FREE GROUPS FROM FIELDS

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

This paper is dedicated to Brian Hartley, in memoriam

1. *Introduction*

In the nineteenth century, field theory brilliantly resolved a number of questions that had taxed mathematicians for centuries; for example, 'The circle cannot be squared' by straight edge and compass, and solving polynomial equations by radicals is not always possible. These successes have continued to be held up as superb examples of the power of mathematical thought, and are demonstrated at an undergraduate level. The purpose of this article is to provide another such *natural* example which leads to a concrete realisation of the free group on 2 generators.

Let p be any odd prime number. Consider the permutations $t_1: x \mapsto x+1$ and $e = e(p): x \mapsto x^p$ of the set of real numbers. In 1986, Samuel White [**7**] proved that if $a_1, \ldots, a_n, k_1, \ldots, k_n$ are arbitrary integers (positive or negative) with $a_2, \ldots, a_n, k_1, \ldots, k_{n-1}$ non-zero, then the map $t_1^{a_1} e^{k_1} \ldots t_1^{a_n} e^{k_n}$ is not the identity map; that is, there is a real number ζ such that

$$((\ldots(\zeta + a_1)^{q_1} + a_2)^{q_2} + \ldots + a_{n-1})^{q_{n-1}} + a_n)^{q_n} \tag{1}$$

is not ζ, where $q_j = p^{k_j}$ (for $j = 1, \ldots, n$). In other words, the subgroup G_p of the symmetric group on $\mathbb{R}$ (the set of real numbers) generated by t_1 and $e(p)$ is *free*; there is no interrelation between t_1 and $e(p)$. Of course, t_1^{-m} is the map $x \mapsto x - m$ and e^{-m} is the map $x \mapsto \sqrt[p^m]{x} = x^{1/p^m}$ (the root in $\mathbb{R}$ being indeed unique).

As a result of some of our recent work, we can now provide a more transparent proof of White's Theorem that requires only background well below that of the full Galois correspondence. We hope that White's Theorem is sufficiently intriguing and the proof we give sufficiently elementary that it will be of interest to a large audience; we have made our explanation sufficiently leisurely to try to ensure this. It could also serve as an introduction to the more elaborate applications of the basic method (see [**2**, **3**, **4**]).

Caution. Although the proof uses 'elementary' ideas and is simpler than White's original one, it is not trivial and involves proving three facts simultaneously by induction (each step requiring a key idea following initial preparations).

2. *Pure extensions*

Let $q = p^m$ be a power of an odd prime p. Also, let E be a subfield of $\mathbb{R}$ and, for $a \in E$, let $\alpha = \sqrt[q]{a} = a^{1/q}$ be the real qth root of a. 'Adjoin' α to E to form the *pure extension* field $F = E(a^{1/q}) = \{\sum_{i=0}^{q-1} \varepsilon_i \alpha^i : \varepsilon_i \in E\}$. If, in fact, a is not the pth power of an

Received 3 November 1994; revised 2 October 1995.

1991 *Mathematics Subject Classification* 20E05.

J. London Math. Soc. (2) 55 (1997) 309–319

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

element in E (that is, $a^{1/p} \notin E$), then the extension F of E is a vector space over E with basis $\{1, \alpha, \ldots, \alpha^{q-1}\}$ and so has degree q. In this case the set of fields intermediate between E and F form a 'tower'

$$E \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_m = F,$$

where $F_i = E(a^{1/p^i})$ for $i = 1, \ldots, m$; each is a pure extension of the previous one of degree p.

Now, clearly, if $b \in E$ is closely related to a by $b = a^t c^q$, where $c \in E$ and $p \nmid t$, then $E(b^{1/q}) = E(a^{t/q}) = E(a^{1/q})$. Conversely, if a and b are elements of E such that $E(a^{1/q}) = E(b^{1/q})$, where $a^{1/p} \notin E$, then $ab^t = c^q$ for some positive integer t (indivisible by p) and $c \in E$.

The above facts are all plausible but not exactly trivial to establish. Some can be derived from results in textbooks (such as the recent one by S. Roman [**6**]) but we present some non-standard parts as Lemmas A and B in an Appendix. Of course, such facts are not restricted to real fields: one can easily consider a pure extension $F = E(a^{1/q})$ of a subfield E of the complex numbers $\mathbb{C}$, where $a \in E$ and $\alpha = a^{1/q}$ has the property that $\alpha^q = a$, though, in general, α is not uniquely defined. In such a case, if E contains a qth root of unity ω ($\neq 1$), we can define an automorphism τ of F (that is, a mapping from F onto itself that is both an additive and a multiplicative isomorphism) such that $\tau(\alpha) = \omega\alpha$ by $\tau(\sum_{i=1}^{q-1} \varepsilon_i \alpha^i) = \sum_{i=0}^{q-1} \varepsilon_i (\omega\alpha)^i$. Indeed τ is an *E-automorphism of F*: it fixes each member of E.

3. *A transcendental chain*

Suppose that p is a fixed odd prime and that we are given a non-empty word w of G_p. When $xw = x + a$ everything is easy; so we may suppose that the bijection w is described by (1), where now each q_j is a power (positive or negative) of p. We want to show that w does not act like the identity on $\mathbb{R}$. To do this, let η be any real transcendental number. We shall prove that $\eta w \neq \eta$. Indeed, take the *orbit* $S(\eta)$ of η under G_p, that is, the subset $S(\eta) = \{\eta w^* : w^* \in G_p\}$ of $\mathbb{R}$. We shall prove that $\zeta w \neq \zeta$ for every $\zeta \in S(\eta)$.

