ON THE ORDER AND DEGREE OF SOLUTIONS TO PURE EQUATIONS

LAWRENCE J. RIŞMAN

ABSTRACT. Let K be a field. Let θ be an element of a field extension of K . The order of θ over K is the smallest positive integer m such that θ^m lies in K , or ∞ . We compare the order m of θ to the degree h of θ over K . Clearly $h \leq m$.

THEOREM. Let K be a field. Let θ be an element of degree h and order m over K . Let p be a prime. Let p^e be the maximum power of p dividing h , and suppose p^s divides m .

- (1) If the characteristic of K is p , then $s \leq e$.
- (2) If $s > e$ and p is odd, then $K(\theta)$ contains a primitive p th root of unity u not in K . Moreover $K(u)$ contains a primitive p^{s-e} root of unity.
- (3) If $s > e$ and $p = 2$, then -1 is not a square in K and $K(\theta)$ contains $i = \sqrt{-1}$. Moreover -1 is a 2^{s-e} power in $K(i)$.

Let K be a field. A polynomial with coefficients in K of the form $a_0 x^{m_0} + a_1 x^{m_1} + \cdots + a_d x^{m_d}$ with all $a_i \neq 0$ is called a multinomial of length d . An element θ in an algebra over K has multinomial degree d if θ satisfies a multinomial of length d and no shorter multinomial. θ has finite multinomial degree d if and only if θ has finite algebraic degree h over K , and clearly $d \leq h$.

For an element θ in an algebra over K we are faced with the problem of determining the multinomial degree d of θ over K . If θ has multinomial degree d let $p(x)$ be a monic polynomial of minimal degree among the multinomials of length d satisfied by θ . $p(x)$ is called a minimal multinomial for θ . Clearly $d = 0$ if and only if θ is nilpotent, and in this case the minimal multinomial for θ is the minimal polynomial for θ over K . If θ is not a zero divisor then we need consider only polynomials with nonzero constant term, i.e., we can require $m_0 = 0$ in the above definition.

If $d = 1$ or if θ is not a zero divisor and $d = 2$, then the minimal multinomial for θ is unique. For in these cases the difference between two minimal multinomials, if not zero, would be a multinomial of length $\leq d$ and lower degree satisfied by θ .

LEMMA 1. Let $\theta \in A$ have a multinomial degree $d \geq 1$. Suppose x^n is the maximum power of x dividing the minimal polynomial $x^n \cdot q(x)$ for θ over K . Then there exist orthogonal idempotents e_1 and e_2 in A that commute with θ such that $e_1 + e_2 = 1$, $\theta_1 = \theta e_1$ is nilpotent, $\theta_2 = \theta e_2$ is invertible in $A_2 = e_2 A e_2$, the minimal polynomial for θ_2 in A_2 is $q(x)$, θ_2 has multinomial degree d in A_2 , and any minimal multinomial for θ is x^n multiplied by a minimal multinomial for θ_2 in A_2 .

Presented to the Society, February 21, 1975; received by the editors March 6, 1975.

AMS (MOS) subject classifications (1970). Primary 12E10, 12F10, 12A20.

© American Mathematical Society 1976

PROOF. If $n = 0$, taking $e_1 = 0$ and $e_2 = 1$ we are done. Suppose $n \neq 0$. Let $r(x)$ and $s(x)$ be polynomials such that $r(x) \cdot x^n + s(x) \cdot q(x) = 1$. Set $e_1 = s(\theta)q(\theta)$ and $e_2 = r(\theta)\theta^n$. It is easily seen that e_1 and e_2 satisfy the required conditions. Note that the unit element of $e_i A e_i$ is not 1 but e_i , and that θ satisfies a polynomial if and only if θ_1 and θ_2 satisfy it considered as elements of $e_1 A e_1$ and $e_2 A e_2$ respectively. Q.E.D.

Note that by the above lemma and the discussion that precedes it the minimal multinomial for any element of multinomial degree $d \leq 2$ is unique. In what follows we assume that θ is not a zero divisor. Then θ has multinomial degree 1 if and only if some positive power of θ is a nonzero element of K .

We define the order of θ over K as the smallest positive integer m such that θ^m lies in K , or ∞ if no positive power of θ lies in K . Thus the order of θ is simply the order of θ considered as an element of the multiplicative group of $K(\theta)$ modulo the multiplicative group of K , and it is finite if and only if θ has multinomial degree 1. If θ has finite order m over K and $a = \theta^m$, then $x^m - a$ is the minimal multinomial for θ and the minimal polynomial for θ divides $x^m - a$. The degree of θ is less than or equal to its order with equality if and only if the minimal polynomial for θ over K is $x^m - a$.

