REAL REPRESENTATIONS OF FINITE GROUPS

STEFAN G. KARPINSKI

1. Reality

Definitions.

An element of a group is called *real* if it is conjugate to its inverse.
A conjugacy class of a group is called *real* if it contains a real element.
A character of a group is called *real* if all its values are real.

Henceforth, let G be a finite group. Notice that if one element of a conjugacy class is real then all of its elements are: let $x, y, z \in G$ such that $y^{-1}xy = x^{-1}$, then

$$(z^{-1}yz)^{-1}(z^{-1}xz)(z^{-1}yz) = (z^{-1}y^{-1}z)(z^{-1}xz)(z^{-1}yz) =$$
$$z^{-1}y^{-1}xyz = z^{-1}x^{-1}z = (z^{-1}xz)^{-1}.$$

Proposition 1.1. The number of real conjugacy classes of G is equal to the number of real, irreducible characters of G.

Proof. Let M be the invertible matrix of the character table for G, and let $\overline{M}$ denote the complex conjugate of M. For each irreducible character χ of G, $\overline{\chi}$ is also an irreducible character of G, so $\overline{M}$ is related to M by permutation of rows:

$$PM = \overline{M}$$

for some permutation matrix P. Similarly, for each irreducible character χ on G and element $g \in G$, $\overline{\chi}(g) = \chi(g^{-1})$, so each column of M is the complex conjugate of its "inverse" column, and $\overline{M}$ is related to M by permutation of columns:

$$MQ = \overline{M}$$

for some permutation matrix Q. Notice the significance of the matrices P and Q:

$$\text{a character is real} \iff \text{it is fixed by } P, \text{ and}$$
$$\text{a conjugacy class is real} \iff \text{it is fixed by } Q.$$

Thus the number of real, irreducible characters of G is the trace of P and the number of real conjugacy classes of G is the trace of Q. But

$$Q = M^{-1}\overline{M} = M^{-1}PM, \quad \text{so} \quad \operatorname{tr} Q = \operatorname{tr} P.$$

□

With this, it is a simple application that the character table for any S_n has only real entries, since all elements of S_n are real and therefore so are all its characters.

Proposition 1.2. G has a non-trivial, real element iff $|G|$ is even.

Proof. If G has even order then it contains a transposition and all transpositions are non-trivial and real. On the other hand, suppose that G has odd order and contains a real element x. So there exists $y \in G$ such that $y^{-1}xy = x^{-1}$. But then

$$y^{-2}xy^2 = y^{-1}(y^{-1}xy)y = y^{-1}x^{-1}y = (y^{-1}xy)^{-1} = x,$$

so y^2 is in the normalizer x^G of x. Since $|G|$ is odd, by Lagrange's Theorem there exists a positive integer n such that $y^{2n+1} = 1$ and thus $y = y^{2(n+1)} \in x^G$; *i.e.*, $y^{-1}xy = x^{-1} = x$, so $x^2 = 1$, and since $|G|$ is odd, x must be the identity. □

Corollary 1.3. G has a non-trivial, real, irreducible character iff $|G|$ is even.

Proof. This follows immediately from Propositions 1.1 and 1.2. □

2. Realization

Definition. A character χ of G is said to be *realizable over* $\mathbb{R}$ if there exists an $\mathbb{R}G$-module with character χ.

Notice that by this definition, not all real characters need be realizable over $\mathbb{R}$. It is the aim of this paper to provide an "easy" method of determining whether a given character is realizable over $\mathbb{R}$ or not.

Every $\mathbb{R}G$-module can be naturally converted to a $\mathbb{C}G$-module of equal dimension: let U be an $\mathbb{R}G$-module and let $\{e_k\}$ be a basis for it; then let V be the $\mathbb{C}G$-module with basis $\{e_k\}$ where G acts on the e_k as before.

