BULL. AUSTRAL. MATH. SOC. 20E06, 12F05, 12F20
VOL. 51 (1995) [73–81]

COMPOSITES OF TRANSLATIONS AND ODD RATIONAL POWERS ACT FREELY

STEPHEN D. COHEN AND A.M.W. GLASS

Dedicated to Gilbert Baumslag belatedly on his 60th birthday
with our appreciation and respect.

It is shown that no non-trivial composition of translations $x \mapsto x + a$ and odd rational powers $x \mapsto^{p/q}$, where p,q are odd co-prime integers, positive or negative with $p/q \neq \pm 1$, acts like the identity on a field of characteristic zero. This extends a theorem of Adeleke, Glass, and Morley in which only odd ***positive*** rational powers were considered. Moreover, the nature of the proof itself (by field theory) is a simplification and natural refinement of previous proofs. It has applications in other settings.

1. INTRODUCTION

Let L be a field of characteristic zero (such as $\mathbb{R}$ or $\mathbb{C}$). Denote by T_L the Abelian group (under composition) of translations $T_L = \{t_a : a \in L\}$, where $xt_a = x + a$, and by P_0^+ that of odd positive rational power maps

$$P_0^+ = \{e_p r_q : p,\ q \text{ odd co-prime positive integers}\},$$

where $xe_p = x^p$ and $xr_q = x^{1/q}$ and it is assumed that the action $x \mapsto x^{p/q}$ is always effected by $e_p r_q$ in that order.

Let w be a non-empty (reduced) word in the (formal) free product $P_0^+ * T_L$; w is a string of elements (not the identity) alternately from P_0^+ and T_L. Then w may be considered to act on an arbitrary $\alpha \in L$ to produce an element in its algebraic closure $\overline{L}$, although, in general, any action of $e_p r_q$ (with $q > 1$) has to prescribe which qth root is extracted. It was shown by Adeleke, Glass and Morley [1] that w cannot act as the identity on L even if there is complete freedom in the selection of roots. Of course, when $L = \mathbb{R}$, w can be regarded naturally as an element of Sym$(\mathbb{R})$, the group

Received 17th March, 1994
We are most grateful to the National Science Foundation for partial support. The project was begun with support for A.M.W. Glass through the NSF US-UK Program and completed through an NSF grant. The paper was written while S.D. Cohen was a visitor at Bowling Green State University and he gratefully acknowledges support from the NSF and BGSU Graduate College and College of Arts and Sciences.

of bijections of $\mathbb{R}$ into itself, and their theorem implies that the subgroup of $\mathrm{Sym}(\mathbb{R})$ generated by $T_{\mathbb{R}}$ and P_0^+ is isomorphic to the free product $P_0^+ * T_{\mathbb{R}}$.

This result incorporates the pioneering work of White [5] who proved that the subgroup of $\mathrm{Sym}(\mathbb{R})$ generated by $T_{\mathbb{R}}$ and e_p for a fixed odd *prime* p is their free product. Later, Cohen [2], overcame major technical obstacles to probe the analogue of the theorem of Adeleke, Glass and Morley for the free product $P^+ * T_L$, where P^+ is the group of all positive rational powers, that is,

$$P^+ = \{e_p r_q \colon p,\, q \text{ co-prime positive integers}\}.$$

It would be natural to seek to extend the above results to the free products $P_0 * T_L$ and $P * T_L$, where P_0, P are the groups of all odd rational powers (positive and negative) and all non-zero rational powers, respectively, that is,

$$P_0 = \{e_p r_q \colon p,\, q \text{ co-prime odd integers}\},$$
$$P = \{e_p r_q \colon p,\, q \text{ non-zero co-prime integers}\}.$$

