DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTER OF SCIENCE-MATHEMATICS
SEMESTER -II

THEORY OF RINGS AND MODULES

DEMATH-2 ELEC-4

BLOCK-1

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 -I

BLOCK-II

BLOCK-1 THEORY OF RING AND MODULE

Introduction to the block-I

Unit 1 NOETHERIAN AND ARTINIAN RINGS: In this unit we discuss about primary decomposition and module over ring also deal with Noetherian and Artinian Ring Basics

Unit 2 HILBERT BASIS THEOREM : This unit deals with Basis theorem and its properties.

Unit 3 NOETHERIAN RING : This Unit deals with Noetherian ring and its example.

Unit 4 MODULE, SUB-MODULE, QUOTIENT MODULE : This unit deals with Module over ring, Sun Module and Quotient Module Over Ring and its properties.

Unit 5 HOMOMORPHISM and ISOMORPHISM : This unit deals with Homomorphism and Isomorphism also deals with its properties.

Unit 6 EXACT SEQUENCE, FOUR AND FIVE LEMMA : This Unit deals with exact sequence and four , five lemma theorem with state and prove.

Unit 7 DIRECT SUM AND PRODUCT OF MODULE : This Unit Deals with direct sum and product of module and its example.

UNIT 1: NOETHERIAN AND ARTINIAN RINGS

STRUCTURE

1.0 OBJECTIVE

Learn about non-commutative rings, it is necessary to distinguish between three very similar concepts:

- A ring is left-Noetherian if it satisfies the ascending chain condition on left ideals.
- A ring is right-Noetherian if it satisfies the ascending chain condition on right ideals.
- A ring is Noetherian if it is both left- and right-Noetherian.

For commutative rings, all three concepts coincide, but in general they are different. There are rings that are left-Noetherian and not right-Noetherian, and vice versa.

There are other, equivalent, definitions for a ring *R* to be left-Noetherian:

- Every left ideal *I* in *R* is finitely generated, i.e. there exist elements a_1, ..., a_n in *I* such that $I = Ra_1 + ... + Ra_n$.
- Every non-empty set of left ideals of *R*, partially ordered by inclusion, has a maximal element with respect to set inclusion.

Similar results hold for right-Noetherian rings.

For a commutative ring to be Noetherian it suffices that every prime ideal of the ring is finitely generated.

1.1 INTRODUCTION: NOETHERIAN RINGS BASICS

Definition. A ring A is noetherian, respectively artinian, if it is noetherian, respectively artinian, considered as an A-module. In other words, the ring A is noetherian, respectively artinian, if every chain a1 ⊆ a2 ⊆ · · · of ideal ai in A is stable, respectively if every chain a1 ⊇ a2 ⊇ · · · of ideals ai in A is stable.

The area of abstract algebra known as ring theory, a Noetherian ring is a ring that satisfies the ascending chain condition on left and right ideals, which means there is no infinite ascending sequence of left (or right) ideals; that is, given any chain of left (or right) ideals,

$$I_1 \subseteq \cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$$

there exists an *n* such that:

$$I_n = I_{n+1} = \cdots$$

Noetherian rings are named after Emmy Noether.

The notion of a Noetherian ring is of fundamental importance in both commutative and noncommutative ring theory, due to the role it plays in simplifying the ideal structure of a ring. For instance, the ring of integers and the polynomial ring over a field are both Noetherian rings, and consequently, such theorems as the Lasker–Noether theorem, the Krull intersection theorem, and Hilbert's basis theorem hold for them. Furthermore, if a ring is Noetherian, then it satisfies the descending chain condition on *prime ideals*. This property suggests a deep theory of dimension for Noetherian rings beginning with the notion of the Krull dimension.

1.1.1 Properties

- If R is a Noetherian ring, then $R[X]$ is Noetherian by the Hilbert basis theorem. By induction, $R[X_1, ..., X_n]$ is a Noetherian ring. Also, $R[[X]]$, the power series ring is a Noetherian ring.
- If R is a Noetherian ring and I is a two-sided ideal, then the factor ring R/I is also Noetherian. Stated differently, the image of any surjective ring homomorphism of a Noetherian ring is Noetherian.
- Every finitely-generated commutative algebra over a commutative Noetherian ring is Noetherian. (This follows from the two previous properties.)
- A ring R is left-Noetherian if and only if every finitely generated left R-module is a Noetherian module.
- Every localization of a commutative Noetherian ring is Noetherian.
- A consequence of the Akizuki-Hopkins-Levitzki Theorem is that every left Artinian ring is left *Noetherian. Another consequence is that a left Artinian ring is right Noetherian if and only if right* Artinian. The analogous statements with "right" and "left" interchanged are also true.
- A left Noetherian ring is left coherent and a left Noetherian domain is a left Ore domain.

- A ring is (left/right) Noetherian if and only if every direct sum of injective (left/right) modules is injective. Every injective module can be decomposed as direct sum of indecomposable injective modules.
- In a commutative Noetherian ring, there are only finitely many minimal prime ideals.
- In a commutative Noetherian domain *R*, every element can be factorized into irreducible elements. Thus, if, in addition, irreducible elements are prime elements, then *R* is a unique factorization domain.

Examples

- Any field, including fields of rational numbers, real numbers, and complex numbers, is Noetherian. (A field only has two ideals — itself and (0).)
- Any principal ideal ring, such as the integers, is Noetherian since every ideal is generated by a single element. This includes principal ideal domains and Euclidean domains.
- A Dedekind domain (e.g., rings of integers) is Noetherian since every ideal is generated by at most two elements. The "Noetherian" follows from the Krull–Akizuki theorem. The bounds on the number of the generators is a corollary of the Forster–Swan theorem (or basic ring theory).
- The coordinate ring of an affine variety is a Noetherian ring, as a consequence of the Hilbert basis theorem.
- The enveloping algebra *U* of a finite-dimensional Lie algebra g is a both left and right Noetherian ring; this follows from the fact that the associated graded ring of *U* is a quotient of $Sym(g)$, which is a polynomial ring over a field; thus, Noetherian. For the same reason, the Weyl algebra, and more general rings of differential operators, are Noetherian.
- The ring of polynomials in finitely-many variables over the integers or a field.

  Rings that are not Noetherian tend to be (in some sense) very large. Here are some examples of non-Noetherian rings:

- The ring of polynomials in infinitely-many variables, X_1, X_2, X_3, etc. The sequence of ideals (X_1), (X_1, X_2), (X_1, X_2, X_3), etc. is ascending, and does not terminate.
- The ring of algebraic integers is not Noetherian. For example, it contains the infinite ascending chain of principal ideals: (2), $(2^{1/2})$, $(2^{1/4})$, $(2^{1/8})$, ...
- The ring of continuous functions from the real numbers to the real numbers is not Noetherian: Let I_n be the ideal of all continuous functions f such that $f(x) = 0$ for all $x \geq n$. The sequence of ideals I_0, I_1, I_2, etc., is an ascending chain that does not terminate.
- The ring of stable homotopy groups of spheres is not Noetherian.

  However, a non-Noetherian ring can be a subring of a Noetherian ring. Since any integral domain is a subring of a field, any integral domain that is not Noetherian provides an example. To give a less trivial example,

- The ring of rational functions generated by x and y/x^n over a field k is a subring of the field $k(x,y)$ in only two variables.

  Indeed, there are rings that are right Noetherian, but not left Noetherian, so that one must be careful in measuring the "size" of a ring this way. For example, if L is a subgroup of Q^2 isomorphic to Z, let R be the ring of homomorphisms f from Q^2 to itself satisfying $f(L) \subset L$. Choosing a basis, we can describe the same ring R as

$$R = \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix} \mid \alpha \in \mathbb{Z}, \beta \in \mathbb{Q}, \gamma \in \mathbb{Q} \right\}$$

This ring is right Noetherian, but not left Noetherian; the subset $I \subset R$ consisting of elements with $\alpha=0$ and $\gamma=0$ is a left ideal that is not finitely generated as a left R-module.

If R is a commutative subring of a left Noetherian ring S, and S is finitely generated as a left R-module, then R is Noetherian. (In the special case when S is commutative, this is known as Eakin's theorem.) However this is not true if R is not commutative: the ring R of the previous paragraph

is a subring of the left Noetherian ring $S = \mathrm{Hom}(Q^2, Q^2)$, and S is finitely generated as a left R-module, but R is not left Noetherian.

A unique factorization domain is not necessarily a Noetherian ring. It does satisfy a weaker condition: the ascending chain condition on principal ideals.

A valuation ring is not Noetherian unless it is a principal ideal domain. It gives an example of a ring that arises naturally in algebraic geometry but is not Noetherian.

1.1.2 Primary Decomposition

In the ring Z of integers, an arbitrary ideal is of the form (n) for some integer n (where (n) denotes the set of all integer multiples of n). If n is non-zero, and is neither 1 nor −1, by the fundamental theorem of arithmetic, there exist primes p_i, and positive integers e_i, with $n = \prod_i {p_i}^{e_i}$. In this case, the ideal (n) may be written as the intersection of the ideals $({p_i}^{e_i})$; that is, $(n) = \bigcap_i ({p_i}^{e_i})$. This is referred to as a *primary decomposition* of the ideal (n).

In general, an ideal Q of a ring is said to be *primary* if Q is proper and whenever $xy \in Q$, either $x \in Q$ or $y^n \in Q$ for some positive integer n. In Z, the primary ideals are precisely the ideals of the form (p^e) where p is prime and e is a positive integer. Thus, a primary decomposition of (n) corresponds to representing (n) as the intersection of finitely many primary ideals.

Since the fundamental theorem of arithmetic applied to a non-zero integer n that is neither 1 nor −1 also asserts uniqueness of the representation $n = \prod_i {p_i}^{e_i}$ for p_i prime and e_i positive, a primary decomposition of (n) is essentially *unique*.

For all of the above reasons, the following theorem, referred to as the *Lasker–Noether theorem*, may be seen as a certain generalization of the fundamental theorem of arithmetic:

Lasker-Noether Theorem. Let R be a commutative Noetherian ring and let I be an ideal of R. Then I may be written as the intersection of finitely many primary ideals with distinct radicals; that is:

$$I = \bigcap_{i=1}^{k} Q_i$$

with Q_i primary for all i and $\text{Rad}(Q_i) \neq \text{Rad}(Q_j)$ for $i \neq j$. Furthermore, if:

$$I = \bigcap_{i=1}^{k} P_i$$

is decomposition of I with $\text{Rad}(P_i) \neq \text{Rad}(P_j)$ for $i \neq j$, and both decompositions of I are *irredundant* (meaning that no proper subset of either $\{Q_1, ..., Q_t\}$ or $\{P_1, ..., P_k\}$ yields an intersection equal to I), $t = k$ and (after possibly renumbering the Q_i) $\text{Rad}(Q_i) = \text{Rad}(P_i)$ for all i.

For any primary decomposition of I, the set of all radicals, that is, the set $\{\text{Rad}(Q_1), ..., \text{Rad}(Q_t)\}$ remains the same by the Lasker–Noether theorem. In fact, it turns out that (for a Noetherian ring) the set is precisely the assassinator of the module R/I; that is, the set of all annihilators of R/I (viewed as a module over R) that are prime.

1.1.3 Krull–Akizuki Theorem

In algebra, the Krull–Akizuki theorem states the following: let A be a one-dimensional reduced noetherian ring, K its total ring of fractions. If B is a subring of a finite extension L of K containing A and is not a field, then B is a one-dimensional noetherian ring. Furthermore, for every nonzero ideal I of B, $\boldsymbol{B/1}$ is finite over A.

Note that the theorem does not say that B is finite over A. The theorem does not extend to higher dimension. One important consequence of the theorem is that the integral closure of a Dedekind domain A in a finite extension of the field of fractions of A is again a Dedekind domain. This consequence does generalize to a higher dimension: the Mori–Nagata theorem states that the integral closure of a noetherian domain is a Krull domain.

Proof

Here, we give a proof when $\boldsymbol{L = K}$. Let $\boldsymbol{p_i}$ be minimal prime ideals of A; there are finitely many of them. Let $\boldsymbol{K_i}$ be the field of fractions of $\boldsymbol{A/p_i}$ and $\boldsymbol{I_i}$ the kernel of the natural map $\boldsymbol{B \to K \to K_i}$. Then we have:

$$\boldsymbol{A/p_i \subset B/I_i \subset K_i}.$$

Now, if the theorem holds when *A* is a domain, then this implies that *B* is a one-dimensional noetherian domain since each $\boldsymbol{B/I_i}$ is and since $\boldsymbol{B = \prod B/I_i}$. Hence, we reduced the proof to the case *A* is a domain. Let $\boldsymbol{0 \neq I \subset B}$ be an ideal and let *a* be a nonzero element in the nonzero ideal $\boldsymbol{I \cap A}$. Set $\boldsymbol{I_n = a^n B \cap A + aA}$. Since $\boldsymbol{A/aA}$ is a zero-dim noetherian ring; thus, artinian, there is an *l* such that $\boldsymbol{I_n = I_1}$ for all $\boldsymbol{n \geq 1}$. We claim

$$\boldsymbol{a^l B \subset a^{l+1} B + A}$$

Since it suffices to establish the inclusion locally, we may assume *A* is a local ring with the maximal ideal $\boldsymbol{m}$. Let *x* be a nonzero element in *B*. Then, since *A* is noetherian, there is an *n* such that $\boldsymbol{m^{n+1} \subset x^{-1} A}$ and so $\boldsymbol{a^{n+1} x \in a^{n+1} B \cap A \subset I_{n+2}}$. Thus,

$$\boldsymbol{a^n x \in a^{n+1} B \cap A + A}$$

Now, assume *n* is a minimum integer such that $\boldsymbol{n \geq l}$ and the last inclusion holds. If $\boldsymbol{n > l}$, then we easily see that $\boldsymbol{a^n x \in I_{n+1}}$. But then the above inclusion holds for $\boldsymbol{n - 1}$, contradiction. Hence, we have $\boldsymbol{n = l}$ and this establishes the claim. It now follows:

$$\boldsymbol{B/aB \simeq a^l B/a^{l+1} B \subset (a^{l+1} B + A)/a^{l+1} B \simeq A/a^{l+1} B \cap A}$$

Hence, $\boldsymbol{B/aB}$ has finite length as *A*-module. In particular, the image of *I* there is finitely generated and so *I* is finitely generated. Finally, the above shows that $\boldsymbol{B/aB}$ has zero dimension and so *B* has dimension one. □

1.2 NOETHERIAN SCHEME

In algebraic geometry, a noetherian scheme is a scheme that admits a finite covering by open affine subsets $\boldsymbol{Spec A_i}$, $\boldsymbol{A_i}$ noetherian rings. More generally, a scheme is locally noetherian if it is covered by spectra of noetherian rings. Thus, a scheme is noetherian if and only if it is locally noetherian and quasi-compact. As with noetherian rings, the concept is named after Emmy Noether.

It can be shown that, in a locally noetherian scheme, if $\boldsymbol{Spec A}$ is an open affine subset, then *A* is a noetherian ring. In particular, $\boldsymbol{Spec A}$ is a

noetherian scheme if and only if *A* is a noetherian ring. Let *X* be a locally noetherian scheme. Then the local rings $\boldsymbol{O_{X,x}}$ are noetherian rings.

A noetherian scheme is a noetherian topological space. But the converse is false in general; consider, for example, the spectrum of a non-noetherian valuation ring.

The definitions extend to formal schemes.

1.2.1 Artinian Ring

In abstract algebra, an Artinian ring (sometimes Artin ring) is a ring that satisfies the descending chain condition on ideals; that is, there is no infinite descending sequence of ideals. Artinian rings are named after Emil Artin, who first discovered that the descending chain condition for ideals simultaneously generalizes finite rings and rings that are finite-dimensional vector spaces over fields. The definition of Artinian rings may be restated by interchanging the descending chain condition with an equivalent notion: the minimum condition.

A ring is left Artinian if it satisfies the descending chain condition on left ideals, right Artinian if it satisfies the descending chain condition on right ideals, and Artinian or two-sided Artinian if it is both left and right Artinian. For commutative rings the left and right definitions coincide, but in general they are distinct from each other.

The Artin–Wedderburn theorem characterizes all simple Artinian rings as the ring of matrices over a division ring. This implies that a simple ring is left Artinian if and only if it is right Artinian.

The same definition and terminology can be applied to modules, with ideals replaced by submodules.

Although the descending chain condition appears dual to the ascending chain condition, in rings it is in fact the stronger condition. Specifically, a consequence of the Akizuki–Hopkins–Levitzki theorem is that a left (resp. right) Artinian ring is automatically a left (resp. right) Noetherian ring. This is not true for general modules; that is, an Artinian module need not be a Noetherian module

Examples

- An integral domain is Artinian if and only if it is a field.
- A ring with finitely many, say left, ideals is left Artinian. In particular, a finite ring (e.g., Z/nZ) is left and right Artinian.
- Let *k* be a field. Then $\boldsymbol{k[t]/t\text{^}(n)}$ is Artinian for every positive integer *n*.
- Similarly, $\boldsymbol{k[x,y]/(x^2,y^3,xy^2) = k \oplus k.x \oplus k.y \oplus k.xy \oplus k.y^2}$) is an Artinian ring with maximal ideal $(\boldsymbol{x,y})$
- If *I* is a nonzero ideal of a Dedekind domain *A*, then $\boldsymbol{A/I}$ is a principal Artinian ring.
- For each $\boldsymbol{n \geq 1}$, the full matrix ring $\boldsymbol{M_n(R)}$ over a left Artinian (resp. left Noetherian) ring *R* is left Artinian (resp. left Noetherian).

  The ring of integers **Z** is a Noetherian ring but is not Artinian.

1.2.2 Modules Over Artinian Rings

Let *M* be a left module over a left Artinian ring. Then the following are equivalent (Hopkins' theorem):

(i) *M* is finitely generated

(ii) *M* has finite length (i.e., has composition series,

(iii) *M* is Noetherian,

(iv) *M* is Artinian

Commutative Artinian Rings

Let *A* be a commutative Noetherian ring with unity. Then the following are equivalent.

- *A* is Artinian.
- *A* is a finite product of commutative Artinian local rings.
- *A* / nil(*A*) is a semisimple ring, where nil(*A*) is the nilradical of *A*.
- Every finitely generated module over *A* has finite length.
- *A* has Krull dimension zero. (In particular, the nilradical is the Jacobson radical since prime ideals are maximal.)
- $\boldsymbol{SpecA}$ is finite and discrete.

- $\boldsymbol{SpecA}$ is discrete.

Let *k* be a field and *A* finitely generated *k*-algebra. Then *A* is Artinian if and only if *A* is finitely generated as *k*-module.

An Artinian local ring is complete. A quotient and localization of an Artinian ring is Artinian.

1.2.3 Simple Artinian Ring

A simple Artinian ring *A* is a matrix ring over a division ring.
Indeed, let *I* be a minimal (nonzero) right ideal of *A*. Then, since $\boldsymbol{AI}$ is a two-sided ideal, $\boldsymbol{AI} = \boldsymbol{A}$ since *A* is simple. Thus, we can choose $\boldsymbol{a_i \epsilon A}$ so that $\boldsymbol{1 \epsilon a_1 I} + \cdots + \boldsymbol{a_k I}$. Assume *k* is minimal with respect that property. Consider the map of right *A*-modules:

$$\begin{cases} \boldsymbol{I^{\oplus k}} \to \boldsymbol{A}, \\ (\boldsymbol{y_1}, \cdots \boldsymbol{y_k}) \longmapsto \boldsymbol{a_1 y_1} + \cdots + \boldsymbol{a_k y_k} \end{cases}$$

It is surjective. If it is not injective, then, say, $\boldsymbol{a_1 y_1} = \boldsymbol{a_2 y_2} + \cdots + \boldsymbol{a_k y_k}$ with nonzero $\boldsymbol{y_1}$. Then, by the minimality of *I*, we have: $\boldsymbol{y_1 A} = \boldsymbol{I}$. It follows:

$$\boldsymbol{a_1 I} = \boldsymbol{a_1 y_1 A} \subset \boldsymbol{a_2 I} + \cdots + \boldsymbol{a_k I},$$

which contradicts the minimality of *k*. Hence, $\boldsymbol{I^{\oplus k}} \simeq \boldsymbol{A}$, and thus $\boldsymbol{A} \simeq \boldsymbol{End_A(A)} \simeq \boldsymbol{M_k(End_A(I)}$

Counter Example

The article presently claims that *R* is Artinian iff *R*/rad(*R*) is a direct product of finitely many fields. This is false; to construct a counterexample, let *k* be a field, and let $k[x_1, x_2, x_3, ...]$ be a polynomial ring over *k* in infinitely many indeterminates. Let *J* be the ideal $(x_1) + (x_1, x_2)^2 + (x_1, x_2, x_3)^3 + ...$, and let $R = k[x_1, x_2, x_3, ...]/J$.

R is clearly not Noetherian: (x_1), (x_1, x_2), (x_1, x_2, x_3), ... is an infinite ascending chain of ideals. Nor is *R* Artinian: (x_1), (x_1x_2), $(x_1x_2x_3)$, ... is an infinite descending chain of ideals. But *R*/rad(*R*) is *k*: Every monomial in $x_1, x_2, ...$ is nilpotent by the definition of *J*, hence every polynomial is nilpotent, and so $\text{rad}(R) = (x_1, x_2, x_3, ...)$.

1. Prove that every prime ideal in *A* is maximal

2. Prove that A has only finitely many prime ideals
3. Prove that rad(A) is nilpotent (obviously it contains only nilpotent elements; show that rad(A)^k = 0 for some k)
4. Prove the following lemma: if M_1, ..., M_n are maximal ideals (in some ring R) whose product is zero, then R is Noetherian if and only if it is Artinian (look at the successive quotients in the chain of partial products of the M_i).
5. Thus A Artinian implies A Noetherian and A / rad(A) is a product of finitely many fields. Conversely. the lemma shows that such a ring is automatically Artinian.

1.2.4 Artin Algebra

In algebra, an Artin algebra is an algebra Λ over a commutative Artin ring R that is a finitely generated R-module. They are named after Emil Artin.

Every Artin algebra is an Artin ring.

Dual and transpose

There are several different dualities taking finitely generated modules over Λ to modules over the opposite algebra Λ^{op}.

- If M is a left Λ module then the right Λ-module M^* is defined to be $\mathrm{Hom}_\Lambda(M,\Lambda)$.
- The dual $D(M)$ of a left Λ-module M is the right Λ-module $D(M) = \mathrm{Hom}_R(M,J)$, where J is the dualizing module of R, equal to the sum of the injective envelopes of the non-isomorphic simple R-modules or equivalently the injective envelope of R/rad R. The dual of a left module over Λ does not depend on the choice of R (up to isomorphism).
- The transpose Tr(M) of a left Λ-module M is a right Λ-module defined to be the cokernel of the map $Q^* \to P^*$, where $P \to Q \to M \to 0$ is a minimal projective presentation of M.

Artinian ideal

In abstract algebra, an Artinian ideal, named after Emil Artin, is encountered in ring theory, in particular, with polynomial rings.

Given a polynomial ring $R = k[X_1, \ldots X_n]$ where k is some field, an Artinian ideal is an ideal I in R for which the Krull dimension of the quotient ring R/I is 0. Also, less precisely, one can think of an Artinian ideal as one that has at least each indeterminate in R raised to a power greater than 0 as a generator.

If an ideal is not Artinian, one can take the Artinian closure of it as follows. First, take the least common multiple of the generators of the ideal. Second, add to the generating set of the ideal each indeterminate of the LCM with its power increased by 1 if the power is not 0 to begin with. An example is below.

Examples

Let $\boldsymbol{R = k[x, y, z]}$, and let $\boldsymbol{I = (x^2, y^5, z^4)}$; $\boldsymbol{J = (x^3, y^2, z^6, x^2yz^4, yz^3)}$ and $\boldsymbol{K = (x^3, y^4, x^2z^7)}$. Here, $\boldsymbol{I}$ and $\boldsymbol{J}$ are Artinian ideals, but $\boldsymbol{K}$ is not because in $\boldsymbol{K}$, the indeterminate $\boldsymbol{z}$ does not appear alone to a power as a generator.

To take the Artinian closure of $\boldsymbol{K}$, $\boldsymbol{\widehat{K}}$, we find the LCM of the generators of $\boldsymbol{K}$, which is $\boldsymbol{x^3, y^4, z^7}$. Then, we add the generators $\boldsymbol{x^4}$, $\boldsymbol{y^5}$, and $\boldsymbol{z^8}$ to $\boldsymbol{K}$, and reduce. Thus, we have , $\boldsymbol{\widehat{K} = x^3, y^4, z^8, x^2z^7}$ which is Artinian.

Check In Progress-I

Q. 1 Define Artin Algebra.

Solution : . . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Q. 2 Define Modulus over Artin Ring.

Solution : . . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

1.3 SERIAL MODULE

In abstract algebra, a uniserial module *M* is a module over a ring *R*, whose submodules are totally ordered by inclusion. This means simply that for any two submodules N_1 and N_2 of *M*, either $\boldsymbol{N_1 \subseteq N_2}$ or $\boldsymbol{N_2 \subseteq N_1}$. A module is called a serial module if it is a direct sum of uniserial modules. A ring *R* is called a right uniserial ring if it is uniserial as a right module over itself, and likewise called a right serial ring if it is a right serial module over itself. Left uniserial and left serial rings are defined in an analogous way, and are in general distinct from their right counterparts.

An easy motivational example is the quotient ring $\boldsymbol{Z/nZ}$ for any integer $\boldsymbol{n > 1}$. This ring is always serial, and is uniserial when *n* is a prime power.

The term *uniserial* has been used differently from the above definition: for clarification .

A partial alphabetical list of important contributors to the theory of serial rings includes the mathematicians Keizo Asano, I. S. Cohen, P.M. Cohn, Yu. Drozd, D. Eisenbud, A. Facchini, A.W. Goldie, Phillip Griffith, I. Kaplansky, V.V Kirichenko, G. Köthe, H. Kuppisch, I. Murase, T. Nakayama, P. Příhoda, G. Puninski, and R. Warfield.

Following the common ring theoretic convention, if a left/right dependent condition is given without mention of a side (for example, uniserial, serial, Artinian, Noetherian) then it is assumed the condition holds on both the left and right. Unless otherwise specified, each ring in this article is a ring with unity, and each module is unital

1.3.1 Properties of Uniserial And Serial Rings And Modules

It is immediate that in a uniserial *R*-module *M*, all submodules except *M* and 0 are simultaneously essential and superfluous. If *M* has a maximal submodule, then *M* is a local module. *M* is also clearly a uniform moduleand thus is directly indecomposable. It is also easy to see that every finitely generated submodule of *M* can be generated by a single element, and so *M* is a Bézout module.

It is known that the endomorphism ring $End_R(M)$ is a semilocal ring which is very close to a local ring in the sense that $End_R(M)$ has at most two maximal right ideals. If *M* is required to be Artinian or Noetherian, then $End_R(M)$ is a local ring.

Since rings with unity always have a maximal right ideal, a right uniserial ring is necessarily local. As noted before, a finitely generated right ideal can be generated by a single element, and so right uniserial rings are right Bézout rings. A right serial ring *R* necessarily factors in the form $\boldsymbol{R = \oplus_{i=1}^{n} e_i R}$ where each e_i is an idempotent element and e_iR is a local, uniserial module. This indicates that *R* is also a semiperfect ring, which is a stronger condition than being a semilocal ring.

Köthe showed that the modules of Artinian principal ideal rings (which are a special case of serial rings) are direct sums of cyclic submodules. Later, Cohen and Kaplansky determined that a commutative ring *R* has this property for its modules if and only if *R* is an Artinian principal ideal ring. Nakayama showed that Artinian serial rings have this property on their modules, and that the converse is not true

The most general result, perhaps, on the modules of a serial ring is attributed to Drozd and Warfield: it states that every finitely presented module over a serial ring is a direct sum of cyclic uniserial submodules (and hence is serial). If additionally the ring is assumed to be Noetherian, the finitely presented and finitely generated modules coincide, and so all finitely generated modules are serial.

Being right serial is preserved under direct products of rings and modules, and preserved under quotients of rings. Being uniserial is preserved for quotients of rings and modules, but never for products. A

direct summand of a serial module is not necessarily serial, as was proved by Puninski, but direct summands of *finite* direct sums of uniserial modules are serial modules

Examples

Any simple module is trivially uniserial, and likewise semisimple modules are serial modules.

Many examples of serial rings can be gleaned from the structure sections above. Every valuation ring is a uniserial ring, and all Artinian principal ideal rings are serial rings, as is illustrated by semisimple rings.

More exotic examples include the upper triangular matrices over a division ring $T_n(D)$, and the group ring $\mathbb{F}[\boldsymbol{G}]$ for some finite field of prime characteristic *p* and group *G* having a cyclic normal *p*-Sylow subgroup.

Structure

This section will deal mainly with Noetherian serial rings and their subclass, Artinian serial rings. In general, rings are first broken down into indecomposable rings. Once the structure of these rings are known, the decomposable rings are direct products of the indecomposable ones. Also, for semiperfect rings such as serial rings, the basic ring is Morita equivalent to the original ring. Thus if *R* is a serial ring with basic ring *B*, and the structure of *B* is known, the theory of Morita equivalence gives that $\boldsymbol{R} \cong \boldsymbol{End_B(P)}$ where *P* is some finitely generated progenerator *B*. This is why the results are phrased in terms of indecomposable, basic rings.

In 1975, Kirichenko and Warfield independently and simultaneously published analyses of the structure of Noetherian, non-Artinian serial rings. The results were the same however the methods they used were very different from each other. The study
of hereditary, Noetherian, prime rings, as well as quivers defined on serial rings were important tools. The core result states that a right Noetherian, non-Artinian, basic, indecomposable serial ring can be described as a type of matrix ring over a Noetherian, uniserial domain *V*, whose Jacobson radical J(*V*) is nonzero. This matrix ring is a subring of

$M_n(V)$ for some *n*, and consists of matrices with entries from *V* on and above the diagonal, and entries from J(*V*) below.

Artinian serial ring structure is classified in cases depending on the quiver structure. It turns out that the quiver structure for a basic, indecomposable, Artinian serial ring is always a circle or a line. In the case of the line quiver, the ring is isomorphic to the upper triangular matrices over a division ring (note the similarity to the structure of Noetherian serial rings in the preceding paragraph). A complete description of structure in the case of a circle quiver is beyond the scope of this article, but the complete description can be found in (Puninski 2001). To paraphrase the result as it appears there: A basic Artinian serial ring whose quiver is a circle is a homomorphic image of a "blow-up" of a basic, indecomposable, serial quasi-Frobenius ring.

1.3.2 A Decomposition Uniqueness Property

Two modules *U* and *V* are said to have the same monogeny class, denoted $[U]_m=[V]_m$, if there exists a monomorphism $\boldsymbol{U \to V}$ and a monomorphism $\boldsymbol{V \to U}$. The dual notion can be defined: the modules are said to have the same epigeny class, denoted $[\boldsymbol{U}]_{\boldsymbol{e}}=[\boldsymbol{V}]_{\boldsymbol{e}}$, if there exists an epimorphism $\boldsymbol{U \to V}$ and an epimorphism $\boldsymbol{V \to U}$.

The following weak form of the Krull-Schmidt theorem holds.
Let $U_1,\dots U_n$, $V_1, \dots, V_t$ be $n+t$ non-zero uniserial right modules over a ring *R*. Then the direct sums $\boldsymbol{U_1 \oplus \cdots \oplus U_n}$ and $\boldsymbol{V_1 \oplus \cdots \oplus V_t}$ are isomorphic *R*-modules if and only if $n=t$ and there exist two permutations $\boldsymbol{\sigma}$ and $\boldsymbol{\tau}$ of $1,2,\dots,n$ such that $[\boldsymbol{U_i}]_{\boldsymbol{m}}=\left[\boldsymbol{V_{\sigma(i)}}\right]_{\boldsymbol{m}}$ and $[\boldsymbol{U_i}]_{\boldsymbol{e}}=\left[\boldsymbol{V_{\tau(i)}}\right]_{\boldsymbol{e}}$ for every $i=1,2,\dots, n$.

This result, due to Facchini, has been extended to infinite direct sums of uniserial modules by Příhoda in 2006. This extension involves the so-called quasismall uniserial modules. These modules were defined by Nguyen Viet Dung and Facchini, and their existence was proved by Puninski. The weak form of the Krull-Schmidt Theorem holds not only for uniserial modules, but also for several other classes of modules (biuniform modules, cyclically presented modules over serial rings,

kernels of morphisms between indecomposable injective modules, couniformly presented modules.)

Notes on alternate, similar and related terms

Right uniserial rings can also be referred to as right chain rings (Faith 1999) or right valuation rings. This latter term alludes to valuation rings, which are by definition commutative, uniserial domains. By the same token, uniserial modules have been called chain modules, and serial modules semichain modules. The notion of a catenary ring has "chain" as its namesake, but it is in general not related to chain rings.

In the 1930s, Gottfried Köthe and Keizo Asano introduced the term *Einreihig* (literally "one-series") during investigations of rings over which all modules are direct sums of cyclic submodules (Köthe 1935). For this reason, *uniserial* was used to mean "Artinian principal ideal ring" even as recently as the 1970s. Köthe's paper also required a uniserial ring to have a unique composition series, which not only forces the right and left ideals to be linearly ordered, but also requires that there be only finitely many ideals in the chains of left and right ideals. Because of this historical precedent, some authors include the Artinian condition or finite composition length condition in their definitions of uniserial modules and rings.

Expanding on Köthe's work, Tadashi Nakayama used the term *generalized uniserial ring* (Nakayama 1941) to refer to an Artinian serial ring. Nakayama showed that all modules over such rings are serial. Artinian serial rings are sometimes called Nakayama algebras, and they have a well-developed module theory.

Warfield used the term homogeneously serial module for a serial module with the additional property that for any two finitely generated submodules *A* and *B*, $\boldsymbol{A/J(A)} \cong \boldsymbol{B/J(B)}$ where *J*(-) denotes the Jacobson radical of the module (Warfield 1975). In a module with finite composition length, this has the effect of forcing the composition factors to be isomorphic, hence the "homogeneous" adjective. It turns out that a serial ring *R*is a finite direct sum of homogeneously serial right ideals if and only if *R* is isomorphic to a full *n*x*n* matrix ring over a local serial ring. Such rings are also known as primary decomposable serial rings

1.3.3 Perfect Ring

In the area of abstract algebra known as ring theory, a left perfect ring is a type of ring in which all left modules have projective covers. The right case is defined by analogy, and the condition is not left-right symmetric; that is, there exist rings which are perfect on one side but not the other. Perfect rings were introduced in (Bass 1960).

A semiperfect ring is a ring over which every finitely generated left module has a projective cover. This property is left-right symmetric.

Definitions

The following equivalent definitions of a left perfect ring R are found in

- Every left R module has a projective cover.
- $R/\mathrm{J}(R)$ is semisimple and $\mathrm{J}(R)$ is left T-nilpotent (that is, for every infinite sequence of elements of $\mathrm{J}(R)$ there is an n such that the product of first n terms are zero), where $\mathrm{J}(R)$ is the Jacobson radical of R.
- (Bass' Theorem P) R satisfies the descending chain condition on principal right ideals. (There is no mistake; this condition on *right* principal ideals is equivalent to the ring being *left* perfect.)
- Every flat left R-module is projective.
- $R/\mathrm{J}(R)$ is semisimple and every non-zero left R module contains a maximal submodule.
- R contains no infinite orthogonal set of idempotents, and every non-zero right R module contains a minimal submodule.

Examples

- Right or left Artinian rings, and semiprimary rings are known to
- The following is an example (due to Bass) of a local ring which is right but not left perfect. Let F be a field, and consider a certain ring of infinite matrices over F.

  Take the set of infinite matrices with entries indexed by $\mathbb{N}\times\mathbb{N}$, and which have only finitely many nonzero entries, all of them

above the diagonal, and denote this set by $\boldsymbol{J}$. Also take the matrix $\boldsymbol{I}$ with all 1's on the diagonal, and form the set

$$\boldsymbol{R} = \{\boldsymbol{f}.\boldsymbol{I} + \boldsymbol{J} \mid \boldsymbol{f} \in \boldsymbol{F}, \boldsymbol{j} \in \boldsymbol{J}\}$$

It can be shown that *R* is a ring with identity, whose Jacobson radical is *J*. Furthermore *R*/*J* is a field, so that *R* is local, and *R* is right but not left perfect.

