equivalent to have a regular ring homomorphism of R into the center of M.

These structures were introduced in [5], where it was shown how to put on every commutative Artin local ring R with residue field k a compatible structure of

Received by the editors February 7, 1963.

(1) Work supported by Air Force Grant AFOSR 62-57.

ring variety. Recall: If R has the same characteristic as k, then there is a lifting $k \to R$ (according to the theorem of Cohen [4]), and R gets the ring variety structure of a finite-dimensional algebra over k. In the other case the characteristic of k is $p > 0$, and that of R is p^{n+1}, $n \geqq 0$. For example, take the ring $W_n(k)$ of Witt vectors of length $n + 1$ (cf. [11]). It can then be shown that R is canonically a finite module over $W_n(k)$, hence a direct sum of cyclic submodules, and the structure of ring variety can be deduced from this. Similarly, every finite module over R gets a compatible structure of module variety. The structure obtained is *maximal* in that every linear mapping is regular; in particular, any other structure is a purely-inseparable image of the maximal one.

(We take this opportunity to correct a small error in [5, Proposition 4, (5), p. 629]. It is necessary to assume that the homomorphism $k \to k$ induced by $\mathfrak{R} \to \mathfrak{R}'$ is the identity, so that $\overline{\mathfrak{R}} \to \overline{\mathfrak{R}}'$ is $W_n(k)$-linear; otherwise the given homomorphism $\overline{\mathfrak{R}} \to \overline{\mathfrak{R}}'$ need not be regular. For example, the endomorphism $x \xrightarrow{\phi} x^{1/p}$ of Ω is certainly not regular. And it must be emphasized that the "extension" mentioned in that proposition refers to "extension of scalars." For example, ϕ is not the extension to Ω of the identity map on the finite field k with p elements; the identity map on Ω is.)

2. The chain conditions.

PROPOSITION 2.1. *Let M be a module variety over the ring variety R. Then every submodule of M is closed and irreducible. Both the ascending and descending chain conditions hold for submodules of M.*

Proof. If the submodule has finitely many generators $x_1, \cdots, x_n$, it is the image of R^n under the regular map $(a_1, \cdots, a_n) \to a_1x_1 + \cdots + a_nx_n$. It is therefore irreducible and contains a nonempty open of its closure. Since it is also a subgroup of M, it must be closed [1, Corollary C, p. 3–02]. An arbitrary submodule is the union of an ascending chain of finitely generated submodules, hence by dimension is finitely generated. The two chain conditions then follow from the same chain conditions for arbitrary irreducible closed subsets.

COROLLARY 2.2. *The underlying ring of a ring variety is Artinian (on both sides).*

QUESTION. Which Artinian rings can be obtained as underlying rings of ring varieties? We answer this later in the commutative case (8.3).

3. **Quotients.** Let N be a submodule of the R-module variety M. We can form the quotient group variety M/N, together with the canonical regular homomorphism $q: M \to M/N$. The mapping $(a, x) \to q(ax)$ of $R \times M \to M/N$ is constant on the cosets of $0 \times N$; hence there is an induced structure of R-module variety on M/N.

In case $M = R$ and N is a two-sided ideal in R, the same argument shows that the induced multiplication on R/N is a regular mapping, hence we can form the quotient ring-variety R/N.

4. The additive group variety. We can characterize the underlying additive group variety of a ring variety, using the structure theory of algebraic groups.

LEMMA 4.1. *If A is an abelian variety and $f: A \times A \to A$ is a biadditive regular map, then $f = 0$.*

Proof. By a basic theorem on abelian varieties [3, p. 9–02, Proposition 1], there are regular maps $f_i: A \to A$, $i = 1,2$, such that $f(x,y) = f_1(x) + f_2(y)$. From biadditivity, we see

$$f_1(x) = f_2(y + y') - f_2(y) - f_2(y')$$

and taking $y' = 0$, f_1 is constant. Similarly f_2 is constant, hence $f = 0$.

LEMMA 4.2. *Let G be a group variety which admits a regular biadditive map of $G \times G$ onto G. Then G is linear.*

Proof. By a structure theorem on group varieties (cf. [6]), G has a unique maximal linear subgroup L; L is normal and G/L is an abelian variety. If we denote the given biadditive map multiplicatively, then for every $a \in G$, $aL \subset L$, $La \subset L$, since these subgroups are also linear (being homomorphic images of linear groups; cf. [6]). Hence there is an induced biadditive map on G/L, which is trivial by Lemma 1. Therefore $G \cdot G \subset L$, whence by hypothesis, $G = L$.

