Final
Abstract Algebra
Math 320
Stephen Giang

Problem 1: Let T be the set of real 2×2 matrices with determinant 1:

$$T = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}; ad - bc = 1 \right\}.$$

Prove or disprove: under the usual matrix addition and multiplication, T is a ring:

Disproof. Notice the following:

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in T, \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \notin T$$

Notice that a and b are both in T as their determinant is equal to 1 and they contain real elements. However, their sum is not in T as their sum's determinant is equal to 2. This shows that T is not closed under addition. **Thus T is NOT a ring**

□

Problem 2: Determine if the following rings are fields. If the ring is a field, explain why. If the ring is not a field, explain why, and provide a zero divisor of the ring:

(a) $\mathbb{Q}[x]/(x^8 - 169x^6 + 52x^3 - 104x + 39)$

Notice that we can prove that $f(x) = x^8 - 169x^6 + 52x^3 - 104x + 39$ is irreducible in $\mathbb{Q}[x]$ using Eisenstein's Criterion. Notice the following:

(a) 13 is Prime

(b) $13 | -169, \qquad 13|52, \qquad 13|-104, \qquad 13|39$

(c) $13 \nmid 1, \qquad 13^2 \nmid 39$

Thus by Eisenstein's Criterion, $f(x)$ is irreducible. Now by Theorem 5.10, because we proved that $f(x)$ is irreducible, we know that **(a) is a field.**

(b) $\mathbb{Q}[x]/(7x^3 + 25x + 51)$

Notice that we can prove that $f(x) = 7x^3 + 25x + 51$ is irreducible in $\mathbb{Q}[x]$ by using Theorem 4.25. We can choose a prime number, 2, which doesn't divide 7. Now if we prove that $f(x)$ is irreducible in $\mathbb{Z}_2[x]$, then it will be irreducible in $\mathbb{Q}[x]$.

We can rewrite $f(x) \in \mathbb{Z}_2[x]$ as $x^3 + x + 1$. Because the degree of $f(x)$ is 3 and its leading coefficient is 1, its factors are polynomials of degree 2 with its roots. And notice that the only numbers in $\mathbb{Z}_2$ are 0 and 1:

$$f(0) = [1] \neq [0]$$
$$f(1) = [1] \neq [0]$$

Because $f(x)$ is irreducible in $\mathbb{Z}_2[x]$, it is also irreducible in $\mathbb{Q}[x]$. Now by Theorem 5.10, because we proved that $f(x)$ is irreducible, we know that **(b) is a field.**

(c) $\mathbb{Z}_5[x]/(x^3 - 3)$

Notice that x^3-3 has a root in $\mathbb{Z}_5$. If we let $f(x) = x^3-3$, then $f(2) = 8-3 = [5] = [0]$. Thus proving that $x - 2$ is a zero divisor, showing that **(c) is not a field.**

(d) $\mathbb{Z}_7[x]/(x^7 + 1)$

Notice that $x^7 + 1$ has a root in $\mathbb{Z}_7$. If we let $f(x) = x^7 + 1$, then $f(6) = 279936 + 1 = [279937] = [39991][7] = [0]$. Thus proving that $x - 6$ is a zero divisor, showing that **(d) is not a field.**

Problem 3: Explain why x^2 does not divide $x-5$ in $\mathbb{Q}[x]$.

By definition, "A polynomial with coefficients in $\mathbb{R}$ is an expression of the form:

$$a_0 + a_1 x + ... + a_n x^n$$

where n is a non-negative integer and $a_i \in \mathbb{R}$". So let x^2 divide $x-5$ such that

$$x - 5 = x^2 a(x)$$

where $a(x)$ is a polynomial in $\mathbb{Q}[x]$. By Theorem 4.2, we can see the following:

$$1 = deg[x-5] = deg[x^2 a(x)] = deg[x^2] + deg[a(x)] = 2 + deg[a(x)]$$

So we can see that $deg[a(x)]$ has to be -1, which would contradict the definition of polynomial as it must have non-negative exponents. Thus $\boldsymbol{x^2}$ **does not divide** $\boldsymbol{x-5}$ **in** $\mathbb{Q}[\boldsymbol{x}]$

Problem 4: : Let F be a field and suppose $f(x) \in F[x]$ is a polynomial of degree 5. Prove that if $f(x)$ has no factors in $F[x]$ of degree 3, then $f(x)$ has no factors in $F[x]$ of degree 2.

