Assignment 1, due February 3

Corrections: Tuesday, Jan. 28, exercise 4 edited to require $b \neq 0$.

Parts of this assignment will be review. The assignment is designed to help students who need review. You may have to look up some of the background material in the class text or elsewhere. If you find yourself lost at some point, please contact me immediately.

1. The first few assignments will have a sequence of exercises related to the *Gaussian integers*, $\mathbb{Z}[i]$. A *Gaussian integer* is something of the form $x = a + bi$, where $i^2 = -1$ and a and b are *rational integers*. Rational integers are "ordinary" integers. The set of Gaussian integers is denoted $\mathbb{Z}[i]$. Show that $\mathbb{Z}[i]$ is a ring.

2. Show that $\mathbb{Z}[i]$ is a *Euclidian domain*. More precisely, show that if $x \in \mathbb{Z}[i]$ and $y \in \mathbb{Z}[i]$, then there is a $z \in \mathbb{Z}[i]$ with $y = zx + r$ and $|r|^2 < |x|^2$.

3. A *unit* in a ring is an invertible element. That is, if $u \in R$ (R being a ring), then u is a unit if there is a $v \in R$ with $uv = 1$. Show that the units in $\mathbb{Z}[i]$ are 1, i, -1, and $-i$. An element $p \in R$ is *prime* if p is not a unit, and $xy = p$ implies that x or y is a unit. Show that if $p \in \mathbb{Z}[i]$ is prime, then there is a unit u with up in the first quadrant. Here, "first quadrant" means $p = a + bi$ with $a > 0$, $b \geq 0$. Show that any $x \in \mathbb{Z}[i]$ may be written uniquely in the form $x = up_1^{a_1} \cdots p_n^{a_n}$, with p_i primes in the first quadrant. (This exercise is a review of prime factorization in euclidean domains. Feel free to review euclidean domains before doing this exercise.)

4. Suppose $R \subseteq \mathbb{F}$ is a ring that is contained in a field. The *field of fractions* of R is the set of all $x \in \mathbb{F}$ that may be written as $x = a/b$ with $a \in R$ and $b \in R$ with $b \neq 0$. Show that the field of fractions is a field. Assume that $0 \neq 1$ in $\mathbb{F}$.

5. Consider the field of fractions of $\mathbb{Z}[i] \subset \mathbb{C}$. Show that this consists of all complex numbers that may be written as $r + si$, where $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$.

6. A ring R is an *integral domain* if $xy \neq 0$ in R if $x \neq 0$ and $y \neq 0$. Suppose $\mathbb{F}$ is a field and $\mathbb{F} \subset R$, with $\mathbb{F}$ being a subring of R. Suppose that R is a finite dimensional vector space over $\mathbb{F}$. Show that R is a field.

7. Suppose $\mathbb{F}$ is a field and that $\mathbb{E}$ and $\mathbb{E}'$ are extension fields of $\mathbb{F}$. We say that $\sigma : \mathbb{E} \to \mathbb{E}'$ is an *isomorphism over* $\mathbb{F}$ if σ is a field isomorphism and if $\sigma(x) = x$ for all $x \in \mathbb{F}$. Suppose $\mathbb{E}$ and $\mathbb{E}'$ are degree 3 extensions of $\mathbb{Q}$ and that the equation $x^3 = 2$ has a solution in $\mathbb{E}$ and in $\mathbb{E}'$. Show that

there is a unique isomorphism from $\mathbb{E}$ to $\mathbb{E}'$ over $\mathbb{Q}$. If $\mathbb{E} \subset \mathbb{C}$ and $\mathbb{E}' \subset \mathbb{C}$, is it necessary that $\mathbb{E} = \mathbb{E}'$?