Solutions to Homework #6

1. The goal of this problem is to prove the general case of Maschke's Theorem: *If G is a finite group and F is any field with* $\mathrm{char}(F) \nmid |G|$*, then any representation of G over F is completely reducible.*

The key part of the proof is the following lemma.

Lemma: *Let G and F be as above, (ρ, V) a representation of G over F and W a G-invariant subspace. Then there exists a G-invariant subspace U such that $V = W \oplus U$.*

Maschke's theorem follows immediately by repeated applications of this lemma (or by induction on $\dim V$).

To prove the lemma, consider the following maps. Choose any subspace Z of V such that $V = W \oplus Z$ and let $P : V \to W$ be the projection onto W along Z, that is, P is the unique linear map such that $P(w) = w$ for all $w \in W$ and $P(Z) = 0$. Now define $Q : V \to V$ by

$$Q(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} P \rho(g)(v).$$

Prove that

(i) $Q(w) = w$ for all $w \in W$ and $\mathrm{Im}(Q) = W$. Deduce that $Q^2 = Q$.

(ii) $\mathrm{Ker}(Q)$ is G-invariant

Deduce from (i) that $V = W \oplus \mathrm{Ker}(Q)$ and therefore $U = \mathrm{Ker}(Q)$ has the desired property.

Solution: (i) If $w \in W$, then $\rho(g)(w) \in W$ and hence $P\rho(g)(w) = P(\rho(g)(w)) = \rho(g)(w)$. Thus $Q(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1}\rho(g)(w) = \frac{|G|}{|G|} w = w$.

Since $Q(w) = w$ for all $w \in W$, we must have $W \subseteq \mathrm{Im}(Q)$. On the other hand, for every $v \in V$ we have $P\rho(g)(v) \in W$ (since $\mathrm{Im}(P) = W$) and hence $\rho(g)^{-1}P\rho(g)(v) \in W$ (since W is $\rho(g)^{-1}$-invariant). Thus, $Q(v) \in W$ and hence $\mathrm{Im}(Q) \subseteq W$. Thus we proved that $\mathrm{Im}(Q) = W$.

Finally, the equality $Q^2 = Q$ is equivalent to saying that Q restricted to its image is the identity mapping. The latter follows immediately from the first two assertions of (i).

(ii) It is not hard to check G-invariance of $\mathrm{Ker}(Q)$ directly. We will give a more conceptual argument by showing that $Q : V \to V$ is a homomorphism of representations (from (ρ, V) to (ρ, V)). Once this is done, we simply deduce that $\mathrm{Ker}(Q)$ is G-invariant from Lemma 13.4.

Take any $h \in G$. Then $\rho(h)^{-1}Q\rho(h) = \rho(h)^{-1}\frac{1}{|G|}\sum_{g\in G}\rho(g)^{-1}P\rho(g)\rho(h) = \frac{1}{|G|}\sum_{g\in G}\rho(h)^{-1}\rho(g)^{-1}P\rho(g)\rho(h) = \frac{1}{|G|}\sum_{g\in G}\rho(gh)^{-1}P\rho(gh)$ (where the last step holds since ρ is a homomorphism).

Since the map $g \mapsto gh$ is a bijection from G to G, the last expression is equal to Q itself. Thus, $\rho(h)^{-1}Q\rho(h) = Q$ or, equivalently, $Q\rho(h) = \rho(h)Q$ for all $h \in G$, that is, Q is a homomorphism of representations.

Finally, we explain why $V = W \oplus \mathrm{Ker}(Q)$. Indeed, since Q restricted to its image is the identity mapping, we must have $\mathrm{Ker}(Q) \cap \mathrm{Im}(Q) = 0$. And since $\dim \mathrm{Ker}(Q) + \dim \mathrm{Im}(Q) = \dim V$ by the rank-nullity theorem, we deduce that $V = \mathrm{Im}(Q) \oplus \mathrm{Ker}(Q) = W \oplus \mathrm{Ker}(Q)$. Thus, $U = \mathrm{Ker}(Q)$ is a G-invariant complement of W we were looking for.

