Math 71: Abstract Algebra

Prishita Dharampal

Credit Statement: Talked to Sair Shaikh'26, Henry Dorr'28 and Math Stack Exchange.

Problem 1. Let x be a nilpotent element of the commutative ring R (cf. the preceding exercise).

1. Prove that x is either zero or a zero divisor.
2. Prove that rx is nilpotent for all $r \in R$.
3. Prove that $1 + x$ is a unit in R.
4. Deduce that the sum of a nilpotent element and a unit is a unit.

Solution.

1. Let n be the smallest positive integer such that $x^n = 0$.
   $x \in R$, $x^k = 0$, trivially holds for $x = 0$. If $x \neq 0$, $x^n = 0 \implies x \cdot x^{n-1} = 0$, where $x^{n-1} \neq 0$ (because, by definition, n is the smallest positive integer such that $x^n = 0$). Hence, x is either zero or a zero divisor.

2. Let n be the smallest positive integer such that $x^n = 0$ and r be an arbitrary element in R. Then,

$$\begin{aligned}(rx)^n &= r^n x^n \text{ (R is commutative)} \\ &= r^n \cdot 0 \\ &= 0\end{aligned}$$

   Hence, $\exists n : (rx)^n = 0 \implies rx$ is nilpotent for all $r \in R$.

3. Let n be the smallest positive integer such that $x^n = 0$. Then we can construct $y \in R : y = (1 + \sum_{j=1}^{n-1} ix^j)$, where $i = \begin{cases} +1, \, j = 0 \pmod 2 \\ -1, \, j = 1 \pmod 2 \end{cases}$

Then,

$$\begin{aligned}(1+x)y &= (1+x)(1+\sum_{j=1}^{n-1} ix^j) \\ &= 1 + x + \sum_{j=1}^{n-1} ix^j + x\sum_{j=1}^{n-1} ix^j \\ &= 1 + x^n \\ &= 1\end{aligned}$$

Hence, $(1+x)$ is a unit in R.

4. Let $a \in R$ be a unit, such that $aa^{-1} = 1$, and $x \in R$ be a nilpotent element such that $x^n = 0$. Then like in subpart (3), we can construct $p, p^{-1} \in R : p = (a+x)$, and $p^{-1} = (a' + \sum_{j=1}^{n-1} ix^j)$ where $i = \begin{cases} +1,\ j = 0 \pmod 2 \\ -1,\ j = 1 \pmod 2 \end{cases}$

   Then,

$$\begin{aligned}pp^{-1} &= (a+x)(a' + \sum_{j=1}^{n-1} i(a')^j x^j) \\ &= aa' + a'x + a\sum_{j=1}^{n-1} i(a')^j x^j + x\sum_{j=1}^{n-1} i(a')^j x^j \\ &= aa' \\ &= 1\end{aligned}$$

   Hence, $(a+x)$ is a unit in R.

Problem 2. Let X be any nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X (the power set of X). Define addition and multiplication on $\mathcal{P}(X)$ by

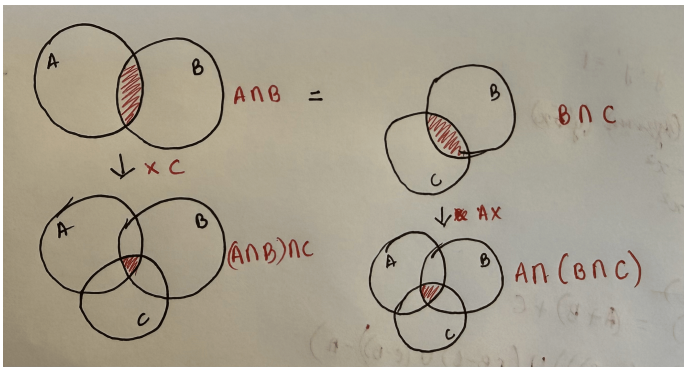
$$A + B = (A - B) \cup (B - A) \qquad \text{and} \qquad A \times B = A \cap B$$

i.e., addition is symmetric difference and multiplication is intersection.

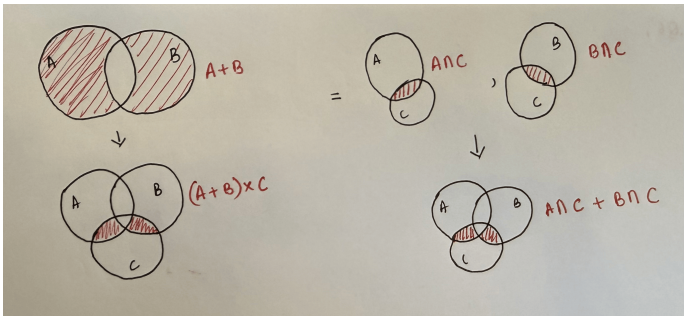
1. Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as rings of sets).
2. Prove that this ring is commutative, has an identity and is a Boolean ring.

Solution.

1. To prove that $\mathcal{P}(X)$ is a ring we need to check the following:
   (a) $(\mathcal{P}(X), +)$ is an abelian group:
      i. Identity is $\varnothing$:
      $$A + \varnothing = (A - \varnothing) \cup (\varnothing - A) = A \cup \varnothing = A$$
      ii. Addition is closed and commutative, and inverses exist:
      $A - B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B - A$ (union is commutative)
      iii. Associativity:
      $x \in A + (B + C) \iff x \in A, B, C$ and $x \in (A + B) + C \iff x \in A, B, C$, i.e $A + (B + C) = (A + B) + C$.
   (b) Multiplication is associative:



   (c) Distributive law holds:

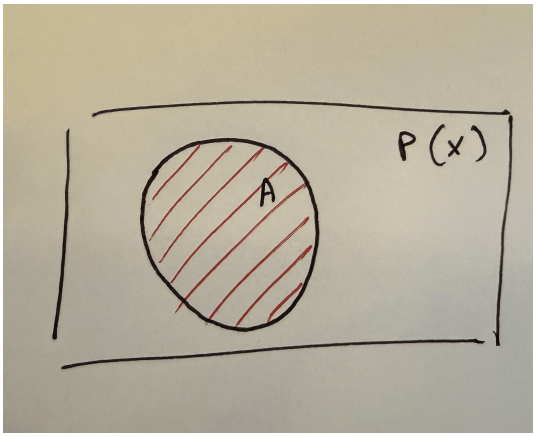


Hence, $\mathcal{P}(X)$ is a ring.

2. (a) The ring is commutative:
   $x \in A \times B \iff x \in A, B$ and $x \in B \times A \iff x \in A, B$, i.e $A \times B = B \times A$.

   (b) The ring has an identity:

$$\mathcal{P}(X) \times A = A = A \times \mathcal{P}(X)$$



   (c) The ring is a Boolean ring:

$$A \times A = A \cap A = A \qquad \forall A \in \mathcal{P}(X)$$

Problem 3. Let I be the ring of integral Hamilton Quaternions and define:

$$N : I \to Z \quad \text{by } N(a+bi+ck+dk) = a^2+b^2+c^2+d^2$$

1. Prove that $N(\alpha) = \alpha\overline{\alpha}$ for all $\alpha \in I$, where if $\alpha = a+bi+cj+dk$, then $\overline{\alpha} = a-bi-cj-dk$.
2. Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in I$.
3. Prove that an element of I is a unit if and only if it has norm $+1$. Show that $I^\times$ is isomorphic to the quaternion group of order 8. [The inverse in the ring of rational quaternions of a nonzero element α is $\frac{\overline{\alpha}}{N(\alpha)}$].

Solution.

