JOURNAL OF COMMUTATIVE ALGEBRA
Volume 6, Number 1, Spring 2014

A THEOREM OF GILMER AND THE CANONICAL UNIVERSAL SPLITTING RING

FRED RICHMAN

ABSTRACT. We give a constructive proof of Gilmer's theorem that if every nonzero polynomial over a field k has a root in some fixed extension field E, then each polynomial in $k[X]$ splits in $E[X]$. Using a slight generalization of this theorem, we construct, in a functorial way, a commutative, discrete, von Neumann regular k-algebra A so that each polynomial in $k[X]$ splits in $A[X]$.

1. Introduction. How do you construct the algebraic closure of a field k? One standard technique is to construct an algebraic extension ring R of k in which every polynomial in $k[X]$ has a root, then divide out by a maximal ideal of R to get a field K, algebraic over k, in which every nonconstant polynomial in $k[X]$ has a root. The ring R is constructed by adjoining indeterminates X_f to k, one for each monic nonconstant polynomial f of $k[X]$, and dividing out by the ideal generated by the polynomials $f(X_f)$. In practice, people often restrict themselves to irreducible polynomials f, but that is not needed and is problematic from a constructive point of view because it assumes that every polynomial can be factored into irreducible polynomials. The maximal ideal is constructed using Zorn's lemma (which, of course, is also problematic from a constructive point of view).

It remains to show that every nonconstant polynomial in $K[X]$ has a root in K. The usual technique, at least before Gilmer's paper [**2**], was to iterate the previous construction a countable number of times. Alternatively, if we could show that every nonzero polynomial in $k[X]$ actually splits over K, that is, factors into linear polynomials in $K[X]$, then it is straightforward to show that K is already algebraically closed. In [**2**], Gilmer showed that if every nonzero polynomial in $k[X]$ has a root in a given extension field K, then each nonconstant polynomial over k already splits in $K[X]$.

Received by the editors on August 27, 2012.
DOI:10.1216/JCA-2014-6-1-101

We would like to give a constructive proof of this very pretty theorem. Essentially, this means finding a proof that does not appeal to the law of excluded middle (see [**5**] for background material). The idea is to determine what computational information you need to factor the given polynomial completely in the extension field.

We deal here exclusively with *discrete* fields, that is, nontrivial commutative rings such that each element is either zero or has an inverse. The computational information here is that we can distinguish the two cases and that we can find the inverse. As it turns out, this is the only information we require. We will sometimes restrict to countable subfields in order to construct an extension field in which a given polynomial has a root. This maneuver is necessary because the polynomial may already have roots in the ground field (of which we are unaware) and we need a systematic way of choosing, in advance, which of these roots is to be identified with the root in the extension field (see [**1**] and [**5**, VI.3, Exercise 1]) should we discover such a root; if the ground field is countable, we can choose the root that appears first in the enumeration.

A monic polynomial with coefficients in a discrete field is *reducible* if we can write it as a product of two polynomials of smaller degree. This is a positive concept–we have to able to construct the factors–as opposed to *irreducible* which means not reducible. We will say that a polynomial over a discrete field is *separable* if it is relatively prime to its (formal) derivative (so it has distinct roots in any extension field).

A discrete field K is *perfect* if every nonzero polynomial over K is a product of separable polynomials. If the characteristic of K is a prime p, then K is perfect exactly when $K = K^p$. In general, K is perfect if, for each prime p, if $pK = 0$, then $K = K^p$ (see [**5**, Theorem VI.7.1]). Every field k can be embedded, essentially uniquely, in a perfect field $\widetilde{k}$ such that if $x \in \widetilde{k}$, then either $x \in k$ or k has finite characteristic p and $x^{p^e} \in k$ for some positive integer e (see [**5**, Theorem VI.7.4]). The field $\widetilde{k}$ is called the *perfect closure* of k. Note that we do not have to know whether the field has finite characteristic in order to form its perfect closure.

We record two lemmas here for later use.

Lemma 1. *Let k be a discrete field and h a monic polynomial with coefficients in k. Let $k[\theta]$ and $k[\lambda]$ be commutative rings containing k*

such that $h(\theta) = 0$ *and* $h(\lambda) = 0$. *If* $g \in k[X]$, *and* $g(\theta) \in k$, *then either* h *is reducible or* $g(\lambda) = g(\theta)$.

