MATH 100B: Homework #5

Due on Feb 15, 2024 at 12:00pm

Professor McKernan

Section A02 6:00PM - 6:50PM
Section Leader: Castellano-Macías

Source Consulted: Textbook, Lecture, Discussion, Office Hour

Ray Tsai
A16848188

Problem 1

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

(a) $x^2 + 7$ over $F = \mathbb{R}$.

Proof. Note that $x^2 + 7$ is of degree two, so it suffice to show that $x^2 + 7$ has no roots in $\mathbb{R}$, by Lemma 8.7. Replace x with any real number a. Since a^2 is non-negative, $a^2 + 7$ must not be 0, and thus it is irreducible. □

(b) $x^3 - 3x + 3$ over $F = \mathbb{Q}$.

Proof. Notice that 3 divides the coefficients of every term other than that of the greatest one and 3^2 does not divide 3, and thus the result follows from the Eisenstein's Criteria. □

(c) $x^2 + x + 1$ over $F = \mathbb{Z}_2$.

Proof. By Lemma 8.7, since $x^2 + x + 1 = 1$ no matter what x is, it is irreducible. □

(d) $x^2 + 1$ over $F = \mathbb{Z}_{19}$.

Proof. By Lemma 8.7, it suffice to show that -1 is not a square in $\mathbb{Z}_{19}$. Since $(-a)^2 = a^2$, we only need to consider $a = 0, 1, \ldots, 9$. Hence,

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16 = -3$$
$$5^2 = 25 = 6, \quad 7^2 = 49 = -8, \quad 8^2 = 64 = 7, \quad 9^2 = 81 = 5,$$

and thus -1 is not a square in $\mathbb{Z}_{19}$. □

(e) $x^3 - 9$ over $F = \mathbb{Z}_{13}$.

Proof. By Lemma 8.7, it suffice to show that 9 is not a cube in $\mathbb{Z}_{13}$. Hence,

$$0^3 = 0, \quad 1^3 = 1, \quad 2^3 = 8, \quad 3^3 = 1, \quad 4^3 = -1$$
$$5^3 = -5, \quad 7^3 = 5, \quad 8^3 = 5, \quad 9^3 = 1, \quad 10^3 = -1$$
$$11^3 = 5, \quad 12^2 = -1,$$

and thus 9 is not a cube in $\mathbb{Z}_{13}$. □

(f) $x^4 + 2x^2 + 2$ over $F = \mathbb{Q}$.

Proof. Notice that 2 divides the coefficients of every term other than that of the greatest one and 2^2 does not divide 2, and thus the result follows from the Eisenstein's Criteria. □

Problem 2

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

Proof. Since there exists a natural inclusion $\mathbb{R} \to \mathbb{C}$, there exists a unique ring homomorphism $\phi : \mathbb{R}[x] \to \mathbb{C}$ that sends $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ to $a_n i^n + a_{n-1} i^{n-1} + \cdots + a_0$, by the universal property of polynomial rings. ϕ is clearly surjective, as there exists $a+bx \in \mathbb{R}[x]$ that gets mapped to $a+bi$, for $a+bi \in \mathbb{C}$. Note that $\mathbb{R}[x]$ is an Euclidean doamin and thus a PID, so Ker ϕ is generated by some $f \in \mathbb{R}[x]$. Since $\phi(x^2+1) = 0$, x^2+1 is in the kernel. However, x^2+1 is irreducible in $\mathbb{R}[x]$, so Ker $\phi = \langle x^2+1 \rangle$. The result now follows from the First Isomorphism Theorem for rings. $\square$

Problem 3

Let $F = \mathbb{Z}_{11}$, the integers mod 11.

(a) Let $p(x) = x^2 + 1$; show that $p(x)$ is irreducible in $F[x]$ and that $F[x]/(p(x))$ is a field having 121 elements.

