REPRESENTATION THEORY
An Electronic Journal of the American Mathematical Society
Volume 25, Pages 897–902 (October 14, 2021)
https://doi.org/10.1090/ert/587

SPLITTING FIELDS OF REAL IRREDUCIBLE REPRESENTATIONS OF FINITE GROUPS

DMITRII V. PASECHNIK

ABSTRACT. We show that any irreducible representation ρ of a finite group G of exponent n, realisable over $\mathbb{R}$, is realisable over the field $E := \mathbb{Q}(\zeta_n) \cap \mathbb{R}$ of real cyclotomic numbers of order n, and describe an algorithmic procedure transforming a realisation of ρ over $\mathbb{Q}(\zeta_n)$ to one over E.

1. Introduction

Let G be a finite group of exponent n. A celebrated result by R. Brauer states that any complex irreducible character $\chi \in \mathrm{Irr}(G)$ of G is afforded by an F-representation $\rho_\chi : G \to \mathrm{GL}_d(F)$, where $F = \mathbb{Q}(\zeta_n)$, the field of cyclotomic numbers of order n (here $\zeta_n := e^{\frac{2\pi i}{n}}$), see [10, (10.3)]. Let $E := \mathbb{Q}(\zeta_n) \cap \mathbb{R} \subset F$ be the maximal real subfield of F. The first result of this note is as follows.

Theorem 1.1. *Let χ be an irreducible real-valued character of G of degree $d := \chi(1)$ with Frobenius-Schur indicator $\nu_2(\chi) = 1$. Then E is a splitting field of χ, i.e. χ is afforded by an E-representation ρ, and the Schur index $m_E(\chi)$ equals 1.*

Our proof of Theorem 1.1 invokes Serre's induction theorem for real characters [13], [2, Theorem 73.18], and then follows the line of proof of Brauer's theorem [10, (10.3)]. It is surprising that it has not appeared anywhere, at least as far as we know.

Remark 1.2. Independently and simultaneously, Robert Guralnick and Gabriel Navarro proved Theorem 1.1 by a similar method, although not using [13].

Recall that the *Frobenius-Schur indicator* $\nu_2(\chi) := \frac{1}{|G|}\sum_{g\in G}\chi(g^2)$ is an invariant classifying complex representations of G into three different types, see [10, (4.5)]. Namely, $\nu_2(\chi) = 0$ if χ is not real-valued, and $\nu_2(\chi) = -1$ if χ is real-valued, but is not afforded by a real-valued representation; $\nu_2(\chi) = 1$ if and only if χ is afforded by a real-valued representation.

For a number field $K \supseteq \mathbb{Q}$, the *Schur index* $m_K(\chi)$ is an invariant of χ controlling the possibility to realise ρ_χ over K, see e.g. [3, Sect. 41] and [10, Chapter 10]. Namely, let $S \supseteq K$ be a splitting field of χ. Then

$$m_K(\chi) := \min_{\substack{K\subseteq M\subseteq S\\ \rho_\chi \text{ realisable over } M}} [M : K(\chi)],$$

where we denoted by $[M : K(\chi)]$ the degree of M as a field extension over $K(\chi)$, the field extension of K generated by the values of χ. In particular, the claim of Theorem 1.1 amounts to stating that $m_E(\chi) = 1$.

Received by the editors July 13, 2021, and, in revised form, July 15, 2021.
2020 *Mathematics Subject Classification.* Primary 20C15, 20-08.

Apart from theoretical significance, the question of finding a splitting field is relevant in group theory algorithms. Standard algorithms such as J. Dixon's algorithm [5] for constructing complex, and real, irreducible representations (one implementation in the computer algebra system GAP [7] of it is described in [4]) do induction from 1-dimensional representations of subgroups of G, which are defined over F. One advantage of working over E instead is that the degree of E is half of the degree of F.

In particular for applications, e.g. in extremal combinatorics, in physics, etc. it is often necessary to reduce a representation to a direct sum of real irreducibles, and exact methods for this process benefit from explicit knowledge of the irreducibles, using well known formulas from [14, Sect. 2.7], as implemented in our GAP package RepnDecomp [9].