1. $N(\alpha) = \alpha\overline{\alpha}$

$$\begin{aligned}
\alpha\overline{\alpha} =& (a+bi+cj+dk)(a-bi-cj-dk)\\
=& a^2 - b^2i^2 - c^2j^2 - d^2k^2 + (abi-abi) + (acj-acj) + (adk-adk)\\
&+ (-bcij - cbji) + (-bdik - dbki) + (-cdjk - dckj)\\
=& a^2 - b^2i^2 - c^2j^2 - d^2k^2 + (-bcij+cbij) + (-bdik+dbik) + (-cdjk+dcjk)\\
=& a^2 - b^2(-1) - c^2(-1) - d^2(-1)\\
=& a^2 + b^2i^2 + c^2j^2 + d^2k^2
\end{aligned}$$

2. To show that $N(\alpha\beta) = N(\alpha)N(\beta)$, we know that $\overline{(xy)} = \overline{y}\,\overline{x}$

$$\begin{aligned}
N(\alpha\beta) &= (\alpha\beta)(\overline{\alpha\beta})\\
&= \alpha(\beta\overline{\beta})\overline{\alpha}\\
&= \alpha(N(\beta))\overline{\alpha} \qquad (N(\beta) \in \mathbb{Z}, \text{ and multiplication by } \mathbb{Z} \text{ is commutative in } \mathbb{H}).\\
&= \alpha\overline{\alpha}N(\beta)\\
&= N(\alpha)N(\beta)
\end{aligned}$$

3. Let $\mathbb{H}$ be the ring of integral Hamilton Quaternions. To prove $x \in I^\times \iff N(x) = +1$
   ($\implies$) Assume $x \in I^\times$
   If $x \in I^\times \implies \exists\, x' : xx' = 1$. Taking norm on both sides,

$$N(xx') = N(1) \implies N(x)N(x') = 1 \implies N(x) = 1/N(x')$$

   But $N(x), N(x') \in \mathbb{Z}^+$, hence both $N(x), N(x')$ must be 1.

($\Longleftarrow$) Assume $N(x) = +1$
If $N(x) = 1$ then $\exists\, \overline{x} \in \mathbb{H} : x\overline{x} = 1$, i.e. $x, \overline{x}$ are both units.
Let coefficients of x be represented as (a, b, c, d). If $x \in I^{\times}$ then one of four cases is true:

(a) $(1,0,0,0) \implies a = \pm 1 \implies x = \pm 1 + 0i + 0j + 0k = \pm 1$

(b) $(0,1,0,0) \implies b = \pm 1 \implies x = 0 + \pm 1i + 0j + 0k = \pm i$

(c) $(0,0,1,0) \implies c = \pm 1 \implies x = 0 + 0i + \pm 1j + 0k = \pm j$

(d) $(0,1,0,1) \implies d = \pm 1 \implies x = 0 + 0i + 0j + \pm 1k = \pm k$

Hence, $I^{\times}$ has 8 elements, that are exactly the same as elements in the quaternion group of order 8. Then, if we define a homomorphism $\varphi : Q_8 \to I^{\times}$ that takes every element in Q_8 to it's corresponding element in $I^{\times}$. Then we can check if the relations in Q_8 hold in $I^{\times}$.

(a) $|-1| = 2$ holds.

(b) $i^2 = j^2 = k^2$ holds.

(c) $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$ holds.

(d) $|\pm i| = |\pm j| = |\pm k| = 4$ holds.

Hence, φ is an isomorphism from $I^{\times}$ to Q_8.

Problem 4. Let $A = \mathbb{Z} \times \mathbb{Z} \times \cdots$ be the direct product of copies of $\mathbb{Z}$ indexed by the positive integers (so A is a ring under component-wise addition and multiplication) and let R be the ring of all group homomorphism from A to itself as described in the preceding exercise. Let ϕ be the element of R defined by $\phi(a_1, a_2, a_3, \cdots) = (a_2, a_3, \cdots)$. Let ψ be the element of R defined by $\psi(a_1, a_2, a_3, \cdots) = (0, a_1, a_2, a_3, \cdots)$.

1. Prove that $\phi\psi$ is the identity of R but $\psi\phi$ is not the identity of R (i.e. ψ is the right inverse for ϕ but not a left inverse).
2. Exhibit infinitely many right inverses for ϕ.
3. Find a nonzero element π in R such that $\phi\pi = 0$ but $\pi\phi \neq 0$.
4. Prove that there is no nonzero element $\lambda \in R$ such that $\lambda\phi = 0$ (i.e., ϕ is a left zero divisor but not a right zero divisor.

Solution.

1. Let $\tau \in R, a \in A$, $a = (a_1, a_2, a_3, \cdots)$, then by definition

$$\phi\psi(a) = \phi\psi(a_1, a_2, a_3, \cdots) = \phi(0, a_1, a_2, a_3, \cdots) = (a_1, a_2, a_3, \cdots) = a$$

Hence, $\phi\psi$ is the identity endomorphism on A, which is also the identity of R. We can check that as follows:

$$\tau\phi\psi(a) = \tau\phi\psi(a_1, a_2, a_3, \cdots) = \tau\phi(0, a_1, a_2, a_3, \cdots) = \tau(a_1, a_2, a_3, \cdots) = \tau(a)$$

And if $\tau(a) = (a_i, a_j, a_k, \cdots)$ for some values of i, j, k,

$$\phi\psi\tau(a) = \phi\psi\tau(a_1, a_2, a_3, \cdots) = \phi(0, a_i, a_j, a_k, \cdots) = (a_i, a_j, a_k, \cdots) = \tau(a)$$

Hence, $\phi\psi$ is the identity for τ. But because τ was an arbitrary element in R, $\phi\psi$ is the identity $\forall\tau \in R$.

However, $\psi\phi(a) \neq a$.

$$\psi\phi(a) = \psi\phi(a_1, a_2, a_3, \cdots) = \psi(a_2, a_3, \cdots) = (0, a_2, a_3, \cdots)$$

Here, we lose the first element of the tuple entirely, i.e isn't the identity endomorphism on A, and hence is not the identity of R.

2. Since ϕ loses the first element of the tuple. So all $\bar{\psi}$ such that $\bar{\psi}(a) = (n, a_1, a_2, a_3, \cdots), \forall n \in \mathbb{Z}$ work as right inverses for ϕ.

$$\phi\bar{\psi}(a) = \phi\bar{\psi}(a_1, a_2, a_3, \cdots) = \phi(n, a_1, a_2, a_3, \cdots) = (a_1, a_2, a_3, \cdots) = a$$

Since there are infinitely many integers, there are infinitely many $\bar{\psi}$ are right inverses for ϕ.

3. Define $\pi(a) = (a_1, 0, 0, \cdots)$. Then,

$$\phi\pi(a) = \phi\pi(a_1, a_2, a_3, \cdots) = \phi(a_1, 0, 0, \cdots) = (0, 0, \cdots) = 0$$

$\phi\pi$ is the zero function in R. However,

$$\pi\phi(a) = \pi\phi(a_1, a_2, a_3, \cdots) = \pi(a_2, a_3, \cdots) = (a_2, 0, \cdots)$$

Hence, $\phi\pi = 0$, but $\pi\phi \neq 0$.

4. Assume that there exists $\lambda \in R : \lambda\phi = 0$. Then,

$$\lambda\phi(a) = \lambda\phi(a_1, a_2, a_3, \cdots) = \lambda(a_2, a_3, \cdots) = (0, 0, \cdots) = 0$$

But $a_i \in \mathbb{Z}, \forall i$, and there are neither nilpotent elements nor zero divisors in $\mathbb{Z}$. Hence if $a_i \cdot x = 0 \implies x = 0$ or $a_i = 0$. Which implies that λ is the zero-map, which goes against our assumption that $\lambda \neq 0$. Hence, there exist no non-zero elements such that $\lambda\phi = 0$.

Problem 5. R is a commutative ring with 1. Define the set $R[[x]]$ of formal power series in the indeterminate x with coefficients from R to be all formal infinite sums:

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots$$

Define addition and multiplication of power series in the same way as for power series with real or complex coefficients i.e., extend polynomial addition and multiplication to power series as though they were "polynomials of infinite degree":

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n$$

Here, formal implies convergence is not considered.

1. Prove that $R[[x]]$ is a commutative ring with 1.
2. Show that $1 - x$ is a unit in $R[[x]]$ with inverse $1 + x + x^2 + \cdots$.
3. Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

Solution.

