Math 71: Algebra **Fall 2022**

PSET 7 — 2022-11-04

Prof. Voight ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***Abstract Algebra*** by **David S. Dummit & Richard M. Foote**.

(b) ***Algebra*** by **Jacob K. Goldhaber & Gertrude Ehrlich**

Problems

1. (DF 7.1.1, 7.1.15)

(a) Show that $(-1)^2 = 1$ in any ring R.

In a ring (with identity), suppose $1 \neq 0$ is well defined as the multiplicative identity. Furthermore, suppose that -1 is well-defined as the *additive inverse* of 1. Then, $1 + (-1) = 0$. By nature of rings, $0 \cdot a = 0$ for all $a \in R$. Therefore:

$$\begin{aligned} 0 \cdot (-1) &= 0 && \text{(since } 0 \cdot a = 0 \text{ for all } a \in R\text{)} \\ (1 + (-1)) \cdot (-1) &= 0 && \text{(addition of additive inverse)} \\ (1 \cdot (-1)) + (-1)^2 &= 0 && \text{(distributivity of multiplication in } R\text{)} \\ -1 + (-1)^2 &= 0 && \text{(multiplication by multiplicative identity)} \\ \therefore (-1)^2 &= 1 \end{aligned}$$

(b) A ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Show that every Boolean ring is commutative. *[Hint: Not every nonzero element of R is a unit.]*

Given $a, b \in R$ such that $a \neq 0$ and $b \neq 0$, then $a + b \in R$ and $a + b = (a + b)^2$. By expanding the right-hand side, we have:

$$\begin{aligned}
a + b = (a + b)^2 &= a^2 + ab + ba + b^2 \quad \text{(since } a = a^2 \text{ for all } a \in R\text{)} \\
a^2 + b^2 &= a^2 + ab + ba + b^2 \quad \text{(since } a = a^2,\ b = b^2\text{)} \\
ab + ba &= 0 \\
ab &= -ba \\
ab &= (-ba)^2 = (ba)^2 = ba \quad \text{(since } -ba = (-ba)^2\text{)} \\
\therefore ab &= ba
\end{aligned}$$

Therefore, given R is a Boolean ring, we see that R is commutative.

2. (DF 7.1.7)

The center of a ring R is

$$Z(R) := \{z \in R : zr = rz \text{ for all } r \in R\}.$$

(a) For a ring R, show that $Z(R) \subseteq R$ is a subring (in particular, containing 1).

(a) 1 is in $Z(R)$ since $1 \cdot r = r \cdot 1 = r$ for all $r \in R$.

(b) Since $Z(R) \subseteq R$, its elements inherit associativity and distributivity from R.

(c) **Closure:**

Given $a, b \in Z(R)$, then $a \cdot r = r \cdot a$ and $b \cdot r = r \cdot b$ for all $r \in R$. Then:

$$(a+b) \cdot r = ar + br = r \cdot (a+b) \implies a + b \in Z(R)$$

$$(a \cdot b) \cdot r = ar \cdot br = r \cdot (a \cdot b) \implies a \cdot b \in Z(R)$$

Therefore, $Z(R)$ contains the identity and is closed under both addition and multiplication, making it a subring.

(b) Show that the center of a division ring is a field.

(a) By definition, the elements of $Z(R)$ commute with all other elements of R.

(b) As shown above — the elements of $Z(R)$ form a subring.

(c) Given R is a *division* ring, then all elements in $Z(R)$ have multiplicative inverses since $Z(R) \subseteq R$.

(d) Given (b) and (c), then $Z(R)$ is a division ring.

(e) Given (a) and (d), then $Z(R)$ is a field.

3. (sorta DF 7.1.24) Let $D \in \mathbb{Z}$ be a nonsquare.

(a) Suppose that $D \equiv 1 \pmod 4$. Show that

$$R = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{a + b\frac{1+\sqrt{D}}{2} : a, b \in \mathbb{Z}\right\} \subset \mathbb{Q}(\sqrt{D})$$

is a subring of $\mathbb{Q}(\sqrt{D})$. What happens when $D \not\equiv 1 \pmod 4$?

