An Ennola duality for subgroups of groups of Lie type

Craven, David

DOI:
10.1007/s00605-022-01676-3

Document Version
Early version, also known as pre-print

Citation for published version (Harvard):
Craven, D 2022, 'An Ennola duality for subgroups of groups of Lie type', *Monatshefte fur Mathematik*, vol. 199, no. 4, pp. 785–799. https://doi.org/10.1007/s00605-022-01676-3

An Ennola duality for subgroups of groups of Lie type

David A. Craven, University of Birmingham,
d.a.craven@bham.ac.uk

28th October, 2021

Abstract

We develop a theory of Ennola duality for subgroups of finite groups of Lie type, relating subgroups of twisted and untwisted groups of the same type. Roughly speaking, one finds that subgroups H of $\mathrm{GU}_d(q)$ correspond to subgroups of $\mathrm{GL}_d(-q)$, where $-q$ is interpreted modulo $|H|$. Analogous results for types other than A are established, including for exceptional types where the maximal subgroups are known, although the result for type D is still conjectural. Let M denote the Gram matrix of a non-zero orthogonal form for a real, irreducible representation of a finite group, and consider $\alpha = \sqrt{\det(M)}$. If the representation has twice odd dimension, we conjecture that α lies in some cyclotomic field. This does not hold for representations of dimension a multiple of 4, with a specific example of the Janko group J_1 in dimension 56 given. (This tallies with Ennola duality for representations, where type D_{2n} has no Ennola duality with ${}^2\mathrm{D}_{2n}$.)

1 Introduction

In [4], Ennola described a conjectural way to extract the character table of $\mathrm{GU}_n(q)$ from that of $\mathrm{GL}_n(q)$, broadly by replacing 'q' by '$-q$' and making some other alterations. (This was proved in [6].) Ennola duality later became the principle that representation-theoretic information about twisted groups of Lie type can be inferred from the untwisted groups via the same method (although this is not the case for type D_n for even n). For example, the set of unipotent degrees of a group of Lie type satisfy this duality, with Ennola duality inducing a self-bijection if there is no corresponding twisted group.

The purpose of this note is to record a phenomenon that appears not to have been noticed before in the literature, that Ennola duality extends to subgroups. What we mean by this is that one can extract from the list of maximal subgroups of $\mathrm{SL}_n(q)$ (most of) the maximal subgroups of $\mathrm{SU}_n(q)$, again by replacing 'q' by '$-q$'.

The precise statement of Ennola duality for type A is given in Theorem 3.1 below, but this gives a flavour for the statement.

Theorem 1.1. *Let H be a finite group and let χ be an irreducible character for H of degree d. Suppose that q and q' are prime powers such that $q' \equiv -q \bmod |H|$, and q and $|H|$ are coprime. If H embeds in $\mathrm{GL}_d(q)$ with (Brauer) character χ then H embeds in $\mathrm{GU}_d(q')$ with (Brauer) character χ.*

Theorem 3.1 is precise about the integers that can be used instead of $|H|$ for the congruences, and can be used with tables such as those in [1] to immediately read off subgroups of $\mathrm{GU}_d(q)$. (If χ is real-valued and H embeds in $\mathrm{GL}_d(q)$, then it embeds in $\mathrm{GL}_d(q')$, $\mathrm{GU}_d(q)$ and $\mathrm{GU}_d(q')$ with the same character, so the content is for χ not real-valued.)

A similar statement, Proposition 3.2, holds for types B and C, but here H always embeds in $G(q')$ whenever it embeds in $G(q)$, with the same hypotheses. For now, type D remains somewhat more difficult to work with, and a form of Ennola duality holds, at least for integral representations (Theorem 3.7). For type D_{28} we give an example to show that there is no number m for which the embedding of the Janko group J_1 into $\mathrm{GO}^+_{56}(q)$ depends only on the congruence of q modulo m. However, for D_n with n odd, we have found no similar examples, and if Conjecture 3.9 is true there are no such example. For D_n and n odd, if Conjecture 3.9 holds (and it does for all integral representations) we simply replace q by $-q$ modulo some integer to switch between GO^+ and GO^-, as with other types.

Notice that this example of J_1 in dimension 56 also throws up another point. It is known that the p-modular reduction can interact badly with algebraic conjugacy when p divides the order of a finite group. This example shows similar behaviour even when p is prime to the order, and in particular means that the type of symmetric bilinear form over $\mathbb{F}_q$ cannot, in a strict sense, be deduced from the character table of a finite group.

There is also no complete proof for exceptional groups. All known subgroups of exceptional groups satisfy the same Ennola-like behaviour, but the maximal subgroups of $E_8(q)$ are not yet known, and for $E_7(q)$ the conjectured list in [3] (see Table 4.4 below) is not known to be complete. We describe the version of Ennola duality that exists for these groups in Section 4. Again, this boils down to replacing q in the tables in Section 4 with $-q$ to obtain the table of the twisted version if there is one, or the same table again if there is not.

Although it does not appear that the ideas in this work have appeared in this generality before, the work on classifying low-dimensional subgroups of classical groups, particularly orthogonal groups, in [1, 9, 10], is distinctly reminiscent of it (if independent, as the author only learned of their ideas after writing this). For example [1, Lemma 4.9.39], which was mentioned (possibly for the first time in the literature) in [11], is given a more general treatment in Proposition 3.4. A posteriori, one might see this article as offering a general framework for the results in those papers.

In the next section we collect some preliminary definitions and results, and discuss fields of values for characters and embedding into linear groups over finite fields. The section after considers classical groups, and Section 4 deals with exceptional groups.

We have written this paper to minimize the use of class field theory, although for groups of type D it seems difficult to prove anything meaningful without at least basic results from it. This means a few preliminary lemmas are included that are standard in class field theory, but we feel that making the paper as self-contained as possible is worth it.

The author would like to thank Gunter Malle for reading through a preliminary version of the manuscript, and particularly Elie Studnia for providing a proof of Proposition 3.6(i).

