Splitting fields of real irreducible representations of finite groups

Dmitrii V. Pasechnik¹

¹Department of Computer Science, University of Oxford, UK*

2021-07-15

Abstract

We show that any irreducible representation $\rho$ 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 $\rho$ over $\mathbb{Q}(\zeta_n)$ to one over $E$.

Introduction

Let $G$ be a finite group of exponent $n$. A celebrated result by R. Brauer states that any complex irreducible character $\chi \in \text{Irr}(G)$ of $G$ is afforded by an $F$-representation $\rho_\chi : G \to \text{GL}_d(F)$, where $F = \mathbb{Q}(\zeta_n)$, the field of cyclotomic numbers of order $n$ (here $\zeta_n := e^{\frac{2\pi i}{n}}$), see [Isa94, (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. Let $\chi$ 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 $\chi$, i.e. $\chi$ is afforded by an $E$-representation $\rho$, and the Schur index $m_E(\chi)$ equals 1.

Our proof of Theorem 1 invokes Serre’s induction theorem for real characters [Ser71], [CR87, Theorem 73.18], and then follows the line of proof of Brauer’s theorem [Isa94, (10.3)]. It is surprising that it has not appeared anywhere, at least as far as we know.

Remark. Independently and simultaneously, Robert Guralnick and Gabriel Navarro proved Theorem 1 by a similar method, although not using [Ser71].

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 [Isa94, (4.5)]. Namely, $\nu_2(\chi) = 0$ if $\chi$ is not real-valued, and $\nu_2(\chi) = -1$ if $\chi$
is real-valued, but is not afforded by a real-valued representation; \( \nu_2(\chi) = 1 \) if and only if \( \chi \) 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 \( \chi \) controlling the possibility to realise \( \rho_\chi \) over \( K \), see e.g. \cite{CR06, Sect. 41} and \cite{Isa94, Chapter 10}. Namely, let \( S \supseteq K \) be a splitting field of \( \chi \). Then \( m_K(\chi) := \min \{ M \subseteq S \mid \rho_\chi \text{ realisable over } M \} \), 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 \( \chi \). In particular, the claim of Theorem 1 amounts to stating that \( m_E(\chi) = 1 \).

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 \cite{Dix93} for constructing complex, and real, irreducible representations (one implementation in the computer algebra system GAP \cite{GAP21} of it is described in \cite{DD10}) 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 \cite[Sect.2.7]{Ser77}, as implemented in our GAP package RepnDecomp \cite{HP20}.

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

**Theorem 2.** Let \( \rho : G \rightarrow \text{GL}_d(F) \) be a representation of \( G \) realisable over \( \mathbb{R} \). Then \( P \in \text{SL}_d(F) \) such that \( P\rho(g) = \rho(g)P \) for any \( g \in G \), and \( P^T = I \), can be explicitly computed from the \( \rho(G) \)-invariant forms. Let \( \xi \in F^* \) s.t. \( -\frac{1}{\xi} \) is not an eigenvalue of \( P \), and \( Q := \frac{\xi}{\xi} + \xi I \). Then \( Q \in \text{GL}_d(F) \) and \( Q^{-1}\rho(G)Q \subset \text{GL}_d(E) \).

The only part of Theorem 2 which uses Theorem 1 is the claim that \( P \) can be chosen so that \( P^TP = I \). Algorithmically, one computes \( P \) s.t. \( P^TP = \mu I \) for \( 0 < \mu \in E \), and then has to solve the norm equation

\[
\mu x = \mu, \quad \text{for } x \in F.
\]  

(1)

Theorem 1 implies that (1) is always solvable. Several parts of the proof of Theorem 2 are contained in \cite{GH97} and \cite{Fie09}, although our approach is more explicit, and for odd \( d \) we provide an explicit solution (Lemma 5), not involving solving (1), which is a nontrivial number-theoretic problem.
Proof of Theorem 1

Our main tool is Serre’s induction theorem [CR87, (73.18)].

