ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 2, Number 1, Winter 1972

GENERATING SETS FOR A FIELD AS A RING EXTENSION OF A SUBFIELD

ROBERT GILMER[1]

1. **Introduction.** Suppose that F is a subfield of the field L. L can be considered as a field extension of F, as a ring extension of F, or as a vector space over F, and hence the term *generating set for* L *over* F may mean either (1) a subset S of L such that $L = F(S)$, or (2) a subset S of L such that $L = F[S]$, or (3) a subset S of L such that S spans L as a vector space over F. Of course, a generating set in the sense of (3) is a generating set in the sense of (2), and if (2) holds for S, then (1) holds for S. Moreover, (1) and (2) are equivalent if L/F is algebraic.

In this paper we are primarily concerned with *ring generating sets* for L/F — that is, subsets of L satisfying (2). We denote by $\rho(L, F)$ the smallest cardinal number α such that there is a ring generating set for L over F of cardinality α. A theorem of Becker and Mac Lane [1] implies that if $[L : F]$ (the cardinality of a vector space basis for L over F) is finite, and if L/F is inseparable, then $\rho(L, F) = r$, where $[L : L^p(L_s)] = [L : L^p(F)] = p^r$ and L_s is the set of elements of L which are separable over F. We prove (Theorem 4) that $\rho(L, F) = [L : F]$ if L/F is algebraic but not finite, and $\rho(L, F) = |L|$ if L/F is not algebraic. In particular, $\rho(K, F) \leqq \rho(L, F)$ if K is a subfield of L containing F.

If $L = F[S]$ and if K is a subfield of L containing F, we prove (Corollary 3) that $K = F[T]$ where $|T| \leqq |S|$, and except in the case when L/F is finite algebraic and K/F is not purely inseparable, it is true that if $K = F[S_0]$, then there is a subset T of S_0 such that $K = F[T]$ and $|T| \leqq |S|$. In §4 we conclude with some observations concerning $\rho(L, F)$ and $[L : F]$.

2. **Preliminaries on cardinality.** We begin by listing some results on cardinal numbers which we shall need in the sequel.

RESULT 1. *If N is a regular multiplicative system in the infinite commutative ring R, then $|R_N| = |R|$; in particular, $|R| = |T|$, where T is the total quotient ring of R.*

Received by the editors August 20, 1970.

AMS 1970 *subject classifications.* Primary 12E99, 12F99; Secondary 13A99.

[1]This research was supported by National Science Foundation Grant GP-19406.

RESULT 2. *If R is a nonzero commutative ring, and if $\{X_\lambda\}_{\lambda\in\Lambda}$ is a set of indeterminates over R, then $|R[\{X_\lambda\}]| = |R|\,|\Lambda|\aleph_0$.*

RESULT 3. *If V is a vector space over a field F, if B is a basis for V, and if F or B is infinite, then $|V| = |F|\,|B|$.*

RESULT 4. *If F is a subfield of the field L and if L/F is algebraic, then $|L| \leqq |F|\aleph_0$. If F is infinite, then $|L| = |F|$ [5, p. 143].*

RESULT 5. *If T is a nonempty subset of a multiplicative semigroup S and if T^* is the subsemigroup of S generated by T, then $|T^*| \leqq |T|\aleph_0$; if T is infinite, then $|T^*| = |T|$.*

Results 1–5 are routine exercises in computations with cardinal numbers; verifications depend, in most cases, upon the fact that if A is an infinite set and if $\mathcal{F}$ is the family of finite subsets of A, then $|\mathcal{F}| = |A|$.

3. **Ring generating sets.** Suppose that F is a subfield of the field K. We seek to determine the nature of a ring generating set for K/F. Our first considerations are aimed at the case when K/F is not algebraic.

THEOREM 1. *Suppose that D is a unique factorization domain with quotient field K and that $\{X_\lambda\}_{\lambda\in\Lambda}$ is a nonempty set of indeterminates over D. Let $\mathcal{P} = \{p_\alpha\}_{\alpha\in A}$ be a complete set of nonassociate prime elements of the domain $J = D[\{X_\lambda\}]$. Then*

(1) $|\mathcal{P}| = |J|$.