This work was partially supported by a Royal Society University Research Fellowship.

2 Preliminaries, Brauer characters and fields of values

In this article, H denotes a finite group and χ is an irreducible ordinary character of H. Write $d = \chi(1)$. Without loss of generality in this article, we may assume that χ is faithful. If $p \nmid |H|$ is a prime, then the reduction modulo p of χ is always an irreducible Brauer character, and we will often conflate χ with this Brauer character, and say that a representation in characteristic p has character χ, when we mean has character the reduction modulo p of χ. (We would never do this for $p \mid |H|$.) Whenever p is a prime, let

k denote an algebraically closed field of characteristic p. Note that, in this article, for simplicity we will not consider representations over fields of characteristic dividing $|H|$, but the results hold whenever the reduction remains irreducible, at least for p odd. (Orthogonal groups in characteristic 2 would need to be treated separately.) For q a power of p, let F_q denote the field automorphism of k given by $x \mapsto x^q$. Given p, let $\bar{H}$ denote a copy of H in $\mathrm{GL}_d(k)$ with Brauer character χ, and note that $\bar{H}$ is necessarily an absolutely irreducible subgroup of $\mathrm{GL}_d(q)$ whenever $\bar{H}$ is a subgroup of it.

The meanings of the terms $\mathrm{Sp}_d(q)$, $\mathrm{GO}_d^+(q)$, and so on, are the full symmetry group of the appropriate form in $\mathrm{GL}_d(q)$. The *exponent* of a finite group is the lowest common multiple of all orders of all elements of it. Let $\zeta_n = \mathrm{e}^{2\pi \mathrm{i}/n}$ be a primitive nth root of unity in $\mathbb{C}$.

The first lemma is well known, and gives the minimal field of definition for a finite group embedding in characteristic $p \neq 0$. (The case for characteristic 0 has no easy answer.) See, for example, [5, Section 5].

Lemma 2.1. *Let $p \nmid |H|$ be a prime. The subgroup $\bar{H}$ of $\mathrm{GL}_d(k)$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$ if and only if the traces (evaluated in k) of all elements of $\bar{H}$ lie in $\mathbb{F}_q$. Thus H embeds in $\mathrm{GL}_d(q)$ with character χ if and only if, under a map sending a primitive $|H|$th root of unity over $\mathbb{C}$ to one over k, the Brauer character values of χ lie in $\mathbb{F}_q$.*

In particular, $\bar{H}$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$ for q such that the exponent of H divides $q-1$.

The second statement follows from the first since the trace of a matrix is the sum of its eigenvalues, and the eigenvalues are roots of unity of order dividing the exponent of H.

There is a subtlety with this lemma, that is not often explicitly mentioned. Let $p = 5$ and suppose that A is a 7-dimensional matrix with eigenvalues ω six times, and ω^2 once, where $\omega^3 = 1$. The trace, -1, certainly lies in $\mathbb{F}_5$, but there is no matrix in $\mathrm{GL}_7(5)$ with those eigenvalues. So the claim is certainly only true for *irreducible* Brauer characters, and tells us something about the eigenvalues of semisimple elements in irreducible subgroups of $\mathrm{GL}_d(k)$, where k has characteristic p.

Lemma 2.2. *Let A be a matrix in $\mathrm{GL}_d(k)$. The multiset of eigenvalues of A is invariant under the Frobenius endomorphism F_q if and only if A is conjugate to an element of $\mathrm{GL}_d(q)$.*

For a proof, a semisimple conjugacy class of $\mathrm{GL}_d(k)$ is determined by its multiset of eigenvalues. The Frobenius endomorphism permutes the classes, and this action is determined by its action on the eigenvalues. Thus a conjugacy class is stabilized by the Frobenius endomorphism if and only if the multiset of eigenvalues is. Now apply, for example, [7, Theorem 26.7] to obtain a semisimple element of $\mathrm{GL}_d(k)$ fixed by the Frobenius endomorphism whenever the class is stabilized by it.

So Lemma 2.1 tells us that, for a simple kH-module M, M is realizable over $\mathbb{F}_q$ if and only if the multiset of eigenvalues of each element of H on M is invariant under F_q. The same will therefore be true of their lifts to $\mathbb{C}$ when performing the Brauer character construction, that they are invariant under $\zeta_n \mapsto \zeta_n^q$, where ζ_n is an appropriate root of unity and the map is on the field $\mathbb{Q}(\zeta_n)$.

We now give a fundamental definition for this article.

Definition 2.3. For a given H and χ, a positive integer n is a *defining modulus* if, whenever q is a prime power congruent to 1 modulo n (and prime to $|H|$), the corresponding subgroup $\bar{H}$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$.

This is closely related to the concept of a defining modulus in class field theory: the defining modulus of a character is the defining modulus of the smallest subfield of $\mathbb{C}$ containing its character values.

It is not obvious from this definition, but defining moduli appear in all tables of maximal subgroups of classical groups. The next lemma teases out the first relevance for the problem.

Lemma 2.4. *An integer n is a defining modulus for H and χ if and only if the values of χ lie in the nth cyclotomic field $\mathbb{Q}(\zeta_n)$*

Proof. Let k be an algebraically closed field of characteristic $p \mid q$, and let $n' = \operatorname{lcm}(|H|, n)$. Abbreviate ζ_n by ζ and $\zeta_{n'}$ by ξ.

Suppose first that the character values of χ lie in $\mathbb{Q}(\zeta)$. Let q (prime to $|H|$) be a prime power congruent to 1 modulo n. In order to show that $\bar{H}$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$, it suffices (by the discussion after Lemma 2.2) to show that the Brauer character values of χ are fixed under map $\xi \mapsto \xi^q = \xi$. This is obviously true, and so the result follows.

