DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTER OF SCIENCE-MATHEMATICS

SEMESTER -II

THEORY OF RINGS AND MODULES

DEMATH-2 ELEC-4

BLOCK-2

UNIVERSITY OF NORTH BENGAL

Postal Address:

The Registrar,

University of North Bengal,

Raja Rammohunpur,

P.O.-N.B.U.,Dist-Darjeeling,

West Bengal, Pin-734013,

India.

Phone: (O) +91 0353-2776331/2699008

Fax:(0353) 2776313, 2699001

Email: regnbu@sancharnet.in ; regnbu@nbu.ac.in

Wesbsite: www.nbu.ac.in

First Published in 2019

FOREWORD

The Self-Learning Material (SLM) is written with the aim of providing simple and organized study content to all the learners. The SLMs are prepared on the framework of being mutually cohesive, internally consistent and structured as per the university's syllabi. It is a humble attempt to give glimpses of the various approaches and dimensions to the topic of study and to kindle the learner's interest to the subject

We have tried to put together information from various sources into this book that has been written in an engaging style with interesting and relevant examples. It introduces you to the insights of subject concepts and theories and presents them in a way that is easy to understand and comprehend.

We always believe in continuous improvement and would periodically update the content in the very interest of the learners. It may be added that despite enormous efforts and coordination, there is every possibility for some omission or inadequacy in few areas or topics, which would definitely be rectified in future.

We hope you enjoy learning from this book and the experience truly enrich your learning and help you to advance in your career and future endeavours.

THEORY OF RING AND MODULE

BLOCK -1

BLOCK-2

BLOCK-2 THEORY OF RING AND MODULE

Introduction to block

Unit 8 FREE MODULE, CYCLIC MODULE SIMPLE AND SEMI-SIMPLE : This unit deals with free module, Cyclic Module and its properties also simple and semi-simple module.

Unit 9 PROJECTIVE AND INJECTIVE MODULE : This unit deals with projective and injective module and its properties.

Unit 10 FLAT MODULE, GENERATED MODULE OVER PID: This unit deals with flat module , generated module and its properties also deals with generated module over PID

Unit 11 EMBEDDING INJECTIVE MODULE: This unit deals with Embedding Injective module and its proof with example

Unit 12 TENSOR PRODUCT OF MODULE : This Unit deals with tensor product of Module and its example

Unit 13 CHAIN CONDITIONS ON MODULE : This unit deals with chain conditions on module and its properties with example

Unit 14 NOETHERIAN AND ARTINIAN MODULES : This unit deals with primary composition and Noetherian and Artinian module with its properties also with examples.

UNIT 8 - FREE MODULE, CYCLIC MODULE SIMPLE AND SEMI-SIMPLE MODULE

STRUCTURE

Notes

8.12 Answer to check your progress

8.0 OBJECTIVE

* Learn How to multiply cyclic module and know about Jacobson of Semi-Simple Sodule.

* Learn Properties of P-Be'Zout Module

* Learn Isotopic Component of Semi-Simple Module

* Learn Length of Semi-Simple Module

8.1 INTRODUCTION: FREE MODULE

In mathematics, a **free module** is a module that has a basis that is, a generating set consisting of linearly independent elements.
Every vector space is a free module, but, if the ring of the coefficients is not a division ring (not a field in the commutative case), then there exist non-free modules.

Given any set *S* and ring *R*, there is a free *R*-module with basis *S*, which is called the *free module on S* or *module of formal R-linear combinations* of the elements of *S*.

A free abelian group is precisely a free module over the ring **Z** of integers.

8.1.1 Definition

For a ring R and an R-module R, the set E ⊂ *F* is a basis for M if:

- E is a generating set for M; that is to say, every element of M is a finite sum of elements of E multiplied by coefficients in R; and
- E is linearly independent, that is, R for R distinct elements of M implies that r1 = r2 = r3……… (where Om is the zero element

  of M and 0 is the zero element of M).

A free module is a module with a basis.

An immediate consequence of the second half of the definition is that the coefficients in the first half are unique for each element of *M*.

If R has invariant basis number, then by definition any two bases have the same cardinality. The cardinality of any (and therefore every) basis is called the **rank** of the free module M. If this cardinality is finite, the free module is said to be *free of rank n*, or simply *free of finite rank.*

8.1.2 Examples

Let *R* be a ring.

- *R* is a free module of rank one over itself (either as a left or right module); any unit element is a basis.
- More generally, a (say) left ideal *I* of *R* is free if and only if it is a principal ideal generated by a left nonzerodivisor, with a generator being a basis.
- If *R* is commutative, the polynomial ring R(x) in indeterminate *X* is a free module with a possible basis 1, *X*, X^2, ...
- Let A(t) be a polynomial ring over a commutative ring *A*, *f* a monic polynomial of degree *d* there, B = A(t) and € the image of *t* in *B*. Then *B* contains *A* as a subring and is free as an *A*-module with a basis .
- For any non-negative integer *n*, Rn = R x R x R x R x …………………, the cartesian product of *n* copies of *R* as a left *R*-module, is free. If *R* has invariant basis number (which is true for commutative *R*), then its rank is *n*.
- A direct sum of free modules is free, while an infinite cartesian product of free modules is generally *not* free (cf. the Baer–Specker group.)

8.1.3 Formal Linear Combinations

Given a set *E* and ring *R*, there is a free *R*-module that has *E* as a basis: namely, the direct sum of copies of *R* indexed by *E*

Explicitly, it is the submodule of the cartesian product E (*R* is viewed as say a left module) that consists of the elements that have only finitely many nonzero components. One can embed *E* into $R^{(E)}$ as a subset by identifying an element *e* with that of $R^{(E)}$ whose *e*-th component is 1 (the unity of *R*) and all the other components are zero. Then each element of $R^{(E)}$ can be written uniquely as where only finitely many E are nonzero. It is called a *formal linear combination* of elements of *E*.

A similar argument shows that every free left (resp. right) *R*-module is isomorphic to a direct sum of copies of *R* as left (resp. right) module.

8.1.4 Generalizations

Many statements about free modules, which are wrong for general modules over rings, are still true for certain generalisations of free modules. Projective modules are direct summands of free modules, so one can choose an injection in a free module and use the basis of this one to prove something for the projective module. Even weaker generalisations are flat modules, which still have the property that tensoring with them preserves exact sequences, and torsion-free modules. If the ring has special properties, this hierarchy may collapse, e.g., for any perfect local Dedekind ring, every torsion-free module is flat, projective and free as well. A finitely generated torsion-free module of a commutative PID is free. A finitely generated *Z*-module is free if and only if it is flat.

8.2 CYCLIC MODULE

In mathematics, more specifically in ring theory, a **cyclic module** or **monogenous module** is a module over a ring that is generated by one element. The concept is analogous to cyclic group, that is, a group that is generated by one element.

A **cyclic module** (or more specifically, a cyclic left R-module over a ring R) is a module that is generated by a single element—the analogue of a cyclic group for modules.

In a left R-module M, the cyclic submodule generated by an element α is often denoted $\langle\alpha\rangle$.

Every cyclic left R-module is isomorphic to a quotient module of the left-regular module over R (that is, a quotient module of R as a left R-module).

8.2.1 Definition

A left *R*-module *M* is called **cyclic** if *M* can be generated by a single element i.e. $M = (x) = Rx = \{rx \mid r \in R\}$ for some *x* in *M*. Similarly, a right *R*-module *N* is cyclic if $N = yR$ for some $y \in N$.

8.2.2 Examples

- Every cyclic group is a cyclic **Z**-module.
- Every simple *R*-module *M* is a cyclic module since the submodule generated by any nonzero element *x* of *M* is necessarily the whole module *M*.
- If the ring *R* is considered as a left module over itself, then its cyclic submodules are exactly its left principal ideals as a ring. The same holds for *R* as a right *R*-module, mutatis mutandis.
- If *R* is *F*[*x*], the ring of polynomials over a field *F*, and *V* is an *R*-module which is also a finite-dimensional vector space over F, then the Jordan blocks of *x* acting on *V* are cyclic submodules. (The Jordan blocks are all isomorphic to $F[x] / (x - \lambda)^n$; there may also be other cyclic submodules with different annihilators; see below.)

8.2.3 Problem

- (a) Prove that a nonzero R-module M is irreducible if and only if M is a cyclic module with any nonzero element as its generator.
- (b) Determine all the irreducible Z-modules.

(a) Prove that a nonzero R-module M is irreducible if and only if M is a cyclic module with any nonzero element as its generator.

(⟹) Suppose that M is an irreducible module.

Let a∈M be any nonzero element and consider the

submodule (a) generated by the element a.

Since a is a nonzero element, the submodule (a) is non-zero. Since Mis irreducible, this yields that

$$M=(a).$$

Hence M is a cyclic module generated by a Since aa is any nonzero element, we conclude that the module M is a cyclic module with any nonzero element as its generator.

(⟸) Suppose that M is a cyclic module with any nonzero element as its generator.

Let N be a nonzero submodule of M. Since N is non-zero, we can pick a nonzero element $a \in N$. By assumption, the non-zero element aa generates the module M.

Thus we have

$$(a) \subset N \subset M = (a).$$

It follows that N=M, and hence M is irreducible.

(b) Determine all the irreducible Z-modules.

By the result of part (a), any irreducible Z-module is generated by any nonzero element.

We first claim that M cannot contain an element of infinite order.

Suppose on the contrary $a \in M$ has infinite order.

Then since M is irreducible, we have

$$M = (a) \cong Z.$$

Since Z-module Z has, for example, a proper submodule 2Z, it is not irreducible. Thus, the module M is not irreducible, a contradiction.

It follows that any irreducible Z-module is a finite cyclic group.

(Recall that any Z-module is an abelian group.)

We claim that its order must be a prime number.

Suppose that $M = Z/nZ$, where $n = ml$ with $m, l > 1$,.

Then

$(\bar{l}) = \{l + nZ, 2l + nZ, \dots, (m-1)l + nZ\}$

is a proper submodule of M, and it is a contradiction.

Thus, n must be prime.

We conclude that any irreducible Z-module is a cyclic group of prime order.

Problem. 1) Let R be a commutative ring with unity and I, J some ideals of R. If there exists a surjective R-module homomorphism $f : R/I \longrightarrow R/J$, then $I \subseteq J$.

2) Show that the result in 1) may not be true in noncommutative rings.

Solution. 1) We have $f(r+I) = 1+J$, for some $r \in R$. Now if $s \in I$, then $sr \in I$ and thus

$$s + J = s(1+J) = sf(r+I) = f(sr+I) = 0.$$

So $s \in J$.

2) Let R be the ring of 2×2 matrices with, say, real entries. Let $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : \ a, b \in \mathbb{R} \right\}$ and $J = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} : \ a, b \in \mathbb{R} \right\}$. See that I, J are left ideals of R and that I is not contained in J. Now define $f : R/I \longrightarrow R/J$ in this way: for any $r = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$ we define $f(r+I) = \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} + J$. It is easy to see that f is a well-defined R-module homomorphism. Also, f is surjective because if $r = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R$ and $s = \begin{pmatrix} 0 & b-a \\ 0 & d-c \end{pmatrix} \in R$, then $f(s+I) = s+J = r+J$, because $r - s \in J$. $\square$

Theorem Let R be a commutative ring and M be a cyclic multiplication module. If every finitely generated prime submodules of M are maximal and for every maximal submodules N of M, there exist ideal I of R such that IM ⊆ N with I ⊆ Rad(R). Then M is a P-Be´zout.

Proof. Let N be a finitely generated prime submodule of M. By hipothesis of theorem yields that N is a maximal submodule and the same way, there exist ideal I of R such that IM ⊆ N with I ⊆ Rad(R). So N + IM = M and hence N = M .. Therefore N is cyclic submodule since M is a cyclic module.

Since every finitely generated prime submodules of M is cyclic then M is a P-B´ezout module. ✷

Theorem Let R be a Noetherian P-Be´zout ring and M be a faithful multiplication module. Then every prime submodules of M are finitely generated and of the form rM for is a prime ideal of R. Furthermore, if either M is a cyclic or simple module then M is P-Be´zout.

Proof. Let N be a prime submodule of M, (N : M) is prime ideal of R. Since R is a Noetherian ring then (N : M) is finitely generated ideal and hence (N : M) is principle by R is a P-B´ezout. Let (N : M) = Rr for r ∈ R. So N = (N : M)M = rM since M is a multiplication module. Since M is a faithful multiplication module hence N is finitely generated. Therefore N is finitely generated and of the form rM for is a prime ideal of R.

Let m ∈ M so that N = rM = rRm = Rrm since M is a cyclic module and hence N is cyclic submodule since N = Rx for x = rm ∈ M. Since every finitely generated prime submodules of M is cyclic then M is a P-B´ezout module.

Pure submodule of M is only 0 Since M is a simple module. If N = 0 clear that N is cyclic finitely generated prime submmodule and hence M is a P-B´ezout module. ✷

8.2.4 Properties Of P-Be´Zout Module

The ring which considered in this paper is commutative with an identity and will be denoted by R. The concept of P-B´ezout ring was introduced and studied in Bakkari [1] as a generalization of the B´ezout ring. A ring R is said to be P-B´ezout if every finitely generated prime ideal I over R is principle.

We will adapt that concept into module. A module M over R is said to be P-B´ezout if every finitely generated prime submodule N of M is cyclic. See [3] for example. Let R be a commutative ring with an identity and M be a cyclic multiplication R-module which has some properties of its submodule, we prove that M is P-B´ezout module.

Lemma Let R be a commutative ring, M be a module over R and N be a prime submodule of M. Then ideal (N : M) of R is prime.

Proof. Suppose AB ⊆ (N : M) for A and B are ideals of R. By definition of annihilator (N : M), it yields (N : M)M ⊆ N and hence ABM ⊆ N since ABM ⊆ (N : M)M. Furthermore, by N is a prime submodule then A ⊆ (N : M) or B ⊆ (N : M) since BM ⊆ N. Since A ⊆ (N : M) or B ⊆ (N : M) so that (N : M) is prime ideal has proved. ✷

The first theorem, we mean, as follows:

Theorem Let R be a Noetherian P-Be´zout ring and M be a faithful multiplication module. Then every prime submodules of M are finitely generated and of the form rM for is a prime ideal of R. Furthermore, if either M is a cyclic or simple module then M is P-Be´zout.

Proof. Let N be a prime submodule of M. By Lemma 3.1, (N : M) is prime ideal of R. Since R is a Noetherian ring then (N : M) is finitely generated ideal and hence (N : M) is principle by R is a P-B´ezout. Let (N : M) = Rr for r ∈ R. So N = (N : M)M = rM since M is a multiplication module. Since M is a faithful multiplication module hence N is finitely generated. Therefore N is finitely generated and of the form rM for is a prime ideal of R.

Let m ∈ M so that N = rM = rRm = Rrm since M is a cyclic module and hence N is cyclic submodule since N = Rx for x = rm ∈ M. Since every finitely generated prime submodules of M is cyclic then M is a P-B´ezout module.

Pure submodule of M is only 0 Since M is a simple module. If N = 0 clear that N is cyclic finitely generated prime submmodule and hence M is a P-B´ezout module.

Check in Progress –I

Note: i) Write your answers in the space given below.

Notes

Q. 1 Let R be a commutative ring, M be a module over R and N be a prime submodule of M. Then ideal (N : M) of R is prime.

Solution.

…………………………………………………………………………..

……………………………………………………………………………

…………………………………………………………………………….

Q. 2Let R be a commutative ring with unity and I, J some ideals of R. If there exists a surjective R-module homomorphism $f : R/I \longrightarrow R/J$, then $I \subseteq J$.

Solution.

…………………………………………………………………………..

……………………………………………………………………………

…………………………………………………………………………….

8.3 CYCLIC AND MULTIPLICATION MODULE

An R-module M is said to be cyclic if it has one generator, that is if M = Rm for some m ∈ M. Similarly, M is finitely generated if it has finitely generators, that is if M = Rm1 + Rm2 + Rm3 + ... + Rmn for finitely many mi ∈ M. A module M is said to be Noetherian if every submodule of M is finitely generated.

The annihilator of M is denoted Ann(M). For any submodule N of M, the annihilator of the factor module M/N will be denoted by (N : M) so that (N : M) = {r ∈ R|rM ⊆ N}. We can see that (N : M) is an ideal of R. A module M is said to be faithful if Ann(M)=0}. A module M is said to be multiplication module if for any submodule N of M, there exist an ideal I of R such that N = IM. It was proven that M is a multiplication module if and only if N = (N : M)M for every submodule N of M. A proper submodule N of M over R is said to be prime if rm ∈ N for r ∈ R and m ∈ M implies that either m ∈ N or r ∈ (N : M). It clear that N is prime submodule of M if IK ⊆ N for submodule K of M and ideal I of R implies that either K ⊆ N or I ⊆ (N : M).

Some properties which used in later section is given as follow. Let M be a faithful multiplication R-module. has proved that M is finitely generated. Let M be a multiplication R-module, N be a submodule of M and let I be an ideal of R contained in the Jacobson radical of R. Ghalanzarzadeh at all [6, Corollary 3.10] said that if IM + N = M then N = M.

Definition. Let R be a ring with unity and let M be an R-module. The annihilator of M in R is defined by $\text{ann}_R(M) = \{r \in R : \ rx = 0, \ \forall x \in M\}$. We say that M is **faithful** if $\text{ann}_R(M) = (0)$.

Remark. Every free R-module is faithful. To see this, let M be a free R-module and let $r \in \text{ann}_R(M)$. If $x \in M$ is an element of a basis of M, then $rx = 0$ implies that $r = 0$ and so M is faithful.

Example 1. Let $R_1, \ldots, R_n, \ n \geq 2$, be some rings with unity and put $R = \bigoplus_{i=1}^n R_i$. Clearly R_1 is an R-module.
Let $K = \bigoplus_{i=2}^n R_i$. Then $R = R_1 \oplus K$ and thus, by Corollary 1 in this post, R_1 is a projective R-module. But $(0, 1, \ldots, 1) \in \text{ann}_R(R_1)$ and hence, by the above remark, R_1 is not free. A similar argument shows that each R_i is a projective but not free R-module. As an example, we know from the Chinese remainder theorem that if $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ is the prime factorization of n, then $\frac{\mathbb{Z}}{n\mathbb{Z}} = \bigoplus_{i=1}^r \frac{\mathbb{Z}}{p_i^{k_i}\mathbb{Z}}$. Thus each $\frac{\mathbb{Z}}{p_i^{k_i}\mathbb{Z}}$ is a projective but not free $\frac{\mathbb{Z}}{n\mathbb{Z}}$ – module.

Example 2. Let k be a field and $R = M_2(k)$, the ring of 2×2 matrices with entries in k. Let

$$P = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : \ \ a, b \in k \right\}.$$

Clearly P is an R-module and $R \cong P \oplus P$, as R-modules. Thus P is a projective R-module. Suppose that P is free and $\{x_i : \ i \in I\}$ is a basis for P. Then, since $\dim_k R = 4$, we have $\dim_k P = 4|I|$. But, by the definition of P, we also have $\dim_k P = 2$. So $2 = 4|I|$, which is absurd. Hence P is not free. You can extend this argument to $R = M_m(k)$, where $m \geq 2$ is any integer. Then each column space of R will be a projective but not a free R-module. □

The next two examples are important in the theory of Azumaya algebras.

Example 3. Let R be a commutative ring and let P_1, P_2 be (finitely generated) projective R-modules. Then $P_1 \otimes_R P_2$ is a (finitely generated) projective R-module.

Proof. So there exist R-modules K_i and free R-modules F_i such that $P_i \oplus K_i = F_i, \ i = 1, 2$. So $F_1 \cong R^m, \ F_2 = R^n$, where m (resp. n) is finite if P_1 (resp. P_2) is finitely generated. See that $R^{mn} \cong F_1 \otimes_R F_2 \cong (P_1 \otimes_R P_2) \oplus K$, where $K \cong (P_1 \otimes_R K_2) \oplus (P_2 \otimes_R K_1) \oplus (K_1 \otimes_R K_2)$. □

Example 4. Let R be a commutative ring and let P be a finitely generated projective R-module. Then $\mathrm{End}_R(P)$ is a finitely generated projective R-module.

Proof. First note that if A is an R-module, then $\mathrm{End}_R(A)$ is an R-module too because we can define $(rf)(a) = f(ra)$ for all $r \in R, a \in A$ and $f \in \mathrm{End}_R(A)$. Now, since P is a finitely generated projective R-module, there exist an R-module K and a free R-module $F \cong R^n$ such that $F = P \oplus K$. Note that

$$\mathrm{End}_R(F) \cong \mathrm{End}_R(R^n) \cong M_n(R) \cong R^{n^2},$$

as R-modules, and so $\mathrm{End}_R(F)$ is a (finitely generated) free R-module. On the other hand by Theorem 1. Now identify $\text{End}_R(P)$ with $\begin{pmatrix} \text{End}_R(P) & 0 \\ 0 & 0 \end{pmatrix}$ and let $f_1 : \text{End}_R(P) \longrightarrow \text{End}_R(F)$ be the inclusion map. Define the map $f_2 : \text{End}_R(F) \longrightarrow \text{End}_R(P)$ by

$$f_2\left(\begin{pmatrix} u & v \\ w & t \end{pmatrix}\right) = \begin{pmatrix} u & 0 \\ 0 & 0 \end{pmatrix},$$

for all $u \in \text{End}_R(P), v \in \text{Hom}_R(K, P), w \in \text{Hom}_R(P, K), t \in \text{End}_R(K).$ Clearly f_1, f_2 are $\text{End}_R(F)$-module homomorphisms and $f_2 f_1$ is the identity map. Thus, by Lemma 3 in this post, $R^{n^2} \cong \text{End}_R(F) \cong \text{End}_R(P) \oplus \ker f_2.$ Therefore $\text{End}_R(P)$ is projective and since $\text{End}_R(F)$ is finitely generated, $\text{End}_R(P)$ is finitely generated too because $\text{End}_R(P) \cong \text{End}_R(F)/\ker f_2.$ □

Theorem. Let R be a commutative ring and let P_1, P_2 be finitely generated projective R-modules. Then, as R-modules, we have

$$\text{End}_R(P_1) \otimes_R \text{End}_R(P_2) \cong \text{End}_R(P_1 \otimes_R P_2).$$

Proof. A nice challenge for the reader! □

8.4 PROJECTIVE MODULES; DEFINITIONS & BASIC FACTS

Corollary 1. An R-module P is projective if and only if there exists an R-module K such that $P \oplus K$ is free.

Proof. If $P \oplus K$ is free, then P is projective by Lemma 2 in part (1). Conversely, suppose that P is projective. By Remark 2 in part (1), there exists an exact sequence $0 \longrightarrow K \xrightarrow{f_1} F \xrightarrow{f_2} P \longrightarrow 0,$ where F is free. This sequence splits by the theorem in part (1), i.e. $P \oplus K \cong F.$ □

Corollary 2. A finitely generated R-module P is projective if and only if there exists an R-module K such that $P \oplus K$ is a finitely generated free R-module, i.e. $P \oplus K \cong R^n$ for some integer $n \geq 1.$

Proof. One side is obvious by Corollary 1 (or Lemma 2 in part (1)). Conversely, suppose that $P = \sum_{i=1}^n Rx_i$ is a finitely generated projective R-module. Let $\{e_1, \ldots, e_n\}$ be a basis for R^n and define the map $f_2 : R^n \longrightarrow P$ by $f_2(\sum r_i e_i) = \sum r_i x_i.$ Clearly f_2 is a well-defined onto R-module homomorphism. Let $K = \ker f_2.$ Then we have an exact sequence $0 \longrightarrow K \xrightarrow{f_1} R^n \xrightarrow{f_2} P \longrightarrow 0,$ where f_1 is the inclusion map. This sequence splits by the theorem in part (1), i.e. $P \oplus K \cong R^n.$ □

Corollary 3. Let $\{A_i : i \in I\}$ be a family of R -modules. Then $A = \bigoplus_{i \in I} A_i$ is projective if and only if A_i is projective for all $i \in I.$

Proof. Suppose first that A is projective and let $j \in I.$ By Corollary 1, there exists an R -module K and a free R -module F such that $F = A \oplus K.$ But then $F \cong A_j \oplus (\bigoplus_{i \in I, \ i \neq j} A_i \oplus K)$ and thus A_j is projective by Corollary 1 again. Conversely, suppose that each A_i is projective. Then for every $i \in I,$ there exists an R -module K_i and a free R -module F_i such that $F_i = A_i \oplus K_i.$ Let $F = \bigoplus_{i \in I} F_i$ and $K = \bigoplus_{i \in I} K_i.$ Then F is a free R-module and $F = A \oplus K.$ Thus A is projective. □

In the next post I will give a few examples of projective modules.

8.5 SIMPLE MODULES

A **simple module** over a ring R is a module that is simple as a group with operators—that is, it is a module with no submodules other than itself and the zero module, and it is not itself the zero module and scalar products are not all equal to 0.

If R is a commutative ring, then every simple module over R is isomorphic (as an R-module) to a quotient ring of R by a maximal ideal; that is, every simple module over R is isomorphic (as an R-module) to a quotient ring of R that is a field. This is not the case when R is not commutative. In this case, every simple left R-module is isomorphic (as a left R-module) to the quotient of R by a maximal left ideal.

For example, all simple modules over the ring of integers $\mathbb{Z}$ are of the form $\mathbb{Z}/p\mathbb{Z}$, where p is a prime. A more interesting example of a simple module is the (left) module of complex numbers over the ring $\mathbb{C}\langle x\rangle$ of complex numbers with a noncommuting indeterminate x adjoined, where x corresponds to complex conjugation.

In mathematics, specifically in ring theory, the **simple modules** over a ring *R* are the (left or right) modules over *R* that are not zero and have no non-zero proper submodules. Equivalently, a module *M* is simple if and only if every cyclic submodule generated by a non-zero element of *M* equals *M*. Simple modules form building blocks for the modules of finite length, and they are analogous to the simple groups in group theory.

In this article, all modules will be assumed to be right unital modules over a ring *R*.

8.6 EXAMPLES

Z-modules are the same as abelian groups, so a simple **Z**-module is an abelian group which has no non-zero proper subgroups. These are the cyclic groups of prime order.

If *I* is a right ideal of *R*, then *I* is simple as a right module if and only if *I* is a minimal non-zero right ideal: If *M* is a non-zero proper submodule of *I*, then it is also a right ideal, so *I* is not minimal. Conversely, if *I* is not minimal, then there is a non-zero right ideal *J* properly contained in *I*. *J* is a right submodule of *I*, so *I* is not simple.

If *I* is a right ideal of *R*, then *R*/*I* is simple if and only if *I* is a maximal right ideal: If *M* is a non-zero proper submodule of *R*/*I*, then the preimage of *M* under the quotient map $R \to R/I$ is a right ideal which is not equal to *R* and which properly contains *I*. Therefore, *I* is not maximal. Conversely, if *I* is not maximal, then there is a right ideal *J* properly containing *I*. The quotient map $R/I \to R/J$ has a non-zero kernel which is not equal to R/I, and therefore R/I is not simple.

Every simple *R*-module is isomorphic to a quotient R/m where *m* is a maximal right ideal of *R*. By the above paragraph, any quotient R/m is a simple module. Conversely, suppose that *M* is a simple *R*-module. Then, for any non-zero element *x* of *M*, the cyclic submodule *xR* must equal *M*. Fix such an *x*. The statement that $xR = M$ is equivalent to the surjectivity of the homomorphism $R \to M$ that sends *r* to *xr*. The kernel of this homomorphism is a right ideal *I* of *R*, and a standard theorem states that *M* is isomorphic to R/I. By the above paragraph, we find that *I* is a maximal right ideal. Therefore, *M* is isomorphic to a quotient of *R* by a maximal right ideal.

If *k* is a field and *G* is a group, then a group representation of *G* is a left module over the group ring *k[G]* (for details, see the main page on this relationship).[2] The simple *k[G]* modules are also known as **irreducible** representations. A major aim of representation theory is to understand the irreducible representations of groups.

A module is simple if it is non-zero and does not admit a proper non-zero submodule. Simplicity of a module M is equivalent to either of:

- Am = M for every m non-zero in M. simple module
- M ' A/m for some maximal left ideal of A.

In particular, simple modules are cyclic; and the annihilator of any non-zero element of a simple module is a maximal left ideal. The annihilator of a simple module is called a primitive ideal. The ring A is primitive ideal primitive if the zero ideal is primitive, or, equivalently, if A admits a faithful simple primitive ring module.

- A module may have no simple submodules. Indeed, simple submodules of AA are minimal left ideals, but there may not be any such (e.g., in Z).
- The module A is simple if and only if A is a division ring. In this case, any simple module is isomorphic to A.

• The Z-module Z/pnZ where p is a prime is indecomposable; it is simple if and only if n = 1.

Let A = Endk V for k a field and V a k-vector space. The set a of finite rank endomorphisms is a two-sided ideal of A. Let B be the subring A generated by the identity endomorphism and a. Then V is a simple B-module (in particular a simple A-module). And B (A if dimk V is infinite. Let W be a codimension 1 subspace of V . The endomorphisms killing W form a minimal left ideal in A (and in B). Thus A and B when dimk V is infinite give examples of primitive rings that admit non-trivial proper two-sided ideals.

Proposition . Let M be a finitely generated A-module and N (M a proper submodule. Then there exists a maximal submodule of M containing N.

Corollary . Let M be finitely generated non-zero. Then there exists a primitive ideal a such that aM (M.

Proof. Choose N maximal submodule and let a = Ann M/N.

When faithful modules with strong properties exist. If a ring admits faithful modules with strong properties (e.g., a primitive ring), then, as might be expected, the ring itself has strong properties

Proposition . Let M be faithful simple and l a minimal left ideal. Then M ' l

Proof. The submodule lM is non-zero by faithfulness. Choose m in M such that lm 6= 0. By simplicity, lm = M. The homomorphism l → M defined by a 7→ am has zero kernel because l is minimal.

Proposition . Let M be a faithful module admitting a composition series Σ. If the opposite of M is of finite type, then every simple A-module is a quotient in Σ.

Proof. Let {mi} be a finite generating set of M over the commutant of A. Consider the map a 7→ (ami) from A into ⨁iM. If ami = 0 for all i, then aM = 0 and so a = 0 by the faithfulness of M. Thus A imbeds into a finite number of copies of M. Every simple module being a quotient of A, we are done.

8.6.1 Basic Properties Of Simple Modules

The simple modules are precisely the modules of length 1; this is a reformulation of the definition.

Every simple module is indecomposable, but the converse is in general not true.

Every simple module is cyclic, that is it is generated by one element.

Not every module has a simple submodule; consider for instance the Z-module Z in light of the first example above.

Let *M* and *N* be (left or right) modules over the same ring, and let $f : M \to N$ be a module homomorphism. If *M* is simple, then *f* is either the zero homomorphism or injective because the kernel of *f* is a submodule of *M*. If *N* is simple, then *f* is either the zero homomorphism or surjective because the image of *f* is a submodule of *N*. If $M = N$, then *f* is an endomorphism of *M*, and if *M* is simple, then the prior two statements imply that *f* is either the zero homomorphism or an isomorphism. Consequently, the endomorphism ring of any simple module is a division ring. This result is known as Schur's lemma.

The converse of Schur's lemma is not true in general. For example, the Z-module Q is not simple, but its endomorphism ring is isomorphic to the field Q.

8.6.2 Simple Modules And Composition Series

If M is a module which has a non-zero proper submodule N, then there is a short exact sequence. A common approach to proving a fact about M is to show that the fact is true for the center term of a short exact sequence when it is true for the left and right terms, then to prove the fact for N and M/N. If N has a non-zero proper submodule, then this process can be repeated. This produces a chain of submodules.

In order to prove the fact this way, one needs conditions on this sequence and on the modules M_i/M_{i+1}. One particularly useful condition is that the length of the sequence is finite and each quotient module M_i/M_{i+1} is simple. In this case the sequence is called a **composition series** for M. In order to prove a statement inductively using composition series, the statement is first proved for simple modules, which form the base case of the induction, and then the statement is proved to remain true under an extension of a module by a simple module. For example, the Fitting lemma shows that the endomorphism ring of a finite length indecomposable module is a local ring, so that the strong Krull-Schmidt theorem holds and the category of finite length modules is a Krull-Schmidt category.

The Jordan–Hölder theorem and the Schreier refinement theorem describe the relationships amongst all composition series of a single module. The Grothendieck group ignores the order in a composition series and views every finite length module as a formal sum of simple modules. Over semisimple rings, this is no loss as every module is a semisimple module and so a direct sum of simple modules. Ordinary character theory provides better arithmetic control, and uses simple **C***G* modules to understand the structure of finite groups *G*. Modular representation theory uses Brauer characters to view modules as formal sums of simple modules, but is also interested in how those simple modules are joined together within composition series. This is formalized by studying the Ext functor and describing the module category in various ways including quivers (whose nodes are the simple modules and whose edges are composition series of non-semisimple modules of length 2) and Auslander–Reiten theory where the associated graph has a vertex for every indecomposable module.

8.6.3 The Jacobson Density Theorem

An important advance in the theory of simple modules was the Jacobson density theorem. The Jacobson density theorem states:

Let U be a simple right R-module and write D = $\mathrm{End}_R(U)$. Let A be any D-linear operator on U and let X be a finite D-linearly independent subset of U. Then there exists an element r of R such that x·A = x·r for all x in X.

In particular, any primitive ring may be viewed as (that is, isomorphic to) a ring of *D*-linear operators on some *D*-space.

A consequence of the Jacobson density theorem is Wedderburn's theorem; namely that any right artinian simple ring is isomorphic to a full matrix ring of *n* by *n* matrices over a division ring for some *n*. This can also be established as a corollary of the Artin–Wedderburn theorem.

Check in Progress –II

Note: i) Write your answers in the space given below.

Q. 1 State Jacob Denisity theorem..

Solution.

……………………………………………………………………..

…………………………………………………………………………

………………………………………………………………………….

Q. 2An R-module P is projective if and only if there exists an R-module K such that $P \oplus K$ is free $I \subseteq J.$

Solution.

……………………………………………………………………..

…………………………………………………………………………

………………………………………………………………………….

8.7 SEMI-SIMPLE MODULES

A **semisimple module** is, informally, a module that is not far removed from simple modules. Specifically, it is a module M with the following property: for every submodule $N \subset M$, there exists a submodule $N' \subset M$ such that $N + N' = M$ and $N \cap N' = 0$, where by 0 we mean the zero module.

In mathematics, especially in the area of abstract algebra known as module theory, a **semisimple module** or **completely reducible module** is a type of module that can be understood easily from its parts. A ring that is a semisimple module over itself is known as an Artinian **semisimple ring**. Some important rings, such as group rings of finite groups over fields of characteristic zero, are semisimple rings. An Artinian ring is initially understood via its largest semisimple quotient. The structure of Artinian semisimple rings is well understood by the Artin–Wedderburn theorem, which exhibits these rings as finite direct products of matrix rings.

8.7.1 Definition

A module over a (not necessarily commutative) ring with unity is said to be **semisimple** (or **completely reducible**) if it is the direct sum of simple (irreducible) submodules.

For a module *M*, the following are equivalent:

1. *M* is semisimple; i.e., a direct sum of irreducible modules.
2. *M* is the sum of its irreducible submodules.
3. Every submodule of *M* is a direct summand: for every submodule *N* of *M*, there is a complement *P* such that $M = N \oplus P$.

For 3 →2 , the starting idea is to find an irreducible submodule by picking any nonzero x € M and letting P be a maximal submodule such that $x \notin P$. It can be shown that the complement of P is irreducible.[1]

The most basic example of a semisimple module is a module over a field; i.e., a vector space. On the other hand, the ring **Z** of integers is not a semisimple module over itself (because, for example, it is not an artinian ring.)

Semisimple is stronger than completely decomposable, which is a direct sum of indecomposable submodules.

Let *A* be an algebra over a field *k*. Then a left module *M* over *A* is said to be **absolutely semisimple** if, for any field extension *F* of *k*, $F \oplus M$ is a semisimple module over $F \otimes M$.

A module is semisimple if it satisfies any of the following equivalent conditions:

• it is a sum of simple submodules.

• it is a direct sum of simple submodules.

• every submodule has a complement.

Before turning to the proof of the equivalence of the three conditions, let us observe that the third condition passes to submodules and quotient modules. Indeed, every quotient is isomorphic to a sub (M/N ' Q, where Q is a complement of N), so it is enough to observe the passage for submodules. If P ⊆ N are submodules, and Q is a complement of P in M, then Q ∩ N is a complement of P in N as is easily verified.

