

## A WEAK VERSION OF ROLLE'S THEOREM

THOMAS C. CRAVEN

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. We investigate the fields with the property that any polynomial over the field which splits in the field has a derivative which also splits.

### 1. INTRODUCTION

In his book *Fields and Rings* [K, p.30], Kaplansky raises the question of which fields  $F$  have the property that any polynomial  $p(x) \in F[x]$  which splits over  $F$  has a derivative which also splits over  $F$ . In particular, this holds for any algebraically closed field, any real closed field, and more generally, any ordered field for which Rolle's theorem holds for polynomials. These latter fields were characterized in [BCP] and have since spawned a number of papers in which they have been called *Rolle fields*. For this reason, we shall call the fields satisfying the weaker condition *SR fields* (for "split Rolle"). Since there is no longer any condition that roots of the derivative lie between roots of the original polynomial, we are no longer restricted to fields with an ordering.

Kaplansky gives as an exercise the problem of proving that, for characteristic other than 2 or 3, the SR condition holds for polynomials of degree 3 if and only if the field is pythagorean (every sum of squares is a square). In particular, an SR field which is not formally real must be quadratically closed except in characteristic 2 or 3. (This is also true of characteristic 3 by Theorem 2.2.) A proof of a more general result (in one direction; the other is an easy computation) can be found in [CC, Theorem 2.8]. This latter paper concerns general questions involving the concept of multiplier sequences.

**Definition.** Let  $\Gamma = \{\gamma_0, \gamma_1, \gamma_2, \dots\}$  be a sequence of elements of a field  $F$ .  $\Gamma$  is called a *multiplier sequence* for  $F$  if for any polynomial  $f(x) = \sum a_i x^i \in F[x]$  which splits over  $F$ , the polynomial  $\Gamma[f(x)] = \sum \gamma_i a_i x^i$  also splits over  $F$ .

For the particular sequence  $\Gamma = \{0, 1, 2, \dots\}$ , we have  $\Gamma[f(x)] = x f'(x)$  for any polynomial  $f$ . Therefore, Kaplansky's problem is to determine the fields for which this particular sequence is a multiplier sequence. The purpose of this paper is to provide a number of results toward determining these fields.

Multiplier sequences originally come from the work of Pòlya in complex analysis (see references in [CC]), and many of the theorems have counterparts in the theory

---

Received by the editors January 23, 1996 and, in revised form, May 13, 1996.

1991 *Mathematics Subject Classification.* Primary 12D10, 12E05; Secondary 12J10.

*Key words and phrases.* Polynomial, multiplier sequence, valuation theory, ordered field.

of formally real fields, such as those in [C]. We shall see here that there are substantial differences between the properties of ordered SR fields and other SR fields. Section 2 deals with results for finite characteristic SR fields. The main result is a complete determination of all those SR fields which are algebraic over their prime subfield. These turn out to be precisely  $\mathbb{F}_2$ ,  $\mathbb{F}_4$  and the algebraic closures  $\bar{\mathbb{F}}_p$  for any prime  $p$ .

Section 3 provides a number of valuation-theoretic results. Valuation theory is particularly useful in dealing with formally real fields. Indeed, the characterization of Rolle fields in [BCP] is valuation-theoretic. These techniques provide a wealth of examples of SR fields.

The last section discusses the minimal SR extension of an arbitrary field  $F$  and shows that it is necessarily normal over  $F$ .

As a matter of standard notation, we write  $\dot{F}$  for  $F \setminus \{0\}$ .

## 2. FINITE CHARACTERISTIC SR FIELDS

In the process of determining all multiplier sequences for finite fields, Craven and Csordas [CC, Theorem 4.11] have shown that the only finite SR fields are  $\mathbb{F}_2$  and  $\mathbb{F}_4$ . The main goal of this section is to prove that any other finite characteristic SR field which is algebraic over its prime subfield is actually algebraically closed. A few other necessary properties of finite characteristic SR fields are obtained along the way. In the next section, we are able to give an example of an SR field of characteristic 2 which is neither algebraically closed nor one of the fields above.

The following lemma provides an important technique for our current work with SR fields.