Proof. Let $f(x) \in F[x]$ be a polynomial of degree 5. Let $f(x)$ have no factors in $F[x]$ of degree 3.

By Theorem 4.2, the degrees of each pair of factors of $f(x)$ have to have a sum of 5. Also notice that by definition of polynomials, all of the exponents of the factors have to be non-negative integers.

Because for all factors with degree 2, they have to be paired with a factor of 3 because $2 + 3 = 5$. Finally, because $f(x)$ has no factors in $F[x]$ of degree 3, then we can conclude that $\boldsymbol{f(x)}$ **has no factors in** $\boldsymbol{F[x]}$ **of degree 2**

□

Problem 5: Let A be the following ring:

$$A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}$$

(a) Prove that $\mathbb{Q}[x]/(x^2 - 1) \cong A$

Proof. Let $f : \mathbb{Q}[x]/(x^2 - 1) \to A$ such that $f(ax + b) = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$.

Notice the following:

$$f(ax + b) = \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} c & d \\ d & c \end{pmatrix} = f(cx + d)$$

Thus the only way for this to be true is if $a = c$ and $b = d$, thus proving that f is injective.

Notice that for all matrices in A, $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, it can be written as a function, $f(ax + b)$, thus showing that f is surjective.

Notice the following homomorphic properties:

$$\begin{aligned} f(ax + b) + f(cx + d) &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ b + d & a + c \end{pmatrix} \\ &= f((a + c)x + (b + d)) = f((ax + b) + (cx + d)) \\ f(ax + b)f(cx + d) &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac + bd & ad + bc \\ ad + bc & ac + bd \end{pmatrix} \\ &= f((ac + bd)x + (ad + bc)) = f(adx^2 + acx + bdx + bc) \\ &= f((ax + b)(dx + c)) = f((ax + b)(cx + d)) \end{aligned}$$

Because we are in $\mathbb{Q}[x]/(x^2 - 1)$, the following is true: $[x^2] = [1]$ and $[x] = 1$. Thus allowing us to say $ad = adx^2$ and $dx + c = cx + d$

Because $f : \mathbb{Q}[x]/(x^2 - 1) \to A$ is bijective and satisfies the homomorphic properties, $\mathbb{Q}[x]/(x^2 - 1) \cong A$

□

(b) Let R, S be rings, and $f : R \to S$ be a ring homomorphism. Show that if $a, b \in R$ and $a \cdot b = 0_R$, then $f(a) \cdot f(b) = 0_S$.

Because f is a ring homomorphism, then the following is true for all $a, b \in R$

$$f(a \cdot b) = f(a) \cdot f(b)$$

Let $a \cdot b = 0_R$, such that the following is true:

$$f(a \cdot b) = f(0_R) = f(a) \cdot f(b)$$

By Theorem 3.10, we know that for all homomorphisms, $f(0_R) = 0_S$, such that we get the following:

$$\boldsymbol{f(a \cdot b) = f(0_R) = 0_S = f(a) \cdot f(b)}$$

(c) Use part (b) to find two zero divisors in A.

Notice that in $\mathbb{Q}[x]/(x^2 - 1)$, $x - 1$ and $x + 1$ are both zero divisors. So we have $(x-1)(x+1) = [0]$. If we take the same $f(ax+b) = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ from part (a), notice the following:

$$\begin{aligned} f((x-1) \cdot (x+1)) &= f(x-1) \cdot f(x+1) = f([0]) \\ &= \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_A \end{aligned}$$

Thus the zero divisors of A are $\boldsymbol{\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}}$**, and** $\boldsymbol{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}}$

Problem 6: Consider the set of lower-triangular matrices with integer coefficients:

$$R = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$$

You may assume that R is a ring (with the usual matrix addition and multiplication).

