CHAPTER XIII

MORE RING THEORY

1. Chain Conditions

We now begin a more systematic treatment of ring theory. There is a substantial difference between the directions which the theory takes in the commuative and non-commutative case. In this course, we shall concentrate mainly on the non-commutative case, but we shall also develop some of the important basic ideas of commutative algebra. We start now with the topic of chain conditions which has relevance both for commutative and non-commutative algebra.

PROPOSITION. *Let S be a partially ordered set. The following two assertions are equivalent.*
(i) Every nondecreasing sequence

$$x_1 \leq x_2 \leq \cdots \leq x_i \leq \ldots$$

eventually stabilizes, i.e., there is an n such that $x_m = x_n$ for $m \geq n$.
(ii) Every non-empty subset of S has a maximal element.

PROOF.
Assume (i). Let T be any non-empty subset of S. Choose $x_1 \in T$. If x_1 is maximal, we are done. Otherwise, choose $x_2 \in T$ with $x_1 < x_2$. If x_2 is maximal, we are done. Keep going in this way. We can construct a strictly increasing sequence of elements of T—which contradicts (i)—unless we eventually come upon a maximal element.

Conversely, suppose (ii) is true. The set of elements in a non-decreasing sequence must have a maximal element and it is clear that the sequence must stabilize with that element.

A partially ordered set with these properties is said to satisfy the *ascending chain condition*. A partially ordered set which satisfies the corresponding conditions for the *reversed order* —i.e., every nonincreasing chain stabilizes and every non-empty set has a minimal element—is said to satisfy the *descending chain condition*.

Let A be a ring and let M be a left A-module. In what follows, we shall generally omit the modifier 'left', but the student should keep in mind that we are developing a theory for left modules. Of course, there is also a parallel theory for right modules. For commutative rings we need not distinguish the two theories.

We say that M is *noetherian* if its family of submodules, ordered by inclusion, satisfies the ascending chain condition. We say the module M is *artinian* if the set of submodules satisfies the descending chain condition.

Examples.

1. Any finite abelian group viewed as a $\mathbf{Z}$-module is both noetherian and artinian.

2. $\mathbf{Z}$ as a $\mathbf{Z}$-module satisfies the ascending chain condition but does not satisfy the descedning chain condition. For example, the set of all nontrivial subgroups of $\mathbf{Z}$ does not have a minimal element.

3. Let p be a prime and let T_p be the subgroup of $\mathbf{Q}/\mathbf{Z}$ of all elements with order a power of p, (i.e., its p-torsion subgroup.) T_p satisfies the descending chain condition on subgroups but not the ascending chain condition. On the other hand $\mathbf{Q}/\mathbf{Z}$ itself satisfies neither the ascending nor descending chain conditions.

PROPOSITION. *Let A be a ring, M a left A-module, and N a submodule of M. Then M is noetherian (artinian) if and only if both N and M/N are noetherian (artinian.)*

PROOF.

Every chain of submodules of N is also a chain of submodules of M so if M is noetherian, N is also noetherian. Similarly, every submodule of M/N is of the form L/N where L is a submodule of M with $L \supseteq N$. Hence, every chain of submodules of M/N yields a chain of submodules of M which must stop if M is noetherian.

Conversely, suppose M/N and N are noetherian. Let

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_i \subseteq \dots$$

be a chain of submodules of M. The chains

$$N \cap M_1 \subseteq N \cap M_2 \subseteq \cdots \subseteq N \cap M_i \subseteq \dots$$

and

$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \cdots \subseteq (M_i + N)/N \subseteq \dots$$

must stabilize by hypothesis. The result now follows from the following lemma.

LEMMA. *Suppose $M' \subseteq M'', N \cap M' = N \cap M''$, and $(M' + N)/N = (M'' + N)/N$. Then $M' = M''$.*

PROOF OF THE LEMMA.

Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N \cap M' & \longrightarrow & M' & \longrightarrow & (M' + N)/N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N \cap M'' & \longrightarrow & M'' & \longrightarrow & (M'' + N)/N & \longrightarrow & 0. \end{array}$$

The rows are exact by the second isomorphism theorem for modules. The homomorphisms on the ends are equalities by hypothesis so by the 5-lemma, the homomorphism (which is the inclusion) is an isomorphism so it is equality.