Properties

For a left perfect ring *R*:

- From the equivalences above, every left *R* module has a maximal submodule and a projective cover, and the flat left *R* modules coincide with the projective left modules.
- An analogue of the Baer's criterion holds for projective modules

1.3.4 Semi-Perfect Ring

Definition

Let *R* be ring. Then *R* is semiperfect if any of the following equivalent conditions hold:

- *R*/J(*R*) is semisimple and idempotents lift modulo J(*R*), where J(*R*) is the Jacobson radical of *R*.
- *R* has a complete orthogonal set e_1, ..., e_n of idempotents with each e_i *R* e_i a local ring.
- Every simple left (right) *R*-module has a projective cover.
- Every finitely generated left (right) *R*-module has a projective cover.
- The category of finitely generated projective $\boldsymbol{R}$-modules is Krull-Schmidt.

Examples

Examples of semiperfect rings include:

- Left (right) perfect rings.
- Local rings.
- Left (right) Artinian rings.

- Finite dimensional *k*-algebras

Properties

Since a ring *R* is semiperfect iff every **simple** left ***R*-module** has a projective cover, every ring **Morita equivalent** to a semiperfect ring is also semiperfect

Check In Progress-II

Q. 1 Let *I* be an ideal in a Noetherian ring *R*; let *M* be a finitely generated *R*-module and let *N* a submodule of *M*. Then there exists an integer $k \geq 1$ so that, for $n \geq k$,

$$I^n M \cap N = I^{n-k}\left((I^k M) \cap N\right)$$

Solution : . . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Q. 2 State and Prove Krull's Principal Ideal Theorem .

Solution : . . . . . .

. . . . . .

. . . .

. . . . . .

. . . . . .

Q. 3 Prove that 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.

Solution : . . . . . .

. . . .

. . . . . .

. . . . . .

1.4 GORENSTEIN RING

n commutative algebra, a Gorenstein local ring is a commutative Noetherian local ring R with finite injective dimension as an R-module. There are many equivalent conditions, some of them listed below, often saying that a Gorenstein ring is self-dual in some sense.

Gorenstein rings were introduced by Grothendieck in his 1961 seminar (published in (Hartshorne 1967)). The name comes from a duality property of singular plane curves studied by Gorenstein (1952) (who was fond of claiming that he did not understand the definition of a Gorenstein ring[*citation needed*]). The zero-dimensional case had been studied by Macaulay (1934). Serre (1961) and Bass (1963) publicized the concept of Gorenstein rings.

Frobenius rings are noncommutative analogs of zero-dimensional Gorenstein rings. Gorenstein schemes are the geometric version of Gorenstein rings.

For Noetherian local rings, there is the following chain of inclusions.

Universally catenary rings ⊃ Cohen–Macaulay rings ⊃ Gorenstein rings ⊃ complete intersection rings ⊃ regular local rings

Definitions

A Gorenstein ring is a commutative Noetherian ring such that each localization at a prime ideal is a Gorenstein local ring, as defined above. A Gorenstein ring is in particular Cohen–Macaulay.

One elementary characterization is: a Noetherian local ring R of dimension zero (equivalently, with R of finite length as an R-module) is Gorenstein if and only if $\mathrm{Hom}_R(k, R)$ has dimension 1 as a k-vector space, where $k$is the residue field of R. Equivalently, R has simple socle as an R-module. More generally, a Noetherian local ring R is Gorenstein if and only if there is a regular sequence $a_1,...,a_n$ in the maximal ideal of R such that the quotient ring $R/(a_1,...,a_n)$ is Gorenstein of dimension zero.

For example, if R is a commutative graded algebra over a field k such that R has finite dimension as a k-vector space, $R = k \oplus R_1 \oplus ... \oplus R_m$,

then R is Gorenstein if and only if it satisfies Poincaré duality, meaning that the top graded piece R_m has dimension 1 and the product $R_a \times R_{m-a} \to R_m$ is a perfect pairing for every a.

Another interpretation of the Gorenstein property as a type of duality, for not necessarily graded rings, is: for a field F, a commutative F-algebra R of finite dimension as an F-vector space (hence of dimension zero as a ring) is Gorenstein if and only if there is an F-linear map $e: R \to F$ such that the symmetric bilinear form $(x, y) := e(xy)$ on R (as an F-vector space) is nondegenerate.

For a commutative Noetherian local ring (R, m, k) of Krull dimension n, the following are equivalent:

- R has finite injective dimension as an R-module;
- R has injective dimension n as an R-module;
- The Ext group $\boldsymbol{Ext_R^i(k, R) = 0}$ for $i \neq n$ while $\boldsymbol{Ext_R^i(k, R) \cong k}$
- $\boldsymbol{Ext_R^i(k, R) = 0}$ for some $i > n$;
- $\boldsymbol{Ext_R^i(k, R) = 0}$ for all $i < n$ and $\boldsymbol{Ext_R^i(k, R) \cong k}$
- R is an n-dimensional Gorenstein ring.

A (not necessarily commutative) ring R is called Gorenstein if R has finite injective dimension both as a left R-module and as a right R-module. If R is a local ring, R is said to be a local Gorenstein ring.

Examples

- Every local complete intersection ring, in particular every regular local ring, is Gorenstein.
- The ring $R = k[x,y,z]/(x^2, y^2, xz, yz, z^2 - xy)$ is a 0-dimensional Gorenstein ring that is not a complete intersection ring. In more detail: a basis for R as a k-vector space is given by: $\{\boldsymbol{1, x, y, z, z^2}\}$ R is Gorenstein because the socle has dimension 1 as a k-vector space, spanned by z^2. Alternatively, one can observe that R satisfies Poincaré duality when it is viewed as a graded ring with x, y, z all of the same degree.

Finally. *R*is not a complete intersection because it has 3 generators and a minimal set of 5 (not 3) relations.

- The ring $R = k[x,y]/(x^2, y^2, xy)$ is a 0-dimensional Cohen–Macaulay ring that is not a Gorenstein ring. In more detail: a basis for *R* as a *k*-vector space is given by: $\{\mathbf{1}, \boldsymbol{x}, \boldsymbol{y}\}$ *R* is not Gorenstein because the socle has dimension 2 (not 1) as a *k*-vector space, spanned by *x* and *y*.

Properties

- A Noetherian local ring is Gorenstein if and only if its completion is Gorenstein.
- The canonical module of a Gorenstein local ring *R* is isomorphic to *R*. In geometric terms, it follows that the standard dualizing complex of a Gorenstein scheme *X* over a field is simply a line bundle (viewed as a complex in degree −dim(*X*)); this line bundle is called the canonical bundle of *X*. Using the canonical bundle, Serre duality takes the same form for Gorenstein schemes as in the smooth case.
- Let (*R*, *m*, *k*) be a Noetherian local ring of embedding codimension *c*, meaning that $c = \dim_k(m/m^2) - \dim(R)$. In geometric terms, this holds for a local ring of a subscheme of codimension *c* in a regular scheme. For *c*at most 2, Serre showed that *R* is Gorenstein if and only if it is a complete intersection.[9] There is also a structure theorem for Gorenstein rings of codimension 3 in terms of the Pfaffians of a skew-symmetric matrix, by Buchsbaum and Eisenbud.

Artin–Rees lemma

In mathematics, the Artin–Rees lemma is a basic result about modules over a Noetherian ring, along with results such as the Hilbert basis theorem. It was proved in the 1950s in independent works by the mathematicians Emil Artin and David Rees;[1][2] a special case was known to Oscar Zariski prior to their work.

Statement

Let *I* be an ideal in a Noetherian ring *R*; let *M* be a finitely generated *R*-module and let *N* a submodule of *M*. Then there exists an integer $k \geq 1$ so that, for $n \geq k$,

$$\boldsymbol{I^n M \cap N = I^{n-k}\left(\left(I^k M\right) \cap N\right)}$$

Proof

The lemma immediately follows from the fact that *R* is Noetherian once necessary notions and notations are set up.

For any ring *R* and an ideal *I* in *R*, we set $\boldsymbol{B_I R} = \bigoplus_{n=0}^{\infty} \boldsymbol{I^n}$ (*B* for blow-up.) We say a decreasing sequence of submodules $\boldsymbol{M = M_0 \supset M_1 \supset M_2 \supset \cdots}$ is an *I*-filtration if $\boldsymbol{IM_n \subset M_{n+1}}$; moreover, it is stable if $\boldsymbol{IM_n = M_{n+1}}$ for sufficiently large *n*. If *M* is given an *I*-filtration, we set $\boldsymbol{B_I M} = \bigoplus_{n=0}^{\infty} \boldsymbol{M_n}$; it is a graded module over $\boldsymbol{B_1 R}$.

Now, let *M* be a *R*-module with the *I*-filtration $\boldsymbol{M_i}$ by finitely generated *R*-modules. We make an observation

> $\boldsymbol{B_1 M}$ is a finitely generated module over $\boldsymbol{B_1 R}$ if and only if the filtration is *I*-stable.

Indeed, if the filtration is *I*-stable, then $\boldsymbol{B_1 M}$ is generated by the first $\boldsymbol{k+1}$ terms $\boldsymbol{M_0 \cdots \cdots M_k}$ and those terms are finitely generated; thus, $\boldsymbol{B_1 M}$ is finitely generated. Conversely, if it is finitely generated, say, by some homogeneous elements in $\bigoplus_{j=0}^{k} \boldsymbol{M_j}$, then, for $\boldsymbol{n \geq k}$, each *f* in $\boldsymbol{M_n}$ can be written as

$$\boldsymbol{f = \sum a_j g_j, \;\; a_j \in I^{n-j}}$$

with the generators $\boldsymbol{g_j}$ in $\boldsymbol{M_j, j \leq k}$. That is, $\boldsymbol{f \in I^{n-k} M_k}$.

We can now prove the lemma, assuming *R* is Noetherian. Let $\boldsymbol{M_n = I^n M}$. Then $\boldsymbol{M_n}$ are an *I*-stable filtration. Thus, by the observation, $\boldsymbol{B_1 M}$ is finitely generated over $\boldsymbol{B_1 R}$. But $\boldsymbol{B_1 R \simeq R[It]}$ is a Noetherian ring since *R* is. (The ring $\boldsymbol{R[It]}$ is called the Rees algebra.) Thus, $\boldsymbol{B_1 M}$ is a Noetherian module and any submodule is finitely generated over $\boldsymbol{B_1 R}$.; in particular, $\boldsymbol{B_1 N}$ is finitely generated when *N* is given the induced filtration; i.e., $\boldsymbol{N_n = M_n \cap N}$. Then the induced filtration is *I*-stable again by the observation.

1.4.1 Proof Of Krull's Intersection Theorem

Besides the use in completion of a ring, a typical application of the lemma is the proof of the Krull's intersection theorem, which says: $\bigcap_{n=1}^{\infty} I^n = 0$ for a proper ideal *I* in a commutative Noetherian local ring. By the lemma applied to the intersection N, we find *k* such that for $n \geq k$,

$$= I^n \cap NI^{n-k}(I^k \cap N)$$

But then $N = IN$ and thus $N = 0$ by Nakayama.

Krull's principal ideal theorem

In commutative algebra, Krull's principal ideal theorem, named after Wolfgang Krull (1899–1971), gives a bound on the height of a principal ideal in a commutative Noetherian ring. The theorem is sometimes referred to by its German name, *Krulls Hauptidealsatz* (*Satz* meaning "proposition" or "theorem").

Precisely, if *R* is a Noetherian ring and *I* is a principal, proper ideal of *R*, then each minimal prime ideal over *I* has height at most one.

This theorem can be generalized to ideals that are not principal, and the result is often called Krull's height theorem. This says that if *R* is a Noetherian ring and *I* is a proper ideal generated by *n* elements of *R*, then each minimal prime over *I* has height at most *n*.

The principal ideal theorem and the generalization, the height theorem, both follow from the fundamental theorem of dimension theory in commutative algebra (see also below for the direct proofs).
Bourbaki's *Commutative Algebra* gives a direct proof.
Kaplansky's *Commutative ring* includes a proof due to David Rees.

1.4.2 Proof of the principal ideal theorem

Let A be a Noetherian ring, *x* an element of it and p a minimal prime over *x*. Replacing *A* by the localization A_p, we can assume A is local with the maximal ideal p. Let $q \subseteq p$ be a strictly smaller prime ideal and

let $\boldsymbol{q^{(n)} = q^n A_q \cap A}$, which is a $\boldsymbol{q}$-primary ideal called the *n*-th symbolic power of $\boldsymbol{q}$. It forms a descending chain of ideals $\boldsymbol{A \supset q \supset q^{(2)} \supset q^{(3)} \supset}$ ⋯. Thus, there is the descending chain of ideals $\boldsymbol{q^{(n)} + (x)/(x)}$ in the ring $\boldsymbol{\overline{A} = A/(x)}$. Now, the radical $\sqrt{(x)}$ is the intersection of all minimal prime ideals containg $\boldsymbol{x}$; $\boldsymbol{p}$ is among them. But $\boldsymbol{p}$ is a unique maximal ideal and thus $\boldsymbol{\sqrt{(x)} = p}$. Since $/(x)$ contains some power of its radical, it follows that $\boldsymbol{\overline{A}}$ is an Artinian ring and thus the chain $\boldsymbol{q^{(n)} + (x)/}$ (x) stabilizes and so there is some *n* such that $\boldsymbol{q^{(n)} + (x) = q^{(n+1)} +}$ (x). It implies:

$\boldsymbol{q^{(n)} = q^{(n+1)} + xq^{(n)}}$,

from the fact $\boldsymbol{q^{(n)}}$ is $\boldsymbol{q}$-primary (if $\boldsymbol{y}$ is in $\boldsymbol{q^{(n)}}$, then $\boldsymbol{y = z +}$ $\boldsymbol{ax}$ with $\boldsymbol{z \in q^{(n+1)}}$ and $\boldsymbol{a \in A}$. Since $\boldsymbol{p}$. is minimal over $\boldsymbol{x}_{,,}$ $\boldsymbol{x \notin q}$ and so $\boldsymbol{ax \in q^{(n)}}$ implies $\boldsymbol{a}$ is in $\boldsymbol{q^{(n)}}$.) Now, quotienting out both sides by $\boldsymbol{q^{(n+1)}}$ yields $\boldsymbol{\frac{q^{(n)}}{q^{(n+1)}} = (x)q^{(n)}/q^{(n+1)}}$. Then, by Nakayama's lemma, letting $\boldsymbol{I = (x)}$, we get that both sides are zero and $\boldsymbol{q^{(n)} = q^{(n+1)}}$, thus $\boldsymbol{q^{(n)}A_q = q^{(n+1)}A_q}$. Using Nakayama's lemma again, $\boldsymbol{q^{(n)}A_q =}$ $\boldsymbol{0}$ and $\boldsymbol{A_q}$ is an Artinian ring; thus, the height of $\boldsymbol{q}$ is zero. □

1.4.3 Proof Of The Height Theorem

Krull's height theorem can be proved as a consequence of the principal ideal theorem by induction on the number of elements. Let $\boldsymbol{x_{1,} \cdots, x_{n,}}$ be elements in $\boldsymbol{A}$, $\boldsymbol{p}$ a minimal prime over $(\boldsymbol{x_{1,} \cdots, x_{n,}})$and q $\subseteq p$ a prime ideal such that there is no prime strictly between them. Replacing A by the localization A_p we can assume (A, p) is a local ring; note we then have $p = \sqrt{(x_{1,} \cdots, x_{n,})}$. By minimality, q cannot contain all the x_i ; relabeling the subscripts, say, $x_i \notin q$. Since every prime ideal containing $q + (x_1)$ is between q and p, $\sqrt{q + (x_1)} = p$ and thus we can write for each $i \geq 2$,

$x_i^{r_i} = y_i + a_i x_i$

with $y_i \in q$ and $a_i \in A$. Now we consider the ring $\bar{A} = \frac{A}{y_2,\cdots,y_n}$ and the corresponding chain $\bar{q} \subset \bar{p}$ in it. If $\bar{\tau}$ is a minimal prime over $\overline{x_1}$, then τ contains $x_1, x_2^{r_2}, \cdots, x_n^{r_h}$ and thus $\tau = p$; that is to say, $\bar{p}$ is a minimal prime over $\overline{x_1}$ and so, by Krull's principal ideal theorem, $\bar{q}$ is a minimal prime (over zero); q is a minimal prime over $(y_{2,} \cdots, y_{n,})$. By inductive hypothesis, $ht(q) \leq n-1$ and thus $ht(p) \leq n$.

1.5 SOME THEOREM FOR EXERCISE

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 $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ 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 $M_0 \subseteq M_1 \subseteq \cdots$, let Σ be the collection of all M_n. This has a maximal element, say $M_n \in \Sigma$. Being maximal, all subsequent terms $M_{n+1}, M_{n+2}, \cdots$ 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 ⊆ M is such that N and M/N are noetherian, then so is M.**

Proof

First statement: let N ⊆ 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 Mcontaining 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 $M_n = M_{n+1}$.

So (M_n) is eventually constant. ♦

Corollary.

- **If M, N are noetherian, so is their direct sum M ⊕ 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 ⊆ M⊕N is a submodule whose quotient is isomorphic to N. Since M and N are noetherian, so is M⊕N. The second statement follows from that M+N is a quotient of M⊕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 ⊂ R; since Ris 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 $(x_1) \subset (x_1, x_2) \subseteq \cdots$ never terminates.

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 $M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ 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 ⊃ 2Z ⊃ 4Z ⊃ … .

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.

1.6 LET US SUM UP

1. Noetherian ring:

A ring is called left (respectively, right) Noetherian if it does not contain an infinite ascending chain of left (respectively, right) ideals. In this case, the ring in question is said to satisfy the ascending chain condition on left (respectively, right) ideals.

A ring is said to be Noetherian if it is both left and right Noetherian. For a ring R, the following are equivalent:

a. R satisfies the ascending chain condition on ideals (i.e., is Noetherian).

b. Every ideal of R is finitely generated.

c. Every set of ideals contains a maximal element.

2. Artinian ring:

A ring is called left (respectively right) Artinian if it does not contain an infinite descending chain of left (resp. right) ideals. In this case the ring in question is said to satisfy the descending chain condition on left (resp. right) ideals.

A ring is called Artinian if it is both left and right Artinian.

Suppose that R is a ring and 1_R is its multiplicative identity. A left R-module M consists of an abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that for all r, s in R and x, y in M, we have

a. r.(x+y)=r.x+r.y
b. (r+s).x=r.x+s.x
c. (rs).x=r.(s.x)
d. IR.x=x

3 Gorenstein Ring:

An algebraic ring which appears in treatments of duality in algebraic geometry. Let A be a local Artinian ring with $m \subset A$ its maximal ideal. Then A is a Gorenstein ring if the annihilator of m has dimension 1 as a vector space over $K = A/m$.

4 Krull–Akizuki theorem: A be a one-dimensional reduced noetherian ring, K its total ring of fractions. If B is a subring of a finite extension L of K containing A and is not a field, then B is a one-dimensional noetherian ring. Furthermore, for every nonzero ideal I of B, $B/1$ is finite over A.

5 Let *I* be an ideal in a Noetherian ring *R*; let *M* be a finitely generated *R*-module and let *N* a submodule of *M*. Then there exists an integer $k \geq 1$ so that, for $n \geq k$,

$$I^n M \cap N = I^{n-k}\left((I^k M) \cap N\right)$$

6 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 $M_n = M_{n+1} = M_{n+2} = \ldots$.

7 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.

1.7 KEYWORD

RING: A ring in the mathematical sense is a set S together with two binary operations.

ARTINIAN: Artin ring

MODULES: Representation of theory of Rings

NOETHERIAN : That Certain Ascending or Descending sequences of subobjects must have finite length

SUBMODULES : A Module Contained in a larger module, both over the same ring

1.8 QUESTIONS FOR REVIEW

Q. 1 If M is noetherian, so is any submodule and quotient module of M.

Q 2 if N ⊆ M is such that N and M/N are noetherian, then so is M.

Q 3 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 $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ of submodules of M, there is an n such that $M_n = M_{n+1} = M_{n+2} = \cdots$. We say that the sequence is **eventually constant**.

1.9 ANSWER FOR CHECK IN PROGRESS

Check In Progress-I

Answer Q. 1 Check in Section 1.2.4

2 Check in Section 1.2.2

Check In Progress-II

Answer Q. 1 check in section 1.2.1

Answer Q 2 Check in Section 1.1.3

Answer Q. 3 Check in section 1.5

1.10 REFERENCES AND SUGGESTION READING

- *Auslander, Maurice; Reiten, Idun; Smalø, Sverre O. (1995), Representation theory of Artin algebras, Cambridge Studies in Advanced Mathematics, 36, Cambridge University Press, doi:10.1017/CBO9780511623608, ISBN 978-0-521-41134-9, MR 1314422*
- Bourbaki, Algèbre
- Charles Hopkins. Rings with minimal condition for left ideals. Ann. of Math. (2) 40, (1939). 712–730.
- *Atiyah, Michael Francis; Macdonald, I.G. (1969), Introduction to Commutative Algebra, Westview Press, ISBN 978-0-201-40751-8*
- *Cohn, Paul Moritz (2003). Basic algebra: groups, rings, and fields. Springer. ISBN 978-1-85233-587-8.*

UNIT 2 - HELBERT BASIS THEOREM

STRUCTURE

2.0 OBJECTIVE

- Learn about Hilbert's Basis Theorem
- Learn Cohen's Structure Theorem
- Learn about isomorphism
- Learn Complementable

2.1 INTRODUCTION

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. (The converse is evidently true as well.)

2.1.1 Preliminaries

One can prove the following propositions:

(1) Let A, B be finite sequences and f be a function. Suppose rngA∪rng B ⊆dom f. Then there exist finite sequences f1, f2 such that f1 = f · A and f2 = f · B and f · (A a B) = f1 a f2.

(2) For every bag b of 0 holds decomp b = hh∅, ∅ii.

(3) For all natural numbers i, j and for every bag b of j such that i ¬ j holds b↾i is an element of Bagsi.

(4) Let i, j be sets, b1, b2 be bags of j, and b ′ 1 , b ′ 2 be bags of i. If b ′ 1 = b1↾i and b ′ 2 = b2↾i and b1 divides b2, then b ′ 1 divides b ′ 2 .

(5) Let i, j be sets, b1, b2 be bags of j, and b ′ 1 , b ′ 2 be bags of i. If b ′ 1 = b1↾i and b ′ 2 = b2↾i, then (b1 −′ b2)↾i = b ′ 1 −′ b ′ 2 and (b1 + b2)↾i = b ′ 1 + b ′ 2 . Let n, k be natural numbers and let b be a bag of n. The functor b extended by k yields an element of Bags n + 1 and is defined as follows: (Def. 1) (b extended by k)↾n = b and (b extended by k)(n) = k. We now state two propositions:

(6) For every natural number n holds EmptyBag n + 1 = EmptyBag n extended by 0.

(7) For every ordinal number n and for all bags b, b1 of n holds b1 ∈rng divisors b iff b1 divides b. Let X be a set and let x be an element of X. The functorUnitBag x yields an element of Bags X and is defined as follows:

UnitBag x = EmptyBag X +· (x, 1). Next we state four propositions:

(8) For every non empty set X and for every element x of X holds support UnitBag x = {x}.

(9) Let X be a non empty set and x be an element of X. Then (UnitBag x)(x) = 1 and for every element y of X such that x 6= y holds (UnitBag x)(y) = 0.

(10) For every non empty set X and for all elements x1, x2 of X such that UnitBag x1 = UnitBag x2 holds x1 = x2.

(11) Let X be a non empty ordinal number, x be an element of X, L be a unital non trivial non empty double loop structure, and e be a function from X into L. Then eval(UnitBagx,e) = e(x).

Let X be a set, let x be an element of X, and let L be a unital non empty multiplicative loop with zero structure. The functor 1 1(x, L) yielding a Series of X, L is defined by:

1(x,L) = 0 (X, L) +· (UnitBag x, 1L).

One can prove the following propositions:

(12) Let X be a set, L be a unital non trivial non empty double loop structure, and x be an element of X. Then (1 1(x,L))(UnitBag x) = 1L and for every bag b of X such that b 6= UnitBag x holds (1 1(x,L))(b) = 0L.

(13) Let X be a set, x be an element of X, and L be an add-associative right zeroed right complementableunital right distributive non trivial non empty double loop structure. Then Support 1 1(x, L) = {UnitBag x}.

Let X be an ordinal number, let x be an element of X, and let L be an add-associative right zeroed right complementableunital right distributive non trivial non empty double loop structure. Observe that 1 1(x,L) is finite-Support.

One can prove the following three propositions:

(14) Let L be an add-associative right zeroed right complementableunital right distributive non trivial non empty double loop structure, X be a non empty set, and x1, x2 be elements of X. If 1 1(x1,L) = 1 1(x2,L), then x1 = x2.

(15) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, x be an element of the carrier of Polynom-Ring L, and p be a sequence of L. If x = p, then −x = −p.

(16) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure, x, y be elements of the carrier of Polynom-Ring L, and p, q be sequences of L. If x = p and y = q, then x − y = p − q.

Let L be a right zeroed add-associative right complementableunital distributive non empty double loop structure and let I be a non empty subset of the carrier of Polynom-Ring L. The functorminlen I yields a non empty subset of I and is defined by:

minlen I = {x; x ranges over elements of I: V x′ ,y′ : Polynomial of L (x ′ = x ∧ y ′ ∈ I ⇒len x ′ ¬ len y ′)}.

We now state the proposition

(17) Let L be a right zeroed add-associative right complementableunital distributive non empty double loop structure, I be a non empty subset of the carrier of Polynom-Ring L, and i1, i2 be Polynomials of L. If i1 ∈minlen I and i2 ∈ I, then i1 ∈ I and len i1 ¬ len i2.

Let L be a right zeroed add-associative right complementableunital distributive non empty double loop structure, let n be a natural number, and let a be an element of the carrier of L. The functormonomial(a,n) yields a Polynomial of L and is defined as follows:

For every natural number x holds if x = n, then (monomial(a,n))(x) = a and if x 6= n, then (monomial(a, n))(x) = 0L.

The following four propositions are true:

(18) Let L be a right zeroed add-associative right complementableunital distributive non empty double loop structure, n be a natural number, and a be an element of the carrier of L. Then if a 6= 0L, then lenmonomial(a,n) = n + 1 and if a = 0L, then len monomial(a,n) = 0 and len monomial(a,n) ¬ n + 1.

(19) Let L be a right zeroed add-associative right complementableunital distributive non empty double loop structure, n, x be natural numbers, a be an element of the carrier of L, and p be a Polynomial of L. Then (monomial(a,n) ∗ p)(x + n) = a · p(x).

(20) Let L be a right zeroed add-associative right complementableunital distributive non empty double loop structure, n, x be natural numbers, a be an element of the carrier of L, and p be a Polynomial of L. Then (p ∗monomial(a,n))(x + n) = p(x) · a.

(21) Let L be a right zeroed add-associative right complementableunital distributive non empty double loop structure and p, q be Polynomials of L. Then

len(p ∗ q) ¬ (len p + len q) −′ 1.

2.1.2 On Ring Isomorphism

The following propositions are true:

(22) Let R, S be non empty double loop structures, I be an ideal of R, and P be a map from R into S. If P is a ring isomorphism, then P ◦ I is an ideal of S.

(23) Let R, S be add-associative right zeroed right complementable non empty double loop structures and f be a map from R into S. If f is a ring homomorphism, then f(0R) = 0S.

(24) Let R, S be add-associative right zeroed right complementable non empty double loop structures, F be a non empty subset of the carrier of R, G be a non empty subset of the carrier of S, P be a map from R into S, l1 be a linear combination of F, L1 be a linear combination of G, and E be a finite sequence of elements of [:the carrier of R, the carrier of R, the carrier of R :]. Suppose that

(i) P is a ring homomorphism,

(ii) len l1 = lenL1,

(iii) E represents l1, and

(iv) for every set i such that i∈dom L1 holds L1(i) = P((Ei)1)· P((Ei)2)· P((Ei)3). Then P(Pl1) = PL1

(25) Let R, S be non empty double loop structures and P be a map from R into S. Suppose P is a ring isomorphism. Then there exists a map P1 from S into R such that P1 is a ring isomorphism and P1 = P −1 .

(26) Let R, S be Abelian add-associative right zeroed right complementable associative distributive well unital non empty double loop structures, F be a non empty subset of the carrier of R, and P be a map from R into S. If P is a ring isomorphism, then P ◦F–ideal = (P ◦F)–ideal.

(27) Let R, S be Abelian add-associative right zeroed right complementable associative distributive well unital non empty double loop structures and P be a map from R into S. If P is a ring isomorphism and R is Noetherian, then S is Noetherian.

(28) Let R be an add-associative right zeroed right complementable associative distributive well unital non trivial non empty double loop structure. Then there exists a map from R into Polynom-Ring(0,R) which is a ring isomorphism.

(29) Let R be a right zeroed add-associative right complementableunital distributive non trivial non empty double loop structure, n be a natural number, b be a bag of n, p1 be a Polynomial of n, R, and F be a finite sequence of elements of the carrier of Polynom-Ring(n,R). Suppose p1 = PF. Then there exists a function g from the carrier of Polynom-Ring(n,R) into the carrier of R such that for every Polynomial p of n, R holds g(p) = p(b) and p1(b) = P(g · F).

Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and let n be a natural number. The functorupm(n,R) yielding a map from Polynom-Ring Polynom-Ring(n,R) into Polynom-Ring(n+1,R) is defined by the condition.

Let p1 be a Polynomial of Polynom-Ring(n,R), p2 be a Polynomial of n, R, p3 be a Polynomial of n + 1, R, and b be a bag of n + 1. If p3 = (upm(n,R))(p1) and p2 = p1(b(n)), then p3(b) = p2(b↾n).

Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and let n be a natural number. One can verify the following observations:

∗upm(n,R) is additive,

∗upm(n,R) is multiplicative,

∗upm(n,R) is unity-preserving, and

∗upm(n,R) is one-to-one.

Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and let n be a natural number. The functormpu(n,R) yields a map from Polynom-Ring(n + 1,R) into Polynom-Ring Polynom-Ring(n,R) and is defined by the condition.

Let p1 be a Polynomial of n + 1, R, p2 be a Polynomial of n, R, p3 be a Polynomial of Polynom-Ring(n,R), i be a natural number, and b be a bag of n. If p3 = (mpu(n,R))(p1) and p2 = p3(i), then p2(b) = p1(b extended by i)

Next we state two propositions:

(30) Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure, n be a natural number, and p be an element of the carrier of Polynom-Ring(n+1,R). Then (upm(n,R))((mpu(n,R))(p)) = p.

(31) Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital commutative non trivial non empty double loop structure and n be a natural number. Then there exists a map from Polynom-Ring Polynom-Ring(n,R) into Polynom-Ring(n+1,R) which is a ring isomorphism.

Let R be a Noetherian Abelian add-associative right zeroed right complementable associative distributive well unital commutative non empty double loop structure. Observe that Polynom-Ring R is Noetherian. One can prove the following propositions:

(32) Let R be a Noetherian Abelian add-associative right zeroed right complementable associative distributive well unital commutative non empty double loop structure. Then Polynom-Ring R is Noetherian.

(33) Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital non trivial

commutative non empty double loop structure. Suppose R is Noetherian. Let n be a natural number. Then Polynom-Ring(n,R) is Noetherian. (34) Every field is Noetherian.

(35) For every field F and for every natural number n holds Polynom-Ring(n, F) is Noetherian.

(36) Let R be an Abelian right zeroed add-associative right complementable well unital distributive associative commutative non trivial non empty double loop structure and X be an infinite ordinal number. Then Polynom-Ring(X,R) is non Noetherian.

2.1.3 Statement

If is a ring, let denote the ring of polynomials in the indeterminate over . Hilbert proved that if is "not too large", in the sense that if is Noetherian, the same must be true for . Formally,

Hilbert's Basis Theorem. Let *R* be a Noetherian ring.

Then *R*[*x*] is a Noetherian ring

Corollary. If *R*[*x*] is a Noetherian ring, then R is a Noetherian ring.

This can be translated into algebraic geometry as follows:
every algebraic set over a field can be described as the set of common roots of finitely many polynomial equations. Hilbert (1890) proved the theorem (for the special case of polynomial rings over a field) in the course of his proof of finite generation of rings of invariants.

Hilbert produced an innovative proof by contradiction using mathematical induction; his method does not give an algorithm to produce the finitely many basis polynomials for a given ideal: it only shows that they must exist. One can determine basis polynomials using the method of Gröbner bases.

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 istnichtMathematik. Das istTheologie. [This is not mathematics. This is theology.]" In time, though, the value of nonconstructive proofs was more widely recognized.

2.1.4 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 $p \in \mathfrak{a}_A$, as desired. ■

From now on we will assume that all rings, unless otherwise stated, are commutative and have an identity element 1

Let R, R0 two rings. A map φ : R → R0 will be called a homomorphism if:

• φ(x + y) = φ(x) + φ(y) for every x, y ∈ R

• $\varphi(xy) = \varphi(x)\varphi(y)$ for every $x, y \in R$

• $\varphi(1) = 1$

The kernel of a homomorphism $\varphi : R \to R0$ is by definition the set:

$\ker\varphi = \{x \in R : \varphi(x) = 0\}$

This is a subgroup of R and it also has the property that if $x \in \ker(\varphi)$ and $y \in R$ then $xy \in \ker(\varphi)$. This motivates the following definition:

Definition A subgroup I of a ring R is called an ideal if for every $x \in I$ and $y \in R$, we have that $xy \in I$.

According to the above definition, nothing prevents the ideal from coinciding with the ring R. From now one we will be making the assumption that, unless otherwise stated, an ideal will not contain the identity, in other words it will be a strict ideal. Also, the ideal (0) will be usually referred to as the trivial ideal.

For every ideal I of the ring R the group R/I can be naturally given the structure of a ring so that the quotient (group) homomorphism:

$q : R \to R/I$

is a ring homomorphism. This is usually referred to as the natural epimorphism associated with the ideal I.

We recall that a ring R is called an integral domain if it has no zero-divisors, i.e. whenever $xy = 0$ then either $x = 0$ or $y = 0$. Also an ideal I will be called prime if whenever $xy \in I$ either $x \in I$ or $y \in I$. This definition is clearly motivated by the ideals pZ of Z for p prime number. We have a natural connection between prime ideals and integral domains:

Proposition Let I be an ideal of the ring R. Then the quotient R/I is an integral domain if and only if I is prime.

Proof: Chasing definitions.

We also recall that a ring, in which every non-zero element has a multiplicative inverse, is called a field. A simple remark gives us:

Proposition A ring R is a field if and only if it has no non-trivial ideals.

An ideal I of R is called maximal if it is not contained in any strictly larger ideal. Then we have that an ideal I is maximal if and only if the quotient R/I is a field. A standard application of Zorn's lemma also gives us that any ideal is contained in a maximal ideal.

Definition The set of prime ideals of a ring R will be denoted by specR and the set of maximal ideals will be denoted by m-specR.

If F is a field then the maximal ideals of F[x] are in one-to-one correspondence with monic irreducible polynomials. If F is further algebraically closed then the maximal ideals are in one-to-one correspondence with the elements of F.

Let R be a ring and I an ideal of R. Then a subset $A \subset R$ is said to generate I if:

$I = \{x1y1 + x2y2 + ... + xnyn|xi \in A, yi \in R\}$

A will be also called a set of generators. If an ideal I has a finite set of generators, then it is called finitely generated. An ideal I is called principal if it is generated by just one element $a \in R$. Such an ideal is denoted by (a). We have the very important:

Definition A ring R is called Noetherian if every ideal $I \subset R$ is finitely generated. Also, a ring R is called a principal ideal domain (p.i.d.) if every ideal in R is principal.

We have the following important characterization of Noetherian rings:

Proposition A ring R is Noetherian if and only if every increasing sequence of ideals.

$I1 \subset I2 \subset I3 \subset ...$

is eventually constant.

Proof: Let R be Noetherian and {In} an increasing sequence of ideals. Then S In is also an ideal and since R is Noetherian it is finitely generated, say, by a1, ..., am Since the ai 's are elements of the union S In, they are each contained in some In. But if we take the ideal with the largest index, then it will contain all of them and it will, thus, coincide with the union.

For the converse, notice that if an ideal $I \subset R$ is not finitely generated, then one can inductively define a strictly increasing sequence of ideals as follows: Let $x1 \neq 0$ be in I. Then set $I1 = (x)$. We have that $I \neq I1$, otherwise I would be finitely generated. So there is $x2 \in I - I1$. Let now $I2 = (x1, x2)$. Then $I \neq I2$ and thus we can find $x3 \in I - I2$. We set $I3 = (x1, x2, x3)$ and continue in the same fashion

One of the early and most important theorems of Commutative algebra is:

Check in Progress-I

Problem 1 Complete the following exercises for your favorite choice of $*$ among $\{a, b, c\}$.

