International Journal of Pure and Applied Mathematics
Volume 48 No. 4 2008, 491-494

ON A THEOREM OF ISAACS

Fernando Barrera-Mora

Centro de Investigación en Matemáticas
Instituto de Ciencias Básicas e Ingeniería
Universidad Autónoma del Estado de Hidalgo
Carretera Pachuca-Tulancingo, km 4.5, Pachuca, Hidalgo, 42184, MEXICO
e-mail: barrera@uaeh.edu.mx

Abstract: I.M. Isaacs has proven a very interesting theorem concerning solvability of polynomials by real radicals. His result deals with an irreducible polynomial over the field of rational numbers which has a real radical element and splits in $\mathbb{R}$. In this note we present a short proof of a generalization of Isaacs Theorem.

AMS Subject Classification: 12E10, 12F99
Key Words: solvability of polynomials, real radicals

1. Introduction

In [5], Isaacs has proven a very interesting theorem concerning solvability of polynomials by real radicals. His result deals with an irreducible polynomial over the field of rational numbers which has a real radical element and splits in $\mathbb{R}$. In this note we present a short proof of a generalization of Isaacs Theorem. Our proof is based on two results: one is Capelli Theorem on irreducible binomials and the other one is a criterion for a radical extension to have a unique subfield for each divisor of its degree.

2. A Theorem of Isaacs

Definition 1. (a) An extension K/F is said to be *radical* if there exists $\alpha \in K$ so that $K = F(\alpha)$ and $\alpha^n \in F$ for some integer $n \geq 1$.

Received: June 24, 2008 © 2008, Academic Publications Ltd.

(b) An extension K/F is said to be a *repeated radical extension*, if there exists a sequence of fields $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = K$ so that F_{i+1}/F_i is radical for all $i = 0, \ldots, r-1$.

We say that the field extension K/F has the *unique subfield property*, abbreviated u.s.p., if for every m dividing the degree $[K : F]$, there exists a unique subfield of K/F whose degree over F is m.

In what follows, $\mu(F)$ will denote the group of roots of one in the field F and ζ_n will denote a primitive n-th root of one.

Theorem 2. (see [3], Theorem 1.2) *Let F be a field, n a positive integer and $a \in F$. The binomial $x^n - a$ is irreducible iff:*

(a) For every prime p dividing n, $a \notin F^p = \{b^p : b \in F\}$.

(b) If 4 divides n and char $F \neq 2$, $-4a \notin F^4$.

Theorem 3. (see [1], Theorem 2.1) *Let $x^n - a$ be irreducible over F, where the characteristic of F does not divide n, and let α be a root of $x^n - a$. Then the extension $F(\alpha)/F$ has the u.s.p. iff:*

(i) for every odd prime p dividing n, $\zeta_p \notin F(\alpha) \setminus F$, and

(ii) if $4|n$, then $\zeta_4 \notin F(\alpha) \setminus F$.

If K/F is a separable algebraic extension of fields and αF^* is a torsion element in the group K^*/F^*, then α defines two numbers: $o(\alpha F^*) = m$ and $[F(\alpha) : F] = n$. A result of Risman [2, Theorem A] establishes the general relationship between m and n, however, under additional assumptions on roots of unity we have that $n = m$ as the following result shows.

Theorem 4. *With the assumptions and notation as above, if $\zeta_{2p} \notin F(\alpha) \setminus F$ for every prime p dividing $o(\alpha F^*)$, then $[F(\alpha) : F] = o(\alpha F^*)$.*

Proof. Since $o(\alpha F^*) = m$, then $x^m - \alpha^m \in F[x]$. If $x^m - \alpha^m$ is reducible, separability of $F(\alpha)/F$ and Theorem 1 imply $\alpha^m \in F^p$ for some prime p dividing m, or if 4 divides m, then $-4\alpha^m \in F^4$. If $\alpha^m = b^p$ for some $b \in F$, then $\alpha^{m/p} = \zeta_p^k b$ for some $0 \leq k < p$. Since $\zeta_{2p} \notin F(\alpha) \setminus F$ then $\alpha^{m/p} \in F$, a contradiction. If $4\alpha^m + b^4 = 0$ for some $b \in F$, then $2\alpha^{m/2} = \pm\zeta_4 b^2$. The assumption $\zeta_{2p} \notin F(\alpha) \setminus F$ implies $\alpha^{m/2} \in F$, a contradiction. □

Theorem 5. *Let F be a field, $f(x) \in F[x]$ a separable and irreducible polynomial, α a root of $f(x)$ and E the splitting field of $f(x)$ over F. Assume that the following hold:*

(i) the element α is contained in a repeated radical extension K/F,

(ii) the fields EK and F have the same roots of one, that is, $\mu(EK) = \mu(F)$.