Consider the field $\mathbb{Q}(\eta)$ of rational functions in η with rational coefficients. Let L be its algebraic closure – so L comprises all roots of polynomials with coefficients in $\mathbb{Q}(\eta)$: it is a subfield of $\mathbb{C}$. Of course, L contains, as a subfield, the field K of all algebraic numbers – these comprising all roots of polynomials with rational coefficients. Then set $L_0 = L \cap \mathbb{R}$, the field of *real* numbers algebraic over $\mathbb{Q}(\eta)$, and $K_0 = K \cap \mathbb{R}$, the field of all real algebraic numbers. (Of course, we can recover L and K by adjoining $\mathrm{i} = \sqrt{(-1)}$ to L_0 and K_0, respectively; see Lemma C of the Appendix.) Clearly, a property of L_0 is that every member has a uniquely defined pth root (and, for that matter, p^mth root, for any $m \geqslant 1$) in L_0. Passing to L (which contains every p^mth root of unity), we obtain a field which contains *all* p^mth roots of every member.

Now, for our specific word w and transcendental η, let ζ be any member of $S(\eta)$. We prepare to define a sequence of transcendentals (in $S(\eta)$) which begins with ζ and ends with ζw. For this purpose, let us denote a *power map* $x \mapsto x^{p^m}$ (for $m \geqslant 1$) by e_m and a *root map* $x \mapsto x^{1/p^m}$ (for $m \geqslant 1$) by r_m. And, for any integer a, we denote the *translation* $x \mapsto x + a$ by t_a. Then w can be expressed as a string of symbols $w = v_1 \ldots v_n$, where the v_i alternate between a translation t_a (with $a \neq 0$) and *either* a power e_m (for $m \geqslant 1$) *or* a root r_m (for $m \geqslant 1$). (Here n is the *length* of w.) Then set $\zeta_1 = \zeta$ and $\zeta_{j+1} = \zeta_j v_j$ for $j = 1, \ldots, n$; in particular, $\zeta_{n+1} = \zeta w$.

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

We shall consider the sequence of fields $K_0(\zeta_1), K_0(\zeta_1, \zeta_2), \ldots, K_0(\zeta_1, \zeta_{n+1})$, where, by $K_0(\zeta_1, \zeta_j)$, we mean that both ζ_1 and ζ_j have been adjoined to K_0, or, equivalently, that ζ_j has been adjoined to the simple transcendental extension $K_0(\zeta_1)$ to yield an algebraic extension (a subfield of L_0). Now, there is no immediate reason why this sequence *must* form a tower

$$K_0(\zeta_1) \subseteq K_0(\zeta_1, \zeta_2) \subseteq \ldots \subseteq K_0(\zeta_1, \zeta_{n+1}). \tag{2}$$

Indeed, if $v_j = e_m$, a power, then $\zeta_{j+1} = \zeta_j^{p^m}$, so that $K_0(\zeta_1, \zeta_{j+1}) \subseteq K_0(\zeta_1, \zeta_j)$; and it is not at all obvious that these two fields are identical – but this is what the truth of (2) would demand.

Suppose that we could prove that (2) holds. We claim that it would follow that $\zeta w \neq \zeta$. For, if there are no roots amongst $v_1, \ldots, v_n$, then (1) is merely a polynomial over $\mathbb{Q}$ and then '$w(\zeta) = \zeta$' really is nonsense – remember, ζ is transcendental. So suppose that the first root is $v_j = r_m$. Then $\zeta_j \in K_0(\zeta_1)$ and $K_0(\zeta_1, \zeta_{j+1}) = K_0(\zeta_1)(\zeta_j^{1/p^m})$ and clearly $\zeta_j^{1/p} \notin K_0(\zeta_1)$. Thus $K_0(\zeta_1, \zeta_{j+1})$ is a pure extension of $K_0(\zeta_1)$ of degree p^m and so, certainly, strictly contains the latter field. Then (2) would imply that $K_0(\zeta_1) \subset K_0(\zeta_1, \zeta_{n+1})$ (strictly). But, of course, if $\zeta_{n+1} = \zeta_1$, then $K_0(\zeta_1, \zeta_{n+1}) = K_0(\zeta_1)$, contrary to the above, and our claim is justified.

We shall use standard field theory to prove (2). Unfortunately, we cannot do this in isolation but only as part of a package of three results. Moreover, instead of (2) itself, we shall build the corresponding tower with i adjoined to each field (that is, with K_0 replaced by K). It will serve the same purpose.

4. *A subchain*

Instead of regarding w as a string of symbols $v_1 \ldots v_n$, we shall gather these into syllables $s_1, \ldots, s_k$ each of which ends in a root r_{m_i}. Call a word f a *polynomial word* if $f = t_a$ or is given by (1) with each q_i a *positive power* of p: thus $f(x)$ is, indeed, a polynomial. Then we can write $w = s_1 \ldots s_k$, where $s_j = f_j r_{m_j}$, and f_j is a polynomial word. Here, generally, (with reference to (1)) all the integers a in f_j are non-zero but $f_1(x)$ *may* be x or have $a_1 = 0$. Similarly, there may be no root at the end of s_k and, additionally, the final a may be zero: in these cases, by convention, set $m_k = 0$. Now define a subchain $\{\mu_1, \ldots, \mu_{k+1}\}$ of $\{\zeta_1, \ldots, \zeta_{n+1}\}$ by $\mu_1 = \zeta_1 = \zeta$, $\mu_{j+1} = \mu_j s_j$, for $1 \leqslant j \leqslant k$. Then $\mu_{k+1} = \zeta_{n+1} = \zeta w$.

Note that, granted (2), we would have the following tower:

$$K_0(\mu_1) \subseteq K_0(\mu_1, \mu_2) \subseteq \ldots \subseteq K_0(\mu_1, \mu_{k+1}).$$

We saw already that the first containment must be strict: the second item in our package is that all are strict, that is,

$$K_0(\mu_1) \subset K_0(\mu_1, \mu_2) \subset \ldots \subset K_0(\mu_1, \mu_{k+1}) \tag{3}$$

(with the exception of the last of these if $m_k = 0$).

