Solutions to Homework #7

0. Prove that $[S_n, S_n] = A_n$ for every $n \geq 2$ (where A_n is the alternating group).

Solution: Since $[f, g] = f^{-1}g^{-1}fg$ is an even permutation for all $f, g \in S_n$ and since A_n is a subgroup, we conclude that $[S_n, S_n] \subseteq A_n$.

For the opposite inclusion, first note that every 3-cycle (a, b, c) lies in $[S_n, S_n]$ since $(a, b, c) = (a, b)(a, c)(a, b)(a, c) = (a, b)^{-1}(a, c)^{-1}(a, b)(a, c) = [(a, b), (a, c)]$. Hence $[S_n, S_n]$ contains the subgroup generated by all 3-cycles. Thus, to prove that $A_n \subseteq [S_n, S_n]$ it suffices to show that A_n is generated by 3-cycles.

Take any $g \in A_n$ and write it as a product of transpositions. Since g is even, the number of transpositions in this product is even, so we can write g as a product of pairs of transpositions $(x, y)(z, w)$. It is enough to represent each such $(x, y)(z, w)$ as a product of 3-cycles. If $\{x, y\} = \{z, w\}$ as sets, then $(x, y)(z, w) = e$, and we can simply eliminate the corresponding pair of transpositions. If the sets $\{x, y\}$ and $\{z, w\}$ have one element in common, WOLOG we can assume that $y = z$ (and x, y, w are distinct), in which case $(x, y)(z, w) = (x, z)(z, w) = (x, z, w)$. Finally, if $\{x, y\}$ and $\{z, w\}$ are disjoint, we write $(x, y)(z, w) = (x, y)(y, z)(y, z)(z, w) = (x, y, z)(y, z, w)$.

1. Let $G = D_{2n}$ be the dihedral group of order $2n$. Recall that G has a presentation $G = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1}\rangle$.

(a) Let $\omega \in \mathbb{C}$ be an n^{th} root of unity (that is, $\omega^n = 1$). Prove that G has a representation $\rho_\omega : G \to GL_2(\mathbb{C})$ such that $\rho(r) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$ and $\rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

(b) Prove that the representation ρ_ω in part (a) is irreducible if and only if $\omega \neq \pm 1$.

(c) Let ω_1 and ω_2 be n^{th} roots of unity different from ± 1. Prove that $\rho_{\omega_1} \cong \rho_{\omega_2}$ (as representations of G) if and only if $\omega_2 = \omega_1$ or $\omega_2 = \omega_1^{-1}$.

(d) Since we can think of isometries of a regular $2n$-gon as invertible linear operators on $\mathbb{R}^2$, we get a 2-dimensional representation of G "for free" (simply representing the elements of D_{2n} by their matrices with respect to the standard basis). If we assume that r is the counterclockwise rotation by $\frac{2\pi}{n}$ and s is the reflection with respect to the x-axis, the corresponding ρ is given by $\rho(r) = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}$ and $\rho(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Note that technically ρ is a real representation (a homomorphism from G to $GL_2(\mathbb{R})$), but since every 2×2 real matrix can be thought of as a 2×2 complex matrix, we can think of ρ as a complex representation. Prove that this ρ is equivalent to some ρ_ω from part (a), explicitly find such ω as well as a matrix $T \in GL_2(\mathbb{C})$ such that $T^{-1}\rho(g)T = \rho_\omega(g)$ for all $g \in G$.

(e) In class we proved that $|G^{ab}|$ (which we know equals the number of one-dimensional complex representations of G) is equal to 2 if n is odd and 4 if n is even. Now describe all one-dimensional complex representations of G explicitly (it is enough to specify the images of r and s under these representations).

Solution: (a) Let $A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. By Theorem A, we just need to verify the relations $A^n = B^2 = I$ and $BAB^{-1} = A^{-1}$, which is done by a (simple) direct computation.