(a) Show that $3(*) \Longrightarrow 2(*) \Longrightarrow 1(*)$ for $* \in \{a, b, c\}$.

(b) Show that $2(*) \Longrightarrow 3(*)$ for $* \in \{a, b, c\}$. . Hint: Take a surjection $\gamma : Rn \to M$, and take the preimages of the various objects under γ.

(c) Show that $1(*) \Longrightarrow (2*)$. Hint: Use induction on n. For $n > 1$, look at the short exact sequence $0 \to R \iota \longrightarrow Rn \pi \longrightarrow Rn-1 \to 0$. Given $M \subset Rn$, think about the modules $M \cap \iota(R)$ and $\pi(M)$. Remark: If R is a field, then 1(b) is obvious, but 2(b) is the first significant theorem in a linear algebra course. So you should expect to need to do some work here.

Solution

……

……

……

……

……

Problem 2 Complete the following exercises for your favorite choice of # among {1, 2, 3}.

(a) Show that $\#(b) \Longrightarrow \#(a)$.

(b) Show that #(c) =⇒#(b).

(c) Show that #(a) =⇒ #(c).

Solution

……

……

……

……

……

2.2 (HILBERT BASIS THEOREM).

Proof: Let J be a non-trivial ideal of R[x] and m the least degree of a non-zero polynomial in J. Then for n ≥ m define:

In = {a ∈R|a is the leading coefficient k of an n-th degree polynomial in J} [{0} }]

It is a routine to check that the In's are ideals of R and that In⊂ In+1. Since R is a Noetherian ring, each of the In is finitely generated and there exists a k ∈ N such that In = Ik for n ≥ k. For each n with m ≤ n ≤ k, let An be a finite set of polynomials of degree n such that their leading coefficients generate In. Let A = S An. Then A is a finite set and we will show that it generates J. We will use induction on the degree of a polynomial in J.

If deg p(x) = m (nothing smaller is possible for a non-zero polynomial!), then there are qi 's in Am and ai∈ R such that the leading coefficient of p(x) coincides with the leading coefficient of Paiqi(x). This means that p(x) − Paiqi(x) has degree strictly less than m, which implies that it is the zero polynomial and our induction is complete for m.

Now, assuming the claim for all naturals between m and n we are going to check it for n + 1. If n + 1 ≤ k then there exist qi(x) in An+1 and ai∈ R such that p(x) − Paiqi(x) is of degree less than n + 1. This polynomial can now be written in terms of the elements of A by induction hypothesis. On

the other hand, if n + 1 > k, then there are polynomials of degree n, qi(x)in J and ai∈ R so that the leading coefficient of p(x) coincides with that of x Paiqi(x). Thus the difference p(x) − x Paiqi(x) is in J and has degree less than n + 1. The inductive hypothesis applied both on the qi(x) and p(x) − x Paiqi(x) concludes the proof.

Recall from the Noetherian Rings page that a ring R is said to be a Noetherian ring if it satisfies the ascending chain condition, that is, for all ascending chains of ideals $I1 \subseteq I2 \subseteq ... \subseteq In \subseteq ...$ there exists an $N \in \mathbb{N}$ such that for all $m \geq N$ we have that $Im = IN$. Equivalently, we proved that R is Noetherian if and only if every ideal I is finitely generated, that is, there exists $x1, x2, ..., xn \in I$ such that $I = (x1, x2, ..., xn)$.

We about to prove a very important result known as the Hilbert basis theorem which tells us that if R is a Noetherian ring then the corresponding ring of polynomials of a single variable x, $R[x]$, is a Noetherian ring. We first need the following lemma.

We first need to get some notation out of the way. If $F \in R[x]$ then F is of the form:

(1) $F(x) = anxn + an-1xn-1 + ... + a1x + a0$

We define the function cof(F) to be the leading coefficient of F. That is, if F has degree n as above then:

(2) $\text{cof}(F) = an$

For $m \geq 0$ and for an ideal I, we define:

(3) $Jm = \{\text{cof}(F) : F \in I, \deg F \leq m\}$

Lemma 1: Let R be a Noetherian ring and let I be an ideal.

Then for all $m \geq 0$, Jm is an ideal.

- **Proof:** Let $a \in Jm$ and let $b \in R$. Then $a = \text{cof}(F)$ for some polynomial $F \in I$ with $\deg F \leq m$.
- Consider the function bF.
- Then $bF \in I$ since I is an ideal. Furthermore, $\deg(bF) = \deg(F) \leq m$.
- Therefore $\text{cof}(bF) \in Jm$. But $\text{cof}(bF) = ab$. So $ab \in Jm$.

- Now let $a,b \in Jm$. Then $a=\text{cof}(F)$ and $b=\text{cof}(G)$ for some polynomials $F,G \in I$ with $\deg F, \deg G \leq m$. Let $\deg F=s$ and let $\deg G=t$. Then F and G have the form:

(4) $F(x)G(x)=axs+as-1xs-1+...+a1x+a0=bxt+bt-1xt-1+...+b1x+b0$

- Without loss of generality, assume that $s \geq t$. Define a new polynomial H by:

(5) $H(x)=F+xs-tG)$

- Since $F,G \in I$ we have that $H \in I$. Furthermore observe that:

(6) $H(x)=[axs+as-1xs-1+...+a1x+a0]+xs-t[bxt+bt-1xt-1+...+b1x+b0]=axs+as-1xs-1+...+a1x+a0+bxs+bt-1xs-1+...+b1xs-t+1+b0xs-t$

- Therefore $\text{cof}(F+xs-tG)=a+b$. Hence $(a+b) \in Jm$. Thus Jm is an ideal.

Theorem 1 (The Hilbert Basis Theorem): Let R be a Noetherian ring. Then $R[x]$ is a Noetherian ring.

Proof: Let $I \subseteq R[x]$ be an ideal and for each $m \geq 0$ let Jm be defined in terms of I.

Consider the following ascending chain of ideals:

(7)

$$J1 \subseteq J2 \subseteq ... \subseteq Jn \subseteq ...$$

Since R is Noetherian, there exists an $N \in \mathrm{N}$ such that for all $m \geq N$ we have that $Jm=JN$.

Also, since R is a Noetherian ring every ideal in R is finitely generated. So for each $m \geq 0$ there exists elements $am1,am2,...,amk$ such that:

(8)

$$Jm=(am1,am2,...,amk)$$

For each $1 \leq j \leq k$, choose a polynomial $Fmj \in I$ such that $amj = \text{cof}(Fmj)$. Let I' be defined as the ideal generatedby the Fmjs for all $m \leq N$. We claim that $I = I'$.

By definition, we have that $I' \subseteq I$. Now suppose that $I' \not\supseteq I$. Then there exists a function $G \in I$ such that $G \notin I'$. Let G be chosen of minimal degree in I' and let $\deg(G) = d$. Then $\text{cof}(G) \in Jd$. So **cof**(G) has the form:

(9)

$$\text{cof}(G) = \sum \alpha j \text{cof}(Fdj)$$

Where $\alpha j \in R$ and Fdj are in the list of generators for I' and where $\deg(Fdj) \leq d$. Let:

(10)

$$Q(x) = \sum \alpha j x d - \deg(Fdj) Fdj$$

Then $Q \in I$ and $\deg(Q) = d$. But $\text{cof}(Q) =$ **cof**(G). Then $G - Q \in I$. But $\deg(G - Q) \leq d - 1$. Since $G \notin I'$ and $Q \in I'$ we hae that $G - Q \notin I'$ and is such that $\deg(G - Q) < d$. But this contradicts G having minimal degree in I.

Therefore $I = I'$. Since I' is finitely generated so is I. So every ideal in $R[x]$ is finite generated, i.e., $R[x]$ is Noetherian.

Check Your Progress-Ii

Problem1. Let R be a Noetherian complete local ring. Any quotient of R is also a Noetherian complete local ring. Given a finite ring map R→S, then S is a product of Noetherian complete local rings.

Solution

……

……

……

Problem2. Let (R,m) be a complete local ring. If m is a finitely generated ideal then R is Noetherian.

Solution

……

……

……

Problem3 Let p be a prime number. Let k be a field of characteristic p. There exists a Cohen ring Λ with $\Lambda/p\Lambda \cong k$.

Solution

……

……

……

2.3 COHEN'S STRUCTURE THEOREM

In mathematics, the **Cohen's structure theorem**, introduced by Cohen (1946), describes the structure of complete Noetherian local rings. Before proceeding, one should consult our notes on Hensel's Lemma, where some subtle differences in definitions between Zariski & Samuel and Atiyah& Macdonald are discussed. In these notes, a local ring is not assumed to be Noetherian and a ring is complete if every Cauchy sequence converges and the intersection $\cap nmn$ is zero (these follow A&M, not Z&S). However, with the conventions of Z&S the same statements with the same proofs are true. In Z&S local rings are Noetherian but completeness does not include the intersection requirement. But all we need is that A has one maximal ideal, limits for Cauchy sequences and $\cap nmn = 0$ - so either set of hypothesis will do.

Some consequences of Cohen's structure theorem include three conjectures of Krull:

- Any complete regular equicharacteristic Noetherian local ring is a ring of formal power series over a field. (Equicharacteristic means that the local ring and its residue field have the same characteristic, and is equivalent to the local ring containing a field.)
- Any complete regular Noetherian local ring that is not equicharacteristic but is unramified is uniquely determined by its residue field and its dimension.
- Any complete Noetherian local ring is the image of a complete regular Noetherian local ring.

Statement

The most commonly used case of Cohen's theorem is when the complete Noetherian local ring contains some field. In this case Cohen's structure theorem states that the ring is of the form $k[[x_1,...,x_n]]/(I)$ for some ideal I, where k is its residue class field.

In the unequal characteristic case when the complete Noetherian local ring does not contain a field, Cohen's structure theorem states that the local ring is a quotient of a formal power series ring in a finite number of variables over a Cohen ring with the same residue field as the local ring. A Cohen ring is a field or a complete characteristic zero discrete valuation ring whose maximal ideal is generated by a prime number p (equal to the characteristic of the residue field).

In both cases, the hardest part of Cohen's proof is to show that the complete Noetherian local ring contains a **coefficient ring** (or **coefficient field**), meaning a complete discrete valuation ring (or field) with the same residue field as the local ring.

Definition 1. Let A be a local ring A with maximal ideal m. We call A an equicharacteristic local ring if A has the same characteristic as its residue field A/m. A field of representatives for A is a subfield L of A which is mapped onto A/m by the canonical mapping of A onto A/m. Since L is a field, the restriction of this mapping to L gives an isomorphism of fields L ∼= A/m.

Lemma 1. Let A be an equicharacteristic local ring with maximal ideal m and characteristic p 6= 0. If mp = (0) then A admits a field of representatives.

Proof. Let Ap be the set of all elements a p where a ranges over A. Then Ap is obviously a subring of A. If a p is any nonzero element of A, then since mp = (0) we must have a /∈ m and consequently a is a unit in A. If ay = 1 then y p is an inverse for x p in Ap , and therefore Ap is a subfield of A. Among all the subfields of A containing Ap , Zorn's Lemma produces a maximal subfield L. Let $\phi : A \longrightarrow A/m$ be canonical. We claim that $\phi(L) = A/m$.

Assume to the contrary that there is $\alpha \in A/m$ with $\alpha / \in \phi(L)$. Since $\alpha^p \in \phi(A^p) \subseteq \phi(L)$ the minimal polynomial of α over $\phi(L)$ is $x^p - \alpha^p$ (see our notes on purely inseparable extensions). Let $a \in A$ be a representative of α, $\phi(a) = \alpha$. Then $a / \in L$ and the isomorphism $L \sim= \phi(L)$ induces a chain of ring isomorphisms

$$L[a] \sim= L[x]/(x^p - a^p) \sim= \phi(L)[x]/(x^p - \alpha^p) \sim= \phi(L)(\alpha)$$

Hence L[a] is a subfield of A, contradiciting the maximality of L. We conclude that $\phi(L) = A/m$, completing the proof.

Theorem 2. An equicharacteristic complete local ring A admits a field of representatives.

Proof. In the case in which A and A/m both have characteristic 0 the Theorem has already been proved in a Corollary to Hensel's Lemma. So we may assume that the characteristic of A and A/m is a prime p 6= 0. Since $p \geq 2$ the maximal ideal $m = m/m^2$ of the local ring A/m^2 satisfies the condition $m^p = (0)$. Clearly A/m^2 satisfies the other conditions of the Lemma, so A/m^2 admits a field of representatives K2. For $n \geq 1$ let ψ_n denote the canonical map $A/m^{n+1} \longrightarrow A/m^n$, and notice that

$$\psi^{-1}_n(m/m^n) = m/m^{n+1} \quad (1)$$ For $n \geq 2$

the ring A/m^n is an equicharacteristic local ring. We now construct by induction on $n \geq 2$, a representative field Kn of A/m^n such that ψ_n induces an isomorphism of K_{n+1} onto Kn. Suppose that Kn has already been constructed. The inverse image $\psi^{-1}_n(K_n)$ is a subring R of

A/mn+1 which contains the kernel p = mn/mn+1 of ψn. Let ξ be any element of R not in a.

Then the image ξ 0 of ξ under ψn is a nonzero element of Kn, and consequently is a unit in A/mn. Hence ξ 0 ∈/ m/mn, and it follows from (1) that ξ /∈ m/mn+1, so ξ is a unit in A/mn+1. If η is the inverse of ξ in A/mn+1 then ψn(η) ∈Kn and so by definition η ∈ R. Thus ξ is invertible in R and we have proved that R is a local ring with maximal ideal p. Since p = mn/mn+1 and m2n ⊆ mn+1 we have p 2 = (0). Clearly both R and R/p ∼= Kn have characteristic p, so the Lemma shows the existence of a representative field Kn+1 of R. Since R/p ∼= Kn it is easy to see that ψn induces an isomorphism of Kn+1 onto Kn, and the canonical morphism A/mn+1 −→ A/m is the composition of ψn and A/mn −→ A/m, so the fact that Kn is a representative field of A/mn implies that Kn+1 is a representative field of A/mn+1.

Since A is complete we have ring isomorphisms A ∼= Ab ∼= lim←− A/mn. So given any sequence of elements (ηn)n≥1 with ηn∈ A/mn there is precisely one element y ∈ A admitting ηn as an mn-residue for all n. Set K1 = A/m and let η = η1 be any element of K1. Consider the elements

η2 = ψ −1 1 (η1), η3 = ψ −1 2 (η2), . . . ηn+1 = ψ −1 n (ηn), . . .

withηi∈ Ki for all i ≥ 1. Denote by u(η) the unique element of A defined by this sequence. It is readily verified that u(0) = 0, u(1) = 1 and u(η + η 0) = u(η) + u(η 0), u(ηη0) = u(η)u(η 0), so u(K1) is a subring of A. Furthermore, for every η 6= 0 in K1 there exists an element η 0 in K1 such that ηη0 = 1 whence u(η 0) is the inverse of u(η) in u(K1). Therefore u(K1) is a subfield of A, and by construction ϕ(u(K1)) = K1 = A/m where ϕ : A −→ A/m is canonical, so we have found a representative field of A.

Lemma 3. Let B be a ring, a an ideal of B, M an B-module, (Mn) an a-filtration of M. Suppose that B is complete in the a-topology and that M is Hausdorff in its filtration topology. Suppose also that G(M) is generated over G(B) by a finite set of homogenous elements ξ1, . . . , ξn of degrees n(i). If xi ∈Mn(i) is equal to ξi in Mn(i)/Mn(i)+1 then the elements x1, . . . , xn generate M over B.

Corollary 4. An equicharacteristic complete regular local ring A is either a field or has dimension $d \geq 1$ and is isomorphic to a formal power series ring over a field in d variables.

Proof. A regular local ring of dimension zero is a field, so assume $d \geq 1$, let m be the maximal ideal of A and let a1, . . . , ad be a regular system of parameters with m = (a1, . . . , ad). By the previous Theorem, A admits a representative field K. From our notes on Analytic Independence there is a morphism of rings

$\phi : K[[x1, . . . , xd]] \longrightarrow A$

which is injective.

The subring B = K[[a1, . . . , ad]] of A is a complete regular local ring with maximal ideal n generated by a1, . . . , ad (in B), so we have $m \cap B = n$. Considering A as a B-module, we are in the situation of the preceeding Lemma. We claim that Gm(A) is generated as a Gn(B)-module by the homogenous element 1 of order zero. We have

Gn(B) = B/n ⊕ n/n 2 ⊕ . . .

Gm(A) = A/m ⊕ m/m 2 ⊕ . . .

It is standard that Gm(A) = (A/m)[a1, . . . , ad]. So it suffices to show that any monomial kan1 1 . . . a nd d in the ai (which is a homogenous element of order Pni in Gm(A)) belongs to the submodule generated by 1. But the ai all belong to n and since K is a representative field $B/n \sim= K \sim= A/m$, so we can manufacture such a monomial in Gn(B) and simply multiply it by $1 \in Gm(A)$ to produce the desired result. The preceeding Lemma now implies that A is generated over B by 1, that is, A = B. So A is isomorphic to a formal power series ring over a field in d variables, as required.

2.4 LET US SUM UP

Let R be a Noetherian Abelian add-associative right zeroed right complementable associative distributive well unital commutative non empty double loop structure. Then Polynom-Ring R is Noetherian.

1. For every ideal I of the ring R the group R/I can be naturally given the structure of a ring so that the quotient (group) homomorphism:

   q : R → R/I is a ring homomorphism.

2. Let I be an ideal of the ring R. Then the quotient R/I is an integral domain if and only if I is prime.

3. A ring R is called Noetherian if every ideal I ⊂ R is finitely generated. Also, a ring R is called a principal ideal domain (p.i.d.) if every ideal in R is principal.

4. The Hilbert Basis Theorem: Let *R* be a Noetherian ring.

   Then *R*[*x*] is a Noetherian ring.

5. Let R be a Noetherian Abelian add-associative right zeroed right complementable associative distributive well unital commutative non empty double loop structure. Then Polynom-Ring R is Noetherian.

6. Let R be an Abelian add-associative right zeroed right complementable associative distributive well unital non trivial commutative non empty double loop structure. Suppose R is Noetherian. Let n be a natural number. Then Polynom-Ring(n,R) is Noetherian.

2.5 KEYWORD

ABELIAN :Having members related by a commutative operation

QUOTIENT :A result obtained by dividing one quantity by another

ISOMORPHIC :Corresponding or similar in form and relations

2.6 QUESTIONS FOR REVIEW

Problem 1 Show that a quotient ring of a noetherian ring is noetherian. [Hint: This is easiest with the third properties.]

Problem2We will now prove the Hilbert basis theorem: If A is noetherian, then A[t] is noetherian.

Problem3This is the original purpose for which Hilbert proved his Basis Theorem. This is even more optional than the rest of the problem set, but it is really fun.

Problem 4(Cohen Structure Theorem). Let (R,m) be a complete local ring.

1. R has a coefficient ring
2. if m is a finitely generated ideal, then R is isomorphic to a quotient

   $\Lambda[[x1,\ldots,xn]]/I$

where Λ is either a field or a Cohen ring.

2.7 ANSWER TO CHECK IN PROGRESS

Check In Progress-1

Answer Q. 1 check in section 1.1

Q. 2 Check in section 1.2

Check In progress-II

Answer Q. 1 Check in section 2

Q. 2 Check in section 3

Q. 3 Check in section 2

2.8 SUGGESTION READING AND REFERENCES

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. Formalized Mathematics, 9(3):565–582, 2001.

[2] GrzegorzBancerek. The fundamental properties of natural numbers. Formalized Mathematics, 1(1):41–46, 1990.

[3] GrzegorzBancerek. The ordinal numbers. Formalized Mathematics, 1(1):91–96, 1990.

[4] GrzegorzBancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. Formalized Mathematics, 1(1):107–114, 1990.

[5] Thomas Becker and Volker Weispfenning. Gr¨obner bases: A Computational Approach to Commutative Algebra. Springer-Verlag, New York, Berlin, 1993.

[6] JózefBiałas. Group and field definitions. Formalized Mathematics, 1(3):433–439, 1990.

[7] CzesławByliński. Binary operations applied to finite sequences. Formalized Mathematics, 1(4):643–649, 1990.

[8] CzesławByliński. Functions and their basic properties. Formalized Mathematics, 1(1):55– 65, 1990.

[9] CzesławByliński. Functions from a set to a set. Formalized Mathematics, 1(1):153–164, 1990.

[10] CzesławByliński. Some basic properties of sets. Formalized Mathematics, 1(1):47–53, 1990.

[11] AgataDarmochwał. Families of subsets, subspaces and mappings in topological spaces. Formalized Mathematics, 1(2):257–261, 1990.

[12] AgataDarmochwał. Finite sets. Formalized Mathematics, 1(1):165–167, 1990.

[13] AgataDarmochwał and Andrzej Trybulec. Similarity of formulae. Formalized Mathematics, 2(5):635–642, 1991.

[14] JarosławKotowicz. Monotone real sequences. Subsequences. Formalized Mathematics, 1(3):471–475, 1990

[15] Eugeniusz Kusak, WojciechLeończuk, and MichałMuzalewski. Abelian groups, fields and vector spaces. Formalized Mathematics, 1(2):335–342, 1990.

[16] Robert Milewski. The ring of polynomials. Formalized Mathematics, 9(2):339–346, 2001.

UNIT 3 - NOETHERIAN RING

STRUCTURE

3.0 OBJECTIVE

In the theory of radicals, rings are usually assumed to be associative, but need not be commutative and need not have an identity element. In particular, every ideal in a ring is also a ring.

A **radical class** (also called **radical property** or just **radical**) is a class σ of rings possibly without identities, such that:

1. the homomorphic image of a ring in σ is also in σ
2. every ring R contains an ideal $S(R)$ in σ that contains every other ideal of R that is in σ
3. $S(R/S(R)) = 0$. The ideal $S(R)$ is called the radical, or σ-radical, of R.

The study of such radicals is called **torsion theory**.

For any class δ of rings, there is a smallest radical class $L\delta$ containing it, called the **lower radical** of δ. The operator L is called the **lower radical operator**.

A class of rings is called **regular** if every non-zero ideal of a ring in the class has a non-zero image in the class. For every regular class δ of rings, there is a largest radical class $U\delta$, called the upper radical of δ, having zero intersection with δ. The operator U is called the **upper radical operator**.

A class of rings is called **hereditary** if every ideal of a ring in the class also belongs to the class

3.1 INTRODUCTION RADICAL OF A RING

In ring theory, a branch of mathematics, a **radical of a ring** is an ideal of "not-good" elements of the ring.

The first example of a radical was the nilradical introduced by Köthe (1930), based on a suggestion of Wedderburn (1908). In the next few years several other radicals were discovered, of which the most important example is the Jacobson radical. The general theory of radicals was defined independently by (Amitsur 1952, 1954, 1954b) and Kurosh (1953).

Examples

3.1.1 The Jacobson Radical

Let *R* be any ring, not necessarily commutative. The Jacobson radical of *R* **is the intersection of the annihilators of all simple right *R*-modules.**

There are several equivalent characterizations of the Jacobson radical, such as:

- J(*R*) is the intersection of the regular maximal right (or left) ideals of *R*.
- J(*R*) is the intersection of all the right (or left) primitive ideals of *R*.
- J(*R*) is the maximal right (or left) quasi-regular right (resp. left) ideal of *R*.

As with the nilradical, we can extend this definition to arbitrary two-sided ideals *I* by defining J(*I*) to be the preimage of J(*R/I*) under the projection map $R \to R/I$.

If *R* is commutative, the Jacobson radical always contains the nilradical. If the ring *R* is a finitely generated **Z**-algebra, then the nilradical is equal to the Jacobson radical, and more generally: the radical of any ideal *I* will always be equal to the intersection of all the maximal ideals of *R* that contain *I*. This says that *R* is a Jacobson ring.

3.1.2 The Baer Radical

The Baer radical of a ring is the intersection of the prime ideals of the ring *R*. Equivalently it is the smallest semiprime ideal in *R*. The Baer radical is the lower radical of the class of nilpotent rings. Also called the "lower nilradical" (and denoted $\mathrm{Nil}_* R$), the "prime radical", and the "Baer-McCoy radical". Every element of the Baer radical is nilpotent, so it is a nil ideal.

For commutative rings, this is just the nilradical and closely follows the definition of the radical of an ideal.

3.1.3 The Upper Nil Radical Or Köthe Radical

The sum of the nil ideals of a ring R is the upper nilradical $\mathrm{Nil}^* R$ or Köthe radical and is the unique largest nil ideal of R. Köthe's conjecture asks whether any left nil ideal is in the nilradical.

3.1.4 Singular Radical

An element of a (possibly non-commutative ring) is called left **singular** if it annihilates an essential left ideal, that is, r is left singular if $Ir = 0$ for some essential left ideal I. The setof left singular elements of a ring R is a two-sided ideal, called the left singular ideal, and is denoted . The ideal N of R such that is denoted by and is called the **singular radical** or the **Goldie torsion** of R. The singular radical contains the prime radical (the nilradical in the case of commutative rings) but may properly contain it, even in the commutative case. However, the singular radical of a Noetherian ring is always nilpotent.

3.1.5 The Levitzki Radical

The Levitzki radical is defined as the largest locally nilpotent ideal, analogous to the Hirsch–Plotkin radical in the theory of groups. If the ring is noetherian, then the Levitzki radical is itself a nilpotent ideal, and so is the unique largest left, right, or two-sided nilpotent ideal.

3.1.6 The Brown–Mccoy Radical

The Brown–McCoy radical (called the **strong radical** in the theory of Banach algebra) can be defined in any of the following ways:

- the intersection of the maximal two-sided ideals
- the intersection of all maximal modular ideals
- the upper radical of the class of all simple rings with identity

The Brown–McCoy radical is studied in much greater generality than associative rings.

3.1.7 The Von Neumann Regular Radical

A von Neumann regular ring is a ring A (possibly non-commutative without identity) such that for every a there is some b with $a = aba$. The von Neumann regular rings form a radical class. It contains every matrix ring over a division algebra, but contains no nil rings.

3.1.8 The Artinian Radical

The Artinian radical is usually defined for two-sided Noetherian rings as the sum of all right ideals that are Artinian modules. The definition is left-right symmetric, and indeed produces a two-sided ideal of the ring. This radical is important in the study of Noetherian rings, as outlined by Chatters (1980).

Nil and Nilpotent ideals.

An element a (respectively, an ideal a) of A is nilpotent if a n = 0 (respectively, a n = 0) for some n ≥ 1. An ideal consisting of nilpotent elements is a nil ideal. We have:

• If a is nilpotent, then 1 − a is a unit with inverse 1 + a 1 + a 2 + . . . (note that the sum is finite).

• An ideal is nilpotent if and only if there exists an n such that the product of any n elements all belonging to the ideal vanishes.

• A nilpotent ideal is clearly nil. But not every nil ideal is nilpotent. In fact, in §?? we exhibit a non-zero nil ideal a such that a 2 = a.

The radical of a module.

The radical Rad M of a module M is the intersection of all its maximal submodules, or, equivalently, the intersection of kernels of all homomorphisms into simple modules. We have:

• Rad M vanishes if and only if M is the submodule of a direct product of simple modules; in particular, a semisimple module has trivial radical.

• Homomorphisms map radicals into radicals. If a submodule N is contained in Rad M, then Rad(M/N) = (Rad M)/N. The radical is the smallest submodule N such that Rad(M/N) vanishes. (however, just

because a submodule N contains Rad M, it does not mean that Rad(M/N) vanishes.)

• $\bigoplus$ Rad Mi = Rad $\bigoplus$Mi $\subseteq$ Rad Q Mi $\subseteq$ Q Rad Mi . • Let M be of finite type. Then

– Rad M = M implies M = 0; more generally, N + Rad M = M for a submodule N implies N = M. (If N (M, then choose P maximal submodule with P $\supseteq$ N—this uses the finite generation of M; then Rad M $\subseteq$ P, so N + Rad M $\subseteq$ P.) – x in M belongs to Rad M if and only if for any finite set x1, . . . , xn of generators of M and any set a1, . . . , an of elements of A, the set x1 + a1x, . . . , xn + anx is also a set of generators. (If x1, . . . , xn are generators and a1, . . . , an are such that x1 + a1x, . . . , xn + anx are not, then choose N maximal submodule containing x1 + a1x, . . . , xn + anx. Then x /$\in$ N, for otherwise x1, . . . , xn belong to N, a contradiction. Conversely, suppose x is not in the radical. Then choose maximal N such that x /$\in$ N. Let a1 be such that x1 + N = a1x + N (such an a1 exists since M/N is simple and x /$\in$ N). Let a2, . . . , an be choosen analogously with respect to x2, . . . , xn. Then x1 − a1x, . . . , xn − anx all belong to N and therefore do not generate M.)

3.2 THE RADICAL OF A RING.

The radical Rad A of A is defined to be its radical as a left module over itself: Rad A := Rad AA. The annihilator of a simple module (in other words, a primitive ideal) is evidently the intersection of the annihilators of the non-zero elements of the module; these being all maximal left ideals, we get Rad A = intersection of annihilators of simple (respectively, semisimple) modules

We have:

• Rad A is a two sided ideal. For, annihilators of modules are two sided ideals.

• (Rad A)M $\subseteq$ Rad M, for M/ Rad M is a submodule of a direct product of simple modules and so killed by Rad A. Equality need not hold even in very good cases: e.g. A = Z and M = Z/pnZ with n $\geq$ 1.

• Nakayama's lemma: If M is a of finite type and N a submodule such that N + (Rad A)M = M, then N = M. (For, (Rad A)M ⊆ Rad M. See the relevant sub-item of the last section.) – Let M be of finite type and m a right ideal contained in the radical Rad A. If AA/m ⊗A M = 0, then M = 0. (For, 0 = AA/m ⊗A M ' M/mM menas (Rad A)M = M.) – Let u : M → N be a A-linear map of modules. Let m be a right ideal contained in Rad A, N be finitely generated, and id ⊗ u : AA ⊗A M → AA ⊗A N be surjective. Then u is surjective.

• Let a be a two sided ideal of A. Then Rad(A/a) ⊇ (Rad A + a)/a. If a ⊆ Rad A, then Rad(A/a) = Rad A/a. (The A-module structure of A/a coincides with that of its structure as a module over itself. Now use the relevant items from the last section.)

• The Rad A is the smallest two sided ideal such that A/ Rad A has no radical. (By the previous item it follows that A/ Rad A has no radical as a ring. Conversely, if Rad (A/a) = 0, then (Rad A + a)/a = 0 (previous item), so Rad A ⊆ a.)

Theorem. An element x of the ring A belongs to the radical if and only if 1 − ax has a left inverse for every a in A.

Proof. This follows from the characterization in the last section of elements belonging to the radical of a module of finite type.

We have as corollaries:

• Rad A is the largest left ideal a such that 1 − x has a left inverse for every x in a.

• Rad A is the largest two sided ideal a such that 1 − x is invertible for every x in a. (By the theorem, it suffices to show that 1 − x is invertible when x is in Rad A. We know that it has a left inverse, say y: y(1 − x) = y − yx = 1. We will show that y is invertible, i.e., it also has a left inverse. It will then follow that (1 − x) = y−1 is also invertible. Since z := 1 − y = −yx belongs to Rad A, there exists y 0 such that y 0 is a left inverse for 1 − z = y.)

• Rad (Aopp) = Rad A. (This is a consequence of the previous item.)

• Any nil ideal (left, right, or two sided) is contained in the radical. (The previous item is used in the proof that a right nil ideal is contained in the radical.)

• The radical of a direct product of rings is the direct product of the radicals.

Not every nilpotent element is contained in the radical (e.g., in Mn(C)). But a nilpotent central element belongs to the radical, for the ideal it generates is nil. Rad A is not necessarily a nil ideal; in particular, not necessarily nilpotent. It can happen that Rad A 2 = Rad A even if Rad A is a nil ideal.

Theorem . A left ideal l is contained in Rad A if and only if for every finitely generated non-zero module M we have lM 6= M

Proof. The 'only if' part is Nakayama's lemma. For the if part, the hypothesis implies that lN = 0 for every simple module N (because simple modules are cyclic and contain no non-trivial proper submodules), which means l ⊆ Rad A.

As examples, we have:

• Let A be the ring k[[X1, . . . , Xn]] of formal power series in finitely many variables over a field k. The units in A are the series with non-zero constant term. The elements with vanishing constant term constitute the unique maximal ideal of A, which therefore is the radical. There are no non-trivial nilpotent elements in A. The quotient field of A has of course no radical. Thus the sub-ring of a ring without radical could well have radical.

• Let C be an integral domain and B the polynomial ring C[X1, . . . , Xn] in finitely many variables over C. Then, if n > 0, B has trivial radical: in fact, for 0 6= f, we have deg(1 − fg) > 0 and so 1 − fg is not a unit for g any element of positive degree. Let k be a field. Then k[X1, . . . , Xn] is without radical. But its over ring k[[X1, . . . , Xn]] has non-trivial radical intersecting k[X1, . . . , Xn] non-trivially.

• Let k be a field, S a set, and A the ring of k valued functions on S. Then A is without radical. Indeed, the evaluation at any point s of S gives a morphism A → k, whose kernel is therefore a maximal ideal. The intersections of these maximal ideals as s varies over S is clearly 0.

Proposition . Let A be a principal ring.

(1) A is without radical if and only if either A is a field or A has infinitely many maximal ideals.

(2) A/Ax is without radical if and only if x is square free.

Proof. Let (pα) be a system of representatives of maximal elements. The maximal ideals of A are Apα. In order that

3.3 THE RADICALS OF ARTINIAN RINGS AND MODULES

Theorem Let A be Artinian. Then Rad A is the largest two sided nilpotent ideal of A.

Proof. Any nil ideal (one-sided or two-sided) is contained in the radical, as has already been observed in the last subsection. It suffices to prove therefore that Rad A is nilpotent (we have also observed that Rad A is a two-sided ideal, being the annihilitor of all simple modules). Set r := Rad A. Choose n large enough so that r n = r n+1 = . . . =: a. It suffices to assume that a 6= 0 and arrive at a contradiction.

Assume a 6= 0. Choose a minimal left ideal l with the property that al 6= 0 (such an ideal exists by the Artinian hypotheis: observe that aA = a 6= 0, so the collection of ideals with the property is non-empty). Now, on the one hand, a(rl) = (ar)l = al 6= 0, so that rl has the property; on the other, rl ⊆ l. So rl = l by the minimality of l.

We claim now that l is finitely generated. It will then follow, by Nakayama's lemma, that l = 0, which is a contradiction, since al 6= 0 by choice of l, and the proof will be over.

To prove the claim, we prove in fact that l is cyclic. Indeed, there exists x ∈ l such that ax 6= 0 (by the choice of l); now Ax is such that aAx 6= 0 and Ax ⊆ l, so that Ax = l by the minimality of l.

Corollary . The radical of a commutative Artinian ring equals the subset of its nilpotent elements.

Proof. By Artinianness, the radical is nilpotent. By commutativity, the ideal generated by a nilpotent element is nilpotent, and so contained in the radical.

TheoremM is semisimple of finite length if and only if it is Artinian and Rad M = 0.

Proof. A finite length module is Artinian (and Noetherian); the radical of a semisimple module vanishes. Conversely, suppose that M is Artinian and Rad M = 0. Consider, using Artinianness, a smallest element—call it N—of the set of submodules that are written as finite intersections of maximal submodules. (This collection is non-empty, M itself being the intersection of the empty collection.) If N 6= 0, choose 0 6= n ∈ N. Since Rad M = 0, there exists a maximal submodule K such that n /∈ K. Now, adding K to the collection from which we obtained N, we get a contradiction to the minimality of N, since K ∩ N (N. This shows N = 0. In other words, we have shown that there exist finitely many maximal submodules N1, . . . , Nk of M such that their intersection is 0. This means M ,→ M/N1 ⊕ · · · ⊕ M/Nk. So M is of finite length and semisimple (since so is M/N1 ⊕ · · · ⊕ M/Nk).

We have, as corollories:

• If M is Artinian, then M/ Rad M is semisimple of finite length.

• A is semisimple if and only if it is Artinian with trivial radical.

• If A is Artinian, A/ Rad A is semisimple.

• A is simple if and only if it is Artinian and its only two sided ideals are 0 and itself.

• The following are equivalent for a commutative ring:

– it is Artinian and contains no non-trivial nilpotent elements;

– it is semisimple;

– it is a finite direct product of fields.

• Let k be a field and A a commutative finite dimensional k-algebra. Assume that Rad A = 0. Then A is a finite direct product of fields, each of which is a finite extension of k.

