MTS 411 ADVANCED ALGEBRA I

This note is aimed at familiarising the students with the contents of the course Advanced Algebra I. This note should not be taken as a full lecture note for the course. However important definitions are stated and several results are stated without proofs. Detailed notes shall be given during lecture periods.

1. Rings and Ideals

Definition (1.1) A ring A is a nonempty set with two binary operations + and . such that:

(i) (A,+) is an abelian group.

(ii) (A,.) is a semigroup.

(iii) . is distributive over + that is

$$a(b+c) = ab + ac, \quad \forall\ a, b, c \in A.$$

If $ab = ba\ \forall\ a, b \in A$, we say that A is commutative.

If there exits $1 \in A$ such that $1.a = a.1 = a\ \forall\ a \in A$, we say that A is a ring with unity.

Except otherwise stated in this note, all rings will be commutative rings with unity.

Example (1.2) $\mathcal{Z}, \mathcal{Q}, \mathcal{R}, \mathcal{C}$ are commutative rings with unity.

Example (1.3) Let A and B be rings. Then $A \times B$ is also a ring.

Example (1.4) Let $(A, +)$ be an abelian group and let End(A) be the set of endomorphisms of the group A into itself. Then (End(A),+,.) is a ring where + and . are defined by

$$\begin{aligned} (\phi + \psi)(x) &= \phi(x) + \psi(x), \\ (\phi\psi)(x) &= \phi(\psi(x)), \quad \forall\ \phi, \psi \in End(A), x \in A. \end{aligned}$$

Example (1.5) Let 2^A be the power set of a nonempty set R. If $X, Y \in 2^A$, define

$$\begin{aligned} X + Y &= (X \cup Y) - (X \cap Y), \\ X.Y &= X \cap Y. \end{aligned}$$

Then $(2^A, +, .)$ is a commutative ring with unity and has the following properties:

(i) $X^2 = X$, and

(ii) $2X = 0, \forall\ X \in 2^A$.

This ring is generally called a Boolean ring.

Definition (1.6) Let A and B be rings with 1. A mapping $\phi : R \to S$ is called a ring homomorphism if

(i) $\phi(x+y) = \phi(x) + \phi(y)$,

(ii) $\phi(xy) = \phi(x)\phi(y) \; \forall \; x, y \in A$.

$\phi(A)$, the image of A under ϕ is defined by $\phi(A) = \{b \in B : \phi(a) = b \text{ for some } a \in A\}$. $Ker\phi$, the kernel of ϕ is defined by $Ker\phi = \{a \in A : \phi(r) = 0_B\}$. We assume always that $\phi(1_A) = 1_B \in B$.

Definition (1.7) Let A be a ring. I is called an ideal of A if I is an additive subgroup of A that is $a, b \in I$ implies that $a - b \in I$ and $AI \subseteq I$ that is if $a \in I$ and $r \in A$, then $ra \in I$. More generally, an ideal of a ring A is a subset $I \subset A$ such that $0 \in I$, and $af + bg \in I \; \forall \; a, b \in A$ and $f, g \in I$. For the ideal generated by elements $a, b \in A$, we write (a,b) or Aa+Ab. Similarly we write $(X) + aA + J$ for the ideal generated by the set X, an element a and an ideal J.

It should be noted that $0 = \{0\} = (0)$ is an ideal of A, and if $1 \in I$, then $I = (1) = A$.

If I is an ideal of A, define $A/I = \{a + I : a \in A\}$. If $a + I, b + I \in A/I$, then $(a+I) + (b+I) = a + b + I$, $(a+I)(b+I) = ab + I$. With this definition, A/I is a commutative ring with unity since A is commutative with unity.

Proposition (1.8) Let $\phi : A \to B$ be a ring homomorphism. Then

(i) $\phi(A)$ is a subring of B.

(ii) $Ker\phi$ is an ideal of A.

(iii) If $I \subset A$ is an ideal, then there exists a ring A/I and a surjective homomorphism $\psi : A \to A/I$ such that $Ker\psi = I$; the pair A/I and ψ is uniquely defined up to isomorphism. ψ is called the quotient or canonical or natural homomorphism.