**Lemma 2.1.** *Let  $F$  be an SR field of characteristic  $p \neq 0$ . If  $\sum_{i=0}^n a_i x^i$  splits over  $F$  and  $0 \leq r \leq n$ , then there exists a sequence  $\{b_0, b_1, \dots, b_n\}$  for which  $\sum b_i a_i x^i$  also splits, where  $b_i = 0$  for  $i \equiv r \pmod{p}$  and  $b_i \in \bar{\mathbb{F}}_p$  for  $i \not\equiv r \pmod{p}$ .*

*Proof.* Multiply the polynomial by  $x^{\lceil \frac{r}{p} \rceil p - r}$ , differentiate and then divide by  $x^{\lceil \frac{r}{p} \rceil p - r - 1}$ , where  $\lceil s \rceil$  denotes the ceiling function applied to  $s$ . This carries  $x^k$  to  $(k + \lceil \frac{r}{p} \rceil p - r)x^k$  in which the coefficient is zero if and only if  $k \equiv r \pmod{p}$ .  $\square$

**Theorem 2.2.** *Let  $F$  be an SR field of odd characteristic  $p$ . Then  $F$  is closed under taking  $n$ th roots for all positive integers  $n$ .*

*Proof.* We prove the theorem by induction on  $n$ . Let  $n > 1$  and assume that  $F$  contains all  $k$ th roots for any  $k < n$ . First we consider the case where  $n \not\equiv 1 \pmod{p}$ ; let  $t \in F$  and consider the polynomial

$$(x^{n-1} + 1)(x - t) = x^n - tx^{n-1} + x - t,$$

which splits by the induction hypothesis. Applying Lemma 2.1 twice and multiplying by a constant, we may eliminate the two middle terms to obtain a polynomial  $bx^n - t$ ,  $b \in \bar{\mathbb{F}}_p$ , which still splits. Since  $t$  was arbitrary and  $b$  is independent of  $t$ , the field  $F$  must contain  $n$ th roots of all its elements. In particular, since  $2 \not\equiv 1 \pmod{p}$ , the field is quadratically closed. On the other hand, if  $n \equiv 1 \pmod{p}$ , consider the polynomial

$$(x^{n-2} + 1)(x^2 - t) = x^n - tx^{n-2} + x^2 - t,$$

which also splits by the induction hypothesis. Again the two middle terms can be removed using Lemma 2.1 without eliminating the first and last terms, so  $F$  contains the  $n$ th roots of all of its elements.  $\square$

**Corollary 2.3.** *If  $F$  is an SR field of odd characteristic  $p$ , then  $F$  is perfect and  $F$  contains  $\overline{\mathbb{F}}_p$ , the algebraic closure of  $\mathbb{F}_p$ .*

*Proof.* All elements of  $\overline{\mathbb{F}}_p$  are roots of 1.  $\square$

Unfortunately, the techniques above are not adequate in characteristic two. The proof in this case requires significantly more work. For any field  $F$  of characteristic two, we denote the additive subgroup  $\{y^2 + y \mid y \in F\}$  by  $\mathcal{S}(F)$ .

**Proposition 2.4.** *An SR field  $F$  of characteristic 2 is perfect.*

*Proof.* For any element  $t \in F$ , the polynomial  $\frac{d}{dx}x(x+1)(x+t) = x^2 + t$  must split in  $F$ .  $\square$

**Theorem 2.5.** *Let  $F$  be an SR field of characteristic 2. Then  $\mathcal{S}(F)$  is closed under multiplication as well as addition.*

*Proof.* Let  $p(x) = x(x+1)(x+a)(x+a+1)(x+b)(x+b+1)$ , where  $a, b \in F$ . Then  $p'(x) = x^4 + x^2 + (a^2 + a)(b^2 + b)$  must split. But this happens if and only if  $(a^2 + a)(b^2 + b)$  again lies in  $\mathcal{S}(F)$ , hence  $\mathcal{S}(F)$  is closed under multiplication.  $\square$

**Corollary 2.6.** *Let  $F \subset \overline{\mathbb{F}}_2$  be an SR field with more than 4 elements. Then  $F = \mathcal{S}(F)$ . In particular,  $F$  contains  $\mathbb{F}_{2^{2^n}}$  for all positive integers  $n$ .*