For these we adopt the conventions that the action of any element of P on zero is undefined and that two words in $P * T_L$ can be supposed to have the same action on L if they agree whenever both are defined. Whereas, however, the exact set of $a \in \mathbb{C}$ with $|a| < 2$ for which t_a and e_{-1} do *not* generate a free product $\mathbb{Z}*(\mathbb{Z}/2\mathbb{Z})$ is unknown, it is certainly non-empty (see [4]); in particular t_1 and e_{-1} themselves do not generate such a free product because, for example $t_1 e_{-1} t_1^{-1} e_{-1} t_1 e_{-1}$ has order 2, yet is not conjugate to e_{-1}, as can easily be seen. It is therefore pointless to investigate these free products in their entirety. So let $S_0(L)$ be the subset of $P_0 * T_L$ comprising those non-empty words in whose reduced form the power $e_{-1} r_1$ $(= e_1 r_{-1})$ (corresponding to $x \mapsto 1/x$) does not appear and $S(L)$ be the corresponding subset of $P * T_L$. Then $S_0(L)$ and $S(L)$ are closed as regards the taking of inverses. We shall show that no member of $S_0(L)$ has the same action as the identity whenever it is defined. We believe that a similar result prevails for $S(L)$ but have not undertaken the details of a proof. Our dual aim is to present the extended result and to display the nature of the proof which is a considerable refinement of those of [5] and [1] distilled from [2] but freed from the technicalities of [2]. Indeed, the proof given here is far more perspicuous than that of [1].

For w in $S_0(L)$ let $\mathbb{Q}_w$ be the field (finitely) generated over $\mathbb{Q}$ by $\{a \in L \colon t_a$ occurs in the expansion of $w\}$. Evidently, for any α in L, αw is undefined only on a finite subset of $\overline{\mathbb{Q}}_w$, the algebraic closure of $\mathbb{Q}_w$.

Theorem 1. *Let L be a field of characteristic zero and w a word in $S_0(L)$. Then for every α in L not in a certain subset of $L \cap \overline{\mathbb{Q}}_w$, αw is defined and $\alpha w \neq \alpha$, no matter how the roots are extracted at any stage.*

https://doi.org/10.1017/S0004972700013903 Published online by Cambridge University Press

Of course in Theorem 1 we can replace L by its algebraic closure. Further, given w, define $K = \overline{\mathbb{Q}}_w$ which we may assume to be a subfield of $\mathbb{C}$. The bulk of the proof is associated with proving that $\zeta w \neq \zeta$ for any element ζ transcendental over K; we may adjoin ζ to L if necessary. It is then easy to deduce the result for α in K, see Section 6. So until then we suppose ζ is a given transcendental.

In fact we deduce Theorem 1 from a stronger result which is the subject of the next section.

2. Hypothesis H

We use notation and conventions developed from [**5**], [**1**] and [**2**].

Any word w in $S_0(L)$ can be expressed (essentially uniquely) as a string of symbols $w = v_1 \dots v_n$ that allow no cancellation. Here n is the *length* of w. Specifically, each v_j $(1 \leqslant j \leqslant n)$ is either t_a $(a(\neq 0) \in L)$, e_p $(p \in \mathbb{Z}, |p| > 1)$ or r_q $(q \in \mathbb{Z}, |q| > 1)$. In particular, any e_p or r_q with $p = \pm 1$ or $q = \pm 1$ have been absorbed into neighbouring symbols. Moreover, r_q must be followed by a translation (unless it is at the end of w). If $v_1 = t_a$, then w will be called a *translation word.* If a consecutive pair $e_p r_q$ has p/q positive we can assume both p and q are positive whereas, if p/q is negative we permit the (harmless) ambiguity about which of the pair p, q is positive. Given $\zeta = \zeta_1$, we define the *transcendental chain* for w to be $\{\zeta_1, \dots, \zeta_{n+1}\}$, where $\zeta_{j+1} = \zeta_j v_j$, $j = 1, \dots, n$ and, when $v_j = r_q$, some choice of root is made.