It is harder to turn a given $\mathbb{C}G$-module into a $\mathbb{R}G$-module. Let V be a $\mathbb{C}G$-module with basis $\{e_k\}$. Let $V_{\mathbb{R}}$ be the $\mathbb{R}G$-module with basis $\{e_k, \mathrm{i}e_k\}$ where multiplication by G is defined by taking the complex number i to the formal i of the new basis elements. Explicitly, if $e_j g = \sum_k (a_{jk} + \mathrm{i}b_{jk})e_k$ in V for $g \in G$, then define multiplication as follows for $V_{\mathbb{R}}$:

$$(*) \qquad e_j g = \sum_k (a_{jk}e_k + b_{jk}(\mathrm{i}e_k)), \qquad (\mathrm{i}e_j)g = \sum_k (-b_{jk}e_k + a_{jk}(\mathrm{i}e_k)).$$

The following proposition uses to $\mathbb{R}G$-module $V_{\mathbb{R}}$ to provide an important criterion for the realizability of irreducible characters over $\mathbb{R}$.

Proposition 2.1. If V is a $\mathbb{C}G$-module with character χ, then the corresponding $\mathbb{R}G$-module $V_{\mathbb{R}}$ has character $\psi = \chi + \overline{\chi}$. Moreover, if V is irreducible and $V_{\mathbb{R}}$ is reducible, then χ is realizable over $\mathbb{R}$.

Proof. Taking $g \in G$ as above, $\chi(g) = \sum_k (a_{kk} + \mathrm{i}b_{kk})$ and by $(*)$, $\psi(g) = 2\sum_k a_{kk}$, so $\psi(g) = \chi(g) + \overline{\chi}(g)$. If $V_{\mathbb{R}}$ is reducible, write $V_{\mathbb{R}} = U + W$ with non-zero $\mathbb{R}G$-modules U and W. If V is irreducible, then χ and $\overline{\chi}$ are each irreducible and U and W must be irreducible as well, having characters χ and $\overline{\chi}$ respectively. □

3. Bilinear Forms

Definitions.
Let β be a bilinear form on a vector space V over field $\mathbb{F}$ with char $\neq 2$.

β is called *symmetric* if $\beta(u, v) = \beta(v, u)$ for all $u, v \in V$.
β is called *symplectic* if $\beta(u, v) = -\beta(v, u)$ for all $u, v \in V$.
β is called *positive-definite* if $\beta(v, v) > 0$ for all non-zero $v \in V$.

If V is an $\mathbb{F}G$-module, then

β is called *G-invariant* if $\beta(ug, vg) = \beta(u, v)$ for all $u, v \in V$ and $g \in G$.

Proposition 3.1. Every $\mathbb{R}G$-module has a G-invariant, symmetric, positive-definite, bilinear form.

Proof. Let V be an $\mathbb{R}G$-module with basis $\{e_k\}$ and let $\{g_j\}$ enumerate G. For $u, v \in V$, take $u_{jk}, v_{jk} \in \mathbb{R}$ such that $ug_j = \sum_k u_{jk}e_k$, and $vg_j = \sum_k v_{jk}e_k$ and define

$$\alpha(u, v) = \sum_{j,k} u_{jk}v_{jk}.$$

This is the desired G-invariant, symmetric, positive-definite, bilinear form on V. □

Proposition 3.2. Let V be an $\mathbb{R}G$-module with G-invariant, bilinear form β. If U is an $\mathbb{R}G$-submodule of V, then so is the perpendicular space $U^{\perp_\beta}$ defined as

$$U^{\perp_\beta} = \{v \in V \mid \beta(u, v) = 0 \text{ for all } u \in U\}.$$

Proof. By elementary results on bilinear forms, $U^{\perp_\beta}$ is a subspace of V. Moreover $U^{\perp_\beta}$ is G-stable: if $u \in U$, $v \in U^{\perp_\beta}$ and $g \in G$, then $\beta(u, vg) = \beta(ug^{-1}, v) = 0$. □