Proof. Consider the polynomial $f(X) = g(X) - g(\theta) \in k[X]$, and let $d(X) = \gcd(f(X), h(X))$. As $d(\theta) = 0$, either h is reducible or h divides f. In the latter case, $f(\lambda) = 0$, so $g(\lambda) = g(\theta)$. □

We say that two elements a and b in a commutative ring R are *comaximal* if $Ra + Rb = R$. For convenience, we say that a polynomial f, with coefficients in an arbitrary commutative ring, is *separable* if f and f' are comaximal. The following lemma is a well-known result.

Lemma 2. *Let* R *be a commutative ring.*

1. *If* I *and* J *are comaximal ideals of* R, *then* R/IJ *is naturally isomorphic to* $R/I \oplus R/J$.

2. *If* $f \in R[X]$ *is separable, and* $f = cd$, *then* c *and* d *are comaximal.*

2. Gilmer's theorem. We phrase Gilmer's theorem in terms of an extension that is a discrete reduced commutative ring rather than a discrete field. A ring R is *reduced* if $r^n = 0$ implies $r = 0$ for each $r \in R$.

Theorem 3 (Gilmer). *Let* k *be a discrete field. If* R *is a discrete reduced commutative ring containing* k, *and every nonconstant polynomial over* k *has a root in* R, *then every nonconstant polynomial over* k *splits in* R.

Proof. Let f be a nonconstant polynomial over k. We first show that we can assume that f is separable. Either we can write f as a product of separable polynomials or we can find a prime p so that $pk = 0$. In the former case, we can replace f by each of its factors. In the latter case, we can identify the perfect closure $k^{p^{-\infty}}$ with a subfield of R because, for each $x \in k$ and positive integer e, there is a unique $\lambda \in R$ such that $\lambda^{p^e} = x$ (because every nonconstant polynomial over k has a root in R, and R is reduced). Moreover, every polynomial g over $k^{p^{-\infty}}$ has a root in R because g^{p^e} has a root in R for some e and R is reduced. So in this case we may replace k by the perfect field $k^{p^{-\infty}}$ and thus assume that f is separable.

We may assume that k is countable by replacing k by the subfield of k generated by the coefficients of f. Induction on $\deg f$ will finish the proof if f is reducible. As k is countable, we can construct a splitting field F for f over k (see [**5**, Theorem VI.3.4]). Because f is separable, $F = k[\theta]$ (see [**5**, Corollary VI.5.5]). Let h be a polynomial over k with $h(\theta) = 0$. We proceed by induction on $\deg h$. By hypothesis, there exists $\lambda \in R$ such that $h(\lambda) = 0$. Let $g_1, \ldots, g_m$ be polynomials over k such that

$$f(X) = (X - g_1(\theta)) \cdot \cdots \cdot (X - g_m(\theta)).$$

Then, by Lemma 1, either h is reducible, in which case we are done by induction, or

$$f(X) = (X - g_1(\lambda)) \cdot \cdots \cdot (X - g_m(\lambda)),$$

which shows that f splits in R. □

Note that we don't need the full force of the hypothesis that R is reduced; only that if p is a prime such that $p1 = 0$, then R is reduced. We may not even need that. Of course, fields are reduced rings.

3. von Neumann regular rings. A commutative ring is *von Neumann regular* if every principal ideal is generated by an idempotent. A ring is said to be *discrete* if, for all r, s in the ring, either $r = s$ or $r \neq s$. Clearly discrete fields are discrete, commutative, von Neumann regular rings. The following lemma is [**3**, Theorem 18.7] of Gilmer's book on semigroup rings. The proof there is constructive. See also Lombardi and Quitté [**4**, Proposition IV.8.11].

Lemma 4. *If R is a discrete, commutative, von Neumann regular ring, then $R[X]$ is a Bezout ring.*

We will be interested in rings of the form $k[X]/(f(X))$ where f is a separable polynomial. Classically, such a ring is a product of fields, but we can't say this constructively because we may not be able to factor f into irreducibles. However, we can show that it is a von Neumann regular ring. Clearly, fields are von Neumann regular, and we have the following lemma.

