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) $\mathbb{Z}_{\text{mod}2}[x]$
(d) $\mathbb{Z}_{\text{mod}3}[x]$
(e) $\mathbb{Z}_{\text{mod}5}[x]$
(f) $\mathbb{Q}[x]$

Solution:

(a) It is reducible (= not irreducible) because it is a cubic polynomial and therefore has a root α. Thus f can be factored as $f(x) = (x - \alpha)g(x)$.
(b) The root from (a) is also a complex number, and so f is reducible in $\mathbb{C}[x]$ as well.
(c) Mod 2, $f_2 = x^3 + x^2 + x$, which has a root at $x = 0$ and so is reducible.
(d) Mod 3, $f_3 = x^3+x^2+x+2$. 0 is not a root, $f_2(1) = 5 = 2 \neq 0$, and finally $f_2(2) = 8+4+2+2 = 16 = 1 \neq 0$. In particular, f_3 is *irreducible*.
(e) Mod 5, $f_5 = x^3 + x^2 + x + 2$. Note 1 is a root, and so f_5 is reducible.
(f) f is irreducible since f_3 is irreducible by Theorem 0.5.

[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 linear terms

Solution: First consider $f(x) = x^4+1$ so that $f(x+1) = (x+1)^4+1 = x^4+4x^3+6x^2+4x^2+2$. Eisenstein's criterion applies and so $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. But thus so is $f(x)$ by Proposition 0.4.

For the second part, consider

$$(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1) = x^4+\sqrt{2}x^3+x^2-\sqrt{2}x^3-2x^2-\sqrt{2}x+x^2+\sqrt{2}x+1 = x^4+1$$

which proves that $f(x)$ is reducible.

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.

Solution: First note that

$$(3x+2)(x+4) = 3x^2+12x+2x+8 = 3x^2+4x+3$$

and that

$$(4x+1)(2x+3) = 8x^2+12x+2x+3 = 3x^2+4x+3$$

On the other hand, $2\cdot 3 = 1$ in $\mathbb{Z}_{\text{mod}5}$, and so

$$(4x+1)(2x+3) = (4x+1)(23)(2x+3) = ((4x+1)2)(3(2x+3)) = (8x+2)(6x+9) = (3x+2)(x+4).$$

This completes the proof.

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

Solution:

(c) $\mathbb{Z}_{\text{mod}2}[x]$, $f = x(x^2+x+1)$
(d) $\mathbb{Z}_{\text{mod}3}[x]$, $f = (x^3+x^2+x+2)$
(e) $\mathbb{Z}_{\text{mod}5}[x]$, $f = (x-1)(x^2+2x+3)$
(f) $\mathbb{Q}[x]$, $f = (x^3+x^2+x+2)$