Lemma 3.3. Let V be a vector space over $\mathbb{R}$ with bilinear forms α and β such that α is positive definite. Moreover, let $u, v \in V$ such that $\beta(u, u) < 0 < \beta(v, v)$. Then there exists a basis $\{e_k\}$ of V such that

$$\begin{aligned} &\alpha(e_j, e_k) = \delta_{jk}, \\ &\beta(e_j, e_k) = 0 \text{ if } j \neq k, \\ &\beta(e_1, e_1) < 0 < \beta(e_2, e_2). \end{aligned}$$

Proof. Let $\{\tilde{e}_k\}$ be a basis for V that is orthogonal with respect to α, *i.e.,*

$$\alpha(\tilde{e}_j, \tilde{e}_k) = \delta_{jk}.$$

Let $B = (b_{jk})$ be the symmetric matrix such that $b_{jk} = \beta(\tilde{e}_j, \tilde{e}_k)$. By a fundamental result on symmetric matrices, there exists a matrix $Q = (q_{jk})$ such that $QQ^t = I$ (*i.e.,* Q is orthogonal) and QBQ^t is diagonal. Let $e_j = \sum_k q_{jk}\tilde{e}_k$. Then

$$\begin{aligned} &\alpha(e_j, e_k) = \delta_{jk}, && \text{since } QIQ^t = I, \text{ and} \\ &\beta(e_j, e_k) = 0 \text{ if } j \neq k, && \text{since } QBQ^t \text{ is diagonal.} \end{aligned}$$

Finally, suppose $\beta(e_k, e_k) \geq 0$ for all k. Then $\beta(u, u) \geq 0$ for all $u \in V$, which contradicts the hypotheses. Wlog, $\beta(e_1, e_1) < 0$ and similarly, $0 < \beta(e_2, e_2)$. □

Proposition 3.4. Let V be an $\mathbb{R}G$-module with G-invariant, symmetric, bilinear form β. If there exist $u, v \in V$ such that $\beta(u, u) < 0 < \beta(v, v)$, then V is reducible.

Proof. Let α be the G-invariant, symmetric, positive-definite, bilinear form on V as provided by Proposition 3.1, and let $\{e_k\}$ be the basis for V as provided by Lemma 3.3. Let $\lambda = \beta(e_2, e_2)^{-1} \in \mathbb{R}$ and for $u, v \in V$, define

$$\gamma(u, v) = \alpha(u, v) - \lambda\beta(u, v).$$

Because α and β are G-invariant, symmetric, bilinear forms on V, so is γ. Moreover, γ is a non-zero, degenerate bilinear form on V: if $v \in V$ and $v = \sum_k v_k e_k$ where $v_k \in \mathbb{R}$, then

$$\gamma(e_1, e_1) = \alpha(e_1, e_1) - \lambda\beta(e_1, e_1) > 1,$$

and

$$\gamma(v, e_2) = v_1\gamma(e_2, e_2) = v_2\left(\alpha(e_2, e_2) - \lambda\beta(e_2, e_2)\right) = 0.$$

Thus, $V^{\perp_\gamma}$ is a non-trivial, proper, $\mathbb{R}G$-submodule, so V is reducible. □

Theorem 3.5. An irreducible character χ of G can be realized over $\mathbb{R}$ iff there exists a $\mathbb{C}G$-module with character χ and a non-zero, G-invariant, symmetric, bilinear form.

Proof. If χ can be realized over $\mathbb{R}$, then there exists an $\mathbb{R}G$-module U with character χ. Let α be the G-invariant, symmetric, positive-definite, bilinear form on U as provided by Proposition 3.1. Let $\{e_k\}$ be a basis for U, and let V be the $\mathbb{C}G$-module with the same basis (as constructed in section 2). For $u, v \in V$ such that $v = \sum_j u_j e_j$ and $v = \sum_k v_k e_k$ where $u_k, v_k \in \mathbb{C}$, define

$$\beta(u,v) = \sum_{j,k} u_j v_k \alpha(e_j, e_k).$$

This is a non-zero, G-invariant, symmetric, bilinear form on V.

