Proceedings of the Edinburgh Mathematical Society (2004) **47**, 119–123 ©
DOI:10.1017/S0013091503000427 Printed in the United Kingdom

ON SUBFIELDS OF A FIELD GENERATED BY TWO CONJUGATE ALGEBRAIC NUMBERS

PAULIUS DRUNGILAS AND ARTŪRAS DUBICKAS

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius 2600, Lithuania (padr0254@uosis.mif.vu.lt; arturas.dubickas@maf.vu.lt)

(Received 27 May 2003)

Abstract Let k be a field, and let α and α' be two algebraic numbers conjugate over k. We prove a result which implies that if $L \subset k(\alpha, \alpha')$ is an abelian or Hamiltonian extension of k, then $[L : k] \leqslant [k(\alpha) : k]$. This is related to a certain question concerning the degree of an algebraic number and the degree of a quotient of its two conjugates provided that the quotient is a root of unity, which was raised (and answered) earlier by Cantor. Moreover, we introduce a new notion of the non-torsion power of an algebraic number and prove that a monic polynomial in X—irreducible over a real field and having m roots of equal modulus, at least one of which is real—is a polynomial in X^m.

Keywords: field; subfield; algebraic numbers; abelian and Hamiltonian extensions; roots of unity

2000 *Mathematics subject classification:* Primary 11R04; 11R20; 11R32; 12F10

1. Results

Let k be a field, and let k^{a} be an algebraic closure of k. In this paper we give a short and self-contained proof of the following theorem.

Theorem 1.1. *Suppose that $\alpha, \alpha' \in k^{\mathrm{a}}$ are conjugate over k, and $L \subset k(\alpha, \alpha')$. If L and $L \cap k(\alpha)$ are Galois extensions of k, then $[L : k][k(\alpha, \alpha') : L(\alpha)] \leqslant [k(\alpha) : k]$.*

The condition of the theorem on $L \cap k(\alpha)$ always holds if L/k is an abelian extension. However, this is not the only case. We say that L is a *Hamiltonian extension* of k if it is a Galois extension and $\mathrm{Gal}(L/k)$ is a Hamiltonian group, namely, a non-abelian group every subgroup of which is normal. For example, the quaternion group Q_8 is Hamiltonian. It occurs as a Galois group over the field of rational numbers $\mathbb{Q}$, since it is a 2-group. See p. 190 of [**8**] for the description of all Hamiltonian groups.

Corollary 1.2. *Suppose that $\alpha, \alpha' \in k^{\mathrm{a}}$ are conjugate over k. If $L \subset k(\alpha, \alpha')$ is an abelian or Hamiltonian extension of k, then $[L : k][k(\alpha, \alpha') : L(\alpha)] \leqslant [k(\alpha) : k]$.*

Corollary 1.3. *Suppose that $\alpha \in k^{\mathrm{a}}$ is of degree d over k, and α' is conjugate to α over k. If $\beta = \alpha'/\alpha$ is a root of unity, then $n = [k(\beta) : k] \leqslant d$.*

https://doi.org/10.1017/S0013091503000427 Published online by Cambridge University Press

Evidently, for every $\beta \neq 0, -1$, we have $\beta = (1+\beta)/(1+\beta^{-1})$ (see also [**5**]). If β is a root of unity, then β and β^{-1} are conjugate over k. Hence so are $\alpha' = 1+\beta$ and $\alpha = 1+\beta^{-1}$. Thus $n = d$, so Corollary 1.3 is sharp.

Let α and α' be conjugate over $\mathbb{Q}$, and let α'/α be a primitive nth root of unity. Cantor asked whether $\phi(n) \leqslant d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, where ϕ stands for Euler's function. This was answered in the affirmative both by himself and by Isaacs [**10**]. Dubickas independently asked a question equivalent to that of Cantor once again in [**4**]. Corollary 1.3 settles this question for an arbitrary field. A different proof of Corollary 1.3 and that of the abelian part of Corollary 1.2 (to be precise, of the inequality $[L : k] \leqslant [k(\alpha) : k]$, where L is a subfield of $k(\alpha, \alpha')$ and is an abelian extension of k) was also given in [**1**].

