THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2070A Algebraic Structures 2019-20
Homework 9
Due Date: 5th December 2019

Compulsory Part

1. Let f be a monic polynomial in $\mathbb{Q}[x]$ with integer coefficients. Show that if $r \in \mathbb{Q}$ is a root of f, then $r \in \mathbb{Z}$.

2. Let F be a field. Let f, g be relatively prime polynomials in $F[x]$. Show that if both f and g divide a polynomial h in $F[x]$, then $fg|h$.

3. Determine if the following polynomials are irreducible in $\mathbb{Q}[x]$:

   (a) $f = x^3 + 6x^2 + 5x + 24257$
   (Hint: First consider f as an element in $\mathbb{Z}[x]$, then determine if its image $\bar{f}$ in $\mathbb{F}_2[x]$ is irreducible.)

   (b) $f = x^4 + x^2 + x + 1$

   (c) $f = 4x^3 - 6x - 1$

Optional Part

1. Let p be a prime.

   (a) Show that for all $k \in \{1, 2, \ldots, p-1\}$, the prime p divides $\binom{p}{k}$.

   (b) Let p be a prime, r an element in $\mathbb{F}_p$. Show that $(x + r)^p = x^p + r^p$ in $\mathbb{F}_p[x]$.

   (c) The **p-th cyclotomic polynomial** is by definition:

   $$\Phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

   Show that Φ_p is irreducible in $\mathbb{Q}[x]$.
   (Hint: First show that:

   $$\Phi_p \circ (x + 1) := (x + 1)^{p-1} + (x + 1)^{p-2} + \cdots + (x + 1) + 1$$

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

2. Consider the polynomials $f = x^2 - x - 2$ and $g = x^3 - 2x + 1$ in $\mathbb{Z}_5[x]$. By adapting the Euclidean Algorithm to $\mathbb{Z}_5[x]$, find $a, b \in \mathbb{Z}_5[x]$ such that $af + bg = gcd(f, g)$.

   (Here, $gcd(f, g)$ is the unique monic polynomial in $\mathbb{Z}_5[x]$ with the property that the ideal (f, g) is equal to the principal ideal $(gcd(f, g))$).

3. Express the following polynomials as products of irreducible factors.

   (a) $x^4 + 1$ in $\mathbb{Z}_2[x]$.

   (b) $x^3 + 1$ in $\mathbb{Z}_3[x]$.

4. Show that the following polynomials are irreducible in $\mathbb{Q}[x]$:

   (a) $2x^5 + 25x + 210$

   (b) $17715x^2 + 1234567x + 4561$

   (c) $x^3 + 6x^2 + 7$

   (d) $4x^3 - 3x + \frac{1}{2}$

   (e) $\frac{1}{3}x^5 - x^4 + 1$

   (f) $x^4 + 5x^2 - 2x - 3$.
   (Hint: Consider the irreducible factors of the polynomial over $\mathbb{F}_2$ and $\mathbb{F}_3$. What conclusion can one draw?)

5. Let k be a field. Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $k[x]$ of degree n. Show that if f is irreducible in $k[x]$, then so is:

$$f^* := a_n + a_{n-1}x + \cdots + a_1 x^{n-1} + a_0 x^n.$$

6. Let F be a field, p a polynomial in $F[x]$. Then a theorem in our lecture notes says that the quotient ring $F[x]/(p)$ is a field if and only if p is irreducible in $F[x]$.

   Determine if each of the following rings is a field:

   (a) $\mathbb{Q}[x]/(x^3 - 1)$

   (b) $\mathbb{Q}[x]/(7x^{59} + 24x^9 + 6x + 156)$

   (c) $\mathbb{Q}[x]/(x^3 + x + 1)$

   (d) $\mathbb{Z}[x]/(x^3 + x + 1)$

   (e) $\mathbb{Q}/(17)$

   (f) $\mathbb{Z}/(17)$

   (g) $\mathbb{Z}[x]/(2, x)$

   (h) $\mathbb{Q}[x]/(x^2 - 3)$

   (i) $\mathbb{R}[x]/(x^2 - 3)$

   (j) $\mathbb{R}[x]/(x^2 + 3)$

   (k) $\mathbb{F}_5[x]/(x^2 + 1)$

   (l) $\mathbb{R}[x]/(x^{17} + x^5 + 8x^2 - x + 1)$

7. **Converse of Euclid's Lemma.** Let F be a field, f a polynomial in $F[x]$ with degree ≥ 1, such that, for $g, h \in F[x]$, the condition $f|gh$ implies that $f|g$ or $f|h$. Show that f is irreducible in $F[x]$.

   (Try to prove this without invoking the unique factorization theorem.)