THE CONJUGATE DIMENSION OF ALGEBRAIC NUMBERS

by NEIL BERRY[†]

(*School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh* EH9 3JZ)

ARTŪRAS DUBICKAS[‡]

(*Department of Mathematics and Informatics, Vilnius University, Naugarduko* 24, *Vilnius* 03225, *Lithuania*)

NOAM D. ELKIES[§]

(*Department of Mathematics, Harvard University, Cambridge*, MA 02138, *USA*)

BJORN POONEN[¶]

(*Department of Mathematics, University of California, Berkeley*, CA 94720-3840, *USA*)

and CHRIS SMYTH[‖]

(*School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh* EH9 3JZ)

[Received 15 September 2003]

Abstract

We find sharp upper and lower bounds for the degree of an algebraic number in terms of the $\mathbb{Q}$-dimension of the space spanned by its conjugates. For all but seven non-negative integers n the largest degree of an algebraic number whose conjugates span a vector space of dimension n is equal to $2^n n!$. The proof, which covers also the seven exceptional cases, uses a result of Feit on the maximal order of finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$; this result depends on the classification of finite simple groups. In particular, we construct an algebraic number of degree 1152 whose conjugates span a vector space of dimension only 4.

We extend our results in two directions. We consider the problem when $\mathbb{Q}$ is replaced by an arbitrary field, and prove some general results. In particular, we again obtain sharp bounds when the ground field is a finite field, or a cyclotomic extension $\mathbb{Q}(\omega_\ell)$ of $\mathbb{Q}$. Also, we look at a multiplicative version of the problem by considering the analogous rank problem for the multiplicative group generated by the conjugates of an algebraic number.

[†] E-mail: neilb@maths.ed.ac.uk

[‡] E-mail: arturas.dubickas@maf.vu.lt

[§] E-mail: elkies@math.harvard.edu

[¶] E-mail: poonen@math.berkeley.edu

[‖] Corresponding author. E-mail: c.smyth@ed.ac.uk

Quart. J. Math. 55 (2004), 237–252; doi: 10.1093/qmath/hah003

Table 1 Maximal-order finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$

n	$d_{\max}(n)/(2^n n!)$	Maximal-order subgroup G	$d_{\max}(n) = \#G$
2	3/2	$W(G_2)$	12
4	3	$W(F_4)$	1152
6	9/4	$\langle W(E_6), -I\rangle$	103680
7	9/2	$W(E_7)$	2903040
8	135/2	$W(E_8)$	696729600
9	15/2	$W(E_8) \times W(A_1)$	1393459200
10	9/4	$W(E_8) \times W(G_2)$	8360755200
all other n	1	$W(B_n) = W(C_n) = (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$	$2^n n!$

1. Introduction

Let $\overline{\mathbb{Q}}$ be an algebraic closure of the field $\mathbb{Q}$ of rational numbers, and let $\alpha \in \overline{\mathbb{Q}}$. Let $\alpha_1, \dots, \alpha_d \in \overline{\mathbb{Q}}$ be the conjugates of α over $\mathbb{Q}$, with $\alpha_1 = \alpha$. Then d is the degree $d(\alpha) := [\mathbb{Q}(\alpha) : \mathbb{Q}]$, the dimension of the $\mathbb{Q}$-vector space spanned by the powers of α. In contrast, we define the *conjugate dimension* $n = n(\alpha)$ of α as the dimension of the $\mathbb{Q}$-vector space spanned by $\{\alpha_1, \dots, \alpha_d\}$.

In this paper we compare $d(\alpha)$ and $n(\alpha)$. By linear algebra, $n \leqslant d$. If α has non-zero trace and has Galois group equal to the full symmetric group S_d, then $n = d$ (see [**21**; Lemma 1]). On the other hand, it is shown in [**5**] that n can be as small as $\lfloor \log_2 d \rfloor$. It turns out that n can be even smaller. Our first main result gives the minimum and maximum values of d for fixed n.

THEOREM 1 *Fix an integer $n \geqslant 0$. If $\alpha \in \overline{\mathbb{Q}}$ has $n(\alpha) = n$, then the degree $d = d(\alpha)$ satisfies $n \leqslant d \leqslant d_{\max}(n)$, where $d_{\max}(n)$ is defined by Table* 1, *equalling* $2^n n!$ *for all $n \notin \{2, 4, 6, 7, 8, 9, 10\}$. Furthermore, for each $n \geqslant 1$, there exists $\alpha \in \overline{\mathbb{Q}}$ attaining the lower and upper bounds.*

We refer to those n with $d_{\max}(n) \neq 2^n n!$ as *exceptional*. To attain $d = d_{\max}(n)$, we will use α for which the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois with Galois group isomorphic to a maximal-order finite subgroup G of $\mathrm{GL}_n(\mathbb{Q})$ given in Table 1.

The groups $W(\cdot)$ are the Weyl groups of classical Lie algebras acting on their maximal tori (see, for instance, [**10**]). They are all reflection groups: each is generated by those elements that act on $\mathbb{Q}^n$ by reflection in some hyperplane. For the standard fact that the negative identity matrix $-I$ is not in $W(E_6)$, see for instance [**10**, p. 82]. In particular, $W(B_n) = W(C_n) = (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$ is better known as the *signed permutation group*, the group of $n \times n$ matrices with entries in $\{-1, 0, 1\}$ having exactly one non-zero entry in each row and each column.

Feit [**6**] proved that for each n a subgroup of $\mathrm{GL}_n(\mathbb{Q})$ of maximal finite order is conjugate to the group given in Table 1. (The paper [**6**] is just a statement of results—no proofs.) Feit's result uses unpublished work of Weisfeiler depending on the classification theorem for finite simple groups (see also [**11**, p. 185]). See `http://weisfeiler.com/boris/philinq-8-28-2000.html` for the sad tale of Weisfeiler's disappearance.

The inequality $d \leqslant d_{\max}(n)$ comes from studying the span of $\{\alpha_1, \dots, \alpha_d\}$ as a representation of $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \dots, \alpha_d)/\mathbb{Q})$. To prove the existence of examples where this upper bound is attained, we

(1) observe that if G is one of the maximal-order finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ listed in Table 1, then the G-invariant subfield $\mathbb{Q}(x_1, \ldots, x_n)^G$ of $\mathbb{Q}(x_1, \ldots, x_n)$ is purely transcendental, say $\mathbb{Q}(f_1, \ldots, f_n)$ (whence $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(f_1, \ldots, f_n)$ is a Galois extension with Galois group G),

(2) apply Hilbert irreducibility to obtain a Galois extension K of $\mathbb{Q}$ with Galois group G, and

(3) choose $\alpha \in K$ generating a suitable subrepresentation of G.

Moreover, we give explicit examples for all n except 6, 7, 8, 9, 10, and outline an explicit construction in these remaining five cases.

Many of the arguments work over base fields other than $\mathbb{Q}$, so we generalize as appropriate (Theorem 14). In particular, Theorem 15 generalizes Theorem 1 by giving the minimal and maximal degrees over any cyclotomic base field $\mathbb{Q}(\omega_\ell)$. The answers change drastically for base fields of positive characteristic: for instance from Theorem 14(v) there are elements of a separable closure of $\mathbb{F}_q(t)$ of conjugate dimension 2 that generate Galois extensions of $\mathbb{F}_q(t)$ of arbitrarily large degree. We also give in section 5 some results on analogous questions concerning the rank of the multiplicative subgroup of $\overline{\mathbb{Q}}^*$ generated by $\alpha_1, \ldots, \alpha_d$, and its generalization over a Hilbertian field.

2. Degree and conjugate dimension over fields in general

2.1. *Representations*

Let k be a field, and let k^s be a separable closure of k. If $\alpha \in k^s$, then let $d = d(\alpha)$ be the degree $[k(\alpha) : k]$, and let $n = n(\alpha)$ be the *conjugate dimension* of α (over k), defined as the dimension of the k-vector space $V(\alpha)$ spanned by the conjugates $\alpha_1, \ldots, \alpha_d$ of α in k^s.

