LIFTING MODULAR REPRESENTATIONS OF FINITE GROUPS

BURTON FEIN

Let \((\pi)\) be the maximal ideal of the ring \(R\) of \(P\)-integral elements of an algebraic number field \(K\), where \(P\) is a prime of \(K\) dividing the rational prime \(p\). The natural homomorphism from \(R\) to \(\overline{K} = R/(\pi)\) induces a map \(S \rightarrow \overline{S}\) from the set of representations by matrices with coefficients in \(R\) of a finite group \(G\) into the set of representations of \(G\) in \(\overline{K}\). The lifting problem in modular representation theory is to determine whether for a given representation \(T\) of \(G\) in \(\overline{K}\) there exists a representation \(S\) of \(G\) by \(R\)-matrices such that \(\overline{S} = T\). In this paper we introduce a notion of lifting projective modular representations from characteristic \(p\) to characteristic zero and show how this concept may be applied to the lifting problem.

**Notation.** Throughout this paper \(G\) denotes a finite group of order \(|G|\) and \(K\) denotes an algebraic number field which is a splitting field for \(G\). Let \(p\) be a rational prime and let \(R\) be the ring of \(P\)-integral elements of \(K\), where \(P\) is a prime of \(K\) dividing \(p\). Let \((\pi)\) be the maximal ideal of \(R\) and set \(\overline{K} = R/(\pi)\). \(\overline{K}\) is a finite field of characteristic \(p\) which is a splitting field for \(G\). For \(a \in R\), set \(\overline{a} = a + (\pi) \in \overline{K}\). If \(A = (a_{ij})\) is a matrix with entries in \(R\) (\(R\)-matrix) we denote by \(\overline{A}\) the matrix \((\overline{a}_{ij})\). By a linear representation of \(G\) in a field \(L\) we shall understand a homomorphism from \(G\) into \(GL(m, L)\) for some \(m\). By a projective integral representation (resp. projective modular representation) of \(G\) in \(R\) (resp. \(\overline{K}\)) we mean a map \(T\) of \(G\) into \(GL(m, R)\) (resp. \(GL(m, \overline{K})\)) satisfying \(T(1) = 1_m\), \(T(g)T(h) = \alpha(g, h) \cdot T(gh)\) where \(\alpha(g, h) \in R\) (resp. \(\overline{K}\)) and \(T(g)\) has entries in \(R\) (resp. \(\overline{K}\)) for all \(g, h \in G\). \(\alpha\) is called the factor set associated with \(T\). If \(\alpha(g, h) = 1\) for all \(g, h \in G\), \(T\) is a linear integral representation (resp. linear modular representation). We identify linear representations with projective representations having trivial factor sets. We refer the reader to [3] and [7] for the relevant theory.

**Definition.** Let \(T\) be a projective modular representation of \(G\) in \(\overline{K}\) and let \(\alpha\) be the associated factor set. \(T\) is **projectively liftable** if there exists a projective integral representation \(S\) of \(G\) in \(R\) with factor set \(\beta\) such that \(\overline{S}(g) = T(g)\) for all \(g \in G\). If \(\alpha(g, h) = 1\) for all \(g, h \in G\) (i.e. \(S\) and \(T\) are linear representations), we say that \(T\) is **liftable.**

Received by the editors November 1, 1966.

This research was supported by NSF Grant GP-5497.
We emphasize that, according to the above definition, if we speak of a modular representation $T$ of $G$ in $\bar{K}$ being liftable to an integral representation $S$ of $G$ in $R$, then both $T$ and $S$ must be linear representations of $G$.

**Lemma 1.** Let $T$ and $W$ be projectively equivalent projective modular representations of $G$ of degree $m$ in $\bar{K}$. If $T$ is projectively liftable, then so is $W$.