3.4 MODULES OVER ARTINIAN RINGS

Proposition . Let A be an Artinian ring and M an A-module. Then the following are equivalent:

• M is semisimple.

• (Rad A)M = 0.

• AM is semisimple. Proof. If M is semisimple, then Rad M = 0; in general, (Rad A)M ⊆ Rad M, so the first implies the second. If AM is semisimple then of course M is so (being a module for AM).

The hypotheis that A is Artinian will be used only now. Let (Rad A)M = 0. Then AM is a quotient of A/ Rad A. But A/ Rad A is semisimple, it being Artinian and without radical. Hence so is AM.

Proposition . Over an Artinian ring, there exist only finitely many isomorphism classes of simple modules, this number being equal to the number of simple components of A/ Rad A.

Proof. Any simple module is a module also for A/ Rad A. And A/ Rad A is a semisimple ring.

Proposition . Let A be a ring admitting a two sided nilpotent ideal n such that A/n is semisimple (e.g., an Artinian ring). For any A-module, the following conditions are equivalent:

• M is of finite length

• M is Artinian

• M is Noetherian

Proof. If M is of finite length then of course it is both Artinian and Noetherian. Now suppose that n p = 0 and that M is Artinian (respectively, Noetherian). Consider the filtration M ⊇ nM ⊇ n 2M ⊇ . . . ⊇ n p−1M ⊇ n pM = 0. The quotients are M/nM, nM/n 2M, . . . , n p−1M/n pM. These being modules over the semisimple ring A/n, they are on the one hand semisimple. On the other, being sub-quotients of M, they are Artinian (respectively, Noetherian). But a semisimple module is of finite length if it is Artinian (or Noetherian). So each of the quotients is of finite length and therefore so is M.

Corollary . A finitely generated module over an Artinian ring is of finite length. In particular, the ring itself is of finite length. Artinian rings are therefore Noetherian.

Proof. A finitely generated module is Artinian. Now apply the proposition.

Check In Progress-I

Q. 1Define Module over Artinian Ring

Solution

……

……

……

……

Q. 2Define Artinian Ring

Solution

……

……

……

……

Q. 3Define radical Of a Ring.

Solution

……

……

……

……

3.5 RADICAL OF A MODULE

In mathematics, in the theory of modules, the radical of a module is a component in the theory of structure and classification. It is a generalization of the Jacobson radical for rings. In many ways, it is the dual notion to that of the socle soc(*M*) of *M*. Let A be a ring (with identity according to our convention) and M an A-module. For additive subgroups U and V of A and M respectively, we denote by UV the subset of M consisting of finite sums P i uivi with ui and vi in U and V respectively. Thus UV is a submodule if U is a left ideal; the product of left ideals is a left ideal; the product of a left ideal and a right ideal is a two-sided ideal.

Definition

Let *R* be a ring and *M* a left *R*-module. A submodule *N* of *M* is called maximal or cosimple if the quotient *M*/*N* is a simple module.

The radical of the module M is the intersection of all maximal submodules of M,

Properties

- In addition to the fact rad(M) is the sum of superfluous submodules, in a Noetherian module rad(M) itself is a superfluous submodule.
- A ring for which rad(M) ={0} for every right R module M is called a right V-ring.
- For any module M, rad(M/rad(M)) is zero.
- M is a finitely generated module if and only if M/rad(M) is finitely generated and rad(M) is a superfluous submodule of M.

3.6 PRIMARY DECOMPOSITION

In mathematics, the Lasker–Noether theorem states that every Noetherian ring is a Lasker ring, which means that every ideal can be decomposed as an intersection, called primary decomposition, of finitely many *primary ideals* (which are related to, but not quite the same as, powers of prime ideals). The theorem was first proven by Emanuel Lasker (1905) for the special case of polynomial rings and convergent power series rings, and was proven in its full generality by Emmy Noether (1921).

The Lasker–Noether theorem is an extension of the fundamental theorem of arithmetic, and more generally the fundamental theorem of finitely generated abelian groups to all Noetherian rings. The Lasker–Noether theorem plays an important role in algebraic geometry, by asserting that every algebraic set may be uniquely decomposed into a finite union of irreducible components.

It has a straightforward extension to modules stating that every submodule of a finitely generated module over a Noetherian ring is a finite intersection of primary submodules. This contains the case for rings as a special case, considering the ring as a module over itself, so that ideals are submodules. This also generalizes the primary decomposition form of the structure theorem for finitely generated modules over a principal ideal domain, and for the special case of

polynomial rings over a field, it generalizes the decomposition of an algebraic set into a finite union of (irreducible) varieties.

The first algorithm for computing primary decompositions for polynomial rings over a field of characteristic 0[Note 1] was published by Noether's student Grete Hermann (1926).[1][*better source needed*] The decomposition does not hold in general for non-commutative Noetherian rings. Noether gave an example of a non-commutative Noetherian ring with a right ideal that is not an intersection of primary ideals.

Definitions

Write R for a commutative ring, and M and N for modules over it.

- A zero divisor of a module M is an element x of R such that $xm = 0$ for some non-zero m in M.
- An element x of R is called nilpotent in M if $x^nM = 0$ for some positive integer n.
- A module M is called coprimary if every zero divisor of M is nilpotent in M. For example, groups of prime power order and free abelian groups are coprimary modules over the ring of integers.
- A submodule M of a module N is called a primary submodule if N/M is coprimary.
- An ideal I is called primary if it is a primary submodule of R. This is equivalent to saying that if ab is in I then either a is in I or b^n is in I for some n, and to the condition that every zero-divisor of the ring R/I is nilpotent.
- A submodule M of a module N is called irreducible if it is not an intersection of two strictly larger submodules.
- An associated prime of a module M is a prime ideal that is the annihilator of some element of M.

Statement

The Lasker–Noether theorem for modules states every submodule of a finitely generated module over a Noetherian ring is a finite intersection of primary submodules. For the special case of ideals it states that every ideal of a Noetherian ring is a finite intersection of primary ideals.

An equivalent statement is: every finitely generated module over a Noetherian ring is contained in a finite product of coprimary modules.

The Lasker–Noether theorem follows immediately from the following three facts:

- Any submodule of a finitely generated module over a Noetherian ring is an intersection of a finite number of irreducible submodules.
- If M is an irreducible submodule of a finitely generated module N over a Noetherian ring then N/M has only one associated prime ideal.
- A finitely generated module over a Noetherian ring is coprimary if and only if it has at most one associated prime.

A proof in a somewhat different flavor is given below.

Minimal Decompositions and Uniqueness

In this section, all modules will be finitely generated over a Noetherian ring R.

A primary decomposition of a submodule M of a module N is called **minimal** if it has the smallest possible number of primary modules. For minimal decompositions, the primes of the primary modules are uniquely determined: they are the associated primes of N/M. Moreover, the primary submodules associated to the **minimal** or **isolated** associated primes (those not containing any other associated primes) are also unique. However the primary submodules associated to the non-minimal associated primes (called **embedded primes** for geometric reasons) need not be unique.

Example: Let $N = R = k[x, y]$ for some field k, and let M be the ideal (xy, y^2). Then M has two different minimal primary decompositions $M = (y) \cap (x, y^2) = (y) \cap (x + y, y^2)$. The minimal prime is (y) and the embedded prime is (x, y).

Non-Noetherian case

The next theorem gives necessary and sufficient conditions for a ring to have primary decompositions for its ideals.

Theorem — Let R be a commutative ring. Then the following are equivalent.

1. Every ideal in R has a primary decomposition.
2. R has the following properties:
   - (L1) For every proper ideal I and a prime ideal P, there exists an x in R - P such that $(I : x)$ is the pre-image of $I R_P$ under the localization map $R \to R_P$.
   - (L2) For every ideal I, the set of all pre-images of $I S^{-1}R$ under the localization map $R \to S^{-1}R$, S running over all multiplicatively closed subsets of R, is finite.

We continue to let A denote a ring and M an A–module. As in the case of ideals, the primary decomposition of modules into primary submodules will be achieved using the auxiliary notion of irreducible submodules. To compare the notions and results discussed in this section to those in the classical case, you may substitute A for M.

Check In Progress-II

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

Q. 1 Let R be a commutative ring. Then the following are equivalent.

1. Every ideal in R has a primary decomposition.

Solution

……

……

……

……

……

Q. 2 Define Radical Of a Module

Solution

……

……

……

……

Definition: Let Q be a submodule of M. We say that Q is primary if Q = M and for any a ∈ A and x ∈ M, we have ax ∈ Q and x /∈ Q =⇒ a nM ⊆ Q for some n ≥ 1. We say that Q is irreducible if Q 6= M and for any submodules N1 and N2 of M we have

Q = N1 ∩ N2 =⇒ Q = N1 or Q = N2.

Clearly, a submodule Q of M is primary iff every zerodivisor of M/Q is nilpotent for M/Q. [An element a ∈ A is said to be nilpotent for M if a nM = 0 for some n ≥ 1. In other words, a is nilpotent for M iff a ∈ p Ann(M).] If Q is a primary submodule of M and p = p Ann(M/Q), we say that Q is p–primary.

As we shall see in the sequel, the above characterization of primary submodules [of f. g. modules over noetherian rings] is extremely useful. For this reason perhaps, it is sometimes taken as a definition of primary submodules [of arbitrary modules]. At any rate, we may tacitly use the above characterizations of primary and p–primary submodules in several of the proofs below.

Lemma. Suppose A is noetherian, M is f. g., and Q1, . . . , Qr are p–primary submodules of M, where r is a positive integer. Then Q1 ∩ · · · ∩ Qr is also p–primary.

Proof: Clearly, Q1 ∩ · · · ∩ Qr 6= M. Moreover, there is a natural injective homomorphism of M/Q1 ∩ · · · ∩ Qr into M/Q1 ⊕ · · · ⊕ M/Qr.

∅ = Ass(M/Q1 ∩ · · · ∩ Qr) ⊆ Ass (⊕ r i=1M/Qi) = ∪ r i=1Ass(M/Qi) = {p}. Thus it follows from that Q1 ∩ · · · ∩ Qr is p–primary.

Lemma. If M is noetherian, then every submodule of M is a finite intersection of irreducible submodules of M.

Proof: Assume the contrary. Then we can find a maximal element, say Q, among the submodules of M which aren't finite intersections of irreducible submodules of M. Now Q can't be irreducible. Also Q 6= M (because M is the intersection of the empty family of irreducible submodules of M). Hence Q = N1 ∩ N2 for some submodules N1 and N2 of M with N1 6= Q and N2 6= Q. By maximality of Q, both N1 and N2 are finite intersections of irreducible submodules of M. But then so is Q, which is a contradiction.

Lemma. Suppose A is noetherian, M is f. g., and Q is an irreducible submodule of M. Then Q is primary.

Proof: Since Q 6= M, Ass(M/Q) 6= ∅. Suppose Ass(M/Q) contains two distinct prime ideals p1 = (0 : ¯x1) and p2 = (0 : ¯x2), where ¯x1, x¯2 denote the images in M/Q of some elements x1, x2 of M. Clearly ¯x1 and ¯x2 are nonzero elements of M/Q. We claim that Ax¯1 ∩Ax¯2 = {0} Indeed, if ax¯1 = bx¯2, with a, b ∈ A, is nonzero, then a /∈ (0 : ¯x1) and b /∈ (0 : ¯x2). Since (0 : ¯x1) is prime, we find that (0 : ¯x1) = (0 : ax¯1) (check!). Similarly, (0 : ¯x2) = (0 : bx¯2). This gives p1 = p2, which is a contradiction. Now if y ∈ (Q + Ax1) ∩ (Q + Ax2), then y = y1 + ax1 = y2 + bx2 for some y1, y2 ∈ Q and a, b ∈ A. But then ax¯1 = bx¯2 in M/Q and thus y ∈ Q. It follows that Q = (Q + Ax1) ∩ (Q + Ax2). Also since ¯x1 6= 0 6= ¯x2, we have (Q + Ax1) 6= Q 6= (Q + Ax2). This contradicts the irreducibility of Q. Thus Ass(M/Q) is singleton so that Q is primary.

Lemma. Suppose A is noetherian, M is f. g., Q is a p–primary submodule of M. Then the inverse image of Qp under the natural map M → Mp (given by x 7→ x 1) is Q.

Proof: Suppose x ∈ M is such that x 1 ∈ Qp. Then tx ∈ Q for some t ∈ A \ p. If x /∈ Q, then x¯, the image of x in M/Q, is nonzero, and thus t ∈ Z(M/Q). Hence from (2.1), we see that t ∈ p, which is a contradiction.

Remark: Given any p ∈ Spec A and a submodule Q0 of Mp, the inverse image of Q0 under the natural map M → Mp is often denoted by Q0 ∩ M. Thus (2.5) can be expressed by saying that if Q is a p–primary submodule of M, then Qp ∩ M = Q. Note that we have been tacitly using

the fact that if Q is any submodule of M and S is any m. c. subset of A, then S −1Q can be regarded as a submodule of S −1M.

Example: Let G be a finite abelian group of order n. Let the notation be as in the Example preceding (1.5). For $1 \leq i \leq h$, let Qi = P1 + · · · + Pi−1 + Pi+1 + · · · + Ph. Then G/Qi ' Pi , and thus Qi is piZ–primary. Observe that (0) = Q1 ∩ · · · ∩ Qh is an irredundant primary decomposition of (0); in fact, this decomposition is unique because each of the associated primes p1Z, . . . , phZ is clearly minimal. In general, if N is a subgroup, i.e., a Z–submodule, of G, and Λ = {i : $1 \leq i \leq h$ and N + Qi 6= G}, then N = ∩i∈Λ(N + Qi) is an irredundant primary decomposition of N, and this too is unique. Verify!

Definition: A prime ideal p of A is called an associated prime of M if p = (0 : x) for some x ∈ M. The set of all associated primes of M is denoted by AssA(M), or simply by Ass(M). Minimal elements of Ass(M) are called the minimal primes of M, and the remaining elements of Ass(M) are called the embedded primes of M.

Lemma. For any submodule N of M, Ass(N) ⊆ Ass(M) ⊆ Ass(N) ∪ Ass(M/N). More generally, if 0 = M0 ⊆ M1 ⊆ · · · ⊆ Mn = M is any chain of submodules of M, then Ass(M) ⊆∪n i=1Ass(Mi/Mi−1).

Proof: The inclusion Ass(N) ⊆ Ass(M) is obvious. Let x ∈ M be such that (0 : x) ∈ Ass(M). If (0 : x) ∈/ Ass(N), then we claim that (0 : x) = (0 : ¯x) ∈ Ass(M/N), where ¯x denotes the image of x in M/N. To see this, note that (0 : x) ⊆ (0 : ¯x) and if a ∈ A is such that ax¯ = 0 6= ax, then ax ∈ N and a /∈ (0 : x), and since (0 : x) is prime, we have b ∈ (0 : ax) ⇔ ba ∈ (0 : x) ⇔ b ∈ (0 : x); consequently, (0 : x) = (0 : ax) ∈ Ass(N), which is a contradiction. Thus Ass(M) ⊆ Ass(N) ∪ Ass(M/N). The last assertion follows from this by induction on n.

Example: Let G be a finite abelian group of order n. Suppose n = p e1 1 . . . p eh h , where p1, . . . , ph are distinct prime numbers and e1, . . . , eh are positive integers. Then G is a Z–module, and the pi–Sylow subgroups Pi , $1 \leq i \leq h$, are Z–submodules of G such that G ' P1 ⊕ · · · ⊕ Ph. Clearly, Ass(Pi) = piZ [indeed, if y is any nonzero element of Pi of order p e i , then elements of (0 : y) are multiples of p e i , and if x = p e−1 i y,

then (0 : x) = piZ]. Thus by (1.4), Ass(G) = {p1Z, . . . , phZ}. More generally, if M is a finitely generated abelian group, then M = Z r ⊕ T for some r ≥ 0 and some finite abelian group T, and it follows from (1.4) that if r > 0 then Ass(M) = {l0Z, l1Z, . . . , lsZ}, where l0 = 0 and l1, . . . ls are the prime numbers dividing the order of T.

3.7 LET US SUM UP

In this unit we study radical module and also study Noetherian Ring which contains a power of radical .We study primary decomposition and its properties. We study module over Artinian Ring and its proposition and some example. We study some lemma for primary decomposition ring. We study Jaconson Radical and Some of its properties.

1. A radical class (also called radical property or just radical) is a class σ of rings possibly without identities, such that:
    1. the homomorphic image of a ring in σ is also in σ
    2. every ring *R* contains an ideal *S*(*R*) in σ that contains every other ideal of *R* that is in σ
    3. *S*(*R*/*S*(*R*)) = 0. The ideal *S*(*R*) is called the radical, or σ-radical, of *R*.

Let *R* be any ring, not necessarily commutative. The Jacobson radical of *R* is the intersection of the annihilators of all simple right *R*-modules.

2. If the ring is noetherian, then the Levitzki radical is itself a nilpotent ideal, and so is the unique largest left, right, or two-sided nilpotent ideal.
3. The Brown–McCoy radical can be defined in any of the following ways:
    1. the intersection of the maximal two-sided ideals
    2. the intersection of all maximal modular ideals
    3. the upper radical of the class of all simple rings with identity
4. An element x of the ring A belongs to the radical if and only if 1 − ax has a left inverse for every a in A.

The radical of a commutative Artinian ring equals the subset of its nilpotent elements.

M is semisimple of finite length if and only if it is Artinian and Rad M = 0.

8. Let A be an Artinian ring and M an A-module. Then the following are equivalent:

• M is semisimple.

• (Rad A)M = 0.

• AM is semisimple. Proof. If M is semisimple, then Rad M = 0; in general, (Rad A)M⊆ Rad M, so the first implies the second. If AM is semisimple then of course M is so (being a module for AM

9. The Lasker–Noether theorem follows immediately from the following three facts:

Any submodule of a finitely generated module over a Noetherian ring is an intersection of a finite number of irreducible submodules.

If *M* is an irreducible submodule of a finitely generated module *N* over a Noetherian ring then *N*/*M* has only one associated prime ideal.

A finitely generated module over a Noetherian ring is coprimary if and only if it has at most one associated prime.

3.8 KEYOWRD

Radical : Advocating or based on thorough or complete political or social change; representing or supporting an extreme or progressive section of a political party.

Module : Each of a set of standardized parts or independent units that can be used to construct a more complex structure, such as an item of furniture or a building.

Noetherian : The adjective *Noetherian* is used to describe objects that satisfy an ascending or descending chain condition on certain kinds of subobjects, *meaning* that certain ascending or descending sequences of .

3.9 QUESTIONS FOR REVIEW

Q. 1 Every ideal of a Noetherian ring contains a power of its radical

Q. 2 Find an example of a Noetherian ring whose Jacobson radical does not equal the nilradical.

Q. 3 Show that if a ring satisfies the d.c.c. on ideals then the nilradical and Jacobson radical are equal.

Q. 4 Find an example of an ideal I of a ring A which does not contain a power of its radical r(I) (so necessarily A is not Noetherian)

Q.. 5 Let A be Noetherian, Q and M ideals of A with M maximal. TFAE

(i) Q is M-primary;

(ii) $r(Q) = M$;

(iii) $M^n \subseteq Q \subseteq M$ $(\exists n > 0)$.

3.10 ANSWER FOR CHECK IN PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 4

Q. 2 Check in Section 3

Q. 3 Check in Section 2

Check in Progress-II

Answer Q. 1 Check in Section 6

Q. 2 Check in Section 5

3.11 SUGGESTION READING AND REFERENCE

- *Andrunakievich, V.A. (2001) [1994], "Radical of ring and algebras", in Hazewinkel, Michiel (ed.), Encyclopedia of Mathematics, Springer*

Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4

- *Chatters, A. W.; Hajarnavis, C. R. (1980), Rings with Chain Conditions, Research Notes in Mathematics, **44**, Boston, Mass.: Pitman (Advanced Publishing Program), pp. vii+197, ISBN 0-273-08446-1, MR 0590045*
- *Divinsky, N. J. (1965), Rings and Radicals, Mathematical Expositions No. 14, University of Toronto Press, MR 0197489*
- *Gardner, B. J.; Wiegandt, R. (2004), Radical Theory of Rings, Monographs and Textbooks in Pure and Applied Mathematics, **261**, Marcel Dekker, ISBN 978-0-8247-5033-6, MR 2015465*
- *Goodearl, K. R. (1976), Ring Theory, Marcel Dekker, ISBN 978-0-8247-6354-1, MR 0429962*
- *Gray, Mary W. (1970), A Radical Approach to Algebra, Addison-Wesley, MR 0265396*
- *Köthe, Gottfried (1930), "Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist", Mathematische Zeitschrift, **32** (1): 161–186, doi:10.1007/BF01194626*
- *Stenström, Bo (1971), Rings and Modules of Quotients, Lecture Notes in Mathematics, **237**, Springer-Verlag, doi:10.1007/BFb0059904, ISBN 978-3-540-05690-4, MR 0325663, Zbl 0229.16003*
- *Wiegandt, Richard (1974), Radical and Semisimple Classes of Rings, Kingston, Ont.: Queen's University, MR 0349734*
  - *Alperin, J.L.; Rowen B. Bell (1995). Groups and representations. Springer-Verlag. p. 136. ISBN 0-387-94526-1.*
  - *Anderson, Frank Wylie; Kent R. Fuller (1992). Rings and Categories of Modules. Springer-Verlag. ISBN 978-0-387-97845-1.*
  - *Gardner, B. J.; Wiegandt, R. (2004), Radical Theory of Rings, Monographs and Textbooks in Pure and Applied Mathematics, **261**, Marcel Dekker, ISBN 978-0-8247-5033-6, MR 2015465*

UNIT 4 - MODULE, SUB-MODULE, QUOTIENT MODULE

STRUCTURE

4.0 OBJECTIVE

* Learn about module theory

* learn sub-module

* work with quotient module

* work on Submorphism and Homomorphism

* Learn relation b/w representation theory

4.1 INTRODUCTION: MODULE

In mathematics, a **module** is one of the fundamental algebraic structures used in abstract algebra. A **module over a ring** is a generalization of the notion of vector space over a field, wherein the corresponding scalars are the elements of an arbitrary given ring (with identity) and a multiplication (on the left and/or on the right) is defined between elements of the ring and elements of the module. A module taking its scalars from a ring *R* is called an *R*-module.

Thus, a module, like a vector space, is an additive abelian group; a product is defined between elements of the ring and elements of the module that is distributive over the addition operation of each parameter and is compatible with the ring multiplication.

Modules are very closely related to the representation theory of groups. They are also one of the central notions of commutative algebra and homological algebra, and are used widely in algebraic geometry and algebraic topology.

4.2 MOTIVATION

In a vector space, the set of scalars is a field and acts on the vectors by scalar multiplication, subject to certain axioms such as the distributive law. In a module, the scalars need only be a ring, so the module concept represents a significant generalization. In commutative algebra, both ideals and quotient rings are modules, so that many arguments about ideals or quotient rings can be combined into a single argument about modules. In non-commutative algebra the distinction between left ideals, ideals, and modules becomes more pronounced, though some ring-theoretic conditions can be expressed either about left ideals or left modules.

Much of the theory of modules consists of extending as many of the desirable properties of vector spaces as possible to the realm of modules over a "well-behaved" ring, such as a principal ideal domain. However, modules can be quite a bit more complicated than vector spaces; for instance, not all modules have a basis, and even those that do, free

modules, need not have a unique rank if the underlying ring does not satisfy the invariant basis number condition, unlike vector spaces, which always have a (possibly infinite) basis whose cardinality is then unique. (These last two assertions require the axiom of choice in general, but not in the case of finite-dimensional spaces, or certain well-behaved infinite-dimensional spaces such as L^p spaces.)

4.3 FORMAL DEFINITION

Suppose that R is a ring and 1_R is its multiplicative identity. A **left R-module** M consists of an abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that for all r, s in R and x, y in M, we have:

1. The operation of the ring on M is called *scalar multiplication*, and is usually written by juxtaposition, i.e. as rx for r in R and x in M, though here it is denoted as $r \cdot x$ to distinguish it from the ring multiplication operation, denoted here by juxtaposition. The notation ${}_RM$ indicates a left R-module M. A **right R-module** M or M_R is defined similarly, except that the ring acts on the right; i.e., scalar multiplication takes the form $\cdot : M \times R \to M$, and the above axioms are written with scalars r and s on the right of x and y.

Authors who do not require rings to be unital omit condition 4 above in the definition of an R-module, and so would call the structures defined above "unital left R-modules". In this article, consistent with the glossary of ring theory, all rings and modules are assumed to be unital.[1]

If one writes the scalar action as f_r so that $f_r(x) = r \cdot x$, and f for the map that takes each r to its corresponding map f_r , then the first axiom states that every f_r is a group endomorphism of M, and the other three axioms assert that the map $f : R \to \mathrm{End}(M)$ given by $r \mapsto f_r$ is a ring homomorphism from R to the endomorphism ring $\mathrm{End}(M)$.[2] Thus a module is a ring action on an abelian group (cf. group action. Also consider monoid action of multiplicative structure of R). In this sense, module theory generalizes representation theory, which deals with group actions on vector spaces, or equivalently group ring actions.

A bimodule is a module that is a left module and a right module such that the two multiplications are compatible.

If R is commutative, then left R-modules are the same as right R-modules and are simply called R-modules.

Examples

- If K is a field, then K-vector spaces (vector spaces over K) and K-modules are identical.
- If K is a field, and $K[x]$ a univariate polynomial ring, then a $K[x]$-module M is a K-module with an additional action of x on M that commutes with the action of K on M. In other words, a $K[x]$-module is a K-vector space M combined with a linear map from M to M. Applying the Structure theorem for finitely generated modules over a principal ideal domain to this example shows the existence of the rational and Jordan canonical forms.
- The concept of a $\mathbf{Z}$-module agrees with the notion of an abelian group. That is, every abelian group is a module over the ring of integers $\mathbf{Z}$ in a unique way. For $n > 0$, let $n \cdot x = x + x + ... + x$ (n summands), $0 \cdot x = 0$, and $(-n) \cdot x = -(n \cdot x)$. Such a module need not have a basis—groups containing torsion elements do not. (For example, in the group of integers modulo 3, one cannot find even one element which satisfies the definition of a linearly independent set since when an integer such as 3 or 6 multiplies an element, the result is 0. However, if a finite field is considered as a module over the same finite field taken as a ring, it is a vector space and does have a basis.)
- The decimal fractions (including negative ones) form a module over the integers. Only singletons are linearly independent sets, but there is no singleton that can serve as a basis, so the module has no basis and no rank.
- If R is any ring and n a natural number, then the Cartesian product R^n is both a left and right R-module over if we use the component-wise operations. Hence when $n = 1$, R is an R-module, where the scalar multiplication is just ring multiplication. The case $n = 0$ yields the trivial R-module $\{0\}$ consisting only of its

identity element. Modules of this type are called free and if R has invariant basis number (e.g. any commutative ring or field) the number n is then the rank of the free module.

- If $\mathrm{M}_n(R)$ is the ring of $n \times n$ matrices over a ring R, M is an $\mathrm{M}_n(R)$-module, and e_i is the $n \times n$ matrix with 1 in the (i, i)-entry (and zeros elsewhere), then e_iM is an R-module, since $re_im = e_irm \in e_iM$. So M breaks up as the direct sum of R-modules, $M = e_1M \oplus ... \oplus e_nM$. Conversely, given an R-module M_0, then $M_0{}^{\oplus n}$ is an $\mathrm{M}_n(R)$-module. In fact, the category of R-modules and the category of $\mathrm{M}_n(R)$-modules are equivalent. The special case is that the module M is just R as a module over itself, then R^n is an $\mathrm{M}_n(R)$-module.
- If S is a nonempty set, M is a left R-module, and M^S is the collection of all functions $f : S \to M$, then with addition and scalar multiplication in M^S defined by $(f + g)(s) = f(s) + g(s)$ and $(rf)(s) = rf(s)$, M^S is a left R-module. The right R-module case is analogous. In particular, if R is commutative then the collection of *R-module homomorphisms* $h : M \to N$ (see below) is an R-module (and in fact a *submodule* of N^M).
- If X is a smooth manifold, then the smooth functions from X to the real numbers form a ring $C^\infty(X)$. The set of all smooth vector fields defined on X form a module over $C^\infty(X)$, and so do the tensor fields and the differential forms on X. More generally, the sections of any vector bundle form a projective module over $C^\infty(X)$, and by Swan's theorem, every projective module is isomorphic to the module of sections of some bundle; the category of $C^\infty(X)$-modules and the category of vector bundles over X are equivalent.
- If R is any ring and I is any left ideal in R, then I is a left R-module, and analogously right ideals in R are right R-modules.
- If R is a ring, we can define the ring R^{op} which has the same underlying set and the same addition operation, but the opposite multiplication: if $ab = c$ in R, then $ba = c$ in R^{op}. Any *left* R-module M can then be seen to be a *right* module over R^{op}, and any right module over R can be considered a left module over R^{op}.
- There are modules of a Lie algebra as well.

4.4 SUBMODULES AND HOMOMORPHISMS

Suppose M is a left R-module and N is a subgroup of M. Then N is a **submodule** (or more explicitly an R-submodule) if for any n in N and any r in R, the product $r \cdot n$ is in N (or $n \cdot r$ for a right R-module).

The set of submodules of a given module M, together with the two binary operations + and ∩, forms a lattice which satisfies the **modular law**: Given submodules U, N_1, N_2 of M such that $N_1 \subset N_2$, then the following two submodules are equal: $(N_1 + U) \cap N_2 = N_1 + (U \cap N_2)$.

If M and N are left R-modules, then a map $f : M \to N$ is a **homomorphism of *R*-modules** if for any m, n in M and r, s in R

.

This, like any homomorphism of mathematical objects, is just a mapping which preserves the structure of the objects. Another name for a homomorphism of R-modules is an R-linear map.

A bijective module homomorphism is an isomorphism of modules, and the two modules are called *isomorphic*. Two isomorphic modules are identical for all practical purposes, differing solely in the notation for their elements.

The kernel of a module homomorphism $f : M \to N$ is the submodule of M consisting of all elements that are sent to zero by f.
The isomorphism theorems familiar from groups and vector spaces are also valid for R-modules.

Given a ring R, the set of all left R-modules together with their module homomorphisms forms an abelian category, denoted by R-**Mod** (see category of modules).

Types of modules

Finitely generated. An R-module M is finitely generated if there exist finitely many elements $x_1, ..., x_n$ in M such that every element of M is a linear combination of those elements with coefficients from the ring R.

Cyclic. A module is called a cyclic module if it is generated by one element.

Free. A free R-module is a module that has a basis, or equivalently, one that is isomorphic to a direct sum of copies of the ring R. These are the modules that behave very much like vector spaces.

Projective. Projective modules are direct summands of free modules and share many of their desirable properties.

Injective. Injective modules are defined dually to projective modules.

Flat. A module is called flat if taking the tensor product of it with any exact sequence of R-modules preserves exactness.

Torsionless module. A module is called torsionless if it embeds into its algebraic dual.

Simple. A simple module S is a module that is not $\{0\}$ and whose only submodules are $\{0\}$ and S. Simple modules are sometimes called *irreducible*.

Semisimple. A semisimple module is a direct sum (finite or not) of simple modules. Historically these modules are also called *completely reducible*.

Indecomposable. An indecomposable module is a non-zero module that cannot be written as a direct sum of two non-zero submodules. Every simple module is indecomposable, but there are indecomposable modules which are not simple (e.g. uniform modules).

Faithful. A faithful module M is one where the action of each $r \neq 0$ in R on M is nontrivial (i.e. $r \cdot x \neq 0$ for some x in M). Equivalently, the annihilator of M is the zero ideal.

Torsion-free. A torsion-free module is a module over a ring such that 0 is the only element annihilated by a regular element (non zero-divisor) of the ring.

Noetherian. A Noetherian module is a module which satisfies the ascending chain condition on submodules, that is, every

increasing chain of submodules becomes stationary after finitely many steps. Equivalently, every submodule is finitely generated.

Artinian. An Artinian module is a module which satisfies the descending chain condition on submodules, that is, every decreasing chain of submodules becomes stationary after finitely many steps.

Graded. A graded module is a module with a decomposition as a direct sum $M = \oplus_x M_x$ over a graded ring $R = \oplus_x R_x$ such that $R_x M_y \subset M_{x+y}$ for all x and y.

Uniform. A uniform module is a module in which all pairs of nonzero submodules have nonzero intersection.

4.5 RELATION TO REPRESENTATION THEORY

If M is a left R-module, then the *action* of an element r in R is defined to be the map $M \to M$ that sends each x to rx (or xr in the case of a right module), and is necessarily a group endomorphism of the abelian group $(M, +)$. The set of all group endomorphisms of M is denoted $\mathrm{End}_{\mathbf{Z}}(M)$ and forms a ring under addition and composition, and sending a ring element r of R to its action actually defines a ring homomorphism from R to $\mathrm{End}_{\mathbf{Z}}(M)$.

Such a ring homomorphism $R \to \mathrm{End}_{\mathbf{Z}}(M)$ is called a *representation* of R over the abelian group M; an alternative and equivalent way of defining left R-modules is to say that a left R-module is an abelian group M together with a representation of R over it.

A representation is called *faithful* if and only if the map $R \to \mathrm{End}_{\mathbf{Z}}(M)$ is injective. In terms of modules, this means that if r is an element of R such that $rx = 0$ for all x in M, then $r = 0$. Every abelian group is a faithful module over the integers or over some modular arithmetic $\mathbf{Z}/n\mathbf{Z}$.

Generalizations

Any ring R can be viewed as a preadditive category with a single object. With this understanding, a left R-module is just a covariant additive

functor from *R* to the category **Ab** of abelian groups, and right *R*-modules are contravariant additive functors. This suggests that, if *C* is any preadditive category, a covariant additive functor from *C* to **Ab** should be considered a generalized left module over *C*. These functors form a functor category *C*-**Mod** which is the natural generalization of the module category *R*-**Mod**.

Modules over *commutative* rings can be generalized in a different direction: take a ringed space (X, O_X) and consider the sheaves of O_X-modules (see sheaf of modules). These form a category O_X-**Mod**, and play an important role in modern algebraic geometry. If *X* has only a single point, then this is a module category in the old sense over the commutative ring $O_X(X)$.

One can also consider modules over a semiring. Modules over rings are abelian groups, but modules over semirings are only commutative monoids. Most applications of modules are still possible. In particular, for any semiring *S*, the matrices over *S* form a semiring over which the tuples of elements from *S* are a module (in this generalized sense only). This allows a further generalization of the concept of vector space incorporating the semirings from theoretical computer science.

Over near-rings, one can consider near-ring modules, a nonabelian generalization of modules.

A module is a separate unit of software or hardware. Typical characteristics of modular components include portability, which allows them to be used in a variety of systems, and interoperability, which allows them to function with the components of other systems. The term was first used in architecture.

In computer programming, especially in older languages such as PL/1, the output of the language compiler was known as an *object module* to distinguish it from the set of *source* language statements, sometimes known as the *source module*. In mainframe systems such as IBM's OS/360, the object module was then linked together with other object modules to form a *load module*. The load module was the executable code that you ran in the computer.

Modular programming is the concept that similar functions should be contained within the same unit of programming code and that separate functions should be developed as separate units of code so that the code can easily be maintained and reused by different programs. Object-oriented programming is a newer idea that inherently encompasses modular programming.

2) In computer hardware and electronics, a module is a relatively compact unit in a larger device or arrangement that is designed to be separately installed, replaced, or serviced. For example, a single in-line memory module is a unit of random access memory (RAM) that you can add to a personal computer.

Check In Progress-I

Q. 1 Define Submodule.

Solution

……

……

……

……

Q. 2 Define Relation of Representation Theorey.

Solution

……

……

……

……

……

4.7 SUBMODULES

It often happens that while working on one project, you need to use another project from within it. Perhaps it's a library that a third party developed or that you're developing separately and using in multiple

parent projects. A common issue arises in these scenarios: you want to be able to treat the two projects as separate yet still be able to use one from within the other.

Here's an example. Suppose you're developing a website and creating Atom feeds. Instead of writing your own Atom-generating code, you decide to use a library. You're likely to have to either include this code from a shared library like a CPAN install or Ruby gem, or copy the source code into your own project tree. The issue with including the library is that it's difficult to customize the library in any way and often more difficult to deploy it, because you need to make sure every client has that library available. The issue with copying the code into your own project is that any custom changes you make are difficult to merge when upstream changes become available.

Git addresses this issue using submodules. Submodules allow you to keep a Git repository as a subdirectory of another Git repository. This lets you clone another repository into your project and keep your commits separate.