(b) "$\Rightarrow$" We argue by contrapositive. Suppose that $\omega = \pm 1$. Then by direct computation the vector $v = e_1 + e_2$ is an eigenvector for both $\rho_\omega(r)$ and $\rho_\omega(s)$, so $W = \mathbb{C}v$ is both $\rho_\omega(r)$-invariant and $\rho_\omega(s)$-invariant.

Let $H = Stab_G(W)$ be the stabilizer of W in G, that is, $H = \{g \in G : W \text{ is } \rho_\omega(g)\text{-invariant}\}$. It is easy to check that H is a subgroup (this is a general statement not using any specific properties of G or ρ_ω), and we just saw that H contains both r and s. Since r and s generate G, we conclude that $H = G$. This is equivalent to saying that W is G-invariant and hence ρ_ω is not irreducible.

"$\Leftarrow$" Suppose that $\omega \neq \pm 1$. The only subspaces of $\mathbb{C}^2$ different from 0 and $\mathbb{C}^2$ are 1-dimensional. Thus, to prove that ρ_ω is irreducible, we just need to show that there are no G-invariant 1-dimensional subspaces.

Since $\omega \neq \pm 1$, we have $\omega^{-1} \neq \omega$ and hence the only 1-dimensional $\rho_\omega(r)$-invariant subspaces are $\mathbb{C}e_1$ and $\mathbb{C}e_2$. Neither of these subspaces is $\rho_\omega(s)$-invariant, so ρ_ω is irreducible.

(c) "$\Rightarrow$" Suppose that $\rho_{\omega_1} \cong \rho_{\omega_2}$, so there exists $T \in GL_2(\mathbb{C})$ such that

$T^{-1}\rho_{\omega_1}(g)T = \rho_{\omega_2}(g)$ for all $g \in G$. In particular, $T^{-1}\begin{pmatrix}\omega_1 & 0\\ 0 & \omega_1^{-1}\end{pmatrix}T = \begin{pmatrix}\omega_2 & 0\\ 0 & \omega_2^{-1}\end{pmatrix}$. Since eigenvalues of a matrix do not change under conjugation, we must have $\{\omega_1, \omega_1^{-1}\} = \{\omega_2, \omega_2^{-1}\}$ as sets, so $\omega_2 = \omega_1$ or $\omega_2 = \omega_1^{-1}$.

"$\Leftarrow$" Now suppose that $\omega_2 = \omega_1$ or $\omega_2 = \omega_1^{-1}$. We need to find $T \in GL_2(\mathbb{C})$ such that $T^{-1}\rho_{\omega_1}(g)T = \rho_{\omega_2}(g)$ for all $g \in G$. Since G is generated by r and s, it is enough to find T which satisfies the above equation for $g = r$ and $g = s$ (this is because the conjugation by a fixed element is an automorphism of a group or, in more plain terms, T-conjugate of a product is equal to the product of T-conjugates). If $\omega_2 = \omega_1$, we can simply set $T = I$, and if $\omega_2 = \omega_1^{-1}$, then $T = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ does the job.

(d) Let $\omega = e^{\frac{2\pi i}{n}}$ and $T = \begin{pmatrix}1 & 1\\ -i & i\end{pmatrix}$. By direct computation we check that $T^{-1}\rho(r)T = \rho_\omega(r)$ and $T^{-1}\rho(s)T = \rho_\omega(s)$. Arguing as in (c), we deduce that $T^{-1}\rho(g)T = \rho_\omega(g)$ for all $g \in G$ and hence $\rho_\omega \cong \rho$.

(e) Let a and b denote the images of r and s in G^{ab}, respectively. Then a and b commute and must also satisfy the respective relations between r and s, that is, $a^n = b^2 = 1$ and $bab^{-1} = a^{-1}$ or, equivalently, $bab^{-1}a^{-1} = a^{-2}$. Since $ab = ba$, we deduce that $a^{-2} = 1$ or equivalently, $a^2 = 1$.