PROPOSITION 4.3. *The underlying additive group variety G of a ring variety R is unipotent.*

Recall that a unipotent algebraic group is one which is isomorphic to a group of matrices with all proper values equal to 1; equivalently, it is a group variety all of whose composition factors are isomorphic to G_a, the additive group of the line.

Proof. By 4.2, G is a commutative linear group. According to the structure theory of such groups [1, Theorem 4, pp. 4–12], G decomposes into the direct product $G_s \times G_u$ of a torus and a unipotent group. Now in a unitary ring there always exist natural numbers n prime to the characteristic of k such that multiplication by n is injective. But a torus always has points of order n. Hence $G = G_u$.

COROLLARY 4.4. *The variety underlying a ring variety is affine space.*

COROLLARY 4.5. *If k has characteristic 0, the underlying additive group variety of any ring variety over k is a vector group.*

For in characteristic 0, G_a^n is the only unipotent group variety of dimension n.

COROLLARY 4.6. *The additive group variety M^+ of any module variety M over a ring variety R is unipotent.*

Proof. M^+ is a quotient of some $(R^+)^n$, hence is unipotent [1, Corollary, pp. 4–11].

QUESTION. In characteristic $p > 0$, can every unipotent group variety be given the structure of additive group of some ring variety or module variety? (Obviously every vector group can.) If not, what are the necessary and sufficient conditions?

5. **Ring varieties in characteristic 0.**

PROPOSITION 5.1. *The category of ring varieties over an algebraically closed field k of characteristic 0 is equivalent to the category of finite dimensional associative unitary algebras over k.*

Proof. By 3.5, we may assume the underlying additive group of R to be G_a^n. Any biadditive mapping $G_a^n \times G_a^n \to G_a^n$ in characteristic 0 must be given by bilinear polynomials. Hence if G_a^n is given its natural structure of vector space over k, R becomes a finite dimensional algebra over k. Moreover every regular homomorphism $G_a^m \to G_a^n$ in characteristic 0 must be a linear transformation. The converse statements are clear.

In characteristic $p > 0$, the additive group G of R is a vector group if and only if the ring R has characteristic p (in general it will have characteristic a power of p by 4.3). Even in this case, a biadditive mapping on G_a^n need no longer be given by bilinear polynomials. Moreover, even if a ring variety R has a compatible structure of finite dimensional algebra over k, this structure need not be intrinsic.

EXAMPLE. Consider the ring variety $k \times k$ (multiplication and addition coordinatewise). Define scalar multiplication by

$$t(x, y) = (tx, t^p y).$$

We obtain an algebra over k. The map $(x, y) \to (y, x)$ is an automorphism of the ring variety but not of the algebra, i.e., does not respect scalar multiplication.

6. **The group of units.** The property in the next theorem was unnecessarily taken as part of the definition of a ring variety in [5].

THEOREM 6.1. *The units in a ring variety form an open subvariety (in the Zariski topology) and under the induced multiplication form a group variety.*

Proof. Consider the multiplication $m: R \times R \to R$. Let $U_1 = m^{-1}(1)$, a closed subspace of $R \times R$. U_1 becomes an algebraic group when we take as multiplication the restriction of $m \times m$, the inverse map being the restriction of the symmetry $(x, y) \to (y, x)$. Let π: $U_1 \to R$ be the projection on the first factor. Then π is an isomorphism of U_1 on the group U of units, as abstract groups.

Now $\pi(U_1)$ contains a nonempty relatively open subset V of its closure (follows from [2, Corollary 1, p. 92]). As x runs through U, the relative opens xV cover U; hence U is open in its closure.

Suppose $P_1(X, Y), \cdots, P_n(X, Y)$ are the polynomials determining the multiplication in some affine coordinate system on R. Then the Jacobian matrix

$$\left(\frac{\partial P_i}{\partial X_j}\right)_{(X,Y)=(1,1)}$$

of the mapping π at the point (1,1) of $R \times R$ is just the identity matrix of dimension n, hence has rank n. Therefore the mapping π is unramified at (1,1), and U_1 has dimension n at this point. It follows that π is birational from U_1 to R [2, p. 211, Corollary 2] and that U has dimension n, hence is open in R.

(I am indebted to C. Chevalley for the last part of this argument. Incidentally, this shows that in the axioms for a group variety, it is unnecessary to assume $x \to x^{-1}$ regular.)

