PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 7, July 1998, Pages 2123–2129
S 0002-9939(98)04257-9

THE REGULAR ELEMENT PROPERTY

FRED RICHMAN

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. The property that an ideal whose annihilator is zero contains a regular element is examined from the point of view of constructive mathematics. It is shown that this property holds for finitely presented algebras over discrete fields, and for coherent, Noetherian, strongly discrete rings that contain an infinite field.

Let R be a commutative ring and M an R-module. For any subset I of R, we write

$$\mathcal{A}_M(I) = \{x \in M : Ix = 0\}$$

for the annihilator of I in M, which is a submodule of M. An element r in R is said to be **M-regular** if $\mathcal{A}_M(r) = 0$.

We say that R has the **regular element property** (**REP**) if for each finitely presented R-module M, and finitely generated ideal I, if $\mathcal{A}_M(I) = 0$, then I contains an M-regular element.

According to Kaplansky [2, page 65], the theorem that a Noetherian ring has the REP is "a result that is among the most useful in the theory of commutative rings." In particular, it is basic to the characterization of depth, for local rings with residue class field k, as the least n such that $\mathrm{Ext}^n(k, M) \neq 0$: it says that if $\mathrm{Ext}^0(k, M) = 0$, then the depth of M is at least 1.

We will investigate this theorem from the point of view of constructive mathematics in the sense of Bishop [1], that is, mathematics done in the context of intuitionistic logic. The casual reader should be able to follow the discussion by thinking in terms of computations and constructions. Notice that if we can interpret the above theorem computationally, and we can always calculate a finite set of generators for $\mathcal{A}_M(I)$, then it tells us how to construct maximal regular sequences.

1. A constructive look at Noetherian rings

First, let's look at the main ideas involved from this point of view. A ring R is **Noetherian** if, given a chain of finitely generated ideals

$$I_1 \subset I_2 \subset I_3 \subset \cdots,$$

you can find n such that $I_n = I_{n+1}$. Not a place where the chain stabilizes, that's too much to ask, but a place where the chain pauses. From a constructive point of view, you can't show that ascending chains of ideals stabilize even over the two-element field: you need not be able to tell whether there is an ideal in

Received by the editors August 21, 1996 and, in revised form, December 17, 1996.
1991 *Mathematics Subject Classification.* Primary 03F65, 13E05; Secondary 13P99, 13C15.

the chain that contains 1, so you can't compute where the chain stabilizes. From a noncomputational point of view, the two notions are equivalent because if the chain does not stabilize, then it has a strictly increasing subchain. Similarly, the restriction to finitely generated ideals is inessential from a classical point of view because, in that context, the ascending chain condition on ideals is equivalent to the ascending chain condition on finitely generated ideals.

Classically every Noetherian ring is **coherent**—finitely generated ideals are finitely presented—but from a computational point of view, this is an additional feature. For example, in a coherent module the intersection of two finitely generated submodules is finitely generated; the construction of those generators requires more than invoking an ascending chain condition. So we will speak, seemingly redundantly, of a coherent Noetherian ring. If R is coherent, and M is a finitely presented R-module, then $\mathcal{A}_M(I)$ is finitely generated for any finitely generated ideal I of R [3, Theorems VIII.2.4 and VIII.2.6].

A set S is said to be **discrete** if for all $x, y \in S$, either $x = y$ or $x \neq y$. From a computational point of view this means that you can determine which alternative holds. The rational numbers form a discrete field. The real numbers are an example of a field that cannot be shown to be discrete. The problem is that no matter how close a rational approximation you have to a real number, you need not be able to tell whether the real number is zero. A ring R is **strongly discrete** if R/I is discrete for each finitely generated ideal I. This means that you can decide whether or not an element of R is in I—we say that I is **detachable**.

Let k be a discrete field. The polynomial ring $k[X_1, \ldots, X_n]$ is coherent, Noetherian, and strongly discrete, as are its quotients modulo finitely generated ideals. This follows from a constructive Hilbert basis theorem [3, Theorem VIII.1.5]. However, Seidenberg [4] showed that you can find primary decompositions of finitely generated ideals in $k[X_1, \ldots, X_n]$ if and only if k satisfies two conditions, which he called F and P. Condition F says that k is **factorial**: any polynomial in $k[X]$ can be written as a product of irreducible factors. Condition P deals with the case when k has finite characteristic p. In its simplest form it says that any finitely generated k^p-subspace of k is finite dimensional over k^p (in [3, VII.3.1] this is shown to be equivalent to Seidenberg's original formulation).