For the converse, suppose that n is a defining modulus. Since $\chi(x)$ lies in $\mathbb{Q}(\xi)$ for all $x \in H$, it suffices to show that $\chi(x)$ is centralized by all elements of $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}(\zeta))$. Viewed as maps in $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, these are given by $\xi \mapsto \xi^a$ for $a \equiv 1 \bmod n$. Let q (prime to $|H|$) be a prime power congruent to a modulo n', and note that $q \equiv 1 \bmod n$. Thus by assumption $\bar{H}$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$, so the lifts of the eigenvalues of elements of $\bar{H}$ to $\mathbb{Q}(\xi)$ are invariant under the map $\xi \mapsto \xi^q = \xi^a$. But this is what is required, and the other direction holds. □

This alternative interpretation of defining moduli has the following easy consequence.

Corollary 2.5. *All defining moduli are multiples of the smallest defining modulus, called the* conductor*. Furthermore, a positive integer m is a defining modulus if and only if* $\gcd(m, |H|)$ *is.*

This is proved simply by invoking Lemma 2.4 and taking the intersections of the appropriate cyclotomic fields. Like defining moduli, the name 'conductor' comes from class field theory.

We now introduce defining residues, which explains the choice of this definition. Given H and χ, and a defining modulus n, let I_n denote the set of all i between 1 and $n-1$, and prime to n, such that the field isomorphism on $\mathbb{Q}(\zeta_n)$ induced by $\zeta_n \mapsto \zeta_n^i$ fixes each value of χ. The set I_n is called the set of *defining residues*. Notice that the set of defining residues is a subgroup of the unit group $\mathbb{Z}_n^\times$. We often abuse terminology and say that an integer a lies in I_n if $a \bmod n$ lies in I_n. Particularly, we do this with negative numbers, so $-i$ lies in I_n for $1 \leqslant i \leqslant n-1$ to mean $n - i \in I_n$.

Theorem 2.6. *For a fixed H and χ, let n be a defining modulus dividing $|H|$. For all prime powers q (prime to $|H|$), $\bar{H}$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$ if and only if the congruence of q modulo n appears in I_n. In particular, if q' (prime to $|H|$) is another prime power and $q \equiv q' \bmod n$, then one may embed H in $\mathrm{GL}_d(q)$ with character χ if and only if one can do the same with $\mathrm{GL}_d(q')$.*

Proof. This proof has the same ideas as that of Lemma 2.4, so we are a little briefer this time. The subgroup $\bar{H}$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$ if and only if the eigenvalues of elements of $\bar{H}$, lifted to $\mathbb{Q}(\zeta_n)$, are invariant under the map $\zeta_n \mapsto \zeta_n^q$. This statement is equivalent to the statement that $q \bmod n$ lies in I_n by definition of I_n, and thus $q \bmod n$ lies in I_n if and only if $\bar{H}$ is conjugate to a subgroup of $\mathrm{GL}_d(q)$, as claimed. □

Finally, we need a well-known result on when $\bar{H}$, which is already conjugated to lie in $\mathrm{GL}_d(q)$, also lies in another classical group. Basically, the answer is 'whenever they stabilize the appropriate form', so there is no need to worry that we might need to increase q to find $\bar{H}$ inside the classical group. Note that, since

groups of odd order have no non-trivial real-valued characters, we may assume that $2 \mid |H|$ when talking about real-valued characters, so q is always odd.

Lemma 2.7. *Suppose that χ is real-valued and $d > 1$, and hence q is odd.*

(i) *If d is odd then $\bar{H}$ is conjugate to a subgroup of $\mathrm{GO}_d(q)$ if and only if it is conjugate to a subgroup of $\mathrm{GL}_d(q)$.*

(ii) *If d is even and χ has indicator -1, then $\bar{H}$ is conjugate to a subgroup of $\mathrm{Sp}_d(q)$ if and only if it is conjugate to a subgroup of $\mathrm{GL}_d(q)$.*

(iii) *If d is even and χ has indicator $+1$, $\bar{H}$ is conjugate to a subgroup of exactly one of $\mathrm{GO}_d^+(q)$ and $\mathrm{GO}_d^-(q)$ via χ if and only if it is conjugate to a subgroup of $\mathrm{GL}_d(q)$.*

Proof. Since the exterior or symmetric square of a simple module has a unique trivial submodule over any field, any module with character H stabilizes a unique bilinear form (quadratic form for $p = 2$). This is enough to prove existence of H in symplectic and orthogonal groups.

In the third case, the uniqueness of the form means that H cannot lie in both plus and minus type orthogonal groups. □

There is a nice way to see whether a character is real-valued from the set I_n.

Lemma 2.8. *Let n be a defining modulus and I_n the defining residues. The following are equivalent:*

(i) *χ is real-valued;*

(ii) *-1 lies in I_n;*

(iii) *I_n is closed under taking negatives, i.e., $-i \in I_n$ whenever $i \in I_n$.*

Proof. The equivalence of the second and third statements follows immediately from the fact that I_n a group under multiplication. Also, -1 lies in I_n if and only if the map $\zeta_n \mapsto \zeta_n^{-1}$ (i.e., complex conjugation) stabilizes χ. But this is true if and only if χ is real-valued. □

3 Ennola duality for classical groups

Our first goal is to state and prove Ennola duality for subgroups of GL and GU. It is not quite as simple as replacing q by $-q$, but it is close. If χ is real-valued then H embeds in a symplectic or orthogonal group, hence embeds in both $\mathrm{GL}_d(q)$ and $\mathrm{GU}_d(q)$ whenever it embeds in one of them. Thus we are most interested in the case where χ is not real-valued, or equivalently that there exists $i \in I_n$ such that $-i \notin I_n$ by Lemma 2.8.