Our second result amounts to the algorithmic counterpart of Theorem 1.1, that is, to a procedure to compute, for a representation $\rho : G \to \mathrm{GL}_d(F)$ realisable over reals, an explicit matrix $Q \in \mathrm{GL}_d(F)$ such that $Q^{-1}\rho(G)Q \subset \mathrm{GL}_d(E)$, i.e. Q transforms ρ to an E-representation.

Theorem 1.3. *Let $\rho : G \to \mathrm{GL}_d(F)$ be a representation of G realisable over $\mathbb{R}$. Then $P \in \mathrm{SL}_d(F)$ such that $P\rho(g) = \overline{\rho(g)}P$ for any $g \in G$, and $P\overline{P} = I$, can be explicitly computed from the $\rho(G)$-invariant forms. Let $\xi \in F^*$ s.t. $-\frac{\overline{\xi}}{\xi}$ is not an eigenvalue of P, and $Q := \overline{\xi P} + \xi I$. Then $Q \in \mathrm{GL}_d(F)$ and $Q^{-1}\rho(G)Q \subset \mathrm{GL}_d(E)$.*

The only part of Theorem 1.3 which uses Theorem 1.1 is the claim that P can be chosen so that $P\overline{P} = I$. Algorithmically, one computes P s.t. $P\overline{P} = \mu I$ for $0 < \mu \in E$, and then has to solve the *norm equation*

$$x\overline{x} = \mu, \qquad \text{for } x \in F. \tag{1.1}$$

Theorem 1.1 implies that (1.1) is always solvable. Several parts of the proof of Theorem 1.3 are contained in [8] and [6], although our approach is more explicit, and for odd d we provide an explicit solution (Lemma 3.4), not involving solving (1.1), which is a nontrivial number-theoretic problem.

2. Proof of Theorem 1.1

Our main tool is Serre's induction theorem [2, (73.18)].

Theorem 2.1 (Serre)**.** *The character χ of a real representation of G is a $\mathbb{Z}$-linear combination*

$$\chi = \sum_{\phi} a_\phi \operatorname{Ind}_H^G(\phi) \tag{2.1}$$

of real-valued induced characters $\operatorname{Ind}_H^G(\phi)$, with $H \leq G$, and ϕ a character of H. Further, ϕ is either linear and takes values ± 1, or $\phi = \lambda + \overline{\lambda}$ for a linear character λ of H, or ϕ is dihedral. □

A *diherdal character* ϕ of a group H is a degree 2 irreducible character of H s.t. $H/\ker\phi \cong D_{2m}$, dihedral group of order $2m$.

Note that by [10, (10.2.f)] $m_E(\chi)$ divides $m_{\mathbb{Q}}(\chi) \leq 2$, where the latter inequality holds by the Brauer-Speiser Theorem [10, p. 171]. Therefore it suffices to show that $m_E(\chi) = 2$ is not possible in our situation.

Let θ be a character of an E-representation of G. Then by [10, (10.2.c)] $m_E(\chi) \mid [\theta, \chi]$. Here $[,]$ is the usual scalar product of characters $[\theta,\chi] = \frac{1}{G}\sum_{g\in G}\theta(g)\overline{\chi(g)}$, cf. [10, (2.16)]. As χ is irreducible, $[\chi,\chi]=1$, thus (2.1) implies

$$1 = [\chi,\chi] = \sum_{\phi} a_\phi [\mathrm{Ind}_H^G(\phi), \chi]. \tag{2.2}$$

If every $\mathrm{Ind}_H^G(\phi)$ is an E-representation, then $m_E(\chi)=2$ is not possible, as otherwise an even integer on the right hand side of (2.2) equals 1.

It remains to see that every $\mathrm{Ind}_H^G(\phi)$ is an E-representation.

This is trivially the case for linear ϕ, and so we are left with the dihedral case and the case $\phi = \lambda + \overline{\lambda}$. To simplify the rest of the proof, we use [10, (10.9)] which says that if a prime p divides $m_E(\chi)$ then the Sylow p-subgroups of G are not elementary abelian. For $p=2$ this means that $4 \mid n$, i.e. $i := \sqrt{-1} \in F$.

Lemma 2.2. *Let $H \le G$, with G of exponent n, $4 \mid n$, and ϕ a character of H, either $\phi = \lambda + \overline{\lambda}$ with λ linear, or ϕ dihedral. Then ϕ is afforded by an E-representation.*

Proof. Note that $E = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and $2\cos\frac{2\pi}{n} = \zeta_n + \zeta_n^{-1}$. As $4 \mid n$, it can be shown that $\sin\frac{2\pi}{n} \in E$ in this case (in general this is not true).