*Proof.* Every element of  $\mathcal{S}(F)$ , being algebraic over  $\mathbb{F}_2$ , has finite multiplicative order, and hence has an inverse in  $\mathcal{S}(F)$  by Theorem 2.5. Thus  $\mathcal{S}(F)$  is a subfield of  $F$ . For any  $\mathbb{F}_q \subset F$ , the set  $\mathcal{S}(F) \cap \mathbb{F}_q$  is a subfield of  $\mathbb{F}_q$  with at least  $\frac{q}{2}$  elements. But this is possible for  $q > 4$  only if  $\mathcal{S}(F) \cap \mathbb{F}_q = \mathbb{F}_q$ . Hence we must have  $F = \mathcal{S}(F)$ . This implies that  $F$  has no quadratic extensions, so the second statement follows.  $\square$

**Theorem 2.7.** *The only SR fields algebraic over  $\mathbb{F}_2$  are  $\mathbb{F}_2, \mathbb{F}_4$  and  $\overline{\mathbb{F}}_2$ .*

*Proof.* Let  $F \subseteq \overline{\mathbb{F}}_2$  be an SR field with more than four elements. We know by Corollary 2.6 above that  $F \supset \mathbb{F}_{2^{2^n}}$  for all positive integers  $n$ . We need to show that  $F$  is algebraically closed. We begin by noting a special property of differentiation for fields of characteristic 2 given by Lemma 2.1; since the odd degree terms of a polynomial can be dropped, we know that

$$(2.8) \quad \text{if } \sum_{k=0}^{2^n} a_k x^k \in F[x] \text{ splits, so does } \sum_{k=0}^{2^{n-1}} a_{2k} x^k.$$

We shall use (2.8) to establish new elements of  $F$ . Take  $f(x) \in \mathbb{F}_2[x]$  to be an arbitrary irreducible polynomial whose roots we wish to show lie in  $F$ . Now  $f(x)$  divides a polynomial of the form  $x^{2^{n-1}} + x$ , for some positive  $n$ , so it will suffice to replace  $f(x)$  by

$$p(x) = (x^{2^{n-1}} + x + f(x))^2 = x^{2^n} + x^2 + f(x)^2$$

and show that  $p(x)$  splits in  $F$ . Note that  $p(x)$  has only terms of even degree and  $p(0) = 1$ . Let  $q(x)$  be a polynomial over  $F$  with only odd degree terms and degree less than  $2^n$ . If  $p(x) + q(x)$  were defined and irreducible over some field  $\mathbb{F}_{2^{2^m}} \subset F$ ,

then its splitting field would be  $\mathbb{F}_{2^{2^m+n}}$ , which is again a subfield of  $F$ . And it would then follow by (2.8) that  $p(x)$  splits in  $F$ . The existence of just such a polynomial  $q(x)$  (or, more precisely, such an irreducible polynomial  $p(x) + q(x)$ ) is guaranteed by an asymptotic result of Cohen [Co, Theorem 1]. Indeed, he shows that the number of irreducible polynomials  $p(x) + ax$ ,  $a \in \mathbb{F}_{2^{2^m}}$ , is  $2^{2^m-n} + O(2^{2^m-1})$ . This establishes our theorem.  $\square$

### 3. VALUATION THEORY

Before we begin with valuation theory, we wish to make a few comments on formally real SR fields. As mentioned in the introduction, any real closed field is SR; in fact, it satisfies the usual Rolle's theorem for polynomials. Now let  $F$  be any intersection of real closed fields inside a fixed algebraic closure. Since the derivative of a polynomial which splits over  $F$  will split in each real closure containing  $F$ , it follows that the derivative will actually split over  $F$ . Thus we see that any intersection of real closed fields is an SR field. In fact, much more is true of these fields; they are characterized by the fact that their multiplier sequences can be determined by just checking them on the polynomials  $(x+1)^n$  [C, Theorem 2.2]. In any case, this provides a large collection of formally real SR fields (most of which do *not* satisfy Rolle's theorem for arbitrary polynomials) and we summarize this in a proposition.