> (a) We easily see that R contains both 0 (by setting $a = 0, b = 0$) and 1 (by setting $a = 1, b = 0$).
>
> (b) We also see that R is closed under addition and multiplication. To see this, suppose $a_1 + b_1\frac{1+\sqrt{D}}{2} \in R$ and $a_2 + b_2\frac{1+\sqrt{D}}{2} \in R$. Then, we have:
>
> $$a_1 + b_1\frac{1+\sqrt{D}}{2} \; + \; a_2 + b_2\frac{1+\sqrt{D}}{2} = (a_1 + a_2) + (b_1 + b_2)\frac{1+\sqrt{D}}{2} \in R$$
>
> $$a_1 + b_1\frac{1+\sqrt{D}}{2} \; \cdot \; a_2 + b_2\frac{1+\sqrt{D}}{2} = a_1a_2 + \frac{b_1b2D}{2} + (a_1b_2 + b_1a_2 + b_1b_2)\frac{1+\sqrt{D}}{2} \in R$$

(b) Let $\mathcal{O} = Z[\omega]$ where $\omega = \sqrt{D}$ or $(1+\sqrt{D})/2$, according as $D \equiv 2, 3 \pmod 4$ or $D \equiv 1 \pmod 4$. Show for $D = 3, 5, 6, 7$ that $\mathcal{O}^\times$ is infinite. *[Hint: see Example, §7.1, pages 229–230.]*

4.

(a) Let R be a commutative ring. Show that $R[x]$ is never a field (even if R is a field).

For $R[x]$ to be a field, it must be a division ring.

(a) Since negative powers are not defined in $R[x]$, any multiplication involving a polynomial of order n will yield a polynomial of order n or higher. When the coefficient from R is a unit (and, therefore, not nilpotent), then the coefficient of the term will never multiply out to 0 and each product will always have a nonzero power of x in it, making the polynomial non-invertible. For instance, take $p(x) = x + k$, then every product of $p(x)$ will contain a nonzero power of x *unless the other element in the product is zero* making $p(x) = x + k$ non-invertible.

(b) For a second example, consider all the polynomials with 0 as the constant term. Since 0 is never a unit in R because $0r = 0$ for all $r \in R$, then every product involving the polynomial will contain 0 as the constant term. This makes it impossible to yield 1, the identity in $R[x]$, and makes the polynomial non-invertible.

(b) How many polynomials of degree d are there in $(\mathbb{Z}/n\mathbb{Z})[x]$?

(a) There are n elements in $\mathbb{Z}/n\mathbb{Z}$.

(b) There are $d + 1$ terms in a polynomial of degree d.

(c) Each term up to the d-th term (the term with x^{d-1}) can take any of the n elements in $\mathbb{Z}/n\mathbb{Z}$ as a coefficient (since it can be zero), making n^d possible combinations for those terms.

(d) However, the leading term must have a nonzero coefficient, so it has $n - 1$ possible coefficients. This makes for a total of $n^d(n-1) = n^{d+1} - n^d$ polynomials of degree d.

(c) Show that $(\mathbb{Z}/8\mathbb{Z})[x]^\times > (\mathbb{Z}/8\mathbb{Z})^\times$, i.e., there is a unit which is not a scalar unit.

First, let's find the units in $\mathbb{Z}/8\mathbb{Z}$, which are the elements in $(\mathbb{Z}/8\mathbb{Z})^\times$:

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$$

Through closer inspection, we see that each element is its own inverse, that is $1^2 = 1$, $3^2 = 9 \equiv 1$, $5^2 = 25 \equiv 1$, and $7^2 = 49 \equiv 1$.

Next, let's analyze the units in $(\mathbb{Z}/8\mathbb{Z})[x]$. Suppose $p(x) = \sum C_i x^i \,:\, i \in Z_{\geq 0}$ is a unit in $(\mathbb{Z}/8\mathbb{Z})[x]$. Since $p(x)$ being a unit implies that $p(x) \cdot q(x) = 1$ for some $q(x) \in (\mathbb{Z}/8\mathbb{Z})[x]$, then all the coefficients C_i of the non-constant terms $C_i x^i,\ i \in Z^+\ p(x)$ must either be 0 or nilpotent.

(a) The first case yields all the units in $\mathbb{Z}/8\mathbb{Z}$ as units in $(\mathbb{Z}/8\mathbb{Z})[x]$.

