Graduate Algebra

Or Dagmi - http://digmi.org

March 24, 2015

Lecture notes of the class of 2014. Dr. Josephine Shamash (josie.shamash@gmail.com)

Contents

Chapter 1

Introduction

11/03/2014

In this course we will mainly talk about non-commutative rings.
The assignments will be 25% of the final grade while the take home exam will be 75%.
Books:

1. Jakobson: Basic Alg II
2. Algebra: A gram algebra course: I.M Isaac.
3. S.Lang - Algebra.

Chapter 2

Modules

2.1 Definition

A module is an additive abelian group.

Definition 2.1.1 If R is a ring (we will always talk about rings with identity), M is a module over R or a **left R-module** if M is an additive abelian group and we have a map: $\begin{array}{c} R \times M \to M \\ (a, x) \mapsto a \cdot x \end{array}$ while $a \in R$ and $x \in M$ that satisfies the following:

1. $a\left(x+y\right) = ax + ay \qquad \forall a \in R,\ \forall x, y \in M$
2. $\left(a+b\right)x = ax + bx \qquad \forall a, b \in R,\ \forall x \in M$
3. $\left(a \cdot b\right)x = a\left(b \cdot x\right) \qquad \forall a, b \in R,\ \forall x \in M$
4. $1_R \cdot x = x \qquad \forall x \in M$

This definition seems very similar to a vector space, only instead of a field we have a ring, and that will be our first example:

Example 2.1.2 () $M = V_F =$ Vector space over a field F. $R = F$.
The operation of F on V is multiplication by scalars.

Just as we have left R-module we can have also a right R-module:

Definition 2.1.3 If R is a ring (always we are talking about a rings with identity), M is a **right R-module** if M is an additive abelian group and we have a map: $\begin{array}{c} M \times R \to M \\ (x, a) \mapsto x \cdot a \end{array}$ while $a \in R$ and $x \in M$ that satisfying the following:

1. $\left(x+y\right)a = xa + ya \qquad \forall a \in R,\ \forall x, y \in M$
2. $x\left(a+b\right) = xa + xb \qquad \forall a, b \in R,\ \forall x \in M$
3. $x\left(a \cdot b\right) = \left(x \cdot a\right)b \qquad \forall a, b \in R,\ \forall x \in M$
4. $x \cdot 1_R = x \qquad \forall x \in M$

One, at first glance, would expect the definitions to be the same, but that will not be true for non-commutative rings. For example the 3rd condition will have different results!

Example 2.1.4 () $M = V_F =$ vector space over a field F, $R =$ the ring of linear operators on V.
If $\varphi \in R$ then $\varphi\left(x+y\right) = \varphi\left(x\right) + \varphi\left(y\right)$, we can write this as a multiplication: $\varphi \cdot \left(x+y\right) = \varphi \cdot x + \varphi \cdot y$.
So M is a left module over R.

✎**Example 2.1.5 ()** If M is any additive abelian group, we can regard it as a $\mathbb{Z}$-module by defining:
For $n \in \mathbb{Z}$ while $n > 0$ we define: $n \cdot x = \underbrace{x + \ldots + x}_{n\text{times}}$ and then we can define $(-n) \cdot x = -(nx)$ and $0 \cdot x = 0$.

2.2 Homomorphisms of R-modules

Definition 2.2.1 (left R-module homomorphism) If M and N are both left R-modules, $\varphi : M \to N$ is a **left R-module homomorphism** if:

1. $\forall x, y \in M \quad \varphi(x+y) = \varphi(x) + \varphi(y)$ (φ is a module homomorphism).
2. $\forall x \in M, a \in R \qquad \varphi(ax) = a\varphi(x)$.

✎**Example 2.2.2 ()** If V, W are vector spaces over F, then V, W are an F-modules, and φ is an F-module homomorphism if and only if φ is a linear transformation.

Another way to look at the second condition is to say that the operations a and φ commute.

✎**Example 2.2.3 ()** If R is a ring then we can take $M = R^+ = \langle R, +, 0 \rangle$ (the additive group of R). Then, let R act on itself through left multiplication then R is a left R-module over itself denoted by ${}_R R$.
And also:
If R is a ring then we can take $M = R^+ = \langle R, +, 0 \rangle$ (the additive group of R). Then, let R act on itself through right multiplication then R is a right R-module over itself denoted by R_R.
This is called the **regular R-module**.

Special case: Division ring. A special case is when R is a division ring (A ring which every non-zero element has an inverse). Modules over division rings are more or less like vector spaces. All theorems on vector spaces that don't depend on commutativity and special field properties will hold. e.g. every module over a division ring has a basis (uses the axiom of choice). Also, we can define the notion of **dimension**.

The additive condition of homomorphism (the first) can be define for any group, not even a module. This will be a group homomorphism.

Definition 2.2.4 If M is a module, we define $\text{End}M = \{\varphi : M \to M \mid \varphi(x+y) = \varphi(x) + \varphi(y) \quad \forall x, y \in M\}$.

It's easy to show that: End$M$ is an additive group, and in fact is a ring with respect to composition and the identity map is the identity element of End$M$.

✎**Example 2.2.5 ()** M is an End$M$-module where $\varphi \cdot x$ is defined as $\varphi(x)$.
We have $\varphi(x+y) = \varphi(x) + \varphi(y)$ so: $\varphi(x+y) = \varphi x + \varphi y$. We have: $(\varphi + \psi) = \varphi x + \psi x$ (the addition in End$M$). $(\varphi\psi)(x) = \varphi(\psi x)$ and for last: $\text{Id}(x) = x$.

In some sense this is a general example as if M is a left R-module, each $a \in R$ defines an endomorphism of R as:

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

Get a map $f : R \to \text{End}M$, $a \in R$, $f(a)$ =endomorphism that a induces on M. i.e. $f(a)(x) = ax$.

In fact f will be a ring homomorphism so $f(R)$ is a subring of End$M$.

Theorem 2.2.6

If R is a ring, then R is isomorphic to some ring of the form End$M$ *for some module(=additive group) M.*

Proof: Take M to be $R^+ = \langle R, +, 0 \rangle$. Define $L : R \to \text{End}M$ to be left multiplication, i.e. $L(a) = a_L$ where $a_L(x) = ax$ with $a, x \in R$.

Clearly L is additive and multiplicative as e.g: $L(ab) = (ab)_L$ and

$$(ab)_L(x) = (ab) \cdot x \underbrace{=}_{\text{associativity in } R} a \cdot (bx) = a_L(b_L(x))$$

$L(1_R) = \mathrm{Id}$ in $\mathrm{End}M$ so $(ab)_L = a_L \cdot b_L$ (composition in $\mathrm{End}M$).

L is a $1-1$ as if $a_L = b_L$ then: $a \cdot 1 = a_L(1) = b_L(1) = b \cdot 1$ so $a = b$. $R \cong L(R) \subseteq \mathrm{End}M$. Meaning that $R \hookrightarrow \mathrm{End}M$. ■

Also, we call this image: R_L.

Remarks 2.2.7 If S is a ring and we have operation form S to $\mathrm{End}M$ $(M = S^+)$ defined by right multiplication: $a \in S$, $a \mapsto a_R$ where $a_R(x) = x \cdot a$.
Then: $a_R(x+y) = (x+y) \cdot a = xa + ya = a_R(x) + a_R(y)$ and $(a+b)_R x = x(a+b) = xa + xb = a_R(x) + b_R(x)$.
This gives an **antihomomorphism** of rings from $S \to \mathrm{End}M$ as: $(ab)_R(x) = x(ab) = b_R a_R(x)$ so: $(ab)_R = b_R a_R$
Meaning that antihomomorphism reverse the operation.

Definition 2.2.8 (Centralizer) In a ring S we define the **centralizer** of a subset $A \subseteq S$:

$$\mathrm{Cent}_S(A) = \{r \in S \mid \ ra = ar \ \forall a \in A\}$$

Theorem 2.2.9

(Assignment 1)
$S_L = \mathrm{Cent}_{\mathrm{End}M}(S_R)$ *and* $S_R = \mathrm{Cent}_{\mathrm{End}M}(S_L)$.

Remarks 2.2.10 $S_L = \{a_L \mid a \in S\}$ while $S_R = \{a_R \mid a \in S\}$ (multiplication form the left and multiplication from the right).

Definition 2.2.11 For a set A, $\mathrm{Sym}A$ =the group of all permutations on the element of A.

2.3 Representations of rings

Definition 2.3.1 Given a module M and a ring R, a ring homomorphism $\eta : R \to \mathrm{End}M$ is called a representation of R.

Given a left R-module M we saw already that the map $a \overset{\eta}{\mapsto} a_L$ is a ring homomorphism from R to $\mathrm{End}M$.

So any R-module gives rise to a representation η defined in this way.

Conversely, given any additive abelian group M and a representation $\eta : R \to \mathrm{End}M$ we can regard M as a left R-module via the representation η by defining for $a \in R, x \in M$:

$$a \cdot x = \eta(a)(x)$$

Meaning R-module $\iff$ Representation of R.

In particular: ${}_RR =$ "The regular module" which is R regarded as a left module over itself by left multiplication defines a representation we call **the regular representation of R**: ρ, $a \overset{\rho}{\mapsto} a_L$ for $a \in R$.

We defined a homomorphism of R-modules $\varphi : M \to N$, so now, we can do this inside M. In particular we can have an endomorphism $\varphi : M \to M$ of R-module M satisfying:

$$\begin{cases} \varphi(x+y) = \varphi(x) + \varphi(y) \\ \varphi(ax) = a\varphi(x) \end{cases}$$

We call this set $\mathrm{End}_R M$ and clearly: $\mathrm{End}_R M \subseteq \mathrm{End}M$.

In fact $\mathrm{End}_R M$ is a subring of $\mathrm{End}M$.

✎**Example 2.3.2 ()** V is a vector space over F i.e. an F-module $\mathrm{End}_F V$= the ring of linear operators on V.

25/03/2014

2.4 Submodules

Definition 2.4.1 An R-submodule $N \subseteq M$ is an additive subgroup of N s.t. $R \cdot N \subseteq N$.

Example 2.4.2 () Let V be a vector space over a field F. And let $T \in \text{End}_F V$ (linear operator on the vector space).
We can view V as an $F[x]$-module as follows:
$f(x) \in \mathbb{F}[x]$, $v \in V$:
So if $f(x) = \sum a_i x^i$ then:

$$f(x) \cdot v = f(T)(v) = a_0 v + a_1 T v + a_2 T^2 v + \ldots + a_n T^n v$$

What are the submodule of V?
W is a subspace which is T-invariant $\iff$ W is a $F[x]$-submodule.
More concretely: If we take $V = \mathbb{Q}^{(3)}$ and take $T \cdot v = \underbrace{\begin{pmatrix} 1 & 3 & 0 \\ 2 & -1 & 0 \\ 0 & 0 & 7 \end{pmatrix}}_{A} v$. For instance it is easy to see that the eigenspaces corresponding to A are T-invariant.
Take the char polynomial:

$$\begin{vmatrix} \lambda - 1 & -3 & 0 \\ -2 & \lambda + 1 & 0 \\ 0 & 0 & \lambda - 7 \end{vmatrix} = (\lambda - 7)\left[\left(\lambda^2 - 1\right) - 6\right] = (\lambda - 7)\left(\lambda^2 - 7\right)$$

We have three eigenspaces, one corresponding to the eigenvalue 7 and two corresponding to $\pm\sqrt{7}$. And so, the submodules of V as an $\underbrace{\mathbb{Q}[\pi]}_{\cong \mathbb{Q}[\pi]}$-module where π (the number) acts on v via the matrix A.

Remarks 2.4.3 If R is a ring, regarded as a left R-module. The Left ideals are the R-submodules.

2.4.1 Quotient modules

Definition 2.4.4 If N is a R-submodule of an R-module M, then we define ${}^{M}\!/\!_{N}$ =quotient of M by N as additive groups to be an R-module by defining for $x \in M$, $a \in R$:

$$a(N + x) = N + a \cdot x$$

Remarks 2.4.5 This is well-defined as if $N + x = N + x'$ then $x - x' \in N$. So $a(x - x') \in N$ So: $N + ax = N + ax'$.

2.5 Isomorphism Theorems

We will start with 2 isomorphism theorems for R-modules.

Theorem 2.5.1

Let M be an R-module.

1. *Let N_1 and N_2 be R-submodules of M. Then:*

$$y_1 + N_2 \overset{\varphi}{\mapsto} y_1 + N_1 \cap N_2,\ y_1 \in N_1$$

   Defines an isomorphism of: ${}^{N_1+N_2}\!/\!_{N_2}$ onto ${}^{N_1}\!/\!_{N_1 \cap N_2}$.

