Math 402 Homework 4

Alexandre Lipson

February 5, 2025

Problem 1. Let F be a field. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $M(F)$.

a) Prove A invertible $\iff ad - bc \neq 0_F$.

b) Prove A is a zero divisor $\iff ad - bc = 0_F$.

Proof of a. The inverse of the 2×2 matrix A is given by

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

where $AA^{-1} = I = A^{-1}A$ and I is the identity matrix. This matrix only exists where $ad - bc \neq 0_F$. $\square$

Proof of b. ($\impliedby$) Consider $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. We have that,

$$AB = \begin{pmatrix} ad - bc & ad - bc \\ ad - bc & ad - bc \end{pmatrix} = BA.$$

But $ad - bc = 0_F \implies AB = BA = O_{M(F)}$, so A is a zero divisor since $B \in M(F)$.

($\implies$) If A is a zero divisor, then $\exists B$ such that

$$AB = BA = 0_{M(F)}.$$

We have already seen a B for which this holds, and all matrix entries of the product are $ad - bc$, which therefore must be zero. $\square$

Problem 2. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $M(\mathbb{Z})$. Prove the following:

a) $ad - bc = \pm 1 \implies A$ invertible in $M(\mathbb{Z})$.

b) $ad - bc \neq 0, \pm 1 \implies A$ is neither a unit nor a zero divisor in $M(\mathbb{Z})$.

Proof of a. We will show that, when $ad - bc = \pm 1, \exists A^{-1} \in M(\mathbb{Z})$. We know that the inverse matrix A^{-1} is given by $\frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, so $A^{-1} \in M(\mathbb{Z})$ only when $\frac{1}{ad-bc} \in \mathbb{Z}$, which occurs when $ad - bc = \pm 1$ as all integers can be expressed as a rational number with denominator of ± 1. $\square$

Proof of b. We have already show that A is invertible iff $ad - bc = \pm 1$.

So, if $ad - bc \neq \pm 1$, then A is not invertible and therefore cannot be a unit.

If $ad - bc = 0$, then A is also not invertible as in Problem 1, so A cannot be a unit under those conditions either.

If $ad - bc = \pm 1$, then A is a unit and therefore not a zero divisor.

Suppose, for a contradiction, that A is a zero divisor when $ad - bc \neq 0$. Then, $\exists B \neq 0_{M(\mathbb{Z})}$ such that $AB = 0_{M(\mathbb{Z})}$.

Note that $\forall A, B$ matrices, $\det AB = \det A \det B$.

So, $\det AB = \det 0_{M(\mathbb{Z})} = 0 = \det A \det B$.

But $B \neq 0_{M(\mathbb{Z})} \implies \det B \neq 0 \implies \det A = 0$.

Then, $\det A = 0 \implies ad - bc = 0$, contradicting the assumption that $ad - bc \neq 0$.

Thus, A must not have been a zero divisor. □

Problem 3. Prove $\mathbb{R}$ is isomorphic to the ring S of 2×2 matrices of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $a \in \mathbb{R}$.

Proof. We will construct an isomorphism $f : \mathbb{R} \to S$. We will show that f is a bijection and a homomorphism.

First, let f be defined by the map
$$a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$
Clearly, this is invertible $\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mapsto a \right)$.

So, f is a bijection. We can also write the map as $a \mapsto aI$, where I is the 2×2 identity matrix.

Now, we will consider the addition and multiplication operations under the image of the map. We have that,
$$f(a + b) = (a + b)I = aI + bI = f(a) + f(b).$$
We also have that,
$$f(ab) = abI = abI^2 = aI\, bI = f(a)f(b).$$
So, f is a homomorphism.

Since f is bijective and homomorphic, then f is an isomorphism.

Since there exists the isomorphism f between $\mathbb{R}$ and S, then these rings are isomorphic. □

Problem 4. Let $\mathbb{Q}(\sqrt{2}) = \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$. Prove $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ given by $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism.

Proof. We see that f is invertible because we can simply flip the sign of the $\sqrt{2}$ part. So, f is a bijection.

Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$.

We will show that f is a homomorphism.

For addition,

$$f(x + y) = f((a + c) + (b + d)\sqrt{2}) = (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}) = f(x) + f(y).$$

For multiplication,

$$f(xy) = f((ac + 2bd) + (ad + bc)\sqrt{2}) = ac - ad\sqrt{2} - bc\sqrt{2} + 2bd = (a - b\sqrt{2})(c - d\sqrt{2}) = f(x)f(y).$$

So, f is a homomorphism.