(b) The second case yields polynomials with only 2, 4, or 6 (the nilpotent elements of $\mathbb{Z}/8\mathbb{Z}$) as coefficients of the non-constant terms. For instance, take $p(x) = 2x + 1$. Then,

$$p(x)^4 = 16x^4 + 32x^3 + 24x^2 + 8x + 1 \equiv 1 \pmod 8$$

In this case, $2x + 1$ is a unit with

$$(2x+1)^3 = 8x^3 + 12x^2 + 6x + 1 \equiv 12x^2 + 6x + 1 \pmod 8$$

as its inverse.

Thus, there are more units in $(\mathbb{Z}/8\mathbb{Z})[x]$ than in $\mathbb{Z}/8\mathbb{Z}$, particularly the non-scalar units such as $2x + 1$. Since $(\mathbb{Z}/8\mathbb{Z})[x]^\times$ consists of the units in $(\mathbb{Z}/8\mathbb{Z})[x]$ while $(\mathbb{Z}/8\mathbb{Z})^\times$ consists of the units in $\mathbb{Z}/8\mathbb{Z}$, it follows that $(\mathbb{Z}/8\mathbb{Z})[x]^\times$ contains $(\mathbb{Z}/8\mathbb{Z})^\times$ *and other elements*.

5. (DF 7.2.6–7.2.7)

Let R be a commutative ring and let $n \in \mathbb{Z}_{\geq 1}$. Let $A = (a_{ij})_{i,j} \in \mathrm{M}_n(R)$ be an $n \times n$-matrix whose (i, j)-entry is $a_{ij} \in R$. Let $E_{ij} \in \mathrm{M}_n(R)$ be the matrix whose (i, j) entry is 1 with all other entries zero. For example,

$$E_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathrm{M}_3(R)$$

(a) Prove that $E_{ij}A$ is the $n \times n$-matrix whose ith row is equal to the jth row of A, with all other rows zero:

$$E_{ij}A = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \\ a_{j1} & \cdots & a_{jn} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

(in the ith row)

Let's consider two matrices $X, Y \in \mathrm{M}_n(R)$ and their product XY.
By definition of matrix multiplication, $XY_{ij} = \sum_{k=1}^{n} X_{ik}Y_{kj}$. Setting $X = E_{ij}$ and $Y = A$, let's consider arbitrary indices i', j' in the matrix $E_{ij}A$:

$$(E_{ij}A)_{i'j'} = \sum_{k=1}^{n} (E_{ij})_{i'k} A_{kj'}$$

When $i' \neq i$, then the index in $E_{ij}A$ has a 0, since E_{ij} has all zeroes in every row except the i-th row. When $i' = i$, then the row i' in E_{ij} has a 1 in the j-th column, and the corresponding row in $E_{ij}A$ is $1\times$ the j-th row of A.

(b) Prove that AE_{ij} is the $n \times n$-matrix whose jth column equals the ith column of A, with all other columns zero:

$$AE_{ij} = \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix}$$

(in the jth column)

Let's consider two matrices $X, Y \in \mathrm{M}_n(R)$ and their product XY.

By definition of matrix multiplication, $XY_{ij} = \sum_{k=1}^{n} X_{ik}Y_{kj}$. Setting $X = A$ and $Y = E_{ij}$, let's consider arbitrary indices i', j' in the matrix AE_{ij}:

$$(AE_{ij})_{i'j'} = \sum_{k=1}^{n} A_{ik}(E_{ij})_{kj'}$$

When $j' \neq j$, then the index in AE_{ij} has a 0, since E_{ij} has all zeroes in every column except the j-th column.

When $j' = j$, then the column j' in E_{ij} has a 1 in the i-th row, and the corresponding column in AE_{ij} is $1\times$ the i-th column of A.

(c) Prove that $E_{pq}AE_{rs}$ is the matrix whose (p, s)-entry is a_{qr}, with all other entries zero.

Following the demonstration in the previous two parts, let's consider arbitrary indices i', j' in the matrix $E_{pq}AE_{rs}$ after the multiplication in part (a) is followed by the multiplication in part (b): When $i' \neq p$ or $j' \neq s$, then the index in $E_{pq}AE_{rs}$ has a 0, since either E_{pq} has all zeroes in that row (when $i' \neq p$) or E_{rs} has all zeroes in that column (when $j' \neq s$).

When $i' = p$ and $j' = s$, then:

(a) The row $i' = p$ in E_{pq} has a 1 in the q-th column, therefore the corresponding row in $E_{pq}A$ is the q-th row of A.

