MSM203a: Polynomials and rings
Exercise sheet 5

Richard Kaye

Autumn term, 2013

Exercise 1. Prove that $X^4 + X^3 + 2$ is irreducible in $\mathbb{F}_3[X]$. How many elements are there in the quotient $\mathbb{F}_3[X]/(X^4 + X^3 + 2)$?

Exercise 2. (a) Show that the map $z \mapsto \overline{z}$ is a homomorphism $\mathbb{C} \to \mathbb{C}$.

(b) Deduce from (a) that if $p(X) \in \mathbb{R}[X]$ and $\alpha \in C$ has $p(\alpha) = 0$ then $p(\overline{\alpha}) = 0$.

(c) Hence show that every polynomial $p(X) \in \mathbb{R}[X]$ of degree greater than 2 is reducible in $\mathbb{R}[X]$. (You may use the fact that every polynomial of degree at least 1 over $\mathbb{C}$ has a root in $\mathbb{C}$.)

Exercise 3. This question concerns irreducibility in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$.

(a) Suppose that $p \in \mathbb{Z}$ is prime and $f(X), g(X), h(X) \in \mathbb{Z}[X]$ are such that $f(X) = g(X)h(X)$ and p divides every coefficient of $f(X)$. Show that *either* p divides every coefficient of $g(X)$ *or* p divides every coefficient of $h(X)$. [Hint: write $g(X) = g_0 + g_1X + \cdots + g_rX^r$ and $h(X) = h_0 + h_1X + \cdots + h_sX^s$. Let i, j be least such that p divides neither g_i nor h_j.]

(b) Suppose that $f(X) \in \mathbb{Z}[X]$ and $g_0(X), h_0(X) \in \mathbb{Q}[X]$ such that $f(X) = g_0(X)h_0(X)$. Show there is $n \in \mathbb{N}^+$ and $g(X), h(X) \in \mathbb{Z}[X]$ such that $nf(X) = g(X)h(X)$.

(c) Deduce from the two previous parts *Gauss's lemma* that says a polynomial $f(X) \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$ if and only if it cannot be written as the product of two polynomials of smaller degree in $\mathbb{Z}[X]$. [Hint: suppose $f[X]$ is reducible in $\mathbb{Q}[X]$. Apply (b) to get $nf(X) = g(X)h(X)$ and look at all primes dividing n.]

Exercise 4. This question concerns a criterion for irreducibility in $\mathbb{Q}[X]$ called *Eisenstein's criterion*. Suppose $f(X) \in \mathbb{Z}[X]$ is a polynomial $f_0 + f_1X + \cdots + f_kX^k$ of degree $k \geqslant 2$ and $q \in \mathbb{N}$ is a prime such that: (i) q does not divide f_k; (ii) q divides f_i for all $i < k$; and (iii) q^2 does not divide f_0. You need to show that $f(X)$ is irreducible in $\mathbb{Q}[X]$. Suppose it is reducible.

(a) Using a previous exercise, show there are $g(X), h(X) \in \mathbb{Z}[X]$ where $g(X) = g_0 + g_1X + \cdots + g_rX^r$ and $h(X) = h_0 + h_1X + \cdots + h_sX^s$ such that $1 \leqslant r, s < k$, $f(X) = g(X)h(X)$ and q divides g_0 but not h_0.

(b) Show that q cannot divide all of the coefficients g_i.

(c) By looking at the least i such that q does not divide g_i obtain a contradiction.

Exercise 5. For the following polynomials over the rings stated, decide whether it is irreducible or not.

(a) $X^4 + 1 \in \mathbb{R}[X]$

(b) $X^4 + 1 \in \mathbb{Q}[X]$

(c) $X^7 + 11X^3 - 33X + 22 \in \mathbb{Q}[X]$

(d) $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$

(e) $X^3 - 7X^2 + 3X + 3 \in \mathbb{Q}[X]$

(f) $X^3 - 5 \in \mathbb{F}_{11}[X]$

Exercise 6. Let F be a field. Prove that a polynomial $f(X)$ is irreducible in $F[X]$ if and only if $f(X+1)$ is irreducible in $F[X]$. Using this, the polynomial $X^{17} - 1$, and the prime $q = 17$, apply Eisenstein's criterion to show that

$$X^{16} + X^{15} + \cdots + X + 1$$

is irreducible in $\mathbb{Q}[X]$.

Exercise 7. (2004, Q11) Let F be a field and $R = F[X]$ be the ring of polynomials over F.

(a) Prove that R has no zero-divisors.

(b) Prove that every ideal in R has the form $p(X)R$ for some polynomial $p(x) \in R$.

(c) Prove that if $p(X)$ is irreducible, then the ideal $p(X)R$ is a maximal ideal.

(d) For each of the following rings, decide whether or not it is a field, and give reasons.

  (a) $\mathbb{Q}[X]/(X^2 + 1)$;
  (b) $\mathbb{Z}_3[X]/(X^4 + X + 1)$;
  (c) $\mathbb{Q}[X]/(X^9 + 3X^2 + 6)$;

[Note: $p(X)R$ is a different notation for the ideal $(p(X))$ of R.]

Exercise 8. (2005, Q12) Which of the following quotient rings are fields? In each case give a brief explanation.

(a) $\mathbb{Z}/9\mathbb{Z}$.

(b) $R[X]/(X^2 + X + 1)$ where $R = \mathbb{Z}/5\mathbb{Z}$.

(c) $R[X]/(X^2 + X + 1)$ where $R = \mathbb{C}$.

(d) $R[X]/(f(X))$ where $R = \mathbb{Q}$ and $f(X) = (X^{41} - 1)/(X - 1)$.

Exercise 9. (a) Find the minimum polynomial of $\alpha \in \mathbb{C}$ over $\mathbb{Q}$ given that $\alpha \notin \mathbb{Q}$ and $\alpha^3 + \alpha^2 - 2\alpha - 2 = 0$.

(b) Find the minimum polynomial of $\beta \in \mathbb{C}$ over $\mathbb{Q}(\sqrt{2})$ given that $\beta \notin \mathbb{Q}(\sqrt{2})$ and $\beta^5 - 2\beta^4 - \beta^3 - 2\beta^2 - 2\beta + 4 = 0$.