(2) *If T is any subset of $K(\{X_\lambda\})$ such that $J[T] = K(\{X_\lambda\})$, then $|T| = |\mathcal{P}|$.*

(3) *If L is an algebraic extension field of $K(\{X_\lambda\})$ and if T is a subset of L such that $J[T] = L$, then $|T| = |L|$.*

PROOF. (1): If D and Λ are finite—say $D = \mathrm{GF}(p^n)$—then it is well known that for any positive integer k, there are $f(k) = \sum_{d|k}\mu(k/d)p^{nd}$ irreducible polynomials of degree k in $D[X_\lambda]$ [5, p. 61, Ex. 1]. Since any prime element of $D[X_\lambda]$ is prime in J, it follows that $|\mathcal{P}| = \aleph_0 = |J|$ if D and Λ are finite. And if D or Λ is infinite, then $\{X_\lambda - d \mid \lambda \in \Lambda, d \in D\}$ is a set of nonassociate prime elements of J of cardinality $|\Lambda|\,|D| = |\Lambda|\,|D|\aleph_0 = |J|$. Hence $|\mathcal{P}| = |J|$ in either case.

(2): Let $T = \{t_b\}_{b\in B}$; the set T must be infinite by Theorem 21 of [6]. For each b in B, we write $t_b = f_b/g_b$, where $f_b, g_b \in J$, $g_b \neq 0$. There are only finitely many p_α's which divide g_b; hence the cardinality of the set of p_α's which divide some g_b is at most $\aleph_0|T| = |T|$. Since $J[T] = K(\{X_\lambda\})$, each p_α in $\mathcal{P}$ must divide some g_b, for $1/p_\alpha \in J[T]$ implies that $1/p_\alpha \in J[t_{b_1}, \cdots, t_{b_n}] \subseteq J[1/g_{b_1} \cdots g_{b_n}]$ for some finite subset $\{t_{b_i}\}_1^n$ of T, and this implies that p_α divides

g_{b_i} for some i between 1 and n. It follows that $|\mathcal{P}| = |J| \leqq |T| \leqq |K(\{X_\lambda\})| = |J| = |\mathcal{P}|$.

(3): Again let $T = \{t_b\}_{b \in B}$. Since t_b is algebraic over $K(\{X_\lambda\})$, there is a nonzero polynomial $f_b(Y)$ in $J[Y]$ such that $f_b(t_b) = 0$. We let d_b be the leading coefficient of $f_b(Y)$; then t_b is integral over $J[1/d_b]$ and $L = J[T]$ is integral over $J[\{1/d_b\}_{b \in B}]$. Therefore, $J[\{1/d_b\}] = K(\{X_\lambda\})$ [3, p. 101], and by (2), $|T| = |B| \geqq |\{1/d_b\}| = |K(\{X_\lambda\})| = |L|$. (The last equality follows from Result 4; since Λ is nonempty, $K(\{X_\lambda\})$ is infinite.)

Remark 1. We note that the assumption "D is a UFD" is not needed in proving (1) of Theorem 1, for if a and b are nonzero elements of an integral domain D with identity such that $(a) \cap (b) = (ab)$, then $(aX_\lambda + b)$ is a prime ideal of $D[X_\lambda]$ by [2, Ex. 15a, p. 84]; in particular, $X_\lambda - d$ is a prime element of $D[X_\lambda]$ for any d in D.

Remark 2. In (2), the set $T = \{1/p_\alpha\}_{\alpha \in A}$ is an efficient ring generating set for $K(\{X_\lambda\})$ over J in the sense that $K(\{X_\lambda\}) = J[T]$, while $K(\{X_\lambda\}) \neq J[T_1]$ for any proper subset T_1 of T. In asserting that $J[T] = K(\{X_\lambda\})$, we are using the assumption that J is a UFD. In fact, if D_1 is an integral domain with identity with quotient field K_1 and if $\{d_\beta\}_{\beta \in B}$ is a set of nonzero elements of D_1, then $K_1 = D_1[\{1/d_\beta\}_{\beta \in B}]$ if and only if each nonzero prime ideal of D_1 contains some d_β. (See the proof of Lemma 3 of [4].) In particular, if $\{d_\beta\}$ is a complete set of nonassociate prime elements of D_1, then $D_1[\{1/d_\beta\}] = K_1$ if and only if each nonzero prime ideal of D_1 contains some d_β, and hence if and only if D_1 is a UFD [6, p. 4]. Since $D[\{X_\lambda\}]$ is a UFD if and only if D is a UFD, it follows that the assertion $D[\{X_\lambda\}][\{1/p_\alpha\}] = K(\{X_\lambda\})$ is equivalent to the statement that D is a UFD.

