Scientia Iranica, Vol. 4, Nos. 1&2, pp 57–59
© Sharif University of Technology, July 1997

SCIENTIA IRANICA

Research Note

Finite Simple Field Extensions

M. Arian-Nejad[1]

In this paper, a new approach to finite simple field extensions based on a generalization of a theorem of Kaplansky, is introduced. Furthermore, a simple method for enumeration of primitive elements in the case of a finite extension of a finite field is obtained.

INTRODUCTION

Let E be a field with a subfield F. An extension E/F is called simple if there exists an element $a \in E$ (primitive element), such that $E = F(a)$. This paper is focused on finite dimensional simple extensions and contains two sections. In the first section, by generalizing Kaplansky's method [1], a new approach to finite simple extensions (Theorem 2) is given. In the second section, the formula for the number of primitive elements is obtained using a simple method, compared with [2,3]. Before stating the obtained results, the following two theorems are recalled.

Theorem A (Steinitz)

A finite extension E/F is simple if, and only if, the number of intermediate fields between E and F is finite [4].

Theorem B

Any finite dimensional extension of $\mathbb{Q}$ contains only a finite number of roots of unity [4].

Let E be a field with a subset L. E is radical over L, if for each element $a \in E$, there exists a natural-number $n(a)$ such that $a^{n(a)} \in L$. E is said to be purely inseparable over L, if for each element $a \in E$ there exists a non-negative integer r such that $a^{p^r} \in L$, where $p =$ char E.

A NEW VIEWPOINT

A theorem of Kaplansky [5] states that if a field E is radical over any of its proper subfields such as F, then char $E = p \neq 0$. However, sometimes conditions in which a finite union of proper subfields should be dealth with, are encountered rather than a proper subfield. Therefore, a generalization of Kaplanskey's Theorem is needed such as the following (see also [6]).

Lemma

Let E be a field and let $K_i \subset E (i = 1, \ldots, m)$ be some proper subfields of E such that $\cup K_i \neq E$. If E is radical over $L = \cup K_i$, then char $E = p \neq 0$.

Proof

Let char $E = 0$. For an arbitrary element a in $E \setminus L$, consider the infinite set $G = \{a, a+1, a+2, \cdots\}$. By the pigeonhole principle, there exists an infinite subset $H = \{a+r_1, a+r_2, \cdots\}$ of G which is radical over one of the intermediate subfields, say K_t, for some $1 \leq t \leq m$. Let K be a finite normal extension of K_t containing a. Since $a \notin K_t$, there exists an automorphism φ of K over K_t such that $b = \varphi(a) \neq a$. For each $i = 1, 2, \cdots$, there exists a fixed integer $n_i > 0$ such that $(a + r_i)^{n_i} \in K_t$. Then,

$$\begin{aligned}(b + r_i)^{n_i} &= (\varphi(a) + r_i)^{n_i} \\ &= \varphi((a + r_i)^{n_i}) = (a + r_i)^{n_i} \ ,\end{aligned}$$

implies that $b + r_i = \omega_i(a + r_i)$, where $\omega_i \neq 1$ is n_i-th root of unity in K. It is clearly seen that if $i \neq j$, then $\omega_i \neq \omega_j$ and by eliminating b, the following equation is obtained:

$$(\omega_i - \omega_j)a = (\omega_j - 1)r_j - (\omega_i - 1)r_i \ .$$

Since ω_i and ω_j are roots of unity, a and hence its conjugate b, are algebraic over the prime field P, thus $[P(a, b) : P] < \infty$. All the ω_i's$(i \in \mathbb{N})$ are found in the field $P(a, b)$, which by Theorem B should contain only a finite number of roots of unity. Thus char $P \neq 0$, otherwise infinite mutually different roots of unity in $P(a, b)$ corresponding to the elements of the infinite set H must exist.□

The following theorem is a revised version of a result in [6] concerning some properties of finite separable extensions.

1. *Department of Mathematical Sciences, Sharif University of Technology, Tehran, I.R. Iran*

Theorem 1

For any finite separable field extension E/F, one, and only one, of the following is true:

i. There exists a primitive element a such that $E = F(a^t)$ for all $t \in \mathbb{N}$.

ii. Every element of $E^* = E - \{0\}$ is torsion.

Proof

Any finite separable extension is simple so, by Theorem A, there exists a finite number of fields $K_i \subset E$ $(i = 1, 2, \ldots, m)$, such that $F \subset K_i \subset E$. Let $L = \bigcup K_i$ and note that every element of $E \backslash L \neq \phi$ is primitive.

There are two possibilities concerning primitive elements. Either there exits a primitive element a such that $a^t \in E\backslash L$ for all $t \in \mathbb{N}$, which yields case (i) of the theorem, or, all primitive elements are radical over L. The latter case means that E is radical over L, hence, by the above Lemma, char $E = p \neq 0$. Given a primitive element a, note that if p_1 and p_2 are two different primes then $a^{p_1} + 1$ and $a^{p_2} + 1$ cannot be in the same subfield K_l. So, there must be infinitely many primes $p_i \neq p$ with $a^{p_i} + 1$ primitive. By the pigeonhole principle there exist natural i and j such that $(a^{p_i} + 1)^{n_i} \in K_l$ and $(a^{p_j} + 1)^{n_j} \in K_l$, for some fixed l. Let K be a finite normal extension of K_l containing a. Since $a \notin K_l$, there exists an automorphism φ of K over K_l such that $b = \varphi(a) \neq a$. Then, the equation $b^{p_i} + 1 = \omega(a^{p_i} + 1)$ together with $b^{p_j} + 1 = \omega'(a^{p_j} + 1)$ implies that:

$$(\omega a^{p_i} + (\omega - 1))^{p_j} - (\omega' a^{p_j} + (\omega' - 1))^{p_i} = 0,$$

where ω and ω' are the n_i-th and the n_j-th roots of unity, respectively.

