MATH 100B: Homework #1

Due on Janurary 18, 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 any field is an integral domain.

Proof. Let F be a field, and let $a, b \in F$, such that $ab = 0$. Suppose for the sake of contradiction that $a, b \neq 0$. Since F is a division ring, there exists $a^{-1} \in F$. But this implies $a^{-1}ab = b = 0$, contradiction. Thus, F is an integral domain. $\square$

Problem 2

Fine all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Proof. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ if and only if $\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ if and only if $b = c = 0$. Thus, only diagonal 2×2 matrices meet the requirement. $\square$

Problem 3

Let R be any ring with unit, S the ring of 2×2 matrices over R.

(a) Check the associative law of multiplication in S.

Proof. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} g & h \\ k & l \end{pmatrix}, \begin{pmatrix} w & x \\ y & z \end{pmatrix} \in S$. Since

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} g & h \\ k & l \end{pmatrix}\right]\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} ag+bk & ah+bl \\ cg+dk & ch+dl \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} agw+bkw+ahy+bly & agx+bkx+ahz+blz \\ cgw+dkw+chy+dly & cgx+dkx+chz+dlz \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left[\begin{pmatrix} g & h \\ k & l \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix}\right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} gw+hy & gx+hz \\ kw+ly & kx+lz \end{pmatrix} = \begin{pmatrix} agw+bkw+ahy+bly & agx+bkx+ahz+blz \\ cgw+dkw+chy+dly & cgx+dkx+chz+dlz \end{pmatrix},$$

the associative law is met. ☐

(b) Show that $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, b, c \in R \right\}$ is a subring of S.

Proof. We name the set L. L contains the unit, namely the identity matrix. If suffices to check that L is closed under addition, additive inverses, and multiplication. Let $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}, \begin{pmatrix} g & h \\ 0 & k \end{pmatrix} \in L$. Since $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} + \begin{pmatrix} g & h \\ 0 & k \end{pmatrix} = \begin{pmatrix} x+g & y+h \\ 0 & z+k \end{pmatrix} \in L$, L is closed under addition. Since there exists $\begin{pmatrix} -x & -y \\ 0 & -z \end{pmatrix} \in L$ such that $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} + \begin{pmatrix} -x & -y \\ 0 & -z \end{pmatrix} = \begin{pmatrix} -x & -y \\ 0 & -z \end{pmatrix} + \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, L is closed under taking additive inverse. Since $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\begin{pmatrix} g & h \\ 0 & k \end{pmatrix} = \begin{pmatrix} xg & xh+yk \\ 0 & zk \end{pmatrix} \in L$, L is closed under multiplication. Therefore, L is a subring. ☐

(c) Show that $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ has an inverse in S if and only if a and c have inverses in R. In that case write down $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1}$ explicitly.

Proof. Suppose that there exists $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} x & y \\ w & z \end{pmatrix} \in S$, such that $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ w & z \end{pmatrix} = \begin{pmatrix} x & y \\ w & z \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then, $\begin{pmatrix} ax+bw & ay+bz \\ cw & cz \end{pmatrix} = \begin{pmatrix} xa & xb+yc \\ wa & wb+zc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Notice that $w = 0$, otherwise $a = c = 0$ and $xa = 0 \neq 1$. Thus, we have $xa = ax + bw = ax = 1$ and $cz = wb + zc = zc = 1$, so a, c have inverse $x, z \in R$, respectively. Since $ay + bc^{-1} = a^{-1}b + yc = 0$, we know $y = -a^{-1}bc^{-1}$, and so $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix}$.

We now suppose that $a^{-1}, c^{-1} \in R$. Then, there exists $\begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix} \in S$, such that

$$\begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and we are done. ☐

Problem 4

Let $F : \mathbb{C} \to \mathbb{C}$ be defined by $F(a+bi) = a - bi$. Show that:

(a) $F(xy) = F(x)F(y)$ for $x, y \in \mathbb{C}$.