Theorem 3.1. *Let H be a finite group and let χ be a faithful irreducible character of H. Let n be a defining modulus and I_n the set of defining residues. For a power q of a prime p not dividing $|H|$, the group H embeds in $\mathrm{GU}_d(q)$ via χ if and only if $-q \bmod n$ lies in I_n.*

Proof. By the remark preceding the theorem, we may assume that χ is no real-valued, i.e., $-1 \notin I_n$. By assumption the eigenvalues of $x \in \bar{H}$ are permuted by the map $\zeta_n \mapsto \zeta_n^i$, but not by the map $\zeta_n \mapsto \zeta_n^{-i}$, the composition of the former map and $\zeta_n \mapsto \zeta_n^{-1}$. Hence $\zeta_n \mapsto \zeta_n^{-i}$ maps χ to $\bar{\chi}$, the complex conjugate, of χ, and $\bar{\chi} \neq \chi$. Since the graph automorphism acts as inverse transpose, for $q \equiv -i \bmod n$, the composition σ of F_q with the graph automorphism stabilizes χ.

This is enough to prove that $\bar{H}$ is conjugate to a subgroup of $\mathrm{GU}_d(q)$. To see this, note first that, since $\bar{H}$ is unique up to conjugacy subject to having character χ, σ stabilizes the $\mathrm{GL}_d(k)$-conjugacy class containing $\bar{H}$, so normalizes some member of it by [7, Theorem 21.11]. Then we apply [1, Lemma 1.8.6], which states that σ must therefore act as some element of $\mathrm{GL}_d(k)$ that normalizes (a conjugate of) $\bar{H}$. Then we apply [7, Corollary 21.8], which implies that σ then centralizes some conjugate of $\bar{H}$, and thus some conjugate of $\bar{H}$ lies inside the fixed points of σ, namely $\mathrm{GU}_d(q)$.

To see the converse, if both F_q and the product with the graph automorphism centralize (a conjugate of) H then the graph automorphism acts as an element of the normalizer in GL_d of H. Such an element stabilizes χ, but the graph automorphism maps χ to its complex conjugate. Thus χ is real-valued and so $-1 \in I_n$, a contradiction. □

We now move on to the other classical groups. Types B and C are easy, since there is no twisted type to be concerned about.

Proposition 3.2. *Given H and χ, suppose that χ is real-valued. Furthermore, suppose that χ has indicator -1, or $\chi(1)$ is odd. If n is a defining modulus and I_n the defining residues, then $i \in I_n$ if and only if $-i \in I_n$.*

Consequently, if $q \equiv -q' \bmod n$, and q and q' are prime powers, H embeds in $\mathrm{Sp}_d(q)$ if and only if H embeds in $\mathrm{Sp}_d(q')$ (via χ), and similarly for $\mathrm{GO}_d(q)$ and $\mathrm{GO}_d(q')$.

The proof is immediate, from Lemma 2.8.

3.1 Groups of type D

Suppose that χ has Frobenius–Schur indicator $+1$, so that χ is the character of a real representation. Let n be a defining modulus and $q \bmod n \in I_n$. Then $\bar{H}$ is conjugate to a subgroup of $\mathrm{GO}^{\varepsilon}_d(q)$ for some $\varepsilon = \pm 1$ by Lemma 2.7, but deciding which is a significant issue. It comes down to knowing the determinant of the matrix of scalar products for the bilinear form stabilized by $\bar{H}$.

Definition 3.3. Given H, and χ with indicator $+1$, a defining modulus m is a *discriminating modulus* if the set I_m can be partitioned into two disjoint subsets $I_m^+ \cup I_m^-$, such that $\bar{H}$ is conjugate to a subgroup of $\mathrm{GO}^+_d(q)$ if and only if $q \bmod m$ lies in I_m^+. The sets I_m^+ and I_m^- are the positive and negative *discriminating residues*.

If χ is afforded by a real representation then not all defining moduli are discriminating moduli. This can be seen most obviously with representations over $\mathbb{Z}$, where 1 is a defining modulus (assuming q is odd), but certainly there are subgroups of $\mathrm{GO}^-_d(q)$ that come from $\mathbb{Z}$-representations, such as the alternating group A_7, which lies in $\mathrm{GO}^-_6(q)$ for $q \equiv 3, 5, 6 \bmod 7$. As with defining moduli, the set of discriminating moduli is of the form $m\mathbb{N}$ for some minimal modulus. However, it is not clear that discriminating moduli always exist. To examine this problem we need a bit more background.

First, changing basis for the bilinear form multiplies the determinant by a square, so we can only determine the determinant up to a square. For example, if the determinant lies in $\mathbb{Z}$, then it can be given by a square-free integer m. A representative of the determinant in F/F^2 (where the matrix is defined over F) is called the *discriminant* of the form. For fields $\mathbb{F}_q$, the set $|\mathbb{F}_q/\mathbb{F}_q^2|$ has order 2, so the determinant is either a square or a non-square.

Over $\mathbb{Q}$, the minimal square-free integer m must be odd: the reduction modulo 2 of the matrix M of the form must be the matrix of a symmetric, hence skew-symmetric bilinear form, and so modulo the radical it has even dimension. Thus an even number of eigenvalues must be even, and $4 \nmid m$. Also, m is positive: by

extending the field to $\mathbb{R}$, we may change basis so that the matrix of the form is diagonal with entries ± 1. The subspace spanned by basis elements with norm 1 yields an invariant subspace, as does that with norm -1. Thus one of these subspaces is zero as the subgroup $\bar{H}$ of $\mathrm{GL}_d(k)$ is irreducible. But the dimension d is even, so the determinant is always positive. The statement that all eigenvalues of M must be positive (or all must be negative) holds for any H and χ, not just $\mathbb{Z}$-representations.

One can also see that if m is divisible by a prime r then either all eigenvalues of the matrix are divisible by r, in which case we can multiply by a scalar to remove them, or the reduction modulo r of the form has a non-zero radical. Thus, in particular, the reduction modulo r of χ cannot be an irreducible Brauer character. This first proves that $m \mid |H|$, and second it even excludes certain primes that divide $|H|$.