Proof. To show $p(x)$ is irreducible, we only need to show -1 is not a square in $\mathbb{Z}_{11}$, by Lemma 8.7. Since $(-a)^2 = a^2$, we only need to consider $a = 0, 1, \dots, 5$. Therefore,

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16 = 5, \quad 5^2 = 25 = 3,$$

so $p(x)$ is indeed irreducible. Note that $\mathbb{Z}[i]/\langle 11 \rangle$ is a field of 121 elements, proven in Midterm 1 challenge problem 2. Since there is a natural inclusion $F \hookrightarrow \mathbb{Z}[i]/\langle 11 \rangle$, the universal property of polynomial rings gives us a unique ring homomorphism $\phi\colon F[x] \to \mathbb{Z}[i]/\langle 11 \rangle$ that sends x to i. Let I be the kernel of ϕ. Since $F[x]$ is an Euclidean domain and thus a PID, $I = \langle a \rangle$, for some noninvertible $a \in F[x]$. We already know $x^2 + 1 \in I$. However, since $x^2 + 1$ is irreducible, $x^2 + 1$ and a are associates, and thus $I = \langle x^2 + 1 \rangle$. By the First Isomorphism Theorem for rings, $F[x]/\langle x^2 + 1 \rangle \simeq \mathbb{Z}[i]/\langle 11 \rangle$, and this completes the proof. $\square$

(b) Let $p(x) = x^3 + x + 4 \in F[x]$; show that $p(x)$ is irreducible in $F[x]$ and that $F[x]/(p(x))$ is a field having 11^3 elements.

Proof. To show $p(x)$ is irreducible, we only need to show $p(x)$ does not have a root in $\mathbb{Z}_{11}$. Therefore,

$$\begin{gathered} 0^3 + 0 + 4 = 4, \quad 1^3 + 1 + 4 = 6, \quad 2^3 + 2 + 4 = 3, \quad 3^3 + 3 + 4 = 1 \\ 4^3 + 4 + 4 = 6, \quad 5^3 + 5 + 4 = 2, \quad 6^3 + 6 + 4 = 6, \quad 7^3 + 7 + 4 = 2 \\ 5^3 + 5 + 4 = 7, \quad 9^3 + 9 + 4 = 5, \quad 10^3 + 10 + 4 = 2, \end{gathered}$$

so $p(x)$ is indeed irreducible. Note that since F is a field, $F[x]$ is an Euclidean domain and thus a PID. Hence, for any ideal $I = \langle k \rangle$ such that $I \neq F[x]$ and contains $\langle x^3 + x + 4 \rangle$, we have $I = \langle x^3 + x + 4 \rangle$, as $x^3 + x + 4$ is irreducible. It follows that $\langle x^3 + x + 4 \rangle$ is maximal, and thus $F[x]/\langle x^3 + x + 4 \rangle$ is a field. It remains to show that $F[x]/\langle x^3 + x + 4 \rangle$ contains 11^3 elements. Note that any $f(x) \in F[x]$ can be written in the unique form of $g(x)(x^3 + x + 4) + (ax^2 + bx + c)$, and thus $f(x) + \langle x^3 + x + 4 \rangle = (ax^2 + bx + c) + \langle x^3 + x + 4 \rangle$, for some $a, b, c \in F[x]$. Since there are 11^3 possible sequence of a, b, c, $F[x]/(p(x))$ has 11^3 elements. $\square$

Problem 4

Construct a field having p^2 elements, for p an odd prime.