Lemma 5. *Let R be a commutative von Neumann regular ring and f a monic separable polynomial in $R[X]$. Then $R[X]/(f)$ is von Neumann regular.*

Proof. Induction on $\deg f$. Note that $R[X]/(f)$ is discrete because R is discrete and we have the division algorithm for monic polynomials. Suppose a is a nonzero element of $A = R[X]/(f)$, so a is represented by $g \in R[X]$ that is not divisible by f. From Lemma 4, we construct $d = sf + tg$ that divides both f and g. We may assume that d is monic. If $d = 1$, then t is an inverse for g modulo f. Otherwise, f has a nontrivial factorization cd, where c and d are comaximal because f is separable. From Lemma 2, it follows that $k[X]/(f)$ is isomorphic to $k[X]/(c) \oplus k[X]/(d)$, and we are done by induction on $\deg f$. □

Theorem 6. *Let k be a field and $R_n = k[X_1, \ldots, X_n]$. Let $f_i \in k[X_i]$ be monic and nonconstant for $i = 1, \ldots, n$, and let J_n be the ideal of R_n generated by the f_i. Then R_n/J_n is a discrete ring that is naturally isomorphic to*

$$S_n = \frac{(R_{n-1}/J_{n-1})[X_n]}{(f_n(X_n))}$$

and $J_n \cap R_{n-1} = J_{n-1}$. If the polynomials f_i are separable, then R_n/J_n is von Neumann regular.

Proof. There are natural epimorphisms

$$R_n \longrightarrow R_{n-1}[X_n] \longrightarrow (R_{n-1}/J_{n-1})[X_n] \longrightarrow S_n.$$

As the map $R_n \to S_n$ takes J_n to zero, we have a natural epimorphism $R_n/J_n \to S_n$. The natural map from R_{n-1}/J_{n-1} to R_n/J_n induces a map from S_n to R_n/J_n. All these maps take the image of X_i to the image of X_i, so these last two maps are isomorphisms. As the map from S_n to R_n/J_n is one-to-one, it must be one-to-one on R_{n-1}/J_{n-1}, so $J_n \cap R_{n-1} = J_{n-1}$. That R_n/J_n is discrete follows by induction on n because S_n is a direct sum of $\deg f_n$ copies of the vector space R_{n-1}/J_{n-1}.

Finally, if the polynomials f_i are separable, then R_n/J_n is von Neumann regular by induction on n using Lemma 5. □

A commutative ring C is said to be *strongly discrete* if C/I is discrete for every finitely generated ideal I. When C/I is discrete, we say that I is *detachable* from C, that is, for each $c \in C$, either $c \in I$ or $c \notin I$.

Theorem 7. *A discrete von Neumann regular commutative ring R is strongly discrete and reduced.*

Proof. First note that any finitely generated ideal of R is generated by an idempotent because the ideal generated by the idempotents e_1 and e_2 is generated by the idempotent $e_1 + e_2 - e_1e_2$. To see that R is strongly discrete, note that an idempotent e_1 is in the ideal generated by the idempotent e_2 exactly when $e_1e_2 = e_1$, which we can decide because R is discrete. Finally, and this is true whether or not R is discrete, if $r^n = 0$, and $Rr = Re$ for e an idempotent, then $e^n = 0$ so $e = 0$. □

4. The algebraic closure. The algebraic closure of a field k is constructed by introducing an indeterminate X_f for each monic polynomial f of degree greater than zero, forming the ring of polynomials in these indeterminants with coefficients in k, dividing out by the ideal generated by the elements $f(X_f)$, and then dividing out by a maximal ideal in that quotient ring. For k a discrete field, this plan can be carried out constructively except for the last step, which can be done if k is countable. By a maximal ideal here, we mean an ideal whose cokernel is a discrete field.

It is somewhat more convenient for us to pass to the perfect closure of k first. This is a natural construction, unlike the algebraic closure. Then we can restrict ourselves to monic *separable* polynomials f of degree greater than zero.

