

**Problem 1.** Prove that the following conditions on an  $R$ -module  $P$  are equivalent.

- (a)  $P$  is projective.
- (b)  $P$  is isomorphic to a direct summand of a free  $R$ -module.
- (c) If  $f : M \rightarrow P$  is surjective, then there exists an  $R$ -module homomorphism  $g : P \rightarrow M$  such that  $f \circ g = \text{id}_P$ .

*Proof.* First we will show that (a) implies (c). Let  $P$  be a projective module and  $f : M \rightarrow P$  be surjective. Then the identity map  $\text{id}_P$  fulfills the projective conditions and there exists a map  $g : P \rightarrow M$  such that  $f \circ g = \text{id}_P$ .

Next we will show that (c) implies (b). Let  $P$  be a module that fulfills property (c). Then let  $F$  be the free group with generators the elements of  $P$  and  $Q$  the free group with generators the relations of  $P$ . This creates a short exact sequence inclusion and projection of the form

$$0 \longrightarrow Q \xrightarrow{i} F \xrightarrow{\pi} P \longrightarrow 0$$

However condition (c) states that this sequence splits. As such  $F \cong Q \oplus P$  by the splitting lemma which implies that condition (b) holds.

Finally we show that (b) implies (a). Let  $F = P \oplus Q$  where  $F$  is free and let  $\pi : F \rightarrow P$  be the projection map. Then let  $f : P \rightarrow N$  and  $g : M \rightarrow N$  where  $g$  is surjective.

Let  $x$  be a generator of  $F$  and  $n_x$  as  $f \circ \pi(x) \in N$ . By surjectivity of  $g$  there exists  $m_x \in M$  such that  $g(m_x) = n_x$ . By the universal property of free modules there exists a unique map  $\tilde{f} : F \rightarrow M$  such that  $g \circ \tilde{f}(x) = f \circ \pi(x)$ . Now define  $\tilde{f} : P \rightarrow M$  by  $\tilde{f}(p) = \tilde{f}(p + 0_q)$ . Then

$$g \circ \tilde{f}(p) = f \circ \pi(p + 0_q) = f(p)$$

which completes the proof. □

**Problem 2.** Let  $F$  be a field and let  $R = F \times F$ . Let  $e = (1, 0) \in R$  and let  $P = Re$ . Show that  $P$  is a projective  $R$ -module, but that  $P$  is not a free  $R$ -module.

Note that  $R$  is a free module over itself. Since  $P \oplus R(0, 1) \cong R$  we have that  $P$  is projective by problem 1. However  $P$  is not free as if we let  $x, y \in F \setminus \{0\}$  then  $(0, y) \cdot (x, 0) = 0$  even though neither element is zero.

**Problem 3.** Show that if  $R$  is a semisimple ring, then so is  $M_n(R)$ .

*Proof.* By Theorem 7.1.28 from Adkins' book a ring is semisimple if and only if every  $R$ -module is semisimple. Since  $M_n(R)$  is an  $R$ -module it is semisimple.

Let  $R = \bigoplus_{i \in I} S_i$  be the decomposition of  $R$  into simple modules. As in the proof of that  $M_n(R)$  is simple if  $R$  is simple decompose  $M_n(R)$  into the direct sum of column vectors  $c_j(M_n(R))$  for  $0 < j \leq n$ . Since the  $M_n(S_i)$  are submodules of  $M_n(R)$  we can decompose the column as  $c_j(M_n(R)) = \bigoplus_{i \in I} (M_n(S_i) \cap c_j(M_n(R)))$  which are simple submodules. It then follows that  $M_n(R) = \bigoplus_{j=1}^n \bigoplus_{i \in I} (M_n(S_i) \cap c_j(M_n(R)))$  is a decomposition of  $M_n(R)$  into simple modules.

Therefore if  $R$  is semisimple then  $M_n(R)$  is semisimple. □

**Problem 4.** Show that if  $R$  is a semisimple ring and  $I$  is any ideal, then  $R/I$  is also semisimple.

*Proof.* Suppose that  $R = \bigoplus_{\alpha} M_{\alpha}$  is a semisimple ring and let  $\pi : R \rightarrow R/I$  be the projection map. Then  $\pi(M_{\alpha})$  is an ideal of  $R/I$  which implies that  $R/I \cong \bigoplus_{\alpha} \pi(M_{\alpha})$ . Moreover since the preimages of ideals are ideals the components  $\pi(M_{\alpha})$  must also be simple otherwise it would violate the simplicity of the  $M_{\alpha}$ s.