PROPOSITION 2 *With notation as above, let $K = k(\alpha_1, \ldots, \alpha_d)$ and let $G = \mathrm{Gal}(K/k)$. Then there exists a faithful n-dimensional k-representation of G.*

Proof. Since $\{\alpha_1, \ldots, \alpha_d\}$ is G-stable, the G-action on K restricts to a G-action on $V(\alpha)$. If $g \in G$ acts trivially on $V(\alpha)$, then g fixes each α_i, so g is the identity on K. Thus $V(\alpha)$ is a faithful k-representation of G. Finally, $\dim_k V(\alpha) = n$, by definition.

A partial converse will be given in Proposition 5 below, whose proof relies on the following representation-theoretic result.

LEMMA 3 *Let k be a field of characteristic* 0*, and let G be a finite group. Let V be a kG-submodule of the regular representation kG. Assume that G acts faithfully on V. Then $V = (kG)\alpha$ for some $\alpha \in V$ with* $\mathrm{Stab}_G(\alpha) = \{1\}$.

Proof. Since k has characteristic zero, V is a direct summand (and hence a quotient) of the regular representation, so the kG-module V can be generated by one element. An element $\alpha \in V$ fails to generate V as a kG-module if and only if $\{g\alpha : g \in G\}$ fails to span V, and this condition can be expressed in terms of the vanishing of certain minors in the coordinates of α with respect to a basis of V. Thus the set $Z := \{\alpha \in V : (kG)\alpha \neq V\}$ of such elements is contained in the zeros of some non-zero polynomial in the coordinates. Also, for each $g \in G - \{1\}$, the set $V^g := \{v \in V : gv = v\}$ is a proper subspace of V, since V is faithful. Since k is infinite, we can choose $\alpha \in V$ outside Z and each V^g for $g \neq 1$.

REMARK 4 We may also allow k to have characteristic $p > 0$, as long as p does not divide $\#G$ and k is infinite. Then V is still a direct summand and a quotient of kG, and the same proof applies. The hypothesis that k is infinite cannot be removed, however, as the following counterexample shows. Let k be a finite field of characteristic p, let k'/k be a finite extension, and take $V = k'$. For any subgroup G_1 of $\mathrm{Gal}(k'/k)$, let G be the semidirect product $k'^* \rtimes G_1$, which acts k-linearly on V. Then every non-zero $\alpha \in V$ has stabilizer isomorphic to G_1. If moreover $\#G_1$ is neither 1 nor a multiple of p, then p does not divide $\#G$, and thus V is a submodule of kG since V is multiplicity-free over $\overline{k}$; but the conclusion of Lemma 3 is false because no $\alpha \in V$ has trivial stabilizer.

PROPOSITION 5 *Let k be a field of characteristic* 0, *and let G be a finite group. Suppose that $G = \mathrm{Gal}(K/k)$ for some Galois extension K of k, and that there is a faithful n-dimensional subrepresentation V of the regular representation of G over k. Then there exists $\alpha \in K$ with $n(\alpha) = n$ and $d(\alpha) = [K : k] = \#G$.*

Proof. By the Normal Basis Theorem, K, as a representation of G over k, is isomorphic to the regular representation. Hence we may identify V with a subrepresentation of K. Lemma 3 gives an element $\alpha \in V$ whose G-orbit has size $\#G$ and spans the n-dimensional space V.

2.2. *Invariant subfields*

PROPOSITION 6 *Let G be one of the groups in Table* 1, *viewed as a subgroup of* $\mathrm{GL}_n(\mathbb{Q})$. *Then for any field k of characteristic* 0, *the invariant subfield $k(x_1, \ldots, x_n)^G$ is purely transcendental over k.*

Proof. We may assume $k = \mathbb{Q}$. Chevalley [**3**] proved that if G is a finite reflection group, then $\mathbb{Q}[x_1, \ldots, x_n]^G = \mathbb{Q}[f_1, \ldots, f_n]$ for some homogeneous polynomials f_i. In this case, we have $\mathbb{Q}(x_1, \ldots, x_n)^G = \mathbb{Q}(f_1, \ldots, f_n)$ as desired.

The only remaining case is $n = 6$ and $G = \langle W(E_6), -I\rangle$. Here $\mathbb{Q}(x_1, \ldots, x_6)^{W(E_6)} = \mathbb{Q}(I_2, I_5, I_6, I_8, I_9, I_{12})$, where each I_j is a homogeneous polynomial of degree j, given explicitly for instance in [**7**] (see also [**10**, p. 59]). Moreover $-I \in G$ acts on this subfield by $I_j \mapsto (-1)^j I_j$, so $\mathbb{Q}(x_1, \ldots, x_6)^G = \mathbb{Q}(I_2, I_6, I_8, I_{12}, I_5^2, I_5 I_9)$.

REMARK 7 Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{R})$. Coxeter showed [**4**] that $\mathbb{R}[x_1, \ldots, x_n]^G$ is a polynomial ring over $\mathbb{R}$ in n algebraically independent generators if G is a finite reflection group. Shephard and Todd proved that this sufficient condition on G is also necessary ([**17**, Theorem 5.1], see also [**10**, p. 65]). For example, $G = \langle W(E_6), -I\rangle$ is not a finite reflection group, and the $\mathbb{R}$-algebra $\mathbb{R}[x_1, \ldots, x_6]^G = \mathbb{R}[I_2, I_6, I_8, I_{12}, I_5^2, I_5 I_9, I_9^2]$ cannot be generated by six polynomials.

2.3. *Hilbert irreducibility*

It is well known that the field $\mathbb{Q}$ is Hilbertian—see for instance [**16**, Theorem 3.4.1] (a form of the Hilbert irreducibility theorem). This implies that Galois extensions of purely transcendental extensions $\mathbb{Q}(f_1, \ldots, f_n)$ can be specialized to Galois extensions of $\mathbb{Q}$ having the same Galois group [**16**, Corollary 3.3.2].

PROPOSITION 8 *Let k be a Hilbertian field. Let a finite subgroup G of* $\mathrm{GL}_n(k)$ *act on* $k(x_1, \ldots, x_n)$ *so that the action on the span of the indeterminates x_i corresponds to the inclusion of G in* $\mathrm{GL}_n(k)$. *If the invariant subfield $k(x_1, \ldots, x_n)^G$ is purely transcendental over k, then there exists a finite Galois extension K of k with Galois group G.*

Proof. By assumption $k(x_1, \dots, x_n)^G = k(f_1, \dots, f_n)$ for some algebraically independent f_i. By Galois theory, $k(x_1, \dots, x_n)$ is a Galois extension of $k(f_1, \dots, f_n)$ with Galois group G. Now use the assumption that k is Hilbertian to specialize.

COROLLARY 9 *If k is a Hilbertian field, and G is one of the groups in Table* 1, *then G is realizable as a Galois group over k.*

Proof. Combine Propositions 6 and 8.

For background material on Hilbert irreducibility see [**15**] or [**16**].

3. Degree and conjugate dimension over $\mathbb{Q}$

3.1. *Proof of Theorem* 1

Proof. The inequality $n \leqslant d$ is immediate. Examples with equality exist by Proposition 5 applied to the standard permutation representation $S_n \hookrightarrow \mathrm{GL}_n(\mathbb{Q})$, since S_n is realizable as a Galois group over $\mathbb{Q}$ (see [**16**, p. 42], for example).

On the other hand, $d \leqslant \#G \leqslant d_{\max}(n)$, where G is the Galois group of α over k, because of Proposition 2, since $d_{\max}(n)$ is the size of the largest finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$.

Finally, we prove that $d = d_{\max}(n)$ is possible for each $n \geqslant 1$. Let G be a maximal finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$, as in Table 1. The given n-dimensional faithful representation of G is a subrepresentation of the regular representation, since otherwise it would contain some irreducible subrepresentation with multiplicity greater than 1, which could be removed once to produce a faithful subrepresentation on a lower-dimensional subspace, contradicting the fact that the function $d_{\max}(n)$ is strictly increasing. (Alternatively, this could be deduced from the fact that the given representation is irreducible for all $n \neq 9, 10$, and is a direct sum of distinct irreducible representations for $n = 9$ and $n = 10$.) Moreover, Corollary 9 shows that G is realizable as a Galois group over $\mathbb{Q}$. Thus Proposition 5 yields $\alpha \in \overline{\mathbb{Q}}$ with $n(\alpha) = n$ and $d(\alpha) = \#G = d_{\max}(n)$.