**Proof.** By assumption there exists a function $\gamma$ from $G$ to $\bar{K}$ and a matrix $U \in GL(m, \bar{K})$ such that $U^{-1}T(g)U = W(g)\gamma(g)$ for all $g \in G$. Let $V \in GL(m, K)$ having entries in $R$ such that $V = U$ and let $\alpha$ be a function from $G$ to $R$ such that $\alpha^{-1}(g) = \gamma(g)$. $\det V$ is a unit in $R$ so $V^{-1}$ has entries in $R$. Hence if $S$ is a projective integral representation which projectively lifts $T$, $V^{-1}SV\alpha$ is a projective lifting of $W$.

The next lemma will permit us to take finite extensions of $K$.

**Lemma 2.** Let $K_1$ be a finite extension of $K$ and let $R_1$ be the ring of $P_1$-integral elements of $K_1$, where $P_1$ is a prime of $K_1$ dividing the prime $P$ of $K$, i.e. $P_1 \cap K = P$. Let $(\pi_1)$ be the maximal ideal of $R_1$ and view $\bar{K}$ as a subfield of $\bar{K}_1 = R_1/(\pi_1)$. Let $T$ be an irreducible linear modular representation of $G$ in $\bar{K}$. If $T$ is liftable when viewed as a $\bar{K}_1$-representation, then $T$ is liftable as a $\bar{K}$-representation.

**Proof.** The lemma is a consequence of the fact that the decomposition matrix of $G$ for the prime $p$ does not depend on $K$ [3, Chapter 12].

**Theorem 1.** Let $G$ be a finite group and suppose that $p \mid |H^2(G, E^*)|$ where $E^*$ is the multiplicative group of an algebraic closure $E$ of $K$ and where $G$ acts trivially on $E^*$. Let $T$ be an irreducible linear modular representation of $G$ in $\bar{K}$ which is projectively liftable. Then $T$ is liftable.

**Proof.** By assumption there is a projective integral representation $S$ of $G$ in $R$ with factor set $\alpha$ such that $S(g) = T(g)$ for all $g \in G$ and $\alpha(g, h) = 1$ for all $g, h \in G$. Let $e$ be the order of $\alpha$ in $H^2(G, E^*)$. Then $\alpha$ is equivalent to $\alpha'$ where $\alpha'(g, h)$ is an $e$th root of unity for all $g, h \in G$ [3, p. 360]. There exists a function $\rho$ from $G$ to $E^*$ such that $\alpha'(g, h) = \alpha(g, h)\rho(g, h)\rho^{-1}(g)\rho^{-1}(h)$ for all $g, h \in G$. In view of Lemma 2 we may assume that $\rho(g) \in K$ for all $g \in G$. Let $\rho(g) = \pi^{r(g)}\gamma(g)$ where $\gamma(g)$ is a unit in $R$ and $\nu(g)$ is an integer. Since $\alpha'(g, h) \neq 0$, $\alpha(g, h) \neq 0$ for all $g, h \in G$, $\nu(g) + \nu(h) = \nu(gh)$. Therefore $\alpha'(g, h) = \alpha(g, h)\gamma(gh)\gamma^{-1}(g)\gamma^{-1}(h)$ for all $g, h \in G$. Let $\gamma^{-1}(g) = \lambda(g)$ and set $Z(g) = \lambda(g)S(g)$ for all $g \in G$. $Z$ is a projective integral representation of $G$ in $R$ with factor set $\alpha'$. $Z$ is projectively equivalent over $\bar{K}$ to $T$. We may assume that $K$ contains a primitive $(|\bar{K}| - 1)$-th root of
unity $\delta$ over the rationals. Define a function $\mu$ from $G$ to the integers by $\lambda(g) = \delta^{\mu(g)}$ where $1 \leq \mu(g) \leq |K| - 1$. Set $\eta(g) = \delta^{-\mu(g)}$ and let $V(g) = \eta(g)Z(g)$. $V$ is a projective integral representation of $G$ in $R$ such that $\overline{V} = T$. The factor set $\beta$ associated with $V$ satisfies

$$\beta(g, h) = \alpha'(g, h)\eta^{-1}(gh)\eta(g)\eta(h)$$

for all $g, h \in G$. Since $\beta(g, h)$ is a root of unity with $\beta(g, h) = 1$ for all $g, h \in G$, we see that $\{\beta\}$ has order $\rho^b$ in $H^2(G, E^*)$. Since $\rho \mid H^2(G, E^*)$ by assumption, $\beta$ is equivalent to the unit factor set. Therefore there is a function $\tau$ from $G$ to $E^*$ such that

