Math 561 H **Fall 2011**
Homework 4 **Drew Armstrong**

---

1. Define the ring of quaternions $\mathbb{H} := \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}$, with the relations $\mathbf{1} = 1$ and $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$. Define the quaternion absolute value by

$$|a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}|^2 := a^2 + b^2 + c^2 + d^2.$$

Note $\mathbb{H}$ is actually isomorphic to $\mathbb{R}^4$ as a vector space, but it has more structure than $\mathbb{R}^4$.

(a) Given $q = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, define the quaternion conjugate $\bar{q} := a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$ and show that $q\bar{q} = |q|^2$.

Proof. Multiplying $q\bar{q}$ gives

$$\begin{aligned}(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = \; & a^2\mathbf{1} - ab\mathbf{i} - ac\mathbf{j} - ad\mathbf{k} \\ & + ba\mathbf{i} + b^2\mathbf{1} - bc\mathbf{k} + bd\mathbf{j} \\ & + ca\mathbf{j} + cb\mathbf{k} + c^2\mathbf{1} - cd\mathbf{i} \\ & + da\mathbf{k} - db\mathbf{j} + dc\mathbf{i} + d^2\mathbf{1}.\end{aligned}$$

Notice that the resulting array of terms is antisymmetric, so all the off-diagonal terms cancel. The remaining diagonal terms give $q\bar{q} = a^2\mathbf{1} + b^2\mathbf{1} + c^2\mathbf{1} + d^2\mathbf{1}$. □

(b) Show that $\mathbb{H}$ is actually a division algebra by finding the inverse of $q = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Note that $\mathbb{H}$ is not a field because it is not commutative.

Proof. By part (a) we know that $q\bar{q} = |q|^2\mathbf{1} + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$, where $|q|^2$ is a real number. If $q \neq 0 \in \mathbb{H}$ then $|q|^2 \neq 0 \in \mathbb{R}$, and we can divide by $|q|^2$ to get $q\frac{\bar{q}}{|q|^2} = 1$, hence

$$q^{-1} = \frac{\bar{q}}{|q|^2} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}).$$

□

(c) The nonzero quaternions $\mathbb{H}^\times$ are isomorphic to a subgroup of $GL_2(\mathbb{C})$ via the map

$$a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \leftrightarrow \begin{pmatrix} a + id & -b - ic \\ b - ic & a - id \end{pmatrix}.$$

Use this to prove that $|uv| = |u||v|$ for all $u, v \in \mathbb{H}$.

Proof. Given a quaternion $q \in \mathbb{H}$, let $[q] \in GL_2(\mathbb{C})$ denote the corresponding matrix. Then for $q = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ we have

$$\begin{aligned}\det[q] = \det\begin{pmatrix} a + id & -b - ic \\ b - ic & a - id \end{pmatrix} &= (a + id)(a - id) - (b - ic)(-b - ic) \\ &= a^2 + b^2 + c^2 + d^2 \\ &= |q|^2.\end{aligned}$$

By the multiplicativity of determinant, we conclude that for all $u, v \in \mathbb{H}$ we have

$$|uv|^2 = \det[uv] = \det[u][v] = \det[u]\det[v] = |u|^2|v|^2.$$

Taking square roots gives the result. □

[The quaternions were discovered by William Rowan Hamilton on October 16, 1843, as he was walking with his wife along the Royal Canal in Dublin. To celebrate the discovery, he immediately carved this equation into the stone of the Brougham Bridge: $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$.]

2. Recall that $\mathbb{Z}/n\mathbb{Z}$ has a unique (cyclic) subgroup of order d for each $d|n$. Use this to prove that $\sum_{d|n} \varphi(d) = n$, where φ is Euler's totient function. This formula can be used to compute φ recursively: $\varphi(n) = n - \sum_{d|n, d<n} \varphi(d)$.

Proof. Let G be a cyclic group of size n. Then G contains elements of order d if and only if $d|n$. We claim that the number of elements of G with order d is $\varphi(d)$. Since every element of G has some order, it will follow that $\sum_{d|n} \varphi(d) = n$.