Since f is a bijection and a homomorphism, then f is an isomorphism. □

Problem 5. Prove that if $f : \mathbb{Z} \to \mathbb{Z}$ is an isomorphism, then f is the identity map.

Proof. Since f is an isomorphism, then f is bijective and homomorphic.

Since f is homomorphic, then we have that

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b). \end{aligned}$$

So,

$$\begin{aligned} f(a) &= f(a + 0) = f(a) + f(0) \\ &= f(a + 0 + \cdots + 0) = f(a) + nf(0). \end{aligned}$$

But $f(a) = f(a) + nf(0)\ \forall n \implies f(0) = 0$.

Similarly,

$$f(1) = f(1 \cdot 1) = f(1)f(1) = \cdots = nf(1).$$

So, $f(1) = nf(1)\ \forall n \implies f(1) = 1$

Then, by the associativity of addition,

$$\begin{aligned} f(1 + 1) &= f(1) + f(1) = 2f(1) \\ f(1 + 1 + 1) &= f(1) + f(1) + f(1) = 3f(1) \\ &\vdots \\ f(n) &= nf(1). \end{aligned}$$

But, $f(n) = nf(1)\ \forall n \implies f(n) = n$.

Thus, f must be the identity map. □

Problem 6. Find the polynomials $q(x), r(x)$ such that $f(x) = g(x)q(x) + r(x)$ and $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

a) $f(x) = 3x^4 - 2x^3 + 6x^2 - x + 2$, $g(x) = x^2 + x + 1$ in $\mathbb{Q}[x]$.

$$\begin{array}{rr}
 & 3x^2 - 5x + 8 \\
x^2+x+1 \big) & \overline{3x^4 - 2x^3 + 6x^2 \quad - x + 2} \\
 & \underline{-3x^4 - 3x^3 - 3x^2} \quad\quad\quad \\
 & -5x^3 + 3x^2 \quad - x \quad\; \\
 & \underline{5x^3 + 5x^2 + 5x} \quad\; \\
 & 8x^2 + 4x + 2 \\
 & \underline{-8x^2 - 8x - 8} \\
 & -4x - 6
\end{array}$$

Thus, $f(x) = (x^2 + x + 1)(3x^2 - 5x + 8) + (-4x - 6)$ in $\mathbb{Q}[x]$.

b) $f(x) = x^4 - 7x + 1$, $g(x) = 2x^2 + 1$ in $\mathbb{Q}[x]$.

$$\begin{array}{rr}
 & \frac{1}{2}x^2 \quad\quad - \frac{1}{4} \\
2x^2+1 \big) & \overline{x^4 \quad\quad\quad - 7x + 1} \\
 & \underline{-x^4 - \frac{1}{2}x^2} \quad\quad\quad\quad \\
 & -\frac{1}{2}x^2 - 7x + 1 \\
 & \underline{\frac{1}{2}x^2 \quad\quad\quad + \frac{1}{4}} \\
 & -7x + \frac{5}{4}
\end{array}$$

Thus, $f(x) = (2x^2 + 1)\left(\frac{1}{2}x^2 - \frac{1}{4}\right) + \left(-7x + \frac{5}{4}\right)$ in $\mathbb{Q}[x]$.

c) $f(x) = 2x^4 + x^2 - x + 1$, $g(x) = 2x - 1$ in $\mathbb{Z}_5[x]$.

$$\begin{array}{rr}
 & x^3 - 2x^2 + 2x - 2 \\
2x-1 \big) & \overline{2x^4 \quad\quad\quad + x^2 \quad - x + 1} \\
 & \underline{-2x^4 + x^3} \quad\quad\quad\quad\quad\quad\quad \\
 & x^3 \quad + x^2 \quad - x + 1 \\
 & \underline{4x^3 - 2x^2} \quad\quad\quad\quad \\
 & 4x^2 \quad - x + 1 \\
 & \underline{-4x^2 + 2x} \quad\quad \\
 & x + 1 \\
 & \underline{4x - 2} \\
 & 4
\end{array}$$

Thus, $f(x) = (2x - 1)(x^3 - 2x^2 + 2x - 2) + 4$ in $\mathbb{Z}_5[x]$.

d) $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$, $g(x) = 3x^2 + 2$ in $\mathbb{Z}_7[x]$.

$$\begin{array}{rr}
 & -x^2 + 3x - 2 \\
3x^2+2 \big) & \overline{4x^4 + 2x^3 + 6x^2 + 4x + 5} \\
 & \underline{3x^4 \quad\quad\quad + 2x^2} \quad\quad\quad\quad \\
 & 2x^3 + \; x^2 + 4x + 5 \\
 & \underline{-9x^3 \quad\quad\quad - 6x} \quad\quad \\
 & x^2 + 3x + 5 \\
 & \underline{6x^2 + \quad\quad 4} \\
 & 3x + 2
\end{array}$$

Thus, $f(x) = (3x^2 + 2)(-x^2 + 3x - 2) + (3x + 2)$ in $\mathbb{Z}_7[x]$.