If k is not factorial, then $k[X_1, \ldots, X_n]$ is coherent, Noetherian, and strongly discrete, but we can't find primary decompositions of finitely generated ideals. The simplest example is gotten by letting k lie between the rational numbers $\mathbf{Q}$ and the Gaussian numbers $\mathbf{Q}(i)$. That is, if you will, k is either $\mathbf{Q}$ or $\mathbf{Q}(i)$, but we don't know which. This lack of knowledge does not prevent us from carrying out computations over k, such as the Euclidean algorithm in $k[X]$. But it does prevent us from factoring $X^2 + 1$ into irreducible factors. In particular, we can't find the primary decomposition of the ideal generated by $X^2 + 1$.

We say that a ring is a **Lasker-Noether** ring if it is coherent, Noetherian, strongly discrete, and the radical of each finitely generated ideal is the intersection of a finite number of finitely generated prime ideals. In a Lasker-Noether ring, each finitely generated ideal has a primary decomposition [3, Theorem VIII.8.5]. In this language, Seidenberg's theorem says that $k[X_1, \ldots, X_n]$ is a Lasker-Noether ring for all n if and only k is factorial and satisfies Condition P. Finite fields clearly have these properties, while the rational numbers are factorial by a well-known argument of Kronecker.

We will show that Lasker-Noether rings have the regular element property, but that is a lot to assume. After all, $k[X]$ has the regular element property for any discrete field k because finitely presented modules over $k[X]$ are direct sums of finitely presented cyclic modules (reduce the appropriate matrix over $k[X]$ to Smith normal form). Our main result is that $k[X_1, \ldots, X_n]$ has the regular element property for any n and any discrete field k. Along the way we show that any coherent, Noetherian, strongly discrete ring that contains an infinite field has the regular element property.

2. The REP and Kaplansky's Theorem 82

The regular element property is not exactly what Kaplansky was talking about in [2, Theorem 82], but I think the statement in the introduction is still accurate. It is instructive to examine the differences.

First off, Kaplansky was talking about the contrapositive property, **REP′**, which states that if $\mathcal{A}_M(r) \neq 0$ for every element r in an ideal I, then $\mathcal{A}_M(I) \neq 0$. That is, if an ideal consists of zero-divisors on M, then there is one witness in M to that fact that works for the whole ideal. Most people don't worry about the distinction between a statement and its contrapositive, but for our purposes it is important. For one thing, we are interested in constructing regular sequences, and REP′ provides no mechanism for doing that. The hypothesis of REP is easy to check because if I is generated by $r_1, \ldots, r_n$, then

$$\mathcal{A}_M(I) = \mathcal{A}_M(r_1) \cap \mathcal{A}_M(r_2) \cap \cdots \cap \mathcal{A}_M(r_n)$$

and, if R is coherent, we can find generators of the submodules $\mathcal{A}_M(r_i)$ and their intersection. The hypothesis of REP′ is difficult to check, even though we can calculate $\mathcal{A}_M(r)$, because we must consider each r in the ideal I, not just in a finite generating set.

The submodules $\mathcal{A}_M(r)$ and $\mathcal{A}_M(I)$ are finitely generated if M is coherent, so if M is also discrete, then they are either zero or nonzero. Because of this, REP′ is the contrapositive of REP, hence follows from it. But not vice versa, at least not within intuitionistic logic.

The second difference is that Kaplansky considers a subring I (not required to have an identity) rather than an ideal. This is a substantive difference from anyone's point of view, but the domain of application is not significantly narrowed by considering only ideals, as most treatments do. To clarify the difference, we can rephrase the REP (respectively, the REP for subrings) to read:

> If F is a finite subset of R such that $\mathcal{A}_M(F) = 0$, then the ideal (respectively, subring) generated by F contains an M-regular element.