For the third item of our package, observe that, since $\mu_2^{p^{m_1}} = f_1(\mu_1)$, then $K_0(\mu_1)((f_1(\mu_1))^{1/p})$ is a pure extension of $K_0(\mu_1)$ of degree p contained in $K_0(\mu_1, \mu_2)$ and so in $K_0(\mu_1, \mu_{k+1})$ (assuming (3)). Can there be *another* pure extension F of $K_0(\mu_1)$ of degree p contained in $K_0(\mu_1, \mu_{k+1})$? The answer (remarkably, we would again suggest) is 'No'. And, for this one, it is important that we replace K_0 by K and allow F to be a pure extension of degree p of $K(\mu_1)$ (other than $K(\mu_1)((f_1(\mu_1))^{1/p})$) contained in $K(\mu_1, \mu_{k+1})$. The answer is still negative.

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

5. *The results*

The three items of our package will be labelled 'Hypothesis H'; they represent a hypothesis that will be proved inductively on the length n of the word w. As we have hinted already, we adjoin i to all the fields and work with K instead of K_0. We denote each field $K(\mu_1, \mu_j)$ by K_j. The theorem is stated for a general transcendental ζ but in the proof we need consider only those ζ in our special orbit $S(\eta)$.

THEOREM 1 (Hypothesis H). *Let $w = v_1 \dots v_n = s_1 \dots s_k$ be a word in G_p and ζ a real transcendental number. Then*

H_1: $K(\zeta_1) \subseteq K(\zeta_1, \zeta_2) \subseteq \dots \subseteq K(\zeta_1, \zeta_{n+1})$;
H_2: $K_1 \subset K_2 \subset \dots \subset K_{k+1}$ (*omitting the last of these if $m_k = 0$*);
H_3: *if F is a pure extension of K_1 of degree p contained in K_{k+1}, then $F \subseteq K_2$.*

COROLLARY 2. *With $m_1, \dots, m_k$ as in Section* 4, *the degree of the extension K_{k+1} of K_1 is p^m, where $m = m_1 + m_2 + \dots + m_k$.*

The reader will easily check that Corollary 2 follows from Theorem 1.

COROLLARY 3 (White's Theorem [7]). *The group G_p is a free group of rank* 2.

Denote by $H(n)$ the truth of Hypothesis H for words of length not exceeding n. It is straightforward to check $H(1)$ and, *for polynomial words*, to check $H(n)$. Hence we can suppose that $k \geqslant 2$. We shall deduce $H(n+1)$ from $H(n)$ according to the scheme:

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

Since $H(n+1)$ has to be tested we shall suppose that $w = v_1 \dots v_{n+1}$ (with corresponding transcendental chain $\{\zeta_1, \dots, \zeta_{n+2}\}$) but retain k for the number of syllables: thus $w = s_1 \dots s_k$ (with $k \geqslant 2$).

Another point: if w begins or ends with a translation, induction will easily yield $H(n+1)$ from $H(n)$ (since, trivially, $K(\zeta_1, \zeta_{n+1}) = K(\zeta_1 + a, \zeta_{n+1})$ and $K(\zeta_1, \zeta_{n+1} + a) = K(\zeta_1, \zeta_{n+1})$). Similarly, in the course of a proof, it sometimes simplifies the discussion to make certain small adjustments (such as replacing ζ_1 by $\zeta_1^{p^s}$) that can be justified by induction or some simple reason. Our intention is to explain all but the simplest adjustments.

Because, however, the induction depends crucially on a lemma about word polynomials, we break off to introduce it. The reader may simply wish to note Lemma 5, and then skip to Section 7 and the induction proof before returning to Section 6.

6. *Polynomial lemmas*

Let f be a polynomial word given by (1) with every q a positive power of p and every a non-zero. Then f need not be square-free, that is, it may have roots (in K) of multiplicity exceeding 1. For example, if

$$f(x) = ((x+a)^p + b)^p - b^p \quad \text{with } ab \neq 0,$$

then $x+a$ is a factor of multiplicity p: all other roots have multiplicity 1. More generally, regard f as $f_{\ell+1}$ in a sequence of polynomial words $f_1, \dots, f_{\ell+1}$ built up from

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

(1) (in an obvious way), with $f_1(x) = x + a_1$. Differentiating, $f' = \prod_{i=1}^{\ell} q_i f_i^{q_i - 1}$, from which it follows that any root of f of multiplicity exceeding 1 is also a root of one (or more) of $f_1, \ldots, f_\ell$. In fact, if $\alpha \in K$ is a root, precisely, of $f_{i_1}, \ldots, f_{i_s}$ (with $i_1 < i_2 < \ldots < i_s \leqslant \ell$) as well as of f, then one obtains $q_{i_1} \ldots q_{i_s}$ as the multiplicity of α as a root of f. All we need is the following consequence.

LEMMA 4. *The multiplicity of a repeated root of a word polynomial is a power of p.*

We now prove the key lemma for Hypothesis H.

LEMMA 5. *Let f be a word polynomial (with $a_1 \ldots a_{\ell+1} \neq 0$) and ω ($\neq 1$) be a pth root of unity (in K). Then an identity of the form*

$$f(x) f^t(\omega x)\, g(x^p) = h^p(x), \tag{4}$$

where t is an integer and g and h are polynomials (or even rational functions) in $K(x)$, is impossible.

Proof. If (4) holds we can clearly suppose that $0 \leqslant t \leqslant p-1$ (absorb the $f^p(\omega x)$ factors into $h^p(x)$) and

$$f(x) f^t(\omega x) = g(x^p)\, h^p(x), \tag{5}$$

where g and h are polynomials.