Corollary 1. *If F is a subfield of the field L and if L/F is not algebraic, then any ring generating set S for L over F is of cardinality $|L|$.*

Proof. S contains a transcendence basis B for L/F, and $B \neq \emptyset$ by hypothesis. Since $F[B][S - B] = L$, part (3) of Theorem 1 shows that $|S - B| = |L|$. Hence $|L| \geqq |S| \geqq |S - B| = |L|$.

It seems that Corollary 1 should be known, and indeed, the result may already appear in the literature. But the result most closely related to Corollary 1 that we have been able to find in the literature is Corollary 2′, page 28, of Amitsur's paper *Algebras over infinite fields*, Proc. Amer. Math. Soc. 7 (1956). Amitsur's Corollary 2′ implies that under the hypothesis of Corollary 1, the dimension of L, as a vector space over F, is greater than or equal to $|F|$.

We turn to the case when L/F is algebraic. Our first results deal with the case of finite purely inseparable extensions.

If $L = F(\theta)$ is a simple extension of F, and if K is any subfield of L containing F, then $K = F(a_0, a_1, \cdots, a_n)$, where the a_i's are the coefficients of a minimal polynomial for θ over K [**10**, pp. 156–157]. If θ is purely inseparable over F of degree p^e, then θ is purely inseparable over K and the minimal polynomial for θ over K is $X^{p^t} - \theta^{p^t}$ for some t between 0 and e. Hence we have

RESULT 6. *Suppose that $L = F(\theta)$ is purely inseparable, of degree $p^e > 1$ over F. Then $\{F(\theta^{p^i})\}_{i=0}^{e}$ is the set of subfields of L containing F, and $[K : F(\theta^{p^i})] = p^i$ for $0 \leqq i \leqq e$.*

COROLLARY 2. *Suppose that $L = F(\theta)$ is purely inseparable over F of degree $p^e > 1$. If $\alpha \in L - F(\theta^p)$, then $L = F(\alpha)$.*

PROOF. Result 6 shows that $F(\theta^p)$ is the unique maximal proper subfield of L containing F.

THEOREM 2. *Suppose that $L = F(\theta_1, \cdots, \theta_t)$ is purely inseparable over F, of degree $p^e > 1$. If $K = F[S]$ is a subfield of L containing F, then there exist elements $\alpha_1, \cdots, \alpha_u$ in S, with $u \leqq t$, such that $K = F(\alpha_1, \cdots, \alpha_u)$.*

PROOF. We use induction on t. If $t = 1$, then Result 6 implies that $\mathcal{S} = \{F(s) \mid s \in S\}$ is a finite linearly ordered set. Hence $K = \bigcup_{s \in S} F(s) = F(s_0)$ for some s_0 in S. We assume that Theorem 2 holds for $t = r$, and for $t = r + 1$, we prove the result by induction on $[L : F]$. If, for some i between 1 and $r + 1$, $\theta_i \in F(\theta_1, \cdots, \theta_{i-1})$, then $L = F(\theta_1, \cdots, \hat{\theta}_i, \cdots, \theta_{r+1})$, and the case $t = r$ implies the desired conclusion. In particular, if $[L : F] \leqq p^r$, then the result is true. Hence we assume that $\theta_i \notin F(\theta_1, \cdots, \theta_{i-1})$ for each i so that $[L : F] = p^m \geqq p^{r+1}$, and we assume that the result is valid for any field $L_1 = F(\mu_1, \cdots, \mu_{r+1})$ purely inseparable over F of degree p^{m-1}. If $K \subseteq F(\theta_1, \cdots, \theta_r, \theta_{r+1}^p)$, then the desired conclusion holds because $[F(\theta_1, \cdots, \theta_r, \theta_{r+1}^p) : F] = p^{m-1}$. If $K = F[S] \nsubseteq F(\theta_1, \cdots, \theta_r, \theta_{r+1}^p)$, then we choose θ in $S - (F(\theta_1, \cdots, \theta_r, \theta_{r+1}^p))$. By Corollary 2, $L = F(\theta_1, \cdots, \theta_r, \theta)$. Hence $K = F(\theta)[S - \{\theta\}]$ is a subfield of $L = F(\theta)(\theta_1, \cdots, \theta_r)$ containing $F(\theta)$, and $L/F(\theta)$ is purely inseparable of finite degree. It follow from the case $t = r$ that there is a subset $\{\alpha_i\}_1^u$ of $S - \{\theta\}$, with $u \leqq r$, such that $K = F(\theta)(\alpha_1, \cdots, \alpha_u)$. This completes the proof of Theorem 2.