2. *If $P \subseteq N \subseteq M$ R-submodules. Then ${}^{N}\!/\!_{P}$ are R-submodules of ${}^{M}\!/\!_{P}$ and $(x + P) + {}^{N}\!/\!_{P} \mapsto x + N$ for $x \in M$ is an isomorphism: ${}^{({}^{M}/_{P})}\!/\!_{({}^{N}/_{P})}$ onto ${}^{M}\!/\!_{N}$.*

Remarks 2.5.2 The usual basic homomorphism theorem holds, i.e. if M, N are R-modules and $\varphi : M \to N$ an R-homomorphism then $\ker\varphi$ is an R-submodule and if φ is surjective then: ${}^{M}\!/_{\ker\varphi} \cong N$.

Proof: The proofs are straight-forward, We will only show that 1 is well-defined.
Suppose $y_1, y_1' \in N_1$ if:

$$y_1 + N_2 = y_1' + N_2$$

Then $y_1 - y_1' \in N_2$ but it is also an element of N_1 so $y_1 - y_1' \in N_1 \cap N_2$ and so: $y_1 + N_1 \cap N_2 = y_1' + N_1 \cap N_2$. ■

Remarks 2.5.3 Any additive group A can be regarded as a $\mathbb{Z}$-module. In that case the $\mathbb{Z}$-submodule are simply the subgroups of A .

2.6 Artinian & Noetherian modules

Definition 2.6.1 A module M is called **Noetherian** if it satisfies the "ascending chain condition" i.e. if every ascending chain of submodules stabilizes. i.e. if:

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$$

inside M then:

$$\exists k : \quad M_k = M_{k+1} = M_{k+2} = \ldots$$

Definition 2.6.2 A module M is called **Artinian** if it satisfies the "descending chain condition" i.e. if every descending chain of submodules stabilizes. i.e. if:

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \ldots$$

inside M then:

$$\exists k : \quad M_k = M_{k+1} = M_{k+2} = \ldots$$

Definition 2.6.3 A ring R is left-Noetherian if every ascending chain of left ideals stabilizes.

Definition 2.6.4 A ring R is left-Artinian if every ascending chain of left ideals stabilizes.

And of course we can talk about right-Noetherian and right-Artinian. The interesting part is that all these combination can happen, a ring can be left-Noetherian without being right-Noetherian.

✎**Example 2.6.5 ()** $\mathbb{Z}$ is Noetherian but not Artinian.
Note that:

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \ldots$$

Is an infinite descending chain.
On the other hand if we have increasing chain then:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq \mathbb{Z}$$

Then $I = \bigcup\limits_{j=1}^{\infty} I_j$ is an ideal in $\mathbb{Z}$ and so $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$ and so $\exists k$ where $n \in I_k$ so $I_k = I_{k+1} = \ldots = I$.

More generally we can say:

Claim 2.6.6

If R is a PID, then R is Noetherian.

Proof: The same proof as for $\mathbb{Z}$. ■

Example 2.6.7 () Let p be a fixed prime, Take a look at the following ring:

$$P = \left\{ \frac{m}{p^k} \mid m \in \mathbb{Z},\ k \in \mathbb{Z} \right\}$$

This is a subring of $\mathbb{Q}$ (regarded as a $\mathbb{Z}$-module) which is neither noetherian nor artinian!
$\mathbb{Z} \subseteq P$, so:

$$\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq \dots$$

This is an infinite descending chain of $\mathbb{Z}$-submodules in P.
But also, we can look at:

$$\mathbb{Z} \subseteq \frac{1}{p}\mathbb{Z} \subseteq \frac{1}{p^2}\mathbb{Z} \subseteq \dots$$

Is an infinite ascending chain.

Remarks 2.6.8 Any finite module will be both noetherian and artinian.

Remarks 2.6.9 A finite dimensional vector spaces over a field F is both noetherian and artinian as an F-module.

Remarks 2.6.10 A vector space of infinite dimensional over field F is neither noetherian nor artinian.

Theorem 2.6.11

If N is a submodule of a module M. Then if M is noetherian(/artinian) then so are N and ${}^{M}/_{N}$ and any homomorphic image of M.

We will prove for noetherian, for artinian the proof is the same. **Proof:** Clearly any chain of submodules of N is also a chain for M-so property holds.
Now, suppose we have a chain of submodules of ${}^{M}/_{N}$:

$$\overline{P_1} \subseteq \overline{P_2} \subseteq \overline{P_3} \subseteq \dots \subseteq {}^{M}/_{N}$$

By homomorphism theorems there are submodules $N \subseteq P_i \subseteq M$ s.t. $\overline{P_i} \subseteq {}^{P_i}/_{N}$. Moreover:

$$P_1 \subseteq P_2 \subseteq P_3 \subseteq \dots$$

So this chain stabilizes, so also $\overline{P_i}$. ■

Theorem 2.6.12 (*The converse*)

If M is a module, and N is a submodule s.t. N and ${}^{M}/_{N}$ both noetherian(/artinian) then so is M.

We will prove for noetherian, for artinian the proof is the same.

Proof: Suppose $P_1 \subseteq P_2 \subseteq P_3 \subseteq \dots$ an increasing chain of submodules in M then: $N \cap P_1 \subseteq N \cap P_2 \subseteq \dots$ is an increasing chain of submodules in N. and so it stabilizes so we have k such that:

$$N \cap P_k = N \cap P_{k+1} = \dots$$

Now, we also know that: ${}^{(N+P_1)}/_{N} \subseteq {}^{(N+P_2)}/_{N} \subseteq \dots$ is increasing chain of submodules in ${}^{M}/_{N}$ and so stabilizes, so we have l such that:

$${}^{(N+P_l)}/_{N} = {}^{(N+P_{l+1})}/_{N} = \dots$$

Let $r = \max\{k, l\}$. From the isomorphism theorem:

$$\begin{array}{ccc} {}^{(N+P_r)}/_{N} & \cong & {}^{P_r}/_{N\cap P_r} = {}^{P_r}/_{N\cap P_{r+1}} \\ || & & \\ {}^{(N+P_{r+1})}/_{N} & \cong & {}^{P_{r+1}}/_{N\cap P_{r+1}} \end{array}$$

Hence:

$${}^{P_r}/_{N\cap P_{r+1}} \cong {}^{P_{r+1}}/_{N\cap P_{r+1} \Rightarrow P_r = P_{r+1}}$$

As required. ■

Theorem 2.6.13

If M and N are both noetherian(/artinian) then so is $M+N$.

Proof: We have:

$$ {}^{M+N}/_{N} \cong {}^{M}/_{N\cap M} $$

quotient of M and so noetherian. N and ${}^{M+N}/_{N}$ are noetherian, and that implies that $M+N$ noetherian from the previous theorem. ■

Definition 2.6.14 (Finitely generated) M is a finitely generated R-module if $\exists x_1, \dots, x_n \in M$ such that:

$$ M = Rx_1 + Rx_2 + \ldots + Rx_n $$

Theorem 2.6.15

If R is left-noetherian then so is every finitely generated left R-module.

Proof: Let $M = Rx_1 + \ldots + Rx_n$ then each Rx_i is homomorphic image of R as a left R-module: $a \in R,\ a \mapsto ax_i$.
So M is a finite sum of noetherian modules, and thus noetherian. ■

Exercise: If R is noetherian and M is an R-module then M is noetherian $\iff$ every submodule of M is finitely generated.

2.7 Free modules

Definition 2.7.1 Let M be an R-module, the set $\{e_\alpha\}_{\alpha\in I}$ is a set of **generators** for M if every element of M can be written in the form:

$$ x = \sum_{i=1}^{k} a_i e_{\alpha_i} \quad \text{for some } a_i \in R\text{and } \alpha_i, \dots, \alpha_k \in I $$

Definition 2.7.2 (Basis) If $\{e_\alpha\}_{\alpha\in I}$ is a set of generators for an R-module M we say it is a **basis** for M if $\sum a_i e_{\alpha_i} = 0$ for $a_i \in R$, $\alpha_1, \dots, \alpha_k \in I$ if and only if $a_i = 0$ for all i.

Remarks 2.7.3 We say that a set with this property (without being a generator) is "independent".

Definition 2.7.4 ((Lang)) M is a free R-module if it has a basis.

Example 2.7.5 () ${}^{\mathbb{Z}}/_{3\mathbb{Z}} \times \mathbb{Z}$ is a non-free $\mathbb{Z}$-module.

Example 2.7.6 () $\prod\limits_{p \text{ prime}} {}^{\mathbb{Z}}/_{p\mathbb{Z}}$ as a $\mathbb{Z}$-module is not free.

01/04/2014

Recall the definition from last week:

Definition 2.7.7 M is a free R-module if it is a R-module and has a **basis** (over R), and then $\operatorname{rank} M =$ cardinality of basis (not well-defined).

And recall that a basis is a set $\{e_\alpha\}$, and every element in M can be represented as $\sum a_i e_{\alpha_i}$ for $a_i \in \mathbb{R}$, and $\sum a_i e_{\alpha_i} = 0 \iff \forall i \quad a_i = 0$.

Example 2.7.8 () $\mathbb{Z}$ is a free $\mathbb{Z}$-module as $\{1\}$ is a basis.
On the other hand, ${}^{\mathbb{Z}}/_{3\mathbb{Z}}$ as a $\mathbb{Z}$-module is not free. And so $({}^{\mathbb{Z}}/_{3\mathbb{Z}}) \times$ any other module as a $\mathbb{Z}$-module is not free.

Denote $R^{(n)} = \{(a_1, \dots, a_n) \mid \ a_i \in R\}$, then $R^{(n)}$ is a free R-module, with basis: $e_i = (0, \dots, 1, \dots, 0)$.

Claim 2.7.9

If M is a free R-module of rank n then $M \cong R^{(n)}$.

Proof: If $\{x_1, \dots, x_n\}$ basis for M, map $x_i \mapsto e_i$ and extend to an isomorphism of R-modules. ■

Claim 2.7.10

Let M be any R-module. $u_1, \dots, u_n \in M$ then there exists a unique homomorphism from $R^{(n)}$ to M sending $e_i \overset{\mu}{\mapsto} u_i$.

This claim is equivalent to the definition we gave, this is the "universal property". We say that F is a free if and only if the above claim holds (where we replace F with $R^{(n)}$ and exists a set of elements).

Proof: Define $\mu\left(\sum a_i e_i\right) = \sum a_i u_i$. This define an homomorphism, and it is unique from the independence. ■

Theorem 2.7.11

If R is commutative and $R^{(m)} \cong R^{(n)}$ then $m = n$.

Proof: Suppose wlog $m < n$ and take $\langle e_1, \dots, e_n \rangle$ and $\langle f_1, \dots, f_m \rangle$ two bases inside $R^{(n)}$ say.

$\exists b_{i,j} \in R$ and $\exists a_{j,i} \in R$ s.t. $f_j = \sum\limits_{i=1}^{n} a_{j,i} e_i$ and $e_i = \sum\limits_{j=1}^{m} b_{i,j} f_j$. Construct two matrices $n \times n$:

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ a_{2,1} & \dots & a_{2,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \dots & a_{m,n} \\ 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

$$B = \begin{pmatrix} b_{1,1} & \dots & b_{1,m} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & \dots & b_{n,m} & 0 & \dots & 0 \end{pmatrix}$$

We get:

$$f_j = \sum_{i=1}^{n} a_{j,i} \left(\sum_{k=1}^{m} b_{i,k} f_k \right) \Rightarrow \sum_{i=1}^{n} a_{j,i} b_{i,k} = \delta_{j,k}$$

$$e_i = \sum_{j=1}^{m} b_{i,j} \left(\sum_{l=1}^{m} a_{j,l} e_l \right) \Rightarrow \sum_{j=1}^{m} b_{i,j} a_{j,l} = \delta_{i,l}$$

By the second equation we get that $BA = I$. It is easy to show that over a commutative ring this means that A, B commute and that B is also a right inverse for A.

But $A \cdot B$ has $n - m$ rows of zeroes. So we get a contradiction. ■

Remarks 2.7.12 If R is non-commutative you can have $R^{(m)} \cong R^{(n)}$ and $m \neq n$. If $A' = \left(a_{i,j}\right)_{m \times n}$ and $B = \left(b_{i,j}\right)_{n \times m}$ as in the previous construction. Get $B'A' = I_{n \times n}$ and $A'B' = I_{m \times m}$ (ex. in Jacobson BAI page 169).