COROLLARY 6.2. *A ring variety admits a birational transformation i into itself whose domain is the group of units and which satisfies $i(x) = x^{-1}$ for every unit x.*

COROLLARY 6.3. *On a ring variety R, there is a regular function $d: R \to k$ such that $x \in R$ is a unit if and only if $d(x) \neq 0$.*

Namely, take $d(x)$ to be the common denominator for the coordinates of x^{-1} when the latter are written as rational functions in the coordinates of x.

(The function d generalizes the *determinant* in a matrix ring; *conjecturally*, $d(xy) = d(x)\, d(y)$ for suitable choice of d.)

7. **Division rings.**

PROPOSITION 7.1. *Up to isomorphism there is a unique ring variety whose underlying ring is a division ring, namely the affine line k with its given structure of field.*

Proof. Let R be such a ring variety. The underlying variety of R is k^n(3.4), and the inverse map $i: x \to x^{-1}$ of R is birational (6.2). But the set of nondefinition of i has codimension 1; since it is reduced to a single point we must have $n = 1$. Hence we can assume the additive group of R to be G_a.

Multiplication, being biadditive, must then have the form

$$(x,y) \to \sum_{i,j} a_{ij} x^{p^i} y^{p^j}$$

(where p is the exponent-characteristic of k). A calculation of degrees in the associative law shows that this polynomial must reduce to axy, with $a \neq 0$. The mapping $x \to a^{-1}x$ is then an isomorphism of the standard field variety with R.

NOTE. The above argument also determines all one-dimensional ring varieties up to isomorphism.

8. Commutative ring varieties in characteristic $p > 0$.

PROPOSITION 8.1. *Every commutative ring variety decomposes uniquely into a finite direct product of local ring varieties.*

We call a ring variety with a unique maximal ideal a *local ring variety*. Since the underlying ring $|R|$ of R is commutative Artinian (2.4), we have $|R| = |R_1| \times \cdots \times |R_n|$ with $|R_i|$ local, uniquely [12, Theorem 3, p. 205]. Each $|R_i|$, being an ideal, has an induced structure of ring variety R_i. We must show that the decomposition is biregular. The map from the product to R is regular since the map is $(x_1, \cdots, x_n) \to x_1 + \cdots + x_n$.

The inverse mapping is $x \to (xe_1, \cdots, xe_n)$, where $1 = e_1 + \cdots + e_n$, hence is also regular.

NOTE. Direct product decompositions for *module varieties* are not in general biregular. For example, let $M = G_a^2$ with scalar multiplication

$$t(x, y) = (tx, t^p y).$$

Let $N =$ all (x, x^p), $N' =$ all $(x, 0)$. Then the projection of M on N along N' is given by $(x, y) \to (y^{1/p}, y)$.

Proposition 8.1 reduces our study to the case of a commutative local ring variety R. Let M be the maximal ideal of R, so that $R/M = k$ (7.1 and §3). We know that the underlying ring $|R|$ of R is canonically a finite algebra over a ring $W_n(k)$ of Witt vectors, if $|R|$ has characteristic p^{n+1} [5].

THEOREM 8.2. *If R is a commutative local ring variety of characteristic p^{n+1} ($p =$ characteristic of k), then the canonical structure of a finite algebra over $W_n(k)$ on the underlying ring $|R|$ of R is compatible with the structure of variety on R, i.e., the canonical homomorphism $W_n(k) \to R$ is regular.*

Proof. Let $U = R - M$ be the group of units in R, ψ: $R \to k$ the canonical homomorphism. We have a strictly exact [7, p. 163] sequence of commutative group varieties

$$1 \to (1 + M) \to U \xrightarrow{\psi} G_m \to 1.$$

Since $1 + M$ is unipotent, there is a unique regular homomorphism $\mu: G_m \to U$ which splits this sequence ([7, p. 171] gives Ext (G_m, Unipotent) $= 0$). For any $t \in G_m$, $\mu(t)$ is the *multiplicative representative* of t.

We claim μ, as a *rational* map $k \to R$, is defined at 0 and $\mu(0) = 0$: For n sufficiently large, the regular map $x \to x^{p^n}$ of R into R is constant on the cosets of M, hence factors through a regular map $\lambda: k \to R$. For $t \in G_m$ we have $\lambda(t) = \mu(t^{p^n})$. Hence 0 is the unique adherence value for μ at 0 [2, Proposition 5, p. 125], whence by Zariski's Main Theorem $\mu(0) = 0$.