Now we prove the equivalence of the three conditions. The second clearly implies the first. Now suppose that the first holds and let N be a submodule. Choose, by Zorn, a submodule maximal P with respect to the following two properties: it is a sum of simple submodules; it intersects N trivially. If N ⊕ P (M, then there is a simple submodule S of M that is not contained in N +P. This means S∩(N +P) = 0, by the simplicity of S, so N ∩ (S + P) = 0. Since S + P) P, the maximality of P is violated. Thus N ⊕ P = M, and the third conditon holds.

Suppose now that the third condition holds. We will show that the second holds too. Choose, by Zorn, a maximal collection C of simple submodules whose sum is their direct sum. Let N be the sum of submodules in such a collection, and suppose that N (M. Choose y ∈ M ⊆ N. Choose, by Zorn, a maximal submodule P of Ay. Let S be complement to P in Ay (it exists by the observation we made before beginning the proof). Being isomorphic to Ay/P, it is simple. And its existence violates the maximality of the collection C, which finishes the proof.

8.7.2 Classification Of Semi-Simple Modules

It happens that semisimple modules have a convenient classification (assuming the axiom of choice). To prove this classification, we first state some intermediate results.

Proposition. Let M be a semisimple left R-module. Then every submodule and quotient module of M is also simple.

Proof. First, suppose that N is a submodule of M. Let T be a submodule of N, and let N' be a submodule of M such that $T \cap N' = 0$ and $T + N' = M$. We note that if $\tau \in T$ and $\nu' \in N$ are elements such that $\tau + \nu' \in N$, then $\nu' \in N$. It follows that

$N = M \cap N = (T + N') \cap N = T + (N' \cap N)$.
Since $T \cap (N' \cap N) = 0$, it follows that N is semisimple.

Now let us consider a quotient module M/N of M, with ϕ the canonical homomorphism $M \to M/N$. Let T be a submodule of M/N. Then $\phi^{-1}(T)$ is a submodule of M, so there exists a submodule $N' \subset M$ such that $\phi^{-1}(T) \cap N' = 0$ and $\phi^{-1}(T) + N' = M$. Then in M/N, since ϕ is surjective,

$$T + \phi(N') = \phi\big(\phi^{-1}(T) + N'\big) = \phi(M) = M/N$$
$$T \cap \phi(N') = \phi\big(\phi^{-1}(T)\big) \cap \phi(N') \subset \phi\big(\phi^{-1}(T) \cap N'\big) = \phi(0) = 0.$$

Therefore M/N is semisimple as well.

Lemma 1. Let R be a ring, and let M be a nonzero cyclic left R-module. Then M contains a maximal proper submodule.

Proof. Let α be a generator of M. Let $\mathfrak{S}$ be the set of submodules that avoid α, ordered by inclusion. Then $\mathfrak{S}$ is nonempty, as $\{0\} \in \mathfrak{S}$. Also, if $(N_i)_{i\in I}$ is a nonempty chain in $\mathfrak{S}$, then $\bigcup_{i\in I} N_i$ is an element of $\mathfrak{S}$, as this is a submodule of M that does not contain α. Then $\bigcup_{i\in I} N_i$ is an upper bound on the chain (N_i); thus every chain has an upper bound. Then by Zorn's Lemma, $\mathfrak{S}$ has a maximal element. ■

Lemma 2. Every cyclic semisimple module has a simple submodule.

Proof. Let M be a cyclic semisimple module, and let α be a generator for M. Let N be a maximal proper submodule of M (as given in Lemma 1), and let N' be a submodule such that $N + N' = M$ and $N \cap N' = 0$. We claim that N' is simple.

Indeed, suppose that T is a nonzero submodule of N'. Since the sum $N + N'$ is direct, it follows that the sum $N + T$ is direct. Since $N + T$ strictly contains N, it follows that $N + T = M$, so $N' \subset N + T$; it follows that $N' = T$; thus N' is simple. ■

Theorem. Let M be a left R-module, for a ring R. The following are equivalent:

1. M is a semisimple R-module;
2. M is isomorphic to a direct sum of simple left R-modules;
3. M is isomorphic to an (internal) sum of R-modules.

Facts about semisimple modules.

(1) A simple module is semisimple. Vector spaces (over division rings) are semisimple. The ring Z is not a semisimple module over itself.

(2) Let M be a sum of simple submodules Ni , i ∈ I. For any submodule N, there exists a subset J of I such that N is isomorphic to the direct sum of Nj , j ∈ J; and there exists a subset K of I such that the direct sum of Nk, k ∈ K, is a complement of N. In particular, M/N ' ⊕k∈KNk.

(3) Subquotients of semisimple modules are semisimple.

8.7.3 Isotypic Components Of Semi-Simple Modules.

For an isomorphism class λ of simple modules, we denote by Mλ the sum of submodules of M that are isomorphic to a representative in the class λ. We call Mλ the λ-isotypic component.

• The isotypic components are semisimple (by definition); their sum is direct.

• N = ⊕λ(N ∩ Mλ) for any submodule N of a semisimple module M.

• The λ-isotypic is mapped to the λ-isotypic under homomorphisms.

• The only submodules that are preserved by all endomorphisms of a semisimple module are the isotpyic components and their sums.

8.7.4 Length Of A Semi-Simple Module

Let M be a semisimple module. If ⊕i∈IMi and ⊕j∈JMj are two expressions for M as a direct sum of simple submodules, then I and J have the same cardinality, which we then call the length of M and denote by `A M. If S is a simple module, we denote by [M : S] the length of the S-isotypic component of M.

• When `A M is finite, M has a composition series, and `A M coincides with Jordan-H¨older length of M.

• Two semisimple modules are isomorphic if and only if their S-isotypic lengths are equal for every simple module S.

• A semisimple module has finite length if and only if it is finitely generated.

• The length of a vector space equals the cardinality of a base.

8.8 SUMMARY

We study in this unit semi simple modules. We study Jacobson Density Theorem. We study free module and cyclic module with its examples. We study length of semi simple module. We study formal linear combinators. We study cyclic and projective module. We study The concept of P-B´ezout ring and module.

1. For a ring R and an R-module R, the set E ⊂ F is a basis for M if:

   E is a generating set for M; that is to say, every element of M is a finite sum of elements of E multiplied by coefficients in R; and

   E is linearly independent, that is, R for R distinct elements of M implies that

   r1 = r2 = r3……… (where Om is the zero element of M and 0 is the zero element of M).

2. A cyclic module (or more specifically, a cyclic left R-module over a ring R) is a module that is generated by a single element—the analogue of a cyclic group for modules.

3. A left *R*-module *M* is called cyclic if *M* can be generated by a single element i.e. $M = (x) = Rx = \{rx \mid r \in R\}$ for some x in *M*. Similarly, a right *R*-module *N* is cyclic if $N = yR$ for some $y \in N$.

4. Let R be a commutative ring and M be a cyclic multiplication module. If every finitely generated prime submodules of M are maximal and for every maximal submodules N of M, there exist ideal I of R such that IM ⊆ N with I ⊆ Rad(R). Then M is a P-Be´zout.

5. A semisimple module is, informally, a module that is not far removed from simple modules. Specifically, it is a module M with the following property: for every submodule $N \subset M$, there exists a submodule $N' \subset M$ such that $N + N' = M$ and $N \cap N' = 0$, where by 0 we mean the zero module.
6. A module over a (not necessarily commutative) ring with unity is said to be semisimple (or completely reducible) if it is the direct sum of simple (irreducible) submodules.

For a module *M*, the following are equivalent:

M is semisimple; i.e., a direct sum of irreducible modules.

M is the sum of its irreducible submodules.

Every submodule of *M* is a direct summand: for every submodule *N* of *M*, there is a complement *P* such that $M = N \oplus P$.

8.9 KEYWORD

Cyclic : Occurring In Cycles; Regularly Repeated

Isotypic : Isotypic (Comparative More Isotypic, Superlative Most Isotypic) (Geology, Of A Crystalline Mineral) Having A Chemical Formula Whose Structure Is Similar To That Of Another

Summands : A Quantity To Be Added To Another

Irreducible : Not Able To Be Reduced Or Simplified

8.10 QUESTIONS FOR REVIEW

Q. 1 Let R be a commutative ring with 1 and let M be an R-module. Prove that the R-module M is irreducible if and only if M is isomorphic to R/I, where I is a maximal ideal of R, as an R-module.

Q 2 Let R be a ring with 1.
A nonzero R-module M is called **irreducible** if 0 and M are the only submodules of M.
(It is also called a **simple** module.)

Q3 Prove that a nonzero R-module M is irreducible if and only if M is a cyclic module with any nonzero element as its generator.

(b) Determine all the irreducible Z-modules.

Q. 4Let R be a commutative ring with 1 and let M be an R-module. Prove that the R-module M is irreducible if and only if M is isomorphic to R/I, where I is a maximal ideal of R, as an R-module.

8.11 SUGGESTION READING AND REFERENCES

1. *Adamson, Iain T. (1972). Elementary Rings and Modules. University Mathematical Texts. Oliver and Boyd. pp. 65–66. ISBN 0-05-002192-3. MR 0345993.*
2. *Keown, R. (1975). An Introduction to Group Representation Theory. Mathematics in science and engineering.* ***116****. Academic Press. ISBN 978-0-12-404250-6. MR 0387387.*
3. *Govorov, V. E. (2001) [1994], "Free module", in Hazewinkel, Michiel (ed.), Encyclopedia of Mathematics, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4.*
4. *B. Hartley; T.O. Hawkes (1970). Rings, modules and linear algebra. Chapman and Hall. pp. 77, 152. ISBN 0-412-09810-5.*
5. *Lang, Serge (1993), Algebra (Third ed.), Reading, Mass.: Addison-Wesley, pp. 147–149, ISBN 978-0-201-55540-0, Zbl 0848.13001*
6. [1] Chahrazade Bakkari, On P-b´ezout rings, International Journal of Algebra, 3 (2009), 669 - 673.
7. [2] A. Barnard, Multiplication modules, Journal of Algebra, 71 (1981), 174 - 178.
8. [3] Muhamad Ali Misri, Irawati and Hanni Garminia Y., Generalization of b´ezout module, Far East Journal of Mathematical Sciences (FJMS), Accepted.
9. [4] Dong-Soo Lee and Hyun-Bok Lee, Some remarks on faithful multiplication modules, Journal of The Chungcheong Mathematical Society, 6 (1993), 131 - 137.

10. [5] Donald S. Passman, A Course in Ring Theory, Wadsworth & Brooks/Cole Advanced Books & Software, USA, 1991.
11. [6] Sh. Ghalanzarzadeh, P Malakoti Rad and S. Shirinkam, Multiplication modules and Cohen theorem, Mathematical Sciences, 2 (2008), 251-260

8.12 ANSWER TO CHECK YOUR PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 2.4

Q 2 Check in Section 2.3

Check in Progress-II

Answer Q. 1 Check in Section 5.4

Q 2 Check in Section 4

UNIT 9 - PROJECTIVE AND INJECTIVE MODULE

STRUCTURE

9.0 OBJECTIVE

- We learn in this unit Projective and Injective Module
- Learn polynomial ring
- Work with Self Injective Ring
- Work with Artinian Example
- Work with Projective module over commutative Ring

9.1 INTRODUCTION: PROJECTIVE MODULE

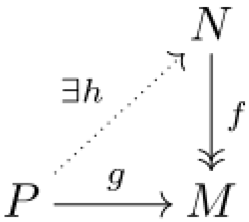
In mathematics, particularly in algebra, the class of **projective modules** enlarges the class of free modules (that is, modules with basis vectors) over a ring, by keeping some of the main properties of free modules. Various equivalent characterizations of these modules appear below.

A free module is a projective module, but the converse may not hold over some rings, such as Dedekind rings. However, every projective module is a free module if the ring is a principal ideal domain such as the integers, or a polynomial ring (this is the Quillen–Suslin theorem).

Projective modules were first introduced in 1956 in the influential book *Homological Algebra* by Henri Cartan and Samuel Eilenberg.

Definition

The usual category theory definition is in terms of the property of *lifting* that carries over from free to projective modules: a module P is projective if and only if for every surjective module homomorphism $f : N \twoheadrightarrow M$ and every module homomorphism $g : P \rightarrow M$, there exists a homomorphism $h : P \rightarrow N$ such that $fh = g$. (We don't require the lifting homomorphism *h* to be unique; this is not a universal property.)



The advantage of this definition of "projective" is that it can be carried out in categories more general than module categories: we don't need a notion of "free object". It can also be dualized, leading to injective modules. The lifting property may also be rephrased as *every morphism from P to M factors through every epimorphism to M*. Thus, by definition, projective modules are precisely the projective objects in the category of *R*-modules.

9.1.1 Split-Exact Eequences

A module *P* is projective if and only if every short exact sequence of modules of the form is a split exact sequence. That is, for every surjective module homomorphism $f : B \twoheadrightarrow P$ there exists a **section map**, that is, a module homomorphism $h : P \to B$ such that $f \circ h = \mathrm{id}_P$. In that case, $h(P)$ is a direct summand of *B*, *h* is an isomorphism from *P* to $h(P)$, and $h \circ f$ is a projection on the summand $h(P)$. Equivalently.

9.1.2 Exactness

An *R*-module *P* is projective if and only if the covariant functor Hom(*P*,-): *R*-Mod → AB is an exact functor, where *R*-Mod is the category of left *R*-modules and AB the category of abelian groups. When the ring *R* is commutative, AB is advantageously replaced by *R*-Mod in the preceding characterization. This functor is always left exact, but, when *P* is projective, it is also right exact. This means that *P* is projective if and only if this functor preserves epimorphisms (surjective homomorphisms), or if it preserves finite colimits.

9.1.3 Elementary Examples And Properties

The following properties of projective modules are quickly deduced from any of the above (equivalent) definitions of projective modules:

Notes

- Direct sums and direct summands of projective modules are projective.
- If $e = e^2$ is an idempotent in the ring R, then Re is a projective left module over R.

Relation to Other Module-Theoretic Properties

The relation of projective modules to free and flat modules is subsumed in the following diagram of module properties:

The left-to-right implications are true over any ring, although some authors define torsion-free modules only over a domain. The right-to-left implications are true over the rings labeling them. There may be other rings over which they are true. For example, the implication labeled "local ring or PID" is also true for polynomial rings over a field: this is the Quillen–Suslin theorem.

9.1.4 Projective Vs. Free Modules

Any free module is projective. The converse is true in the following cases:

- if R is a field or skew field: *any* module is free in this case.
- if the ring R is a principal ideal domain. For example, this applies to $R = \mathbf{Z}$ (the integers), so an abelian group is projective if and only if it is a free abelian group. The reason is that any submodule of a free module over a principal ideal domain is free.
- if the ring R is a local ring. This fact is the basis of the intuition of "locally free = projective". This fact is easy to prove for finitely generated projective modules. In general, it is due to Kaplansky (1958).

In general though, projective modules need not be free:

- Over a direct product of rings $R \times S$ where R and S are nonzero rings, both $R \times 0$ and $0 \times S$ are non-free projective modules.

- Over a Dedekind domain a non-principal ideal is always a projective module that is not a free module.
- Over a matrix ring $M_n(R)$, the natural module R^n is projective but not free. More generally, over any semisimple ring, *every* module is projective, but the zero ideal and the ring itself are the only free ideals.

The difference between free and projective modules is, in a sense, measured by the algebraic *K*-theory group $K_0(R)$, see below.

9.1.5 Projective vs. Flat Modules

Every projective module is flat. The converse is in general not true: the abelian group **Q** is a **Z**-module which is flat, but not projective.

Conversely, a finitely related flat module is projective.

Govorov (1965) and Lazard (1969) proved that a module *M* is flat if and only if it is a direct limit of finitely-generated free modules.

In general, the precise relation between flatness and projectivity was established by Raynaud &Gruson (1971) (see also Drinfeld (2006) and Braunling, Groechenig& Wolfson (2016)) who showed that a module *M* is projective if and only if it satisfies the following conditions:

- *M* is flat,
- *M* is a direct sum of countably generated modules,
- *M* satisfies a certain Mittag-Leffler type condition

9.1.6 The Category Of Projective Modules

Submodules of projective modules need not be projective; a ring *R* for which every submodule of a projective left module is projective is called left hereditary.

Quotients of projective modules also need not be projective, for example **Z**/*n* is a quotient of **Z**, but not torsion free, hence not flat, and therefore not projective.

The category of finitely generated projective modules over a ring is an exact category. (See also algebraic K-theory).

9.1.7 Projective Resolutions

Given a module, M, a **projective resolution** of M is an infinite exact sequence of modules

$$\cdots \to P_n \to \cdots \to P_2 \to P_1 \to P_0 \to M \to 0,$$

with all the P_is projective. Every module possesses a projective resolution. In fact a **free resolution** (resolution by free modules) exists. The exact sequence of projective modules may sometimes be abbreviated to $P(M) \to M \to 0$ or $P_\bullet \to M \to 0$. A classic example of a projective resolution is given by the Koszul complex of a regular sequence, which is a free resolution of the ideal generated by the sequence.

The *length* of a finite resolution is the subscript n such that P_n is nonzero and $P_i = 0$ for i greater than n. If M admits a finite projective resolution, the minimal length among all finite projective resolutions of M is called its **projective dimension** and denoted pd(M). If M does not admit a finite projective resolution, then by convention the projective dimension is said to be infinite. As an example, consider a module M such that pd(M) = 0. In this situation, the exactness of the sequence $0 \to P_0 \to M \to 0$ indicates that the arrow in the center is an isomorphism, and hence M itself is projective.

9.1.8 Projective Modules Over Commutative Rings

Projective modules over commutative rings have nice properties.

The localization of a projective module is a projective module over the localized ring. A projective module over a local ring is free. Thus a projective module is *locally free* (in the sense that its localization at every prime ideal is free over the corresponding localization of the ring).

The converse is true for finitely generated modules over Noetherian rings: a finitely generated module over a commutative noetherian ring is locally free if and only if it is projective.

However, there are examples of finitely generated modules over a non-Noetherian ring which are locally free and not projective. For instance, a Boolean ring has all of its localizations isomorphic to $\mathbf{F}_2$, the field of two elements, so any module over a Boolean ring is locally free, but there are some non-projective modules over Boolean rings. One example is R/I where R is a direct product of countably many copies of $\mathbf{F}_2$ and I is the direct sum of countably many copies of $\mathbf{F}_2$ inside of R. The R-module R/I is locally free since R is Boolean (and it is finitely generated as an R-module too, with a spanning set of size 1), but R/I is not projective because I is not a principal ideal. (If a quotient module R/I, for any commutative ring R and ideal I, is a projective R-module then I is principal.)

However, it is true that for finitely presented modules M over a commutative ring R (in particular if M is a finitely generated R-module and R is noetherian), the following are equivalent.

1. M is flat.
2. M is projective.
3. M is free as R-module for every maximal ideal m of *R*.
4. M is free as R-module for every prime ideal m of *R*.
5. There exist f € R generating the unit ideal such that M is free as R-module for each *i*.
6. M is a locally free sheaf on R (where R is the sheaf associated to *M*.)

Moreover, if R is a noetherian integral domain, then, by Nakayama's lemma, these conditions are equivalent to

- The dimension of the R–vector space M is the same for all prime ideals r of *R*, where *R* is the residue field. That is to say, *M* has constant rank (as defined below).

Let A be a commutative ring. If B is a (possibly non-commutative) A-algebra that is a finitely generated projective A-module containing A as a subring, then A is a direct factor of B.

9.1.9 Rank

Let P be a finitely generated projective module over a commutative ring R and X be the spectrum of R. The *rank* of P at a prime ideal in X is the rank of the free R-module M. It is a locally constant function on X. In particular, if X is connected (that is if R or its quotient by its nilradical is an integral domain), then P has constant rank.

A basic motivation of the theory is that projective modules (at least over certain commutative rings) are analogues of vector bundles. This can be made precise for the ring of continuous real-valued functions on a compact Hausdorff space, as well as for the ring of smooth functions on a smooth manifold (see Serre–Swan theorem that says a finitely generated projective module over the space of smooth functions on a compact manifold is the space of smooth sections of a smooth vector bundle).

Vector bundles are *locally free*. If there is some notion of "localization" which can be carried over to modules, such as the usual localization of a ring, one can define locally free modules, and the projective modules then typically coincide with the locally free modules.

9.1.10 Projective Modules Over A Polynomial Ring

The Quillen–Suslin theorem, which solves Serre's problem, is another deep result: if K is a field, or more generally a principal ideal domain, and $R = K[X_1,...,X_n]$ is a polynomial ring over K, then every projective module over R is free. This problem was first raised by Serre with K a field (and the modules being finitely generated). Bass settled it for non-finitely generated modules and Quillen and Suslin independently and simultaneously treated the case of finitely generated modules.

Since every projective module over a principal ideal domain is free, one might ask this question: if R is a commutative ring such that every (finitely generated) projective R-module is free, then is every (finitely generated) projective $R[X]$-module free? The answer is *no*. A counterexample occurs with R equal to the local ring of the curve $y^2 = x^3$ at the origin. Thus the Quillen-Suslin theorem could never be proved by a simple induction on the number of variables.

Theorem 5. Every free module F over a ring R with identity is projective.

Proof. Assume that we are given a diagram of homomorphisms of unitary R-modules:

with g an epimorphism and F a free R-module on the set X (ι : X −→ F). For each x ∈ X, f(ι(x)) ∈ B. Since g is an epimorphism, there exists ax ∈

A with g(ax) = f(ι(x)). Since F is free, the map X −→ A given by x 7→ ax induces an R-module homomorphism h : F −→ A such that h(ι(x)) = ax for all x ∈ X. Consequently, ghι(x) = g(ax) = f ι(x) for all x ∈ X so that ghι = f ι : X −→ B. By the uniqueness part of the Theorem 4 we have gh = f. Therefore F is projective.

Corollary . Every module A over a ring R is the homomorphic image of a projective R-module.

Theorem. Let R be a ring. The following conditions on an R-module P are equivalent.

(1) P is projective;

(2) every short exact sequence 0 −→ A f −→ B g −→ P −→ 0 is split exact (hence B ∼= A ⊕ P);

(3) there is a free module F and an R-module K such that F ∼= K ⊕ P.

Proof. • (1) ⇒ (2)

with bottom row exact by the hypothesis. Since P is projective there is an R-module homomorphism h : P −→ B such that gh = 1p.

Therefore, the short exact sequence 0 −→ A f −→ B g h P −→ 0 is split and B ∼= A ⊕ P

. • (2) ⇒ (3there is free R-module F and an epimorphismg : F −→ P. If K = Ker g, then 0 −→ K ⊂ −→ι F g −→ P −→ 0 is exact. By hypothesis the sequence splits so that F ∼= K ⊕ P.

• (3) ⇒ (1) Let π be the composition F ∼= K ⊕P −→ P where the second map is the canonical projection. Similarly let ι be the composition P −→ K ⊕ P ∼= F with the first map the canonical injection. Given a diagram of R-module homomorphisms

Since F is projective by Theorem 5, there is an R-module homomorphism h1 : F −→ A such that gh1 = fπ. Let h = h1ι : P −→ A. Then gh = gh1ι = (fπ)ι = f(πι) = f1P = f. Therefore, P is projective.

Example . Projective but not free: If R = Z6, then Z3 and Z2 are Z6-modules and there is Z6-module isomorphism Z6 ∼= Z2 ⊕ Z3. Hence both Z2 and Z3 are projective Z6-modules that are not free Z6-modules.

Notes

Proposition 1. Let R be a ring. A direct sum of R-modules X i∈I Pi is projective iff each Pi is projective. Proof. Suppose PPi is projective. Since the proof of

(3) ⇒ (1) uses only the fact that F is projective, it remains valid with X i∈IPi , X i6=j Pi and Pj in place of F, K and P respectively. The converse is proved by similar techniques using the diagram

If each Pj is projective, then for each j there exists hj :Pj −→ A such that ghj = f ιj . Bthere is a unique homomorphism h :PPi −→ A with hιj = hj for every j and we also have gh = f.

Check In Progress-I

Note: i) Write your answers in the space given below.

Q. 1Define Projective Module.

Solution

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

Q.2Define Flat Module.

Solution

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

9.2 INJECTIVE MODULE

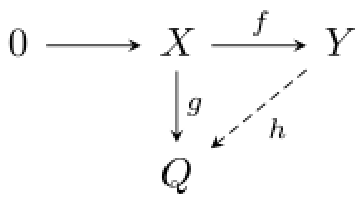
In mathematics, especially in the area of abstract algebra known as module theory, an **injective module** is a module *Q* that shares certain desirable properties with the **Z**-module **Q** of all rational numbers. Specifically, if *Q* is a submodule of some other module, then it is already a direct summand of that module; also, given a submodule of a module *Y*, then any module homomorphism from this submodule to *Q* can be extended to a homomorphism from all of *Y* to *Q*. This concept is dual to that of projective modules. Injective modules were introduced in (Baer 1940) and are discussed in some detail in the textbook (Lam 1999, §3).

Injective modules have been heavily studied, and a variety of additional notions are defined in terms of them: Injective cogenerators are injective modules that faithfully represent the entire category of modules. Injective resolutions measure how far from injective a module is in terms of the injective dimension and represent modules in the derived category. Injective hulls are maximal essential extensions, and turn out to be minimal injective extensions. Over a Noetherian ring, every injective module is uniquely a direct sum of indecomposable modules, and their structure is well understood. An injective module over one ring, may not be injective over another, but there are well-understood methods of changing rings which handle special cases. Rings which are themselves injective modules have a number of interesting properties and include rings such as group rings of finite groups over fields. Injective modules include divisible groups and are generalized by the notion of injective objects in category theory.

9.2.1 Definition

A left module Q over the ring R is injective if it satisfies one (and therefore all) of the following equivalent conditions:

- If Q is a submodule of some other left R-module M, then there exists another submodule K of M such that M is the internal direct sum of Q and K, i.e. $Q + K = M$ and $Q \cap K = \{0\}$.
- Any short exact sequence $0 \rightarrow Q \rightarrow M \rightarrow K \rightarrow 0$ of left R-modules splits.
- If X and Y are left R-modules, $f : X \rightarrow Y$ is an injective module homomorphism and $g : X \rightarrow Q$ is an arbitrary module homomorphism, then there exists a module homomorphism $h : Y \rightarrow Q$ such that $hf = g$, i.e. such that the following diagram commutes:



- The contravariant functor Hom(-,*Q*) from the category of left *R*-modules to the category of abelian groups is exact.

Injective right *R*-modules are defined in complete analogy.

9.2.2 Examples

Trivially, the zero module {0} is injective.

Given a field *k*, every *k*-vector space *Q* is an injective *k*-module. Reason: if *Q* is a subspace of *V*, we can find a basis of *Q* and extend it to a basis of *V*. The new extending basis vectors span a subspace *K* of *V* and *V* is the internal direct sum of *Q* and *K*. Note that the direct complement *K* of *Q* is not uniquely determined by *Q*, and likewise the extending map *h* in the above definition is typically not unique.

The rationals **Q** (with addition) form an injective abelian group (i.e. an injective **Z**-module). The factor group **Q**/**Z** and the circle group are also injective **Z**-modules. The factor group **Z**/*n***Z** for *n* > 1 is injective as a **Z**/*n***Z**-module, but *not* injective as an abelian group.

9.2.3 Commutative Examples

More generally, for any integral domain *R* with field of fractions *K*, the *R*-module *K* is an injective *R*-module, and indeed the smallest injective *R*-module containing *R*. For any Dedekind domain, the quotient module *K*/*R* is also injective, and its indecomposable summands are the localizations Rp/R for the nonzero prime ideals p. The zero ideal is also prime and corresponds to the injective *K*. In this way there is a 1-1 correspondence between prime ideals and indecomposable injective modules.

A particularly rich theory is available for commutative noetherian rings due to EbenMatlis, (Lam 1999, §3I). Every injective module is uniquely a direct sum of indecomposable injective modules, and the indecomposable injective modules are uniquely identified as the injective hulls of the quotients R/P where P varies over the prime spectrum of the ring. The injective hull of R/P as an R-module is canonically an R_P module, and is the R_P-injective hull of R/P. In other words, it suffices to consider local rings. The endomorphism ring of the injective hull of R/P is the completion R of R at P.

Two examples are the injective hull of the **Z**-module **Z**/*p***Z** (the Prüfer group), and the injective hull of the $k[x]$-module k (the ring of inverse polynomials). The latter is easily described as $k[x,x^{-1}]/xk[x]$. This module has a basis consisting of "inverse monomials", that is x^{-n} for $n = 0, 1, 2, \ldots$. Multiplication by scalars is as expected, and multiplication by x behaves normally except that $x \cdot 1 = 0$. The endomorphism ring is simply the ring of formal power series.

9.2.4 Artinian Examples

If G is a finite group and k a field with characteristic 0, then one shows in the theory of group representations that any subrepresentation of a given one is already a direct summand of the given one. Translated into module language, this means that all modules over the group algebra kG are injective. If the characteristic of k is not zero, the following example may help.

If A is a unital associative algebra over the field k with finite dimension over k, then $\mathrm{Hom}_k(-, k)$ is a duality between finitely generated left A-modules and finitely generated right A-modules. Therefore, the finitely generated injective left A-modules are precisely the modules of the form $\mathrm{Hom}_k(P, k)$ where P is a finitely generated projective right A-module. For symmetric algebras, the duality is particularly well-behaved and projective modules and injective modules coincide.

For any Artinian ring, just as for commutative rings, there is a 1-1 correspondence between prime ideals and indecomposable injective modules. The correspondence in this case is perhaps even simpler: a prime ideal is an annihilator of a unique simple module, and the corresponding indecomposable injective module is its injective hull. For finite-dimensional algebras over fields, these injective hulls are finitely-generated modules .

Check In Progress-II

Note: i) Write your answers in the space given below.

Q. 1Define Injective Module.

Solution

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

Q.2Define Free Module.

Solution

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

9.2.5 Injective Cogenerators

Maybe the most important injective module is the abelian group **Q**/**Z**. It is an injective cogenerator in the category of abelian groups, which means that it is injective and any other module is contained in a suitably large product of copies of **Q**/**Z**. So in particular, every abelian group is a subgroup of an injective one. It is quite significant that this is also true over any ring: every module is a submodule of an injective one, or "the category of left *R*-modules has enough injectives." To prove this, one uses the peculiar properties of the abelian group **Q**/**Z** to construct an injective cogenerator in the category of left *R*-modules.

For a left *R*-module *M*, the so-called "character module" $M^+ = \mathrm{Hom}_{\mathbf{Z}}(M,\mathbf{Q}/\mathbf{Z})$ is a right *R*-module that exhibits an interesting duality, not between injective modules and projective modules, but between injective modules and flat modules (Enochs&Jenda 2001, pp. 78–80). For any ring *R*, a left *R*-module is flat if and only if its character module is injective. If *R* is left noetherian, then a left *R*-module is injective if and only if its character module is fla

9.2.6 Injective Resolutions

Every module M also has an **injective resolution**: an exact sequence of the form

$$0 \to M \to I^0 \to I^1 \to I^2 \to \ldots$$

where the I^j are injective modules. Injective resolutions can be used to define derived functors such as the Ext functor.

The *length* of a finite injective resolution is the first index n such that I^n is nonzero and $I^i = 0$ for i greater than n. If a module M admits a finite injective resolution, the minimal length among all finite injective resolutions of M is called its **injective dimension** and denoted id(M). If M does not admit a finite injective resolution, then by convention the injective dimension is said to be infinite. (Lam 1999, §5C) As an example, consider a module M such that id(M) = 0. In this situation, the exactness of the sequence $0 \to M \to I_0 \to 0$ indicates that the arrow in the center is an isomorphism, and hence M itself is injective.

Equivalently, the injective dimension of M is the minimal integer (if there is such, otherwise ∞) n such that Ext^N
$_A(-,M) = 0$ for all $N > n$.

9.2.7 Indecomposables

Every injective submodule of an injective module is a direct summand, so it is important to understand indecomposable injective modules, (Lam 1999, §3F).

Every indecomposable injective module has a local endomorphism ring. A module is called a *uniform module* if every two nonzero submodules have nonzero intersection. For an injective module M the following are equivalent:

- M is indecomposable
- M is nonzero and is the injective hull of every nonzero submodule
- M is uniform
- M is the injective hull of a uniform module
- M is the injective hull of a uniform cyclic module
- M has a local endomorphism ring

Over a Noetherian ring, every injective module is the direct sum of (uniquely determined) indecomposable injective modules. Over a commutative Noetherian ring, this gives a particularly nice understanding of all injective modules, described in (Matlis 1958). The indecomposable injective modules are the injective hulls of the modules R/p for p a prime ideal of the ring R. Moreover, the injective hull M of R/p has an increasing filtration by modules M_n given by the annihilators of the ideals p^n, and M_{n+1}/M_n is isomorphic as finite-dimensional vector space over the quotient field $k(p)$ of R/p to $\mathrm{Hom}_{R/p}(p^n/p^{n+1}, k(p))$.

9.2.8 Change Of Rings

It is important to be able to consider modules over subrings or quotient rings, especially for instance polynomial rings. In general, this is difficult, but a number of results are known, (Lam 1999, p. 62).

Let S and R be rings, and P be a left-R, right-S bimodule that is flat as a left-R module. For any injective right S-module M, the set of module homomorphisms $\mathrm{Hom}_S(P, M)$ is an injective right R-module. For instance, if R is a subring of S such that S is a flat R-module, then every injective S-module is an injective R-module. In particular, if R is an integral domain and S its field of fractions, then every vector space over S is an injective R-module. Similarly, every injective $R[x]$-module is an injective R-module.

For quotient rings R/I, the change of rings is also very clear. An R-module is an R/I-module precisely when it is annihilated by I. The submodule $\mathrm{ann}_I(M) = \{ m \text{ in } M : im = 0 \text{ for all } i \text{ in } I \}$ is a left submodule of the left R-module M, and is the largest submodule of M that is an R/I-module. If M is an injective left R-module, then $\mathrm{ann}_I(M)$ is an injective left R/I-module. Applying this to $R=\mathbf{Z}$, $I=n\mathbf{Z}$ and $M=\mathbf{Q}/\mathbf{Z}$, one gets the familiar fact that $\mathbf{Z}/n\mathbf{Z}$ is injective as a module over itself. While it is easy to convert injective R-modules into injective R/I-modules, this process does not convert injective R-resolutions into injective R/I-resolutions, and the homology of the resulting complex is one of the early and fundamental areas of study of relative homological algebra.

9.2.9 Self-Injective Rings

Every ring with unity is a free module and hence is a projective as a module over itself, but it is rarer for a ring to be injective as a module over itself, (Lam 1999, §3B). If a ring is injective over itself as a right module, then it is called a **right self-injective ring**. Every Frobenius algebra is self-injective, but no integral domain that is not a field is self-injective. Every proper quotient of a Dedekind domain is self-injective.

A right Noetherian, right self-injective ring is called a quasi-Frobenius ring, and is two-sided Artinian and two-sided injective, (Lam 1999, Th. 15.1). An important module theoretic property of quasi-Frobenius rings is that the projective modules are exactly the injective modules.

Lemma . Baer's Criterion: Let R be a ring with identity. A unitary Rmodule J is injective if and only if for every left ideal L of R, any R-module homomorphism $L \longrightarrow J$ may be extended to an R-module homomorphism $R \longrightarrow J$.

Proof. To say that $f : L \longrightarrow J$ may be extended to R means there is a homomorphism $h : R \longrightarrow J$ such that the diagram is commutative. Clearly, such an h always exists if J is injective. Conversely, suppose J has the stated extension property and suppose we are given a diagram of module homomorphisms

with top row exact. To show that J is injective we must find a homomorphism $h : B \longrightarrow J$ with $hg = f$. Let S be the set of all R-module homomorphismsh : $C \longrightarrow J$, where $\text{Im } g \subset C \subset B$. S is non empty since $fg{-}1 : \text{Im } g \longrightarrow J$ is an element of S (g is a monomorphism). Partially order S by extension : $h1 \leq h2$ iff Dom h1 $\subset$ Dom h2 and h2 | Dom h1 = h1. We can verify that the hypotheses of Zorn's Lemma are satisfied and conclude that S contains a maximal element $h : H \longrightarrow J$ with $hg = f$. We shall complete the proof by showing H = B.