Therefore since the  $\pi(M_{\alpha})$ s are simple and ideals of  $R/I$  we have a decomposition of  $R/I$  into simple submodules as a  $R/I$  module. It then follows that  $R/I$  is a semisimple ring.  $\square$

**Problem 5 (7.2).** Let  $F$  be a field and let

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in F \right\}$$

be the ring of upper triangular matrices over  $F$ . Let  $M = F^2$  and make  $M$  into a (left)  $R$ -module by matrix multiplication. Show that  $\text{End}_R(M) \cong F$ . Conclude that the converse of Schur's lemma is false, i.e.,  $\text{End}_R(M)$  can be a division ring without  $M$  being a simple  $R$ -module.

*Proof.* Define a map  $\psi : F \rightarrow \text{End}_R(M)$  by  $\Psi(x) = \varphi_x$  where  $\varphi_x$  is defined as

$$\varphi_x \begin{pmatrix} d \\ e \end{pmatrix} = \begin{pmatrix} xd \\ xe \end{pmatrix}$$

Since the maps  $\varphi_x$  are equivalent to scalar multiplication by field elements it is clear from the definition that  $\varphi_x$  are in fact endomorphisms and respect the module structure. Now we will show that  $\psi$  is indeed an isomorphism.

The fact that the kernel of  $\psi$  is trivial follows from the fact that we are multiplying by field elements and as such there are no zero divisors. However to show that  $\psi$  is surjective we must utilize the fact that the endomorphisms play nice with the module structure.

First note that for  $\phi \in \text{End}_R(M)$  we have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \phi \begin{pmatrix} d \\ e \end{pmatrix} = \phi \left( \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d \\ e \end{pmatrix} \right)$$

If we split  $\phi$  into two pieces like so

$$\phi \begin{pmatrix} d \\ e \end{pmatrix} = \begin{pmatrix} \phi_1(d, e) \\ \phi_2(d, e) \end{pmatrix}$$

The module structure gives us two equations

$$a\phi_1(d, e) + b\phi_2(d, e) = \phi_1(ad + be, ce)$$

and

$$c\phi_2(d, e) = \phi_2(ad + be, ce)$$

Note that we could define a new endomorphism by swapping  $\phi_1$  and  $\phi_2$ . As such any statement we make about one applies to the other.

First if we let  $a = 1, b = c = 0$  in the latter equation this gives us that  $\phi_2(d, 0) = 0$ . Thus  $\phi_1$  and  $\phi_2$  are zero whenever the right coordinate are zero. Next let  $a = 1, b = -1, c = 0$  in the first equation and we get that  $\phi_1(d, e) = \phi_2(d, e)$ . Finally if we set  $b = 0, c = 1$  and let  $a \in F$  we get that we can pull constants out of the right term. Similarly setting  $a = 1, b = 0$  and letting  $c \in F$  we get that we can pull constants out of the right term. This implies that  $\phi_1$  and  $\phi_2$  are equivalent to multiplying by  $\phi(1, 1) = x$ . Thus the map  $\phi = \varphi_x$  and implying that  $\psi$  is surjective.

Therefore  $\psi$  is in fact an isomorphism and as such  $F \cong \text{End}_R(M)$ . Since  $M$  is not simple but it's endomorphisms form a field this is a counterexample to the converse of Schur's lemma.  $\square$

**Problem 6** (7.4). An  $R$ -module  $M$  is said to satisfy the descending chain condition (DCC) on submodules if any strictly decreasing chain of submodules of  $M$  of finite length.

- (a) Show that if  $M$  satisfies the DCC, then any nonempty set of submodules of  $M$  contains a minimal element.
- (b) Show that  $\ell(M) < \infty$  if and only if  $M$  satisfies both the ACC and DCC.

*Proof.* (a) Let  $\mathcal{M}$  be the set of submodules of  $M$  partially ordered by reverse inclusion. Since  $M$  satisfies DCC every chain in  $\mathcal{M}$  will have a maximal element and as such by Zorn's lemma there is a maximal element of  $\mathcal{M}$  that corresponds to a minimal submodule.

- (b) Suppose that  $\ell(M) < \infty$ . Then given a series of submodules  $\{N\}$  we can refine it to a composition series  $\{N'\}$  which will be of finite length. Since the length of  $\{N\}$  is less than that of  $\{N'\}$  it must also have finite length and as such has a minimal point and a maximal point. Since this holds for any series it follows that  $M$  satisfies both ACC and DCC.