The proof for artinian modules is similar.

COROLLARY. *Any finite sum of noetherian (artinian) modules is noetherian (artinian.)*

PROOF.

Use induction on the number of factors.

A ring is said to be noetherian or artinian if it is such viewed as a module over itself. In the non-commutative case, we must distinguish between *left*-noetherian and *right*-noetherian and similarly for "artinian".

COROLLARY. *If A is noetherian (artinian) then every finitely generated A-module is noetherian (artinian.)*

PROOF.

Any finitely generated module is an epimorphic image of a finite direct sum of copies of A.

PROPOSITION. *Let A be a ring and M a module over A. M is noetherian if and only if every submodule of M is finitely generated. In particular, M is itself finitely generated.*

PROOF.

Suppose M is noetherian, and let N be a submodule of M. The family of *finitely generated submodules* of N has a maximal element N'. We claim $N' = N$. Otherwise, we could choose $y \in N$, $y \notin N'$, and it is clear that $N' + ky$ is a finitely generated submodule of N strictly containing N'.

Suppose conversely that every submodule of M is finitely generated. The union of any ascending chain

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \dots$$

of submodules of M is clearly a submodule N so it is finitely generated. However, each generator of N must be contained in some submodule N_i in the chain, so N must also be included in N_j where j the largest index needed for any of the finite set of generators. It follows that $N = N_j$, and the chain must stabilize.

PROPOSITION. *If A is a principal ideal domain, then it satisfies the ascending chain condtion, i.e., every PID is noetherian.*

PROOF.
Every submodule of A (ideal) is generated by a single element so it is finitely generated. Hence A is noetherian.

It follows from the proposition that if k is a *field*, then $k[X]$ is noetherian since it is a Euclidean domain and hence a PID. However, $k[X]$ is not artinian since the chain of submodules (ideals)

$$(X) \supseteq (X^2) \supseteq (X^3) \supseteq \dots$$

clearly does not stablize.

PROPOSITION. *Let k be a commutative, noetherian (artinian) ring. If A is a k-algebra which is finitely generated as a k-module, then A is both left and right noetherian (artinian).*

PROOF.
We consider the noetherian case; the artinian case is similar.
Any left (right) ideal of A is easily also seen to be a k-submodule. Since k is noetherian, and A is finitely generated as a k-module, it follows from the above propositions that A is noetherian as a k-module. However, if the chain condition holds for k-submodules, it also holds for left or right ideals.

PROPOSITION. *If A is a noetherian (artinian) ring, then every epimorphic image of A is noetherian (artinian.)*

PROOF.
If A'' is an epimorphic image of A, then the pull back to A of a chain of ideals in A'' is a chain of ideals in A. Also, the images in A'' of the ideals in A are the original ideals in A''. Since the chain in A must stabilize, the image chain in A'' must stablize.

THEOREM (HILBERT BASIS THEOREM). *If A is a commutative noetherian ring and X is an indeterminate, then $A[X]$ is noetherian.*

PROOF.
Let I be an ideal in $A[X]$. Let $\overline{I}$ denote the set of elements in A which are *leading coefficients* for polynomials $f(X) = aX^n + bX^{n-1} + \dots \in I$. It is not hard to see that $\overline{I}$ is an ideal in A. Since A is noetherian, $\overline{I}$ is finitely generated, say by $a_1, \dots, a_k$. Let $f_i(X)$ be a polynomial in I with leading coefficient a_i for $i = 1, \dots, k$. Let $r_i = \deg f_i(X)$, and let r be the largest of the r_i. Let I' be the ideal generated by $f_1(X), \dots, f_k(X)$. If

$$f(X) = aX^n + bX^{n-1} + \dots \in I$$

then $a = \sum_i u_i a_i$ for appropriate $u_i \in A$. We claim that

$$f(X) = f'(X) + g(X) \qquad \text{where } \deg g(X) < r \text{ and } f'(X) \in I'.$$

For, if $\deg f(X) < r$, we can take $f(X) = g(X)$. Otherwise, take

$$h(X) = f(X) - \sum_i X^{n-r_i} u_i f_i(X).$$

The coefficient of X^n in $h(X)$ is $a - \sum_i u_i a_i = 0$ so its degree is less than n, and clearly $f(X) - h(X) \in I'$. Arguing by induction gives us the desired decomposition.