Proof. Consider the field $\mathbb{F}_p[x]/\langle g(x)\rangle$, for some irreducible quadratic $g(x) \in \mathbb{F}_p[x]$. We first show that such $g(x)$ exists. Suppose that a monic quadratic $f(x) = x^2 + ax + b \in \mathbb{F}_p[x]$ is reducible. Then $f(x) = (x+m)(x+n)$, so we need to solve for $\begin{cases} m+n=a \\ mn=b \end{cases}$. However, since $\mathbb{F}_p$ is a field, there exists a unique solution to m, n. This means that there is a bijection between the reducible monic quadratics in $\mathbb{F}_p[x]$ and the unordered pairs of elements in $\mathbb{F}_p$. Since there are $\binom{p}{2}+p$ possiblilities of unordered pairs in $\mathbb{F}_p$, there are $\binom{p}{2}+p$ reducible monic quadratics, and thus the number of irreducible monic quadratics is $p^2 - \binom{p}{2} + p > 0$. Therefore, there exists an irreducible monic quadratic $g(x) \in \mathbb{F}_p[x]$. Note that $\mathbb{F}_p$ is a field, so $\mathbb{F}_p[x]$ is an Euclidean domain and thus a PID. Hence, $\langle g(x)\rangle$ is maximal, as $g(x)$ is irreducible, so $\mathbb{F}_p[x]/\langle g(x)\rangle$ is indeed a field. It remains to show that $\mathbb{F}_p[x]/\langle g(x)\rangle$ contains p^2 elements. Since $\mathbb{F}_p[x]$ is an Euclidean domain, any polynomial $k(x)$ in $\mathbb{F}_p[x]$ can be written in the unique form of $k(x) = h(x)g(x) + (\alpha x + \beta)$, as $g(x)$ is of degree two. Since, $k(x) + \langle g(x)\rangle = (\alpha x + \beta) + \langle g(x)\rangle$, the left cosets of $\langle g(x)\rangle$ are characterized by the remainders of polynomials in $\mathbb{F}_p[x]$ after divided by $g(x)$, and there are p^2 of them. Hence, we conclude that $\mathbb{F}_p[x]/\langle g(x)\rangle$ has p^2 elements. □

Problem 5

In Example 5, show that because $g(x)$ is irreducible in $\mathbb{Q}[x]$, then so is $f(x)$.

Proof. Since 5 divides coefficients of all terms except for that of the largest one in $g(x) = x^4 + 5x^3 + 10x^2 + 10x + 5$ and 25 also does not divide 5, it meets the Eisenstein Criteria and thus $g(x)$ is irreducible in $\mathbb{Q}[x]$. Note that the map $\mathbb{Q}[x] \to \mathbb{Q}[x]$ that sends $h(x)$ to $h(x+1)$ is an one-to-one correspondence. Suppose for contradiction that $f(x) = w(x)u(x)$, for some nonconstant $w(x), u(x) \in \mathbb{Q}[x]$. Then, $w(x+1)u(x+1) = g(x)$, contradiction. Hence, $f(x)$ is also irreducible. $\square$

Problem 6

Prove that $f(x) = x^3 + 3x + 2$ is irreducible in $\mathbb{Q}[x]$.

Proof. By Gauss' Lemma, it suffices to show that $f(x)$ has not roots in $\mathbb{Z}[x]$. Since $x^3+3x+2 = x(x^2+3)+2$, we need to show that $x(x^2+3) \neq -2$ for any $x \in \mathbb{Z}$. Suppose that it is false. We know -2 can be factorized into $-1 \cdot 2$ or $-2 \cdot 1$, so x is either -1 or -2, as $x^2 + 3 > 0$. However, $x^2 + 3 > 2$ for $x = 1, 2$, contradiction. Hence, $x(x^2 + 3) \neq -2$, so $f(x)$ is irreducible in $\mathbb{Z}[x]$. $\square$

Problem 7

Show that there is an infinite number of integers a such that $f(x) = x^7 + 15x^2 - 30x + a$ is irreducible in $\mathbb{Q}[x]$. What a's do you suggest?