**Theorem 3.** (Serre) The character $\chi$ of a real representation of $G$ is a $\mathbb{Z}$-linear combination

$$\chi = \sum \phi a_{\phi} \text{Ind}_{H}^{G}(\phi) \quad (2)$$

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

A dihedral character $\phi$ 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 [Isa94, (10.2.f)] $m_{E}(\chi)$ divides $m_{Q}(\chi) \leq 2$, where the latter inequality holds by the Brauer-Speiser Theorem [Isa94, p.171]. Therefore it suffices to show that $m_{E}(\chi) = 2$ is not possible in our situation.

Let $\theta$ be a character of an $E$-representation of $G$. Then by [Isa94, (10.2.c)] $m_{E}(\chi) | \langle \theta, \chi \rangle$. Here $\langle \cdot, \cdot \rangle$ is the usual scalar product of characters $\langle \theta, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \theta(g)\overline{\chi(g)}$, cf. [Isa94, (2.16)]. As $\chi$ is irreducible, $\langle \chi, \chi \rangle = 1$, thus (2) implies

$$1 = \langle \chi, \chi \rangle = \sum \phi a_{\phi} \langle \text{Ind}_{H}^{G}(\phi), \chi \rangle. \quad (3)$$

If every $\text{Ind}_{H}^{G}(\phi)$ is an $E$-representation, then $m_{E}(\chi) = 2$ is not possible, as otherwise an even integer on the right hand side of (3) equals 1.

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

This is trivially the case for linear $\phi$, 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 [Isa94, (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 $4 | n$, i.e. $i := \sqrt{-1} \in F$.

**Lemma 1.** Let $H \leq G$, with $G$ of exponent $n$, $4 | n$, and $\phi$ a character of $H$, either $\phi = \lambda + \overline{\lambda}$ with $\lambda$ linear, or $\phi$ dihedral. Then $\phi$ 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 $4 | n$, 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 $n$, $\mathbb{C} \cong \langle \zeta_{m} \rangle$. We have $Z_{m} := \left( \begin{array}{cc} \cos \frac{2\pi}{m} & -\sin \frac{2\pi}{m} \\ \sin \frac{2\pi}{m} & \cos \frac{2\pi}{m} \end{array} \right) \in \text{SL}_{2}(E)$, and

$$\rho_{\phi} : C \to \text{SL}_{2}(E)$$

$$\zeta_{m}^{k} \mapsto Z_{m}^{k}, \quad 0 \leq k < m.$$
is the desired $E$-representation of $C$ with character $\phi$.

For dihedral $\phi$ 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 $Z_m \in \text{SL}_2(E)$ as in the previous case, and $R_0 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \text{GL}_2(E)$ satisfying $R_0Z_mR_0 = Z_m^{-1}$ and

$$\rho_\phi : D \to \text{GL}_2(E)$$

$$a^k b^\ell \mapsto Z_m^k R_0, \quad 0 \leq k < m, \quad 0 \leq \ell \leq 1,$$

is the desired $E$-representation of $D$ with character $\phi$. \hfill \Box

This completes the proof of Theorem 1. The last step, i.e. the proof of Lemma 1, could also be accomplished in a less explicit way, by invoking the construction of Theorem 2; the matrix $P$ mapping $\rho_\phi$ to its conjugate can be chosen to be equal to $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, satisfying the only condition, $P^T = I$. In particular this approach allows to prove a more general version of Lemma 1 which does not require $4 \mid n$.

**Proof of Theorem 2**

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

Recall that in general, $\chi$ has values in $F$, while a real-valued character has values in $E$. Whenever $\chi$ is $E$-valued, the image $\rho(G)$ of $G$ under a representation $\rho := \rho_\chi$ affording $\chi$ 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 $\chi$ is afforded by a real representation $\rho$, and $\nu_2(\chi) = 1$, cf. [Isa94, (4.19)].