**Proposition 3.1.** *Any intersection of real closed fields (in some fixed larger field) is an SR field.*

For any valued field  $(F, v)$ , we shall write  $F_v$  for the residue field,  $A_v$  for the valuation ring,  $\mathfrak{m}_v$  for the maximal ideal of  $A_v$  and  $\Gamma_v$  for the (additively written) value group.

**Proposition 3.2.** *Let  $(F, v)$  be a valued field. If  $F$  is SR, then so is  $F_v$ .*

*Proof.* Assume that  $F_v$  is not SR. Let  $f \in F_v[x]$  be any polynomial which splits over  $F_v$  but whose derivative has a root  $\beta \notin F_v$ . Lift  $f$  to a polynomial  $h(x) \in F[x]$  which splits by lifting each factor of  $f$ . Then the derivative  $h'$  must split since  $F$  is SR. But  $h'$  has image  $f'$  over the residue field and all its roots lie in  $F$ , a contradiction of  $\beta$  not being in the residue field.  $\square$

In view of the previous section, this proposition shows that the  $p$ -adic numbers  $\hat{\mathbb{Q}}_p$  are not SR for  $p$  odd. The 2-adic numbers, having a residue class field satisfying SR, provide an interesting example, discussed in Example 3.5. In particular, they show that the following partial converse of Proposition 3.2 actually requires the hypothesis of an ordering.

**Theorem 3.3.** *Let  $F$  be an ordered field and  $v$  a henselian valuation compatible with the ordering of  $F$ . If  $F_v$  is SR, then so is  $F$ .*

*Proof.* Let  $f \in F[x]$  be a polynomial which splits over  $F$ . Let  $a < b$  be two consecutive roots of  $f$ . Replacing  $f(x)$  by  $f((b-a)x+a)$ , we may write  $f(x) = x(x-1) \prod ((b-a)x+a-r_j)$ , where 0 and 1 are consecutive roots. Next, divide each of the latter factors  $(b-a)x+(a-r_j)$  by  $b-a$  if  $v(b-a) \leq v(a-r_j)$  or by  $a-r_j$  if  $v(b-a) > v(a-r_j)$ . This results in a polynomial (which we again call  $f$ ) having all coefficients in  $A_v$  and such that  $\bar{f}$  splits over  $F_v$ . Now  $F_v$  is also an ordered field, its ordering being induced by that of  $F$ . Furthermore, 0 and 1 are

consecutive roots of  $\bar{f}$ , so the real closure of  $F_v$  has a simple root  $\beta$ ,  $0 < \beta < 1$ , of  $\bar{f}'$  by Rolle's theorem. The hypothesis that  $F_v$  is SR implies that  $\beta \in F_v$ . By Hensel's lemma, the factor  $x - \beta$  of  $\bar{f}'$  lifts to a factor  $x - \alpha$  of  $f'$  with  $\bar{\alpha} = \beta$ , whence  $0 < \alpha < 1$ . Undoing the transformations made earlier on  $f$ , we obtain a root of the original  $f'$  in  $F$  between  $a$  and  $b$ . This holds for each pair of consecutive roots of  $f$ . As usual, multiple roots of  $f$  give roots of  $f'$  of multiplicity one less, so a count of the roots of  $f'$  in  $F$  shows that  $f'$  splits.  $\square$

Without orderings, we need a condition on the value group also.

**Theorem 3.4.** *Let  $F$  be a field with henselian valuation  $v$ , residue field  $F_v$  which is SR and divisible value group. Then  $F$  is SR.*

*Proof.* Assume  $F$  is not SR. Then there is a polynomial  $p(x) \in F[x]$  which splits over  $F$ , but for which the derivative  $p'(x)$  does not split over  $F$ . Without loss of generality, we can assume that  $p(x)$  is monic with all coefficients in the valuation ring  $A_v$ . (Replace  $\prod_{i=1}^n (x - r_i)$  with  $v(r_1) \leq v(r_2) \leq \dots \leq v(r_n)$  by  $r_1^{-n} \prod (r_1 x - r_i)$ .) Since  $p'(x)$  does not split, it has a root  $\alpha \notin F$ , which generates a proper extension field  $K = F(\alpha)$ . The valuation  $v$  extends uniquely to a valuation  $w$  on  $K$ . Since the valuation is henselian and the value group is divisible, the residue field of  $w$  is  $F_v(\bar{\alpha})$ , where  $[K : F] = [F_v(\bar{\alpha}) : F_v]$ . On the other hand,  $\bar{p}(x) \in F_v[x]$  is a polynomial which splits over  $F_v$ , whence its derivative  $\bar{p}'(x)$  must also split; i.e.,  $\bar{\alpha} \in F_v$ , a contradiction.  $\square$