Let M be the A-submodule of $A[X]$ consisting of all polynomials of degree $< r$. The above decomposition shows that $I \subseteq I' + M$. If follows that *as an A-module*, I/I' is isomorphic to a submodule of

$$(I' + M)/I' \cong M/M \cap I'.$$

Since A is noetherian, and since M is finitely generated over A, it follows that $(I' + M)/I'$ is noetherian over A. Hence I/I' is even a finitely generated A-module, and clearly any set of A-module generators is also a set of $A[X]$-module generators. Since I' and I/I' are finitely generated $A[X]$-modules, so is I.

COROLLARY. *Let A be a commutative noetherian ring. Any finitely generated A-algebra $A[x_1, x_2, \ldots, x_n]$ is noetherian.*

PROOF.

Such a ring is an epimorphic image of a polynomial ring over A in n indeterminates, and such a ring is noetherian by induction.

Exercises.

1. Verify the assertions in the text about $\mathbf{Q}/\mathbf{A}$ as a $\mathbf{Z}$-module: (a) $\mathbf{Q}/\mathbf{Z}$ satisfies neither chain condition (b) T_p, its p-torsion subgroup, satisfies the descending chain condition but not the ascending chain condition.

2. Let A be a commutative ring and let I be an ideal in $A[X]$. Let $\overline{I}$ be the set of leading coefficients of polynomials in I. Show as stated in the text that $\overline{I}$ is an ideal in A.

3. Let A be a ring and let M be a noetherian left A-module. Suppose $f \in \mathrm{Hom}_A(M, M)$ is an epimorphism.
(a) Let $K_n = \mathrm{Ker}\, f^n$ for $n = 1, 2, \ldots$. Show that there is an $n > 0$ such that $K_n = K_{n+1}$.
(b) Show that $\mathrm{Ker}(f) = \{0\}$ so that f is an isomorphism. (Hint: Since f is an epimorphism, so is f^n; write $x \in \mathrm{Ker}\, f$ as $x = f^n(y)$.)
(c) Is the corresponding result true if we assume f is a monomorphism?
(d) Show that if A is left noetherian, then every left invertible element is also right invertible and vice versa. (Hint: Take $M = A$ so that $\mathrm{Hom}_A(A, A) \cong A$.)

2. The radical of a ring

Let A be a ring. A nontrivial left A-module M is called *simple* if it has no submodules other than $\{0\}$ and M. There is of course a corresponding notion for right modules. As before, in what follows 'module' will generally mean 'left module', but the corresponding theory for right modules follows in parallel. One way to study a ring is to try to discover all its simple modules.

Associated with any A-module M is a *representation* $\phi : A \to \mathrm{Hom}_{\mathbf{Z}}(M, M)$ where $\phi(a)(x) = ax$. If the module is simple, we call the representation *irreducible*. The kernel of this representation is called the *annihilator* of M:

$$\mathrm{Ann}_A(M) = \{a \in A \,|\, ax = 0 \text{ for all } x \in M\}.$$

By the first isomorphism theorem, $\mathrm{Im}\,\phi \cong A/\mathrm{Ann}_A(M)$ so we may be able to find out something about the ring A by studying this quotient which is isomorphic to a subring of an *endomorphism ring* of some abelian group. If $\mathrm{Ann}_A(M) = \{0\}$ then ϕ imbeds A monomorphically in $\mathrm{Hom}(M, M)$, and we call the module or the representation *faithful*.

Note that $\mathrm{Ann}_A(M)$ is a (2-sided) ideal of A, and moreover if I is any (2-sided) ideal contained in $\mathrm{Ann}_A(M)$, then M may be viewed as an A/I-module by setting $(a + I)x = ax$. Also, if N is a submodule of M, then clearly $\mathrm{Ann}_A(N) \supseteq \mathrm{Ann}_A(M)$. Finally, if N_1 and N_2 are submodules of M, then

$$\mathrm{Ann}_A(N_1 + N_2) = \mathrm{Ann}_A(N_1) \cap \mathrm{Ann}_A(N_2).$$

You should prove the above assertions.