(iv) In the notation of (iii), the mapping

$$\psi^{-1} : [\text{ideals of A/I}] \to [\text{ideals of A containing I}]$$

is a 1-1 correspondence.

Recall that if A is a ring, then $a \in A$ is a zero divisor if $a \neq 0$ but $\exists b \in A$ such that $b \neq 0$ and $ab = 0$. A ring with no zero divisor is called an integral domain.

If $a \in A$ and $\exists n \in \mathcal{Z}$ such that $a^n = 0$, then we say that a is nilpotent. An element $a \in A$ is invertible or a unit of A if it has an inverse in A that is $\exists b \in A$ such that $ab = 1$. An element $a \in A$ is idempotent if $a^2 = a$.

Exercise (1.9) (a) If a and b are nilpotent elements in A, show that:

(i) 1-a is invertible in A

(ii) $\alpha a + \beta b$ is nilpotent $\forall \; \alpha, \beta \in A$, so that the set of nilpotent elements of A is an ideal.

(b) If $a \in A$ is idempotent, show that:

(i) $b = 1 - a$ is idempotent

(ii) $a+b=1$

(iii) $ab=0$. In this case we say that a and b are complementary orthogonal idempotent.

By writing $x=xa+x(1-a)$ for any $x \in A$, we see that A is a direct sum of rings $A=A_1 \oplus A_2$ where $A_1 = Aa$ and $A_2 = A(1-a)$.

Proposition (1.10) Every nilpotent element is a zero divisor.

Exercise (1.11) Let A be a commutative ring with 1 and let X be the set of all units of A. Show that X is an abelian group.

Definition (1.12) Let I be an ideal of A. I is said to be generated by $x \in A$ if $(x) = I = \{xa : a \in A\}$.

Recall that a field is an integral domain A in which every nonzero element is a unit. Every field is an integral domain but the converse is false.

Theorem (1.13) Let A be a nonzero ring. Then the following are equivalent:

(i) A is a field.

(ii) (0) and (1) are the only ideals of A.

(iii) Every homomorphism $f : A \to B$ where B is a nonzero ring is injective.

Exercise (1.14) Let I and J be ideals of a ring A. Then

(i) $I+J=\{i+j : i \in I, j \in J\}$,

(ii) $I \cap J$,

(iii) $IJ=\{\sum_k^n i_k j_k : i_k \in I, j_k \in J\}$,

(iv) $(I:J)=\{a \in A : aJ \subseteq I\}$

are ideals of A.

Definition (1.15) I+J is called the ideal generated by I and J, (I:J) is called the ideal quotient of I and J and IJ is called the product of I and J. Generally, if I_p is any family of ideals of A, then $\cap I_p$ is also an ideal of A.

Example (1.16) Let $A=\mathcal{Z}$, $I=<a>, J=<b>$. Compute:

(i) $I \cap J$

(ii) $I+J$

(iii) IJ.

Solution:(i) $I \cap J = <[a,b]>$.

(ii) $I+J=<(a,b)>$.

(iii) $IJ=<ab>$.

Example (1.17) Let $A=\mathcal{Z}$. Compute (I:J) given that

(i) $I=<5>, J=<20>$

(ii) $I =< 60 >, J =< 70 >$

(iii) $I =< 42 >, J =< 132 >$.

Solution: (i) By definition,

$$(I : J) = (< 5 >:< 20 >) = \{a \in A : a < 20 > \subseteq < 5 >\}$$

and thus we have $20pa = 5q$ so that $20m = 5q$ and therefore we have $m = q/4$. Since m is an integer, we must have $q = 0, \pm 4, \pm 8, \pm 12, \pm 16 \cdots$ and so, $m = 0, \pm 1, \pm 2, \pm 3, \pm 4 \cdots$. Hence $(< 5 >:< 20 >) = \mathcal{Z} =< 1 >$. Similarly, we obtain $(< 60 >:< 70 >) =< 6 >$ and $(< 42 >:< 132 >) =< 7 >$ (iii) $I =< 42 >, J =< 132 >$.