**Example 3.5.** (1) Applying the previous theorem to our work in section 2, we see that the field  $\mathbb{F}_2((t))(t^{1/n})$ ,  $n = 2, 3, \dots$ ) is a nonreal field which is SR but is not algebraically closed.

(2) The 2-adic field  $\hat{\mathbb{Q}}_2$  is not SR; indeed, it is not pythagorean, so the condition fails for polynomials of degree 3. This example shows that the hypotheses that  $F$  be ordered in Theorem 3.3 and that the value group be divisible in Theorem 3.4 cannot be omitted.

**Theorem 3.6.** *Let  $(F, v)$  be a henselian valued field with algebraically closed residue field. If  $F$  is SR, then  $F$  is algebraically closed.*

*Proof.* It will suffice to show that  $\Gamma_v$  is divisible. Let  $\gamma = v(t) > 0$  in  $\Gamma_v$  and consider the polynomial  $f(x) = x^{n+1} - tx - 1 \in F[x]$ . Then  $\bar{f}(x) = x^{n+1} - 1$  splits with distinct roots in  $F_v$  if the characteristic  $p$  of  $F_v$  is zero or if  $n \not\equiv 0 \pmod{p}$ ; in the latter case,  $\bar{f}'(x) = x^n$ , hence has no zero in common with  $\bar{f}(x)$ . By Hensel's lemma,  $f(x)$  splits in  $F$ . But  $F$  is SR, so the derivative  $f'(x) = (n + 1)x^n - t$  splits in  $F$ ; that is,  $\frac{t}{n+1}$  has an  $n$ th root in  $F$  and, therefore,  $\gamma$  is divisible by  $n$  in  $\Gamma_v$ . If  $p \neq 0$ , then  $n$  has the form  $mp$  for some positive integer  $m$  and  $\gamma$  is also divisible by  $m$ . Note that  $m$ , or  $n$  in characteristic zero, can be chosen arbitrarily. Obviously,  $-\gamma$  and  $0$  are also divisible by  $n$  for any natural number  $n$ , so  $\Gamma_v$  is a divisible group.  $\square$

*Remark 3.7.* Theorem 2.2 gave us this result earlier for an SR field of finite characteristic  $p \neq 2$  since it showed that such a field must have a divisible value group. Theorem 3.6 shows that the situation for nonreal fields is quite different than for formally real fields even in characteristic zero. For example,  $\mathbb{R}((t))$  is an SR field by Theorem 3.3. (In fact, being hereditarily pythagorean, it is an intersection of real closed fields.) But Theorem 3.6 says that  $\mathbb{C}((t))$  is not SR. In fact, the smallest SR

field containing  $\mathbb{C}((t))$  is its algebraic closure,  $\mathbb{C}((t))(t^{1/n}, n = 2, 3, 4, \dots)$ . The field  $\mathbb{C}((t))$  is another example showing that Theorem 3.3 is false without the hypothesis that the field be ordered.

**Corollary 3.8.** *Let  $(F, v)$  be a valued field with residue field algebraically closed. Then the completion (in the sense of [R, p. 72])  $\hat{F}$  is SR if and only if it is algebraically closed.*

*Proof.* By [R, Théorème 4, p. 198],  $\hat{F}$  is henselian, so this follows immediately from the theorem.  $\square$

#### 4. GALOIS THEORY

Unfortunately, we have very few examples of SR fields which are not either algebraically closed or intersections of real closed fields. It would be nice to have other examples. Along this line, we consider the minimal SR field  $\tilde{F}$  over any field  $F$ . It is easily seen that this field is uniquely determined as a subfield of a fixed algebraic closure of  $F$ . In fact, the details are found in the proof of the next theorem in which we show that  $\tilde{F}$  is normal over  $F$ .