We now need the discriminant of the form for the two orthogonal groups $\mathrm{GO}_d^\varepsilon(q)$. If d is divisible by 4, or $d \equiv 2 \bmod 4$ and $q \equiv 1 \bmod 4$ then the discriminant for $\mathrm{GO}_d^+(q)$ is a square, and if $d \equiv 2 \bmod 4$ and $q \equiv 3 \bmod 4$ then the determinant is a non-square. The discriminant for $\mathrm{GO}_d^+(q)$ is a square in $\mathbb{F}_q$ if and only if the discriminant for $\mathrm{GO}_d^-(q)$ is a non-square. Thus if $\bar{H}$ is a subgroup of $\mathrm{GL}_d(q)$ and we can determine the discriminant for the invariant bilinear form then we know which of the two orthogonal groups $\bar{H}$ embeds into.

Ennola duality for type D_n with n odd goes through as before, at least if the discriminant over $\mathbb{Q}$ is an odd positive integer. (This therefore includes the case where the representation is over $\mathbb{Z}$.) Although this proposition is later subsumed into a more general result, representations over $\mathbb{Z}$ are common enough for it to be useful to have the formulae derived in the proof.

Proposition 3.4. *Let H and χ be given, and suppose that χ has indicator $+1$, arising from a representation over $\mathbb{Z}$. Suppose that $d \equiv 2 \bmod 4$, and that the discriminant of the form is an odd positive integer m. Let n be a multiple of $4m$ such that n is a defining modulus for χ.*

(i) *The number n is a discriminating modulus for H and χ.*

(ii) *The set I_n^+ is a subgroup of index 2 in I_n and $I_n^- = \{-i : i \in I_n^+\}$.*

Proof. Let q be a power of a prime $p \nmid |H|$. In order to determine the discriminant of the form for $\bar{H}$, which is the reduction modulo p of m, it suffices to check whether m has a square root in $\mathbb{F}_q$. If q is an even power of p, this is always the case. If q is an odd power of p, then this is equivalent to whether m has a square root in $\mathbb{F}_p$, which is given by the Legendre symbol (m/p). Note we will also need to take into account the discriminant for the standard form for $\mathrm{GO}_d^\varepsilon(q)$, so we need the congruence modulo 4 as well, which is the Legendre symbol $(-1/p)$. Thus $\bar{H}$ is conjugate to a subgroup of $\mathrm{GO}_d^+(q)$ if and only if $q \bmod m$ lies in I_m, and either q is a square or $(-m/p) = 1$.

We consider the second condition. Writing $m = m_1 \dots m_r$ with each m_i prime, by quadratic reciprocity,

$$\left(\frac{-m}{p}\right) = (-1)^{(p-1)/2} \prod_{i \in I} \left(\frac{m_i}{p}\right) = (-1)^{(p-1)/2} (-1)^{(m-1)(p-1)/4} \prod_{i \in I} \left(\frac{p}{m_i}\right) = (-1)^{(m+1)(p-1)/4} \prod_{i \in I} \left(\frac{p}{m_i}\right). \tag{3.1}$$

If $m \equiv 3 \bmod 4$ then this reduces to $\prod(p/m_i)$, and whether this is 1 depends only on the congruence of p modulo $\prod m_i = m$. Furthermore, this set of congruences is a subgroup of index 2 in $\mathbb{Z}/m\mathbb{Z}^\times$, and contains all squares in $\mathbb{Z}/m\mathbb{Z}^\times$ (so $q \bmod m$ lies in it whenever q is a square). Also, $p \bmod m$ lies in this set if and only if p^i lies in it for any odd i. Since n is a multiple of m, the same holds modulo n as well. Thus I_n^+ is well defined, and has index 2 in I_n.

Finally, if $p \equiv -1 \bmod n$ then each $(1/m_i)$ is 1 if $m_i \equiv 1 \bmod 4$, and -1 if $m_i \equiv 3 \bmod 4$. Thus -1 does not lie in I_n^+ since $m \equiv 3 \bmod 4$, and the result holds.

Thus we assume that $m \equiv 1 \bmod 4$, so the formula above reduces to $(-1)^{(p-1)/2} \prod_i (p/m_i)$. Now whether this is 1 depends only on the congruence of p modulo $4m$. Again, this set is a subgroup of index 2 in $\mathbb{Z}/m\mathbb{Z}^\times$, contains all squares, and $p \mod 4m$ lies in the set if and only if $p^i \bmod m$ lies in it for any odd i. Again, if $p \equiv -1 \bmod 4m$ then $p \equiv 3 \bmod 4$, so the sign at the front is -1, and the product evaluates to -1. Thus $-1 \notin I_n^+$. This completes the proof. □

If $4 \mid d$ then the same proof works, but we do not obtain that -1 lies in I_n^-, and so I_n^+ has index at most 2 in I_n. (An example where $I_n^+ = I_n$ is $\Omega_8^+(2)$, which lies in $\Omega_8^+(p)$ for all primes, and not in $\Omega_8^-(p)$.) The formula for whether $i \in I_n$ lies in I_n^+ now becomes

$$\left(\frac{m}{p}\right) = \prod_{i \in I} \left(\frac{m_i}{p}\right) = (-1)^{(m-1)(p-1)/4} \prod_{i \in I} \left(\frac{p}{m_i}\right). \tag{3.2}$$

We see in the proof of Proposition 3.4 that the important thing was that the square root of the discriminant lies in $\mathbb{F}_q$ if and only if q lies in some set modulo some integer. This motivates the following definition.

Definition 3.5. Given H and ρ, let α denote the determinant of a scalar product matrix of the form stabilized by ρ. We say that ρ is *root cyclotomic* if the square root of α lies in some cyclotomic field, i.e., $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ is an abelian extension.

If ρ is root cyclotomic then we can prove a version of Ennola duality for H even when ρ is not over the integers. The proof uses class field theory, which appears not to be avoidable at this point.

First, we need to extend results from class field theory about splitting of polynomials from fields $\mathbb{F}_p$ to fields $\mathbb{F}_q$, which of course is of interest to us here. This does not appear to be a standard part of class field theory, so we have to do it ourselves here.