There is also a syllable form for w. To this end, call a word f none of whose symbols is a root a *rational word* because ζf is a rational function in $K(\zeta)$. Associated with its action is a rational function $f(x)$ which is either $x + a$ $(a \neq 0)$ or

$$f(x) = (\dots((x + a_1)^{p_1} + a_2)^{p_2} + \dots + a_\ell)^{p_\ell} + a_{\ell+1}\,(\ell \geqslant 1), \tag{2.1}$$

where $|p_j| > 1$, $1 \leqslant j \leqslant \ell$ and $a_j \neq 0$, $2 \leqslant j \leqslant \ell$, though a_1 or $a_{\ell+1}$ may be zero. From this, w has an expression (essentially unique) as $w = s_1 \dots s_k$ $(k \geqslant 1)$, where for each $j = 1, \dots, k-1$, the *syllable* s_j has the shape $s_j = f_j r_{q_j}$, with f_j a rational word that, for $j > 1$, is necessarily a translation word. When $j = k$ there need not be a concluding root r_{q_k} though it is sometimes convenient to interpret q_k as 1 in the latter situation. Associated with the syllable form is the *syllable transcendental chain* $\{\mu_1, \dots, \mu_{k+1}\}$, where

$$\mu_1 = \zeta_1 = \zeta,\ \mu_{j+1} = \mu_j s_j,\ 1 \leqslant j \leqslant k.$$

This is a sub-chain of $\{\zeta_1, \dots, \zeta_{n+1}\}$. In association with either chain we sometimes use notation such as (μ_i, μ_j) $(i < j)$ as shorthand for a sub-word $s_i \dots s_{j-1}$ of w whose action sends μ_i to μ_j.

When $k = 1$ and w is a rational word (represented by (2.1)) we can dispose of Theorem 1 by the following argument. By an easy induction on ℓ, f is a quotient of co-prime polynomials f_1/f_2 with $\max(\deg f_1, \deg f_2) = |p_1 \dots p_\ell|$ and the result is immediate.

When f is not rational word, for each $j = 1, \dots, k+1$, define $K_j = K(\mu_1, \mu_j)$, where each such field is evidently an algebraic extension of K_1. We shall show that, in fact, $K_{k+1} \neq K_1$ and hence $(\zeta_{n+1} = \mu_{k+1} =)\ \zeta w \neq \zeta(= \zeta_1 = \mu_1)$, which implies Theorem 1 for ζ. This assertion is incorporated in the main result we shall prove which we label Hypothesis H for comparison with [**1**] and [**2**]. (Recall that a field F is a pure extension of a field E if $F = E(b^{1/m})$ for some $b \in E$ and positive integer m.)

THEOREM 2. (Hypothesis H) *Let $w = v_1 \dots v_n = s_1 \dots s_k$ be a word in $S_0(L)$ and ζ be transcendental over K. Then*

$H_1 : K(\zeta_1) \subseteq K(\zeta_1, \zeta_2) \subseteq \dots \subseteq K(\zeta_1, \zeta_{n+1})$;

$H_2 : K_1 \subset K_2 \subset \dots \subset K_{k+1}$, *where the inclusions are strict (except the final one if $q_k = 1$).*

H_3: *if F is a pure extension of K_1 contained in K_{n+1}, then $F \subseteq K_2$.*

Note that H_1 implies that $K_1 \subseteq K_2 \subseteq \dots \subseteq K_{k+1}$ and that the substance of H_2 is that generally these containments are strict. We also note the following immediate consequence of Theorem 2 (specifically of H_2).

COROLLARY 3. *For w, ζ as in Theorem 2, $[K_{k+1} : K_1] = |q_1 \dots q_k|$.*

The truth of Theorem 2 for words of length not exceeding n will be labelled $H(n)$ and that of each part $H_j(n)$, $j = 1, 2, 3$, as appropriate. $H(n)$ is established by induction on n. $H(1)$ is simple and the induction step proceeds in stages according to the scheme

$$H(n) \Rightarrow H_1(n+1) \Rightarrow H_2(n+1) \Rightarrow H_3(n+1).$$

Since we shall always assume $H(n)$ and be investigating $H(n+1)$, throughout we shall suppose that $\omega = v_1 \dots v_{n+1}$ (with associated transcendental chain $\{\zeta_1, \dots, \zeta_{n+2}\}$). Nevertheless we shall continue to suppose $w = s_1 \dots s_k$ has k syllables and use the notation of this section. The theorem is easy if $k = 1$ so we assume $k \geqslant 2$.

