MSM203a: Polynomials and rings
Exercise sheet 3

Richard Kaye

Autumn term, 2013

In the following, the *degree* of a nonzero polynomial $p(X) \in R[X]$ is the highest value of n such that $p(X)$ has a nonzero term aX^n. If $p(X)$ is the zero polynomial, so there is no nonzero term aX^n, we shall say (in this module) that $p(X)$ has degree -1.

If R has 1 then a *monic polynomial* is some $p(X) \in R[X]$ where the highest power of X occurs as $1 \cdot X^n$. (I.e. n here is the degree of $p(X)$ and the leading coefficient is 1.)

A polynomial $p(X) \in R[X]$ is *reducible* if it can be written as a product $q(X)r(X)$ where each of $q(X)$, $r(X)$ is in $R[X]$ and has degree greater than or equal to 1. If this is not the case, $p(X)$ is *irreducible*.

You may find it helpful to use the fact (from lectures) that given R and $a \in R$ the evaluation function $v_a : p(X) \mapsto p(a)$ is a homomorphism of rings $R[X] \to R$.

For a prime $p \in \mathbb{Z}$, $\mathbb{F}_p$ is an alternative name for the ring of integers modulo p. (The $\mathbb{F}$ is used to emphasise that it is a field, which indeed it is as we saw in the last exercise sheet.) We will continue to use $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$ when n is *not* prime.

Exercise 1. Show that it is not true in general that, for a ring R and nonzero polynomials $p(X), q(X)$ each of degree at least 1, the degree of $p(X)q(X)$ is the sum of the degrees of $p(X), q(X)$, but that this is true whenever R is an integral domain. [The first part asks for a counter-example: be as specific as you can. The second part asks for a proof.]

Exercise 2. If F is a field and $p(X)$ is a polynomial of degree 2 or 3 over F, show that $p(X)$ is irreducible if and only if $p(a) \neq 0$ for all $a \in F$.

Exercise 3. If R is an integral domain and $p(X)$ is a *monic* polynomial of degree 2 or 3 over R, show that $p(X)$ is irreducible if and only if $p(a) \neq 0$ for all $a \in R$. [Hint: show first that if $p(X)$ is reducible it can be written as a product of monic polynomials.]

Exercise 4. Give an example of a reducible polynomial $p(X) \in \mathbb{R}[X]$ of degree 4 which has no real root. [So the useful result in Exercise 2 fails for degree 4 or more.]

Exercise 5. Factorise $X^4 + X$ fully over the field $\mathbb{F}_2$ into monic polynomials. Prove each of your factors is irreducible.

Exercise 6. Factorise $X^4 + 2X^3 + X + 2$ over the field $\mathbb{F}_3$ fully, giving your answer as a product of irreducible monic polynomials.

Exercise 7. Show that $X^2 + 1$ is irreducible over $\mathbb{F}_3$ and write down a multiplication table for $R = \mathbb{F}_3[X]/(X^2 + 1)$.