Conversely, if V is a $\mathbb{C}G$-module with character χ and non-zero, G-invariant, symmetric, bilinear form β, then there exist $u, v \in V$ such that $\beta(u,v) \neq 0$. Observe that

$$\beta(u+v, u+v) = \beta(u,u) + \beta(v,v) + 2\beta(u,v),$$

so at least one choice of $w = u, v, u+v$ has $\beta(w,w) \neq 0$. Let $\{e_k\}$ be a basis for V with $e_1 = w\beta(w,w)^{-1/2}$. Then $\{e_k, \mathrm{i}e_k\}$ is a basis for the $\mathbb{R}G$-module $V_{\mathbb{R}}$ as seen in section 2. Let σ be the natural bijection from $V_{\mathbb{R}}$ to V: let $\sigma\colon V_{\mathbb{R}} \to V$, taking

$$\sum_k (a_k e_k + b_k(\mathrm{i}e_k)) \longmapsto \sum_k (a_k + \mathrm{i}b_k) e_k$$

For $u, v \in V_{\mathbb{R}}$ define

$$\gamma(u,v) = \mathrm{Re}[\beta(\sigma u, \sigma v)].$$

Notice that γ is G-invariant, symmetric and bilinear because β is and because σ is a linear G-map. Observe that

$$\gamma(e_1, e_1) = \beta(e_1, e_1) = 1, \qquad \gamma(\mathrm{i}e_1, \mathrm{i}e_1) = \mathrm{i}^2\gamma(e_1, e_1) = -1,$$

so we may apply Proposition 3.4 to see that $V_{\mathbb{R}}$ is reducible and by Proposition 2.1, χ is realizable over $\mathbb{R}$. □

4. The Indicator Function

Definition. For χ an irreducible character of G, define the *indicator* ι on χ:

$$\iota\chi = \langle \chi_S - \chi_A, 1_G \rangle = \langle \chi_S, 1_G \rangle - \langle \chi_A, 1_G \rangle.$$

Notice that

$$\begin{aligned} \langle \chi_S, 1_G \rangle + \langle \chi_A, 1_G \rangle &= \langle \chi_S + \chi_A, 1_G \rangle \\ &= \langle \chi^2, 1_G \rangle = \langle \chi, \overline{\chi} \rangle = \begin{cases} 0, & \text{if } \chi \text{ is not real,} \\ 1, & \text{if } \chi \text{ is real.} \end{cases} \end{aligned}$$

So if χ is not real then $\iota\chi = \langle \chi_S, 1_G \rangle = \langle \chi_A, 1_G \rangle = 0$, and if χ is real then either $\langle \chi_S, 1_G \rangle = 1$, or $\langle \chi_A, 1_G \rangle = 1$ but not both. Thus,

$$\iota\chi = 0, \pm 1 \quad \text{and} \quad \iota\chi \neq 0 \Leftrightarrow \chi \text{ is real.}$$

Lemma 4.1. If V and W are $\mathbb{C}G$-modules, with $\mathbb{C}G$-homomorphism $\pi\colon V \to W$ between them, then there is a $\mathbb{C}G$-submodule, $U \subseteq V$ such that $V = U \oplus \mathrm{Ker}\,\pi$ and $U \cong \mathrm{Im}\,\pi$.

Theorem 4.2. Let V be an irreducible $\mathbb{C}G$-module with character χ.

(1) There exists a non-zero G-invariant, bilinear form β on V iff $\iota\chi \neq 0$.
(2) β is symmetric iff $\iota\chi = 1$, and β is symplectic iff $\iota\chi = -1$.

Proof. (1) Suppose β is a non-zero, G-invariant, bilinear form on V. Let $\{e_k\}$ be a basis for V. Then $\{e_j \otimes e_k\}$ forms a basis for $V \otimes V$. Define $\pi\colon V \otimes V \to \mathbb{C}$ by

$$\pi(e_j \otimes e_k) = \beta(e_j, e_k),$$

extending linearly to all of $V \otimes V$. This is a non-zero $\mathbb{C}G$-homomorphism because β is a non-zero G-invariant bilinear form. By Lemma 4.1, $V \otimes V$ has a trivial $\mathbb{C}G$-submodule, so $\left\langle \chi^2, 1_G \right\rangle = 1$ and thus $\iota\chi \neq 0$.