$$\beta(g, h) = \tau(g\alpha)\tau^{-1}(g)\tau^{-1}(h)$$

for all $g, h \in G$. As before we may assume that $\tau(g) \in R$ for all $g \in G$. Let $W(g) = \tau(g)V(g)$. $W$ is a projective integral representation of $G$ in $R$ and $\overline{W}(g) = \tau(g)\overline{V}(g) = \tau(g)T(g)$ for all $g \in G$. Since $\beta(g, h) = 1$ for all $g, h \in G$, $\overline{W}$ is a linear modular representation of $G$ in $\overline{K}$. Let $\overline{\tau}(g) = \overline{\delta}(g)$ where $1 \leq \theta(g) \leq |K| - 1$. Let $M(g) = \delta^{\theta(g)}W(g)$ for all $g \in G$. $M$ is a linear integral representation of $G$ in $R$ and $\overline{M} = T$ and so $T$ is liftable.

We refer the reader to [3, p. 361] for the definition and construction of a representation-group of a finite group with respect to an algebraically closed field (see also [7]). A representation-group $G^*$ of $G$ with respect to $E$ is a central extension of $G$ with kernel $A \cong H^2(G, E^*)$ with the following property: Let $T$ be a projective representation of degree $m$ of $G$ in $E$. Then if $\{u_g: g \in G\}$ is a set of coset representatives of $A$ in $G^*$, there exists a projective representation $T'$ of $G$ in $E$ which is projectively equivalent to $T$ and a linear representation $S$ of $G^*$ with $S(a) \in E^* \cdot 1_m$ for all $a \in A$ and $S(u_g) = T'(g)$ for all $g \in G$. If $S$ and $T'$ have this relationship we say that $S$ linearizes $T'$. Let $\overline{E}$ be an algebraic closure of $\overline{K}$. If $\rho \mid H^2(G, E^*)$, then a representation-group for $G$ with respect to $E$ is also one with respect to $\overline{E}$ [1, Satz 2].

**Definition.** We say that $G$ has property $(\rho, m)$ if every irreducible linear modular representation of degree $m$ of $G$ in $\overline{K}$ is liftable.

In view of Lemma 2 we see that property $(\rho, m)$ does not depend on the splitting field chosen.

**Lemma 3.** Let $G^*$ be a representation-group for $G$ with respect to $E$ and suppose that $K$ is a splitting field for both $G$ and $G^*$. Assume also that $\rho \mid H^2(G, E^*)$ and $G^*$ has property $(\rho, m)$ (with respect to $\overline{K}$). Let $T$ be an absolutely irreducible projective modular representation of degree $m$ of $G$ in $\overline{K}$. Then there exists a finite extension $K_1$ of $K$ such that, in the context of Lemma 2, $T$ is projectively liftable (to an $R_1$-representation) when viewed as a representation of $G$ in $\overline{K}_1$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. As noted above $G^*$ is a representation-group for $G$ with respect to both $E$ and $E$. $T$ is projectively equivalent over $E$ to an irreducible projective representation $T'$ of $G$ in $E$, where $T'$ is linearizable. Let $S$ be a linear representation of $G^*$ in $E$ which linearizes $T'$. Hence there is a finite extension $L$ of $K$ such that the entries of $S(h)$ and $T'(g)$ lie in $L$ for all $h \in G^*$ and all $g \in G$ and $T'$ is projectively equivalent to $T$ over $L$. In view of Lemma 1 we may assume that $T = T'$. There exists a finite extension $K_1$ of $K$ containing a valuation ring $R_1$ with maximal ideal $(\pi_1)$ such that $L = K_1 = R_1/(\pi_1)$. Since $K_1$ is a splitting field for $G^*$, $G^*$ has property $(\rho, m)$ with respect to $K_1$. $S$ is an irreducible linear modular representation of degree $m$ of $G$ in $K_1$ and so $S$ is liftable. Let $V$ be a linear integral representation of $G^*$ in $R_1$ with $V(h) = S(h)$ for all $h \in G^*$, $G^*$ is a central extension of $G$ with kernel $A$, say. If $a \in A$, then $S(a) = \lambda(a)1_m$ with $\lambda(a) \in K_1$. $V(a) = \mu(a)1_m$, with $\mu(a) = \lambda(a)$. Let $\{u_g : g \in G\}$ be a set of coset representatives of $A$ in $G^*$. Set $U(g) = V(u_g)$ for all $g \in G$. Then $U$ is a projective lifting of $T$, $T$ being viewed as a $K_1$-representation. This proves the result.