1. To prove that $R[[x]]$ is a commutative ring with 1, we need to prove the following:
   (a) Additive identity exists:
   Define $k \in R[[x]] : k = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots$, such that $a_n = 0, \forall n$, then $k = 0 \implies k + x = x + k = x, \forall x \in R[[x]]$.
   (b) Closure under inverses and addition:

$$\sum_{n=0}^{\infty} a_n x^n - \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n - b_n) x^n$$

   We need to show that $(a_n - b_n)x^n \in R[[x]], \forall a_n, b_n \implies a_n - b_n \in R$ ($x^n \in R[[x]], \forall n$ by definition of a formal sum). But that is true by definition of a ring: the commutative ring R is closed under addition and inverses,
   (c) Addition is commutative:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n, \qquad \sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} (b_n + a_n) x^n$$

We need to show that $a_n + b_n = b_n + a_n, \forall n$. But, $a_n, b_n \in R$, and addition is commutative in R (by definition of a ring).

(d) Additive associativity holds:
We need to show that:

$$\sum_{n=0}^{\infty} a_n x^n + \left(\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n \right) = \left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n \right) + \sum_{n=0}^{\infty} c_n x^n$$

First,

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n + \left(\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n \right) &= \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} (b_n + c_n) x^n \\ &= \sum_{n=0}^{\infty} (a_n + (b_n + c_n)) x^n \end{aligned}$$

And,

$$\begin{aligned} \left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n \right) + \sum_{n=0}^{\infty} c_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n + \sum_{n=0}^{\infty} c_n x^n \\ &= \sum_{n=0}^{\infty} ((a_n + b_n) + c_n) x^n \end{aligned}$$

So we basically need to show that $(a_n + (b_n + c_n)) = ((a_n + b_n) + c_n)$, which is trivially true because $a_n, b_n, c_n \in$ Ring R.
Hence, $(R[[x]], +)$ is an abelian group.

(e) Multiplicative identity exists:
Define $k \in R[[x]] : k = 1 + \sum_{n=1}^{\infty} a_n x^n = 1 + a_1 x + a_2 x^2 + \cdots$, such that $a_n = 0, \forall n$, then $k = 1 \implies k \cdot x = x \cdot k = x, \forall x \in R[[x]]$.

(f) Multiplication is commutative:

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n \qquad \sum_{n=0}^{\infty} b_n x^n \times \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} b_k a_{n-k} \right) x^n$$

We need to show that

$$\sum_{k=0}^{n} b_k a_{n-k} = \sum_{k=0}^{n} a_k b_{n-k}$$

Let $k' = n - k$, then we can re-write $\sum_{k=0}^{n} a_k b_{n-k}$ as $\sum_{k'=0}^{n} a_{n-k'} b_{k'}$ But we know that $xy = yx, \forall x, y \in R$, and what we call the summation variable is completely arbitrary and does not affect the sum.

$$\implies \sum_{k=0}^{n} b_k a_{n-k} = \sum_{k'=0}^{n} a_{n-k'} b_{k'}$$

Hence, we can say that multiplication is commutative in $R[[x]]$.

(g) Distributive law holds:

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n \times \left(\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n \right) &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k (b_{n-k} + c_{n-k}) \right) x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} + a_k c_{n-k} \right) x^n \\
&\text{(distributive law holds in } R\text{)} \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n + \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k c_{n-k} \right) x^n \\
&= \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} c_n x^n
\end{aligned}$$

(h) Multiplicative associativity holds: We need to show that:

$$\sum_{n=0}^{\infty} a_n x^n \times \left(\sum_{n=0}^{\infty} b_n x^n \times \sum_{n=0}^{\infty} c_n x^n \right) = \left(\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n \right) \times \sum_{n=0}^{\infty} c_n x^n$$

First,

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n x^n \times \left(\sum_{n=0}^{\infty} b_n x^n \times \sum_{n=0}^{\infty} c_n x^n \right) &= \sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} b_k c_{n-k} \right) x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} a_j \sum_{k=0}^{n-j} b_k c_{n-j-k} \right) x^n \\
&= \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} \sum_{k=0}^{n-j} a_j b_k c_{n-j-k} \right) x^n
\end{aligned}$$

And,

$$\left(\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n\right) \times \sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n \times \sum_{n=0}^{\infty} c_n x^n$$
$$= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n-j} b_k c_{n-j-k} \sum_{m=0}^{n} a_j\right) x^n$$
$$= \sum_{n=0}^{\infty} \left(\sum_{m=0}^{n} \sum_{k=0}^{n-j} b_k c_{n-j-k} a_j\right) x^n$$

So we basically need to show that $(a_j b_k c_{n-j-k}) = (b_k c_{n-j-k} a_j)$, which is trivially true because the coefficients are in the Ring R.

Hence, $R[[x]]$ is a commutative ring with 1.

2.

$$(1-x)\sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} x^n - x\sum_{n=0}^{\infty} x^n$$
$$= \sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} x \cdot x^n$$
$$= \sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} x^{n+1}$$
$$= \sum_{n=0}^{\infty} x^n - \sum_{m=1}^{\infty} x^m \text{ (m = n +1)}$$
$$= 1 + \sum_{n=1}^{\infty} x^n - \sum_{m=1}^{\infty} x^m$$
$$= 1$$

$\implies (1-x)$ is a unit.

3. ($\implies$)
The formal power series does not have negative powers, inverses of powers of x do not exist in $R[[x]]$. Hence the only term that can be the unit must be x free, i.e., a_0. (We can isolate a_0 from $\sum_{n=0}^{\infty} a_n x^n$ similar to the subpart (2)).

If a_0 is a unit in $R[[x]]$, then $\exists\, b_0 \in R[[x]]$ such that $a_0 b_0 = 1$. But both a_0, b_0 are coefficients, i.e $a_0, b_0 \in R \implies a_0, b_0$ are units in R.

($\impliedby$)
If a_0 is a unit in R, then $\exists\, b_0 \in R$ such that $a_0 b_0 = 1$. Then we can construct

$a = \sum_{n=0}^{\infty} a_n x^n, b = \sum_{n=0}^{\infty} b_n x^n$, such that $a_i = b_i = 0, 1 \leq i \leq n \implies a = a_0, b = b_0 \implies ab = 1, ab \in R[[x]]$.

Hence, $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

Problem 6. Let S be a ring with identity $1 \neq 0$. Let $n \in \mathbb{Z}^+$ and let A be an $n \times n$ matrix with entries from S whose i, j entry is a_{ij}. Let E_{ij} be the element of $M_n(S)$ whose i, j entry is 1 and whose other entries are all 0.

1. Prove that $E_{ij}A$ is the matrix whose i-th row equals the jth row of A and all other rows are zero.
2. Prove that AE_{ij} is the matrix whose i-th column equals the jth column of A and all other columns are zero.
3. Deduce that $E_{pq}AE_{rs}$ is the matrix whose p, s entry is a_{qr} and all other entries are zero.

Solution.

1. The i, j-th entry of the resulting matrix $P = E_{ij}A$ looks like:

$$p_{xy} = \sum_{z=1}^{n} e_{xz} a_{zy}$$

where p_{xy}, e_{xz}, a_{zy} are respectively the x, y-th, x, z-th, z, y-th entries of P, E_{ij}, and A. Then there are 3 cases:

(a) $x \neq i \implies e_{xz} = 0 \implies p_{xy} = 0$.

(b) $x = i, z \neq j \implies e_{xz} = 0 \implies p_{xy} = 0$.

(c) $x = i, z = j \implies e_{xz} = 1, a_{zy} = a_{jy} \implies p_{xy} = 1 \cdot a_{jy} = a_{jy}$.

Hence, for all $1 \leq x, y, z \leq n$, $p_{xy} \neq 0$ only when $x = i, z = j$, and then $p_{iy} = a_{jy}$. I.e $P = E_{ij}A$ is the matrix whose i-th row equals the jth row of A and all other rows are zero.