If H 6= B and $b \in B - H$, then $L = \{r \in R \mid rb \in H\}$ is left ideal of R. The map $L \longrightarrow J$ given by r 7→ h(rb) is a well- defined R-module homomorphism. By the hypothesis there is a R-module homomorphism k : $R \longrightarrow J$ such that $k(r) = h(rb)$ for all $r \in L$. Let $c \in k(1R)$ and define a map h¯ : $H + Rb \longrightarrow J$ by a + rb 7→ h(a) + rc. We claim that h¯ is well-defined. For if $a1 + r1b = a2 + r2b \in H + Rb$, then $a1 - a2 = (r2 - r1)b \in$

H T Rb. Hence r2 − r1 ∈ L and h(a1) − h(a2) = h(a1 − a2) = h((r2 − r1)b) = k(r2 − r1) = (r2 − r1)k(1R) = (r2 − r1)c. Therefore, h¯ : R + Rb −→ J is an R-module homomorphism that is an element of the set S. This contradicts.

themaximality of h since b /∈ H and hence H $ H + Rb. Therefore, H = B and J is injective.

Example: If R is a ring with identity, P is a projective R-module and f : M → P is an epimorphism of R-modules then M ∼= P ⊕ Ker(f).

Proof. We have a short exact sequence 0 −→ Ker(f)−→M f −→ P −→ 0

Theorem. If R is a PID, F is a free R-module of a finite rank, and M ⊆ F is a submodule then M is a free module and rank M ≤ rank F.

Definition. An R-module P is a projective module if there exists an Rmodule Q such that P ⊕ Q is a free R-module.

Proposition 1.4: For an A-module P, the following are equivalent:

(a) P is projective.

(b) The functorHomA(P, •) : A-Mod → Ab is exact.

(c) Every A-linear map onto P has a section.

(d) Every exact sequence 0 → M → N → P → 0 in A-Mod splits.

(e) P is a direct summand of a free A-module.

Proof. (a) ⇒ (b). The functorHomA(P, •) is already left exact, so the only thing to verify is that for every surjective A-linear map M → N, the induced map HomA(P, M) → HomA(P, N) is surjective. But this is just a rewording..

(b) ⇒ (c). Let M P be an A-linear map. Then by (b) there exists a map s : P → M such that f s = idP, which is precisely what we want.

(c) ⇒ (d). This is one of the avatars of the well-known splitting lemma for exact sequences.1

(d) ⇒ (e). For every A-module P we can always find a surjective A-linear map φ : N → P with N free.2 By (d), the exact sequence 0 → Ker φ → N f → 2 For example, we can take N to be the free A-module generated by the elements of P. P → 0 splits, so that P is a direct factor of the free module N.

(e) ⇒ (a). First assume that P = L λ∈ΛAλ is free. Let f : Q R and g : P → R be A-linear maps and take an A-basis {aλ}λ∈Λ for P. Since f is surjective, we can lift each aλ to some element bλ∈ Q. Then we can define an A-linear map h : P → Q by sending each aλ to bλ and extending by A-linearity; clearly f h = g, as desired. In the general case, Let P ∼= M ⊕ N with M free and let f and g be as before. The map g can be extended to g˜ : M → R, (p, n) 7→ g(p). As M is free, g˜ can be lifted to ˜h : M → Q. Then h = ˜h|P : P → Q is an A-linear map satisfying f h = g, whence P is projective.

Note. For a ring R and R-modules L, M let HomR(L, M) be the set of all R-module homomorphisms ϕ: L → M. Notice that HomR(L, M) is an abelian group (with respect to the pointwise addition of homomorphisms). Moreover, for any homomorphism of R-modules f : M → N the map

f∗ :HomR(L, M) → HomR(L, N), f∗(ϕ) = f ◦ ϕ is a homomorphism of abelian groups.

This defines a functor

HomR(L, −): R-Mod −→ Ab

This functor is in general not exact. Take e.g. R = Z, L = Z/2Z. We have a short exact sequence of abelian groups:

0 → Z ·2 −→ Z −→ Z/2Z → 0

On the other hand the sequence

0 → HomZ(Z/2Z, Z) −→ HomZ(Z/2Z, Z) −→ HomZ(Z/2Z, Z/2Z) → 0

is not exact since HomZ(Z/2Z, Z) ∼= 0 and HomZ(Z/2Z, Z/2Z) ∼= Z/2Z.

Theorem (Baer's Criterion). Let R be a ring with identity and let J be an R-module. The following conditions are equivalent.

1) J is an injective module.

2) For every left ideal I C R and for every homomorphisms of R-modules f : I → J there is a homomorphism ¯f : R → J such ¯f|I = f.

Proof. 1) ⇒ 2) Given a homomorphism f : I → J we have a diagram where i: I ,→ R is the inclusion homomorphism. By the definition of an injective module there is a homomorphism ¯f : R → J such that f = ¯f i = ¯f|I

2) ⇐ 1) Assume that J is an R-module satisfying 2). It is enough to show that if M is an R-module, N is a submodule of M, and f : N → J is an Rmodule homomorphism then there exists a homomorphism ¯f : M → J such that ¯f|N = f

Let S be a set of all pairs (K, fK) such that

(i) K is a submodule of M such that N ⊆ K ⊆ M

(ii) fK : K → J is a homomorphism such that fK|N = f

Define partial ordering on S as follows:

(K, fK) ≤ (K0 , fK0) if K ⊆ K0

and fK0|K = fK Check: assumptions of Zorn's Lemma are satisfied in S, and so S contains a maximal element (K0, fK0).

It will suffice to show that K0 = M. Assume, by contradiction, that K0 6= M, and let m0 ∈ M − K0. Define

I := {r ∈ R | rm0 ∈ K0}

Check: I is an ideal of R and the

map g : I → J, g(r) = fK0 (rm0)

is a homomorphism of R-modules. By the assumptions on J we have a homomorphism g¯: R → J such that g¯|I = g. Define

K0 + Rm0 := {k + rm0 | k ∈ K, r ∈ R}

Check: K0 + Rm0 is a submodule of M and the

map f 0 : K0 + Rm0 → J, f0 (k + rm0) = fK0 (k) + ¯g(r)

is a well defined homomorphism of R-modules such that f 0 |N = f. This shows that (K0 + Rm0, f0)∈ S. We also have

(K0, fK0)< (K0 + Rm0, f0)

This is impossible since by assumption (K0, fK0) is a maximal element in S.

Corollary. Let R be an integral domain and let K the field of fractions of R. Then K is an injective R-module.

Proof. Let I be an ideal of R and let f : I → K be a homomorphism of Rmodules. For 0 6= r, s ∈ I we have

rf(s) = f(rs) = sf(r)

As consequence in K we have f(r)/r = f(s)/s for any 0 6= r, s ∈ I. Denote this element by a. Define

¯f : R → K, ¯f(r) := ra

Check: ¯f is a homomorphism of R-modules and ¯f|I = f.

9.3 SUMMARY

We study in this section free module and its examples. We study injective module and projective module. We study self injective ring. We study change of ring and self injective module over ring. We study commutative example and artinian examples. We study split exact sequence. We study the category of projective module. We study projective module over polynomial module.

1. A module *P* is projective if and only if for every surjective module homomorphism $f : N \twoheadrightarrow M$ and every module homomorphism $g : P \to M$, there exists a homomorphism $h : P \to N$ such that $fh = g$.
2. Let *P* be a finitely generated projective module over a commutative ring *R* and *X* be the spectrum of *R*. The *rank* of *P* at a prime ideal in X is the rank of the free R-module M.
3. Every free module F over a ring R with identity is projective.
4. Let R be a ring. The following conditions on an R-module P are equivalent.

   (a) P is projective;

   (b) every short exact sequence 0 −→ A f −→ B g −→ P −→ 0 is split exact (hence B ∼= A ⊕ P);

   (c) there is a free module F and an R-module K such that F ∼= K ⊕ P.

5. If R is a PID, F is a free R-module of a finite rank, and M ⊆ F is a submodule then M is a free module and rank M ≤ rank F.

6. Baer's Criterion. Let R be a ring with identity and let J be an R-module. The following conditions are equivalent.

a) J is an injective module.

b) For every left ideal I C R and for every homomorphisms of R-modules f : I → J there is a homomorphism ¯f : R → J such ¯f|I = f.

9.4 KEYWORD

Injective :An *injective* function or injection or one-to-one function is a function that preserves distinctness

Projective :Relating to the unconscious transfer of one's desires or emotions to another person

Integral Domain :An *integral domain* is basically *defined* as a nonzero commutative ring in which the product of any two nonzero elements is nonzero

9.5 QUESTIONS FOR REVIEW

Q. 1. Projective but not free: If R = Z6, then Z3 and Z2 are Z6-modules and there is Z6-module isomorphism Z6 ∼= Z2 ⊕ Z3. Hence both Z2 and Z3 are projective Z6-modules that are not free Z6-modules.

Q. 2 If R is a ring with identity then every free R-module is projective.

Q. 3 Z/2Z and Z/3Z are non-free projective Z/6Z-modules.

Q. 4 Let R be a ring with identity and let P be an R-module. The following conditions are equivalent.

1) P is a projective module.

2) For any homomorphism f : P → N and an epimorphism g : M → N there is a homomorphism h: P → M such that the following diagram commutes:

3) Every short exact sequence 0 → N f −→ M g −→ P → 0 splits.

Q. 5 If R is a ring with identity, P is a projective R-module and $f : M \to P$ is an epimorphism of R-modules then $M \cong P \oplus \text{Ker}(f)$.

9.6 SUGGESTION READING AND REFERENCES

1. William A. Adkins; Steven H. Weintraub (1992). Algebra: An Approach via Module Theory. Springer. Sec 3.5.
2. Iain T. Adamson (1972). Elementary rings and modules. University Mathematical Texts. Oliver and Boyd. ISBN 0-05-002192-3.
3. Nicolas Bourbaki, Commutative algebra, Ch. II, §5
4. Braunling, Oliver; Groechenig, Michael; Wolfson, Jesse (2016), "Tate objects in exact categories", Mosc. Math. J., **16** (3), arXiv:1402.4969v4, MR 3510209
5. Paul M. Cohn (2003). Further algebra and applications. Springer. ISBN 1-85233-667-6.
6. Drinfeld, Vladimir (2006), "Infinite-dimensional vector bundles in algebraic geometry: an introduction", in Pavel Etingof; Vladimir Retakh; I. M. Singer (eds.), The Unity of Mathematics, Birkhäuser Boston, pp. 263–304, arXiv:math/0309155v4, doi:10.1007/0-8176-4467-9_7, ISBN 978-0-8176-4076-7, MR 2181808
7. Govorov, V. E. (1965), "On flat modules (Russian)", Siberian Math. J., **6**: 300–304
8. Hazewinkel, Michiel; Gubareni, Nadiya; Kirichenko, Vladimir V. (2004). Algebras, rings and modules. Springer Science. ISBN 978-1-4020-2690-4.
9. Kaplansky, Irving (1958), "Projective modules", Ann. of Math., 2, **68**: 372–377, doi:10.2307/1970252, MR 0100017
10. Lang, Serge (1993). Algebra (3rd ed.). Addison–Wesley. ISBN 0-201-55540-9.
11. Lazard, D. (1969), "Autour de la platitude", Bulletin de la SociétéMathématique de France, **97**: 81–128
12. Milne, James (1980). Étalecohomology. Princeton Univ. Press. ISBN 0-691-08238-3.

13. Donald S. Passman (2004) A Course in Ring Theory, especially chapter 2 Projective modules, pp 13–22, AMS Chelsea, ISBN 0-8218-3680-3 .
14. Raynaud, Michel; Gruson, Laurent (1971), "Critères de platitude et de projectivité. Techniques de "platification" d'un module", Invent. Math., **13**: 1–89, Bibcode:1971InMat..13....1R, doi:10.1007/BF01390094, MR 0308104
15. Paulo Ribenboim (1969) Rings and Modules, §1.6 Projective modules, pp 19–24, Interscience Publishers.
16. Charles Weibel, The K-book: An introduction to algebraic K-theory
17. Baer, Reinhold (1940), "Abelian groups that are direct summands of every containing abelian group", Bulletin of the American Mathematical Society, **46** (10): 800–807, doi:10.1090/S0002-9904-1940-07306-9, MR 0002886, Zbl 0024.14902
18. Chase, Stephen U. (1960), "Direct products of modules", Transactions of the American Mathematical Society, Transactions of the American Mathematical Society, Vol. 97, No. 3, **97** (3): 457–473, doi:10.2307/1993382, JSTOR 1993382, MR 0120260

9.7 ANSWER TO CHECK YOUR PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 1.10

Q 2 Check in Section 1.5

Check in Progress-II

Answer Q. 1 Check in Section 3

Q 2 Check in Section 4

UNIT 10 - FLAT MODULE, GENERATED MODULE OVER PID

STRUCTURE

10.0 OBJECTIVE

- We learn in this unit Flat module , Flat Cove

Notes

- Learn Finitely Generated Module Over PID
- Learn Non-Finitely Generated Module
- Learn Chinese Remainder Theorem For PID
- Learn Finitely Generated Abelian Group

10.1 INTRODUCTION : FLAT MODULE

In homological algebra and algebraic geometry, a **flat module** over a ring *R* is an *R*-module *M* such that taking the tensor product over *R* with *M* preserves exact sequences. A module is **faithfully flat** if taking the tensor product with a sequence produces an exact sequence if and only if the original sequence is exact.

A module M over a unit ring R is called flat iff the tensor product functor $-\otimes_R M$ (or, equivalently, the tensor product functor $M\otimes_R -$) is an exact functor.

For every R-module, M obeys the implication

$$M \text{ free} \Longrightarrow M \text{ projective} \Longrightarrow M \text{ flat},$$

which, in general, cannot be reversed.

A $\mathbb{Z}$-module is flat iff it is torsion-free: hence $\mathbb{Q}$ and the infinite direct product $\mathbb{Z}\times\mathbb{Z}\times\cdots$ are flat $\mathbb{Z}$-modules, but they are not projective. In fact, over a Noetherian ring or a local ring, flatness implies projectivity only for finitely generated modules. This property, together with Serre's problem, allows it to be concluded that the three above implications are equivalences if M is a finitely generated module over a polynomial ring $k[X_1, \ldots, X_n]$, where k is a field.

Flatness was introduced by Serre (1956) in his paper *GéometrieAlgébriqueetGéométrieAnalytique*. See also flat morphism.

10.1.1 Characterizations Of Flatness

Since tensoring with *M* is, for any module *M*, a right exact functor

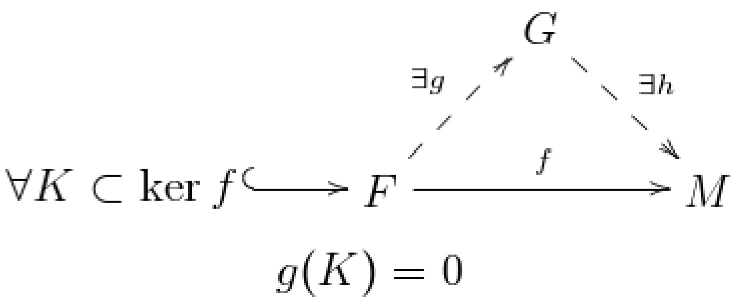
between the category of *R*-modules and abelian groups), *M* is flat if and only if the preceding functor is exact.

It can also be shown in the condition defining flatness as above, it is enough to take M, the ring itself, and R a finitely generated ideal of *R*.

Flatness is also equivalent to the following equational condition, which may be paraphrased by saying that *R*-linear relations that hold in *M* stem from linear relations which hold in *R*: for every linear dependency, K with M and R, there exist a matrix M and an element R such that M and R Furthermore, *M* is flat if and only if the following condition holds: for every map F : F→M where F is a finitely generated free R-module, and for every finitely

generated -submodule K of ker F the map F factors through a

map *g* to a free -module g(K)=0 such that



Examples and relations to other notions

Flatness is related to various other conditions on a module, such as being free, projective, or torsion-free. This is partly summarized in the following graphic:

Free or projective modules vs. flat modules

Free modules are flat over any ring *R*. This holds since the functor is exact. For example, vector spaces over a field are flat modules. Direct summands of flat modules are again flat. In particular, projective modules (direct summands of free modules) are flat. Conversely, for a commutative Noetherian ring *R*, finitely generated flat modules are projective.

Further Permanence Properties

In general, arbitrary direct sums and filtered colimits (also known as direct limits) of flat modules are flat, a consequence of the fact that the tensor product commutes with direct sums and filtered colimits (in fact with all colimits), and that both direct sums and filtered colimits are exact functors. In particular, this shows that all filtered colimits of free modules are flat.

Lazard (1969) proved that the converse holds as well: *M* is flat if and only if it is a direct limit of finitely-generated free modules. As a consequence, one can deduce that every finitely-presented flat module is projective. The direct sum Mi is flat if and only if each Mi is flat.

Products of flat *R*-modules need not in general be flat. In fact, Chase (1960) showed a ring *R* is coherent (i.e., any finitely generated ideal is finitely presented) if and only if arbitrary products of flat *R*-modules are again flat.

10.1.2 Flat Ring Extensions

If $\phi : R \rightarrow S$ is a ring homomorphism, *S* is called flat over *R* (or a flat *R*-algebra) if it is flat as an *R*-module. For example, the polynomial ring *R*[*t*] is flat over *R*, for any ring *R*. Moreover, for any multiplicatively closed subset S of a commutative ring R, the localization ring R is flat over *R*. For example, Q is flat over Z (though not projective).

Let S be a polynomial ring over a noetherian ring R and f € S a nonzerodivisor. Then S/fS is flat over R if and only if f is primitive (the coefficients generate the unit ideal).[5] This yields an example of a flat module that is not free.

Kunz (1969) showed that a noetherian local ring R of positive characteristic *p* is regular if and only if the Frobenius morphism f : X→ Y is flat and R is reduced.

Flat ring extensions are important in algebra, algebraic geometry and related areas. A morphism F : X→ Y of schemes is a flat morphism if, by one of several equivalent definitions, the induced map on local rings

is a flat ring homomorphism for any point *x* in *X*. Thus, the above-mentioned properties of flat (or faithfully flat) morphisms established by methods of commutative algebra translate into geometric properties of flat morphisms in algebraic geometry.

10.1.3 Local Aspects Of Flatness Over Commutative Rings

In this section, the ring *R* is supposed to be commutative. In this situation, flatness of *R*-modules is related in several ways to the notion of localization: *M* is flat if and only if the module Mp is a flat Rp-module for all prime ideals p of *R*. In fact, it is enough to check the latter condition only for the maximal ideals, as opposed to all prime ideals. This statement reduces the question of flatness to the case of (commutative) local rings.

If *R* is a local (commutative) ring and either *M* is finitely generated or the maximal ideal of *R* is nilpotent (e.g., an artinian local ring) then the standard implication "free implies flat" can be reversed: in this case *M* is flat if and if only if its free.

The **local criterion for flatness** states:

Let *R* be a local noetherian ring, *S* a local noetherian *R*-algebra with S⊂ Ms, and *M* a finitely generated *S*-module. Then *M* is flat

over *R* if and only if

The significance of this is that *S* need not be finite over *R* and we only need to consider the maximal ideal of *R* instead of an arbitrary ideal of *R*.

The next criterion is also useful for testing flatness:

Let *R*, *S* be as in the local criterion for flatness.
Assume *S* is Cohen–Macaulay and *R* is regular. Then *S* is flat

over *R* if and only if

10.1.4 Flat Resolutions

A **flat resolution** of a module M is a resolution of the form

where the F_i are all flat modules. Any free or projective resolution is necessarily a flat resolution. Flat resolutions can be used to compute the Tor functor.

The *length* of a finite flat resolution is the first subscript n such that F_n is nonzero and $F_i = 0$ for $i > n$. If a module M admits a finite flat resolution, the minimal length among all finite flat resolutions of M is called its flat dimension and denoted fd(M). If M does not admit a finite flat resolution, then by convention the flat dimension is said to be infinite. As an example, consider a module M such that fd(M) = 0. In this situation, the exactness of the sequence $0 \to F_0 \to M \to 0$ indicates that the arrow in the center is an isomorphism, and hence M itself is flat.

In some areas of module theory, a flat resolution must satisfy the additional requirement that each map is a flat pre-cover of the kernel of the map to the right. For projective resolutions, this condition is almost invisible: a projective pre-cover is simply an epimorphism from a projective module. These ideas are inspired from Auslander's work in approximations. These ideas are also familiar from the more common notion of minimal projective resolutions, where each map is required to be a projective cover of the kernel of the map to the right. However, projective covers need not exist in general, so minimal projective resolutions are only of limited use over rings like the integers.

10.1.5 Flat Covers

While projective covers for modules do not always exist, it was speculated that for general rings, every module would have a flat cover, that is, every module M would be the epimorphic image of a flat module F such that every map from a flat module onto M factors through F, and any endomorphism of F over M is an automoprhism. This **flat cover conjecture** was explicitly first stated in (Enochs 1981, p 196). The conjecture turned out to be true, resolved positively and proved simultaneously by L. Bican, R. El Bashir and E. Enochs.[15] This was preceded by important contributions by P. Eklof, J. Trlifaj and J. Xu.

Since flat covers exist for all modules over all rings, minimal flat resolutions can take the place of minimal projective resolutions in many circumstances. The measurement of the departure of flat resolutions from projective resolutions is called *relative homological algebra*, and is covered in classics such as (MacLane 1963) and in more recent works focussing on flat resolutions such as (Enochs&Jenda 2000).

10.2 STRUCTURE THEOREM FOR FINITELY GENERATED MODULES OVER A PRINCIPAL IDEAL DOMAIN

In mathematics, in the field of abstract algebra, the **structure theorem for finitely generated modules over a principal ideal domain** is a generalization of the fundamental theorem of finitely generated abelian groups and roughly states that finitely generated modules over a principal ideal domain can be uniquely decomposed in much the same way that integers have a prime factorization. The result provides a simple framework to understand various canonical form results for square matrices over fields.

10.2.1 Statement

When a vector space over a field F has a finite generating set, then one may extract from it a basis consisting of a finite number n of vectors, and the space is therefore isomorphic to F^n. The corresponding statement with the F generalized to a principal ideal domain R is no longer true, since a basis for a finitely generated module over R might not exist. However such a module is still isomorphic to a quotient of some module R^n with n finite (to see this it suffices to construct the morphism that sends the elements of the canonical basis of R^n to the generators of the module, and take the quotient by its kernel.) By changing the choice of generating set, one can in fact describe the module as the quotient of some R^n by a particularly simple submodule, and this is the structure theorem.

The structure theorem for finitely generated modules over a principal ideal domain usually appears in the following two forms.

10.2.2 Fundamental Theorem of Arithmetic

This theorem says that any integer is uniquely expressible as a product of prime numbers. In terms of abstract algebra, it says that the ring of integers Z is a Unique Factorization Domain. (Of course we already know this, since Z is a Euclidean Domain, and Euclidean Domain =⇒ Principal Ideal Domain =⇒ Unique Factorization Domain.)

Fundamental theorem of algebra This says that any polynomial with coefficients from C factors into a product of linear factors. In terms of abstract algebra, it says that the primes in the Euclidean Domain C[x] are all linear polynomials of the form ax + b where a 6= 0.

Fundamental theorem of finite abelian groups This says that every finite abelian group can be expressed uniquely as a product of p-groups.

In this handout, the main goal is to understand and apply a new "fundamental theorem." This theorem describes in precise detail the structure of a finitely-generated module over a P.I.D. Recall that if R is any ring, then an R-module M is an abelian group (we'll use + as the operation) such that we can multiply group elements from M by scalars from R. This multiplication by scalars is compatible with the group operation in all the usual ways: multiplication by scalars distributes over addition, etc. If N is any other R-module, then a map $\varphi : M \longrightarrow N$ is an R-module homomorphism if it is a group homomorphism that is also R-linear, i.e. $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(rx) = r\varphi(x)$. In other words, φ preserves addition and multiplication by scalars. The canonical example of a ring module that you should keep in mind is a vector space, where the scalars come from a field F. In this case, an F-module homomorphism is just a linear transformation. We will explore other very natural examples of ring modules in this handout.

An R-module M is finitely-generated if there is a finite subset {x1, . . . , xn} in M such that if x is any element in M, there exist scalars {r1, . . . , rn} in R such that

$$x = r1x1 + r2x2 + \cdots + rnxn.$$

In other words, the set {x1, . . . ,xn} is a spanning set. If for every group element x the scalars ri are unique, then we call the set {x1, . . . ,xn} a basis for M.

I'll be assuming throughout that you are conversant with the following terms: ring, unit, ideal, factor ring or quotient ring, field, Euclidean Domain, Principal Ideal Domain, Integral Domain, prime element in a P.I.D., R-module, R-module homomorphism, etc. You should also be comfortable with basic linear algebra ideas, e.g. the correspondence between linear transformations and matrices, how a change of basis affects a matrix for a linear transformation, the notion of similar matrices, etc.

Here is the theorem that is the showpiece of this handout (we will also refer to it as the Structure Theorem):

10.2.3 Fundamental Theorem Of Finitely-Generated Modules Over P.I.D.

Let M be a (non-zero) finitely-generated R-module, where R is a P.I.D. Then there exist non-negative integers s and t and non-zero ring elements a1, a2, . . . , as for which

$$M \sim= R/ha1i \times R/ha2i \times \cdots \times R/hasi \times R\ t\ ,$$

where a1|a2| · · · |as. Moreover, this decomposition of M is unique in the following sense: if k and l are non-negative integers and b1, b2, . . . ,bk are ring elements satisfying b1|b2| · · · |bk for which

$$M \sim= R/hb1i \times R/hb2i \times \cdots \times R/hbki \times R\ l\ ,$$

then k = s, l = t, and hbii = haii for all $1 \leq i \leq s$.

The ai 's are called the invariant factors for the module M. The theorem says that the invariant factors for M are unique up to units.

Application 1: The Structure Theorem and finite-dimensional vector spaces.

Before proving the Structure Theorem, it might be profitable first to look at some applications. Intuitively, one should think of an R-module as an additive group M whose elements can be multiplied by scalars from the ring R. So, when R = F is a field, any F-module is just a vector space. We would like to apply the Structure Theorem to finitely-generated vector spaces. An F-vector space V is finitely-generated as an F-module if there is a finite set of elements $\{v_1, \ldots, v_n\}$ in V such that if v is any element in V , then there exist scalars $c_1, \ldots, c_n$ for which,

$$v = c_1v_1 + c_2v_2 + \cdots c_nv_n.$$

In other words, $\{v_1, \ldots, v_n\}$ is a finite spanning set. We obtain our first corollary of the Structure Theorem:

Corollary (Classification of Finitely-generated Vector Spaces) Let V be a finitely-generated vector space over a field F. Then as an F-module,

$$V \cong F^t$$

for some non-negative integer t.

Proof. By the Structure Theorem, we may write

$$V \cong F/\langle a_1\rangle \times F/\langle a_2\rangle \times \cdots \times F/\langle a_s\rangle \times F^t$$

for non-zero field elements a_i . Since each a_i is non-zero, then each a_i is invertible in F, and hence the ideal $\langle a_i\rangle$ generated by a_i is all of F. That is, $F/\langle a_i\rangle = 0$ for each i. So $V \cong F^t$.

Of course, we call t the dimension of the vector space V . Is there ever a situation in which you would know that a vector space is finitely-generated without already knowing its dimension? Yes, and here is an example: suppose V is finite-dimensional over F, and suppose W is any F-module. Let $T : V \longrightarrow W$ be any linear transformation. We claim that T(V) is finitely-generated as a submodule of W, and hence is finite-dimensional. To see this, notice that T(V) is a submodule, i.e. subspace, of W. (First, note that T(V) is closed under subtraction: $T(x) - T(y) = T(x - y)$. Second, T(V) is closed under multiplication by scalars: $\lambda T(x) = T(\lambda x)$.) Next, let $\{v_1, \ldots, v_t\}$ be a generating set for V . It is easy to see that $\{T(v_1), \ldots, T(v_t)\}$ is a generating set for T(V).

Corollary A vector space V of dimension t has a basis of t elements. Moreover, if $\{v_1, \ldots, v_n\}$ is a basis for V , then n = t.

Exercise Prove the previous corollary.

Check in Progress-I

Note: i) Write your answers in the space given below.

Q. 1 Define Flat Module.

Solution.

…………………………………………………………………….

……………………………………………………………………..

……………………………………………………………………..

Q. 2 Define PID.

Solution.

…………………………………………………………………….

……………………………………………………………………..

……………………………………………………………………

10.2.4 Indecomposable Modules

By contrast, unique decomposition into *indecomposable* submodules does not generalize as far, and the failure is measured by the ideal class group, which vanishes for PIDs.

For rings that are not principal ideal domains, unique decomposition need not even hold for modules over a ring generated by two elements. For the ring $R = Z[\sqrt{-5}]$, both the module R and its submodule M generated by 2 and $1 + \sqrt{-5}$ are indecomposable. While R is not isomorphic to M, $R \oplus R$ is isomorphic to $M \oplus M$; thus the images of the M summands give indecomposable submodules $L_1, L_2 < R \oplus R$ which give a different decomposition of $R \oplus R$. The failure of uniquely factorizing $R \oplus R$ into a direct sum of indecomposable modules is directly related (via the ideal class group) to the failure of the unique factorization of elements of R into irreducible elements of R.

However, over a Dedekind domain the ideal class group is the only obstruction, and the structure theorem generalizes to finitely generated modules over a Dedekind domain with minor modifications. There is still a unique torsion part, with a torsionfree complement (unique up to isomorphism), but a torsionfree module over a Dedekind domain is no longer necessarily free. Torsionfree modules over a Dedekind domain are determined (up to isomorphism) by rank and Steinitz class (which takes value in the ideal class group), and the decomposition into a direct sum of copies of R (rank one free modules) is replaced by a direct sum into rank one projective modules: the individual summands are not uniquely determined, but the Steinitz class (of the sum) is.

10.2.5 Non-Finitely Generated Modules

Similarly for modules that are not finitely generated, one cannot expect such a nice decomposition: even the number of factors may vary. There are **Z**-submodules of $\mathbf{Q}^4$ which are simultaneously direct sums of two indecomposable modules and direct sums of three indecomposable modules, showing the analogue of the primary decomposition cannot hold for infinitely generated modules, even over the integers, **Z**.

Another issue that arises with non-finitely generated modules is that there are torsion-free modules which are not free. For instance, consider the ring **Z** of integers. Then **Q** is a torsion-free **Z**-module which is not free. Another classical example of such a module is the Baer–Specker group, the group of all sequences of integers under termwise addition. In general, the question of which infinitely generated torsion-free abelian groups are free depends on which large cardinals exist. A consequence is that any structure theorem for infinitely generated modules depends on a choice of set theory axioms and may be invalid under a different choice.

10.2.6 Fundamental Theorem Of Finite Abelian Groups

Any finite abelian group is expressible uniquely as a product of p-groups. That is, if G is a finite abelian group, then there exist primes p_i ($1 \le i \le k$) and positive integers α_i for which

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}.$$

Moreover, if there are primes q_j ($1 \le j \le l$) and positive integers β_j for which

$$G \cong Z q \beta1\ 1 \times \cdots \times Z q \beta l\ l,$$

then l = k, and after appropriately permuting the list of qj 's we have

$$pi = qi \text{ and } \alpha i = \beta i \text{ for } 1 \le i \le k.$$

Guided Discovery Proof. We proceed in steps.

1 Use the Structure Theorem to write

$$G \cong Za1 \times \cdots \times Zas \times Z\ t$$

for non-negative integers s and t and for positive integers ai for which a1| · · · |as. Say why we must have t = 0.

2. If a is a positive integer, use the Fundamental Theorem of Arithmetic to express a as a product of powers of distinct primes, i.e.

$$a = p\ \alpha1\ 1\ p\ \alpha2\ 2 \cdots p$$

αnn for distinct primes p1, . . . , pn. What theorem allows us to conclude that

$$Za \cong Zp\ \alpha1\ 1 \times \cdots \times Zp$$

αnn ? Hint: This theorem is prominently featured in one of the appendices.

3. Now put these two items together to complete the proof of the existence of a decomposition for G as claimed in the Corollary statement.

4. The uniqueness of this decomposition of G into p-groups follows from the uniqueness of the invariant factors. . . how?

10.2.7 Chinese Remainder Theorem For P.I.D.'

Let R be a P.I.D., and let q1, q2, . . . ,qk be relatively prime, i.e. for all i 6= j, hqii + hqji = R. (In other words, some linear combination of qi and qj is equal to 1.) Then

$$R/hq1q2 \cdots qki = R/hq1i \cap \cdots \cap hqki \cong R/hq1i \times \cdots \times R/hqki$$

You are asked to prove this in Exercise #6 in the problem set (the proof should not be too different from the proof of the Chinese Remainder Theorem for Z sketched in an earlier handout). So now suppose that we have a finitely-generated R-module M (where R is a P.I.D.) and that a ∈

R is one of the invariant factors for M. As above, we can write a = p α1 1 p α2 2 · · · p αk k . Apply the Chinese Remainder Theorem to R/hai by setting qi := p αii for each i. Each qi is an elementary divisor for M. (This observation basically coincides with Exercise #7, where you are then asked to apply the result to find the elementary divisors for R[x]/hx 4 − 1i.) We now have this principle:

To obtain the elementary divisors for a finitely-generated R-module M, apply the Chinese Remainder Theorem for P.I.D.'s to R/hai for each invariant factor a.

Exercise Find the elementary divisors for the R[x]-module

R[x]/hx − 2i × R[x]/hx 2 + x − 6i × R[x]/hx 3 − x 2 − 8x + 12i.

The next question is: If we have a list of the elementary divisors of M, can we recover the invariant factors? The answer is "Yes," and to do so we can use a simple algorithm. This procedure says first to find the highest power of each distinct prime appearing in the list of elementary divisors and multiply these together. This will be the largest invariant factor. Next, go through the list of remaining elementary divisors and pick out the highest power of each distinct prime in the remaining list. Multiply these together to get the second largest invariant factor. Continue this procedure until the elementary divisors are all used up., you are asked to carry this out for a specific abelian group with a given list of elementary divisors.

ExampleLet R be a PID. Then, every nonempty set of ideals of R has a maximal element.

Proof. Let S be the set of all proper ideals of R. It follows that S is non-empty and it is partially ordered by inclusion. Let I1 ⊆ I2 ⊆ ... be an arbitrary increasing chain of ideals in S. Let I=S n In. Since the chain of In's are nonempty, it follows that I is nonempty. I is an ideal. Since R is a PID, I = (a). We find that a ∈ I = S n In so a ∈ In for some n. We get In = In+1 = ... Each chain of ideals has an upper bound. By Zorn's lemma, the nonempty set of I 0 n s of R has a maximal element, the maximal ideal containing I.

Definition . Let r be a nonzero element of R that is not a unit. The element r is called irreducible in R, if whenever r = ab with a, b ∈ R, at least one of a or b must be a unit in R. Otherwise, r is reducible.

Definition A nonzero element p ∈ R is called prime if the ideal (p) generated by p is a prime ideal.

Lemma . In an integral domain, a prime element is always irreducible.

Proof . If p is a prime element, then (p) is a prime ideal. Let (p) be some arbitrary nonzero ideal such that p = ab where a, b ∈ R. Clearly, ab = p ∈ (p). By the definition of a prime ideal, it follows that either p divides a or p divides b. Without loss of generality, suppose a ∈ (p). Then, a = pm where m ∈ R. We see that a = pm = abm so bm = 1. It follows that b is a unit. Therefore, we have shown that in a integral domain a prime element is always irreducible.

Definition. **A Unique Factorization Domain (UFD**) is an integral domain R in which every nonzero element r ∈ R that is not a unit has the following two properties:

(1) r can be written as a finite product of irreducibles pi of R (not necessarily distinct): r = p1p2...pn and

(2) this decomposition is unique up to associates: if r = r1r2...rm is another factorization of r into irreducibles, then m = n and there is some renumbering of the factors so that pi is associate to ri for i = 1, 2, ..., n.

Proposition . Every Principal Ideal Domain is a Unique Factorization Domain.