3.2. *Explicit numbers attaining $d_{\max}(n)$*

In theory, given $n \geqslant 1$, we can construct explicit $\alpha \in \overline{\mathbb{Q}}$ with $n(\alpha) = n$ and $d(\alpha) = d_{\max}(n)$ as follows. Let G be a maximal-order finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$. Take e_j to be the column vector in $\mathbb{Z}^n$ having jth entry 1 and the rest 0, let G_1 be the stabilizer of e_1 under the left action of G, and put $N = |G : G_1|$, the size of the orbit of e_1 under this action. For most of the groups we consider, all of $e_1, \dots, e_n$ are in this orbit, and so we denote the whole orbit by $e_1, \dots, e_n, \dots, e_N$. We then find an *auxiliary polynomial* P_N of degree N, irreducible over $\mathbb{Q}$, whose splitting field has Galois group G over $\mathbb{Q}$. Further, n zeros $\beta_1, \dots, \beta_n$ of P_N can be chosen so that the full list of conjugates $\beta_1, \dots, \beta_N$ of β_1 are the $(\beta_1, \dots, \beta_n)e_j$ for $j = 1, \dots, N$.

The auxiliary polynomial P_N arises, at least generically, as follows: by Proposition 6, we can write $\mathbb{Q}(x_1, \dots, x_n)^G = \mathbb{Q}(I_1, \dots, I_n)$, where the I_j are G-invariant homogeneous polynomials in the x_i. Choose $c_1, \dots, c_n \in \mathbb{Q}$, and define a zero-dimensional variety $\mathcal{V}$ by the polynomial equations

$$\begin{aligned} I_1(x_1, \dots, x_n) &= c_1, \\ &\vdots \\ I_n(x_1, \dots, x_n) &= c_n. \end{aligned}$$

Then successively eliminate $x_n, x_{n-1}, \ldots, x_2$ to get a monic polynomial $R(x_1)$ of degree d_R given by $d_R = \prod_{j=1}^n \deg I_j$. Clearly $\mathbf{x}g \in \mathcal{V}$ for any $\mathbf{x} \in \mathcal{V}$ and $g \in G$, so the multiset of zeros of R is $\{\mathbf{x}ge_1 \mid g \in G\}$, which consists of $\#G_1$ copies of $\{\mathbf{x}e_j \mid j = 1, \ldots, N\}$. Thus $R(x_1) = P_N(x_1)^{\#G_1}$ for some polynomial P_N. For reflection groups and unitary reflection groups we can choose the I_j so that $d_R = \#G$; in this case P_N has degree N. The polynomial P_N is our auxiliary polynomial.

Choose $b_1, \ldots, b_n \in \mathbb{Q}$ such that $b_1x_1 + \cdots + b_nx_n$ is not fixed by any $g \in G$ except the identity. Then $\alpha = b_1\beta_1 + \cdots + b_n\beta_n$ has $n(\alpha) = n$ and degree $d_{\max}(n)$, its conjugates being $(\beta_1, \ldots, \beta_n)g(b_1, \ldots, b_n)^T$ for $g \in G$. (This is the standard 'primitive element' construction for the Galois closure of $\mathbb{Q}(\beta)$.) For most choices of $(c_1, \ldots, c_n)$ (that is, for all choices outside a 'thin set', in the sense of [**16**]), this construction will produce the required α. For small n (such as $n = 2$, considered in sections 3.4 and 4.2), this procedure works well. For much larger n, however, the elimination process becomes impractical. Also, it becomes hard to check whether a particular choice of $(c_1, \ldots, c_n)$ yields a suitable α. The difficulty is to choose $c_1, \ldots, c_n$ so that not only is P_N irreducible, but also it has Galois group G (instead of a subgroup). For this reason, the following sections discuss more practical ways of constructing α, in the non-exceptional case and for $n = 4$.

For the larger exceptional values of n, even these methods would require special treatment for each value, and the large size of $\#G$ (see Table 1) has dissuaded us from trying to do the same for these n. One approach to constructing $\alpha \in \overline{\mathbb{Q}}$ attaining $d_{\max}(n)$ for $6 \leqslant n \leqslant 10$ is to start with Shioda's beautiful analysis relating the Weyl groups of E_6, E_7, E_8 and their invariant rings with the Mordell–Weil lattices of rational elliptic surfaces with an additive fibre. For instance, in [**18**, pp.484–5] Shioda uses this theory to exhibit a monic polynomial in $\mathbb{Z}[X]$ with Galois group $W(E_7)$, whose roots are the images of the 56 minimal vectors of the E_7^* lattice under a $\mathbb{Q}$-linear, $W(E_7)$-equivariant map from $E_7^* \otimes \mathbb{Q}$ to $\overline{\mathbb{Q}}$. The image under this map of any vector in $E_7^* \otimes \mathbb{Q}$ with trivial stabilizer in $W(E_7)$ (that is, in the interior of a Weyl chamber) is then an $\alpha \in \overline{\mathbb{Q}}$ with $n(\alpha) = 7$ and $d(\alpha) = \#W(E_7) = d_{\max}(7)$. A similar construction will work for $n = 8$, and (combined with the analysis of algebraic numbers of conjugate dimension 1, 2) also for $n = 9, 10$. The case $n = 6$ will require additional work, because Shioda's construction, which yields Galois group $W(E_6)$, will have to be modified to produce $\langle W(E_6), -I\rangle$.

3.3. *Explicit numbers attaining $d_{\max}(n)$ for non-exceptional n*

PROPOSITION 10 *Let k be a field of characteristic not 2 and let $n \geqslant 2$. Suppose $f(x) = x^n - a_1x^{n-1} + \cdots + (-1)^n a_n \in k[x]$ is a separable polynomial of degree n with Galois group S_n and discriminant Δ. Let $r_1, \ldots, r_n \in \overline{k}$ be the zeros of $f(x)$. Choose a square root $\sqrt{r_i}$ of each r_i, and let $K = k(\sqrt{r_1}, \ldots, \sqrt{r_n})$. If $a_n \notin \Delta^{\mathbb{Z}} k^{*2}$ and either n is even or $r_1 \notin k^* k(r_1)^{*2}$, then $[K : k] = 2^n n!$.*

Proof. The action of the group $G := \mathrm{Gal}(K/k)$ on $\{\sqrt{r_1}, -\sqrt{r_1}, \ldots, \sqrt{r_n}, -\sqrt{r_n}\}$ is faithful and preserves the partition $\{\{\sqrt{r_1}, -\sqrt{r_1}\}, \ldots, \{\sqrt{r_n}, -\sqrt{r_n}\}\}$, so G is a subgroup of the signed permutation group $W(B_n)$. Recall that $W(B_n)$ is a semidirect product

$$0 \to V \to W(B_n) \to S_n \to 1,$$

where V as a group with S_n-action is the standard permutation representation of S_n over $\mathbb{F}_2$. Since f has Galois group S_n, the group G surjects onto the quotient S_n of $W(B_n)$. Considering the conjugation action of G on itself gives a (possibly non-split) exact sequence

$$0 \to W \to G \to S_n \to 1$$

for some subrepresentation W of V. The only subrepresentations of V are 0, $\mathbb{F}_2$ with trivial S_n-action, the sum-zero subspace of $V = \mathbb{F}_2^n$, and V itself. If $W = V$, we are done.

If W is contained in the sum-zero subspace, then W acts trivially on the square root $\beta := \sqrt{r_1} \dots \sqrt{r_n}$ of a_n. Hence the action of G on β is given by either the trivial character or the sign character of S_n. Thus either $\beta \in k$ or $\beta\sqrt{\Delta} \in k$. Squaring yields $a_n \in \Delta^{\mathbb{Z}} k^{*2}$, contrary to assumption.

The only remaining case is where n is odd and $W = \mathbb{F}_2$. Then W acts trivially on the square root $\beta_1 := \sqrt{r_2}\sqrt{r_3} \dots \sqrt{r_n}$ of $r_2 r_3 \dots r_n = a_n / r_1$. Hence the action of $\mathrm{Gal}(K/k(r_1))$ on β_1 is given by either the trivial character or the sign character of $S_{n-1} = \mathrm{Gal}(k(r_1, \dots, r_n)/k(r_1))$. Thus either $\beta_1 \in k(r_1)$ or $\beta_1\sqrt{\Delta} \in k(r_1)$. Squaring shows that $r_1 \in k^* k(r_1)^{*2}$, again contrary to assumption.

