Problem Set 3
Abstract Algebra

Bennett Rennier
bennett@brennier.com

Ex 1. Let M, A, B, C, and C' be semi-simple R-modules of finite length such that $M = A \oplus C = B \oplus C'$. If C and C' are isomorphic, show that A and B are isomorphic R-modules.

Proof. We note that since $C \simeq C'$, they have the same length. Since $A \oplus C = B \oplus C'$ have the same length as well, it must be that A and B have the same length.

Now, we will prove the statement using induction on the length of A. If the length of A is zero, then A must be the zero module. Since A and B have the same length, B must be the zero module as well. Thus, A and B are isomorphic.

Now suppose A has length $k+1$ and that the statement holds for any modules of length less than $k+1$. Since A and B both have the same length, we may write $A = \oplus_{i \le k+1} N_i$ and $B = \oplus_{i \le k+1} M_i$. Additionally, since $C \simeq C'$, they must have the same length and their factors must be isomorphic up to permutation. Without loss of generality, we may write $C = \oplus_{k+1 < i \le n} N_i$ and $C' = \oplus_{k+1 < i \le n} M_i$ where $N_i \simeq M_i$ for $k+1 < i \le n$. Since we know that

$$\bigoplus_{1 \le i \le n} N_i = A \oplus C = B \oplus C' = \bigoplus_{1 \le i \le n} M_i,$$

there must be some permutation $\sigma \in S_n$ such that $N_i \simeq M_{\sigma(i)}$ for $1 \le i \le n$. Let ℓ be the least positive integer such that $\sigma^\ell(1) \le k+1$. We note that such a k must exist as $|\sigma|$ satisfies the condition. We see then that

$$N_1 \simeq M_{\sigma(1)} \simeq N_{\sigma(1)} \simeq M_{\sigma^2(1)} \simeq N_{\sigma^2(1)} \simeq \ldots \simeq N_{\sigma^{\ell-1}(1)} \simeq M_{\sigma^\ell(1)}.$$

Thus, we have that $C \oplus N_1 \simeq C' \oplus M_{\sigma^\ell(1)}$. Since we know that

$$\left(\bigoplus_{2 \le i \le k+1} N_i \right) \oplus (C \oplus N_1) = A \oplus C = B \oplus C' = \left(\bigoplus_{\substack{1 \le i \le k+1 \\ i \ne \sigma^\ell(1)}} M_i \right) \oplus (C' \oplus M_{\sigma^\ell(1)})$$

and that $\oplus_{2 \le i \le k+1} N_i$ is of length k, we have by the induction hypothesis that

$$\left(\bigoplus_{2 \le i \le k+1} N_i \right) \simeq \left(\bigoplus_{\substack{1 \le i \le k+1 \\ i \ne \sigma^\ell(1)}} M_i \right).$$

As $N_1 \simeq M_{\sigma^\ell(1)}$, this proves that $A \simeq B$. $\square$

Ex 2. [This extends Ex 3 of the previous homework] Let $\{e_{ij} : (i,j) \in \mathbb{N} \times \mathbb{N}\}$ be a basis of a vector space V. Define $J_n = \{f \in \mathrm{End}(V) : f(e_{ij}) = 0 \text{ for all } j > n\}$.

a) Verify that J_n is a left ideal of R.

b) Prove that $J_n + I$ is different from $J_{n+1} + I$ for all $n \in \mathbb{N}$.

c) Deduce that the (simple) ring R/I is not noetherian and hence not semi-simple.

Proof.

a) Let $f, g \in J_n$, we see that $(f+g)(e_{ij}) = f(e_{ij}) + g(e_{ij}) = 0 + 0 = 0$ for all $j > n$, which proves that $f + g \in J_n$. Furthermore, if $f \in J_n$ and $g \in R$, we have that $(g \circ f)(e_{ij}) = g(f(e_{ij})) = g(0) = 0$ for all $j > n$. This proves that J_n is a left ideal of R.