The point is that if $\mathcal{A}_M(S) = 0$ for a subset S of a Noetherian ring, then (classically) $\mathcal{A}_M(F) = 0$ for some finite subset F of S. The reader might note that in our applications, Corollaries 5 and 6, the ring is an algebra over a field and we actually show that the subalgebra generated by F contains an M-regular element. Also, in Corollary 2, where the ring is required to be a Lasker-Noether ring, the proof referred to is the standard one which shows that the subring generated by F contains an M-regular element.

3. Primary decomposition and the REP

If M is an R-module, then a prime ideal P of R is an **associated prime ideal** of M if $P = \mathcal{A}_R(x)$ for some x in M. The associated prime ideals of an ideal I of R are the associated prime ideals of the module R/I. If R is a Lasker-Noether ring, and M is finitely presented, then we can find a complete set of associated prime ideals of M.

Theorem 1. *Let R be a Lasker-Noether ring and M a finitely presented R-module. Then the associated prime ideals of M are finitely generated and form a finite set.*

Proof. Proceed by induction on the number of generators of M. If M is cyclic, then the primes associated with M are simply the primes associated with the ideal $\mathcal{A}_R(M)$. If M is generated by $n > 1$ elements, then let N be the submodule generated by the first $n-1$ of them. By induction, the prime ideals associated with N and M/N are finitely generated and form a finite set. We first show that the primes associated with M are among those.

Suppose $P = \mathcal{A}_R(x)$ is a prime ideal for some x in M. Because P is prime, $P = \mathcal{A}_R(y)$ for any nonzero y in Rx. So if $Rx \cap N \neq 0$, then P is associated with N, while if $Rx \cap N = 0$, then P is associated with M/N.

Now we have to eliminate those primes that are associated with N or with M/N, but not with M. Suppose P is any finitely generated prime ideal. Consider $K = \mathcal{A}_M(P)$, which is a finitely generated R/P-module. Then P will be associated with M exactly when K has an R/P-regular element. Because R/P is a domain, this happens exactly when one of the generators of K is R/P-regular, and we can test a generator z because $\mathcal{A}_R(z)$ is finitely generated, and P is detachable. □

Corollary 2. *If R is a Lasker-Noether ring, then R has the regular element property.*

Proof. Let M be a finitely presented module, I a finitely generated ideal such that $\mathcal{A}_M(I) = 0$. Let $P_1, \ldots, P_n$ be the primes associated with M. Then I is certainly not contained in any P_i. So there is an element r in I that is not in any P_i. This is the standard maneuver—for a constructive treatment see [3, II.2.3]. We need the fact that I is finitely generated and the P_i are detachable.

Why is r an M-regular element? If $rx = 0$, then the primes associated with the ideal $\mathcal{A}_R(x)$ contain r and are among the P_i. So there are no primes associated with $\mathcal{A}_R(x)$, that is, $x = 0$. □

4. The ring $k[X_1, \ldots, X_n]$ has the REP

First we observe a very general fact about annihilators.

Lemma 3. *Let R be a commutative ring and M an R-module. Let $I_1, \ldots, I_n$ be ideals in R, and set $N_i = \mathcal{A}_M(I_i)$. If $N_i \cap N_j = 0$ for all $i \neq j$, then the N_i are independent submodules of M.*

Proof. It suffices to show that $N_m \cap (N_1 + \cdots + N_{m-1}) = 0$. Suppose $x_m = x_1 + \cdots + x_{m-1}$ with $x_i \in N_i$. Then $I_m x_m = 0$, so $I_m x_i = 0$ for each $i < m$ because $N_1, \ldots, N_{m-1}$ are independent by induction. Therefore $x_i \in N_m \cap N_i = 0$ for each $i < m$. □

The next theorem is slightly technical. It has the logical form

$$\forall n(A_n \vee B) \Rightarrow B$$

which may seem a bit strange because in classical logic that is equivalent to $\forall n\, A_n \Rightarrow B$ as the hypothesis is equivalent to $(\forall n\, A_n) \vee B$. From a constructive point of view the latter hypothesis is stronger, as it involves the determination of whether $\forall n\, A_n$ holds or B holds. A classic example, close to our application here, is the construction of a primitive element in a separable field extension. The classical argument divides into two cases, depending on whether the field is finite or infinite. Think of A_n as saying that the field contains at least n elements, so $\forall n\, A_n$ says that the field is infinite. It turns out that you just need lots of elements, not an infinite number, for the infinite case argument to go through. So if, for each n, you can show that the field contains at least n elements, or is finite, then you can prove the theorem without deciding whether the field is infinite.