Definition (1.18) (i) An ideal M in a ring A is called maximal if $M \neq A$ and M is such that if I is an ideal of A with $M \subseteq I \subseteq A$ then $I = M$ or $I = R$.

(ii) An ideal P in a ring A is called a prime ideal if I and J are ideals in A such that $IJ \subseteq P$, then $I \subseteq P$ or $J \subseteq P$.

Example (1.19) In any integeral domain, (0) is a prime ideal. A commutative ring A is an integral domain iff (0) is a prime ideal of A. For each prime integer p, the ideal (p) in $\mathcal{Z}$ is a prime ideal.

Theorem (1.20) (i) P is a prime ideal iff A/P is an integral domain.

(ii) M is a maximal ideal iff A/M is a field.

Corrolary (1.21) A maximal ideal is a prime ideal.

Proof: Suppose that M is maximal. Then A/M is a field so that A/M is an integral domain and hence M is prime. In general, the converse is false.

Theorem (1.22) Let $\phi : A \to B$ be a ring homomorphism.

(i) If P is a prime ideal in B, then $\phi^{-1}(P)$ is a prime ideal in A.

(ii) If M is a maximal ideal in B, it is not true that $\phi^{-1}(M)$ is maximal in A. To see this, consider the inclusion map $\psi : \mathcal{Z} \to \mathcal{Q}$. it is clear that (0) is maximal in $\mathcal{Q}$ because $\mathcal{Q}$ is a field but then $\phi^{-1}((0)) = (0)$ and (0) is not maximal in $\mathcal{Z}$ since $\mathcal{Z}$ is not a field.

Theorem (1.23) Every nonempty commutative ring A with 1 has at least one maximal ideal.

Corrolary (1.24)(i) Let I be an ideal of A. Then I is contained in a maximal ideal of A.

(ii) Every nonunit of A is contained in a maximal ideal.

Definition (1.25) A ring A is called a local ring if it has exactly one maximal ideal. Every field is a local ring.

Theorem (1.26) (i) Let A be a ring and let $M \neq (1)$ be an ideal of A such that every $x \in A - M$ is a unit in A. Then A is a local ring and M is its maximal ideal.

(ii) Let A be a ring and M a maximal ideal of A such that every element of 1+M is a unit in A. Then A is a local ring.

Definition (1.27)(i) A ring with finite number of maximal ideals is called a semi-local ring.

(ii) A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Theorem(1.28) If A is a PID then every prime ideal is maximal.

Proposition (1.29) Let N be the set of all nilpotent elements in a ring A. Then:

(i) N is an ideal of A,

(ii) A/N has no nilpotent element different from 0.

Definition (1.30) The ideal N of Theorem (1.29) is called the nilradical of A denoted by nilrad A. A is said to be a reduced ring if $nilradA = 0$.

Definition (1.31) The Jacobson radical of A is the intersection of all the maximal ideals of A.

Proposition (1.32) The nilradical of A is the intersection of all the prime ideals.

Proposition (1.33) $x \in J$ iff 1-xy is a unit in A for all y in A.

Definition (1.34) Let J be any ideal of A.

(i) The ideal quotient (0,J) is called the annihilator of J and it is denoted by Ann(J). It is the set of all x in A such that $xJ = 0$.

(ii) The radical of J denoted by r(J) is the set

$$r(J) = \{x \in A : x^n \in J \text{ for some } n > 0.$$

SPECIMEN QUESTIONS

1. (a) Let e and I be an element and a subset in a ring A respectively. When do we say that:

    i. e is idempotent ?

    ii. I is a prime ideal ?

    iii. I is a maximal ideal ?

    iv. A is an integral domain ?

    v. A is a division ring ?

    vi. A is a Boolean ring ?

   (b) If A has more than one element and if $ax = b$ has a solution $\forall \ (a \neq 0) \in A$ and $\forall \ b \in A$, show that A is a division ring.

   (c) Let A be a commutative ring with unity and let M and P be any two ideals of A. Show that:

i. P is prime iff A/P is an integral domain,

ii. M is maximal iff A/M is a field,

iii. A maximal ideal of A is prime ideal in A. Give an example to show that the converse is false,

iv. If A is a Boolean ring, then each prime ideal $P \neq A$ is maximal.