Then $\zeta_p \in F$ for each prime p dividing $[E : F]$ and every subfield M with $F \subset M \subset E$ and $[E : M] = p$ is radical.

In the proof of Theorem 5 we need the following:

Lemma 6. *Let $F \subseteq E$ be a separable radical extension, say $E = F(\alpha)$ with $\alpha^n \in F$ and n minimum. Assume that $\mu(E) = \mu(F)$. If $F \subseteq L \subseteq E$ with L/F normal, then $\zeta_p \in F$ for every prime p dividing $[L : F]$.*

Proof. Since n is minimum and $\mu(E) = \mu(F)$, from Theorem 4 one has $n = [F(\alpha) : F]$, in particular $x^n - \alpha^n = x^n - a \in F[x]$ is irreducible. From Theorem 2 we have that $F(\alpha)/F$ has the u.s.p., hence $L = F(\sqrt[m]{a})$ with m dividing n and $[L : F] = m$, since L/F is normal we must have $\zeta_m \in L \subseteq F(\alpha)$, hence $\zeta_m \in F$. □

Proof of Theorem 5. We shall use part of Isaacs proof. Let $G = \mathrm{Gal}\,(E/F)$ be the Galois group of E/F, then $|G| = [E : F]$. If p is a prime dividing $|G|$, let N be the subgroup of G generated by the elements of G of order p. It is clear that N is normal in G. By Cauchy Theorem, $1 < N$, hence $L = E^N \neq E$ and by the Fundamental Theorem of Galois theory, L/F is normal hence $\alpha \notin L$, since otherwise normality of L/F would imply $L = E$. Let $H = \mathrm{Gal}(E/F(\alpha))$. The condition $F(\alpha) \not\subseteq L$ is equivalent to $N \not\subseteq H$, hence we may choose $\sigma \in N \setminus H$ of order p. Define $M := E^\sigma$, hence $F(\alpha) \not\subseteq M$. The assumption on α guarantees the existence of a repeated radical extension $F = F_0 \subseteq F_1 \cdots \subseteq F_r = K$ so that $\alpha \in F_r$ with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{n_i} \in F_{i-1}$. For each $i = 1, \ldots, r$ set $M_i = MF_i$ then $F_i \subseteq M_i \subseteq EF_r$, hence $\alpha \in M_r = EF_r$, thus there exists $s \geq 1$ so that $\alpha \in M_s \setminus M_{s-1}$. We also have that $M \subseteq M_{s-1} \cap E \subseteq M_s \cap E \subseteq E$. From the definition of M, $[E : M] = p$. Since $\alpha \notin M_{s-1} \cap E$ and $\alpha \in M_s \cap E$ then we must have $M = M_{s-1} \cap E$ and $E = E \cap M_s$.

From Galois theory we have EM_{s-1}/M_{s-1} is Galois of degree p. We also have, from the definition of M_s, that M_s/M_{s-1} is a radical extension. The assumption $\mu(EF_r) = \mu(F)$ implies $\mu(M_s) = \mu(M_{s-1})$, hence the assumptions of the previous lemma are satisfied, so $\zeta_p \in M_{s-1} \subseteq EF_r$. Applying again the assumption on n-th roots we have $\zeta_p \in F$.

The last conclusion follows from Kummer theory, since E/M is cyclic of degree p and $\zeta_p \in F$. □

Remark 7. Assumption ii) in Theorem 5 can be replaced by the weaker condition: for every prime p, $\zeta_{2p} \notin EK \setminus F$. This situation occurs in co-Galois theory, see [4] for the basic results on co-Galois extensions.

Acknowledgements

The ellaboration of the paper was partially supported by Conacyt through research project 61996.

References

[1] M. Acosta, W.Y. Vélez, The lattice of subfields of radical extensions, *J. Number Th.*, **15** (1982), 388-405.

[2] F. Barrera Mora, On subfields of radical extensions, *Communications in Algebra*, **27**, No. 10 (1999), 4641-4649.

[3] F. Barrera Mora, W.Y. Vélez, Some results on radical extensions, *Journal of Algebra*, **162**, No. 2 (1993), 295-301.

[4] C. Greither, D.K. Harrison, A Galois correspondence for radical extensions of fields, *J. Pure Appl. Algebra*, **43** (1986), 257-270.

[5] I.M. Isaacs, Solution of polynomials by real radicals, *The American Math. Monthly*, **92**, No. 8 (1985), 571-575.