November 18, 2025

Written assignment

Exercise 1. (10 pts) Let p be a prime. Let $\mathbf{H}_p$ be the group of 3×3 upper triangular matrices with 1's on the diagonal over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with respect to the matrix multiplication.

(a) Let

$$a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Show that the element $c = aba^{-1}b^{-1}$ is central in $\mathbf{H}_p$, and that any element in $\mathbf{H}_p$ can be written uniquely as a product $a^m c^n b^k$, where $0 \leq m, n, k \leq p-1$.

(b) Give a presentation of $\mathbf{H}_p$ in generators and relations.

(c) Let $z \in \mathbb{C}$ be a p-th root of unity, $z^p = 1$ and define the map from $\mathbf{H}_p$ to the endomorphisms of the space of the complex-valued functions on $\mathbb{F}_p$ by

$$\rho_z(a)f(x) = f(x-1), \quad \rho_z(b)f(x) = z^x f(x).$$

Show that ρ_z defines a representation of $\mathbf{H}_p$.

(d) Determine the values of z for which ρ_z is irreducible, and the conditions for ρ_{z_1} and ρ_{z_2} to be inequivalent.

(e) Classify all 1-dimensional representations of $\mathbf{H}_p$.

(f) Use (c), (d), (e) and the structure theorem for semisimple finite dimensional algebras to classify the irreducible representations of $\mathbf{H}_p$.

(g) For the values of z such that ρ_z is not irreducible, decompose it as a direct sum of irreducible representations.

(h) Describe the conjugacy classes of $\mathbf{H}_p$ and compute the characters of the irreducible representations for $\mathbf{H}_p$.

Solution 1. (a) (1 point) We have

$$c = aba^{-1}b^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathrm{Id} + \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and this matrix commutes with any upper triangular 3×3 matrix with 1's on the diagonal. Then we have

$$a^m c^n b^k = \begin{pmatrix} 1 & m & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m & n \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix}.$$

With $0 \leq m, n, k \leq p-1$, this gives all elements of $\mathbf{H}_p$, and clearly $a^{m_1}c^{n_1}b^{k_1} = a^{m_2}c^{n_2}b^{k_2}$ if and only if $m_1 = m_2, n_1 = n_2, k_1 = k_2$ modulo p. This is the finite *Heisenberg group* $\mathbf{H}_p$ of order p^3.

(b) (1 point) It follows from (a) that a and b generate $\mathbf{H}_p$. The relations are $a^p = b^p = 1$ and $aba^{-1}b^{-1} = ba^{-1}b^{-1}a$, $baba^{-1} = aba^{-1}b$. The last two relations express the fact that $c = aba^{-1}b^{-1}$ is central. Note that the relation $c^p = 1$ follows from these. Indeed, using that a commutes with $ba^{-1}b^{-1}$ we get

$$c^p = (aba^{-1}b^{-1})(aba^{-1}b^{-1})(aba^{-1}b^{-1})\dots(aba^{-1}b^{-1}) = (ba^{-1}b^{-1})(ba^{-1}b^{-1})(ba^{-1}b^{-1})\dots(ba^{-1}b^{-1})a^p =$$

$$= ba^{-p}b^{-1}a^p = bb^{-1} = 1.$$

So we can consider, for example:

$$\mathbf{B}_p = \langle a, b \mid a^p = 1,\ b^p = 1,\ aba^{-1}b^{-1} = ba^{-1}b^{-1}a,\ baba^{-1} = aba^{-1}b \rangle.$$

Alternatively we can define the Heisenberg group with three generators

$$\mathbf{B}_p = \langle a, b, c \mid a^p = 1,\ b^p = 1,\ c = aba^{-1}b^{-1},\ ac = ca,\ bc = cb \rangle.$$

(1 point) We show that the abstract group $\mathbf{B}_p$ is isomorphic to the group $\mathbf{H}_p$. To do so, we can consider the map $\Phi : \mathbf{B}_p \to \mathbf{H}_p$ which is defined by sending a, b, c to a, b, c respectively. Then since every element in $\mathbf{H}_p$ can be written as $a^n b^m c^k$ it follows that Φ is surjection. To show injection, we note that $|\mathbf{B}_p| \leq p^3$ since using the relations repetitevely, we can write every element in $\mathbf{B}_p$ can be written in the form $a^n b^m c^k$, and thus number of elements are less than equal to p^3. Since Φ is surjection, it follows that $|\mathbf{B}_p| \leq p^3$ and so Φ is an isomorphism.