Problem 7. Prove that is F is a field, then $F[x]$ is not a field.

Proof. Consider $x \in F[x]$.

The identity in $F[x]$ is the polynomial 1.

Note that, $\forall p(x) \in F[x]$, $\deg p(x) \geq 0$ (except when $p(x) = 0 \implies \deg p(x) = -\infty$).

Then, $x \cdot f(x) = 1$ has the solution $f(x) = x^{-1}$, but $\deg f(x) = -1 < 0$, which means that $f(x) \notin F[x]$.

So, an element $x \in F[x]$ does not have an inverse in $F[x]$.

Thus, $F[x]$ is not a field. □

Problem 8. Let $\varphi : R[x] \to R$ be the function that maps each polynomial in $R[x]$ onto its constant term in R. Prove φ is a surjective homomorphism of rings.

Proof. First, we will show that φ is surjective.

$\forall r \in R$, $r \in R[x]$ as well. So, the entire codomain is covered by the map φ from just the constant polynomials already in $R[x]$.

There are infinitely many polynomials with a given constant term r, but we have that all such $r \in R$ are covered as they belong in $R[x]$ as well.

Next, we will show that φ is a homomorphism.

Let $f(x) = r + a_1x + \cdots + a_nx^n$ and $g(x) = s + b_1x + \cdots b_mx^m$.

Then, for addition,

$$\begin{aligned}
\varphi(f(x) + g(x)) &= \varphi(r + s + a_1x + b_1x + \cdots + b_mx^m + \cdots + a_nx^n) \\
&= r + s \\
&= \varphi(r + a_1x + \cdots + a_nx^n) + \varphi(s + b_1x + \cdots b_mx^m) \\
&= \varphi(f(x)) + \varphi(g(x)).
\end{aligned}$$

For multiplication,

$$\begin{aligned}
\varphi(f(x)g(x)) &= \varphi(a_nb_mx^{n+m} + \cdots + a_1b_1x^2 + a_1sx + b_1rx + rs) \\
&= rs \\
&= \varphi(r + a_1x + \cdots + a_nx^n)\varphi(s + b_1x + \cdots b_mx^m) \\
&= \varphi(f(x))\varphi(g(x)).
\end{aligned}$$

So, f is a homomorphism.

Thus, f is a surjective homomorphism. □

Problem 9. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ be the function that maps polynomials $a_0 + a_1x + \cdots + a_kx^k$ in $\mathbb{Z}[x]$ onto polynomials $[a_0] + [a_1]x + \cdots + [a_k]x^k$ where $[a]$ denotes the congruence class of a in $\mathbb{Z}_n$. Prove φ is a surjective homomorphism of rings.

Proof. First, we will show that φ is surjective.

Consider $f(x) \in \mathbb{Z}_n[x]$. Then, the canonical representation of every such polynomial also belongs in $\mathbb{Z}[x]$.

So, all elements in the codomain are mapped to by φ by at least $f(x) \in \mathbb{Z}[x]$.

Thus, φ is surjective.

Next, we will show that φ is a homomorphism.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots b_mx^m$. WLOG assume $m < n$.

Note that $[a + b] = [a] + [b]$ and $[ab] = [a][b]$.

Then, for addition,

$$\begin{aligned}
\varphi(f(x) + g(x)) &= \varphi((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n) \\
&= [a_0 + b_0] + [a_1 + b_1]x + \cdots + [a_m + b_m]x^m + [a_{m+1}]x^{m+1} + \cdots + [a_n]x^n \\
&= [a_0] + [a_1]x + \cdots + [a_n]x^n + [b_0] + [b_1]x + \cdots [b_m]x^m \\
&= \varphi(f(x)) + \varphi(g(x)).
\end{aligned}$$

For multiplication,

$$\begin{aligned}
\varphi(f(x)g(x)) &= \varphi(a_0b_0 + a_0b_1x + a_1b_0x + \cdots + a_nb_mx^{n+m}) \\
&= [] \\
&.
\end{aligned}$$

□

Problem 10. Use the Euclidean Algorithm to find the gcd (monic) of the given polynomials.

i) $x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Q}[x]$.
We will preform successive polynomial long divisions, performing division with of the resulting divisor by the resulting remainder, ignoring the quotient.