We observe that induction always takes care (easily) of words that begin or end with a translation so we may assume this is not the case. Moreover, as far as Theorem 2 is concerned, we may replace ζ_1 by ζ_1^{-1} and/or ζ_{n+2} by ζ_{n+2}^{-1}, if necessary, and assume that w begins and ends with a positive power e_p $(p > 1)$ or positive root r_q $(q > 1)$.

3. Proof of $H_1(n+1)$

By $H_1(n)$ (applied to $v_1 \dots v_n$ and $v_2 \dots v_{n+1}$)

$$K(\zeta_1) \subsetneq K(\zeta_1, \zeta_2) \subsetneq \dots \subsetneq K(\zeta_1, \zeta_{n+1}) \tag{3.1}$$

and

$$K(\zeta_2) \subsetneq K(\zeta_2, \zeta_3) \subsetneq \dots \subsetneq K(\zeta_2, \zeta_{n+2}). \tag{3.2}$$

Suppose, however, that $K(\zeta_1, \zeta_{n+2})$ does not contain $K(\zeta_1, \zeta_{n+1})$. Then obviously v_{n+1} is a power (and s_k does not end in a root). Trivially, $\zeta_{n+2} = \zeta_{n+1}v_{n+1} \in K(\zeta_{n+1})$ and hence $K(\zeta_1, \zeta_{n+2})$ is strictly contained in $K(\zeta_1, \zeta_{n+1})$. Further, v_1 is a root because otherwise $\zeta_2 \in K(\zeta_1)$ and the inconsistent conclusion $K(\zeta_1, \zeta_{n+1}) \subsetneq K(\zeta_1, \zeta_{n+2})$ is a consequence of adjoining ζ_1 to the final two fields in the chain (3.2). Moreover, we may also assume that $K(\zeta_1, \zeta_{n+2}) \cap K(\zeta_1, \zeta_2) = K(\zeta_1)$; for this purpose, if $v_1 = r_q$ $(q > 1)$ it may be necessary to replace ζ_1 $(= \zeta_2^q)$ by ζ_2^m, where m $(\neq q)$ is a positive divisor of q, and v_1 by $r_{q/m}$. Since $\zeta_{n+2} \in K(\zeta_{n+1})$ and $\zeta_1 \in K(\zeta_2)$ we deduce that

$$K(\zeta_1, \zeta_{n+1}) = K(\zeta_2, \zeta_{n+2}) = K(\zeta_2, \zeta_{n+1}), \tag{3.3}$$

this field strictly containing $K(\zeta_1, \zeta_{n+2})$.

In terms of syllables, (3.1)–(3.3) yield the following (for which we note that $\mu_1 = \zeta_1 = \mu_2^q$):

$$K(\mu_1, \mu_k) = K(\mu_2, \mu_{k+1}) = K(\mu_2, \mu_k), \tag{3.4}$$

a field which strictly contains $K_{k+1} = K(\mu_1, \mu_{k+1})$. Moreover, $K_{k+1} \cap K_2 = K_1$ and $K_k = K_{k+1}(\mu_2)$ is a pure extension of K_{k+1} of degree q.

Suppose that $k = 2$. Then $w = r_q f$, where f is a rational translation word. From the above, $K_3 \cap K_2 = K_1$ so that $\mu_3 = f(\mu_2) \in K(\mu_1) = K(\mu_2^q)$. Hence, identically

$$f(x) = g(x^q) \tag{3.5}$$

for some rational function g. This is easily seen to be impossible since f is a translation word: in any case it is covered by Lemma 4 below.

