CHAPTER XVI

NONCOMMUTATIVE RINGS

1. Semisimplicity

Let A be a (not necessarily commutative) ring. As usual, "module" will mean "left A-module", but of course there is a parallel theory for right modules. A module M over A is said to be *semi-simple* if it can be decomposed as a direct sum of simple A-modules.

Examples.

If A is a field (or more generally a division ring), simple A-modules are one-dimensional vector spaces, and there is only one such up to isomorphism. Since every vector space is a direct sum of one-dimensional subspaces, every module is semi-simple.

For $A = \mathbf{Z}$, a module is simple if and only if it is cyclic of prime order. Hence, most $\mathbf{Z}$-modules are not semi-simple.

We shall see other more typical examples below.

Clearly, any direct sum of semi-simple modules is semi-simple.

PROPOSITION. *Let A be a ring and let M be an A-module. The following are equivalent.*
(i) M is semi-simple.
(ii) M is a sum (not necessarily direct) of a family of simple submodules.
(iii) Every A-module epimorphism $M \to L$ splits.
(iv) Every submodule N of M is a direct summand of M.

PROOF. (ii) $\Rightarrow$ (i). Suppose $M = \sum_{i\in I} M_i$. Consider subsets $J \subseteq I$ such that $\sum_{j\in J} M_j$ is a direct sum, i.e.,

$$M_i \cap \sum_{\substack{j\in J \\ j\neq i}} M_j = \{0\} \qquad \text{for each } i \in J.$$

If we order these sets by inclusion, it is not hard to see that they form an inductively ordered set. (Prove it!) Hence, by Zorn's Lemma, there is a maximal such subset J. If $J = I$ we are done, so assume $J \subsetneqq I$. Let $M' = \sum_{j\in J} M_j$. Consider M_i for $i \in I - J$. $M_i \cap M'$ is a submodule of M_i so by simplicity,

$$M_i \cap M' = \begin{cases} \{0\} \\ \text{or} \\ M_i \end{cases}$$

If $M_i \cap M' = \{0\}$, it is easy to see that $\sum_{j\in J} + M_i$ is a direct sum which contradicts the maximality of J. Hence, $M_i \cap M' = M_i$ which implies $M_i \subseteq M'$. It follows that $M = \sum_{i\in I} \subseteq M'$ so the two are equal. Since M' is a direct sum of simple modules we are done.

(i) $\Rightarrow$ (iv). Assume $M = \sum_{i\in I} M_i$ is a direct sum with each M_i simple. Let N be a submodule of M. Using Zorn's Lemma again, choose $J \subseteq I$ maximal such that $M' = N + \sum_{j\in J} M_j$ is a direct sum. Argue as above. For each $i \in I$, $M_i \cap M' = \{0\}$ implies that $M' + M_i = N + \sum_{j\in J} M + M_i$ is direct, so we conclude instead that $M_i \subseteq M'$. Hence, $M = M'$.

(iv) $\Leftrightarrow$ (iii). Consider the short exact sequence

$$0 \to N \xrightarrow{g} M \xrightarrow{f} L \to 0$$

where either $N = \operatorname{Ker} f$ if f is assumed given or $L = \operatorname{Coker} g$ if g is assumed given. Since the sequence splits at one end if and only if it splits at the other, the equivalence is established.

(iii) & (iv) $\Rightarrow$ (ii). If $M = \{0\}$, then M is an empty sum of simple submodules. Suppose that $M \neq \{0\}$. First, we note that any submodule M' of M or quotient module M'' of M also satisfies (iii) and (iv). For example, if $f : M \to M''$ is an epimorphism and $g : M'' \to L$ is an epimorphism from that quotient, then by (iii) the epimorphism $gf : M \to L$ splits, so there is a homomorphism $h : L \to M$ such that $hgf = Id_L$. It follows that $hg : L \to M''$ splits f. The argument for submodules is similar. Next we show that (iii) & (iv) together imply that M (also any submodule of M) has at least one simple submodule. To see this choose $x \neq 0 \in M$ and let $g : A \to M$ be defined by $g(a) = ax$. Then $\operatorname{Ker} g$ is a left ideal of A so it is contained in a maximal left ideal L. $A/\operatorname{Ker} g \cong Ax$ which is a submodule of M. Hence, by (iii) the epimorphism $A/\operatorname{Ker} g \to A/L$ splits, so $Ax \cong A/\operatorname{Ker} g$ contains a direct summand isomorphic to the simple module A/L. Consider finally the submodule N of M which is the sum (not generally direct) of all the simple submodules of M. (In general, this submodule is called the *socle* of M.) By (iv), $M = N \oplus M'$ where M' is a complementary submodule. If $M' \neq \{0\}$, then it contains a simple submodule P which is not contained in N. Since by definition N contains all simple submodules of M, we conclude $M = N$.

Corollary. *If M is a semi-simple A-module, then every submodule and every quotient module of M is semi-simple.*

Proof. As we remarked in the above proof, properties (iii) and (iv) are inherited by sumodules and quotient modules.