For our application, the u_i below will be taken from a subfield of R.

Theorem 4. *Let R be a coherent, Noetherian, strongly discrete ring, I a finitely generated ideal of R, and M a finitely presented R-module such that $\mathcal{A}_M(I) = 0$. Let $u_1, u_2, \ldots$ be a sequence of elements of R such that for each n, either $u_i - u_j$ is M-regular for all distinct i, j in $\{1, \ldots, n\}$, or there is an M-regular element in I. Then there is an M-regular element in I.*

Proof. Let $r_0, \ldots, r_m$ generate I. Consider the sequence of elements

$$s_i = r_0 + u_i r_1 + u_i^2 r_2 + \cdots + u_i^m r_m$$

in I, and set $N_i = \mathcal{A}_M(s_i)$. If $N_i = 0$, then s_i is our desired element. Our hypotheses imply that N_i is finitely generated, and M is discrete, so either $N_i = 0$ or we can find a nonzero element of N_i. The idea is to look at the submodules N_i, and their various intersections, construct an ascending chain of finitely generated submodules of M, and invoke the Noetherian property of M to find i such that $N_i = 0$.

We first show that the intersection of any $m + 1$ of the N_i is zero, or there is an M-regular element in I. Suppose $s_i x = 0$ for $i = i_0, i_1, \ldots, i_m$. Then the Vandermonde determinant

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ u_{i_0} & u_{i_1} & \cdots & u_{i_m} \\ u_{i_0}^2 & u_{i_1}^2 & \cdots & u_{i_m}^2 \\ \vdots & \vdots & \vdots & \vdots \\ u_{i_0}^m & u_{i_1}^m & \cdots & u_{i_m}^m \end{vmatrix}$$

must kill $r_j x$ for each j. But either that determinant is a product of M-regular elements, so $Ix = 0$, whence $x = 0$, or there is an M-regular element in I.

Now consider the following sequence of propositions P_t for $t = 0, 1, \ldots$:

- For each n, either there is an M-regular element in I, or there is a set S of 2^t integers greater than n, such that $\bigcap_{i \in S} N_i \neq 0$.

We know that P_0 holds, and that if P_t holds for $2^t \geq m + 1$, then there is an M-regular element in I. So it suffices to show that P_t implies P_{t+1}.

Accordingly, suppose P_t holds. Then for each n we can construct a sequence of disjoint subsets S_j, each of cardinality 2^t and consisting of integers greater than n,

so that for each j either there is an M-regular element in I, or $\bigcap_{i\in S_j} N_i \neq 0$. As M is Noetherian, there exists q so that

$$\bigcap_{i\in S_q} N_i \subset \sum_{j<q} \bigcap_{i\in S_j} N_i.$$

From this, and the lemma, it follows that either $\bigcap_{i\in S_q} N_i = 0$, in which case there is an M-regular element in I, or there are distinct j and k so that

$$\bigcap_{i\in S_j\cup S_k} N_i \neq 0,$$

proving P_{t+1}. □

Corollary 5. *Let R be a coherent, Noetherian, strongly discrete ring that contains an infinite field. Then R has the regular element property.*

Proof. Let $u_1, u_2, \dots$ be distinct elements of the infinite subfield and invoke Theorem 4. □

Corollary 6. *If k is a discrete field, then $k[X_1, \dots, X_n]$ has the regular element property.*

Proof. Set $R = k[X_1, \dots, X_n]$. Let I be a finitely generated ideal of R, and M a finitely presented R-module such that $\mathcal{A}_M(I) = 0$. Let k_0 be the subfield of k generated by the coefficients of the polynomials generating I, together with the coefficients of the polynomials that make up a finite presentation of M. Set $R_0 = k_0[X_1, \dots, X_n]$. We first show that R_0 has the regular element property.