(c) (1 point) We have

$$\rho_z(a^k)f(x) = f(x-k), \quad \rho_z(a^p)f(x) = f(x-p) = f(x);$$
$$\rho_z(b^k)f(x) = z^{kx}f(x), \quad \rho_z(b^p)f(x) = z^{px}f(x) = f(x).$$

Also,

$$\rho_z(aba^{-1}b^{-1})f(x) = \rho_z(aba^{-1})z^{(p-1)x}f(x) = \rho_z(ab)z^{(p-1)(x-(p-1))}f(x-(p-1)) =$$
$$= \rho_z(a)z^{x+(p-1)x-(p-1)^2}f(x-(p-1)) = \rho_z(a)z^{-1}f(x+1)) = z^{-1}f(x).$$

Therefore, the element c acts by multiplication by a scalar $\rho_z(c) = z^{-1}$, and $\rho_z(c^p) = z^{-p} = 1$. We have that $\rho_z(a)\rho_z(c) = \rho_z(c)\rho_z(a)$ and $\rho_z(b)\rho_z(c) = \rho_z(c)\rho_z(b)$. Since all relations in $\mathbf{H}_p$ are satisfied, we have indeed a p-dimensional representation of $\mathbf{H}_p$.

(d) (1 point) Introduce a basis of characteristic functions $\{\delta_y\}_{y=0}^{p-1}$ from $\mathbb{F}_p$ to $\mathbb{C}$, such that $\delta_y(x) = 1$ if $y = x$ and 0 otherwise. Then we have

$$\rho_z(a)\delta_y = \delta_{y+1},$$

therefore an invariant subspace of $\rho_z(a)$ has to be of the form $\lambda \sum_{y\in\mathbb{F}_p} \delta_y$. However, we also have

$$\rho_z(b)\delta_y = z^y\delta_y, \quad \rho_z(b)\sum_{y\in\mathbb{F}_p}\delta_y = \sum_{y\in\mathbb{F}_p} z^y\delta_y.$$

Then an invariant subspace has to satisfy $\sum_{y\in\mathbb{F}_p}\delta_y = \sum_{y\in\mathbb{F}_p} z^y\delta_y$, which happens if and only if $z = 1$. Therefore ρ_z is irreducible if and only if $z \neq 1$. The representations ρ_{z_1} and ρ_{z_2} for $z_1 \neq z_2$ are inequivalent because the action of the central element c in both representations is by different constants.

(e) (1 point) In a 1-dimensional representation we have to define the action of the generators a and b by complex nonzero numbers. Since $a^p = 1, b^p = 1$, we necessarily have that $\rho(a) = \xi^k$ and $\rho(b) = \xi^m$, where $\xi = e^{\frac{2\pi i}{p}}$, for some integers $0 \leq k, m \leq p-1$. Then $\rho(c) = \rho(aba^{-1}b^{-1}) = \rho(1) = 1$ and all remaining relations are satisfied. These representations are obviously inequivalent for different pairs (k, m) with $0 \leq k, m \leq p-1$. So we have p^2 inequivalent 1-dimensional representations.

The same list of 1-dimensional representations of $\mathbf{H}_p$ can be obtained by *abelianization* of the group. Namely, the generator $c \in \mathbf{H}_p$ generates a subgroup $\langle c \rangle \subset \mathbf{H}_p$ that is normal since c is central. The quotient group $\mathbf{H}_p/\langle c \rangle = \langle a, b \,|a^p = b^p = 1, ab = ba \rangle$ is abelian and isomorphic to the direct product of two cyclic groups $C_p \times C_p$, with the inequivalent irreducible representations parametrized by the couples (k, m) with $0 \leq k, m \leq p-1$. These give rise to the 1-dimensional representations of $\mathbf{H}_p$ that we have computed above, where c acts trivially.