Proof . First we show that the decomposition exists. Let R be a arbitrary principal ideal domain. Suppose P is the set of all elements in R that do not admit a finite decomposition into a finite product of irreducibles. If P is empty, we are done (for the existence part)., there is a maximal element x in P (in the sense the ideal generated by x is maximal among all the ideals generated by a single element in P P). By the assumption on , x cannot be irreducible (otherwise it has a decomposition into a finite product of irreducibles, namely x = x). So x is reducible and we

Notes

may write x = yz with y, z both not units. So (x) $ (y) and (x) $ (z). By maximality of x in P, we have y 6∈ P and z 6∈ P. So y and z can be written as finite products of irreducibles; as a result, x can be written as a finite product of irreducibles, a contradiction. So P must be empty and thus every x ∈ R can be decomposed into a finite product of irreducible

Then, we show that the decomposition is unique up to associates in R by induction on m prime ideals. If r = p where p is a prime ideal, then it follows that another decomposition of r will be the same since there is only one factorization of r. Assume, by way of the inductive hypothesis, that uniqueness holds for m prime factors. Suppose r1...rmrm+1 = r = u1p1...pn. By the definition of a prime ideal, rm+1 must divide one of the p 0 i s on the right hand side so rm+1 = u1pi . After cancelling the term rm+1 on the left hand side, it follows from our inductive hypothesis that decomposition is unique up to associates for m prime ideals. Hence, induction holds.

We will now turn our attention toward the Chinese Remainder Theorem for Modules. This theorem will help us derive one form of the Structure Theorem for Finitely Generated Modules over a Principal Ideal Domain.

Check In Progress-II

Note: i) Write your answers in the space given below.

Q. 1State Chinese Remainder Theorem.

Solution :

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

Q.2State UFD.

Solution :

…………………………………………………………………………

…………………………………………………………………………

……………………………………………………………………………

10.3 FINITELY-GENERATED ABELIAN GROUPS

Structure Theorem for Finitely-Generated Abelian Groups. Let G be a finitely-generated abelian group. Then there exist

• a nonnegative integer t and (if t > 0) integers $1 < d1 \mid d2 \mid \cdots \mid dt$,

• a nonnegative integer r such that G takes the form

$G \approx Z/d1Z \oplus Z/d2Z \oplus \cdots \oplus Z/dtZ \oplus Z \oplus r$.

The integers d1, . . . ,dt are called the elementary divisors of G. The nonnegative integer r is called the rank of G. The elementary divisors and the rank of G are unique. The case t = r = 0 is understood to mean that G is trivial.

The argument to be given here is chosen for its resemblance to techniques that one sees in a linear algebra course and for its visual layout. However, the reader should be aware that the argument takes for granted at the outset that the finitelygenerated abelian group G has a presentation, meaning a description in terms of its generators and relations among them. We will return later in the semester to the fact that a presentation exists.

Proof. The group G is described by a set of r nontrivial integer-linear relations on a minimal set of g generatorsa11x1 + a12x2 + · · · + a1gxg = 0 a21x1 + a22x2 + · · · + a2gxg = 0 . . . . . . ar1x1 + ar2x2 + · · · + argxg = 0

Here we assume that g > 0, otherwise G is trivial and the result is clear. Also we assume that r > 0 since if there are no relations then $G \approx Z \oplus g$ and we are done. The circumstance that in practice one does not initially know whether a set of generators is minimal will be addressed later in the handout. The relations rewrite more concisely as

Xg j=1 aijxj = 0, i = 1, . . . , r.

Even more concisely, they encode as an r × g integer matrix,

Notes

A = [aij]r×g.

We will now prove the structure theorem for finitely generated abelian groups, since it will be crucial for much of what we will do later.

Let $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ denote the ring of integers, and for each positive integer n let $\mathbf{Z}/n\mathbf{Z}$ denote the ring of integers modulo n, which is a cyclic abelian group of order n under addition.

Definition 3.0.1 (Finitely Generated) A group G is if there exists $g_1, \ldots, g_n \in G$ such that every element of G can be obtained from the g_i.

Theorem 3.0.2 (Structure Theorem for Abelian Groups) *Let G be a finitely generated abelian group. Then there is an isomorphism*

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r,$$

where $n_1 > 1$ and $n_1 \mid n_2 \mid \cdots \mid n_s$. Furthermore, the n_i and r are uniquely determined by G.

We will prove the theorem as follows. We first remark that any subgroup of a finitely generated free abelian group is finitely generated. Then we see that finitely generated abelian groups can be presented as quotients of finite rank free abelian groups, and such a presentation can be reinterpreted in terms of matrices over the integers. Next we describe how to use row and column operations over the integers to show that every matrix over the integers is equivalent to one in a canonical diagonal form, called the Smith normal form. We obtain a proof of the theorem by reinterpreting in terms of groups.

Proposition 3.0.3 *Suppose G is a free abelian group of finite rank n, and H is a subgroup of G. Then H is a free abelian group generated by at most n elements.*

The key reason that this is true is that G is a finitely generated module over the principal ideal domain $\mathbf{Z}$. We will give a complete proof of a beautiful generalization of this result in the context of Noetherian rings next time, but will not prove this proposition here.

Corollary 3.0.4 *Suppose* G *is a finitely generated abelian group. Then there are finitely generated free abelian groups* F_1 *and* F_2 *such that* $G \cong F_1/F_2$.

Proof. Let $x_1, \ldots, x_m$ be generators for G. Let $F_1 = \mathbf{Z}^m$ and let $\varphi : F_1 \to G$ be the map that sends the ith generator $(0, 0, \ldots, 1, \ldots, 0)$ of $\mathbf{Z}^m$ to x_i. Then φ is a surjective homomorphism, the kernel F_2 of φ is a finitely generated free abelian group. This proves the corollary. □

Suppose G is a nonzero finitely generated abelian group. By the corollary, there are free abelian groups F_1 and F_2 such that $G \cong F_1/F_2$. Choosing a basis for F_1, we obtain an isomorphism $F_1 \cong \mathbf{Z}^n$, for some positive integer n. By Proposition 3.0.4, $F_2 \cong \mathbf{Z}^m$, for some integer m with $0 \leq m \leq n$, and the inclusion map $F_2 \hookrightarrow F_1$ induces a map $\mathbf{Z}^m \to \mathbf{Z}^n$. This homomorphism is left multiplication by the $n \times m$ matrix A whose columns are the images of the generators of F_2 in $\mathbf{Z}^n$. The of this homomorphism is the quotient of $\mathbf{Z}^n$ by the image of A, and the cokernel is isomorphic to G. By augmenting A with zero columns on the right we obtain a square $n \times n$ matrix A with the same cokernel. The following proposition implies that we may choose bases such that the matrix A is diagonal, and then the structure of the cokernel of A will be easy to understand.

Notes

Proposition 3.0.5 (Smith normal form) *Suppose* A *is an* $n \times n$ *integer matrix. Then there exist invertible integer matrices* P *and* Q *such that* $A' = PAQ$ *is a diagonal matrix with entries* $n_1, n_2, \ldots, n_s, 0, \ldots, 0$*, where* $n_1 > 1$ *and* $n_1 \mid n_2 \mid \ldots \mid n_s$*. This is called the Smith normal form of* A.

roof. The matrix P will be a product of matrices that define elementary row operations and Q will be a product corresponding to elementary column operations. The elementary operations are:

1. Add an integer multiple of one row to another (or a multiple of one column to another).
2. Interchange two rows or two columns.
3. Multiply a row by -1.

Each of these operations is given by left or right multiplying by an invertible matrix E with integer entries, where E is the result of applying the given operation to the identity matrix, and E is invertible because each operation can be reversed using another row or column operation over the integers.

To see that the proposition must be true, assume $A \neq 0$ and perform the following steps :

1. By permuting rows and columns, move a nonzero entry of A with smallest absolute value to the upper left corner of A. Now attempt to make all other entries in the first row and column 0 by adding multiples of row or column 1 to other rows (see step 2 below). If an operation produces a nonzero entry in the matrix with absolute value smaller than $|a_{11}|$, start the process

over by permuting rows and columns to move that entry to the upper left corner of A. Since the integers $|a_{11}|$ are a decreasing sequence of positive integers, we will not have to move an entry to the upper left corner infinitely often.

2. Suppose a_{i1} is a nonzero entry in the first column, with $i > 1$. Using the division algorithm, write $a_{i1} = a_{11}q + r$, with $0 \leq r < a_{11}$. Now add $-q$ times the first row to the ith row. If $r > 0$, then go to step 1 (so that an entry with absolute value at most r is the upper left corner). Since we will only perform step 1 finitely many times, we may assume $r = 0$. Repeating this procedure we set all entries in the first column (except a_{11}) to 0. A similar process using column operations sets each entry in the first row (except a_{11}) to 0.
3. We may now assume that a_{11} is the only nonzero entry in the first row and column. If some entry a_{ij} of A is not divisible by a_{11}, add the column of A containing a_{ij} to the first column, thus producing an entry in the first column that is nonzero. When we perform step 2, the remainder r will be greater than 0. Permuting rows and columns results in a smaller $|a_{11}|$. Since $|a_{11}|$ can only shrink finitely many times, eventually we will get to a point where every a_{ij} is divisible by a_{11}. If a_{11} is negative, multiple the first row by -1.

After performing the above operations, the first row and column of A are zero except for a_{11} which is positive and divides all other entries of A. We repeat the above steps for the matrix B obtained from A by deleting the first row and column. The upper left entry of the resulting matrix will be divisible by a_{11}, since every entry of B is. Repeating the argument inductively proves the proposition. □

Example 3.0.6 The matrix $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ and the matrix $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ is equivalent to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Note that the determinants match, up to sign.

Proof. [Theorem 3.0.3] Suppose G is a finitely generated abelian group, which we may assume is nonzero. As in the paragraph before Proposition 3.0.6, we use Corollary 3.0.5 to write G as a the cokernel of an $n \times n$ integer matrix A. By Proposition 3.0.6 there are isomorphisms $Q : \mathbf{Z}^n \to \mathbf{Z}^n$ and $P : \mathbf{Z}^n \to \mathbf{Z}^n$ such that $A' = PAQ$ is a diagonal matrix with entries $n_1, n_2, \ldots, n_s, 0, \ldots, 0$, where $n_1 > 1$ and $n_1 \mid n_2 \mid \ldots \mid n_s$. Then G is isomorphic to the cokernel of the diagonal matrix A', so

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r, \qquad (3.1)$$

as claimed. The n_i are determined by G, because n_i is the smallest positive integer n such that nG requires at most $s + r - i$ generators (we see from the representation) of G as a product that n_i has this property and that no smaller positive integer does).

10.4 SUMMARY

We Study inthis unit flat module over Principal Ideal Domain. We study finitely generated abelian group. We study Chinese remainder Theorem. We study finitely Flat cover and flat module. We study Fundamental Theorem of Arithmetic. We study flat ring extension. We also study

Fundamental theorem for finite abelian group. We study fundamental theorem for principal ideal domain.

1. A module M over a unit ring R is called flat iff the tensor product functor $-\otimes_R M$ (or, equivalently, the tensor product functor $M\otimes_R -$) is an exact functor.
2. Fundamental theorem of finite abelian groupsThis says that every finite abelian group can be expressed uniquely as a product of p-groups.
3. An R-module M is finitely-generated if there is a finite subset {x1, . . . , xn} in M such that if x is any element in M, there exist scalars {r1, . . . , rn} in R
   such that x = r1x1 + r2x2 + · · · + rnxn.
4. Let M be a (non-zero) finitely-generated R-module, where R is a P.I.D. Then there exist non-negative integers s and t and non-zero ring elements a1, a2, . . . , as for which
   M ∼= R/ha1i × R/ha2i × · · · × R/hasi × R t
5. Let V be a finitely-generated vector space over a field F. Then as an F-module,

   V ∼= F t for some non-negative integer t.

6. A Unique Factorization Domain (UFD) is an integral domain R in which every nonzero element r ∈ R that is not a unit has the following two properties:
   (a) r can be written as a finite product of irreducibles pi of R (not necessarily distinct): r = p1p2...pn and
   (b) this decomposition is unique up to associates: if r = r1r2...rm is another factorization of r into irreducibles, then m = n and there is some renumbering of the factors so that pi is associate to ri for i = 1, 2, ..., n.

10.5 KEYWORD

Determinants :A quantity obtained by the addition of products of the elements of a square matrix according to a given rule

Invertiable :Capable of being inverted or subjected to inversion an **invertible** matrix.

Decomposition :The state or process of rotting; decay

Conjecture :An opinion or conclusion formed on the basis of incomplete information

10.6 QUESTIONS FOR REVIEW

Q. 1 Let V be a t-dimensional F-vector space. Then the following are equivalent:

1. The set {v1, . . . ,vt} is a basis for V .

2. The set {v1, . . . ,vt} spans V .

3. The set {v1, . . . ,vt} is linearly independent.

Q. 2 A vector space V of dimension t has a basis of t elements. Moreover, if {v1, . . . ,vn} is a basis for V , then n = t.

Q. 3 Let R be a PID. Then, every nonempty set of ideals of R has a maximal element.

Q. 4 Structure Theorem for Abelian Groups) *Let G be a finitely generated abelian group. Then there is an isomorphism*

$$G \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r,$$

where $n_1 > 1$ *and* $n_1 \mid n_2 \mid \cdots \mid n_s$*. Furthermore, the* n_i *and* r *are uniquely determined by* G.

Q. 5 Suppose G *is a free abelian group of finite rank* n*, and* H *is a subgroup of* G*. Then* H *is a free abelian group generated by at most* n *elements.*

Q. 6 (1) Abelian groups, which are the same thing as a Z-module

(2) The field R is a R-module, Q-module, and Z-module.

(3) The free module of rank n over R as discussed

Q. 7 (The First Isomorphism Theorem for Modules). Let M and N be R-modules and let ϕ : M → N be an R-module homomorphism. Then, ker ϕ is a submodule of M and M/ ker ϕ ~= ϕ(M).

Q. 8 Suppose we have a ring R. Let n be a natural number. An example of a free module is Rn, which has a rank n over R.

10.7 SUGGESTION READING AND REFERENCES

1. Bourbaki, Ch. I, § 2. Proposition 13, Corollay 1.
2. Matsumura 1970, Corollary 1 of Theorem 55, p. 170
3. Matsumura 1970, Theorem 56
4. *"Flatness of Power Series Rings". mathoverflow.net.*
5. Eisenbud, Exercise 6.4.
6. Matsumura, Prop. 3.G
7. Eisenbud 1994, Theorem 6.8
8. Eisenbud 1994, Theorem 18.16
9. Proof: Suppose is faithfully flat. For an *A*-module *N*, the map exhibits *B* as a pure subring and so is injective. Hence, is injective. Conversely, if is amodule over
10. SGA 1, Exposé VIII., Corollay 4.3.
11. *"Amitsur Complex". ncatlab.org.*
12. Similarly, a right *R*-module *M* is flat if and only if for all and all left *R*-modules *X*.
13. Lam 1999, p. 183.
14. A module isomorphic to an flat module is of course flat.
15. Bican, El Bashir &Enochs 2001.
16. Richman 1997.
17. *Bican, L.; El Bashir, R.; Enochs, E. (2001), "All modules have flat covers", Bull. London Math. Soc.,* ***33*** *(4): 385–390, doi:10.1017/S0024609301008104, ISSN 0024-6093, MR 1832549*
18. N. Bourbaki, *Commutative Algebra*

Notes

19. *Chase, Stephen U. (1960), "Direct products of modules", Transactions of the American Mathematical Society,* ***97****: 457–473, doi:10.2307/1993382, MR 0120260*

20. *Eisenbud, David (1995), Commutative algebra, Graduate Texts in Mathematics,* ***150****, Berlin, New York: Springer-Verlag, doi:10.1007/978-1-4612-5350-1, ISBN 978-0-387-94268-1, MR 1322960, ISBN 978-0-387-94269-8*

21. *Enochs, Edgar E. (1981), "Injective and flat covers, envelopes and resolvents", Israel J. Math.,* ***39*** *(3): 189–209, doi:10.1007/BF02760849, ISSN 0021-2172, MR 0636889*

22. *Enochs, Edgar E.; Jenda, Overtoun M. G. (2000), Relative homological algebra, de Gruyter Expositions in Mathematics,* ***30****, Berlin: Walter de Gruyter& Co., doi:10.1515/9783110803662, ISBN 978-3-11-016633-0, MR 1753146*

23. *Kunz, Ernst (1969), "Characterizations of regular local rings of characteristic p", American Journal of Mathematics,* ***91****: 772–784, doi:10.2307/2373351, MR 0252389*

24. *Lam, Tsit-Yuen (1999), Lectures on modules and rings, Graduate Texts in Mathematics No. 189, Berlin, New York: Springer-Verlag, doi:10.1007/978-1-4612-0525-8, ISBN 978-0-387-98428-5, MR 1653294*

10.8 ANSWER TO CHECK YOUR PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 1

Q 2 Check in Section 1.3

Check in Progress-II

Answer Q. 1 Check in Section 3.3

Q 2 Check in Section 3.3

UNIT 11 - EMBEDDING INJECTIVE MODULE

STRUCTURE

11.0 OBJECTIVE

After study this unit we able to know about injective Embedding module. Learn to know R-Module.

* Learn Injective Hulls

* Learn Maximum Essense Extension

* Learn a module without radical

11.1 INTRODUCTION: INJECTIVE MODULE

Notes

This chapter discusses the pure-injective modules. A module is called pure-injective if it is a direct summand of every module in which it is a pure submodule. A non-zero pure-injective module is not slender; in fact, any non-zero homomorphic image of a pure-injective module is not slender. Thus any module which contains a non-zero homomorphic image of a pure-injective module, or contains a copy of R^{ω}, is not slender. Pure-injective modules over general rings have been studied in great depth by algebraists and model-theorists. This chapter deals with abelian groups, i.e., Z-modules, which refers to simply as groups. The cotorsion groups are precisely the homomorphic images of pure-injective groups. It is not true that every subgroup of a cotorsion group is cotorsion; in fact every group is a subgroup of a divisible, hence cotorsion, group.

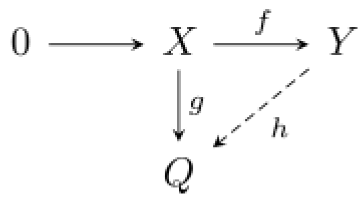
In mathematics, especially in the area of abstract algebra known as module theory, an **injective module** is a module *Q* that shares certain desirable properties with the **Z**-module **Q** of all rational numbers. Specifically, if *Q* is a submodule of some other module, then it is already a direct summand of that module; also, given a submodule of a module *Y*, then any module homomorphism from this submodule to *Q* can be extended to a homomorphism from all of *Y* to *Q*. This concept is dual to that of projective modules. Injective modules were introduced in (Baer 1940) and are discussed in some detail in the textbook (Lam 1999, §3).

Injective modules have been heavily studied, and a variety of additional notions are defined in terms of them: Injective cogenerators are injective modules that faithfully represent the entire category of modules. Injective resolutions measure how far from injective a module is in terms of the injective dimension and represent modules in the derived category. Injective hulls are maximal essential extensions, and turn out to be minimal injective extensions. Over a Noetherian ring, every injective module is uniquely a direct sum of indecomposable modules, and their structure is well understood. An injective module over one ring, may not be injective over another, but there are well-understood methods of changing rings which handle special cases. Rings which are themselves injective modules have a number of interesting properties and include rings such as group rings of finite groups over fields. Injective modules include divisible groups and are generalized by the notion of injective objects in category theory.

11.1.1 Definition

A left module Q over the ring R is injective if it satisfies one (and therefore all) of the following equivalent conditions:

- If Q is a submodule of some other left R-module M, then there exists another submodule K of M such that M is the internal direct sum of Q and K, i.e. $Q + K = M$ and $Q \cap K = \{0\}$.
- Any short exact sequence $0 \to Q \to M \to K \to 0$ of left R-modules splits.
- If X and Y are left R-modules, $f : X \to Y$ is an injective module homomorphism and $g : X \to Q$ is an arbitrary module homomorphism, then there exists a module homomorphism $h : Y \to Q$ such that $hf = g$, i.e. such that the following diagram commutes:



- The contravariant functor Hom(-,Q) from the category of left R-modules to the category of abelian groups is exact.

Injective right R-modules are defined in complete analog

• Every R-module M has an injective hull or injective envelope, denoted by ER(M), which is an injective module containing M, and has the property that any injective module containing M contains an isomorphic copy of ER(M).

• A nonzero injective module is indecomposable if it is not the direct sum of nonzero injective modules. Every injective R-module is a direct sum of indecomposable injective R-modules.

• Indecomposable injective R-modules are in bijective correspondence with the prime ideals of R; in fact every indecomposable injective R-module is isomorphic to an injective hull ER(R/p), for some prime ideal p of R.

• The number of isomorphic copies of ER(R/p) occurring in any direct sum decomposition of a given injective module into indecomposable injectives is independent of the decomposition.

• Let (R, m) be a complete local ring and E = ER(R/m) be the injective hull of the residue field of R. The functor (−) ∨ = HomR(−, E) has the following properties, known as Matlis duality:

(1) If M is an R-module which is Noetherian or Artinian, then M∨∨∼= M.

(2) If M is Noetherian, then M∨ is Artinian.

(3) If M is Artinian, then M∨ is Noetherian.

Definition. Let A be an integral domain. A A-module D is divisible if for every d e D and every 0 $ A E A there exists c e D such that Ac = d. Note that we do not require the uniqueness of c. We list a few examples:

(a) As 71-module the additive group of the rationals Q is divisible. In this example c is uniquely determined.

(b) As 71-module Q/Z is divisible. Here c is not uniquely determined.

(c) The additive group of the reals IR, as well as IR/Z, are divisible.

(d) A non-trivial finitely generated abelian group A is never divisible. Indeed. A is a direct sum of cyclic groups, which clearly are not divisible.

11.2 EMBEDDING MODULE

Let & be a class of rings and let &' be the class of all couples (A, M) where A is an element of & and where n/I is an A-module. By a morphism of a couple (A, M) into a couple (A', M') we mean a couple (ar, p) such that

a: is a homomorphism of rings of A into A';

p is a homomorphism of Z-modules of M into M' and Qa E A Qm E M 4am) = 44 &+

Such a couple (01, p) will be called an embedding (of (A, M) into (A', M')) if ~1 and p are both one-one. The reader may translate in this terminology the problem discussed in the previous section.

Among the elements of &?' are all the couples (A, A,), also denoted by (A, A), where A is an element of & and A, is the ring A considered as a left A-module. We will be concerned with the following problem, which will be called for convenience the embedding problem:

Is it possible to embed any element (A, M) of M in an element of the form (B, B) of &! ? We will only treat a few examples, some of which will be exploited in Section 4. In all of them J/ is an elementary class (in the wider sense) of rings.

Example 1 The embedding problem has a positive answer if ~2 is the class of (aZZ) commutative rings.

Proof. Let (-4, M) b e an element of &'. The following well-known multiplication transforms the additive group A x M into a commutative ring B:

(a, .m) . (a', m') = (au', ain' -+ a'm).

The morphism (01, p) of (A, M) into (B, B) such that

'da E A a(a) = (a, 0); vm E M p(m) = (0, m)

is an embedding.

PROPOSITION . The embedding problem has a positive answer in the following cases:

(i) &' is the class of division rings.

(ii) d is the class of jields.

Proof. Let (a, M) be an element of JBZ. Let E = (ei)icl be a basis of the d-module M. Let 01 be a (one-one) homomorphism of r-l into an element B of ~8 such that the dimension of the a(d)-module B is at least equal to

Notes

the dimension of the d-module M (such an CL clearly exists). Let f be a one-one map

of the set E into a basis F of the a(A)-module B. We define /~:M--fBby It is then easy to check that the couple (or, p) is an embedding of (A, M) into (B, B). Before stating the main result of this section we need to recall some definitions and facts.

Example Let A be a commutative absolutely flat ring. Then any A-module is without radical.

Proof. This is an immediate consequence of part of the two following facts: (VILLAMAYOR). For any Gng A the following conditions are eqzlivalent:

(1) Any simple A-module is injective.

(2) Atiy (left) ideal is the intersection of (left) maximal ideals.

(3) Any A-module is zuithout radical. (For background on the rings satisfying conditions (l), (2), (3), see [S]).

Example The embedding problem has a negative answer in the following cases:

(i) JZZ is the class of integral domains.

(ii) & is th e c 1 ass o frzn . g s w I zzc ' h are elementarily equivalent to the ring Z of integers.

Proof, Let us consider an element of Jz' of the form (2, M). It is easy to see that such an element can be embedded in an element of J&' of the form (A, -4) (if and) only if the Z-module M is torsion-free.

THEOREM Let JXI be an elementary class of rings. If d has a modelcompanion and if the embedding problem has a positive answer, then ~22 also has a model-companion.

Proof. It is clear that A?' is an elementary class. Let z?'* denote the modelcompanion of JTZ and let A'* denote the class of all pairs (A, M) where A is an element of &* and M is a free 8-module having a basis of cardinal 1. One easily checks that A?* is an elementary class which is the modelcompanion of A.

Example The class of p-rings has a model-completion.

Proof. It is enough to prove that the class of p-rings has a modelcompanion. Let us consider first the class of Boolean rings (p - 2). We claim that the class of atomless Boolean rings is the model-companion of the class of Boolean rings. We recall first the following well-known facts:

(a) An atomless Boolean ring is infinite.

(b) A countable Boolean ring is atomless if and only if it is free on X, generators and therefore any two countable atomless Boolean rings are isomorphic.

(c) It is possible to axiomatize the notion of atomless Boolean ring by a set of t/3 sentences.

Check in Progress-I

Note: i) Write your answers in the space given below.

Q. 1 The embedding problem has a positive answer if ~2 is the class of (aZZ) commutative rings.

Solution …………………………………………………………………

……………………………………………………………………………

…………………………………………………………………………….

Q. 2 Define Injective Module.

Solution …………………………………………………………………

……………………………………………………………………………

…………………………………………………………………………….

Theorem . Let A be a principal ideal domain. A A-module is injective if and only if it is divisible.

Proof First suppose D is injective. Let d e D and 0 $ A E A. We have to show that there exists c e D such that Ac = d. Define a : A-->D by a(1) = d and p : A--+A by µ(1) = A. Since A is an integral domain, i; A = 0 if and only if i; = 0. Hence p is monomorphic. Since D is injective. there exists fl: A-+D such that /iµ = a. We obtain

d=a(1)=/3µ(l)=/3(l)=2/3(11.

Hence by setting c = /3(1) we obtain d = Ac. (Notice that so far no use is made of the fact that A is a principal ideal domain.)

Now suppose D is divisible

We have to show the existence of fl: B--+D such that /3µ = a. To simplify the notation we consider p as an embedding of a submodule A into B. We look at pairs (A,, a) with A S A; C B, aj: Aj-*D such that aJIA = a. Let 0 be the set of all such pairs. Clearly 0 is nonempty, since (A, a) is in d.. The relation (A;, a)5 (Ak, ak) if A; c Ak and aklaj = ai defines an ordering in P. With this ordering 0 is inductive. Indeed, every chain (A;, 05), j e J has an upper bound, namely (U A;, U a) where UAW is simply the union, and Ua is defined as follows: If a e UA;, then a e Ak for some k e J. We define U+a,(a) = ak(a). Plainly U aj is welldefined and is a homomorphism, and

(A,,a,):! (UA,,Ua)

By Zorn's Lemma there exists a maximal element (A, a) in 0. We shall show that A = B, thus proving the theorem. Suppose A + B; then there exists b e B with b 0 A. The set of A e A such that Ab e A is readily seen to be an ideal ofA. Since A is a principal ideal domain, this ideal is generated by one element, say A0. If A0 + 0. then we use the fact that D is divisible to find c e D such that a(A0 b) = A c. If 20 = 0, we choose an arbitrary c. The homomorphism a may now be extended to the module A generated by A and b, by setting &(a + A b) = a() + A c. We have to check that this definition is consistent. If 2b e A, we have &(A b) = Ac. But A = l; A0 for some E A and therefore A b = l; 20 b. Hence

b) 1 c=Ac. Since (A, a) < (A, &),

this contradicts the maximality of (A, a), so that A = B as desired.

Proposition . Every quotient of a divisible module is divisible.

Proof. Let e : D--» E be an epimorphism and let D be divisible. For e e E and 0+ 2 E A there exists d c- D with s(d) = e and d' e D with Ad'=d. Setting e' = e(d') we have 2 e' = As(d') = e(2 d') = s(d) = e

Corollary . Let A be a principal ideal domain. Every quotient of an injective A-module is injective.

Proposition . Every abelian group may be embedded in a divisible (hence injective) abelian group. which says that every A-module is a quotient of a free, hence projective, Amodule.

Proof. We shall define a monomorphism of the abelian group A into a direct product of copies of Q/Z.

suffice. Let 0 + a e A and let (a) denote the subgroup of A generated by a. Define a : (a)-+Q2/7 as follows: If the order of a e A is infinite choose 0 $ a(a) arbitrary. If the order of a e A is finite, say n, choose 0+a(a) to have order dividing n. Since Q2/71 is injective, there exists a map A--+ Q2/7 such that the diagram

is commutative. By the universal property of the product, the Na define a unique homomorphism/3: A- H (Q 171)a. Clearly isamonomorphism since /3a(a) + 0 if a + 0. Q

For abelian groups, the additive group of the integers 71 is projective and has the property that to any abelian group G + 0 there exists a nonzero homomorphism p : 7-+G. The group Q2/71 has the dual properties; it is injective and to any abelian group G + 0 there is a nonzero homomorphism y,: G-+Q2/7L. Since a direct sum of copies of 71 is called free, we shall term a direct product of copies of Q/71 cofree. Note that the two properties of 7L mentioned above do not characterize 71 entirely. Therefore "cofree" is not the exact dual of "free", it is dual only in certain respects. In Section 8 the generalization of this concept to arbitrary rings is carried through.

Notes

Lemma . Let M be a module. Then M is injective iff HomR(−, M) is exact.

Proof. Let $0 \to N0 \to N \to N00 \to 0$ be an exact sequence. In general it follows that $0 \to HomR(N00, M) \to HomR(N, M) \to HomR(N0 , M)$ is exact. To make it right exact, we just need that $HomR(N, M) \to HomR(N0 , M)$ is surjective. This map is surjective for all exact sequences iff M is injective by definition.

Lemma . Let A be a Z-module. Then there exists an injective module I and a monomorphism $\phi : M \to I$.

Proof. Recall that Q/Z is injective. For a Z-module B define B∨ := HomZ(B, Q/Z). We now have a natural map as follows:

$$\psi : A \to A \vee$$

$$\vee\ a\ 7\to (\phi\ 7\to \phi(a))$$

One can easily see that this map is injective since Q/Z is injective. Now let j∈J Z → A∨ be a surjection, then we get an embedding A∨∨ = HomZ(A∨, Q/Z) → HomZ(L j∈J Z, Q/Z) ∼= (Q/Z) J . Hence we have an embedding A → (Q/Z) J . So, this last module is injective, and hence we are done.

Lemma . Let R be an S algebra. Let A be an injective S-module and P a projective R-module. Then HomS(P, A) is an injective R-module.

Proof. We need to show that HomR(−, HomS(P, A)) is exact. First notice that HomR(−, HomS(P, A)) ∼= HomS(−⊗RP, A) (universial property of tensor product). Now notice that the functor −⊗R P is exact since P is projective. As A is injective, it follows that HomS(−, A) is exact. Combine both to obtain the result.

Theorem . Let M be an R-module. Then there is an injective module I and a monomorphism $\phi : M \to I$.

Proof. First consider M as Z-module and by Lemma 1.7 there is a Z-injective module I1 such that we have a monomorphism $\phi 1 : M \to I1$. By the previous lemma, since R is projective over R, HomZ(R, I1) is injective. Consider the following map:

$\phi : M \to$ HomZ(R, I1)

m 7→ (r 7→ ϕ1(rm))

One can easily show that ϕ is R-linear and that ϕ is injective. Indeed, if ϕ(m) = 0, then ϕ1(m) = ϕ1(1cm˙) = 0 in I, hence m = 0.

11.3 INJECTIVE HULLS

Definition Let M be a module. A module E ⊃ M is called an essential extension of M if every non-zero submodule of E intersect M non-trivially. We denote this as E ⊃e M. Such an essential extension is called maximal if no module properly containing E is an essential extension of M.

Remarks. i. If E2 ⊃e E1 and E1 ⊃e M, then E2 ⊃e M (follows directly). ii. Let E ⊃ M. Then E is an essential extension of M if for any 0 6= a ∈ E we have Ra ∩ M ≠ 0.

Lemma . A module M is injective iff M has no proper essential extensions.

Proof. =⇒ : Suppose that M is injective and let E ⊃e M be an essential extension. Apply Lemma 1.3 ii, to see that 0 → M → E splits, that is, E = M ⊕ E0 for some submodule E0 ⊂ E. But then E0 ∩ M = 0, and hence E0 = 0 and M = E. ⇐=: Now suppose that M has no proper essential extension. Embed M into an injective module I and let S be a maximal submodule such that S ∩M = 0 (Zorn). Then I/S is an essential extension of I, hence M = I/S, hence I = M ⊕ S. that M itself is injective.

Lemma . Any module M has a maximal essential extension.

Proof. Embed M into an injective module I. We claim that there are maximal essential extensions of M in I. We order the set of essential extensions of M in I by inclusion. The union of a chain of essential extensions is again essential , and by Zorn's lemma there are maximal essential extensions of M in I. We claim that such an extension is a maximal essential extension (in general). Let E be such a maximal essential extension inside I and suppose that E0)e E ⊃e M. Since E → E0 is an inclusion and I is injective, we can extend the inclusion E → I to a map ϕ : E0 → I. Since Ker(ϕ) ∩ M = 0 (by construction), it follows that ϕ is injective (E0 ⊃e M is essential), but this contradicts the maximality of E inside.

Theorem . For modules M ⊂ I, the following are equivalent:

ii. I is a maximal essential extension of M.

iii. I is injective, and is essential over M.

iv. I is minimal injective over M.

Proof. i =⇒ ii: It follows that I is maximal essential, I it injective.

ii =⇒ iii: Suppose that M ⊂ I 0 ⊂ I is injective. Then I = I 0 ⊕ J for some submodule J As M ⊂ I 0 , it follows that J ∩ M = 0, since I ⊃e M, it follows that J = 0 and hence I = I 0 .

iii =⇒ i: it follows that there is a maximal essential extension E of M contained in I. By i =⇒ ii we see that E is injective. Since I was a minimal injective module containing M, we have E = I.

Definition . If M ⊂ I satisfy the equivalent properties of the above theorem, then I is called an injective hull of M.

Lemma . Let I, I0 be injective hulls of M. Then there exists an isomorphism g : I 0 → I which is the identity on M.

Proof. The map M → I 0 can be extended, by injectivity of I, to a map g : I → I 0 . The map is the identity on M and as before since (kerg) ∩ M = 0, it follows by essentiality that g is injective. Since I 0 was minimal injective, it follows that g is surjectie as well.

Check In Progress

Note: i) Write your answers in the space given below.

Q. 1 Any module M has a maximal essential extension.

Solution

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

Q. 2Let M be an R-module. Then there is an injective module I and a monomorphism ϕ : M → I.

Solution

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

11.4 SOME THEOREMS AND LEMMA

Notation . 'The' injective hull of M is denoted by E(M).

Lemma . i. If I is an injective module containing M, then I contains a copy of E(M). ii. If M ⊂e N, then N can be enlarged to a copy of E(M) and E(M) = E(N).

Proof. i. Embed M into an injective module I. We claim that there are maximal essential extensions of M in I. We order the set of essential extensions of M in I by inclusion. The union of a chain of essential extensions is again essential (use Remark 2.2), and by Zorn's lemma there are maximal essential extensions of M in I. We claim that such an extension is a maximal essential extension (in general). Let E be such a maximal essential extension inside I and suppose that E0)e E ⊃e M. Since E → E0 is an inclusion and I is injective, we can extend the inclusion E → I to a map ϕ : E0 → I. Since Ker(ϕ) ∩ M = 0 (by construction), it follows that ϕ

ii. It follows that E(N) ⊃e N ⊃e M. Hence E(N) ⊃e N and it is still a maximal essential extension. It follows that E(M) = E(N).

Proposition . Let M and E be R-modules.

(1) If E is injective and M ⊆ E, then any maximal essential extension of M in E is an injective module, hence is a direct summand of E.

(2) Any two maximal essential extensions of M are isomorphic.

Proof. (1) Let E0 be a maximal essential extension of M in E and let E0 ⊆ Q be an essential extension. Since E is injective, the identity map E0 −→ E lifts to a homomorphism ϕ : Q −→ E. Since Q is an essential extension of E0 , it follows that ϕ must be injective. This gives us M ⊆ E0 ⊆ Q ,→ E, and the maximality of E0 implies that Q = E0 . Hence E0 has no proper essential extensions, and so it is an injective module

(2) Let M ⊆ E and M ⊆ E0 be maximal essential extensions of M. Then E0 is injective, so M ⊆ E0 extends to a homomorphism ϕ : E −→ E0 . The inclusion M ⊆ E is an essential extension, so ϕ is injective. But then ϕ(E) is an injective module, and hence a direct summand of E0 . Since M ⊆ ϕ(E) ⊆ E0 is an essential extension, we must have ϕ(E) = E0 .