It's not hard to show that, for each m, either k_0 is finite or contains at least m distinct elements [3, Theorem VI.5.4]. So we can construct a sequence of elements $u_1, u_2, \dots$ in k_0 so that for each m either $u_1, u_2, \dots, u_m$ are distinct, or k_0 is finite. If k_0 is finite, then R_0 has the regular element property by Corollary 2. So R_0 has the regular element property by Theorem 4.

Now we want to find an element r of I such that $\mathcal{A}_M(r) = 0$. Note that $R = k \otimes_{k_0} R_0$. Then there are a finitely generated ideal I_0 of R_0, and a finitely presented R_0-submodule M_0 of M so that $I = k \otimes_{k_0} I_0$ and $M = k \otimes_{k_0} M_0$.

We have $\mathcal{A}_{M_0}(I_0) = 0$ because I_0 generates I, and $M_0 \subset M$. So $\mathcal{A}_{M_0}(r) = 0$ for some r in I_0, as R_0 has the regular element property. Multiplication by r induces a monomorphism $M_0 \to M_0$, hence a monomorphism $M \to M$ (any module over a discrete division ring is flat). Thus $\mathcal{A}_M(r) = 0$. □

5. Localization and the REP

Now that we know that $k[X_1, \dots, X_n]$ has the regular element property, it's of interest to know what happens when we pass to quotients and localizations.

Theorem 7. *If R has the regular element property, then so does R/J for any finitely generated ideal J.*

Proof. Let M be a finitely presented R/J-module. Then $(R/J)^m$ maps onto M with finitely generated kernel K. So R^m maps onto M with kernel equal to the preimage of K in R^m, which is also finitely generated. Thus M is a finitely presented R-module.

A finitely generated ideal of R/J corresponds to a finitely generated ideal of R containing J. Suppose $I \supset J$ is a finitely generated ideal of R such that $\mathcal{A}_M(I) = 0$.

As R has the regular element property, $\mathcal{A}_M(r) = 0$ for some r in I. So R/J has the regular element property. □

Theorem 8. *If R is a coherent ring with the regular element property, and S is a multiplicatively closed subset of R, then R_S has the regular element property.*

Proof. Let M' be a finitely presented R_S-module, and I' an ideal of R_S such that $\mathcal{A}_{M'}(I') = 0$. Then $I' = I_S$ for some ideal I of R, and we have an exact sequence

$$R_S^m \to R_S^n \to M' \to 0$$

of R_S-modules. We may assume that the free generators of R_S^m go to images of elements of R^n in R_S^n. This gives an exact sequence

$$R^m \to R^n \to M \to 0$$

of R-modules. As R_S is a flat R-module, tensoring through with R_S shows that $M' = M_S$. The submodule $\mathcal{A}_M(I)$ is finitely generated, so $M/\mathcal{A}_M(I)$ is finitely presented. Moreover $\mathcal{A}_M(I)$ goes to zero in M_S, because $\mathcal{A}_{M_S}(I_S) = 0$, so $M' = (M/\mathcal{A}_M(I))_S$, whence we may assume that $\mathcal{A}_M(I) = 0$.

As R has the regular element property, there is r in I so that $\mathcal{A}_M(r) = 0$. That is, multiplication by r gives a monomorphism $M \to M$, hence a monomorphism $M_S \to M_S$. □

So finitely presented algebras over discrete fields, and their localizations, have the regular element property. The question remains open as to whether any coherent, Noetherian, strongly discrete ring has the regular element property (without the hypothesis that it contains an infinite field).

References

1. Bishop, Errett, *Foundations of constructive analysis*, McGraw-Hill, 1967. MR **36:**4930
2. Kaplansky, Irving, *Commutative rings*, University of Chicago Press, 1974. MR **49:**10674
3. Mines, Ray, Fred Richman and Wim Ruitenburg, *A course in constructive algebra*, Springer-Verlag, 1988. MR **89d:**03066
4. Seidenberg, Abraham, *Constructions in Algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313. MR **50:**2141

Department of Mathematics, Florida Atlantic University, Boca Raton, Florida 33431-0991

E-mail address: richman@acc.fau.edu