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

The proof of Frobenius-Schur in [Isa94, (4.19)] starts with the elementary fact that if $Q$ is a transformation making $\rho$ real then $Q^{-1}\rho Q = \overline{Q^{-1}}\rho\overline{Q}$, thus $\overline{Q}Q^{-1} = \rho \overline{Q}Q^{-1}$, and $P := \overline{Q}Q^{-1}$ transforms $\rho$ to $\overline{\rho}$, i.e. $P^{-1}\overline{\rho}P = \rho$. Such a $P \in \text{GL}_d(C)$ must exist irrespective of the existence of $Q$, as the characters of $\rho$ and $\overline{\rho}$ are equal, although we can give an explicit construction $P = \Sigma^{-1}M$, with $M$ as above, and $\Sigma$ the matrix of a positive definite Hermitian $\rho(G)$-invariant form.

**Lemma 2.** Let $\chi$ be a real-valued character of $G$, and $\rho = \rho_\chi$ an $F$-representation affording $\chi$. Then $P := \Sigma^{-1}M \in \text{GL}_d(F)$ satisfies $P \rho(g) = \rho(g)P$ for all $g \in G$. 

4
Proof. As $\chi$ is real, $\rho$ leaves invariant a nonzero $G$-invariant bilinear form $M$, i.e. $g^\top M g = M$ for all $g \in \rho$, cf. e.g. [Isa94, (4.14)]. As $M$ can be found in the trivial sub-representation of the tensor square of $\rho$, $M \in M_d(F)$. As well, $\det M \neq 0$, as the kernel of $M$ would give rise to a sub-representation of $\rho$, contradicting irreducibility of $\rho$.

Let $\Sigma := \sum_{h \in \rho(G)} h^\top h$ - note that $\Sigma$ is a Hermitian positive definite matrix, in particular $\det \Sigma > 0$, and $g^\top \Sigma g = \Sigma$ for any $g \in \rho(G)$. Choose $P := \Sigma^{-1} M$. Let’s check that $P^{-1} \rho P = \rho$ (we use $\det M \neq 0$ here). Let $g \in \rho(G)$. Then, as $(g \Sigma^{-1} g^\top)^{-1} = (g^\top)^{-1} \Sigma^{-1} = \Sigma$,

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

as required. \hfill \Box

Now we have the equation

$$PQ = \overline{Q}, \quad \det Q \neq 0$$

implying $P \overline{P} Q = \overline{P} \overline{Q} = Q$, i.e. $P \overline{P} = I$. The latter is an extra restriction, in the sense that our procedure does not guarantee that $P$ computed as in Lemma 2 satisfies $P \overline{P} = I$. In general, one will need to solve (1) and multiply $P$ by the inverse of a solution. However, (1) will always be solvable by Theorem 1.

Lemma 3. Let $P \in \text{GL}_d(F)$ such that $P g = \overline{\rho} P$ for any $g \in \rho(G)$. Then $P \overline{P} = \mu I$ for some $\mu \in E$.

Proof. Note that $\overline{P} g = g \overline{P}$. Thus $P \overline{P} Q = P g \overline{P} = \overline{\rho} P \overline{P}$. 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 2, and recalling that $\Sigma$ and $\Sigma^{-1}$ are Hermitian positive definite, i.e. $\Sigma^{-1} = U \overline{U}^\top$, and $M = M^\top$, we have $\mu I = P \overline{P} = \Sigma^{-1} M \Sigma^{-1} M$, i.e.

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

implying $\mu = \overline{\rho}$.

It remains to solve (4) so that $Q$ has entries in the splitting field of $\rho$. Note that the solution of (4) in [Isa94, Ch. 4] assumes that $\rho$ 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 [GH97, Prop. 1.3], there is an algorithmic proof of existence of the required solution of (4). In [loc.cit.] it is done for finite fields (and in bigger generality, for a field automorphism $\sigma$ of finite order, referring to this result as a generalisation of Hilbert’s Theorem 90), and in [Fie09] 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 \( Q := \overline{Y} + \overline{PY} \) produces a solution to (4) with high
probability. Here is an easy to prove variation of this claim.

