THREE ALGEBRAIC CONJUGATES SUMMING TO ZERO: DEGREES 28 AND 35 ARE IMPOSSIBLE, DEGREE 55 IS NOT

KOREA SUPERINTELLIGENCE LABS

Abstract. Let α be an algebraic number of degree d over $\mathbb{Q}$. Dubickas asked, as Problem 11123 of the *American Mathematical Monthly*, whether three distinct conjugates of α can sum to zero when $3 \nmid d$, and Stong's polynomial $t^{20} + 4 \cdot 5^9 t^{10} + 16 \cdot 5^{15}$ shows that they can. Baronėnas, Drungilas and Jankauskas [1] proved that no such relation exists in degree 16, that 20 is the least degree not divisible by 3 that admits one, and listed the sixteen degrees $d \le 100$ at which the question is open: $28, 35, 44, 52, 55, 56, 65, 68, 70, 76, 77, 85, 88, 91, 92, 95$. We settle three of them. Degrees 28 and 35 admit no such relation; the proof is an exhaustive test over all 1854 transitive groups of degree 28 and all 407 of degree 35, and over every orbit of 3-subsets of the underlying set. Degree 55 does admit one: the group $C_{11} \rtimes C_5$ acting on $\mathbb{Q}(\zeta_{11})$, together with $\kappa = -(1 + \zeta_{11})$, produces through Hilbert's Theorem 90 an element w with $w + \zeta_{11} w + \sigma(w) = 0$ whose orbit has exactly 55 elements. The two arithmetic facts that carry that construction are machine-checked: the norm condition $\mathrm{N}_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\sqrt{-11})}(\kappa) = 1$, which reduces to the cyclotomic identity $\prod_{a \in \mathrm{QR}(11)} (1 + \zeta_{11}^a) = -1$, and the freeness certificate $(1 + \zeta_{11})^{11} \neq -1$. The same construction yields an algebraic number of degree $p(p-1)/2$ with three conjugates summing to zero for every prime $p \equiv 11 \pmod{24}$ with $(p-1)/2$ prime, a degree divisible by neither 3 nor 20; 55 is its only member below 100. We also record a machine-checked form of the prime-power divisibility theorem of [1] and of its Sylow lemma. No explicit polynomial of degree 55 is exhibited: the last step of the construction is a realizability theorem and is not constructive.

1. Introduction

1.1. **The question.** Let α be an algebraic number of degree $d > 1$ over $\mathbb{Q}$ and let $\alpha_1, \dots, \alpha_d$ be its conjugates. Dubickas asked, as Problem 11123 of the *American Mathematical Monthly* [5], proposed in the issue of December 2004, whether a relation

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \qquad \alpha_1, \alpha_2, \alpha_3 \text{ pairwise distinct conjugates}, \tag{1}$$

forces $3 \mid d$. It does not. In the solution printed in December 2006 under the names of Dubickas, Smyth and Stong [5], Stong exhibited the irreducible polynomial

$$t^{20} + 4 \cdot 5^9 \, t^{10} + 16 \cdot 5^{15},$$

three of whose roots sum to zero, so that $d = 20$ occurs. (The printed proposal carries Dubickas's name alone; [1] attributes the question to Dubickas and Smyth, and cites the 2006 solution for it.) Both the cubic $t^3 - t - 1$ and Stong's example propagate upwards: if (1) holds in degree d and γ has degree s over $\mathbb{Q}$ and over $\mathbb{Q}(\alpha_1)$, then $\beta_j = \alpha_j(a + \gamma)$ has degree ds for all large rational integers a and satisfies $\beta_1 + \beta_2 + \beta_3 = 0$. So every multiple of 3 and every multiple of 20 is attainable [1, §5]. The natural question is then

> *for which degrees d does there exist an algebraic number of degree d three of whose conjugates sum to zero?*

Note that impossibility does not propagate: 56 is a multiple of 28 and 70 of 35, and knowing that 28 is impossible says nothing about 56. Only attainability propagates upwards.

1.2. **The sixteen open degrees.** Baronėnas, Drungilas and Jankauskas [1] settle the impossibility half in a large range of degrees. We name the results of [1] by the labels its source file gives them, because the paper shares one counter between `theorem` and `lemma` and the labels are stable while the numbers need not be; in v1, the version cited throughout, `p1`, `p2`, `t1`, `t2` print as Theorems 1–4 and `l1`, `lefpte` as Lemmas 5 and 6.

Their Theorem `p2` states that if $d = p^m$ with p a prime $\neq 3$, or $d = 2p^m$ with $p \geq 5$ prime and $m \geq 1$, then $\alpha_1 + \alpha_2 \pm \alpha_3 \neq 0$ for any three roots of an irreducible polynomial of degree d; and their Theorem `p1` states that the least degree $d > 1$ not a multiple of 3 at which (1) occurs is $d = 20$. Every degree below 20 that is not a multiple of 3 is a prime power or twice an odd prime power, so Theorem `p2` covers them all, the title case $d = 16$ included. Crossing out from $[2, 100]$ the multiples of 3, the multiples of 20 and the degrees forbidden by Theorem `p2` leaves sixteen values, and [1, §5] records, verbatim, that these are

> `28, 35, 44, 52, 55, 56, 65, 68, 70, 76, 77, 85, 88, 91, 92, 95`
>
> *for which neither solutions to the equation $\alpha_1 + \alpha_2 + \alpha_3 = 0$ in conjugate algebraic numbers $\alpha_1, \alpha_2, \alpha_3$ of degree d are currently known, nor the non-existence of such solutions have been established.*

Those sixteen degrees are the subject of this paper.

1.3. **Results.** We settle three of the sixteen.

(1) *Degrees* 28 *and* 35 *are impossible* (Theorem 3.1): no algebraic number of degree 28, and none of degree 35, has three conjugates summing to zero. The proof is exhaustive over the classified transitive permutation groups of those two degrees — 1854 of degree 28 and 407 of degree 35 — and over every orbit of 3-subsets of the permuted set. What is tested is a module condition equivalent to (1), described in §2; the direction of that equivalence used here is unconditional.

(2) *Degree* 55 *is attainable* (Theorem 5.1): there is an irreducible $f \in \mathbb{Q}[t]$ of degree 55 with three distinct roots summing to zero, and hence one of degree $55s$ for every $s \geq 1$, in particular of degree 110. The construction takes $E = \mathbb{Q}(\zeta_{11})$, $\sigma\colon \zeta_{11} \mapsto \zeta_{11}^3$ of order 5, $F = E^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{-11})$ and $\kappa = -(1 + \zeta_{11})$, and applies Hilbert's Theorem 90 to the cyclic extension E/F.

(3) *The arithmetic core of that construction is machine-checked.* Two facts carry it, and both are verified by a proof assistant: the norm condition $\mathrm{N}_{E/F}(\kappa) = 1$ (Theorem 4.3), which rests on the cyclotomic identity $\prod_{a \in \mathrm{QR}(11)}(1 + \zeta_{11}^a) = -1$ (Proposition 4.2); and the freeness certificate $(1+\zeta_{11})^{11} \neq -1$ (Theorem 4.4), which is what makes the relevant orbit have exactly 55 elements rather than fewer.