Suppose therefore that $k > 2$. Now K_k/K_{k+1} is a cyclic Galois extension of degree q (since K, being algebraically closed, contains all qth roots of unity). We apply to K_k a generating automorphism τ of its Galois group. Thus τ fixes K_{k+1} (element-wise) and sends μ_2 to $\omega\mu_2$, where ω is a primitive qth root of unity. Set

$\overline{\mu}_3 = \tau(\mu_3) \in K_k$ and let the second syllable s_2 be $f r_d$. An application of τ to the expression $\mu_3 = f(\mu_2)$ yields $\overline{\mu}_3^d = f(\omega\mu_2)$. Both $K_3 = K(\mu_2, \mu_3)$ and $K(\mu_2, \overline{\mu}_3)$ are pure extensions of $K_2 = K(\mu_2)$ of degree d contained in K_k and so, by $H_3(n)$ applied to the word (μ_2, μ_k), we deduce that these two fields are identical. From the basic result on pure extensions (see Exercise 16.16 of [3]) it follows that for some t (prime to d) $\mu_3\overline{\mu}_3^t \in K(\mu_2)$. Hence, taking dth powers and, setting $x = \mu_2$, we have

$$f(x)f^t(\omega x) = h^d(x), \tag{3.6}$$

identically for some rational function $h(x)$. Evidently, (3.6) is impossible when $f(x) = x + a$. For other cases it is timely to introduce a lemma adapted from [5], [1] and [2]. It disposes immediately of (3.5) and (3.6) and plays a similar role in the verification of H_2 and H_3. For other cases it is timely to introduce a lemma adapted from [5], [1] and [2].

Lemma 4. *Suppose that p, q, d are odd integers of absolute value exceeding 1 and ω $(\neq 1)$ is a qth root of unity. Suppose also that f, g, h are rational functions in $K(x)$ with $f(x) = f_0((x+a)^p)$, $a \neq 0$, $f \neq f_1^d$. Then, for no integer t is there an identity of the form*

$$f(x)f^t(\omega x)g(x^q) = h^d(x). \tag{3.7}$$

Proof: Easily we may assume that p, q and d are positive. Assuming (3.7), we may multiply it by $\left(f_2(x)f_2^t(\omega x)q_2(x^q)\right)^d$, where f_2 and g_2 are the denominators of f and g, respectively, and obtain an analogous identity with f and g replaced by *polynomials* $f_2^d f$ and $g_2^d g$, respectively in which case the "new" h is also a polynomial. The result is then immediate from Lemma 10 of [1] or Lemma 9.1 of [2]. □

4. Proof of $H_2(n+1)$

We can now assume $H_1(n+1)$ in addition to $H(n)$. By $H_2(n)$, it remains to prove that $K_k \subset K_{k+1}$ when s_k ends in r_q $(q \geqslant 3)$. Assume that $K_k = K_{k+1}$. This is unaffected when q is replaced by a prime divisor d. If $\mu_{k+1} \in K(\zeta_2, \mu_k)$, then $K(\zeta_2, \mu_k) = K(\zeta_2, \mu_{k+1})$ contradicting $H_2(n)$ applied to (ζ_2, ζ_{n+2}). Hence $\mu_{k+1} \notin K(\zeta_2, \mu_k)$ and, in particular, w must begin with a power, $v_1 = e_p$ $(p \geqslant 3)$, say.

Now, by assumption and $H_1(n+1)$,

$$\begin{aligned} K(\zeta_2, \mu_k)(\mu_{k+1}) &= K(\zeta_2, \mu_{k+1}) \\ &\subseteq K(\zeta_1, \mu_{k+1}) = K(\zeta_1, \mu_k) = K(\zeta_2, \mu_k)(\zeta_1). \end{aligned} \tag{4.1}$$

From (4.1) the field $K(\zeta_2, \mu_{k+1})$ intermediate between $K(\zeta_2, \mu_k)$ and $K(\zeta_1, \mu_k)$ has the form $K(\zeta_1^s, \mu_k)$ for some proper divisor s of p. Since $d = [K(\zeta_2, \mu_{k+1})\colon K(\zeta_2, \mu_k)]$, we have $p = sd$. By replacing v_1 by $e_{p/s}$ we can assume $p = d$. Summarising, $\zeta_1 \notin K(\zeta_2, \mu_k)$, yet