2. The i, j-th entry of the resulting matrix $P = AE_{ij}$ looks like:

$$p_{xy} = \sum_{z=1}^{n} a_{xz} e_{zy}$$

where p_{xy}, a_{xz}, e_{zy} are respectively the x, y-th, x, z-th, z, y-th entries of P, A, and E_{ij}. Then there are 3 cases:

(a) $z \neq i \implies e_{zy} = 0 \implies p_{xy} = 0$.

(b) $z = i, y \neq j \implies e_{zy} = 0 \implies p_{xy} = 0$.

(c) $z = i, y = j \implies e_{zy} = 1, a_{xz} = a_{xj} \implies p_{xy} = a_{xj} \cdot 1 = a_{xj}$.

Hence, for all $1 \leq x, y, z \leq n$, $p_{xy} \neq 0$ only when $z = i, y = j$, and then $p_{xj} = a_{xi}$. I.e $P = E_{ij}A$ is the matrix whose j-th column equals the i-th column of A and all other columns are zero.

3. $E_{pq}AE_{rs} = (E_{pq}A)E_{rs}$. From (1) we know that $E_{pq}A$ is a matrix, whose p-th row equals the q-th row of A and all other rows are zero. Then $(E_{pq}A)E_{rs}$ looks like:

$$((e_{pq}a)e_{rs})_{xy} = \sum_{z=1}^{n} (e_{pq}a)_{xz}e_{zy}$$

where $((e_{pq}a)e_{rs})_{xy}, (e_{pq}a)_{xz}, e_{zy}$ are respectively the x, y-th, x, z-th, z, y-th entries of $(E_{pq}A)E_{rs}, (E_{pq}A)$, and E_{rs}. Then there are 3 cases:

   (a) $x \neq p \implies (e_{pq}a)_{xz} = 0 \implies ((e_{pq}a)e_{rs})_{xy} = 0.$

   (b) $x = p, z \neq r, y \neq s \implies e_{zy} = 0 \implies ((e_{pq}a)e_{rs})_{xy} = 0.$

   (c) $x = p, z = r, y = s \implies e_{zy} = 1, (e_{pq}a)_{xz} = a_{qr} \implies ((e_{pq}a)e_{rs})_{xy} = (e_{pq}a)_{xz} \cdot 1 = a_{qr} \cdot 1 = a_{qr}.$

   Hence, $((e_{pq}a)e_{rs})_{xy} \neq 0$ only when $x = p, y = s$, and $((e_{pq}a)e_{rs})_{ps} = a_{qr}$.

Problem 7. Prove that the center of the ring $M_n(R)$ is the set of scalar matrices. [Use the preceding exercise.]

Solution.

The center of the ring $M_n(R)$ are all elements in $M_n(R)$ that commute with everything in the ring.

$(\implies)$
If a matrix $K \in \mathcal{Z}(M_n(R))$, then $\forall E_{ij} \in M_n(R)$, $E_{pq}KE_{rs} = E_{pq}E_{rs}K$, where p, q, r, s are arbitrary indices between 1 and n.

1. From part (3) of Problem 6, we know that $E_{pq}KE_{rs} = k_{qr}E_{ps}$. I.e the p, s-th entry of the resulting matrix is equal to the q, r-th entry of K and all other entries are zero.

2. $E_{pq}E_{rs} = E_{ps} \iff q = r$, else E_{ps} is the zero matrix. Hence, $q \neq r \implies E_{ps} = 0 \implies k_{qr}E_{ps} = 0$. So $q = r$ for all q, r. Hence, K is a diagonal matrix.

3. $k_{qq}E_{ps} = E_{ps}k_{qq} \neq 0 \implies p = s$. Then $k_{qq}E_{pp} = KE_{pp}$ (from 1) and $KE_{pp} = E_{pp}KE_{pp} = k_{pp}E_{pp} \implies k_{qq} = k_{pp}$. Since p, q were arbitrary, all diagonal entries of K are equal. Hence, K is a scalar matrix.

$(\impliedby)$
A scalar matrix K can be represented as $K = kI$, where I is the $n \times n$ identity matrix, and $k \in R$. Then $\forall A \in M_n(R)$, we know the following,

$$AK = AkI = (Ak)I = Ak \qquad KA = kIA = k(IA) = kA$$

So, we need to show that $Ak = kA$, but Ak is defined as multiplying the $ij-$th entry of A by k. I.e, if $C = Ak$, $c_{ij} = a_{ij} \cdot k$. Similarly, if $D = kA$, $d_{ij} = k \cdot a_{ij}$. Then $C = D \iff c_{ij} = d_{ij}$, for all $i, j : 1 \leq i, j \leq n$.

$$\begin{aligned} c_{ij} &= a_{ij} \cdot k \\ &= k \cdot a_{ij} \ (a_{ij}, k \in R, R \text{ is a commutative ring}) \\ &= d_{ij} \end{aligned}$$

Hence, the set of scalar matrices is in the center of the ring $M_n(R)$.

Problem 8. Let $G = \{g_1, \cdots, g_n\}$ be a finite group. Prove that the element $N = g_1 + g_2 + \cdots + g_n$ is in the center of the group ring RG.

Solution.

Multiplication in RG is defined as $(r_i g_i)(r_j g_j) = (r_i r_j)(g_i g_j)$. For all terms in N, the coefficient in R is 1, and 1 by definition commutes with everything. So we only need to prove about multiplication between N and elements in group G is commutative. G is a finite group, i.e., it is closed under multiplication.

$$gG = G, \forall g \in G$$

That is, g just permutes the order of addition of elements in N, and that doesn't change the sum because $(RG, +)$ is abelian. Similarly, under right multiplication:

$$Gg = G, \forall g \in G$$

Again, this just permutes the order of the terms being added and doesn't change the sum. Thus, $gG = Gg = G$. I.e. multiplication between N and elements in group G is commutative. Hence $N \in \mathcal{Z}(RG)$.

Problem 9. Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\phi : R \to S$ be a nonzero homomorphism of rings.

1. Prove that if $\phi(1_R) \neq 1_S$ then $\phi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

2. Prove that if $\phi(1_R) = 1_S$ then $\phi(u)$ is a unit in S and that $\phi(u^{-1}) = \phi(u)^{-1}$ for each unit u of R.

Solution.

1. If $\phi(1_R) \neq 1_S$, then $\phi(1_R)$ is either 0, or $a \in S$, $a \neq 0, a \neq 1_S$.

   (a) If $\phi(1_R) = 0$, then for some $x \in R$, $\phi(x) = \phi(x \cdot 1_R) = \phi(x)\phi(1_R) = \phi(x) \cdot 0 = 0$. Since, x was an arbitrary element in R, this would mean that ϕ is the zero map. But since ϕ is a non-zero homomorphism, this is not possible.

   (b) If $\phi(1_R) = a$, where a is a non-zero, non-identity element in S, then $(1_S - a) \neq 0$.

   $$a(1_S - a) = a - a^2$$

   But,

   $$\phi(1_R)^2 = \phi(1_R^2) = \phi(1_R)$$

   i.e. $\phi(1_R)$ is idempotent $\implies a - a^2 = a - a = 0$.

   Hence, if $\phi(1_R) \neq 1_S$, then $\phi(1_R)$ is a zero divisor in S. But if S is an integral domain, then by definition S has no zero-divisors, and ϕ must send 1_R to 1_S. Since, ϕ was an arbitrary non-zero ring homomorphism from R to S, we can say that any non-zero ring homomorphism must send 1_R to 1_S if S is an integral domain.

2. If $\phi(1_R) = 1_S \implies \phi(1_R) = \phi(uu^{-1}) = \phi(u)\phi(u^{-1}) = 1_S$. Hence $\phi(u), \phi(u^{-1})$ are units in S. Let $\phi(u) = p, \phi(u^{-1}) = p'$. But $p' = p^{-1} = \phi(u)^{-1} = \phi(u^{-1})$. Hence, $\phi(u^{-1}) = \phi(u)^{-1}$ for each unit u of R.

Problem 10. Prove that every (two-sided) ideal of $M_n(R)$ is equal to $M_n(J)$ for some (two-sided) ideal J of R.

