MASCHKE'S THEOREM OVER GENERAL FIELDS

KEITH CONRAD

Let G be a finite group. If V is a finite-dimensional $\mathbf{C}$-vector space on which there is a representation of G, then Maschke's theorem says every subrepresentation of V has a complementary subrepresentation: if W is a $\mathbf{C}[G]$-submodule of V then $V = W \oplus W'$ for some $\mathbf{C}[G]$-submodule W' of V (it's not just a subspace: G carries W' back to itself). A standard proof of Maschke's theorem uses a G-invariant Hermitian inner product on V: if $\langle \cdot, \cdot \rangle$ is any Hermitian inner product on V (for example, one defined relative to a choice of basis of V) then we can create a G-invariant Hermitian inner product on V by averaging:

$$\langle v, v' \rangle_G = \frac{1}{|G|} \sum_{s \in G} \langle s(v), s(v') \rangle.$$

The function $\langle \cdot, \cdot \rangle_G \colon V \times V \to \mathbf{C}$ is easily checked to be a Hermitian inner product on V. For example $\langle v, v \rangle_G = (1/|G|) \sum_{s \in G} \langle s(v), s(v) \rangle \geq 0$, with equality if and only if $v = 0$ since $\langle s(v), s(v) \rangle \geq 0$ with equality if and only if $s(v) = 0$, which is the same as $v = 0$. The function $\langle \cdot, \cdot \rangle$, by construction, is G-invariant: $\langle g(v), g(v') \rangle_G = \langle v, v' \rangle$ for all $v, v' \in V$ and $g \in G$. Therefore if W is a $\mathbf{C}[G]$-submodule of V, its orthogonal subspace

$$W^{\perp} = \{v \in V : \langle w, v \rangle_G = 0 \text{ for all } w \in W\}$$

is also a $\mathbf{C}[G]$-submodule of V because

$$v \in W^{\perp}, w \in W, g \in G \Rightarrow \langle w, g(v) \rangle_G = \langle g^{-1}(w), v \rangle_G = 0,$$

the last equality following from $g^{-1}(w)$ lying in W. Thus $g(W^{\perp}) \subset W^{\perp}$ for all $g \in G$. From the way Hermitian inner products work, $V = W \oplus W^{\perp}$.

Is Maschke's theorem still true if we replace $\mathbf{C}$ by an arbitrary field k? That is, if V is a finite-dimensional k-vector space on which there is a representation of G, does every subrepresentation of V have a complementary subrepresentation? The averaging technique used above would run into problems if $|G| = 0$ in k (which happens if k has positive characteristic p and $|G|$ is divisible by p), so we will assume $|G| \neq 0$ in k, which is automatically true if k has characteristic 0. Another problem with extending the proof technique above to general fields is that *Hermitian* inner products rely heavily on $\mathbf{C}$ having the complex conjugation operation. Replacing the Hermitian inner product on a complex vector space by a nondegenerate bilinear form on a k-vector space (like the dot product relative to a basis) will not help us, because an orthogonal subspace relative to a nondegenerate bilinear form need not be complementary to the original subspace: necessarily $\dim(W) + \dim(W^{\perp}) = \dim(V)$, but $W \cap W^{\perp}$ might be nonzero so we might *not* have $V = W \oplus W^{\perp}$. For example, on k^2 with the nondegenerate bilinear form $\langle (x, y), (x', y') \rangle = xx' - yy'$, the subspace $W = k(1, 1)$ has $W^{\perp} = W$.

It turns out we can prove Maschke's theorem for representations of a finite group over field other than $\mathbf{C}$ with an averaging trick, but we need to drop the use of bilinear forms to find the complementary subrepresentation.