In the situation of Proposition 10, when its hypotheses are satisfied, we can take the auxiliary polynomial to be $P_{2n}(x) = f(x^2)$.

The following corollary is needed in section 3.5.

COROLLARY 11 *Let $n \geqslant 2$. Suppose $f(x) = x^n - a_1 x^{n-1} + \dots + (-1)^n a_n \in k[x]$ is a polynomial of degree n over a field $k \subset \mathbb{R}$, with Galois group S_n. Suppose that the zeros $r_1, \dots, r_n$ of $f(x)$ are real and satisfy $r_1 < 0 < r_2 < \dots < r_n$. Choose a square root $\sqrt{r_i} \in \overline{k}$ of each r_i, and let $K = k(\sqrt{r_1}, \dots, \sqrt{r_n})$. Then $[K : k] = 2^n n!$.*

Proof. It suffices to check the hypotheses of Proposition 10. The discriminant Δ satisfies $\Delta > 0$, but $a_n = r_1 \dots r_n < 0$, so $a_n \notin \Delta^{\mathbb{Z}} k^{*2}$.

If $r_1 \in k^* k(r_1)^{*2}$, say $r_1 = c\gamma_1^2$ with $c \in k^*$ and $\gamma_1 \in k(r_1)$, then applying an automorphism yields $r_2 = c\gamma_2^2$ with $\gamma_2 \in k(r_2)$. These two equations force $c < 0$ and $c > 0$, respectively, a contradiction.

PROPOSITION 12 *For $n = 1$ let $r_1 = 2$, while for $n \geqslant 2$ let $r_1, \dots, r_n \in \overline{\mathbb{Q}}$ be the zeros of $f(x) = x^n + (-1)^n (x - 1)$. Choose a square root of each r_i, and let $\alpha = \sqrt{r_1} + 2\sqrt{r_2} + \dots + n\sqrt{r_n}$. Then $n(\alpha) = n$ and $d(\alpha) = 2^n n!$.*

Proof. By [**16**, p. 42], the polynomial $(-1)^n f(-x) = x^n - x - 1$ has Galois group S_n over $\mathbb{Q}$, so $f(x)$ has Galois group S_n over $\mathbb{Q}$. Also by [**16**, p. 42], each inertia group of $\mathrm{Gal}(\mathbb{Q}(r_1, \dots, r_n)/\mathbb{Q})$ is either trivial or generated by a transposition; it follows that the same is true for the Galois group G of f over $\mathbb{Q}(i)$. The group G has index at most 2 in S_n, so G is S_n or A_n. We claim that $G = S_n$. For $n = 2$ we check this directly.

Take $n \geqslant 3$. If $G = A_n$, then as G would contain no transpositions, all the inertia groups in G would be trivial, and $\mathbb{Q}(i)$ would have an A_n-extension unramified at all places. The existence of such an extension contradicts the Minkowski discriminant bound for $n \geqslant 4$, and contradicts class field theory for $3 \leqslant n \leqslant 4$. Thus $G = S_n$.

In particular, if Δ is the discriminant of $f(x)$, then $\Delta \notin \mathbb{Q}(i)^{*2}$, so $|\Delta| \notin \mathbb{Q}^{*2}$. Therefore $a_n := -1$ is not in $\Delta^{\mathbb{Z}} \mathbb{Q}^{*2}$.

We now finish checking the hypotheses in Proposition 10 by showing that the assumptions n odd and $r_1 \in \mathbb{Q}^* \mathbb{Q}(r_1)^{*2}$ lead to a contradiction. Suppose n is odd, and $r_1 = c\gamma^2$, with $c \in \mathbb{Q}^*$ and $\gamma \in \mathbb{Q}(r_1)^*$. Taking $N_{\mathbb{Q}(r_1)/\mathbb{Q}}$ of both sides yields $(-1)^n \equiv c^n \pmod{\mathbb{Q}^{*2}}$. Since n is odd, $c \equiv -1 \pmod{\mathbb{Q}^{*2}}$. Without loss of generality, $c = -1$. Since γ generates $\mathbb{Q}(r_1)$, the monic minimal polynomial $g(t) \in \mathbb{Q}[t]$ of γ is of degree n. Write $g(t)g(-t) = h(t^2)$ for some polynomial $h \in \mathbb{Q}[x]$. Substituting $t = \gamma$ shows that $h(-r_1) = 0$, but h has degree n, so $h(x) = f(-x)$.

Thus the polynomial $-f(-t^2) = t^{2n} - t^2 - 1$ factors as $-g(t)g(-t)$. However, it is known to be irreducible (Ljunggren [**12**, Theorem 3]).

By Proposition 10, the field $K = \mathbb{Q}(\sqrt{r_1}, \ldots, \sqrt{r_n})$ has degree $2^n n!$. Each $\sqrt{r_i}$ lies outside the field generated by the other square roots over $\mathbb{Q}(r_1, \ldots, r_n)$, so $\sqrt{r_1}, \ldots, \sqrt{r_n}$ are linearly independent over $\mathbb{Q}$. The conjugates of α are the numbers of the form $\sum_{j=1}^{n} \varepsilon_j j \sqrt{r_{\sigma(j)}}$, where $\sigma \in S_n$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$. The linear independence of the square roots guarantees that these $2^n n!$ elements are distinct.

3.4. *An explicit number attaining $d_{\max}(n)$ for $n = 2$*

For $n = 2$, we can take $P_6(x) = x^6 - 2$. Taking one zero β of P_6, all zeros are spanned by the two zeros $\beta, \omega_3\beta$, where ω_3 is a primitive cube root of unity. Then $\alpha = \beta + 3\omega_3\beta$ has $n(\alpha) = 2$ and $d(\alpha) = 12$, and minimal polynomial $y^{12} + 572y^6 + 470596$.

REMARK 13 This example can be produced using the procedure outlined in section 3.2, as follows. The group $W(G_2)$ from Table 1 equals $\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$, and has invariants $I_1 = x_1^2 - x_1x_2 + x_2^2$ and $I_2 = (x_1x_2(x_1 - x_2))^2$. Taking $c_1 = 0$, $c_2 = 2$, $b_1 = 1$, $b_2 = -3$, we get the minimal polynomial of α as the x_2-resultant of $I_1(y + 3x_2, x_2)$ and $I_2(y + 3x_2, x_2) - 2$.

3.5. *An explicit number attaining $d_{\max}(n)$ for $n = 4$*

For $n = 4$, one maximal-order finite subgroup of $GL_4(\mathbb{Q})$ is the order-1152 group $W(F_4)$ generated by its index-3 subgroup $W(B_4)$ (of order 384) and the order-2 matrix

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Thus by Galois correspondence we should be able to apply the construction of section 3.2 for β defined over a suitable cubic extension of $\mathbb{Q}$. And indeed, this is possible.

Define $s_{2k} = z_1^{2k} + z_2^{2k} + z_3^{2k} + z_4^{2k}$ for $k = 1, 2, \ldots$. Four independent homogeneous invariants for $W(F_4)$ are known [**13**] to be

$$I_{2k} = (8 - 2^{2k-1})s_{2k} + \sum_{j=1}^{k-1} \binom{2k}{2j} s_{2j}s_{2k-2j}$$

for $k = 1, 3, 4, 6$. Using the Newton identities and with the help of MAPLE these can be written entirely as polynomials in s_2, s_4, s_6, s_8 as follows:

$$I_2 = 6s_2, \qquad I_6 = -24\, s_6 + 30\, s_2\, s_4, \qquad I_8 = -120\, s_8 + 56\, s_2\, s_6 + 70\, s_4^2,$$
$$I_{12} = -\, 540\, s_4\, s_8 + 244\, s_6^2 - 1365\, s_2^2\, s_8 + \frac{1365}{2}\, s_2^2\, s_4^2 + 255\, s_4^3$$
$$-\, 710\, s_2^4\, s_4 + 1250\, s_2^3\, s_6 + \frac{159}{2}\, s_2^6 + 110\, s_2\, s_4\, s_6.$$

