M 431: Assignment 13

Nathan Stouffer

Page 163 — Problem 3

Problem. Find the greatest common divisor of the following polynomials over $\mathbb{Q}$, the field of rational numbers.

(a) $x^3 - 6x + 7$ and $x + 4$
(b) $x^2 - 1$ and $2x^7 - 4x^5 + 2$
(c) $3x^2 + 1$ and $x^6 + x^4 + x + 1$
(d) $x^3 - 1$ and $x^7 - x^4 + x^3 - 1$

Proof. I'm running short on time, so I didn't show much work on these ones.

(a) Here, $x + 4$ is irreducible so we only need to test if $x + 4$ divides $x^3 - 6x + 7$. Using long division, I found that this was not the case. So the greatest common divisor is the polynomial 1.

(b) Here $x^2 - 1 = (x + 1)(x - 1)$. Using long divion again, I found that $x - 1$ divides $2x^7 - 4x^5 + 2$ but $x + 1$ does not so the greatest common divisor is $x - 1$.

(c) $3x^2 + 1$ is irreducible in $\mathbb{R}[x]$ so it is certainly irreducible in $\mathbb{Q}$. For this problem, I found the zeros of $3x^2 + 1$ in the comple plane then computed their output in the polynomial $x^6 + x^4 + x + 1$. Neither resulted in 0, so $3x^2 + 1$ does not divide $x^6 + x^4 + x + 1$ and the greatest common divisor is 1.

(d) For this one, $x^7 - x^4 + x^3 - 1 = x^4(x^3 - 1) + 1(x^3 - 1) = (x^4 + 1)(x^3 - 1)$ so $x^3 - 1$ is the greatest common divisor!

□

Page 164 — Problem 5

Problem. In the previous problem, let $I = \{f(x)a(x)+g(x)b(x)\}$ where $f(x), g(x)$ run over $\mathbb{Q}[x]$ and $a(x)$ is the first polynomial and $b(x)$ is the second one in each part of the problem. Find $d(x)$ so that $I = (d(x))$ for each part.

Proof.

$\square$

Page 164 — Problem 10

Problem. Show that the following polynomials are irreducible over the field F indicated.

(a) $x^2 + 7$ over $\mathbb{R}$
(b) $x^3 - 3x + 3$ over $\mathbb{Q}$
(c) $x^2 + x + 1$ over $\mathbb{Z}_2$
(d) $x^2 + 1$ over $\mathbb{Z}_{19}$
(e) $x^3 - 9$ over $\mathbb{Z}_{13}$
(f) $x^4 + 2x^2 + 2$ over $\mathbb{Q}$

Proof.

$\square$

Page 164 — Problem 13

Problem. Let $\mathbb{R}$ be the field of real numbers and $\mathbb{C}$ that of complex numbers. Show that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Proof.

$\square$

Page 165 — Problem 16

Problem. Let $F = \mathbb{Z}_p$ for some prime number p and $q(x) \in F[x]$ where $q(x)$ is irreducible with degree n. Show that $F[x]/(q(x))$ has exactly p^n elements.

Proof.

$\square$

Page 171 — Problem 6

Problem. Let F be the field and φ an automorphism of $F[x]$ such that $\varphi(a) = a$ for all $a \in F$. If $f(x) \in F[x]$, prove that $f(x)$ is irreducible in $F[x]$ if and only if $g(x) = \varphi(f(x))$ is.

Proof.

$\square$