Guralnick [**7**] recently obtained a more precise version of Cantor's result for cyclotomic extensions (see also [**1**] and [**11**] for other results in abelian extensions). For fields, it states that if L/k is cyclic and L is contained in the Galois closure of $k(\alpha)$ over k, then $[L : k] \leqslant [k(\alpha) : k]$. Its proof depends upon the classification of finite simple groups. The example given on p. 95 in [**1**] shows that this fails for abelian extensions. More precisely, there are abelian extensions contained in the Galois closure of $k(\alpha)$ over k for which $[L : k] \geqslant 2^{d/2\log_2 d}$, where $d = [k(\alpha) : k]$. Applied to roots of unity, Guralnick's result implies that if a rational function in conjugates of an algebraic number of degree d is a pth root of unity with p being prime, then $p - 1 \leqslant d$.

Both the theorem and Corollary 1.2 are results of a different kind. Unlike Guralnick's result, they do not weaken Cantor's assumption on L (to lie in a field generated by just two conjugates) at the expense of strengthening his assumption on L/k, but show that the same inequality still holds under a weaker assumption on L/k (instead of L/k being abelian). The theorem gives probably the weakest possible assumption. Furthermore, if $L(\alpha)$ is a proper subfield of $k(\alpha, \alpha')$, then our inequality is stronger, because of an extra factor on the left-hand side.

One needs some assumption on L or on its subfield, for otherwise $[L : k]$ can be large compared with $[k(\alpha) : k]$. Indeed, if d is a prime number and k is a number field, we can take an algebraic number α of degree d over k such that $\mathrm{Gal}(K/k)$, where K is the Galois closure of $k(\alpha)$ over k, is isomorphic to the one-dimensional affine group $AGL_1(d)$. This group is of order $d(d-1)$ (see [**3**, p. 52]). It is generated by a d-cycle and a $(d-1)$-cycle. So, by Galois theory, K can be generated by two conjugates, say, $k(\alpha, \alpha') = K$. Setting $L = k(\alpha, \alpha') = K$, we see that L/k is normal, $[L : k] = d(d-1)$ and $[k(\alpha) : k] = d$.

2. Connections with other work

Let N be the smallest positive integer such that α^N is torsion free. As in [**4**], a number α algebraic over k is called *torsion free* if no quotient of its two distinct conjugates is a root of unity. We then call N a *non-torsion power* of α over k. For α being separable over k, the number α^N has the smallest degree over k among all positive integer powers of α. Of course, for such α, $N = 1$ if and only if no quotient α'/α, where α' runs over every conjugate of α distinct from α, is a root of unity.

Given a positive integer m, we denote by $\hat{m}$ the largest positive integer for which $\phi(\hat{m}) \leqslant m$. We are now able give a sharp version of Proposition 2 in [**4**].

https://doi.org/10.1017/S0013091503000427 Published online by Cambridge University Press

Corollary 2.1. *Suppose that $\alpha \in \bar{\mathbb{Q}}$ is of degree d and of non-torsion power N over $\mathbb{Q}$. Then $N \leqslant \hat{d}$.*

From analytic number theory it is well known that

$$\liminf_{m\to\infty} \frac{\phi(m)\log\log m}{m} = \exp(-\gamma),$$

where $\gamma = \lim_{m\to\infty} = 1+\frac{1}{2}+\cdots+1/m-\log m = 0.557\,215\ldots$ is Euler's constant (see, for example, [**9**, p. 267]). Therefore, there is a positive constant c such that $\hat{d} < cd\log\log d$ for every d. For d sufficiently large, c can be taken as $1.781\,073 > \exp(\gamma)$. So

$$N < 1.781\,073\, d\log\log d$$

for every sufficiently large d. Of course, this inequality can be replaced by a slightly weaker inequality valid for all d by use of the inequalities for $\phi(m)$ in the classical paper [**13**].

The non-torsion power of an algebraic number appears naturally in the investigation of multiplicative forms in conjugate algebraic numbers. Apparently, the first result in this direction is that of Smyth [**15**], who showed that the equality $\alpha^2 = \alpha'\alpha''$, where α, α', α'' are conjugate over $\mathbb{Q}$, is only possible if α'/α is a root of unity. (See, for example, [**4**] for more references on further work in this direction.) By raising an algebraic number to its non-torsion power, one obtains a torsion-free algebraic number. Corollary 2.1 shows that the smallest such power must be quite small.

The non-torsion power is related to the so-called multinomial degree of an algebraic number. In [**14**], Schacher and Straus defined the *multinomial degree* of a number α algebraic over k as the smallest positive integer q for which there exist positive integers $a_1 < \cdots < a_{q-1}$ such that $1, \alpha^{a_1}, \ldots, \alpha^{a_{q-1}}$ are linearly dependent over k. Of course, if the non-torsion power of α over k is equal to N, then $q-1$ is at most the degree of α^N over k.