Solution.

Let I be an ideal of $M_n(R)$, and A be a matrix in $M_n(R)$. Then let J be the ideal generated by all entries x_{ij} of all matrices in I. By definition $I \subseteq M_n(J)$. To show equality, we need to prove the other direction, $M_n(J) \subseteq I$.

Let $A \in M_n(J)$, and α_{ij} be the i, j-th entry of this matrix. We know (by definition) that $\alpha_{ij} \in J \implies \exists x_1, x_2, \cdots, x_n$ (generators of J, i.e. entries of matrices in I) such that

$$\alpha_{ij} = \sum_{k=1}^{n} r_k x_k, r_k \in R$$

Again, by definition, there exists some matrix B_k such that its u, v-th entry is $x_k, \forall x_k$. Using Part 3 of Problem 6, we know we can come up with matrices $E_{iu}, E_{vj} : E_{iu} B_k E_{vj}$ results a matrix that has the u, v-th entry of B_k in the i, j-th position. If we then multiply this matrix by the scalar $r_k \in R : r_k B_k \in I$. This is one term in the summation of α_{ij}. We can see that, although a tedious process, it is possible to find all $r_k B_k \in I$ that sum to α_{ij} for all α_{ij} in A.

Since A was an arbitrary matrix in $M_n(J)$, this proves that $M_n(J) \subseteq I \implies M_n(J) = I$, for some ideal J in R.

And since I was an arbitrary ideal of $M_n(R)$, we can find a corresponding ideal J in R for all I. Hence, every ideal of $M_n(R)$ is equal to $M_n(J)$ for some ideal J of R.

Problem 11. The characteristic of a ring R is the smallest positive integer n such that $1+1+1+\cdots+1=0$ (n times) in R; if no such integer exists the characteristic of R is said to be 0. For example, $\mathbb{Z}/n\mathbb{Z}$ is a ring of characteristic n for each positive integer n and $\mathbb{Z}$ is a ring of characteristic 0.

1. Prove that the map $\mathbb{Z} \to R$ defined by

$$k \mapsto \begin{cases} 1+1+\cdots+1 \ (k \text{ times}) & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -1-1-\cdots-1 \ (-k \text{ times}) & \text{if } k < 0 \end{cases}$$

   is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R (this explains the use of the terminology "characteristic 0" instead of the archaic "characteristic ∞" for rings in which no sum of 1's is zero).

2. Determine the characteristics of the rings $\mathbb{Q}$, $\mathbb{Z}[x]$, $(\mathbb{Z}/n\mathbb{Z})[x]$.

3. Prove that if p is a prime and if R is a commutative ring of characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$.

Solution.

1. Let $k(1) = 1+1+\cdots+1$ (k-times), $-k(1) = -1-1-\cdots-1$ (-k-times), where 1 is the identity in R. Then φ is a homomorphism if it satisfies the following two relations:

$$\varphi(xy) = \varphi(x)\varphi(y) \qquad \varphi(x+y) = \varphi(x) + \varphi(y)$$

   (a) $\forall x, y \in \mathbb{Z}$,

$$\begin{aligned} \varphi(x+y) &= (x+y)(1) \\ &= \underbrace{1+1+\cdots+1}_{(x+y) \text{ times}} \\ &= \underbrace{1+1+\cdots+1}_{x \text{ times}} + \underbrace{1+1+\cdots+1}_{y \text{ times}} \\ &= x(1) + y(1) \\ &= \varphi(x) + \varphi(y) \end{aligned}$$

(b) By definition $k(1) = \sum_{1=0}^{k} 1$, then $\forall x, y \in \mathbb{Z}$,

$$\begin{aligned}
\varphi(x)\varphi(y) &= x(1)y(1) \\
&= \left(\sum_{i=1}^{x} 1\right)\left(\sum_{i=1}^{y} 1\right) \\
&= \sum_{i=1}^{x}\sum_{i=1}^{y} 1 \\
&= \sum_{i=1}^{xy} 1 \\
&= xy(1) \\
&= \varphi(xy)
\end{aligned}$$

Hence, φ is a ring homomorphism. The kernel of a ring homomorphism is everything that maps to 0.

$$ker(\varphi) = \{\varphi(x) = x(1) = 0, \forall x \in \mathbb{Z}\}$$

If no positive value x satisfy that relation, then $ker(\varphi) = \{0\}$. However, if n is the characteristic of R, then by definition $n(1) = 0 \implies \varphi(n) = 0$. We can see that $\forall a \in \mathbb{Z}$, $\varphi(an) = \varphi(a) \cdot 0 = 0 \implies \varphi : n\mathbb{Z} \to 0$.

Hence, $n\mathbb{Z} \subseteq ker(\varphi)$.

Conversely let $k \in ker(\varphi)$, then $\varphi(k) = k(1) = 0$. If characteristic is zero, then no positive number maps to zero, i.e., $ker(\varphi) = \{0\}$. Else if, characteristic $n > 0$, then for some $0 \leq r \leq n-1$ and some q, $k = qn + r \implies \varphi(k) = \varphi(q)\varphi(n) + \varphi(r) \implies \varphi(k) = 0 + \varphi(r) = \varphi(r)$. But $\varphi(k) = 0 \implies \varphi(r) = 0$. But since $r < n \implies r = 0$. Hence, $k = qn$, where n is the characteristic of the group and $q \in \mathbb{Z}$. $ker(\varphi) \subseteq n\mathbb{Z}$. Thus, $ker(\varphi) = n\mathbb{Z}$.

2. Let characteristic n of a ring R be represented by $n(R)$.

   (a) $n(\mathbb{Q}) = x \cdot 1 = 0$, for any $x \in \mathbb{Q}$. We can see that the only rational number that satisfies this relation is 0. Hence, the characteristic of the ring $\mathbb{Q}$ is zero.

   (b) $n(\mathbb{Z}[x]) = a \cdot 1 = 0$, for any $a \in \mathbb{Z}[x]$. For all polynomials $p \in \mathbb{Z}[x]$, $p \cdot 1 = p$, so the only polynomial that results in zero upon being multiplied by the identity is $p = 0$. Hence, the characteristic of the ring $\mathbb{Q}$ is zero.

   (c) $n((\mathbb{Z}/n\mathbb{Z})[x]) = a \cdot 1 = 0$. We know that characteristic of $\mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}$. Then the smallest $a \in (\mathbb{Z}/n\mathbb{Z})[x]$ such that $a \cdot 1 = 0$ is n. i.e the characteristic of $(\mathbb{Z}/n\mathbb{Z})[x]$ is n.

3. Let a, b be arbritary elements in R. Using the binomial theorem,

$$(a+b)^p = \binom{p}{0} a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + \binom{p}{p} b^p$$

If $0 < i < p$, $\binom{p}{i} = p \cdot x$, for some x (Since p is prime, no number less than p divides it). But since R is characteristic p, $p \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0$. And if $i = 0$ or $i = p$, $\binom{p}{i} = 1$. Hence, the middle term in the equation above is zero,

$$(a+b)^p = a^p + 0 + b^p = a^p + b^p$$

Hence proved.

Problem 12. Let R be a commutative ring. Recall that an element $x \in R$ is nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Prove that the set of nilpotent elements form an ideal - called the nilradical of R and denoted by $\mathfrak{N}(R)$. [Use the Binomial Theorem to show that $\mathfrak{N}(R)$ is closed under addition.]

Solution.

Let $\mathfrak{N}(R)$ be the set of nilpotent elements in R. Then $\mathfrak{N}(R)$ is an ideal if it is a subrng, and is closed under multiplication with elements in R.