Case 1: n is odd. In this case $a^n = 1$ and $a^2 = 1$ force $a = 1$. Thus, any 1-dimensional complex representation of G^{ab} must send a to 1 and b to ± 1 (the latter holds since $b^2 = 1$). So we have at most two choices, and since $|G^{ab}| = 2$, both possibilities occur. Thus, there are two 1-dimensional complex representations of G – the trivial representation, which sends both r and s to 1, and the other representation which sends r to 1 and s to -1.

Case 2: n is even. In this case $a^n = 1$ follows from $a^2 = 1$. Since $a^2 = b^2 = 1$, we have (at most) 4 possibilities for 1-dimensional complex representations (send a to ± 1 and b to ± 1). Again since $|G^{ab}| = 4$, all 4 possibilities occur. The corresponding representations of G have the same description with a and b replaced by r and s, respectively.

2. Given a field F, the *Heisenberg group over* F is the group $Heis(F)$ consisting of all 3×3 upper unitriangular matrices in $GL_3(F)$, that is, matrices of the form $\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix}$ with $a, b, c \in F$. Denote by $E_{ij}(\lambda)$ the matrix which has 1's on the diagonal, λ in the position (i, j) and 0 everywhere else.

Let $G = Heis(\mathbb{Z}_p)$ for some prime p.

(a) Prove that $[G, G] = \{E_{13}(\lambda) : \lambda \in \mathbb{Z}_p\}$ and that $G^{ab} \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

(b) Let $x = E_{12}([1])$, $y = E_{23}([1])$ and $z = E_{13}([1])$ where $[1]$ is the unity element of $\mathbb{Z}_p$. Prove that

$$G = \langle x, y, z \mid x^p = 1, y^p = 1, z^p = 1, xz = zx, yz = zy, x^{-1}y^{-1}xy = z\rangle$$

(c) Describe all one-dimensional complex representations of G.

Solution: (a) Let $Z = \{E_{13}(\lambda) : \lambda \in \mathbb{Z}_p\}$. By direct computation each commutator $[g, h]$ with $g, h \in G$ lies in Z. Since Z is clearly a subgroup, we conclude that $[G, G] \subseteq Z$. On the other hand, $[E_{13}(\lambda)] = [E_{12}(\lambda), E_{23}(1)] \in [G, G]$ for every $\lambda \in \mathbb{Z}_p$, so $Z \subseteq [G, G]$.

Now we prove that $G^{ab} \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Define the map $\pi : G \to \mathbb{Z}_p \times \mathbb{Z}_p$ by $\pi\left(\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}\right) = (a, b)$. By direct computation π is a homomorphism, clearly π is surjective and $\operatorname{Ker} \pi = Z = [G, G]$. Thus, by the first isomorphism theorem $G^{ab} = G/[G, G] \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

(b) Let $\widetilde{G}$ be the group with the presentation $\langle X, Y, Z \mid X^p = 1, Y^p = 1, Z^p = 1, XZ = ZX, YZ = ZY, X^{-1}Y^{-1}XY = Z\rangle$. In other words, $\widetilde{G}$ is a group generated by abstract symbols X, Y, Z which satisfy the above six relations and where all other relations follow from those six. [1] Now define a map $\varphi : \widetilde{G} \to G$ by

$$\varphi(w(X, Y, Z)) = w(x, y, z).$$

In other words, we take $g \in \widetilde{G}$, write it as $w(X, Y, Z)$, some word in $X^{\pm 1}, Y^{\pm 1}$ and $Z^{\pm 1}$, and map it to the same word in $x^{\pm 1}, y^{\pm 1}, z^{\pm 1}$. Our goal is to prove that φ is an isomorphism (of groups). We proceed in 4 steps.

(i) φ is well defined. To justify this we just need to check that the relations $x^p = 1, y^p = 1, z^p = 1, xz = zx, yz = zy, x^{-1}y^{-1}xy = z$ do hold in G (which is done by direct computation). Let us explain why this implies that φ is well defined.