(4) *An infinite family* (Theorem 5.5): for every prime $p \equiv 11 \pmod{24}$ with $(p-1)/2$ prime there is an algebraic number of degree $d = p(p-1)/2$ with three conjugates summing to zero, and that d is divisible by neither 3 nor 20. The first cases are $d = 55, 1711, 3403, 5671, 15931$; only 55 lies below 100, which is why exactly one of the sixteen degrees falls to this construction. The family rests on a sign law for $\prod_{a \in \mathrm{QR}(p)}(1 + \zeta_p^a)$ (Proposition 5.4) whose instances at $p = 11$ and $p = 7$ are machine-checked.

(5) *The prime-power theorems of* [1]*, in machine-checked form* (§6). We state and verify the group-theoretic engine of that paper's Theorem `t1`, its Lemma `l1`, and the prime-power half of its Theorem `p2`, for an abstract transitive action in place of a Galois group. These are the results of [1]; only their verified form is ours.

1.4. **What is verified by machine, and what is not.** This distinction runs through the paper and we state it once, plainly. The statements of §4 and §6 — the cyclotomic identity, the norm condition, the freeness certificate, their controls, and the prime-power theorems — have been checked in Lean 4 [16] against Mathlib [17]; §8 says exactly what the machine checks. Everything else is ordinary mathematics, and in two places it rests on computation that is exhaustive but not machine-checked:

- the reduction of §2 and the sweep behind Theorem 3.1 (the classification of transitive groups of degrees 28 and 35 is not available to the proof assistant, and there is no route to making it available);

- the classical ingredients of Theorem 5.1 — Hilbert's Theorem 90, the normal basis theorem, and the realizability of a solvable group as a Galois group over $\mathbb{Q}$ — which we take from the literature.

§7 states precisely which claims rest on exhaustive computation and how large each search was.

1.5. **Relation to other work.** Three points of provenance should be made explicit.

The graph-theoretic predecessor. The paper [1] has an earlier version [2], by the same three authors and under the same title, with a different proof: "employing the classification of vertex-transitive graphs on 16 vertices of degree 6, we prove that $d \neq 16$". That version supplies the graph-theoretic layer of the reduction — the graph on the conjugates joining $\alpha' \sim \alpha''$ when some third conjugate completes a zero-sum triple, its vertex-transitivity and 6-regularity, the fact that two distinct relations meet in at most one conjugate, and the trace-zero condition, which is its Lemma intro3 and which it credits to Dubickas and Jankauskas [8] — and eliminates the 40 vertex-transitive graphs on 16 vertices of valency 6 one by one, taking the explicit list from the graph data set of [12]. It treats no degree other than 16 and contains no sweep over transitive groups. Everything in that layer is theirs, and we use it as background only.

The method behind the norm condition is published, and the source does not cite it. Dubickas and Smyth [4] prove (their Theorem 1.1) that a non-zero algebraic number β can be written as a quotient α/α' of two conjugates over K if and only if there is a σ in the relevant Galois group with $P(\sigma, \beta)$ a root of unity, where $P(\sigma, \beta)$ is the product of β over its $\langle\sigma\rangle$-orbit. That is exactly the test that $\kappa = -(1 + \zeta_{11})$ passes in §5, with $P(\sigma, \kappa) = 1$. So the *technique* of §5 is in print, by the two authors under whose names, with Stong's, the solution of Problem 11123 appeared; that paper treats two conjugates, states no three-term relation and names no degree, and it is not cited in [1]. What is claimed here is the instance: that this test, at $p = 11$, settles one of the sixteen open degrees.

A race, not a gap in the literature. The strongest evidence that degrees 28, 35 and 55 were open when this work was done is the sentence quoted above from [1, §5], dated 4 August 2026 and written by the authors who had published the $d \neq 16$ graph argument two months earlier. But the graph census on which [2] relies [12] covers vertex-transitive graphs on up to 47 vertices, so degree 28 is within reach of that paper's own method. A follow-up by the same group could settle 28 at any time. We record this as a race rather than as a hidden prior result.

2. The reduction to transitive permutation modules

Nothing in this section is machine-checked.

Let Ω be a finite set with $|\Omega| = d$, let $(e_x)_{x\in\Omega}$ be the standard basis of $\mathbb{Q}^\Omega$, and for a 3-subset $T = \{i, j, k\} \subseteq \Omega$ write $e_T = e_i + e_j + e_k$. A group G acting on Ω acts on $\mathbb{Q}^\Omega$ by permuting coordinates, and we write $\mathbb{Q}[G]\, e_T$ for the $\mathbb{Q}[G]$-submodule generated by e_T.

Proposition 2.1 (the criterion)**.** *The following are equivalent.*

(1) *There is an irreducible $f \in \mathbb{Q}[t]$ of degree d with three distinct roots summing to zero.*
(2) *There are a finite group G occurring as a Galois group over $\mathbb{Q}$, a transitive action of G on a d-set Ω, and a 3-subset $T \subseteq \Omega$ such that the $\mathbb{Q}[G]$-submodule $N = \mathbb{Q}[G]\, e_T \subseteq \mathbb{Q}^\Omega$ contains no vector $e_a - e_b$ with $a \neq b$.*

The implication (1)⇒(2) *requires no hypothesis.*

Proof sketch. For (1)⇒(2), let L be the splitting field of f, $G = \mathrm{Gal}(L/\mathbb{Q})$ and Ω the set of roots, on which G acts transitively because f is irreducible. The space $A_\mathbb{Q} = \{a \in \mathbb{Q}^\Omega : \sum_x a_x x = 0\}$ is a $\mathbb{Q}[G]$-submodule and contains e_T for the triple T of the relation, hence contains N; and $e_a - e_b \in A_\mathbb{Q}$ with $a \neq b$ would say that two distinct roots of a separable polynomial are equal.