We say that the *ring* A is *semi-simple* if it is semi-simple as a left module over itself, that is

$$A \cong \oplus_{i \in I} L_i$$

where each L_i is a simple submodule of A, i.e., a minimal left ideal of A. As before, we should distinguish between "left semi-simple" and "right semi-simple", but we shall see below that the two notions are the same. Note that if A is semi-simple, then every (left) A-module is semi-simple since it is a quotient of a free module, and a free module is semi-simple because it is a direct sum of copies of A. Hence, any short exact sequence of A-modules

$$0 \to M' \to M \to M'' \to 0$$

splits. It follows that every A-module is a direct summand of a free A-module. In general, modules with this property are called *projective*. Hence, every module over a semi-simple ring is projective.

Projective modules share a mapping property previously stated for free modules.

Proposition. . *Let A be a ring and let P be a left A-module. The following are equivalent.*

(i) P is a direct summand of a free module.

(ii) If $f : M \to M''$ is an epimorphism, and $g'' : P \to M''$ is any module homomorphism, then there exists a module homomorphism $g : P \to M$ such that

$$\begin{array}{ccc} & & P \\ & \swarrow^{g} & \downarrow g'' \\ M & \underset{f}{\twoheadrightarrow} & M'' \end{array}$$

commutes.

(iii) Every epimorphism $M \to P$ splits.

Proof. (ii) $\Rightarrow$ (iii) is clear by taking $g = \mathrm{Id} : P \to P$.

(iii) $\Rightarrow$ (i) since P is certainly a quotient of a free module.

(i) $\Rightarrow$ (ii) is left as an exercise for the student.

A module Q is called *injective* if it satisfies the dual of the condition stated in (ii). It is not very hard to see that that condition is equivalent to the assertion that every monomorphism $Q \to M$ splits. (There is no simple analogue of (i). However, it is true that every module is isomorphic to a submodule of an injective module.)

COROLLARY. *A ring A is semi-simple if and only if every A-module is projective.*

PROOF. We already noted that if A is semi-simple, then every module is projective. Conversely, suppose every module is projective. In particular if $A \to M$ is any epimorphism, it splits by (iii) above. Hence A is semisimple by (iii) of the Proposition characterizing semi-simple modules.

PROPOSITION. *A ring A is semi-simple if and only if every A-module is injective.*

PROOF. Exercise. Use the fact that "everything splits."

Exercises.

1. Prove (i) $\Rightarrow$ (ii) in the proposition showing that the three possible definitions of projective module are equivalent.

2. Let A be a ring and let Q be an A-module. Prove that (i) and (ii) below are equivalent. (In either case, we say Q is *injective*.

(i) If $f : M' \to M$ is a monomorphism, and $g' : M' \to Q$ is any module homomorphism, then there exists a module homomorphism $g : M \to Q$ such that $gf = g'$.

(ii) Every monomorphism $f : Q \to M$ splits, i.e., $\exists h : M \to Q$ such that $hf = \mathrm{Id}_Q$.

Hint: To prove that (ii) $\Rightarrow$ (i), let $N = (Q \oplus M)/\{(g(x), -f(x)) \,|\, x \in M'\}$ and construct a commutative diagram

$$\begin{array}{ccc} Q & \xrightarrow{F} & N \\ {\scriptstyle g}\uparrow & & \uparrow{\scriptstyle H} \\ M' & \xrightarrow[f]{} & M \end{array}$$

and show that the F you define is a monomorphism. (N is called a pushout.)

3. Show that a ring A is semi-simple if and only if every A-module is injective.

2. Some important semi-simple rings

We shall shortly prove one of Wedderburn's fundamental theorems: a semi-simple ring is isomorphic to a direct product of rings each of which is a matrix ring $M_n(D)$ over a division ring D. This is a surprising result because it shows us that a relatively abstract definition leads to a reasonably concrete kind of object. Before proving this theorem of Wedderburn, we show how one may construct semi-simple rings.

Matrix rings. Let D be a division ring. If you go back and examine the basic theorems of linear algebra over fields, you will discover that those theorems did not for the most part depend on the commutativity of the field. For example, every D-module M has a basis, and the number of elements in a basis is independent of the basis. Hence, we can define $\dim_D M$ as that number. However, if D is not commutative, we must distinguish between left and right modules. Moreover, it is possible for the division ring D to act on M on both the left and the right so that the two actions are consistent but with the dimension of the left module different from the dimension of the right module. (In fact, P. M. Cohn has found an example of division rings $D \subseteq D'$ with the left dimension of D' over D equal to 2 and the right dimension infinite.)

Suppose M is a finite dimensional left D-module, and $\{x_1, \ldots, x_n\}$ is a basis. For each $f \in \mathrm{Hom}_D(M, M)$ we have

$$f(x_i) = \sum_{j=1}^{n} a_{ij} x_j, \qquad i = 1, \ldots, n.$$

(Note that we use a_{ij} instead of a_{ji} in the sum.) Thus, we may associate with f the $n \times n$ matrix A with entries in D. Some simple calculation shows that $f \mapsto A$ preserves sums but that it *reverses* products — where the product of matrices is calculated in the usual way except that you have to be careful about the order. Hence, we get an anti-isomorphism of rings

$$\mathrm{Hom}_D(M, M) \to M_n(D).$$

One way to deal with the problem of anti-isomorphisms is to introduce the concept of the *opposite* ring. If R is any ring, R^{op} is the ring with the same additive group structure but with the product reversed (so R and R^{op} are anti-isomorphic.) With this notation we may say

$$\mathrm{Hom}_D(M, M) \cong M_n(D)^{op} \cong M_n(D^{op}).$$

(How is the second isomorphism defined?)