Conversely, suppose that $\iota\chi \neq 0$. Then $\left\langle \chi^2, 1_G \right\rangle = 1$ and $V \otimes V$ has a trivial $\mathbb{C}G$-submodule, $U \cong \mathbb{C}$. Then the natural projection $\pi\colon V \otimes V \to U$ is a non-zero $\mathbb{C}G$-homomorphism, and $\beta(u, v) = \pi(u \otimes v)$ is a non-zero, G-invariant, bilinear form on V, since π is a non-zero $\mathbb{C}G$-homomorphism.

(2) Since $V \otimes V = \mathrm{Sym}(V \otimes V) \oplus \mathrm{Alt}(V \otimes V)$ we may write

$$\pi = \pi_S + \pi_A$$

where $\pi_S\colon\ \mathrm{Sym}(V \otimes V) \to \mathbb{C}$, and $\pi_A\colon\ \mathrm{Alt}(V \otimes V) \to \mathbb{C}$, given explicitly by

$$\pi_S(u \otimes v) = \tfrac{1}{2}\pi(u \otimes v + v \otimes u),$$
$$\pi_A(u \otimes v) = \tfrac{1}{2}\pi(u \otimes v - v \otimes u).$$

If $\iota\chi = 1$, then the trivial $\mathbb{C}G$-submodule U lies entirely inside $\mathrm{Sym}(V \otimes V)$, so $\pi_A = 0$, and $\beta(v, u) = \pi_S(v \otimes u) = \pi_S(u \otimes v) = \beta(u, v)$. If $\iota\chi = -1$, then the trivial $\mathbb{C}G$-submodule U lies entirely inside $\mathrm{Alt}(V \otimes V)$, so $\pi_S = 0$, and $\beta(v, u) = \pi_A(v \otimes u) = -\pi_A(u \otimes v) = -\beta(u, v)$. □

Now it is simply a matter of pulling together the various pieces into the final result due to Frobenius and Schur, often called the "Count of Involutions," after its last part. This result not only turns the question of realizability over $\mathbb{R}$ into a simple matter of computing the indicator function, but also it provides a deep relationship between the internal structure of the and the values of the indicator on the irreducible characters of the group.

Corollary 4.3 (The Frobenius-Schur Count of Involutions)**.**
For each irreducible character χ of G,

$$\iota\chi = \begin{cases} 0, & \text{if } \chi \text{ is not real,} \\ 1, & \text{if } \chi \text{ is realizable over } \mathbb{R}, \\ -1, & \text{if } \chi \text{ is not realizable over } \mathbb{R}. \end{cases} \tag{1}$$

Furthermore, for all $g \in G$,

$$\sum_{\chi} (\iota\chi)\chi(x) = \left|\left\{ y \in G \mid y^2 = x \right\}\right|, \tag{2}$$

and in particular

$$\sum_{\chi} (\iota\chi)\chi(1) = \sum_{\chi} (\iota\chi)(\dim\chi) = 1 + t \tag{3}$$

where t is the number of involutions in G.

Proof. (1) follows immediately from Theorems 3.5, and 4.2.

(2) Let $\vartheta\colon G \to \mathbb{C}$ be defined by

$$\vartheta(x) = \left|\left\{ y \in G \mid y^2 = x \right\}\right|.$$

Note that ϑ is a class function on G, and therefore is a linear combination of the irreducible characters of G, so we may sensibly take its inner product with χ:

$$\langle \vartheta, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \vartheta(g)\chi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2) = \langle \chi_S - \chi_A, 1_G \rangle = \iota\chi.$$

Writing ϑ as a sum of its constituents yields $\vartheta = \sum(\iota\chi)\chi$ as desired.

(3) The count of involutions itself is simply the special case of (2) for $g = 1$. $\square$

References

1. Gordon James and Martin Liebeck, *Representations and characters of groups*, Cambridge Mathematical Textbooks, ch. 22 Real Representations, pp. 260–278, Cambridge University Press, Cambridge, UK, 1993.