In the case $\phi = \lambda + \overline{\lambda}$ we have $H/\ker\phi$ a cyclic group C of order m dividing n, $C \cong \langle\zeta_m\rangle$. We have $Z_m := \begin{pmatrix}\cos\frac{2\pi}{m} & -\sin\frac{2\pi}{m}\\ \sin\frac{2\pi}{m} & \cos\frac{2\pi}{m}\end{pmatrix} \in \mathrm{SL}_2(E)$, and

$$\begin{aligned}\rho_\phi : C &\to \mathrm{SL}_2(E)\\ \zeta_m^k &\mapsto Z_m^k, \qquad 0 \le k < m\end{aligned}$$

is the desired E-representation of C with character ϕ.

For dihedral ϕ we have $H/\ker\phi$ a dihedral group $D = \langle a, b \mid 1 = a^m = b^2 = (ab)^2\rangle$ of order $2m$ dividing n, with normal cyclic subgroup C of order m, so that the restriction $\phi_C = \lambda + \overline{\lambda}$ is as in the previous case, and $\phi_{D-C} = 0$. We have $Z_m \in \mathrm{SL}_2(E)$ as in the previous case, and $R_0 := \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \in \mathrm{GL}_2(E)$ satisfying $R_0 Z_m R_0 = Z_m^{-1}$ and

$$\begin{aligned}\rho_\phi : D &\to \mathrm{GL}_2(E)\\ a^k b^\ell &\mapsto Z_m^k R_0^\ell, \qquad 0 \le k < m,\ 0 \le \ell \le 1,\end{aligned}$$

is the desired E-representation of D with character ϕ. □

This completes the proof of Theorem 1.1. The last step, i.e. the proof of Lemma 2.2, could also be accomplished in a less explicit way, by invoking the construction of Theorem 1.3; the matrix P mapping ρ_ϕ to its conjugate can be chosen to be equal to $P = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, satisfying the only condition, $P\overline{P} = I$. In particular this approach allows to prove a more general version of Lemma 2.2 which does not require $4 \mid n$.

3. Proof of Theorem 1.3

The case $n = 2$ is trivial, and we will assume $n \ge 3$ in what follows.

Recall that in general, χ has values in F, while a real-valued character has values in E. Whenever χ is E-valued, the image $\rho(G)$ of G under a representation $\rho := \rho_\chi$ affording χ leaves invariant a unique, up to scalar multiplication, non-zero G-invariant form M. It is a classical result due to Frobenius and Schur that if M is symmetric then χ is afforded by a real representation ρ, and $\nu_2(\chi) = 1$, cf. [10, (4.19)].

Without loss of generality, $\chi(1) > 1$. Indeed, if $\chi(1) = 1$ then ρ is the same as χ, and we are done.

The proof of Frobenius-Schur in [10, (4.19)] starts with the elementary fact that if Q is a transformation making ρ real then $Q^{-1}\rho Q = \overline{Q^{-1}\rho Q}$, thus $\overline{Q}Q^{-1}\rho = \overline{\rho Q}Q^{-1}$, and $P := \overline{Q}Q^{-1}$ transforms ρ to $\overline{\rho}$, i.e. $P^{-1}\overline{\rho}P = \rho$. Such a $P \in \mathrm{GL}_d(\mathbb{C})$ must exist irrespective of the existence of Q, as the characters of ρ and $\overline{\rho}$ are equal, although we can give an explicit construction $P = \Sigma^{-1}M$, with M as above, and Σ the matrix of a positive definite Hermitian $\rho(G)$-invariant form.

Lemma 3.1. *Let χ be a real-valued character of G, and $\rho = \rho_\chi$ an F-representation affording χ. Then $P := \Sigma^{-1}M \in \mathrm{GL}_d(F)$ satisfies $P\rho(g) = \overline{\rho(g)}P$ for all $g \in G$.*

Proof. As χ is real, ρ leaves invariant a non-zero G-invariant bilinear form M, i.e. $g^\top Mg = M$ for all $g \in \rho$, cf. e.g. [10, (4.14)]. As M can be found in the trivial sub-representation of the tensor square of ρ, $M \in M_d(F)$. As well, $\det M \neq 0$, as the kernel of M would give rise to a sub-representation of ρ, contradicting irreducibility of ρ.

