Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 648 - Abstract Algebra
Instructor: Professor Arkady Berenstein

Homework - Week 4
ID: 952091294
Term: Winter 2025
Due Date: 5^{th} February, 2025

Problem 16.1.2
True or false? If V is an $\mathbb{R}$-module and $\operatorname{End}_R(V)$ is a division ring, then V is irreducible.

Solution: This is false. Consider the ring $\mathbb{Q}$ of rational numbers, viewed as a $\mathbb{Z}$-module.
Claim: $\operatorname{End}_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}$.
Proof: Given $\frac{p}{q} \in \mathbb{Q}$, we could define a endomorphism $\mathbb{Q} \to \mathbb{Q}$ by sending any rational number $\frac{t}{s} \in \mathbb{Q}$ to $\frac{pt}{qs} \in \mathbb{Q}$. This is a $\mathbb{Z}$-module homomorphism since multiplication in $\mathbb{Q}$ is commutative. So we have $\mathbb{Q} \subset \operatorname{End}_{\mathbb{Z}}\mathbb{Q}$. On the other hand, given $\phi \in \operatorname{End}_{\mathbb{Z}}\mathbb{Q}$, for any $m \in \mathbb{Z}$ and $n \in \mathbb{Z} - 0$, the commutativity of multiplication in $\mathbb{Q}$ tells us that

$$\phi(\frac{m}{n}) = m\phi(\frac{1}{n}) = \frac{m}{n} \cdot n\phi(\frac{1}{n}) = \frac{m}{n}\phi(1).$$

This shows that ϕ is completely determined by the image $\phi(1) \in \mathbb{Q}$, so we have $\operatorname{End}_{\mathbb{Z}}\mathbb{Q} \subset \mathbb{Q}$. Now we have $\operatorname{End}_{\mathbb{Z}}\mathbb{Q} = \mathbb{Q}$. ■

We know that $\operatorname{End}_{\mathbb{Z}}\mathbb{Q} \cong \mathbb{Q}$ is a division ring, but $\mathbb{Q}$ is not simple, which has a proper submodule $\mathbb{Z} \subset \mathbb{Q}$.

Problem 16.1.6
True or false? If A is a commutative algebra over an algebraically closed field then all irreducible A-modules are 1-dimensional.

Solution: This is false. Consider the $\mathbb{C}$-algebra $\mathbb{C}(x)$. Let $A = \mathbb{C}(x)$ and view A as a regular left A-module. A is a field so it is simple since the only submodules are 0 and A itself. But A is a infinite dimensional $\mathbb{C}$-vector space with a basis $\{1, x, x^{-1}, x^2, x^{-2}, \ldots\}$.

Problem 16.1.7
True or false? If A is a finite dimensional commutative algebra over a field, then all irreducible A-modules are 1-dimensional.

Solution: This is false. Consider $A = \mathbb{C}$ as an $\mathbb{R}$-algebra. $\mathbb{C}$ can be viewed as a left regular $\mathbb{C}$-module. $\mathbb{C}$ as a field is simple, but it is a 2-dimensional $\mathbb{R}$-vector space.

Problem 16.1.10
If D is a division ring, then $M_n(D)$ is a simple ring.

Solution: We prove this by induction on n. When $n = 1$, $M_1(D) \cong D$ as a division ring is simple. When $n \geq 2$, suppose we have proved $M_{n-1}(D)$ is a simple ring. Given $A \in M_n(D)$ is an $n \times n$ matrix with entries in D, we are going to show that the two-sided ideal generated by A must be the whole ring $M_n(D)$ or the zero ideal (0). If every entry in A is zero, then the ideal (A) must be the zero ideal. Suppose there is an entry in A which is not zero. We know we can switch rows and columns in A by multiplying the elementary matrices on the left or on the right. So we may assume the $(1, 1)$th entry a_{11} in A is not zero. Since D is a division ring, by multiply $\begin{pmatrix} a_{11}^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$ on the left we can make $a_{11} = 1$. Next, for $2 \leq m \leq n$, we can multiply the first row with $-a_{m1}$ then add it to the mth row. This is elementary operations and can be done via multiplying elementary matrices on the left. This makes all $a_{m1} = 0$. Do the same for all a_{1m}, and in this case it is just multiplying elementary matrices on the right. Now A has the form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

where $B \in M_{n-1}(D)$. If B has no nonzero entries, then A can be viewed as in $M_{n-1}(D)$ with only one nonzero entry at upper left corner, we have proved this case by assumption on n. Similarly, if B has at least one nonzero entry, then by the assumption there exists $B_1, B_2 \in M_{n-1}(D)$ such that

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B_1 & \\ 0 & & & \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B_2 & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix} = I_n$$

This shows that the two sided ideal generated by A must contain I_n, which just means $(A) = M_n(D)$. So $M_n(D)$ is a simple ring.