If M were a *right* D-module instead, then we would write

$$f(x_i) = \sum_{j=1}^{n} x_j a_{ji}, \qquad i = 1, \ldots, n.$$

In this case the correspondence between endomrophisms and matrices would be an isomorphism of rings

$$\mathrm{Hom}_D(M, M) \cong M_n(D).$$

It is easy to see that the ring $M_n(D)$ is semi-simple if D is a division ring. Just let L_j be the set of $n \times n$ matrices which are zero everywhere except possibly in the jth column. If you multiply such a matrix on the left by any $n \times n$ matrix, you again get such a matrix, so L_j is a left ideal in $M_n(D)$. If the matrix $A \neq 0 \in L_j$, then by multiplying A on the left by suitable matrices you can obtain the matrices $E_{ij}, i = 1, 2, \ldots, n$. Hence, any single nonzero element of L_j generates it as a module over $M_n(D)$ from which it follows easily that L_j is a simple left submodule of $M_n(D)$. Since $M_n(D) = \oplus_j L_j$, it follows that $M_n(D)$ is semi-simple. If we had used rows instead of columns, we could have showed that $M_n(D)$ is a direct sum of simple right submodules. Hence, $M_n(D)$ is semi-simple by both the right hand and left hand theories. It is not hard to see that $M_n(D)$ is both noetherian and artinian. For, it is a (left or right) free module over D of rank n^2, and, by finite dimensionality, there are no infinite chains of D-submodules. We shall see later that any semi-simple ring (with identity) is both artinian and noetherian in any case.

Recall that we proved earlier in an exercise that the ring $M_n(k)$ is simple if k is a field. Essentially the same proof works for matrix rings over division rings. Hence, $M_n(D)$ (or equivalently $\mathrm{Hom}_D(M, M)$ is both simple and semi-simple. As we shall see below, this is no accident, and of course the choice of language suggests the relation: semi-simple rings are direct products of simple rings.

Group rings. Let k be a field, and let G be a group, and denote by kG the group ring of G as defined in the exercises.

THEOREM (Maschke). *Let k be a field, G a finite group and suppose the characteristic of k does not divide $|G|$. Then kG is semi-simple.*

PROOF. Let $f : M \to M''$ be an epimorphism of kG-modules. If we view f just as an epimorphism of k-modules, then its splits because every field is semi-simple. Choose $h : M'' \to M$ a k-module homomorphism such that $fh = \mathrm{Id}_{M''}$. Define $j : M'' \to M$ by

$$j(m'') = \frac{1}{|G|} \sum_{x \in G} x^{-1} h(xm'').$$

Then, j is a kG-module homomorphism. For, if $y \in G$, then

$$\begin{aligned} j(ym'') &= \frac{1}{|G|} \sum_{x \in G} x^{-1} h(xym'') \\ &= \frac{1}{|G|} y \sum_{x \in G} y^{-1} x^{-1} h(xym'') \\ &= y \frac{1}{|G|} \sum_{z \in G} z^{-1} h(zm'') = yj(m''). \end{aligned}$$

Since, j is certainly a k-module homomorphism, it follows that it is a kG-module homomorphsim. Also, $fj = \mathrm{Id}_{M''}$. For,

$$\begin{aligned} f(j(m'')) &= \frac{1}{|G|}\sum_{x\in G} x^{-1}f(h(xm'')) \\ &= \frac{1}{|G|}\sum_{g\in G} x^{-1}xm'' \\ &= \frac{1}{|G|}|G|m'' = m''. \end{aligned}$$

It follows that every epimorphism splits.

PROPOSITION. *Let A be a semi-simple ring.*
(i) A is a direct sum of finitely many simple submodules.
(ii) A is artinian and noetherian.

PROOF. (ii) follows from (i) since any simple A-module is certainly artinian (noetherian), and any finite direct sum of artinian (noetherian) modules is artinian (noetherian).

To prove (i) suppose that

$$A = \oplus_{i\in I} L_i$$

where each L_i is a minimal left ideal (i.e. simple submodule.) Then

$$1 = \sum_{i\in I} e_i$$

where $e_i \in L_i$, and only finitely many $e_i \neq 0$. Let

$$J = \{j \in I \,|\, e_j \neq 0\}.$$

It follows that each $a \in A$ may be written

$$a = \sum_{i\in J} ae_i$$

and since $ae_i \in L_i$, it follows that $A = \oplus_{i\in J} L_i$.

The following theorem tells us that we can always get a semi-simple ring by factoring out the radical of an artinian ring.

THEOREM. *Let A be a ring. Then A is semi-simple if and only if it is artinian and* $\mathrm{rad}(A) = \{0\}$.

PROOF. Suppose A is semi-simple. We saw above that it is artinian, and it is a direct sum $\oplus_{i\in J} L_j$ of finitely many minimal ideals L_j. It is easy to see that for each $j \in J$, $M_j = \sum_{i\neq j} L_i$ is a maximal left ideal of A and $\bigcap_j M_j = \{0\}$. It follows that the intersection of all maximal left ideals is trivial so $\mathrm{rad}(A) = \{0\}$.