We now assume that the minimal polynomial for θ over K is irreducible so that $K(\theta)$ is a field extension of K . If θ has finite order then the Galois group of θ over K is solvable, but certainly not conversely. For an extensive discussion of the "pure equation" $x^m - a$, see [2, Part I, Chapters 6 and 12].

By Proposition 1 of [4] if the degree of θ over K is odd and the order of θ is finite, then the order of θ is odd. By Proposition 2 of [4] if K is the field of rational numbers and θ has odd degree over K , then the order of θ equals its degree. By Lemma 3.1 of [1] if θ has degree h and order m over a field L which is finitely generated over the prime field, then $m \leq M \cdot h!$ where M is as follows. M is an integer so that $u^M = 1$ for all roots of unity u satisfying $[K(u): K] \leq h!$.

In this paper we investigate how the degree is related to the order of an element θ , and how the minimal polynomial of θ is related to the polynomial $x^m - a$. Some of the complications that arise are illustrated by the following examples. If p is an odd prime, a primitive p th root of unity has degree $p - 1$ over the rationals and order p . Let m be any integer > 2 , and let θ be a primitive m root of unity in the complex numbers. Then θ has degree 2 over the real numbers. The order of θ over the reals is m if m is odd and $m/2$ if m is even.

Let K be the field of rational numbers. Let L be the field $K(\sqrt{-3})$ which contains the primitive 3rd root of unity $u = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. Let b be a nonzero rational number. Set $\theta = b \cdot u \cdot \sqrt{-3}$. Then the minimal polynomial for θ over K is $x^2 + 3bx + 3b^2$ and $\theta^6 = -27b^6$. The order of θ over K is 6.

Observe that over any field

$$x^{4n} + 4b^4 = (x^{2n} + 2bx^n + 2b^2)(x^{2n} - 2bx + 2b^2).$$

Furthermore the quadratic polynomials $x^2 + 2bx + 2b^2$ and $x^2 - 2bx + 2b^2$ are irreducible over a field K of characteristic $\neq 2$ if and only if -1 is not a square in K . Let K and b be as above. Set $\theta = b + bi$ with $i^2 = -1$. Then the minimal polynomial for θ over K is $x^2 - 2bx + 2b^2$ and $\theta^4 = -4b^4$. The order of θ over K is 4.

From the above examples it is clear that in estimating the order of θ over K we must take into account both the degree of θ over K and the roots of unity in $K(\theta)$ not in K . We have the following results.

PROPOSITION 1. *Let K be a field. Let θ be an element of finite order m over K . Then $m = t \cdot n$ where n is an integer dividing the degree h of θ over K and t is an integer satisfying the following condition. For each prime p that divides t , $K(\theta)$ contains a p th root of -1 not in K .*

REMARK. The stated condition on t is clearly equivalent to the following two conditions

(1) For each odd prime p that divides t , $K(\theta)$ contains a p th root of unity not in K .

(2) If 2 divides t , then -1 is a square in $K(\theta)$ but not in K .

PROOF. Let $a = \theta^m$. Let us factor $m = t \cdot n$ with t and n relatively prime as follows. For each odd prime p dividing m , p divides n if and only if a is not a p th power of any element of K . If m is even but not divisible by 4, 2 divides n . If 4 divides m , 2 divides n (and hence 4 divides n) if and only if $a \neq -4b^4$ for any $b \in K$. It remains to show that t and n satisfy the above conditions.

Suppose $m = r \cdot s$ with $r > 1$. If $a = b^r$ for some $b \in K$, then $(\theta^s)^r = b^r$. Hence $\theta^s = b \cdot u$ for an r th root of unity u in $K(\theta)$. If $u \in K$, $\theta^s \in K$ contradicting the minimality of m . Thus either $K(\theta)$ contains an r th root of unity not in K , or a is not an r th power of any element of K . This conclusion holds, in particular, for r any prime divisor of m . Thus if m is even a is not a square of any element of K .

By our choice of n we can conclude from Capelli's Theorem [3, Theorem 16, Chapter 8, §9] that the polynomial $x^n - a$ is irreducible over K . Since θ^n satisfies this polynomial, $x^n - a$ is the minimal polynomial of θ^n over K . Hence n is the degree of θ^n over K . As $\theta^n \in K(\theta)$ we conclude that n divides the degree of θ over K .

By the choice of t if an odd prime p divides t , then a is a p th power of an element of K . Hence $K(\theta)$ contains a p th root of unity not in K . Suppose 2 divides t . Then 4 divides m and $a = -4b^4$ for some $b \in K$. Since $a \neq 0$ the characteristic of $K \neq 2$. As a is not a square in K , it follows that -1 is not a square in K . $(\theta^{m/2}/2b^2)^2 = -1$. Hence -1 is a square in $K(\theta)$. Q.E.D.

The proof of the above proposition yields the following corollaries.

