METU, Spring 2018, Math 523.

Homework 1 (due February 28)

1. Show that $\{\pm 1, \pm i\}$ are all the units in the ring of Gaussian integers $\mathbf{Z}[i]$.

2. Show that the ring $\mathbf{Z}[\sqrt{2}\,]$ has infinitely many units.

3. Show that Euclidean algorithm does not work in the integral domain $\mathbf{Z}[\sqrt{-6}\,]$ under the norm map $N(a+b\sqrt{-6}) = a^2 + 6b^2$. Do not use the fact ED $\Rightarrow$ PID $\Rightarrow$ UFD.

4. Determine all solutions of the following Diophantine equations:

   - $x^2 + 2y^2 = 3z^2$.
   - $3x^2 + 4y^2 = 5z^2$.

5. Let R be a principal ideal domain and let A be a nonzero ideal of R. Show that A is prime if and only if A is maximal.

6. Construct a field $\mathbf{F}_{16} \cong R/\mathfrak{m}$ with 16 elements by choosing a ring R and a maximal ideal $\mathfrak{m} \subset R$ suitably.

   - Determine an element $r \in R$ such that the corresponding element in $\mathbf{F}_{16}$ generates the multiplicative group $\mathbf{F}_{16}^{\times}$. Construct a subfield $\mathbf{F}_4$ of $\mathbf{F}_{16}$ with 4 elements.
   - What is $[\mathbf{F}_{16} : \mathbf{F}_4]$? Is there a nontrivial automorphism of $\mathbf{F}_{16}$ fixing the subfield $\mathbf{F}_4$ pointwise?

7. Let K be a field extension of $\mathbf{Q}$ such that $[K : \mathbf{Q}] = 2$. Show that $K = \mathbf{Q}[\sqrt{m}\,]$ for some integer $m \in \mathbf{Z}$. Give an example of a field extension $L/\mathbf{Q}$ such that $[L : \mathbf{Q}] = 3$ and $L \ncong \mathbf{Q}[\sqrt[3]{m}\,]$ as rings for any integer $m \in \mathbf{Z}$.

8. Let $R = \mathbf{Z}[\sqrt{-3}\,]$ and let $I = \langle 2, 1+\sqrt{-3}\,\rangle$. Show that $I \neq \langle 2 \rangle$ but $I^2 = 2I$. Conclude that ideals in R do not factor uniquely into prime ideals.