We have thus shown that the multiplicative representatives $\mu: k \to R$ are given by a regular map.

It follows that the mapping

$$(x_0, \cdots, x_n) \to \mu(x_0) + \mu(x_1)p + \cdots + \mu(x_u)p^n$$

is a regular bijective mapping of affine $(n+1)$-space onto a subring variety (by the same argument as in the proof of 2.1 this is a closed subvariety) R_0 of R. Now the Witt-vector $\sum_{i=0}^{n} \mu(x_i)p^i$ has coordinates $(x_0, x_1^p, \cdots, x_n^{p^n})$. Therefore to show that the induced ring isomorphism $W_n(k) \xrightarrow{\sim} R_0$ is a regular map, we must show that the map

$$x \to \mu(x)p^m$$

of k into R_0 has order of inseparability at least p^m, for all $m = 1, \cdots, n$, so that the mapping

$$x \to \mu(x^{1/p^m})p^m$$

is regular. This will be a consequence of the following lemma, due to J.-P. Serre, which generalizes a formula on Witt vectors.

LEMMA. *Let G be a commutative group variety over the field k of characteristic $p > 0$. Then for every $m > 0$ there is a factorization*

$$p^m = V_m F^m$$

where this p^m means "multiplication by p^m," F^m is the Frobenius mapping iterated m times, and V_m is a suitable regular map.

(Recall that F^m is the canonical mapping of G onto the variety $G_{(m)}$ with the same base space but sheaf of p^mth powers of the regular functions on G.)

We factor p^m by

$$G \xrightarrow{\delta} G^{(p^m)} \xrightarrow{\sigma} G$$

where the middle term is the symmetric product of G with itself p^m times, δ is the diagonal map and σ is the sum. By [7, Proposition 21, p. 62], δ is a homeomorphism onto a subvariety isomorphic to $G_{(m)}$.

COROLLARY 8.3. *If k has characteristic $p > 0$, the commutative rings which can occur as underlying rings of ring varieties over k are the finite algebras over Witt rings with coefficients in k.*

9. Noncommutative ring varieties.

PROPOSITION 9.1. *If R is a ring variety, then its center C is a closed subspace and inherits a structure of commutative unitary associative algebraic ring.*

Proof. For every $x \in R$, the centralizer $C(x)$ is the kernel of the additive homomorphism

$$y \to xy - yx,$$

hence is closed. C is the intersection of all $C(x)$'s.

C need not be a ring variety, i.e., need not be connected as is shown by the following.

EXAMPLE 9.2. Let R have additive group G_a^2 with multiplication

$$(x_0, x_1)(y_0, y_1) = (x_0 y_0, x_0 y_1 + x_1 y_0^{p^n}).$$

The center C is the finite field with p^n elements, i.e., all $(a_0, 0)$ such that $a_0^{p^n} = a_0$.

Thus 8.3 is false when we drop the assumption of commutativity. However we do have a necessary and sufficient condition.

PROPOSITION 9.3. *(Still in characteristic $p > 0$.) The ring variety R has a structure of algebra variety over some $W_n(k)$ if and only if the center C of R is connected.*

If R is an algebra variety over $W_n(k)$, then C, being a finite module over $W_n(k)$, must be connected. Conversely, if C is a commutative ring variety, then by §8 it has a natural structure of algebra variety over some $W_n(k)$, hence R has.

PROPOSITION 9.4. *(In any characteristic.) Up to isomorphism, the only ring varieties whose underlying rings are simple are the full matrix rings with coefficients in k.*

The theory of simple Artin rings tells us the underlying ring is a matrix ring over a division ring. However we require an isomorphism of *ring varieties.*

Let (e_{ij}) be a system of matrix units in R. Put $e = e_{11}$. The division ring we want may be taken to be eRe. Since $x \to exe$ is a regular homomorphism of R^+, eRe is a subgroup variety of R^+. Multiplication in eRe is the restriction of multiplication from R, hence is given by a regular map. Thus eRe is a ring variety which by 7.1 is isomorphic to k.

Finally we obtain a biregular isomorphism of R with the ring of $n \times n$ matrices over k as follows: An element $x \in R$ is assigned the matrix $(e_{1j} x e_{j1})_{i,j}$. A matrix $(a_{ij})_{i,j}$ is sent back to the element

$$\sum_{i,j} e_{i1} a_{ij} e_{1j}$$

in R.

COROLLARY 9.5. *The semi-simple ring varieties are the direct products of matrix rings over k.*

As in the proof of 8.1, the direct product decomposition is biregular.