Starting with Submodules

We'll walk through developing a simple project that has been split up into a main project and a few sub-projects.

Let's start by adding an existing Git repository as a submodule of the repository that we're working on. To add a new submodule you use the git submodule add command with the absolute or relative URL of the project you would like to start tracking. In this example, we'll add a library called "DbConnector"

Call a subgroup M' of an A-module M a submodule if M' is closed under scalar multiplication, that is,

$(\forall a \in A)(\forall x \in M')\ ax \in M'$.

In this case we can form the quotient group

$M/M' = \{ x + M' \mid x \in M \}$,

which becomes an A-module by defining

$a(x + M') = ax + M'$ $(\forall a \in A , x \in M)$.

Call M/M' the quotient of M by M'

Easy to see:

The natural map:

$M \to M/M' , x \mapsto x + M'$

is a surjective module homomorphism with kernel M' ,

which induces a one-one correspondence between submodules of M/M' and submodules of M which contain M' .

Let $f : M \to N$ be a module homomorphism.

Terminology and notation: write

$\ker f = \{ x \in M \mid f(x) = 0 \}$,

$\text{im } f = f(M) = \{ f(x) \mid x \in M \}$,

$\text{coker } f = N/\text{im } f$

for the kernel, image and cokernel of f respectively.

Easy to check:

ker f is a submodule of M , and

im f is a submodule of N (so coker f makes sense).

Consider a submodule M' of M such that

$M' \subseteq \ker f$.

Define

$f : M/M' \to N$ by $x + M' \mapsto f(x)$ $(\forall x \in M)$.

This is well-defined because if

$x + M' = x0 + M'$

then $x - x0 \in M' \subseteq \ker f$, so that

$f(x) = f(x - x0 + x0) = f(x - x0) + f(x0)$

$= 0 + f(x0) = f(x0)$.

It is routine to verify that f is a module homomorphism, and

$\ker f = \ker f/M'$

Call f the homomorphism induced by f .

If $M' = \ker f$ then f becomes one-one, which proves another version of the

4.8 QUOTIENT MODULE

In algebra, given a module and a submodule, one can construct their **quotient module**.

This construction, described below, is very similar to that of a quotient vector space. It differs from analogous constructions of quotient groups and quotient rings by the fact that in these cases, the subspace that is used for defining the quotient is not of the same nature as the ambient space (that is, the quotient of a group by a subgroup is not always a group, and a quotient ring is the quotient of a ring by an ideal, not a subring).

Given a module *A* over a ring *R*, and a submodule *B* of *A*, the quotient space *A*/*B* is defined by the equivalence relation

if and only if

for any *a* and *b* in *A*. The elements of *A*/*B* are the equivalence classes $[a] = \{a + b : b \text{ in } B\}$.

The addition operation on *A*/*B* is defined for two equivalence classes as the equivalence class of the sum of two representatives from these classes; and scalar multiplication of elements of *A*/*B* by elements of *R* is defined similarly. Note that it has to be shown that these operations are well-defined. Then *A*/*B* becomes itself an *R*-module, called the *quotient module*. In symbols, $[a] + [b] = [a + b]$, and $r \cdot [a] = [r \cdot a]$, for all *a*, *b* in *A* and *r* in *R*

Examples

Consider the ring **R** of real numbers, and the **R**-module $A = \mathbf{R}[X]$, that is the polynomial ring with real coefficients. Consider the submodule

$$B = (X^2 + 1)\,\mathbf{R}[X]$$

of A, that is, the submodule of all polynomials divisible by $X^2 + 1$. It follows that the equivalence relation determined by this module will be

$P(X) \sim Q(X)$ if and only if $P(X)$ and $Q(X)$ give the same remainder when divided by $X^2 + 1$.

Therefore, in the quotient module A/B, $X^2 + 1$ is the same as 0; so one can view A/B as obtained from $\mathbf{R}[X]$ by setting $X^2 + 1 = 0$. This quotient module is isomorphic to the complex numbers, viewed as a module over the real numbers **R**.

Definition Let R be a ring and let M, N be R-modules.

1 A map $\varphi : M \to N$ is an R-module homomorphism provided

$\varphi(x + y) = \varphi(x) + \varphi(y), \forall x, y, \in M$, and 2 $\varphi(rx) = r\varphi(x), \forall r \in R; x \in M$.

2 An R-module isomorphism is an R-module homomorphism which is also bijective.

3 Suppose $\varphi : M \to N$ is an R-module homomorphism. $\ker(\varphi) = \{m \in M \mid \varphi(m) = 0N\}$. $\varphi(M) = \{\varphi(m) \mid m \in M\}$.

4 $\mathrm{HomR}(M, N) = \{\varphi : M \to N \mid \varphi \text{ is an R-module homomorphism}\}$.

Definition Let R be a ring and let M, N be R-modules.

1 A map $\varphi : M \to N$ is an R-module homomorphism provided

$$\varphi(x + y) = \varphi(x) + \varphi(y), \forall x, y, \in M, \text{ and}$$

2 $\varphi(rx) = r\varphi(x), \forall r \in R; x \in M$. 2 An R-module isomorphism is an R-module homomorphism which is also bijective.

3 Suppose $\varphi : M \to N$ is an R-module homomorphism. $\ker(\varphi) = \{m \in M \mid \varphi(m) = 0N\}$. $\varphi(M) = \{\varphi(m) \mid m \in M\}$.

4 $\mathrm{HomR}(M, N) = \{\varphi : M \to N \mid \varphi \text{ is an R-module homomorphism}\}$.

Note For an R-module homomorphism $\varphi : M \to N$,

$\ker(\varphi)$ is a submodule of M and

$\varphi(M)$ is a submodule of N.

Let (T be a kernel functor. A A-module E is called a-injective if it has the following property: if M is any module and N is a submodule of M such that u(M/N) = M/N, th en every A-homomorphism from N to E extends to a homomorphism from M to E. The module E is called faithfulb u-injective if, in the same notation, the homomorphism from N to E has a uniqzze extension to M.

PROPOSITION . The followi?zg are equivalent:

(1) E is faithfully u-injective.

(2) E is a-injective arzd o(E) = 0.

Proof. (1) * (2)

Clearly (1) implies that E is a-injective. Furthermore, the zero map from 0 C u(E) to E has a unique extension to o(E) and hence u(E) = 0.

(2) * (1)

If NC M is such that u(M/N) = M/N, then the only homomorphism fromzM/N into a u-torsion-free module is 0. Hence (2) => (1). Exactly as for the usual absolute notion of injectivity, we have:

PROPOSITION . The following are equivalent:

(I) E is u-irzjective.

(2) If % E y-o and g : 5X + E is a A-homomorphism, tlzerz g extends to A.

Proof. (1) + (2) is a consequence of the definition.

(2) * (1)

Suppose that f : N -+ E is a fl-homomorphism where N is a submodule of M such that M/N is u-torsion. If N' is a submodule of M which contains N, then M/N' is also a a-torsion module. Consider all pairs (N', f ') with

N' as above, and f' an extension off to N'. In an obvious ordering, Zorn's lemma is applicable, and there is a largest extension off. Let that be N and f itself. We must then show that N = M. If x E M, the fact that u(M/N) = M/N implies that '% = {a E fl 1 ax E N} is an ideal in Y0 . Define g : 2l ---f E by

g(u) =$(a.~). Clearly g is a A-homomorphism, so that (2) asserts the extendibility of g to A. Namely, there is an element r] of E such that g(u) = a~ for a E 58. Now define f' : N + Ax -+ E by f'(y + a~) =f(y) + UT. Because a E '9I implies that f(azc) = a~, the function f' is well-defined and is a A-homomorphism, and f' coincides with f on N. The maximality of N implies that x E N, i.e., that N = M.

In the particular case where 0 = 0 every module is faithfully u-injective. If 0 = co, then a-injectivity is the same as absolute injectivity. However in this case the only faithfully o-injective module is 0. (In fact, 0 is the only u-torsion-free module.)

Before entering into the question of the existence of o-injective modules, we consider some further simple properties of such modules.

Check In Progress-II

Q. 1 Define quotient Ring.

Solution

……
……
……
……
……
……

Q. 2 Define submodule.

……

……

……

……

PROPOSITION . Suppose that 0 --f F -+ E -+ L --f 0 is an exact sequence in which E is a-injective and L is cs-torsion-free. Then F is a-injective.

Proof. Let 2I be an ideal in .FO and f : ?f -+ F a A-homomorphism. Because of the o-injectivity of E, there is an element x E E such thatf (a) = a~ for a E ?I. In particular, '%x = f (5X) CF, and hence the image of IV in L lies in o(L). We have assumed that a(L) = 0, hence x' ~3' and thus F is cT-injective.

An analogue of the last result which we shall find useful is the following:

PROPOSITION . Suppose that 0 -+ F --f E + L -+ 0 is an exact sequence such that F is cJ-injective and L is a a-torsion module. Then the sequence splits, If in addition E is a-torsion-free, then F = E.

PROOf. If we apply the definition to F, then the identity map from F to itself extends to a map from E to F. This implies that the sequence splits, and E is isomorphic to the direct sum of F and L. If w(E) = 0 then also a(L) = 0, while u(L) = L. Hence L = 0.

The test for a-injectivity of a module is somewhat simplified if one already knows of the module under consideration that it is o-torsion-free. Such situations will arise frequently.

LEMMA . Let I be a o-torsion-free module, let N be a submodule of a module ;"I such that M/N is a a-torsion module and Zet f : A- E be a homomorphism. Suppose there exists a submodule N' of N such that N/N' is a a-tomian module and such that the restriction off to N' extends to a homomorphism ,from M to E. Then f extends to a homomorphism from &I to E.

Proof. Denote by f' the restriction off to N' and by g its extension to ild. Then f andg I,,, are homomorphisms from N to E which coincide on N'. Hence

f -g IN induces a homomorphism from N/N' to E while u(N/N') = N/N' and a(E) = 0. Hence f and g IN coincide and g is an extension off. We shall apply the lemma immediately to obtain the following very useful

criterion. (It should be remarked that there is no analogue of this result in the ordinary theory of absolute injective modules.)

PROPOSITION . Let u be an idempotent kernel functor, E a o-torsion-free module and M a submodule of E such that E/M is a a-torsion module. Assume further that for every ideal % E YFO every homomorphism from % to M extends to a homomorphism from A to E. Then E is (faithfully) o-injective

Proof. Let 52l be an ideal in y0 and f : 2I -+ E a homomorphism. Let 8 = {b E 2I 1 f(b) E M), so that 8 C 9I and B = f -‘(f (2X) n M). Then 2Ij23 is isomorphic to a submodule of E/M and therefore %/S is u-torsion. Since u is idempotent, it follows that 8 is also in y0 . The restriction off to 23 maps !$3 into M and hence, by hypothesis, this restriction extends to a homomorphism from /l to E. By the lemma, f extends to a homomorphism from fl to E. Thus E is u-injective.

From now on we shall be principally concerned with idempotent kernel functors. If u is such a functor and M is a A-module, we shall now consider the question of assigning to M a faithfully a-injective module which is minimal in some sense. We start under the assumption that u(M) = 0. Given such a module, let G be an absolute injective module which is an essential extension of M. Certainly G is a u-injective module. Furthermore, 0 = U(M) = M n U(G), so that the fact that G is an essential extension of M implies that u(G) = 0. Thus G is a faithfully a-injective module. Now let E be the submodule of G, containing ill, which maps onto o(G/M) under the map G -+ G/M. Then G/E is isomorphic to G/M/u(G/M), and the fact that u is idempotent implies that G/E is u-torsion-free. We may now apply to conclude that E is also faithfully u-injective. Furthermore, E/M is isomorphic to u(G/M), so that E/M is a u-torsion module. Thus we have proved the following:

THEOREM. Let u be an idempotent kerneifunctor. If M is a u-torsion-free module, then there is a faithfully u-injective module E containing M and such that E/M is u-torsion.

The module E just constructed is an essential extension of M because of the particular way it was arrived at. Actually some of its properties

already imply that E is an essential extension of M. Since we shall need to use this later, we isolate this fact.

LEMMA. Let a be a kernel functor, X a u-torsion-free module and Y a submodule of X such that X/Y is a o-torsion nwdule. Then X is an essential extension of Y.

Proof. If x E X, the fact that a(X/Y) = X/Y implies the existence of an 2l E 3PU with %x C Y. Also, because c(X) = 0, '%x cannot be 0 unless x = 0. Hence, if x + 0, then 2Ix C Y n Ax and %x f 0.

The module E whose existence is asserted in that theorem is unique in a strong sense. Namely, if E' is another module with the properties as in then there is a zcnique isomorphism from E to E' which is the identity on M. Namely, the fact that o(E/M) = E/M combined with the fact that E' is faithfully cr-injective implies that the identity map from M + iV C E' has a unique extension to a homomorphism from E to E'. Furthermore E is an essential extension of M, so that this homomorphism is a monomorphism. Thus E is isomorphic to a module squeezed between M and E'.

Let u be an idempotent kernel functor. Let iVi be a u-torsion-free module. Denote by 52 the set of pairs (2I, f) where '$I is an ideal in SU andf : 2I -+ M is a A-homomorphism. Two elements (2l, f) and (W,f') of !2 are called equivalent, (8, f) - (7',f'), if there is an ideal 8 E TV with 23 C (LT n 3 such that f and f' coincide on 23. This is obviously an equivalent relation; we denote by QJM) the set of equivalence classes. We shall also use the symbol [CZ, f] for the equivalence class of I.[, f j.

If (XS) and (26 gj are in 52, set K = rU: n 23 and letf' andg' be the restrictions to (5 off and g, respectively. Then (!!I, f) - (6, f ') and (23, g) - ((.I., g'). It is a simple matter to verify that [c, f' + g'] depends only on [%, f] and [B,g] and not on the particular choice of representatives '%, f, etc. It is equally simple to verify that the composition just defined gives Q,(M) the structure of an abelian group. Let ('2,f) G Q and let x be and.

Let ('2,f) G Q and let x be an element of fl. Then, there is an ideal 23 E rU such that 8x C $9l. Define g : 23 -+ M by g(b) =f(bx). Then ('B, g) E Q and, as above, [23, g] is determined by [?I, f] and x. We denote the equivalence class [S,g] by xc%, f]. (Note the side!) This defines a

composition A x Q,(M) -+ g$k?), and we leave to the reader the simple verification of the details that this gives Qo(M) the structure of a left fl-module.

If N E M, definej(x) : /l + M byj(x)(a> = ax. Then (A,i(x)) is an element of 0. Define i : M + Q,(M) by i(x) = [A,i(z)]. That i is a A-homomorphism is trivial. Now x E M is in the kernel of i if (A, i(x)) N (A, 0), or if there is an ideal %!I E Y- such that i(x) vanishes on 2I. This latter condition is the same as $?I?[x =0, or that x E u(M). Since we have assumed that u(M) = 0, it follows that i is a monomorphism.

Let f E&(M), and let (%,f) b e a representative of f in Q. If a E 2I, then at = [A,if(a)], so that Fu,$ C i(M). Thus, Q0(M)/i(A4) is a o-torsion module. Furthermore, if a4 = 0, then by the discussion in the previous paragraph, f(a) = 0. Hence, if 2I[= 0, then f = 0 and 5 = 0. Thus, for 5 # 0, ‘2I.$ C i(M) n At, and 2If f 0. This shows that Q,(M) is an essential extension of M. In particular, because G(M) = 0, and M is isomorphic with i(M), we conclude that c+&(M)> = 0. Finally, to verify that QO(M) is o-injective we use. If 2I E Y0 and f : 2I + M is a homomorphism, then form E = [‘$I, f] E Q,(M). Exactly as above, if a E ‘$I, then at = [A, jf (u)], or at = if (a), showing that f extends to a homomorphism from A to Q,(M).

Still assuming that G is an idempotent kernel functor, let M be an arbitrary left A-module. Then, the module of quotients of M with respect to CJ is defined to be QO(M/u(M)) together with the map from M to QJM/u(M)) gotten by composing the homomorphism M-z- M/u(M) with the monomorphism M/u(M) -+ Q,(M/u(M)). If necessary we shall denote the map M--f Q,(M/o(M)) by i0 . Furthermore, we shall also use the notation &(M) in place of Q,(M/u(M)).

Let M and A/’ be A-modules, and let f : M’-+ M be a homomorphism. Then f induces a homomorphism f’ : M’/o(M’) -+ M/u(M), and the properties of Q0 imply the existence of a unique homomorphism fO : QO(M) -+ QJM’) which is such that the diagram

is commutative. The pair M + Q,(M) and f .+ fv forms a covariant functor, and it is this functor, together with i, : M + Q,(M), that constitutes the formation of the module of quotients with respect to CT.

We emphasize that the module of quotients is defined here only for idempotent kernel functors. We shall describe briefly the connection between the general construction just given and the familiar situation in commutative rings. Let A be a commutative ring and let S be a subset of A closed under multiplication. Let Y be the set of ideals of A which contain an element of S. Then Y is and ideal topology in A (because S is closed under multiplication) and hence defines a kernel functor u. If M is a module, then a(M) consists of the elements annihilated by some element of S. That this functor is idempotent is well-known, and is due to the fact that S is closed under multiplication. The extreme case where u = 0 corresponds to the case where S consists entirely of units of A, and 0 = 03 corresponds to the case wherein S contains the zero element of A.

4.10 LET US SUM UP

In This units we study submodule and its properties. We study submodule and its proposition with example. We study quotient module and ring with its lemma and properties.

1. A bimodule is a module that is a left module and a right module such that the two multiplications are compatible.
2. If R is commutative, then left R-modules are the same as right R-modules and are simply called R-modules.
3. If M and N are left R-modules, then a map $f : M \to N$ is a homomorphism of R-modules if for any m, n in M and r, s in R.
4. Cyclic. A module is called a cyclic module if it is generated by one element.
5. Flat. A module is called flat if taking the tensor product of it with any exact sequence of R-modules preserves exactness.
6. Torsion-free. A torsion-free module is a module over a ring such that 0 is the only element annihilated by a regular element (non zero-divisor) of the ring.

7. Graded. A graded module is a module with a decomposition as a direct sum $M = \bigoplus_x M_x$ over a graded ring $R = \bigoplus_x R_x$ such that $R_x M_y \subset M_{x+y}$ for all x and y.
8. Uniform. A uniform module is a module in which all pairs of nonzero submodules have nonzero intersection.

4.11 KEYWORD

Submodule : A module making up part of a larger module

Monomorphism : A *monomorphism* is an injective homomorphism

4.12 QUESTIONS FOR REVIEW

1 . Let M = Mmn(R) be the set of all m × n matrices with entries in R. Then M is an R-module, where addition is ordinary matrix addition, and multiplication of the scalar c by the matrix A means multiplication of each entry of A by c.

2. Every abelian group A is a Z-module. Addition and subtraction is carried out according to the group structure of A; the key point is that we can multiply x ∈ A by the integer n. If n > 0, then nx = x + x + ⋯ + x (n times); if n < 0, then nx = −x − x −⋯− x (|n| times).

In all of these examples, we can switch from left to right modules by a simple notational change. This is definitely not the case in the next example.

3 Let I be a left ideal of the ring R; then I is a left R-module. (If x ∈ I and r ∈ R then rx (but not necessarily xr) belongs to I.) Similarly, a right ideal is a right R-module, and a two-sided ideal is both a left and a right R-module.

An R-module M permits addition of vectors and scalar multiplication. If multiplication of vectors is allowed, we have an R-algebra.

4 Every commutative ring R is an algebra over itsel

5 An arbitrary ring R is always a Z-algebra

6 If R is a commutative ring, then Mn(R), the set of all n × n matrices with entries in R, is an R-algebra.

7 If R is a commutative ring, then the polynomial ring R[X] is an R-algebra, as is the ring R[[X]] of formal power series;). The compatibility condition is satisfied because an element of R can be regarded as a polynomial of degree 0.

8. If E/F is a field extension, then E is an algebra over F. This continues to hold if E is a division ring, and in this case we say that E is a division algebra over F

9 If I is an ideal of the ring R, show how to make the quotient ring R/I into a left R-module, and also show how to make R/I into a right R-module.

10. Let A be a commutative ring and F a field. Show that A is an algebra over F if and only if A contains (an isomorphic copy of) F as a subring

11. Give an example of an R-module M with nonzero elements $r \in R$ and $x \in M$ such that $rx = 0$.

12. Let M be the additive group of rational numbers. Show that any two elements of M are linearly dependent (over the integers Z).

13. Continuing Problem 4, show that M cannot have a basis, that is, a linearly independent spanning set over Z.

14. Prove the modular law for subgroups of a given group G: With the group operation written multiplicatively,

$$A(B \cap C)=(AB) \cap C$$

4.13 ANSWER FOR CHECK IN 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 3

Q. 2 Check in Section 2

4.14 REFERENCES

- F.W. Anderson and K.R. Fuller: *Rings and Categories of Modules*, Graduate Texts in Mathematics, Vol. 13, 2nd Ed., Springer-Verlag, New York, 1992, ISBN 0-387-97845-3, ISBN 3-540-97845-3
- Nathan Jacobson. *Structure of rings*. Colloquium publications, Vol. 37, 2nd Ed., AMS Bookstore, 1964, ISBN 978-0-8218-1037-8
- *Dummit, David S. & Foote, Richard M. (2004). Abstract Algebra. Hoboken, NJ: John Wiley & Sons, Inc. ISBN 978-0-471-43334-7.*
- ^ This is the endomorphism ring of the additive group *M*. If *R* is commutative, then these endomorphisms are additionally *R* linear.
- ^ Jacobson (1964), p. 4, Def. 1; Irreducible Module at PlanetMath.org.

UNIT 5 - HOMOMORPHISM AND ISOMORPHISM

STRUCTURE

5.0 OBJECTIVE

- Learn Endomorphism
- Learn Monomorphism
- Learn group Homomorphism

- Work on Epimorphism
- Know about kernel

5.1 INTRODUCTION: HOMOMORPHISM

In algebra, a **homomorphism** is a structure-preserving map between two algebraic structures of the same type (such as two groups, two rings, or two vector spaces). Theword homomorphism comes from the ancient Greek language: ὁμός (homos) meaning "same"
and μορφή (morphe) meaning "form" or "shape". However, the word was apparently introduced to mathematics due to a (mis)translation of German ähnlich meaning "similar" to ὁμός meaning "same".

Homomorphisms of vector spaces are also called linear maps, and their study is the object of linear algebra.

The concept of homomorphism has been generalized, under the name of morphism, to many other structures that either do not have an underlying set, or are not algebraic. This generalization is the starting point of category theory.

A homomorphism may also be an isomorphism, an endomorphism, an automorphism, etc. (see below). Each of those can be defined in a way that may be generalized to any class of morphisms.

Definition

A homomorphism is a map between two algebraic structures of the same type (that is of the same name), that preserves the operations of the structures. This means a map between two sets *A*, *B* equipped with the same structure such that, if is an operation of the structure (supposed here, for simplification, to be a binary operation), then

for every pair *x*, *y* of elements of *A*. says often that *f* preserves the operation or is compatible with the operation.

The operations that must be preserved by a homomorphism include 0-ary operations, that is the constants. In particular, when an identity element is required by the type of structure, the identity element of the first structure

must be mapped to the corresponding identity element of the second structure.

For example:

- A semigroup homomorphism is a map between semigroups that preserves the semigroup operation.
- A monoid homomorphism is a map between monoids that preserves the monoid operation and maps the identity element of the first monoid to that of the second monoid (the identity element is a 0-ary operation).
- A group homomorphism is a map between groups that preserves the group operation. This implies that the group homomorphism maps the identity element of the first group to the identity element of the second group, and maps the inverse of an element of the first group to the inverse of the image of this element. Thus a semigroup homomorphism between groups is necessarily a group homomorphism.
- A ring homomorphism is a map between rings that preserves the ring addition, the ring multiplication, and the multiplicative identity. Whether the multiplicative identity is to be preserved depends upon the definition of *ring* in use. If the multiplicative identity is not preserved, one has a rng homomorphism.
- A linear map is a homomorphism of vector space, That is a group homomorphism between vector spaces that preserves the abelian group structure and scalar multiplication.
- A module homomorphism, also called a linear map between modules, is defined similarly.
- An algebra homomorphism is a map that preserves the algebra operations.
    - An algebraic structure may have more than one operation, and a homomorphism is required to preserve each operation. Thus a map that preserves only some of the operations is not a homomorphism of the structure, but only a homomorphism of the substructure obtained by considering only the preserved operations. For example, a map between monoids that preserves

the monoid operation and not the identity element, is not a monoid homomorphism, but only a semigroup homomorphism.

- The notation for the operations does not need to be the same in the source and the target of a homomorphism. For example, the real numbers form a group for addition, and the positive real numbers form a group for multiplication. The exponential function
- and is thus a homomorphism between these two groups. It is even an isomorphism (see below), as its inverse function, the natural logarithm.
- and is also a group homomorphis

5.1.2 Endomorphism

An endomorphism is a homomorphism whose domain equals the codomain, or, more generally, a morphism whose source is equal to the target.

The endomorphisms of an algebraic structure, or of an object of a category form a monoid under composition.

The endomorphisms of a vector space or of a module form a ring. In the case of a vector space or a free module of finite dimension, the choice of a basis induces a ring isomorphism between the ring of endomorphisms and the ring of square matrices of the same dimension.

5.1.3 Automorphism

An automorphism is an endomorphism that is also an isomorphism.

The automorphisms of an algebraic structure or of an object of a category form a group under composition, which is called the automorphism group of the structure.

Many groups that have received a name are automorphism groups of some algebraic structure. For example, the general linear group is the automorphism group of a vector space of dimension *n* over a field *k*.

The automorphism groups of fields were introduced by Évariste Galois for studying the roots of polynomials, and are the basis of Galois theory.

5.1.4 Monomorphism

Algebraic structures, monomorphisms are commonly defined as injective homomorphisms.

In the more general context of category theory, a monomorphism is defined as a homomorphism that is **left cancelable**. This means that a (homo)morphism is a monomorphism if, for any pair *g*, *h* of morphisms from any other object *C* to *A*, then implies *g* = *h*.

These two definitions of *monomorphism* are equivalent for all common algebraic structures. More precisely, they are equivalent for fields, for which every homomorphism is a monomorphism, and for varieties of universal algebra, that is algebraic structures for which operations and axioms (identities) are defined without any restriction (fields are not a variety, as the multiplicative inverse is defined either as a unary operation or as a property of the multiplication, which are, in both cases, defined only for nonzero elements).

In particular, the two definitions of a monomorphism are equivalent for sets, magmas, semigroups, monoids, groups, rings, fields, vector spaces and modules.

A **split monomorphism** is a homomorphism that has a left inverse and thus it is itself a right inverse of that other homomorphism. That is, a homomorphism is a split homomorphism if there exists a homomorphism such that A split monomorphism is always a monomorphism, for both meanings of *monomorphism*. For sets and vector spaces, every monomorphism is a split homomorphism, but this property does not hold for most common algebraic structures.

5.1.5 Epimorphism

In algebra, **epimorphisms** are often defined as surjective homomorphisms. On the other hand, in category theory, epimorphisms are defined as **right cancelable**. This means that a (homo)morphism is an epimorphism if, for any pair *g*, *h* of morphisms from *B* to any other object *C*, the equality implies *g* = *h*.

A surjective homomorphism is always right cancelable, but the converse is not always true for algebraic structures. However, the two definitions

of *epimorphism* are equivalent for sets, vector spaces, abelian groups, modules (see below for a proof), and groups. The importance of these structures in all mathematics, and specially in linear algebra and homological algebra, may explain the coexistence of two non-equivalent definitions.

Algebraic structures for which there exist non-surjective epimorphisms include semigroups and rings. The most basic example is the inclusion of integers into rational numbers, which is an homomorphism of rings and of multiplicative semigroups. For both structures it is a monomorphism and a non-surjective epimorphism, but not an isomorphism.

A wide generalization of this example is the localization of a ring by a multiplicative set. Every localization is a ring epimorphism, which is not, in general, surjective. As localizations are fundamental in commutative algebra and algebraic geometry, this may explain why in these areas, the definition of epimorphisms as right cancelable homomorphisms is generally preferred.

A **split epimorphism** is a homomorphism that has a right inverse and thus it is itself a left inverse of that other homomorphism. That is, a homomorphism is a split epimorphism if there exists a homomorphism such that A split epimorphism is always an epimorphism, for both meanings of *epimorphism*. For sets and vector spaces, every epimorphism is a split epimorphism, but this property does not hold for most common algebraic structures.

In summary, one hasthe last implication is an equivalence for sets, vector spaces, modules and abelian groups; the first implication is an equivalence for sets and vector spaces.

Check in Progress-I

Q. 1 Define Epimorphism.

Solution

…….

……

…….

……

Q. 2 Define Automorphism.

Solution

…….

……

…….

……

5.1.7 Kernel

The kernel of a ring homomorphism $f : R \longrightarrow S$ is the set of all elements of R which are mapped to zero. It is the kernel of f as a homomorphism of additive groups. It is an ideal of R.

Any homomorphism $f : X \to Y$ defines an equivalence relation ~ on X by $a \sim b$ if and only if $f(a) = f(b)$. The relation ~ is called the **kernel** of f. It is a congruence relation on X. The quotient set X / ~ can then be given a structure of the same type as X, in a natural way, by defining the operations of the quotient set by $[x] * [y] = [x * y]$, for each operation $*$ of X. In that case the image of X in Y under the homomorphism f is necessarily isomorphic to X / ~; this fact is one of the isomorphism theorems.

When the algebraic structure is a group for some operation, the equivalence class K of the identity element of this operation suffices to characterize the equivalence relation. In this case, the quotient by the equivalence relation is denoted by X/K (usually read as "X mod K"). Also in this case, it is K, rather than ~, that is called the kernel of f. The kernels of homomorphisms of a given type of algebraic structure are naturally equipped with some structure. This structure type of the kernels is the same as the considered structure, in the case of abelian groups, vector spaces and modules, but is different and has received a specific name in other cases, such as normal subgroup for kernels of group homomorphisms and ideals for kernels of ring

homomorphisms (in the case of non-commutative rings, the kernels are the two-sided ideals).

5.2 HOMOMORPHISMS AND MATRICES

Homomorphisms are the maps between algebraic objects. There are two main types: group homomorphisms and ring homomorphisms. (Other examples include vector space homomorphisms, which are generally called linear maps, as well as homomorphisms of modules and homomorphisms of algebras.)

Generally speaking, a homomorphism between two algebraic objects A,B is a function $f:A \to B$ which preserves the algebraic structure on A and B. That is, if elements in A satisfy some algebraic equation involving addition or multiplication, their images in B satisfy the same algebraic equation. The details of the definitions of homomorphisms in various contexts depend on the algebraic structures of A and B.

Suppose that M is a free R-module with a finite basis of n elements v1,...,vn, sometimes called a free module of rank n. We know from Section 4.3 that M is isomorphic to the direct sum of n copies of R. Thus we can regard M as Rn, the set of all n-tuples with components in R. Addition and scalar multiplication are performed componentwise, as in (4.1.3),

Example . Note also that the direct sum coincides with the direct product, since we are summing only finitely many modules. Let N be a free R-module of rank m, with basis w1,...,wm, and suppose that f is a module homomorphism from M to N. Just as in the familiar case of a linear transformation on a finite-dimensional vector space, we are going to represent f by a matrix. For each j, f(vj) is a linear combination of the basis elements wj , so that f(vj) = m i=1 aijwi, j = 1,...,n (1) where the aij belong to R.

It is natural to associate the m × n matrix A with the homomorphism f, and it appears that we have an isomorphism of some sort, but an isomorphism of what? If f and g are homomorphisms of M into N, then f and g can be added (and subtracted): (f + g)(x) = f(x) + g(x). If f is represented by the matrix A and g by B, then f + g corresponds to A + B.

This gives us an abelian group isomorphism of HomR(M,N), the set of all R-module homomorphisms from M to N, and Mmn(R), the set of all m × n matrices with entries in R. In addition, Mmn(R) is an R-module, so it is tempting to say "obviously, we have an R-module isomorphism". But we must be very careful here. If f ∈HomR(M,N) and s ∈ R, we can define sf in the natural way: (sf)(x) = sf(x). However, if we carry out the "routine" check that sf ∈HomR(M,N), there is one step that causes alarm bells to go off:

where the aij belong to R. It is natural to associate the m × n matrix A with the homomorphism f, and it appears that we have an isomorphism of some sort, but an isomorphism of what? If f and g are homomorphisms of M into N, then f and g can be added (and subtracted): (f + g)(x) = f(x) + g(x). If f is represented by the matrix A and g by B, then f + g corresponds to A + B. This gives us an abelian group isomorphism of HomR(M,N), the set of all R-module homomorphisms from M to N, and Mmn(R), the set of all m × n matrices with entries in R. In addition, Mmn(R) is an R-module, so it is tempting to say "obviously, we have an R-module isomorphism". But we must be very careful here. If f ∈HomR(M,N) and s ∈ R, we can define sf in the natural way: (sf)(x) = sf(x). However, if we carry out the "routine" check that sf ∈HomR(M,N), there is one step that causes alarm bells to go off:

(sf)(rx) = sf(rx) = srf(x), but r(sf)(x) = rsf(x)

and the two expressions can disagree if R is not commutative. Thus HomR(M,N) need not be an R-module. Let us summarize what we have so far

Proposition The set of even permtuations in Sn is a subgroup of Sn. This group is called the alternating group of order n, and is denoted by An. Moreover, |An| = n! 2 .

Proof (Sketch) If σ, τ ∈ An then they can be written as the product of an even number of transpositions, so στ can be as well (by concatenation). Moreover, since σ and σ −1 have the same number of cycles of the same lengths in their disjoint cycle decomposition, they can be written as the product of the same number of transposition so σ ∈An =⇒ σ −1 ∈ An. To see that |An| = n! 2 , observe that the set map T : An → Sn\An defined by T(σ) = (1 2)σ is a bijection: |An| = |Sn\|An|, and the result follows.

5.1.1 Examples Of Group Homomorphism

A group homomorphism is a map $f : G \to H$ between two groups such that the group operation is preserved: $f(g_1 g_2) = f(g_1) f(g_2)$ for all $g_1, g_2 \in G$, where the product on the left-hand side is in G and on the right-hand side in H.

As a result, a group homomorphism maps the identity element in G to the identity element in H: $f(e_G) = e_H$.

Note that a homomorphism must preserve the inverse map because $f(g) f\left(g^{-1}\right) = f\left(g\, g^{-1}\right) = f(e_G) = e_H$, so $f(g)^{-1} = f\left(g^{-1}\right)$.

In particular, the image of G is a subgroup of H and the group kernel, i.e., $f^{-1}(e_H)$ is a subgroup of G. The kernel is actually a normal subgroup, as is the preimage of any normal subgroup of H. Hence, any (nontrivial) homomorphism from a simple group must be injective.

Here's some examples of the concept of group homomorphism.

Example 1:

Let G={1,−1,i,−i}G={1,−1,i,−i}, which forms a group under multiplication and I=I= the group of all integers under addition, prove

that the mapping ff from II onto GG such that f(x)=in∀n∈If(x)=in∀n∈I is a homomorphism.

Solution: Since f(x)=in,f(m)=imf(x)=in,f(m)=im, for all m,n∈Im,n∈I

f(m+n)=im+n=im·in=f(m)·f(n)f(m+n)=im+n=im·in=f(m)·f(n)

Hence ff is a homomorphism.

Example 2:

Show that the mapping ff of the symmetric group PnPn onto the multiplicative group G′={1,−1}G′={1,−1} defined by f(α)=1f(α)=1 or −1−1.

According as αα is an even or odd permutation in PnPn is a homomorphism of PnPn onto G′G′.

Solution: We know that the product of two permutations both even or both odd is even while the product of one even and one odd permutation is odd. We shall show that

f(αβ)=f(α)f(β)∀α,β∈Pnf(αβ)=f(α)f(β)∀α,β∈Pn

(i) if α,βα,β are both even, then

f(αβ)=1=1·1=f(α)·f(β)f(αβ)=1=1·1=f(α)·f(β)

Definition. Let (G, ·) and (G0 , ?) be groups. A homomorphism is a set map φ : G → G0 that preserves the group operation in the respective groups; that is,

φ(a · b) = φ(a) ? φ(b) for all a, b ∈ G.

Check Your Progress-II

1. Define Kernel

Solution :

……

……

……

……

2. Group Homomorphism.

……

……

……

……

……

……

5.2 ISOMORPHISM THEOREMS

Isomorphism is a very general concept that appears in several areas of mathematics. The word derives from the Greek *iso*, meaning "equal," and *morphosis*, meaning "to form" or "to shape."