REMARK 3. Theorem 2 does not carry over to the case when $[L : F]$ is finite, but L/F is not purely inseparable. For example, if L/F is finite dimensional and separable, and if there exist distinct maximal proper subfields K_1, K_2 of L containing F, then L, K_1, and K_2 are simple extensions of F — say $L = F(\theta)$, $K_1 = F(\theta_1)$, $K_2 = F(\theta_2)$ — then $L = F(\theta) = F(\theta_1, \theta_2)$, but $L \supset F(\theta_1)$ and $L \supset F(\theta_2)$. (For a specific example, take $L = Q(\sqrt{2} + \sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$.) The procedures we have just described are as general as possible in the case when L/F is finite dimensional and separable. That is, the following result holds.

If L/F is n-dimensional (where $n > 1$) and separable, then each ring generating set S for L/F contains an element s such that $L = F(s)$ if and only if there is a unique maximal proper subfield of L containing F. In order that this property (that is, the property that $K = F[T]$ implies that $K = F(t)$ for some t in T) carry over to each subfield K of L containing F, it is necessary and sufficient that the set of subfields of L containing F is linearly ordered.

REMARK 4. If L/K is finite normal separable with Galois group G, if G has a unique nontrivial minimal subgroup H, and if the set of subgroups of G is not linearly ordered, then the set of proper subfields of L containing F will contain a unique maximal element, but will not be linearly ordered. The quaternion groups $Q_{2^{n+1}}$, for $n \geqq 2$, are groups (in fact, the only groups) with the property described [7, pp. 191–192].

THEOREM 3. *Suppose that F is a subfield of the field $L = F[S]$ and that $K = F[T]$ is an intermediate field. If L/F is not finite algebraic or if K/F is purely inseparable, then there is a subset T_1 of T such that $K = F[T_1]$ and $|T_1| \leqq |S|$.*

PROOF. We consider three cases.

Case 1. L/F is not algebraic. Then Corollary 1 shows that $|S| = |L| \geqq |T|$ and we can take $T_1 = T$.

Case 2. L/F is finite algebraic and K/F is purely inseparable. We let L_s be the set of elements of L which are separable over F, and without loss of generality we assume that $S = \{\theta_i\}_{i=1}^r$ is finite. Then $L = L_s(\theta_1, \cdots, \theta_r)$, L/L_s is purely inseparable of finite degree p^e, and we assume that $p^e > 1$ ($L = L_s$ implies that $K = F$ and the theorem is trivial). Applying Theorem 2 to the subfield $L_s(K) = L_s(F[T]) = L_s[T]$ of L, we conclude that there are elements $\alpha_1, \cdots, \alpha_u$ *in* T, with $u \leqq r$, such that $L_s(K) = L_s(\alpha_1, \cdots, \alpha_u)$. The fields L_s and K are linearly disjoint over F, as are the fields L_s and $F(\alpha_1, \cdots, \alpha_u)$ over F. Hence $L_s(K) = L_s \otimes_F K = L_s \otimes_F F(\alpha_1, \cdots, \alpha_u)$ so that

$$[L_s(K) : F] = [L_s : F]\,[K : F] = [L_s : F]\,[F(\alpha_1, \cdots, \alpha_u) : F]$$

[5, Chapter 1, §10; Chapter 4, §5]. Consequently, $[K:F] = [F(\alpha_1, \cdots, \alpha_u) : F]$, and since $F(\alpha_1, \cdots, \alpha_u) \subseteq K$, $K = F(\alpha_1, \cdots, \alpha_u)$. This completes the proof in Case 2.

Case 3. L/F is algebraic, but not of finite degree. Then S is necessarily infinite, and without loss of generality, we can assume that $1 \in S$. We let S^* be the multiplicative semigroup generated by S. We have $|S^*| = |S|$ by Result 5, and S^* spans $L = F[S]$ as a vector space over F. Hence S^* contains a basis S' for K over F and we have $|S'| \leqq |S^*| = |S|$. If $[K:F]$ is finite, then $K = F[T_1]$ for some finite subset T_1 of T and $|T_1| < |S|$. If $[K:F]$ is infinite, then by the proof just given, $T^* \cup \{1\}$ contains a vector space basis T' for K/F. We have $|S| \geqq |S'| \geqq |T'| = |T' - \{1\}|$. Each element t' of $T' - \{1\}$ is representable in the form $t_{\alpha_1}^{n_1} \cdots t_{\alpha_w}^{n_w}$, where the t_{α_i}'s are in T and the n_i's are positive (the representation of t' in this form may not be unique). For each t' in $T' - \{1\}$, we take a representation of the preceding form, and we consider the subset T_1 of T consisting of these t_{α_i}'s which occur in the chosen representation of some t' in $T' - \{1\}$. Since $T' - \{1\}$ is infinite, $|T_1| \leqq |T' - \{1\}|$. It is clear, however, that $K = F[T_1]$, and $|T_1| \leqq |T' - \{1\}| \leqq |S|$.