Conversely, suppose A is artinian, and $\mathrm{rad}(A) = \{0\}$. Consider left ideals L of A such that $A = S \oplus L$ where S is a semi-simple left submodule of A. For example, take $L = A, S = \{0\}$. Since A is artinian, there is a minimal such L. We shall show that if $L \neq \{0\}$, then it can be further decomposed $L = M \oplus L'$ where M is a minimal left ideal and L' is a left ideal. Since $A = S \oplus M \oplus L'$ and $S \oplus M$ is semisimple, since L' is strictly contained in L, this leads to a contradiction.

Suppose $L \neq \{0\}$ and let M be any minimal left ideal (simple left submodule) contained in L. (Invoke the minimum principle.) M^2 is a left submodule of M so $M^2 = \{0\}$ or M. In the former case, M is a nilpotent left ideal so it is contained in $\mathrm{rad}(A) = \{0\}$, i.e. $M = \{0\}$. It follows that $M^2 = M$. Choose $x \in M$ such that $Mx \neq \{0\}$. Again, Mx is a submodule of M so by simplicity $Mx = M$. Hence, there is an $e \in M$ such that $ex = x$. It follows that $e^2x = ex$ or $(e^2 - e)x = 0$. However,

$$M_1 = \{z \in M \,|\, zx = 0\}$$

is an ideal contained in M, and $M_1 \neq M$ (since $Mx \neq \{0\}$) so $M_1 = \{0\}$. Since $e^2 - e \in M_1$, it follows that

$$e^2 = e.$$

$e \in M$ is called an *idempotent*.

We have $1 = e + (1 - e)$. Hence, each element $a \in L$ may be written $a = ae + a(1 - e)$. Thus, $L \subseteq Le + L(1-e)$. On the other hand, Le is contained in M and $e = e^2 \in Le$ is notrivial so $Le = M$. Also, $L(1 - e) \subseteq L + Le \subseteq L$ (since $e \in L$). It follows that

$$L = M + L' \qquad \text{where } L' = L(1 - e).$$

Finally, the sum is direct since if $ae = b(1 - e)$, then

$$ae = ae^2 = b(1 - e)e = b(e - e^2) = 0.$$

Exercises.

1. Let $\mathbf{H}$ be the algebra of quaternions defined as follows. $\mathbf{H} = \mathbf{R} \times \mathbf{V}$ where $\mathbf{V} \cong \mathbf{R}^3$ is the real vector space of ordinary vectors in 3-space. Then $\mathbf{H} \cong \mathbf{R}^4$ as a real vector space. Introduce the following product in $\mathbf{H}$.

$$(a, u)(b, v) = (ab - u \cdot v, av + bu + u \times v).$$

(a) Verify the associative law in $\mathbf{H}$. You may use whatever identities for the vector product $u \times v$ you can find in elementary text books on vector algebra.

Assume that $\mathbf{H}$ becomes an algebra over $\mathbf{R}$ with the above product and its underlying vector space structure. Note that $\mathbf{R}$ is imbedded in $\mathbf{H}$ as the set of elements of the form $(a, 0)$.

(b) For $\alpha = (a, u)$ define $\overline{\alpha} = (a, -u)$. Show that $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$.

(c) For $\alpha = (a, u)$ define $\|\alpha\| = \sqrt{a^2 + |u|^2}$ where $|v|$ is the ordinary Euclidean length of the vector v. Show that $\|\alpha\beta\| = \|\alpha\| \, \|\beta\|$. Hint: Show that $\alpha\overline{\alpha} = (\|\alpha\|^2, 0)$.

(d) Conclude that every nonzero element of $\mathbf{H}$ is invertible.

2. Show that the association $f \mapsto (a_{ij})$ defined in the text reverses products. What would go wrong if we tried to define the matrix of f in the usual manner by $f(x_i) = \sum_j a_{ji}x_j$? Check that if M is a right D-module, then using the latter formula instead preserves products.

3. Let k be a field and let $A = k^n$ be the direct product of n copies of k viewed as a ring with component operations. (That is the product in the category of rings.) Show that every ideal of A is obtained by taking the set of all elements whose coordinates at a specified set of indices is 0. Show that the Jacobson radical of A is trivial.

4. Let k be a field and let A be the subring of $M_n(k)$ consisting of all matrices with zeroes below the main diagonal.

(a) Show that A is both noetherian and artinian.

(b) Show that the Jacobson radical of A is the ideal N of all matrices which are zero on the main diagonal and also below the main diagonal. Hint: Show that A/N is isomorphic to the direct product k^n.

3. Wedderburn's First and Second Theorems

THEOREM (Wedderburn). *A semi-simple ring A is a direct product of simple artinian rings.*

PROOF. Since A is semi-simple, we have

$$A = \sum_i L_i$$

where each L_i is a minimal left ideal, and, as we noted above, the sum is finite. For each pair L_i and L_j, L_iL_j is also a left ideal and it is contained in L_j. Hence $L_iL_j = \{0\}$ or L_j. Suppose $L_iL_j = L_j$. Then

there is an $x \in L_j$ such that $L_i x \neq \{0\}$ so $L_i x = L_j$. (In this case, note for future reference that $a \mapsto ax$ is an A-isomorphism between L_i and L_j.) It is not hard to check that the relation $L_i L_j \neq \{0\}$ defines an equivalence relation on the set of ideals L_i. For, $L_i^2 \neq \{0\}$ since $\mathrm{rad}(A) = \{0\}$ as discussed earlier; hence, $L_i^2 = L_i$. Also, if $L_i L_j \neq \{0\}$, then $L_j L_i L_j = L_j L_j \neq \{0\}$, so $L_j L_i \neq \{0\}$. Finally, if $L_i L_j \neq \{0\}$ and $L_j L_k \neq \{0\}$, then $L_i L_k = L_i L_j L_k = L_j L_k \neq \{0\}$.