Suppose that $w(X, Y, Z) = w'(X, Y, Z)$ for some words w, w'. This means that the equality $w(X, Y, Z) = w'(X, Y, Z)$ follows (formally) from the six

[1] Here we do not address the question why such a group exists. For those of you familiar with free groups, $\widetilde{G}$ is the quotient F/N where F is the free group on 3 generators X, Y, Z and N is the smallest normal subgroup of F containing $X^p, Y^p, Z^p, (XZ)^{-1}ZX = [Z, X], (YZ)^{-1}ZY = [Z, Y]$ and $Z^{-1}X^{-1}Y^{-1}XY = Z^{-1}[X, Y]$.

defining relations of $\widetilde{G}$ (and general group axioms). Since we verified that the corresponding six relations hold in G, we can conclude that $w(x,y,z) = w'(x,y,z)$ in G as well, that is, φ is well defined.

(ii) φ is a homomorphism. This is pretty clear from the definition (once we know φ is well defined). Indeed, for any words w_1 and w_2, let w_1w_2 be their concatenation (simply write w_2 to the right of w_1). We have

$$\begin{aligned}\varphi(w_1(X,Y,Z)w_2(X,Y,Z)) &= \varphi((w_1w_2)(X,Y,Z)) = (w_1w_2)(x,y,z)\\ &= w_1(x,y,z)w_2(x,y,z) = \varphi(w_1(X,Y,Z))\varphi(w_2(X,Y,Z)).\end{aligned}$$

(iii) φ is a surjective. From the definition of φ it is clear that its image $\mathrm{Im}(\varphi)$ is the subgroup of G generated by x, y and z. But this subgroup is the entire G; for instance, we can write $\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix} = x^a y^b z^{c-ab}$ for all $a, b, c \in \mathbb{Z}_p$. Thus φ is indeed surjective.

(iv) φ is a injective. From (iii) we already know that $|\widetilde{G}| \geq |G| = p^3$. If we show the opposite inequality $|\widetilde{G}| \leq p^3$, it would follow that $|\widetilde{G}| = |G|$ and hence the surjective map $\varphi : \widetilde{G} \to G$ must be injective.

To prove that $|\widetilde{G}| \leq p^3$ it suffices to show that every element of $\widetilde{G}$ can be written as $X^aY^bZ^c$ with $0 \leq a, b, c \leq p-1$ (since the number of distinct expressions of this form is p^3). The fact that every $g \in G$ can be written as $X^aY^bZ^c$ follows easily from the defining relations. Starting with an arbitrary word in $X^{\pm 1}, Y^{\pm 1}$ and $Z^{\pm 1}$, we first make all the exponents positive (using $X^p = Y^p = Z^p = 1$). Then using $XZ = ZX$ and $X^{-1}Y^{-1}XY = Z$ (or equivalently $YX = XYZ^{-1} = XYZ^{p-1}$), we move all the X's to the left and then using $YZ = ZY$ all the Z's to the right. We then get an element of the form $X^aY^bZ^c$, and finally using $X^p = Y^p = Z^p = 1$, we move the exponents a, b, c to the interval $[0, p-1]$.

(c) Since $z = [x,y] \in [G,G]$, it must map to 1 under any 1-dimensional representation. Since $x^p = y^p = 1$, both x and y must map to p^{th} roots of unity. This already limits the number of possibilities to p^2. Since we know that $|G^{ab}| = p^2$, each of those possibilities must occur.

It is easy to describe the 1-dimensional complex representations of G explicitly as maps from G to $\mathbb{C}^\times$ (not just their images on generators). For every pair of integers $0 \leq k, l \leq p-1$ we have a unique representation

$\varphi_{k,l} : G \to \mathbb{C}^\times$ given by

$$\varphi_{k,l}\left(\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}\right) = e^{\frac{2\pi(ak+bl)i}{n}}.$$

3. A representation (ρ, V) of a group G is called **cyclic** if there exists $v \in V$ such that the smallest G-invariant subspace of V containing v is V itself.