Problem 16.1.11
True or false? If V is a vector space over a field $\mathbb{F}$, then $\mathrm{End}_{\mathbb{F}}(V)$ is a simple ring.

Solution: This is false. Consider a $\mathbb{C}$-vector space V with a countable ordered basis $\{v_1, \ldots, v_n, \ldots\}$. Let $S = \oplus_{n=1}^{\infty} M_n(\mathbb{C})$. Each element in $M_n(\mathbb{C})$ can be viewed as a linear transformation on the first n base vectors and sending the rest to 0. $S \subset \mathrm{End}_{\mathbb{C}} V$ is a two sided ideal since every matrix in S has only finite rank. Consider $f : V \to V$ sends v_i to v_{i+1} for all $1 \leq i$. $f \in \mathrm{End}_{\mathbb{C}} V$ but $f \notin S$ since f operates on infinitely many base vectors. This proves that S is a proper two sided ideal in $\mathrm{End}_{\mathbb{C}} V$, so $\mathrm{End}_{\mathbb{C}} V$ is not a simple ring.

Problem 16.2.2
Let R be a ring. Then R is left semisimple if and only if every left ideal of R is generated by an idempotent.

Solution: Suppose R is left semisimple. By Lemma 16.2.1, R as a left regular R-module is completely reducible. So for any left ideal $I \subset R$, there exists a left ideal $J \subset R$ such that $I \oplus J = R$. This means there exists $a \in I$ such that $1 - a \in J$. $I \cap J = 0$ implies that $ra \in I$ for any $r \in R$. Also, we have

$$a = a \cdot 1 = a(a + (1 - a)) = a^2 + a(1 - a).$$

Note that $a(1 - a) \in J$ and both a and a^2 are in I, so $a(1 - a) = 0$. This proves $a = a^2$ is an idempotent. Moreover, for any $x \in I$, we have

$$x = x \cdot 1 = xa^2 = xa.$$

This proves the left ideal I is generated by an idempotent a.

Conversely, suppose every left ideal in R is generated by an idempotent. Given a left ideal $I \subset R$, we know that I is generated by an idempotent a. We know that a and $1 - a$ are orthogonal idempotents and $a + 1 - a = 1$, by Lemma 14.5.1, $R = Ra \oplus R(1 - a) = I \oplus R(1 - a)$. This proves that R as a left regular R-module is completely reducible, so R is a left semisimple ring.

Problem 16.2.4
Find a group G for which not every finite dimensional $\mathbb{C}G$-module is completely reducible.

Solution: Consider

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{C} \right\}$$

and a $\mathbb{C}G$-module

$$V = \left\{ \begin{pmatrix} m \\ n \end{pmatrix} \right\} \mid m, n \in \mathbb{C}.$$

V is left $\mathbb{C}G$-module and a 2-dimensional $\mathbb{C}$-vector space. Consider the submodule $W \subset V$ where

$$W = \left\{ \begin{pmatrix} m \\ 0 \end{pmatrix} \mid m \in \mathbb{C} \right\}.$$

W is indeed a submodule of V since for any $c \in \mathbb{C}$, we have

$$c \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m \\ 0 \end{pmatrix} = \begin{pmatrix} cm \\ 0 \end{pmatrix} \in W.$$

Suppose V is completely reducible, then there exists a submodule $W' \subset V$ such that $V = W \oplus W'$. Since $W \cap W' = 0$, so $\begin{pmatrix} 1 \\ -1 \end{pmatrix} \in V$ and $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in V$ are both in W', but we have

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \in W.$$

A contradiction. So V is not completely reducible.

Problem 16.2.17
True or false? If R is a ring with no non-trivial left ideals, then it also has no non-trivial right ideals.

Solution: This is true. We prove R is a division ring, so that R has no non trivial right ideal. First we prove that R has no zero divisors. Suppose $ab = 0$ and $0 \neq a \in R, 0 \neq b \in R$. R having no left ideals implies there exists $r \in R$ such that $ra = 1$. So we have

$$b = (ra)b = r(ab) = r \cdot 0 = 0.$$

This contradicts the assumption that $b \neq 0$. So R has no zero divisors. Now for any $x \in R$, there exists $y \in R$ such that $yx = 1$ since R has no non trivial left ideals. So y is the left inverse of x in R. Note that we have

$$y = (yx)y = y(xy).$$

This implies that $y(xy - 1) = 0$. Since R has no zero divisors, so $xy = 1$. This shows that y is also the right inverse of x. Thus, we proved that R is a division ring.

Problem 16.2.19
True or false? If A and B are semisimple complex algebras of dimension 3, then $A \cong B$.