Proof. By Eisenstein's Criteria, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if there is a prime p that divides 15, -30, and a, but not 1 and p^2 does not divide a^2. We show that any integers in $S = (\langle 3 \rangle \backslash \langle 9 \rangle) \cup (\langle 5 \rangle \backslash \langle 25 \rangle)$ suffices to be a. Suppose $a \in S$. a is a multiple of 3 or 5. If a is a multiple of 3, we may pick $p = 3$ and $f(x)$ would meet Eisenstein's Criteria, as $9 \nmid a$. Otherwise, we may pick $p = 5$ and $f(x)$ would also meet Eisenstein's Criteria, as $25 \nmid a$. $\square$

Problem 8

Let F be the field and φ an automorphism of $F[x]$ such that $\varphi(a) = a$ for every $a \in F$. 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. Suppose that $f(x)$ is irreducible in $F[x]$. $f(x) \neq k(x)h(x)$, for any noninvertible $k(x), h(x) \in F[x]$. Since φ is an automorphism, $g(x) = \varphi(f(x)) \neq \varphi(k(x)h(x)) = \varphi(k(x))\varphi(h(x))$, and thus $g(x)$ is irreducible. This also applies for φ^{-1}, and thus the converse is also true. $\square$

Problem 9

Let F be a field. Define the mapping

$$\varphi : F[x] \to F[x] \quad \text{by} \quad \varphi(f(x)) = f(x+1)$$

for every $f(x) \in F[x]$. Prove that φ is an automorphism of $F[x]$ such that $\varphi(a) = a$ for every $a \in F$.

Proof. Let $f(x), g(x) \in F[x]$. Suppose that $f(x) = g(x)$. Then, $\varphi(f(x)) = f(x+1) = g(x+1) = \varphi(g(x))$, so φ is well defined. Since there exists $f(x-1) \in F[x]$ such that $\varphi(f(x-1)) = f(x)$, φ is surjective. Let $f(x)$ be in the kernel of φ. Then, $\varphi(f(x)) = f(x+1) = 0$, so $f(x) = 0$. Hence, the kernel is trivial, and thus φ is injective. Since the constant polynomials do not depend on x, $\varphi(a) = a$, for all $a \in F$. Since $\varphi(f(x)g(x)) = f(x+1)g(x+1) = \varphi(f(x))\varphi(g(x))$, $\varphi(f(x)+g(x)) = f(x+1)+g(x+1) = \varphi(f(x))+\varphi(g(x))$ and $\varphi(1) = 1$, φ is an automorphism. $\square$

Problem 10

Let F be a field and $b \neq 0$ an element of F. Define the mapping

$$\varphi : F[x] \to F[x] \quad \text{by} \quad \varphi(f(x)) = f(bx) \quad \text{for every} \quad f(x) \in F[x].$$

Prove that φ is an automorphism of $F[x]$ such that $\varphi(a) = a$ for every $a \in F$.

Proof. Let $f(x), g(x) \in F[x]$. Suppose that $f(x) = g(x)$. Then, $\varphi(f(x)) = f(bx) = g(bx) = \varphi(g(x))$, so φ is well defined. Since F is a field, there exists $f(b^{-1}x) \in F$ such that $\varphi(f(b^{-1}x)) = f(x)$, and thus φ is surjective. Let $f(x)$ be in the kernel of φ. Then, $\varphi(f(x)) = f(bx) = 0$, so $f(x) = 0$. Hence, the kernel is trivial, and thus φ is injective. Since the constant polynomials do not depend on x, $\varphi(a) = a$, for all $a \in F$. Since $\varphi(f(x)g(x)) = f(bx)g(bx) = \varphi(f(x))\varphi(g(x))$, $\varphi(f(x) + g(x)) = f(bx) + g(bx) = \varphi(f(x)) + \varphi(g(x))$ and $\varphi(1) = 1$, φ is an automorphism. $\square$

Problem 11

Let F be a field, $b \neq 0$, c elements of F. Define the mapping

$$\varphi : F[x] \to F[x] \text{ by } \varphi(f(x)) = f(bx+c) \text{ for every } f(x) \in F[x].$$

Prove that φ is an automorphism of $F[x]$ such that $\varphi(a) = a$ for every $a \in F$.

Proof. Define the mapping

$$\phi : F[x] \to F[x] \quad \text{by} \quad \phi(f(x)) = f(bx) \quad \text{for every} \quad f(x) \in F[x].$$

By Problem 10, we already know ϕ is an automorphism of $F[x]$ such that $\phi(a) = a$ for every $a \in F$.

