**MATH 436: Homework VIII.**
**Due in class on Wednesday, Nov 19**

1. **Quaternions.** Recall the complex numbers $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$. If $z \in \mathbb{C}$, the complex conjugate of $z$ is $\bar{z} = a - bi$. It is well known that $\mathbb{C}$ is a field and that if $z$ is a nonzero complex number, its multiplicative inverse is $\frac{\bar{z}}{z\bar{z}}$.

(a) Show that the set $Q = \{\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} | z, w \in \mathbb{C}\}$ is a subring of $Mat_2(\mathbb{C})$, the ring of $2 \times 2$ complex matrices.

(b) Recall if $\mathbb{A} = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}$ then we define $Adj(\mathbb{A}) = \begin{bmatrix} z_{22} & -z_{12} \\ -z_{21} & z_{11} \end{bmatrix}$. As usual we have $\mathbb{A}Adj(\mathbb{A}) = det(\mathbb{A})\mathbb{I} = Adj(\mathbb{A})\mathbb{A}$. Explain how this identity shows that a nonzero $\mathbb{A} \in Mat_2(\mathbb{C})$ is a unit if and only if $det(\mathbb{A}) \neq 0$ and is a zero divisor if and only if $\det(\mathbb{A}) = 0$, $\mathbb{A} \neq \mathbb{O}$.

(c) Check that every nonzero element of $Q$ is a unit and that $Q$ is noncommutative. Thus $Q$ is a division ring but not a field. $Q$ is called the division ring of quaternions.

(d) Show that $Q$ is a real-vector space, i.e., that is is closed under scalar multiplication by real numbers $r \cdot \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix} = \begin{bmatrix} rz_{11} & rz_{12} \\ rz_{21} & rz_{22} \end{bmatrix}$. Show that $\{\hat{e}, \hat{i}, \hat{j}, \hat{k}\}$ is a basis of $Q$ as a real vector space where
$\hat{e} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\hat{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $\hat{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $\hat{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.
Furthermore check that $\hat{i}^2 = \hat{j}^2 = \hat{k}^2 = -\hat{e}$, $\hat{i}\hat{j} = \hat{k} = -\hat{j}\hat{i}$, $\hat{j}\hat{k} = \hat{i} = -\hat{k}\hat{j}$ and $\hat{k}\hat{i} = \hat{j} = -\hat{i}\hat{k}$.

(e) By (d), we may write a quaternion $\mathbb{A} = \begin{bmatrix} \alpha_0 + i\alpha_1 & \alpha_2 + i\alpha_3 \\ -\alpha_2 + i\alpha_3 & \alpha_0 - i\alpha_1 \end{bmatrix}$ as
$\mathbb{A} = \alpha_0\hat{e} + \alpha_1\hat{i} + \alpha_2\hat{j} + \alpha_3\hat{k}$ where $\alpha_j \in \mathbb{R}$.
Show that under this convention, $Adj(\mathbb{A}) = \alpha_0\hat{e} - \alpha_1\hat{i} - \alpha_2\hat{j} - \alpha_3\hat{k}$. This is called the quaternionic conjugate of $\mathbb{A}$, and is denoted $\bar{\mathbb{A}}$.
Conclude then in general for all $\mathbb{A} = \alpha_0\hat{e} + \alpha_1\hat{i} + \alpha_2\hat{j} + \alpha_3\hat{k} \in Q$ we have:

$$\mathbb{A}\bar{\mathbb{A}} = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)\hat{e}.$$

The nonnegative real number $\sum_{i=0}^{3} \alpha_i^2$ is called the quaternionic norm of $\mathbb{A}$, and is denoted $D(\mathbb{A})$. Check that if $\mathbb{A}$ is a nonzero quaternion, $\mathbb{A}^{-1} = \frac{\bar{\mathbb{A}}}{D(\mathbb{A})}$ and that $D : (Q, \cdot) \to (\mathbb{R}_{\geq 0}, \cdot)$ is a homomorphism of monoids.

(f) Since $Q$ is a division ring, $Q^* = \{\mathbb{A} \in Q | \mathbb{A} \neq \mathbb{O}\}$ is a group under (matrix) multiplication. Check that $Q_8 = \{\pm\hat{e}, \pm\hat{i}, \pm\hat{j}, \pm\hat{k}\}$ is a subgroup of order 8. It is called the quaternionic group of order 8. By counting orders of elements, show that it is **not** isomorphic to $D_8$, the dihedral group of order 8. [Note: One can show that $D_8$ and $Q_8$ are the only nonAbelian groups of order 8 up to isomorphism.(See Hungerford.)]