2.8 Universal property

Theorem 2.8.1

~~*Let F be a free R-module with bases $\{x_\alpha\}_{\alpha \in I}$ and M be any R module $\{y_\alpha\}_{\alpha \in I} \subseteq M$ arbitrary elements. Then*~~ *there exists a unique homomorphism $\mu : F \to M$ s.t. $\mu\left(x_\alpha\right) = y_\alpha$.*

Corollary 2.8.2

Any two free R modules with bases of equal cardinality are isomorphic.

Proof: If $\{x_\alpha\}_{\alpha\in I}$ is a basis for F, $\{x'_\alpha\}$ a basis for F' then the map sending $x_\alpha \mapsto x_\alpha$ will be invertible and so an isomorphism. ■

Chapter 3

Tensor product

3.1 Balanced product

Definition 3.1.1 (Balanced product) For a ring R, let $M = M_R$ be a right R-module and $N =_R N$ be a left R-module.
A **balanced product** of M and N is an additive abelian group P and map $f : M \times N \to P$ such that $\forall x, x' \in M \; \forall y, y' \in N$:

1. $f(x + x', y) = f(x, y) + f(x', y)$.
2. $f(x, y + y') = f(x, y) + f(x, y')$.
3. $f(xr, y) = f(x, ry) \; \forall r \in R$.

We denote this by (P, f).

✎**Example 3.1.2 ()** $M = N = \mathbb{Z} = P$. And the map: $f(x, y) = x \cdot y$.

✎**Example 3.1.3 ()** Let R be a ring, $R^{(n)} = \{(a_1, \ldots, a_n) \mid \quad a_i \in R\}$ as a left R-module (w.r.t coordinate-wise multiplication on the left).
${}^{(m)}R = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \mid \; a_i \in R \right\}$ is a right R-module.
Let $P = M_{m \times n}(R)$ as an additive group. And we define the map as:

$$f\left(\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}, (b_1, \ldots, b_n) \right) \underbrace{=}_{\text{Matrix prod.}} \begin{pmatrix} a_1 b_1 & a_1 b_2 & \ldots & a_1 b_n \\ \vdots & & & \\ a_m b_1 & \ldots & \ldots & a_m b_n \end{pmatrix}$$

(P, f) is a balanced product.

3.1.1 Some claims

Claim 3.1.4

$f(0, y) = 0 = f(x, 0)$.

Claim 3.1.5

$f(-x, y) = -f(x, y) = f(x, -y)$.

3.2 Tensor Product Definition

Definition 3.2.1 (Tensor product) A **tensor product** of M_R (right R-module) and ${}_RN$ (left R-module) is a balanced product. $(M \otimes_R N, \otimes)$ (We denote $P = M \otimes_R N$ and $f = \otimes$) such that for any other balanced product (P, f) of M and N there exists a unique homomorphism $\varphi : M \otimes_R N \to P$ s.t.

$$\forall x \in M,\ \forall y \in N : \quad \varphi\left(x \otimes y\right) = f\left(x, y\right)$$

Remarks 3.2.2 We are using the notation: $\otimes\left(x, y\right) = x \otimes y$.

i.e. tensor product is a balanced product with a "universal property":

$$\begin{tikzcd}
M \times N \arrow[r, "f"] \arrow[d, "\otimes"'] & P \\
M \otimes_R N \arrow[ur, dashed, "\exists!\varphi"'] &
\end{tikzcd}$$

Remarks 3.2.3 From uniqueness it follows that every element in $M \otimes_R N$ will be a finite sum of "pure tensors" i.e. of the form:

$$\sum_{i=1}^{n} x_i \otimes y_i$$

3.3 Construction of a tensor product explicitly

Let F be a free additive group on set of generators $M \times N$ (i.e. a set of formal finite sums $\sum\limits_{i=1}^{n} \left(x_i, y_i\right)$ where $x_i \in M$ and $y_i \in N$).

Look at the subgroup G in F generated by the following set of elements $\forall x \in M,\ y \in N,\ r \in R$:

(1) $(x + x', y) - (x, y) - (x', y)$

(2) $(x, y + y') - (x, y) - (x, y')$

(3) $(xr, y) - (x, ry)$

Define $M \otimes_R N = {}^F\!/_G$, $x \otimes y = (x, y) + G$.

Clearly, $(M \otimes_R N, \otimes)$ is a balanced product by definition of G . Now we show it satisfies the universal property:

Let (P, f) be a balanced product of M and N. As F is a free group, there is a unique homomorphism of groups $\psi : F \to P$ s.t. $\psi\left(x, y\right) = f\left(x, y\right)$ where $x \in M$ and $y \in N$.

Let $\ker\psi = K$. For $(x, y), (x', y) \in M \times N$ we have:

$$\psi\left(x + x', y\right) - \psi\left(x, y\right) - \psi\left(x', y\right) = f\left(x + x', y\right) - f\left(x, y\right) - f\left(x', y\right) \underbrace{=}_{f\text{is a balanced product}} 0$$

So:

$$\psi\left[\left(x + x', y\right) - \left(x, y\right) - \left(x', y\right)\right] = 0$$

Meaning all the elements of type (1) are in $\ker\psi$. Similarly all the elements of type (2) and (3) are in $\ker\psi$. So $\ker\psi$ contains all the generators of G and so $G \subseteq \ker\psi$. So ψ induces a homomorphism φ from $M \otimes_R N = {}^F\!/_G$ to P.

$$\varphi\left(x \otimes y\right) = \varphi\left(\left(x, y\right) + G\right) = \psi\left(x, y\right) = f\left(x, y\right)$$

Since $G \subseteq \ker\psi$ this is a well-defined homomorphism. And can show it is unique.

3.4 Examples

✎**Example 3.4.1 ()** ${}^{(m)}R \otimes_R R^{(n)} \cong M_{m,n}(R)$.

✎**Example 3.4.2 ()** If V and W are vector spaces over a field F with bases $\{v_\alpha\}$, $\{w_\beta\}$ respectively then $V \otimes_F W$ is the vector space with basis $\left\{ v_\alpha \otimes w_\beta \mid \begin{array}{c} v_\alpha \in \text{basis for } V \\ w_\beta \in \text{basis for } W \end{array} \right\}$
In particular, if $\dim V, \dim W < \infty$ then:

$$\dim V \otimes_F W = \dim V \cdot \dim W$$

✎**Example 3.4.3 ()** If M is an additive group, we can regard M as a $\mathbb{Z}$-module.
We can construct a tensor product:$\mathbb{Q} \otimes_{\mathbb{Z}} M$. This is an additive group and we can regard it as a $\mathbb{Q}$-module i.e. for $r, s \in \mathbb{Q}$ $s(r \otimes x) \underbrace{=}_{\text{def.}} sr \otimes x$, $\mathbb{Q} \otimes_{\mathbb{Z}} M$ is a vector space over $\mathbb{Q}$.
$M \hookrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} M$, $x \mapsto 1 \otimes x$.
In general, if $R \subseteq S$ subring, and M is an R-module, extend M to an S-module by: $S \otimes_R M = M'$ and define $s_1(s_2 \otimes x) = s_1 s_2 \otimes x$.

08/04/2014

Chapter 4

Group theory theorems with R-modules analogues

4.1 Normal Series

Definition 4.1.1 (Normal series) A **normal series** for a group G is a chain:

$$1 = G_{s+1} \lhd G_s \lhd \ldots \lhd G_1 = G$$

$$G_{i+1} \lhd G_i \quad \forall i$$

Definition 4.1.2 Two series are equivalent if can permute indices to give isomorphic quotients. i.e. Given also $1 = H_{t+1} \lhd H_t \lhd \ldots \lhd H_1 = G$. Then the 2 series equivalent if $t = s$ and we have correspondence $i \mapsto i'$ s.t. ${}^{G_i}/_{G_{i+1}} \cong {}^{H_{i'}}/_{H_{i'}+1}$.

Example 4.1.3 () For example:

$$\begin{aligned} 1 &\lhd C_3 \lhd C_3 \times C_5 \lhd C_3 \times C_5 \times C_7 \\ 1 &\lhd C_5 \lhd C_5 \times C_7 \lhd C_3 \times C_5 \times C_7 \end{aligned}$$

Look at the quotients:

$$\begin{aligned} 1 &\lhd C_3 \lhd C_3 \times C_5 \lhd C_3 \times C_5 \times C_7 \qquad C_3, C_5, C_7 \\ 1 &\lhd C_5 \lhd C_5 \times C_7 \lhd C_3 \times C_5 \times C_7 \qquad C_5, C_7, C_3 \end{aligned}$$

It's clear these two are not the same series, but they are equivalent by our definition.

Definition 4.1.4 (Refinement) A series $\{G_i\}$ is **refinement** of a series $\{H_i\}$ if $\{G_i\} \supseteq \{H_i\}$ (i.e. $\{H_i\}$ are subsequences of $\{G_i\}$).

Definition 4.1.5 (Composition series) A c**omposition series** is normal series which has no nontrivial refinements.

Example 4.1.6 () Both of the series:

$$\begin{aligned} 1 &\lhd C_3 \lhd C_3 \times C_5 \lhd C_3 \times C_5 \times C_7 \\ 1 &\lhd C_5 \lhd C_5 \times C_7 \lhd C_3 \times C_5 \times C_7 \end{aligned}$$

Are composition series, but equivalent.

In modules we can define:

Definition 4.1.7 A series of an R-module M is a chain of R-modules s.t.

$$1 = M_{s+1} \lhd M_s \lhd \ldots \lhd M_1 = M$$

4.1.1 Schreier Refinement theorem

Theorem 4.1.8 (*Schreier Refinement theorem*)

Any two normal series for a finite group have equivalent refinements.
Any two series of R-submodules have equivalent refinements.

Remarks 4.1.9 If $N \lhd G$ and $H \leq G$ a subgroup, then $N \cdot H = H \cdot N$ is a subgroup as well.

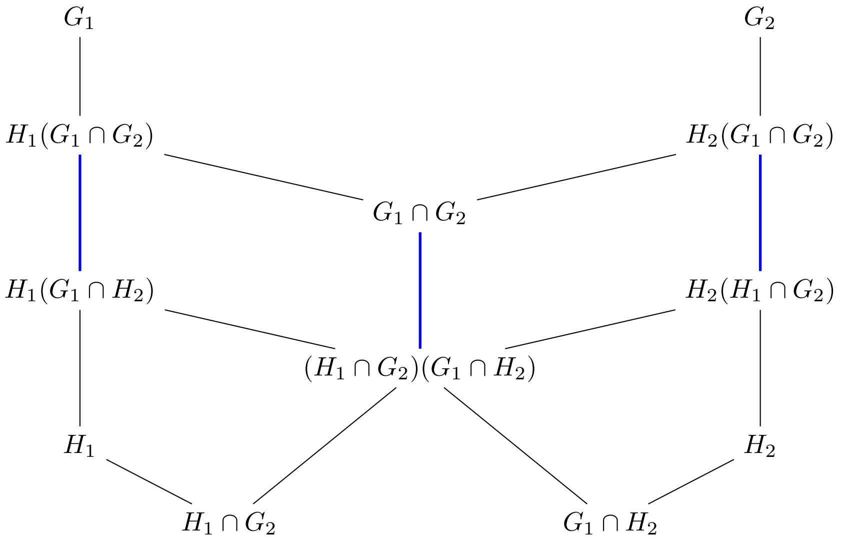
Lemma 4.1.10 (*Zassenhaus' Lemma (Butterfly Lemma)*)

Let G_1, G_2 be subgroups of a group G, And let $H_i \lhd G_i$ for $i = 1, 2$. Then:

$$\begin{aligned} H_1 (G_1 \cap H_2) &\lhd H_1 (G_1 \cap G_2) \\ (H_1 \cap G_2) H_2 &\lhd (G_1 \cap G_2) H_2 \end{aligned}$$

And we have:

$${}^{H_1(G_1\cap G_2)}\big/_{H_1(G_1\cap H_2)} \cong {}^{(G_1\cap G_2)H_2}\big/_{(H_1\cap G_2)H_2}$$



Proof: Note that every coset of $H_1 (G_1 \cap H_2)$ in $H_1 (G_1 \cap G_2)$ can be represented by an element of $G_1 \cap G_2$, as if $xy \in H_1 (G_1 \cap G_2)$ with $x \in H_1$ and $y \in G_1 \cap G_2$ then:

$$xyH_1 (G_1 \cap H_2) \underbrace{=}_{\text{normality}} xH_1y (G_1 \cap H_2) = H_1y (G_1 \cap H_2) \underbrace{=}_{\text{normality}} yH_1 (G_1 \cap H_2)$$

Similarly, any coset $(H_1 \cap G_2) H_2$ in $(G_1 \cap G_2) H_2$ can be represented by an element in $G_1 \cap G_2$ so for $y \in G_1 \cap G_2$. Map: $y \cdot H_1 (G_1 \cap G_2) \mapsto y (H_1 \cap G_2) H_2$ and verify this is an isomorphism. ■

Proof of Schreier Refinement Theorem:

Proof: Given two normal series of finite length:

$$\begin{aligned} 1 &= G_{s+1} \lhd G_s \lhd \ldots \lhd G_1 = G \\ 1 &= H_{t+1} \lhd H_t \lhd \ldots \lhd H_1 = G \end{aligned}$$

We show these series have equivalent refinements.