Theorem 1. *Let V be a finite-dimensional k-vector space on which there is a representation of a finite group G. If $|G| \neq 0$ in k then each $k[G]$-submodule W of V has a complementary $k[G]$-submodule: there is a $k[G]$-submodule W' such that $V = W \oplus W'$.*

Proof. The result is obvious if $W = V$ (use $W' = \{0\}$) or $W = \{0\}$ (use $W' = V$), so we can assume W is a nonzero proper subspace of V. By extending a basis of W to a basis of V, we can write $V = W \oplus \widetilde{W}$ where $\widetilde{W}$ is the span of the part of that basis of V not lying in W. While $\widetilde{W}$ is a subspace complement of W, it has no reason to be carried back to itself under the action of G. Still, it's going to be useful that $W + \widetilde{W} = V$ and $W \cap \widetilde{W} = \{0\}$.

Let $\mathrm{pr}\colon V \to W$ be the projection from V to W using the direct sum decomposition $V = W \oplus \widetilde{W}$. This is obviously k-linear, but it is not obvious whether it preserves the G-action. The map $f\colon V \to V$ defined as the average

$$f(v) = \frac{1}{|G|}\sum_{s\in G} s(\mathrm{pr}(s^{-1}(v))) \tag{1}$$

is k-linear, has values in W since pr has values in W and W is a $k[G]$-submodule of V, and f preserves the G-action: $f(g(v)) = g(f(v))$ for all $v \in V$ and $g \in G$. Indeed, for $g \in G$ and $v \in V$,

$$\begin{aligned} f(g(v)) &= \frac{1}{|G|}\sum_{s\in G} s(\mathrm{pr}(s^{-1}(gv))) \\ &= \frac{1}{|G|}\sum_{s\in G} (gs)(\mathrm{pr}((gs)^{-1}(gv))) \\ &= \frac{1}{|G|}\sum_{s\in G} (gs)(\mathrm{pr}(s^{-1}g^{-1}(gv))) \\ &= g\left(\frac{1}{|G|}\sum_{s\in G} s(\mathrm{pr}(s^{-1}(v)))\right) \\ &= g(f(v)). \end{aligned}$$

For $w \in W$ we have $s^{-1}(w) \in W$ for all $s \in G$, so

$$f(w) = \frac{1}{|G|}\sum_{s\in G} s(\mathrm{pr}(s^{-1}(w))) = \frac{1}{|G|}\sum_{s\in G} s(s^{-1}(w)) = \frac{1}{|G|}\sum_{s\in G} w = \frac{1}{|G|}|G|w = w.$$

Therefore $f\colon V \to W$ has the "projection property" $f^2 = f$: for each $v \in V$, $f(v) \in W$ so $f(f(v)) = f(v)$, and thus $f^2(v) = f(v)$.

Set $W' = \ker(f)$. This subspace of V is a $k[G]$-submodule: if $f(w') = 0$ then $f(g(w')) = g(f(w')) = g(0) = 0$. We will prove $V = W \oplus W'$.

First we show $V = W + W'$. For $v \in V$ we can write $v = f(v) + (v - f(v))$, with $f(v) \in W$. The difference $v - f(v)$ is in W' since $f(v - f(v)) = f(v) - f^2(v) = f(v) - f(v) = 0$.

Next we show $W \cap W' = \{0\}$. If $w \in W \cap W'$ then $w \in W \Rightarrow f(w) = w$, while $w \in W' \Rightarrow f(w) = 0$. Thus $w = 0$. □

It is important in the definition of f in (1) that we have s^{-1} on the inside of the formula. The modified function $F\colon V \to V$ defined by

$$F(v) = \frac{1}{|G|}\sum_{s\in G} s(\mathrm{pr}(v))$$

has values in W but F need not preserve the G-action. Here is an example of that.