2. **Gaussian Integers** Define $D : \mathbb{C} \to \mathbb{R}_{\geq 0}$ by $D(a+bi) = a^2 + b^2$, thus for nonzero $z \in \mathbb{C}$ we have $\frac{1}{z} = \frac{\bar{z}}{D(z)}$.
(a) We define $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. Show that additively, $(\mathbb{Z}[i], +)$ is isomorphic to a free Abelian group of rank 2. $\mathbb{Z}[i]$ is called the ring of Gaussian Integers.
(b) Show that $D : (\mathbb{C}, \cdot) \to (\mathbb{R}_{\geq 0}, \cdot)$ is a homomorphism of monoids. Show that it restricts to a homomorphism of monoids $D : (\mathbb{Z}[i], \cdot) \to (\mathbb{N}, \cdot)$. Use this to show that if $u$ is a unit of $\mathbb{Z}[i]$ then $D(u) = 1$. Conversely determine $\{u \in \mathbb{Z}[i] | D(u) = 1\}$ and show that these are precisely the units of $\mathbb{Z}[i]$. List them out explicitly.
(c) Check that the image $D(\mathbb{Z}[i])$ is equal to

$$TwoSquare = \{n \in \mathbb{N} | n = a^2 + b^2 \text{ where } a, b \in \mathbb{Z}\}.$$

Note that $TwoSquare$ is the set of all natural numbers that can be written as the sum of two integer squares. Conclude that $TwoSquare$ is a submonoid of $(\mathbb{N}, \cdot)$.
(d) Show that given $n \in \mathbb{N}$ we have $n \equiv 3 \bmod 4$ implies $n \notin TwoSquare$. Check that $0, 1, 2 \in TwoSquare$ and that $n^2 \in TwoSquare$ for all $n \in \mathbb{N}$.
(e) Show that if $p$ is an odd prime then $p \equiv 1$ or $3 \bmod 4$.
(f) Let $n$ be a natural number that can be written as the sum of two squares, i.e., $n = a^2 + b^2$. Check that in $\mathbb{Z}[i]$ we have $n = (a+ib)(a-ib)$. We will use this idea later to show that any prime $p \equiv 1 \bmod 4$ is in $TwoSquare$. Given this fact explain how the following theorem follows:

**Theorem 0.1 (Two Square Theorem).** *Let $n \in \mathbb{N}$ be a nonzero natural number and suppose $n$ has a prime factorization $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ where $p_1 < \dots < p_k$ are primes and $\alpha_j$ are integers such that $\alpha_j$ is an even integer whenever $p_j$ is congruent to 3 mod 4.*

*Then $n = a^2 + b^2$ for $a, b \in \mathbb{N}$.*

(g) For any $z \in \mathbb{C}$, show that there exists $\alpha \in \mathbb{Z}[i]$ such that $D(z - \alpha) \leq \frac{1}{2}$.
(h) Show that for any nonzero $\alpha, \beta \in \mathbb{Z}[i]$, there exists $q, r \in \mathbb{Z}[i]$ such that

$\alpha = q\beta + r$ with $D(r) \leq \frac{1}{2}D(\beta)$.

3. **Integral Quaternions** Recall the division ring of Quaternions $Q$ had a quaternionic norm $D : Q \to \mathbb{R}_{\geq 0}$ which is a homomorphism of multiplicative monoids. We define the integral quaternions $Q_{\mathbb{Z}}$ to be the set

$$Q_{\mathbb{Z}} = \{\alpha_0\hat{e} + \alpha_1\hat{i} + \alpha_2\hat{j} + \alpha_3\hat{k} | \alpha_j \in \mathbb{Z} \text{ for } j = 0, 1, 2, 3\}.$$