b) Let f be the linear map defined on the basis elements as

$$f(e_{ij}) = \begin{cases} 0 & j > n+1 \\ e_{ij} & \text{otherwise} \end{cases}$$

which is an element of J_{n+1} and hence an element of $J_{n+1} + I$. Suppose that $f = g + h$ where $g \in J_n$ and $h \in I$. We see then that

$$h(e_{in}) = 0 + h(e_{in}) = g(e_{in}) + h(e_{in}) = f(e_{in}) = e_{in}.$$

But this is for any $i \in \mathbb{N}$, implying that $\dim \operatorname{im} h$ is infinite, which contradicts h being in I. Thus, f is an element of $J_{n+1} + I$ but not of $J_n + I$.

c) We can easily see that $J_n \subseteq J_{n+1}$. By part (b), we have that $J_0 + I \subsetneq J_1 + I \subsetneq J_2 + I \ldots$ is an infinite ascending chain of distinct ideals of R/I. Thus, R/I is not noetherian as a ring. This proves that R/I is not noetherian as an R/I-module, so it can't be a semi-simple ring.

$\square$

Ex 3. Prove that the short exact sequence of $k[G]$-modules

$$0 \longrightarrow \ker(\varepsilon) \xhookrightarrow{i} k[G] \xrightarrow{\varepsilon} k \longrightarrow 0$$

where $\varepsilon(\sum_{i=1}^n k_i g_i) = \sum_{i=1}^n k_i$ does not split if either G is infinite or G is finite with $|G|$ being a multiple of the characteristic of k.

Proof. Suppose that the sequence does split. That means there exists a $k[G]$ homomorphism $\sigma : k \to k[G]$ such that $\varepsilon \circ \sigma = \mathrm{Id}_k$. Let us examine the element $\sigma(1) = \sum_{i=1}^n k_i g_i$ of $k[G]$. Since σ is a $k[G]$-module homomorphism, we see that for any $g \in G$,

$$g \cdot \left(\sum_{i=1}^n k_i g_i \right) = g.\sigma(1) = \sigma(g.1) = \sigma(\varepsilon(g)1) = \sigma(1 \cdot 1) = \sigma(1) = \sum_{i=1}^n k_i g_i.$$

Thus, the element $\sigma(1)$ must be invariant under muliplication by any element $g \in G$. Since the action of G on itself by left multiplication is transitive and $\sigma(1)$ can't be zero as $\varepsilon(\sigma(1)) = \mathrm{Id}_k(1) = 1$, we see that every element of g must appear in the sum $\sigma(1)$ and that all the k_i's must be equal to some single k'. In the case that $|G|$ is infinite, this is a contradiction as infinite sums are not allowed in $k[G]$. Furthermore, we have that

$$1 = \mathrm{Id}_k = \varepsilon(\sigma(1)) = \varepsilon\left(\sum_{g\in G} k'g\right) = \sum_{g\in G} k' = k'|G|.$$

In the case that the characteristic of k divides $|G|$, this is a contradiction as it would imply that $1 = 0$. Thus, if $|G|$ is infinite or if the characteristic of k divides $|G|$, there can be no such σ, proving that the short exact sequence does not split. □

Ex 4.

a) If R is a commutative ring and x is a nonzero nilpotent element of R, show that the principal ideal $(x) = Rx$ is not a direct summand of the R-module R.

b) Give an example of a ring R and a nonzero nilpotent element x of R such that the left ideal Rx is a direct summand of the R-module R.

Proof.

a) Let $N = Rx$ and let S be an R-module such that $R = N + S$. Let $s \in S$ be nonzero. Since x is nilpotent, there is some n such that $x^n = 0$. We see then that

$$(x^{n-1} - s)x + (x)s = x^n - sx + xs = 0 - xs + xs = 0.$$

Since we know that $x \neq 0$, this means that there are two ways of representing zero, proving that $R \neq N \oplus S$. As S was arbitrary, this proves that N is not the direct summand of R as an R-module.

b) Consider the ring $M_4(\mathbb{R})$. We see that the matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and the matrix $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are both nilpotent (their square is zero). However,

$$\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right) = M_n(\mathbb{R}) \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} : a, b, c, d \in \mathbb{R}\right\} = \left\{\begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix} : a, c \in \mathbb{R}\right\}$$

and

$$\left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right) = M_n(\mathbb{R}) \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} : a, b, c, d \in \mathbb{R}\right\} = \left\{\begin{bmatrix} b & 0 \\ d & 0 \end{bmatrix} : a, c \in \mathbb{R}\right\}.$$

We have then that

$$\left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right) \oplus \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right) = M_n(\mathbb{R})$$

so $M_n(\mathbb{R})$ is in fact the direct sum of two ideals which are both generated by a nilpotent element.