**Theorem 4.1.** *Let  $F$  be any field and let  $K$  be the minimal SR field containing  $F$ . Then  $K$  is a normal extension of  $F$ .*

*Proof.* We construct  $K$  as follows: Set  $K_0 = F$ ; for each  $n > 0$ , set  $K_n$  equal to  $K_{n-1}$  with the roots of all polynomials  $f'$  adjoined, where  $f$  splits over  $K_{n-1}$ . Set  $K = \bigcup_{n=0}^{\infty} K_n$ . This clearly gives the minimal SR field containing  $F$ . By construction, each  $K_n$  is normal over  $K_{n-1}$ . We shall show normality over  $F$  by induction. Assume that  $K_{n-1}$  is normal over  $F$  (true for  $n = 1, 2$ ). For any  $\phi \in \text{Aut}(\bar{F}/F)$ , we also write  $\phi$  for its natural extension to  $\bar{F}[x]$ . If  $p(x) = \sum a_i x^i \in \bar{F}[x]$ , we have  $\phi(p(x))' = \sum \phi(a_i) i x^{i-1} = \sum \phi(a_i) i x^{i-1} = \phi(p'(x))$ , so  $\phi$  preserves differentiation. Let  $\alpha \in K_n \setminus K_{n-1}$  and let  $f \in K_{n-1}[x]$  be a polynomial which splits over  $K_{n-1}$  which has  $f'(\alpha) = 0$ . Since  $K_{n-1}/F$  is normal, any  $\phi \in \text{Aut}(\bar{F}/F)$  carries  $K_{n-1}$  into itself. Let  $\beta$  be any conjugate of  $\alpha$  over  $F$ . Then there exists  $\phi \in \text{Aut}(\bar{F}/F)$  such that  $\phi(\alpha) = \beta$ . But then  $\phi(f) \in K_{n-1}[x]$  splits over  $K_{n-1}$  and  $\phi(f)' = \phi(f')$ , so  $0 = \phi(f'(\alpha)) = (\phi f)'(\phi(\alpha)) = (\phi f)'(\beta)$ , hence  $\beta \in K_n$  by construction. Thus  $K_n$  contains all conjugates of each of its elements, hence is normal over  $F$ . It follows that the union  $K$  is also normal over  $F$ .  $\square$

Note that the minimal SR field  $K$  of the previous theorem need not be separable over  $F$ . Indeed, if  $F = \mathbb{F}_p(t)$ , then from §2 (Theorem 2.2 and Proposition 2.4), we know that  $K$  must contain a  $p$ -th root of  $t$ , an inseparable element over  $F$ .

Even for the rational numbers, the situation is not clear. Of course,  $\tilde{\mathbb{Q}}$  is a subfield of  $\check{\mathbb{Q}}$ , the maximal normal extension to which the ordering of  $\mathbb{Q}$  extends. This field is described in [C, §1]; it contains (exactly) the roots of all irreducible polynomials over  $\mathbb{Q}$  which split in  $\mathbb{R}$ . It is the intersection of all real closures of  $\mathbb{Q}$  inside the algebraic closure  $\check{\mathbb{Q}}$ . One would not expect that  $\tilde{\mathbb{Q}} = \check{\mathbb{Q}}$ , but this remains an open question.

#### REFERENCES

- [BCP] R. Brown, T. Craven and M.J. Pelling, *Ordered fields satisfying Rolle's theorem*, Illinois J. Math. **30** (1986), 66–78. MR **87f**:12004  
[Co] S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arithm. **17** (1970), 255–271. MR **43**:3234

- [C] T. Craven, *Intersections of real closed fields*, Canadian J. Math. **32** (1980), 431–440. MR **81i:12026**
- [CC] T. Craven and G. Csordas, *Multiplier sequences for fields*, Illinois J. Math. **21** (1977), 801–817. MR **58:27921**
- [K] I. Kaplansky, *Fields and Rings*, 2nd ed., University of Chicago Press, Chicago, 1972. MR **50:2139**
- [R] P. Ribenboim, *Théorie des Valuations*, Les Presses de l'Université de Montréal, Montreal, Quebec, 1964/1968. MR **40:2670**

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII, HONOLULU, HAWAII 96822  
*E-mail address:* `tom@math.hawaii.edu`