Denote $G_{i_k} = G_{i+1}\left(G_i \cap H_k\right)$ and $H_{k_i} = \left(H_k \cap G_i\right) H_{k+1}$ where $1 \leq k \leq t+1$ and $1 \leq i \leq s+1$. By Zassenhaus we have that: $G_{i_{k+1}} \lhd G_{i_k}$ and $H_{k_{i+1}} \lhd G_{k_i}$ and: $G_{i_k}/G_{i_{k+1}} \cong H_{k_i}/H_{k_{i+1}}$.

$$\begin{aligned}
G_{i_1} &= G_{i+1}\left(G_i \cap \overbrace{H_1}^{G}\right) = G_{i+1}G_i = G_i \\
H_{k_1} &= H_k \\
G_{i_{t+1}} &= G_{i+1}\left(G_i \cap \overbrace{H_{t+1}}^{1}\right) = G_{i+1}
\end{aligned}$$

We now get two normal series of length $s \cdot t$:

$$\begin{aligned}
G &= \underbrace{G_1}_{G_1} \rhd G_{1_2} \rhd \ldots \rhd G_{1_{t+1}} = \underbrace{G_2}_{G_{2_1}} \rhd G_{2_2} \rhd \ldots \rhd G_{s_{t+1}} = 1 \\
H &= \underbrace{H_1}_{H_{1_1}} \rhd \ldots
\end{aligned}$$

These will be equivalent because of the isomorphisms of $G_{i_k}/G_{i_{k+1}} \cong H_{k_i}/H_{k_{i+1}}$ with $(i_k)' = k_i$. ■

Example 4.1.11 ()

$$\begin{aligned}
1 &\lhd \mathbb{Z}/3\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z} \\
1 &\lhd \mathbb{Z}/2\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z}
\end{aligned}$$

Example 4.1.12 () $\mathbb{Z}$ has no composition series as a $\mathbb{Z}$-module.

$$\begin{aligned}
\text{quotient of order } 3\mathbb{Z} &\supset 3\mathbb{Z} \supset 9\mathbb{Z} \supset \ldots \\
\text{quotient of order } 5\mathbb{Z} &\supset 5\mathbb{Z} \supset 25\mathbb{Z} \supset \ldots
\end{aligned}$$

Two infinite series which do not have equivalent refinements. Each quotient is of prime order.

Example 4.1.13 () $1 \lhd \langle (1\,2)\,(3\,4) \rangle \lhd V_4 \lhd A_4 \lhd S_4$. Composition series ($V_4$ is Klein 4 group).

4.2 Jordan Holder Theorem

An immediate consequence of the Schreier Refinement Theorem is the Jordan Holder theorem:

Theorem 4.2.1

Any two composition series for a group/R-module are equivalent.

Proof: User Schreier refinement theorem (and throw out trivial quotients). ■

Definition 4.2.2 (Irreducible module) An R-module M(group G) is **irreducible** (simple) if it has no nontrivial submodules (normal subgroups).

Remarks 4.2.3 In a composition series, all quotients will be irreducible.

Theorem 4.2.4

A module $M \neq 0$ has a composition series $\iff$ it is both noetherian and artinian.

Proof: Suppose M ha a composition series:

$$M = M_1 \supset M_2 \supset \ldots \supset M_{s+1} = 0$$

And suppose an arbitrary series of submodules:

$$M = N_1 \supset N_2 \supset \ldots \supset N_t \supset \ldots$$

Look at the sequence that ends with a 0:

$$M = N_1 \supset N_2 \supset \ldots \supset N_t \supset 0$$

Then, this has a refinement equivalent to our composition series. So $t \leq s$.

Similarly, every increasing sequence has length $\leq s$. Thus M is both artinian and noetherian.

Now we want to show the other direction. Assume M is noetherian and artinian. $M = M_1$ has a proper maximal submodule M_2 (otherwise we have an infinite increasing chain). M_2 is also noetherian so has a maximal submodule M_3. Get descending chain:

$$M = M_1 \supset M_2 \supset M_3 \supset \ldots$$

Which must be of finite length as M also artinian. So we got a composition series. ■

4.3 Krull-Schmidt Theorem

Definition 4.3.1 (Indecomposable module) M is **indecomposable** if it has no nontrivial submodules M_1, M_2 s.t. $M = M_1 \oplus M_2$.

Remarks 4.3.2 Clearly irreducible→indecomposable. But not the other way around.

✎**Example 4.3.3 ()** $\mathbb{Z}$ is not irreducible as a $\mathbb{Z}$-module. But note that it cannot be that $\mathbb{Z} = \underbrace{M_1}_{n\mathbb{Z}} \oplus \underbrace{M_2}_{m\mathbb{Z}}$ because $n\mathbb{Z} \cap m\mathbb{Z} \neq 0$ (unless n or $m = 0$).

Note:

Given R-modules $M_1, \ldots, M_r$ we can construct $M_1 \times \ldots \times M_k = M$ with coordinate-wise operations

Get R-homomorphisms: $i_j : M_j \to M$ the natural injections and $p_j : M \to M_j$ the natural projections.

$e_j = i_j p_j : M \to M$. $e_j \in \text{End}M$:

$$e_j^2 = i_j \underbrace{(p_j i_j)}_{1_{M_j}} p_j = e_j$$

So e_j is idempotent.

If $j \neq k$ then:

$$e_j e_k = i_j \underbrace{(p_j i_k)}_{0} p_k = 0$$

So $e_1, \ldots, e_k$ are orthogonal idempotents. And: $e_1 + \ldots + e_k = 1_M$. Denote $e_j(M) = M_j' \cong M_j$.

If $x \in M$ then:

$$x = 1_M x = \underbrace{e_1 x}_{\in M_1'} + \ldots + \underbrace{e_k x}_{\in M_k'}$$

So M is a direct sum of submodules $M_1', \ldots, M_k'$. $M = M_1' \oplus \ldots \oplus M_k'$ as we have:

$$M_k' \cap \left(\bigoplus_{j \neq k} M_j' \right) = 0$$

Conversely, given $M = M_1 \oplus \ldots \oplus M_k$ where M_i are submodules. Can define injection and projections:

$$\begin{aligned} i_j : M_i &\to M \\ p_j : M &\to M_i \end{aligned}$$

s.t. $e_j \in \mathrm{End}M$ idempotents, orthogonal and $e_1 + \ldots + e_k = 1_M$.

Conclude: $M \neq 0$ is indecomposable $\iff$ End$M$ does not contain a non-trivial idempotent (i.e.$\neq 0, 1$)

Proof: Clearly showed that if M =nontrivial direct sum, then End$M$ has nontrivial idempotents. $M = M_1 \oplus M_2$. $e_1 + e_2 = 1_M$ and $e_1 (M_1) = M_2$ and $e_2 (M_2) = M_2$.
Now, assume $e \in \mathrm{End}M$, nontrivial idempotent. Define $e(M) = M_1$, $(1-e)M = M_2$ and get $M_1 \oplus M_2 = M$.

$$e_1 e_2 = e(1-e) = e - e^2 = 0$$

$M_2, M_1 \neq 0$ as if $M_1 = 0$ then $e = 0$ contradiction.
And if $M_2 = 0$ then $1_M - e = 0$ giving $e = 1_M$ contradiction. ■

Remarks 4.3.4 End$\mathbb{Z} \cong \mathbb{Z}$ contains no nontrivial idempotents.

29/04/2014

4.4 Indecomposable

Remarks 4.4.1 Decomposition to direct sum of finite number of indecomposable is generally not unique.
e.g.

$$\mathbb{R}^3 = \mathrm{span}\left\{\begin{pmatrix}1\\0\\0\end{pmatrix}\right\} \oplus \mathrm{span}\left\{\begin{pmatrix}0\\1\\0\end{pmatrix}\right\} \oplus \mathrm{span}\left\{\begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$$

but also:

$$\mathbb{R}^3 = \mathrm{span}\left\{\begin{pmatrix}1\\1\\0\end{pmatrix}\right\} \oplus \mathrm{span}\left\{\begin{pmatrix}0\\1\\0\end{pmatrix}\right\} \oplus \mathrm{span}\left\{\begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$$

But here we do have isomorphisms between components.

We shall need a string condition on End$M$ we get uniquness up to isomorphisms of decompositions.
Recall that:

Definition 4.4.2 A ring R is <u>**local**</u> if the set of non-units is an ideal.

✎**Example 4.4.3 ()** $M_2(\mathbb{Q})$ is not local as: $\begin{pmatrix}1&0\\0&0\end{pmatrix} + \begin{pmatrix}0&0\\0&1\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix}$
but:

$$S = \left\{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0,\ 2 \nmid n\right\}$$

is local. $2S$ =set of non-units and is an ideal.

Remarks 4.4.4 Local rings do not contain idempotents $\neq 0, 1$.

Definition 4.4.5 (Strongly indecomposable) M is <u>**strongly indecomposable**</u> if End$M$ is local.

<u>**Theorem 4.4.6**</u>

If M has 2 decomposable $N_1 \oplus \ldots \oplus N_l = M = M_1 \oplus \ldots \oplus M_k$ where N_i are indecomposable and the M_i are strongly indecomposable, then $k = l$ and there exists a permutation $j \mapsto j'$ s.t. $M_j \cong N_j$.

✎**Example 4.4.7 ()** $\mathbb{Z}$ is indecomposable but not strongly indecomposable as End$\mathbb{Z} \cong \mathbb{Z}$ not local.

Lemma 4.4.8

Suppose M, N modules, $f : M \to N$ homomorphism. $M \neq 0, N$ is indecomposable, $g : N \to M$ homomorphism s.t. gf automorphism (of M), then f and g are isomorphisms.

Proof: Suppose k inverse of gf so $kgf = 1_M$.

Let $l = kg : N \to M$, $lf = 1_M$ so f is left invertible.

Look at $fl = e$, $e^2 = flfl = f\left(lf\right)l = fl = e$, so e is idempotent. As N is indecomposable, it must have $e = 0$ or $e = 1$. Now $lf = 1_M$ so we cant have $e = 0$ because then: $1_M = \left(lf\right)^2 = lflf = l\underbrace{\left(fl\right)}_{\neq 0}f$. So $e \neq 0$ so $e = 1$ and f is also right invertible (l is its right inverse) and so an isomorphism. Now $g = k^{-1}f^{-1}$ so g also an isomorphism. ■

Now we want to prove the theorem: **Proof:** By induction on k.

$k = 1$ then $M = M_1$ indecomposable so $l = 1$ and $N_1 \cong M_1$.

Now assume for any $m < k$ and prove for k.

Define projections: $e_j : M \to M_j$ for $1 \leq j \leq k$ and $f_j : M \to N_j$ for $1 \leq j \leq l$.

Look at: $h_j = f_j e_1 : M \to N_j$ and $k_j = e_1 f_j : M \to M_1$, then

$$\sum_{j=1}^{l} k_j h_j = \sum e_1 f_j f_j e_1 = e_1 \left(\sum \underbrace{f_j^2}_{f_j}\right) e_1 = e_1 1_M e_1 = e_1$$

Restricting e_1 to M_1: $e_1 \mid_{M_1} = e_1'$, $k_j \mid_{N_1} = k_j'$, $h_j \mid_{M_1} = h_j'$.

So $\sum k_j' h_j' = e_1'$ and $e_1' = 1_{M_1}$ and M_1 is strongly indecomposable. EndM_1 is local, so we cannot have everyone of the $k_j' h_j'$ non-units. So $\exists j$ s.t. $k_j' h_j'$ is automorphism of M_1.

Now, use the lemma, WLOG suppose $j = 1$, h_1', k_1' must be isomorphisms. $h_1' : M_1 \to N_1$ so $M_1 \cong N_1$.