Partition the set of minimal left ideals L_i into equivalence classes and for each class form the sum A' of the L_i in that class. Then A' is a 2-sided ideal in A. For, A' is a left ideal since it is a sum of left ideals. On the other hand, if L_i is any of the minimal left ideals in the decomposition of A, then $A' L_i = \{0\}$ if L_i is not in the equivalence class defining A', and $A' L_i = L_i \subseteq A'$ if L_i is in that equivalence class. Hence, since $A = \sum_i L_i$, $A' A \subseteq A'$, and A' is also a right ideal.

Suppose then that we number these ideals $A_1, A_2, \ldots, A_r$ so that we have a direct sum decomposition (as left A-modules)

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_r.$$

Note that since $L_i L_j = \{0\}$ for L_i and L_j in different classes, it follows that $A_i A_j = \{0\}$ for $i \neq j$, i.e., multiplication as well as addition in A is done componentwise. It follows that *in the category of rings*

$$A \cong A_1 \times A_2 \times \cdots \times A_r$$

except for one small sticking point: we don't know that the ideals A_i are rings until we show they have multiplicative identitites. To deal with this point, write

$$1 = e_1 + e_2 + \cdots + e_r$$

where $e_i \in A_i$. From $1^2 = 1$ and $e_i e_j = 0$, it follows that each e_i is idempotent, i.e., $e_i^2 = e_i$. If $a \in A_i$, then

$$a = a1 = ae_1 + ae_2 + \cdots + ae_i + \cdots + ae_r = ae_i$$

so that e_i is a right identity on A_i. An analagous argument shows that it is a left identity.

Each A_i is an epimorphic image of A in the category of rings so it follows that it is artinian. Hence, to complete the proof we need only show that each A_i is simple. Write $A' = A_i$ to simplify the notation. Then as above

$$A' = \oplus_j L_j$$

where the L_j are minimal left ideals and $L_j L_k = L_k$ for each j, k. Let I be a 2-sided ideal of A'. Then IL_j is a left ideal contained in L_j so it is $\{0\}$ or L_j. If it vanishes for one L_j, it vanishes for all since $IL_k = IL_j L_k$. In that case $I = IA' = \sum IL_j = \{0\}$. Otherwise, $IL_j = L_j$ for each j. However, since I is a two sided ideal $IL_j \subseteq I$ so every $L_j \subseteq I$. Hence, $A' = \sum L_j \subseteq I$ so $I = A'$.

We shall show shortly that any simple artinian ring is a matrix ring over a division ring, hence it is semi-simple. It follows that any direct product of simple artinian rings is semi-simple.

PROPOSITION (Schur's Lemma). *Let A be a ring and let M and N be simple A-modules.*
(i) Any module homomorphism $f : M \to N$ is either 0 or an isomorphism.
(ii) $\mathrm{Hom}_A(M, M)$ *is a division ring.*

PROOF. (i) is clear since $\mathrm{Im}\, f$ is a submodule of N so $\mathrm{Im}\, f = \{0\}$ or N. In the first case $\mathrm{Ker}\, f = N$, and in the second case $\mathrm{Ker}\, f \neq N$ so $\mathrm{Ker}\, f = \{0\}$. Hence, in the second case f is an isomorphism.
(ii) follows from (i) by taking $M = N$.

Let M be a left A-module, and let $D = \mathrm{Hom}_A(M, M)$. For $\alpha \in D$, write $\alpha x = \alpha(x)$ for $x \in M$. In this way, we may treat M as a left D-module. For $a \in A$, define $\lambda_a : M \to M$ by $\lambda_a(x) = ax$. $\lambda_a \in \mathrm{Hom}_D(M, M)$. For,

$$\lambda_a(\alpha x) = a(\alpha x) = a\alpha(x) = \alpha(ax)$$

since $\alpha \in \mathrm{Hom}_A(M, M)$)

$$= \alpha(\lambda_a(x)) = \alpha\lambda_a(x).$$

Define $\phi : A \to \mathrm{Hom}_D(M, M)$ by $\phi(a) = \lambda_a$. ϕ is easily seen to be a ring homomorphism.

THEOREM (Rieffel). *Suppose A is a simple ring, $M \neq \{0\}$ is a left ideal in A, and $D = \mathrm{Hom}_A(M, M)$. Then $\phi : A \to \mathrm{Hom}_D(M, M)$ as defined above is an isomorphism.*

PROOF. Since A is simple, $\mathrm{Ker}\,\phi = \{0\}$; hence we need only show that ϕ is an epimorphism.

First note that $\phi(M)$ is a left ideal in $\mathrm{Hom}_D(M, M)$. For, if $u \in M$ and $g \in \mathrm{Hom}_D(M, M)$, then

$$(g\phi(u))(x) = g(\phi(u)(x)) = g(ux).$$

However, the mapping $u \mapsto ux$ is an A-module endomorphism of M since

$$au \mapsto (au)x = a(ux).$$

Hence, $\exists \alpha \in D = \mathrm{Hom}_A(M, M)$ such that $\alpha(u) = xu$ for $u \in M$. Thus

$$(g\phi(u))(x) = g(ux) = g(\alpha u) = \alpha g(u) = g(u)x = \lambda_{g(u)}(x) = \phi(g(u))(x),$$

so that $g\phi(u) = \phi(g(u))$.

