Graduate Algebra

Homework 4

Fall 2014

Due 2014-09-24 at the beginning of class

1. Recall the quaternion group from homework 2.

   (a) Show that $Q$ has the following presentation: $Q \cong \langle i, j | i^2 = j^2 = (ij)^2 \rangle$.

   (b) Deduce that $|\text{Aut}(Q)| = 24$. [Hint: Make a list of the orders of the elements of $Q$.]

Proof. (a): If $i^2 = j^2 = ijj$ then $j = iji$ and, squaring, $j^2 = ijjj = ijj = i^4$ so $i^4 = 1$ and similarly $j^4 = (ij)^4 = 1$. Since $jj = i$ we get $ji = ij^3$ so every word in $T = \langle i, j | i^2 = j^2 = (ij)^2 \rangle$ is of the form $i^k j r$. Using $i^4 = j^4 = 1$ we deduce that as a set $T \subset \{1, i, i^2, j, ij, i^2 j, i^3 j\}$. These are all distinct because the order of $i$ is 4 and $j \notin \langle i \rangle$ (e.g., because $i$ and $j$ do not commute). Thus $T$ has order 8.

Write $I = \begin{pmatrix} -1 & 1 \\ i & i \end{pmatrix}$ and $J = \begin{pmatrix} 1 & 1 \\ i & i \end{pmatrix}$. Then $IJ = IJ^3$ and so $i \mapsto I$ and $j \mapsto J$ gives a homomorphism $T \to Q$. It is an isomorphism because it is injective between two sets of order 8.

(b): Let $\phi \in \text{Aut}(Q) = \text{Aut}(T)$. Then $\phi(i)$ and $\phi(j)$ have order 4 and $\phi(j) \notin \langle \phi(i) \rangle$. For ease of exposition, write $i^2 = j^2 = (ij)^2 = -1 \in Z(Q)$ and $k = ij$. Then $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Thus $\phi(i) \in \{\pm i, \pm j, \pm k\}$ (6 choices) and $\phi(j)$ must be in the same set and $\neq \pm \phi(i)$ (4 choices). Thus $|\text{Aut}(Q)| \leq 24$. It remains to show that each such choice yields an automorphism of $Q$.

Note that $i^2 = j^2 = k^2 = (ij)^2 = (ki)^2 = (jki)^2$ and that $i = jk$ and $j = ki$. Thus, relabelling, $Q \cong \langle j, k | j^2 = k^2 = (jk)^2 \cong \langle k, i | k^2 = i^2 = (ki)^2 \rangle$ as in each case we get the same set using the same formulae. This implies that any of the 6 choices sending $i, j$ to $i, j, k$ will produce an automorphism.

Also note that if we write $I = -i$ then $I^2 = j^2 = (jI)^2$ and we recover $i = -I$ and $k = jI$ so $Q \cong \langle j, I \rangle^2 = \langle jI \rangle^2$ simply relabelling the generators. Thus $i \mapsto -i$ and $j \mapsto j$ yields an automorphism of $Q$.

Finally, note that every one of the 24 choices sending $i, j$ to $\pm i, \pm j, \pm k$ is a composition of the two types of automorphisms described above. For $\sigma \in S_{\{i, j, k\}}$ write $\phi_\sigma$ for the automorphism sending $i, j, k$ to $\sigma(i), \sigma(j), \sigma(k)$ and write $\tau$ for the automorphism $i \mapsto -i$ and $j \mapsto j$. Then $i \mapsto -\sigma(i)$ and $j \mapsto \sigma(j)$ is $\phi_\sigma \circ \tau$; $i \mapsto \sigma(i)$ and $j \mapsto -\sigma(j)$ is $\phi_{ij} \circ \phi_\sigma \circ \tau \circ \phi_{ij}$; finally $i \mapsto -\sigma(i)$ and $j \mapsto -\sigma(j)$ is a composition of the previous two automorphisms. □

2. Let $G$ be the group $\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \rangle \subset \text{GL}(2, \mathbb{R})$. Show that the subgroup of matrices with 1-s on the diagonal is not finitely generated.

Proof. Note that

$$
\begin{pmatrix} 1 & 2^{-n} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-n} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-n} \in G
$$
Consider the map $G \to \mathbb{Q}$ given by $\begin{pmatrix} 1 & x \\ 1 & 1 \end{pmatrix} \mapsto x$ (it's $\mathbb{Q}$ because the matrices have rational entries and $\text{GL}(2, \mathbb{Q})$ is a group). It is an injective homomorphism of groups sending $G$ to a subgroup of $\mathbb{Q}$ which contains, by the above, $2^{-n}$ for all $n$. Suppose $G$ is finitely generated. Then its image in $\mathbb{Q}$ is, say generated by $\frac{m_1}{n_1}, \ldots, \frac{m_k}{n_k}$. But then $G$ inside $\mathbb{Q}$ is a subset of $\{ \sum d_i \frac{m_i}{n_i} | d_i \in \mathbb{Z} \} \subset \{ \frac{k}{n_1, \ldots, n_k} | k \in \mathbb{Z} \}$ and this does not contain $2^{-N}$ if $2^N > [n_1, \ldots, n_k]$. \hfill \Box

3. Suppose $A$ and $B$ are two groups and $f : Z_1 \to Z_2$ is an isomorphism between the subgroups $Z_1 \subset Z(A)$ and $Z_2 \subset Z(B)$.