(a) Prove that any irreducible representation is cyclic.

(b) Give an example of a cyclic representation (of some group) which is not irreducible.

Solution: (a) Let (ρ, V) be irreducible. By definition $V \neq 0$, so we can find a nonzero $v \in V$. The smallest G-invariant subspace of V containing v cannot be 0, so by irreducibility it must equal the entire V. Thus, (ρ, V) is cyclic.

(b) Let $G = \langle a \rangle$ be a cyclic group of order 2 and $\rho : G \to GL_2(\mathbb{C})$ the unique representation such that $\rho(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $\mathbb{C}e_1$ is G-invariant (so the representation is not irreducible), but the smallest G-invariant subspace containing $e_1 + e_2$ is the entire $\mathbb{C}^2$, so the representation is cyclic.

4. A representation (ρ, V) of a group G is called *faithful* if $\rho : G \to GL(V)$ is injective. Prove that if G is a finite abelian group which is NOT cyclic, then G does not have any faithful *irreducible* complex representations.

Solution: We will prove the following general result:

Theorem: *Let G be a finite group. If $\rho : G \to \mathbb{C}^\times$ is any homomorphism, then $\rho(G)$ is cyclic.*

Let us first explain why this Theorem implies the result of Problem 4. Indeed, Theorem implies that any finite non-cyclic group does not have any faithful 1-dimensional complex representations (since if ρ is faithful, then $\rho(G) \cong G$). We also know that if G is abelian, then any irreducible complex representation of G is 1-dimensional. Combining these two facts, we conclude that if G is finite abelian and not cyclic, it does not have any complex representations which are both irreducible and faithful.

Let us now prove the Theorem. Let $n = |G|$. Then $g^n = 1$ for all $g \in G$ and hence $\rho(g)^n = \rho(g^n) = 1$. In other words, $\rho(G)$ is contained in $\mu_n(\mathbb{C})$, the set of n^{th} roots of unity. But $\mu_n(\mathbb{C})$ is a subgroup of $\mathbb{C}^\times$ which is clearly cyclic generated by $e^{\frac{2\pi i}{n}}$. Thus, $\rho(G)$ is a subgroup of a cyclic group and hence itself cyclic.

5. Let (ρ_1, V_1) and (ρ_2, V_2) be equivalent representations of a group G, and let $(\rho, V_1 \oplus V_2)$ be their direct sum. Let $T : V_1 \to V_2$ be an isomorphism of representations and let $W = \{(v, T(v)) : v \in V_1\} \subset V_1 \oplus V_2$. Prove that W is a G-invariant subspace and that $(W, \rho_{|W})$ is isomorphic to (ρ_1, V_1) as a G-representation. **Note:** We will use the result of this problem in the course of the proof of orthogonality relations between characters.

Solution: We are given that $T\rho_1(g) = \rho_2(g)T$ for all $g \in G$. Hence for all $v \in V_1$ and $g \in G$ we have

$$\rho(g)(v, T(v)) = (\rho_1(g)v, \rho_2(g)Tv) = (\rho_1(g)v, T(\rho_1(g)v)) \in W.$$

Thus, W is G-invariant.

Define $S : V_1 \to W$ by $S(v) = (v, T(v))$. It is clear that S is an isomorphism of vector spaces. Finally, for every $g \in G$ and $v \in V$ we have

$$S\rho_1(g)v = (\rho_1(g)v, T(\rho_1(g)v)) = (\rho_1(g)v, \rho_2(g)Tv) = \rho(g)(v, Tv) = \rho_{|W}(g)S(v).$$

(Note that this calculation is essentially equivalent to the one we did to prove G-invariance of W). Thus, $S\rho_1(g) = \rho_{|W}(g)S$, so S is an isomorphism of representations.