Let $\Sigma := \sum_{h\in\rho(G)} h^\top\overline{h}$ – note that Σ is a Hermitian positive definite matrix, in particular $\det\Sigma > 0$, and $g^\top\Sigma\overline{g} = \Sigma$ for any $g \in \rho(G)$.

Choose $P := \Sigma^{-1}M$. Let's check that $P^{-1}\overline{\rho}P = \rho$ (we use $\det M \neq 0$ here). Let $g \in \rho(G)$. Then, as $(\overline{g}\Sigma^{-1}g^\top)^{-1} = (g^\top)^{-1}\Sigma\overline{g}^{-1} = \Sigma$,

$$\Sigma^{-1}Mg = \overline{g}\Sigma^{-1}g^\top Mg = \overline{g}\Sigma^{-1}M,$$

as required. □

Now we have the equation

$$PQ = \overline{Q}, \qquad \det Q \neq 0 \tag{3.1}$$

implying $\overline{P}PQ = \overline{PQ} = Q$, i.e. $\overline{P}P = I$. The latter is an extra restriction, in the sense that our procedure does not guarantee that P computed as in Lemma 3.1 satisfies $\overline{P}P = I$. In general, one will need to solve (1.1) and multiply P by the inverse of a solution. However, (1.1) will always be solvable by Theorem 1.1.

Lemma 3.2. *Let $P \in \mathrm{GL}_d(F)$ such that $Pg = \overline{g}P$ for any $g \in \rho(G)$. Then $P\overline{P} = \mu I$ for some $\mu \in E$.*

Proof. Note that $\overline{Pg} = g\overline{P}$. Thus $P\overline{P}\overline{g} = Pg\overline{P} = \overline{g}P\overline{P}$. Thus $P\overline{P}$ lies in the centraliser of an irreducible representation $\overline{\rho}$. Hence, by Schur's Lemma, $P\overline{P} = \mu I$, for some $\mu \in F$.

It remains to show that $\mu \in E$. Using Lemma 3.1, and recalling that Σ and Σ^{-1} are Hermitian positive definite, i.e. $\Sigma^{-1} = U\overline{U}^\top$, and $M = M^\top$, we have $\mu I = P\overline{P} = \Sigma^{-1}M\overline{\Sigma^{-1}M}$, i.e.

$$\mu\Sigma = M\overline{\Sigma^{-1}M} = M\overline{U\overline{U}^\top M} = M\overline{U}U^\top\overline{M} = (M\overline{U})(\overline{M\overline{U}})^\top = \overline{\mu\Sigma}^\top = \overline{\mu}\Sigma,$$

implying $\mu = \overline{\mu}$. □

It remains to solve (3.1) so that Q has entries in the splitting field of ρ. Note that the solution of (3.1) in [10, Ch. 4] assumes that ρ is unitary; i.e. $\Sigma = I$; so in this case $P^{\top} = P$, and an explicit formula for Q is provided – which however does not work for us, as it involves square roots of eigenvalues of P. Fortunately, in [8, Prop. 1.3], there is an algorithmic proof of existence of the required solution of (3.1). In [loc. cit.] it is done for finite fields (and in bigger generality, for a field automorphism σ of finite order, referring to this result as a generalisation of *Hilbert's Theorem 90*), and in [6] it was noted that it works for number fields as well. One can also find there an easier observation, that for a randomly chosen $Y \in M_d(F)$ setting $Q = \overline{Y} + \overline{P}Y$ produces a solution to (3.1) with high probability. Here is an easy to prove variation of this claim.

Lemma 3.3. *Let $P, Y \in M_d(F)$ and $P\overline{P} = I$. Then $Q := \overline{Y} + \overline{P}Y$ satisfies $PQ = \overline{Q}$. Choosing $Y = \xi P$, with $\xi \neq 0$ and $-\xi/\overline{\xi}$ not being an eigenvalue of $\overline{P}$ we have that $Q \in M_d(F)$ satisfies* (3.1)*.*

Proof. Note that $PQ = P\overline{Y} + P\overline{P}Y = Y + P\overline{Y} = \overline{Q}$, as claimed. The claimed choice of ξ is possible as F is dense in $\mathbb{C}$. Further, with $Q = \overline{\xi P} + \xi\overline{P}P = \overline{\xi}(\overline{P} + \frac{\xi}{\overline{\xi}}I)$ we see that $Qv = 0$ holds for a non-zero vector v if and only if $\overline{P}v = -\frac{\xi}{\overline{\xi}}v$, which is not possible by the choice of ξ. $\square$

To complete the proof of Theorem 1.3 is suffices to observe that $Q^{-1}\rho(g)Q \in M_d(E)$ for any $g \in G$.