In Theorem 6 of [**4**], Dubickas considered those algebraic numbers expressible as a sum of two distinct conjugate algebraic numbers. It was shown there that if the degree of β over $\mathbb{Q}$, n, is prime and $\beta = \alpha+\alpha'$, where $\alpha \neq \alpha'$ are conjugate over $\mathbb{Q}$, then the smallest possible degree of α over $\mathbb{Q}$ is either equal to n or it is equal to $2n$. Setting $L = k(\alpha+\alpha')$, where α and α' are conjugate over k, in Corollary 1.2, we see that if $\beta = \alpha+\alpha'$ is such that $k(\beta)/k$ is either an abelian or Hamiltonian extension, then the degree of α over k is at least n.

Boyd [**2**] was interested in the following question. Assume that the monic irreducible polynomial $P(X) \in \mathbb{Q}[X]$ has exactly m roots of equal modulus, one of which, say α, is real. Is it true that $P(X) = F(X^m)$ with $F(X) \in \mathbb{Q}[X]$? This was answered in the affirmative by Ferguson [**6**]. In general, with the above definition of the non-torsion power, we can only say that, given an algebraic-over-k number α, its minimal polynomial $P(X) \in k[X]$ (which is monic) divides $F(X^N)$, where N is the non-torsion power of α, and $F(X) \in k[X]$ is the minimal polynomial of α^N. However, assuming Boyd's condition, one can easily see that if k is a subfield of the field of real numbers and α is real, then (up to a sign) α^m equals the product of all these m roots $\pm\alpha\alpha_2\cdots\alpha_m$, because the set

https://doi.org/10.1017/S0013091503000427 Published online by Cambridge University Press

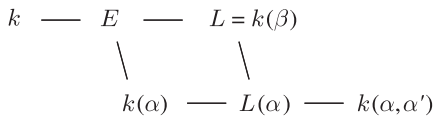
of conjugates is invariant under complex conjugation. Let G be the Galois group of the normal closure of $k(\alpha)$ over k. On applying all $\sigma \in G$ to the equality $\alpha^m = \pm\alpha\alpha_2 \cdots \alpha_m$, we obtain a list of $|G|$ such equalities. In particular, consider all equalities containing the conjugates of α of largest modulus on the left-hand side. By modulus considerations, every conjugate on the right-hand side must also be of largest modulus. Moreover, every such conjugate appears an equal number of times and so every conjugate of largest modulus appears in the product expressing the mth powers of the conjugates with largest moduli only. We can now consider the list of equalities with the conjugates of α^m of the second largest modulus, and so on. As soon as we come to the list of equalities of modulus $|\alpha^m|$, we see that the right-hand sides of these are all equal to $\pm\alpha\alpha_2 \cdots \alpha_m$, because all conjugates having larger moduli are already 'occupied'. Hence $\alpha^m = \alpha_2^m = \cdots = \alpha_m^m$. Mapping this to other conjugates, we obtain d/m such equalities, where d is the degree of α over k. Note that α^m is the unique conjugate of α^m having modulus $|\alpha^m|$. Thus $N = m$ and $\deg P = d = m \deg \alpha^m = m \deg F$. Now, by degree considerations and because both polynomials are monic, we deduce that $P(X) = F(X^m)$. This proves the result of Boyd and Ferguson in the following more general setting.

Proposition 2.2. *Let k be a subfield of the field of real numbers. If $P(X) \in k[X]$ is a monic polynomial irreducible over k which has exactly m roots of equal modulus at least one of which is real, then $P(X) = F(X^m)$ with $F(X) \in k[X]$.*

Note that our argument, unlike Ferguson's, does not use the above-mentioned lemma of Smyth.

3. Proofs

Proof of Theorem 1.1. Set $E = L \cap k(\alpha)$. Since L/k is separable, by the Primitive Element Theorem [**12**, p. 243], $L = k(\beta)$. Let ℓ be the degree of α over E, and let s be the degree of β over E. Then $[L : k] = [E : k]s$ and $[k(\alpha) : k] = [E : k]\ell$, so it suffices to show that $s[k(\alpha, \alpha') : L(\alpha)] \leqslant \ell$.



Using the fact that L/k is normal, we first prove that β is of degree s over $k(\alpha)$. Let $P(X)$ be the minimal polynomial of β over $k(\alpha)$. Note that every coefficient of $P(X)$ is expressible as a polynomial in β with coefficients in k, since every conjugate of β over k is so expressible. At the same time, every coefficient of $P(X)$ is expressible as a polynomial in α with coefficients in k. But $k(\alpha) \cap k(\beta) = E$, so $P(X) \in E[X]$. It follows that $P(X)$ is also the minimal polynomial of β over E.