2. (a) Let A be a commutative ring and let M and P be any two ideals of A. Define the following:

i. M+P, when is M and P coprime or comaximal?

ii. $M \cap P$,

iii. MP,

iv. (M:P), the ideal quotient of M and P,

v. Ann(M), the annihilator of M,

vi. r(M), the radical of M,

vii. J(M), the Jacobson radical of M,

viii. N(M), the nilradical of M.

(b) Show that:

i. MP is an ideal of A,

ii. (M:P) is an ideal of A,

iii. r(M) is an ideal of A,

iv. $a \in J(M)$ iff (1-ab) is a unit in A $\forall\, b \in A$,

v. $(M : P)P \subseteq M$,

vi. $r(r(M)) = r(M)$,

vii. r(M) is the intersection of all prime ideals containing M,

viii. M and P are coprime iff r(M) and r(P) are coprime.

(c) Let $A = \mathcal{Z}$ and let $M = (42)$ and $P = (132)$. Compute the following:

i. M+P,

ii. $M \cap P$,

iii. MP,

iv. (M:P).

2. Modules

Definition (2.1) Let A be a commutative ring. An A-module is an abelian group (M,+) on which A acts linearly. It is a pair (M, μ) where (M,+) is an abelian group and $\mu : A \times M \to M$ such that if we write ax for $\mu(a, x)$ with $a \in A, x \in M$, the following axioms are satisfied:

(i) $a(x + y) = ax + ay$,

(ii) $(a + b)x = ax + bx$,

(iii) $(ab)x = a(bx)$,

(iv) $1x = x$, for all $a, b \in A, x, y \in M$.

Equivalently, (M,+) is an abelian group together with a ring homomorphism $A \to E(M)$, where E(M) is the ring of endomorphisms of the abelian group M.

The notion of a module is a common generalization of several concepts for example, vector spaces. If A is a field, then an A-module M is an A-vector space or a vector space M over the field A.

Example (2.2) (i) An Ideal I of A is an A-module. In particular A itself is an A-module.

(ii) If A is a field K, then A-module is K-vector space.

(iii) If $A = \mathcal{Z}$, then $\mathcal{Z}$-module is an abelian group.

(iv) If $A = K[x]$, where K is a field, an A-module is a K-vector space with a linear transformation.

(v) If G is a finite group, $A = K(G)$ is a group algebraof G over the field K, thus A is not commutative unless G is. Then A-module is the K-representation of G.

(vi) If V is a vector space over a field F, then V is an F-module.

Definition (2.3) Let M and N be A-modules. A mapping $f : M \to N$ is an A-module homomorphism or is A-linear if

$$\begin{aligned} f(x + y) &= f(x) + f(y), \\ f(ax) &= af(x), \quad \forall\ x, y \in M, \quad a \in A. \end{aligned}$$

If A is a field, an A-module homomorphism is the same as a linear transformation of vector spaces.

It can easily be shown that the composition of A-module homomorphisms is again an A-module homomorphism.

The set of all A-homomorphisms from M to N can be made an A-module by defining (f+g) and (af) by

$$(f + g)(x) = f(x) + g(x),$$

$$(af)(x) \quad = \quad af(x), \quad \forall\ x \in M.$$

With this definition, it can easily be checked that the axioms for an A-module is satisfied. This A-module is denoted by Hom(M,N).

Definition (2.4) A submodule N of an A-module M is a subgroup of M which is closed under multiplication by elements of A. The abelian group M/N then inherits an A-module structure from M, defined by $a(x + N) = ax + N$. The A-module M/N is the quotient of M by N. The natural map $\phi : M \to M/N$ is an A-homomorphism.

If $f : M \to N$ is an A-homomorphism, the kernel of of f is the set

$$Ker\ f = \{x \in M : f(x) = 0\}$$

and is a submodule of M. The image of f is the set

$$Imf = f(M)$$

and is a submodule of N. The cokernel of f is

$$coker\ f = N/Imf$$

which is a quotient module of N.