We now use resultants to eliminate s_4 and s_6. This shows that s_8 is cubic over $\mathbb{Q}(I_2, I_6, I_8, I_{12})$, and also that $s_4, s_6 \in \mathbb{Q}(I_2, I_6, I_8, I_{12})(s_8)$. Specifically, we take $I_2 = 6s_2 = 30$, $I_6 = 1410$, $I_8 = 13670$ and $I_{12} = 1161749$, and then $\gamma := s_8$ (the real root, say) satisfies

$$\gamma^3 + \frac{5735}{32}\gamma^2 + \frac{5811288377}{36864}\gamma - \frac{114051068048293}{6220800} = 0.$$

Then, with the Newton identities, we compute the values of the elementary symmetric functions of the z_i^2. This gives a polynomial Q_4 satisfied by the z_i^2:

$$\begin{aligned} Q_4(x) = x^4 - 5\,x^3 &+ \frac{20261200695}{3175710433}\,x^2 + \frac{34560}{3175710433}\,x^2\,\gamma^2 - \frac{47690820}{3175710433}\,x^2\,\gamma \\ &+ \frac{36679035170}{9527131299}\,x - \frac{28800}{3175710433}\,x\,\gamma^2 + \frac{39742350}{3175710433}\,x\,\gamma - \frac{203476507483}{38108525196} \\ &- \frac{72000}{3175710433}\,\gamma^2 - \frac{56249419}{12702841732}\,\gamma. \end{aligned}$$

We write its zeros as $\beta_1^2, \beta_2^2, \beta_3^2, \beta_4^2$ say. They are real and close to $-1, 1, 2$ and 3. (The values for the invariants were chosen to be close to the values they would have had if z_i^2, $i = 1, \ldots, 4$, had been *exactly* $-1, 1, 2, 3$.) Furthermore, its discriminant $223967999/97200$ is not a square in $\mathbb{Q}(\gamma)$. Now, shifting x in this quartic by $5/4$ to obtain a polynomial $z^4 + b_2z^2 + b_1z + b_0$ having zero cubic term, its cubic resolvent $z^3 + 2b_2z^2 + (b_2^2 - 4b_0)z - b_1^2$ is readily checked to be irreducible over $\mathbb{Q}(\gamma)$. Hence by [**8**, Example 14.7, p. 117], the Galois closure of $\mathbb{Q}(\gamma, \beta)$ over $\mathbb{Q}(\gamma)$ has Galois group S_4. Then, as $\beta_1^2 < 0 < \beta_2^2 < \beta_3^2 < \beta_4^2$, we have $[\mathbb{Q}(\beta_1, \beta_2, \beta_3, \beta_4) : \mathbb{Q}] = 2^4 \cdot 4! = 384$, on applying Corollary 11 with $k = \mathbb{Q}(\gamma)$.

If we now take the resultant of $Q_4(x^2)$ and the minimal polynomial of γ, to eliminate γ, we obtain the degree-24 auxiliary polynomial

$$\begin{aligned} P_{24}(x) = x^{24} - 15\,x^{22} &+ \frac{375}{4}\,x^{20} - \frac{2405}{8}\,x^{18} + \frac{65435}{128}\,x^{16} - \frac{25905}{64}\,x^{14} - \frac{181583}{3072}\,x^{12} \\ &+ \frac{8367137}{18432}\,x^{10} - \frac{28198575}{65536}\,x^8 + \frac{1338226651}{5308416}\,x^6 - \frac{895964239}{8847360}\,x^4 \\ &+ \frac{4234139}{294912}\,x^2 - \frac{24389830879}{1592524800}. \end{aligned}$$

This polynomial is irreducible, with zeros $\frac{1}{2}(\pm\beta_1 \pm \beta_2 \pm \beta_3 \pm \beta_4)$ as well as $\pm\beta_1$, $\pm\beta_2$, $\pm\beta_3$, $\pm\beta_4$. Now $(1, 2, 3, 5)^T$ is not a fixed point of any $g \neq I$ in $W(F_4)$. It follows that $\alpha = \beta_1 + 2\beta_2 + 3\beta_3 + 5\beta_4$ has $n(\alpha) = 4$ and degree $d(\alpha) = 1152$, its conjugates being the numbers $(\beta_1, \beta_2, \beta_3, \beta_4)g(1, 2, 3, 5)^T$ for $g \in W(F_4)$.

4. Conjugate dimensions over other fields

4.1. *General results*

The conjugate dimension can behave differently if we use ground fields other than $\mathbb{Q}$. For a field k and a positive integer n, let $D(k, n)$ be the maximal degree of $\alpha \in k^s$ of k-conjugate dimension at most n. For instance $D(\mathbb{Q}, n) = d_{\max}(n)$. If the degree is unbounded, we set $D(k, n) = \infty$. This can happen even for Hilbertian fields of characteristic zero. For example, $D(\mathbb{C}(t), 1) = \infty$, because for each $d \geqslant 1$ a dth root of t generates the Galois extension $\mathbb{C}(t^{1/d})$ of degree d, and all conjugates of $t^{1/d}$ generate the same 1-dimensional space. Nevertheless we can generalize some of our results to various ground fields other than $\mathbb{Q}$. We obtain the following.

THEOREM 14 (i) *If k is a number field of degree m over $\mathbb{Q}$, then $d_{\max}(n) \leqslant D(k, n) \leqslant d_{\max}(mn)$ for all $n \geqslant 1$.*

(ii) *If k is a Hilbertian field of characteristic not dividing ℓ and k contains the ℓth roots of unity, then $D(k, n) \geqslant \ell^n n!$.*

(iii) *If k is a finitely generated transcendental extension of $\mathbb{C}$, then $D(k, n) = \infty$ for all $n \geqslant 1$.*

(iv) *If k is a finite field of q elements, then $D(k, n) = q^n - 1$.*

(v) *If k is a finitely generated transcendental extension of a finite field k_0, then $D(k, 1) = q - 1$, where q is the size of the largest finite subfield of k, and $D(k, n) = \infty$ for all $n \geqslant 2$.*

Proof. (i) By Proposition 2, if $\alpha \in k^s$ has degree d and conjugate dimension n then there exists a d-element subgroup of $\mathrm{GL}_n(k)$. If $[k : \mathbb{Q}] = m$, then an n-dimensional vector space over k can be viewed as an mn-dimensional vector space over $\mathbb{Q}$, so we get an injection $\mathrm{GL}_n(k) \hookrightarrow \mathrm{GL}_{mn}(\mathbb{Q})$. Hence $d \leqslant d_{\max}(mn)$. For the lower bound, note that the specialization made in Proposition 8 can, by [**15**, Theorem 46, p. 298], be made in such a way that the minimal polynomial of the algebraic number with conjugate dimension n remains irreducible over the field k. This gives an example of an algebraic number of degree $d_{\max}(n)$ over k and k-conjugate dimension at most n, so $d_{\max}(n) \leqslant D(k, n)$.

(ii) If k contains the ℓth roots of unity then $\mathrm{GL}_n(k)$ contains the group of size $\ell^n n!$ consisting of the permutation matrices whose entries are ℓth roots of unity in k. Moreover, the invariant ring of this group is polynomial, being generated by the elementary symmetric functions of the ℓth powers of the coordinates. Thus the invariant field is purely transcendental over k. Therefore, by Propositions 5 and 8, there exist $\alpha \in k^s$ of conjugate dimension n and degree $\ell^n n!$.

(iii) This follows from (ii), using the fact that every such field is Hilbertian [**15**, Theorem 49, p. 308].

(iv) The Galois group of any $k(\alpha)/k$ with $n(\alpha) = n$ must be contained in $\mathrm{GL}_n(k)$, but must also be cyclic because k is a finite field $\mathbb{F}_q$. Hence $\#G \leqslant q^n - 1$, as may be seen using the characteristic equation of an invertible matrix in $\mathrm{GL}_n(k)$. We claim that the field of q^{q^n-1} elements is generated by an element α of conjugate dimension n over k. Let g be a generator of $\mathbb{F}_{q^n}^*$, and let $f(x) = \sum_{i=0}^n c_i x^i$ be its minimal polynomial over $\mathbb{F}_q$. Let $\alpha \in \overline{\mathbb{F}}_q^*$ be a zero of $\sum_{i=0}^n c_i X^{q^i}$. Make the $\mathbb{F}_q$-vector space $\overline{\mathbb{F}}_q$ into a module over the polynomial ring $\mathbb{F}_q[\tau]$ by letting τ act as the endomorphism $z \mapsto z^q$. Then the ideal I of $\mathbb{F}_q[\tau]$ that annihilates α contains $f(\tau)$, but $I \neq (1)$. Since f is irreducible, $I = (f(\tau))$. Thus the $\mathbb{F}_q$-span of α and its conjugates is an $\mathbb{F}_q[\tau]$-module isomorphic to $\mathbb{F}_q[\tau]/(f(\tau))$. In particular, $n(\alpha) = \deg f = n$. Also $d(\alpha)$ is the smallest d such that $\tau^d(\alpha) = \alpha$, which is the smallest d such that $\tau^d = 1$ in $\mathbb{F}_q[\tau]/(f(\tau))$; by choice of g, we get $d = q^n - 1$.