Remarks 4.4.9 Note: we are not done yet, as we can have $M_1 \cong N_1$ but ${}^{M}/{}_{M_1} \ncong {}^{M}/{}_{N_1}$. e.g. M is infinite dimensional vector space with basis $\{x_i\}_{i=1}^{\infty}$ and $\underbrace{\text{span}\{x_2, x_3, \ldots\}}_{M_1} \cong \underbrace{\text{span}\{x_3, x_4, \ldots\}}_{N_1}$.

Claim 4.4.10

$M = N_1 \oplus M_2 \oplus \ldots \oplus M_k$.

First show $N_1 \cap (M_2 \oplus \ldots \oplus M_k) = 0$, Let $x \in N_1 \cap (M_2 \oplus \ldots \oplus M_k)$, $e_1\left(x\right) = 0$ as $x \in M_2 \oplus \ldots \oplus M_k$. $f_1\left(x\right) = x$ as $x \in N_1$. $k_1\left(x\right) = e_1 f_1\left(x\right) = 0$, but k_1' is an isomorphism from N_1 to M_1, so this implies $x = 0$.

It remains to show that $M_1 \subseteq N_1 \oplus M_2 \oplus \ldots \oplus M_k = M'$. Let $x \in M_1$, note that $e_1\left(N_1\right) = e_1 f_1\left(N_1\right) = k_1\left(N_1\right) = k'\left(N_1\right) = M_1$, so there exists $y \in N_1$ s.t. $x = e_1\left(y\right)$ hence:

$$\sum_{i=1}^{k} e_i\left(y\right) = y$$

So we get:

$$x = e_1\left(y\right) = y - \sum_{i=2}^{k} e_i\left(y\right) \in M'$$

So now we do have:

$$N_2 \oplus \ldots \oplus N_l \cong {}^{M}/{}_{N_1} \cong M_2 \oplus \ldots \oplus M_k$$

And get our result by induction. ■

4.5 Fitting's Lemma

Lemma 4.5.1 (*Fitting's Lemma*)

Let M be both artinian and noetherian, and $f \in \operatorname{End}_R M$. Then $M = f^{\infty}(M) \oplus f^{-\infty}(0)$ where

$$\begin{aligned} f^{\infty}(M) &= \cap_{n=0}^{\infty} f^n(M) \\ f^{-\infty}(0) &= \bigcup_{n=1}^{\infty} \ker f^n \end{aligned}$$

And $f\mid_{f^{\infty}(M)}$ is an automorphism and $f\mid_{f^{-\infty}(0)}$ is nilpotent.

Proof:

$$\begin{aligned} M &\supseteq f(M) \supseteq f^2(M) \supseteq \ldots \\ 0 &\subseteq \ker f \subseteq \ker f^2 \subseteq \ldots \end{aligned}$$

Since M is artinian and noetherian, both chains stabilize. So $\exists r$ s.t. $f^r(M) = f^{r+1}(M) = \ldots = f^{\infty}(M)$, $\ker f^r(M) = \ker f^{r+1}(M) = \ldots = f^{-\infty}(0)$.

Suppose $z \in \ker f^r(M) \cap f^r(M)$. Then, $\exists y \in M$ s.t. $z = f^r(y)$ and $f^r(z) = 0$ giving $f^{2r}(y) = 0$ so $y \in \ker f^{2r} = \ker f^r$ hence $z = f^r(y) = 0$.

Now, take $x \in M$, we show that $x \in f^{\infty}(M) \oplus f^{-\infty}(0)$.

$$f^r(x) \in f^r(M) = f^{2r}(M)$$

so $\exists y \in M : f^r(x) = f^{2r}(y)$. So $f^r(x - f^r(y)) = 0$. So $x - f^r(y) \in \ker f^r$.

$$x \in \underbrace{\ker f^r}_{f^{-\infty}(0)} \oplus \underbrace{f^r(M)}_{f^{\infty}(M)}$$

We now show $f\mid_{f^{-\infty}(0)}$ is nilpotent.

For all $x \in f^{-\infty}(0) = \ker f^r$, $f^r(x) = 0$ so $\left(f\mid_{f^{-\infty}(0)}\right)^r = 0$.

We show $f\mid_{f^{\infty}(M)}$ is an automorphism:

$$f^{\infty}(M) = f^r(M) = f^{r+1}(M)$$

So $f\mid_{f^{\infty}(M)}$ is surjective.

Suppose $x \in f^{\infty}(M)$ and $f(x) = 0$ so $x \in \ker f \subseteq f^{-\infty}(0)$ so $x = 0$. So $f\mid_{f^{\infty})M}$ is injective and surjective. ■

Example 4.5.2 () Counterexample:
Let V be an infinite dimensional vector space over a field, $\{x_i\}_{i=1}^{\infty}$ basis. So V neither artinian nor noetherian.
f is a linear operator that project onto $\operatorname{span}\{x_1\}$. i.e. if $x = \sum_{i=1}^{k} c_i x_i$ then $f(x) = c_1 x_1$.
g is the linear operator $g(x) = \sum_{i=1}^{k} c_i x_{i+1}$.
Let $T = f + g$. What is its kernel?
If $T(x) = 0$ then $f(x) + g(x) = 0$. If x as above $T(x) = c_1 x_1 + \sum\limits_{i=1}^{k} c_i x_{i+1} = c_1(x_1 + x_2) + c_2 x_3 + \ldots + c_k x_{k+1}$ implies $c_i = 0$ for all i so $x = 0$ and $\ker T = 0 \to T^{-\infty}(0) = 0$.
But note that:

$$\begin{aligned} T(V) &= \operatorname{span}\{x_1 + x_2, x_3, x_4, \ldots\} \\ T^2(x) &= T(c_1(x_1 + x_2) + c_2 x_3 + \ldots) = c_1 x_1 + c_1 x_2 + c_1 x_3 + c_2 c_4 + \ldots \\ T^2(V) &= \operatorname{span}\{x_1 + x_2 + x_3, x_4, x_5, \ldots\} \\ \bigcap_{n=1}^{\infty} T^n(V) &= 0 \end{aligned}$$

Remarks 4.5.3 Applying Fitting's lemma to a finite dimensional vector space and operator T we get some r s.t. $V = T^r(V) \oplus \ker T^r$ (both of them are T invariant subspaces).
In particular, if $T = A - \lambda I$ where A is a matrix and λ an eigenvalue, then $\ker T^r$ is the generalized eigenspace for λ.
We can decompose the $T^r(V)$ subspace w.r.t. $A - \mu I$ where μ is another eigenvalue.
Continue decompose V to generalized eigenspaces of A and get the Jordan decomposition of the matrix A.

Corollary 4.5.4

Let M be indecomposable, artinian and noetherian. Then every endomorphism of M is either nilpotent or an isomorphism - in fact M is strongly indecomposable.

Proof: Let $f \in \text{End}M$.

By Fitting's lemma $M = f^{\infty}(M) \oplus f^{-\infty}(0)$, but M is indecomposable, so one of these submodules is 0 and $M = f^{\infty}(M)$ and f is automorphism or $M = f^{-\infty}(0)$ and f is nilpotent.

It remains to show that End$M$ is local.

The set of non-units = set of all nilpotent endomorphisms.

Remarks 4.5.5 If f is nilpotent, $f \neq 0$, then $\exists r \geq 2$ $f^r = 0$ and $f^{r-1} \neq 0$ so f cannot be invertible.

Remarks 4.5.6 In a commutative ring we have f, g nilpotent, taking k large enough $(f+g)^k = 0$ as we get linear combinations $f^{k-l}g^l$.

■

Corollary 4.5.7

Let M be an indecomposable module that is both artinian and noetherian. Then every endomorphism of M is either an automorphism or nilpotent and in fact End$M$ *is local, i.e. M is strongly indecomposable.*

Proof: We showed that every endomorphism is nilpotent or an automorphism. It remains to show that the set of nonunits in End$M$ is an ideal. $I = \{f \in \text{End}M \mid f \text{ is nilpotent}\}$.

Let $f \in I$, $g \in \text{End}M$ then $g \circ f$ and $f \circ g$ are not invertible. As if $f \neq 0$, $f^k = 0$ and $f^{k-1} \neq 0$ then $(gf) f^{k-1}$=0, $f^{k-1}(fg) = 0$.

So if say gf is invertible and h is inverse, we would have $\underbrace{h(gf)}_{1} f^{k-1} = f^{k-1} = 0$ contradiction.

Suppose that $f_1, f_2 \in I$, $f_1 + f_2 \notin I$ so $f_1 + f_2$ automorphism. So we have $g \in \text{End}M$ such that $g(f_1 + f_2) = (f_1 + f_2) g = 1$.

Let $h_i = f_i g$. so $h_i \in I$ and so it is nilpotent, thus exists k s.t. $h_i^k = 0$. we then have $\underbrace{(1 - h_i)}_{\text{invertible}} \left(1 + h_i + h_i^2 + \ldots + h_i^{k-1}\right) = 1$. But $h_1 + h_2 = 1$ so h_2 is invertible. Contradiction. ■

Theorem 4.5.8

If $M \neq 0$ is both artinian and noetherian then M contains indecomposable submodules M_i s.t. $M = M_1 \oplus \ldots \oplus M_n$.

Proof: As M is artinian and noetherian, it has a composition series. By Jordan-Holder, any two composition series are equivalent and so the length is well-defined.

We prove the theorem by induction on the length $\ell(M)$ of a composition series.

If $\ell(M) = 1$ then M is irreducible and so indecomposable.

Now assume $\ell(M) > 1$. if M is indecomposable we are done.

So now assume M not indecomposable. So $M = N_1 \oplus N_2$. $N_1, N_2 \neq 0$. We claim $\ell(N_i) < \ell(M)$ as if we form the chain $0 \subset N_i \subset M$ which can be refined to a composition series giving $\ell(N_i) < \ell(M)$.

So now, using induction hypothesis on N_1, N_2 we get that M is direct sum of indecomposable. ■

We got:

Theorem 4.5.9 (*Krull-Schmidt Theorem*)

Let $M \neq 0$ be both artinian and noetherian and suppose $N_1 \oplus N_2 \oplus \ldots \oplus N_l = M = M_1 \oplus \ldots \oplus M_k$ then $k = l$ and we have permutation $i \to i'$ s.t. $M_i \cong N_{i'}$.

Wedderburn - 1909 proved for finite groups with a gap, and Remak in 1911 filled the gap.

Krull in 1925 proved for abelian groups with operators, modules over rings, and Schmidt in 1928 proved for arbitrary groups.

4.6 Completely Reducible Modules

Theorem 4.6.1

The following are equivalent:

1. *M is an irreducible right R-module.*
2. *$M \neq 0$ and M is generated by any $x \neq 0$ as a right R-module.*
3. *$M \cong {}^{R}/_{I}$ with I max right ideal in R.*

Proof: $1 \Rightarrow 2$: clearly if $x \neq 0$, $xR=$ right R-submodule. *So* if $x \neq 0$ must have $xR = M$.

$2 \Rightarrow 3$: Take $x \in M$, $x \neq 0$ and the map $a \overset{\varphi}{\mapsto} xa$ module homomorphism $R \to M$. $\mathrm{Im}\varphi = M$ as $xR = M$, $I = \ker\varphi=$ right ideal and it is maximal. As otherwise would have $b \in R$, $I' := bR + I \subsetneq R$. But then ${}^{I'}/_{I}$ would correspond to a submodule N in M, $N := \varphi(I')$, $N \cong {}^{I'}/_{I}$ so would have $y \in N$ in submodule but $yR = M$ by condition 2.

$3 \Rightarrow 1$: If I is maximal, clearly ${}^{R}/_{I}$ must be irreducible as if it had a submodule $N \neq 0$, M would have corresponding right ideal I' :$0 \subset I \subset I' \subset R$ and ${}^{I'}/_{I} \cong N$. ■

4.6.1 Schur's Lemma

Theorem 4.6.2 (*Schur's Lemma*)

Let M, N be irreducible module. $f \in \mathrm{Hom}_R(M,N)$, then either $f \equiv 0$ or f isomorphism. In particular: if $M \cong N$, $\underbrace{\mathrm{End}_R(M)}_{\cong \mathrm{Hom}_R(M,N)}$ = division ring and if $M \cong N$, $\mathrm{Hom}_R(M,N) = 0$.