Define the mapping

$$\psi : F[x] \to F[x] \quad \text{by} \quad \psi(f(x)) = f(x+1)$$

for every $f(x) \in F[x]$. By Problem 9, we already know ψ is an automorphism of $F[x]$ such that $\psi(a) = a$ for every $a \in F$.

Since

$$\underbrace{\psi \circ \cdots \circ \psi}_{c \text{ times}} \circ \phi(f(x)) = \underbrace{\psi \circ \cdots \circ \psi}_{c \text{ times}}(f(bx)) = \underbrace{\psi \circ \cdots \circ \psi}_{c-1 \text{ times}}(f(bx+1)) = f(bx+c) = \varphi(f(x)),$$

φ is an automorphism of $F[x]$ such that $\varphi(a) = a$ for every $a \in F$. $\square$

Problem 12

Let φ be an automorphism of $F[x]$, where F is a field, such that $\varphi(a) = a$ for every $a \in F$. Prove that if $f(x) \in F[x]$, then $\deg \varphi(f(x)) = \deg f(x)$.

Proof. Since $\varphi(a) = a$ for every $a \in F$, φ is the unique ring homomorphism corresponding to the natural inclusion $F \hookrightarrow F[x]$, by the universal property of polynomial rings. Since φ maps

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

to

$$a_n(\varphi(x))^n + a_{n-1}(\varphi(x))^{n-1} + \cdots + a_0,$$

it suffices to show that $\varphi(x)$ is of degree 1, as $\deg \varphi(f(x)) = \deg \varphi(x) \deg f(x)$. $\deg \varphi(x)$ cannot be 0, otherwise $\varphi(f(x)) \in F$, then φ is not surjective and thus not an automorphism. Suppose for the sake of contradiction that $\deg \varphi(x) > 1$. Then, for non-constant $f(x) \in F[x]$, $\deg \varphi(f(x)) = \deg \varphi(x) \deg f(x) > \deg f(x) \geq 1$, which implies that the image of the automorphism ϕ does not contain polynomials of degree 1, contradiction. $\square$

Problem 13

Let φ be an automorphism of $F[x]$, where F is a field, such that $\varphi(a) = a$ for every $a \in F$. Prove there exist $b \neq 0$, c in F such that $\varphi(f(x)) = f(bx + c)$ for every $f(x) \in F[x]$.

Proof. Since $\varphi(a) = a$ for every $a \in F$, φ is the unique ring homomorphism corresponding to the natural inclusion $F \hookrightarrow F[x]$, by the universal property of polynomial rings. By problem 12, we know $\varphi(x)$ is a polynomial of degree 1 if φ is an automorphism, say $bx + c$. Then,

$$\begin{aligned}\varphi(f(x)) &= \varphi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) \\ &= a_n(\varphi(x))^n + a_{n-1}(\varphi(x))^{n-1} + \cdots + a_0 \\ &= f(\varphi(x)) = f(bx + c),\end{aligned}$$

and we are done. $\square$

Problem 14

Find a nonidentity automorphism φ of $\mathbb{Q}[x]$ such that φ^2 is the identity automorphism of $\mathbb{Q}[x]$.

Proof. From the natural inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}[x]$, the universal property gives us a ring homomorphism ϕ such that $\phi(x) = -x$. ϕ is obviously injective, as its kernel is trivial. For $p(x) \in \mathbb{Q}[x]$, there exists $p(-x) \in \mathbb{Q}[x]$ such that $\phi(p(-x)) = p(x)$, so ϕ is surjective. It follows that ϕ is a bijection and thus an automorphism. Now consider ϕ^2. $\phi^2(p(x)) = \phi(\phi(p(x))) = \phi(p(-x)) = p(x)$, and thus ϕ^2 is the identity automorphism. $\square$

Problem 15

Show that in Problem 14 you do not need the assumption $\varphi(a) = a$ for every $a \in \mathbb{Q}$ because any automorphism of $\mathbb{Q}[x]$ automatically satisfies $\varphi(a) = a$ for every $a \in \mathbb{Q}$.