**Lemma 4.** Let \( P, Y \in M_d(F) \) and \( \overline{P} \overline{Y} = \overline{I} \). Then \( Q := \overline{Y} + \overline{PY} \) satisfies
\( PQ = \overline{Q} \). Choosing \( Y = \xi P \), with \( \xi \neq 0 \) and \( -\xi^2/\xi \) not being an eigenvalue of \( \overline{P} \)
we have that \( Q \in M_d(F) \) satisfies (4).

**Proof.** Note that \( PQ = \overline{PY} + P\overline{PY} = Y + P\overline{Y} = \overline{Q} \), as claimed. The claimed
choice of \( \xi \) is possible as \( F \) is dense in \( \mathbb{C} \). Further, with \( Q = \xi \overline{P} + \xi \overline{P} P =
\xi(\overline{P} + \xi \overline{I}) \) we see that \( Qv = 0 \) holds for a non-zero vector \( v \) if and only if
\( \overline{P}v = -\xi^{-1}v \), which is not possible by the choice of \( \xi \).

To complete the proof of Theorem 2 it suffices to observe that \( Q^{-1} \rho(g)Q \in M_d(E) \) for any \( g \in G \).

One can solve (1) in the case of odd \( d \) without resorting to number-theoretic
tools.

**Lemma 5.** Let \( d = 2k + 1 \). Then, (1) for \( \mu \) 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
\( \mu = \overline{\lambda} = \frac{\lambda}{\mu^{2k}} \). Replacing \( P \) with \( P' = \frac{1}{\lambda} P \) we see that \( P' \overline{P'} = I \).

### Related work and remarks

The paper [Fie09] 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, com-
puter algebra systems designed for computing in groups, such as GAP [GAP21]
and Magma [BCP97] typically use cyclotomic fields for computation with char-
acteristic zero representations of finite groups. In particular, this work came as
an analysis of a question [Ros21] posed on the GAP discussion forum.

Lemma 2 and its proof are essentially a refinement of an argument from the
proof of [Ser77, Thm.31]. Lemmata 5 and 4 appear to be novel, as well as
Theorem 1.

### Acknowledgement.

The author thanks Denis Rosset, Stephen Glasby, Kaashif Hymabaccus, Robert
Guralnick, and many participants of MathOverflow, in particular Will Sawin
[Saw21], 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

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[CR87] 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.

[CR06] 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.

[DD10] Vahid Dabbaghian and John D. Dixon. Computing matrix representations. *Math. Comp.*, 79(271):1801–1810, 2010.

[Dix93] John D. Dixon. Constructing representations of finite groups. In *Groups and computation (New Brunswick, NJ, 1991)*, volume 11 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 105–112. Amer. Math. Soc., Providence, RI, 1993.

[Fie09] Claus Fieker. Minimizing representations over number fields. II. Computations in the Brauer group. *J. Algebra*, 322(3):752–765, 2009.

[GAP21] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.

[GH97] S. P. Glasby and R. B. Howlett. Writing representations over minimal fields. *Comm. Algebra*, 25(6):1703–1711, 1997.

[HP20] Kaashif Hymabaccus and Dmitrii V. Pasechnik. RepnDecomp: A GAP package for decomposing linear representations of finite groups. *Journal of Open Source Software*, 5(50):1835–1836, 2020.

[Isa94] 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)].

[Ros21] Denis Rosset. Repsn: constructing representations with real coefficients, 2021. GAP-Forum post, https://mail.gap-system.org/pipermail/forum/2021/006240.html.
[Saw21] Will Sawin. Is every positive real cyclotomic number the norm of a cyclotomic? MathOverflow, 2021. https://mathoverflow.net/q/391269 (version: 2021-04-27).

[Ser71] Jean-Pierre Serre. Conducteurs d’Artin des caractères réels. Invent. Math., 14:173–183, 1971.

[Ser77] Jean-Pierre Serre. Linear representations of finite groups. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.