Definition . The injective hull or injective envelope of an R-module M is a maximal essential extension of M, and is denoted by ER(M).

Proposition (Bass). A ring R is Noetherian if and only if every direct sum of injective R-modules is injective.

Proof. We first show that if M is a finitely generated R-module, then

HomR(M, ⊕iNi) ∼= ⊕i HomR(M, Ni).

Independent of the finite generation of M, there is a natural injective homomorphism ϕ : ⊕i HomR(M, Ni) −→ HomR(M, ⊕iNi). If M is finitely generated, the image of a homomorphism from M to ⊕iNi is contained in the direct sum of finitely many Ni . Since Hom commutes with forming finite direct sums, ϕ is surjective as well.

Let R be a Noetherian ring, and Ei be injective R-modules. Then for an ideal a of R, the natural map HomR(R, Ei) −→ HomR(a, Ei) is surjective. Since a is finitely generated, the above isomorphism implies that HomR(R, ⊕Ei) −→ HomR(a, ⊕Ei) is surjective as well. Baer's criterion now implies that ⊕Ei is injective.

If R is not Noetherian, it contains a strictly ascending chain of ideals a1

(a2 (a3 (. . . . Let a = ∪iai .

The natural maps a ,→ R −→→ R/ai ,→ ER(R/ai) give us a homomorphism a −→ Q i ER(R/ai). The image lies in the submodule ⊕iER(R/ai), (check!) so we have a homomorphism ϕ : a −→ ⊕iER(R/ai). Lastly, check that ϕ does not extend to homomorphism R −→ ⊕iER(R/ai).

Theorem . Let E be an injective module over a Noetherian ring R. Then

E ∼= ⊕iER(R/pi),

where pi are prime ideals of R. Moreover, any such direct sum is an injective R-module.

Proof. The last statement follows. Let E be an injective R-module. By Zorn's Lemma, there exists a maximal family {Ei} of injective submodules of E such that Ei ∼= ER(R/pi), and their sum in E is a direct sum. Let E0 = ⊕Ei , which is an injective module, and hence is a direct summand of E. There exists an R-module E00 such that E = E0 ⊕ E00. If E00 6= 0, pick a nonzero element x ∈ E00. Let p be an associated prime of Rx. Then R/p ,→ Rx ⊆ E00, so there is a copy of ER(R/p) contained in E00 and E00 = ER(R/p) ⊕ E000, contradicting the maximality of family {Ei}.

Theorem . Let p be a prime ideal of a Noetherian ring R, and let E = ER(R/p) and κ = Rp/pRp, which is the fraction field of R/p. Then

(1) if x ∈ R \ p, then E x−→ E is an isomorphism, and so E = Ep;

(2) 0 :E p = κ;

(3) κ ⊆ E is an essential extension of Rp-modules and E = ERp (κ);

(4) E is p-torsion and Ass(E) = {p};

(5) HomRp (κ, E) = κ and HomRp (κ, ER(R/q)p) = 0 for primes q .

Proof. (1) κ is an essential extension of R/p by Example 1.8, so E contains a copy of κ and we may assume $R/p \subseteq \kappa \subseteq E$. Multiplication by $x \in R\backslash p$ is injective on κ, and hence also on its essential extension E. The submodule xE is injective, so it is a direct summand of E. But $\kappa \subseteq xE \subseteq E$ are essential extensions, so xE = E.

(2) 0 :E p = 0 :E pRp is a vector space over the field κ, and hence the inclusion $\kappa \subseteq$ 0 :E p splits. But $\kappa \subseteq$ 0 :E p $\subseteq$ E is an essential extension, so 0 :E p = κ

(3) The containment $\kappa \subseteq E$ is an essential extension of R-modules, hence also of Rp-modules. Suppose $E \subseteq M$ is an essential extension of Rp-modules, pick $m \in M$. Then m has a nonzero multiple $(r/s)m \in E$, where $s \in R \setminus p$. But then rm is a nonzero multiple of m in E, so $E \subseteq M$ is an essential extension of R-modules, and therefore M = E

(4) Let $q \in$ Ass(E). Then there exists $x \in E$ such that $Rx \subseteq E$ and 0 :R x = q. Since $R/p \subseteq E$ is essential, x has a nonzero multiple y in R/p. But then the annihilator of y is p, so q = p and Ass(E) = {p}

If a is the annihilator of a nonzero element of E, then p is the only associated prime of R/a ,→ E, so E is p-torsion.

(5) For the first assertion,

HomRp (κ, E) = HomRp (Rp/pRp, E) ∼= 0 :pRp E = κ.

Since elements of R\q act invertibly on ER(R/q), we see that ER(R/q)p = 0 if q * p. In the case $q \subseteq p$, we have

HomRp (κ, ER(R/q)p) ∼= 0 :pRp ER(R/q)p = 0 :pRp ER(R/q).

If this is nonzero, then there is a nonzero element of ER(R/q) killed by p, which forces q = p since Ass ER(R/q) = {q}.

Theorem . Let (R, m, K) be a local ring. Then ER(K) = ERb(K).

Proof. The containment $K \subseteq$ ER(K) is an essential extension of R-modules, hence also of Rb-modules. If ER(K) $\subseteq$ M is an essential extension of Rbmodules, then M is m-torsion. (Prove!) If $m \in M$ is a nonzero element, then Rmb ∩ ER(K) 6= 0. But Rmb = Rm, so ER(K) $\subseteq$

M is an essential extension of R-modules, which implies M = ER(K). It follows that ER(K) is a maximal essential extension of K as an Rb-module.

11.5 EXERCISE SOLVED

Exercise 1. Verify that f∗(M) is a left R-module using this definition of f · φ.

Proof : f∗(M) has the following additional structure. Let A be a R-module, so A is also a Z-module by forgetting the R-module structure. For a Z-module K, define ψA : HomZ(A,K) → HomR(A,HomZ(R,K)) by ψA(h) ∈ HomR(A,HomZ(R,K)) is defined by ψA(h)(a)(x) = h(x·a), where a ∈ A and x ∈ R. Here f∗(K) = HomZ(R,K)) is regarded as a R-module as in Exercise

Exercise 2. Show that for h ∈ HomZ(A,K), ψA(h) ∈ HomR(A,HomZ(R,K)).

Prof : For A and K as above, define τA : HomR(A,HomZ(R,K)) → HomZ(A,K) by τA(g)(a) = g(a)(1), for a ∈ A. It is very easy to check that τA(g) ∈ HomZ(A,K).

Exercise 3. Show that ψA and τA are inverse isomorphisms.

Proof : Let now B also be a R-module, with R-module homomorphism φ : A → B. Define φ ∗ Z : HomZ(B,K) → HomZ(A,K) by φ ∗ Z (f) = f ◦ φ. Define φ ∗ R : HomR(B,HomZ(R,K)) → HomR(A,HomZ(R,K)) by φ ∗ R(g) = g ◦ φ.

Exercise 4. Show the diagram is commutative, i.e., φ ∗ R ◦ ψB = ψA ◦ φ ∗ Z .

We may now explain how to construct injective R-modules.

Proposition 1. Let E be an injective Z-module. Then f∗(E) = HomZ(R,E) is an injective R-module.

Proof: Let i : M → N be an embedding of R-modules. We must show i ∗ R : HomR(N,f∗(E)) → HomR(M,f∗(E)) is surjective. By Exercise 4 applied with $i : M \to N$ in place of $\varphi : A \to B$ and with E in place of K, we have $i * R \circ \psi N = \psi M \circ i * Z$. Since E is an injective Z-module, $i * Z$: HomZ(N,E) → HomZ(M,E) is surjective by definition of injective module. By Exercise 3, it follows that $\psi M \circ i * Z$ is surjective, so $i * R \circ \psi N$ is surjective. In particular, $i * R$ is surjective, which completes the proof.

Theorem . Let M be a left R-module. Then there is an embedding M → G, where G is an injective R-module.

Proof : Regard M as a Z-module. there is an embedding of Z-modules h : M → E, where E is an injective Z-module. Define $\eta : M \to f*(E) =$ HomZ(R,E) by the formula $\eta(m)(r) = h(r \cdot m)$.

Exercise 5. η is a R-module homomorpism.

Definition. A natural transformation of functors T : F → G assigns to each object X of C a morphism TX : F(X) → G(X) with the property that for any two objects X,Y of C and each morphism f : X → Y in MorC(X,Y), then $G(f) \circ TY = TX \circ F(f)$, i.e., the following diagram commutes:

Exercise 6. : Prove that this T is a natural transformation between the contravariant functors F and G.

Proof : Further, we remark that f∗ as defined before is a covariant functor from (Z−mod) to (R − mod). We may define a covariant functor from (R − mod) to (Z − mod) by forgetting the R-module structure. This is an example of a forgetful functor and may be denoted by f ∗ (M) = M, where on the left M is regarded as a R-module, and on the right M is regarded as a Z-module by forgetting the R-module structure. In this language, we may restate the conclusion of Exercise 3 as stating that for R-module B and Z-module K, HomR(B,f∗(K)) ∼= HomZ(f ∗B,K). Then f∗ and f ∗ are called adjoint functors, and f∗ is called right adjoint of f ∗ and f ∗ is called left adjoint of f∗. There are many examples of this in mathematics.

Lemma . Every Abelian group can be embedded in a divisible Abelian group.

Proof. Let G be an Abelian group, and choose F = # g∈G Z and E = # g∈G Q, where Q is the additive group of rational numbers. Define the well-defined function θ : F → G by θ({ng}) = $ngg, where ng = 0 for all but a finite number of g ∈ G. We will first show that θ is a Z-epimorphism. Note that for every {ng}, {mg} ∈ F and z ∈ Z

θ({ng} + {mg}) = θ({ng + mg})

= ∑. g∈G (ng + mg) g

= ∑.g∈G ngg + mgg

= θ({ng}) + θ({mg})

And

θ(z{ng}) = θ({zng})

=∑..g∈G zngg

= zθ({ng}),

o θ is an Z-homomorphism. Let g0 ∈ G, and choose {ng} ∈ F so that ng = 0 if g (= g0 and ng = 1 if g = g0. Thus, θ({ng}) = $ngg = 1g0 = g0, showing that θ is a Z-epimorphism.

Note that F/Ker(θ) is a subgroup of E/Ker(θ). Now, since Q is divisible, so is E = # g∈G Q. Thus, E/Ker(θ) is a divisible Abelian group Because G ≈ F/Ker(θ) ι −→ E/Ker(θ), where ι is the inclusion mapping, G can be embedded in a divisible Abelian group

Lemma . Let D be a divisible abelian group. Then HomZ(R, D) is an injective Rmodule.

Proof. Recall that HomZ(R, D) is an R-module via (f + g)(x) = f(x) + g(x) and (rf)(x) = f(xr) for every r, x ∈ R and f,g ∈ HomZ(R, M). Let f : I → HomZ(R, D) be an Rhomomorphism, where I is a left ideal of R. Define the well-defined function h : I → D by h(a)=[f(a)](1R). Also, note that for every a, b ∈ I and z ∈ Z,

h(a + b)=[f(a + b)](1R)

= [f(a)](1R)+[f(b)](1R)

$$= h(a) + h(b),$$

so h is an Z-homomorphism, a.k.a. a group homomorphism. Since D is an injective Zmodule , there exists a Z-homomorphism (: R → D, so (|I= h. Now, let g : R → HomZ(R, D) be the well-defined function given by [g(r)](x) = ((xr) for every x ∈ R, where g(r) ∈ HomZ(R, D). Note that for every a, b ∈ R, g(a + b) = g(a) + g(b) since for every x ∈ R,

$$[g(a + b)](x) = ((x[a + b])$$

$$=l((xa + xb)$$

$$= ((xa) + ((xb)$$

$$= [g(a)](x)+[g(b)](x)$$

and g(ab) = ag(b) since for every x ∈ R,

$$g(ab)](x) = ((x[ab])$$

$$= (([xa]b)$$

$$= [g(b)](xa)$$

$$= a[g(b)](x).$$

Thus, g is an R-homomorphism. Lastly, observe that g(r) = f(r) for every r ∈ I since for every x ∈ R,

$$[g(r)](x) = ((xr) = h(xr)=[f(xr)](1R) = x[f(r)](1R)=[f(r)](x).$$

Hence, HomZ(R, D) is an injective R-module.

Corollary . Let M be an injective Abelian group. Then HomZ(R, M) is an injective R-module.

Theorem . Every R-module has an injective extension.

Proof. Let M be an R-module. Then, there is an injective R-module J such that a function f : M → J is an R-monomorphism. there is an R-module extension B of M that is R-isomorphic to J. Thus, B is an injective extension of M.

11.6 SUMMARY

We study in this unit embedding injective module and its properties and examples. We study injective Hulls and Embedding modules and its properties with some important examples and lemma.We study some examples of extension module. We study principal ideal domain of the module.

1. Let (R, m) be a complete local ring and E = ER(R/m) be the injective hull of the residue field of R. The functor (−) ∨ = HomR(−, E) has the following properties, known as Matlis duality:

   (a) If M is an R-module which is Noetherian or Artinian, then M∨∨∼= M.

   (b) If M is Noetherian, then M∨ is Artinian.

   (c) If M is Artinian, then M∨ is Noetherian.
2. Let A be a principal ideal domain. A A-module is injective if and only if it is divisible.
3. Let M be a module. Then M is injective iffHomR(−, M) is exact.
4. Let M be a module. A module E ⊃ M is called an essential extension of M if every non-zero submodule of E intersect M non-trivially. We denote this as E ⊃e M. Such an essential extension is called maximal if no module properly containing E is an essential extension of M.
5. Let E be an injective module over a Noetherian ring R. Then E ∼= ⊕iER(R/pi),

   where pi are prime ideals of R. Moreover, any such direct sum is an injective R-module.
6. Let M be a left R-module. Then there is an embedding M → G, where G is an injective R-module.

11.7 KEYWORD

Hulls : The main body of a ship or other vessel, including the bottom, sides, and deck but not the masts, superstructure, rigging, engines, and other fittings

Samonomorphism :A transformation of one set into another that preserves in the second set the relations between elements of the first

Embedding : Fix (an object) firmly and deeply in a surrounding mass

Couples : Two people or things of the same sort considered together

11.8 QUESTIONS FOR REVIEW

Q. 1 Prove the following proposition: The A module I is injective if and only if for every left ideal J C A and for every A-module homomorphism a : J--+I the diagram J--*A aI I may be completed by a homomorphism f : A--+I such that the resulting triangle is commutative.

Q. 2 Let F--.A--.O be a short exact sequence of abelian groups, with F free. By embedding F in a direct sum of copies of Q. show how to embed A in a divisible group.

Q. 3. Show that every abelian group admits a unique maximal divisible subgroup.

Q. 4 Show that if A is a finite abelian group, then Hom7(A, Q/Z) = A. Deduce that if there is a short exact sequence of abelian groups with A finite, then there is a short exact sequence

Q. 5 Show that a torsion-free divisible group D is a Q-vector space. Show that Hom7(A, D) is then also divisible. Is this true for any divisible group D?

Q. 6 Show that Q is a direct summand in a direct product of copies of Q/1L.

Q. 7 For example Q/Z is Z-injective. This follows easily from Baer's criterion (it shows that a group is injective iff the group is divisble).

Q. 8 Let Mj ⊂ Ej for all j ∈ J be modules over R. Then L L j∈J Mj ⊂e j∈J Ej iff for all j ∈ J : Mj ⊂e Ej .

Q. 9 Let Mj for $1 \leq j \leq n$ be R-modules. Then E(Ln j=1 Mj) = Ln j=1 E(Mj).

Q. 10 Let R be a domain. Then we know that Q(R) is injective (Example 1.6), and Q(R) is essential over R. Hence E(R) = Q(R).

Q. 11 Let Cn denote the cyclic group of order n. Define Cp∞ = S i∈Z≥1 Cpi . One can easily check that this group is divisble, hence injective over Z. It is easy to see that Cp∞ is essential over Cpi for i ∈ Z≥1. Therefore E(Cpi) = Cp∞ for i ∈ Z≥1.

Q. 12 Let k be a field, then k is injective over k (see Example 1.6). Let R be a finite algebra over k. Let Rˆ := Homk(R, k). We have seen in Lemma 1.8 that Rˆ is injective. Let S ⊂ Rˆ be the module generated by all simple submodules of Rˆ. Since any module contains a simple submodule, it follows that E(S) = Rˆ. One can show that S ∼= R/radR where radR is the Jacobson radical of R (the intersection of the maximal ideals

Q. 13 Let R be an integral domain. An R-module M is divisible if rM = M for every nonzero element r ∈ R.

(1) Prove that an injective R-module is divisible.

(2) If R is a principal ideal domain, prove that an R-module is divisible if and only if it is injective.

(3) Conclude that Q/Z is an injective Z-module.

(4) Prove that any nonzero Abelian group has a nonzero homomorphism to Q/Z.

11.9 SUGGESTION READING AND REFERENCES

- Baer, Reinhold (1940), "Abelian groups that are direct summands of every containing abelian group", Bulletin of the American Mathematical Society, **46** (10): 800–807, doi:10.1090/S0002-9904-1940-07306-9, MR 0002886, Zbl 0024.14902

Notes

- Chase, Stephen U. (1960), "Direct products of modules", Transactions of the American Mathematical Society, Transactions of the American Mathematical Society, Vol. 97, No. 3, **97** (3): 457–473, doi:10.2307/1993382, JSTOR 1993382, MR 0120260
- Dade, Everett C. (1981), "Localization of injective modules", Journal of Algebra, **69** (2): 416–425, doi:10.1016/0021-8693(81)90213-1, MR 0617087
- Eckmann, B.; Schopf, A. (1953), "Über injektive Moduln", Archiv der Mathematik, **4** (2): 75–78, doi:10.1007/BF01899665, MR 0055978
- Lambek, Joachim (1963), "On Utumi's ring of quotients", Canadian Journal of Mathematics, **15**: 363–370, doi:10.4153/CJM-1963-041-4, ISSN 0008-414X, MR 0147509
- Matlis, Eben (1958), "Injective modules over Noetherian rings", Pacific Journal of Mathematics, **8**: 511–528, doi:10.2140/pjm.1958.8.511, ISSN 0030-8730, MR 0099360[permanent dead link]
- Osofsky, B. L. (1964), "On ring properties of injective hulls", Canadian Mathematical Bulletin, **7**: 405–413, doi:10.4153/CMB-1964-039-3, ISSN 0008-4395, MR 0166227
- Papp, Zoltán (1959), "On algebraically closed modules", Publicationes Mathematicae Debrecen, **6**: 311–327, ISSN 0033-3883, MR 0121390
- Smith, P. F. (1981), "Injective modules and prime ideals", Communications in Algebra, **9** (9): 989–999, doi:10.1080/00927878108822627, MR 0614468
- Utumi, Yuzo (1956), "On quotient rings", Osaka Journal of Mathematics, **8**: 1–18, ISSN 0030-6126, MR 0078966
- Vámos, P. (1983), "Ideals and modules testing injectivity", Communications in Algebra, **11** (22): 2495–2505, doi:10.1080/00927878308822975, MR 0733337

11.10 ANSWER TO CHECK YOUR PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 2

Q 2 Check in Section 1

Check in Progress-II

Answer Q. 1 Check in Section 3

Q 2 Check in Section 2

UNIT 12 - TENSOR PRODUCT OF MODULE

STRUCTURE

12.0 OBJECTIVE

* Learn tensor product of module and balanced product

* learn an element as a bilinear map

* Learn vector space tensor product

* learn universal property

12.1 INTRODUCTION:

In mathematics, the **tensor product of modules** is a construction that allows arguments about bilinear maps (e.g. multiplication) to be carried out in terms of linear maps. The module construction is analogous to the construction of the tensor product of vector spaces, but can be carried out for a pair of modules over a commutative ring resulting in a third module, and also for a pair of a right-module and a left-module over any ring, with result an abelian group. Tensor products are important in areas of abstract algebra, homological algebra, algebraic topology, algebraic geometry, operator algebras and noncommutative geometry. The universal property of the tensor product of vector spaces extends to more general situations in abstract algebra. It allows the study of bilinear or multilinear operations via linear operations. The tensor product of an algebra and a module can be used for extension of scalars. For a commutative ring, the tensor product of modules can be iterated to form the tensor algebra of a module, allowing one to define multiplication in the module in a universal way.

One of the things which distinguishes the modern approach to Commutative Algebra is the greater emphasis on modules, rather than just on ideals. An ideal a and its quotient ring A/a are both examples of modules. The collection of all modules over a given ring contains the collection of all ideals of that ring as a subset. The concept of modules is in fact a generalization of the concept of ideals. In this chapter, we give the definition and elementary properties of modules. Throughout this report,let A denote a commutative ring with unity 1.

12.1.1 Balanced Product

For a ring R, a right R-module M, a left R-module N, and an abelian group G, a map $\varphi: M \times N \to G$ is said to be ***R*-balanced**, ***R*-middle-linear** or an ***R*-balanced product** if for all m, m' in M, n, n' in N, and r in R the following hold:

The set of all such balanced products over R from $M \times N$ to G is denoted by $L_R(M, N; G)$.

If φ, ψ are balanced products, then each of the operations $\varphi + \psi$ and $-\varphi$ defined pointwise is a balanced product. This turns the set $L_R(M, N; G)$ into an abelian group.

For M and N fixed, the map $G \mapsto L_R(M, N; G)$ is a functor from the category of abelian groups to the category of sets. The morphism part is given by mapping a group homomorphism $g : G \to G'$ to the function $\varphi \mapsto g \circ \varphi$, which goes from $L_R(M, N; G)$ to $L_R(M, N; G')$.

Remarks

1. Property (Dl) states the left and property (Dr) the right distributivity of φ over addition.
2. Property (A) resembles some associative property of φ.
3. Every ring R is an R-R-bimodule. So the ring multiplication $(r, r') \mapsto r \cdot r'$ in R is an R-balanced product $R \times R \to R$.

The tensor product of two R-modules is built out of the examples given above. Let M and N be two R-modules. Here is the formula for M ⊗ N:

$M \otimes N = Y/Y(S)$, $Y = L(M \times N)$,…………….. (1)

and S is the set of all formal sums of the following type:

1. (rv, w) − r(v, w).

2. (w, rv) − r(v, w).

3. (v1 + v2, w) − (v1, w) − (v2, w).

4. (v, w1 + w2) − (v, w1) − (v, w2).

Our convention is that (v, w) stands for 1(v, w), which really is an element of L(M × N). Being the quotient of an R-module by a submodule, M ⊗ N is another R-module. It is called the tensor product of M and N. There is a map $B : M \times N \to M \otimes N$ given by the formula

$B(m, n) = [(m, n)] = (m, n) + Y(S)$,………………………………….. (2)

namely, the Y (S)-coset of (m, n). The traditional notation is to write

$$m \otimes n = B(m, n) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots .. (3)$$

The operation $m \otimes n$ is called the tensor product of elements.

Given the nature of the set S in the definition of the tensor product, we have the following rules:

1. $(rv) \otimes w = r(v \otimes w)$.

2. $r \otimes (rw) = r(v \otimes w)$.

3. $(v1 + v2) \otimes w = v1 \otimes w + v2 \otimes w$.

4. $v \otimes (w1 + w2) = v \otimes w1 + v \otimes w2$.

These equations make sense because $M \otimes N$ is another R-module. They can be summarised by saying that the map B is bilinear . We will elaborate below.

An Example: Sometimes it is possible to figure out $M \otimes N$ just from using the rules above. Here is a classic example. Let R = Z, the integers. Any finite abelian group is a module over Z. The scaling rule is just mg = g + ... + g (m times). In particular, this is true for Z/n. Let's show that $Z/2 \otimes Z/3$ is the trivial module.

Consider the element $1 \otimes 1$. We have

$$2(1 \otimes 1) = 2 \otimes 1 = 0 \otimes 1 = 0(1 \otimes 1) = 0.$$

At the same time

$$2(1 \otimes 1) = 1 \otimes 3 = 1 \otimes 0 = 0(1 \otimes 1) = 0.$$

But then

$$1(1 \otimes 1) = (3 - 2)(1 \otimes 1) = 0 - 0 = 0.$$

Hence $1 \otimes 1$ is trivial. From here it is easy to see that $a \otimes b$ is trivial for all $a \in Z/2$ and $b \in Z/3$. There really aren't many choices. But $Z/2 \otimes Z/3$ is the span of the image of $M \times N$ under the tensor map. Hence $Z/2 \otimes Z/3$ is trivial.

12.1.2 The Universal Property

Linear and Bilinear Maps: Let M and N be R-modules. A map $\varphi : M \to N$ is R-linear (or just linear for short) provided that

1. $\varphi(rv) = r\varphi(v)$.

2. $\varphi(v1 + v2) = \varphi(v1) + \varphi(v2)$.

A map $\varphi : M \times N \to P$ is R-bilinear if

1. For any $m \in M$, the map $n \to \varphi(m, n)$ is a linear map from N to P.

2. For any $n \in N$, the map $m \to \varphi(m, n)$ is a linear map from M to P

Existence of the Universal Property: The tensor product has what is called a universal property. The name comes from the fact that the construction to follow works for all maps of the given type.

Lemma Suppose that $\varphi : M \times N \to P$ is a bilinear map. Then there is a linear map $b\varphi : M \otimes N \to P$ such that $\varphi(m, n) = b\varphi(m \otimes n)$. Equivalently, $\varphi = b\varphi \circ B$, where $B : M \times N \to M \otimes N$ is as above

Proof: First of all, there is a linear map $\psi : Y(M \times N) \to P$. The map is given by

$$\psi(r1(v1, w1) + ... + rn(vn, wn)) = r1\psi(v1, w1) + ... + rn\psi(vn, wn). \quad (4)$$

That is, we do the obvious map, and then simplify the sum in P. Since φ is bilinear, we see that $\psi(s) = 0$ for all $s \in S$. Therefore, $\psi = 0$ on $Y(S)$. But then ψ gives rise to a map from $M \otimes N = Y/Y(S)$ into P, just using the formula

$$\varphi(a + Y(S)) = \psi(a). \quad (5)$$

Since ψ vanishes on $Y(S)$, this definition is the same no matter what coset representative is chosen. By construction $b\varphi$ is linear and satisfies $b\varphi(m\otimes n) = \varphi(m, n)$. ♠

Uniqueness of the Universal Property: Not only does $(B, M \otimes N)$ have the universal property, but any other pair $(B', (M \otimes N)')$ with the same property is essentially identical to $(B, M \otimes N)$. The next result says this precisely.

Lemma Suppose that $(B', (M \otimes N)')$ is a pair satisfying the following axioms:

- $(M \otimes N)'$ is an R-module.
- $B' : M \times N \to (M \otimes N)'$ is a bilinear map.
- $(M \otimes N)'$ is spanned by the image $B'(M \times N)$.
- For any bilinear map $T : M \times N \to P$ there is a linear map $L : (M \otimes N)' \to P$ such that $T = L \circ B'$.

Then there is an isomorphism $I : M \otimes N \to (M \otimes N)'$ and $B' = I \circ B$.

Proof: Since $(B, M \otimes N)$ has the universal property, and we know that $B' : M \times N \to (M \otimes N)'$ is a bilinear map, there is a linear map $I : M \otimes N \to (M \otimes N)'$ such that

$$B' = I \circ B.$$

We just have to show that I is an isomorphism. Reversing the roles of the two pairs, we also have a linear map $J : (M \otimes N)' \to M \otimes N$ such that

$$B = J \circ B'.$$

Combining these equations, we see that

$$B = J \circ I \circ B.$$

But then $J \circ I$ is the identity on the set $B(M \times N)$. But this set spans $M \otimes N$. Hence $J \circ I$ is the identity on $M \otimes N$. The same argument shows that $I \circ J$ is the identity on $(M \otimes N)'$. But this situation is only possible if both I and J are isomorphisms.

Check in Progress-I

Note: i) Write your answers in the space given below.

Q. 1 Define Universal Property.

Solution ………………………………………………………………

…………………………………………………………………………..

……………………………………………………………………………

Q. 2 Define Balance Product.

Solution ………………………………………………………………

…………………………………………………………………………..

……………………………………………………………………………

12.1.3 Properties Of The Tensor Product

Going back to the general case, here I'll work out some properties of the tensor product. As usual, all modules are unital R-modules over the ring R.

Lemma $M \otimes N$ is isomorphic to $N \otimes M$.

Proof: This is obvious from the construction. The map $(v, w) \to (w, v)$ extends to give an isomorphism from $Y_{M,N} = L(M \times N)$ to $Y_{N,M} = L(N \times N)$, and this isomorphism maps the set $S_{M,N} \subset Y_{M,N}$ of bilinear relations set $S_{N,M} \subset Y_{N,M}$ and therefore gives an isomorphism between the ideals $Y_{M,N}$ $S_{M,N}$ and $Y_{N,M}$ $S_{N,M}$. So, the obvious map induces an isomorphism on the quotients.

Lemma $R \otimes M$ is isomorphic to M.

Proof: The module axioms give us a surjective bilinear map $T : R \times M \to M$ given by $T(r, m) = rm$. By the universal property, there is a linear map $L : R \otimes M \to M$ such that $T = L \circ B$. Since T is surjective, L is also surjective. At the same time, we have a map $L* : M \to R \otimes M$ given by the formula

$$L*(v) = B(1, v) = 1 \otimes v. \qquad (9)$$

The map $L*$ is linear because B is bilinear. We compute

$$L* \circ L(r \otimes v) = L*(rv) = 1 \otimes rv = r \otimes v. \qquad (10)$$

So $L * \circ L$ is the identity on the image $B(R \times M)$. But this image spans $R \otimes M$. Hence $L * \circ L$ is the identity. But this is only possible if L is injective. Hence L is an isomorphism.

Lemma $M \otimes (N1 \times N2)$ is isomorphic to $(M \otimes N1) \times (N \otimes N2)$.

Proof: Let $N = N1 \times N2$. There is an obvious isomorphism φ from Y = YM,N to $Y1 \times Y2$, where Yj = YM,Nj , and $\varphi(S) = S1 \times S2$. Here Sj = SM,Nj . Therefore, φ induces an isomorphism from Y/Y S to $(Y1/Y1S1) \times (Y2/Y2S2)$.

Lemma $M \otimes Rn$ is isomorphic to Mn.

Proof: By repeated applications of the previous result, $M \otimes Rn$ is isomorphic to $(M \otimes R)$ n , which is in turn isomorphic to Mn . ♠

Lemma Suppose that Y is a module and $Y' \subset Y$ and $I \subset Y$ are both submodules. Let $I' = I \cap Y'$. Then there is an injective linear map from Y'/I' into Y/I.

Proof: We have a linear map $\varphi : Y' \to Y/I$ induced by the inclusion from Y' into Y . Suppose that $\varphi(a) = 0$. Then $a \in I$. But, at the same time $a \in Y'$. Hence $a \in I'$. Conversely, if $a \in I'$ then $\varphi(a) = 0$. In short, the kernel of φ is I'. But then the usual isomorphism theorem shows that φ induces an injective linear map from Y'/I' into Y/I. ♠

Lemma Suppose that $M' \subset M$ and $N' \subset N$ are submodules. Then there is an injective linear map from $M' \otimes N'$ into $M \otimes N$. This map is the identity on elements of the form $a \otimes b$, where $a \in M'$ and $b \in N'$.

Proof: We apply the previous result to the module Y = YM,N and the submodules I = SM,N and M′ = YM′ ,N′. ♠

In view of the previous result, we can think of $M' \otimes N'$ as a submodule of $M \otimes N$ when $M' \subset N$ and $N' \subset N$ are submodules.

This last result says something about vector spaces. Let's take an example where the field is Q and the vector spaces are R and R/Q. These two vector spaces are infinite dimensional. It follows from Zorn's lemma that they both have bases. However, You might want to see that $R \otimes R/Q$

is nontrivial even without using a basis for both. If we take any finite dimensional subspaces V ⊂ R and W ⊂ R/Q, then we know V ⊗ W is a submodule of R ⊗ R/Q. Hence R ⊗ R/Q is nontrivial. In particular, we can use this to show that the element 1 ⊗ [α] is nontrivial when α is irrational.

12.1.4 Additional Structure

If S and T are commutative R-algebras, then $S \otimes_R T$ will be a commutative R-algebra as well, with the multiplication map defined by $(m_1 \otimes m_2)(n_1 \otimes n_2) = (m_1n_1 \otimes m_2n_2)$ and extended by linearity. In this setting, the tensor product become a fibered coproduct in the category of R-algebras.

If M and N are both R-modules over a commutative ring, then their tensor product is again an R-module. If R is a ring, ${}_RM$ is a left R-module, and the commutator

$$rs - sr$$

of any two elements r and s of R is in the annihilator of M, then we can make M into a right R module by setting

$$mr = rm.$$

The action of R on M factors through an action of a quotient commutative ring. In this case the tensor product of M with itself over R is again an R-module. This is a very common technique in commutative algebra.

12.1.5 An Element As A (Bi)Linear Map

In the general case, each element of the tensor product of modules gives rise to a left R-linear map, to a right R-linear map, and to an R-bilinear form. Unlike the commutative case, in the general case the tensor product is not an R-module, and thus does not support scalar multiplication.

- Given right R-module E and right R-module F, there is a canonical homomorphism $\theta : F \otimes_R E^* \to \mathrm{Hom}_R(E, F)$ such that $\theta(f \otimes e')$ is the map $e \mapsto f \cdot \langle e', e \rangle$.

- Given left R-module E and right R-module F, there is a canonical homomorphism $\theta : F \otimes_R E \rightarrow \mathrm{Hom}_R(E^*, F)$ such that $\theta(f \otimes e)$ is the map $e' \mapsto f \cdot \langle e, e' \rangle$.

Both cases hold for general modules, and become isomorphisms if the modules E and F are restricted to being finitely generated projective modules (in particular free modules of finite ranks). Thus, an element of a tensor product of modules over a ring R maps canonically onto an R-linear map, though as with vector spaces, constraints apply to the modules for this to be equivalent to the full space of such linear maps.

- Given right R-module E and left R-module F, there is a canonical homomorphism $\theta : F^* \otimes_R E^* \rightarrow \mathrm{L}_R(F \times E, R)$ such that $\theta(f' \otimes e')$ is the map $(f, e) \mapsto \langle f, f' \rangle \cdot \langle e', e \rangle$. Thus, an element of a tensor product $\xi \in F^* \otimes_R E^*$ may be thought of giving rise to or acting as an R-bilinear map $F \times E \rightarrow R$.

12.1.6 Basic Idea

Today we talk tensor products. Specifically this post covers the construction of the tensor product between two modules over a ring. But before jumping in, I think now's a good time to ask, "What are tensor products good for?" Here's a simple example where such a question might arise:

Suppose you have a vector space V over a field F. For concreteness, let's consider the case when V is the set of all 2×2 matrices with entries in R and let F=R. In this case we know what "F-scalar multiplication" means: if M∈V is a matrix and c∈R, then the new matrix cM makes perfect sense. But what if we want to multiply M by *complex* scalars too? How can we make sense of something like (3+4i)M? That's precisely what the tensor product is for! We need to create a set of elements of the form(complex number) "times" (matrix)(complex number) "times" (matrix)so that the mathematics still makes sense. With a little massaging, this set will turn out to be C⊗RV.

So in general, if F is an arbitrary field and V an F-vector space, the tensor product answers the question "How can I define scalar multiplication by some *larger* field which contains F?" And of course this holds if we replace the word "field" by "ring" and consider the same scenario with modules.

Let R be a ring with 1 and let M be a right R-module and NN a left R-module and suppose A is any abelian group. Our goal is to create an abelian group M⊗RN, called the **tensor product** of M and N, such that if there is an R-balanced map i:M×N→M⊗RN and any R-balanced map φ:M×N→A, then there is a unique abelian group homomorphism Φ:M⊗RN→ such that φ=Φ∘, i.e. so the diagram below commutes.