(a) Prove that the following subset I of R is an ideal in R:

$$I = \left\{ \begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} : b \in \mathbb{Z} \right\}$$

Notice that $0_R \in I$ by letting $X = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \in I$ with x = 0:

$$0_R = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = X \in I$$

Notice that I is closed under subtraction, and let $X = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} \in I$:

$$X - Y = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ (x-y) & 0 \end{pmatrix} \in I$$

Notice that I satisfies the absorption property, and let $X = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \in I$ and $Z = \begin{pmatrix} z_1 & 0 \\ z_2 & z_3 \end{pmatrix} \in R$

$$XZ = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \begin{pmatrix} z_1 & 0 \\ z_2 & z_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ xz_1 & 0 \end{pmatrix} \in I$$
$$ZX = \begin{pmatrix} z_1 & 0 \\ z_2 & z_3 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ xz_3 & 0 \end{pmatrix} \in I$$

Thus $\boldsymbol{I}$ of $\boldsymbol{R}$ is an ideal of $\boldsymbol{R}$

(b) Show that

$$\begin{pmatrix} 1 & 0 \\ -4 & 6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 16 & 6 \end{pmatrix} \mod I$$

By definition of $a \equiv b \mod I$, the following needs to be true: $a - b \in I$

$$\begin{pmatrix} 1 & 0 \\ -4 & 6 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 16 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -20 & 0 \end{pmatrix} \in I$$

Thus the following is true:

$$\boldsymbol{\begin{pmatrix} 1 & 0 \\ -4 & 6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 16 & 6 \end{pmatrix} \mod I}$$

Problem 7: Prove that the following polynomials are irreducible in $\mathbb{Q}[x]$:

(a)

$$k(x) = x^{17} + 16$$

Notice that we know $k(x)$ is irreducible if $k(x+1)$ is irreducible. So if we were to simplify $k(x+1)$, we would get:

$$k(x+1) = (x+1)^{17} + 16 = \sum_{n=0}^{17} \left[\binom{17}{n} x^{17-n} \right] + 16 = x^{17} + \sum_{n=1}^{16} \left[\binom{17}{n} x^{17-n} \right] + 17$$

Now by Eisenstein's Criterion, we can choose a prime number 17. We can see for all integers $n \in [1, 16]$, 17 divides $\binom{17}{n}$ because they are all multiples of 17. We can also see that 17 does not divide the leading coefficient, 1, and 17^2 does not divide the constant term, 17

Because $\boldsymbol{k(x+1)}$ is irreducible, $\boldsymbol{k(x)}$ is irreducible

(b)

$$f(x) = \frac{(x+7)^5 - 12005x - 16807}{x^2}$$

Notice we can simplify $f(x)$ to:

$$\begin{aligned} f(x) &= \frac{x^5 + 35\,x^4 + 490\,x^3 + 3430\,x^2 + 12005\,x + 16807 - 12005x - 16807}{x^2} \\ &= x^3 + 35\,x^2 + 490x + 3430 \end{aligned}$$

Notice that we can prove that $f(x) = x^3 + 35\,x^2 + 490x + 3430$ is irreducible in $\mathbb{Q}[x]$ by using Theorem 4.25. We can choose a prime number, 3, which doesn't divide 1. Now if we prove that $f(x)$ is irreducible in $\mathbb{Z}_3[x]$, then it will be irreducible in $\mathbb{Q}[x]$.

We can rewrite $f(x) \in \mathbb{Z}_3[x]$ as follows:

$$f(x) = x^3 + 2x^2 + x + 1$$

Because the degree of $f(x)$ is 3 and its leading coefficient is 1, its factors are polynomials of degree 2 with its roots. And notice that the only numbers in $\mathbb{Z}_3$ are 0,1,2:

$$\begin{aligned} f(0) &= [1] \neq [0] \\ f(1) &= [2] \neq [0] \\ f(2) &= [1] \neq [0] \end{aligned}$$

Because $\boldsymbol{f(x)}$ is irreducible in $\mathbb{Z}_3[\boldsymbol{x}]$, it is also irreducible in $\mathbb{Q}[\boldsymbol{x}]$

(c)

$$g(x) = \frac{x^{19} - 524288}{x - 2}$$

Notice that we know $g(x)$ is irreducible if $g(x+2)$ is irreducible. So if we were to simplify $g(x+2)$, we would get:

$$g(x{+}2) = \frac{(x+2)^{19} - 524288}{(x+2) - 2} = \frac{\sum_{n=0}^{19}\left[\binom{19}{n}2^n x^{19-n}\right] - 2^{19}}{x} = x^{18} + \sum_{n=1}^{17}\left[\binom{19}{n}2^n x^{18-n}\right] + 19(2^{18})$$