(b) The column $j' = s$ in E_{rs} has a 1 in the r-th row, therefore the corresponding column in AE_{rs} is the r-th column of $E_{pq}A$.

(c) After the two operations, only the intersection of the p-th row and the s-th row will retain an entry from A. Particularly, the p-th row of the product will equal the q-th column of A as shown in (a), and the s-th column of the product will equal the r-th column of $E_{pq}A$. Consequently, the intersection of the row and column will contain the element initially at position (q, r) in A.

(d) Prove that the center of $\mathrm{M}_n(R)$ is the set (subring!) of scalar matrices (i.e., diagonal matrices with the same entry down the diagonal).

[Hint: if you get lost in the indices, do the cases $n = 2$ and maybe $n = 3$ first.]

By definition, the center of a ring must commute with all other elements in the ring.

For a simpler case, let's consider $M_3(R)$, with

$X = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in Z(\mathrm{M}_3(R))$ and $Y = \begin{pmatrix} j & k & l \\ m & n & o \\ p & q & r \end{pmatrix} \in \mathrm{M}_3(R)$. We must have that $XY = YX$.

$$XY = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \times \begin{pmatrix} j & k & l \\ m & n & o \\ p & q & r \end{pmatrix} = \begin{pmatrix} aj + bm + cp & ak + bn + cq & al + bo + cr \\ dj + em + fp & dk + en + fq & dl + eo + fr \\ gj + hm + ip & gk + hn + iq & gl + ho + ir \end{pmatrix}$$

$$YX = \begin{pmatrix} j & k & l \\ m & n & o \\ p & q & r \end{pmatrix} \times \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} ja + kd + lg & jb + ke + lh & jc + kf + li \\ ma + nd + og & mb + ne + oh & mc + nf + oi \\ pa + qd + rg & pb + qe + rh & pc + qf + ri \end{pmatrix}$$

Comparing the two matrices, we see that the elements have different constituent terms, therefore

$XY \neq YX$ in general unless $X = Y$.

However, the terms at positions $(1, 1)$, $(2, 2)$, and $(3, 3)$ share a component in each matrix. Particularly;

$XY_{11} = aj + bm + cp$ and $YX_{11} = aj + kd + lg$.

$XY_{22} = dk + en + fq$ and $YX_{22} = mb + en + oh$.

$XY_{33} = gl + ho + ir$ and $YX_{33} = pc + qf + ri$.

The common terms are those occurring yielded from the diagonal elements. One way to make $XY = YX$ is to set X and Y such that the diagonal elements are nonzero and all other terms are 0.

$$X = \begin{pmatrix} a & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & i \end{pmatrix}, \quad Y = \begin{pmatrix} d & 0 & 0 \\ 0 & n & 0 \\ 0 & 0 & r \end{pmatrix}$$

$$XY = \begin{pmatrix} ad & 0 & 0 \\ 0 & en & 0 \\ 0 & 0 & ir \end{pmatrix}$$

$$YX = \begin{pmatrix} ad & 0 & 0 \\ 0 & en & 0 \\ 0 & 0 & ir \end{pmatrix}$$

However, in the case of the center, we need to have no restrictions on the second matrix. Thus, consider the less restricted case when $X = \begin{pmatrix} a & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & i \end{pmatrix}$ and $Y = \begin{pmatrix} j & k & l \\ m & n & o \\ p & q & r \end{pmatrix}$. We see that:

$$XY = \begin{pmatrix} aj & ak & al \\ em & en & eo \\ ip & iq & ir \end{pmatrix}$$

$$YX = \begin{pmatrix} aj & ek & il \\ am & en & io \\ ap & eq & ir \end{pmatrix}$$

Other than the diagonal entries, the product matrices have entirely different elements! However, we see that each pair of positions for indices (i, j) in X and Y involves the same element from Y and only the elements from X change.

For instance; $XY_{12} = ak$ and $YX_{12} = ek$.

$XY_{13} = al$ and $YX_{13} = il$.

$XY_{21} = em$ and $YX_{21} = am$.

$XY_{23} = eo$ and $YX_{23} = io$.

$XY_{31} = ip$ and $YX_{31} = ap$.

$XY_{32} = iq$ and $YX_{32} = eq$.

Therefore, setting $a = e = i$ and setting every other entry equal to 0 in X makes $XY = YX$ for any unrestricted matrix $Y \in \mathrm{M}_3(R)$.