Suppose that α is a root of f of multiplicity 1. Then any root of $(x + a_1)^{q_1} - (\alpha + a_1)^{q_1}$ is also a root of f of multiplicity 1. Thus, if $f^*(x)$ is the product of all factors $x - \alpha$ (for α in K) of multiplicity 1, then $f^*(x) = f_0((x + a_1)^{q_1})$ for some polynomial f_0.

Suppose first that $t = 0$. Then, by Lemma 4, for some polynomial g_0,

$$f^*(x) = f_0((x + a_1)^{q_1}) = g_0(x^p). \tag{6}$$

But, if $N = \deg f^*$, it is evident that the left side of (6) has a non-zero term in x^{N-1} and the right side does not. So we may assume that $1 \leqslant t \leqslant p-1$.

In that case, again by Lemma 4, (5) must hold with f replaced by f^*. Let α be a root of f^* and suppose, for each $i = 0, \ldots, p-1$, that $\omega^i \alpha$ has multiplicity m_i as a root of f^*. Then each $m_i = 0$ or 1 and $m_0 = 1$. Moreover, $\omega^i \alpha$ has multiplicity m_{i-1} as a root of $f(\omega x)$ (or m_{p-1} when $i = 0$). Since each $\omega^i \alpha$ has the same multiplicity as a root of $g(x^p)$, we deduce from (5) that, modulo p, we have

$$m_0 + t m_{p-1} \equiv m_1 + t m_0 \equiv \ldots \equiv m_{p-1} + t m_{p-2}.$$

Adding these we conclude that either $m_0 + \ldots + m_{p-1} \equiv 0 \pmod p$ or $t \equiv -1 \pmod p$ (that is, $t = p-1$). But either of these imply that all the $m_i = 1$ and so $f^*(x) = g_0(x^p)$ as at (6), which we already know to be impossible.

7. *Proof of* $H_1(n+1)$

We assume the discussion of Section 5 using the notation of that and earlier sections. We assume $H(n)$. One further convention, whose usefulness will be apparent immediately, is to employ notation such as (ζ_i, ζ_j) for the subword $v_i \ldots v_{j-1}$ of w whose action sends ζ_i to ζ_j. We make a number of (apparently) insignificant initial observations and adjustments.

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

By $H_1(n)$ (applied to (ζ_1, ζ_{n+1}) and (ζ_2, ζ_{n+2})), we have

$$K(\zeta_1) \subseteq K(\zeta_1, \zeta_2) \subseteq \ldots \subseteq K(\zeta_1, \zeta_{n+1}), \tag{7}$$

$$K(\zeta_2) \subseteq K(\zeta_2, \zeta_3) \subseteq \ldots \subseteq K(\zeta_2, \zeta_{n+2}). \tag{8}$$

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 $m_k = 0$. 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 r_m because, otherwise, $\zeta_2 \in K(\zeta_1)$ and the inconsistent conclusion $K(\zeta_1, \zeta_{n+1}) \subseteq K(\zeta_1, \zeta_{n+2})$ is a consequence of adjoining ζ_1 to the final two fields in the tower (8). An adjustment (replacing $\zeta_1 = \zeta_2^{p^m}$ by $\zeta_2^{p^s}$, where $1 \leqslant s \leqslant m$, and replacing s by m) allows us to suppose that $K(\zeta_1, \zeta_{n+2}) \cap K(\zeta_1, \zeta_2) = K(\zeta_1)$. Since $\zeta_{n+2} \in K(\zeta_{n+1})$ and $\zeta_1 \in K(\zeta_2)$, we deduce from (7) and (8) that $K(\zeta_1, \zeta_{n+1}) = K(\zeta_2, \zeta_{n+2}) = K(\zeta_2, \zeta_{n+1})$, this field strictly containing $K(\zeta_1, \zeta_{n+2})$.

In terms of syllables the above yields the following (for which we note that $\mu_1 = \zeta_1 = \mu_2^q, q = p^m$):

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

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}. Since $\mu_1 \in K(\mu_2)$ and $\mu_2 \in K_j$ (for $j = 2, \ldots, k$) by (7), it follows that $K_j = K(\mu_2, \mu_j)$ for $2 \leqslant j \leqslant k$. Thus, by an adjustment, K_k can be assumed to be of degree q over K_{k+1}.

The situation is represented in Figure 1.

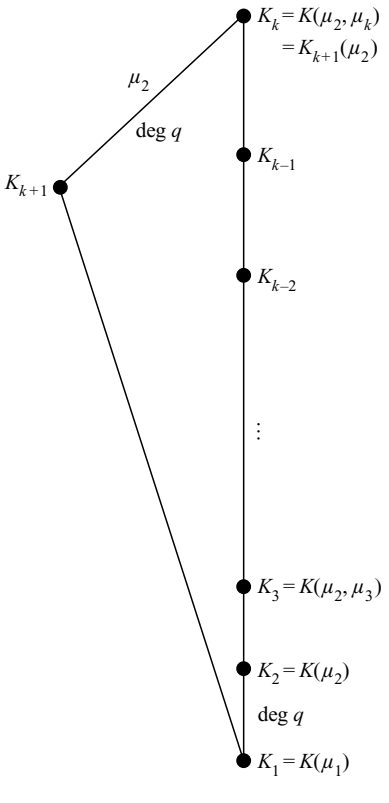


Fig. 1

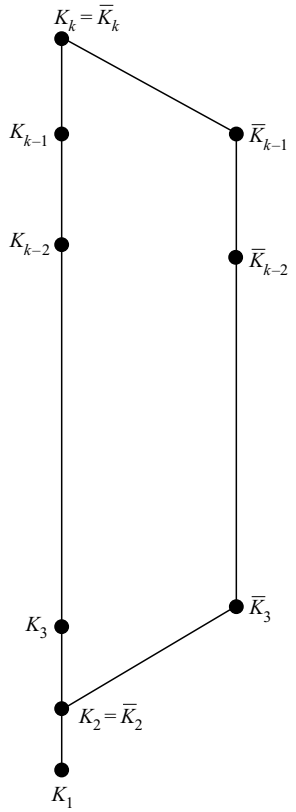


Fig. 2

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

Suppose that $k \geqslant 3$. We see that K_{k+1} is an extension of K_1 contained in K_k, but is not necessarily pure.