Definition: Let X be a set. A group F is said to be a **free group** on X if there is a function i:X→F such that for any group G and any set map φ:X→G there exists a unique group homomorphism Φ:F→G such that the following diagram commutes: (i.e. φ=Φ∘i) set map, so in particular we just want our's to be R-balanced:

Let R be a ring with 1. Let M be a right R-module, N a left R-module, and A an abelian group. A map φ:M×N→R is called R-balanced if for all m,m1,m2∈M, all n,n1,n2∈Nand all r∈R,

φ(m1+m2,n)=φ(m1,n)+φ(m2,n)
=φ(m,n1+n2)=φ(m,n1)+φ(m,n2))φ(mr,n)=φ(m,rn)
By "replacing" F by a certain quotient group F/H (We'll
define H precisely below.)

These observations give us a road map to construct the tensor product. And so we begin:

Step 1

Let F be a free abelian group generated by M×N and let A be an abelian group. Then by definition (of free groups), if φ:M×N→ is any set map, and M×N↪F by inclusion, then there is a unique abelian group homomorphism Φ:F→ A

Step 2

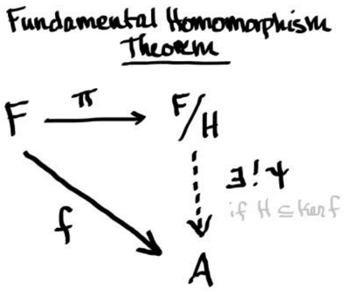
that the inclusion map $M \times N \hookrightarrow F$ is not R-balanced! To fix this, we must "modify" the target space F by replacing it with the quotient F/H where $H \leq F$ is the subgroup of F generated by elements of the form

- $(m1+m2,n)-(m1,n)-(m2,n)$
- $(m,n1+n2)-(m,n1)-(m,n2)$
- $(mr,n)-(m,rn)$

where $m1,m2,m \in M$, $n1,n2,n \in N$ and $r \in R$. Why elements of this form? Because if we define the map $i:M \times N \to F/H$ by$i(m,n)=(m,n)+H$,we'll see that ii is indeed R-balanced!

So, are we done now? Can we really just replace F with F/H and replace the inclusion map with the map ii, and *still* retain the existence of a unique homomorphism $\Phi:F/H \to A$? No! Of course not. F/H is *not* a free group generated by $M \times N$.

Step 3

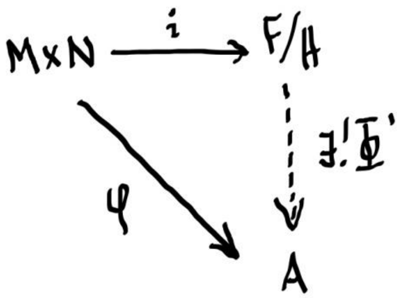


$H \subseteq \ker(f)$, that is as long as $f(h)=0$ for all $h \in H$. And notice that this condition, $f(H)=0$, forces f to be R-balanced!

Sooooo... homomorphisms $f:F \to A$ such that $H \subseteq \ker(f)$ are the same as R-balanced maps from $M \times N$ to A! (Technically, I should say *homomorphisms* f *restricted to* $M \times N$ In other words, we have

In conclusion, to say "abelian group homomorphisms from F/H to A are the same as (isomorphic to) R-balanced maps from $M \times N$ to A" is the simply the *hand-wavy* way of saying

Whenever i:M×N→F is an R-balanced map and φ:M×N→A is an R-balanced map where A is an abelian group, there exists a unique abelian group homomorphism Φ:F/H→A. such that the following diagram commutes:



And this is just want we want! The last step is merely the final touch:

Step 4

the abelian quotient group F/H to be the tensor product of M and N,

$$F/H := M \otimes_R N$$

whose elements are cosets,

$$(m,n) + H := m \otimes n$$

where m⊗n for m∈M and n∈N is referred to as a *simple tensor*. And there you have it! The tensor product, constructed.

The tensor product between modules A and B is a more general notion than the vector space tensor product. In this case, we replace "scalars" by a ring R. The familiar formulas hold, but now α is any element of R,

$$(a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b \tag{1}$$
$$a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2 \tag{2}$$
$$\alpha (a \otimes b) = (\alpha a) \otimes b = a \otimes (\alpha b). \tag{3}$$

This generalizes the definition of a tensor product for vector spaces since a vector space is a module over the scalar field. Also, vector bundles can be considered as projective modules over the ring of functions, and group representations of a group G can be thought of as modules over CG. The generalization covers those kinds of tensor products as well.

There are some interesting possibilities for the tensor product of modules that don't occur in the case of vector spaces. It is possible for $A \otimes_R B$ to be identically zero. For example, the tensor product of C_2 and C_3 as modules over the integers, $C_2 \otimes_Z C_3$, has no nonzero elements. It is enough to see that $a \otimes b = 0$. Notice that $1 = 3 - 2$. Then

$$(1)\, a \otimes b = (3 - 2)\, a \otimes b = (-2\, a) \otimes b + a \otimes (3\, b) = 0 + 0 \quad (4)$$

since $-2\, a = -a - a = 0$ in C_2 and $3\, b = b + b + b = 0$ in C_3. In general, it is easier to show that elements are zero than to show they are not zero.

Another interesting property of tensor products is that if $f : A \to B$ is a surjection, then so is the induced map $g : A \otimes C \to B \otimes C$ for any other module C. But if $f : A \to B$ is injective, then $g : A \otimes C \to B \otimes C$ may not be injective.

For example, $f : C_2 \to C_4$, with $f\,(1) = 2$ is injective, but $g : C_2 \otimes_Z C_2 \to C_4 \otimes_Z C_2$, with $g\,(1 \otimes 1) = 2 \otimes 1$, is not injective. In $C_4 \otimes_Z C_2$, we have $2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$.

There is an algebraic description of this failure of injectivity, called the tor module.

Another way to think of the tensor product is in terms of its universal property: Any bilinear map from $A \times B : \to C$ factors through the natural bilinear map $A \times B \to A \otimes B$

The vector space tensor product $V \otimes W$ of two group representations of a group G is also a representation of G. An element g of G acts on a basis element $v \otimes w$ by

$$g\,(v \otimes w) = g\,v \otimes g\,w.$$

If G is a finite group and V is a faithful representation, then any representation is contained in $\otimes^n V$ for some n. If V_1 is a representation of G_1 and V_2 is a representation of G_2, then $V_1 \otimes V_2$ is a representation of $G_1 \times G_2$, called the external tensor product. The regular tensor product is a special case, with the diagonal embedding of G in $G \times G$.

12.2 VECTOR SPACE TENSOR PRODUCT

The tensor product of two vector spaces V and W, denoted $V \otimes W$ and also called the tensor direct product, is a way of creating a new vector space analogous to multiplication of integers. For instance,

$$\mathbb{R}^n \otimes \mathbb{R}^k \cong \mathbb{R}^{n\,k}. \tag{1}$$

In particular,

$$\mathbf{r} \otimes \mathbb{R}^n \cong \mathbb{R}^n. \tag{2}$$

Also, the tensor product obeys a distributive law with the direct sum operation:

$$U \otimes (V \oplus W) \cong (U \otimes V) \oplus (U \otimes W). \tag{3}$$

The analogy with an algebra is the motivation behind K-theory. The tensor product of two tensors a and b can be implemented in the Wolfram Language as:

TensorProduct[a_List, b_List] := Outer[List, a, b]

Algebraically, the vector space v is spanned by elements of the form , and the following rules are satisfied, for any scalar α. The definition is the same no matter which scalar field is used.

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w \qquad (4)$$

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2 \qquad (5)$$

$$\alpha (v \otimes w) = (\alpha v) \otimes w = v \otimes (\alpha w) \qquad (6)$$

One basic consequence of these formulas is that

$$0 \otimes w = v \otimes 0 = 0. \qquad (7)$$

A vector basis v_i of V and w_j of W gives a basis for $V \otimes W$, namely $v_i \otimes w_j$, for all pairs (i, j). An arbitrary element of $V \otimes W$ can be written uniquely as $\sum a_{i,j} \, v_i \otimes w_j$, where $a_{i,j}$ are scalars. If V is n dimensional and W is k dimensional, then $V \otimes W$ has dimension $n\,k$.

Using tensor products, one can define symmetric tensors, antisymmetric tensors, as well as the exterior algebra. Moreover, the tensor product is generalized to the vector bundle tensor product. In particular, tensor products of the tangent bundle and its dual bundle are studied in Riemannian geometry and physics. Sections of these bundles are often called tensors. In addition, it is possible to take the representation tensor product to get another representation.

All of these versions of tensor product can be understood as module tensor products. The trick is to find the right way to think of these spaces as modules.

Theorem . In M *R N, m *0 = 0 and 0 * n = 0.

Proof. This is just like the proof that a · 0 = 0 in a ring: since m*n is additive in n with m fixed, m * 0 = m * (0 + 0) = m * 0 + m *0. Subtracting m * 0 from both sides, m * 0 = 0. That 0 * n = 0 follows by a similar argument.

Example . If A is a finite abelian group, Q *Z A = 0 since every elementary tensor is 0: for a * A, let na = 0 for some positive integer n. Then in Q * Z A, r * a = n(r/n) * a = r/n* na = r/n*0 = 0. Every tensor is a sum of elementary tensors, and every elementary tensor is 0, so all tensors are 0. (For instance, (1/3) * (5 mod 7) = 0 in Q * Z Z/7Z. Thus we can have m * n = 0 without m or n being 0.) To show Q*Z A = 0, we don't need A to be finite, but rather that each element of A has finite order. The group Q/Z has that property, so Q* Z (Q/Z) = 0. By a similar argument, Q/Z *Z Q/Z = 0.

Since M * R N is spanned additively by elementary tensors, each linear (or just additive) function out of M * R N is determined on all tensors from its values on elementary tensors. This is why linear maps on tensor products are in practice described only by their values on elementary tensors. It is similar to describing a linear map between finite free modules using a matrix. The matrix directly tells you only the values of the map on a particular basis, but this information is enough to determine the linear map everywhere.

However, there is a key difference between basis vectors and elementary tensors: elementary tensors have lots of linear relations. A linear map out of R2 is determined by its values on (1, 0), (2, 3), (8, 4), and (−1, 5), but those values are not independent: they have to satisfy every linear relation the four vectors satisfy because a linear map preserves linear relations. Similarly, a random function on elementary tensors generally does not extend to a linear map on the tensor product: elementary tensors span the tensor product of two modules, but they are not linearly independent.

Functions of elementary tensors can't be created out of a random function of two variables. For instance, the "function" f(m * n) = m + n makes no sense since m ⊗ n = (−m) ⊗ (−n) but m + n is usually not −m

− n. The only way to create linear maps out of M ⊗R N is with the universal mapping property of the tensor product (which creates linear maps out of bilinear maps), because all linear relations among elementary tensors – from the obvious to the obscure – are built into the universal mapping property of M * R N.. Understanding how the universal mapping property of the tensor product can be used to compute examples and to prove properties of the tensor product is the best way to get used to the tensor product; if you can't write down functions out of M *R N, you don't understand M *R N.

The tensor product can be extended to allow more than two factors. Given k modules M1, . . . , Mk, there is a module M1 * R · · · * R Mk that is universal for k-multilinear maps: it admits a k-multilinear map M1 × · · · × Mk ⊗−−→ M1 ⊗R · · · ⊗R Mk and every k-multilinear map out of M1 × · · · × Mk factors through this by composition with a unique linear map out of M1 * R · · · * R Mk:

Check In Progress – II

Note: i) Write your answers in the space given below.

Questions

(1) What is m * n?

(2) What does it mean to say m * n = 0?

(3) What does it mean to say M *R, N = 0?

(4) What does it mean to say m1 * n1 + · · · + mk * nk = m0 1 * n 0 1 + · · · + m0 ` * n 0 ` ?

(5) Where do tensor products arise outside of mathematics?

(6) Is there a way to picture the tensor product?

Answers:

(1) Strictly speaking, m*n is the image of (m, n) ∈ M ×N under the canonical bilinear map M × N ⊗−−→ M ⊗R N in the definition of the tensor product. Here's

another answer, which is not a definition but more closely aligns with how m * n occurs in practice: m ⊗ n is that element of M * R N at which the linear map M ⊗R N → P corresponding to a bilinear map M × N B −−→ P takes the value B(m, n).

(2) We have m * n = 0 if and only if every bilinear map out of M × N vanishes at (m, n). Indeed, if m * n = 0 then for each bilinear map B : M × N → P for some linear map L, so B(m, n) = L(m * n) = L(0) = 0. Conversely, if every bilinear map out of M × N sends (m, n) to 0 then the canonical bilinear map M × N → M ⊗R N, which is a particular example, sends (m, n) to 0. Since this bilinear map actually sends (m, n) to m * n, we obtain m * n = 0.

A very important consequence is a tip about how to show a particular elementary tensor m * n is not 0: find a bilinear map B out of M × N such that B(m, n) 6= 0.

(3) The tensor product M *R N is 0 if and only if every bilinear map out of M × N (to all modules) is identically 0. First suppose M *R N = 0. Then all elementary tensors m* n are 0, so B(m, n) = 0 for all bilinear maps out of M ×N by the answer to the second question. Thus B is identically 0. Next suppose every bilinear map out of M ×N is identically 0. Then the canonical bilinear map M ×N ⊗−−→ M ⊗RN, which is a particular example, is identically 0. Since this function sends (m, n) to m * n, we have m * n = 0 for all m and n. Since M *R N is additively spanned by all m * n, the vanishing of all elementary tensors implies M *R N = 0.

So, that Q *Z A = 0 if each element of A has finite order is another way of saying every Z-bilinear map out of Q×A is identically zero, which can be verified directly: if B is such a map (into an abelian group) and na = 0 with n ≥ 1, then B(r, a) = B(n(r/n), a) = B(r/n, na) = B(r/n, 0) = 0.

Turning this idea around, to show some tensor product module M *R N is not 0, find a bilinear map on M × N that is not identically 0.

(4) We have Pk i=1 mi * ni = P` j=1 m0 j * n 0 j if and only if for all bilinear maps B out of M × N, Pk i=1 B(mi , ni) = P` j=1 B(m0 j , n0 j). The justification is along the lines of the previous two answers and is left to the reader. For example, the condition Pk i=1 mi * ni = 0 means Pk i=1 B(mi , ni) = 0 for all bilinear maps B on M × N

(5) Tensors are used in physics and engineering (stress, elasticity, electromagnetism, metrics, diffusion MRI), where they transform in a multilinear way under a change in coordinates.

(6) There isn't a simple picture of a tensor (even an elementary tensor) analogous to how a vector is an arrow. Some physical manifestations of tensors are in the previous answer, but they won't help you understand tensor products of modules.

Theorem . For positive integers a and b with d = (a, b), Z/aZ *Z Z/bZ *= Z/dZ as abelian groups. In particular, Z/aZ *Z Z/bZ = 0 if and only if (a, b) = 1.

Proof. Since 1 spans Z/aZ and Z/bZ, 1 * 1 spans Z/aZ *Z Z/bZ then

a(1 * 1) = a * 1 = 0 * 1 = 0 and b(1 * 1) = 1 * b = 1 * 0 = 0,

the additive order of 1 * 1 divides a and b, and therefore also d, so #(Z/aZ * Z Z/bZ) ≤ d.

To show Z/aZ * Z Z/bZ has size at least d, we create a Z-linear map from Z/aZ * Z Z/bZ onto Z/dZ. Since d|a and d|b, we can reduce Z/aZ → Z/dZ and Z/bZ → Z/dZ in the natural way. Consider the map Z/aZ × Z/bZ B −−→ Z/dZ that is reduction mod d in each factor followed by multiplication: B(x mod a, y mod b) = xy mod d. This is Z-bilinear, so the universal mapping property of the tensor product says there is a (unique) Z-linear map f : Z/aZ ⊗Z Z/bZ → Z/dZ commute, so f(x⊗y) = xy. In particular, f(x⊗1) = x, so f is onto. Therefore Z/aZ has size at least d, so the size is d and we're done.

Example . The abelian group Z/3Z Z Z/5Z is 0. This type of collapsing in a tensor product often bothers people when they first see it, but it's saying something pretty concrete: each Z-bilinear map B : Z/3Z × Z/5Z → A to an abelian group A is identically 0, which is easy to show directly: 3B(a, b) = B(3a, b) = B(0, b) = 0 and 5B(a, b) = B(a, 5b) = B(a, 0) = 0, so B(a, b) is killed by 3Z + 5Z = Z, hence B(a, b) is killed by 1, which is another way of saying B(a, b) = 0.

In Z/aZ * Z Z/bZ all tensors are elementary tensors: x * y = xy(1 * 1) and a sum of multiples of 1 * 1 is again a multiple, so Z/aZ * Z Z/bZ = Z(1 * 1) = {x * 1 : x * Z}. How the map f : Z/aZ ⊗Z Z/bZ → Z/dZ was created from the bilinear map B : Z/aZ × Z/bZ → Z/dZ and the universal mapping property of tensor products. Quite generally, to define a linear map out of M * R N that sends all elementary tensors m* n to particular places, always back up and start by defining a bilinear map out of M × N sending (m, n) to the place you want m * n to go. Make sure you show the map is bilinear! Then the universal mapping property of the tensor product gives you a linear map out of M * R N sending m * n to the place where (m, n) goes, which gives you what you wanted: a (unique) linear map on the tensor product with specified values on the elementary tensors.

Remark . For ideals I and J, a few operations produce new ideals: I + J, I ∩ J, and IJ. The intersection I ∩ J is the kernel of the linear map R → R/I ⊕ R/J where r 7→ (r, r). So, s I + J is the kernel of the linear map R → R/I ⊗R R/J where r 7→ r(1 ⊗ 1).

Theorem . There is a unique R-module isomorphism

M *R (N * P) = (M *R N) ((M *R P)

where m ⊗ (n, p) 7→ (m ⊗ n, m ⊗ p).

Proof. Instead of directly writing down an isomorphism, we will put to work the essential uniqueness of solutions to a universal mapping problem by showing (M xR N) x (M xR P) has the universal mapping property of the tensor product M xR (N x P). Therefore by abstract nonsense these modules must be isomorphic. That there is an isomorphism whose effect on elementary tensors in M *R (N xP) is as indicated in the statement of the theorem will fall out of our work.

For (M xRN)x(MxR P) to be a tensor product of M and N xP, it needs a bilinear map to it from $M \times (N \oplus P)$. Let $b : M \times (N \oplus P) \to (M \otimes R\ N) \oplus (M \otimes R\ P)$ by $b(m,(n, p)) = (m \otimes n, m \otimes p)$. This function is bilinear. We verify the additivity of b in its second component, leaving the rest to the reader:

$$b(m,(n, p) + (n\ 0 , p0)) = b(m,(n + n\ 0 , p + p\ 0))$$

$$= (m* (n + n *), m * (p + p\ 0))$$

$$= (m* n + m * n\ 0 , m * p + m * p\ 0)$$

$$= (m * n, m * p) + (m * n\ 0 , m * p\ 0)$$

$$= b(m,(n, p)) + b(m,(n\ 0 , p0)).$$

To show (M*RN)*(M*RP) and b have the universal mapping property of M*R(N *P) and $\otimes$, let $B : M \times (N \oplus P) \to Q$ be a bilinear map. We seek an R-linear map L making commute. Being linear, L would be determined by its values on the direct summands, and these values would be determined by the values of L on all pairs (m * n, 0) and (0, m * p) by additivity.

$$L(m*n, 0) = L(b(m,(n, 0))) = B(m,(n, 0)) \text{ and } L(0, m*p) = L(b(m,(0, p))) = B(m,(0, p)).$$

To construct L, the above formulas suggest the maps $M \times N \to Q$ and $M \times P \to Q$ given by $(m, n)\ 7\!\to B(m,(n, 0))$ and $(m, p)\ 7\!\to B(m,(0, p))$. Both are bilinear, so there are R-linear maps $M \otimes R\ N\ L1 \longrightarrow Q$ and $M \otimes R\ P\ L2 \longrightarrow Q$ where

$$L1(m * n) = B(m,(n, 0)) \text{ and } L2(m * p) = B(m,(0, p)).$$

Notes

Define L on (M *R N) * (M *R P) by L(t1, t2) = L1(t1) + L2(t2). (Notice we are defining L not just on ordered pairs of elementary tensors, but on all pairs of tensors. We need L1 and L2 to be defined on the whole tensor product modules M *R N and M *R P.) The map L is linear since L1 and L2 are linear,

L(b(m,(n, p))) = L(b(m,(n, 0) + (0, p)))

= L(b(m,(n, 0)) + b(m,(0, p)))

= L((m * n, 0) + (0, m* p)) by the definition of b

= L(m * n, m * p)

= L1(m * n) + L2(m * p) by the definition of L

= B(m,(n, 0)) + B(m,(0, p))

= B(m,(n, 0) + (0, p))

= B(m,(n, p)).

Now that we've shown (M *R N) * (M *R P) and the bilinear map b have the universal mapping property of M *R (N * P) and the canonical bilinear map *, there is a unique linear map f making the diagram

commute, and f is an isomorphism of R-modules because it transforms one solution of a universal mapping problem into another. Taking (m,(n, p)) around the diagram both ways,

$$f(b(m,(n, p))) = f(m * n, m * p) = m * (n, p).$$

Therefore the inverse of f is an isomorphism M ⊗R (N ⊕ P) → (M ⊗R N) ⊕ (M ⊗R P) with the effect m ⊗ (n, p) 7→ (m ⊗ n, m ⊗ p). We look at the inverse because the theorem is saying something about an isomorphism out of M *R (N *P), which is the target of f.

12.3 SUMMARY

We study in this unit Tensor Product on Module. We study Z-Bilinear and Canonical Module and its properties. We study Additional structure of Tensor Product. We study Z-Module.We study vector space tensor product and its example. We study of the property of the tensor product and its some important examples. We study R-balance , R-balance linear module and its definition with examples.

1. Linear and Bilinear Maps: Let M and N be R-modules. A map φ : M → N is R-linear (or just linear for short) provided that
   a. φ(rv) = rφ(v).
   b. φ(v1 + v2) = φ(v1) + φ(v2).
2. Suppose that M′ ⊂ M and N′ ⊂ N are submodules. Then there is an injective linear map from M′ ⊗ N′ into M ⊗ N. This map is the identity on elements of the form a ⊗ b, where a ∈ M′ and b ∈ N′.
3. In M *R N, m *0 = 0 and 0 * n = 0
4. For positive integers a and b with d = (a, b), Z/aZ *Z Z/bZ *= Z/dZ as abelian groups. In particular, Z/aZ *Z Z/bZ = 0 if and only if (a, b) = 1

12.4 KEYWORD

Tensor : A mathematical object analogous to but more general than a vector, represented by an array of components that are functions of the coordinates of a space

Z-Bilinear : The bilinear transformation is a mathematical mapping of variables. In digital filtering, it is a standard method of mapping the s or analog plane into the z or digital plane. It transforms analog filters, designed using classical filter design techniques, into their discrete equivalents

Canonical : Included in the list of sacred books officially accepted as genuine

12.5 QUESTIONS FOR REVIEW

Q. 1 Let {mα : α * A} be a set of generators for an R-module M, and {nβ : β * B} a set of generators for an R-module N. Then

$$\{m\alpha * n\beta : \alpha * A, \beta * B\}$$

is a set of generators[8] for M *R N.

Q. 2 Tensor products M * R N exist.

Q. 3 Tensor products M * R N are unique up to unique isomorphism. That is, given two tensor products $\tau 1 : M \times N \longrightarrow T1$ $\tau 2 : M \times N \longrightarrow T2$ there is a unique isomorphism $i : T1 \longrightarrow T2$. Then commutes, that is, $\tau 2 = i \circ \tau 1$.

Q. 4 The monomial tensors m * n (for m * M and n * N) generate M *R N as an R-module.

Q. 5 Consider the Z-modules Z/2 and Z/3. We claim that Z/2*ZZ/3 = 0. Equivalently, any map $f : Z/2 \times Z/3 \to M$ to a Z-module M must be the zero map. One may see this by taking any such f and considering for any x * Z/2, y * Z/3,

$$f(x, y) = 3f(x, y) - 2f(x, y) = f(x, 3y) - f(2x, y) = f(x, 0) - f(0, y) = 0.$$

Q. 6 For fixed a, b * Z, consider the Z-modules Z/a and Z/b. Then, Z/a *Z Z/b = Z/gcd(a, b).

12.6 SUGGESTION READING AND REFERENCES

- Bourbaki, Algebra
- Helgason, Sigurdur (1978), Differential geometry, Lie groups and symmetric spaces, Academic Press, ISBN 0-12-338460-5
- Northcott, D.G. (1984), Multilinear Algebra, Cambridge University Press, ISBN 613-0-04808-4.
- Hazewinkel, Michiel; Gubareni, Nadezhda Mikhaĭlovna; Gubareni, Nadiya; Kirichenko, Vladimir V. (2004), Algebras, rings and modules, Springer, ISBN 978-1-4020-2690-4.
- Peter May (1999), A concise course in algebraic topology, University of Chicago Press.

12.7 ANSWER TO CHECK YOUR PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 1.2

Q 2 Check in Section 1.1

Check in Progress-II

Answer check in section 2 all solution given.

UNIT 13 - CHAIN CONDITIONS ON MODULE

STRUCTURE

13.0 OBJECTIVE

After study this unit we are able to know that A satisfies pan-acc if and only if A satisfies the following conditions:

(i) A is reduced,

(ii) there exists only a finite number of primes p in Z such that pa = 0 for some non-zero element a in A, and

(iii) every countably generated torsion-free submodule of A is free.

In particular, if A is a torsion Z-module then A satisfies pan-acc if and only if A satisfies 1-acc. The situation for torsion-free Z-modules is quite different. Let A be a Z-module. Given a prime p in Z, we shall say that A is a p-module if for each $a \in A$ there exists a positive integer n such that p na = 0. Note the following simple fact which may be well known but which we include for convenience. Recall that a Z-module A is called reduced provided A does not contain a non-zero divisible submodule.

13.1 INTRODUCTION

All rings have identity elements and all modules are unital right modules, unless stated otherwise. Let R be a ring and let M be an R-module. Given a positive integer n, the module M satisfies n-acc provided every ascending chain of n-generated submodules terminates. Moreover, the module M satisfies pan-acc in case M satisfies n-acc for every positive integer n. In particular, R-module satisfies pan-acc. He also gave an example of a right Noetherian ring R such that every free right R-module of infinite rank does not satisfy .Renault's paper was the inspiration for this present work. proved that if R is a commutative Noetherian ring then every direct product RI of copies of the R-module R indexed by a set I is an R-module satisfying pan-acc, for every such index set I.

The purpose of this note is to show that if R is a right and left Noetherian ring then the right (or left) R-module RI satisfies pan-acc, thus generalizing the theorems of both Renault and Frohn. In fact, we shall prove rather more, namely that if S and R are rings and M a left S-, right R-bimodule such that M is Noetherian both as a left S-module and as a right R-module then the right Rmodule MI satisfies pan-acc and the left S-module MI satisfies pan-acc, for every index set I. Note R is a ring with finite right uniform dimension then any direct productof nonsingular Noetherian right R-modules satisfies pan-acc. In particular, if R is a right nonsingular right Noetherian ring then the right R-module RI satisfies pan-acc, for every index set I.

It might be worth reminding ourselves of what happens for Abelian groups. Let Z denote the ring of integers. Pontrjagin proved that a countably generated torsionfree Z-module A satisfies pan-ac Z-module.

Some Important Theorem

Lemma 1. Let p be any prime in Z and let a Z-module A be a p-module. Then every homomorphic image of A satisfies pan-acc if and only if there exists a positive integer k such that p kA = 0.

Proof. The sufficiency follows by [4, Theorem 3] because every homomorphic image of A is clearly reduced if $p^kA = 0$ for some k. Conversely, suppose that every homomorphic image of A satisfies pan-acc. Suppose that there does not exist a positive integer k such that $p^kA = 0$. By [8, Vol I Theorem 32.3] there exists a submodule B of A such that B is a direct sum of cyclic submodules and A/B is divisible. Thus A = B and A is a direct sum of cyclic submodules. There exists a submodule C of A such that $C = \bigoplus_{i\geq 1} Zc_i$, where c_i is an element of A of order p^i for every positive integer i.

Let $D = Z(c_1 - pc_2) \oplus Z(c_2 - pc_3) \oplus \ldots$

Then $C \neq D$ and C/D is a non-zero divisible submodule of A/D so that A has a nonzero divisible homomorphic image, a contradiction. Thus $p^kA = 0$ for some positive integer k.

Our first theorem is a consequence of the above theorem of Baumslag and Baumslag.

Theorem 2. Let Z denote the ring of integers and let A be a Z-module. Then every homomorphic image of A is a Z-module satisfying pan-acc if and only if $A = F \oplus T$ for some finitely generated free submodule F of A and some submodule T of A such that $nT = 0$ for some positive integer n.

Proof. (⇒) Note first that gives that A/B is reduced for every submodule B of A. Let T denote the torsion submodule of A. Then A/T is a torsion free Z-module satisfying pan-acc. Suppose that A/T is not finitely generated. Then there exists a submodule C of A, containing T, such that C/T is countably, but not finitely, generated., C/T is free and hence the Z-module Q is a homomorphic image of C/T. This implies that Q is a homomorphic image of A, a contradiction. Thus A/T is finitely generated and hence $A = T \oplus F$ for some finitely generated free submodule F of A. Now suppose that T is non-zero. Again using there exist finitely many distinct primes p_i ($1 \leq i \leq t$) in Z, for some positive integer t, such that $T = T(p_1) \oplus \cdots \oplus T(p_t)$, where $T(p_i)$ is the p_i-primary component of T, for each $1 \leq i \leq t$. By Lemma 1, for each $1 \leq i \leq t$ there exists a positive integer k_i such that $p_i^{k_i}T(p_i) = 0$. Let $n = p_1^{k_1} \ldots p_t^{k_t}$. Then $nT = 0$.

(⇐) Now suppose that A = F ⊕T where F is a finitely generated free submodule and T is a torsion submodule such that nT = 0 for some non-zero n in Z. Let D be any proper submodule of A. Let E be the submodule of A containing D such that E/D is the torsion submodule of A/D. Note that D +T ⊆ E. In particular, T ⊆ E so that A/E is finitely generated torsion-free and hence free. Moreover E/(D + T) is also finitely generated, so that mE⊆ D + T for some positive integer m. Thus mnE⊆ D. it follows that A/D satisfies pan-acc.

We chose to prove Theorem 2 to point out that if A is a Z-module such that every homomorphic image of A satisfies pan-acc then A is a direct sum of cyclic submodules . In view of this fact and Pontrjagin's Theorem above it would appear that there is some relationship between direct sum decompositions and the property pan-acc. Now in order to prove the above results of Renault and Frohn we shall look at modules satisfying a particular property which can be stated in terms of direct sum decompositions.

Let R be a ring. An R-module M will be said to satisfy the direct sum condition provided every countably generated submodule is contained in a direct sum of finitely generated submodules of M. Clearly every free module and every semisimple module satisfies the direct sum condition. More generally, every direct sum of finitely generated R-modules satisfies the direct sum condition. Note also that if M_i is an R-module satisfying the direct sum condition, for all i in some index set I, then the R-module $\bigoplus_{i\in I} M_i$ also satisfies the direct sum condition. For, let N be any countably generated submodule of the module $M = \bigoplus_{i\in I} M_i$. For each $i\in I$, let $\pi_i : M \to M_i$ denote the canonical projection. Because, for each $i\in I$, $\pi_i(N)$ is a countably generated submodule of M_i , there exists a submodule K_i of M_i such that K_i is a direct sum of finitely generated submodules and $\pi_i(N) \subseteq K_i$. Let $K = \bigoplus_{i\in I} K_i$. Then N is contained in the submodule K of M and K is a direct sum of finitely generated submodules.

We want to show that certain direct products satisfy the direct sum condition, in particular modules of the form M^I , the direct product of copies of a module M indexed by a set I. If J is a non-empty subset of I then MJ will be considered a submodule of MI in the natural way. If R and S are rings and M a left S-, right R-bimodule then MI is a left S-, right R-bimodule in the natural way. We first note the following simple fact.

Lemma 3. Let R be a ring and let L be a countably generated submodule of an R-module M. Then the following statements are equivalent.

(i) L is contained in a direct sum of finitely generated submodules of M.

(ii) There exists a submodule K of M containing L such that every finitely generated submodule of L is contained in a finitely generated direct summand of K.

Proof. (i) ⇒ (ii). Let Mi (i∈ I) be a collection of finitely generated submodules of M such that L ⊆⊕i∈IMi . Then K = ⊕i∈IMi satisfies (ii).

(ii) ⇒ (i). Let L = x1R + x2R + ... By hypothesis there exist submodules E1 and F1 of K such that K = E1 ⊕F1, E1 is finitely generated and x1R ⊆ E1. Again, by hypothesis, there exist submodules E2 and F2 of K such that K = E2 ⊕F2, E2 is finitely generated and E1 + x2R ⊆ E2. Note that x1R + x2R ⊆ E2 = E1 ⊕(E2 ∩ F1). Repeat this argument. For each positive integer n ≥ 2, there exist submodules En and Fn of K such that K = En⊕Fn, En is finitely generated and contains x1R + · · · + xnR. Note that En = E1 ⊕(E2 ∩ F1) ⊕. . .(En ∩ Fn−1). It follows that L is contained in the direct sum E1 ⊕(E2 ∩ F1) ⊕(E3 ∩ F2). . . , which is a direct sum of finitely generated submodules because En is a finitely generated submodule for each positive integer n.

Lemma 4. Let R and S be rings and let M be a left S-, right R-bimodule such that the left S-module M is Noetherian. Let I denote an index set and X the left S-, right R-bimodule MI . Then, for each finitely generated submodule F of the right R-module X, there exist a finite subset J of I and an R-isomorphism φ : X → X such that φ(F) ⊆ MJ .

Proof. Let F be any finitely generated submodule of the right R-module X. Then there exist a positive integer k and elements xi ∈ F (1 ≤ i ≤ k) such that $F = x_1R + \cdots + x_kR$. Let $x = x_1$. There exist elements $m_i \in M$ ($i \in I$) such that $x = (m_i)$. The S-submodule $\sum_{i\in I} Sm_i$ is finitely generated and hence there exists a finite subset J_1 of I such that $\sum_{i\in I} Sm_i = \sum_{j\in J_1} Sm_j$. For each i in I there exist elements $s_{ij} \in S$ ($j \in J_1$) such that $m_i = \sum_{j\in J_1} s_{ij}m_j$. Define a mapping $\varphi_1 : X \to X$ as follows: for each element (u_i) in X, $\varphi_1(u_i) = (v_i)$ where $v_i = u_i$ if $i \in J_1$ and $v_i = u_i - \sum_{j\in J_1} s_{ij}u_j$ if $i \in I \setminus J_1$. It is not difficult to check that φ_1 is an R-isomorphism from X to X and that $\varphi_1(x) \in M^{J_1}$.

Let $I_1 = I \setminus J_1$, let $X_1 = M^{J_1}$ and let $X_2 = M^{I_1}$ so that $X = X_1 \oplus X_2$. For each $2 \leq i \leq k$ there exist elements $y_i \in X_1$ and $z_i \in X_2$ such that $\varphi_1(x_i) = y_i + z_i$. By induction on k there exists a finite subset J_2 of I_1 and an R-isomorphism $\varphi_2 : X_2 \to X_2$ such that $\varphi_2(z_2R + \cdots + z_kR) \subseteq M^{J_2}$. Now $\varphi_3 = \iota + \varphi_2$ is an R-isomorphism from X to X where ι is the identity mapping on X_1. Finally note that $\varphi = \varphi_3\varphi_1$ is an R-isomorphism from X to X such that $\varphi(F) \subseteq M^J$ where J is the finite subset $J_1 \cup J_2$ of I

Theorem 5. Let R and S be rings and let M be a left S-, right R-bimodule such that the left S-module M is Noetherian and the right R-module M is finitely generated. Then the right R-module M^I satisfies the direct sum condition for every index set I.

Proof. Let F be any finitely generated submodule of the right R-module $X = M^I$. By Lemma 4 there exist a finite subset J of I and an R-isomorphism $\varphi : X \to X$ such that $\varphi(F) \subseteq M^J$. Let $J' = I \setminus J$, let $X_1 = \varphi^{-1}(M^J)$ and let $X_2 = \varphi^{-1}(M^{J'})$. Then the right R-module $X = X_1 \oplus X_2$ is a direct sum of the submodules X_1 and X_2, X_1 is a finitely generated right R-module and $F \subseteq X_1$. By Lemma 3 X satisfies the direct sum condition

Next we give an example of a module M which satisfies the direct sum condition but which is not itself a direct sum of finitely generated submodules.