Proof. Let $x = a + bi, y = c + di \in \mathbb{C}$.

$$\begin{aligned} F(xy) &= F[(a+bi)(c+di)] \\ &= F(ac - bd + (ad+bc)i) \\ &= ac - bd - (ad+bc)i \\ &= (a-bi)(c-di) = F(x)F(y). \end{aligned}$$

□

(b) $F(x\bar{x}) = |x|^2$.

Proof.

$$F(x\bar{x}) = F((a+bi)(a-bi)) = F(a^2+b^2) = |x|^2.$$

□

(c) Using Parts (a) and (b), show that

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

Proof.

$$\begin{aligned} (a^2+b^2)(c^2+d^2) &= F(x\bar{x})F(y\bar{y}) \\ &= F(x\bar{x}y\bar{y}) \\ &= F(xy\bar{x}\bar{y}) \\ &= F(xy\overline{xy}) \\ &= |xy|^2 \\ &= (ac-bd)^2 + (ad+bc)^2. \end{aligned}$$

□

Problem 5

Show that the only quaternions commuting with i are of the form $\alpha + \beta i$.

Proof. Let $q = ai+bj+ck+d$ be a quaternion that commutes with i. This means that $qi = -a-bk+cj+di = -a + bk - cj + di = iq$, so $b = -b$ and $c = -c$. Thus, $b = c = 0$, so $q = d + ai$ is of the form $\alpha + \beta i$. $\square$

Problem 6

Find the quaternions that commute with both i and j.

Proof. Let $q = ai + bj + ck + d$ be a quaternion that commutes with both i and j. This means that $qi = -a - bk + cj + di = -a + bk - cj + di = iq$ and $qj = ak - b - ci + dj = -ak - b + ci + dj = jq$, so $b = -b, c = -c$, and $a = -a$. Thus, $a = b = c = 0$, so q is a real number. $\square$

Problem 7

Show that there is an *inifnite* number of solutions to $x^2 = -1$ in the quaternions.

Proof. Consider $x = bi + cj + dk$. Then, $x^2 = -(b^2 + c^2 + d^2) = -1$, but $b^2 + c^2 + d^2 = 1$ has infinitly many real solutions. Therefore, there is an inifnite number of solutions to $x^2 = -1$ in the quaternions. $\square$

Problem 8

In the quaternions, consider the following set G having eight elements: $G = \{\pm 1, \pm i, \pm j, \pm k\}$.

(a) Prove that G is a group under multiplication.

Proof. Since the quaternions from a division ring, it suffices to show that G is closed under multiplication and taking inverses. By the quaternions multiplication rule carved on the Brougham Bridge in Dublin, G is closed under multiplication. Since the inverse of each element in G is just the conjugate of itself, which is also in G, G is closed under taking inverses, and this completes the proof. $\square$

(b) List all subgroups of G.

Proof. G itself and the trivial subgroup $\{1\}$ are subgroups of G. By Lagrange's Theorem, the remaining subgroups are of sizes either 2 or 4. We first consider subgroups generated by a single element. We know $\langle -1 \rangle = \{\pm 1\}$. Consider the subgroup generated by i or $-i$. We get $\langle i \rangle = \langle -i \rangle = \{\pm 1, \pm i\}$. By symmetry, we also have $\{\pm 1, \pm j\}$ and $\{\pm 1, \pm k\}$. Since any pair of elements $\neq \pm 1$ and not from the same subgroup listed above would generate G, we have listed all the subgroups of G. $\square$

(c) What is the center of G.

Proof. Since only ± 1 commute with all elements in G, $\{\pm 1\}$ is the center of G. $\square$

(d) Show that G is a nonabelian group all of whose subgroups are normal.

Proof. Since $ij \neq ji$, G is nonabelian. Since subgroups of order 4 is half the size of G, all subgroups of order 4 are normal. However, the remaining subgroups of G are the trivial subgroup, the center, and G itself, so all subgroups of G are normal. $\square$

Problem 9

Define the map * in the quaternions by

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)^* = (\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k).$$

Show that

(a) $x^{**} = (x^*)^* = x$.