Since $K_k = K_{k+1}(\mu_2)$ is a pure extension of K_{k+1} of degree q and we have ensured that K_k contains a pth root of unity ω ($\neq 1$) (this was the point of using K instead of K_0), then, as noted in Section 2, we can define a K_{k+1}-automorphism τ of K_k that sends $\mu_2 \mapsto \omega\mu_2$. (Of course, τ sends the underlying real field $K_0(\mu_1, \mu_k)$ onto a genuinely complex field.) Set $\bar{\mu}_3 = \tau(\mu_3) \in K_k$ and let the second syllable s_2 of w be fr_ℓ. An application of τ to the expression $\mu_3^{p^\ell} = f(\mu_2)$ yields $\bar{\mu}_3^{p^\ell} = f(\omega\mu_2)$. Thus $K_3 = K(\mu_2, \mu_3)$ and $\bar{K} = K(\mu_2, \bar{\mu}_3)$ are both pure extensions of degree p^ℓ of $K_2 = K(\mu_2)$ contained in $K_k = K(\mu_2, \mu_k)$. (In fact, with $\tau(\mu_j) = \bar{\mu}_j$ and $\bar{K}_j = K(\mu_2, \bar{\mu}_j)$, we have a second tower $K_2 = \bar{K}_2 \subset \bar{K}_3 \subset \ldots \subset \bar{K}_k = K_k$, which ends in K_k (see Figure 2); but we only need to consider $\bar{K}_3$.)

If $\ell = 1$, the crucial application of $H_3(n)$ to the word (μ_2, μ_k) (evidently of length less than n) yields immediately that $\bar{K}_3 = K_3$. If $\ell > 1$, a supplementary argument yields the same conclusion. For example, if $K_3 \cap \bar{K}_3 = K_2$, then $K_2(\mu_3^{p^{\ell-1}})$ is a pure extension of $K(\mu_2)$ of degree p contained in $K(\mu_2, \mu_k)$ but not in K_3, in contradiction to $H_3(n)$.

Now, from Section 2, $K(\mu_2)(\mu_3) = K(\mu_2)(\bar{\mu}_3)$ implies that, for some t (indivisible by p), $\mu_3 \bar{\mu}_3^t \in K(\mu_2)$. Raise this element to the pth power and replace the transcendental μ_2 by x to yield an identity $f(x) f^t(\omega x) = h^{p^\ell}(x)$. This is impossible by Lemma 5 (with g constant). Thus $k \not\geqslant 3$.

Finally, if $k = 2$ and $w = r_m f$, with f a polynomial word (necessarily of the form $f_0^{p^\ell}$, where $v_{n+1} = e_\ell$), we must have $K_3 = K_1$ and so $\mu_3 = f(\mu_2) \in K_1 = K(\mu_2^q)$. This quickly leads to $f_0(x) = g(x^p)$ and a contradiction.

8. *Proof of* $H_2(n+1)$

We can now assume $H_1(n+1)$ (in addition to $H(n)$): it is pervasive and we do not stop to point out every use of it. We shall use the induction hypothesis on the *inverse* of a subword of w. But first we make some preliminary observations and adjustments.

By $H_2(n)$ we must prove that $K_k \subset K_{k+1}$ when $m_k \geqslant 1$. For reductio ad absurdum, assume that $K_{k+1} = K_k$. Since this necessitates that $\mu_{k+1} \in K_k$, then, certainly, $\mu_{k+1}^{p^{m_k - 1}} \in K_k$: so replacing μ_{k+1} by $\mu_{k+1}^{p^{m_k-1}}$ we can assume that $m_k = 1$. 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 $v_1 = e_q$.

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

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

Actually, by an adjustment to ζ_1, we can assume that $q = 1$ and that equality holds in the above, that is, $\zeta_1 \notin K(\zeta_2, \mu_k)$, yet $K(\zeta_2, \mu_{k+1}) = K(\zeta_1, \mu_k) = K(\mu_1, \mu_{k+1})$.

Write the end of the word w as

$$w = \ldots e_m g^{-1} r_\ell f r_1 \quad \text{for } m, \ell \geqslant 1, \tag{9}$$

where f and g are both polynomial words (beginning with a genuine translation) and g^{-1} denotes the inverse of g. That is, if g is the polynomial word

$$t_{b_1} e_{\ell_1} t_{b_2} e_{\ell_2} \ldots e_{\ell_j} t_{b_{j+1}} \quad \text{with } b_1 \ldots b_{j+1} \neq 0,$$

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

then $g^{-1} = t_{-b_{j+1}} r_{\ell_j} \dots r_{\ell_2} t_{-b_2} r_{\ell_1} t_{-b_1}$; of course $g(x)$ may simply be a translation $x+b$ ($b \neq 0$), in which case $g^{-1}(x) = x-b$. In similar vein, let $u = (s_1 \dots s_{k-1})^{-1}$ be the inverse in G_p of the bijection $s_1 \dots s_{k-1}$. We could easily write down its symbol representation from that of w; clearly it has the same length as $s_1 \dots s_{k-1}$ (which is less than n) and ends in r_1. In particular, $\mu_k u = \zeta_1$, so $u = (\mu_k, \zeta_1)$. Let $\{v_1 = \mu_k, v_2, \dots\}$ be the syllable transcendental chain of u.