For (2)⇒(1), let $H = \mathrm{Stab}_G(i_0)$, so that $\mathbb{Q}^\Omega \cong \mathbb{Q}[G/H] =: M$ is a direct summand of the regular module; $\mathbb{Q}[G]$ is semisimple, so M/N embeds in $\mathbb{Q}[G]$. Choose $L/\mathbb{Q}$ Galois with group G. By the normal basis theorem $L \cong \mathbb{Q}[G]$ as $\mathbb{Q}[G]$-modules, so there is a G-map $\psi\colon M \to L$ with kernel exactly N. Put $\alpha = \psi(e_{i_0})$ and $\alpha_x = \psi(e_x)$. For $g \in G$, $g\alpha = \alpha$ if and only if $e_{g(i_0)} - e_{i_0} \in N$, i.e. if and

only if $g(i_0) = i_0$; so $\mathrm{Stab}_G(\alpha) = H$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [G : H] = d$, the α_x are pairwise distinct, and $\psi(e_T) = \alpha_i + \alpha_j + \alpha_k = 0$. □

Proposition 2.1 is not new; it is Girstmair's, and we claim nothing in it. Girstmair [3] fixes a Galois extension L/K with group G and a subgroup H, lets $\sum_{\bar{s}} a_{\bar{s}}\bar{s} \in K[G/H]$ act on an $x \in L$ with $G_x = H$ by $\sum_{\bar{s}} a_{\bar{s}} s(x)$, and calls a subset $M \subseteq K[G/H]$ *admissible* when some such x is killed by every element of M (his Definition 1). He proves — by the normal basis theorem, exactly as in the proof above — that admissibility is equivalent to the purely group-theoretic condition that some $\mu \in K[G]$ with $G_\mu = H$ be killed in the same sense by M (his Proposition 1 and Definition 3). His Theorem 1 then characterises the admissible submodules $V \subseteq K[G/H]$ as those containing no $U(H') = K[G]\langle \bar{s} - \bar{1} : s \in H' \rangle$ with $H' > H$, and the remark following it restates that condition as: $\bar{s} - \bar{1} \notin V$ for every $s \in G \setminus H$. With $\Omega = G/H$ and $V = N = \mathbb{Q}[G]e_T$ that is precisely the difference-freeness test used here, and that remark is precisely why it suffices to test the differences with $a = 1$. Of that theorem Girstmair writes "In the main it is identical with Proposition 1" of his earlier paper (Manuscripta Math. **39** (1982), 81–97). What Proposition 2.1 adds to [3] is only the quantifier: Girstmair works inside a fixed L/K, whereas a statement about degrees over $\mathbb{Q}$ must also ask that G occur as a Galois group over $\mathbb{Q}$. [1] cites [3] for this framework.

Operationally, for a transitive $G \leq \mathrm{Sym}(\Omega)$: compute the G-orbits on 3-subsets of Ω; for one representative T of each orbit, spin e_T under the generators of G, maintaining a reduced row-echelon basis, which produces $N = \mathbb{Q}[G]e_T$ with $\dim N \leq d$; and declare that G *passes with* T when $\dim N < d$ and no $e_1 - e_b$ reduces to zero against that basis. Testing only the differences with $a = 1$ suffices, because N is G-invariant and G is transitive.

3. Degrees 28 and 35

Nothing in this section is machine-checked.

Theorem 3.1. *There is no algebraic number of degree* 28*, and none of degree* 35*, three of whose conjugates sum to zero.*

Proof. By the unconditional direction (1)⇒(2) of Proposition 2.1, such a number would produce a transitive group G of that degree and a 3-subset T with $\mathbb{Q}[G]e_T$ containing no difference $e_a - e_b$. All transitive permutation groups of degree 28 (1854 of them) and of degree 35 (407) are classified — the degrees up to 30 by Hulpke [13], the remaining degrees below 48 in the census of Holt and Royle [12] — and are available in the transitive groups library of GAP [14, 15]. The test described at the end of §2 was run, in exact rational arithmetic, on every one of them and on every orbit of 3-subsets. No pair (G, T) passes. □

The two counts 1854 and 407 are what the library reports and what those censuses record.

The proof is an exhaustive computation, and the two things that make such a proof believable are validation against known values and independent reimplementation. Both were done.

Validation. The same test was run at every degree below 23 for which the transitive groups are available, plus the two degrees at issue. Writing $h(d)$ for the number of transitive groups of degree d that pass with at least one 3-subset:

d	transitive groups	$h(d)$	expected
3	2	2	$t^3 - t - 1$
5	5	0	prime power, forbidden by p2
6	16	7	multiple of 3
9	34	25	multiple of 3
10	45	0	$2 \cdot 5$, forbidden by p2
12	301	108	multiple of 3
14	63	0	$2 \cdot 7$, forbidden by p2
15	104	58	multiple of 3
16	1954	0	the title result of [1]
20	1117	7	Stong's degree
21	164	84	multiple of 3
22	59	0	$2 \cdot 11$, forbidden by p2
28	1854	0	open in [1]
35	407	0	open in [1]

The two rows that matter are $d = 16$, where the test independently reproves the main theorem of [1] from nothing but the group library, and $d = 20$, where it independently rediscovers that Stong's degree is attainable. An earlier run of the same test covered thirty degrees $d \leq 38$ with no disagreement with any published value. At $d = 20$ the seven groups that pass are, in the numbering of the library, T20#5, 9, 15, 30, 35, 36, 65, with first passing triples $\{1, 3, 6\}$, $\{1, 3, 6\}$, $\{1, 4, 19\}$, $\{1, 4, 19\}$, $\{1, 3, 19\}$, $\{1, 3, 19\}$, $\{1, 4, 20\}$ and $\dim N = 16$ in every case; the first of them has order 20, is therefore regular, and is structurally Stong's example. Independently, Stong's polynomial was recomputed to 90 digits: it is irreducible and has exactly 20 zero-sum triples of roots.

Independent reimplementation. The results at $d = 16, 20, 28, 35$ were reproduced by a second, disjoint implementation which enumerates all $\binom{d}{3}$ subsets by mark-and-sweep rather than taking orbit representatives, builds the full point–block incidence matrix rather than spinning a module, uses the host system's own linear algebra rather than the reduction described above, asserts that the orbit sizes sum to $\binom{d}{3}$, and at $d = 20$ tests all $\binom{20}{2} = 190$ pairs (a, b) rather than only $a = 1$. The two implementations agree everywhere.

Remark 3.2 (where the obstruction sits). The computation also says *how* degrees 28 and 35 fail, and the answer is not that candidates are scarce. Call a G-orbit $\mathcal{T}$ of 3-subsets *linear* if any two of its members meet in at most one point; this is necessary for the criterion of Proposition 2.1, since $|T' \cap T''| = 2$ gives $1_{T'} - 1_{T''} = e_a - e_b \in N$. For a linear orbit, with $\lambda = 3|\mathcal{T}|/d$ the number of members through a point and Γ the graph joining two points when some member contains both, the point–block incidence matrix B (rows indexed by points) satisfies $BB^{\mathsf{T}} = \lambda I + A_\Gamma$, and the criterion becomes the requirement that $-\lambda$ be an eigenvalue of Γ whose eigenspace separates the points. At $d = 28$ there are 722 linear orbits and at $d = 35$ there are 390, with $\lambda \in \{3, 6, 9, 12\}$; in every one of them $\lambda I + A_\Gamma$ is non-singular. At $d = 20$, by contrast, some of the 204 linear orbits have $-\lambda = -3$ as an eigenvalue with multiplicity 4. So the obstruction at 28 and 35 is an eigenvalue statement about vertex-transitive graphs, which is why §9 names it as the route that could settle several degrees at once.