Theorem 2. Let $G$ be a finite group possessing an abelian normal subgroup $A$ such that every proper subgroup of $B = G/A$ is $p$-solvable. Suppose also that $p \nmid |H^2(G, E^*)|$, $p \nmid |H^2(B, E^*)|$ and that the algebraic number field $K$ is now a splitting field for all subquotients of $G^*$ and $B^*$, where $G^*$ and $B^*$ are some two representation-groups of $G$ and $B$ respectively. If $B^*$ possesses property $(\rho, m)$ (with respect to $K$) then so does $G$.

Proof. Let $T$ be an irreducible linear modular representation of degree $m$ of $G$ in $K$ and let $T_A$ denote the restriction of $T$ to $A$. By Clifford's Theorem we have

$$T_A \sim e(T_1 + \cdots + T_r)$$

where $T_1, \cdots, T_r$ are inequivalent conjugate irreducible linear representations of $A$ in $K$. Since $K$ is also a splitting field for $A$ and $A$ is abelian, each of the $T_i$'s has degree one.

Case 1. $r > 1$. Let $I$ be the inertia group of $T_1$ in $G$ and view $eT_1$ as a representation $W$ of $I$. $I \subseteq A$ and $I$ is a proper subgroup of $G$ so $I$ is $p$-solvable. $W$ is an irreducible linear modular representation of $I$ in $K$ such that $W^I \sim T$, where $W^I$ is the induced representation of $W$ to $G$ [3, p. 348]. Since $I$ is $p$-solvable, there exists an irreducible linear integral representation $S$ of $I$ in $K$ with $S(g) = W(g)$ for all $g \in I$ [6, Theorem 6]. Let $V = S^g$, $\overline{V}$ and $\overline{S}^g = W^g \sim T$ have the same character and the same degree. Since $T$ is irreducible, $\overline{V} \sim T$ and so $T$ is liftable.
Case 2. \( r = 1 \). We have \( T \sim C \times D \) (Kronecker product) where \( C, D \) are irreducible projective representations of \( G \) in \( \overline{E} \) such that \( C \) is one-dimensional and \( D(g) = 1_m \) for \( g \in A \) [3, Theorem 51.7]. Extending \( K \) if necessary, we may assume that the entries of \( C(g), D(g) \) lie in \( \overline{K} \) for all \( g \in G \), that \( T \) is equivalent to \( C \times D \) over \( \overline{K} \), and that \( D \) is projectively liftable with respect to \( \overline{K} \). We refer to Lemmas 2 and 3 to justify this step. \( C \) is projectively liftable since \( C \) is a 1-dimensional representation. Hence \( C \times D \) is projectively liftable and it follows from Theorem 1 that \( T \) is liftable.

Remark. The hypothesis that \( p \nmid H^2(G, E^*) \) is satisfied, for example, when \( G \) has a cyclic Sylow \( p \)-subgroup [5, p. 49]. If \( p \) is a prime, \( p \geq 5 \), then \( LF(2, p) \) is a minimal simple group [4, Chapter 12]. The hypotheses of Theorem 2 are satisfied when \( p \nmid |A|, B = G/A \cong LF(2, p) \) where \( p \geq 5 \), \( \overline{K} \) has characteristic \( p \), and \( m = (p - 1)/2 \) or \( (p+1)/2 \) [2, p. 590].

References


4. L. Dickson, Linear groups, Leipzig, 1901.


University of California, Los Angeles