Proposition 3.6. *Let α be an element of a cyclotomic field. Let f be its minimal polynomial over $\mathbb{Z}$, and m be minimal such that α lies in the mth cyclotomic field. Suppose that the leading coefficient of f is only divisible by primes dividing m. Suppose that p and p' are primes not dividing m, and let q and q' be powers of p and p' respectively.*

(i) *If $q \equiv q' \bmod m$, then the polynomial f splits over $\mathbb{F}_q$ if and only if it splits over $\mathbb{F}_{q'}$.*

(ii) *The polynomial f splits over $\mathbb{F}_q$ if and only if its has a root in $\mathbb{F}_q$.*

Proof. Let $m' = \operatorname{lcm}(q-1, m)$, and L be the m'th cyclotomic field. Let $K = \mathbb{Q}(\alpha)$. Let $\mathfrak{p}$ be some prime ideal of L above p, let $\mathcal{O}_p$ be the local ring and k the residue field. Write

$$f(x) = a \prod_{i=1}^{n} (x - x_i),$$

where $x_i \in \mathcal{O}_p \cap K$ and a lies in $\mathbb{Z}_{(p)}^\times$.

The polynomial f splits over $\mathbb{F}_q$ if and only if the image of each of the x_i in k lies in $\mathbb{F}_q$, and this is true if and only if, for each i, the images of x_i and x_i^q in k are the same. Letting $q = p^r$, let σ denote the Frobenius at p, so that f splits over $\mathbb{F}_q$ if and only if the images of x_i and $\sigma^r(x_i)$ are the same in k.

Note that $\sigma^r(x_i)$ is some root of f, hence $\sigma^r(x_i) = x_j$ for some j. Since f is separable modulo p by assumption on p (as the only ramified primes divide m), the images of the x_i in k are all distinct. Thus f splits in $\mathbb{F}_q$ if and only if σ^r fixes all of the x_i, so it lies in $\operatorname{Gal}(L/K)$.

But σ^r lies in $\mathrm{Gal}(L/\mathbb{Q})$, and is dependent only on its action on $\zeta_{m'} = \mathrm{e}^{2\pi\mathrm{i}/m'}$, and of course $\sigma^r(\zeta_{m'}) = \zeta_{m'}^q$, which is in turn only dependent on the congruence of q modulo m'. By the Chinese remainder theorem, this depends only on q modulo m, i.e., whether f splits in $\mathbb{F}_q$ depends only on the congruence of q modulo m.

This completes the proof of (i).

For the proof of (ii), note that, since $K/\mathbb{Q}$ is an abelian extension, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts regularly on the roots. In particular, all elements of $\mathrm{Gal}(K/\mathbb{Q})$ act fixed-point freely on the roots of f. Since reduction modulo p yields an embedding of the Galois group over $\mathbb{F}_p$ into the Galois group over $\mathbb{Q}$, this shows that the Galois group over $\mathbb{F}_p$ acts semi-regularly. In particular, if f has a root over a particular finite field it splits over it. □

With this, we are able to prove Ennola duality for type D_n with n odd, and that something more complicated happens for n even (as is the case for representations).

Theorem 3.7. *Given H and χ, assume that χ has indicator $+1$. Let ρ be a representation affording χ, and suppose that ρ is root cyclotomic.*

(i) *There exist discriminating moduli for H and χ.*

(ii) *If m is a discriminating modulus then I_m^+ is a subgroup of index at most 2 in I_m.*

(iii) *If $4 \mid d$ then $-1 \in I_m^+$, and so I_m^+ is closed under taking negatives. If $d \equiv 2 \bmod 4$ then $-1 \in I_m^-$, and thus $I_m^- = \{-i : i \in I_m^+\}$.*

Proof. By [8] (proved independently by Guralnick–Navarro), ρ can be chosen with image in $\mathbb{Q}(\zeta_n) \cap \mathbb{R}$ for some integer n. Let α be the determinant for the matrix of scalar products for a bilinear form associated to ρ. Since we are assuming that ρ is root cyclotomic, $\sqrt{\alpha}$ lies in some cyclotomic field, which we can assume is $\mathbb{Q}(\zeta_n)$ by increasing n if necessary. We see that n is a defining modulus for H and χ.

Let f be the minimal polynomial for $\sqrt{\alpha}$, and apply Proposition 3.6. This means that, for q a power of $p \nmid |H|$, whether f splits over $\mathbb{F}_q$ depends only on $q \bmod n$. Thus α being a square in $\mathbb{F}_q$ depends only on $q \bmod n$. If n is not already a multiple of 4, and $d \equiv 2 \bmod 4$, multiply n by 4 so as to account for the change in discriminant of the form of $\mathrm{GO}_d^+(q)$ according to $q \bmod 4$. Since n is already a defining modulus for H and χ, it must now be a discriminating modulus as well.

Let J_1 denote the subset of I_n that consists of all elements i such that $\zeta_n \mapsto \zeta_n^i$ fixes all values of χ *and* fixes $\pm\sqrt{\alpha}$. Thus J_1 is a subgroup of index 2 in I_n, and J_1 contains -1. To see this, notice that α is real (since the matrix is symmetric), and it is positive, as we noted at the start of this section. Thus $\pm\sqrt{\alpha}$ is a pair of real numbers, which are left invariant under complex conjugation, i.e., the field automorphism on $\mathbb{Q}(\zeta_n)$ such that $\zeta_n \mapsto \zeta_n^{-1}$.