Proof: Take $f \neq 0$ in $\mathrm{Hom}(M,N)$. $\ker f$ is a submodule of M, $\ker f \neq M$ as $f \neq 0$, M is irreducible so get $\ker f = \{0\}$. $\mathrm{Im}f$ is a submodule of N, $f \neq 0$ so $\mathrm{Im}f \neq 0$. N is irreducible so we get $\mathrm{Im}f = N$ so f is an isomorphism as required. ■

Example 4.6.3 () V is a finite dimensional vector space over a field F. $R = \mathrm{End}_F(V) \cong M_n(F)$.
$\mathrm{End}_R(V)$ = set of all linear operators that commute with every other linear operator = center of $M_n(F)$ (= set of scalar matrices $\cong F$).
V is an irreducible R-module as given any $0 \neq v \in V$ and $w \in V$ then exists $\varphi \in \mathrm{End}_F(V)$ s.t. $\varphi(v) = w$ so $Rv = V$. So by Schur's Lemma, $\mathrm{End}_R(V)$= a division ring = center of $M_n(F)$ so commutative, so it is a field.

Definition 4.6.4 Suppose $\{M_\alpha\}_{\alpha \in A}$ is a set of submodules of a module M. Denote by $\sum\limits_{\alpha \in A} M_\alpha$ = set of all elements of the form $x_{\alpha_1} + \ldots + x_{\alpha_k}$. $\alpha_i \in A$, $x_{\alpha_i} \in M_{\alpha_i}$, i.e. finite sums of elements in the M_α, so $\sum\limits_{\alpha \in A} M_\alpha$ will be submodule of M.

Definition 4.6.5 S is independent set of submodules if $M_\alpha \cap \left(\sum\limits_{\substack{\beta \in A \\ \beta \neq \alpha}} M_\beta \right) = 0$ for all $\alpha \in A$.

Example 4.6.6 () $\{x_\alpha\}_{\alpha\in A}$ is independent set of elements iff $\{Rx_\alpha\}_{\alpha\in A}$ are an independent set of submodules.

Claim 4.6.7

If $S = \{M_\alpha\}_{\alpha\in A}$ is dependent, then there exists a finite subset of S which is dependent.

Proof: We have α s.t. $M_\alpha \cap \left(\sum\limits_{\beta\neq\alpha} M_\beta\right) \neq 0$, so $\exists x_\alpha \in M_\alpha$ and $x_{\beta_i} \in M_{\beta_i}$, $1 \leq i \leq k$ s.t. $x_\alpha = x_{\beta_i} + \ldots + x_{\beta_k}$ and then $M_\alpha \cap \left(\sum\limits_{i=1}^{k} M_{\beta_i}\right) \neq 0$ so $\{M_\alpha, M_{\beta_1}, \ldots, M_{\beta_k}\}$ is dependent set. ■

Claim 4.6.8

If T independent subset of S, then there exists T_0, $T \subseteq T_0 \subseteq S$, s.t. T_0 is maximal independent containing T.

Proof: Using Zorn's Lemma, look at the set $\mathcal{B} = \{B \subseteq S \mid T \subseteq B \text{ and } B \text{is independent}\}$. $\mathcal{B} \neq \varnothing$ as $T \in \mathcal{B}$. Given any chain in $\mathcal{B}$: $B \subset B' \subset \ldots$ the union B^* will be in $\mathcal{B}$, otherwise we would have B^* dependent and so a finite subset of B^* would be dependent and contained in an element of the chain.

Thus by Zorn, $\mathcal{B}$ has maximal element. ■

Definition 4.6.9 (Direct sum) If $M = \sum\limits_{\alpha\in A} M_\alpha$, $\{M_\alpha\}_{\alpha\in A}$ independent, We say M is a **direct sum** of the M_α and write $M = \bigoplus\limits_{\alpha\in A} M_\alpha$.

Definition 4.6.10 (Completely reducible) M is completely reducible if it is a direct sum of irreducible submodules.

e.g. any irreducible module is completely reducible!

Lemma 4.6.11

Suppose $\{M_\alpha\}_{\alpha\in A}$ independent set of submodules of M and N submodule of M s.t. $N \cap \left(\sum\limits_{\alpha\in A} M_\alpha\right) = 0$, then $\{M_\alpha\}_{\alpha\in A} \cup \{N\}$ is independent .

Proof: Suppose not, then we have $\beta \in A$ and $0 \neq x_\beta \in M_\beta$ s.t. $x_\beta = y + x_{\alpha_1} + \ldots + x_{\alpha_k}$ for some $y \in N$, $x_{\alpha_i} \in M_{\alpha_i}$, $\alpha_i \in A$.

Then $y = x_{\alpha_1} + \ldots + x_{\alpha_k} - x_\beta \in N \cap \left(\sum_{i=1}^{k} M_{\alpha_i} + M_\beta\right) = 0$ so $y = 0$. giving $x_\beta \in \sum\limits_{i=1}^{k} M_{\alpha_i}$ contradiction to independence. ■

Lemma 4.6.12

Suppose $\{M_\alpha\}_{\alpha\in A}$ independent set of irreducible submodules and $M = \sum_{\alpha\in A} M_\alpha$ (i.e. M completely reducible). and let $N \subseteq M$ submodule.
Then there exists a subset $B \subset A$ s.t. $\{N\} \cup \{M_\beta\}_{\beta\in B}$ is independent.

Proof: Assume first $N = M$ - trivial. So now $N \neq M$. Define $\mathcal{B} = \left\{B \subseteq A \mid \{N \cup M_\beta\}_{\beta\in B} \text{ is independent}\right\}$. $\mathcal{B} \neq \varnothing$ as if $M \neq N$ then we have α s.t. $M_\alpha \not\subset N$, in which case $M_\alpha \cap N = 0$ as $M_\alpha \cap N$ is a submodule of M_α which is irreducible. So $\{N, M_\alpha\}$ independent and $\{\alpha\} \in \mathcal{B}$.

We will continue this next week.... ■

Corollary 4.6.13

Taking $N = 0$ we get that if $M =$sum of irreducibles.
Then $M=$ direct sum of the irreducibles.

Corollary 4.6.14

If M is completely reducible then every submodule N of M has a direct complement (i.e. "the lattice of submodules of M is fully complemented").

Turns out that the converse of this corollary is true as well.

Example 4.6.15 () Let V be a vector space over a field F, we can write $V = \sum\limits_{x \in V} Fx$. Each Fx is a one dimensional subspace, and so it is irreducible. By the first corollary, V is a direct sum of some of the Fx, i.e. V has a basis.

Lemma 4.6.16

Suppose M is a module s.t. its lattice of submodules is fully complemented. Then so are $L(N)$ and $L\left(\overline{M}\right)$ where N is a submodule of M and $\overline{M}$ is homomorphic image of M.

Remarks 4.6.17 We define $L(M) = \{N \mid 0 \subseteq N \subseteq M \text{ submodule}\}$.

Proof: Let $P \subseteq N$ be a submodule of N so it is also a submodule of M and so has a direct complement P'. $M = P \oplus P'$.

And then, $P' \cap N$ is a direct complement for P inside N as:

$$N = (P \oplus P') \cap N = \underbrace{(P \cap N)}_{P} \oplus (P' \cap N)$$

Now let $\overline{M} = {}^{M}/_{P}$ with P submodule. Since P has a direct complement in M, P' i.e. $P' \oplus P \cong M$. Then $P' \cong \overline{M}$. By what we already have shown, $L(P')$ is fully complemented, and so $L\left(\overline{M}\right)$. ■

Lemma 4.6.18

Suppose $M \neq 0$, $L(M)$ is fully complement. Then M contains irreducible submodules.

Remarks 4.6.19 $\mathbb{Z}$ has no irreducible submodules.

Proof: Let $x \neq 0$ be in M and look at $\mathcal{N} = \{N \mid N \text{ submodule of } M\text{and } x \notin N\}$. By Zorn, $\mathcal{N}$ contains maximal elements. Let P be a maximal element in $\mathcal{N}$.

Let K be a direct complement for P in M: $K \oplus P = M$. We claim that K is irreducible.

Suppose $K = K' \oplus K''$, we want to show that one of these has to be 0. Assume towards contradiction that $K', K'' \neq 0$. $P \subsetneq P \oplus K'$, so $x \in P \oplus K'$. And $P \subsetneq P \oplus K''$ so $x \in P \oplus K''$. We can write $p_2 + k'' = x = p_1 + k'$ for $p_1, p_2 \in P$ and $k' \in K'$ and $k'' \in K''$. Then:

$$\underbrace{p_1 - p_2}_{\in P} = \underbrace{k' - k''}_{\in K} \Rightarrow p_1 - p_2 = 0 \Rightarrow k' - k'' = 0 \Rightarrow k' = k'' \Rightarrow k' = 0 = k''$$

Then we get $x = p_1 \in P$, contradiction. ■

Theorem 4.6.20

The following are equivalent for a module M:

1. *$M = \sum M_\alpha$ where M_α irreducible.*
2. *M is completely reducible.*
3. *$L(M)$ is fully complemented.*

Proof: $1 \Rightarrow 2$: by corollary 4.6.13.

$2 \Rightarrow 3$: by corollary 4.6.14.

It remains to show 3 ⇒ 1: By lemma 4.6.18, M contains irreducible submodules. Let:

$$M' = \sum_{N \text{irreducible submodule of } M} N$$

We claim that $M' = M$. Suppose $M' \subsetneq M$ then M' has a direct complement $0 \neq M''$ s.t. $M' \oplus M'' = M$. By lemma 4.6.16, $L(M'')$ is fully complemented and so by lemma 4.6.18, M'' contains irreducible submodule $P \neq 0$.

But then P is also an irreducible submodule of M and so $P \subseteq M'$, contradiction (as the irreducible submodules of M are in M'). ■

Definition 4.6.21 Let M be module, N an irreducible module:

$$\begin{aligned} M(N) &= \text{homogeneous complement of } M \text{determined by } N \\ &= \sum_{\substack{N' \subseteq M \text{ submodule} \\ N' \cong N}} N' \end{aligned}$$

Remarks 4.6.22 If M is not submodule isomorphic to N then $M(N) = 0$.

Theorem 4.6.23

Let $M = \bigoplus_{\alpha \in A} M_\alpha$, M_α irreducible submodules. Then:

1. *For any $N \neq 0$ irreducible submodule of M we have:*

$$M(N) = \sum_{M_\alpha \text{ s.t. } M_\alpha \cong N} M_\alpha$$

2. *$M = \bigoplus_{\substack{N \text{ irreducible} \\ N \neq 0}} M(N)$ (sum runs over representative of all isomorphism types of irreducible modules).*

   And of converse if $N \ncong P$ then $M(N) \cap M(P) = 0$.

Proof: $M(N) \supseteq \bigoplus_{M_\alpha \cong N} M_\alpha$ is trivial.

It remains only to show $M(N) \subseteq \bigoplus_{M_\alpha \cong N} M_\alpha$.

Let N' be a submodule of M which is isomorphic to N. We need to show that $N' \subseteq \bigoplus_{M_\alpha \cong N} M_\alpha$.

As N' is irreducible it is generated by a single element $N' = Rx$. Since $M = \bigoplus_{\alpha \in A} M_\alpha$, there exists $\alpha_1, \ldots, \alpha_k \in A$ s.t. $N' \subset M_{\alpha_1} \oplus \ldots \oplus M_{\alpha_k}$.

Using projections π_α determined by the direct sum decomposition of M we get:

$$N' \subset \pi_{\alpha_1}(N') \oplus \pi_{\alpha_2}(N') \oplus \ldots \oplus \pi_{\alpha_k}(N')$$

Since M_α is irreducible for any α, $\pi_\alpha(N')$ submodule of M_α so equal to either 0 or M_α. In fact by Schur's Lemma, each $\pi_{\alpha_i}|_N$ homomorphism from N' to M_{α_i} (both of which are irreducible) will be either 0 or an isomorphism. Not all will be 0, as $N' \subset \pi_{\alpha_1}(N') \oplus \ldots \oplus \pi_{\alpha_k}(N')$.

If $N' \cong N$ then $N' \subseteq$sum of some of the $M_\alpha$that are isomorphic to N. As if $M_{\alpha_i} \cong N'$ ($\pi_{\alpha_i}|_{N'_i}$=isomorphism). Then $M_{\alpha_i} \cong N' \cong N$. So N' is indeed contained in $\bigoplus_{M_\alpha \cong N} M_\alpha$. ■

Chapter 5

Structure theory of rings

5.1 Structure theory

Any left R-module, M gives rise to a representation $\rho : R \to \mathrm{End}M$ by defining: $\rho(a)x = a \cdot x$. Likewise, every representation of R into additive group M determines an action of R on M turning it into an R-module.
$\ker \rho = \{b \in R \mid \ b \cdot M = 0\} = \mathrm{ann}_R M$ 2-sided ideal in R.

Definition 5.1.1 ρ is a faithful representation if $\ker \rho = 0$.
M is a faithful module if $\mathrm{ann}_R M = 0$.