Definition (2.5) Let M be an A-module and let $\{M_i\}$ be a family of A submodules of M. Their sum $\sum M_i$ is the set of all finite sums x_i where $\{x_i \in M_i\}$ for all i and almost all the x_i are zero. $\sum M_i$ is the smallest submodule of M which contains all the M_i.

The intersection $\cap M_i$ is again a submodule of M. Thus the submodules of M form a complete lattice with respect to inclusion.

Proposition (2.6) (i) If L, M and N are A-modules such that $N \subseteq M \subseteq L$, then

$$[L/N]/[M/N] \cong L/M.$$

(ii) If P and Q are submodules of M, then

$$[P + Q]/P \cong Q/[P \cap Q].$$

Definition (2.7) Let M be an A-module and let I be an ideal of A. The product IM is the set of all finite sums $\sum a_i x_i$ with $a_i \in I, x_i \in M$ and it is a submodule of M.

If N and P are A-submodules of M, (N:P) is defined to be the set of all $a \in A$ such that $aP \subseteq N$. It is a an ideal of A. In particular, (0:M) is the set of all $a \in A$ such that $aM = 0$. This is also an ideal called the annihilator of M and is denoted by Ann(M). If $I \subseteq Ann(M)$, we may regard M as an A/I-module as follows:

If $\overline{x} \in A/I$ is represented by $x \in A$, define $\overline{x}m$ to be xm with $m \in M$: this is independent of the choice of the representation x of $\overline{x}$, since $IM = 0$.

Definition (2.8) An A-module M is faithful if $Ann(M) = 0$. If $Ann(M) = I$, then M is faithful an an A/I-module.

Proposition (2.9) (i) If M and N are A-modules, then

$$Ann(M + N) = Ann(M) \cap Ann(N).$$

(ii) If N and P are A-submodules of M, then

$$(N : P) = Ann((N + P)/N).$$

Definition (2.10) If S is a subset of an A-module M, then (S) will denote the intersection of all the submodules of M that contains S. This is called the submodule of M generated by S, while the elements of S are called generators of (S).

Thus (S) is a submodule of M that contains S and it is contained in every submodule of M that contains S, that is (S) is the smallest submodule of M containing S. If $S = \{x_1, \cdots x_n\}$ we write $(x_1, \cdots x_n)$ for the submodule generated by S.

Lemma (2.11) Let M be an A-module and let $S \subseteq M$.

(i) If $S = \emptyset$ then $(S) = \{0\}$.

(ii) If $S \neq \emptyset$ then

$$(S) = \left\{ \sum_{i=1}^{n} a_i s_i : n \in \mathcal{N}, a_i \in A, s_i \in S \right\}.$$

Definition (2.12) An A-module M is said to be finitely generated if $M = (S)$ for some finite subset S of M.

M is said to be cyclic if $M = (m)$ for some element $m \in M$. If M is finitely generated, then let $\mu(M)$ denote the minimal number of generators of M. If M is not finitely generated, then we define $\mu(M) = \infty$. $\mu(M)$ is called the rank of M.

Remark (2.13) (i) By (2.11)(i), we have $\mu(\{0\}) = 0$ and $M \neq \{0\}$ is cyclic iff $\mu(M) = 1$.

(ii) The concept of cyclic A-module generalizes the concept of cyclic group. Thus an abelian group G is cyclic iff it is a cyclic $\mathcal{Z}$-module.

(iii) If A is a PID, then any A-submodule M of A is an ideal, and so $\mu(M) = 1$.

If M is a finitely generated A-module and N is any submodule, then M/N is clearly finitely generated, and in fact, $\mu(M/N) \leq \mu(M)$ since the image in M/N of any generating set of M is a generating set of M/N.

Proposition (2.14) Suppose that M is an A-module and N is a submodule. If N and M/N are finitely generated then

$$\mu(M) \leq \mu(N) + \mu(M/N).$$

Definition (2.15) If $\{N_\alpha\}$ is a family of A-modules of M, then the submodule generated by N_α is $(\cup_\alpha N_\alpha)$. This is just the set of all sums $n_{\alpha_1} + n_{\alpha_2} + \cdots + N_{\alpha_k}$ where $n_{\alpha_i} \in N_{\alpha_i}$ that is $\sum_{\alpha \in \lambda} N_\alpha$. If λ is a finite set then $\lambda = \{1, 2, \ldots, m\}$ and we write $\sum_{\alpha=1}^{m} N_\alpha$ for the submodule generated by $N_1, N_2, \cdots, N_m$.