Solution: This is true. By Theorem 16.2.18, since $\mathbb{C}$ is algebraically closed, A and B are isomorphic to

$$M_{n_1}(\mathbb{C}) \times M_{n_m}(\mathbb{C}).$$

Note that $M_2(\mathbb{C})$ has complex dimension 4. So $n_1 = \cdots = n_m = 1$. This implies $A \cong B \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \cong \mathbb{C}^3$.

Problem 16.2.21
Let C_n be the cyclic group of order n and let $\mathbb{F}C_n$ denote its group algebra over a field $\mathbb{F}$.

(1) Prove that $\mathbb{F}C_n \cong \mathbb{F}[x]/(x^n - 1)$.

(2) How many isomorphism classes of irreducible $\mathbb{C}C_n$-modules are there? What are their dimensions?

(3) Decompose $\mathbb{C}C_n$ explicitly as a direct sum of simple algebras.

(4) How many isomorphism classes of irreducible $\mathbb{Q}C_n$-modules are there up to isomorphism? What are their dimensions?

(5) Describe the Wedderburn-Artin decomposition of $\mathbb{Q}C_n$ up to isomorphism.

Solution:

(1) Let $c \in C_n$ be the generator of C_n. Consider the following map

$$f : \mathbb{F}[x] \to \mathbb{F}C_n,$$
$$x \mapsto c.$$

This is a well-defined map of algebras since the group algebra $\mathbb{F}C_n$ is defined $\mathbb{F}$-linearly and the group operation in C_n is just multiplication by the power of c. f is also surjective since elements in $\mathbb{F}C_n$ is just $\mathbb{F}$-linear combination of powers of c. Consider the ideal $I = (x^n - 1) \subset \mathbb{F}[x]$. Every element $p \in I$ can be written as $p(x) = (x^n - 1)g(x)$ and we have $f(p) = (c^n - 1)g(c) = 0$. So $I \subset \ker f$. Note that $\ker f \subset \mathbb{F}$ is an ideal in a PID $\mathbb{F}[x]$, so $\ker f$ must be generated by one nonzero polynomial p. Since $I \subset \ker f$, we know that $p|(x^n - 1)$. Suppose $\deg p < n$. We know $p(c) \neq 0$ in $\mathbb{F}C_n$, so $\deg p = n$. This implies $\ker f = (x^n - 1)$. By the first isomorphism theorem, we have

$$\mathbb{F}[x]/(x^n - 1) \cong \mathbb{F}C_n.$$

(2) Let $R = \mathbb{C}C_n$. Note that R is commutative. By Exercise 14.1.25, the set of isomorphism classes of simple R-modules is bijective to the set of maximal ideals of R. So we only need to classify maximal ideals in R. By Wedderburn-Artin Theorem for Algebras, $R = \mathbb{C}C_n \cong \mathbb{C}^{\oplus n}$ since R is commutative and has a basis $\{e, c, c^2, \ldots, c^{n-1}\}$ where $c \in C_n$ is the generator and e is the identity element in the group C_n. The maximal ideal in $\mathbb{C}^n$ is isomorphic to $\mathbb{C}^{n-1}$, so we have n maximal ideals in R and there are n isomorphisms classes of simple R-modules. Every one of them is isomorphic to $\mathbb{C}^n/\mathbb{C}^{n-1} \cong \mathbb{C}$ and is 1-dimensional.

(3) Let $w = e^{\frac{2\pi i}{n}}$. For $0 \leq r \leq n-1$, define

$$e_r = \sum_{j=0}^{n-1} w^{rj} c^j.$$

Note that $\frac{1}{n} e_r$ is an idempotent since

$$\begin{aligned}
e_r^2 &= (1 + w^r c + w^{2r} c^2 + \cdots + w^{(n-1)r} c^{n-1})^2 \\
&= 1 + w^r c + w^{2r} c^2 + \cdots + w^{(n-1)r} c^{n-1} \\
&\quad + w^r c + w^{2r} c^2 + \cdots + w^{(n-1)r} c^{n-1} + 1 \\
&\quad + \cdots \\
&\quad + w^{(n-1)r} c^{n-1} + 1 + w^r c^+ \cdots + w^{(n-2)r} c^{n-2} \\
&= n(1 + w^r c + \cdots + w^{(n-1)r} c^{n-1}) \\
&= n e_r
\end{aligned}$$

Next, we prove that $e_0, e_1, \ldots, e_{n-1}$ are orthogonal. For $0 \leq r \neq s \leq n-1$, we have

$$e_r = \sum_{j=0}^{n-1} w^{rj} c^j = \sum_{j=0}^{n-1} w^{r(i+j)} c^{i+j}$$

for any i because both w and c are nth root of 1. And this only gives a permutation on every summand.