10. **Rationality questions.** Suppose now R is a ring variety and k_0 is a field of definition for the underlying variety and for the addition and multiplication maps of R. The set R_0 of points of R rational in k_0 then forms a subring.

PROPOSITION 10.1. *If k_0 is perfect and the ring variety R is defined over k_0, then for any ideal $\mathfrak{a}$ of R_0, we have $\mathfrak{a}R \cap R_0 = \mathfrak{a}$ and R_0 is an Artin ring.*

Proof. Assume first $\mathfrak{a}$ has finitely many generators $a_1, \cdots, a_n$. Define a regular map f of R^n onto $\mathfrak{a}R$ by

$$f(x_1, \cdots, x_n) = x_1 a_1 + \cdots + x_n a_n.$$

Then f is defined over k_0. Let $\mathfrak{b} = f^{-1}(0)$. Then $\mathfrak{b}$ is a module variety for R defined over k_0 (since k_0 is perfect). In particular, $\mathfrak{b}$ is unipotent (4.6), and since k_0 is perfect, $\mathfrak{b}$ is k-solvable [6].

If now $c \in \mathfrak{a}R \cap R_0$, $f^{-1}(c)$ is a principal homogenous space for $\mathfrak{b}$ defined over k_0, hence admits a rational point in k_0 [7, p. 170, Lemma 2]. Thus $c \in \mathfrak{a}$.

An arbitrary ideal in R_0 is the union of an ascending chain of finitely generated ideals. Raising this chain to R, we see it is finite; contracting to R_0 then shows the original chain is finite. Similarly the descending chain condition holds in R_0.

NOTE. 10.1 generalizes at once to module varieties of R defined over k_0.

QUESTION. If an ideal in R is k_0-closed and k_0 is perfect, does the ideal admit a set of generators rational over k_0? One can ask more generally whether a module-variety M defined over the perfect field k_0 is generated as a module by its rational points M_0. The answer is yes when k_0 is infinite, for by a result of Rosenlicht, M_0 is then dense in M.

11. **Concluding remarks.** We have seen that the center of a noncommutative ring variety need not be connected. Thus we are led to the general study of a unitary associative algebraic ring R. It is obvious that the connected component R_1 of 0 is a two-sided ideal, and R/R_1 is a finite ring. R_1 is a connected associative algebraic ring, but need not have an identity element. Thus the correct category stable under these natural operations is that of associative algebraic rings, not necessarily connected and not necessarily unitary.

We mention a further extension: In characteristic $p > 0$, the ring of regular endomorphisms of the additive group G_a consists of all p-polynomials

$$P(x) = \sum_{j=0}^{\infty} a_j x^{p^j}, \quad \text{almost all } a_j = 0,$$

with the multiplication given by $(QP)(x) = Q(P(x))$. The completion of this ring consists of all p-power series and is coordinatized by infinite-dimensional affine space; it is the projective limit of a system of ring varieties. Thus we are led to the category of *pro-algebraic rings*, analogous to that of pro-algebraic groups

[8]. One can ask whether these considerations extend to the ring of endomorphisms of an arbitrary commutative algebraic group.

Bibliography

1. C. Chevalley, *Classification des groupes de Lie algébriques*. I, Inst. Henri Poincaré, Paris, 1956–1958.

2. ———, *Fondements de géométrie algébrique*, Inst. Henri Poincaré, Paris, 1958.

3. ———, *Variétés de Picard*, Inst. Henri Poincaré, Paris, 1958–1959.

4. I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. **59** (1946), 54–106.

5. M. J. Greenberg, *Schemata over local rings*, Ann. of Math. (2) **73** (1961), 624–648.

6. M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443.

7. J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

8. ———, *Groupes proalgébriques*, Inst. Hautes Études Sci. Publ. Math. **7** (1960), 341–403.

9. ———, *Sur les corps locaux à corps résiduel algébriquement clos*, Bull. Soc. Math. France **89** (1961), 105–154.

10. A. Weil, Exposé 186, Séminaire Bourbaki, IIième année, Inst. Henri Poincaré, Paris, 1958–1959.

11. E. Witt, *Zyklische Korper und Algebren der Characteristik p vom* Grad p^n, J. Reine Angew. Math. **176** (1936), 126–140.

12. O. Zariski and P. Samuel, *Commutative algebra*, Vol. 1, Van Nostrand, Princeton, N. J. 1958.

University of California,
Berkeley, California