(v) Without loss of generality, suppose that k_0 is the largest finite subfield of k, so $\#k_0 = q$. Suppose $\alpha \in \overline{k}$ has $n(\alpha) = 1$. Proposition 2 bounds $d(\alpha)$ by the size of the largest finite subgroup of $\mathrm{GL}_1(k) = k^*$. Elements of finite order in k^* are roots of unity, hence contained in k_0^*. Thus $D(k, 1) \leqslant q - 1$. The opposite inequality follows from (ii) since, by [**15**, Theorem 47, p. 301], k is Hilbertian.

Now suppose $n \geqslant 2$. Choose a finite Galois extension L of k with $[L : k] = n - 1$. (For instance, let L be the compositum of a suitable subfield of a cyclotomic extension of k with some

Artin–Schreier extensions of k.) Let V be the $\mathbb{F}_q$-span of a $\mathrm{Gal}(L/k)$-stable finite subset of L that spans L as a k-vector space. Define

$$P_{V,\varepsilon}(X) := \prod_{x\in V}(X-x)+\varepsilon \in k[X,\varepsilon],$$

where ε is an indeterminate. Then $P_{V,0}(X)$ is a q-linearized polynomial in X, that is, a k-linear combination of $X, X^q, X^{q^2}, \dots$. (See [**9**, Corollary 1.2.2], for instance.) It has distinct roots, namely the elements of V. Therefore $P_{V,\varepsilon}(X)$, considered as a polynomial in X, has distinct roots, which constitute a translate of V in the separable closure of $k(\varepsilon)$. Moreover, $P_{V,\varepsilon}(X)$ is irreducible, because it is a monic polynomial in ε of degree 1. Since k is Hilbertian, it contains $c \neq 0$ such that $P_{V,c} \in k[X]$ is irreducible. Let α be a zero of $P_{V,c}$. Then α is an element of k^s of degree $\#V$. Since the set of conjugates of α is $\{\alpha + v \mid v \in V\}$, the k-span of this set is equal to the span of $V \cup \{\alpha\}$. However $\alpha \notin L$ since $d(\alpha) = \#V \geqslant q^{n-1} > n-1$. So, as the k-span of V is L, $n(\alpha) = [L:k]+1 = n$. Thus $D(k,n) \geqslant \#V$. Since V can be taken arbitrarily large, $D(k,n) = \infty$.

4.2. *Results for cyclotomic fields*

Theorem 1 generalizes to finite cyclotomic extensions of $\mathbb{Q}$. Let ω_ℓ be a primitive ℓth root of unity.

THEOREM 15 *Fix an integer $n \geqslant 0$ and an even integer $\ell \geqslant 4$. If $\alpha \in \overline{\mathbb{Q}}$ has conjugate dimension n over $\mathbb{Q}(\omega_\ell)$ then the degree d of α over $\mathbb{Q}(\omega_\ell)$ satisfies*

$$n \leqslant d \leqslant D(\mathbb{Q}(\omega_\ell), n),$$

where $D(\mathbb{Q}(\omega_\ell), n)$ is defined by Table 2. In particular, $D(\mathbb{Q}(\omega_\ell), n) = \ell^n n!$ for

$$(n,\ell) \notin \{(2,4),(2,8),(2,10),(2,20),(4,4),(4,6),(4,10),(5,4),(6,6),(6,10),(8,4)\}.$$

Furthermore, for each pair (n,ℓ) with $n \geqslant 1$ and $\ell \geqslant 4$ even, there exist $\alpha \in \overline{\mathbb{Q}}$ attaining the lower and upper bounds.

Table 2 is a list of groups isomorphic to maximal-order finite subgroups G of $\mathrm{GL}_n(\mathbb{Q}(\omega_\ell))$, quoted from Feit [**6**]. (An error in the first line of his table has been corrected.) In this table ST_j refers to the jth unitary reflection group in [**17**, Table VII], and the wreath product $G \wr S_n$ is the semidirect product $(G\times\cdots\times G)\rtimes S_n$ in which S_n acts on the n-fold product of G by permuting the coordinates; see also [**20**, Table 7.3.1].

Proof. The proof is a generalization of that of Theorem 1. For fixed ℓ, $D(\mathbb{Q}(\omega_\ell), n)$ is a strictly increasing function of n. Thus to carry over the proof, it remains to show that the invariant subfield $\mathbb{Q}(\omega_\ell)(x_1,\dots,x_n)^G$ is purely transcendental over $\mathbb{Q}(\omega_\ell)$ in each case of Table 2. This is immediate for all the Shephard–Todd groups in the table, by the extension of Chevalley's theorem to unitary reflection groups by Shephard and Todd ([**17**]; see also [**2**, p. 115, Theorem 4; **10**, p. 65]). For example, when $G = (\mathbb{Z}/\ell\mathbb{Z})^n \rtimes S_n$, the field of invariants $\mathbb{Q}(\omega_\ell)(x_1,\dots,x_n)^G$ is $\mathbb{Q}(\omega_\ell)(e_1,\dots,e_n)$, where e_j is the jth elementary symmetric function of $x_1^\ell,\dots,x_n^\ell$. The three remaining cases are handled by Lemma 17 below.

LEMMA 16 *Let k be a field. Let the symmetric group S_m act on*

$$K = k(x_1^{(1)},\dots,x_1^{(m)};\dots;x_n^{(1)},\dots,x_n^{(m)})$$

by acting on the superscripts. Then K^{S_m} is purely transcendental over k.

Table 2 Maximal-order subgroups of $\mathrm{GL}_n(\mathbb{Q}(\omega_\ell))$ for $\ell \geqslant 4$ even

n	ℓ	$D(\mathbb{Q}(w_\ell), n)/(\ell^n n!)$	Maximal-order subgroup G	$D(\mathbb{Q}(\omega_\ell), n) = \#G$
2	4	3	$\mathrm{ST}_8 = \langle \mathrm{GL}_2(\mathbb{F}_3), \omega_4 I\rangle$	96
2	8	3/2	$\mathrm{ST}_9 = \langle \mathrm{GL}_2(\mathbb{F}_3), \omega_8 I\rangle$	192
2	10	3	$\mathrm{ST}_{16} = \langle \omega_5 I\rangle \times \mathrm{SL}_2(\mathbb{F}_5)$	600
2	20	3/2	$\mathrm{ST}_{17} = \langle \mathrm{SL}_2(\mathbb{F}_5), \omega_{20} I\rangle$	1200
4	4	15/2	ST_{31}	46080
4	6	5	ST_{32}	155520
4	10	3	$\mathrm{ST}_{16} \wr S_2$	720000
5	4	3/2	$\mathrm{ST}_{31} \times \langle \omega_4 I\rangle$	184320
6	6	7/6	ST_{34}	39191040
6	10	9/5	$\mathrm{ST}_{16} \wr S_3$	1296000000
8	4	45/28	$\mathrm{ST}_{31} \wr S_2$	4246732800
all other (n, ℓ), $\ell \geqslant 4$ even		1	$\mathrm{ST}_2(\ell, 1, n) = (\mathbb{Z}/\ell\mathbb{Z})^n \rtimes S_n$	$\ell^n n!$

Proof. If E/F is a Galois extension of fields with Galois group G, and V is an E-vector space equipped with a semilinear action of G, there exists an E-basis of V consisting of G-invariant vectors [**19**, II.5.8.1].