If $4 \mid d$ then $J_1 = I_n^+$ and the theorem is proved. Thus we assume that $d \equiv 2 \bmod 4$, and so we need to work further. Let J_2 consist of those elements of I_n congruent to 1 modulo 4, another subgroup of index 2, and not containing -1, so $J_1 \neq J_2$. Since the determinant of the form for $\mathrm{GO}_d^+(q)$ is a square for $q \equiv 1 \bmod 4$ and a non-square for $q \equiv 3 \bmod 4$, I_n^+ consists of the union of $J_1 \cap J_2$ and $I_n \setminus (J_1 \cup J_2)$. Since J_1 and J_2 both have index 2, I_n^+ is also a subgroup of index 2 (it is the other overgroup of $J_1 \cap J_2$) and does not contain -1.

We have therefore proved the second part of the theorem. □

Unfortunately, not all H and χ are root cyclotomic, but counterexamples appear rare in low dimension.

Example 3.8. Let H be the Janko sporadic group J_1 and χ be one of the two irreducible characters of degree 56. Then $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{5}) = K$. Choosing a representation with image in $\mathrm{GL}_{56}(K)$, we find that the determinant α is difficult to write down except with a computer, but certainly the extension $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ is not Galois. To see this, note that if χ' is the other character of degree 56, and letting α' correspond to χ', if $\alpha = a + b\sqrt{5}$ then $\alpha' = a - b\sqrt{5}$. If $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ were Galois then α would have a square root in $\mathbb{F}_p$ if and only if α' does, by Proposition 3.6. However, if $p = 101$, then one of the 56-dimensional representations of H is conjugate to a subgroup of $\mathrm{GO}^+_{56}(101)$ and the other is conjugate to a subgroup of $\mathrm{GO}^-_{56}(101)$. The Galois group of $\mathbb{Q}(\sqrt{\alpha}, \sqrt{\alpha'})/\mathbb{Q}$ is dihedral of order 8, so not abelian either.

For some primes there are two classes of subgroups J_1 in $\mathrm{GO}^+_{56}(p)$, in some there are two in $\mathrm{GO}^-_{56}(p)$, and for some there is one class in each.

Thus there is in general no congruence for embedding simple groups for type D_n with n even, in contrast to the tables for small dimensions in [1, 9, 10]. Indeed, dimension 56 appears to be the smallest dimension for which there is a representation that is not root cyclotomic, so there is no modulus by which we can distinguish the discriminant of the bilinear form.

However, for D_n for n odd, all representations for $\mathrm{PSL}_2(r)$ for $r \leqslant 31$, and other simple groups of dimension d up to 250 with $d \equiv 2 \bmod 4$, are root cyclotomic. This leads to the following conjecture.

Conjecture 3.9. If $d \equiv 2 \bmod 4$ and χ has indicator $+1$, if ρ affords χ then ρ is root cyclotomic.

This conjecture holds if and only if Ennola duality holds for twice-odd dimensional orthogonal groups, which is expected.

For all type D groups, even over $\mathbb{Z}$ so they are root cyclotomic, the modulus involved cannot obviously be read off from the character table, so it becomes another invariant of real representations that needs to be calculated. For example, for HS and McL in dimension 22, the discriminants are 5 and 15 respectively.[1]

4 Ennola duality for exceptional groups

Before we start this section, we underscore here that we will only be considering subgroups H that occur in algebraic groups in characteristic p, where $p \nmid |H|$.

For exceptional groups, it is first not clear that there is such an analogue of the defining modulus. We will have to use the case-by-case lists of maximal subgroups of the finite exceptional groups to proceed. We also must consider what the analogue of an irreducible representation is, which we used when deciding which subgroups to embed into GL_d.

We will only consider 'Lie primitive' subgroups. Recall that a subgroup of a reductive algebraic group is *irreducible* if it does not lie in a proper parabolic subgroup, and is *Lie primitive* if it does not lie in a proper, positive-dimensional subgroup. Understanding Lie primitive subgroups, plus induction on the dimension of the reductive group, generally allows us to understand all irreducible subgroups. For our purposes of understanding maximal subgroups of finite groups, we restrict our attention to Lie primitive subgroups.

If the ambient algebraic group $\mathbf{G}$ is of type G_2 or F_4 then everything works, defining moduli exist, and the set I_n is closed under taking negatives, just as with types B and C. See Table 4.1 for Lie primitive subgroups of $G_2(q)$, taken from [1, Table 8.41], and Table 4.2 for Lie primitive subgroups of $F_4(q)$, taken from [2].

[1] One might be tempted to look at higher Frobenius–Schur indicators: for HS and McL they are the same for $r = 3, 5, 11$, and are 0, 1 and 4 respectively. The two groups differ for $r = 7$, with values 3 and 4.

Subgroup	q
$2^3 \cdot \mathrm{PSL}_3(2)$	All q
$\mathrm{PSL}_2(13)$	$q \equiv \pm 1, \pm 3, \pm 4 \bmod 13$
$\mathrm{PSL}_2(8)$	$q \equiv \pm 1 \bmod 9$
$\mathrm{PSU}_3(3).2$	All q

Table 4.1: Lie primitive subgroups H of $G_2(q)$, $\gcd(q, |H|) = 1$.

Subgroup	q
$3^3 \cdot \mathrm{SL}_3(3)$	All q
$\mathrm{PSL}_2(8)$	$q \equiv \pm 1 \bmod 7$
$\mathrm{PGL}_2(13)$	$q \equiv \pm 1 \bmod 7$
$\mathrm{PSL}_2(17)$	$q \equiv \pm 1, \pm 2, \pm 4, \pm 8 \bmod 17$
$\mathrm{PSL}_2(25).2$	All q
$\mathrm{PSL}_2(27)$	$q \equiv \pm 1 \bmod 7$

Table 4.2: Lie primitive subgroups H of $F_4(q)$, $\gcd(q, |H|) = 1$.