Remark: Recall that in this class we restrict ourselves to representations on finite-dimensional spaces. However, the statement of Maschke's theorem remains true even if we allow V to be infinite-dimensional. The proof given above needs to be modified in two places. First, one can no longer deduce Maschke's theorem from Lemma by induction (or iterated applications of Lemma). Instead one needs to use something called Zorn's Lemma. Second, in the last step of the proof we cannot apply rank-nullity theorem. This step is easy to modify, as we can deduce that $\mathrm{Im}(Q) + \mathrm{Ker}(Q) = V$ directly from $Q^2 = Q$. Indeed, for every $v \in V$ we have $v = Qv + (v - Qv)$, and $Qv \in \mathrm{Im}(Q)$ while $v - Qv \in \mathrm{Ker}(Q)$ since $Q(v - Qv) = Qv - Q^2v = 0$.

2. Given a vector space V, let $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ (we previously denoted this set by $\mathcal{L}(V)$). Elements of $\mathrm{End}(V)$ are called *endomorphisms of* V. If X is an algebraic structure (e.g. group, ring, vector space), an endomorphism of X is a homomorphism from X to itself.

(a) Prove that $\mathrm{End}(V)$ is a ring with 1 (where addition is the usual pointwise addition of maps and multiplication is given by composition). Clearly state where you use the fact that elements of $\mathrm{End}(V)$ are linear maps.

Now suppose that (ρ, V) is a representation of some group G. Let $\mathrm{End}_\rho(V)$ be the set of those elements of $\mathrm{End}(V)$ which are homomorphisms of representations (from (ρ, V) to (ρ, V)). Prove that

(b) $\mathrm{End}_\rho(V)$ is a subring of $\mathrm{End}(V)$ which contains 1 and also that $\mathrm{End}_\rho(V)$ is a vector subspace of $\mathrm{End}(V)$.

(c) If $g \in G$ is a central element, then $\rho(g) \in \mathrm{End}_\rho(V)$.

Solution: (a) Verification of the ring axioms is straightforward, so we will only mention where linearity needs to be used. First, we naturally need to refer to linearity to prove that $\mathrm{End}(V)$ is closed under both addition and composition. The only other axiom where linearity is used is distributivity on the right: given $R, T, S \in \mathrm{End}(V)$ and $v \in V$, we have

$$\begin{aligned}(R(T+S))(v) &= R((T+S)(v)) = R(T(v)+S(v) \\ &= R(T(v)) + R(S(v)) = RT(v) + RS(v) = (RT+RS)(v).\end{aligned}$$

The equality $R(T(v)+S(v) = R(T(v)) + R(S(v))$ uses linearity of R.

Note that distributivity on the left does not use linearity. Perhaps even more surprisingly, $Func(V,V)$, the set of all functions from V to V, does satisfy almost all ring axioms (including closure under addition and composition) except for distributivity on the right.

(b) We need to show that $\mathrm{End}_\rho(V)$ contains 0, I (the identity operator), is closed under addition, composition and scalar multiplication. We will check closure under composition (the other verifications are similar). let $S, T \in \mathrm{End}_\rho(V)$. Then $S\rho(g) = \rho(g)S$ and $T\rho(g) = \rho(g)T$ for all $g \in G$. Hence $(ST)\rho(g) = S(T\rho(g)) = S(\rho(g)T) = (S\rho(g))T = (\rho(g)S)T = \rho(g)(ST)$, so $ST \in \mathrm{End}_\rho(V)$.

(c) Let $g \in Z(G)$, the center of G. Then for all $h \in G$ we have $gh = hg$, whence $\rho(g)\rho(h) = \rho(gh) = \rho(hg) = \rho(h)\rho(g)$, and therefore $\rho(g) \in \mathrm{End}_\rho(V)$.

3. At the beginning of Lecture 14 we will show that if G is an abelian group, then any irreducible representation of G over an algebraically closed field is one-dimensional (this is a straightforward consequence of Corollary 13.5)

(a) Let $n > 2$ be an integer. Construct an irreducible representation of $\mathbb{Z}_n$ over $\mathbb{R}$ (reals) which is not one-dimensional.

(b) Prove that any irreducible representation of $\mathbb{Z}_2$ over any field is one-dimensional.

(c) (bonus) Describe (with proof) all finite abelian groups G such that any irreducible representation of G over any field is one-dimensional.

Solution: (a) Let $V = \mathbb{R}^2$ and $A \in GL(V)$ the rotation by $\frac{2\pi}{n}$. Then $A^n = I$, so there exists a representation (ρ, V) of $\mathbb{Z}_n$ with $\rho([1]) = A$.