Now by Eisenstein's Criterion, we can choose a prime number 19. We can see for all integers $n \in [1, 17]$, 19 divides $\binom{19}{n}$ because they are all multiples of 19. We can also see that 19 does not divide the leading coefficient, 1, and 19^2 does not divide the constant term, 4980736

Because $\boldsymbol{g(x+2)}$ is irreducible, $\boldsymbol{g(x)}$ is irreducible in $\mathbb{Q}[\boldsymbol{x}]$

Problem 8: Find two rings of cardinality 125 of the form $\mathbb{Z}_p[x]/(q(x))$ that are not isomorphic to each other, and prove that they are not isomorphic.

Notice the following rings:

$$A = \mathbb{Z}_5[x]/(x^3 + 2x^2 + 2x + 2), \qquad B = \mathbb{Z}_5[x]/(x^3 - 3)$$

Notice that A and B's congruence classes can be written in the form of $ax^2 + bx + c$, with the coefficients being in $\mathbb{Z}_5$. This mean there exists 125 distinct congruence classes in each ring. This shows that both rings have cardinality 125.

Notice that $q(x) = x^3 + 2x^2 + 2x + 2$ is irreducible in $\mathbb{Z}_5[x]$. Because the degree of $q(x)$ is 3 and its leading coefficient is 1, its factors are polynomials of degree 2 with its roots. And notice that the only numbers in $\mathbb{Z}_5$ are 0,1,2,3,4:

$$q(0) = [2] \neq [0]$$
$$q(1) = [2] \neq [0]$$
$$q(2) = [2] \neq [0]$$
$$q(3) = [3] \neq [0]$$
$$q(4) = [1] \neq [0]$$

Because $q(x)$ is irreducible in $\mathbb{Z}_5[x]$, by Theorem 5.10, A is a field.

Notice that x^3-3 has a root in $\mathbb{Z}_5$. Notice if we let $p(x) = x^3-3$, then $p(2) = 8-3 = [5] = [0]$. Thus proving that $x - 2$ is a zero divisor, showing that B is not a field.

Propeties are preserved by isomorphisms. This means that isormorphisms will map zero divisors of the first ring to the zero divisors of the second ring. If one ring, A, doesn't have any zero divisors while the other ring, B does, then they can't be isomorphic to each other. In short, both rings have to be fields or both not fields, and A is a field, while B is not.

Thus A and B are two rings of cardinality 125 of the form $\mathbb{Z}_p[x]/(q(x))$ that are not isomorphic to each other

Problem EC: Prove that the following polynomial is irreducible in $\mathbb{Q}[x]$:

$$h(x) = \frac{x^7 - 109375x + 468750}{x^2 - 10x + 25}$$

Notice that we know $h(x)$ is irreducible if $h(x+5)$ is irreducible, so if we were to to simplify $h(x+5)$, we would get

$$\begin{aligned}
h(x+5) &= \frac{(x+5)^7 - 109375(x+5) + 468750}{((x+5)-5)^2} \\
&= \frac{\sum_{n=0}^{7} \left[\binom{7}{n} 5^n x^{7-n}\right] - 109375x - 78125}{x^2} \\
&= \frac{\sum_{n=0}^{5} \left[\binom{7}{n} 5^n x^{7-n}\right]}{x^2} \\
&= \sum_{n=0}^{5} \binom{7}{n} 5^n x^{5-n} \\
&= x^5 + \sum_{n=1}^{4} \left[\binom{7}{n} 5^n x^{5-n}\right] + 21(3125)
\end{aligned}$$

Now by Eisenstein's Criterion, we can choose a prime number 7. We can see for all integers $n \in [1,4]$, 7 divides $\binom{7}{n}$ because they are all multiples of 7. We can also see that 7 does not divide the leading coefficient, 1, and 7^2 does not divide the constant term, 65625

Because $h(x+5)$ is irreducible, $h(x)$ is irreducible in $\mathbb{Q}[x]$