Consider MA. Since M is a left ideal and A is a 2-sided ideal, MA is a 2-sided ideal of A. It is not trivial so by simplicity, $MA = A$. Hence, $\phi(A) = \phi(MA) = \phi(M)\phi(A)$. Since $\phi(M)$ is a left ideal in $\mathrm{Hom}_D(M, M)$, it follows that $\phi(A)$ is a left ideal in that ring. Since $1 \in \phi(A)$, $\phi(A) = \mathrm{Hom}_D(M, M)$.

COROLLARY. *Let A be a simple artinian ring, M a minimal left ideal of A, and $D = \mathrm{Hom}_A(M, M)$. Then*

$$A \cong \mathrm{Hom}_D(M, M) \cong M_n(D^{op})$$

where $n = \dim_D M$. Hence, A is a simple artinian ring if and only if it is isomorphic to a matrix ring over a division ring.

PROOF. Use the following lemma.

LEMMA. *Let D be a division ring and let M be a D-module. Then $\mathrm{Hom}_D(M, M)$ is artinian if and only if $\dim_D M < \infty$.*

PROOF OF LEMMA. If $\dim_D M = n < \infty$, then as we saw earlier, $\mathrm{Hom}_D(M, M) \cong M_n(D^{op})$ and we know the latter ring is artinian. On the other hand, if M is infinite dimensional over D, then we may form an ascending chain of subspaces

$$M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_k \subsetneqq \ldots$$

Let $L_k = \{f \in \mathrm{Hom}_D(M, M) \mid f(M_k) = 0\}$, It is easy to see that L_k is a left ideal and $L_{k+1} \supsetneqq L_k$ since we can always find a D-linear function which vanishes on a basis for M_k, but does not vanish on M_{k+1}. So $\mathrm{Hom}_D(M, M)$ is not artinian.

Since $M_n(D)$ —with D a division ring—is semi-simple either as a left or a right module, it follows that any direct product of matrix rings (i.e. simple artinian rings) is semi-simple. Hence, we can say

THEOREM. *Let A be a ring. A is left semi-simple if and only if it is right semi-simple if and only if it is isomorphic to a finite direct product of matrix rings $M_n(D)$ over division rings D.*

Note that this result assures us that a semi-simple ring is both left and right artinian and also left and right noetherian. In general, however, a ring could be left artinian (noetherian) without being right artinian (noetherian). [For example, let D be a division ring and M a D-bimodule which has finite dimension as a left D-module and infinite dimension as a right D-module. (As mentioned earlier, P. M. Cohn has constructed such an example.) Let $A = D \oplus M$, and make A into a ring by using the product

$$(a, m)(a', m') = (aa', am' + ma').$$

Then any left D-subspace of M is a left A-submodule and similarly for right subspaces and right A-submodules. It follows that A is left artinian and noetherian but it is not right artinian or right noetherian.]

THEOREM. *Let A be a ring. If A is left (right) artinian, then it is left (right) noetherian.*

PROOF. We do the left handed case. The right handed case is similar.
Let $J = \mathrm{rad}(A)$. Then since J is nilpotent, we have a tower

$$A \supseteq J \supseteq J^2 \supseteq \cdots \supseteq J^k \supseteq J^{k+1} = \{0\}$$

of ideals. Since A is artinian, so is A/J, and since $\mathrm{rad}(A/J) = \{0\}$, it follows that A/J is semisimple. Consider the left A-modules J^i/J^{i+1}. In fact, J^i/J^{i+1} is an A/J-module and the action of A factors through the action of A/J. Since A is left artinian as an A-module, so is J^i/J^{i+1}. Since it is an $A/J - module$, it breaks up as a direct sum of simple submodules. If that sum were not finite, then it is easy to see that J^i/J^{i+1} could not be artinian. Hence, J^i/J^{i+1} is a direct sum of finitely many simple A/J (or A) submodules, so it is noetherian. Thus all the quotients in the above tower are noetherian, so A is also noetherian as a module over itself.

Question: Each J^i/J^{i+1} is also a right A/J-module. Why can't we also conclude it is right noetherian?

Exercises.

1. Let A be a commutative artinian ring. Suppose

$$1 = e_1 + \cdots + e_r$$

is a decomposition of 1 into primitive orthogonal idempotents. Show that any idempotent of A is of the form

$$e = e_{i_1} + \cdots + e_{i_k}$$

for some subset $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}$.

4. Uniqueness questions for semisimple rings

THEOREM. *Let A be a simple artinian ring. All simple left A-modules M are isomorphic. In particular, if $M_n(D) \cong M_{n'}(D')$ where D and D' are division rings then $n = n'$ and $D \cong D'$.*

PROOF. Let M be a simple A-module, and let L be any minimal left ideal of A. Consider $LM \subseteq M$. LM is an A-submodule of M so $LM = \{0\}$ or $LM = M$. If $LM = \{0\}$, then $L \subseteq \mathrm{Ann}_A(M) = \{0\}$ since A is simple. Hence, $LM = M$. Choose $x \in M$ such that $Lx \neq \{0\}$. Then $Lx = M$. Also, the mapping $a \mapsto ax$ provides an A-homomorphism $L \to M$, and by the above remarks, that homomorphism is an isomorphism. Hence, any simple A-module M is isomorphic to L.