(a) Show that $Z = \{(x, f(x)^{-1}) \in A \times B | x \in Z \}$ is a normal subgroup of $A \times B$. The quotient $A \ast_f B = A \times B/Z$ is called the **central product** of $A$ and $B$ with respect to $f$.

(b) Show that $A \to A \ast_f B$ given by $a \mapsto (a, 1)Z$ and $B \to A \ast_f B$ given by $b \mapsto (1, b)Z$ are injective homomorphisms giving $A \cap B$ as a subgroup of $A \ast_f B$ isomorphic to $Z$.

(c) Let $H$ be the Heisenberg group from homework 2. Consider the identity map $Z(H) \to Z(H)$. Show that the central product $H \ast_{id} H$ is isomorphic to the group of matrices

$$
\begin{pmatrix}
1 & a_1 & a_2 & b \\
1 & 1 & c_1 & c_2 \\
 & & 1 & \\
 & & & 1
\end{pmatrix}
$$

$a_1, a_2, b, c_1, c_2 \in \mathbb{Z}/p\mathbb{Z}$

This central product is again a Heisenberg group (think position and momentum of two particles).

**Proof.** (a): Need to show that if $(a, b) \in A \times B$ and $(x, f(x)^{-1}) \in Z$ then $(a, b)(x, f(x)^{-1})(a^{-1}, b^{-1}) \in Z$. But this is $(axa^{-1}, b(f(x)^{-1})b^{-1}) = (x, f(x)^{-1})$ since $x \in Z(A)$ and $f(x) \in Z(B)$.

(b): If $(a, 1)Z = Z$ then $(a, 1) = (x, f(x)^{-1})$ for some $x \in Z_1$. But then $f(x) = 1$ so $x = 1$ since $f$ is an isomorphism. Thus $a \mapsto (a, 1)Z$ is injective. Identically $b \mapsto (1, b)Z$ is injective. What is $A \cap B$? An element in the intersection is $(a, 1)Z$ in $A$ equal to some $(1, b)Z$ in $B$. But $(a, 1)Z = (1, b)Z$ iff $(a, 1)^{-1}(1, b) \in Z$ iff $(a^{-1}, b) \in Z$ iff $(a^{-1}, b) = (x, f(x)^{-1})$ for some $x \in Z_1$ if $a = x^{-1}$ and $b = f(x)^{-1} = f(a)$ and so the intersection consists of $(x, 1)Z = (1, f(x))Z$ for $x \in Z_1$ which means that it is $\cong Z$.

(c): Write $(a, c; b)$ as in the solution to the Heisenberg group problem from homework 2. Write $(a_1, a_2, c_1, c_2; b)$ for the matrix in this problem. Given a group $G$, what is $G \ast G$ with respect to the identity map on $Z(G)$? It is pairs $(g, h) \in G \times G$ up to the equivalence $(g, h)z = (g, hz)$ for $z \in Z(G)$.

Consider the map $\phi : (a_1, a_2, c_1, c_2; b) \mapsto ((a_1, c_1; b) \ast (a_2, c_2; 0))$. I claim this is an isomorphism. Indeed, $(a_1, a_2, c_1, c_2; b)(a_1', a_2', c_1', c_2'; b') = (a_1 + a_1', a_2 + a_2', c_1 + c_1', c_2 + c_2'; b + b' + a_1c_1' + a_2c_2')$. For $\phi$ to be a homomorphism we need to check that

$$( (a_1, c_1; b) \ast (a_2, c_2; 0))((a_1', c_1'; b') \ast (a_2', c_2'; 0)) = (a_1 + a_1', c_1 + c_1'; b + b' + a_1c_1' + a_2c_2') \ast (a_2 + a_2', c_2 + c_2'; 0)$$

and, multiplying out the LHS, this becomes

$$(a_1 + a_1', c_1 + c_1'; b + b' + a_1c_1') \ast (a_2 + a_2', c_2 + c_2'; 0) = (a_1 + a_1', c_1 + c_1'; b + b' + a_1c_1' + a_2c_2') \ast (a_2 + a_2', c_2 + c_2'; 0)$$

and this is immediate from $(g, h)(0, 0; b')$ is in the center of the Heisenberg group. It remains to check that $\phi$ is a bijection. Note that $(a, c; b) \ast (a', c'; b') = (a, c; b + b') \ast (a', c'; 0)$ in the central product (as above, since $(0, 0; b')$ is in the center) so the map is surjective. Suppose $(a, c; b) \ast (a', c'; 0)$ is trivial. Then $(a, c; b) \times (a', c'; 0) \in Z$ so $(a, c; b)$ and $(a', c'; 0)$ are in the center of $H$ and their product is 1. In other words $a = a' = c = c' = 0$ and $b = 0$. Thus $\phi$ is also injective. \hfill \Box
4. For a matrix \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{R}) \) and \( z \in \mathbb{C} \) define, if possible, \( g \cdot z = \frac{az+b}{cz+d} \).