Define

$$\mathrm{rad}(A) = \bigcap_{\substack{M \text{ a simple} \\ \text{left } A\text{-module}}} \mathrm{Ann}_A(M).$$

$\mathrm{rad}(A)$ is called the *Jacobson radical* of A. (There is another related radical called the *nil radical* which we shall discuss later.) It is certainly an ideal of A, and it has the property that every simple A-module is also an $A/\mathrm{rad}(A)$-module. Conversely, it is easy to see that any simple $A/\mathrm{rad}(A)$-module becomes a simple A-module through the quotient epimorphism $A \to A/\mathrm{rad}(A)$. Hence, the classes of simple (left) A-modules and simple (left) $A/\mathrm{rad}(A)$-modules are the same. Thus, it is easy to see that the following is true.

PROPOSITION. *Let A be a ring. Then* $\operatorname{rad}(A/\operatorname{rad}(A)) = \{0\}$.

At this point you might worry about the Jacobson radical for the theory of right modules. Fortunately, we shall see later that the left and right handed theories produce the same Jacobson radical.

THEOREM. *Let A be a ring. Then*

$$\operatorname{rad}(A) = \bigcap_{\substack{L \text{a maximal proper} \\ \text{left ideal in } A}} L.$$

PROOF. Let L be a maximal proper left ideal of A. Then $M = A/L$ is a simple A-module since any submodule would correspond to an intermediate left ideal between L and A. Hence, $\operatorname{rad}(A)(A/L) = \{0\}$, i.e. $\operatorname{rad}(A) = \operatorname{rad}(A)A \subseteq L$ so that so $\operatorname{rad}(A) \subseteq \bigcap_L L$.

Conversely, let M be any A-module. It is not hard to see that

$$\operatorname{Ann}_A(M) = \bigcap_{x \in M} \operatorname{Ann}_A(x)$$

where $\operatorname{Ann}_A(x) = \{a \in A \,|\, ax = 0\}$. (See the Exercises.) However, it is easy to check that each $L = \operatorname{Ann}_A(x)$ is a left ideal; indeed it is the kernel of the A-module homomorphism $A \to M$ defined by $a \mapsto ax$. Also, *if M is simple*, and $x \neq 0$, L is a maximal proper left ideal. For, Ax is a non-zero left A-submodule of M so by simplicity, $Ax = M$. Hence, $A/L \cong M$. $L \neq A$ since $M \neq \{0\}$, and it is maximal, as above, because M is simple. It now follows that $\operatorname{Ann}_A(M) \supseteq \bigcap_{L \text{ maximal}} L$ since it equals the intersection of some of them. Hence, $\operatorname{rad}(A) = \bigcap_{M \text{ simple}} \operatorname{Ann}_A(M) \supseteq \bigcap_L L$. Putting this together with the previous inclusion gives the theorem.

Note that the above proof shows that every simple left A-module is isomorphic to one of the form A/L where L is a maximal left ideal (of the form $\operatorname{Ann}(x)$ for some $x \neq 0 \in M$). Note also that in the commutative case the argument is a bit simpler since $L \subseteq \operatorname{Ann}_A(A/L)$, i.e. $LA = AL \subseteq L$. However, in the general case this argument fails becasue L is only a left ideal.

THEOREM. *Let A be a ring. Then the Jacobson radical of A is given by*

$$\begin{aligned}\operatorname{rad}(A) &= \{x \in A \,|\, 1 - axb \in U(A) \text{ for all } a, b \in A\} \\ &= \{x \in A \,|\, 1 - ax \text{ is left invertible for all } a \in A\} \\ &= \{x \in A \,|\, 1 - xb \text{ is right invertible for all } b \in A\}.\end{aligned}$$

COROLLARY. *The left Jacobson radical of a ring A is the same as the right Jacobson radical of A (the intersection of the annihilators of all simple right A-modules). In particular,* $\operatorname{rad}(A)$ *is the intersection of all maximal right ideals of A.*

PROOF OF THE THEOREM.

Let J denote the first set on the right in the statement of the theorem, and let J_l denote the second set, J_r the third set. Since every invertible element is left invertible, taking $b = 1$ shows that $J \subseteq J_l$. *We shall show below* that $J_l \subseteq \operatorname{rad}(A) \subseteq J$ from which it follows that all three are equal. By the same argument in the right handed theory, we can show similarly that $J_r = \operatorname{rad}_{right}(A) = J$ so it will follow that $J = J_l = J_r$ and that both radicals are equal to J and hence the same.