1. $(\mathfrak{N}(R), +)$ is a group
   (a) Identity exists:
   $$\forall n \in \mathbb{Z}^+, 0^n = 0$$
   (b) Closure under addition and inverses:
   $\forall x, y \in \mathfrak{N}(R)$, and n, n' be the smallest positive integers such that $x^n = 0, y^{n'} = 0$
   $$(x-y)^{n+n'} = \sum_{i=0}^{n+n'} \binom{n+n'}{i} x^{n+n'-i}(-1)^i y^i$$
   For all $i \geq n'$, $y^i = 0$. If $i < n' \implies n + n' - i > n \implies x^{n+n'-i} = 0$.
   Hence every term in that sum is zero and $(x - y)$ is a nilpotent element.
   (c) Associativity and commutativity are inherited from R.
2. Distributivity and Associativity are inherited from R.
3. Closure under multiplication:
   $\forall x, y \in \mathfrak{N}(R), xy = yx \in \mathfrak{N}(R)$ (Problem 1.2).
4. Let $x \in \mathfrak{N}(R)$, $r \in R$, then $rx, xr \in \mathfrak{N}(R)$ (Problem 1.2).

Problem 13. *Quadratic units.* Write $\mathcal{O}_D = \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

1. Prove that if $D < 0$, then the group $\mathcal{O}_D^\times$ is finite and find all possibilities for this group. Hint. Think about the topology of the subset $\mathcal{O}_D \subset \mathbb{C}$ and the norm map.
2. By contrast, it is true (but we will not prove it in this class) that if $D > 0$ then $\mathcal{O}_D^\times$ is infinite. Show that $\mathcal{O}_D^\times$ is infinite for $D = 3, 5, 6, 7$.

Solution.

1. We know the following,

   (a) $\mathcal{O}_D = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, where $\omega = \begin{cases} \sqrt{D}, D \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{D}}{2}, D \equiv 1 \pmod 4 \end{cases}$.

   (b) $\mathcal{O}_D^\times = \{\alpha \mid N(\alpha) = \pm 1\}$ (DF page 230).

   (c) $N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = \begin{cases} a^2 - b^2 D, D \equiv 2, 3 \pmod 4 \\ a^2 + ab + \frac{1-D}{4} b^2, D \equiv 1 \pmod 4 \end{cases}$

   where, $\bar{\omega} = \begin{cases} -\sqrt{D}, D \equiv 2, 3 \pmod 4 \\ \frac{1-\sqrt{D}}{2}, D \equiv 1 \pmod 4 \end{cases}$.

   If $D < 0$, then we can re-write the norm equation as:

   $$N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = \begin{cases} a^2 + b^2 abs(D), D \equiv 2, 3 \pmod 4 \\ a^2 + ab + \frac{1+abs(D)}{4} b^2, D \equiv 1 \pmod 4 \end{cases}$$

   where $abs(D)$ is the absolute value of D. When $D \equiv 2, 3 \pmod 4$,

   $$N(a + b\omega) = a^2 + b^2 abs(D)$$

   both of the terms in the equation are non-negative, hence, the only value the norm of a

unit can have is 1. When $D = 1 \pmod 4$

$$\begin{aligned} N(a+b\omega) &= a^2 + ab + \frac{1+abs(D)}{4}b^2 \\ &= a^2 + ab + \left(\frac{b}{2}\right)^2 + \left(\frac{1+abs(D)}{4} - \frac{1}{4}\right)b^2 \\ &= \left(a + \frac{b}{2}\right)^2 + \frac{abs(D)}{4}b^2 \end{aligned}$$

Again, both of the terms in the equation are non-negative, hence, the only value the norm of a unit can have is 1. I.e. for any $\alpha = (p + q\omega) \in \mathcal{O}_D^\times$,

$$N(\alpha) = 1 = \begin{cases} p^2 + q^2 abs(D),\ D \equiv 2, 3 \pmod 4 \\ \\ \left(p + \frac{q}{2}\right)^2 + \frac{abs(D)}{4}q^2,\ D \equiv 1 \pmod 4 \end{cases}$$

Clearly, if $D \equiv 2, 3 \pmod 4$, the only possible values are $p = \pm 1, q = 0 \implies \mathcal{O}_D^\times = \{1, -1\}$. (The smallest possible α we can have here is $\alpha = 1 + \sqrt{-2}$, for which $N(\alpha) = 3$ i.e it is not a unit.

If $D \equiv 1 \pmod 4$,

$$N(\alpha) = p^2 + pq + \frac{1+abs(D)}{4}q^2$$

$\frac{1+abs(D)}{4}q^2 > 1$, if $q \neq 0, D > 1$.
Hence, the only possible values are $q = 0, p = \pm 1 \implies \mathcal{O}_D^\times = \{1, -1\}$.

If $D = 1$, $\alpha = p + qi$,

$$N(\alpha) = p^2 - q^2(-1) = p^2 + q^2$$

then, either $q = 0 \implies p = \pm 1$, or $p = 0 \implies q = \pm 1 \implies \mathcal{O}_D^\times = \{1, -1, i, -i\}$.

2. We know that $N(\alpha) = 1 \iff \alpha$ is a unit. So if we find such an α and show that it has infinite order, we can claim that $\mathcal{O}_D^\times$ is infinite.

   (a) $D = 3$
   Take $\alpha = (2+\sqrt{3})$, $N(\alpha) = (2+\sqrt{3})(2-\sqrt{3}) = 4-3 = 1$. Hence, $(2+\sqrt{3})$ is a unit in $\mathcal{O}_3$. Because α is positive, and we know that positive powers of positive numbers are positive (in $\mathbb{Z}$), we can say

   $$\alpha^n > 0, \forall n \in \mathbb{Z}^+ \implies |\alpha| = \infty \implies |\mathcal{O}_3^\times| = \infty$$

   (b) $D = 5$ (1 mod 4)
   Take $\alpha = \left(0 + \frac{3+\sqrt{5}}{2}\right)$, $N(\alpha) = \left(0 + \frac{3+\sqrt{5}}{2}\right)\left(0 + \frac{3-\sqrt{5}}{2}\right) = \left(\frac{9-5}{4}\right) = 1$. Hence, $\left(0 + \frac{3+\sqrt{5}}{2}\right)$ is a unit in $\mathcal{O}_5$. Because α is positive, and we know that positive powers of positive numbers are positive (in $\mathbb{Z}$), we can say

   $$\alpha^n > 0, \forall n \in \mathbb{Z}^+ \implies |\alpha| = \infty \implies |\mathcal{O}_3^\times| = \infty$$

   .

   (c) $D = 6$
   Take $\alpha = (5+4\sqrt{6})$, $N(\alpha) = (5+4\sqrt{6})(5+4\sqrt{6}) = 25-24 = 1$. Hence, $(5+4\sqrt{6})$ is a unit in $\mathcal{O}_6$. Because α is positive, and we know that positive powers of positive numbers are positive (in $\mathbb{Z}$), we can say

   $$\alpha^n > 0, \forall n \in \mathbb{Z}^+ \implies |\alpha| = \infty \implies |\mathcal{O}_3^\times| = \infty$$

   .

   (d) $D = 7$
   Take $\alpha = (6+5\sqrt{7})$, $N(\alpha) = (6+5\sqrt{7})(6+5\sqrt{7}) = 36-35 = 1$. Hence, $(6+5\sqrt{7})$ is a unit in $\mathcal{O}_7$. Because α is positive, and we know that positive powers of positive numbers are positive (in $\mathbb{Z}$), we can say

   $$\alpha^n > 0, \forall n \in \mathbb{Z}^+ \implies |\alpha| = \infty \implies |\mathcal{O}_3^\times| = \infty$$

   .

Problem 14. *Quaternions.* Let F be a field and $\mathbb{H}_F$ be the ring of F-quaternions, whose elements are

$$a + bx + cy + dz, \qquad a, b, c, d \in F$$

and where addition and multiplication is defined to be the associative and distributive operations with the relations $x^2 = y^2 = z^2 = -1$ and $xy = z = -yx$, $zx = y = -xz$, $yz = x = -zy$. Note that these are the same relations as in the usual (real) quaternions, though the reason why we aren't using i, j, and k will be quickly apparent. As before, $\mathbb{H}_F$ is a unital F-algebra (see the notations section above).