Theorem 8. *Let k be a discrete field and P a set of monic nonconstant separable polynomials in $k[X]$. Let X_f be an indeterminate for each $f \in P$ and J the ideal in $R = k[X_f : f \in P]$ generated by $\{f(X_f) : f \in P\}$. Then R/J is a discrete, nontrivial, von Neumann regular ring.*

Proof. Let r be an element of R. Let P' be a finite subset of P so that $r \in R' = k[X_f : f \in P']$. Then $J' = R' \cap J$, and R'/J' is discrete and

von Neumann regular, by Theorem 6. The principal ideal generated by the image of r in R'/J' is generated by an idempotent; hence, the same is true for the principal ideal generated by the image of r in R/J. Thus R/J is von Neumann regular. □

To apply this theorem to construct the "canonical universal splitting ring" of an arbitrary discrete field k, we first embed k in its perfect closure K, then let P be the set of monic nonconstant separable polynomials in $K[X]$. The result is a discrete, nontrivial, von Neumann regular, algebraic k-algebra in which every polynomial with coefficients in k has a root. By Theorem 3, every monic polynomial in $k[X]$ splits in this k-algebra.

To get an algebraic closure of k, we map this splitting ring onto a field. We can do this if k is countable.

Theorem 9. *A nontrivial countable strongly discrete ring admits a homomorphism onto a discrete field.*

Proof. Let $r_0, r_1, \ldots$ be an enumeration of the strongly discrete ring R. We construct a maximal ideal of R recursively. Let $I_0 = 0$. Having constructed the proper finitely generated ideal I_n, let $I_{n+1} = Rr_n + I_n$, if $1 \notin Rr_n + I_n$, and $I_{n+1} = I_n$ otherwise. Set M equal to the union of the chain of proper ideals I_n. An element r_n of R is either in $I_{n+1} \subseteq M$, or is invertible modulo $I_n \subseteq M$, so R/M is a (discrete) field. □

To finish this development, we need to prove that if $k \subset C$ are discrete fields with C algebraic over k, and every nonconstant polynomial over k has a root in C, then C is algebraically closed. The key lemma appears to be the following.

Lemma 10. *Let $k \subset C$ be discrete fields with C algebraic over k. If $f \in C[X]$ is a nonzero monic polynomial, then there exists $h \in k[X]$ such that f divides h.*

Proof. Suppose $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in C[X]$. Let k_0 be a countable subfield of k over which $a_0, a_1, \ldots, a_{n-1}$ are algebraic.

Let θ be a root of f in an extension field of $k_0[a_0, \dots, a_{n-1}]$ and h a monic polynomial over k such that $h(\theta) = 0$. As $f(\theta) = h(\theta) = 0$, it follows that $d = \gcd(f, h) \neq 1$. If $d \neq f$, then we are done by induction on $\deg f$. If $d = f$, then f divides h. □

Corollary 11. *Let $k \subset C$ be discrete fields with C algebraic over k. If every nonconstant polynomial in $k[X]$ has a root in C, then C is algebraically closed.*

Proof. Let $f \in C[X]$ be a nonconstant monic polynomial. From the lemma, there exists $h \in k[X]$ such that f divides h. From Theorem 3, we know that h splits in C. So f splits in C. □

Acknowledgments. I'd like to thank Tim Ford for assuring me that the canonical universal splitting ring was reduced, and Warren McGovern for pointing me to Gilmer's proof that a polynomial ring over a von Neumann regular ring is a Bezout ring.

REFERENCES

1. Michael P. Fourman and Andre Scedrov, *The "world's simplest axiom of choice" fails*, Manuscr. Math. **38** (1982), 325–332.

2. Robert W. Gilmer, *A note on the algebraic closure of a field*, Amer. Math. Month. **75** (1968), 1101–1102.

3. ———, *Commutative semigroup rings*, University of Chicago Press, Chicago, 1984.

4. Henri Lombardi and Claude Quitté, *Algèbre commutative, Méthodes constructives*, Calvage & Mounet, Paris, 2011.

5. Ray Mines, Fred Richman and Wim Ruitenburg, *A course in constructive algebra*, Springer, Berlin, 1988.

6. Fred Richman, *van der Waerden's construction of a splitting field*, Comm. Alg. **34** (2006), 2351–2356.

7. B.L. van der Waerden, *Eine Bemerkung über die Unzerlegbarkeit von Polynomen*, Math. Annal. **102** (1930), 738–739.

8. ———, *Modern algebra*, Frederick Ungar Publishing Co., New York, 1953.

Florida Atlantic University, Department of Mathematics, Boca Raton, FL 33431
Email address: fred@math.fau.edu