To show that $\operatorname{rad}(A) \subseteq J$, it suffices to show that every element of $1 + \operatorname{rad}(A)$ is invertible. For $x \in \operatorname{rad}(A) \;\Rightarrow\; -axb \in \operatorname{rad}(A)$, so in that case, any $1 - axb \in U(A)$ and $x \in J$. Suppose then that $y \in \operatorname{rad}(A)$, and consider the left ideal $A(1 + y)$. If $A(1 + y) = A$, then $u(1 + y) = 1$ has a solution u so $1 + y$ has a left inverse. Otherwise, $A(1 + y)$ is a proper left ideal of A. We shall show that this is false. To this end consider the family of all proper left ideals L of A such that $L \supseteq A(1 + y)$. By Zorn's Lemma, there is a maximal, proper left ideal L_0 containing $A(1 + y)$. However, $\operatorname{rad}(A)$ is contained in every maximal, proper left ideal

of A, so $y \in L_0$. Since $1+y \in L_0$, it follows that $1 \in L_0$ which contradicts the fact that L_0 is proper. Hence, we conclude that $1+y$ has a left inverse u. On the other hand, the equation

$$u(1+y) = u + uy = 1$$

implies that $u = 1 + (-uy)$ so u is left invertible by the same argument since $-uy \in \mathrm{rad}(A)$. Call that left inverse t. Since $tu = 1$ and $u(1+y) = 1$, it follows as usual by associativity that $t = 1 + y$ so u is also a right inverse for $1 + y$. Hence, $1 + y \in U(A)$ as claimed.

Next we show that $J_l \subseteq \mathrm{rad}(A)$. Suppose $x \in J_l$. Let M be any simple left A-module. Let $m \neq 0 \in M$. Then Axm is a submodule of M, and since M is simple, either $Axm = \{0\}$, whence $xm = 0$, or $Axm = M$. In the latter case, there is an $a \in A$ such that $axm = m$, i.e., $(1 - ax)m = 0$. However, by the definition of J_l, $1 - ax$ is left invertible so $m = 0$. It follows that $xm = 0$ for all $m \in M$ so $x \in \mathrm{Ann}_A(M)$. Since this holds true for every simple M, it follows that $x \in \mathrm{rad}(A)$.

If L and M are additive subgroups of the ring A, then we define LM as usual to be the subgroup generated by all products xy with $x \in L, y \in M$. Hence L^k is the subgroup generated by all products $x_1 x_2 \dots x_k$ with $x_i \in L, i = 1, \dots, k$. If L is a left ideal (right ideal, 2-sided ideal), then the same is true of L^k. We call an ideal (left, right, or both) *nilpotent* if $L^k = \{0\}$ for some $k > 0$. That is the same as saying $x_1 x_2 \dots x_k = 0$ whenever $x_1, x_2, \dots, x_k \in L$. In particular, if $L^k = \{0\}$, it follows that $x^k = 0$ for all $x \in L$. If $x^k = 0$ for some $k > 0$ (which could depend on x) then x is said to be nilpotent. If L satisfies the somewhat weaker condition that every element is nilpotent, we say that L is *nil*. As we just noted, every nilpotent ideal is certainly nil, but not necessarily vice versa.

THEOREM. *Let A be a ring. Then* $\mathrm{rad}(A)$ *contains every nil right ideal and every nil left ideal. Moreover, if A is left (right) artinian, then* $\mathrm{rad}(A)$ *is nilpotent—so it is the maximal nilpotent left or right ideal.*

PROOF.

Suppose that L is any nil left ideal, $x \in L$, and $a \in A$. Then $y = ax \in L$ since L is a left ideal and y is also nilpotent, say $y^k = 0$. Then

$$1 = 1 - y^k = (1 + y + y^2 + \cdots + y^{k-1})(1 - y)$$

so $1 - y = 1 - ax$ is left invertible. It follows from the theorem above that $x \in \mathrm{rad}(A)$; hence $L \subseteq \mathrm{rad}(A)$. A similar argument shows that any nil right ideal is contained in $\mathrm{rad}(A)$.