4. The arithmetic core of the degree-55 construction

Every statement of this section is machine-checked (§8). Throughout, $\mathrm{QR}(p)$ denotes the set of nonzero quadratic residues modulo p, and Φ_p the p-th cyclotomic polynomial. We state the identities for an arbitrary commutative ring R and an arbitrary $\zeta \in R$ with $\Phi_{11}(\zeta) = 0$, both because that is the natural generality and because it lets finite rings serve as witnesses and controls.

Lemma 4.1. $\mathrm{QR}(11) = \{1, 3, 4, 5, 9\}$*; this set is the cyclic group* $\langle 3 \rangle = \{3^l : l < 5\}$ *generated by* 3 *in* $(\mathbb{Z}/11)^\times$*; and* 3 *has order exactly* 5 *modulo* 11*. Consequently* $\sigma\colon \zeta_{11} \mapsto \zeta_{11}^3$ *generates* $\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\sqrt{-11}))$*, which is cyclic of degree* 5*.*

Proof. A finite computation in $\mathbb{Z}/11$: the image of squaring on $(\mathbb{Z}/11)^\times$ is $\{1,3,4,5,9\}$, the orbit $\{3^l : l<5\}$ is the same set, $3^5=1$, and $3^k\neq 1$ for $0<k<5$. The last sentence is then the standard description of the quadratic subfield of $\mathbb{Q}(\zeta_{11})$, which is $\mathbb{Q}(\sqrt{-11})$ because $11\equiv 3 \pmod 4$. □

Proposition 4.2. *Let R be a commutative ring and $\zeta\in R$ with $1+\zeta+\zeta^2+\cdots+\zeta^{10}=0$. Then*

$$\prod_{a\in \mathrm{QR}(11)} (1+\zeta^a) = (1+\zeta)(1+\zeta^3)(1+\zeta^9)(1+\zeta^5)(1+\zeta^4) = -1.$$

In particular the identity holds for a primitive 11-th root of unity in a domain, and so in $\mathbb{Q}(\zeta_{11})$.

Proof. The explicit factorisation in $\mathbb{Z}[X]$

$$(1+X)(1+X^3)(1+X^9)(1+X^5)(1+X^4)+1 = \Phi_{11}(X)\cdot Q(X),$$
$$Q = X^{12}-X^{10}+X^9+X^8-X^6+X^4+X^3-X^2-X+2,$$

evaluated at ζ. Over a domain, a primitive 11-th root of unity satisfies the hypothesis because $\Phi_{11}(X)=1+X+\cdots+X^{10}$. □

Proposition 4.2 is elementary, and we do not claim it as new; it also follows in a paragraph from $1+\zeta^a=(1-\zeta^{2a})/(1-\zeta^a)$ and the unit structure of the quadratic subfield, which is the argument of Proposition 5.4 below. A search of the cyclotomic-unit literature for the identity and for the sign law returned no statement of either, but the argument is of a kind that literature contains, and we assume both are classical.

The first of the two facts that carry the degree-55 construction is the following. Its content is not the identity of Proposition 4.2 but the use of that identity as a norm certificate at a degree listed as open in [1, §5].

Theorem 4.3 (the norm condition)**.** *Let $E=\mathbb{Q}(\zeta_{11})$, $F=\mathbb{Q}(\sqrt{-11})$, $\sigma\colon \zeta_{11}\mapsto\zeta_{11}^3$ and $\kappa=-(1+\zeta_{11})$. Then*

$$\mathrm{N}_{E/F}(\kappa)=\prod_{l=0}^{4}\sigma^l(\kappa)=\prod_{l=0}^{4}\bigl(-(1+\zeta_{11}^{3^l})\bigr)=1.$$

More generally, $(-(1+\zeta))(-(1+\zeta^3))(-(1+\zeta^9))(-(1+\zeta^5))(-(1+\zeta^4))=1$ in every commutative ring in which $1+\zeta+\cdots+\zeta^{10}=0$. This is exactly the hypothesis under which Hilbert's Theorem 90 for the cyclic degree-5 extension E/F produces $w\in E^\times$ with $\sigma(w)/w=\kappa$, that is, with $w+\zeta_{11}w+\sigma(w)=0$.

Proof. By Lemma 4.1 the exponents 3^l, $l<5$, run over $\mathrm{QR}(11)$, so the product is $(-1)^5\prod_{a\in\mathrm{QR}(11)}(1+\zeta^a)=(-1)(-1)=1$ by Proposition 4.2. The identification of $\prod_{l<5}\sigma^l$ with $\mathrm{N}_{E/F}$ is Lemma 4.1: $\langle\sigma\rangle$ is the full Galois group of E/F. □

The sign is doing real work, and it is not an accident of the number 11; see Proposition 4.6(i) and Proposition 5.4.

The second fact is what forces the orbit in §5 to have 55 elements and not fewer.

Theorem 4.4 (the freeness certificate)**.** *Let R be a commutative ring of characteristic zero and $\zeta\in R$ with $1+\zeta+\cdots+\zeta^{10}=0$. Then*

$$(1+\zeta)^{11}\neq -1, \qquad \textit{equivalently} \qquad \kappa^{11}\neq 1 \quad \textit{for } \kappa=-(1+\zeta).$$

So κ is not an 11-th root of unity.

Proof. A Bézout certificate in $\mathbb{Z}[X]$: with

$$U = 6556X^9+4554X^8+3003X^7+5126X^6+5126X^5+3003X^4+4554X^3+6556X^2+9607$$

there is $V\in\mathbb{Z}[X]$ with $U(X)\bigl((1+X)^{11}+1\bigr)+V(X)\Phi_{11}(X)=15709$. If $(1+\zeta)^{11}=-1$ then both bracketed quantities vanish at ζ, so $15709=0$ in R, contradicting characteristic zero. □

Remark 4.5 (the certificate is sharp about its hypothesis). Characteristic zero cannot be dropped, and the Bézout constant says exactly where the argument breaks: $15709 = 23 \cdot 683$. Modulo 23 the element $\zeta = 4$ satisfies $\Phi_{11}(\zeta) = 0$ and $\kappa = -(1+\zeta) = 18$ satisfies $\kappa^{11} = 1$, so there κ genuinely *is* an 11-th root of unity. No reduction to $\mathbb{F}_{23}$ can certify the freeness of the orbit.