To prove the second statement, let $A = M_n(D) \overset{\phi}{\cong} A' = M_{n'}(D')$, let L be the minimal left ideal of A consisting of matrices which vanish except in the first column, and let L' be the corresponding minimal left ideal of A'. Using the isomorphism ϕ, we may view L' also as an A-module. Thus there is an isomorphism $f : L \to L'$ of simple modules. It is not hard to see that $D = \mathrm{Hom}_A(L, L)$, and similarly $D' = \mathrm{Hom}_{A'}(L', L') = \mathrm{Hom}_A(L', L')$. Consider the map $\mathrm{Hom}(L, L) \to \mathrm{Hom}(L', L')$ defined by $\alpha \mapsto f\alpha f^{-1}$. It is not hard to check that this map carries A-endomorphisms of L into A-endomorphisms (i.e., A'-endomorphisms) of L'. Also, it is one-to-one and onto so it yields an isomorphism $\mathrm{Hom}_A(L, L) \cong \mathrm{Hom}_{A'}(L', L')$. On the other hand, it is not hard to see by matrix manipulation that every element of $\mathrm{Hom}_A(L, L)$ is of the form ρ_α for $\alpha \in D$ where $\rho_\alpha(x) = x\alpha$. Also, it is not hard to see that $\rho : D \to \mathrm{Hom}_A(L, L)$ is a one-to-one map which preserves sums but *reverses* products so it yields an isomorphism $D^{op} \cong \mathrm{Hom}_A(L, L)$. Similarly, $D'^{op} \cong \mathrm{Hom}_A(L', L')$, so it follows that $D \cong D'$. Finally, it is not hard to see that $f : L \to L'$ carries the structure of L as a *right* vector space over D into L' viewed as as a right vector space over D', and $n = \dim_D L = \dim_{D'} L' = n'$.

THEOREM. *Let $A = A_1 \oplus A_2 \oplus \cdots \oplus A_r$ where each A_i is a minimal 2-sided ideal. Any two such decompositions are the same except for the order of the summands.*

PROOF. Let B be any 2-sided ideal of A. For each i, we have $BA_i \subseteq A_i$. By minimality, $BA_i = \{0\}$ or A_i. Thus, $B = BA = \sum_{i=1}^{r} BA_i = \sum' A_i$ where the last sum is taken over the subset of those i for which $BA_i = A_i$. It follows that every 2-sided ideal of A is obtained by summing some subset of the set of the ideals $A_1, \ldots, A_r$. Thus, we know all possible minimal 2-sided ideals of A.

Note that the minimal 2-sided ideals A_i are actually simple rings and

$$A \cong A_1 \times \cdots \times A_r$$

in the category of rings. As in previous arguments, $A_iA_j = \{0\}$ if $i \neq j$ and if $1 = e_1 + \cdots + e_r$ with $e_i \in A_i$, then e_i is the identity of A_i. However, A_i is *not* generally *a subring* of A since its identity $e_i \neq 1 \in A$.

COROLLARY. *The decomposition of a semi-simple ring as a direct product of simple rings is unique up to isomorphism.*

PROOF. If $A = A_1 \times A_2 \times \cdots \times A_r$, then $A_i' = \{0\} \times \{0\} \times \ldots A_i \times \{0\}$ is a minimal 2-sided ideal of A and $A = A_1' \oplus \cdots \oplus A_r'$.

COROLLARY. *Let A be a left artinian ring. Up to isomorphism, there are only finitely many simple A-modules.*

PROOF. We mentioned in the discussion of the radical that the simple A-modules are the same as the simple $A/\operatorname{rad}(A)$-modules. Hence, we may suppose $\operatorname{rad}(A) = \{0\}$ and A is semi-simple. Let

$$A = A_1 \oplus \cdots \oplus A_r$$

where each A_i is a minimal 2-sided ideal (i.e., simple ring). Let M be any simple A-module. $A_iM = \{0\}$ or M by the usual argument. $M = AM = \sum A_iM$ so $A_iM = M$ for at least one i, but for $j \neq i$, we have $A_jM = A_jA_iM = \{0\}$ (since $A_jA_i = \{0\}$). Moreover, the identity e_i of A_i (where $1 = e_1 + \cdots + e_r$) acts as the identity on M since $e_jM = \{0\}$ for $j \neq i$. It follows that M is an A_i-module for exactly one of the simple factors A_i of A. Since a simple ring has only one simple module up to isomorphism, we are done.

Note that as rings $A_i \cong A/(\oplus_{j \neq i} A_j)$, and, by the above discussion, the action of A_i on M is the same if we view it either as an ideal of A or as a factor ring of A.

Exercises.

1. Verify two of the unproved statements in the proof of the first theorem in the section.

5. Commutative artinian rings

Suppose A is semi-simple and commutative. Then it is isomorphic to a direct product of matrix rings over division rings. The only such commutative rings are matrix rings of degree 1 over fields. Hence, *a commutative semi-simple artinian ring is isomorphic to a direct product of fields*. Moreover, for *any* commutative artinian ring A, we shall see that the direct product decomposition of $A/\operatorname{rad}(A)$ may be "lifted" to A.

