MATH 593
Assignment # 4
(Due Wednesday, October 9)

HAND IN: #'s 1,2,3,4

NOTE: THIS MATERIAL WILL BE COVERED ON THE HOUR EXAM ON OCTOBER 7. HOWEVER YOU DON'T NEED TO HAND IN (OR WRITE UP) THE PROBLEMS UNTIL WEDNESDAY OCTOBER 9.

(#1). **(Characteristic of an integral domain).** Let R be an integral domain. Given a positive integer $m \in \mathbf{Z}$ and $a \in R$, define

$$m \cdot a \;=\; a + a + \ldots + a \quad \text{(m times)};$$

when $m < 0$, $m \cdot a$ is defined analogously with a replaced by $-a$.

(a). Denote by $\phi : \mathbf{Z} \longrightarrow R$ the homomorphism

$$\phi : \mathbf{Z} \longrightarrow R \quad , \quad m \mapsto m \cdot 1_R.$$

Show that the image of ϕ is isomorphic either to $\mathbf{Z}$ or to $\mathbf{Z}/p\mathbf{Z}$ for some prime number p. In the first case one says that R has *characteristic zero*; in the second case one says that R has *characteristic* p. For instance $\mathbf{Z}$ has characteristic zero, and $\mathbf{Z}/p\mathbf{Z}$ has characteristic p.

(b). For each prime p, give an example of an infinite integral domain of characteristic p.

(c). If R has characteristic p, show that that $p \cdot a = 0$ for every $a \in R$.

(d). Assume that R has characteristic p. Prove that the mapping

$$F : R \longrightarrow R \quad , \quad a \mapsto a^p$$

is a ring homomorphism. It is called the *Frobenius homomorphism*.

(#2). Let R be an integral domain and $P \subseteq R$ a prime ideal. Consider a monic polynomial

$$f(x) \;=\; x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \;\in\; R[x].$$

Assume that all the coefficients $a_0, \ldots, a_{n-1}$ are in the prime ideal P and that $a_0 \notin P^2$. Show that then f is irreducible in $R[x]$. (HINT: Reduce modulo P.) This is called *Eisenstein's criterion*.

(#3). (a). Let p be a prime number, and consider the polynomial

$$\Phi_p(x) \;=\; x^{p-1} + x^{p-2} + \ldots + x + 1 \;\in\; \mathbf{Z}[x].$$

Prove that $\Phi_p(x)$ is irreducible. (HINT: Apply Eisenstein's criterion after making a judicious linear change of variables.)

(b). Is it true more generally that given any natural number $m > 0$ the polynomial

$$x^{m-1} + x^{m-2} + \ldots + x + 1 \ \in \ \mathbf{Z}[x]$$

is irreducible?

(#4). Let p be a prime number, and let $F = \mathbf{Z}/p\mathbf{Z}$. There are p^2 monic polynomials in $F[x]$ degree 2. How many of them are irreducible?

(#5). Given an integer $d \in \mathbf{Z}$ which is not a square, denote by $\mathbf{Z}[\sqrt{d}\,]$ the ring

$$\mathbf{Z}[\sqrt{d}\,] = \Big\{ a + b\sqrt{d} \ \big| \ a, b \in \mathbf{Z} \Big\}.$$

(a). Prove that if $d < 0$, then the group of units in $\mathbf{Z}[\sqrt{d}\,]$ is finite.

(b). Show that the group of units in $\mathbf{Z}[\,\sqrt{2}\,]$ is infinite.