For any $x \in M$ define: $\mathrm{ann}_R x = \{a \in R \mid \ ax = 0\}$. This is a left ideal in R.

Definition 5.1.2 A representation ρ is called irreducible if the corresponding module is irreducible.

Claim 5.1.3

$\mathrm{ann}_R M = \bigcap\limits_{x \in M} \mathrm{ann}_R x$.

Claim 5.1.4

$Rx \cong {}^{R}/_{\mathrm{ann}_R x}$ (as left R-module).

Definition 5.1.5

1. R is primitive if it has a faithful irreducible representation.
2. R is semi-primitive if for any $a \neq 0$ in R there exists an irreducible representation ρ s.t. $\rho(a) \neq 0$.

Clearly, primitive$\Rightarrow s$ semi-primitive.

Definition 5.1.6 R is a sub-direct product of rings $\{R_\alpha\}_{\alpha \in A}$ if R can be embedded in $\prod\limits_{\alpha} R_\alpha$. $i : R \hookrightarrow \prod\limits_{\alpha} R_\alpha$, s.t. if p_α is projection, $p_\alpha : \prod\limits_{\alpha \in R} R_\alpha \to R_\alpha$, then $i_\alpha = p_\alpha i$ is surjective from R onto R_α.

Example 5.1.7 () R is a sub-direct product of R with R, $a \in R$, $a \overset{i}{\mapsto} (a, a)$ embeds R in $R \times R$.
$p_1(a, b) = a$.
$p_2(a, b) = b$.

Example 5.1.8 () $\mathbb{Z}$ is a sub-direct product of fields $\{{}^{\mathbb{Z}}/_{p\mathbb{Z}}\}_{p \text{ prime}}$. $i : \mathbb{Z} \to \prod\limits_{p \text{ prime}} {}^{\mathbb{Z}}/_{p\mathbb{Z}}$. $i(n) = (n(\mod p))_p = p$th coordinate.
Clearly if π_p projection of $\prod\limits_{p \text{ prime}} ({}^{\mathbb{Z}}/_{p\mathbb{Z}})$ onto ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$. Then $i\pi_p =$ surjective.

Proposition 5.1.9

The following conditions on a ring are equivalent:

1. *R is semi-primitive.*
2. *R has a faithful completely reducible representation/module.*
3. *R is a sub-direct product of primitive rings.*

Proof: $1 \Rightarrow 2$: For any $a \neq 0$ in R let M_a be an irreducible module s.t. $a \cdot M_a \neq 0$ (or equivalently $\rho_{M_\alpha}(a) \neq 0$) . Look at $M = \bigoplus\limits_{a\neq 0} M_a$. By definition, it is a completely reducible. Let $b \in R$ and assume $b \cdot M = 0$ then $bM_a = 0$ for all $a \in R$ but $b \cdot M_b \neq 0$ contradiction.

$2 \Rightarrow 3$:

Let $M = \bigoplus\limits_{\alpha} M_\alpha$, M_α irreducible and $\text{ann}_R M = 0$. Note that:

$$0 = \text{ann}_R M = \bigcap_\alpha \text{ann}_R M_\alpha$$

Since M_α is irreducible. Let $R_\alpha = {}^{R}\!/_{\text{ann}_R M_\alpha}$ (the $\text{ann}_R M_\alpha$ is a two sided ideal). We can regard M_α as in R_α-module by defining: $(a + \text{ann}_R M_\alpha)\, x = ax$ for $x \in M_\alpha$, $a \in R$. This is well-defined as if $a + R_\alpha = a' + R_\alpha$ then $a - a' \in \text{ann}_R M_\alpha$ so that $(a - a')\, x = 0\ \forall x \in M_\alpha$ and $ax = a'x$.

M_α is a faithful R_α-module, so R_α is a primitive ring. $i : R \to \prod\limits_\alpha R_\alpha$, natural embedding: $i(a)_\alpha = a + \text{ann}_R M_\alpha \in R_\alpha$. i is 1-1 as $\bigcap\limits_\alpha \text{ann}_R M_\alpha = 0$ and $i_\alpha = p_\alpha \cdot i$ is surjection onto R_α, $p_\alpha : i_\alpha R_\alpha \to R_\alpha$.

$3 \Rightarrow 1$: Suppose $i : R \to \prod\limits_\alpha R_\alpha$ embedding, R_α is primitive and if p_α projection of $\prod\limits_\alpha R_\alpha$ onto R_α then $p_\alpha i$ is surjection.

For every α we have an irreducible faithful R_α-module: M_α. Suppose the representation associated with this is ρ_α. Let $a \neq 0$ in R:

$$\bigcap_\alpha \ker \rho_\alpha i_\alpha \underbrace{=}_{\rho_\alpha \text{is faithful, so } \ker \rho_\alpha = 0} \bigcap_\alpha \ker i_\alpha = 0$$

as if $b \in \bigcap\limits_\alpha \ker i_\alpha = 0$ then $i_\alpha(b) = 0$ for all α, so $p_\alpha(i(b)) = 0$ for all α.

p_α projection form $\prod\limits_\alpha R_\alpha \to R_\alpha$ so $p_\alpha(i(b)) = 0$ for all $\alpha \iff i(b) = 0 \iff b = 0$. $\rho_\alpha i_\alpha : R \to \text{End} M_\alpha$ is a representation of R.

Now let $a \neq 0$ in R then as $\bigcap\limits_\alpha \ker \rho_\alpha i_\alpha = 0$, we must have some α s.t. $a \notin \ker \rho_\alpha i_\alpha$ so $\rho_\alpha i_\alpha(a) \neq 0$. So R is semi-primitive. ■

An “internal” characterization of primitive and semi-primitive:

Definition 5.1.10 Let I be a left ideal of R, $(I : R) = \{b \in R \mid\ bR \subseteq I\}$.

Lemma 5.1.11

$I \supseteq (I : R)$ and $(I : R)$ is a two-sided ideal.

Proof: Suppose $K \subseteq I$, 2-sided ideal, then for any $b \in K$: $bR \subseteq K \subseteq I$ so $b \in (I : R)$. So $(I : R) =$ the largest 2-sided ideal contained in I.

Now note that $(I : R)$ is clearly additive, and it is multiplicative, hence it is a two-sided ideal. ■

Claim 5.1.12

If $M \cong {}^{R}\!/_{I}$ (isomorphism as left R-modules) then $\text{ann}_R M = (I : R)$.

Proof: If $b \in (I : R)$.

Remarks 5.1.13 M can be regarded as an R-module by defining $ax = a(r+I) = ar + I$ for $r + I = x \in M$, $r \in R$, $a \in R$, we can show it is well-defined.

So $bR \subseteq I$, so $b(r+I) = \underbrace{br}_{\in I} + I = I$. So $bM = 0$ and $b \in \operatorname{ann}_R M$. Conversely if $b \in \operatorname{ann}_R M$ then for any $r \in R$, $br \in I$ and so $bM = 0$. ■

Claim 5.1.14

1. *R is primitive if and only if R contains a maximal left ideal I containing no nonzero two-sided ideal.*
2. *R is semi-primitive if and only if $R \neq 0$ and $\bigcap_{I\text{maximal left ideal}} (I : R) = 0$.*

Proof:

1. If R is primitive we have an irreducible module M and $\operatorname{ann}_R M = 0$. By previous claim $R/I \cong M$ for some maximal left ideal in R. $0 = \operatorname{ann}_R M = (I : M)$ and so I contains no nonzero two-sided ideal. Converse: read from end to beginning.
2. Suppose $R \neq 0$ and $\bigcap_{I\text{maximal left ideal in } R} (I : R) = 0$. For I a maximal left idea R/I would be an irreducible R-module. We form the direct sum: $\bigoplus_{I\text{maximal left ideal}} R/I = M$. $\operatorname{ann}_R M = \bigcap_{I\text{maximal left ideal in } R} \operatorname{ann}_R (R/I) = \bigcap_{I\text{maximal left ideal in } R} (I : R) = 0$ by assumption. So, for any $0 \neq a \in R$ we have some maximal left ideal I s.t. $a \notin (I : R)$ and so $a \notin \operatorname{ann}_R (R/I)$ so R is semi-primitive.
   Conversely, if R is semi-primitive then for any $a \neq 0$ in R we have an irreducible module M_a s.t. $a \cdot M_a \neq 0$. So we have a maximal left ideals I_a s.t. $R/I_a \cong M_a$. Since $aM_a \neq 0$ we must have that: $\bigcap_{0\neq a\in R} \operatorname{ann}_R M_a = 0$. $\bigcap_{0\neq a\in R} \operatorname{ann}_R M_a = \bigcap_{0\neq a\in R} (I_a : R) = 0$ but note that it is trivial that: $\bigcap_{I\text{maximal left ideal}} (I : R) \subseteq \bigcap_{0\neq a\in R} (I_a : R)$ hence $\bigcap_{I\text{maximal left ideal}} (I : R) = 0$.

■

Corollary 5.1.15

R is simple→R is primitive.

Remarks 5.1.16 Converse is not true - example later.

Corollary 5.1.17

If R is commutative:

1. *R is primitive if an only if R is a field (if and only if R is simple).*
2. *R is semi-primitive if and only if R is a sub-direct product of fields.*

✎**Example 5.1.18 ()** $\mathbb{Z}$ is a sub-direct product of $\mathbb{Z}/p\mathbb{Z}$, p is primitive. $i : \mathbb{Z} \hookrightarrow \prod_{p\text{prime}} \mathbb{Z}/p\mathbb{Z}$, so $\mathbb{Z}$ is a semi-primitive ring.

5.2 Jacobson Radical

Definition 5.2.1 $J(R) = \text{Jacobson radical} = \bigcap_{\rho\text{irreducible representation}} \ker \rho$.

$J(R)$ is a two-sided ideal of R (intersection of two-sided ideals).

Definition 5.2.2 if $P \triangleleft R$ ideal in R we say it is a primitive ideal if ${}^{R}\!/_{P}$ is primitive ring.

✎**Example 5.2.3 ()** If P is a maximal ideal then it is primitive.

Lemma 5.2.4

$P \triangleleft R$ is a primitive ideal if and only if $P = (I : R)$ where I is some maximal left ideal in R.

Proof: If $P = (I : R)$, I a maximal left ideal in R then $M = {}^{R}\!/_{I}$ is irreducible R-module. $\text{ann}_R M = (I : R) = P$. Regard M as an ${}^{R}\!/_{P}$-module by defining for $x \in M,\ a \in R$:

$$(a + P)\, x = ax$$

It is well-defined as if $a + P = a' + P \Rightarrow \underbrace{(a - a')}_{\in P = \text{ann}_R M} x = 0$ so $ax = a'x$. M is a faithful ${}^{R}\!/_{P}$ module and irreducible.

So ${}^{R}\!/_{Y}$ is a primitive ring.

Converse: Let $P \triangleleft R$ be a primitive ideal. So ${}^{R}\!/_{I}$ is a primitive ring. So it has a faithful irreducible module M. Regard M as an R-module by defining $x \in M,\ a \in R\ ax = (a + P)\, x$. $\text{ann}_R M = P$ as M is a faithful ${}^{R}\!/_{P}$-module (as it's an irreducible ${}^{R}\!/_{P}$-module).