Proposition 4.6 (controls)**.** (1) *The value of* $\prod_{a \in \mathrm{QR}(p)}(1+\zeta_p^a)$ *is not always* -1*: for* $p = 7$ *one has* $(1+\zeta)(1+\zeta^2)(1+\zeta^4) = +1$ *whenever* $\Phi_7(\zeta) = 0$*. Witnessed over* $\mathbb{F}_{29}$ *at* $\zeta = 16$*, a root of* Φ_7*, where the product is* 1 *and hence not* -1*. So the statement "the quadratic-residue product is* -1 *for every prime* $p \geq 7$*" is false, and the sign of Proposition 4.2 depends on* p*.*

(2) *The hypothesis* $\Phi_{11}(\zeta) = 0$ *is not vacuous over a finite ring:* $\zeta = 64$ *in* $\mathbb{Z}/67$ *satisfies* $\Phi_{11}(\zeta) = 0$*,* $\zeta \neq 1$ *and* $\zeta^{11} = 1$*, and there the product of Proposition 4.2 equals* $66 = -1$*.*

(3) *Proposition 4.2 is a statement about the quadratic residues and not about any five exponents: over* $\mathbb{Z}/67$ *at* $\zeta = 64$ *the product over* $\{1,2,3,4,5\}$ *is* 58*, neither* -1 *nor* $+1$*. And the sign is load-bearing: the* $\mathrm{QR}(11)$ *product is not* $+1$*, which is what makes* $(-1)^5 \cdot (-1) = 1$ *in Theorem 4.3.*

Proof. Each item is a finite evaluation in the named ring, together with, for the first item, the identity $(1+X)(1+X^2)(1+X^4) - 1 = X \cdot \Phi_7(X)$ in $\mathbb{Z}[X]$. □

5. Degree 55

Theorem 5.1 is not machine-checked; its two arithmetic ingredients, Theorems 4.3 and 4.4, are.

Theorem 5.1. *There is an irreducible* $f \in \mathbb{Q}[t]$ *of degree* 55 *with three distinct roots summing to zero. Consequently, by the scaling construction of* [1, §5]*, degree* $55s$ *is attainable for every* $s \geq 1$*; in particular degree* 110 *is attainable.*

Proof. Write $\zeta = \zeta_{11}$, $E = \mathbb{Q}(\zeta)$, $\sigma\colon \zeta \mapsto \zeta^3$, $F = E^{\langle\sigma\rangle}$ and $\kappa = -(1+\zeta)$.

(i) The extension. By Lemma 4.1, σ has order 5 and $\langle 3\rangle = \mathrm{QR}(11)$, so $F = \mathbb{Q}(\sqrt{-11})$ and E/F is cyclic of degree 5.

(ii) Hilbert 90. By Theorem 4.3, $\mathrm{N}_{E/F}(\kappa) = 1$. Since E/F is cyclic with group $\langle\sigma\rangle$, Hilbert's Theorem 90 gives $w \in E^\times$ with $\sigma(w)/w = \kappa = -(1+\zeta)$, that is,

$$w + \zeta w + \sigma(w) = 0.$$

(iii) The module. Let $G = \mu_{11} \rtimes \langle\sigma\rangle \cong C_{11} \rtimes C_5$, the non-abelian group of order 55, act $\mathbb{Q}$-linearly on $V = E \cong \mathbb{Q}^{10}$ with μ_{11} acting by multiplication and σ as the field automorphism; the relation $\sigma \circ (\cdot\zeta) \circ \sigma^{-1} = (\cdot\zeta^3)$ makes V a $\mathbb{Q}[G]$-module. It is $\mathbb{Q}$-irreducible of dimension 10, being already simple over $\mathbb{Q}[\mu_{11}] = \mathbb{Q}(\zeta)$, a field.

(iv) The orbit is free. Put $c_i = \sigma^i(w)/w = \prod_{l<i}\sigma^l(\kappa)$, so that $\mathrm{Stab}_G(w) = \{(a,i) : \zeta^a c_i = 1\}$. Since $w \neq 0$, the projection of the stabiliser to $\mathbb{Z}/5$ is injective, with image $S = \{i : c_i \in \mu_{11}\}$; and $c_{i+j} = c_i\sigma^i(c_j)$ together with $\sigma(\mu_{11}) = \mu_{11}$ makes S a subgroup of $\mathbb{Z}/5$. As 5 is prime, S is trivial as soon as $c_1 = \kappa \notin \mu_{11}$, and that is Theorem 4.4. Hence $\mathrm{Stab}_G(w) = 1$ and $|G \cdot w| = 55$.

(v) Realisation. G is solvable — it is metacyclic of order 55 — so by Shafarevich's theorem it occurs as a Galois group over $\mathbb{Q}$ [7]; take $L/\mathbb{Q}$ Galois with group G. By the normal basis theorem $L \cong \mathbb{Q}[G]$ as $\mathbb{Q}[G]$-modules, so the simple module V embeds G-equivariantly, $\psi\colon V \hookrightarrow L$. Put $\alpha = \psi(w)$. Then $\mathrm{Stab}_G(\alpha) = \mathrm{Stab}_G(w) = 1$ by (iv), so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 55$, the 55 elements $\psi(g \cdot w)$ are the conjugates of α, and $\psi(w) + \psi(\zeta w) + \psi(\sigma(w)) = 0$. The three are pairwise distinct because $\zeta \neq 1$ and, by Theorem 4.4, $\kappa \notin \mu_{11}$, so $\kappa \neq 1$ and $\kappa \neq \zeta$. The minimal polynomial of α is the required f. The final assertion is the scaling construction quoted in §1. □

Remark 5.2 (no explicit polynomial). Step (v) is not constructive: it produces L from a realizability theorem and ψ from the normal basis theorem. We therefore exhibit no explicit polynomial of degree 55, and we make no claim to have one. Producing one is a genuine problem — class field theory over $\mathbb{Q}(\sqrt{-11})$, or a rigidity construction — and we note in §9 what would be needed to turn such a polynomial into a fully verified proof of Theorem 5.1.

Remark 5.3 (why 35 and 55 differ). $55 = 5 \cdot 11$ with $5 \mid 11 - 1$, so the non-abelian group $C_{11} \rtimes C_5$ exists and carries the construction. For $35 = 5 \cdot 7$ neither $5 \mid 6$ nor $7 \mid 4$, so C_{35} is the only group of order 35. That is a heuristic and not a proof — transitive groups of degree 35 need not have order 35 — and the proof of Theorem 3.1 is the exhaustive run. But it is the right predictor to test, and §9 says how.

5.1. **A sign law, and an infinite family.** *Neither statement of this subsection is machine-checked, but the instances of Proposition 5.4 at $p = 11$ and $p = 7$ are* (Proposition 4.2 and Proposition 4.6(i)).

Proposition 5.4 (sign law)**.** *Let $p \geq 7$ be prime and ζ a primitive p-th root of unity. Then*

$$\prod_{a \in \mathrm{QR}(p)} (1 + \zeta^a) = \begin{cases} +1, & p \equiv 1 \text{ or } 7 \pmod 8, \\ -1, & p \equiv 3 \pmod 8, \end{cases}$$

and for $p \equiv 5 \pmod 8$ the product is not a rational integer.

Proof sketch. Write $A = \prod_{a \in \mathrm{QR}(p)}(1 - \zeta^a)$ and $B = \prod_{b \notin \mathrm{QR}(p) \cup \{0\}}(1 - \zeta^b)$. From $1 + \zeta^a = (1 - \zeta^{2a})/(1 - \zeta^a)$ the product equals $A/A = 1$ when 2 is a quadratic residue, i.e. when $p \equiv \pm 1 \pmod 8$, and B/A otherwise. For $p \equiv 3 \pmod 4$ complex conjugation interchanges residues and non-residues, so $B = \overline{A}$, while $AB = \Phi_p(1) = p$ and $A \in \mathbb{Q}(\sqrt{-p})$; writing $A = (u + v\sqrt{-p})/2$ with $u^2 + pv^2 = 4p$ forces $u = 0$ and $v = \pm 2$, i.e. $A = \pm\sqrt{-p}$, whence $B/A = \overline{A}/A = -1$. For $p \equiv 5 \pmod 8$ the quadratic subfield is real and the same argument does not close, consistently with the value not being rational. □

The law was checked numerically for every prime $5 \leq p \leq 200$; see §7.

