

Homework #7. Due Saturday, October 30th

Reading:

1. For this homework assignment: online class notes (Lectures 14 and 15) and Steinberg, second half of 4.1.
2. Next week we will talk a bit more about groups defined by generators and relations and then move to characters of groups (Lectures 16 and 17 in online class notes and Steinberg 4.2, 4.3 and 4.4). Note that our order of exposition will be quite different from Steinberg's book.

Problems:

1. In all parts of this problem include ALL relevant computations. Make sure to read a note on pages 4-5 before starting this problem.

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 $\rho_\omega : G \rightarrow GL_2(\mathbb{C})$ 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 counter-clockwise 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) Recall that the number of one-dimensional complex representations of G is equal to $|G^{ab}|$. In online Lecture 15 it is shown that $|G^{ab}|$ is equal to 2 if n is odd and 4 if n is even (we will give a different proof in class on Tue, Oct 26). Now describe all one-dimensional complex representations of G explicitly (it is enough to specify the images of r and s under these representations).

We will soon prove that every complex irreducible representation of D_{2n} is 1-dimensional or 2-dimensional and, in the latter case, isomorphic to some ρ_ω as in part (a).

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

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

Note: You can argue similarly to the proof of Theorem 15.2 in online lecture 15 (we will also discuss the latter in class on Tue, Oct 26).

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

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.

4. 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 $T : V_1 \rightarrow V_2$ 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.

On groups defined by generators and relations

Let G a group given by a presentation $G = \langle x_1, \dots, x_k \mid R \rangle$. Let Q be another group. Note that a homomorphism $\rho : G \rightarrow Q$ is completely determined by the elements $\rho(x_i) \in Q$, with $1 \leq i \leq k$; however, given $q_1, \dots, q_k \in Q$, it is not always possible to find a homomorphism $\rho : G \rightarrow Q$ such that $\rho(x_i) = q_i$ for each i . The following proposition describes exactly when that is possible.

Theorem A: *Let $q_1, \dots, q_k \in Q$. Then a homomorphism $\rho : G \rightarrow Q$ such that $\rho(x_i) = q_i$ for each i exists \iff each relation in R holds if we substitute each x_i by q_i .*

Note: In the setting of representation theory we will be applying this result in the case when $Q = GL(V)$ for some vector space V .

Proof: “ \Rightarrow ” Let $u(x_1, \dots, x_k) = v(x_1, \dots, x_k)$ be a relation in R . Here the notations $u(x_1, \dots, x_k)$ and $v(x_1, \dots, x_k)$ indicate that both sides of the relations are words in x_i 's and their inverses. Since $\rho : G \rightarrow Q$ is a homomorphism and $\rho(x_i) = q_i$ for each i , we must have

$$\rho(u(x_1, \dots, x_k)) = u(\rho(x_1), \dots, \rho(x_k)) = u(q_1, \dots, q_k)$$

(here $u(q_1, \dots, q_k)$ is the expression obtained from $u(x_1, \dots, x_k)$ by replacing each x_i by q_i). Likewise $\rho(v(x_1, \dots, x_k)) = v(q_1, \dots, q_k)$. Thus, the equality $u(x_1, \dots, x_k) = v(x_1, \dots, x_k)$ forces $u(q_1, \dots, q_k) = v(q_1, \dots, q_k)$.

“ \Leftarrow ” Conversely, suppose that for every relation $u(x_1, \dots, x_k) = v(x_1, \dots, x_k)$ from R we have the corresponding equality $u(q_1, \dots, q_k) = v(q_1, \dots, q_k)$ in Q . Define $\rho : G \rightarrow Q$ by

$$\rho(w(x_1, \dots, x_k)) = w(q_1, \dots, q_k).$$

In other words, we take $g \in G$, represent it as word $w(x_1, \dots, x_k)$ in $x_i^{\pm 1}$ (which we always can since G is generated by x_1, \dots, x_k) and send it to the same word in q_1, \dots, q_k . It is straightforward to see that ρ constructed in this way will be a homomorphism (and will send each x_i to q_i) as long as it is WELL defined.

So why is ρ well defined? Suppose that some $g \in G$ is represented by two different words $w(x_1, \dots, x_k)$ and $w'(x_1, \dots, x_k)$, that is, we have a relation $w(x_1, \dots, x_k) = w'(x_1, \dots, x_k)$ in G . Since R is a set of defining relations, we can show that this relation holds in G ONLY using relations from R . But by assumption for each relation $a(x_1, \dots, x_k) = b(x_1, \dots, x_k)$ from R the corresponding relation $a(q_1, \dots, q_k) = b(q_1, \dots, q_k)$ in Q holds. Hence using

these relations, we can also show that $w(q_1, \dots, q_k) = w'(q_1, \dots, q_k)$, which means precisely that ρ is well-defined. \square

Presentation for the abelianization.

Theorem B: *Suppose that G has a presentation $G = \langle x_1, \dots, x_k \mid R \rangle$. Then its abelianization G^{ab} has a presentation $G^{ab} = \langle x_1, \dots, x_k \mid R \cup C \rangle$ where C is the set of commutation relations: $C = \{x_i x_j = x_j x_i : i < j\}$.*

“Proof”: (stated quite informally). In general, if we start with a presentation for some group X and add some relations, we get a presentation for some quotient of X . It is easy to see that if any two generators of a group commute, then the group is abelian. Thus, the presentation $\langle x_1, \dots, x_k \mid R \cup C \rangle$ defines an abelian quotient of G .

We know that relations R must hold in G^{ab} (since G^{ab} is a quotient of G) and relations C must hold in G^{ab} since G^{ab} is abelian. This means that G^{ab} is a quotient of the group \tilde{G} given by the presentation $\langle x_1, \dots, x_k \mid R \cup C \rangle$. But we know that \tilde{G} is an abelian quotient of G and G^{ab} is the LARGEST abelian quotient of G . Thus, the only way G^{ab} could be a quotient of \tilde{G} is if it is the quotient by the trivial subgroup, and the latter means precisely that $\langle x_1, \dots, x_k \mid R \cup C \rangle$ is a presentation for G^{ab} . \square

Corollary C: *If Q is abelian group and G is any group, then there is a natural bijection between $\text{Hom}(G, Q)$ and $\text{Hom}(G^{ab}, Q)$ where $\text{Hom}(X, Y)$ is the set of homomorphisms from a group X to a group Y .*

“Proof”: Recall that Corollary C was already proved in class (Lemma 17.2). We now give another (somewhat informal) proof using Theorems A and B. For simplicity of notation we shall assume that G is generated by finitely many elements x_1, \dots, x_k .

Choose a presentation $\langle x_1, \dots, x_k \mid R \rangle$ for G . By Theorem B, G^{ab} then has a presentation $\langle x_1, \dots, x_k \mid R \cup C \rangle$ where C is the set of commutation relations between the generators. By Theorem A we can construct all homomorphisms from G to Q by sending generators x_1, \dots, x_k of G to k -tuples (q_1, \dots, q_k) of elements of Q satisfying the relations R . Likewise, homomorphisms from G^{ab} to Q must send generators of G to k -tuples (q_1, \dots, q_k) satisfying the relations $R \cup C$ (and this is the only restriction). But since Q is abelian, the elements (q_1, \dots, q_k) will automatically satisfy the relations C . Thus, the images of x_1, \dots, x_k under homomorphisms from G^{ab} to Q satisfy exactly the same restrictions as in the case of homomorphisms from G to Q , which yields a natural bijection between $\text{Hom}(G^{ab}, Q)$ and $\text{Hom}(G, Q)$. \square