Set $F = K(\mu_k, \mu_{k+1})$. Since $\mu_{k+1}^p = f(\mu_k)$, F is a pure extension of $K(v_1)$ $(= K(\mu_k))$ of degree p contained in $K(\mu_k, \zeta_1)$ but not $K(\mu_k, v_2)$. Apply $H_3(n)$ to the word u with respect to $K(v_1) \subseteq F \subseteq K(\mu_k, \zeta_1)$. Then $F \subseteq K(v_1, v_2)$. Moreover, unless u is a monosyllable, by $H_1(n)$ applied to u, we have $K(v_1, v_2) \subseteq K(v_1, \zeta_2) = K(\mu_k, \zeta_2)$, which yields the contradiction $\mu_{k+1} \in F \subseteq K(\zeta_2, \mu_k)$. Hence u is monosyllabic with $\zeta_1^p \in K(\mu_k)$; thus $K(\mu_k)(\zeta_1) = K(\mu_k)(\mu_{k+1}) = F$. Therefore in (9), $m = 1$, and the entire word w is $e_1 g^{-1} r_\ell f r_1$. Further, for some t (indivisible by p) $\mu_{k+1} \mu_1^t \in K(\mu_k)$. Raising this to the pth power and again replacing the specific transcendental μ_k by the indeterminate x, we get $f(x) g^t(x^{p^\ell}) = h^p(x)$, which contradicts Lemma 5 (with $t = 0$ in (4)).

One bonus, now that we have established $H_2(n+1)$, is that we can assume that Corollary 2 holds for words of length not exceeding $n+1$.

9. *Proof of* $H_3(n+1)$

We may assume $H_1(n+1)$, $H_2(n+1)$, $H_3(n)$ and Corollary 2.

Let F be a pure extension of degree p of K_1 contained in K_{k+1} but not in K_2. By $H_1(n+1)$ and $H_3(n)$, we can suppose that s_k ends in a root, that is, $m_k \geqslant 1$. Again by $H_3(n)$ we can suppose that $F \not\subseteq K_k$. Set $F_1 = F(\mu_k)$. Since both μ_1 and μ_k are in F_1, then $K_k \subseteq F_1$; indeed, F_1 is a pure extension of K_k of degree p contained in K_{k+1} (see Figure 3). By Corollary 2 we know that K_{k+1} is a pure extension of K_k of degree p^{m_k} and so

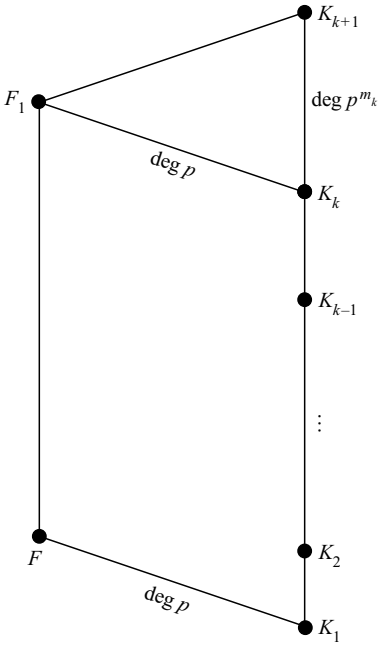


Fig. 3

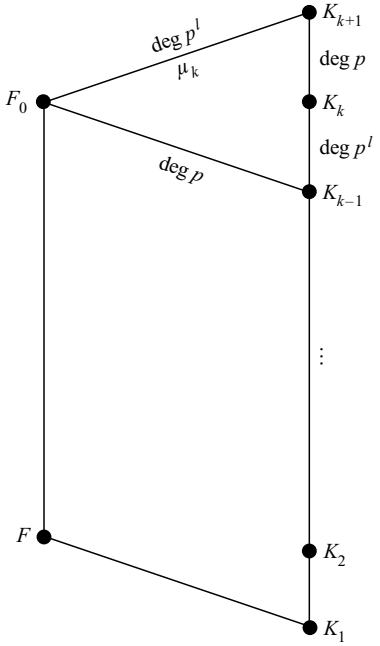


Fig. 4

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

$F_1 = K_k(\mu_{k+1}^{p^{m_k-1}})$. By an adjustment (to μ_{k+1}), we may suppose that $m_k = 1$ and $F_1 = K_{k+1}$.

Again write the final section of w as in (9). Put $F_0 = F(\mu_{k-1})$, a subfield of $F_1 = K_{k+1}$. Since μ_1 and μ_{k-1} are in F_0, then F_0 contains K_{k-1} and, indeed, is an extension of it of degree p. On the other hand, by Corollary 2, K_{k+1} is an extension of K_{k-1} of degree $p^{\ell+1}$. Hence (see Figure 4), $F_1 = F_0(\mu_k)$ is a pure extension of F_0 of degree p^ℓ (that is, $\mu_k^{p^{\ell-1}} \notin F_0$). Hence there is an F_0-automorphism τ of K_{k+1} which maps $\mu_k \mapsto \omega\mu_k$, where $\omega\,(\neq 1)$ is a pth root of unity. Set $\bar{\mu}_{k+1} = \tau(\mu_{k+1}) \in K_{k+1}$. Then $\bar{\mu}_{k+1}^p = f(\omega\mu_k) \in K(\mu_k)$. So $K_k(\bar{\mu}_{k+1})$ is a pure extension of K_k of degree p contained in K_{k+1} and therefore must be identical to $K_{k+1} = K_k(\mu_{k+1})$.