(a) Show that \( \text{Im}(g \cdot z) = \frac{\det(g) \text{Im}(z)}{|cz+d|^2} \).

(b) Show that the subgroup \( \text{GL}(2, \mathbb{R})^+ \) of matrices with positive determinant acts on \( \mathcal{H} = \{ z \in \mathbb{C} \mid \text{Im} z > 0 \} \) via \( g \mapsto (z \mapsto g \cdot z) \).

(c) Show that this action is transitive, i.e., all of \( \mathcal{H} \) is one orbit, and compute \( \text{Stab}(i) \) and \( \text{Stab}(\zeta_3) \).

**Proof.**

(a) \[
\text{Im} g \cdot z = (2i)^{-1}(g \cdot z + \bar{y} \cdot \bar{z}) = (2i)^{-1}(\frac{az+b}{cz+d} + \frac{a\bar{z}+b}{c\bar{z}+d}) = (2i)^{-1} \frac{(ad-bc)(z-\bar{z})}{(cz+d)(c\bar{z}+d)} = \frac{\det g \text{Im} z}{|cz+d|^2}.
\]

(b) If \( \det g > 0 \) and \( \text{Im} z > 0 \) then by (a) \( \text{Im} g \cdot z > 0 \) so \( \text{GL}(2, \mathbb{R})^+ \) preserves \( \mathcal{H} \). Need to check action, i.e., that \( (gh) \cdot z = g \cdot (h \cdot z) \). But

\[
\begin{pmatrix} m & n \\ p & q \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \begin{pmatrix} m \frac{az+b}{cz+d} + n \frac{a\bar{z}+b}{c\bar{z}+d} \\ p \frac{az+b}{cz+d} + q \frac{a\bar{z}+b}{c\bar{z}+d} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z.
\]

(c) If \( z = x + iy \) then

\[
z = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \cdot i
\]

and \( \text{Im} z = \det \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} > 0 \). Thus every \( z \) is in the orbit of \( i \).

What about the stabilizers. We seek \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) such that \( \frac{a+ib}{cz+d} = i \), i.e., \( a = d \) and \( c = -b \) so \( \text{Stab}(i) = \{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \} \). We now seek \( a, b, c, d \) such that \( \frac{a\zeta_3+b}{cz+d} = \zeta_3 \) which multiplies out to \( a\zeta_3+b = c\zeta_3^2+d\zeta_3 = -c+(d-c)\zeta_3 \). Thus \( a = d-c \) and \( b = -c \) so \( \text{Stab}(\zeta_3) = \{ \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix} \} \).

\[ \square \]

5. Let \( \text{GL}(2, \mathbb{Z}) \) consist of \( 2 \times 2 \) matrices with entries in \( \mathbb{Z} \) and determinant \( \pm 1 \).

(a) Show that \( \text{GL}(2, \mathbb{Z}) \) is a group and that it acts on \( \mathbb{Z}^2 \) by matrix multiplication.

(b) Show that the set \( S = \{ \begin{pmatrix} d \\ 0 \end{pmatrix} \mid d \in \mathbb{Z}_{\geq 1} \} \) parametrizes the orbits of \( \text{GL}(2, \mathbb{Z}) \) acting on \( \mathbb{Z}^2 \), i.e., in each orbit there is a unique element from the set \( S \) and this provides a bijection between the orbits and the set \( S \). [Hint: Show that the orbit of \( \begin{pmatrix} d \\ 0 \end{pmatrix} \) consists of \( \begin{pmatrix} a \\ b \end{pmatrix} \) with \( (a, b) = d \).]
Proof. (a): Note that 
\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}
\]
so \( \text{GL}(2, \mathbb{Z}) \) is a group since \( ad - bc = \pm 1 \).

[In fact \( \text{GL}(n, \mathbb{Z}) \) is a group as \( A^{-1} = (\det A)^{-1}A^* \) where \( A^* \) has entries equal to determinants of minors of \( A \), thus integers. Since \( \det A = \pm 1 \) we deduce that \( \text{GL}(n, \mathbb{Z}) \) is a group.]

(b): Suppose \((a, b) = d \) so \( a = a'd \) and \( b = b'd \) with \((a', b') = 1 \). Then there exist integers \( p, q \) such that \( a'p + b'q = 1 \). Let \( g = \begin{pmatrix} p & q \\ -b' & -a' \end{pmatrix} \). Then \( g \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix} \) and \( \det g = 1 \). Thus \( \begin{pmatrix} a \\ b \end{pmatrix} \) is in the orbit of \( \begin{pmatrix} d \\ 0 \end{pmatrix} \). Reciprocally, suppose \( \begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot \begin{pmatrix} d \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \). Then \( pd = a \) and \( rd = b \) and so \( d \mid a, b \). But \((p, r) = 1 \) because if an integer divides the first column of the matrix then it divides the determinant, which is \( \pm 1 \).

In fact there is a typo in the statement of the problem. The zero vector \( \begin{pmatrix} 0 \\ 0 \end{pmatrix} \) is also an arbit. \( \square \)