Formally, an isomorphism is bijective morphism. Informally, an isomorphism is a map that preserves sets and relations among elements. "A is isomorphic to B" is written $A \cong B$. Unfortunately, this symbol is also used to denote geometric congruence.

An isomorphism from a set of elements onto itself is called an automorphism.

In mathematics, specifically abstract algebra, the **isomorphism theorems** (also known as **Noether's isomorphism theorems**) are theorems that describe the relationship between quotients, homomorphisms, and subobjects. Versions of the theorems exist for groups, rings, vector spaces, modules, Lie algebras, and various other algebraic structures. In universal algebra, the isomorphism theorems can be generalized to the context of algebras and congruences.He isomorphism theorems were formulated in some generality for homomorphisms of modules by Emmy Noether in her paper *AbstrakterAufbau der Idealtheorie in algebraischenZahl- und Funktionenkörpern* which was published in 1927 in MathematischeAnnalen. Less general versions of these theorems can be found in work of Richard Dedekind and previous papers by Noether.

Three years later, B.L. van der Waerden published his influential *Algebra*, the first abstract algebra textbook that took the groups-rings-fields approach to the subject. Van der Waerden

credited lectures by Noether on group theory and Emil Artin on algebra, as well as a seminar conducted by Artin, Wilhelm Blaschke, Otto Schreier, and van der Waerden himself on ideals as the main references. The three isomorphism theorems, called *homomorphism theorem*, and *two laws of isomorphism* when applied to groups, appear explicitly.

Statement of the theorems

Theorem A

Let G and H be groups, and let φ: $G \to H$ be a homomorphism. Then:

1. The kernel of φ is a normal subgroup of G,
2. The image of φ is a subgroup of H, and
3. The image of φ is isomorphic to the quotient group G / ker(φ).

In particular, if φ is surjective then H is isomorphic to G / ker(φ).

Theorem 1 (First Isomorphism Theorem)

Let $\varphi : G \to G0$ be a homomorphism of groups. Then $G/\ker(\varphi) \sim= \varphi(G)$

Proof. For simplicity let $K = \ker(\varphi)$. Define the homomorphism

$\psi : G/K \to \varphi(G)$ by $\psi(Kg) = \varphi(g)$.

We claim that ψ is a group isomorphism. First, we need to check that ψ is well-defined and is a homomorphism. In order to establish that it is well defined, we need to check that if a is in the coset Kg then $\varphi(a) = \varphi(g)$. But this is the case because, a = a 0 g, so

$$\varphi(a) = \varphi(a\ 0\ g) = \varphi(a\ 0\ )\varphi(g) = \varphi(g).$$

Now to see that ψ is a homomorphism, consider Kg, Kh$\in$ G/K. Then for any a, b $\in$ K we have

$$\psi(Kg \cdot Kh) = \psi(Kgh) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(Kg)\psi(Kh),$$

so ψ is a homomorphism. We now need to establish ψ is injective and surjective. For injectivity, we must prove that $\ker(\psi) = K$. To see this, observe that

$$\psi(Kg) = 1 \Longleftrightarrow \varphi(g) = 1 \Longleftrightarrow g \in \ker(\varphi) \Longleftrightarrow g \in K \Longleftrightarrow Kg = K.$$

So ker(ψ) = K. Finally we need to see that ψ is surjective. Indeed if φ(g) ∈ φ(G), then φ(g) has preimage Kg.

Example. 1. Let φ :GLn(R) → R\{0}, φ(A) = det(A). Then ker(φ) = SLn(R), and φ(GLn(R)) = R\{0} so

$$GLn(R)/SLn(R) \sim= R\{0\}.$$

2. φ : Sn → Z/2Z, φ(σ) = 1 if σ is odd, φ(σ) = 0 if σ is even.

Then φ is a surjective homomorphism with ker(φ) = An. Thus Sn/An∼= Z/2Z. Thus |An| = n!

Theorem (Fourth/Lattice Isomorphism Theorem) Let N ✂ G. Then every subgroup of G/N is of the form H/N where N ≤ H ≤ G. Moreover, if H, K are subgroups of G containing N then

1. H ≤ K if and only if H/N ≤ K/N

2. H ✂ G if and only if H/N ✂ G/N

3. if H ≤ K, then [K : H] = [K/N : H/N]

4. (H ∩ K)/N ∼= H/N ∩ K/N

Proof. Consider natural projection π : G → G/N, defined by π(g) = Ng. Let A ≤ G/N. Then the π −1 (A), the preimage of A under π, is a subgroup of G that contains π −1 (1) in G/N. But π −1 (1) = N, so N is a subgroup of H = π −1 (A), and π(H) = A so A = H/N. The four parts above all follow and we leave them as exercises.

Theorem (Third Isomorphism Theorem) Let K, N be normal subgroups of G, with N ✂ K. Then

$$K/N \text{ ✂ } G/N \text{ and } (G/N)/(K/N) \sim= G/K.$$

Proof. That K/N ✂ G/N follows from the previous theorem. Now define

$$\varphi : G/N \to G/K$$

by φ(Ng) = Kg. By the First Isomorphism Theorem, (G/N)/ ker(φ) ∼= φ(G). It is clear φ is onto, so φ(G) = G/K. Now

$$\ker(\varphi) = \{Ng \in G/N \mid Kg = K\} = \{Ng \in G/N \mid g \in K\} = K/N.$$

Thus by the First Isomorphism Theorem, $(G/N)/(K/N) \sim= G/K$.

Theorem (Second isomorphism theorem). Let R be a ring, let $S \subset R$ be a subring, and let I be an ideal of R. Then:

(1) $S + I := \{s + a : s \in S, a \in I\}$ is a subring of R,

(2) $S \cap I$ is an ideal of S, and

(3) $(S + I)/I$ is isomorphic to $S/(S \cap I)$.

Proof. (1): S is a subring and I is an ideal so $1 + 0 \in S + I$. Let $s1 + a1$ and $s2 + a2$ be elements of $S + I$. Then

$(s1+a1)-(s2+a2) = (s1 - s2) \mid \{z\} \in S + (a1 - a2) \mid \{z\} \in I$ and
$(s1+a1)(s2+a2) = s1s2 \mid \{z\} \in S + s1a2 + a1s2 + a1a2 \mid \{z\} \in I$.

Hence $S + I$ is a subring of R.

(2): The intersection $S \cap I$ is nonempty since 0 is contained in I and S. Let $a1, a2 \in S \cap I$ and let $s \in S$. Then $a1+a2 \in S \cap I$ since S and I are both closed under addition. Furthermore sa1 and a1s are in $S \cap I$ since I is closed under multiplication from $R \supset S$ and S is closed under multiplication. Therefore $S \cap I$ is an ideal of S

(3): Consider the map $\varphi: S \to (S +I)/I$ which sends an element s to s+I. This is a ring homomorphism by definition of addition and multiplication in quotient rings. We claim that it is surjective with kernel $S \cap I$, which would complete the proof by the first isomorphism theorem. Consider elements $s \in S$ and $a \in I$. Then $s + a + I = s + I$ since $a \in I$, so $s + a + I \in \text{im } \varphi$ and hence φ is surjective. Let $s \in S$ be an element of $\ker \varphi$. Then $s + I = I$ which holds if and only if $s \in I$ or equivalently if $s \in S \cap I$. Thus $\ker \varphi = S \cap I$ and we have our desired result.

Theorem (Third isomorphism theorem). Let R be a ring and let $J \subset I$ be ideals of R. Then I/J is an ideal of R/J and

$$R/J \; I/J \sim= R/I.$$

Proof. Since I and J are ideals, they are nonempty and so I/J = {a + J : a ∈ I} is also nonempty. Let a1, a2 ∈ I and let r ∈ R. By definition of addition and multiplication of cosets, we have

$$(a1 + J) + (a2 + J) = (a1 + a2) + J,$$

$$(r + J)(a1 + J) = ra1 + J,$$

$$\text{and } (a1 + J)(r + J) = a1r + J.$$

Since I is an ideal, a1 + a2, ra1, and a1r are contained in I so I/J is an ideal of R/J.

Consider the map φ: R/J → R/I that sends r + J to r + I. We claim that this is a well-defined surjective homomorphism with kernel equal to I/J. (Then (R/J)/(I/J) is isomorphic to R/I by the first isomorphism theorem.

Theorem on ring homomorphisms. The kernel I of f is an ideal of A, the image C of f is a subring of B. The quotient ring A/I is isomorphic to C

Proof. Consider the map g: A/I → C, a+I 7→ f(a). It is well defined: a+I = a 0 +I implies a − a 0 ∈ I implies f(a) = f(a 0).

The element a + I belongs to the kernel of g iffg(a + I) = f(a) = 0, i.e. a ∈ I, i.e. a + I = I is the zero element of A/I. Thus, ker(g) = 0.

The image of g is g(A/I) = {f(a) : a ∈ A} = C.

Thus, g is an isomorphism. The inverse morphism to g is given by f(a) 7→ a + I.

Correspondence theorem. Let I be an ideal of a ring A. Then there is a bijection between the set of all ideals J of A such that I ⊂ J and the set of all ideals of A/I :

{J : I an ideal of A, I ⊂ J} −→ {K : K an ideal of A/I}

J −→ J/I

Proof. Denote by h the morphism h: A → A/I, a 7→ a + I, its image is A/I and its kernel is I

For an ideal J of A, $I \subset J$, denote by $h|J : J \to A/I$, $j \mapsto j + I$ the restriction of h to J. Its kernel is I. Similarly to the proof of the previous theorem we deduce that h|J (J) is isomorphic to J/I which is an ideal of A/I.

For an ideal K of A/I define $K0 = h^{-1}(K)$ of A. Then K0 is an ideal of A, $I \subset K$.

Now we have two maps, $J \mapsto J/I$ and $K \mapsto h^{-1}(K)$. They are inverse to each other, i.e. $h^{-1}(J/I) = J$ and $h^{-1}(K)/I = K$. Thus, there is a one-to-one correspondence between the ideals.

The intersection of ideals of A is an ideal of A. Given a subset S of A, one can speak about the minimal ideal of A which contains S. This ideal is equal to

$$\{a1s1 + \cdots + amsm : ai \in A, si \in S, m > 1\}.$$

Often it is called the ideal generated by S .

Let I, J be ideals of a ring A.

Their sum I + J is the minimal ideal of A which contains both I and J, more explicitly

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

Certainly, I + (J + K) = (I + J) + K. Similarly one defines the sum of several ideals Ik.

Their product IJ is the minimal ideal which contains all $ij : i \in I, j \in J$, more explicitly.

$$IJ = \{i1j1 + \cdots + injn : n > 1, im \in I, jm \in J\}.$$

The product is associative:

$$(IJ)K = I(JK)$$

and distributive:

$$(I + J)K = IK + JK.$$

Similarly one defines the product of several ideals I1 . . . In. Note that (I +J1)(I +J2) is the minimal ideal which contains products (i1 +j1)(i2 + j2) = (i1i2 + i2j1 + i1j2) + j1j2, so it is contained in I + J1J2:

$$(I + J1)(I + J2) \subset I + J1J2,$$

but the inverse inclusion does not hold in general.

For an element a of A the principal ideal generated by a is

$$(a) = aA = \{ab : b \in A\}.$$

In particular, (0) = {0} is the smallest ideal of A and (1) = A is the largest ideal of A. Unless A = {0}, these are two distinct ideals of A.

For several elements a1, . . . , an of A the ideal generated by the ai is denoted

$$(a1, \ldots, an) = a1A + \cdots + anA = \{a1b1 + \cdots + anbn : bi \in A\}.$$

A ring A is a field if it contains a nonzero element and every nonzero element of A is invertible in A.

Lemma. A nonzero ring is a field iff it has exactly two different ideals, (0) and (1). Proof. If I is a nonzero ideal of a field F , then I contains a nonzero element a. Therefore it contains aa□1 = 1 and therefore it contains 1b = b for every b in F ; so I = F .

Conversely, if a nonzero ring has only two distinct ideals then it is a field: for every nonzero element aA must be equal to (1), hence a multiple of a is 1 and a is invertible.

An ideal I of a ring A is called maximal if I 6= A and every ideal J such that I _ J _ A either oincides with A or with I. By 1.1 this equivalent to: the quotient ring A=I has no proper ideals. By the previous lemma this is equivalent to A=I is a field. So we proved.

Lemma. I is a maximal ideal of Aiff A=I is a field. A ring A is an integral domain if A 6= 0 and for every a; b 2 A ab = 0 implies a = 0 or b = 0.

Example: every field is an integral domain: ab = 0 and a 6= 0 implies b = a□1ab = 0. Z is an ntegral domain. More generally, every nonzero subring of an integral domain is an integral domain.

If A is an integral domain, one can form the field of fractions F of A as fa=b : a 2 A; b 2 A n f0gg:

By definition a=b = c=d iff ad = bc.

This is an equivalence relation: if a=b = c=d and c=d = e=f then ad = bc and cf = ed so adf = bcf = bed, d(af* be) = 0. As d is not zero, af = be. Define two ring operations a=b + c=d = (ad + bc)=(bd) and (a=b)(c=d) = (ac)=(bd).
The zero of F is 0=1 = 0=a for any nonzero a. Every nonzero element a=b of F isinvertible: if a=b 6= 0 then (a=b)1 = b=a. Thus F is a field. The ring homomorphism A !F , a 7! a=1 is injective: a=1 = 0=1 implies a = 0. Thus A can be identified with the subring A=1 of F . Then a=b can be identified with ab□1 giving the meaning of fraction to the symbol a=b.

Thus, every integral domain is a nonzero subring of a field, and the latter is an integral domain. So the class of integral domains coincides with the class of nonzero subrings of fields.

An ideal I of a ring A is called prime if I 6= A and for every a; b 2 A the inclusion ab 2 I implies that either a 2 I or b 2 I. Example: every field has a prime ideal: (0).

Lemma. I is a prime ideal of Aiff A=I is an integral domain.
Proof. Let I be a prime ideal of A. Let (a + I)(b + I) = 0 + I, then ab 2 I. So atleast one of a; b is in which means that either a + I = 0 + I or b + I = 0 + I. Thus,A=I is an integral domain.

Conversely, let A=I be an integral domain. If ab 2 I then (a+I)(b+I) = I = 0+I,hence either a + I = I and so a 2 I, or b + I = I and so b 2 I. Thus, I is a prime ideal of A.

Example: for a prime number p the ideal pZ is a prime ideal of Z. The zero ideal (0) is a prime ideal of Z.
Corollary. Every maximal ideal is prime.
Proof. Every field is an integral domain.

Remark. In general, not every prime ideal is maximal. For instance, (0) is a prime ideal of Z which is not maximal.
For rings Ai define their product A1 _ _ _ _ _ An as the set theoretical product endowed with the componentwise addition and multiplication.

Modules over Rings

Let A be a ring. An abelian group M is called an Amodule if there is a multiplication A _M ! M such that a(x + y) = ax + ay; (a + b)x = ax + bx; a(bx) = (ab)x; 1x = x.

Examples. Every abelian group is a Zmodule,so the class of abelian groups coincide with the class of Zmodules.
Every vector space over a field F is an F module.

A map f:M ! N is called a homomorphism of Amodules
if f(x + y) = f(x) + f(y) for every x; y 2 M and f(ax) = af(x) for every a 2 A, x 2 M. A homomorphism
f of Amodules is called an isomorphism of Amodules, or alternatively an Aisomorphism, if f is bijective.
A subgroup N of an Amodule M is called an Asubmodule of M if an 2 N for every a 2 A; n 2 N.

Example: Submodules of the Amodule A are ideals of A. For an AmoduleM and its submodule N define the quotient module M=N as the quotient set of cosets m + N with the natural addition and multiplication by elements of A.
Similarly to 1.1 one proves: If M;N are Amodules and f:M ! N is an Amodule homomorphism, then the kernel of f is a submodule of M and the image of f is a submodule of N, and M= ker(f) is Aisomorphic to im(f).
Similarly to 1.1 submodules of the quotient module M=N are in 1–1 correspondence with submodules of M containing N.
In particular, if f:M ! N is an Amodule homomorphism, and K is a submodule of ker(f), then f nduces an Amodule homomorphism g:M=K ! N; m + K 7! f(m).

For AmodulesM;N the intersection M \ N is an Amodule.So if M;Nare contained in a larger module L, one can speak about the minimal Amodulewhichcontains a fixed set of elements related to M and N.
Then the M + N = fm + n : m 2 M; n 2 Ng is the minimal Amodule which contains all all elements of M and N.
Define the direct sum of modules as the set theoretical product with the natural addition and multiplication by elements of A.

Lemma. Let N;K be Asubmodules of an Amodule M. A map f:N_K ! N+K, f((n; k)) = n+k is a surjective Amodulehomomorpism whose kernel is Aisomorphic to the submodule N \K. Therefore, if N \K = f0g, N _K is isomorphic to N +K.
Proof. Clearly f is surjective. Its kernel is f(n; k) : n + k = 0g. Then n = □k 2 N \ K. A map f(n; k) : n + k = 0g ! N \ K; (n;n) 7! n is a bijection.

The submodule M generated by elements xi is the minimal submodule which contains all of them, it consists of finite Alinear combinations of xi ; elements xi 2 M are called generators of M
The minimal number of generators (if it exists) of M is called the rank of M. M is said to be of finite type if it has a finite number of generators.
An Amodule M is called free if M has generators xi such that P aixi = 0 implies ai = 0 for all i. The set of xi is called then a basis of M.

Example Let A = F be a field. Let M;N be two F vector spaces of dimensions d1 and d2. In accordance with the previous theorem the vector space of linear maps M N ! F is isomorphic to the vector space of bilinear maps M _F N !F . In accordance with Example in 3.2 the dimension of the space Bil(M;N; F) is d1d2; if m1; : : : ;md1 is a basis of M and n1; : : : ; nd2 is a basis of N, then every bilinear map f:M _ N ! F is determined by its values on f(mi; nj)g. Therefore, the dimension of the vector space HomF (M F N; F) is d1d2. It is known from linear algebra that the dimension of a vector space V equals to the dimension of HomF (V; F). So the dimension of M N is d1d2; the F vector space M F N has a basis mi nj , 1 6 i 6 d1; 1 6 j 6 d2. Note that in the particular case of M = N the space N F N has dimension equal to the square of the dimension of

N. In physics, N over F = C represents the state vector of a particle, and N C N represents the state vectors of two independent particles of the same kind.

5.3 LET US SUM UP

In this unit we study group homomorphism and its examples. We study isomorphism and its definition and properties. We study Automorphism and its examples. We study Endomorphism and its definiton. We study third isomorphism theorem and its proof. We study Kernel and epimorphism. We study theorem on ring homomorphism.

- A homomorphism is a map between two algebraic structures of the same type , that preserves the operations of the structures. This means a map between two sets *A, B* equipped with the same structure such that, if is an operation of the structure then

for every pair *x, y* of elements of *A*. says often that *f* preserves the operation or is compatible with the operation.

- The endomorphisms of a vector space or of a module form a ring. In the case of a vector space or a free module of finite dimension, the choice of a basis induces a ring isomorphism between the ring of endomorphisms and the ring of square matrices of the same dimension.
- A split epimorphism is a homomorphism that has a right inverse and thus it is itself a left inverse of that other homomorphism.
- The kernel of a ring homomorphism $f : R \longrightarrow S$ is the set of all elements of R which are mapped to zero. It is the kernel of f as a homomorphism of additive groups. It is an ideal of R.
- Isomorphism Theorem:

Let φ : G → G0 be a homomorphism of groups. Then G/ ker(φ) ∼= φ(G)

- Theorem on ring homomorphisms. The kernel I of f is an ideal of A, the image C of f is a subring of B. The quotient ring A/I is isomorphic to C

5.4 KEYWORD

Independent :Free from outside control; not subject to another's authority.

Isomorphism :An isomorphism is a homomorphism or morphism (i.e. a mathematical .... Then a general definition of isomorphism

Lattice :A structure consisting of strips of wood or metal crossed and fastened together with square or diamond-shaped spaces left between, used as a screen or fence or as a support for climbing plants

5.5 QUESTIONS FOR REVIEW

1 If $\varphi : GL2(R) \to R\backslash\{0\}$ is given by $\varphi(A) = \det(A)$ then $\ker(\varphi(A)) = SL2(R)$ and $\text{im}(\varphi) = R\backslash\{0\}$

2 Let $\varphi : G \to G0$ be a homomorphism.

Then

1. $\ker(\varphi)$ is a subgroup of G, and φ is injective if and only if $\ker(\varphi) = eG$.

2. $\text{im}(\varphi)$ is a subgroup of G0 , and φ is surjective if and only if $\text{im}(\varphi) = G0$ (or equivalently, $\varphi(G) = G0$)

3. Suppose $\sigma * Sn$ is written as a product of transposition in two different ways, say $\sigma = \beta1\beta2 \cdots \beta r$ and $\sigma = \gamma1\gamma2 \cdots \gamma s$. Then $r \equiv s \bmod 2$.

4 The set of even permtuations in Sn is a subgroup of Sn. This group is called the alternating group of order n, and is denoted by An. Moreover, $|An| = n!\ 2$

5.6 ANSWER FOR CHECK IN PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 1.4

Q. 2 Check in Section 1.2

Check in Progress-II

Answer Q. 1 Check in Section 1.5

Q. 2 Check in Section 2.1

5.7 SUGGESTION READING AND REFERENCES

1. *"Whence "homomorphism" and "homomorphic"?". mathoverflow.net. Retrieved 21 March 2018.*
2. ^ Jump up to:[a b c d e] *Birkhoff, Garrett (1967) [1940], Lattice theory, American Mathematical Society Colloquium Publications,* ***25*** *(3rd ed.), Providence, R.I.: American Mathematical Society, ISBN 978-0-8218-1025-5, MR 0598630*
3. ^ Jump up to:[a b c] *Stanley N. Burris; H.P. Sankappanavar (2012). A Course in Universal Algebra (PDF). ISBN 978-0-9880552-0-9.*
4. ^ Jump up to:[a b c] *Mac Lane, Saunders (1971). Categories for the Working Mathematician. Graduate Texts in Mathematics.* ***5****. Springer-Verlag. Exercise 4 in section I.5. ISBN 0-387-90036-5. Zbl 0232.18001.*
5. ^ Linderholm, C. E. (1970). A group epimorphism is surjective. *The American Mathematical Monthly*, 77(2), 176-177.
6. ^ *Dăscălescu, Sorin; Năstăsescu, Constantin; Raianu, Şerban (2001). Hopf Algebra: An Introduction. Pure and Applied Mathematics.* ***235****. New York, NY: Marcel Dekker. p. 363. ISBN 0824704819. Zbl 0962.16026.*
7. ^ Section 17.4, in Gunther Schmidt, 2010. *Relational Mathematics*. Cambridge University Press, ISBN 978-0-521-76268-7
8. ^ Seymour Ginsburg, *Algebraic and automata theoretic properties of formal languages*, North-Holland, 1975, ISBN 0-7204-2506-9,

9. ^ T. Harju, J. Karhumäki, Morphisms in *Handbook of Formal Languages*, Volume I, edited by G. Rozenberg, A. Salomaa, Springer, 1997, ISBN 3-540-61486-9.
10. Emmy Noether, *AbstrakterAufbau der Idealtheorie in algebraischenZahl- und Funktionenkörpern*, MathematischeAnnalen **96** (1927) pp. 26–61
11. Colin McLarty, 'Emmy Noether's 'Set Theoretic' Topology: From Dedekind to the rise of functors' in *The Architecture of Modern Mathematics: Essays in history and*
12. *Hall, ISBN 0130878685*

UNIT 6 - EXACT SEQUENCE, FOUR AND FIVE LEMMA

STRUCTURE

6.0 OBJECTIVE

After reading this unit we learn to know about four lemma. Learn abhout short exact sequence,long exact sequence, Ring lemma and diagram chasing. We also learn about commutative diagram.

6.1 INTRODUCTION: COMMUTATIVE DIAGRAM

Let RR be an integral domain and α:R→R′α:R→R′ an injective ring homomorphism. Let KK and K′K′ be the fields of fractions
of RR and R′R′ respectively. I know that there is a commutative diagram of rings

Rα□ ↓□ R′−→−−−ι−→−−−ι′Kβ□ ↓□ K′R→ιKα↓β↓R′→ι′K′

where ιι and ι′ι′ are the canonical inclusion maps. Here ββ can be defined by β(r/s)=α(r)/α(s)β(r/s)=α(r)/α(s) for r∈Rr∈R and s∈R−0
My question: is there a similar commutative diagram if we replace respectively K and K′ by arbitrary extension fields F and F′?
n mathematics, and especially in category theory, a **commutative diagram** is a diagram such that all directed paths in the diagram with the same start and endpoints lead to the same result. Commutative diagrams play the role in category theory that equations play in algebra.

6.1.1 Arrow Symbols

In algebra texts, the type of morphism can be denoted with different arrow usages:

- monomorphisms with a
- epimorphisms with a
- isomorphisms with a .
- the dashed arrow typically represents the claim that the indicated morphism exists whenever the rest of the diagram holds; the arrow may optionally be labeled .

If the dashed arrow is labeled or , the morphism is furthermore unique.

These conventions are common enough that texts often do not explain the meanings of the different types of arrow.

6.1.2 Diagram Chasing

Diagram chasing (also called **diagrammatic search**) is a method of mathematical proof used especially in homological algebra. Given a commutative diagram, a proof by diagram chasing involves the formal use of the properties of the diagram, such as injective or surjective maps, or exact sequences. A syllogism is constructed, for which the graphical display of the diagram is just a visual aid. It follows that one ends up "chasing" elements around the diagram, until the desired element or result is constructed or verified.

Examples of proofs by diagram chasing include those typically given for the five lemma, the snake lemma, the zig-zag lemma, and the nine lemma.

6.1.3 Diagrams As Functors

A commutative diagram in a category *C* can be interpreted as a functor from an index category *J* to *C;* one calls the functor a diagram**.**

More formally, a commutative diagram is a visualization of a diagram indexed by a poset category:

- one draws a node for every object in the index category,
- an arrow for a generating set of morphisms,

  omitting identity maps and morphisms that can be expressed as compositions,

- and the commutativity of the diagram (the equality of different compositions of maps between two objects) corresponds to the uniqueness of a map between two objects in a poset category.

Conversely, given a commutative diagram, it defines a poset category:

- the objects are the nodes,
- there is a morphism between any two objects if and only if there is a (directed) path between the nodes,

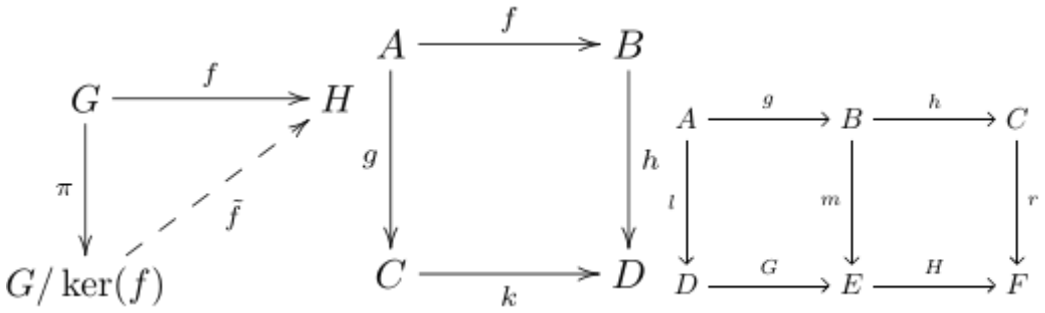
- with the relation that this morphism is unique (any composition of maps is defined by its domain and target: this is the commutativity axiom).

However, not every diagram commutes (the notion of diagram strictly generalizes commutative diagram): most simply, the diagram of a single object with an endomorphism (), or with two parallel arrows as used in the definition of equalizer need not commute. Further, diagrams may be messy or impossible to draw when the number of objects or morphisms is large (or even infinite).

Example

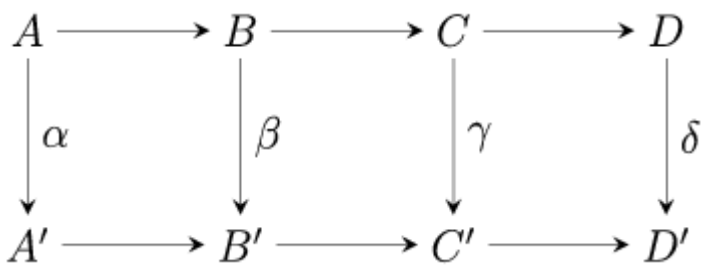
In the bottom-left diagram, which expresses the first isomorphism theorem, commutativity means that while in the bottom-right diagram,

commutativity of the square means :



For the diagram below to commute, we must have the three equalities:. Since the first equality follows from the last two, for the diagram to commute it suffices to show (2) and (3). However, since equality (3) does not generally follow from the other two equalities, for this diagram to commute it is generally not enough to only have equalities (1) and (2).

6.2 FOUR LEMMA



A diagram lemma which states that, given the above commutative diagram with exact rows, the

following holds:

1. If α is surjective, and β and δ are injective, then γ is injective;

2. If δ is injective, and α and γ are surjective, then β is surjective.

This lemma is closely related to the five lemma, which is based on a similar diagram obtained by adding a single column.

Diagram chasing is a method of mathematical proof used especially in homological algebra. Homological algebra studies, in particular, the homology of chain complexes in abelian categories – therefore the name. From a modern perspective, homological algebra is the study of algebraic objects, (such as groups, rings or Lie algebras, or sheaves of such objects), by 'resolving them', replacing them by more stable objects whose homotopy category is the derived category of an abelian category. Given a commutative diagram, a proof by diagram chasing involves the formal use of the properties of the diagram, such as injective or surjective maps, or exact sequences. A syllogism is constructed, for which the graphical display of the diagram is just a visual aid. It follows that one ends up "chasing" elements around the diagram, until the desired element or result is constructed or verified. Examples of proofs by diagram chasing include those typically given for the Snake Lemma, Four Lemma, Five Lemma, Nine Lemma, and Zig-Zag Lemma.

Definition 1 An **exact sequence** is a sequence, either finite or infinite, of objects and morphisms between them such that the image of one morphism equals the kernel of the next.

Definition 2 A **short exact sequence** is a finite sequence of objects and morphisms between them such that the image of one morphism equals the kernel of the next.

Definition 3 A **long exact sequence** is an infinite sequence of objects and morphisms between them such that the image of one morphism equals the kernel of the next.

Formally, an exact sequence is a sequence of maps

$$\alpha_i : A_i \to A_{i+1}$$

between a sequence of spaces A_i, which satisfies

$$im(\alpha_i) = \ker(\alpha_{i+1}),$$

where im denotes the image and $\ker$ the group kernel. That is, $a \in A_i, \alpha_i(a) = 0$ iff $a = \alpha_{i-1}(b)$ for some $b \in A_{i-1}$. It follows that $\alpha_{i+1} \circ \alpha_i = 0.$ The notion of exact sequence makes sense when the spaces are groups, modules, chain complexes, or sheaves. The notation for the maps may be suppressed and the sequence written on a single line as

$$\cdots \to A_{i-1} \to A_i \to A_{i+1} \to \cdots .$$

1. A short exact sequence:

   $$0 \to A \to B \to C \to 0.$$

   beginning and ending with zero, meaning the zero module $\{0\}$.

2. A long exact sequence:

   $$\cdots \to A \to B \to C \to \cdots .$$

Special information is conveyed when one of the spaces is the zero module. For instance, the sequence

$$0 \to A \to B$$

is exact iff the map is injective. Similarly,

$$A \to B \to 0$$

is exact iff the map is surjective.

In homological algebra, given a short exact sequence $0 \to M' \to M \to M'' \to 0$ of G-modules, there is a canonical long exact sequence

where the δ_i are certain "connecting homomorphisms" (or "snake maps"). This can be deduced from the Snake Lemma. For the proof the latter, one can engage in "diagram chasing". One can see, in the movie *It's My Turn* (1980) a proof given for the Snake Lemma using diagram chasing. To define δ: given $x'' \in \ker(\gamma) \subseteq C$, lift x" to B, push it into B' by β, then check that the image has a preimage in A'. Then verify that the result is well-defined, et cetera.

Lemma 1 (Snake Lemma) Given the commuting diagram

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' \end{array}$$

in which the rows are exact, there is a canonical map $\delta : \ker(\gamma) \to coker(\alpha)$, induced by $\delta x'' = f'^{-1} \circ \beta \circ g^{-1} x''$ such that the sequence

is exact.

Proof: Suppose we are given a commutative diagram

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' \end{array}$$

with exact rows. We wish to prove that the sequence

is exact.

First we claim that if any square

$$\begin{array}{ccc} X_1 & \longrightarrow & Y_1 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ X_2 & \longrightarrow & Y_2 \end{array}$$

is commutative, then there are well-defined morphisms $\ker(\varphi) \to \ker(\psi)$ and $coker(\varphi) \to coker(\psi)$. For example, if $x \in \ker(\varphi)$, then the square

$$\begin{array}{ccc} x & \longmapsto & y \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ 0 & \longmapsto & 0 \end{array}$$

must commute, and so the image of x in the top row must be in $\ker(\psi)$. The proof of the claim for cokernels is similar. Thus we have two sequences,

each of which inherits being a complex from the original diagram.

Suppose $x \in \ker(\beta)$ is sent to $0 \in \ker(\gamma)$. By exactness, x has a preimage $x' \in A$. Because the diagram

$$\begin{array}{ccc} x' & \longmapsto & x \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ y' & \longmapsto & 0 \end{array}$$

is commutative and the bottom morphism is injective, $y' = 0$ and so $x' \in \ker(\alpha)$. So the sequence

$$0 \to \ker(\alpha) \to \ker(\beta) \to \ker(\gamma)$$

is exact. The proof of the claim for the cokernel sequence is similar.

So now all we need to do is find a connecting morphism $\ker(\gamma) \to coker(\alpha)$ such that the resulting sequence is exact at both of those points.

Suppose $x'' \in \ker(\gamma)$. Then x'' has at least one preimage in B. So let x and $\widehat{x}$ be preimages of x''. Thus $\widehat{x} - x \mapsto 0$ and so by exactness has a preimage $x' \in A$. By commutativity of the diagram, $\beta(x)$ has a preimage y', which is unique by injectivity of the morphism $A' \to B'$. But we know that the square

$$\begin{array}{ccc} x' & \longmapsto & \widehat{x} - x \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ \alpha(x') & \longmapsto & \beta(\widehat{x} - x) \end{array}$$

is commutative. We wish to define $\ker(\gamma) \to coker(\alpha)$ by $x'' \mapsto y' + im(\alpha)$. Observe that

$$y' + \alpha(x') \mapsto \beta(x) + \beta(\widehat{x} - x) = \beta(\widehat{x}),$$

and so the choice of preimage of x'' does not affect which cokernel element we ultimately select. So now we have our connecting morphism. By applying this definition we see that

$$\ker(\beta) \to \ker(\gamma) \to coker(\alpha) \to coker(\beta)$$

is a complex.

Suppose $x'' \in \ker(\gamma)$ is sent to 0 by the connecting morphism. Thus we have a diagram

$$\begin{array}{ccccc} x' & & x & \longmapsto & x'' \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ y' & \longmapsto & \beta(x) & \longmapsto & 0 \end{array}$$

which is commutative. Let $\widehat{x}$ be the image of x' under the morphism $A \to B$. Exactness of the diagram implies that $x - \widehat{x}$ is a

preimage of x''. But $\beta(x - \widehat{x}) = 0$. So the kernel-cokernel sequence is exact at $\ker(\gamma)$. The proof that it is exact at $coker(\alpha)$ is similar.

Check in Progress-I

Q. 1 Define four lemma.

Solution

……

……

……

……

Q. 2 Define Diagram Chasing.

Solution

……

……

……

……

6.3 THE RING LEMMA

For each n > 3, let cn denote the infimum of the radii among n discs surrounding the unit disc. Then cn > 0. The sharp ring lemma states that cn = (F 2 n−1 + F 2 n−2 − 1), −1 where Fk is the k th Fibonacci number, and that this lower limit is attained in essentially unique configurations, see section 3 for the precise statement. We will use the Descartes circle theorem in the following special case, where the balls are required to have pairwise disjoint interiors. Just as halfplanes are viewed as discs of infinite radius, half-spaces are considered to be balls of infinite radius in R 3 ∪ {∞}, having disjoint interiors if they only intersect at infinity, in which case they are also tangent.

The Descartes circle theorem. Suppose N + 2 pairwise tangent balls in R N, N > 2, have pairwise disjoint interiors and inverse radii b1, . . . , bN+2. Then N P i b 2 i = (P i bi).