It follows that $\mu_{k+1}\bar{\mu}_{k+1}^t \in K_k$ for some t (indivisible by p). Further,

$$K(\mu_k, \mu_{k+1}\bar{\mu}_{k+1}^t) \subseteq K(\mu_k, \mu_1),$$

yet $(\mu_{k+1}\bar{\mu}_{k+1}^t)^p = f(\mu_k) f^t(\omega\mu_k) \in K(\mu_k)$. Thus $K(\mu_k, \mu_{k+1}\bar{\mu}_{k+1}^t)$ is a pure extension of $K(\mu_k)$ of degree p contained in $K_k = K(\mu_k, \mu_1)$. As in Section 8, by applying $H_3(n)$ to $u = (s_1 \dots s_{k-1})^{-1}$ with syllable transcendental chain $\{v_1 = \mu_k, v_2, \dots\}$ we deduce that $\mu_{k+1}\bar{\mu}_{k+1}^t \in K(v_1, v_2) = K(\mu_k)(v_2)$. Hence, for some s (divisible by p^{m-1} but not p^m), we have

$$\mu_{k+1}\bar{\mu}_{k+1}^t v_2^s \in K(\mu_k).$$

Taking pth powers and (as usual) replacing μ_k by x, we obtain

$$f(x) f^t(\omega x)\, g^s(x^{p^\ell}) = h^p(x),$$

for some polynomial h. This contradicts Lemma 5 in its most general form.

With this the induction is complete and Theorem 1 is established. White's Theorem follows.

10. *Concluding remarks and further reading*

The reader may wonder how many *algebraic* ζ satisfy the equation $\zeta w = \zeta$. for any w. For $e\,(= e(p))$ it can be shown that, if $w = t_1^{a_1} e^{k_1} \dots t_n^{a_n} e^{k_n}$, with $n \geqslant 1$, $k_1, \dots, k_n, a_1, \dots, a_n$ integers and $k_1, \dots, k_{n-1}, a_2, \dots, a_n$ non-zero, then $\{\zeta \in \mathbb{R} : \zeta w = \zeta\}$ has size at most p^k, where $k = |k_1| + \dots + |k_n|$. This is exactly what we would expect: if all of $k_1, \dots, k_n$ were positive, then w would be a polynomial of degree p^k and so would have at most p^k real roots.

In fact, White's Theorem (Corollary 3) holds for any (not necessarily prime) odd integer p (positive or negative) or 'odd' rational number other than ± 1 (see [**1**, **3**]). There is also a version over $\mathbb{C}$ for *all positive* rationals other than 1 (see [**2**]). We believe that the more intricate techniques of [**2**] will prove the result for all negative rationals p $(\neq -1)$ too, but we have not checked the details. White's Theorem fails for $p = +1$ (since $e(1)$ is the identity) and also for $p = -1$ since $e(-1)^2$ and $(t_1 e(-1) t_1^{-1} e(-1) t_1 e(-1))^2$ are identity maps. See also [**4**] for an analogue in prime characteristic and [**5**] for an informal introduction to the general question of the concrete realisation of free groups and free products of groups.

Finally, we remark that, despite the above, it seems much harder to prove Corollary 3 with p replaced by an irrational number (algebraic or transcendental) and we have so far failed in that endeavour. It could prove an interesting challenge!

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

Appendix

At the request of the referee we justify some of the preliminary non-standard facts stated in Sections 2 and 3. Of course these can be extended to more general fields of characteristic 0 and to degrees that are not prime powers.

LEMMA A. *Let E be a subfield of $\mathbb{R}$ and p an odd prime. Also let m, n be integers with $1 \leqslant m \leqslant n$ and $a, b \in E$ such that $a^{1/p} \notin E$ and $b^{1/p} \notin E$. Suppose that $E(a^{1/p^m}) \subseteq E(b^{1/p^n})$. Then $E(a^{1/p^m}) = E(b^{1/p^m})$ and $ab^t = c^{p^m}$ for some $c \in E$ and integer t indivisible by p.*

Proof. It is a standard fact that $[E(a^{1/p^m}) : E] = p^m$ (under the above hypotheses); this follows from [**6**, Theorem 13.1.5], for example. More generally, if $A \in E$ and ℓ is the largest integer satisfying $0 \leqslant \ell \leqslant n$ such that $A^{1/p^\ell} \in E$, then $[E(A^{1/p^n}) : E] = p^{n-\ell}$. We use these truths in what follows.

Assume that $E(a^{1/p^m}) \subseteq E(b^{1/p^n})$. We prove the lemma by induction on n. If $n = m = 1$, then since $E(a^{1/p}) \subseteq E(b^{1/p})$ and both fields have degree p over E, it follows that $E(a^{1/p}) = E(b^{1/p})$. Hence $F(a^{1/p}) = F(b^{1/p})$, where $F = E(\zeta)$ with ζ a primitive pth root of unity. Hence $ab^t = c^p$, for some t coprime to p and $c \in F$ by [**6**, Theorem 13.2.8]. Thus $c^p \in E$; so $[E(c) : E]$ divides p, yet $[F : E]$ is a divisor of $p-1$ [**6**, Theorem 10.2.8] that exceeds 1, since p is odd and $\zeta \notin E$. It follows that $c \in E$ and the result holds.

Now suppose that $n > 1$. We first show that $E(a^{1/p^m}) = E(b^{1/p^m})$ for which purpose we can assume that $n > m$. By induction we may also suppose that $E(a^{1/p^m}) \not\subseteq E(b^{1/p^{n-1}})$. Put $E_1 = E(B)$, where $B = b^{1/p^{n-m}}$ so that $E_1(B^{1/p^m}) = E(b^{1/p^n})$. Then, evidently, $E_1(a^{1/p^m}) \subseteq E_1(B^{1/p^m})$. Let ℓ (with $0 \leqslant \ell \leqslant m$) be maximal such that $a^{1/p^\ell} \in E_1$, and $A = a^{1/p^\ell}$. Then $E_1(A^{1/p^{m-\ell}}) \subseteq E_1(B^{1/p^m})$, where $A^{1/p}, B^{1/p} \notin E_1$. By induction, $E_1(a^{1/p^m}) = E_1(A^{1/p^{m-\ell}}) = E_1(B^{1/p^{m-\ell}}) = E(b^{1/p^{n-\ell}})$. It follows that $a^{1/p^m} \in E(b^{1/p^{n-\ell}})$ and so, by assumption, $\ell = 0$; that is, $E_1(a^{1/p^m}) = E_1(B^{1/p^m})$. Thus, by induction, $a^{1/p^m} B^{u/p^m} = d \in E_1$ for some u coprime to p; that is,