$$\begin{array}{r|l}
 & \hfill x - 1 \\ \hline
x^4 + 2x^3 + 5x^2 + 4x + 4 & x^5 + x^4 + 2x^3 - x^2 - x - 2 \\
 & - x^5 - 2x^4 - 5x^3 - 4x^2 - 4x \\ \cline{2-2}
 & \hfill - x^4 - 3x^3 - 5x^2 - 5x - 2 \\
 & \hfill x^4 + 2x^3 + 5x^2 + 4x + 4 \\ \cline{2-2}
 & \hfill - x^3 \qquad\qquad - x + 2
\end{array}$$

Now, we will compute for $x^4 + 2x^3 + 5x^2 + 4x + 1$ and $-x^3 - x + 2$.

$$\begin{array}{r|l}
 & \hfill - x - 2 \\ \hline
- x^3 - x + 2 & x^4 + 2x^3 + 5x^2 + 4x + 1 \\
 & - x^4 \qquad\quad - x^2 + 2x \\ \cline{2-2}
 & \hfill 2x^3 + 4x^2 + 6x + 1 \\
 & \hfill - 2x^3 \qquad\quad - 2x + 4 \\ \cline{2-2}
 & \hfill 4x^2 + 4x + 5
\end{array}$$

Next, for $-x^3 - x + 2$ and $4x^2 + 4x + 5$.

$$\begin{array}{rr}
 & -\frac{1}{4}x + \frac{1}{4} \\ \cline{2-2}
4x^2+4x+5 \big) & -x^3 \qquad\qquad -x + 2 \\
 & \underline{x^3 + x^2 + \frac{5}{4}x \quad\;\;} \\
 & x^2 + \frac{1}{4}x + 2 \\
 & \underline{-x^2 \;\; - x - \frac{5}{4}} \\
 & -\frac{3}{4}x + \frac{3}{4}
\end{array}$$

Finally, for $4x^2 + 4x + 5$ and $-\frac{3}{4}x + \frac{3}{4}$.

$$\begin{array}{rr}
 & -\frac{16}{3}x - \frac{32}{3} \\ \cline{2-2}
-\frac{3}{4}x + \frac{3}{4} \big) & 4x^2 \;\; + 4x \;\; + 5 \\
 & \underline{-4x^2 \;\; + 4x \quad\;\;} \\
 & 8x \;\; + 5 \\
 & \underline{-8x \;\; + 8} \\
 & 13
\end{array}$$

So, we see $x - 1$ is the gcd of $x^5 + x^4 + 2x^3 - x^2 - x - 2$ and $x^4 + 2x^3 + 5x^2 + 4x + 4$ in $\mathbb{Q}[x]$.

ii) $4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $3x^3 + 5x^2 + 6x$ in $\mathbb{Z}_7[x]$.

$$\begin{array}{rr}
 & -x \\ \cline{2-2}
3x^3+5x^2+6x \big) & 4x^4 + 2x^3 + 6x^2 + 4x + 5 \\
 & \underline{3x^4 + 5x^3 + 6x^2 \qquad\quad\;\;} \\
 & 5x^2 + 4x + 5
\end{array}$$

$$\begin{array}{rr}
 & -5x \\ \cline{2-2}
5x^2+4x+5 \big) & 3x^3 + 5x^2 + 6x \\
 & \underline{4x^3 + 6x^2 + 4x} \\
 & 4x^2 + 3x
\end{array}$$

$$\begin{array}{rr}
 & -4 \\ \cline{2-2}
4x^2+3x \big) & 5x^2 + 4x + 5 \\
 & \underline{2x^2 + 5x \quad\;\;} \\
 & 2x + 5
\end{array}$$

$$\begin{array}{rr}
 & 2x \\ \cline{2-2}
2x+5 \big) & 4x^2 + 3x \\
 & \underline{-4x^2 - 3x} \\
 & 0
\end{array}$$

Thus, $(2x + 5)4 = x + 3$ in $\mathbb{Z}_7[x]$ is the gcd.

iii) $x^4 + x + 1$ and $x^2 + x + 1$ in $\mathbb{Z}_2[x]$.

$$\begin{array}{rr}
 & x^2 + x \\ \cline{2-2}
x^2+x+1 \big) & x^4 \qquad\qquad + x + 1 \\
 & \underline{-x^4 - x^3 - x^2 \qquad\quad\;\;} \\
 & x^3 + x^2 + x + 1 \\
 & \underline{-x^3 - x^2 - x \quad\;\;} \\
 & 1
\end{array}$$

So, $x^2 + x + 1$ is the gcd of $x^4 + x + 1$ and $x^2 + x + 1$ in $\mathbb{Z}_2[x]$.