COROLLARY 1. *The integers t and n in the proposition can be chosen relatively prime and such that $x^n - a$ is the minimal polynomial for θ^n over K .*

COROLLARY 2. *Let θ be an element of finite order m over a field K , and let $a = \theta^m$. Suppose $K(\theta)$ contains no p th root of -1 not in K for any p . Then $x^m - a$ is the minimal polynomial for θ over K .*

By Corollary 2, an element θ whose minimal polynomial over K has length greater than 1 has multinomial degree greater than 1, unless $K(\theta)$ contains a p th root of -1 not in K . We note that the above-cited results of [4] follow easily from Proposition 1.

We restate the proposition as follows.

COROLLARY 3. *Let K be a field. Let θ be an element of degree h and finite order*

m over K . If p is a prime that divides m to a higher power than it divides h , then $K(\theta)$ contains a p th root of -1 not in K .

COROLLARY 4. Let θ be an element of degree 2 over the rationals K . If θ has finite order m over the rationals, then $m = 2^j$, $m = 3^j$, or $m = 2 \cdot 3^j$.

PROOF. If $K(\theta) = K(\sqrt{-1})$, then $m = 2^j$ with $j \geq 1$ by the proposition. If $K(\theta) = K(\sqrt{-3})$ then by the proposition either $m = 2$, $m = 3^j$, or $m = 2 \cdot 3^j$ with $j \geq 1$. In all other cases $K(\theta)$ contains no irrational roots of unity, and $m = 2$ by the proposition. Q.E.D.

We now specify more precisely the factor t of the above proposition so as to conclude, in particular, that the exponent j in Corollary 4 is not too large.

PROPOSITION 2. Let K be a field. Let θ be an element of degree h and finite order m over K . Let p be a prime. Let p^e be the exact power of p dividing h , and suppose p^s divides m . If $s > e$, then $K(\theta)$ contains a p -power root of unity v whose order over K is p^{s-e} .

PROOF. Let $a = \theta^m$ and $\alpha = \theta^{m/p^s}$. Then $\alpha^{p^s} = a$ and α has order p^s over K . The conjugates of α over K in any normal extension of K are of the form $\alpha \cdot u$ for various p -power roots of unity u . Let r be the degree of α over K . As $\alpha \in K(\theta)$ r divides h . The constant term of the minimal polynomial for α over K is clearly $(-1)^r \alpha^r \cdot v$ where v is a p -power root of unity. Hence the norm of α from $K(\alpha)$ to K , $N(\alpha) = \alpha^r v$.

Since the g.c.d. of h and p^s is p^e , the order of α^h over K is p^{s-e} . As r divides h the order of α^r over K is p^j with $j \geq s - e$.

Since $v = N(\alpha)/\alpha^r$ with $N(\alpha)$ in K , the order of v over K is p^j . Q.E.D.

Combining the above results we obtain the following.

PROPOSITION 3. Let K be a field. Let θ be an element of degree h and finite order m over K . Let p be a prime. Let p^e be the exact power of p dividing h , and suppose p^s divides m .

- (1) If the characteristic of K is p , then $s \leq e$.
- (2) If $s > e$ and p is odd, then K does not contain a primitive p th root of unity and $K(\theta)$ contains a primitive p^{s-e} root of unity.
- (3) if $s > e$ and $p = 2$, then -1 is not a square in K and -1 is a 2^{s-e} power in $K(\theta)$.

PROOF. Immediate from Corollary 3 to Proposition 1, together with Proposition 2.

COROLLARY 1. Let θ be an element of degree 2 over the rationals. If θ has finite order m over the rationals, then $m = 2, 4, 3$ or 6 .

PROOF. Immediate from Corollary 4 to Proposition 1 together with Proposition 3. It is clear how and when these values of m do occur.

COROLLARY 2. Let K be a field. Let θ be an element of degree h and finite order m over K . Suppose the group of roots of unity in $K(\theta)$ modulo the group of roots of unity in K is finite of order T . Then m divides $h \cdot T$.

PROOF. Immediate. In fact T can be replaced by the order of the subgroup

generated by the p -power roots of unity for those p such that L contains a p th root of -1 not in K .

Every finitely generated group of roots of unity in a field is a finite cyclic group. Hence every finitely generated subgroup of the group of roots of unity in $K(\theta)$ modulo the roots of unity in K is a finite cyclic group. Thus if the group of roots of unity in $K(\theta)$ modulo the roots of unity in K is infinite, $K(\theta)$ contains roots of unity of arbitrarily large order over K . Thus we have the following corollary.