Apply this to $E = k(x_1^{(1)}, \ldots, x_1^{(m)})$, $G = S_m$, $F = E^G$ (the purely transcendental extension of k generated by the symmetric functions in $x_1^{(1)}, \ldots, x_1^{(m)}$), and V the E-subspace of K spanned by all the $x_i^{(j)}$ with $i \geqslant 2$. Choose an E-basis $\{v_s\}$ of G-invariant vectors as above. Let $K_0 = k(\{v_s\})$. Since $EK_0 = K$, we have $[K : K_0] \leqslant [E : F] = m!$ On the other hand, $K_0 \subseteq K^G$ with $[K : K^G] = m!$, so $K_0 = K^G$. Since the $x_i^{(j)}$ are algebraically independent over E, the v_s are algebraically independent over k.

LEMMA 17 *Let k be a field, and let G be a finite subgroup of $\mathrm{GL}_n(k)$ whose field of invariants $k(x_1, \ldots, x_n)^G$ is purely transcendental over k. Let $G \wr S_m$ act on*

$$L = k(x_1^{(1)}, \ldots, x_n^{(1)}; \ldots; x_1^{(m)}, \ldots, x_n^{(m)})$$

by letting the ith of the m copies of G act linearly on the span of $x_1^{(i)}, \ldots, x_n^{(i)}$ while S_m acts on the superscripts. Then $L^{G\wr S_m}$ is purely transcendental over k.

Proof. Since $G \wr S_m$ is a semidirect product of S_m by G^m, we have $L^{G\wr S_m} = \left(L^{G^m}\right)^{S_m}$. If $k(x_1, \ldots, x_n)^G = k(I_1, \ldots, I_n)$, then

$$L^{G^m} = k(I_1^{(1)}, \ldots, I_n^{(1)}; \ldots; I_1^{(m)}, \ldots, I_n^{(m)}),$$

and S_m acts on this by acting on superscripts. Now apply Lemma 16.

EXAMPLE Using the elimination procedure outlined in section 3.2, we can give an example of an algebraic number α of degree 96 over $\mathbb{Q}(i)$ with $\mathbb{Q}(i)$-conjugate dimension 2 and Galois group ST_8, as in Table 2. Now $\mathrm{ST}_8 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix} \right\rangle$, with invariants

$$\begin{aligned} I_8(x_1, x_2) =& x_1^8 + 4(1+i)\, x_1^7 x_2 + 14 i\, x_1^6 x_2^2 - 14(1-i)\, x_1^5 x_2^3 - 21\, x_1^4 x_2^4 - 14(1+i)\, x_1^3 x_2^5 \\ & - 14 i\, x_1^2 x_2^6 + 4(1-i)\, x_1 x_2^7 + x_2^8, \\ I_{12}(x_1, x_2) =& 2\, x_1^{12} + 12(1+i)\, x_1^{11} x_2 + 66 i\, x_1^{10} x_2^2 - 110(1-i)\, x_1^9 x_2^3 - 231\, x_1^8 x_2^4 \\ & - 132(1+i)\, x_1^7 x_2^5 - 132(1-i)\, x_1^5 x_2^7 - 231\, x_1^4 x_2^8 - 110(1+i)\, x_1^3 x_2^9 \\ & - 66 i\, x_1^2 x_2^{10} + 12(1-i)\, x_1 x_2^{11} + 2\, x_2^{12}. \end{aligned}$$

The x_2-resultant of $I_8 - 1 - i$ and $I_{12} - 1$ is $P_{24}(x_1)^4$, where the auxiliary polynomial P_{24} is

$$P_{24}(x) = 27\, x^{24} - 270(1+i)\, x^{16} + 270\, x^{12} - 810\, i\, x^8 + 54(1+i)\, x^4 - 9 + 8\, i.$$

Two zeros β and β' of P_{24} can be chosen so that the conjugates of β are

$$\omega\beta, \quad \omega\beta', \quad \omega(\beta + \beta'), \quad \omega(\beta - i\beta'), \quad \omega(\beta + (1-i)\beta'), \quad \omega((1+i)\beta + \beta'),$$

where $\omega \in \{\pm 1, \pm i\}$. Then $\alpha = \beta + 2\beta'$ has degree 96 over $\mathbb{Q}(i)$, with conjugates $(\beta, \beta')g(1, 2)^T$ for $g \in \mathrm{ST}_8$. The minimal polynomial of α can be computed directly as the resultant with respect to x_2 of $I_8(y - 2x_2, x_2) - 1 - i$ and $I_{12}(y - 2x_2, x_2) - 1$.

4.3. *$D(k, n)$ depends on more than ℓ and n*

Let k be a number field, and let ℓ be the number of roots of unity in k. It seems reasonable to guess, as in the case of cyclotomic fields $\mathbb{Q}(\omega_\ell)$, that $D(k, n) = \ell^n n!$ for all but finitely many n. However, it is possible that two number fields k and k' contain the same number of roots of unity, but $D(k, n) \neq D(k', n)$ for some n. For example, we can take $k = \mathbb{Q}(\cos(2\pi/m), \sin(2\pi/m))$, where $m > 6$, and $k' = \mathbb{Q}$. In both cases $\ell = 2$, but $D(k, 2) > D(\mathbb{Q}, 2) = 12$. Indeed, there exist $a, b \in k$ such that $\alpha = \sqrt[m]{a}(1 + b\omega_m)$ is of degree $2m > 12$ over k. Its conjugate dimension over k is 2; its conjugates are spanned by $\sqrt[m]{a}$ and $i\sqrt[m]{a}$. This example also shows that the number of exceptional cases can be arbitrarily large, since we may simply take m with $2m > 2^n n!$.

Another example is $D(\mathbb{Q}(\sqrt{5}), 3) \geqslant 120$, obtained from the icosahedral subgroup of $\mathrm{GL}_3(\mathbb{Q}(\sqrt{5}))$ (reflection group ST_{23}) via Propositions 5 and 8.

5. Multiplicative conjugate rank

Instead of the dimension $n(\alpha)$ of the $\mathbb{Q}$-vector space spanned by the d conjugates α_i of an algebraic number α, we may consider the rank $r(\alpha)$ of the multiplicative subgroup of $\overline{\mathbb{Q}}^*$ they generate. We call this the (*multiplicative*) *conjugate rank* of α. As before, we have the trivial inequality $r(\alpha) \leqslant d(\alpha)$, which is sharp in the case of maximal Galois group (again by [**21**, Lemma 1]). Unlike in the additive case, we can have no non-trivial lower bound without some further hypothesis, because if α is a root of unity then $r(\alpha) = 0$ while $d(\alpha)$ is unbounded. However, also unlike the additive case, we have the following result over a very general field. The main difficulty in the proof below is to show that this bound is sharp for Hilbertian fields.

THEOREM 18 *Suppose that α is separable and algebraic of degree $d(\alpha)$ over a field k, and the multiplicative subgroup of $(k^s)^*$ generated by the conjugates $\alpha_1, \dots, \alpha_d$ of α is torsion-free. Then the rank $r(\alpha)$ of this subgroup satisfies $r(\alpha) \leqslant d(\alpha) \leqslant d_{\max}(r(\alpha))$, with $d_{\max}(\cdot)$ defined by Table* 1 *as before. If k is Hilbertian, then for each integer $r \geqslant 1$ there are $\alpha \in k^s$ of conjugate rank r attaining the lower and upper bounds.*

The upper bound is given by the same function $d_{\max}(\cdot)$ that we found for the conjugate dimension over $\mathbb{Q}$, and this bound is independent of the ground field k, although it need not always be sharp.

Proof. For any $\alpha \in k^s$, let $\Gamma = \Gamma(\alpha)$ be the multiplicative group generated by the α_i. We observed already that the lower bound $d(\alpha) \geqslant r(\alpha)$ is immediate. For the upper bound, we argue as we did for $n(\alpha)$. The Galois group G acts faithfully on Γ. By hypothesis, $\Gamma \cong \mathbb{Z}^{r(\alpha)}$, so G acts faithfully also on $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$, which is a $\mathbb{Q}$-vector space of dimension $r(\alpha)$. Hence $\#G$ is bounded above by $d_{\max}(r(\alpha))$, the size of the largest finite subgroup of $\mathrm{GL}_{r(\alpha)}(\mathbb{Q})$. Hence $d(\alpha) \leqslant \#G \leqslant d_{\max}(r(\alpha))$.

The proof that there are examples attaining equality when k is Hilbertian uses two corollaries of the following technical result.