□

Ex 5. Let k be a field, n a natural number, and A an element of $M_n(k)$. Consider the ring $R = k[A] = \{p(A) : p \in k[x]\}$ which is the smallest k-subalgebra of $M_n(k)$ containing A.

a) Give, in terms of the minimal polynomal $m_A(x)$ of A, a necessary and sufficient condition for R to be semi-simple.

b) Prove that the ring R is semi-simple if and only if the R-module k^n is semi-simple.

Proof.

a) We see that the kernel of the evaluation map $\phi : k[x] \to k[A]$ where $\phi(p(x)) = p(A)$ is the ideal $\{p \in k[x] : p(A) = 0\}$, which is generated by $m_A(x)$. Thus, we have that $k[A] \simeq k[x]/(m_A(x))$, meaning $k[A]$ is semi-simple if and only if $k[x]/(m_A(x))$ is. If we factor $m_A(x)$ into irreducible polynomials $\prod_i^k p_i(x)^{e_i}$, then by the Chinese Remainder Theorem, we have that

$$\frac{k[x]}{(m_A(x))} \simeq \frac{k[x]}{(p_1(x)^{e_1})} \oplus \frac{k[x]}{(p_2(x)^{e_2})} \oplus \cdots \oplus \frac{k[x]}{(p_k(x)^{e_k})}.$$

If $m_A(x)$ has no repeated factors, then $e_i = 1$ for all $1 \leq i \leq k$. As $p_i(x)$ is irreducible and $k[x]$ is a PID, the ideal $(p_i(x))$ is maximal, proving that $k[A]$ is the direct sum of fields, which are simple. This proves that $k[x]/(m_A(x))$ is semi-simple.

Now if $m_A(x)$ has a repeated factor, then $e_j > 1$ for some $1 \leq j \leq k$. For simplicity, we write $p_j(x)^{e_j}$ as simply $p(x)^e$. We note that $k[x]/(p(x)^e)$ is a commutative ring where $p(x) + (p(x)^e)$ is a non-zero nilpotent element. This proves that the ideal generated by $p(x) + (p(x)^e)$ is not a direct summand of $k[x]/(p(x)^e)$, proving $k[x]/(p(x)^e)$ is not semi-simple. Since $k[x]/(p(x)^e)$ is a direct summand of $k[x]/(m_A(x))$, $k[x]/(m_A(x))$ cannot be semi-simple either. Thus, $k[A]$ is semi-simple if and only if $m_A(x)$ contains no repeated factors.

b) We note that k^n can be considered as an $k[x]$-module via the action $p(x).(k_1, \ldots, k_n) = p(A)(k_1, \ldots, k_n)$. Using the direct sum decomposition of k^n via invariant factors, we have that

$$k^n \simeq \frac{k[x]}{(a_1(x))} \oplus \cdots \oplus \frac{k[x]}{(a_m(x))}$$

where $a_i(x)$ are polynomials such that $a_1 \mid a_2 \mid \ldots \mid a_m$ and $a_m(x) = \min_A(x)$.

Let R be semi-simple. By part (a), this means that $m_A(x)$ has no repeated factors. We see then that since $\min_A(x)$ has no repeated factors, neither do any of the invariant factors $a_i(x)$. Thus, by similar reasoning to the previous part using the Chinese Remainder Theorem, each $k[x]/(a_i(x))$ is semi-simple. This proves that k^n is the direct sum of semi-simple modules and is thus semi-simple.