So fix $d|n$ and recall that G contains a unique (cyclic) subgroup $H \leq G$ of size d. Note that the elements of H with order d are precisely the generators of H, and we know that there are $\varphi(d)$ of these. Hence we have found $\varphi(d)$ elements of order d in G. Are there any more? If $a \in G$ has order d, then $\langle a \rangle \leq G$ is a subgroup of size d. By the uniqueness of H we conclude that $\langle a \rangle = H$, and hence $a \in H$. That is, a has already been counted. We conclude that G contains **exactly** $\varphi(d)$ elements of order d, which proves the claim. □

3. Let G be a group and recall that its center is a normal subgroup $Z(G) \trianglelefteq G$. **Prove:** If $G/Z(G)$ is cyclic then G is abelian.

Proof. Suppose that the quotient group $G/Z(G)$ is cyclic, generated by the coset $gZ(G)$. This means that every coset looks like $g^i Z(G)$ for some $i \in \mathbb{Z}$. But the cosets partition the group, hence every element of G looks like $g^i z$ for some integer $i \in \mathbb{Z}$ and some element $z \in Z(G)$ of the center. This implies that any two elements of G, say $g^i z$ and $g^j z'$ commute, since

$$g^i z g^j z' = g^i g^j z z' = g^{i+j} z' z = g^j g^i z' z = g^j z' g^i z.$$

□

4. Explicitly describe the conjugacy classes of the Dihedral group

$$D_n := \langle r, \rho : r^2 = \rho^n = 1, \rho r = r\rho^{-1} \rangle.$$

Hint: Every element of D_n looks like $r\rho^k$ or ρ^k for some k.

Proof. First we compute the conjugacy class of a rotation ρ^k. If we conjugate it by some ρ^i then we get $\rho^i \rho^k \rho^{-i} = \rho^k$, which gives us nothing new. If we conjugate it by some $r\rho^i$ then we get $r\rho^i \rho^k (r\rho^i)^{-1} = r\rho^i \rho^k \rho^{-i} r = r\rho^k r = rr\rho^{-k} = \rho^{-k}$. Hence the conjugacy class of ρ^k consists of $\{\rho^k, \rho^{-k}\}$. That is, the rotations come in inverse pairs. If n is odd then the set $\{1, \rho, \ldots, \rho^{n-1}\}$ breaks into classes $\{1\}$ and $\{\rho^i, \rho^{-i}\}$ for $i = 1..(n-1)/2$. If n is even then $\{1, \rho, \ldots, \rho^{n-1}\}$ breaks into two singletons, $\{1\}$ and $\{\rho^{n/2}\}$, together with pairs $\{\rho^i, \rho^{-i}\}$ for $i = 1..(n-2)/2$.

Next we compute the conjugacy class of a reflection $r\rho^k$. If we conjugate by some ρ^i we get $\rho^i r \rho^k \rho^{-i} = r\rho^{-i} \rho^k \rho^{-i} = r\rho^{k-2i}$. If we conjugate by some $r\rho^i$ (and move all copies of r to the left) we get $r\rho^i r \rho^k (r\rho^i)^{-1} = r\rho^i r \rho^k \rho^{-i} r = rrr\rho^i \rho^{-k} \rho^i = r\rho^{2i-k}$. That is, the conjugacy class of $r\rho^k$ consists of $\{r\rho^{k-2i} : i \in \mathbb{Z}\}$. If n is odd, all of the reflections form a single conjugacy class, and if n is even then the reflections break into two classes:

$$\{r, r\rho^2, r\rho^4 \ldots, r\rho^{n-2}\} \quad \text{and} \quad \{r\rho, r\rho^3, \ldots, r\rho^{n-1}\}.$$

What does all of this mean in terms of the symmetries of a regular polygon? What does conjugacy mean in this case? One could alternatively solve this problem using pictures instead of algebra, but I didn't have time for that... □