Let $f(a)$ be the left hand side of the above equation, which is a polynomial in a with coefficients in $P(\omega, \omega')$ and P is the prime subfield. First suppose that all coefficients of $f(a)$ are zero. By the choice of p_i's, the coefficient of $a^{p_i(p_j-1)}$ is $p_j \omega^{p_j-1}(\omega - 1)$, which must be zero. Since $p_j \neq p$ then, $\omega = 1$ is obtained. Similarly, from the coefficient of $a^{p_j(p_i-1)}$ it is concluded that $\omega' = 1$. Thus, $a^{p_i} = b^{p_i}$ and $a^{p_j} = b^{p_j}$, hence $a = b$, which is a contradiction. So let some coefficients of $f(a)$ be nonzero, then a will become algebraic over $P(\omega, \omega')$ and hence algebraic over P. Now, let $r \in F$, then $a + r \in E\backslash L$, hence $a + r$ and $r = (a+r) - a$ are also algebraic over P. In other words, all of the elements of F are algebraic over P. Hence any element of E is algebraic over P, consequently the elements of E^* are all torsion.□

The following approach to finite simple extensions can now, be given.

Theorem 2

For any finite simple extension E/F one of the following is true:

i. E is separable over F and there exists a primitive element a such that $E = F(a^t)$, for all $t \in \mathbb{N}$.

ii. Every element of E^* is torsion.

iii. char $F = p \neq 0$ and there exists a primitive element a such that $E = F(a^m)$ for all $m \in \mathbb{N}$ such that $(m, p) = 1$.

Note that only cases (ii) and (iii) can occur simultaneously.

Proof

Let $S = S(E/F)$ be the separable closure of F in E. If $S = E$, then E is separable over F, and by Theorem 1, only cases (i) and (ii) can occur. So suppose $S \neq E$. Let $K_i (i = 1, 2, 3, \ldots, r)$ be all of the intermediate subfields of E over F. E is purely inseparable and hence radical over $L = \cup K_i$. Let L' be the union of all of the intermediate subfields over E which is purely inseparable, in other words $L' = \bigcup_{S \subseteq K_i} K_i$.

Now, two separate cases could be realized, either all of the primitive elements are radical over $L \setminus L'$, or there exists a primitive element which is not radical over $L \setminus L'$. In the former case, any primitive element radical over some intermediate field which is not contained in L' has at least a different conjugate in some finite normal extension of that field, hence the same argument as in Theorem 1 leads to the case (ii) of the theorem. For the latter case, consider the primitive element a which is not radical over $L \setminus L'$. Clearly, a is purely inseparable over L'. If the element a^m is not primitive for some $m \in \mathbb{N}$, such that $(m, p) = 1$, it must be in some subfield such as K_i in $L'(1 \leq i \leq r)$; therefore, $a \in K_i$, which is a contradiction. Hence case (iii) of the theorem is obtained. □

THE NUMBER OF PRIMITIVE ELEMENTS

Let F be a finite field with q elements and let E be a finite extension of F with the degree of n. Let $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ be the prime decomposition of n. As it is known, the elements of E are characterized by the roots of the separable polynomial $f(x) = x^{q^n} - x$. Also for any divisor d of n, E has a unique subextension K_d with the dimension d over F and conversely, every subextension K of E over F has dimension d for some divisor d of n. This means that every maximal subfield of E is of dimension $n_i = \frac{n}{p_i}$ (for some $1 \leq i \leq r$) and is uniquely determined by its dimension. Let K_i be the maximal subfield corresponding to dimension n_i. The nonempty set $S = E \backslash \cup K_i$ forms the set of all primitive elements of E over F. The cardinality of S is computed by "the principle of inclusion and exclusion". Since for $i \neq j$, $\mid K_i \cap K_j \mid = q^{n_{i,j}}$, where $n_{i,j} = \frac{n}{p_i p_j}$, and for

$i \neq j \neq k, \mid K_i \cap K_j \cap K_k \mid = q^{n_{i,j,k}}$, where $n_{i,j,k} = \frac{n}{p_i p_j p_k}$ $, \ldots,$ it may be concluded that:

$$|S| = q^n - \sum_i q^{n_i}$$

$$+ \sum_{i,j} q^{n_{i,j}} + \cdots + (-1)^r q^{n_{1,2,\ldots,r}} .$$

If the "Mobius" function is denoted by μ, then the above equation can be written in the following "well known" notation:

$$|S| = \sum_{d|n} \mu(n/d) q^d .$$

Every irreducible monic polynomial of degree n corresponds to n distinct elements of S. Hence N_n, the number of irreducible monic polynomials of degree n [4], is equal to $\frac{|S|}{n}$, in other words:

$$N_n = n^{-1} \sum_{d|n} \mu(n/d) q^d . \square$$

REFERENCES

1. Kaplansky, I. "A theorem on division rings", *Canadian j. of Mathematics*, **3**, pp 290–292 (1951).
2. Van Lint, J.H. and Wilson, R.M. *A Course in Combinatorics*, Cambridge University Press, p 116 (1992).
3. Ireland, K. and Rosen, M. *A Classical Introduction to Modern Number Theory*, Springer-Verlag, p 84 (1990).
4. Jacobson, N. *Basic Algebra I*, 2nd Edition, Freeman and Company, New York, USA (1985).
5. Lam, T.Y. *A First Course in Non-Commutative Rings*, Springer-Verlag, p 258 (1991).
6. Mahdavi-Hezavehi, M. et al. "On Derived Groups of Division Rings II", *Communications in Algebra,* **23**(8), pp 2881–2887 (1995).