Suppose next that A is left artinian, and let $J = \mathrm{rad}(A)$. Consider the descending chain of ideals

$$J \supseteq J^2 \supseteq \cdots \supseteq J^n \supseteq \dots$$

These are all left ideals since J is a left ideal, so by the descending chain condition, it stabilizes, say for $n \geq k$. If $J^k = \{0\}$, then J is nilpotent, so suppose $J' = J^k \neq \{0\}$. Consider all left ideals L such that $L \subseteq J'$ and $J'L \neq 0$. Since $J'J = J^{k+1} = J^k \neq 0$, it follows that $L = J$ is such an ideal; hence this set of left ideals is nonempty. By the minimum condition on left ideals, it follows that there is a minimal L' in this family of left ideals. Since $J'L' \neq 0$, we may choose $x \in L'$ such that $J'x \neq 0$. (In particular $x \neq 0$.) However, $J'x$ is a left ideal (since J' is a 2-sided ideal). Also, $J'x \subseteq J'$ and $J'(J'x) = J^{2k}x = J^k x = J'x \neq 0$. Because L' is minimal, and $x \in L'$, it follows that $L' = J'x$. Thus, we can find $u \in J' \subseteq J$ such that $x = ux$, i.e., $(1 - u)x = 0$. However, since $u \in J = \mathrm{rad}(A)$, it follows from the theorem proved above that $1 - u$ is invertible; hence $x = 0$. That contradicts the above assumptions so we must have $J' = J^k = \{0\}$.

COROLLARY. *If A is an artinian ring, then every nil ideal is nilpotent.*

Exercises.

1. Prove the unproved assertions in the text about the annihilator of a module. In particular prove that

$$\mathrm{Ann}_A(M) = \bigcap_{x \in M} \mathrm{Ann}_A(x)$$

2. Show that the Jacobson radical of $\mathbf{Z}$ is trivial.

3. If the Jacobson radical of a ring in trivial, then the only nil ideal is the trivial ideal. Show that a commutative ring with trivial Jacobson radical does not have any nilpotent elements other than 0.

4. Let k be a field.

(a) Show that the ring $M_n(k)$ of $n \times n$ matrices with entries in k has no nontrivial 2-sided ideals. Hint: Any element in $M_n(k)$ can be written $\sum_{i,j} a_{ij}E_{ij}$ where E_{ij} is the matrix which is 1 in the i,j-position and zero elsewhere. Think about the products $E_{ij}E_{rs}$.

(b) Show that the Jacobson Radical of $M_n(k)$ is trivial. Does $M_n(k)$ have nilpotent elements other than 0?

3. Nakayama's Lemma

THEOREM. *Let A be a ring, J is a right ideal contained in* $\mathrm{rad}(A)$*, and M a finitely generated left A-module. If $JM = M$, then $M = \{0\}$.*

PROOF. Suppose $M \neq \{0\}$, and choose a minimal generating set $\{x_1, \ldots, x_k\}$ for M. Then since $M = JM$, any element $y \in M$ may be expressed as a sum of elements of the form ax with $a \in J, x \in M$. Each x may be expressed as a linear combination of $\{x_1, \ldots, x_k\}$ with coefficients in A. Since J is a *right* ideal, we can combine terms to express y as a sum of elements of the form $a_i x_i$ with $a_i \in J$. In particular, we have

$$x_1 = a_1x_1 + a_2x_2 + \cdots + a_kx_k$$

with $a_1, \ldots, a_k \in J$. Hence,

$$(1 - a_1)x_1 = a_2x_2 + \cdots + a_kx_k.$$

However, since $a_1 \in J \subseteq \mathrm{rad}(A)$, it follows that $1 - a_1$ is invertible, so x_1 can be expressed as a linear combination of $x_2, \ldots, x_k$. This contradicts the minimality of the generating set.

COROLLARY. *Let A be a ring, J is a right ideal contained in* $\mathrm{rad}(A)$*, M a finitely generated A-module, and N a submodule. If $M = N + JM$, then $N = M$.*

PROOF. Apply Nakayama's Lemma to M/N which is also finitely generated. The hypothesis $M = N + JM$ implies that $J(M/N) = \{0\}$ so $M/N = \{0\}$ and $M = N$.

