WORKSHEET # 8
IRREDUCIBLE POLYNOMIALS

We recall several different ways we have to prove that a given polynomial is irreducible. As always, k is a field.

Theorem 0.1 (Gauss' Lemma)**.** *Suppose that $f \in \mathbb{Z}[x]$ is monic of degree > 0. Then f is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible when viewed as an element of $\mathbb{Q}[x]$.*

Lemma 0.2. *A degree one polynomial $f \in k[x]$ is always irreducible.*

Proposition 0.3. *Suppose that $f \in k[x]$ has degree 2 or 3. Then f is irreducible if and only if $f(a) \neq 0$ for all $a \in k$.*

Proposition 0.4. *Suppose that $a, b \in k$ with $a \neq 0$. Then $f(x) \in k[x]$ is irreducible if and only if $f(ax+b) \in k[x]$ is irreducible.*

Theorem 0.5 (Reduction mod p)**.** *Suppose that $f \in \mathbb{Z}[x]$ is a monic[1] polynomial of degree > 0. Set $f_p \in \mathbb{Z}_{modp}[x]$ to be the reduction mod p of f (ie, take the coefficients mod p). If $f_p \in \mathbb{Z}_{modp}[x]$ is irreducible for some prime p, then f is irreducible in $\mathbb{Z}[x]$.*

WARNING: The converse need not be true.

Theorem 0.6 (Eisenstein's Criterion)**.** *Suppose that $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x^1 + a_0 \in \mathbb{Z}[x]$ and also that there is a prime p such that $p|a_i$ for all i but that p^2 does* NOT *divide a_0. Then f is irreducible.*

1. Consider the polynomial $f(x) = x^3 + x^2 + x + 2$. In which of the following rings of polynomials is f irreducible? Justify your answer.

(a) $\mathbb{R}[x]$
(b) $\mathbb{C}[x]$
(c) $\mathbb{Z}_{\mathrm{mod}2}[x]$
(d) $\mathbb{Z}_{\mathrm{mod}3}[x]$
(e) $\mathbb{Z}_{\mathrm{mod}5}[x]$
(f) $\mathbb{Q}[x]$

[1]The same is true as long as the leading coefficient is not divisible by p.

2. Show that $x^4 + 1$ is irreducible in $\mathbb{Q}[x]$ but not irreducible in $\mathbb{R}[x]$.

Hint: For $\mathbb{Q}[x]$, use Proposition 0.4. For $\mathbb{R}[x]$, try a factorization into two quadratic terms

3. Consider $3x^2 + 4x + 3 \in \mathbb{Z}_{\text{mod}5}[x]$. Show it factors both as $(3x + 2)(x + 4)$ and as $(4x + 1)(2x + 3)$. Explain why this *does NOT* contradict unique factorization of polynomials.

4. Completely factor all the polynomials in question 1. into irreducible polynomials in each of the rings (c)–(f).