Theorem 5.5. *Let $p \equiv 11 \pmod{24}$ be a prime for which $(p - 1)/2$ is also prime. Then there is an algebraic number of degree $d = p(p - 1)/2$ three of whose conjugates sum to zero, and d is divisible by neither 3 nor 20. The first values are*

$$p = 11, 59, 83, 107, 179 \;\longrightarrow\; d = 55, 1711, 3403, 5671, 15931,$$

and $d = 55$ is the only member of the family below 100.

Proof sketch. Run the proof of Theorem 5.1 with ζ_p in place of ζ_{11}, with $\sigma\colon \zeta_p \mapsto \zeta_p^g$ for g a generator of $\mathrm{QR}(p)$, of order $r = (p - 1)/2$, and with $\kappa_p = -(1 + \zeta_p)$. Since $p \equiv 11 \pmod{24}$ we have $p \equiv 3 \pmod 8$, so Proposition 5.4 gives $\prod_{a \in \mathrm{QR}(p)}(1 + \zeta_p^a) = -1$; as r is odd, $\prod_{l<r} \sigma^l(\kappa_p) = (-1)^r(-1) = 1$ and Hilbert 90 applies. The set $S = \{i : c_i \in \mu_p\}$ is again a subgroup of $\mathbb{Z}/r$, so it is trivial once r is prime and $\kappa_p \notin \mu_p$; and $\kappa_p \in \mu_p$ would give a vanishing sum $1 + \zeta_p + \zeta_p^k = 0$ of three p-th roots of unity, which needs $3 \mid p$. The orbit therefore has $pr = p(p - 1)/2$ elements and the group $\mu_p \rtimes \langle\sigma\rangle$ is metacyclic, hence solvable, hence realizable over $\mathbb{Q}$ [7]. Finally $p \equiv 11 \pmod{24}$ gives $p \equiv 2 \pmod 3$, so $3 \nmid d$; and $d = pr$ is odd, so $20 \nmid d$. □

Remark 5.6. Theorem 5.5 explains why only one of the sixteen open degrees falls to this construction. A systematic search over the natural generalisation — conductor n, an automorphism $\zeta_n \mapsto \zeta_n^m$ of order r, a divisor $e \mid n$ with $e \geq 3$, and $\kappa = -\zeta_n^{-c}(1 + \zeta_n^b)$ subject to $\prod_{l<r} \sigma^l(\kappa) = 1$ — was run for all conductors $n \leq 40$. Among the degrees it reaches that are divisible by neither 3 nor 20, the only ones below 120 are 55 and 110. None of $44, 52, 56, 65, 68, 70, 76, 77, 85, 88, 91, 92, 95$ is reached. That is evidence about where to spend effort, not a proof that those degrees are impossible.

6. The prime-power theorems of Baronėnas, Drungilas and Jankauskas, verified

Every statement of this section is machine-checked, and every one of them is a result of [1]*;* what is ours is only the verified form. The Galois situation enters the argument of [1] through three facts about the mod-p reduction $A \subseteq \mathbb{F}_p^{\Omega}$ of the lattice of integer relations among the roots: that a p-group acts transitively on Ω, that A is invariant, and that A is proper. We therefore state the theorems for an abstract transitive action. Throughout, a group H acts on $\mathbb{F}_p^{\Omega}$ by permuting coordinates, $(h \cdot u)(x) = u(h^{-1} \cdot x)$, which is the action of [1].

Theorem 6.1 (the p-group step)**.** *Let p be prime, let a p-group H act transitively on a finite nonempty set Ω, and let $W \subseteq \mathbb{F}_p^{\Omega}$ be a nonzero H-invariant subspace. Then the all-ones vector lies in W.*

Proof. Every nonzero element of W has additive order p, so p divides $|W|$; a p-group acting on a set of size divisible by p has a number of fixed points divisible by p (Lemma lefpte of [1], which cites Lemma 6.3 of Chapter I of [9]); the zero vector is fixed, so there are at least $p \geq 2$ fixed vectors and hence a nonzero one; a vector fixed by a transitive coordinate action is constant; scale. □

Theorem 6.2 (Theorem t1 of [1], mod-p form)**.** *Under the same hypotheses on H and Ω, let $A \subsetneq \mathbb{F}_p^{\Omega}$ be a proper H-invariant subspace. Then $\sum_{x\in\Omega} a_x = 0$ for every $a \in A$.*

Proof. Let $A^{\perp}$ be the orthogonal complement of A for the standard dot product. It is nonzero because A is proper, and it is H-invariant because the dot product is invariant under simultaneous permutation of both arguments. By Theorem 6.1 the all-ones vector lies in $A^{\perp}$, and pairing it against $a \in A$ gives $\sum_x a_x = 0$. □

Theorem 6.3 (Lemma l1 of [1], prime-power case)**.** *Let a finite group G act transitively on a set Ω with $|\Omega| = p^m$. Then every Sylow p-subgroup of G acts transitively on Ω.*

Proof. Fix $x \in \Omega$ and let $K = \mathrm{Stab}_G(x)$, so $[G : K] = p^m$. For a Sylow p-subgroup P of order p^n, the stabiliser $\mathrm{Stab}_P(x)$ embeds in K and has order p^j, so p^{m+j} divides $|G|$ and $m + j \leq n$. The P-orbit of x therefore has size $[P : \mathrm{Stab}_P(x)] = p^{\,n-j} \geq p^m = |\Omega|$. □

[1] states Lemma l1 as an immediate consequence of Lemma 2.2 of [10], and refers also to Theorem 3.4′ of [11]. Both numbered attributions are as printed in [1], and we have checked neither against its original.

Theorem 6.4 (Theorem t1 of [1], integer form)**.** *Let a p-group H act transitively on a finite nonempty Ω, let $A \subsetneq \mathbb{F}_p^{\Omega}$ be a proper H-invariant subspace, and let $c\colon \Omega \to \mathbb{Z}$ be an integer vector whose reduction modulo p lies in A. Then p divides $\sum_{x\in\Omega} c_x$.*

Proof. Theorem 6.2 applied to the reduction of c. □

With Ω the set of roots of an irreducible f of degree p^m, H a Sylow p-subgroup of the Galois group — transitive by Theorem 6.3 — and A the mod-p reduction of the relation lattice, Theorem 6.4 is Theorem t1 of [1]: if $\sum_j c_j\alpha_j = 0$ with $c_j \in \mathbb{Z}$ then $p \mid \sum_j c_j$. That last translation — the passage from f to the triple (G, Ω, A), including the properness of the reduced relation lattice — is *not* part of the verified development; see §8.