Example 6. Let Z denote the ring of integers and let M denote the direct product Z^I for any infinite index set I. Then the Z-module M satisfies the direct sum condition but M is not a direct sum of finitely generated submodules.

Proof. By Theorem 5 the Z-module M satisfies the direct sum condition. However M is not a direct sum of finitely generated submodules because M is not projective.

Let R be a ring and let M be a non-zero module. Then M has finite uniform dimension provided M does not contain an infinite direct sum of non-zero submodules. In this case there exists a positive integer n such that n is the maximum number of submodules of M which form a direct sum. The integer n is called the uniform dimension of M and is denoted by u(M). In case M = 0 we say that M is zero dimensional and write u(M) = 0. The ring R has finite right uniform dimension in case the right R-module R has finite uniform dimension Note that every Noetherian module has finite uniform dimension. The next two results concern rings with finite right uniform dimension.

Lemma 7. Let R be a ring with finite right uniform dimension, let n be a positive integer and let M be a nonsingular n-generated R-module. Then M has finite uniform dimension and $u(M) \leq nu(R)$.

Proof. There exists an epimorphism from F = R(n) to M with kernel K. Because M is nonsingular, K is an essentially closed submodule of F and hence $u(M) = u(F/K) \leq u(F) = nu(R)$

Let R be a ring and let M be any R-module. Then the singular submodule Z(M) of M is defined to be the set of elements m in M such that mE = 0 for some essential right ideal E of R. The second singular submodule of M is the submodule Z2(M) of M containing Z(M) such that Z2(M)/Z(M) is the singular submodule of the module M/Z(M). In the Goldie torsion theory, a module M is torsion if M = Z2(M) and is torsion-free if it is nonsingular, i.e. Z(M) = 0 (see [15] for more details).

Let R be a ring and let M be an R-module such that MA = 0 for some ideal A of R. Then M is both an R-module and an (R/A)-module. The singular submodule of the R-module M need not coincide with the singular submodule of the (R/A)-module M and we shall denote these submodules by Z(MR) and Z(MR/A), respectively. Similarly we denote by Z2(MR) and Z2(MR/A) the second singular submodules of M considered as an R-module and as an (R/A)-module, respectively. When there is no ambiguity we shall use Z(M) and Z2(M), as indicated above. We want to make one further observation at this point, namely if R is a prime (or even semiprime) right Noetherian ring then Z2(M) = Z(M) for every R-module M.

Given a ring R and an R-module M, if N is a submodule of M then Zorn's Lemma gives a submodule K of M maximal among the submodules H of M such that $N \cap H = 0$. In this case, K is called a complement of N (in M). Note that K is essentially closed in M in the sense of [9]. The next result is crucial for the remainder of this paper.

Theorem 8. Let R be a right Noetherian ring, let M be a right R-module which satisfies the direct sum condition and let n be a positive integer. Then M satisfies n-acc if and only if Z2(M) satisfies n-acc.

Proof. The necessity is clear. Conversely, suppose that Z2(M) satisfies n-acc. Let $L1 \subseteq L2 \subseteq L3 \subseteq \ldots$ be any ascending chain of n-generated submodules of M. Let $L = \cup_{i\geq 1} Li$. Let K be a complement of Z2(L) in L. Note that for all $i \geq 1$, Li/Z2(Li) is an n-generated nonsingular module and hence $u(Li/Z2(Li)) \leq nu(R)$ by Lemma 7. Moreover note that for all $i \geq 1$, $Li \cap K$ embeds in Li/Z2(Li) so that $u(Li \cap K) \leq nu(R)$. Now the ascending chain $L1 \cap K \subseteq L2 \cap K \subseteq \ldots$ gives that $Li \cap K$ is essential in $Li+1 \cap K$ for all $i \geq k$, for some positive integer k, and hence $Lk \cap K$ is essential in K. By hypothesis, there exists a submodule H of M such that $L \subseteq H$, $H = H1 \oplus H2$ for some submodules H1 and H2, H1 is finitely generated and $Lk \subseteq H1$. Let $\pi : H \to H2$ denote the canonical projection. Let $x \in L$. Because $Z2(L) \oplus K$ is essential in L, we have (xR + K)/K is Goldie torsion and hence so too is $[xR + (Lk \cap K)]/(Lk \cap K)$. It follows that π(xR) is Goldie torsion. Thus $\pi(L1) \subseteq \pi(L2) \subseteq \ldots$ is an ascending chain of n-generated submodules of Z2(M). There exists a positive integer t such that $\pi(Lt) = \pi(Lt+1) = \ldots$. But H1 is Noetherian and hence, without loss of generality, $Lt \cap H1 = Lt+1 \cap H1 = \ldots$. It follows that $Lt = Lt+1 = \ldots$, as required.

Corollary 9. Let R be a right Noetherian ring and let M be a nonsingular right R-module which satisfies the direct sum condition. Then M satisfies pan-acc.

Proof. By the theorem.

Lemma 10. Let R be a right Noetherian ring and let M be a right R-module which satisfies the direct sum condition but does not satisfy pan-acc. Let P be an ideal of R which is maximal in the collection of ideals A of R such that there exist a positive integer k and a properly ascending chain $H1 \subseteq H2 \subseteq H3 \ldots$ of k-generated submodules Hi $(i \geq 1)$ of M with $HiA = 0$ for all $i \geq 1$. Then P is a prime ideal of R.

Proof. There exist a positive integer n and a properly ascending chain $L1 \subseteq L2 \subseteq L3 \subseteq \ldots$ of n-generated submodules Li $(i \geq 1)$ such that $LiP = 0$ for all $i \geq 1$. Suppose that P is not a prime ideal of R. Then there exist ideals A and B of R, each properly containing P, such that $AB \subseteq P$. Note that A is a q-generated right ideal of R, for some positive integer q, and hence LiA is an nq-generated submodule of M for each $i \geq 1$. By the choice of P, the ascending chain $L1A \subseteq L2A \subseteq \ldots$ must terminate and hence there exists a positive integer s such that $LsA = Ls+1A = Ls+2A = \ldots$. Let L denote the countably generated submodule $\cup_{i\geq 1} Li$. By hypothesis there exists a submodule K of M such that $L \subseteq K$, $K = K1 \oplus K2$ for some submodules K1 and K2, K1 is finitely generated and $Ls \subseteq K1$. Let $\pi : K \rightarrow K2$ denote the canonical projection. Note that $\ker \pi = K1$ which is a Noetherian module. Moreover, for each $i \geq s$, $\pi(Li)$ is an n-generated submodule of M such that $\pi(Li)A \subseteq \pi(Ls) = 0$. By the choice of P, there exists an integer $t \geq s$ such that $\pi(Lt) = \pi(Lt+1) = \ldots$. But K1 is Noetherian so that without loss of generality we can suppose that $Lt \cap K1 = Lt+1 \cap K1 = \ldots$. It follows that $Lt = Lt+1 = \ldots$, a contradiction. Thus P is a prime ideal of R.

Lemma 11. Let R be a commutative Noetherian ring and let M be an R-module which satisfies the direct sum condition but does not satisfy n-acc for some positive integer n. Let P be an ideal of R which is maximal in the collection of ideals A of R such that there exists a properly ascending chain $H1 \subseteq H2 \subseteq H3 \subseteq \ldots$ of n-generated submodules Hi $(i \geq 1)$ of M with $HiA = 0$ for all $i \geq 1$. Then P is a prime ideal of R.

Proof. We adapt the proof of Lemma 10. In this case we can replace the ideals A and B by elements a and b. Note that Lia is an n-generated submodule of M for each $i \geq 1$ and the proof proceeds as before.

Let R be a ring and let M be an R-module. Given a non-empty set W in M, the annihilator of W in R will be denoted by ann(W), i.e. ann(W) is the set of

elements r in R such that wr = 0 for all $w \in W$. Note that ann(W) is a right ideal of R and in case W is a submodule of M then ann(W) is an ideal of R.

Theorem 12. Let R be a commutative Noetherian ring, let M be an R-module which satisfies the direct sum condition and let n be a positive integer. Then M satisfies n-acc if and only if for each ascending chain L1 ⊆ L2 ⊆ L3 ⊆ . . . of n-generated submodules Li ($i \geq 1$) of M there exists a positive integer k such that ann(Lk) = ann(Lk+1) = ...

Proof. The necessity is clear. Conversely, suppose that M satisfies the stated condition but that M does not satisfy n-acc. By Lemma 11 there exists a prime ideal P of R such that P is maximal with the property that LiP = 0 for all submodules Li ($i \geq 1$) such that L1 ⊆ L2 ⊆ . . . is a proper ascending chain of n-generated submodules of M. Let N denote the set of elements $m \in M$ such that mP = 0. Then the right (R/P)-module N does not satisfy n-acc. By Theorem 8, Z(NR/P) does not satisfy n-acc. Therefore there exist a properly ascending chain H1 ⊆ H2 ⊆ . . . of n-generated submodules of Z(NR/P). By hypothesis, there exists a positive integer k such that ann(Hk) = ann(Hk+1) = ... Because Hk is finitely generated there exists an ideal A of R, properly containing P, such that HkA = 0. But then HiA = 0 for all $i \geq k$, which contradicts the choice of P. The result follows.

A prime ring is called right bounded if every essential right ideal contains a nonzero two-sided ideal. Also a ring R is called fully right bounded if every prime homomorphic image of R is right bounded. A ring R is called a right FBN ring if R is a right Noetherian right fully bounded ring. Clearly commutative Noetherian rings are FBN rings and so too are right Noetherian rings which satisfy a polynomial identity (see, for example. We have the following result for right FBN rings.

Theorem 13. Let R be a right FBN ring and let M be a right R-module which satisfies the direct sum condition. Then M satisfies pan-acc if and only if for each positive integer n and each ascending chain $L1 \subseteq L2 \subseteq . . .$ of n-generated submodules Li $(i \geq 1)$ of M there exists a positive integer k such that ann(Lk) = ann (Lk+1) = ...

Proof. Try Self

Lemma 14. Let R be a right Noetherian ring and let M be a right R-module which satisfies the direct sum condition such that for each prime ideal P of R for which LiP = 0 for all submodules Li $(i \geq 1)$ of M such that $L1 \subseteq L2 \subseteq . . .$ is an ascending chain of n-generated submodules of M there exists a finite subset F of $\cup$ i≥1 Li with P = ann(F). Then M satisfies pan-acc.

Proof. Suppose that M does not satisfy pan-acc. With the notation of that proof we obtain an ascending chain $H1 \subseteq H2 \subseteq . . .$ of n-generated submodules of Z(NR/P), where N is the set of $m \in M$ such that mP = 0. By hypothesis, there exists a finite subset F of N such that P = ann(F). But for each f in F there exists a right ideal E of R, containing P, such that E/P is an essential right ideal of R/P and fE = 0. Thus there exists a right ideal E′ of R, containing P, such that E′/P is an essential right ideal of R/P and gE′ = 0 for all $g \in F$. Thus $E' \subseteq P$, a contradiction. It follows that M satisfies pan-acc.

Lemma 15. Let S and R be rings and let M be a left S-, right R-bimodule such that M is a finitely generated left S-module. Let X denote the direct product MI and let A be an ideal of R such that A = ann(Y) for some submodule Y of the right R-module X. Then A = ann(F) for some finite subset F of Y .

Proof. Let L denote the set of elements m in M such that m is a component of some element of Y . Clearly uA = 0 for all $u \in L$. Now SL is a submodule of the left S-module M so that $SL = Sx1 + \cdots + Sxn$ for some positive integer n and elements $xi \in L$ $(1 \leq i \leq n)$. There exists a finite subset F of elements of Y such that for each $1 \leq i \leq n$, x_i is a component of an element of F. It is now clear that if an element r in R satisfies $fr = 0$ for all $f \in F$ then $x_i r = 0$ for all $1 \leq i \leq n$ so that $SLr = 0$ and hence $Y r = 0$. It follows that $A = ann(F)$.

Theorem 16. Let S and R be rings and let M be a left S-, right R-bimodule such that the left S-module M is Noetherian and the right R-module M is Noetherian. The the right R-module M^I satisfies pan-acc, for every index set I.

Proof. Let $A = ann(M_R)$. Note that $M = Sm_1 + \cdot \cdot \cdot + Sm_k$ for some positive integer k and elements $m_i \in M$ $(1 \leq i \leq k)$. Define a mapping φ : $R \rightarrow M^{(k)}$ by $\varphi(r) = (m_1r, \ldots, m_kr)$ for all $r \in R$. Then φ is an R-homomorphism with kernel A so that the ring R/A is right Noetherian. Without loss of generality we can suppose that $A = 0$.

Corollary 17. Let S and R be rings and let M be a left S-, right R-bimodule such that the left S-module M is Noetherian and the right R-module M is Noetherian. Let N_i $(i \in I)$ be any non-empty collection of submodules of the right R-module M. Then the right R-module $\prod_{i \in I} N_i$ satisfies pan-acc.

Proof: Try Self

Check In Progress-I

Note: i) Write your answers in the space given below.

Q. 1 Let R be a ring with finite right uniform dimension, let n be a positive integer and let M be a nonsingular n-generated R-module. Then M has finite uniform dimension and $u(M) \leq nu(R$

Solution :

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

Q. 2. Let S and R be rings and let M be a left S-, right R-bimodule such that the left S-module M is Noetherian and the right R-module M is

Noetherian. The the right R-module MI satisfies pan-acc, for every index set I.

Solution :

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

13.2 CHAIN CONDITIONS

Imposing chain conditions on the poset of submodules of a module, or on the poset of ideals of a ring,

makes a module or ring more tractable and facilitates the proofs of deep theorems.

Proposition: Let Σ be a poset with respect to $\leq$. TFAE

(i) Every increasing sequence
$x1 \leq x2 \leq \ldots \leq xn \leq \ldots$ in Σ

is stationary, that is,

$(\exists n)(\forall m \geq n)\ xm = xn$;

(ii) Every nonempty subset of Σ has a maximal element.

Proof: (i) =⇒ (ii): If (ii) is false, then there is a nonempty subset X of Σ with no maximal element, so $\exists x1 \in X$;

$$(\exists x2 \in X)\ x1 < x2 ;$$

$$(\exists x3 \in X)\ x1 < x2 < x3 ;$$

so continuing, X contains

$$x1 < x2 < x3 < \ldots < xn < \ldots$$

which is strictly increasing, so (i) fails.

(ii) =⇒ (i): If (ii) holds and

$$x1 \leq x2 \leq \ldots \leq xn \leq \ldots (*)$$

is an increasing sequence in Σ , then

$$\{ x1, \ldots , xn , \ldots \}$$

has a maximal element, say xk , so for every $m \geq k$,

$$xm \geq xk \geq xm ,$$

whence equality, proving (∗) is stationary, and (i) holds.

Let Σ be the set of submodules of a module M . Regarding Σ as a poset with respect to $\subseteq$, we refer to

(i) as the ascending chain condition (a.c.c.) and

(ii) as the maximal condition.

Any module satisfying the a.c.c. or equivalently the maximal condition is called Noetherian.

On the other hand regarding Σ as a poset with respect to $\supseteq$, we refer to

(i) as the descending chain condition (d.c.c.) and

(ii) as the miminal condition.

Any module satisfying the d.c.c. or equivalently the minimal condition is called Artinian.

Examples: (1) Any finite module satisfies both the a.c.c. and d.c.c

These include all finite abelian groups, regarded as Z-modules.

(2) The ring Z (regarded as a Z-module) satisfies the a.c.c but not the d.c.c.

(3) Consider the group Q under addition. Then Z is a subgroup and we may form the quotient group

$Q/Z = \{ q + Z \mid q \in Q \}$.

Fix a prime number p , and put

$G = \{ a/pn + Z \mid n \geq 0 , a \in Z \}$

and, for $i \geq 0$,

$$G_i = \{ a/p^i + Z \mid a \in Z \} .$$

Clearly G is a subgroup of Q/Z and each G_i is a subgroup of G .

Moreover, $G_0 \subset G_1 \subset . . . G_n \subset . .$ …………………………… (∗)

is a strictly increasing sequence, so, regarded as a Z-module,

G does not satisfy the a.c.c.

Exercise: Prove that the only subgroups of G are G and G_i for $i \geq 0$.

By (∗) and this exercise, there are no infinite strictly descending chains of subgroups of G , so, as a Z-module,G satisfies the d.c.c

(4) Fix a prime number p and put

$H = \{ m/p^n \mid m \in Z , n \geq 0 \}$

Then clearly H is a subgroup of Q and

$0 \longrightarrow Z \longrightarrow H \longrightarrow H/Z = G \longrightarrow 0$

is exact, where the second mapping is inclusion and G is the group of (3). Thus

H doesn't satisfy the d.c.c.

because it has a subgroup Z which doesn't, and

H doesn't satisfy the a.c.c.

because it has a quotient G which doesn't.

(5) The polynomial ring F[x] , where F is a field, satisfies the a.c.c. but not the d.c.c. on ideals.

The proof is left as an exercise, using the fact that F[x] is a PID, and copying the details of (2).

(6) The polynomial ring $F[x_1 , x_2 , . . .]$ using infinitely many indeterminates does not satisfy the d.c.c. on ideals (as for (5)),

but also does not satisfy the a.c.c. since

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \ldots \subset \langle x_1, \ldots x_n \rangle \subset \ldots$$

is an infinite strictly increasing chain of ideals.

Proposition: Let M be an A-module. Then M is Noetherian iff every submodule of M is finitely generated.

Proof: (=⇒) Suppose M is Noetherian and let N be a submodule of M . Let

$\Sigma = \{$ finitely generated submodules of N $\}$.

Then Σ has a maximal element N_0

If $N \neq N_0$ then

$$\exists x \in N \setminus N_0 ,$$

so $\langle N_0 \cup \{x\} \rangle$ is a finitely generated submodule of N bigger than N_0 , contradicting maximality.

Hence $N_0 = N$, so N is finitely generated.

(⇐=) Suppose all submodules of M are finitely generated. Let

$$M_1 \subseteq M_2 \subseteq \ldots \subseteq M_n \subseteq \ldots (*)$$

be an ascending chain of submodules. Then $\bigcup_{i=1}^{\infty} M_i$ is easily seen to be a submodule of M ,

so is generated by finitely many elements, say

$$x_1 , \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots , x_r .$$

Then

$$(\forall j = 1, \ldots , r)\ (\exists i_j)\ x_j \in M_{i_j} .$$

Put $m = \max \{ i_1 , \ldots , i_r \}$ so

$$(\forall j)\ x_j \in M_m .$$

so equality holds, and (∗) is stationary.

Theorem: Let $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ be an exact sequence of A-modules. Then M is Noetherian [Artinian] iff M' and M'' are.

Proof: We prove the result for Noetherian, the argument for Artinian being similar.

(=⇒) Suppose M is Noetherian.

Because α is injective, any ascending chain of submodules of M' corresponds to an ascending chain of submodules of M , so the former is stationary, since the latter is.

Hence M' is Noetherian.

Because β is surjective,

$$M'' \cong M/\ker\beta$$

so that submodules of M'' correspond to submodules of M containing ker β , and the correspondence is inclusion preserving.

Hence any ascending chain of submodules of M'' corresponds to an ascending chain of submodules of M , so the former is stationary, since the latter is.

Hence M'' is Noetherian.

(⇐=) Suppose M' , M'' are Noetherian.

$$\text{Let } L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n \subseteq \ldots \qquad (*)$$

be an ascending chain of submodules of M . Then

$$\alpha^{-1}(L_1) \subseteq \alpha^{-1}(L_2) \subseteq \ldots \subseteq \alpha^{-1}(L_n) \subseteq \ldots$$

s an ascending chain of submodules of M' , and

$$\beta(L_1) \subseteq \beta(L_2) \subseteq \ldots \subseteq \beta(L_n) \subseteq \ldots$$

is an ascending chain of submodules of M'' .

Since these sequences are stationary,

$(\exists n_1)(\forall m \geq n_1)\ \alpha^{-1}(L_m) = \alpha^{-1}(L_{n_1})$

$(\exists n_2)(\forall m \geq n_2)\ \beta(L_m) = \beta(L_{n_2})$

Put $n = \max\{n_1, n_2\}$, so $(\forall m \geq n)$,

$\alpha^{-1}(L_m) = \alpha^{-1}(L_n)$ and $\beta(L_m) = \beta(L_n)$.

We will prove that

$(\forall m \geq n)\ L_m = L_n$.

Let $m \geq n$ and $x \in L_m$. Then

$$\beta(x) \in \beta(L_m) = \beta(L_n) ,$$

so, for some $y \in L_n$, $\beta(x) = \beta(y)$, so, by exactness,

$$x - y \in \ker \beta = \operatorname{im} \alpha .$$

But $L_n \subseteq L_m$, so $x - y \in L_m$, giving

$$x - y = \alpha(z)\ \exists z \in \alpha^{-1}(L_m)$$

But $\alpha^{-1}(L_m) = \alpha^{-1}(L_n)$, so $\alpha(z) \in L_n$, giving

$$x = y + \alpha(z) \in L_n$$

Hence

$$L_m \subseteq L_n \subseteq L_m ,$$

whence equality. This proves (∗) is stationary, so M is Noetherian, and the Theorem is proved.

Corollary: If $M_1 , \ldots , M_n$ are Noetherian [Artinian] A-modules then so is

$$M_1 \oplus \ldots \oplus M_n .$$

Proof: This follows by induction and the previous Theorem applied to the exact sequence

$$0 \longrightarrow M_n \xrightarrow{\alpha} \bigoplus_{i=1}^{n} M_i \xrightarrow{\beta} \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0$$

where

$$\alpha : x \mapsto (0, \ldots , 0, x)$$

$$\beta : (x_1, \ldots , x_n) \mapsto (x_1, \ldots , x_{n-1}) .$$

Call a ring A Noetherian [Artinian] if it is so as an A-module, that is, if it satisfies the a.c.c. [d.c.c.] on ideals.

Check In Progress-II

Note: i) Write your answers in the space given below.

Q. 1 Let $0 \longrightarrow M' \alpha \longrightarrow M \beta \longrightarrow M''; \longrightarrow 0$ be an exact sequence of A-modules. Then M is Noetherian [Artinian] iff M′ and M′′ are.

Solution :

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

Q. 2. Any finite module satisfies both the a.c.c. and d.c.c

Solution :

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

13.3 ASCENDING CHAIN CONDITION

In mathematics, the ascending chain condition (ACC) and descending chain condition (DCC) are finiteness properties satisfied by some algebraic structures, most importantly ideals in certain commutative rings. These conditions played an important role in the development of the structure theory of commutative rings in the works of David Hilbert, Emmy Noether, and Emil Artin. The conditions themselves can be stated in an abstract form, so that they make sense for any partially ordered set. This point of view is useful in abstract algebraic dimension theory due to Gabriel and Rentschler.

Definition:- A partially ordered set (poset) *P* is said to satisfy the ascending chain condition (ACC) if every strictly ascending sequence of elements eventually terminates.Equivalently, given any weakly ascending sequence

$a_1 \leq a_2 \leq a_3 \leq a_3 \leq a_4 \leq a_5 \leq \ldots\ldots\ldots\ldots\ldots\ldots$

there exists a positive integer *n* such that

$$a_n = a_{n+1} = a_{n+2} = \cdots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$

Similarly, *P* is said to satisfy the descending chain condition (DCC) if every strictly descending sequence of elements of *P* eventually terminates, that is, there is no infinite descending chain. Equivalently, every weakly descending sequence

$a_1 \geq a_2 \geq a_3 \geq a_3 \geq a_4$ …………………………………..of elements of *P* eventually stabilizes.

Comments

- The descending chain condition on *P* is equivalent to *P* being well-founded: every nonempty subset of *P* has a minimal element (also called the minimal condition or minimum condition).
- Similarly, the ascending chain condition is equivalent to *P* being converse well-founded: every nonempty subset of *P* has a maximal element (the maximal condition or maximum condition).
- Trivially every finite poset satisfies both ACC and DCC.
- A totally ordered set that satisfies the descending chain condition is a well-ordered set (assuming the axiom of dependent choice).

13.4 SUMMARY

We study in this unit about Ascending Chain Condition and its properties. We study Chain Condition and its properties. We study some lemma for chain condition on module. We study chain conditions with its examples and proposition. We study Z-Module and its examples.

1. Let p be any prime in Z and let a Z-module A be a p-module. Then every homomorphic image of A satisfies pan-acc if and only if there exists a positive integer k such that p kA = 0.
2. Let R be a ring and let L be a countably generated submodule of an R-module M. Then the following statements are equivalent.

L is contained in a direct sum of finitely generated submodules of M.

There exists a submodule K of M containing L such that every finitely generated submodule of L is contained in a finitely generated direct summand of K.

3. Let R be a right Noetherian ring, let M be a right R-module which satisfies the direct sum condition and let n be a positive integer. Then M satisfies n-acc if and only if Z2(M) satisfies n-acc.
4. Let R be a ring with finite right uniform dimension, let n be a positive integer and let M be a nonsingular n-generated R-module. Then M has finite uniform dimension and u(M) ≤ nu(R).
5. Let S and R be rings and let M be a left S-, right R-bimodule such that the left S-module M is Noetherian and the right R-module M is Noetherian. The the right R-module MI satisfies pan-acc, for every index set I.

13.5 KEYWORD

Ascending :Increasing in size or importance

Chain Condition :The ascending chain condition, commonly abbreviated "A.C.C.," for a partially ordered set requires that all increasing sequences in become eventually constant. A module fulfils the ascending chain condition if its set of submodules obeys
the condition with respect to inclusion

Epimorphism :A morphism in a category is an *epimorphism* if, for any two morphisms , implies . In the categories of sets, groups, modules, etc.

13.6 EXERCISE

(1) Any ring with only finitely many ideals (such as a finite ring or a field) is certainly both Noetherian and Artinian.

(2) The ring F[x1, . . . ,xn, . . .] where F is a field is neither Noetherian nor Artinian, but is an integral domain, so has a field of fractions, which

is both Noetherian and Artinian. Thus subrings of Noetherian [Artinian] rings need not be Noetherian [Artinian]. However quotients are well-behaved. we get immediately

Corollary: Any homomorphic image of a Noetherian [Artinian] ring is Noetherian [Artinian].

Theorem: Let A be a Noetherian [Artinian] ring and M a finitely generated A-module. Then M is Noetherian [Artinian].

Proof: By general theory (M ∼= An / N for some n > 0 and some submodule N of An . But An is Noetherian [Artinian], being a direct sum of Noetherian [Artinian] modules.

Hence, by the previous Corollary, M is Noetherian [Artinian].

13.7 SUGGESTION READING AND REFERENCES

- Atiyah, M. F., and I. G. MacDonald, *Introduction to Commutative Algebra*, Perseus Books, 1969, ISBN 0-201-00361-9
- MichielHazewinkel, NadiyaGubareni, V. V. Kirichenko. *Algebras, rings and modules*. Kluwer Academic Publishers, 2004. ISBN 1-4020-2690-0
- John B. Fraleigh, Victor J. Katz. *A first course in abstract algebra*. Addison-Wesley Publishing Company. 5 ed., 1967. ISBN 0-201-53467-3
- Nathan Jacobson. Basic Algebra I. Dover, 2009. ISBN 978-0-486-47189-1
- M. E. AntunesSim˜oes and P. F. Smith, Direct products satisfying the ascending chain condition for submodules with a bounded number of generators, Comm. Algebra 23 (1995), 3525-3540.
  M. E. AntunesSim˜oes and P. F. Smith, On the ascending chain condition for submodules with a bounded number of generators, Comm. Algebra 24 (1996), 1713-1721.

- M. E. AntunesSim˜oes and P. F. Smith, Rings whose free modules satisfy the ascending chain condition on submodules with a bounded number of generators, J. Pure Appl. Algebra 123 (1998), 51-66.
- B. Baumslag and G. Baumslag, On ascending chain conditions, Proc. London Math. Soc. (3) 22 (1971), 681-704.

13.8 ANSWER TO CHECK YOUR PROGRESS

Check in Progress-I

Answer Q. 1 Check in Theorem 16

Q 2 Check in Lemma 7

Check in Progress-II

Answer check in section 2 all solution given.

UNIT 14 -: NOETHERIAN AND ARTINIAN MODULES

STRUCTURE

14.0 OBJECTIVE

* We able to study in this unit about Artinian Module and Ring

* Learn Hilbert Basis Theorem

* Learn Zorn’s Lemma

* Learn Noetherian Module

14.1 INTRODUCTION: NOETHERIAN MODULE

In abstract algebra, a **Noetherian module** is a module that satisfies the ascending chain condition on its submodules, where the submodules are partially ordered by inclusion.

Historically, Hilbert was the first mathematician to work with the properties of finitely generated submodules. He proved an important theorem known as Hilbert's basis theorem which says that any ideal in the multivariate polynomial ring of an arbitrary field is finitely generated. However, the property is named after Emmy Noether who was the first one to discover the true importance of the property.

A module for which every submodule has a finite system of generators. Equivalent conditions are: the ascending chain
condition for submodules (every strictly ascending chain of submodules breaks off after finitely many terms); every non-empty set of submodules ordered by inclusion contains a maximal element. Submodules and quotient modules of a Noetherian module are Noetherian. If, in an exact sequence

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

$M'M'$ and $M''M''$ are Noetherian, then so is MM. A module over a Noetherian ring is Noetherian if and only if it is finitely generated. A module has a composition series if and only if it is both Artinian and Noetherian.

14.1.1 Characterizations And Properties

In the presence of the axiom of choice, two other characterizations are possible:

- Any nonempty set *S* of submodules of the module has a maximal element (with respect to set inclusion.) This is known as the maximum condition.
- All of the submodules of the module are finitely generated.

If M is a module and K a submodule, then *M* is Noetherian if and only if *K* and *M*/*K* are Noetherian. This is in contrast to the general situation with finitely generated modules: a submodule of a finitely generated module need not be finitely generated.

Examples

- The integers, considered as a module over the ring of integers, is a Noetherian module.
- If $R = M_n(F)$ is the full matrix ring over a field, and $M = M_{n\ 1}(F)$ is the set of column vectors over *F*, then *M* can be made into a module using matrix multiplication by elements of *R* on the left of elements of *M*. This is a Noetherian module.
- Any module that is finite as a set is Noetherian.
- Any finitely generated right module over a right Noetherian ring is a Noetherian module.

14.1.2 Use In Other Structures

A right Noetherian ring *R* is, by definition, a Noetherian right *R* module over itself using multiplication on the right. Likewise a ring is called left Noetherian ring when *R* is Noetherian considered as a left *R* module. When *R* is a commutative ring the left-right adjectives may be dropped, as they are unnecessary. Also, if *R* is Noetherian on both sides, it is customary to call it Noetherian and not "left and right Noetherian".

The Noetherian condition can also be defined on bimodule structures as well: a Noetherian bimodule is a bimodule whose poset of sub-bimodules satisfies the ascending chain condition. Since a sub-bimodule of an *R*-*S* bimodule *M* is in particular a left R-module, if *M* considered as a left *R* module were Noetherian, then *M* is automatically a Noetherian bimodule. It may happen, however, that a bimodule is Noetherian without its left or right structures being Noetherian.

Let R be a ring and M a left R-module. Then we say that M is a **Noetherian module** if it satisfies the following property, known as the ascending chain condition (ACC):

For any ascending chain

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$$

of submodules of M, there exists an integer n so that $M_n = M_{n+1} = M_{n+2} = \cdots$ (i.e. the chain eventually stabilizes, or terminates).

We say that a ring R is left (right) Noetherian if it is Noetherian as a left (right) R-module. If R is both left and right Noetherian, we call it simply Noetherian.

Theorem. The following conditions are equivalent for a left R-module:

1. M is Noetherian.
2. Every submodule N of M is finitely generated (i.e. can be written as $Rm_1 + \cdots + Rm_k$ for some $m_1, \ldots, m_k \in N$).
3. Every collection of submodules of M has a maximal element.

The second condition is also frequently used as the definition for Noetherian.

We also have right Noetherian modules with the appropriate adjustments.

Proof. In general, condition 3 is equivalent to ACC. It thus suffices to prove that condition 2 is equivalent to ACC.

Suppose that condition 2 holds. Let $M_0 \subseteq M_1 \subseteq \cdots$ be an ascending chain of submodules of M. Then $\bigcup_{n \geq 0} M_n$ is a submodule of M, so it must be finitely generated, say by elements $a_1, \ldots, a_n$. Each of the a_k is contained in one of $M_0, M_1, \ldots$, say in $M_{t(k)}$. If we set $N = \max t(k)$, then for all $n \geq N$, $\{a_1, \ldots, a_n\} \subset M_n$, so

$$M_n = M_N = \bigcup_{n \geq 0} M_n.$$

Thus M satisfies ACC.

On the other hand, suppose that condition 2 does not hold, that there exists some submodule M' of M that is not finitely generated. Thus we can recursively define a sequence of elements $(a_n)_{n=0}^{\infty}$ such that a_n is not in the submodule generated by $a_0, \dots, a_{n-1}$. Then the sequence $(a_0) \subset (a_0, a_1) \subset (a_0, a_1, a_2) \subset \cdots$ is an ascending chain that does not stabilize. ■

Note: The notation $(a, b, c \dots)$ *denotes the module* generated by $a, b, c, \dots$.

Hilbert's Basis Theorem guarantees that if R is a Noetherian ring, then $R[x_1, \dots, x_n]$ is also a Noetherian ring, for finite n. It is not a Noetherian R-module.

14.1.3 Hilbert's Basis Theorem

Hilbert's Basis Theorem is a result concerning Noetherian rings. It states that if A is a (not necessarily commutative) Noetherian ring, then the ring of polynomials $A[x_1, x_2, \dots, x_n]$ is also a Noetherian ring. (The converse is evidently true as well.)

Note that n must be finite; if we adjoin infinitely many variables, then the ideal generated by these variables is not finitely generated.

The theorem is named for David Hilbert, one of the great mathematicians of the late nineteenth and twentieth centuries. He first stated and proved the theorem in 1888, using a nonconstructive proof that led Paul Gordan to declare famously, "Das ist nicht Mathematik. Das ist Theologie. [This is not mathematics. This is theology.]" In time, though, the value of nonconstructive proofs was more widely recognized.

Proof

By induction, it suffices to show that if A is a Noetherian ring, then so is $A[x]$.

To this end, suppose that $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$ is an ascending chain of (two-sided) ideals of $A[x]$.

Let $\mathfrak{c}_{i,j}$ denote the set of elements a of A such that there is a polynomial in $\mathfrak{a}_i$ with degree at most i and with a as the coefficient of x^j. Then $\mathfrak{c}_{i,j}$ is a two-sided ideal of A; furthermore, for any $i' \geq i$, $j' \geq j$, $\mathfrak{c}_{i,j} \subset \mathfrak{c}_{i',j}, \mathfrak{c}_{i,j'}$. Since A is Noetherian, it follows that for every $i \geq 0$, the chain $\mathfrak{c}_{i,0} \subset \mathfrak{c}_{i,1} \subset \cdots$ stabilizes to some ideal $\mathfrak{m}_i$. Furthermore, the ascending chain $\mathfrak{m}_0, \mathfrak{m}_1, \ldots$ also stabilizes to some ideal $\mathfrak{m} = \mathfrak{c}_{A,B}$. Then for any $i \geq A$ and any $j \geq 0$, $\mathfrak{c}_{i,j} = \mathfrak{c}_{A,j}$. We claim that the chain $(\mathfrak{a}_k)_{k=0}^{\infty}$ stabilizes at $\mathfrak{a}_A$. For this, it suffices to show that for all $k \geq A$, $\mathfrak{a}_k \subset \mathfrak{a}_A$. We will thus prove that all polynomials of degree n in $\mathfrak{a}_k$ are also elements of $\mathfrak{a}_A$, by induction on n.

For our base case, we note that $\mathfrak{c}_{k,0} = \mathfrak{c}_{M,0}$, and these ideals are the sets of degree-zero polynomials in $\mathfrak{a}_k$ and $\mathfrak{a}_M$, respectively.

Now, suppose that all of $\mathfrak{a}_k$'s elements of degree $n-1$ or lower are also elements of $\mathfrak{a}_M$. Let p be an element of degree n in $\mathfrak{a}_k$. Since $\mathfrak{c}_{k,n} = \mathfrak{c}_{A,n}$, there exists some element $q \in \mathfrak{a}_A$ with the same leading coefficient as p. Then by inductive hypothesis, $p - q \in \mathfrak{a}_A$, so $p \in \mathfrak{a}_A$,

14.1.4 Zorn's Lemma

Background

Let A be a partially ordered set.