Apollonian configurations The sharp ring lemma, which we will give a proof of below, gives that the sharp value of the ring lemma constant is attained in essentially unique configurations. Those configurations, which we will call Apollonian configurations, are defined as follows.

We recursively construct a configuration of discs A1, A2, . . . such that for each n > 3, the discs A1, . . . , An surround the unit disc D0 (figure 2). First, we let A1, A2, A3 be discs with pairwise disjoint interiors that are externally tangent to the unit disc and where A1, A2 have infinite radii, hence A3 has unit radius. Given discs A1, . . . , An, n > 3, we let An+1 be externally tangent to D0, An−1 and An.

Definition. A configuration of n > 3 discs surrounding the unit disc is said to be an Apollonian configuration if it is equal to A1, . . . , An – as defined above – up to reflection and rotation. We see that the Apollonian configurations of three discs are unique up to rotation, and that Apollonian configurations of order four and higher are uniquely determined by the position of the third and fourth largest discs, corresponding to A3 and A4, respectively.

6.3.1 Method of Proof

We will prove the sharp ring lemma using a compactness argument in strip configurations, defined below. A more ‘dynamic’ approach, which we will not use, is as follows. Noting that given k ∈ {3, . . . , n}, the radius of Ak in an Apollonian configuration of n discs cannot be increased if A1, . . . , Ak−1 are fixed, it would be natural to try to successively modify the radii in an arbitrary configuration in order to reduce it to a configuration.

An Apollonian configuration of six discs A1, . . . , A6 surrounding the unit disc D0. The radius of A6 is the smallest possible for six discs surrounding the unit disc.having this property. That is, given discs D1, . . . , Dn surrounding D0 we want to find a permutation (i1, . . . , in) of (1, . .

. , n) such that in the k th step the radius of Dik is increased – forcing Dik+1 , . . . , Din to change in order to maintain the surround property – until Dik touches the already increased Di1 , . . . , Dik−1 . For this smaller set of configurations, the sharp ring lemma can be verified using a monotonicity property of the Descartes circle theorem.

The difficulty with this approach is determining in what order to modify the discs, while preventing the smallest radius from increasing after all the adjustments. Given the properties of the Apollonian configurations, a natural candidate is to index by size, so that rik > rik+1 . However, one must be more careful as the following simple counterexample shows (figure 3). Let D1, . . . , D6 be discs surrounding the unit disc D0, numbered clockwise by their tangency with D0, having radii r1 = r2 = +∞, r3 = 1, r5 = 1 5 and where D3 and D5 share an extra tangency; we see that this gives min(r4, r6) < 1 12 . The largest disc that can be increased without decreasing the radius of a larger disc is D5, and increasing the radius of this disc as much as D1, D2 and D3 allow, we see that the new radii satisfy min(r4, r6) = 1 12

This method of proof was pursued in more detail by Hansen [12] and Stephenson [21]. Here we will reduce the problem to a simpler class of.

2 The radii of the discs D1, D2, D3 in (a) cannot be increased without decreasing a larger disc. Increasing the largest remaining disc D5 until it is stopped by D1, D2, D3 gives the configuration in (b), where min(r1, . . . , r6) has increased.

Definition. Sequentially tangent discs D1, . . . , Dn, n > 2, are said to lie in a strip configuration if all discs lie between two parallel straight lines L1 and L2, have pairwise disjoint interiors and are tangent to L1, and moreover D1, Dn are tangent to L2. A tangency between Di and Di+1,i = 1, . . . , n−1, is said to be ordinary, and other tangencies, except those with L1, are said to be extra tangencies.

Lemma. Suppose DI and DII are non-outermost discs that share an ordinary tangency in a strip configuration. Construct a new strip configuration by adding a disc DIII that shares an ordinary tangency with DI and DII. Let h be the distance from the common line in the strip

configuration to the tangency between DI and DII. Suppose that h or one the of radii rI, rII, rIII is minimal among the strip configurations obtained by varying DI, DII and DIII, while maintaining the extra tangency between DI and DII. Then DI or DII has an additional extra tangency.

Proof. Let DA and DB be discs such that DA, DI, DIII, DII, DB are sequentially tangent discs with ordinary tangencies, and let 2L be the centerto-center distance between DA and DB, as measured parallel to the common line in the strip configuration.

6.4 THE RING LEMMA IN THREE DIMENSIONS

Introduction A generalization of the ring lemma to three dimensions should determine the infimum of the radii for a set of n balls with pairwise disjoint interiors surrounding the unit ball. It is not clear, however, in what sense a finite set of balls should 'surround' the unit ball. For instance, given any finite number of balls tangent to the unit ball, one can always find a smooth curve starting on the unit sphere that escapes to infinity without passing through any of the balls.

Surrounding and hiding packings

All balls are closed, and we remind that we view half-spaces as balls of infinite radius in R 3 ∪ {∞}, having disjoint interiors if they only intersect at infinity, in which case they are also tangent.

For each set of balls B1, . . . , Bn we define a combinatorial complex K(B1, . . . , Bn) of vertices, edges and faces as follows: start with n vertices v1, . . . , vn, add edges between vi, vj, i≠ j if Bi, Bj are tangent, i, j = 1, . . . , n, and faces given by every set of three edges corresponding to three pairwise tangent balls.

Definition. Suppose B1, . . . , Bn, n > 4, are balls with pairwise disjoint interiors that are externally tangent to the unit ball B0. We say that the balls B1, . . . , Bn surround B0 if K(B1, . . . , Bn), as defined above, has a subcomplex, containing all the vertices, that triangulates the unit sphere, and if the triangulation can be embedded without overlap in the unit sphere in such a way that:

I vi is the point of tangency between B0 and Bi

,ii each edge is a shortest path on the unit sphere between its endpoints, and

(iii) the faces are spherical triangles Tijk satisfying area(Tijk) 6 2π. If, additionally, every straight half-line starting at the origin intersects B1 ∪ · · · ∪ Bn, we say that B1, . . . , Bn hide B0.

Condition (iii) gives the convexity property that between any two points in Tijk there is a shortest path on the unit sphere that is contained in Tijk, and consequently that any shortest path strictly shorter than π between points in Tijk is contained in Tijk.

Remark. In two dimensions, unless two of the discs are half-planes, no curve starting on the unit disc can escape to infinity without passing through one of the surrounding discs. Hence, a hide property is less interesting in two dimensions.

Remark. Portions of lattice structures such as hexagonal close packing or face-centered cubic – lattices which are of great practical importance – do not satisfy this definition. In fact, both packings can be realized as stacked layers of identical balls forming a hexagonal pattern, making each ball tangent to twelve others. If we select a ball, corresponding to the unit ball and consider the balls tangent to it, six of the balls form a closed chain around the original ball and the other six are divided between two layers, each containing three balls. The above definition only considers groups of three pairwise tangent balls, and we see that we get six 'holes' formed between groups of four cyclically tangent balls. We may, however, add a ball in each 'hole' in order to satisfy the definition.

6.5 LEMMA FOR THE LOWER BOUND

Take x^≠ 0. Denote by Φ the reflection in S(x, 1 ^) – that is, the sphere centered at x^ with unit radius – which is a Möbius transformation satisfying Φ−1 = Φ and Φ S (|x^| ± r) x^ |x^| , r = P |x^| ± 1 2r , where

P(α) = x ∈ R 3 ; x · x^ |x^| = α ∪ {∞} is a plane. Furthermore, we let r, r′ , ri and so on denote the radii of correspondingly marked balls B, B′ ,

Lemma. Suppose B1, . . . , Bn surround B0. Let B∗ be one of the surrounding balls and x^ its intersection with B0. Denote by Φ the reflection in S(x, 1 ^). If the spherical triangle Tpqr contains the antipode of x^, then 1 r ′ i + 1 r ′ j > 4 for all i, j ∈ {p, q, r} with r ′ i , r′ j < +∞ and i≠ j, where r ′ i is the radius of Φ(B.

Proof. Transforming the configuration using Φ gives a kind of threedimensional 'strip configuration' where the balls tangent to B∗ for closed chain of balls tangent to the half-spaces B ′ ∗ = Φ(B∗) and B ′ 0 = Φ(B0).

For purposes of orientation, we consider B ′ 0 to lie below B ′ ∗ – a point x lies below another point x ′ , and x ′ above x, if x is closer to the boundary of B ′ 0 than x ′ is – and in the original configuration we let x^ be the north pole of B0

To simplify the notation, we renumber so that (p, q, r) = (1, 2, 3). If Bi, Bj, i≠ j, are tangent at etij we let tij = etij |etij| , which is the point on B0 closest to the tangency between Bi and Bj.

Suppose first that B∗≠ Bi, i = 1, 2, 3. Referring to the 'strip configuration' – figure 7 (b) – consider the three planes P ′ 12, P′ 13, P′ 23 that are parallel to the boundary of B ′ 0 and where P ′ ij passes through B ′ i ∩ B ′ j . Aiming to show that x^ = Φ(∞) lies on or above at least one of the planes, we assume this is not the case. Then the planes P ′ ij are mapped by Φ to spheres that contain Bi ∩ Bj, are tangent to B∗ at x^ and enclose B∗\{x^}, and it follows that t12, t13 and t23 lie in the interior of the northern hemisphere. We obtain the required contradiction by showing that the spherical triangle T123 cannot enclose the south pole −x^, contradicting the construction.

Since the points of tangencies between the balls B1, B2, B3 lie on the northern hemisphere of B0, we see that at most one of them can be tangent to the southern hemisphere of B0. If all balls B1, B2, B3 are tangent to the northern hemisphere, we obtain the contradiction

immediately, hence we may assume without loss of generality that B1 is tangent to the interior of the southern hemisphere of B0. Consider first the plane through the tangencies between B0, B1 and B2 (figure 8). The plane passes through the center of B0 and determines a great circle on B0. We see that the length α2 of the shortest path on the unit sphere between t01 and t12, satisfies $\alpha 2 < \pi 2$, and the same holds for the correspondingly defined length α3.

The points t12 and t13 lie on the northern hemisphere, and we claim that since the lengths α2, α3 satisfy $\max(\alpha 2, \alpha 3) < \pi 2$, the spherical triangle T123 cannot enclose −x^. First, note that it is sufficient to consider the spherical triangle contained in T123 that has vertices t12, t13, t01, where we may assume that t12 and t13 lie on the equator. Suppose now that the south pole is contained in this smaller triangle. Since the triangle does not contain a great circle, a shortest path on the unit sphere from t01 to the south pole – a path which lies within the triangle – may be extended within the triangle along its great circle until it intersects the side between t12 and t13 at a point x. The intersection is at a right angle, and, without loss of generality, we may assume that the shortest path between x and t13 is shorter than π 2 and also exclude the trivial case x = t13. Letting a, b, c be the lengths of the sides opposite to x, t13 and t01, respectively, the spherical Pythagorean theorem yields cos a = cos b cos c. We have that $a < \pi 2$, b 6 π, c 6 π 2 , hence cos a > 0 and cos c > 0, so that $b < \pi 2$, which is impossible since the corresponding shortest path passes through both the equator and the south pole.

Now consider the case where B∗ = Bi for some i; without loss of generality we may assume that B∗ = B3. Using the previous construction of P ′ 12, we again assume that x^ lies strictly below P ′ 12, and, as above, it follows that t12 lies on the northern hemisphere of B0. Furthermore, we see that the projection x 7→ x |x| on B0 of the entire ball B3 = B∗ lies on the northern hemisphere of B0, hence so does t13, t23. Again this means that the spherical triangle T123 determined by B1, B2, B3 cannot enclose −x^.

Hence x^ – which is a distance 1 2 from B ′ 0 – must lie on or above at least one plane P ′ ij. Since the distance between P ′ ij and B ′ 0 is 2 1 r ′ i

+ 1 r ′ j , −1 just like in the two-dimensional case, we get the desired inequality.

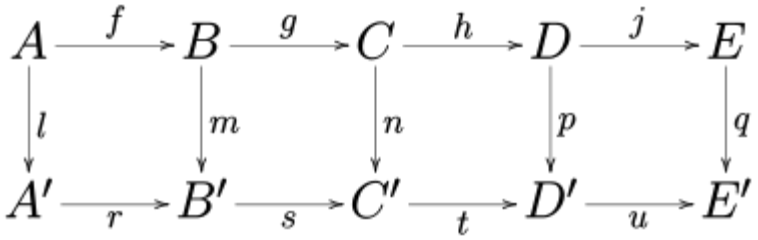
6.6 FIVE LEMMA

In mathematics, especially homological algebra and other applications of abelian category theory, the **five lemma** is an important and widely used lemma about commutative diagrams. The five lemma is not only valid for abelian categories but also works in the category of groups, for example.

The five lemma can be thought of as a combination of two other theorems, the **four lemmas**, which are dual to each othe

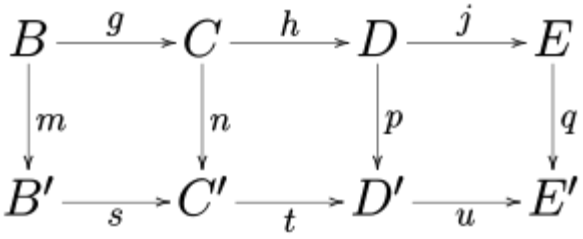
6.7 STATEMENTS

Consider the following commutative diagram in any abelian category (such as the category of abelian groups or the category of vector spaces over a given field) or in the category of groups.



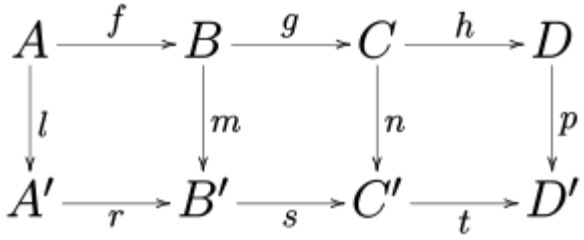
The five lemma states that, if the rows are exact, *m* and *p* are isomorphisms, *l* is an epimorphism, and *q* is a monomorphism, then *n* is also an isomorphism.

The two four-lemmas state:
(1) If the rows in the commutative diagram



are exact and *m* and *p* are epimorphisms and *q* is a monomorphism, then *n* is an epimorphism.

(2) If the rows in the commutative diagram



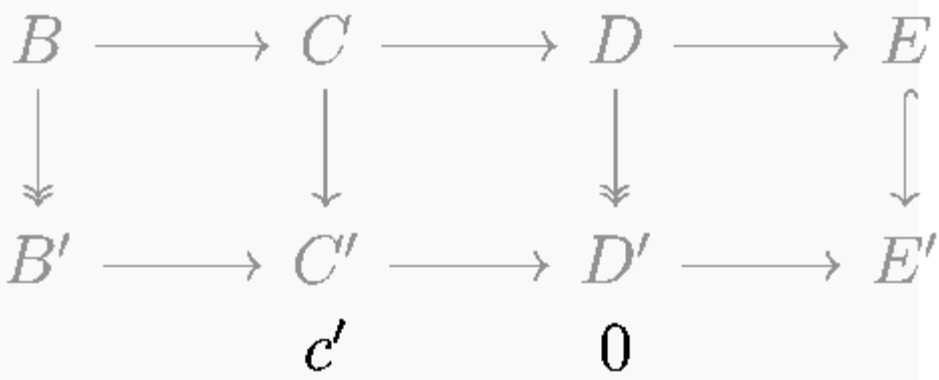
are exact and *m* and *p* are monomorphisms and *l* is an epimorphism, then *n* is a monomorphism.

Proof

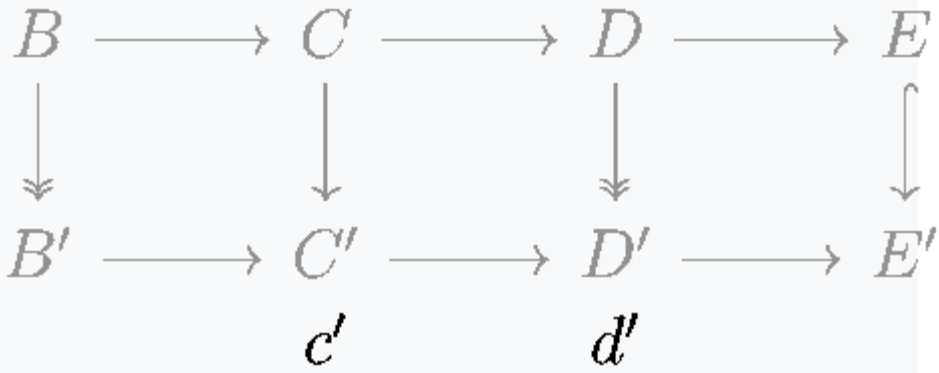
The method of proof we shall use is commonly referred to as diagram chasing.[1] We shall prove the five lemma by individually proving each of the two four lemmas.

To perform diagram chasing, we assume that we are in a category of modules over some ring, so that we may speak of *elements* of the objects in the diagram and think of the morphisms of the diagram as *functions* (in fact, homomorphisms) acting on those elements. Then a morphism is a monomorphism if and only if it is injective, and it is an epimorphism if and only if it is surjective. Similarly, to deal with exactness, we can think of kernels and images in a function-theoretic sense. The proof will still apply to any (small) abelian category because of Mitchell's embedding theorem, which states that any small abelian category can be represented as a category of modules over some ring. For the category of groups, just turn all additive notation below into multiplicative notation, and note that commutativity of abelian group is never used.

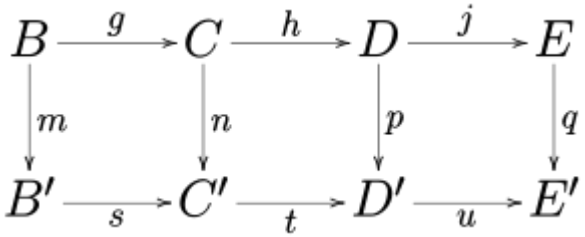
So, to prove (1), assume that *m* and *p* are surjective and *q* is injective.



A proof of (1) in the case where .



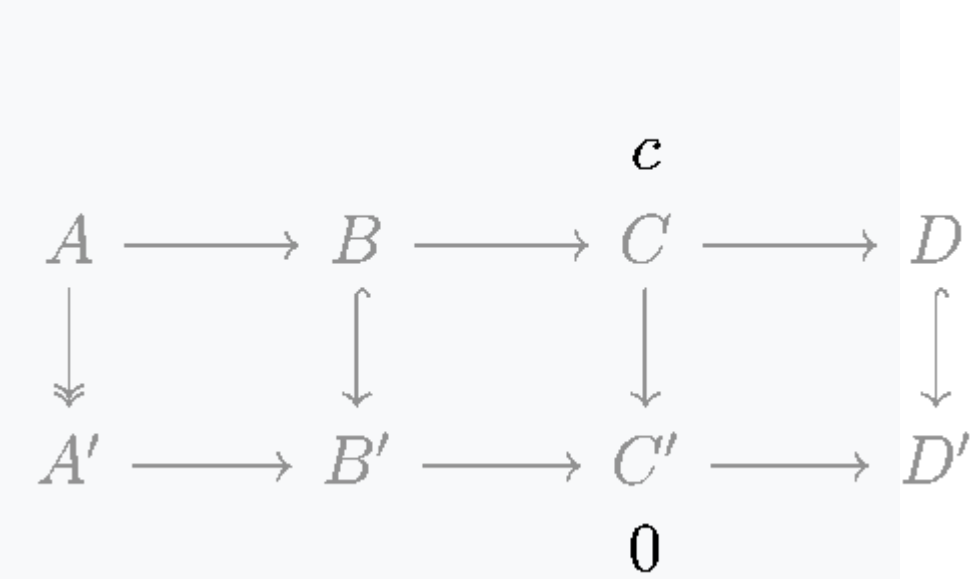
A proof of (1) in the case where .



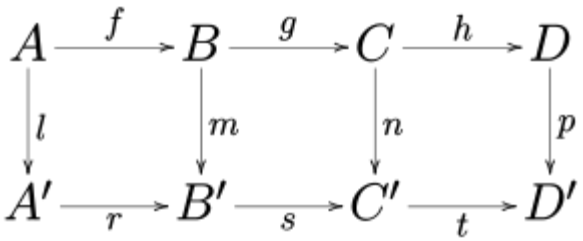
- Let c' be an element of C'.
- Since p is surjective, there exists an element d in D with $p(d) = t(c')$.
- By commutativity of the diagram, $u(p(d)) = q(j(d))$.
- Since im t = ker u by exactness, $0 = u(t(c')) = u(p(d)) = q(j(d))$.
- Since q is injective, $j(d) = 0$, so d is in ker j = im h.

- Therefore, there exists c in C with $h(c) = d$.
- Then $t(n(c)) = p(h(c)) = t(c')$. Since t is a homomorphism, it follows that $t(c' - n(c)) = 0$.
- By exactness, $c' - n(c)$ is in the image of s, so there exists b' in B' with $s(b') = c' - n(c)$.
- Since m is surjective, we can find b in B such that $b' = m(b)$.
- By commutativity, $n(g(b)) = s(m(b)) = c' - n(c)$.
- Since n is a homomorphism, $n(g(b) + c) = n(g(b)) + n(c)$ $= c' - n(c) + n(c) = c'$.
- Therefore, n is surjective.

Then, to prove (2), assume that m and p are injective and l is surjective.



A proof of (2).



- Let c in C be such that $n(c) = 0$.
- $t(n(c))$ is then 0.
- By commutativity, $p(h(c)) = 0$.

- Since p is injective, $h(c) = 0$.
- By exactness, there is an element b of B such that $g(b) = c$.
- By commutativity, $s(m(b)) = n(g(b)) = n(c) = 0$.
- By exactness, there is then an element a' of A' such that $r(a') = m(b)$.
- Since l is surjective, there is a in A such that $l(a) = a'$.
- By commutativity, $m(f(a)) = r(l(a)) = m(b)$.
- Since m is injective, $f(a) = b$.
- So $c = g(f(a))$.
- Since the composition of g and f is trivial, $c = 0$.
- Therefore, n is injective.

Combining the two four lemmas now proves the entire five lemma.

Applications

The five lemma is often applied to long exact sequences: when computing homology or cohomology of a given object, one typically employs a simpler subobject whose homology/cohomology is known, and arrives at a long An **exact sequence** is a concept in mathematics, especially in group theory, ring and module theory, homological algebra, as well as in differential geometry. An exact sequence is a sequence, either finite or infinite, of objects and morphisms between them such that the image of one morphism equals the kernel of the next.

exact sequence which involves the unknown homology groups of the original object. This alone is often not sufficient to determine the unknown homology groups, but if one can compare the original object and sub object to well-understood ones via morphisms, then a morphism between the respective long exact sequences is induced, and the five lemma can then be used to determine the unknown homology groups.

Check in Progress-II

Q. 1 Define five lemma.

Solution

……

……

……

……

Q, 2 Define Lemma for Lower bound.

Solution

……

……

……

……

Definition

In the context of group theory, a sequenceof groups and group homomorphisms is called **exact** if the image of each homomorphism is equal to the kernel of the next:

The sequence of groups and homomorphisms may be either finite or infinite.

A similar definition can be made for other algebraic structures. For example, one could have an exact sequence of vector spaces and linear maps, or of modules and module homomorphisms. More generally, the notion of an exact sequence makes sense in

any category with kernels and cokernels**.**

6.7.1 Simple Cases

To understand the definition, it is helpful to consider relatively simple cases where the sequence is finite and begins or ends with the trivial group. Traditionally, this, along with the single identity element, is denoted 0 (additive notation, usually when the groups are abelian), or denoted 1 (multiplicative notation).

- The sequence $0 \to A \to B$ is exact at A if and only if the map from A to B has kernel {0}; i.e., if and only if that map is a monomorphism (injective, or one-to-one).
- Dually, the sequence $B \to C \to 0$ is exact at C if and only if the image of the map from B to C is all of C; i.e., if and only if that map is an epimorphism (surjective, or onto).
- Therefore, the sequence $0 \to X \to Y \to 0$ is exact if and only if the map from X to Y is both a monomorphism and epimorphism (that is, a bimorphism), and thus, in many cases, an isomorphism from X to Y.

6.7.2 Short Exact Sequence

Important are **short exact sequences**, which are exact sequences of the form

As established above, for any such short exact sequence, f is a monomorphism and g is an epimorphism. Furthermore, the image of f is equal to the kernel of g. It is helpful to think of A as a subobject of B with f embedding A into B, and of C as the corresponding factor object (or quotient), B/A, with g inducing an isomorphismis called **split** if there exists a homomorphism $h : C \to B$ such that the composition $g \circ h$ is the identity map on C. It follows that if these are abelian groups, B is isomorphic to the direct sum of A and C (see Splitting lemma):

6.7.3 Long Exact Sequence

A **long exact sequence** is an exact sequence consisting of more than three nonzero terms, often an infinite exact sequence.

A long exact sequenceis equivalent to a sequence of short exact

sequences .

6.7.4 Examples Integers Modulo Two

Consider the following sequence of abelian groups:

The first homomorphism maps each element i in the set of integers **Z** to the element 2i in **Z**. The second homomorphism maps each element i in **Z** to an element j in the quotient group, i.e., j = i mod 2. Here the hook indicates that the map 2× from **Z** to **Z** is a monomorphism, and the two-headed arrow indicates an epimorphism (the map mod 2). This is an exact sequence because the image 2**Z** of the monomorphism is the kernel of the epimorphism. Essentially "the same" sequence can also be written as

In this case the monomorphism is 2n ↦ 2n and although it looks like an identity function, it is not onto (i.e. not an epimorphism) because the odd numbers don't belong to 2**Z**. The image of 2**Z** through this monomorphism is however exactly the same subset of **Z** as the image of **Z** through n ↦ 2n used in the previous sequence. This latter sequence does differ in the concrete nature of its first object from the previous one as 2**Z** is not the same set as **Z** even though the two are isomorphic as groups.

The first sequence may also be written without using special symbols for monomorphism and epimorphism:

Here 0 denotes the trivial group, the map from **Z** to **Z** is multiplication by 2, and the map from **Z** to the factor group **Z**/2**Z** is given by reducing integers modulo 2. This is indeed an exact sequence:

The image of the map 0 → **Z** is {0}, and the kernel of multiplication by 2 is also {0}, so the sequence is exact at the first **Z**.

The image of multiplication by 2 is 2**Z**, and the kernel of reducing modulo 2 is also 2**Z**, so the sequence is exact at the second **Z**.

The image of reducing modulo 2 is **Z**/2**Z**, and the kernel of the zero map is also **Z**/2**Z**, so the sequence is exact at the position **Z**/2**Z**.

The first and third sequences are somewhat of a special case owing to the infinite nature of **Z**. It is not possible for a finite group to be mapped by inclusion (i.e. by a monomorphism) as a proper subgroup of itself.

Instead the sequence that emerges from the first isomorphism theorem iswhere is the dihedral group of order 2n, which is a non-abelian group.

6.7.5 Intersection And Sum Of Modules

Let I and J be two ideals of a ring R. Thenis an exact sequence of R-modules, where the module homomorphism maps each element x of to the element of the direct sum , and the homomorphsim maps each element These homomorphisms are restrictions of similarly defined homomorphisms that form the short exact sequencePassing to quotient modules yield another exact sequence.

6.7.6 Grad, Curl And Divergent In Differential Geometry

Another example, from differential geometry, especially relevant for work on the Maxwell equations, isare the domains for the curl and div operators respectively.This is based on the fact that on properly defined Hilbert spaces, one hasand, in addition, curl-free vector fields can always be written as a gradient of a scalar function (as soon as the space is assumed to be simply connected, see **Note 1** below), and that a divergenceless field can be written as a curl of another field.[1]

This example makes use of the fact that 3-dimensional space is topologically trivial.

Properties

The splitting lemma states that if the short exact sequence

admits a morphism t : B → A such that t ∘ f is the identity on A or a morphism u: C → B such that g ∘ u is the identity on C, then B is a direct sum of A and C (for non-commutative groups, this is a semidirect product). One says that such a short exact sequence splits.

The snake lemma shows how a commutative diagram with two exact rows gives rise to a longer exact sequence. The nine lemma is a special case.

The five lemma gives conditions under which the middle map in a commutative diagram with exact rows of length 5 is an isomorphism; the short five lemma is a special case thereof applying to short exact sequences.

The importance of short exact sequences is underlined by the fact that every exact sequence results from "weaving together" several overlapping short exact sequences. Consider for instance the exact sequencewhich implies that there exist objects C in the category such that. Suppose in addition that the cokernel of each morphism exists, and is isomorphic to the image of the next morphism in the sequence:

(This is true for a number of interesting categories, including any abelian category such as the abelian groups; but it is not true for all categories that allow exact sequences, and in particular is not true for the category of groups, in which coker(f) : G → H is not H/im(f) but the quotient of H by the conjugate closure of im(f).) Then we obtain a commutative diagram in which all the diagonals are short exact sequences:

6.8 LET US SUM UP

We study in this unit four leema and five lemma with its example. We study Chasing Diagram and its properties. We study intersection and sum of module.We study ring lemma and ring lemma in three dimonsions. We study simple case. We study ring lemma in three dimension. We study short exact sequence and long exact sequence. We study lemma for the lower bound.

1. A commutative diagram in a category *C* can be interpreted as a functor from an index category *J* to *C;* one calls the functor a diagram.
2. An exact sequence is a sequence, either finite or infinite, of objects and morphisms between them such that the image of one morphism equals the kernel of the next.

3. A short exact sequence is a finite sequence of objects and morphisms between them such that the image of one morphism equals the kernel of the next.
4. A long exact sequence is an infinite sequence of objects and morphisms between them such that the image of one morphism equals the kernel of the next.
5. The splitting lemma states that if the short exact sequence admits a morphism t : B → A such that t ∘ f is the identity on A or a morphism u: C → B such that g ∘ u is the identity on C, then B is a direct sum of A and C

6.9 KEYWORD

Chasing : Drive or cause to go in a specified direction

Commutative :relating to or involving substitution or exchange

Diagram: A diagram is a simple drawing which consists mainly of lines and is used

Homological : Having the same or a similar relation; corresponding, as in relative position or structure

6.10 QUESTIONS FOR REVIEW

Q. 1 . For an R-module M, we have the following statements. (a) If 2 ∈/ S, then ΓSˆ(R(+)M) = ⊕|M| 2 ΓS(R). (b) If 2 ∈ S, then ΓSˆ(R(+)M) = ⊕|M| 2 ΓS(R) ⊕ (⊕|S|K|M|).

Q. 2 The following statements hold.

(a) gr(ΓS(R)) ≤ gr(ΓS˜(R/I));

(b) diam(ΓS˜(R/I)) ≤ diam(ΓS(R));

(c) If ΓS˜(R/I) is a complete graph, then diam(ΓS(R)) ≤ 2; and,

(d) If ΓS˜(R/I) is not a complete graph, then diam(ΓS˜(R/I)) = diam(ΓS(R)).

Q. 3 Let R be a commutative ring. Then the following statements hold.

(a) If $2x \notin S$ for some $x \in R$, then $x + I$ is a co-clique in $\Gamma S(R)$.

(b) If $2x \in S$ for some $x \in R$, then $x + I$ is a clique in $\Gamma S(R)$.

Q. 4 Let x and y be two elements of R. Then the following statements are equivalent:

(a) x is adjacent to y in $\Gamma S(R)$;

(b) $x + I$ is adjacent to $y + I$ in $\Gamma S\tilde{}(R/I)$;

(c) each element of $x + I$ is adjacent to each element of $y + I$ in $\Gamma S(R)$; and,

(d) there exist $x + i$ in $x + I$ and $y + i$ 0 in $y + I$ which are adjacent in $\Gamma S(R)$.

Q. 5 By using the above notation, $S\tilde{}$ is a saturated multiplicatively closed subset of R/I.

Q. 6 Suppose that S is an ideal of R with $|S| = \alpha$. Set $A := \{x+S : x \in R \setminus S \text{ and } 2x \in S\}$ and $B := \{x + S : x \in R \setminus S \text{ and } 2x 6\in S\}$. Then $\Gamma S(R)$ is the disjoint union of $|A| + 1$ times $K\alpha$ and $|B|/2$ times $K\alpha,\alpha$.

Q. 7 The graph $\Gamma S(R)$ is complete if and only if $S = R$ or char $R = 2$ and $S = R \setminus \{0\}$

6.11 ANSWER FOR CHECK IN PROGRESS

Check in Progress –I

Answer Q. 1 Check in section 2

Q. 2 Check in Section 1.2

Check in Progress –I

Answer Q. 1 Check in section 6

Q. 2 Check in Section 5

6.12 SUGGECTION READING AND REFERENCES

Notes

- *Adámek, Jiří; Horst Herrlich; George E. Strecker (1990). Abstract and Concrete Categories (PDF). John Wiley & Sons. ISBN 0-471-60922-6.* Now available as free on-line edition (4.2MB PDF).
- *Barr, Michael; Wells, Charles (2002). Toposes, Triples and Theories (PDF). ISBN 0-387-96115-1.* Revised and corrected free online version of *Grundlehren der mathematischen Wissenschaften (278)* Springer-Verlag, 1983).
  - W. R. Scott: *Group Theory*, Prentice Hall, 1964.
  - *Massey, William S. (1991), A basic course in algebraic topology, Graduate texts in mathematics, **127** (3rd ed.), Springer, ISBN 978-0-387-97430-9*

[1] D. Aharonov, The sharp constant in the ring lemma, Complex Var. Theory Appl. 33 (1997), 27–31. [2] D. Aharonov and K. Stephenson, Geometric sequences of discs in the Apollonian packing, Algebra i Analiz 9 (1997), 104–140.

[3] , Geometric sequences of discs in the Apollonian packing, St. Petersburg Math. J. 9 (1998), 509–542.

[4] L. V. Ahlfors, Möbius transformations in several dimensions, Ordway Professorship Lectures in Mathematics, School of Mathematics, University of Minnesota, 1981, revised third printing.

[5] T. M. Apostol, Modular functions and Dirichlet series in number theory, second ed., Graduate Texts in Mathematics, vol. 41, SpringerVerlag, New York, 1990.

[6] W. S. Brown, The kiss precise, Amer. Math. Monthly 76 (1969), no. 6, 661–663.

[7] H. Fukagawa and D. Pedoe, Japanese temple geometry problems – San Gaku, Charles Babbage Research Centre, 1989.

[8] T. Gosset, The kiss precise, Nature 139 (1937), 62.

[9] R. L. Graham, J. C. Lagarias, C. L. Mallows, A. R. Wilks, and C. H. Yan, Apollonian circle packings: geometry and group theory – I. The Apollonian group, Discrete Comput. Geom. 34 (2005), 547–585.

[10] , Apollonian circle packings: geometry and group theory – II. Super-Apollonian group and integral packings, Discrete Comput. Geom. 35 (2006), 1–36.

[11] , Apollonian circle packings: geometry and group theory – III. Higher dimensions, Discrete Comput. Geom. 35 (2006), 37–72.

[12] L. J. Hansen, On the Rodin and Sullivan ring lemma, Complex Var. Theory Appl. 10 (1988), 23–30.

UNIT 7 - DIRECT SUM AND PRODUCT OF MODULE

STRUCTURE

7.0 OBJECTIVE

After study this unit we familiar with vector space and abelian group. Learn about two abelian group. Learn construction of two vector spaces.

We learn about direct product, vector product of vector space and learn binary relation.

7.1 INTRODUCTION: DIRECT SUM OF MODULES

In abstract algebra, the **direct sum** is a construction which combines several modules into a new, larger module. The direct sum of modules is the smallest module which contains the given modules as submodules with no "unnecessary" constraints, making it an example of a coproduct. Contrast with the direct product, which is the dual notion.

The most familiar examples of this construction occur when considering vector spaces (modules over a field) and abelian groups (modules over the ring **Z** of integers). The construction may also be extended to cover Banach spaces and Hilbert spaces.

7.1.1 Construction For Vector Spaces And Abelian Groups

We give the construction first in these two cases, under the assumption that we have only two objects. Then we generalise to an arbitrary family of arbitrary modules. The key elements of the general construction are more clearly identified by considering these two cases in depth.

7.1.2 Construction For Two Vector Spaces

Suppose V and W are vector spaces over the field K. The cartesian product $V \times W$ can be given the structure of a vector space over K (Halmos 1974, §18) by defining the operations componentwise:

- $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$
- $\alpha\,(v, w) = (\alpha\, v, \alpha\, w)$

for $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$, and $\alpha \in K$.

The resulting vector space is called the *direct sum* of V and W and is usually denoted by a plus symbol inside a circle:

> It is customary to write the elements of an ordered sum not as ordered pairs (v, w), but as a sum $v + w$.