$$\begin{aligned}
e_r e_s =&(\sum_{j=0}^{n-1} w^{rj} c^j)(\sum_{i=0}^{n-1} w^{si} c^i) \\
=&\sum_{i,j=0}^{n-1} w^{rj+si} c^{j+i} \\
=&\sum_{i,j=0}^{n-1} w^{r(j+i)-ri+si} c^{j+i} \\
=&\sum_{i,j=0}^{n-1} w^{(s-r)i} w^{rj} c^j \\
=&(\sum_{i=0}^{n-1} w^{(s-r)i}) e_r.
\end{aligned}$$

Here $r-s \neq 0$. If $r-s$ is coprime with n, then

$$\sum_{i=0}^{n-1} w^{(r-s)i} = 1 + w + w^2 + \cdots + w^{n-1} = 0.$$

If $1 < d = \gcd(|r-s|, n)$ where $d|n$, then

$$\sum_{i=0}^{n-1} w^{(r-s)i} = 1 + w^d + w^{2d} + \cdots + w^{(n-1)d} = 0.$$

This proves that $e_0, e_1, \ldots, e_{n-1}$ are orthogonal. Note that $e_0 + e_1 + \cdots + e_{n-1} = n(1)$. By Lemma 14.5.1, we have a decomposition

$$\mathbb{C}C_n \cong \mathbb{C}C_n e_0 \oplus \cdots \mathbb{C}C_n e_{n-1}.$$

We check that for any $0 \leq r \leq n-1$, $\mathbb{C}C_n e_r$ is a simple ideal. Suppose $\sum_{i=0}^{n-1} a_i c^i \in \mathbb{C}C_n$, we have

$$\begin{aligned}
(\sum_{i=0}^{n-1} a_i c^i)(\sum_{j=0}^{n-1} w^{rj} c^j) &= \sum_{i,j=0}^{n-1} a_i w^{rj} c^{i+j} \\
&= \sum_{i,j=0}^{n-1} a_i w^{-ri} w^{r(j+i)} c^{i+j} \\
&= \sum_{i,j}^{n-1} a_i w^{-ri} w^{rj} c^j \\
&= (\sum_{i=0}^{n-1} a_i w^{-ri}) e_r.
\end{aligned}$$

This proves $\mathbb{C}C_n e_r \cong \mathbb{C}e_r$ is a ideal in R. Moreover, since $\mathbb{C}$ is a field, this shows that $\mathbb{C}e_r$ is a simple ideal. So we have written $R = \mathbb{C}C_n$ as a product of simple ideals

$$\mathbb{C}C_n \cong \mathbb{C}e_0 \oplus \cdots \oplus \mathbb{C}e_{n-1}.$$

(4) Let $R = \mathbb{Q}C_n$. R is commutative and by Exercise 14.1.25, we only need to classify the isomorphism classes of maximal ideals in R. Note that by (1), R is isomorphic to $\mathbb{Q}[x]/(x^n - 1)$. Note that on the field $\mathbb{Q}$, $x^n - 1 = \prod_{d|n} \Phi_d(x)$ where $\Phi_d(x)$ is the cyclotomic polynomials corresponding to the dth primitive root of unity. For any $d|n$, by Theorem 13.3.2, $\Phi_d(x)$ is irreducible and by Chinese remainder theorem, $\mathbb{Q}[x]/(x^n - 1) \cong \prod_{d|n} \mathbb{Q}[x]/(\Phi_d(x))$. So each $\mathbb{Q}[x]/\Phi_d(x)$ is simple as a R-module since $\Phi_d(x)$ is maximal in $\mathbb{Q}[x]$. This gives an isomorphism class of simple R-module. For any $d|n$, the dimension of $\mathbb{Q}[x]/\Phi_d(x)$ as a $\mathbb{Q}$-vector space is just the degree of $\Phi_d(x)$, which is $\varphi(d)$, where φ is the Euler's totient function.

(5) Note that $\mathbb{Q}C_n$ is semisimple by Maschke's theorem. Since $R = \mathbb{Q}C_n$ is commutative, by Wedderburn-Artin theorem for algebras, R is isomorphic to $D_1 \times D_2 \times \cdots \times D_m$ where D_i is a finite extension of $\mathbb{Q}$. From (4) and by uniqueness of Wedderburn-Artin, we know each D_i is isomorphic to $\mathbb{Q}[x]/\Phi_d(x)$ for some $d|n$. Note that the cyclotomic polynomial $\Phi_d(x)$ is the minimal polynomial for the dth cyclotomic field, which can be obtained by adjoining a complex primitive dth root ω_d to $\mathbb{Q}$. So we have

$$D_d \cong \mathbb{Q}[x]/\Phi_d(x) \cong \mathbb{Q}(\omega_d).$$

We have a decomposition $\mathbb{Q}C_n \cong \prod_{d|n} \mathbb{Q}(\omega_d)$.