Proposition (2.16) Let A be a ring and let $M = (m)$ be a cyclic A-module. Then

$$M \cong A/Ann(m).$$

Corrolary (2.17) If F is a field and M is a nonzero cyclic F-module, then $M \cong F$.

Definition (2.18) Let M be an A-module and let $I \subseteq A$ be an ideal. Then

$$IM = \left\{ \sum_{i=1}^{n} a_i m_i : n \in \mathcal{Z}, a_i \in I, m_i \in M \right\}.$$

The set IM is clearly a submodule of M. The product IM is a generalization of the concept of product of ideals.

Remark (2.19) If A is commutative and $I \subseteq Ann(M)$, then there is a map

$$[A/I] \times M \rightarrow M$$

defined by $(a + I)m = am$.

Definition (2.20) Let A be an integral domain and let M be an A-module. An element $x \in M$ is a torsion element if $Ann(x) \neq \{0\}$. Thus an element $x \in M$ is torsion iff there exists an $a \neq 0 \in A$ such that $ax = 0$. Let M_τ be the set of torsion elements of M. M is said to be torsion-free if $M_\tau = \{0\}$, and M is a torsion module if $M = M_\tau$.

Proposition (2.21) Let A be an integral domain and let M be an A-module. Then

(i) M_τ is a submodule of M, called the torsion submodule.

(ii) M/M_τ is torsion-free.

Example (2.22) (i) If G is an abelian group, then the torsion $\mathcal{Z}$-module of G is the set of all elements of G of finite order. Thus $G = G_\tau$, meaning that every element of G is of finite. In particular, any finite abelian group is torsion. The converse is not true. For example if we take $G = \mathcal{Q}/\mathcal{Z}$, then $\mid G \mid = \infty$, but every element of $\mathcal{Q}/\mathcal{Z}$ has finite order since $q(p/q + \mathcal{Z}) = p + \mathcal{Z} = 0 \in \mathcal{Q}/\mathcal{Z}$. Thus $(\mathcal{Q}/\mathcal{Z})_\tau = \mathcal{Q}/\mathcal{Z}$.

(ii) An abelian group is torsion-free if it has no elements of finite order other than zero. For example, let us take $G = \mathcal{Z}^n$ for any natural number n.
(iii) Let $V = F^2$ and consider the linear transformation $T : F^2 \to F^2$ defined by $T(u, v) = (v, 0)$. Then F[X] module V_T determined by T is a torsion module. In fact $Ann\,(V_T) = (X^2)$.
Proposition (2.23) Let A be an integral domain and let M be a finitely generated torsion A-module. Then $Ann(M) \neq (0)$. In fact, if $M = (x_1, x_2, \cdots, x_n)$, then

$$Ann(M) = Ann(x_1) \cap \cdots \cap Ann(x_n) \neq (0).$$

Proposition (2.24) Let F be a field and let V be a vector space over F, that is an F-module. Then V is torsion-free.
Definition (2.25) Let M and N be A-modules. $M \oplus N$ the direct sum of M and N is defined by

$$M \oplus N = \{(x, y) : x \in M, y \in N\}.$$

This can be made an A-module if we define addition and scalar multiplication by

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d), \\ r(a, b) &= (ra, rb). \end{aligned}$$