For $E_6(q)$ and ${}^2E_6(q)$, if one takes the simple group, or the triple cover, then there is no longer a defining modulus for the subgroup $\mathrm{PSL}_2(8).3$. This is a subgroup of the algebraic group, but whether it lies in the simple group depends not only on the congruence modulo 7 ($\mathrm{PSL}_2(8)$ embeds in $E_6(q)$ if $q \equiv 1, 2, 4 \bmod 7$), but on the presence of a cube root of $\sqrt{-7} + 1$ in $\mathbb{F}_q$. Formally (see [2, Theorem 6.8], the group $\mathrm{PSL}_2(8).3$ embeds in the finite simple group $E_6(q)$ if and only if $q \equiv 2 \bmod 3$, or q is a cube, or $\sqrt{-7}+1$ has a cube root in $\mathbb{F}_q$. This latter condition cannot be expressed as a simple congruence modulo some number (to see this notice that the root does not lie in a cyclotomic field), so for simply connected groups, and almost simple subgroups, one has no defining modulus in general.

If, however, one uses adjoint versions of $E_6(q)$, so $E_6(q)$ with any diagonal automorphisms added on, then there are defining moduli, and the Lie primitive subgroups for $E_6(q)$ and ${}^2E_6(q)$ can be given in one table. The Lie primitive subgroups of ${}^\varepsilon E_6(q)$ are in Table 4.3: notice that we can switch between the two groups simply by replacing q by $-q$.

We also include a table of the known Lie primitive subgroups of $E_7(q)$, a list from [3] that is expected

Subgroup	q
$3^{3+3} \cdot \mathrm{SL}_3(3)$	$3 \mid (q - \varepsilon 1)$
$\mathrm{PSL}_2(8).3$	$\varepsilon q \equiv 1, 2, 4 \bmod 7$
$\mathrm{PSL}_2(11)$	$q \equiv \pm 1 \bmod 5$, $\varepsilon q \equiv 1, 3, 4, 5, 9 \bmod 11$
$\mathrm{PSL}_2(13)$	$\varepsilon q \equiv 3, 5, 6 \bmod 7$, $q \equiv \pm 2, \pm 5, \pm 6 \bmod 13$
$\mathrm{PSL}_2(19)$	$q \equiv \pm 1 \bmod 5$, $\varepsilon q \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \bmod 19$
$\mathrm{PGL}_2(13)$ (nov)	$\varepsilon q \equiv 1, 2, 4 \bmod 7$, $q \equiv \pm 1, \pm 3, \pm 4 \bmod 13$

Table 4.3: Lie primitive subgroups H of the adjoint group of type ${}^\varepsilon E_6(q)$ for $\varepsilon = \pm$, $\gcd(q, |H|) = 1$. The novelty Lie primitive subgroup occurs for an almost simple group inducing a graph automorphism on ${}^\varepsilon E_6(q)$ (its derived subgroup is contained in G_2).

Subgroup	q
$\mathrm{PSU}_3(3)$	$q \equiv \pm 1 \bmod 8$
$\mathrm{PSU}_3(8).6$	All q
$\mathrm{PSL}_2(37)$	$q \equiv \pm 1, \pm 3, \pm 4, \pm 7, \pm 9, \pm 10, \pm 11, \pm 12, \pm 16 \bmod 37$
$\mathrm{PSL}_2(29)$	$q \equiv \pm 1 \bmod 5$, $q \equiv \pm 1, \pm 4, \pm 5, \pm 6, \pm 7, \pm 9, \pm 13 \bmod 29$
$\mathrm{PSL}_2(27)$	$q \equiv \pm 1 \bmod 13$
$\mathrm{PSL}_2(19)$	$q \equiv \pm 1 \bmod 5$, $q_{19} \equiv q_3 \bmod 2$
$\mathrm{PGL}_2(19)$	$q \equiv \pm 1 \bmod 5$

Table 4.4: Known Lie primitive subgroups H of the adjoint group of type $E_7(q)$, $\gcd(q, |H|) = 1$. Here, q_{19} is the order of q modulo 19 and q_3 is the order of q modulo 3.

to be complete. It displays the same behaviour, that replacing q by $-q$ leaves the table invariant. We have again used the adjoint version: $\mathrm{PSU}_3(8).6$ and $\mathrm{PGL}_2(19)$ lie in the simple group (if they are in the adjoint group) if and only if $q \equiv \pm 1 \bmod 8$. Note that all self-dual representations for $\mathrm{PSU}_3(3)$ are definable over $\mathbb{Z}$, so the defining modulus is 1. However, for embedding in $E_7(q)$, we need $q \equiv \pm 1 \bmod 8$.

References

[1] John Bray, Derek Holt, and Colva Roney-Dougal, *The maximal subgroups of low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, no. 407, Cambridge University Press, Cambridge, 2013.

[2] David A. Craven, *The maximal subgroups of the exceptional groups $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ and related almost simple groups*, preprint, 2020.

[3] ———, *On the maximal subgroups of the exceptional groups $E_7(q)$ and related almost simple groups*, preprint, 2021.

[4] Veikko Ennola, *On the characters of the finite unitary groups*, Ann. Acad. Sci. Fenn. Ser. A No. **323** (1963), 35.

[5] Christoph Jansen, Klaus Lux, Richard Parker, and Robert Wilson, *An atlas of Brauer characters*, Oxford University Press, New York, 1995.

[6] Noriaki Kawanaka, *Generalized Gelfand–Graev representations and Ennola duality*, Algebraic groups and related topics (Kyoto/Nagoya, 1983), Adv. Stud. Pure Math., vol. 6, North-Holland, Amsterdam, 1985, pp. 175–206.

[7] Gunter Malle and Donna Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge University Press, 2011.

[8] Dimitrii Pasechnik, *Splitting fields of real irreducible representations of finite groups*, preprint, arXiv:2107.03452, 2021.

[9] Daniel Rogers, *Maximal subgroups of classical groups in dimensions 16 and 17*, Ph.D. thesis, University of Warwick, 2017.

[10] Anna Schröder, *The maximal subgroups of classical groups in dimension 13, 14 and 15*, Ph.D. thesis, University of St Andrews, 2015.

[11] Alexandre Turull, *Schur index two and bilinear forms*, J. Algebra **157** (1993), 562–572.