Due in class W 12 Dec.

In the following five exercises, $F$ is a field, and $F^\times := F \setminus \{0\}$, which is a group under multiplication. The goal is to prove a result needed in class for the proof of Fermat’s theorem on sums of squares.

1. Show that in any field there are at most two elements $a$ such that $a^2 = 1$, and therefore at most one element of order 2 in $F^\times$.

2. Now suppose $|F| = q < \infty$. Show that $F^\times$ contains an element of order 2 if and only if $q$ is odd. (Hint: Use the fact I proved in class, that every finite group of even order has an element of order 2.)

3. Let $\phi : F^\times \to F^\times$ be the function defined by $\phi(a) = a^2$. When $q$ is odd, show that $|\ker \phi| = 2$ and that $G := \phi(F^\times)$ is a subgroup of index 2 of $F^\times$.

4. Show that if $q \equiv 1 \mod 4$, then there exists $a \in F^\times$ such that $a^2 = -1$.

5. Use the previous exercise applied to $F = \mathbb{Z}/p$ to show: if $p$ is a prime number such that $p \equiv 1 \mod 4$, then there exists an integer $m$ such that $p | m^2 + 1$.

In the following, we consider the complex numbers

$$\sqrt{-3} := i\sqrt{3}, \quad \omega := -\frac{1}{2} + \frac{\sqrt{-3}}{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$ 

Let $S = \{ a + b\sqrt{-3} \mid a, b \in \mathbb{Z} \}$ and $R = \{ a + b\omega \mid a, b \in \mathbb{Z} \}$.

6. Show that $S$ and $R$ are subrings of $\mathbb{C}$. (Hint: $\omega^2 = -1 - \omega$.)

7. Show that

$$R = \{ \frac{a}{2} + \frac{b}{2}\sqrt{-3} \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \mod 2 \}. $$

(As a consequence, $S \subseteq R$.)

8. For any complex number $z$ let $N(z) := z\overline{z} = \|z\|^2$, and recall that $N(1) = 1$ and $N(zw) = N(z)N(w)$. Show that $N$ restricts to functions

$$N : R \to \mathbb{Z}_{\geq 0} \quad \text{and} \quad N : S \to \mathbb{Z}_{\geq 0}.$$ 

9. Determine the sets of units $S^\times$ and $R^\times$ in the rings $S$ and $R$. (Hint: $R^\times \neq S^\times$.)

10. Show that $S$ is not a UFD. (Hint: consider elements $z \in S$ with $N(z) = 4$.)

11. Show that for every complex number $z \in \mathbb{C}$, there exists a $q \in R$ with the property that $\|z - q\| < 1$. (Hint: first show you can almost always find a $q \in S$ with this property.)

12. Prove that for all $x, y \in R$ with $y \neq 0$, there exist $q, r \in R$ such that: $x = qy + r$ and $N(r) < N(y)$.

13. Show that $R$ is a PID (and therefore a UFD by the theorem proved in class.)

14. For each prime number $p < 32$, determine whether it is irreducible as an element of $R$. (Hint: if $p = xy$ for $x, y \in R$, what can you say about $N(x)$?) Make a conjecture about which prime numbers are irreducible in $R$.

Department of Mathematics, University of Illinois, Urbana, IL

E-mail address: rezk@illinois.edu

Date: December 5, 2018.