Proof. Let ϕ be a ring automorphism of $\mathbb{Q}[x]$. We know $\phi(0) = 0$ and $\phi(1) = 1$. Since $\phi(x)+\phi(y) = \phi(x+y)$, we may prove by induction that $f(z) = f(z-1) + f(1) = zf(1) = z$, for all $z \in \mathbb{Z}$. Suppose that there exists $\frac{p}{q} \in \mathbb{Q}$ such that $\phi(\frac{p}{q}) \neq \frac{p}{q}$, $p, q \in \mathbb{Z}$. Then, $p = \phi(p) = \phi(q)\phi(\frac{p}{q}) \neq q \cdot \frac{p}{q}$, contradiction. Hence, $\phi(a) = a$, for all $a \in \mathbb{Q}$. $\square$

Problem 16

Let $\mathbb{C}$ be the field of complex numbers. Given an integer $n > 0$, exhibit an automorphism φ of $\mathbb{C}[x]$ of order n.

Proof. Consider $\varphi(f(x)) = f(e^{\frac{2i\pi}{n}}x)$. By problem 11, φ is an automorphism. Since

$$\varphi^n(f(x)) = \underbrace{\varphi \circ \cdots \circ \varphi}_{n \text{ times}}(f(x)) = \varphi\left(\left(\prod^n e^{\frac{2i\pi}{n}}\right)x\right) = \varphi(e^{2i\pi}x) = \varphi(x),$$

φ is of order n. $\square$

Problem 17

Given a ring R, let $S = R[x]$ be the ring of polynomials in x over R, and let $T = S[y]$ be the ring of polynomials in y over S. Show that:

(a) Any element $f(x, y)$ in T has the form $\sum a_{ij}x^iy^j$, where the a_{ij} are in R.

Proof. Let $f(x, y) \in T$. Since $f(x, y) \in S[y]$, $f(x, y) = \sum_j p(x)y^j = \sum_j \left(\sum_i a'_{ij}x^i\right) y^j = \sum a_{ij}x^iy^j$, for $p(x) \in S$ and $a_{ij}, a'_{ij} \in R$. □

(b) In terms of the form of $f(x, y)$ in T given in Part (a), give the condition for the equality of two elements $f(x, y)$ and $g(x, y)$ in T.

Proof. $f(x, y) = \sum f_{ij}x^iy^j = \sum g_{ij}x^iy^j = g(x, y)$, if and only if $f_{ij} = g_{ij}$, for all i, j. □

(c) In terms of the form for $f(x, y)$ in Part (a), give the formula for $f(x, y) + g(x, y)$, for $f(x, y), g(x, y)$ in T.

Proof. $f(x, y) + g(x, y) = \sum f_{ij}x^iy^j + \sum g_{ij}x^iy^j = \sum(h_{ij} + g_{ij})x^iy^j$. □

(d) Give the form for the product of $f(x, y)$ and $g(x, y)$ if $f(x, y)$ and $g(x, y)$ are in T. (T is called the ring of polynomials in two variables over R, and is denoted by $R[x, y]$).

Proof.

$$f(x,y)g(x,y) = \left(\sum f_{ij}x^iy^j\right)\left(\sum g_{ij}x^iy^j\right) = \sum \left(\sum_{m+n=i,p+q=j} f_{mp}g_{nq}\right) x^iy^j.$$

Since the product is of the form of $\sum a_{ij}x^iy^j$, it is in T. □

Problem 18

If D is an integral domain, show that $D[x, y]$ is an integral domain.

Proof. Since D is a commutative ring, $D[x][y] \simeq D[x, y]$, by Lemma 9.12. By Lemma 7.4, $D[x]$ is also an integral domain, and thus $D[x][y]$ is also an integral domain. $\square$