$$K(\zeta_2, \mu_{k+1}) = K(\zeta_1, \mu_k) = K(\mu_1, \mu_{k+1}). \tag{4.2}$$

For an analysis of (4.2) write

$$w = \ldots e_m g^{-1} r_q f r_d, \tag{4.3}$$

where only the latter section of w is displayed and f and g are rational translation words with g^{-1} denoting the inverse of g. Also let $u = (s_1 \ldots s_{k-1})^{-1} = (\mu_k, \zeta_1)$ have $\{\nu_1 = \mu_k, \nu_2, \ldots\}$ as its associated syllable transcendental chain and put $F = K(\mu_k, \mu_{k+1})$. Since $\mu_{k+1}^d = f(\mu_k)$, F is a pure extension of $K(\nu_1)$ $(= K(\mu_k))$ of prime degree d contained in $K(\mu_k, \zeta_1)$ but not $K(\mu_k, \zeta_2)$. Apply $H_3(n)$ to the word u with respect to $K(\nu_1) \subseteq F \subseteq K(\mu_k, \zeta_1)$. Then $F \subseteq K(\nu_1, \nu_2)$. Unless u is a monosyllable, by $H_1(n)$ applied to u, $K(\nu_1, \nu_2) \subseteq K(\nu_1, \zeta_2) = K(\mu_k, \zeta_2)$ which yields the contradiction $\mu_{k+1} \in K(\zeta_2, \mu_k)$. Thus u is indeed monosyllabic with $K(\mu_k)(\zeta_1) = K(\mu_k)(\mu_{k+1}) = F$ and, necessarily, $m = d$ and

$$w = e_d g^{-1} r_q f r_d. \tag{4.4}$$

Hence, for some t (prime to d), $\mu_{k+1}\mu_1^t \in K(\mu_k)$. Raising this to the dth power and setting $x = \mu_k$ we obtain from (4.4)

$$f(x) g^t(x^q) = h^d(x)$$

for some rational function h. This contradicts Lemma 4. □

We remark that now that $H_2(n+1)$ has been established we may use Corollary 3.

5. Proof of $H_3(n+1)$

We may assume $H_1(n+1)$, $H_2(n+1)$, $H_3(n)$ and Corollary 3.

Let F be a pure extension of K_1 contained in K_{k+1} but not in K_2. By $H_3(n)$ we can suppose s_k ends in a root r_q $(q > 1)$. To obtain a contradiction, it suffices to suppose that $F/(K_2 \cap F)$ is a pure extension of *prime* degree d. Again by $H_3(n)$ we can suppose that $F \nsubseteq K_k$. Hence $F(\mu_k)$ $(= F_1$, say), which clearly contains K_k, must be a pure extension of K_k of degree d contained in K_{k+1}. By Corollary 3 we may replace the final root r_q of w by r_d and assume that $F_1 = K_{k+1}$.

Again write w as (4.3) (where q has a new meaning). When $k \geqslant 3$ let F_0 be the subfield $F(\mu_{k-1})$ of F_1. When $k = 2$, defer the possibility

$$K_1 \subset K_2 \subset F = F_1 = K_3 \tag{5.1}$$

https://doi.org/10.1017/S0004972700013903 Published online by Cambridge University Press

meantime, and otherwise set $F_0 = F$. Then F_0 contains K_{k-1}, yet F_0/K_{k-1} ($F_0/(K_2 \cap F_0)$ when $k = 2$) must be an extension of degree d. By Corollary 3, $[K_{k+1} : K_{k-1}] = qd$ and so $F_0 \neq F_1$, whereas $F_0(\mu_k) = K_{k+1}$; in particular, K_{k+1}/F_0 is a pure extension of degree dividing q. Hence there is an F_0-automorphism τ of K_{k+1} which maps $\mu_k \mapsto \omega\mu_k$, where ω ($\neq 1$) is a qth root of unity. Moreover, if $k = 2$ and (5.1) holds, then K_3/K_1 is a cyclic extension of degree dq and there is a K_1-automorphism τ of K_3 with a similar property. Set $\overline{\mu}_{k+1} = \tau(\mu_{k+1}) \in K_{k+1}$. Then, in either case, clearly $K_k(\overline{\mu}_{k+1}) = K_k(\mu_{k+1})$ ($= K_{k+1}$), whence $\mu_{k+1}\overline{\mu}_{k+1}^t \in K_k$ for some integer t (indivisible by d). Further, $K(\mu_k, \mu_{k+1}\overline{\mu}_{k+1}^t) \subseteq K(\mu_k, \mu_1)$ yet

