Math 503 Problem Set #5 Due the week of Feb. 12, 2018, in lab.

Read Artin, Chapter 12, sections 1,2,5.

1. From Artin, Chapter 12, do these problems (pages 378-382): 1.3, 1.4(a), 2.1(b,c), 2.4, 2.5, 2.8, 2.10, 5.1(a,b).

2. a) Show that $\sqrt{2}$ is irrational.

b) More generally, show that if $m \in \mathbb{Z}$ and $x^2 - m$ has no root in $\mathbb{Z}$, then $x^2 - m$ has no root in $\mathbb{Q}$.

c) Still more generally, show that if $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, and if the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ has no root in $\mathbb{Z}$, then it has no root in $\mathbb{Q}$.

d) What if, in part (c), the polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ (for some integers $a_0, a_1, \ldots, a_n$) is considered instead?

3. A commutative ring R is called *local* if R has exactly one maximal ideal.

a) Which of the following rings are local? For those that are, find the unique maximal ideal. For those that are not, find at least two distinct maximal ideals.
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{C}[x]/(x^3)$, $\mathbb{Z}[i]/(2)$, $\mathbb{Z}[i]/(5)$, $\mathbb{R}[[x]]$, $\mathbb{R}[x]$, $\mathbb{R}(x)$.

b) Let R be the subring of $\mathbb{C}(x)$ consisting of rational functions that are defined at $x = 0$ (and therefore in some neighborhood of that point). Show that R is local. (This example gives rise to the terminology. A function in $\mathbb{C}[x]$ is viewed as "global.")

c) Let R be the subring of $\mathbb{Q}$ consisting of rational numbers with odd denominator. Show that R is local.

4. Let $p > 2$ be a prime number and let $a \in \mathbb{Z}$ be relatively prime to p.

a) Show that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. [Hint: Consider $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.]

b) Show that a is congruent to a square modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. [Hint: What is the structure of the group $(\mathbb{Z}/p\mathbb{Z})^\times$?]

5. For each positive integer n, consider the group $U_n = (\mathbb{Z}/n\mathbb{Z})^\times$ of units modulo n. Find generators of U_5 and U_{25}, and determine whether there exist generators of U_{27} and U_{21}. Conjectures?