We say that A is *inductively ordered* if every totally ordered subset T of A has an upper bound, i.e., an element $a \in A$ such that for all $x \in T$, $x \leq a$. We say that A is *strictly inductively ordered* if every totally ordered subset T of A has a least upper bound, i.e., an upper bound a so that if b is an upper bound of T, then $a \leq b$.

An element $m \in A$ is maximal if the relation $a \geq m$ implies $a = m$. (Note that a set may have several maximal elements.)

We say a function $f : A \to A$ is *increasing* if $x \leq f(x)$ for all $x \in A$.

Statement

Every inductively ordered set A has a maximal element.

Proof (using the Axiom of Choice)

We first prove some intermediate results, viz., Bourbaki's Theorem (also known as the Bourbaki-Witt theorem).

Let A be a strictly inductively ordered set, and let $f : A \to A$ be an increasing function. Pick some $a \in A$. Let A' be the set of elements $x \in A$ such that $a \leq A$. Evidently, A' is stricty inductively ordered, for if T is a totally ordered subset of A', then it has a least upper bound in A, which is evidently greater than a, so this least upper bound is an element of A'. We say that a subset $B \subseteq A'$ is *admissable* if it satisfies these conditions:

- $a \in B$
- $f(B) \subseteq B$
- For every totally ordered subset $T \subseteq B$, the least upper bound of T in A' is an element of B.

Let M be the intersection of all admissable subsets of A'. We note that M is not empty, as A' is an admissable subset of itself, and all admissable sets contain a. Then M is the least admissable set, under order by inclusion.

We say that an element $c \in M$ is an *extreme point* if $x \in M$, $x < c$ together imply $f(x) \leq c$. For an extreme point c denote by M_c the set of $x \in M$ such that $x \leq c$ or $f(c) \leq x$.

Lemma 1.

For each extreme point c, $M_c = M$.

Proof. It suffices to show that M_c is an admissable set.
Evidently, $a \leq c$, so $a \in M_c$. Now, let x be an element of M_c.
If $x = c$, then evidently, $f(c) \leq f(x)$, so $f(x) \in M_c$. If $x < c$,

then since c is an extreme point, $f(x) \leq c$, so $f(x) \in M_c$. On the other hand, if $f(c) \leq x$, then $f(c) \leq x \leq f(x)$, so $f(x) \in M_c$. Therefore $f(M_c) \subseteq M_c$.

Let T be a totally ordered subset of M_c. Then T has a least upper bound $s \in A'$. Since M is admissable, $s \in M$. Now, if $s \leq c$, then evidently $s \in M_c$. On the other hand, if $s \geq c$, then either $f(c) \leq s$, or every element of T is less than or equal to c, so $s \leq c$. Hence the least upper bound of every totally ordered subset T of M_c is an element of M_c, so M_c is admissable. Therefore $M \subseteq M_c$; since we know $M_c \subseteq M$, it follows that $M = M_c$. ■

Lemma 2.

Every element of M is an extreme point.

Proof. Let E be the set of extreme points of M. As before, it suffices to show that E is an admissable set. Evidently, a is an extreme point of M, as no element of M is less than a, so every element less than a is also less than or equal to $f(a)$. Now, suppose c is an extreme point of M. Then for any $x \in M$, if $x < f(c)$, then by Lemma 1, $x \leq c$. If $x = c$, then $f(x) = f(c)$, so $f(x) \leq f(c)$; if $x < c$, then since c is an extreme point, $f(x) \leq c \leq f(c)$. Therefore $f(c)$ is an extreme point, so $f(E) \subseteq E$.

Now, let T be a totally ordered set of extreme points. Consider the least upper bound s of T in M. If x is an element of M strictly less than s, then x must be strictly less than some element $c \in T$. But c is an extreme point, so $f(x) \leq c \leq s$. Therefore s is an extreme point, i.e., an element of E. It follows that E is an admissable set, so as before, $E = M$. ■

Theorem 3 (Bourbaki).

For any strictly inductively ordered set A and any increasing function $f : A \to A$, there exists an element x_0 of A such that $x_0 = f(x_0)$.

Proof. Choose an arbitrary $a \in A$, and define A' as before. Let M be the least admissable subset of A', as before. By Lemmata 2 and 1, for all elements $a, b \in M$, either $a \leq b$, or $b \leq f(b) \leq a$. Therefore M is totally ordered under the ordering induced by A. Then M has a least upper bound x_0 which is an element of M. We note that $f(x_0) \in M$, so $f(x_0) \leq x_0$, and since f is increasing, $x_0 \leq f(x_0)$.
Hence $x_0 = f(x_0)$, as desired. ■

Note that thus far, we have not used the Axiom of Choice. In the next corollary, however, we will use the Axiom of Choice.

Corollary 4.

Let A be a strictly inductively ordered set. Then A has a maximal element.

Proof. Suppose the contrary. Then by the Axiom of Choice, for each $x \in A$, we may define $f(x)$ to be an element strictly greater than x. Then f is an increasing function, but for no $x \in A$ does $x = f(x)$, which contradicts the Bourbaki-Witt Theorem. ■

Corollary 5 (Zorn's Lemma).

Let A be an inductively ordered set. Then A has a maximal element.

Proof. Let T be the family of totally ordered subsets of A.

We claim that under the order relation $\subseteq$, T is a strictly inductively ordered set. Indeed, if $\{X_i\}_{i \in I}$ is a totally ordered subset of T, then $Z = \bigcup_{i \in I} X_i$ is evidently the least upper bound of the X_i, and if $a, b \in Z$, then for some $i, j \in I$, $a \in X_i$ and $b \in X_j$; one of X_i and X_j is a subset of the other, by assumption, so a and b are comparable. It follows that Z is totally ordered, i.e., $Z \in T$.

Now, by Corollary 4, there exists a maximal element P of T. This set P is totally ordered, so it has an upper bound x_0 in A.
Then $P \cup \{x_0\}$ is a totally ordered set, so by the maximality of P

Notes

, $x_0 \in P$. Now, if $y \geq x_0$, then $P \cup \{y\}$ is a totally ordered set, so $y \in P$ and $y \leq x_0$, so $y = x_0$. Therefore x_0 is a maximal element, as desired. ■

Check in Progress-I

Note: i) Write your answers in the space given below.

Q. 1 State Zorn's Lemma.

Solution …………………………………………………………….

…………………………………………………………………......

………………………………………………………………………

……………………………………………………………………..

Q. 2 State Hilbert Basis Theorem.

Solution …………………………………………………………….

…………………………………………………………………......

………………………………………………………………………

……………………………………………………………………..

14.2 DEFINITIONS AND ELEMENTARY PROPERTIES

A module is Artinian (respectively Noetherian) if it satisfies either of the following equivalent conditions:

• every non-empty collection of submodules contains a minimal (repsectively maximal) element with respect to inclusion.

• any descending (respectively ascending) chain of submodules stabilises.

A module is Artinian (respectively Noetherian) if and only if it is so over its ring of homotheties

An infinite direct sum of non-zero modules is neither Artinian nor Noetherian. A vector space is Artinian (respectively Noetherian) if and only if its dimension is finite

We now list some elementary facts about Artinian and Noetherian modules. The following would continue to be true if we replaced 'Artinian' by 'Noetherian':

• Submodules and quotient modules of Artinian modules are Artinian.

• If a submodule N of a module M and the quotient M/N by it are Artinian, then so is M.

• A finite direct sum is Artinian if and only if each of the summands is so. A comment about the simultaneous presence of the both conditions:

• A module is both Artinian and Noetherian if and only if it has finite length. Pertaining to the Noetherian condition alone, we make two more observations:

• Any subset S of a Noetherian module contains a finite subset that generates the same submodule as S.

• A module is Noetherian if and only if every submodule of it is finitely generated.

14.3 DECOMPOSITION INTO INDECOMPOSABLES OF A FINITE LENGTH MODULE.

Let u be an endomorphism of a module M. We have

$$0 \subseteq \operatorname{Ker} u \subseteq \operatorname{Ker} u^2 \subseteq \operatorname{Ker} u^3 \subseteq \ldots$$

$$M \supseteq \operatorname{Im} u \supseteq \operatorname{Im} u^2 \supseteq \operatorname{Im} u^3 \supseteq \ldots$$

Suppose that the ascending chain above stabilises (e.g., when M is Noetherian), say $\operatorname{Ker} u^n = \operatorname{Ker} u^{n+1}$. Then $\operatorname{Ker} u^n \cap \operatorname{Im} u^n = 0$. Indeed if and $u^n x = 0$ and $x = u^n y$, then $u^{2n} y = 0$, so $y \in \operatorname{Ker} u^{2n} = \operatorname{Ker} u^n$ and $x = u^n y = 0$. If u were also surjective, then so would be u^n, which means $\operatorname{Im} u^n = M$, and so $\operatorname{Ker} u^n = 0$, which means u^n (and so also u) is injective. Thus

A surjective endomorphism of a Noetherian module is bijective

Suppose that the descending chain above stablises (e.g., when M is Artinian), say $\operatorname{Im} u^n = \operatorname{Im} u^{n+1}$. Then $M = \operatorname{Ker} u^n + \operatorname{Im} u^n$. Indeed, for $x \in M$, choosing y such that $u^n x = u^{2n} y$, we have $x = (x - u^n y) + u^n y$. If u were also injective, then so would be u^n, which means $\operatorname{Ker} u^n = 0$, so $M = \operatorname{Im} u^n$, which means u^n (and so also u) in surjective. Thus:

An injective endomorphism of an Artinian module is bijective.

Suppose now that M is of finite length (equivalently, both Noetherian and Artinian). Then the above considerations show that for sufficiently large n we have a direct sum decomposition.

M = Ker u n ⊕ Im u n

If M were also indecomposable, then either Ker u n = M, in which case u is nilpotent, or Ker u n = 0 and Im u n = M, in which case u n (and so also u) is invertible, which proves the first half of the following

Proposition 1. The non-invertible endomorphisms of an indecomposable module M of finite length are nilpotent and form a two sided ideal.

Proof. The first half having already been proved, we need only prove the second half. For a nilpotent endomorphism u, and ϕ any endomorphism, ϕu and uϕ are non-invertible, and so nilpotent. Now suppose u and v are nilpotent endomorphisms. Suppose u + v is not nilpotent. Then it is invertible. Let ϕ be such that ϕ(u+v) = 1. Writing ϕu = 1−ϕv, we observe that ϕu is on the one hand nilpotent and on the other invertible.

Theorem 2. A module of finite length is a finite direct sum of indecomposable submodules. Further, any two such decompositions with no trivial factors are the Krull-Remaksame, i.e., the components are respectively isomorphic after a permutation.

Proof. The decomposition into a finite direct sum of indecomposable submodules follows easily by an induction on the length. We will now prove the uniqueness. Suppose ⊕m i=1Mi and ⊕m0 i 0=1M0 i 0 are two such decompositions of a module M. We prove the following claim by induction and that will suffice:

for 0 ≤ j ≤ m there exists an automorphism αj of M such that, after a possible rearrangement of the Mi , we have αjM0 k = Mk for 1 ≤ k ≤ j.

The base case of the induction (j = 0) is vacuous: we can take α0 to be the identity. Now, assuming the statement for some j − 1 < k, we will prove it for j. Writing αj−1M0 i 0 =: M00 i 0 , consider the decomposition ⊕m0 i 0=1M00 i 0 . We have M00 k = Mk for 1 ≤ k < j.

Let pk, p 0 k , and p 00 k denote respectively the projection onto Mk, M0 k , and M00 k with respect to the respective decompositions. The restriction to M00 j of the projection p 00 j is of course the identity but it also equals P k p 00 j pk. By the previous proposition, there exists a 1 ≤ k ≤ n such that p 00 j pk is an automorphism of M00 j . We claim that j ≤ k. Indeed, if k < j, then, since pkM00 j ⊆ Mk = M00 k , we have p 00 j pkM00 j = 0, a contradiction, and the claim is proved:

After a rearrangement of the Mk if necessary, we can take k = j. The automorphism αj is now defined as ϕαj−1 where ϕ is the endomorphism of M that is identity on all M00 l except l = j and is pj on M00 j : ϕ := 1 − p 00 j + pkp 00 j . We claim that ϕ is injective. It follows from the claim and what has been said earlier in this subsection that ϕ is bijective and that αj is an automorphism. To prove the claim, suppose that ϕx = 0. Write x − p 00 j x = −pkp 00 j x ∈ Mk; we see that p 00 j pkp 00 j x = 0 since p 00 j clearly kills the left side. But p 00 j pk being an automorphism of M00 j , we conclude that p 00 j x = 0, so 0 = ϕx = x, and the claim is proved.

It remains only to show that αjM0 k = Mk for 1 ≤ k ≤ j. This is evident for k < j: indeed, ϕαj−1M0 k = ϕM00 k = M00 k = Mk. We now prove αjM0 j = Mj . Since αjM0 j = ϕM00 j ⊆ Mj , it follows that Mj = ϕM00 j

***Theorem**. For an* R*-module* M*, the following are equivalent:*

- *any non-empty collection Σ of submodules of M has a maximal element N (i.e. N ∈ Σ, and whenever M' ∈ Σ we have M' ⊆ N);*
- *for any increasing sequence* $M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$ *of submodules of M, there is an n such that* $M_n = M_{n+1} = M_{n+2} = \ldots$. *We say that the sequence is* ***eventually constant****.*

Proof

⇒: assume the first property; given $M_0 \subseteq M_1 \subseteq \ldots$, let Σ be the collection of all M_n. This has a maximal element, say $M_n \in \Sigma$. Being maximal, all subsequent terms $M_{n+1}, M_{n+2}, \ldots$ must be equal to M_n.

⇐ : suppose Σ is non-empty and has no maximal element; pick $M_0 \in \Sigma$; this is not maximal, so we can pick $M_1 \in \Sigma$ which properly contains M_0; again this is not maximal, so pick $M_2 \in \Sigma$ properly containing M_1; repeat. ♦

Definition. *A module M which satisfies the two properties in the above theorem is said to be (left)* **noetherian**. *A ring is (left)* **noetherian** *if it is noetherian as a module over itself.*

The following result is a basic property of noetherian modules.

Theorem.

- *If M is noetherian, so is any submodule and quotient module of M.*
- *Conversely, if* $N \subseteq M$ *is such that N and M/N are noetherian, then so is M.*

Proof

First statement: let $N \subseteq M$. Any increasing sequence of submodules of N is also an increasing sequence of submodules of M, so it must terminate. Similarly, any increasing sequence of submodules of M/N corresponds to a sequence of submodules of M containing N, so it must terminate.

Second statement: let (M_n) be an increasing sequence of submodules of M. Then $(N \cap M_n)$ is an increasing sequence of submodules of N so it is eventually constant. Also, $((N+M_n)/N)$ is an increasing sequence of submodules of M/N so it is eventually constant. So for large n, we have:

$$M_n \subseteq M_{n+1}, \quad N \cap M_n = N \cap M_{n+1}, \quad N + M_n = N + M_{n+1}.$$

This implies $M_n = M_{n+1}$. [Proof : if $x \in M_{n+1}$, then by third equality $x = y+z$ for $y \in N$ and $z \in M_n$. So $y = x-z$ is in $N \cap M_{n+1} = N \cap M_n$, and $x-z \in M_n$ means $x \in M_n$.] So (M_n) is eventually constant. ♦

Corollary.

- *If M, N are noetherian, so is their direct sum* $M \oplus N$.
- *If M, N are noetherian submodules of P, so is M+N.*
- *If M is a finitely generated module over a noetherian ring, then M is noetherian.*

Proof

Indeed, $M \subseteq M \oplus N$ is a submodule whose quotient is isomorphic to N. Since M and N are noetherian, so is $M \oplus N$. The second statement follows from that $M+N$ is a quotient of $M \oplus N$.

For the third statement, let M be generated by $x_1, \ldots, x_n$. Then M is a sum of Rx_i, as submodules of M. Each Rx_i is a quotient of the form R/I for some left ideal $I \subset R$; since R is noetherian, so is R/I, and M. ♦

Examples

1. A simple module is noetherian since it has only two submodules. Thus a finitely generated semisimple module is noetherian. [#] In particular, a semisimple ring is noetherian.

[#] Subtle point: show that a finitely generated semisimple module M must be a direct sum of finitely many simple submodules. *Warning: even if M is generated by k elements, it is not true that M is a direct sum of k or less simple submodules. E.g. as* **Z**-*module,* **Z**/6 *is generated by 1 element but* **Z**/6 = **Z**/2 ⊕ **Z**/3.

2. The **Z**-module **Z** is noetherian, i.e. **Z** is a noetherian ring. Thus, a finitely generated abelian group is a noetherian **Z**-module.

3. The **Z**-module **Q** is *not* noetherian, for we have an infinite increasing sequence **Z** ⊂ (1/2)**Z** ⊂ (1/4)**Z** ⊂ … . This example also shows that $M := \{\frac{a}{2^m} : a, m \in \mathbf{Z}\}$ is not noetherian. Since **Z** is noetherian, it implies M/**Z** is non-noetherian.

4. The **Q**-module **Q** is obviously noetherian though. More generally, all division rings are noetherian.

5. **Z**[√2] is a finitely generated **Z**-module, so it is noetherian as a **Z**-module. This implies it is a noetherian ring, since every (left) ideal of **Z**[√2] is also a **Z**-module.

6. The infinite polynomial ring $\mathbf{R}[x_1, x_2, \ldots] := \cup_{n\geq 1}\mathbf{R}[x_1, \ldots, x_n]$ is a non-noetherian ring since the sequence of ideals $(x_1) \subset (x_1, x_2) \subsetneq \cdots$ never terminateS.

14.4 ARTINIAN MODULES AND RINGS

Reversing the direction of inclusion in the definition of noetherian rings, we get a similar concept. We will merely state the results since the proofs are identical to the above.

Theorem. *For an* R-*module* M, *the following are equivalent:*

- *any non-empty collection Σ of submodules of M has a minimal element N (i.e. N ∈ Σ, and whenever M' ∈ Σ we have M' ⊇ N);*
- *for any decreasing sequence* $M_0 \supseteq M_1 \supseteq M_2 \supseteq \ldots$ *of submodules of M, there is an n such that* $M_n = M_{n+1} = M_{n+2} = \ldots.$

Definition. *A module which satisfies the above two properties is said to be (left)* ***artinian***. *A ring is (left)* ***artinian*** *if it is artinian as a module over itself.*

Again we have the following basic property.

Theorem.

- *If M is artinian, so is any submodule and quotient module of M.*
- *Conversely, if N ⊆ M is such that N and M/N are artinian, then so is M.*

Corollary.

- *If M, N are artinian, so is their direct sum M ⊕ N.*
- *If M, N are artinian submodules of P, so is M+N.*
- *A finitely generated module over an artinian ring is also artinian.*

Examples

1. A simple module is artinian since it has only two submodules. Thus, a finitely generated semisimple module is artinian. In particular a semisimple ring is noetherian and artinian!

2. The **Z**-module **Z** is not artinian since it contains an infinite decreasing sequence of left ideals **Z** ⊃ 2**Z** ⊃ 4**Z** ⊃ … .

3. The module $M := \{\frac{a}{2^m} : a, m \in \mathbf{Z}\}$ is not artinian since it contains **Z**; however, *M*/**Z** is artinian! The proof is left as an exercise.

Easy Exercises

Prove that if *R* is a noetherian (resp. artinian) ring, then for any two-sided ideal *I*, *R*/*I* is also noetherian (resp. artinian).

Prove that if *R* and *S* are noetherian (resp. artinian) rings, so is *R* × *S*.

Summary. *Noetherian and artinian modules are both concepts of "finite" modules. Finite sums, submodules and quotients of noetherian modules are noetherian. A finitely generated module over a noetherian* *ring is noetherian. All the above holds when we replace "noetherian" with "artinian".*

In case you missed the above examples, let us reiterate that ***semisimple rings are noetherian and artinian****.*

Finally, to further emphasize the fact that noetherian / artinian modules are the correct analogy for "finite", we have the following important lemma. Recall that for a finite set *X*, a function $f : X \to X$ is bijective ⇔ *f* is injective ⇔ *f* is surjective. Likewise:

Lemma*. Let M be a noetherian and artinian module. The following are equivalent for a module map* $f : M \to M$.

- *f is bijective;*
- *f is injective;*
- *f is surjective.*

Proof

Suppose *f* is injective. We get

$$\mathrm{im} f \supseteq \mathrm{im} f^2 \supseteq \mathrm{im} f^3 \supseteq \ldots.$$

Since *M* is artinian, eventually $\mathrm{im} f^k = \mathrm{im} f^{k+1}$. To prove that *f* is surjective, let $x \in M$.

Then $f^k(x) \in \mathrm{im} f^k = \mathrm{im} f^{k+1}$ so $f^k(x) = f^{k+1}(y)$ for some $y \in M$.

Now $f^k(x - f(y)) = 0$ and since *f* is injective we have $x = f(y) \in \mathrm{im}\, f$.

The case where *f* is surjective ⇒*f* is injective, is left as an exercise for the reader. Hint: replace im with ker and you get an increasing sequence. ♦

Subtleties on Noetherian and Artinian

In the above examples, we saw that a noetherian module may not be artinian, and vice versa. But when it comes to rings, *an artinian ring must be noetherian*! [Hopefully we will eventually get around to proving this.] The apparent asymmetry is rather surprising at first glance, but it may be partially explained by the following heuristics.

Suppose *R* is a commutative ring which is artinian (thus, all left ideals are two-sided). If we let ∑ be any collection of ideals of *R*, then the collection of products $I_1 I_2 \ldots I_n$ of ideals from ∑ has a lower bound, so eventually $I_1 I_2 \ldots I_n = I_1 I_2 \ldots I_{n+1} = I_1 I_2 \ldots I_{n+2} = \ldots.$ This suggests that R has only finitely many ideals, so the artinian condition is a rather strong one.

Let us mention a result for noetherian modules which has no parallel for artinian ones.

Theorem. *An R-module M is noetherian ⇔ all its submodules are finitely generated.*

Proof

⇒: since a submodule of M is noetherian, it suffices to show a noetherian module is finitely generated. Now, if M is noetherian, let ∑ be the collection of all finitely generated submodules of M. This has a maximal $N \in \sum$, which is finitely generated. If $N \neq M$,

pick x in M outside N; then $N + Rx$ is a finitely generated submodule of M which is strictly bigger than N, contradicting its maximality.

Hence $N=M$, so M is finitely generated.

⇐: take any increase sequence $M_0 \subseteq M_1 \subseteq \cdots$ of submodules of M. Let $N := \cup_{n\geq 0} M_n$, which is a submodule of M, so it is finitely generated by, say, $x_1, \ldots, x_k$. Since there are only finitely many x_i, some M_n must contain all of them, but this

means $M_n = N$ so $M_n = M_{n+1} = \ldots$. ♦

Left and Right Modules

Finally, note that we've been talking about left modules throughout, but we can also define the concept of noetherian and artinian for right modules. [Or just note that a right R-module is the same as a left R^{op}-module.] You may be surprised to learn that *a left noetherian ring is not necessarily right noetherian*. In fact, here we have a ring which is left noetherian and left artinian, but neither right noetherian nor right artinian!

Proof

It's not right artinian or right noetherian because it has right ideals of the form $\begin{pmatrix} 0 & 0 \\ A & 0 \end{pmatrix}$ where A is a subspace of **R** as a **Q**-vector space. It is easy to see that the collection of such subspaces has no maximal or minimal element.

On the other hand, R is a direct sum of left ideals

Clearly J is simple. And I has a simple submodule $I' := \begin{pmatrix} \mathbf{Q} & 0 \\ 0 & 0 \end{pmatrix}$, and the resulting quotient is I/I' is isomorphic to J. Since I', I/I' and J are simple, they're noetherian and artinian. Thus R is left noetherian and left artinian. ♦

Check In Progress-II

Note: i) Write your answers in the space given below.

Q. 1 *An R-module M is noetherian* ⇔ *all its submodules are finitely generated.*

Solution :

……………………………………………………………………………….

………………………………………………………………………………

………………………………………………………………………………

Q. 2 The non-invertible endomorphisms of an indecomposable module M of finite length are nilpotent and form a two sided ideal.

Solution :

……………………………………………………………………………….

………………………………………………………………………………

………………………………………………………………………………

14.5 ARTINIAN MODULE

A module that satisfies the descending chain condition for submodules. The class of Artinian modules is closed with respect to passing to submodules, quotient modules, finite direct sums and extensions. Extension in this context means that if the modules B and A/B are Artinian, then so is A. Each Artinian module can be decomposed into a direct sum of submodules which are no longer decomposable into a direct sum. A module has a composition series if and only if it is both Artinian and Noetherian. See also Artinian ring.

In abstract algebra, an **Artinian module** is a module that satisfies the descending chain condition on its poset of submodules. They are for modules what Artinian rings are for rings, and a ring is Artinian if and only if it is an Artinian module over itself (with left or right multiplication). Both concepts are named for Emil Artin.

In the presence of the axiom of choice, the descending chain condition becomes equivalent to the minimum condition, and so that may be used in the definition instead.

Like Noetherian modules, Artinian modules enjoy the following heredity property:

- If *M* is an Artinian *R*-module, then so is any submodule and any quotient of *M*.

The converse also holds:

- If *M* is any *R* module and *N* any Artinian submodule such that *M*/*N* is Artinian, then *M* is Artinian.

As a consequence, any finitely-generated module over an Artinian ring is Artinian. Since an Artinian ring is also a Noetherian ring, and finitely-generated modules over a Noetherian ring are Noetherian, it is true that for an Artinian ring *R*, any finitely-generated *R*-module is both Noetherian and Artinian, and is said to be of finite length; however, if *R* is not Artinian, or if *M* is not finitely generated, there are counterexamples.

Left and right Artinian rings, modules and bimodules

The ring *R* can be considered as a right module, where the action is the natural one given by the ring multiplication on the right. *R* is called right Artinian when this right module *R* is an Artinian module. The definition of "left Artinian ring" is done analogously. For noncommutative rings this distinction is necessary, because it is possible for a ring to be Artinian on one side only.

The left-right adjectives are not normally necessary for modules, because the module *M* is usually given as a left or right *R* module at the outset. However, it is possible that *M* may have both a left and right *R* module structure, and then calling *M* Artinian is ambiguous, and it becomes necessary to clarify which module structure is Artinian. To separate the properties of the two structures, one can abuse terminology and refer to *M* as left Artinian or right Artinian when, strictly speaking, it is correct to say that *M*, with its left *R*-module structure, is Artinian.

The occurrence of modules with a left and right structure is not unusual: for example *R* itself has a left and right *R* module structure. In fact this is an example of a bimodule, and it may be possible for an abelian group *M* to be made into a left-*R*, right-*S* bimodule for a different ring *S*. Indeed, for any right module *M*, it is automatically a left module over the ring of integers **Z**, and moreover is a **Z**-*R* bimodule. For example, consider the rational numbers **Q** as a **Z**-**Q** bimodule in the natural way. Then **Q** is not Artinian as a left **Z** module, but it is Artinian as a right **Q** module.

The Artinian condition can be defined on bimodule structures as well: an **Artinian bimodule** is a bimodule whose poset of sub-bimodules satisfies the descending chain condition. Since a sub-bimodule of an *R*-*S* bimodule *M* is a fortiori a left *R*-module, if *M* considered as a left *R* module were Artinian, then *M* is automatically an Artinian bimodule. It may happen, however, that a bimodule is Artinian without its left or right structures being Artinian, as the following example will show.

Example: It is well known that a simple ring is left Artinian if and only if it is right Artinian, in which case it is a semisimple ring. Let *R* be a simple ring which is not right Artinian. Then it is also not left Artinian. Considering *R* as an *R*-*R* bimodule in the natural way, its sub-bimodules are exactly the ideals of *R*. Since *R* is simple there are only two: *R* and the zero ideal. Thus the bimodule *R* is Artinian as a bimodule, but not Artinian as a left or right *R*-module over itself.

Lemma. An R-module M is of finite length if and only if it is both Noetherian and Artinian.

Proof. If M is of finite length, then all strict chains of submodules of M are finite (b) and (c). So in this case M is clearly both Noetherian and Artinian. Conversely, assume that M is both Noetherian and Artinian. Starting from M0 = 0, we try to construct a chain M0 (M1 (M2 (··· of submodules of M as follows: for n ∈ N let Mn+1 be a minimal submodule of M that strictly contains Mn — as long as Mn 6= M this works (b) since M is Artinian. But as M is Noetherian as well, we cannot get such an infinite ascending chain of submodules, and thus we conclude that we must have Mn = M for some n ∈ N. The resulting chain 0 = M0 (M1 (··· (Mn = M is then a composition series for M, since by construction there are no submodules between Mi−1 and Mi for all i = 1,...,n.

Exercise . Let M be an R-module, and let ϕ : M → M be an R-module homomorphism. If M is Noetherian (hence finitely generated) and ϕ is surjective, you already know that ϕ has to be an isomorphism. Now show that if M is Artinian and ϕ is injective, then ϕ is again an isomorphism. (Hint: Consider the images of ϕ n for n ∈ N.) So far we have mostly considered chain conditions for general modules. For the rest of this chapter we now want to specialize to the case of rings. In this case we can obtain stronger results, however we will also see that this is where the Noetherian and Artinian conditions begin to diverge drastically. So let us consider these two conditions in turn, starting with the more important case of Noetherian rings. The one central result on Noetherian rings is Hilbert's Basis Theorem, which implies that "most rings that you will meet in practice are Noetherian".

Lemma . Let N ⊂ M be a R-submodule. Then M is Noetherian (resp. Artinian) if and only if both N and M/N are Noetherian.

Proof. We do the proof of the Noetherian property. The Artinian property is proved in the same way

There are two statements to prove now. Let first us assume that M is Noetherian, and show that N and M/N are also Noetherian. A chain of submodules in N is at the same time a chain of submodules in M. Since the latter chains stabilize, N is Noetherian. Now take a chain of submodules in M/N. This chain gives us a chain of submodules in M, and it must stablize, so must the original chain.

Now let us assume that both N and M/N are Noetherian. To show that M is Noetherian, consider a chain of submodules in M:

$$M1 \subset M2 \subset \cdots \subset M$$

and this gives rise to two other chains:

$$M1 \cap N \subset M2 \cap N \subset \cdots \subset N$$

And $(M1 + N)/N \subset (M2 + N)/N \subset \cdots \subset M/N.$

Both of the new chains stabilize since N and M/N are Noetherian: for i ≥ n we have

$$Mi \cap N = Mi+1 \cap N$$

$$(Mi + N)/N = (Mi+1 + N)/N$$

Note that by from the Third Isomorphism Theorem we have a natural isomorphism

$$(Mi + N)/N \text{ ' } Mi/(Mi \cap N).$$

Now comparing the two adjacent submodules Mi , Mi+1 for i ≥ n we see that they have the same submodule

$$K := Mi \cap N = Mi+1 \cap N$$

such that the quotient modules Mi/K, Mi+1/K are also the same as submodules in M/K. This forces Mi = Mi+1.

14.6 SUMMARY

We study in this unit about Noethrian And Artinian Module and its properties also study some examples of Noetgrian And Artinian Module. We study sub module of Noethrian and Artinian Module. We study R-

Notes

Module ans its examples with proposition. We study left and right module over module.

1. The following conditions are equivalent for a left R-module:

   a) M is Noetherian.

   b) Every submodule N of M is finitely generated (i.e. can be written as $Rm_1 + \cdots + Rm_k$ for some $m_1, \ldots, m_k \in N$).

   c) Every collection of submodules of M has a maximal element.

2. Hilbert's Basis Theorem is a result concerning Noetherian rings. It states that if A is a (not necessarily commutative) Noetherian ring, then the ring of polynomials $A[x_1, x_2, \ldots, x_n]$ is also a Noetherian ring.

3. For any strictly inductively ordered set A and any increasing function $f : A \to A$, there exists an element x_0 of A such that $x_0 = f(x_0)$.

4. *For an* R-*module* M*, the following are equivalent:*
   any non-empty collection Σ of submodules of M has a minimal element N (i.e. N ∈ Σ, and whenever M' ∈ Σ we have M' ⊇ N);
   for any decreasing sequence $M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ *of submodules of M, there is an n such that* $M_n = M_{n+1} = M_{n+2} = \ldots$.

5. *Let M be a noetherian and artinian module. The following are equivalent for a module map f : M → M.*
   f is bijective;
   f is injective;

   f is surjective.

6. Let N ⊂ M be a R-submodule. Then M is Noetherian (resp. Artinian) if and only if both N and M/N are Noetherian.

14.7 KEYWORD

Krull : What can you do some things in life are just so

Generated : produce (a set or sequence of items) by performing specified mathematical or logical operations on an initial set

Trivial : Denoting a subgroup that either contains only the identity element or is identical with the given group

14.8 QUESTIONS FOR REVIEW

Q. 1 Let R be a Noetherian ring. Show:

(a) If R is an integral domain, every non-zero non-unit a ∈ R can be written as a product of irreducible elements of R.

(b) For any ideal I ER there is an n ∈ N such that (√ I) n ⊂ I.

Q. 2 Let S be a multiplicatively closed subset of a ring R. If R is Noetherian (resp. Artinian), show that the localization S −1R is also Noetherian (resp. Artinian).

Q. 3 Prove for any R-module M:

(a) If M is Noetherian then R/annM is Noetherian as well.

(b) If M is finitely generated and Artinian, then M is also Noetherian

Q. 4 For any ring R we have: R is Artinian ⇔ R is Noetherian and every prime ideal of R is maximal.

Q. 5 Let R be an Artinian ring.

(a) There are (not necessarily distinct) maximal ideals P1,...,Pn ER such that P1 · ··· ·Pn = 0.

(b) R has only finitely many prime ideals, all of them are maximal, and occur among the P1,...,Pn in (a).

Q. 6 Any finitely generated algebra over a Noetherian ring is itself a Noetherian ring.

Q. 7 Let M be an R-module, and let $\phi : M \to M$ be an R-module homomorphism. If M is Noetherian (hence finitely generated) and ϕ is surjective.

Q. 8 An R-module M is of finite length if and only if it is both Noetherian and Artinian.

Q. 9 Let M and N be R-modules.

(a) The direct sum $M \oplus N$ is Noetherian if and only if M and N are Noetherian.

(b) If R is Noetherian and M is finitely generated, then M is also Noetherian.

The same statements also hold with "Noetherian" replaced by "Artinian".

Q. 10 Let N be a submodule of an R-module M.

(a) M is Noetherian if and only if N and M/N are Noetherian.

(b) M is Artinian if and only if N and M/N are Artinian.

Q. 11 (Equivalent conditions for Noetherian and Artinian modules). Let M be an R-module.

(a) M is Noetherian if and only if every non-empty family of submodules of M has a maximal element.

(b) M is Artinian if and only if every non-empty family of submodules of M has a minimal element.

(c) M is Noetherian if and only if every submodule of M is finitely generated.

Q. 12 Any field K is trivially Noetherian and Artinian as it has only the trivial ideals (0) and K. More generally, a K-vector space V is Noetherian if and only if it is Artinian if and only if it is finite-dimensional.

14.9 SUGGESTION READING AND REFERENCES

1. *Atiyah, M.F.; Macdonald, I.G. (1969). "Chapter 6. Chain conditions; Chapter 8. Artin rings". Introduction to Commutative Algebra. Westview Press. ISBN 978-0-201-40751-8.*
2. *Cohn, P.M. (1997). "Cyclic Artinian Modules Without a Composition Series". J. London Math. Soc. Series 2.* ***55*** *(2): 231–235. doi:10.1112/S0024610797004912. MR 1438626.*
3. *Hartley, B. (1977). "Uncountable Artinian modules and uncountable soluble groups satisfying Min-n". Proc. London Math. Soc. Series 3.* ***35*** *(1): 55–75. doi:10.1112/plms/s3-35.1.55. MR 0442091.*
4. *Lam, T.Y. (2001). "Chapter 1. Wedderburn-Artin theory". A First Course in Noncommutative Rings. Springer Verlag. ISBN 978-0-387-95325-0.*
5. Eisenbud *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1995.
7. C. Faith, "Algebra: rings, modules, and categories" , **1** , Springer (1973)
9. C. Faith, "Algebra" , **II. Ring theory** , Springer (1976)
10. Lang, S. *Algebra*, *Revised Third Edition.* Springer (2002), ISBN 0-387-95385-X.

14.10 ANSWER TO CHECK YOUR PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 1.4

Q 2 Check in Section 1.3

Check in Progress-II

Answer Q. 1 Check in Section 4

Q 2 Check in Section 3