Theorem 6.5 (Theorem p2 of [1], prime-power half)**.** *Under the hypotheses of Theorem 6.4, suppose A contains the indicator vector of a triple (i, j, k) of points of Ω. Then $p = 3$. If instead A contains the signed vector $e_i + e_j - e_k$, the hypotheses are contradictory: for no prime p does a proper invariant subspace under a transitive p-group contain such a vector.*

Proof. The coordinate sums are 3 and 1 respectively, and Theorem 6.2 makes both vanish in $\mathbb{F}_p$: from $3 = 0$ we get $p \mid 3$, and $1 = 0$ is impossible. □

At $p = 2$, $m = 4$ the first assertion of Theorem 6.5 is the title result $d \neq 16$ of [1].

Remark 6.6 (why this section is here). Verifying someone else's published theorem needs a reason. The reason is that [1] states, in its acknowledgments, that the proofs of its Theorems t1 and t2 were supplied by an anonymous referee who reported having produced them with the assistance of a large language model, and that the authors independently verified and revised those proofs and take responsibility for their correctness. The argument was re-derived from scratch here and then checked by machine; nothing from the proofs printed in [1] was taken on authority. The verification confirms them, in the abstract form stated above.

Proposition 6.7 (controls for §6)**.** *Each of the three hypotheses of Theorem 6.2 is necessary, and the conclusion of Theorem 6.5 is sharp.*

(1) p-group*: S_3 acts transitively on a 3-set and preserves the proper line spanned by the all-ones vector, whose coordinate sum is $1 \neq 0$ in $\mathbb{F}_2$.*
(2) transitive*: the trivial group on a 2-set is a p-group for every p and preserves the proper line spanned by e_0, whose coordinate sum is $1 \neq 0$.*
(3) proper*: the full space $A = \mathbb{F}_p^{\Omega}$ is invariant under every group and contains e_0, whose coordinate sum is $1 \neq 0$, although the acting group can be a transitive 2-group.*
(4) *The hypotheses are jointly satisfiable with $A \neq 0$: the symmetric group on a 2-set is a transitive 2-group and the all-ones line is proper and invariant.*
(5) *The conclusion $p = 3$ is sharp: $3 = 0$ in $\mathbb{F}_q$ if and only if $q = 3$.*

Proof. Five finite verifications. □

7. The extent of the computation

We state which claims rest on exhaustive computation and how large each search was.

- **Theorem 3.1 is the exhaustive claim.** The search is: every transitive permutation group of degree 28 (1854 groups) and of degree 35 (407), and for each of them every orbit on 3-subsets — 722 linear orbits at degree 28 and 390 at degree 35 among many more in total (Remark 3.2) — with exact rational linear algebra and no floating point. The complete sweep reported in §3, that is all fourteen degrees of the validation table including 28 and 35, cost 80.0 CPU-seconds and under 1 GB of memory; degree 28 alone accounts for 40.5 seconds and degree 35 for 17.9. The classification of the transitive groups of those degrees is taken from the library [15] and is not reverified here.
- **Validation and reimplementation.** The fourteen-degree table of §3; an earlier run of the same test over thirty degrees $d \leq 38$; and a second, structurally disjoint implementation at $d = 16, 20, 28, 35$ (§3). No disagreement anywhere.
- **Stong's polynomial** was recomputed independently to 90 digits: irreducible, with exactly 20 zero-sum triples of roots. So was the list of sixteen open degrees, as $[2, 100]$ minus the multiples of 3, the multiples of 20, the prime powers and the numbers $2p^m$ with $p \geq 5$; it agrees with [1, §5] exactly.
- **Proposition 5.4** is proved, not computed; but its statement was also verified numerically for every prime $5 \leq p \leq 200$, in well under one CPU minute.
- **The verified statements rest on no search.** Lemma 4.1, Propositions 4.2, 4.6 and 6.7, Theorems 4.3, 4.4 and 6.1–6.5 are polynomial identities in $\mathbb{Z}[X]$, finite evaluations in $\mathbb{Z}/23$, $\mathbb{Z}/29$ and $\mathbb{Z}/67$, and group-theoretic arguments uniform in p. The largest objects among them are the degree-12 cofactor Q of Proposition 4.2 and the Bézout pair of Theorem 4.4.
- **The search of the literature** that frames the novelty claims was: the forward citations of [3] (twenty-five citing works, retrieved from two independent bibliographic databases which returned the same list, and read by title — the only algorithmic one, [6], computes the relation lattice of a *given* polynomial and does not decide existence at a fixed degree); the forward citations of [1] and of two neighbouring papers, all empty at the time of writing; the bibliography of [1] read in full, which is how [2] was found; [3] itself, read in full, which is what §2 reports; the cyclotomic-unit literature, searched for the identity of Proposition 4.2 and the law of Proposition 5.4, with no statement of either found; a repository search for existing formal developments, which returned none; and a search of the online encyclopedia of integer sequences for the list of sixteen open degrees and for the attainable degrees, which returned nothing. Read those as "not found", not as "new"; the positive evidence is the sentence quoted from [1, §5], and the qualification is the race described in §1.5.

8. Verification

Lemma 4.1, Propositions 4.2, 4.6 and 6.7, Theorems 4.3, 4.4, 6.1, 6.2, 6.3, 6.4 and 6.5, and Remark 4.5, have been machine-checked in Lean 4 [16] against Mathlib [17]: thirty-three theorems, and

one definition, in three files. The cyclotomic identities are stated for an arbitrary commutative ring and an arbitrary element killed by $1 + X + \cdots + X^{10}$, so that they specialise both to $\mathbb{Q}(\zeta_{11})$ and to the finite rings used as witnesses and controls, and they are discharged by the polynomial identities displayed in their proofs; the prime-power theorems are stated for an abstract transitive action of an abstract p-group, and their proofs use Mathlib's fixed-point congruence for p-groups and its duality for finite-dimensional spaces. There is no `sorry` and no added axiom anywhere in the development, and no step uses compiled evaluation: every finite check — the arithmetic in $\mathbb{Z}/23$, $\mathbb{Z}/29$ and $\mathbb{Z}/67$, and the exponent bookkeeping in $\mathbb{Z}/11$ — is performed by the kernel itself, so that the axiom closure of each statement is the standard propositional extensionality, quotient soundness and choice, and of several statements only the first two. Two things are deliberately outside the development and are marked as such above: the dictionary from an irreducible $f \in \mathbb{Q}[t]$ to the triple (G, Ω, A) used in §6, and everything in §2, §3 and §5 that depends on the classification of transitive groups or on Hilbert 90, the normal basis theorem and realizability. Repository reference to be added at submission.

9. What remains

Thirteen of the sixteen degrees are still open: $44, 52, 56, 65, 68, 70, 76, 77, 85, 88, 91, 92, 95$. We record what each natural route costs.