4. **The symbol $\rho(L, F)$ and $[L:F]$.** As stated in the introduction, we define $\rho(L, F)$ to be the smallest cardinal number α such that there exists a ring generating set for L over F of cardinality α. Corollary 1 shows that $\rho(L, F) = |L|$ if L/F is transcendental, and the proof of Theorem 3 in Case 3 shows that if L/F is algebraic but not finite dimensional, then for any ring generating set S for L over F, we have $|S| \geqq [L:F]$. Hence $\rho(L, F) \geqq [L:F]$, but the reverse inequality always holds (a vector space basis for L/F is a ring generating set for L/F). Therefore, $\rho(L, F) = [L:F]$ if L/F is algebraic but not finite.

In Theorem 6 of [1], Becker and Mac Lane prove that if L/F is purely inseparable of finite degree $p^e > 1$, then $\rho(L, F) = r$, where $[L : L^p(F)] = p^r$. Becker and Mac Lane also observe that if L/F is finite dimensional and inseparable, but not purely inseparable, then $\rho(L, F) = \rho(L, L_s)$, where L_s is the separable part of L/F. And it is, of course, well known that $\rho(L, F) = 1$ if L/F is finite dimensional and separable. We have proved

THEOREM 4. *If F is a proper subfield of the field L, then*
(i) $\rho(L, F) = |L|$ *if L/F is transcendental.*
(ii) $\rho(L, F) = [L:F]$ *if L/F is algebraic but not finite dimensional.*
(iii) $\rho(L, F) = 1$ *if L/F is separable and finite dimensional.*

(iv) $\rho(L, F) = r$, *where* $[L : L^p(L_s)] = p^r$, *if* L/F *is inseparable of finite dimension, and* L_s *is the separable part of* L/F.

THEOREM 5. *If* F *is a subfield of the field* K *and if* K *is a subfield of the field* L, *then* $\rho(L, K) \leqq \rho(L, F)$ *and* $\rho(K, F) \leqq \rho(L, F)$; *except for the case when* L/F *is finite dimensional and inseparable,* $\rho(L, F) = \max\{\rho(L, K), \rho(K, F)\}$.

PROOF. In view of Theorem 4, there are four assertions of Theorem 5 which might merit some justification; we list these as

(A) If L/F is transcendental and K/F is algebraic but not finite dimensional, then $\rho(K, F) \leqq \rho(L, F)$.

(B) If K/F and L/F are finite dimensional and inseparable, then $\rho(K, F) \leqq \rho(L, F)$.

(C) If L/F is transcendental, then $\rho(L, F) = \max\{\rho(L, K), \rho(K, F)\}$.

(D) If L/F is algebraic but not finite dimensional, then $\rho(L, F) = \max\{\rho(L, K), \rho(K, F)\}$.

In (A), we have $\rho(L, F) = |L| \geqq |K| \geqq [K : F] = \rho(K, F)$.

To prove (B), we note that $\rho(K, F) = \rho(K, K_s)$ and $\rho(L, F) = \rho(L, L_s)$. Moreover, $\rho(L, L_s) = \rho(L, K_s)$, for L_s is the separable part of L/K_s. Hence, we prove that $\rho(L, K_s) \geqq \rho(K, K_s)$. This follows immediately from Theorem 3, for K/K_s is purely inseparable.

(C): If L/K is transcendental, then $|L| = \rho(L, F) = \rho(L, K)$. If L/K is algebraic, then K/F is transcendental and $\rho(L, F) = |L| = |K| = \rho(K, F)$.

(D): We have $\rho(L, F) = [L : F] = [L : K][K : F] = \max\{[L : K], [K : F]\}$ (since the product is an infinite cardinal) $= \max\{\rho(L, K), \rho(K, F)\}$.