(f) (1 point) Since the group algebra of $\mathbf{H}_p$ is semisimple and finite dimensional over $\mathbb{C}$, it satisfies the sum of squares formula. There are $(p-1)$ p-dimensional representations corresponding to the roots of unity of degree p different from 1, and p^2 1-dimensional representations. Summing up the squares of their dimensions, we get

$$(p-1)p^2 + p^2 = p^3 = |G|.$$

Therefore, we have accounted for all inequivalent irreducible representations of $\mathbf{H}_p$.

(g) (1 point) The representation ρ_z with $z = 1$ is given by $\rho_1(a)f(x) = f(x-1)$ and $\rho_1(b)f(x) = f(x)$. Therefore $\rho_1(b) = \mathrm{Id}$ and $\rho_1(c) = \mathrm{Id}$ and the matrix of $\rho_1(a)$ in the basis of the characteristic functions is given by

$$\rho_1(a) = \begin{pmatrix} 0 & 1 & \dots & & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & & & & \\ \dots & & & 0 & 1 \\ 1 & 0 & \dots & & 0 \end{pmatrix}.$$

This matrix is diagonalizable with the eigenvalues of the form $\{\lambda_k = e^{\frac{2k\pi i}{p}}\}_{k=0}^{p-1}$. Therefore we have the decomposition

$$V_{\rho_1} = \bigoplus_{k=0}^{p-1} V_{\lambda_k},$$

where $\rho_{\lambda_k}(a) = \lambda_k$ and $\rho_{\lambda_k}(b) = 1$. These representations correspond to the couples $(k, 1)$ for $0 \leq k \leq p-1$ in the classification of the one-dimensional representations obtained in (e).

(h) (1 point) Note that $aba^{-1} = (aba^{-1}b^{-1})b = cb$ and $bab^{-1} = (bab^{-1}a^{-1})a = c^{-1}a = ac^{-1}$. Using these identities, we deduce that conjugation of $a^t c^n b^q$ by a or b only changes the power of c:

$$aa^t c^n b^q a^{-1} = a^t c^n a b^q a^{-1} = a^t c^{n+q} b^q, \qquad ba^t c^n b^q b^{-1} = ba^t b^{-1} c^n b^q = a^t c^{n-t} b^q.$$

Therefore, each pair (t, q) such that $0 \leq t, q \leq p-1$ are not both zeros, defines a conjugacy class $\{a^t c^* b^q\}$. There are $(p-1)p + (p-1) = p^2 - 1$ such conjugacy classes. In addition, each central element c^i, $i = 0, \ldots, (p-1)$ defines its own conjugacy class. We have a total of $p^2 - 1 + p$ conjugacy classes, same as the number of the irreducible representations.

(1 point) Let us compute the character of the irreducible representation ρ_z, $z \neq 1$. We have $\chi_z(c^i) = pz^{-i}$ since c^i acts by the scalar z^{-i} in the p-dimensional representation. The matrices of $\rho_z(c^*)$ and $\rho_z(b^q)$ are diagonal and the matrix of $\rho_z(a^t)$ is a nontrivial permutation matrix for all $0 \leq t, q \leq p-1$, where not both q and t are zero. Therefore the trace of the matrix $\rho_z(a^t c^* b^q)$ is zero and we have $\chi_z(a^t c^* b^q) = 0$.

Let us compute the character of the 1-dimensional irreducible representations parametrized by the couples (k, m) with $0 \leq k, m \leq p-1$. We have $\chi_{k,m}(c^i) = 1$ for all $0 \leq i \leq p-1$ since $\rho_{k,m}(c) = 1$. We have also $\chi_{k,m}(a^t c^* b^q) = \xi^{kt+mq}$, where $\xi = e^{\frac{2\pi i}{p}}$. One can check that the orthogonality relations hold.