Now, we show that α and α' are both of degree ℓ over E, because E/k is normal. Let ℓ' be the degree of α' over E, and let $T(X) \in E[X]$ be the minimal polynomial of α over E. Any automorphism which takes α to α' maps the equality $T(\alpha) = 0$ to $S(\alpha') = 0$, where $S(X)$ is a polynomial of degree ℓ in X with coefficients in E. Thus $\ell' \leqslant \ell$. Similarly, mapping α' to α we obtain that $\ell \leqslant \ell'$. Hence $\ell' = \ell$.

https://doi.org/10.1017/S0013091503000427 Published online by Cambridge University Press

Since $k(\alpha) \subset k(\alpha, \beta) = L(\alpha) \subset k(\alpha, \alpha')$ and the degree of β over $k(\alpha)$ is s, we deduce that $s[k(\alpha, \alpha') : L(\alpha)] = [k(\alpha, \alpha') : k(\alpha)]$. The degree of α' over the field $k(\alpha)$ cannot exceed the degree of α' over its subfield E, which is equal to $\ell' = \ell$. Hence $[k(\alpha, \alpha') : k(\alpha)] \leqslant \ell$, and the proof is completed. □

Proof of Corollaries 1.2 and 1.3. Note that in both (abelian and Hamiltonian) cases every subgroup of $\mathrm{Gal}(L/k)$ is normal. In particular, this implies that $L \cap k(\alpha)$ is a normal extension of k. Corollary 1.2 now follows from Theorem 1.1. Setting $L = k(\beta)$, we see that Corollary 1.3 is an immediate consequence of Corollary 1.2, since $k(\beta)/k$ is abelian for β a root of unity. □

Proof of Corollary 2.1. Assume that $N > \hat{d}$, i.e. $\phi(N) > d$. Then $N > 1$, hence $\beta = \alpha'/\alpha$ is a root of unity for some $\alpha' \neq \alpha$ conjugate to α over $\mathbb{Q}$. By the definition of non-torsion power, $(\alpha'/\alpha)^N$ cannot be a root of unity distinct from 1. So $\alpha^N = \alpha'^N$, i.e. $\beta^N = 1$ and N is minimal with this property. Thus β is a primitive Nth root of unity. By Corollary 1.3, $n = [\mathbb{Q}(\beta) : \mathbb{Q}] = \phi(N) \leqslant d$, a contradiction. □

Acknowledgements. We thank Professor R. M. Guralnick for pointing out some relevant references. The research of A.D. was partly supported by the Lithuanian State Science and Studies Foundation.

References

1. M. G. Aschbacher and R. M. Guralnick, On Abelian quotients of primitive groups, *Proc. Am. Math. Soc.* **107** (1989), 89–95.
2. D. W. Boyd, Irreducible polynomials with many roots of maximal modulus, *Acta Arithm.* **68** (1994), 85–88.
3. J. D. Dixon and B. Mortimer, *Permutation groups,* Graduate Texts in Mathematics, vol. 163 (Springer, 1996).
4. A. Dubickas, On the degree of a linear form in conjugates of an algebraic number, *Illinois J. Math.* **46** (2002), 571–585.
5. A. Dubickas and C. J. Smyth, Variations on the theme of Hilbert's Theorem 90, *Glasgow Math. J.* **44** (2002), 435–441.
6. R. Ferguson, Irreducible polynomials with many roots of equal modulus, *Acta Arithm.* **78** (1997), 221–225.
7. R. M. Guralnick, Cyclic quotients of transitive groups, *J. Alg.* **234** (2000), 507–532.
8. M. Hall, *The theory of groups*, (Macmillan, New York, 1959).
9. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 3rd edn (Oxford University Press, 1954).
10. I. M. Isaacs, Quotients which are roots of unity (solution of problem 6523), *Am. Math. Mon.* **95** (1988), 561–562.
11. L. G. Kovács and C. E. Praeger, Finite permutation groups with large Abelian quotients, *Pac. J. Math.* **136** (1989), 283–292.
12. S. Lang, *Algebra*, 3rd edn, Graduate Texts in Mathematics, vol. 211 (Springer, 2002).
13. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.
14. M. Schacher and E. G. Straus, Some applications of a non-Archimedean analogue of Descartes' rule of signs, *Acta Arithm.* **25** (1974), 353–357.
15. C. J. Smyth, Conjugate algebraic numbers on conics, *Acta Arithm.* **40** (1982), 333–346.

https://doi.org/10.1017/S0013091503000427 Published online by Cambridge University Press