COROLLARY 3. *Let K be a field and let L be a finite extension field of K . There is a finite bound to the orders of elements of L of finite order over K if and only if the group of roots of unity in L modulo the roots of unity in K is finite.*

The hypothesis of Corollary 2 certainly fails for the complex numbers over the reals. However, there is no paucity of fields satisfying the hypothesis of Corollary 2. As observed in [1], in any field finitely generated over the prime field the group of roots of unity is finite. It is well known that in any field with a discrete valuation and finite residue class field the group of roots of unity is finite. In fact, if L is a field with discrete valuation whose residue class field contains only finitely many roots of unity, then L contains only finitely many roots of unity. To sharpen the above results we require the following lemma.

LEMMA 2. *Let M be an extension field of K , and let L be a subextension of M over K . Let θ be an element of M of finite order m over K . Let r be the order of θ over L . Then r divides m and θ^r has order m/r over K .*

PROOF. Elementary. This result is valid if M is merely assumed to be a group L a subgroup of M , and K a subset of L .

PROPOSITION 4. *We adopt the hypotheses and notation of Proposition 3.*

(1) *If $s > e$ and p is odd, let u be a primitive p th root of unity in $K(\theta)$. Then $K(u)$ contains a primitive p^{s-e} root of unity.*

(2) *if $s > e$ and $p = 2$, let i be a square root of -1 in $K(\theta)$. Then -1 is a 2^{s-e} power in $K(i)$.*

PROOF. Suppose $s > e$ and p is odd. Let m' be the order of θ over $K(u)$, and let h' be the degree of θ over $K(u)$. Note that the degree of u over $K \leq p - 1$, so it is certainly not divisible by p . Since p divides h to the exact power p^e , p divides h' to the exact power p^e . Since $K(u)$ contains a primitive p th root of unity u , by Proposition 3 p cannot divide m' to any power higher than p^e . By hypothesis p^s divides m , and by the lemma m' divides m . $\theta^{m'}$ is an element of $K(u)$ of order m/m' over K , and p^{s-e} divides m/m' . By Proposition 3, $K(u)$ contains a primitive p^{s-e} root of unity.

Suppose $s > e$ and $p = 2$. Let m' be the order of θ over $K(i)$, and let h' be the degree of θ over $K(i)$. Note that the degree of i over K is 2. Hence $h' = h/2$ and 2 divides h' to the exact power 2^{e-1} . Since -1 is a square in $K(i)$, 2 cannot divide m' to any higher power than 2^{e-1} by Proposition 3. By hypothesis 2^s divides m , and by the lemma m' divides m . $\theta^{m'}$ is an element of $K(i)$ of order m/m' over K , and 2^{s-e+1} divides m/m' . By Proposition 3, -1 is a 2^{s-e} power in $K(i)$. Q.E.D.

COROLLARY 1. Suppose $p = 2$, $s > e$, and neither 2 nor -2 is a square in K . Then $s = e + 1$.

PROOF. By hypothesis, 4 is not a 4th power in K . By Proposition 3, -1 is not a square in K . Hence $x^4 + 1$ is irreducible over K by the above-cited theorem of [3]. Hence -1 is not a 4th power in $K(i)$. By Proposition 4, $s \leq e + 1$. Q.E.D.

It is clear how the statement of Corollary 2 to Proposition 3 can be strengthened in the light of Proposition 4. Note that the above propositions give necessary conditions for an irreducible polynomial, the minimal polynomial of θ , to divide a polynomial of the form $x^m - a$.

COROLLARY 2. Let K be the field of rational numbers. Let θ be an element of degree h and finite order m over K .

(1) Let p be a prime. Let p^e be the exact power of p dividing h , $0 \leq e$. Suppose p^s divides m and $s > e$. Then $s = e + 1$ and $p - 1$ divides h .

(2) Then $m = t \cdot n$ where n divides h , t is square free, and $\phi(t)$ divides h , where ϕ is Euler's ϕ function.

PROOF. A primitive p^i root of unity has degree $(p - 1)p^{i-1}$ over K . Assertion 1 follows by the proposition. A primitive t th root of unity has degree $\phi(t)$ over the rationals. Assertion 2 follows from Assertion 1 and the proposition. Q.E.D.

ACKNOWLEDGMENT. I wish to express my appreciation to my colleagues at the Technion, and to Mrs. Connie Moller, the typist.

REFERENCES

1. Israel N. Herstein, Claudio Procesi and Murray Schacher, *Algebraic valued functions on noncommutative rings*, J. Algebra **36** (1975).
2. Irving Kaplansky, *Fields and rings*, Univ. of Chicago Press, Chicago, Ill., 1969. MR **42** #4345.
3. Serge Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965. MR **33** #5416.
4. Lawrence Risman, *On the multinomial degree of an element and solutions to pure equations*, Technion Preprint Series No. MT-234, 1975.

DEPARTMENT OF MATHEMATICS, TECHNION-ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA, ISRAEL