Otherwise suppose that  $\ell(M) = \infty$  and let  $\{N\}$  be a composition series. Since all composition series have the same length this series must be infinite and as such  $M$  breaks either ACC or DCC.

□

**Problem 7** (7.5). Let

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b \in \mathbb{R}; c \in \mathbb{Q} \right\}$$

$R$  is a ring under matrix addition and multiplication. Show that  $R$  satisfies the ACC and DCC on left ideals but neither chain condition is valid for right ideals. Thus  $R$  is of finite length as a left  $R$ -module, but  $\ell(R) = \infty$  as a right  $R$ -module.

Starting with  $R$  as a left  $R$ -module we can construct a composition series as

$$\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \subset \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \subset \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

the quotients of which are isomorphic to  $\mathbb{R}, \mathbb{R}$ , and  $\mathbb{Q}$  respectively. Since we have a composition series of finite length it must be that  $\ell(R) < \infty$  as a left module and from the prior problem satisfies ACC and DCC.

However for  $R$  as a right module start with the submodule that has  $a = c = 0$  and  $b \in \mathbb{Q}$ . Multiplication looks like

$$\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} = \begin{bmatrix} 0 & cf \\ 0 & 0 \end{bmatrix}$$

Since  $f \in \mathbb{Q}$  it will be closed under the action of  $R$ . Then create an ascending series of submodules by adjoining roots of primes  $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \dots]$ . Since there are infinitely many primes this chain is infinite and as such  $\ell(R) = \infty$  as a right  $R$ -module.

For the descending series let  $\mathcal{B}$  be a basis for  $\mathbb{R}$  over  $\mathbb{Q}$ . Then do the same construction as above but instead each time take away an element of  $\mathcal{B}$ . This will create an infinite descending series.

**Problem 8** (7.11). Let  $F$  be a field, let  $V$  be a finite-dimensional vector space over  $F$ , and let  $T \in \text{End}_F(V)$ . We shall say that  $T$  is semisimple if the  $F[X]$ -module  $V_T$  is semisimple. If  $A \in M_n(F)$ , we shall say that  $A$  is semisimple if the linear transformation  $T_A : F^n \rightarrow F^n$  (multiplication by  $A$ ) is semisimple. Let  $\mathbb{F}_2$  be the field with 2 elements and let  $F = \mathbb{F}_2(Y)$  be the

rational function field in the indeterminate  $Y$ , and let  $K = F[X]/\langle X^2 + Y \rangle$ . Since  $X^2 + Y \in F[X]$  is irreducible,  $K$  is a field containing  $F$  as a subfield. Now let

$$A = C(X^2 + Y) = \begin{bmatrix} 0 & Y \\ 1 & 0 \end{bmatrix} \in M_2(F)$$

Show that  $A$  is semisimple when considered in  $M_2(F)$  but  $A$  is not semisimple when considered in  $M_2(K)$ . Thus, semisimplicity of a matrix is not necessarily preserved when one passes to a larger field. However, prove that if  $L$  is a subfield of the complex numbers  $\mathbb{C}$ , then  $A \in M_n(L)$  is semisimple if and only if it is also semisimple as a complex matrix.

From Adkins' book the linear transformation will be semisimple as described above if the minimal polynomial is the product of irreducible factors. The minimal polynomial for  $A$  is  $X^2 + Y$  which is irreducible for  $F$  but not irreducible for  $K$ .

*Proof.* Let  $\mathbb{L}$  be a subfield of  $\mathbb{C}$  and  $A \in M_n(\mathbb{L})$ . Then as above the matrix  $A$  is semisimple only when its minimal polynomial is the product of distinct irreducible factors. If  $A$  is irreducible as a complex matrix then it will definitely be irreducible as a matrix over  $\mathbb{L}$ . On the other hand if the minimal polynomial of  $A$  is the product of distinct irreducible factors over  $\mathbb{L}$  then it will factor into linear terms when we move to  $\mathbb{C}$  as  $\mathbb{C}$  is a perfect field.

Therefore a matrix is semisimple on a subfield of the complex numbers if and only if it is semisimple over the complex numbers themselves.  $\square$

**Problem 9** (7.17). (a) Prove that if  $R$  is a semisimple ring and  $I$  is an ideal, then  $R/I$  is semisimple.

(b) Show (by example) that a subring of a semisimple ring need not be semisimple.

*Proof.* (a) See problem 4.

(b) The rationals are simple, and as such semisimple, since they are a field. However the integers are a subring of the rationals and the integers are not semisimple.  $\square$