Suppose k^n is semi-simple as an R-module and that the minimal polynomial has the form $m_A(x) = q(x)p(x)^2$ for some $p, q \in k[x]$. Consider the R-submodule $U = \ker(q(A)p(A))$ residing in k^n. We note that $U \neq k^n$, as that would imply that $\ker(q(A)p(A)) = k^n$ and that $q(A)p(A) = 0$, contradicting the minimality of $m_A(x)$. Since k^n is a semi-simple R-module, it must be that $k^n = U \oplus W$ where W is some R-submodule of k^n. Now let $w \in W$. Since

$$q(A)p(A)(p(A)w) = q(A)p(A)^2 w = m_A(A)w = 0w = 0,$$

we see that $p(A)w \in U$. As W is a R-submodule, we have that $p(A)w \in W$ as well. It must be then that $p(A)w = 0$ and therefore that $q(A)p(A)w = 0$. This means that $w \in U \cap W$, proving that $w = 0$. Since w was arbitrary, we have that $W = \{0\}$ which is a contradiction as $k^n \neq U \oplus \{0\}$. Thus, $m_A(x)$ must have no repeated factors.

□

Ex 6. For a prime number p, define $A = \mathbb{Z}[1/p] = \{m/p^n : a \in \mathbb{Z}, m \in \mathbb{N}_0\}$, which is a subgroup of $(\mathbb{Q}, +)$. Next, define the quotient $M = A/\mathbb{Z}$ considered as a $\mathbb{Z}$-module.

a) Show that every proper submodule of M is cyclic.

b) Show that M is an Artinian but not a noetherian $\mathbb{Z}$-module.

Proof.

a) Let N be a proper submodule of M. As the elements $\frac{1}{p^n} + \mathbb{Z}$ generate M and $N \neq M$, there is a least positive integer ℓ such that $\frac{1}{p^\ell} + \mathbb{Z}$ is not in N. Let L be the cyclic module $\left(\frac{1}{p^{\ell-1}} + \mathbb{Z}\right) = \mathbb{Z} \cdot \frac{1}{p^{\ell-1}} + \mathbb{Z} = \left\{\frac{m}{p^n} : n \geq \ell - 1\right\}$. We note that by the minimality of ℓ we know that $\frac{1}{p^{\ell-1}} \in N$, which means $L \subseteq N$.

Suppose then that N contained some element of the form $\frac{a}{p^k} + \mathbb{Z}$ not in L, that is where $\gcd(a, p^k) = 1$ and $k \geq \ell$. Since $\gcd(a, p^k) = 1$ this means that $1 = \alpha a + \beta p^k$ for some $\alpha, \beta \in \mathbb{Z}$. Since N is a $\mathbb{Z}$-module, we have that $\alpha \frac{a}{p^k} + \mathbb{Z} \in N$, which means

$$\alpha \frac{a}{p^k} + \mathbb{Z} = \alpha \frac{a}{p^k} + \beta + \mathbb{Z} = \alpha \frac{a}{p^k} + \frac{\beta p^k}{p^k} + \mathbb{Z} = \frac{\alpha a + \beta p^k}{p^k} + \mathbb{Z} = \frac{1}{p^k} + \mathbb{Z}$$

is an element of N. Thus, the element $p^{k-\ell} \frac{1}{p^k} + \mathbb{Z} = \frac{1}{p^\ell} + \mathbb{Z}$ is in N, which contradicts our assumption on ℓ. This proves that there is no element in $M \setminus L$, proving that M equals the cyclic submodule L.

b) Let M_i be the cyclic submodules $\left(\frac{1}{p^i} + \mathbb{Z}\right)$ that we identified in the previous part. We see that $M_i \subsetneq M_{i+1}$, which means that $M_1 \subsetneq M_2 \subsetneq \ldots$ is an ascending chain of submodules, proving that M is not Noetherian.

Let $N_1 \supseteq N_2 \supseteq \ldots$ be a descending chain of submodules. By the previous part all submodules are of the form $M_i = \left(\frac{1}{p^i} + \mathbb{Z}\right)$, thus $N_1 = M_{j_1}$ for some $j_1 \in \mathbb{N}$, $N_2 = M_{j_2}$ where $j_2 \leq j_1$, $N_3 = M_{j_3}$ where $j_3 \leq j_2$, and so on. This gives a decreasing sequence of natural numbers $\{j_i\}_{i \in \mathbb{N}}$. Any such sequence is eventually constant, which proves that for some $n \in \mathbb{N}$ we have that $N_n = N_i$ for all $i \geq n$. This proves that M is Artinian.

$\square$