COROLLARY 3. *If* F *is a subfield of* K *and if* K *is a subfield of the field* L, *then for each subset* S *of* L *such that* $L = F[S]$, *there is a subset* T *of* K *such that* $K = F[T]$ *and* $|T| \leqq |S|$.

Corollary 3 is merely a restatement of the inequality $\rho(K, F) \leqq \rho(L, F)$ in Theorem 5; we have stated the corollary explicitly because it avoids the one exceptional case of Theorem 3.

REMARK 5. We could also establish (B) in Theorem 5 by Becker and Mac Lane's formula. We first observe that $L^p(F) = L^p(L_s)$ and $K^p(F) = K^p(K_s)$, for $L^p(L_s)$ is both separable and purely inseparable over $L^p(F)$; similarly for $K^p(K_s)$ over $K^p(F)$. We have $[L : K^p(F)] = [L : K][K : K^p(F)] = [L : L^p(F)][L^p(F) : K^p(F)]$. The isomorphism $x \rightarrow x^p$ of L sends L onto L^p and K onto K^p, and hence $[L : K] = [L^p : K^p] \geqq [L^p(F) : K^p(F)]$. It follows that $[K : K^p(F)] = [K : K^p(K_s)] \leqq [L : L^p(F)] = [L : L^p(L_s)]$, and $\rho(K, F) \leqq \rho(L, F)$.

It should be observed, however, that Theorem 6 of [1] does not yield Case 2 of our Theorem 3.

REMARK 6. In general, we are able to assert little more than the relation $\rho(L, F) \geqq \max\{\rho(L, K), \rho(K, F)\}$ when L/F is finite dimensional and inseparable. One positive result in this direction is that $\rho(L, F) = \rho(L, K) + \rho(K, F)$ if L/F is purely inseparable of exponent one over F. Hence if L/F is purely inseparable of exponent 1, then the equality $\rho(L, F) = \max\{\rho(L, K), \rho(K, F)\}$ holds for the intermediate field K if and only if $K = L$ or $K = F$.

We have considered the function $f(L, F)$ defined to be the smallest cardinal α such that $L = F(S)$ for some subset S of L with cardinality α. Aside from a few obvious relations, such as $f(L, F) = \rho(L, F)$ when L/F is algebraic, we have concluded that this is not likely to be a very fruitful field of endeavor. For example, the question of whether $f(K, F) \leqq n$ when L/F is purely transcendental of degree n is a classical problem for $n \geqq 2$; see [9, p. 404], [11].

REFERENCES

1. M. F. Becker and S. Mac Lane, *The minimum number of generators for inseparable algebraic extensions,* Bull. Amer. Math. Soc. **46** (1940), 182–186. MR **1**, 198.

2. N. Bourbaki, *Algèbre commutative.* Chap. 7, Actualités Scientifiques et Indust., no. 1314, Hermann, Paris, 1965. MR **41** #5339.

3. R. Gilmer, *Multiplicative ideal theory,* Queen's Papers in Pure and Appl. Math., no. 12, Queen's University, Kingston, Ontario, 1968. MR **37** #5198.

4. ———, *The pseudo-radical of a commutative ring,* Pacific J. Math. **19** (1966), 275–284. MR **34** #4294.

5. N. Jacobson, *Lectures in abstract algebra.* III: *Theory of fields and Galois theory,* Van Nostrand, Princeton, N. J., 1964. MR **30** #3087.

6. I. Kaplansky, *Commutative rings,* Allyn and Bacon, Boston, Mass., 1970. MR **40** #7234.

7. E. Schenkman, *Group theory,* Van Nostrand, Princeton, N. J., 1965. MR **33** #5702.

8. E. Steinitz, *Algebraische Theorie der Körper,* Chelsea, New York, 1950. MR **12**, 238.

9. N. G. Čebotarev, *Foundations of the Galois theory,* Gos. Ven. Tekh. Teoret. Izdat., Leningrad, 1937; German transl., Noordhoff, Groningen, 1950. MR **12**, 666.

10. B. L. van der Waerden, *Moderne algebra,* vol. I, 2nd rev. ed., Springer, Berlin, 1937; English transl., Ungar, New York, 1949. MR **10**, 587.

11. O. Zariski, *On Castelnuovo's criterion of rationality $p_a = P_2 = 0$ of an algebraic surface,* Illinois J. Math. **2** (1958), 303–315. MR **20** #6426.

FLORIDA STATE UNIVERSITY, TALLAHASSEE, FLORIDA 32306