We claim that (ρ, V) is irreducible. Indeed, a rotation by an angle in the interval $(0, \pi)$ does not preserve any lines, so there are no 1-dimensional A-invariant subspaces. Since $A = \rho([1])$, V does not have any 1-dimensional G-invariant subspaces. But $\dim(V) = 2$, so the only subspaces of V which are not 1-dimensional are 0 and V. This implies that (ρ, V) is irreducible.

(b) and (c) Let G be a finite abelian group. We claim that any irreducible representation of G over any field is one-dimensional $\iff$ all elements of G have order at most 2. By the classification theorem this is equivalent to saying that G is a direct product of several copies of $\mathbb{Z}_2$.

"$\Rightarrow$" We argue by contrapostive. Suppose that G has an element of order > 2. We want to construct an irreducible representation of G which is not 1-dimensional.

By the classification theorem we can write G as a direct product $G = A \times B$ where A is cyclic of order > 2. By (a), there is an irreducible representation $\rho : A \to GL(V)$ with $\dim(V) > 1$. Let $\pi : G \to A$ be the projection onto the first component. Then $\rho \circ \pi : G \to GL(V)$ is a representation of G.

We claim that $(\rho \circ \pi, V)$ is also irreducible (as a G-representation). Indeed, let $W \subseteq V$ be a G-invariant subspace. This means that W is $\rho(\pi(g))$-invariant for every $g \in G$. Since $\pi : G \to A$ is surjective, this means that W is $\rho(a)$-invariant for every $a \in A$. And since (ρ, V) is irreducible as an A-representation, we deduce that $W = 0$ or V.

"$\Leftarrow$" Suppose now that all elements of G have order at most 2 (for this direction we do not need to use the fact that G is finite).

By Corollary 14.2 from class any irreducible representation of any abelian group over an algebraically closed field is 1-dimensional. An analysis of the proof yields a more general statement where we do not have to assume that the field is algebraically closed. Let H be an abelian group, and let (ρ, V) be an irreducible representation of V over some field. If for every $h \in H$ the operator $\rho(h)$ has at least one eigenvector $v \in V$, then $\dim(V) = 1$.

Thus, we only need to verify the latter condition in our case. Let (ρ, V) be a representation of G. By assumption for every $g \in G$ we have $g^2 = e$ and hence $\rho(g)^2 = I$ or equivalently, $(\rho(g) + I)(\rho(g) - I) = 0$. If $\rho(g) = I$, then any nonzero $v \in V$ is an eigenvector, and we are done. And if $\rho(g) \neq I$, choose w such that $v = (\rho(g) - I)w$ is nonzero. Then $(\rho(g) + I)(v) = 0$, so $\rho(g)v = -v$ and v is an eigenvector.

4. Let (α, V) and (β, W) be representations of the same group over the same field. The *tensor product* of these representations is the representation $(\rho, V \otimes W)$ where $\rho(g) = \alpha(g) \otimes \beta(g)$ for each $g \in G$ (in the notations from Problem 2 in HW#5). In other words, $\rho(g) \in GL(V \otimes W)$ is the unique linear map such that $\rho(g)(v \otimes w) = (\alpha(g)v) \otimes (\beta(g)w)$ for all $v \in V$ and $w \in W$.

(a) Prove that $(\rho, V \otimes W)$ is indeed a representation, that is, $\rho : G \to GL(V \otimes W)$ is a homomorphism.

(b) Prove that if (α, V) is NOT irreducible and $W \neq 0$, then $(\rho, V \otimes W)$ is not irreducible either.

(c) Now prove that if (α, V) is irreducible and $\dim(W) = 1$, then $(\rho, V \otimes W)$ is irreducible.

Solution: (a) We need to show that $\rho(gh) = \rho(g)\rho(h)$ for all $g, h \in G$. Since both $\rho(gh)$ and $\rho(g)\rho(h)$ are linear maps from $V \otimes W$ to $V \otimes W$ and since $V \otimes W$ is spanned by simple tensors, it suffices to check that

$$\rho(gh)(v \otimes w) = (\rho(g)\rho(h))(v \otimes w) \text{ for all } v \in V, w \in W.$$