$$a^{1/p^m} b^{u/p^n} = d \in E(b^{1/p^{n-m}}).$$

Now $d^{p^n} = a^{p^{n-m}} b^u \in E$ and so, since $E(d) : E]$ divides $[E(b^{1/p^{n-m}}) : E] = p^{n-m}$, then $e = d^{p^{n-m}} \in E$ and $E(e^{1/p^{n-m}}) \subseteq E(b^{1/p^{n-m}})$, where $e^{1/p^{n-m}} = d$. By induction, $e^{1/p^{n-m}} b^{v/p^{n-m}} = c \in E$ for some v (possibly $p \mid v$). We conclude that

$$a^{1/p^m} b^{u/p^n} b^{v/p^{n-m}} = c \in E, \quad \text{that is,} \quad a^{1/p^m} b^{t/p^n} = c \in E,$$

where $t = u + p^m v$, so that $p \nmid t$ (since $p \nmid u$). It follows that $E(a^{1/p^m}) = E(b^{t/p^n}) = E(b^{1/p^n})$, since $b \in E$ and $1 = tx + p^n y$ for some integers x and y. This is a contradiction since $[E(a^{1/p^m}) : E] = p^m$ and $[E(b^{1/p^n}) : E] = p^n$. We have therefore shown that $E(a^{1/p^m}) = E(b^{1/p^m})$ for all $m \in \{1, \ldots, n\}$. Hence for all such m, we have $E(a^{1/p^{m-1}}) = E(b^{1/p^{m-1}})$. Moreover, by induction we have, if $m > 1$, then $a^{1/p^{m-1}} b^{u/p^{m-1}} = d \in E$, for some u coprime to p. Hence,

$$d^{1/p} = a^{1/p^m} b^{u/p^m} \in E(a^{1/p^m}, b^{1/p^m}) = E(b^{1/p^m}), \quad \text{that is,} \quad E(d^{1/p}) \subseteq E(b^{1/p^m}).$$

By the first part we have $E(d^{1/p}) \subseteq E(b^{1/p})$ and $d^{1/p} b^{v/p} = c \in E$, for some v, where possibly $p \mid v$. Hence

$$a^{1/p^m} b^{t/p^m} = c \in E, \quad \text{where } t = u + p^{m-1} v \quad \text{and} \quad p \nmid t.$$

This completes the proof.

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press

LEMMA B. *Let E be a subfield of $\mathbb{R}$ and p^m be an odd prime power. Suppose that $a \in E$ where $a^{1/p} \notin E$. Then a subfield F of $E(a^{1/p^m})$ containing E necessarily has the form $E(a^{1/p^\ell})$ for some ℓ with $0 \leqslant \ell \leqslant m$.*

Proof. Suppose that F is a field such that $E \subseteq F \subseteq E(a^{1/p^m})$ that is not of the claimed form. Replacing E by an appropriate field of the form $E(a^{1/p^r})$, replacing a by a^{1/p^r} and m by a suitable integer which is at most m, we can assume that $a^{1/p} \notin F$ and F is still not of the claimed form. Note, however, that $F(a^{1/p^m}) = E(a^{1/p^m})$, where $a^{1/p} \notin F$. It follows that $[E(a^{1/p^m}) : F] = p^m = [E(a^{1/p^m}) : E]$ which yields the contradiction that $F = E$.

Finally, the following simple result is quoted in Section 3.

LEMMA C. *Let E be a subfield of $\mathbb{R}$ with algebraic closure $A \subseteq \mathbb{C}$. Set $A_0 = A \cap \mathbb{R}$. Then $A = A_0(\mathrm{i})$.*

Proof. Evidently $A_0(\mathrm{i}) \subseteq A$. Suppose that $\alpha = a + \mathrm{i}b \in A$, where $a, b \in \mathbb{R}$. Since A is a field that is closed under complex conjugation (because $f(\alpha) = 0$ with $f(x) \in E[x]$ implies that $f(\bar{\alpha}) = 0$), then $a = \frac{1}{2}(\alpha + \bar{\alpha}) \in A_0$ and $b = (1/2\mathrm{i})(\alpha - \bar{\alpha}) \in A_0$. Thus $\alpha \in A_0(\mathrm{i})$.

References

1. S. A. ADELEKE, A. M. W. GLASS and L. MORLEY, 'Arithmetic permutations', *J. London Math. Soc.* (2) 43 (1991) 255–268.
2. S. D. COHEN, 'The group of translations and positive rational powers is free', *Quart. J. Math. Oxford Ser.* (2) 46 (1995) 21–93.
3. S. D. COHEN and A. M. W. GLASS, 'Composites of translations and odd rational powers act freely', *Bull. Austral. Math. Soc.* 51 (1995) 73–81.
4. S. D. COHEN and A. M. W. GLASS, 'Free products in prime characteristic: a representation of Fuchsian groups', *J. Algebra*, 179 (1996) 92–114.
5. A. M. W. GLASS, 'The ubiquity of free groups', *Math. Intelligencer* 14 (1992) 54–57.
6. S. ROMAN, *Field theory*, Graduate Texts in Mathematics 158 (Springer, Heidelberg, 1995).
7. 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
Ohio 43403-0221
USA

https://doi.org/10.1112/S002461079600436X Published online by Cambridge University Press