More generally, if $\{M_i\}_{i\in\lambda}$ is any family of A-modules, then their direct sum $\oplus_{i\in\lambda} M_i$ is a set whose elements are families $(x_i)_{i\in\lambda}$ such that $x_i \in M_i$ for each $i \in \lambda$ and almost all x_i are zero.
Definition (2.6) An A-module M is said to be free if it is isomorphic to an A-module of the form $\oplus_{i\in\lambda} M_i$ where each $M_i \cong A$ as an A-module.
Remark (2.27) The direct sum has an important homomorphism property, which, can be used to characterize direct sum. To see this, suppose that $f_i : M_i \to N$ are A-module homomorphisms. Then there is a map

$$f : M_1 \oplus \cdots \oplus M_n$$

defined by

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n} f_i(x_i).$$

It can be easily be checked that f is an A-module homomorphism.
Theorem (2.28) Let M be an A-module and let $M_1, M_2, \cdots, M_n$ be submodules such that
(i) $M_1 + M_2 + \cdots + M_n$, and
(ii) for $1 \leq i \leq n$,

$$M_i \cap (M_1 + \cdots + M_{i-1} + \cdots + M_n) = 0.$$

Then $M \cong M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

Proposition (2.29) M is a finitely generated A-module iff M is isomorphic to a quotient of A^n for some integer $n > 0$.

Proposition (2.30) Let M be a finitely generated A-module, let I be an ideal of A, and let ϕ be an A-module endomorphism of M such that $\phi(M) \subseteq IM$. Then ϕ satisfies the equation of the form

$$\phi^n + a_1\phi^{n-1} + a_2\phi^{n-2} + \cdots + a_n = 0, \quad a_i \in I.$$

Corrolary (2.31) Let M be a finitely generated A-module and let I be an ideal of A such that $IM = M$. Then there exists $x \equiv 1 mod I$ such that $xM = 0$.

Proposition (2.32) [**Nakayama's Lemma**] Let M be a finitely generated A-module and I an ideal of A contained in the Jacobson radical J of A. Then $IM = M$ implies that $M = 0$.

Corrolary (2.33) Let M be a finitely generated A-module, N a submodule of M, $I \subseteq J$ an ideal. Then

$$M = IM + N \quad \Rightarrow \quad M = N.$$

Definition (2.34) If M is an A-module and $M_1 \subseteq M$ is a submodule, we say that M_1 is a direct summand of M, or is complemented in M, if there is a submodule $M_2 \subseteq M$ such that $M_1 \cong M_1 \oplus M_2$.

SPECIMEN QUESTIONS

1. Define the following:

    (a) Module,

    (b) Submodule,

    (c) Faithful module,

    (d) Cyclic module,

    (e) Torsion module,

    (f) Free module,

    (g) Quotient module,

    (h) A-module homomorphism,

    (i) Exact sequence,

    (j) Cokernel.

2. (a) If A is a field K, show that an A-module M is a K-vector space.

(b) Let M and N be A-modules and let $\mathrm{Hom}_A(M, N)$ be the set of all A-homomorphisms from M into N. Define $\forall\ f, g \in \mathrm{Hom}_A(M, N)$ and $\forall\ x \in M$:

$$\begin{aligned}(f+g)(x) &= f(x)+g(x),\\ (af)(x) &= af(x), a \in A.\end{aligned}$$

Show that $\mathrm{Hom}_A(M, N)$ is an A-module.

(c) Let M, M', N, N' be A-modules and let $u : M' \to M$ and $v : N \to N'$ be A-module homomorphisms which induce the mappings

$$\bar{u} : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N),$$

$$\bar{v} : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'),$$

respectively defined by

$$\begin{aligned}\bar{u}(f) &= f \circ u,\\ \bar{v}(f) &= v \circ f, \quad \forall\ f \in \mathrm{Hom}_A(M, N).\end{aligned}$$

Show that $\bar{u}$ and $\bar{v}$ are A-homomorphisms.

3. (a) If M and N are A-modules, show that

$$Ann(M+N) = Ann(M) \cap Ann(N).$$

(b) If N and P are A-submodules of an A-module M, show that

$$(N : P) = Ann((N+P)/N).$$

(c) Let $M = (m)$ be a cyclic A-module. Show that

$$M \cong A/Ann(m).$$

(d) Show that M is a finitely generated A-module iff M is isomorphic to a quotient of A^n for some integer $n > 0$.

References

1. Atiyah M.F. and Macdonald I., Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass., 1969.

2. Cohn P.M., Algebra, Wiley, London, 1989.

3. Miles Reid, Undergraduate Commutative Algebra, London Mathematical Society Texts **29**, Cambridge University Press, 1995.