The subspace $V \times \{0\}$ of $V \oplus W$ is isomorphic to V and is often identified with V; similarly for $\{0\} \times W$ and W. (See *internal direct sum* below.) With this identification, every element of $V \oplus W$ can be written in one and only one way as the sum of an element of V and an element of W. The dimension of $V \oplus W$ is equal to the sum of the dimensions of V and W. One elementary use is the reconstruction of a finite vector space from any subspace W and its orthogonal complement:This construction readily generalises to any finite number of vector spaces.

7.1.3 Construction For Two Abelian Groups

For abelian groups G and H which are written additively, the direct product of G and H is also called a direct. Thus the cartesian product $G \times H$ is equipped with the structure of an abelian group by defining the operations componentwise:

- $(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$

for g_1, g_2 in G, and h_1, h_2 in H.

Integral multiples are similarly defined componentwise by

- $n(g, h) = (ng, nh)$

for g in G, h in H, and n an integer. This parallels the extension of the scalar product of vector spaces to the direct sum above.

The resulting abelian group is called the *direct sum* of G and H and is usually denoted by a plus symbol inside a circle:

> It is customary to write the elements of an ordered sum not as ordered pairs (g, h), but as a sum $g + h$.

The subgroup $G \times \{0\}$ of $G \oplus H$ is isomorphic to G and is often identified with G; similarly for $\{0\} \times H$ and H. (See *internal direct sum* below.) With this identification, it is true that every element of $G \oplus H$ can be written in one and only one way as the sum of an element of G and an element of H. The rank of $G \oplus H$ is equal to the sum of the ranks of G and H.

This construction readily generalises to any finite number of abelian groups.

7.1.4 Construction For An Arbitrary Family Of Modules

One should notice a clear similarity between the definitions of the direct sum of two vector spaces and of two abelian groups. In fact, each is a special case of the construction of the direct sum of two modules. Additionally, by modifying the definition one can accommodate the direct sum of an infinite family of modules. The precise definition is as follows (Bourbaki 1989, §II.1.6).

Let R be a ring, and $\{M_i : i \in I\}$ a family of left R-modules indexed by the set I. The *direct sum* of $\{M_i\}$ is then defined to be the set of all sequences where for cofinitely many indices i. (The direct product is analogous but the indices do not need to cofinitely vanish.)

It can also be defined as functions α from I to the disjoint union of the modules M_i such that $\alpha(i) \in M_i$ for all $i \in I$ and $\alpha(i) = 0$ for cofinitely many indices i. These functions can equivalently be regarded as finitely supported sections of the fiber bundle over the index set I, with the fiber

over being .

This set inherits the module structure via component-wise addition and scalar multiplication. Explicitly, two such sequences (or functions) α and β can be added by writing for all i (note that this is again zero for all but finitely many indices), and such a function can be multiplied with an element r from R by defining for all i. In this way, the direct sum becomes a left R-module, and it is denoted

It is customary to write the sequence as a sum . Sometimes a primed summation is used to indicate that cofinitely many of the terms are zero.

7.1.5 Properties

- The direct sum is a submodule of the direct product of the modules M_i (Bourbaki 1989, §II.1.7). The direct product is the set of all functions α from I to the disjoint union of the modules M_i with $\alpha(i) \in M_i$, but not necessarily vanishing for all but finitely many i. If the index set I is finite, then the direct sum and the direct product are equal.
- Each of the modules M_i may be identified with the submodule of the direct sum consisting of those functions which vanish on all indices different from i. With these identifications, every element x of the direct sum can be written in one and only one way as a sum of finitely many elements from the modules M_i.
- If the M_i are actually vector spaces, then the dimension of the direct sum is equal to the sum of the dimensions of the M_i. The same is true for the rank of abelian groups and the length of modules.
- Every vector space over the field K is isomorphic to a direct sum of sufficiently many copies of K, so in a sense only these direct sums have to be considered. This is not true for modules over arbitrary rings.
- The tensor product distributes over direct sums in the following sense: if N is some right R-module, then the direct sum of the tensor products of N with M_i (which are abelian groups) is naturally isomorphic to the tensor product of N with the direct sum of the M_i.
- Direct sums are commutative and associative (up to isomorphism), meaning that it doesn't matter in which order one forms the direct sum.
- The group of R-linear homomorphisms from the direct sum to some left R-module L is naturally isomorphic to the direct product of the sets of R-linear homomorphisms from M_i to L:

Indeed, there is clearly a homomorphism τ from the left hand side to the right hand side, where $\tau(\theta)(i)$ is the R-linear homomorphism sending $x \in M_i$ to $\theta(x)$ (using the natural inclusion of M_i into the direct sum). The inverse of the homomorphism τ is defined byMifor any α in the direct sum of the modules M_i. The key point is that the definition of τ^{-1} makes sense because $\alpha(i)$ is zero for all but finitely many i, and so the sum is finite.

In particular, the dual vector space of a direct sum of vector spaces is isomorphic to the direct product of the duals of those spaces.

7.2 INTERNAL DIRECT SUM

Suppose M is some R-module, and M_i is a submodule of M for every i in I. If every x in M can be written in one and only one way as a sum of finitely many elements of the M_i, then we say that M is the **internal direct sum** of the submodules M_i (Halmos 1974, §18). In this case, M is naturally isomorphic to the (external) direct sum of the M_i as defined above (Adamson 1972, p.61).

A submodule N of M is a **direct summand** of M if there exists some other submodule N' of M such that M is the *internal* direct sum of N and N'. In this case, N and N' are **complementary submodules**.

7.2.1 Universal Property

In the language of category theory, the direct sum is a coproduct and hence a colimit in the category of left R-modules, which means that it is characterized by the following universal property. For every i in I, consider the *natural embedding*which sends the elements of M_i to those functions which are zero for all arguments but i. If $f_i : M_i \to M$ are arbitrary R-linear maps for every i, then there exists precisely one R-linear map:

such that $f \circ j_i = f_i$ for all i.

7.2.2 Grothendieck Group

The direct sum gives a collection of objects the structure of a commutative monoid, in that the addition of objects is defined, but not subtraction. In fact, subtraction can be defined, and every commutative

monoid can be extended to an abelian group. This extension is known as the Grothendieck group. The extension is done by defining equivalence classes of pairs of objects, which allows certain pairs to be treated as inverses. The construction, detailed in the article on the Grothendieck group, is "universal", in that it has the universal property of being unique, and homomorphic to any other embedding of an abelian monoid in an abelian group.

7.3 DIRECT SUM OF MODULES WITH ADDITIONAL STRUCTURE

If the modules we are considering carry some additional structure (e.g. a norm or an inner product), then the direct sum of the modules can often be made to carry this additional structure, as well. In this case, we obtain the coproduct in the appropriate category of all objects carrying the additional structure. Two prominent examples occur for Banach spaces and Hilbert spaces.

In some classical texts, the notion of direct sum of algebras over a field is also introduced. This construction, however, does not provide a coproduct in the category of algebras, but a direct product (*see note below* and the remark on direct sums of rings).

7.3.1 Direct sum of algebras

A direct sum of algebras X and Y is the direct sum as vector spaces, with product

Consider these classical examples:

X is ring isomorphic to split-complex numbers, also used in interval analysis.

Y is the algebra of tessarines introduced by James Cockle in 1848.

Z called the split-biquaternions, was introduced by William Kingdon Clifford in 1873.

Joseph Wedderburn exploited the concept of a direct sum of algebras in his classification of hypercomplex numbers. See his *Lectures on Matrices* (1934), page 151. Wedderburn makes clear the distinction between a direct sum and a direct product of algebras: For the direct sum

the field of scalars acts jointly on both parts: while for the direct product a scalar factor may be collected alternately with the parts, but not both:. Ian R. Porteous uses the three direct sums above, denoting them , as rings of scalars in his analysis of Clifford Algebras and the Classical Groups (1995).

The construction described above, as well as Wedderburn's use of the terms *direct sum* and *direct product* follow a different convention from the one in category theory. In categorical terms, Wedderburn's *direct sum* is a categorical product, whilst Wedderburn's *direct product* is a coproduct (or categorical sum), which (for commutative algebras) actually corresponds to the tensor product of algebras.

7.3.2 Composition Algebras

A composition algebra (A, *, n) is an algebra over a field A, an involution * and a "norm" $n(x) = x\,x^*$. Any field K gives rise to a series of composition algebras beginning with K, and the trivial involution, so that $n(x) = x^2$. The inductive step in the series involves

forming the direct sum $A \oplus A$ and using the new involution

Leonard Dickson developed this construction
doubling quaternions for Cayley numbers, and the doubling method involving the direct sum $A \oplus A$ is called the Cayley–Dickson construction. In the instance beginning with $K = \mathbb{R}$, the series generates complex numbers, quaternions, octonions, and sedenions. Beginning with $K = \mathbb{C}$ and the norm $n(z) = z^2$, the series continues with bicomplex numbers, biquaternions, and bioctonions.

Max Zorn realized that the classical Cayley–Dickson construction missed constructing some composition algebras that arise as real subalgebras in the $(\mathbb{C}, z^2)$ series, in particular the split-octonions. A modified Cayley–Dickson construction, still based on use of the direct sum $A \oplus A$ of a base algebra A, has since been used to exhibit the series $\mathbb{R}$, split-complex numbers, split-quaternions, and split-octonions.

7.3.3 Direct sum of Banach Spaces

The direct sum of two Banach spaces X and Y is the direct sum of X and Y considered as vector spaces, with the norm $\|(x,y)\| = \|x\|_X + \|y\|_Y$ for all x in X and y in Y.

Generally, if X_i is a collection of Banach spaces, where i traverses the index set I, then the direct sum $\oplus_{i\in I} X_i$ is a module consisting of all functions x defined over I such that $x(i) \in X_i$ for all $i \in I$ and

The norm is given by the sum above. The direct sum with this norm is again a Banach space.

For example, if we take the index set $I = \mathbf{N}$ and $X_i = \mathbf{R}$, then the direct sum $\oplus_{i\in\mathbf{N}} X_i$ is the space l_1, which consists of all the sequences (a_i) of reals with finite norm $\|a\| = \sum_i |a_i|$.

A closed subspace A of a Banach space X is **complemented** if there is another closed subspace B of X such that X is equal to the internal direct sum . Note that not every closed subspace is complemented.

7.4 DIRECT SUM OF MODULES WITH BILINEAR FORMS

Let $\{(M_i,b_i) : i \in I\}$ be a family indexed by I of modules equipped with bilinear forms. The **orthogonal direct sum** is the module direct sum with bilinear form B defined by in which the summation makes sense even for infinite index sets I because only finitely many of the terms are non-zero.

Direct sum of Hilbert spaces

Further information: Positive-definite kernel § Connection with reproducing kernel Hilbert spaces and feature maps

If finitely many Hilbert spaces $H_1,...,H_n$ are given, one can construct their orthogonal direct sum as above (since they are vector spaces), defining the inner product as:

The resulting direct sum is a Hilbert space which contains the given Hilbert spaces as mutually orthogonal subspaces.

If infinitely many Hilbert spaces H_i for i in I are given, we can carry out the same construction; notice that when defining the inner product, only finitely many summands will be non-zero. However, the result will only be an inner product space and it will not necessarily be complete. We then define the direct sum of the Hilbert spaces H_i to be the completion of this inner product space.

Alternatively and equivalently, one can define the direct sum of the Hilbert spaces H_i as the space of all functions α with domain I, such that $\alpha(i)$ is an element of H_i for every i in I and:

The inner product of two such function α and β is then defined as:

This space is complete and we get a Hilbert space.

For example, if we take the index set $I = \mathbf{N}$ and $X_i = \mathbf{R}$, then the direct sum $\bigoplus_{i\in\mathbf{N}} X_i$ is the space l_2, which consists of all the sequences (a_i) of reals with finite norm . Comparing this with the example for Banach spaces, we see that the Banach space direct sum and the Hilbert space direct sum are not necessarily the same. But if there are only finitely many summands, then the Banach space direct sum is isomorphic to the Hilbert space direct sum, although the norm will be different.

Every Hilbert space is isomorphic to a direct sum of sufficiently many copies of the base field (either **R** or **C**). This is equivalent to the assertion that every Hilbert space has an orthonormal basis. More generally, every closed subspace of a Hilbert space is complemented: it admits an orthogonal complement. Conversely, the Lindenstrauss–Tzafriri theorem asserts that if every closed subspace of a Banach space is complemented, then the Banach space is isomorphic (topologically) to a Hilbert space.

Check In Progress-I

Q. 1 Define composition algebra.

Solution

……

……

…….

…….

.

Q. 2 Define direct sum.

Solution

……

…….

…….

…….

7.5 DIRECT PRODUCT

In mathematics, one can often define a **direct product** of objects already known, giving a new one. This generalizes the Cartesian product of the underlying sets, together with a suitably defined structure on the product set. More abstractly, one talks about the product in category theory, which formalizes these notions.

Examples are the product of sets (see Cartesian product), groups (described below), the product of rings and of other algebraic structures. The product of topological spaces is another instance.

There is also the direct sum – in some areas this is used interchangeably, while in others it is a different concept.

The problems concerning direct products of projective modules, to which we now turn, are more difficult. We shall consider a more general situation, which leads us to a rather ambitious generalization of the theorem of Baer mentioned in the introduction. We shall show, roughly speaking, that if the direct product of a "large" number of copies of a ring £ can be embedded in a certain way in a direct sum of left £-modules, each of which is generated by a "small" number of elements, then £ must satisfy the descending chain condition on principal right ideals. First we introduce several concepts which will be needed in the proof of the main result.

Definition. Let £ be a ring, A be a left £-module, and A' be a submodule of A. A' will be called a pure submodule of A if A'(~\aA =aA' for all d££.

Definition . Let £ be a ring, and A be a left £-module. Let {Cß} be a family of left £-modules (where ß traces some index set) and let fß £Homje(j4, Cß). The family {fß} will be called aí>-family of homomorphisms if the following conditions are satisfied for any X9^0 in A :

(a) fß(x) =0 for almost all ß.

(b) fß(x) 9¿0 for some ß.

Definition Let £ be a ring, and 7 be a left or right ideal in £. 7 will be called left T-nilpotent ii, for any sequence di, a2, ■ • • of elements of 7, there exists « > 0 such that did2 • • • an = 0 (right £-nilpotence requires that anan-i • • • di = 0 for some «).

Examples

- If we think of R as the set of real numbers, then the direct product R x R is just the Cartesian product RxR.
- If we think of R as the group of real numbers under addition, then the direct product RxR still has { (x, y | x, y € R)} as its underlying set. The difference between this and the preceding example is that R x R is now a group, and so we have to also say how to add their

  elements. This is done by defining .
- If we think of R as the ring of real numbers, then the direct product { (x, y | x, y € R)} again has { (x, y | x, y € R)} as its underlying set. The ring structure ring consists of addition defined by (a , b) + (c , d) = (a + c, b + d) and multiplication defined by (a, b)(c, d) = (ac, bd).
- However, if we think of R x R as the field of real numbers, then the direct product R R does not exist – naively defining addition and multiplication componentwise as in the above example would not

result in a field since the element R x R x R x R ……. does not have a multiplicative inverse.

In a similar manner, we can talk about the direct product of finitely many algebraic structures, e.g. R x R x R x R ……. . This relies on the fact that the direct product is associative up to isomorphism. That is, R x R for any algebraic structures R x Rx R x R x R of the same kind. The direct sum is also commutative up to isomorphism, i.e. A x B ≅ BxA for any algebraic structures A and B of the same kind. We can even talk about the direct product of infinitely many algebraic structures; for example we can take the direct product of countably many copies of , which we write as R x R x R x R ……. .

7.5.1 Group Direct Product

In group theory one can define the direct product of two groups $(G, \circ)$ and $(H, \cdot)$, denoted by $G \times H$. For abelian groups which are written additively, it may also be called the direct sum of two groups, denoted

by .

It is defined as follows:

- the set of the elements of the new group is the *Cartesian product* of the sets of elements of G and H, that is $\{(g, h): g \in G, h \in H\}$;
- on these elements put an operation, defined element-wise:

$$(g, h) \times (g', h') = (g \circ g', h \cdot h')$$

(Note that $(G, \circ)$ may be the same as $(H, \cdot)$)

This construction gives a new group. It has a normal subgroup isomorphic to G (given by the elements of the form $(g, 1)$), and one isomorphic to H (comprising the elements $(1, h)$).

The reverse also holds, there is the following recognition theorem: If a group K contains two normal subgroups G and H, such that $K = GH$ and the intersection of G and H contains only the identity, then K is isomorphic to $G \times H$. A relaxation of these conditions, requiring only one subgroup to be normal, gives the semidirect product.

As an example, take as G and H two copies of the unique (up to isomorphisms) group of order 2, C_2: say $\{1, a\}$ and $\{1, b\}$. Then $C_2 \times C_2 = \{(1,1), (1,b), (a,1), (a,b)\}$, with the operation element by element. For instance, $(1,b)*(a,1) = (1*a, b*1) = (a,b)$, and $(1,b)*(1,b) = (1,b^2) = (1,1)$.

With a direct product, we get some natural group homomorphisms for free: the projection maps define bycalled the **coordinate functions**.

Also, every homomorphism f to the direct product is totally determined by its component functions .

For any group $(G, \circ)$ and any integer $n \geq 0$, repeated application of the direct product gives the group of all n-tuples G^n (for $n = 0$ we get the trivial group), for example $\mathbf{Z}^n$ and $\mathbf{R}^n$.

7.5.2 Direct Product of Modules

The direct product for modules (not to be confused with the tensor product) is very similar to the one defined for groups above, using the Cartesian product with the operation of addition being componentwise, and the scalar multiplication just distributing over all the components. Starting from $\mathbf{R}$ we get Euclidean space $\mathbf{R}^n$, the prototypical example of a real n-dimensional vector space. The direct product of $\mathbf{R}^m$ and $\mathbf{R}^n$ is $\mathbf{R}^{m+n}$.

Note that a direct product for a finite index is identical to the direct

sum . The direct sum and direct product differ only for infinite indices,where the elements of a direct sum are zero for all but for a finite number of entries. They are dual in the sense of category theory: the direct sum is the coproduct, while the direct product is the product.

For example, consider ,the infinite direct product and direct sum of the real numbers. Only sequences with a finite number of non-zero elements are in Y. For example, (1,0,0,0,...) is in Y but (1,1,1,1,...) is not. Both of these sequences are in the direct product X; in fact, Y is a proper subset of X (that is, $Y \subset X$).

Check in Progress-II

Q. 1 Define direct product of module.

Solution

……

……

……

……

Q. 2 Define Direct product.

Solution

……

……

……

……

7.6 TOPOLOGICAL SPACE DIRECT PRODUCT

The direct product for a collection of topological spaces X_i for i in I, some index set, once again makes use of the Cartesian product

Defining the topology is a little tricky. For finitely many factors, this is the obvious and natural thing to do: simply take as a basis of open sets to be the collection of all Cartesian products of open subsets from each factor:

This topology is called the product topology. For example, directly defining the product topology on $\mathbf{R}^2$ by the open sets of **R** (disjoint unions of open intervals), the basis for this topology would consist of all disjoint unions of open rectangles in the plane (as it turns out, it coincides with the usual metric topology).

The product topology for infinite products has a twist, and this has to do with being able to make all the projection maps continuous and to make all functions into the product continuous if and only if all its component functions are continuous (i.e. to satisfy the categorical definition of product: the morphisms here are continuous functions): we take as a

basis of open sets to be the collection of all Cartesian products of open subsets from each factor, as before, with the proviso that all but finitely many of the open subsets are the entire factor:

The more natural-sounding topology would be, in this case, to take products of infinitely many open subsets as before, and this does yield a somewhat interesting topology, the box topology. However it is not too difficult to find an example of bunch of continuous component functions whose product function is not continuous (see the separate entry box topology for an example and more). The problem which makes the twist necessary is ultimately rooted in the fact that the intersection of open sets is only guaranteed to be open for finitely many sets in the definition of topology.

Products (with the product topology) are nice with respect to preserving properties of their factors; for example, the product of Hausdorff spaces is Hausdorff; the product of connected spaces is connected, and the product of compact spaces is compact. That last one, called Tychonoff's theorem, is yet another equivalence to the axiom of choice.

For more properties and equivalent formulations, see the separate entry product topology.

7.7 DIRECT PRODUCT OF BINARY RELATIONS

On the Cartesian product of two sets with binary relations R and S, define $(a, b)\mathrm{T}(c, d)$ as $a\mathrm{R}c$ and $b\mathrm{S}d$. If R and S are both reflexive, irreflexive, transitive, symmetric, or antisymmetric, then T will be also.[3] Combining properties it follows that this also applies for being a preorder and being an equivalence relation. However if R and S are total relations, T is in not general total.

Direct product in universal algebra

If Σ is a fixed signature, I is an arbitrary (possibly infinite) index set, and $(\mathbf{A}_i)_{i\in I}$ is an indexed family of Σ algebras, the **direct product** $\mathbf{A} = \prod_{i\in I} \mathbf{A}_i$ is a Σ algebra defined as follows:

1. The universe set A of $\mathbf{A}$ is the Cartesian product of the universe sets A_i of $\mathbf{A}_i$, formally: $A = \prod_{i \in I} A_i$;
2. For each n and each n-ary operation symbol $f \in \Sigma$, its interpretation $f^{\mathbf{A}}$ in $\mathbf{A}$ is defined componentwise, formally: for all $a_1, \ldots, a_n \in A$ and each $i \in I$, the ith component of $f^{\mathbf{A}}(a_1, \ldots, a_n)$ is defined as ${f^{\mathbf{A}}}_i(a_1(i), \ldots, a_n(i))$.

For each $i \in I$, the ith projection $\pi_i : A \to A_i$ is defined by $\pi_i(a) = a(i)$. It is a surjective homomorphism between the Σ algebras $\mathbf{A}$ and $\mathbf{A}_i$.

As a special case, if the index set $I = \{ 1, 2 \}$, the direct product of two Σ algebras $\mathbf{A}_1$ and $\mathbf{A}_2$ is obtained, written as $\mathbf{A} = \mathbf{A}_1 \times \mathbf{A}_2$. If Σ just contains one binary operation f, the above definition of the direct product of groups is obtained, using the notation $A_1 = G$, $A_2 = H$, ${f^{\mathbf{A}}}_1 = \circ$, ${f^{\mathbf{A}}}_2 = \cdot$, and $f^{\mathbf{A}} = \times$. Similarly, the definition of the direct product of modules is subsumed here.

7.8 CATEGORICAL PRODUCT

The direct product can be abstracted to an arbitrary category. In a general category, given a collection of objects A_i *and* a collection of morphisms p_i from A with i ranging in some index set I, an object A is said to be a **categorical product** in the category if, for any object B and any collection of morphisms f_i from B to A_i, there exists a unique morphism f from B to A such that $f_i = p_i f$ and this object A is unique. This not only works for two factors, but arbitrarily (even infinitely) many.

For groups we similarly define the direct product of a more general, arbitrary collection of groups G_i for i in I, I an index set. Denoting the Cartesian product of the groups by G we define multiplication on G with the operation of componentwise multiplication; and corresponding to the p_i in the definition above are the projection maps

7.9 INTERNAL AND EXTERNAL DIRECT PRODUCT

Some authors draw a distinction between an **internal direct product** and an **external direct product.** If then we say that X is an *internal* direct

product of *A* and *B*, while if *A* and *B* are not subobjects then we say that this is an *external* direct product.

7.10 METRIC AND NORM

A metric on a Cartesian product of metric spaces, and a norm on a direct product of normed vector spaces, can be defined in various ways, see for example p-norm.

Definition .1. Let {Mi }i∈I be a family of left R-modules. The direct product of {Mi }i∈I is the cartesian product: Q i∈IMi = {(ai)i∈I | ai∈Mi for all i∈ I } in which (ai)i∈I = (bi)i∈I if and only if ai = bi for all i∈ I.

Proposition 2. Let {Mi }i∈I be a family of left R-modules.

(1) Define addition on Q i∈IMi as follows:
(2) (ai)i∈I + (bi)i∈I = (ai +bi)i∈I , for all (ai)i∈I , (bi)i∈I∈ Q i∈IMi .
Then (Qi∈IMi ,+) is an abelian group.

(2) Q i∈IMi is a left R-module. Proof. (1)Exercise.

(2) Define • : R × Q i∈IMi → Q i∈IMi by r • (ai)i∈I = (r ai)i∈I , for all r ∈ R and for all (ai)i∈I∈ Q i∈IMi . Then • is a module multiplication, since for all r,s∈ R and for all (ai)i∈I , (bi)i∈I∈ Q i∈IMi we have that r •((ai)i∈I + (bi)i∈I) = r •((ai +bi)i∈I) = (r (ai +bi))i∈I = (r ai +r bi)i∈I = (r ai)i∈I + (r bi)i∈I = r • (ai)i∈I + r • (bi)i∈I and (r +s) • (ai)i∈I = ((r +s)ai)i∈I = (r ai +s ai)i∈I = (r ai)i∈I + (s ai)i∈I = r • (ai)i∈I +s • (ai)i∈I . Also, (r s)•(ai)i∈I = ((r s)ai)i∈I = (r (s ai))i∈I = r •(s ai)i∈I = r •(s •(ai)i∈I). Thus • is a module multiplication and hence Q i∈IMi is a left R-module.

Definition. Let {Mi }i∈I be a family of left R-modules. The external direct sum of {Mi }i∈I is denoted by ` i∈IMi and defined as follows: ` i∈IMi = {(xi)i∈I∈ Q i∈IMi | xi = 0Mi for all i but finite many i∈ I }.

Theorem 2.1. For any ring R the following statements are equivalent:

(a) The direct product of any family of flat right R-modules is flat.

(b) £Ae direct product of any family of copies of R is flat as a right Rmodule.

(c) A ny finitely generated submodule of a free left R-module is finitely related.

(d) Any finitely generated left ideal in R is finitely related.

Proof. (a)=>(b): Trivial, since £ is a flat right £-module.

(b)=>(c) : Let G be a free left £-module, and £ be a finitely generated submodule of G. Clearly we may assume that G is finitely generated; hence, for some integer 5>0, we may identify G with the left £-module of all 5-tuples (Xi, • • • , X,) of elements of £. Let Ui, • • • , ur generate L, where uk = (Xjti, • • • , X*,)- Let £ be a free left £-module with basis Xi, • • • , xT, and define an epimorphism /: £—>£ by f(xk)=uk. Set £ = ker(/), and for each a££ let RM be a copy of £. Define A = ITasx£(a), which we shall view as a right £-module. If a = di(a)xi-f- • • • +ar(a)xr is in K, then di(a)7ii+ • • ■ +ar(a)ur=f(a)=0, and so 2~ll~i d*(a)X*y = 0 for all j^s. Thus, setting d* = {dt(a)} £.4 for k = 1, • • • , r, we get that 2~Ll-i ak\kj = 0 for j — s.

By **hypothesis**, A is a flat right £-module; hence there exist h, • • • , b,,EA and {pik}ç.R (i^n, k^r) satisfying the conditions of Set Zi= 2^.1-1 PikXkEF for 7^»; then f(z/) = X*-i M.*"* = 0, since 2~lt-i /»«X*y = 0 for all j = s.

Hence Zi, • • • ,zn££. Write £><={¿»¿(a)}, where ¿>(d): Trivial

(d)=>(b): Let {£(a)} be any family of copies of £, and A = JJ« RM> which we shall view as a right £-module. Suppose that diXi+ • • • +drXr = 0, where a*= {ak(ct)} EA and Xt££, k = r. Let 7 be the left ideal in £ generated by Xi, • ■ • ,Xr, £ be a free left £-module with basis xi, • • ■ , xr, and /: £—>7 be the epimorphism defined hyf(xk) =X*. Let £ be the kernel of/; by hypothesis, K is finitely generated. Let z\, ■ • ■ , z,, be a set of generators of £, and write z,= ^¡b-iMi***- Setting u(a) =ai(a)xi+ • • • +ar(ct)xT, we have that f(u(a))=ai(a)\i+ • ■ ■ +dr(a)Xr = 0, and so there exist 6.

(c)=*(a):Let {Aa} beafamily of flat right £-modules, and set A = lL,^«. Define a functor F from the category of left £-modules to the category of abelian groups by V(C) = lT,, (Aa®iiC). It is well-known that F is additive and exact [3, p. 31, Exercise 2]. Define a natural transformation t:A®R(-) -*V(-) as follows: If C is a left £-module, then tc: A®BC-+V(C) is defined by tc({aa}®c) = {aa®c}, where cQC and {aa}£.4. Now let 0—»£—>£—»C—»0 be an exact sequence of left £-modules, where C is finitely generated and £ is free of finite rank. We then get the following commutative diagram:

where the rows are exact. That V is additive, F(£) «.4, and £ is free of finite rank implies immediately that tf is an isomorphism. It then follows from routine diagram-chasing that tc is an epimorphism. Suppose now that K is also finitely generated; i.e., C is finitely related. Then, replacing C by K in the above argument, we obtain that ix is an epimorphism. Further diagram-chasing then shows that tc is an isomorphism. But since £ is a finitely generated submodule of a free left £-module, it follows from our hypotheses that K is finitely related; hence tg. is an isomorphism, too. We may then conclude that the sequence 0—>A®rK—>A®rF -^A®rC—>0 is exact, and thus Torf(.á, C)=0.

Now let C be any finitely generated left £-module, and 0—*£—>£—>C—*0 he an exact sequence, where £ is free of finite rank. The family {£$} of all finitely generated submodules of K form, in the obvious way, a directed system of which the direct limit is K. Then C is the direct limit of the induced directed system {Cß}, where Cß = F/Kß. We obtain from our previous remarks that Tor?C

Clearly every left Noetherian ring satisfies condition (d) of Theorem 2.1. Hence the theorem may be viewed as a generalization of , which states that the direct product of a family of flat right modules over a left Noetherian ring is again flat. Indeed, the final part of the proof given above follows to some extent the proof suggested in that exercise.

We shall now present a purely ideal-theoretic characterization of the class of rings described in Theorem 2.1. This characterization is based upon a result concerning residual division in commutative rings, which

was communicated to me by J. Eagon. We need first a couple of definitions and lemmas.

Lemma Let I = Rai+ • • • +Ran be a left ideal in a ring R, and let d££. Set J=I+Ra, and let F be a free left R-module with basis Xi, • • - , x„+i. Define a homomorphism f: F—+J by f(x/) = a< for i^n and f(xn+i) = a. Let K = ker(f), and set F' = Rxi+ ■ ■ ■ +RxnQF and £' = £H£'. Then there exists a homomorphism g: K—>(I: a) such that ker(g) =£'.

Proof. If uEK, write u=\iXi+ • • • +X„x„-r-Xuxn+i; then Xidi+ • • • +X„d„+Xud=/(«) = 0, and so X„£(7:a). Define g by g(u)=\u. Straightforward computations then complete the proof.

7.11 LET US SUM UP

We study in this unit about direct product of binary realation. We study norm and metric. We study category product. We study direct product in topological space. We study construction of finite and abelian group. We study direct sum of module and additional structure.

1. Suppose V and W are vector spaces over the field K. The cartesian product $V \times W$ can be given the structure of a vector space over K (Halmos 1974, §18) by defining the operations component wise:

   $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$

   $\alpha (v, w) = (\alpha v, \alpha w)$ for $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$, and $\alpha \in K$.

2. For abelian groups G and H which are written additively, the direct product of G and H is also called a direct. Thus the cartesian product $G \times H$ is equipped with the structure of an abelian group by defining the operations componentwise:

   $(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$

   for g_1, g_2 in G, and h_1, h_2 in H.

3. The direct sum gives a collection of objects the structure of a commutative monoid, in that the addition of objects is defined, but not subtraction. In fact, subtraction can be defined, and every commutative

monoid can be extended to an abelian group. This extension is known as the Grothendieck group.

4. The direct sum of two Banach spaces *X* and *Y* is the direct sum of *X* and *Y* considered as vector spaces, with the norm $||(x,y)|| = ||x||_X + ||y||_Y$ for all *x* in *X* and *y* in *Y*.
5. Let £ be a ring, A be a left £-module, and A' be a submodule of A. A' will be called a pure submodule of A if A'(~\aA =aA' for all d££.
6. Let {Mi }i∈I be a family of left R-modules. The direct product of {Mi }i∈I is the cartesian product: Q i∈IMi = {(ai)i∈I | ai∈Mi for all i∈ I } in which (ai)i∈I = (bi)i∈I if and only if ai = bi for all i∈ I.

7.12 KEYWORD

Banach Space: A *Banach space* is a vector *space* X over any scalar field K, which is equipped with a norm and which is complete with respect to the distance function induced by the norm.

Krull-Schmidt :A Krull–Schmidt category is a generalization of categories in which the Krull–Schmidt theorem holds. They arise, for example, in the study of finite-dimensional modules over an algebra.

Chasing :Drive or cause to go in a specified direction

7.13 QUESTIONS FOR REVIEW

Example1. Let R = Q i∈N F be a product of fields F and let Mi = FR. Then M = L i∈NMi is semisimple and E(M) = Q i∈N F, thus M is a quasi-injective R-module which is not injective.

Example 2.. Let R = F F 0 F with F a field. Then M = F F 0 0 is an injective R-module and N = 0 0 0 F is a quasi-injective R-module. However, M ⊕ N = R is not a quasi-injective R-module.

Example 3. Consider Zp and Zp2 , where p is a prime number. Each of these is a quasi-injective Z-module. However, Zp⊕Zp 2 is not a quasi-injective Z-module.

Example4 E = Ln i=1 Ei is injective iff each Ei is injective for $1 \leq i \leq n$.

Example 5 If M = L $\alpha \in I$ Mα is injective if and only if each Mα is injective and (A1) holds where I is an index.

Example.6 Let R be a ring which has only 3 right ideals but which is not left artinian. Then M = RR is continuous but not quasi-injective. Since if so, R will be right self-injective and hence quasi-Frobenius, a contradiction.

Example7Zp,Zp 3 are quasi-injective Z-modules, where p is a prime number; consequently, each of these modules is quasi-injective hence (quasi-)continuous, and so extending. However, Zp$\oplus$Zp 3 is not an extending Z-module.

Example8 Direct sums of extending modules are not extending in general:

(i) Let M = L∞ i=1 Z. Then M is not an extending Z-module, while the domain Z is uniform and hence extending;

(ii) Let R = Z[X]. Thus R is a commutative Noetherian domain (hence quasicontinuous), but R $\oplus$ R is not an extending R-module.

Example 9. Let M = L i$\in$IMi where I is an index set. If I is finite or R is right Noetherian, then M is continuous if and only if each Mi is continuous and Mj -injective for all j 6= i$\in$ I

Example 10. The Z-module Zpn$\oplus$ Zpn+1 is self-ojective but not self-injective

Example 11. Let M = M1 $\oplus \cdots \oplus$Mn, where the Mi are uniform. Then M is extending and the decomposition is exchangeable if and only if Mi is Mj -ojective for all i 6= j $\in$ I.

7.14 ANSWER FOR CHECK IN PROGRESS

Check in Progress-I

Answer Q. 1 Check in Section 1.6.2

Q. 2 Check in Section 1.1

Check in Progress-II

Answer Q. 1 Check in Section 2.1

Q. 2 Check in Section 2

7.15 SUGGESTION READING AND REFERENCES

- *Milnor, J.; Husemoller, D. (1973). Symmetric Bilinear Forms. Ergebnisse der Mathematik und ihrerGrenzgebiete. **73**. Springer-Verlag. pp. 4–5. ISBN 3-540-06009-X. Zbl 0292.10016.*
- *Iain T. Adamson (1972), Elementary rings and modules, University Mathematical Texts, Oliver and Boyd, ISBN 0-05-002192-3*
- *Bourbaki, Nicolas (1989), Elements of mathematics, Algebra I, Springer-Verlag, ISBN 3-540-64243-9.*
- *Dummit, David S.; Foote, Richard M. (1991), Abstract algebra, Englewood Cliffs, NJ: Prentice Hall, Inc., ISBN 0-13-004771-6.*
- *Halmos, Paul (1974), Finite dimensional vector spaces, Springer, ISBN 0-387-90093-4*
- *Mac Lane, S.; Birkhoff, G. (1999), Algebra, AMS Chelsea, ISBN 0-8218-1646-2.*
- *W., Weisstein, Eric. "Direct Product". mathworld.wolfram.com. Retrieved 2018-02-10.*
- ^ *W., Weisstein, Eric. "Group Direct Product". mathworld.wolfram.com. Retrieved 2018-02-10.*
- ^ Equivalence and Order
- ^ Stanley N. Burris and H.P. Sankappanavar, 1981. *A Course in Universal Algebra.* Springer-Verlag. ISBN 3-540-90578-2. Here: Def.7.8, p.53 (=p. 67 in pdf file)

- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR 1878556