Let A be a semi-simple commutative ring, and let

$$A = A_1 \oplus \cdots \oplus A_r$$

where each A_i is an ideal which is a field. Then, as above,

$$1 = e_1 + \cdots + e_r$$

the idempotent $e_i \in A_i$ is the multiplicative identity of A_i. In addition, $e_ie_j = 0$ for $i \neq j$. In any ring, in such circumstances we say that 1 is decomposed into *orthogonal idempotents*. Since in the present case $Ae_i = A_i$ is a field, it is not hard to see that e_i cannot be further decomposed $e_i = e_i' + e_i''$ where $e_i'e_i'' = 0$. Thus we call the e_i *indecomposable* or *primitive* idempotents.

PROPOSITION. *Let A be a commutative artinian ring and suppose*

$$1 = \overline{e}_1 + \cdots + \overline{e}_i + \cdots + \overline{e}_r$$

is a decomposition into indecomposable orthogonal idempotents in $A/\operatorname{rad}(A)$. Then there exist elements $e_1, \ldots, e_r \in A$ such that $e_i \bmod \operatorname{rad}(A) = \overline{e}_i$ and

$$1 = e_1 + \cdots + e_i + \cdots + e_r,$$

is a decomposition into indecomposable orthogonal idempotents in A.

PROOF. Since A is artinian, $J = \operatorname{rad}(A)$ is nilpotent. Let n be the smallest positive integer such that $J^n = 0$. n is called the exponent of J. We proceed by induction on n. For $n = 1$, the result is true because $A = A/\operatorname{rad}(A)$ is semi-simple. Suppose the Proposition is true for $1, 2, \ldots, n-1$. Let $I = J^{n-1}$ and note that $I^2 = 0$. Then $\operatorname{rad}(A/I) = J/I$ has exponent $n-1$ so the result is true for A/I. Choose $f_1, \ldots, f_r \in A$ such that $f_1 \bmod I, f_2 \bmod I, \ldots, f_r \bmod I$ provide a decomposition of 1 into orthogonal idempotents in A/I. Consider elements of the form $f_i + x_i$ with $x_i \in I$. We have

$$(f_i + x_i)^2 = {f_i}^2 + 2f_i x_i + {x_i}^2 = f_i^2 + 2f_i x_i,$$

so $f_i + x_i$ is idempotent if and only if

$$\begin{aligned} {f_i}^2 + 2f_i x &= f_i + x_i \\ \text{or} \quad (1 - 2f_i)x_i &= {f_i}^2 - f_i. \end{aligned}$$

However, $1 - 2f_i$ is invertible. For,

$$(1 - 2f_i)^2 = 1 - 4f_i + 4{f_i}^2 = 1 - 4(f_i - {f_i}^2) = 1 + z$$

where $z = -4(f_i - {f_i}^2 \in 1 + I$. However, $(1 + z)(1 - z) = 1 - z^2 = 1$ since $z^2 = 0$ so $1 + z$ and hence any factor of it is invertible. Thus, we can choose $x_i = (1 - 2f_i)^{-1}({f_i}^2 - f_i) \in I$ so that $e_i = f_i + x_i$ is idempotent and lifts the idempotent $f_i \bmod I$ in A/I. We have $e_i e_j = 0$ for $i \neq j$ since

$$e_i e_j \equiv 0 \bmod I \;\Rightarrow\; e_i e_j \in I \;\Rightarrow\; e_i e_j = {e_i}^2 {e_j}^2 = (e_i e_j)^2 \in I^2 = \{0\}.$$

Similarly, we have

$$1 = e_1 + e_2 + \cdots + e_r + y$$

where $y \in I$. Multiplying by e_i shows that $e_i y = 0$ for each i, and squaring then shows that

$$1 = e_1 + e_2 + \cdots + e_r.$$

Finally, it is not hard to show that e_i is indecomposable since $e_i \bmod I$ is indecomposable.

We leave it to the student to show that the decomposition is unique. (Hint: Show that any idempotent e is a sum of some subset of the idempotents $e_1, \ldots, e_r$.)

THEOREM. *Let A be a commutative artinian ring. Then A may be written*

$$A \cong A_1 \times A_2 \times \cdots \times A_r$$

where each A_i is a commutative artinian local ring. Also, this decomposition is unique up to order and isomorphism.

PROOF. Let $1 = e_1 + \cdots + e_r$ be a decomposition of 1 into indecomposable orthogonal idempotents, and let $A_i = Ae_i$. It is easy to check that $A_i A_j = 0$, e_i acts as the identity on A_i, and

$$A = A_1 \oplus \cdots \oplus A_r.$$

Each A_i is a local ring. For, consider $A_i/\operatorname{rad}(A_i)$. It is semi-simple and hence isomorphic to a direct product of fields. If the sum involved more than one constituent, the we could lift a decomposition of $e_i \bmod \operatorname{rad}(A_i)$ to A and decompose the identity e_i of A_i which we know is indecomposable. It follows that $A_i/\operatorname{rad}(A_i)$ is a field so $\operatorname{rad}(A_i)$ is a maximal ideal and A_i is a local ring.

Exercises.

1. Show that in a commutative artinian ring, the decomposition of 1 as a sum of orthogonal primitive idempotents is unique except for the order of the factors.