1. Define the 2×2 complex Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

   These play a role in quantum mechanics. Prove that the $\mathbb{R}$-subspace A of $M_2(\mathbb{C})$ spanned by $I, i\sigma_x, i\sigma_y, i\sigma_z$ is a unital $\mathbb{R}$-algebra isomorphic to $\mathbb{H}_{\mathbb{R}}$. **Hint.** Realize that $M_2(\mathbb{C})$ is an $\mathbb{R}$-algebra under matrix multiplication, and show that A is an $\mathbb{R}$-subalgebra, so that you only need to check that A is closed under matrix multiplication.

2. Prove that $\mathbb{H}_{\mathbb{C}}$ is isomorphic, as unital $\mathbb{C}$-algebras, to $M_2(\mathbb{C})$.

3. For every odd prime p, prove that $\mathbb{H}_{\mathbb{F}_p}$ is isomorphic, as unital $\mathbb{F}_p$-algebras, to $M_2(\mathbb{F}_p)$. **Hint.** The idea is to find replacements for the Pauli matrices. First, if -1 is a square in $\mathbb{F}_p^\times$, then you can literally use the Pauli matrices, replacing i by a square root of -1. Prove that for p odd, -1 is a square in $\mathbb{F}_p^\times$ if and only if $p \equiv 1 \pmod 4$. To do this, recall the (as of yet unproved) fact that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, which is even since p is odd. Then the squares form a subgroup of index 2 in $\mathbb{F}_p^\times$, and in fact any element of order 4 in $\mathbb{F}_p^\times$ is a square root of -1. But $\mathbb{F}_p^\times$ has an element of order 4 if and only if $p-1$ is divisible by 4. So what about the case $p \equiv 3 \pmod 4$? Here you need to come up with different matrices whose square is $-I$, which by linear algebra must have trace 0 and determinant 1. The following fact will be useful: when p is odd, there are $(p+1)/2$ squares in $\mathbb{F}_p$ (this follows immediately from the preceding discussion, together with the fact that 0 is a square).

4. Prove that $\mathbb{H}_{\mathbb{F}_2}$ is isomorphic to the group ring $\mathbb{F}_2[G]$, where G is a Klein-four group.

Solution.

1. (a) $M_2(\mathbb{C})$ is an $\mathbb{R}$-algebra under matrix multiplication.
   We know that $M_2(\mathbb{C})$ is a ring, then we only need to check that the following

condition holds

$$(aX)(bY) = (ab)(XY) \qquad \forall a, b \in \mathbb{R}, \forall X, Y \in M_2(\mathbb{C})$$

$$\begin{aligned}((aX)(bY))_{ij} &= \sum_{k=1}^{2}(ax_{ik})(by_{kj}) \\ &= \sum_{k=1}^{2}(ab)(x_{ik}y_{kj}) \\ &= (ab)\sum_{k=1}^{2}(x_{ik}y_{kj}) \\ \implies (aX)(bY) &= (ab)(XY)\end{aligned}$$

(b) $A = \{aI + b(i\sigma_x) + c(i\sigma_y) + d(i\sigma_z), \forall a, b, c, d \in \mathbb{R}\}$ is a sub-algebra.
To show that subspace A is a subalgebra we only need to check if it is closed under matrix multiplication:

i. $\forall x \in A$, $Ix = x$.

ii. $i\sigma_x \cdot i\sigma_y$

$$\begin{aligned}i\sigma_x \cdot i\sigma_y &= i\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \cdot i\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \\ &= \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \\ &= \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix} \\ &= -i\sigma_z\end{aligned}$$

$\implies i\sigma_x \cdot i\sigma_y \in A.$

iii. $i\sigma_y \cdot i\sigma_x$

$$\begin{aligned}i\sigma_y \cdot i\sigma_x &= i\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \cdot i\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \\ &= \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}0 & i\\ i & 0\end{pmatrix} \\ &= \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} \\ &= i\sigma_z\end{aligned}$$

$\implies i\sigma_y \cdot i\sigma_x \in A.$

iv. $i\sigma_y \cdot i\sigma_z$

$$\begin{aligned} i\sigma_y \cdot i\sigma_z &= i \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \cdot i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\ &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= -i\sigma_x \end{aligned}$$

$\implies i\sigma_y \cdot i\sigma_z \in A.$

v. $i\sigma_z \cdot i\sigma_y$

$$\begin{aligned} i\sigma_z \cdot i\sigma_y &= i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot i \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= i\sigma_x \end{aligned}$$

$\implies i\sigma_z \cdot i\sigma_y \in A.$

vi. $i\sigma_z \cdot i\sigma_x$

$$\begin{aligned} i\sigma_z \cdot i\sigma_x &= i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= -i\sigma_y \end{aligned}$$

$\implies i\sigma_z \cdot i\sigma_x \in A.$

vii. $i\sigma_x \cdot i\sigma_z$

$$\begin{aligned} i\sigma_x \cdot i\sigma_z &= i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= i\sigma_y \end{aligned}$$

$\implies i\sigma_x \cdot i\sigma_z \in A.$

Hence, A is a $\mathbb{R}$-subalgebra.

(c) A is a unital $\mathbb{R}$-algebra.
$I \in A$, and $I \cdot A_i = A_i, \forall A_i \in A$ so A is unital.

(d) A is isomorphic to $\mathbb{H}_{\mathbb{R}}$.
Note: from the given relations we know that $xy = z, z^2 = -1$ then $xyz = z^2 = -1$. Hence it suffices to prove that that relation holds instead of the 6 others.

$$\mathbb{H}_{\mathbb{R}} = \{a + bx + cy + dz \mid x^2 = y^2 = z^2 = xyz = -1\}$$

$\varphi : A \to \mathbb{H}_{\mathbb{R}}$ is a isomorphism if we can map the generators of A to the generators of $\mathbb{H}_{\mathbb{R}}$ and prove that the relations hold.
Let $\varphi(i\sigma_x) \to x$, $\varphi(i\sigma_z) \to y$, $\varphi(i\sigma_y) \to z$, $\varphi(I) \to 1$.
Checking if the relation $x^2 = y^2 = z^2 = xyz = -1$ holds for A.

i. $(i\sigma_x)^2$

$$\begin{aligned} i\sigma_x \cdot i\sigma_x &= i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= -I \end{aligned}$$

$\implies (i\sigma_x)^2 = -I$

ii. $(i\sigma_y)^2$

$$\begin{aligned} i\sigma_y \cdot i\sigma_y &= i\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \cdot i\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= -I \end{aligned}$$

$\implies (i\sigma_y)^2 = -I$

iii. $(i\sigma_z)^2$

$$\begin{aligned} i\sigma_z \cdot i\sigma_z &= i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= -I \end{aligned}$$

$\implies (i\sigma_z)^2 = -I$

iv. $i\sigma_x \cdot i\sigma_y \cdot i\sigma_z$

$$\begin{aligned} i\sigma_x \cdot i\sigma_y \cdot i\sigma_z &= i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot i\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= -I \end{aligned}$$

$\implies i\sigma_x \cdot i\sigma_z \cdot i\sigma_y = -I.$

The relations hold, hence φ is an isomorphism.

Hence proved, A is a unital $\mathbb{R}$-algebra isomorphic to $\mathbb{H}_{\mathbb{R}}$.

2. The dimensions of $\mathbb{H}_{\mathbb{C}}$ and $M_2(\mathbb{C})$ are both equal to 4. For the map $\varphi : M_2(\mathbb{C}) \to= \mathbb{H}_{\mathbb{R}}$ to be isomorphic the following is required:

   (a) Map the generators of $M_2(\mathbb{C})$ to the generators of $\mathbb{H}_{\mathbb{C}}$ and prove that the relations hold. Already checked this in part (1).