(b) $(x + y)^* = x^* + y^*$.

(c) $xx^* = x^*x$ is real and nonnegative.

(d) $(xy)^* = y^*x^*$.

Proof. Let $x = a + bi + cj + dk$, $y = m + yi + wj + zk$.

(a) $x^{**} = (a - bi - cj - dk)^* = a + bi + cj + dk = x$

(b)

$$\begin{aligned}
(x + y)^* &= ((a + m) + (b + y)i + (c + w)j + (d + z)k)^* \\
&= (a + m) - (b + y)i - (c + w)j - (d + z)k \\
&= (a - bi - cj - dk) + (m - yi - wj - zk) = x^* + y^*.
\end{aligned}$$

(c) $xx^* = (a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2 = (a-bi-cj-dk)(a+bi+cj+dk) = x^*x$, which is a sum of squares.

(d)

$$\begin{aligned}
(xy)^* &= ((a + bi + cj + dk)(m + yi + wj + zk))^* \\
&= ((am - by - cw - dz) + (ay + bm - cz + dw)i + (az - bx + cm + dy)j + (aw + bx - cy + dm)k)^* \\
&= (am - by - cw - dz) - (ay + bm - cz + dw)i - (az - bx + cm + dy)j - (aw + bx - cy + dm)k, \\
y^*x^* &= am + aw - ayi + azi - bmi - bw - by + bz + cm + cw - cyi + czi + dmi + dw + dy - dz \\
&= (am + bw + cz + dy) - (ay + bm - cz + dw)i - (az + bx - cm - dy)j - (aw - bx + cy - dm)k,
\end{aligned}$$

so $(xy)^* = y^*x^*$.

$\square$

Problem 10

If R is an integral domain and $ab = ac$ for $a \neq 0, b, c \in R$, show that $b = c$.

Proof. $ab = ac$ implies $ab - ac = a(b - c) = 0$. Since R is an integral domain and $a \neq 0$, we know $b - c = 0$, and so $b = c$. $\square$

Problem 11

If R is a finite integral domain, show that R is a field.

Proof. Since R is an integral domain, $R - \{0\}$ is closed under multiplication. Thus, it suffices to show that R is closed under taking inverse and contains the unit. Suppose for the sake of contradiction that $a \neq 0$ does not have an multiplicative inverse in $R - \{0\}$. Then, $a^i \neq 1$ for finite i, which makes R an infinite group, contradiction. Therefore, $R - \{0\}$ is closed under taking inverse. With the same arguement, we may also show that R contains the unit, and this completes the proof that R is a field. $\square$

Problem 12

If F is a finite field, show that:

(a) There exists a prime p such that $pa = 0$ for all $a \in F$.

Proof. Denote $[k]$ as 1 added to itself $k \in \mathbb{N}$ times. Note that $[i][j] = [ij]$, for $i, j \in \mathbb{N}$. Then,

$$ka = \underbrace{a + a + \cdots + a}_{k \text{ times}} = (\underbrace{1 + 1 + \cdots + 1}_{k \text{ times}})a = [k]a.$$

Since F is finite, there exists k such that $[k]a = 0$. Since F is an integral domain, $[k]a = 0$ implies $[k] = 0$. Suppose that k is a composite number, say $k = xy$. Then, $[k] = [x][y] = 0$, so one of $[x], [y]$ is equal to 0. Suppose that $[x] = 0$. We may recursively take $[x]$ as our current $[k]$ and decompose it to eventually end up with a prime number p such that $[p] = 0$, and thus $pa = [p]a = 0$, for all $a \in F$. $\square$

(b) If F has q elements, then $q = p^n$ for some integer n.

Proof. Since $pa = 0$ for all $a \in F$, all non-identity elements in F are of order p under addition. Therefore, there does not exists prime number $m \neq p$ that divides q, otherwise there exists an element of order m, by Sylow's Theorem. $\square$