PROPOSITION 19 *Let L/k be a finite Galois extension of fields with Galois group G, and suppose that k is not algebraic over a finite field. Then the $\mathbb{Z}G$-module L^* contains a free $\mathbb{Z}G$-module of rank* 1.

Proof. For each $g \in G - \{1\}$, choose $a_g \in L$ that is not fixed by g. Choose $b \in L$ that is not algebraic over a finite field. Let S be the union of the G-orbits of the a_g and of b. Then S is finite. Let L_0 be the minimal subfield of L containing S. Let k_0 be the subfield $(L_0)^G$ fixed by G. The action of G on S is faithful, so G acts faithfully on L_0, and L_0/k_0 is Galois with group G. In this way we reduce to the case where k and L are finitely generated fields (finitely generated over their minimal subfield).

Choose finitely generated $\mathbb{Z}$-algebras $A \subseteq B$ with fraction fields k and L, respectively. Without loss of generality we may assume, by localization, that B is a finite étale Galois algebra over A. Since L is not algebraic over a finite field, $\dim A = \dim B \geqslant 1$. By [**14**, Theorem 4], there is a maximal ideal $\mathfrak{m}_1$ of B lying over a maximal ideal $\mathfrak{m}$ of A such that the residue field extension $B/\mathfrak{m}_1$ over $A/\mathfrak{m}$ is trivial. Thus $\mathfrak{m}$ splits completely: if $n = \#G$, there are n distinct maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ of B lying over $\mathfrak{m}$, and they are are permuted transitively by G. By [**1**, Proposition 1.11], there exists a non-zero $\beta \in \mathfrak{m}_1$ lying outside all of $\mathfrak{m}_2, \dots, \mathfrak{m}_n$. We can label the conjugates β_i of β so that $\beta_i \in \mathfrak{m}_j$ if and only if $i = j$. Any non-trivial relation $\prod_{i=1}^n \beta_i^{b_i} = 1$ with $b_i \in \mathbb{Z}$, would, after moving the factors with negative exponent to the other side, give an equality between an element in $\mathfrak{m}_i$ and an element outside $\mathfrak{m}_i$, for some i. Hence the $\mathbb{Z}G$-module generated by β in L^* is free of rank 1.

COROLLARY 20 *Let k be a field that is not algebraic over a finite field. If k has a Galois extension with Galois group S_r, then there exists $\alpha \in (k^s)^*$ with $r(\alpha) = d(\alpha) = r$.*

Proof. Let L be the S_r-extension of k. By Proposition 19, the $\mathbb{Z}S_r$-module L^* contains a copy of $\mathbb{Z}S_r$, which contains a copy of the $\mathbb{Z}S_r$-module $\mathbb{Z}^r$ on which S_r acts by permuting coordinates. The element $(1, 0, \dots, 0) \in \mathbb{Z}^r$ corresponds to $\alpha \in L^*$ with the desired properties.

COROLLARY 21 *Let k be a field that is not algebraic over a finite field, and let G be a finite group. Suppose that $G = \mathrm{Gal}(K/k)$ for some Galois extension K of k, and that there is a faithful*

r-dimensional subrepresentation V of the regular representation of G over $\mathbb{Q}$. Then there exists $\alpha \in K^*$ whose conjugates generate a torsion-free multiplicative group with $r(\alpha) = r$ and $d(\alpha) = [K : k] = \#G$.

Proof. Apply Proposition 19 and then Lemma 3 with $k = \mathbb{Q}$. This gives $\alpha \in K^* \otimes_{\mathbb{Z}} \mathbb{Q}$ with the desired properties, and we replace α by a power so that it is represented by an element of K^*.

We now prove the final statement of Theorem 18. Since k is Hilbertian, k has S_r-extensions for all r. In particular, k is not algebraic over a finite field. Applying Corollary 20 yields α with $r(\alpha) = d(\alpha) = r$. Combining Corollaries 9 and 21 gives a different α with $r(\alpha) = r$ and $d(\alpha) = d_{\max}(r)$, for any $r \geqslant 1$.

We end by giving an explicit algebraic number of conjugate rank n and degree $2^n n!$ over $\mathbb{Q}$.

PROPOSITION 22 *Let $\sqrt{r_1}, \ldots, \sqrt{r_n}$ be as in Proposition* 12. *Let $s_i = (1 + \sqrt{r_i})/(1 - \sqrt{r_i})$ and $\alpha = s_1 s_2^2 \cdots s_n^n$. Then $r(\alpha) = n$ and $d(\alpha) = 2^n n!$ over $\mathbb{Q}$.*

Proof. The proof of Proposition 12 showed that $[\mathbb{Q}(\sqrt{r_1}, \ldots, \sqrt{r_n}) : \mathbb{Q}] = 2^n n!$, so its Galois group G is the signed permutation group $W(B_n)$. The elements of G act on α by permuting the exponents $1, 2, \ldots, n$ and changing their signs independently. In particular, the group generated by the conjugates of α is of finite index in the subgroup generated by the s_i. On the other hand, the s_i are multiplicatively independent since they are not roots of unity and since there is an automorphism inverting any one of them while fixing all the others. Thus α has $2^n n!$ distinct conjugates, and they generate a subgroup of rank n.

Acknowledgments

We thank Hendrik Lenstra for suggesting the proof of Lemma 16, and Walter Feit for some helpful correspondence.

Noam Elkies also thanks David Moulton for communicating the topic to him, as a problem on the list compiled by Gerry Myerson at the 2001 Asilomar meeting.

The second author was supported in part by the Lithuanian State Studies and Science Foundation, and the London Mathematical Society. The third author was supported in part by NSF grant DMS-0200687. The fourth author was supported in part by NSF grant DMS-0301280 and a Packard Fellowship.

References

1. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison Wesley, Reading, MA, 1969.
2. N. Bourbaki, Groupes et algèbres de Lie, *Éléments de Mathématique*, Chapitres 4, 5 et 6, Masson, Paris, 1981.
3. C. Chevalley, Invariants of finite groups generated by reflections, *Amer. J. Math.* **77** (1955), 778–782.
4. H. S. M. Coxeter, The product of the generators of a finite group generated by reflections, *Duke Math. J.* **18** (1951), 765–782.
5. A. Dubickas, Additive relations with conjugate algebraic numbers, *Acta Arith.* **107** (2003), 35–43.
6. W. Feit, Orders of finite linear groups, *Proceedings of the First Jamaican Conference on Group Theory and its Applications*, The University of the West Indies, Kingston, 1996, 9–11.

7. J. S. Frame, The classes and representations of the groups of 27 lines and 28 bitangents, *Ann. Mat. Pura Appl.* **32** (1951), 83–119.

8. D. J. H. Garling, *A Course in Galois Theory*, Cambridge University Press, Cambridge, 1986.

9. D. Goss, *Basic Structures of Function Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 35, Springer, Berlin, 1996.

10. J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge Studies in Advanced Mathematics 29, Cambridge University Press, Cambridge, 1990.

11. J. Kuzmanovich and A. Pavlichenkov, Finite groups of matrices whose entries are integers, *Amer. Math. Monthly* **109** (2002), 173–186.

12. W. Ljunggren, On the irreducibility of certain trinomials and quadrinomials, *Math. Scand.* **8** (1960), 65–70.

13. M. L. Mehta, Basic sets of invariant polynomials for finite reflection groups, *Comm. Algebra* **16** (1988), 1083–1098.

14. B. Poonen, Points having the same residue field as their image under a morphism, *J. Algebra* **243** (2001), 224–227.

15. A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications 77, Cambridge University Press, Cambridge, 2000. With an Appendix by Umberto Zannier.

16. J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics 1, Jones & Bartlett, Boston MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon]. With a foreword by Darmon and the author.

17. G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274–304.

18. T. Shioda, Theory of Mordell–Weil lattices, *Proceedings of the International Congress of Mathematicians*, Vols I, II (Kyoto, 1990), Mathematical Society of Japan, Tokyo, 1991, 473–489.

19. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1992. Corrected reprint of the 1986 original.

20. L. Smith, *Polynomial Invariants of Finite Groups*, Research Notes in Mathematics 6, A. K. Peters, Wellesley MA, 1995.

21. C. J. Smyth, Additive and multiplicative relations connecting conjugate algebraic numbers, *J. Number Theory* **23** (1986), 243–254.