$$\left(\mu_{k+1}\overline{\mu}_{k+1}^t\right)^d = f(\mu_k)f^t(\mu_k) \in K(\mu_k).$$

As in Section 4 (following (4.3)), by applying $H_3(n)$ to $u = (s_1 \ldots s_{k-1})^{-1}$ with syllable transcendental chain $\{\mu_k = \nu, \nu_2, \ldots\}$ we deduce that $\mu_{k+1}\overline{\mu}_{k+1}^t \in K(\nu_1, \nu_2) = K(\mu_k)(\nu_2)$. Hence $d \mid m$ and, for some integer u, divisible by m/d,

$$\mu_{k+1}\overline{\mu}_{k+1}^t\nu_2^u \in K(\mu_k).$$

Taking dth powers and replacing μ_k by x yields

$$f(x)f^t(\omega x)g^u(x^q) = h^d(x),$$

for some rational function h. This contradicts Lemma 4. ∎

The proof of Theorem 2 is complete.

6. Completion of the proof of Theorem 1

With w, ζ as in Theorem 2 and Corollary 3 we can explicitly construct $P(z, y)$, a monic irreducible polynomial in z of degree $|q_1 \ldots q_k|$ with coefficients in $K(y)$ such that $P(\mu_{k+1}, \mu_1)$ ($= P(\zeta w, \zeta)) = 0$. The same P is obtained no matter how we extract roots when we consider the action of w.

Set $P_{k+1}(z, y) = z - y$ and define $P_j(z, y)$, $j = k, \ldots, 1$, as follows:

$$\text{let } P_j(z, \mu_j) = \prod_{i=0}^{Q_j - 1} P_{j+1}(z, \omega_{j+1}^i \mu_{j+1}), \qquad j = k, \ldots, 1,$$

where $Q_j = |q_j|$ and ω_{j+1} is a primitive Q_jth root of unity. Then $P_j(z, \mu_j)$ is a polynomial in z whose coefficients are rational functions in $K(\mu_j) \subseteq K(\zeta, \mu_j)$ with μ_j transcendental over K. To obtain $P_j(z, y)$ simply replace these coefficients by the corresponding rational functions in an indeterminate y (transcendental over $K(z)$). Put $P(z, y) = P_1(z, y)$ and our claim is justified (by Corollary 3).

It follows that $P(z, \zeta)$ certainly cannot have $z - \zeta$ as a factor. Specialising $\zeta \to \alpha \in K$ we conclude that $P(z, \alpha)$ is undefined or has a factor $a - \alpha$ for only finitely many values of α. For all other values of α in K, $P(\alpha, \alpha) \neq 0$ and so $\alpha w \neq \alpha$. This completes the proof. ∎

References

[1] S.A. Adeleke, A.M.W. Glass and L. Morley, 'Arithmetic permutations', *J. London Math. Soc.* **43** (1991), 255–268.

[2] S.D. Cohen, 'The group of translations and positive rational powers is free', *Quart. J. Math. Oxford* (to appear).

[3] D.J.H. Garling, *A course in Galois theory* (Cambridge University Press, Cambridge, 1986).

[4] R.C. Lyndon and J.L. Ullman, 'Groups generated by two parabolic linear fractional transformations', *Canad. J. Math.* **21** (1969), 1388–1403.

[5] S. White, 'The group generated by $x \mapsto x+1$ and $x \mapsto x^p$ is free', *J. Algebra* **118** (1988), 408–422.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW
Scotland

Department of Mathematics and Statistics
Bowling Green State University
Bowling Green OH 43403-0221
United States of America