(a) Show that $Q_{\mathbb{Z}}$ is a subring of $Q$ which is additively isomorphic to a free Abelian group of rank 4.
(b) Given $\mathbb{A} \in Q$, show that there exists $\alpha \in Q_{\mathbb{Z}}$ such that $D(\mathbb{A} - \alpha) \leq 1$.
(c) Show that $D$ restricts to a homomorphism of monoids $D : (Q_{\mathbb{Z}}, \cdot) \to \mathbb{N}$ with image $FourSquare = \{n \in N | n = a^2 + b^2 + c^2 + d^2 | a, b, c, d \in \mathbb{Z}\}$. Conclude that $FourSquare$ is a submonoid of $(\mathbb{N}, \cdot)$. Show also that $Units(Q_{\mathbb{Z}}) = \{\mathbb{A} \in Q_{\mathbb{Z}} | D(\mathbb{A}) = 1\}$. List the units of $Q_{\mathbb{Z}}$ explicitly.
(d) Lagrange showed that every prime number is a sum of 4 integral squares. (We will see more on this later.) Explain why this shows that every nonnegative integer is a sum of 4 integer squares. (This is called Lagrange's Four Square Theorem).
(e) Verify for $a, b$ integers we have $(a + b)^4 + (a - b)^4 = 2a^4 + 12a^2b^2 + 2b^4$. Use this to show that if $x_1, x_2, x_3, x_4$ are integers we have

$$\sum_{1 \leq i < j \leq 4} [(x_i + x_j)^4 + (x_i - x_j)^4] = 6\sum_{i=1}^{4} x_i^4 + 12 \sum_{1 \leq i < j \leq 4} x_i^2 x_j^2 = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2.$$

(f) Take $n \in \mathbb{N}$ and write $n = 6k + r$ with $k, r \in \mathbb{N}, 0 \leq r \leq 5$. Apply Lagrange's theorem to $k$ to write $k = a_1^2 + a_2^2 + a_3^2 + a_4^2$, where $a_j \in \mathbb{Z}$. Then we apply Lagrange's theorem again to each $a_j$ to write $a_j = \sum_{s=1}^{4}(a_{js})^2$ where $a_{js} \in \mathbb{Z}$. Using (e), show that $6k$ is a sum of at most 48 integer 4-th powers. Conclude that $n = 6k + r$ is a sum of at most 53 integer 4-th powers. Thus you have shown that any natural number is a sum of at most 53 integer 4-th powers. [Note: These sort of problems are refered to collectively as Waring Problems in number theory. 53 is not the best bound for 4-th powers but I believe that the best bound is still unknown.]

4. **Grothendieck rings** A semiring $(S, +, \cdot)$ is a set with two binary operations $+, \cdot$ such that:
(A) It is a commutative monoid under $+$ with identity 0.
(B) It is a monoid under $\cdot$ with identity 1.

(C) We have distributivity $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ for all $a, b, c \in S$.

Recall in a previous HW we had constructed an Abelian group $(G(S), +) = \{[a \ominus b] | a, b \in S\}$ whose elements were equivalence classes of formal differences. We showed the addition $[a \ominus b] + [c \ominus d] = [(a+c) \ominus (b+d)]$ was well-defined and made $G(S)$ into an Abelian group. Recall $a_1 \ominus a_2 \sim b_1 \ominus b_2$ if and only if there is an $s \in S$ such that $a_1 + b_2 + s = a_2 + b_1 + s$ in $S$.
(a) Show that $[a \ominus b] \cdot [c \ominus d] = [(ac + bd) \ominus (bc + ad)]$ gives a well-defined multiplication on $G(S)$ making it into a ring with identity $[1 \ominus 0]$.
(b) Check that the canonical map $i : S \to G(S)$ given by $i(s) = [s \ominus 0]$ is a homomorphism of semirings, i.e., it is a monoid homomorphism for both $+$ and $\cdot$.
(c) Let $G$ be a fixed group. Let us consider the category of finite $G$-sets. This category has objects which are $G$-sets, i.e., sets $X$ with a prescribed $G$-action. The morphisms between two $G$-sets $X$ and $Y$ are the equivariant maps $f : X \to Y$ i.e., the maps $f$ with $f(g \cdot x) = g \cdot f(x)$ for all $x \in X, g \in G$.

Two $G$-sets are hence isomorphic in this category if there is a equivariant bijection between them.

Let $b(G) = \{\text{Isomorphism classes of finite } G - \text{sets }\}$. We define $+$ and $\times$ on this set as follows:

$X + Y$ is the $G$-set obtained from the disjoint union of $X$ and $Y$ with the original $G$-actions on each piece.

$X \times Y$ is the $G$-set obtained from the Cartesian product of the original two $G$-sets using the product action $g \cdot (x, y) = (g \cdot x, g \cdot y)$.

Show that these two operations make $b(G)$ into a semiring where the additive identity is the emptyset and the multiplicative identity is the singleton set. (Both with the "obvious" $G$-actions).

(Note: The Grothendieck completion of the semiring $b(G)$ is called the Burnside ring of $G$ and denoted $B(G)$. This ring is important in algebraic topology and representation theory.)