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.

(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) For this problem, I found the zeros of $3x^2 + 1$ in the complex 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. So $3x^2 + 1$ is irreducible in $\mathbb{R}[x]$ so it is certainly irreducible in $\mathbb{Q}[x]$.

(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!

$\square$

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. In the proof of Theorem 4.5.7 in the textbook, it is noted that for an ideal $I = \{f(x)a(x)+g(x)b(x) \mid f(x), g(x) \in \mathbb{Q}[x]\}$ with fixed $a(x), b(x)$ that $I = (d(x))$ where $(a(x), b(x)) = d(x)$ the greatest common divisor. Thus the $d(x)$ that we search for in this problem is given by the answers to the last problem.

□

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.

(a) Using the bijection between real numbers $x \mapsto \sqrt{7}y$, map x^2+7 to $(\sqrt{7}y)^2+7 = 7y^2+7 = 7(y^2+1)$. Then, by the result in the next problem $\mathbb{R}[y]/(y^2+1)$ is a field so (y^2+1) is maximal which means y^2+1 is irreducible over $\mathbb{R}$. This implies that x^2+7 is irreducible in $\mathbb{R}[x]$.

(b) For $x^3 - 3x + 3$, note that $p = 3$ satisfies the Eisenstein criterion so the polynomial is irreducible in $\mathbb{Z}[x]$. Then Gauss' lemma tells us that the same polynomial is irreducible over $\mathbb{Q}$.

(c) For this one, just plug in the two options to $p(x) = x^2 + x + 1$. We have $p(0) = p(1) = 1$ so $p(x)$ is irreducible over $\mathbb{Z}_2$.

(d) Looking at $x^2 + 1$ over $\mathbb{Z}_{19}$, we know $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ so it is also irreducible in $\mathbb{Z}_{19}[x]$.

(e) For $x^3 - 9$ over $\mathbb{Z}_{13}$, has no zeros in $\mathbb{Z}_{13}$ so it is irreducible.

(f) Here we use the Eisenstein criterion with $p = 2$ to show that $x^4 + 2x^2 + 2$ is irreducible over $\mathbb{Z}$ and Gauss' lemma tells us that the same polynomial is irreducible over $\mathbb{Q}$.

$\square$

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. We will show this with the first isomorphism theorem. To do this, we need a surjective homomorphism $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ with $\ker \varphi = (x^2 + 1)$. Consider the map $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ defined by taking the polynomial $a_k x^k + \cdots + a_1 x + a_0$ to the complex number $a_k i^k + \cdots + a_1 i + a_0$.

That φ is a surjection is immediate by choosing $bx + a \in \mathbb{R}[x]$ for the complex number $a + ib \in \mathbb{C}$. Now we verify that φ is a homomorphism. The addition component can be checked easily. For multiplication, pick $a(x), b(x) \in \mathbb{R}[x]$. Then we have $\varphi(a_0 + \cdots + a_k x^k)\varphi(b_0 + \cdots + b_l x^l) = (a_0 + \cdots + a_k i^k)(b_0 + \cdots + b_l i^l)$ and $\varphi(a(x)b(x)) = \varphi((a_0 + \cdots + a_k x^k)(b_0 + \cdots + b_l x^l))$ where multplying the polynomials has the same "structure" as multiplying the complex numbers (ie foiling) so the multiplicative property of the homomorphism φ holds.

Now to check that $\ker \varphi = (x^2 + 1)$. Going to the left, pick any $p(x) \in (x^2 + 1) \implies$ there exists some $f(x) \in \mathbb{R}[x]$ such that $p(x) = f(x)(x^2 + 1) \implies \varphi(p(x)) = \varphi(f(x)(x^2 + 1)) = \varphi(f(x))\varphi(x^2 + 1) = \varphi(f(x))(i^2 + 1) = \varphi(f(x))0 = 0$ so $p(x) \in \ker \varphi$. Now going to the right, fix any $p(x) \in \ker \varphi$. Then $\varphi(p(x)) = p_0 + p_1 i + \cdots p_n i^n = 0$. Now let p take any complex number as an input instead of just real inputs (p is a member of $\mathbb{C}[z]$ as well as $\mathbb{R}[x]$). In the context of $\mathbb{C}$, this means that $p(i) = 0$, which is to say that $z^2 + 1 \mid p(z)$. But then all the coefficients are real so we must also have $x^2 + 1 \mid p(x) \implies p(x) \in (x^2 + 1)$.

Thus we have all the requirements for φ to be the map in the first isomorphism theorem and we can conclude that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

$\square$

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. I couldn't quite prove equality on this one, maybe I'm missing something super obvious. I did prove that the set $F[x]/(q(x))$ has at least p^n elements. Since $q(x)$ has degree n we know that $q(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$ and the irreducibility implies that the ideal $(q(x))$ contains only one element (0) that has degreen less than n. Thus each $p(x)$ with $\deg p(x) < n$ produces a unique element of $F[x]/(q(x))$. The polynomial $p(x) \in \mathbb{Z}_p$ has the form $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ where each a_i (of which there are n) has $|\mathbb{Z}_p| = p$ options. Thus we have at least p^n elements in the set $F[x]/(q(x))$. I look forward to reading the solutions to learn how to show the upper bound.

□

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. If $\varphi(f(x)) = f(x)$ then this problem is trivial. Let's show that this is the case. Since φ is an automorphism, it is an isomorphism from $F[x] \longrightarrow F[x]$. Fix $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ and consider the following

$$\begin{aligned}\varphi(f(x)) &= \varphi(a_0 + a_1x + \cdots + a_nx^n)\\ &= \varphi(a_0) + \varphi(a_1x) + \cdots + \varphi(a_nx^n)\\ &= \varphi(a_0) + \varphi(a_1)\varphi(x) + \cdots + \varphi(a_n)\varphi(x^n)\\ &= a_0 + a_1\varphi(x) + \cdots + a_n\varphi(x)^n\\ &= a_0 + a_1x + \cdots + a_nx^n = f(x)\end{aligned}$$

where made several crucial steps based on the fact that φ is a homomorphism with the property that $\varphi(a) = a$ for any $a \in F$. Note that all the $a_i \in F$ and $x \in F$ so our steps were justified.

□