COROLLARY. *Let A be a ring. Every maximal proper 2-sided ideal I of A contains* $\mathrm{rad}(A)$*.*

PROOF. Suppose I is a maximal 2-sided ideal. Take $J = \mathrm{rad}(A), M = A$, and $N = I$. Then $I + JA = I + J$ is a 2-sided ideal and it contains I. By maximality, $I + J = A$ or $I + J = I$. In the former case, the previous corollary tells us that $A = I$; hence (since I is proper) the latter case holds and $J \subseteq I$.

Nakayama's Lemma is one of those results in mathematics which is basically trivial but which has many profound consequences. For this reason, it is named after Nakayama although it is hardly the most important or most difficult theorem proved by that distinguished mathematician.

The commutative case.

If A is a commutative ring, the theory simplifies. In that case

$$\mathrm{rad}(A) = \{x \in A \,|\, 1 - ax \in U(A) \text{ for all a } \in A\}.$$

Also, if A is commutative, the set N of all nilpotent elements of A is an ideal. For, if $x^i = 0$ and $y^j = 0$, then by the binomial theorem

$$(x + y)^{i+j} = \sum_{r=0}^{i+j} \binom{i+j}{r} x^r y^{i+j-r}.$$

In each term, either $r \geq i$ or $i + j - r = (i - r) + j \geq j$, so the sum is 0. Hence, N is closed under addition. It is also closed under multiplication by elements of A since in the commutative case $(ax)^i = a^i x^i$. Hence, it is an ideal. N is called the *nil radical* of A. We shall denote it $N(A)$.

Since rad(A) contains every nil ideal, we see that if A is commutative, then *the Jacobson radical always contains the nil radical*. However, in general the two need not be equal. In fact, if A is commutative, we need not distinguish left from right ideals so the *Jacobson radical* is the intersection of all *maximal* ideals of A. But, we shall show later in this course that the *nil radical* is the intersection of all *prime* ideals of A. Hence, the existence of nonmaximal prime ideals raises the possibility that $\mathrm{rad}(A) \supsetneq N(A)$. Of course, if A is an *artinian commutative* ring, then *the Jacobson radical equals the nil radical* since the former is nilpotent.

Exercises.

1. Let A be the subring of $\mathbf{Q}$ consisting of all fractions a/b with $a, b \in \mathbf{Z}, \gcd(a, b) = 1$ and such that 2 does not divide b. Show that A has a unique maximal ideal, namely the principal ideal (2). Hence, this must be the Jacobson radical. On the other hand, since A is a domain, it has no nonzero nilpotent elements, and its nil radical is (0). (Note that (0) is also a prime ideal.)

General ring theoretic exercises.

2. Let k be a commutative ring and let G be a group. Let $k[G]$ be the free k-module with basis the underlying set of G. Thus any element of $k[G]$ can be written $\sum_{g\in G} a_g g$ where $a_g \in k$ and almost all $a_g = 0$. Define

$$(\sum_g a_g g)(\sum_h b_h) = \sum_k (\sum_{gh=k} a_g b_h)k.$$

(a) Show that this operation makes $k[G]$ into an associative ring. (Try to organize your proof so that the argument is convincing but leave out as much detail as is consistent with that goal.)

(b) Imbed k in $k[G]$ by $\phi : k \to k[G]$ where $\phi(a) = a1$ (i.e., $a_g = 0$ for $g \neq 1$.)

Show that $k[G]$ becomes a k-algebra.

$k[G]$ is called the *group algebra* of G over k. The elements of the basis of $k[G]$ form a group under multiplication in $k[G]$ which we may readily identify again with G. Note that G is thereby contained in the group of units $U(k[G])$.

(c) Suppose that A is any k-algebra and $f : G \to U(A)$ is a homomorphism of G into the group of units of A. Show that f may be extended uniquely to a k-algebra homomorphism $F : k[G] \to A$.

(d) If $f : G \to G'$ is a homomorphism of groups, how should you define a k-algebra homomorphism $k[f] : k[G] \to k[G']$ so that $k[-]$ becomes a functor from the category of groups to the category of k-algebras?

If G is a group and V is a vector space over a field k, then a homomorphism $f : G \to Gl(V)$ is called a representation of G over k.

(e) Show that the representations of G over k are in one-to-one correspondence with the $k[G]$-modules V.