   (b) Show that $M_2(\mathbb{C})$ is a $\mathbb{C}$-algebra:
   Again, since we know that $M_2(\mathbb{C})$ is a ring we only need to check that the following condition holds:

   $(a+bi)X(c+di)Y = (a+bi)(c+di)(XY) \qquad \forall (a+bi), (c+di)) \in \mathbb{C}, \forall X, Y \in M_2(\mathbb{C})$

$$
\begin{aligned}
((a+bi)X(c+di)Y)_{ij} &= \sum_{k=1}^{2}((a+bi)x_{ik})((c+di)y_{kj}) \\
&= \sum_{k=1}^{2}(a+bi)(c+di)(x_{ik}y_{kj}) \\
&= (a+bi)(c+di)\sum_{k=1}^{2}(x_{ik}y_{kj}) \\
\implies (a+bi)X(c+di)Y &= (a+bi)(c+di)XY
\end{aligned}
$$

(c) $I \in \mathrm{M}_2(\mathbb{C})$, and $I \cdot M_i = M_i, \forall M_i \in M_2(\mathbb{C})$ so $M_2(\mathbb{C})$ is unital.

(d) Linearity: If $\forall M_i \in M_2(\mathbb{C})$, $M_i = aI + b(i\sigma_x) + c(i\sigma_y) + d(i\sigma_z)$, where $a, b, c, d \in \mathbb{C}$, then the image of M_i is:

$$\varphi(M_i) = \varphi(aI) + \varphi(b(i\sigma_x)) + \varphi(c(i\sigma_y)) + \varphi(d(i\sigma_z)) = a \cdot 1 + b \cdot x + c\dot{z} + d \cdot y$$

We need to show that $\varphi(\lambda M_i) = \lambda\varphi(M_i)$.

$$
\begin{aligned}
\varphi(\lambda M_i) &= \varphi(\lambda(aI + b(i\sigma_x) + c(i\sigma_y) + d(i\sigma_z))) \\
&= \varphi(\lambda aI + \lambda b(i\sigma_x) + \lambda c(i\sigma_y) + \lambda d(i\sigma_z)) \\
&= \varphi(\lambda aI) + \varphi(\lambda b(i\sigma_x)) + \varphi(\lambda c(i\sigma_y)) + \varphi(\lambda d(i\sigma_z)) \\
&= \lambda a \cdot 1 + \lambda b \cdot x + \lambda c \cdot z + \lambda d \cdot y \\
&= \lambda(a \cdot 1 + b \cdot x + c \cdot z + d \cdot y) \\
&= \lambda(\varphi(M_i))
\end{aligned}
$$

Since, all of the above hold, we can say that φ is an isomorphism and $M_2(\mathbb{C})$ is isomorphic to $\mathbb{H}_{\mathbb{C}}$.

3. To show that for every odd prime p, $\mathbb{H}_{\mathbb{F}_p}$ is isomorphic to $M_2(\mathbb{F}_p)$, we need to first find generators for $M_2(\mathbb{F}_p)$. If -1 is a square in $\mathbb{F}_p$, we can use the Pauli matrices. To check this, let's consider the order of $\mathbb{F}_p$ (mod 4). Since p is an odd prime, there are two possibilities: $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

   (a) $p \equiv 1 \pmod 4$
   Claim: -1 is a square in $\mathbb{F}_p^\times \iff p \equiv 1 \pmod 4$.
   ($\implies$)
   If -1 is a square in $\mathbb{F}_p^\times$ then there exists an element $n \in \mathbb{F}_p$ with order 4 ($|-1| = 2$).

That means if there exists square root of -1 in $\mathbb{F}_p^\times$ then $4 \mid |\mathbb{F}_p^\times| \implies 4 \mid p-1 \implies p \equiv 1 \pmod 4$.

($\Longleftarrow$)
If $p \equiv 1 \pmod 4 \implies p-1 \equiv 0 \pmod 4 \implies 4 \mid p-1 \implies 4 \mid |\mathbb{F}_p^\times| \implies \exists x :| x |= 4$ (converse of Lagrange's Theorem for Abelian Groups).

Claim: Any element of order 4 is a square root of 1 in $\mathbb{F}_p^\times$.
If the order of and element x in $\mathbb{F}_p^\times$, then $x^4 = 1 \implies (x^2)^2 = 1 \implies x^2 = \pm 1$. But if $x^2 = 1$, the order of the element would be 2, hence a contradiction. $\implies x^2 = -1 \implies x = \sqrt{-1}$
Hence, if $p \equiv 1 \pmod 4$ -1 is a square in $F_p^\times$.
Let $p \in \mathbb{F}_p^\times : p^2 = -1$, then our map φ could be defined as:

$$\varphi : 1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\varphi : x \to \begin{pmatrix} 0 & p \\ p & 0 \end{pmatrix}$$
$$\varphi : y \to \begin{pmatrix} p & 0 \\ 0 & -p \end{pmatrix}$$
$$\varphi : z \to \begin{pmatrix} 0 & -p \\ p & 0 \end{pmatrix}$$

The rest of the checks to prove isomorphism are the same as part (2).

(b) $p \equiv 3 \pmod 4$
Claim: The subgroup X of $\mathbb{F}_p^\times$ consisting of all the squares in the group has $(p-1)/2$ elements.

$$\mathbb{F}_p^\times = \{\langle x^k \rangle : 1 \leq k \leq p\}$$

Then the map $\phi : y \to y^2 \implies \phi : x^k \to x^{2k \pmod p}, \forall x^k \in \mathbb{F}_p^\times$ Since there are exactly $(p-1)/2$ even exponents, the index of the subgroup X is:

$$[G : X] = (p-1)/((p-1)/2) = 2$$

Because $p-1$ is $\langle x^{2k} \rangle, k = (p-1)/2$, there exist $a^2, b^2 : a^2 + b^2 = p - 1 \equiv -1$

(mod p). Then we can define our generating matrices to be

$$\varphi : 1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\varphi : x \to \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$\varphi : y \to \begin{pmatrix} b & a \\ a & -b \end{pmatrix}$$
$$\varphi : z \to \begin{pmatrix} -a & b \\ b & a \end{pmatrix}$$

Checking the relations:

$$(\varphi(x))^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$
$$(\varphi(y))^2 = \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$
$$(\varphi(z))^2 = \begin{pmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$
$$\varphi(x)\varphi(y)\varphi(z) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b & a \\ a & -b \end{pmatrix} \begin{pmatrix} -a & b \\ b & a \end{pmatrix} = \begin{pmatrix} -a & b \\ b & a \end{pmatrix} \begin{pmatrix} -a & b \\ b & a \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$$

The rest of the checks to prove isomorphism are the same as part (2).

Hence, for both cases, $\mathbb{H}_{\mathbb{F}_p} \cong M_2(\mathbb{F}_p)$.

4. In $\mathbb{H}_{\mathbb{F}_2}$ the relations look different because the order of the field $\mathbb{F}_p$ is 2:
   (a) $1 \equiv -1$
   (b) $x^2 = y^2 = z^2 = -1 = 1$
   (c) $xy = z = (-1)yx \equiv yx$
   (d) $yz = x = (-1)zy \equiv zy$
   (e) $zx = y = (-1)xz \equiv xz$
   (f) Equivalently, $xyz = -1 \equiv 1$

   Then elements of $\mathbb{H}_{\mathbb{F}_2}$ look like:

$$\mathbb{H}_{\mathbb{F}_p} = \{a + bx + cy + dz \mid a, b, c, d \in \{0, 1\}\}$$

   Order of $|\mathbb{H}_{\mathbb{F}_2}| = 16$.

Then elements of $\mathbb{F}_2[V_4]$ look like:

$$\mathbb{F}_2[V_4] = \{r_1 + r_2a + r_3b + r_4(ab) \mid 1, a, b, ab \in V_4, r_i \in \{0, 1\}\}$$

Order of $|\mathbb{F}_2[V_4]| = 16$.

If we define a map $\varphi : \mathbb{H}_{\mathbb{F}_2} \to \mathbb{F}_2[V_4]$ such that:

$$\begin{aligned}\varphi(1) &= 1\\ \varphi(x) &= a\\ \varphi(y) &= b\\ \varphi(z) &= ab\end{aligned}$$

We know that the order of all of the non-identity elements is 2, and that any two non-identity elements give the third non-identity element under multiplication. Hence, all relations hold and φ is an isomorphism.