Degree 44 *is within reach of the same method.* The obstruction is a library boundary and nothing else: the transitive groups library used here covers degrees up to 38, while later versions cover degrees up to 47 and therefore include the 2113 transitive groups of degree 44 [12]. Extrapolating from the measured 40.5 seconds for the 1854 groups of degree 28, and allowing for the four times larger number of 3-subsets, the sweep at degree 44 should cost minutes rather than hours. Degrees 52 and above are out of reach of the library at any version, which stops at 47.

Five degrees might fall to one argument. Each of $65, 77, 85, 91, 95$ is a product qr of odd primes with $q < r$, $q \nmid r - 1$ and $r \nmid q - 1$, so C_{qr} is the only group of that order. If every transitive group of degree qr under those hypotheses contains a transitive abelian subgroup, all five fall at once, because a zero-sum triple of conjugates whose Galois group is abelian forces $3 \mid d$: the relation $w + g_1 w + g_2 w = 0$ gives $1 + \chi(g_1) + \chi(g_2) = 0$ for the relevant characters, and a vanishing sum of three roots of unity has ratios the primitive cube roots of 1. There is a free and decisive test of any such argument: it must also prove $d = 35$ impossible, which it is, and it must *fail* at $d = 55$, where $5 \mid 11 - 1$ and $C_{11} \rtimes C_5$ exists. An argument that does not separate 35 from 55 is wrong.

One theorem could settle all thirteen. By Remark 3.2 the question at a fixed degree is when a vertex-transitive graph whose edge set is partitioned into triangles, λ through each vertex, attains smallest eigenvalue exactly $-\lambda$; the census says this never happens at $d = 16, 28, 35$ and does happen at $d = 20$ with $\lambda = 3$. This is the theory of graphs with prescribed smallest eigenvalue. It is the only route that could close every remaining degree at once, and the only one that might fail entirely.

An explicit polynomial of degree 55. Remark 5.2 explains why we have none. If one is produced, the natural next step is to make the whole of Theorem 5.1 machine-checkable, for which the missing input is irreducibility: the Galois group $C_{11} \rtimes C_5$ has no element of order 55, so no prime makes f irreducible modulo p, and an Eisenstein presentation — obtainable by tuning the Hilbert 90 solution w, which is unique up to $F^\times$ — is the practical route.

References

[1] Ž. Baronėnas, P. Drungilas and J. Jankauskas, *No three algebraic conjugates of degree sixteen sum to zero*, e-print arXiv:2608.03583 [math.NT], submitted 4 August 2026. Cited throughout in version v1, which on 3 September 2026 was the only version on the arXiv record and carried no journal reference. Theorems `p1`, `p2`, `t1`, Lemma `l1` and §5 are used here; in v1 these print as Theorems 1, 2, 3 and Lemma 5.

[2] Ž. Baronėnas, P. Drungilas and J. Jankauskas, *No three algebraic conjugates of degree sixteen sum to zero*, e-print arXiv:2606.06222 [math.NT, math.CO], 4 June 2026 (v1, the only version). The earlier version of [1], with a different proof, using the classification of the vertex-transitive graphs on 16 vertices of degree 6; it treats no degree other than 16. Its Lemma `intro3` is the trace-zero condition quoted in §1.5.

[3] K. Girstmair, *Linear relations between roots of polynomials*, Acta Arith. **89** (1999), no. 1, 53–96; DOI 10.4064/aa-89-1-53-96. Corrigendum: Acta Arith. **110** (2003), 203; DOI 10.4064/aa110-2-10. Definition 1, Proposition 1,

Definition 3 and Theorem 1 of the 1999 paper are what §2 uses; Girstmair relates his Theorem 1 there to Proposition 1 of his *Linear dependence of zeros of polynomials and construction of primitive elements*, Manuscripta Math. **39** (1982), 81–97.

[4] A. Dubickas and C. J. Smyth, *Variations on the theme of Hilbert's Theorem 90*, Glasgow Math. J. **44** (2002), no. 3, 435–441; DOI 10.1017/S0017089502030082. Theorem 1.1 of that paper is the orbit-product criterion discussed in §1.5; the numbering was checked against the authors' preprint.

[5] A. Dubickas, *Problem 11123*, Amer. Math. Monthly **111** (2004), no. 10, 916; solution: A. Dubickas, C. J. Smyth and R. Stong, *Polynomials with three distinct zeros summing to zero: 11123*, Amer. Math. Monthly **113** (2006), no. 10, 941–942.

[6] T. Combot, *Computing linear relations between polynomial roots*, Math. Comp. **95** (2026), no. 358, 999–1022; DOI 10.1090/mcom/4081, published electronically 11 March 2025.

[7] I. R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Ser. Mat. **18** (1954), 525–578; English translation by E. Lehmer, Amer. Math. Soc. Transl. (2) **4** (1956), 185–237.

[8] A. Dubickas and J. Jankauskas, *Simple linear relations between conjugate algebraic numbers of low degree*, J. Ramanujan Math. Soc. **30** (2015), no. 2, 219–235.

[9] S. Lang, *Algebra*, revised 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002. [1] cites Lemma 6.3 of Chapter I of this book for the fixed-point congruence for p-groups used in Theorem 6.1.

[10] J. Bamberg, A. Bors, A. Devillers, M. Giudici, C. E. Praeger and G. F. Royle, *Orbits of Sylow subgroups of finite permutation groups*, J. Algebra **607** (2022), 107–133; DOI 10.1016/j.jalgebra.2021.06.017. Lemma 2.2 there is what [1] cites for its Lemma l1.

[11] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London, 1964, x+114 pp.

[12] D. F. Holt and G. F. Royle, *A census of small transitive groups and vertex-transitive graphs*, J. Symbolic Comput. **101** (2020), 51–60; DOI 10.1016/j.jsc.2019.06.006. The catalogue covers the transitive groups of degree less than 48 and the vertex-transitive graphs on at most 47 vertices. Graph data set: G. Royle and D. Holt, *Vertex-transitive graphs on fewer than 48 vertices*, Zenodo, 2020; DOI 10.5281/zenodo.4010122.

[13] A. Hulpke, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), no. 1, 1–30; DOI 10.1016/j.jsc.2004.08.002. With the author's dissertation *Konstruktion transitiver Permutationsgruppen* (RWTH Aachen, 1996), this is the source the library [15] names for its transitive groups of degrees 16–30, degree 28 among them.

[14] The GAP Group, *GAP — Groups, Algorithms, and Programming*, version 4.11.1 (2 March 2021).

[15] A. Hulpke, *TransGrp — Transitive Groups Library*, GAP package, version 2.0.6 (28 February 2020). The version used here provides degrees 2–31 and 33–38; its documentation attributes the groups of degrees 16–30 to [13] and the author's 1996 dissertation, degree 32 to J. Cannon and D. Holt, and degrees 34–46 to D. Holt, whose census with Royle is [12].

[16] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.

[17] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381; DOI 10.1145/3372885.3373824.