MA10209 Algebra

Sheet 7 Problems: GCS

12-xi-18

Hand in work to your tutor at the time specified by your tutor. The latest possible hand in time will be 17:15, Monday Nov 19th.

1. A polynomial $\sum_{i=0}^{n} a_i X^i$ is *monic* if $a_n = 1$. We will work in $\mathbb{R}[X]$, the ring of polynomials in X with coefficients in $\mathbb{R}$. In each case, is the given statement true or false?

   (a) The zero polynomial is monic.

   (b) The sum of two monic polynomials is monic.

   (c) The difference of two monic polynomials is monic.

   (d) The product of two monic polynomials is monic.

   (e) Every polynomial is a product of a non-zero real number and a monic polynomial.

2. Work in $\mathbb{Q}[X]$. Divide $X^5 + 4X + 1$ by $X^2 + 1$ to leave a remainder of smallest possible degree. Expressed more formally, find polynomials $q, r \in \mathbb{Q}[X]$ with $\deg r < 2$ such that $X^5 + 4X + 1 = q \cdot (X^2 + 1) + r$.

3. Let R be a ring. A polynomial $f \in R[X]$ of positive degree is called *irreducible* if whenever $g, h \in R[X]$ are such that $f = gh$, then either g or h has degree 0 (i.e. is a non-zero constant). Let $f_1 = X^2 - 2$ and $f_2 = X^2 + 2$.

   (a) Is either f_1 or f_2 irreducible, viewed as an element of $\mathbb{Q}[X]$?

   (b) Is either f_1 or f_2 irreducible, viewed as an element of $\mathbb{R}[X]$?

   (c) Is either f_1 or f_2 irreducible, viewed as an element of $\mathbb{C}[X]$?

4. Suppose that $\zeta \in \mathbb{C}$. By considering $\zeta + \overline{\zeta}$ and $\zeta\overline{\zeta}$, prove that there is $f \in \mathbb{R}[X]$ of degree 2 such that $f(\zeta) = 0$ (i.e. ζ is a root of f).

5. The *Fundamental Theorem of Algebra* states that if $f \in \mathbb{C}[X]$ and $\deg f > 0$, then there is $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. A proof of this result is beyond the scope of this course, but assume it for the purposes of this question. The remainder theorem will be covered in lectures, but I will put up notes on the web site for you to consult.

(a) Prove that every irreducible polynomial in $\mathbb{C}[X]$ has degree 1.

(b) Prove that every irreducible polynomial in $\mathbb{R}[X]$ has degree at most 2.

(c) Suppose that $f \in \mathbb{C}[X]$ has degree $n \geq 1$. Prove that f has at most n roots in $\mathbb{C}$.

(d) Suppose that $f \in \mathbb{R}[X]$ has degree $n \geq 1$. Prove that f has at most n roots in $\mathbb{R}$.

6. Suppose that R is a ring. Show that R is an integral domain if, and only if, $R[X]$ is an integral domain.

7. A polynomial $f \in \mathbb{Z}[X]$ is called *primitive* if the gcd of its coefficients is 1. Prove that the product of two primitive polynomials is primitive. *This is due to Gauss. You might approach the proof like this. Suppose, for contradiction, that a prime number p is a common divisor of the coefficients of the product of two primitive polynomials. Now interpret this fact in $\mathbb{Z}_p[X]$ and become concerned.*

8. Suppose that $f \in \mathbb{Z}[X]$ and $f \neq 0$. We define the *content* $c(f)$ of f to be the gcd of the coefficients of f.

   (a) Prove that $f = c(f)\widehat{f}$ where $\widehat{f} \in \mathbb{Z}[X]$ and $\widehat{f}$ is primitive.

   (b) Prove that if $n \in \mathbb{N}$ and $f \in \mathbb{Z}[X]$ is primitive, then $c(nf) = n$.

   (c) Suppose that m, n are positive integers, and that $f, g \in \mathbb{Z}[X]$ are primitive polynomials. Suppose that $mf = ng$. Prove that $m = n$ and $f = g$.

   (d) Prove that if $f, g \in \mathbb{Z}[X]$ and $f \neq 0 \neq g$, then $c(fg) = c(f)c(g)$.

   (e) *Harder, use previous parts cleverly.* Suppose that $f \in \mathbb{Z}[X]$. Prove that f is irreducible in $\mathbb{Z}[X]$ if, and only if, f is irreducible in $\mathbb{Q}[X]$.

9. Suppose that $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ and that there is a prime p such that p does not divide a_0, but p divides a_i for $1 \leq i \leq n$ but p^2 does not divide a_n. Prove that f is irreducible in $\mathbb{Q}[X]$. *Use Problem 8(e), and worry about what happens in $\mathbb{Z}_p[X]$.*

10. (Challenge!) Find all $f \in \mathbb{R}[X]$ such that $q \in \mathbb{Q}$ if, and only if, $f(q) \in \mathbb{Q}$.