Example 2. Let $G = \{e, g\}$ have order 2 and let G act on $V = k^2$ (where $2 \neq 0$ in k) by having e act as the identity and g act as the coordinate swap: $g\binom{x}{y} = \binom{y}{x}$. Then $W = k\binom{1}{1}$ is a subrepresentation of V and a complementary subspace to W is $\widetilde{W} = k\binom{1}{0}$. Then $\binom{x}{y} = \binom{y}{y} + \binom{x-y}{0}$ expresses each element of V according to the decomposition $W \oplus \widetilde{W}$, so $\operatorname{pr}\binom{x}{y} = \binom{y}{y}$. Then

$$F\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{2}\left(\operatorname{pr}\begin{pmatrix} x \\ y \end{pmatrix} + g\left(\operatorname{pr}\begin{pmatrix} x \\ y \end{pmatrix}\right)\right) = \frac{1}{2}\left(\begin{pmatrix} y \\ y \end{pmatrix} + g\begin{pmatrix} y \\ y \end{pmatrix}\right) = \frac{1}{2}\left(\begin{pmatrix} y \\ y \end{pmatrix} + \begin{pmatrix} y \\ y \end{pmatrix}\right) = \begin{pmatrix} y \\ y \end{pmatrix},$$

so $F(g\binom{x}{y}) = F\binom{y}{x} = \binom{x}{x}$ while $g\left(F\binom{x}{y}\right) = g\binom{y}{y} = \binom{y}{y}$. Thus when $x \neq y$ in k we have $F(g\binom{x}{y}) \neq g(F\binom{x}{y})$.

Unlike $\ker f$ in the proof of Theorem 1, $\ker F = k\binom{1}{0}$ is *not* a subrepresentation of k^2.

The condition that $|G| \neq 0$ in k in Theorem 1 is necessary for the proof to work, since the formula for f involves division by $|G|$. If $|G| = 0$ in k then problems really can occur: a subrepresentation need not have a complementary subrepresentation.

Example 3. Let k be a field with prime characteristic p and $G = \mathbf{Z}/(p)$. Then there is a representation of G on $V = k^2$ by $a \cdot \binom{x}{y} = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\binom{x}{y} = \binom{x+ay}{y}$.

The subspace $W = k\binom{1}{0}$ is a subrepresentation of V that has no complementary subrepresentation in V: if W' were a complementary subrepresentation of W then $\dim(W') = 1$ and each element of G has W' as an eigenspace. In particular, W' is an eigenspace for the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Its only eigenvalue in k is 1 and its 1-eigenspace in V is W, so we have a contradiction.

Theorem 4. *Let k be a field with prime characteristic p, G be a finite group of p-power order, and V be a finite-dimensional k-vector space on which there is a nontrivial representation of G. Then some subrepresentation of V does not have a complementary subrepresentation.*

This theorem is about groups with order equal to a power of p, not groups with the weaker property of having order divisible by p.

Proof. We begin by showing every representation of G on a nonzero finite-dimensional k-vector space U has a one-dimensional trivial subrepresentation. Pick $u \neq 0$ in U. Then $W = \mathbf{F}_p[G]u$ is an $\mathbf{F}_p$-vector subspace of V that is G-stable and *finite*, so the action of G on W is an action of a finite p-group on a finite set. A theorem about group actions says that for an action of a finite p-group on a finite set, the number of fixed points is divisible by p. Since 0 is a fixed point, there must be a nonzero fixed point $w \in W$. Then $g(w) = w$ for all $g \in G$, so kw is a one-dimensional subspace of U on which G acts trivially.

Returning to the theorem we want to prove, assume every subrepresentation of V has a complementary subrepresentation. Then forming nonzero complementary subrepresentations until we can't go any further (this will happen since $\dim_k(V)$ is finite), V is a direct sum of subrepresentations V_i that are irreducible: each one is nonzero and has no proper nonzero subrepresentations. From the first paragraph, each V_i has a one-dimensional subrepresentation on which G acts trivially, so by irreducibility V_i is a one-dimensional trivial representation of G. Then the direct sum V is a trivial representation of G, which is a contradiction of the hypothesis that V is not a trivial representation for G. $\square$