One can solve (1.1) in the case of odd d without resorting to number-theoretic tools.

Lemma 3.4. *Let $d = 2k + 1$. Then,* (1.1) *for μ in $P\overline{P} = \mu I$ is solved by $x = \mu^{-k} \det P$.*

Proof. Let $\lambda := \det P$. Then $\det(P\overline{P}) = \lambda\overline{\lambda} = \overline{\lambda}\lambda = \det(\mu I) = \mu^{2k+1}$. Thus $\mu = \overline{\mu} = \frac{\lambda}{\mu^k}\frac{\overline{\lambda}}{\mu^k}$. Replacing P with $P' = \frac{\mu^k}{\lambda}P$ we see that $P'\overline{P'} = I$. $\square$

4. Related work and remarks

The paper [6] studies a closely related algorithmic question of minimising the degree of the number field needed to write down a complex representation. It is known that such a field need not be cyclotomic. On the other hand, computer algebra systems designed for computing in groups, such as GAP [7] and Magma [1], typically use cyclotomic fields for computation with characteristic zero representations of finite groups. In particular, this work came as an analysis of a question [11] posed on the GAP discussion forum.

Lemma 3.1 and its proof are essentially a refinement of an argument from the proof of [14, Thm. 31]. Lemmata 3.4 and 3.3 appear to be novel, as well as Theorem 1.1.

Acknowledgments

The author thanks Denis Rosset, Stephen Glasby, Kaashif Hymabaccus, Robert Guralnick, and many participants of MathOverflow, in particular Will Sawin [12], for fruitful discussions.

Special thanks go to Robert Guralnick, who, in his capacity of a moderator for arXiv.org, caught a glaring omission in an earlier version of this text, submitted there.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[2] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. II*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1987. With applications to finite groups and orders; A Wiley-Interscience Publication. MR892316

[3] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original, DOI 10.1090/chel/356. MR2215618

[4] Vahid Dabbaghian and John D. Dixon, *Computing matrix representations*, Math. Comp. **79** (2010), no. 271, 1801–1810, DOI 10.1090/S0025-5718-10-02330-6. MR2630014

[5] John D. Dixon, *Constructing representations of finite groups*, Groups and computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 105–112. MR1235797

[6] Claus Fieker, *Minimizing representations over number fields. II. Computations in the Brauer group*, J. Algebra **322** (2009), no. 3, 752–765, DOI 10.1016/j.jalgebra.2009.05.009. MR2531221

[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.

[8] S. P. Glasby and R. B. Howlett, *Writing representations over minimal fields*, Comm. Algebra **25** (1997), no. 6, 1703–1711, DOI 10.1080/00927879708825947. MR1446124

[9] Kaashif Hymabaccus and Dmitrii V. Pasechnik, *RepnDecomp: A GAP package for decomposing linear representations of finite groups*, J. Open Source Softw. **5** (2020), no. 50, 1835–1836.

[10] I. Martin Isaacs, *Character theory of finite groups*, Dover Publications, Inc., New York, 1994. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423 (57 #417)]. MR1280461

[11] Denis Rosset, *Repsn: constructing representations with real coefficients*, 2021, GAP-Forum post, `https://mail.gap-system.org/pipermail/forum/2021/006240.html`.

[12] Will Sawin, *Is every positive real cyclotomic number the norm of a cyclotomic?*, MathOverflow, 2021, `https://mathoverflow.net/q/391269` (version: 2021-04-27).

[13] Jean-Pierre Serre, *Conducteurs d'Artin des caractères réels* (French), Invent. Math. **14** (1971), 173–183, DOI 10.1007/BF01418887. MR321908

[14] Jean-Pierre Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, Vol. 42, Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott. MR0450380

Department of Computer Science, University of Oxford, United Kingdom
Email address: `dima@pasechnik.info`