By definition of the tensor product of two maps we have $\rho(gh)(v \otimes w) = (\alpha(gh) \otimes \beta(gh))(v \otimes w) = (\alpha(gh)v) \otimes (\beta(gh)w)$. On the other hand,

$$\begin{aligned}(\rho(g)\rho(h))(v \otimes w) &= \rho(g)(\rho(h)(v \otimes w)) \\ &= \rho(g)(\alpha(h)v \otimes \beta(h)w) = (\alpha(g) \otimes \beta(g))(\alpha(h)v \otimes \beta(h)w) \\ &= (\alpha(g)\alpha(h)v) \otimes (\beta(g)\beta(h)w) = (\alpha(gh)v) \otimes (\beta(gh)w).\end{aligned}$$

(b) Let $U \neq 0, V$ be a G-invariant subspace; in other words, U is $\alpha(g)$-invariant for all $g \in G$. Since $W \neq 0$, it is straightforward to check that $U \otimes W$ considered as a subspace of $V \otimes W$ is not equal to 0 or $V \otimes W$. Thus, if we show that $U \otimes W$ is $\rho(g)$-invariant for all $g \in G$, it would follow that $(\rho, V \otimes W)$ is not irreducible.

Since $U \otimes W$ is spanned by simple tensors, it suffices to show that $\rho(g)(u \otimes w) \in U \otimes W$ for all $u \in U$ and $w \in W$. By definition $\rho(g)(u \otimes w) = \alpha(g)u \otimes \beta(g)w$. The vector $\beta(g)w$ automatically lies in W and $\alpha(g)u \in U$ since U is $\alpha(g)$-invariant. Thus, $\rho(g)(u \otimes w) \in U \otimes W$, as desired.

(c) We start with a lemma:

Lemma: *Fix a nonzero element $w_0 \in W$. Then for every $z \in V \otimes W$ there exists unique $v \in V$ such that $z = v \otimes w_0$.*

Proof: We know that z can be written as a sum of simple tensors $z = \sum_{i=1}^{k} v_i \otimes w_i$ for some $v_i \in V$ and $w_i \in W$. Since $\dim(W) = 1$, we can write $w_i = \lambda_i w_0$ for some $\lambda_i \in F$. But then $z = \sum_{i=1}^{k} v_i \otimes (\lambda_i w_0) = (\sum_{i=1}^{k} \lambda_i v_i) \otimes w_0$. This proves the existence part.

Now take any $v \neq v' \in V$ and let $u = v - v'$. Then $u \neq 0$, so we can find a basis β of V with $u \in \beta$. Since $\{w_0\}$ is a basis of W, the set $\beta \otimes w_0$ is a basis of $V \otimes W$, and since $u \otimes w_0 \in \beta \otimes w_0$, we conclude that $u \otimes w_0 \neq 0$. But $u \otimes w_0 = (v - v') \otimes w_0 = v \otimes w_0 - v' \otimes w_0$, so $v \otimes w_0 \neq v' \otimes w_0$. Thus, $v \neq v'$ implies $v \otimes w_0 \neq v' \otimes w_0$. This proves the uniqueness part. $\square$

Let us go back to (c). We will assume that $(\rho, V \otimes W)$ is not irreducible and deduce that (α, V) is not irreducible. So assume that there exists a G-invariant subspace Z of $V \otimes W$ with $Z \neq 0, V \otimes W$. By Lemma Z has the form $U \otimes w_0$ for some (uniquely defined) subset U of V, and since Z is a subspace, U must also be a subspace; moreover, $U \neq 0, V$. If we show that U is G-invariant, we will be done.

Take any $u \in U$. Then $u \otimes w_0 \in Z$. Since Z is G-invariant, we have $\rho(g)(u \otimes w_0) \in Z$, and hence $\rho(g)(u \otimes w_0) = u' \otimes w_0$ for some $u' \in U$. On the other hand,

$$\rho(g)(u \otimes w_0) = \alpha(g)u \otimes \beta(g)w_0 = \beta(g)\alpha(g)u \otimes w_0.$$

Here we can move $\beta(g)$ from the second component to the first component because $\dim(W) = 1$ and hence $\beta(g)$ is a SCALAR! If $\dim(W) \neq 1$, such a transition would have been completely false; in fact, even the expression $\beta(g)\alpha(g)u$ would not make sense.

Thus, we conclude that $u' \otimes w_0 = \beta(g)\alpha(g)u \otimes w_0$, and by the uniqueness part of the Lemma $u' = \beta(g)\alpha(g)u$. Again since $\beta(g)$ is a (nonzero) scalar and since $u' \in U$, we get $\alpha(g)u = \frac{1}{\beta(g)}u' \in U$. This shows that U is G-invariant and completes the proof.