Exercise 2. (5 pts)

(a) Let $G = C_a \times C_b$ a direct product of two cyclic groups or orders $a, b \in \mathbb{N}$. Compute the character table of G.

(b) Let N be a $n \times n$ complex matrix such that $|N_{ij}| = 1$ for all entries and $N\overline{N}^T = n\,\mathrm{Id}$. Use representation theory of finite abelian groups to show that for any $n \geq 1$ there exists a matrix N satisfying these conditions.

(c) Let M be a $n \times n$ matrix such that $M_{ij} = \pm 1$ and $MM^T = n\,\mathrm{Id}$. An example of such a matrix M is

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Use representation theory of finite abelian groups to show the existence of such M for any $n = 2^k$, $k \geq 1$.

Solution 2. (a) (2 points) Let $C = \langle t : t^a = 1 \rangle$ and $C_b = \langle s : s^b = 1 \rangle$. Then $G = C_a \times C_b$ has the elements $\{(t^k, s^m)\}_{0 \leq k \leq a, 0 \leq m \leq b}$. Each element of $G = C_a \times C_b$ constitutes a conjugacy class in G, so there are totally ab irreducible one-dimensional representations. Let $\xi = e^{2\pi i/a}$ and $\mu = e^{2\pi i/b}$. Define a one-dimensional representation χ_{ij} of G by setting that the element (t, s) acts in $\mathbb{C}_{ij}$ by multiplication by a product of ξ^i and μ^j for $0 \leq i < a$, $0 \leq j < b$, so we have $\chi_{ij}(t, s) = \xi^i \mu^j$. This gives the list of inequivalent irreducible representations of G for $0 \leq i < a$ and $0 \leq j < b$. Finally we have the entries of the square matrix of characters given by $\chi_{ij}(t^k, s^m) = \xi^{ik} \mu^{jm}$.

(b) (2 points) Let G be an abelian group of order n. Then the number of conjugacy classes are $|G|$ and so we have exactly $|G|$ irreducible representations. Let $g_1, \cdots, g_n$ be the elements and let $V_1, \cdots, V_n$ be the irreducible representations. Then the character table can be seen as a matrix N with entries $N_{ij} = \chi_{V_i}(g_j)$. The first orthogonality relation is exactly the statement that $N\overline{N}^T = n\mathrm{Id}$, which is also equivalent to mutual orthogonality of the rows of N. By the structure theorem of finite abelian groups, G is isomorphic to a direct product of cyclic groups, so we can write $G = C_{m_1} \times \cdots \times C_{m_k}$ for some k and cyclic groups C_{m_i}. Since the representations of cyclic groups C_k are given by k-th roots of unity, the elements in the character table are products of roots of unity.

For any $n \geq 1$, we can consider the character table N of the group $G = C_n$. By above, each entry of the matrix N is a root of unity, we have $N\overline{N}^T = n\mathrm{Id}$ and thus N satisfies the required conditions.

(c) (1 point) The characters of the group C_2 are reals and given by ± 1. Thus the character table of the group $G = (C_2)^k$ of order $|G| = 2^k$ has entries ± 1. Thus $M\overline{M}^T = MM^T = n\mathrm{Id}$ which is exactly the mutual orthogonality of rows and columns. This shows the existence of a $n \times n$ matrix M that satisfies the required conditions for any $n = 2^k$.

A square matrix H is said to be **Hadamard matrix** if it's entries are $+1$ or -1 and rows and columns are mutually orthogonal. The size of the matrix is said to be the order of Hadamard matrix.

Hadamard matrices are used in coding theory to construct error-correcting codes and subject of immense study. In general, it is a hard problem to construct Hadamard matrices. In fact, the Hadamard conjecture proposes that Hadamatrix matrix of order $4n$ exists for any $n \geq 1$ and is an open problem for last 150 years. In this exercise, we see how representation theory of finite abelian groups can be used to construct some Hadamard matrices and their complex generalizations.