M is an irreducible R-module, so corresponds to some maximal left ideal I s.t. ${}^{R}\!/_{I} \cong M$. And then as before $P = \text{ann}_R\left({}^{R}\!/_{I}\right) = (I : R)$. ■

Claim 5.2.5

1. *$J(R) = \bigcap_{P \text{primitive ideal in } R} P$.*
2. *$J(R) = \bigcap_{I \text{maximal left ideal of } R} I$.*

Proof:

1. By defining:

$$\begin{aligned} J(R) &= \bigcap_{\rho \text{irreducible representations}} \ker \rho \\ &= \bigcap_{M \text{irreducible } R\text{-modules}} \text{ann}_R M \\ &= \bigcap_{I \text{maxaimal left ideal}} \text{ann}_R\left({}^{R}\!/_{I}\right) \\ &= \bigcap_{I \text{maxaimal left ideal}} (I : R) \\ &= \bigcap_{P \text{primitive itdeal in } R} P \end{aligned}$$

2. Note that $\text{ann}_R M = \bigcap_{0 \neq x \in M} \text{ann}_R x$ ($\text{ann}_R x$ = left ideal). $J(R) = \bigcap_{M \text{irreducible } R\text{-modules}} \text{ann}_R M$. If M is irreducible and $x \in M,\ x \neq 0$ then $\text{ann}_R x$ = maximal left ideal as map φ sending $a \in R$ to ax has $\text{ann}_R x = \ker \varphi$, φ is surjective and $M \cong {}^{R}\!/_{\text{ann}_R x}$ ($\text{ann}_R x$ = maximal left ideal). So:

$$J(R) = \bigcap_{M \text{irreducible } R\text{-modules}} \text{ann}_R M = \bigcap_{M \text{irreducible } R\text{-modules}} \left(\bigcap_{0 \neq x \in M} \text{ann}_R x \right)$$

But it's clear that:

$$\bigcap_{M \text{irreducible } R\text{-modules}} \left(\bigcap_{0 \neq x \in M} \text{ann}_R x \right) \supseteq \bigcap_{I \text{maximal left ideal}} I$$

(because each $\operatorname{ann}_R x$ is a maximal left ideal). On the other hand, Left ideal $I \supseteq (I:R)$ so:

$$\bigcap_{I\text{maximal left ideal}} I \supseteq \bigcap_{I\text{maximal left ideal}} (I:R) \underbrace{=}_{\text{previous lemma}} \bigcap_{P\text{primitive}} P \overbrace{=}^{\text{part 1}} J(R)$$

■

Example 5.2.6 () $\mathbb{Z}$. $I = \max$ (left) ideal $\iff I = p\mathbb{Z}$ with p prime.

$$\bigcap_{I\text{maximal left ideal}} I = \bigcap_{p\text{prime}} p\mathbb{Z} = 0$$

So $J(\mathbb{Z}) = 0$.

10/06/2014

Theorem 5.2.7

1. *R is semi-primitive if and only if $J(R) = 0$ (follows from the fact that R is semi-primitive $\iff \bigcap_{I\text{maximal left ideal}} (I:R)$.*
2. *If $R \neq 0$, R/J is semi-primitive (i.e. $J(R/J) = 0$) and if B is an ideal s.t. R/B is semi-primitive then $B \supseteq J$.*

Proof:

1.
2. Given any ideal $B \triangleleft R$, $\overline{R} = R/B$. Every ideal $\overline{P} \triangleleft \overline{R}$ correspond to an ideal P of R s.t. $P \supseteq B$ and $\overline{R}/\overline{P} \cong R/P$. If P is primitive ideal then we have R/P primitive $\iff \overline{R}/\overline{P}$ primitive $\iff \overline{P}$ primitive in $\overline{R}$.
Now, suppose that R/B is semi-primitive. So
$$J(R/B) = 0 \Rightarrow \bigcap_{\overline{P}\text{primitive in } R/B} \overline{P} = 0 \Rightarrow \bigcap_{\substack{P\text{primitive in } R\\ P \supseteq B}} P/B = 0 \Rightarrow \bigcap_{\substack{P\text{primitive in } R\\ P \supseteq B}} P/B = 0$$
So we get $\bigcap_{\substack{P\text{primitive in } R\\ P \supseteq B}} P = B$ so $B \supseteq J = \bigcap_{\substack{P\text{primitive in } R\\ P \supseteq B}} R$.
Now look at $\tilde{R} = R/J$, by previous calculation:
$$J\left(\tilde{R}\right) = \bigcap_{\tilde{P}\text{primitive in } \tilde{R}} \tilde{P} = \bigcap_{\substack{P\text{primitive in } R\\ P \supseteq J}} P/J \underbrace{=}_{\text{every primitive ideal} \supseteq J}$$
$$\bigcap_{P\text{primitive in } R} P/J = \bigcap_{P\text{primitive in } R} P/J = J/J = 0$$

■

Recall: we say that R is local if the set of non-units = a 2-sided ideal.

Theorem 5.2.8

Let $R \neq 0$ be a ring. Then the following are equivalent:

1. *R is local.*
2. *$J(R)$ is the set of non-units.*
3. *$\exists!$ maximal left ideal.*

4. *$\exists!$ maximal right ideal.*

Remarks 5.2.9 If R is local then $\exists!$ maximal 2-sided ideal.

Proof: We will prove that $4 \Rightarrow 3$ later on. And it is trivial that $2 \Rightarrow 1$. We want to show that $1 \Rightarrow 3$:

Let I =set of non-units. So I is a maximal left ideal and clearly the only one.

$3 \Rightarrow 2$:

$$J(R) = \bigcap_{I \text{maximal left ideals}} I = \text{the unique maximal left ideal}$$

Clearly $J(R) \subseteq$set of non units.

Let x be a non-unit. Assume $x \notin J(R)$, Rx is a left ideal as $Rx \nsubseteq J(R)$ must have $Rx = R$, So x is left invertible. So we have $y \in R$ s.t. $yx = 1$.

Look at Ry, if $Ry = R$ then y is 2-sided invertible, and its right inverse, x, will also be its left inverse meaning that x is a unit - contradiction. So Ry is a proper left ideal and so contained in $J(R)$. So $y \in J(R)$, so $1 = y \cdot x \in J(R)$ - contradiction.

$3 \Rightarrow 4$:

Since $J(R)$ =the intersection of all maximal left ideal, we have that $J(R) =$ the unique maximal left ideal.

$J(R)$ is also a right ideal, Let I' be a maximal right ideal containing $J(R)$ we want to show that it is the only maximal right ideal.

Suppose I'' is a maximal right ideal and $I'' \neq I'$. Let $x \in I'' \backslash I'$, so $x \notin J(R)$ (since $J(R) \subseteq I'$).

As before if $Rx = R$ so $\exists y \in R$ s.t. $yx = 1$ so x as an element in I'' cannot be right invertible. So Ry is a proper left ideal. This gives $Ry \subseteq J(R)$ so $y \in J(R)$ and $yx = 1 \in J(R)$ a contradiction. ■

5.2.1 An element characterization of $J(R) = J$

Definition 5.2.10 For $z \in R$, R a ring:

1. z is left quasi-regular if $1 - z$ is left invertible in R. (z is right quasi-regular if $1 - z$ is right invertible in R respectively).
2. z is quasi-regular if it is both left and right quasi-regular.
3. An ideal is left (right respectively) quasi-regular if all its elements are left (right respectively) quasi-regular.

✎**Example 5.2.11 ()** If z is nilpotent that z is quasi-regular:

$$(1 - z)\left(1 + z + z^2 + \ldots + z^k\right) = 1$$

If $z^{k+1} = 0$.

Theorem 5.2.12

1. *$J(R)$ is a left quasi-regular ideal and it contains every left quasi-regular ideal.*
2. *$J(R) = \{z \in R \mid\ az$ is left quasi-regular for all $a \in R\}$.*
3. *Every element of $J(R)$ is both left and right quasi-regular.*

1. "right" version of (1).*

2. "right" version of (2).*

Proof:

1. Let $z \in J(R)$, Suppose that it is not a left quasi-regular, so $1-z$ is not left invertible so $R(1-z) \neq R$. So $R(1-z) \subseteq I_0$, I_0 is a maximal left ideal. So $1-z \in I_0$ but also $z \in I_0$ as $J(R) \subseteq I_0$ So $1=(1-z)+z \in I_0$, a contradiction.
   We shall show that if Z is a left quasi-regular ideal then $Z \subseteq J(R)$. Suppose not, So there exists some maximal left ideal I s.t. $Z \not\subseteq I$. Because I is maximal, $I+Z=R$, so we can write $1=b+z$. With $b \in I$ and $z \in Z$, so z is left quasi-regular. So $b=1-z$ is left invertible but then $Rb=R$ but $Rb \subseteq I$ a contradiction. So $Z \subseteq J(R)$.

2. By (1) all elements of $J(R)$ are left quasi-regular and if $z \in J(R)$ so is az for all $a \in R$ and so az will be left quasi-regular as well.
   Now, assume az is left quasi-regular for all $a \in R$. So Rz is a left quasi-regular ideal, so by (1), $Rz \subseteq J(R)$ so $z \in J(R)$.

3. Let $z \in J(R)$. We need to show that $1-z$ is right invertible. Since $1-z$ is left invertible we have $s \in R$ s.t. $s(1-z)=1$. Let $y=1-s$, we have:

$$1=(1-y)(1-z)=1-y-z+yz \Rightarrow y+z=yz \text{ or } (y-1)z=y$$

   So y is a multiple of $z \in J(R)$ and so $y \in J(R)$. So y is left quasi regular so $1-y=s$ is left invertible. And so s is the 2-sided inverse of $1-z$ and so z is quasi-regular.

1*,2*. We can now define a so-called “right” Jacobson radical.

$$J' = \bigcap_{I' \text{maximal right ideal}} \qquad I' = \bigcap_{P' \text{"right primitive" ideal}} \qquad P' = \{z \mid \ za \text{ right quasi regular for all } a \in R\}$$

By all previous theorems on left ideal and (3) we have that J' is also a left quasi-regular ideal (we can repeat 3 on the other direction). But J contains all the left quasi-regular ideals so we get $J \supseteq J'$. Since J' is a right quasi-regular ideal (1*) and (2*) are true for J', we can have (1*) for J' i.e. J' contains every right quasi-regular ideal. But J is also a right quasi-regular ideal, So $J \subseteq J'$ and $J=J'$.

■

Corollary 5.2.13

R “left semi-primitivity” is equivalent to “right semi-primitivity”.

5.2.2 Example of a primitive ring that is not simple

Let V be an infinite dimensional vector space over a division ring Δ. Left $L=\mathrm{End}_\Delta V$ =linear operators on V over Δ.

We shall show that L acts faithfully and irreducibly on V. The representation is identity map - so faithful.

To show irreducibility we need to show that if we have and element $x \in V$ s.t. $x \neq 0$ then $Lx=V$. But if $y \in V$, we have a linear operator mapping x to y.

We show L is not simple. Let $I_0=\{l \in L \mid \ l(V) \text{ is finite dimension}\}$. We shall show that I_0 is a non-trivial ideal. Clearly $I_0 \neq 0, L$.

If $\varphi, \psi \in I_0$ then $(\varphi+\psi)(V)$ =finite dimension. Now let $\varphi \in I_0$, $l \in L$.

$$l(\varphi(V)) = \text{image of a finite dimension subspace under } l\text{- so also finite dimension}$$

$$\varphi(l(V)) \subseteq \varphi(V) = \text{finite dimension.}$$

So $\varphi l \in I_0$ and $l\varphi \in I_0$

Remarks 5.2.14 One can show that I_0 is a minimal ideal.

If $\dim_\Delta V = \aleph_0$ then I_0 is the only 2-sided ideal in L so ${}^{L}\!/{}_{I_0}$ is simple.

If $\dim_\Delta V > \aleph_0$ then we also have an ideal $I_1 \supseteq I_0$ and $I_1=\{l \in L \mid \ l(V) \text{ has countable dimension}\}$. 17/06/2014

Chapter 6

Density

6.1 Density theorem for completely reducible modules

Theorem 6.1.1 (*Density theorem for completely reducible modules*)

Let M be a completely reducible R-module.
Denote:

$$\begin{aligned} R' &= \mathrm{End}_R M \\ R'' &= \mathrm{End}_{R'} M = \{\varphi \in \mathrm{End} M \mid \varphi \text{ commutes with all Rendomorphisms}\} \end{aligned}$$

Let $\{x_1, \ldots, x_n\} \in M$ and $a'' \in R''$ then there exists $a \in R$ s.t. $a'' x_i = a x_i$ for all $i \leq i \leq n$.

In order to prove this theorem we use 2 lemmas:

Lemma 6.1.2

Let M completely reducible, If N is an R-submodule of M then N is an R''-submodule.

Proof: We know that M is completely reducible hence we have an R-submodule P s.t. $P \oplus N = M$. Let e be the projection of M onto N w.r.t the decomposition. $e(M) = N$. As N and P are R-submodules, e is an R-endomorphism. That is: $e \in R'$. Let $a'' \in R''$:

$$a''(N) = a''(e(M))$$

But a'' commutes with every R-endomorphism, in particular with e hence:

$$= e(a''(M)) \subseteq e(M) = N$$

■

Lemma 6.1.3

Let M be a module. $M^{(n)} = \underbrace{M \oplus \ldots \oplus M}_{n}$. Then $\mathrm{End}_R M^{(n)}$ =set of maps $(u, \ldots, u_n) \mapsto (v_1, \ldots, v_n)$ where:

$$v_i = \sum a'_{i,j} u_j \qquad a'_{i,j} \in R' = \mathrm{End}_R M$$

It is easy to show that each such map is an element of $\mathrm{End}_R M^{(n)}$. We want to show that every element is of this form.

Proof: Let $\ell \in \mathrm{End}_R M^{(n)}$. For any vector $(u_1, \ldots, u_n) \in M^{(n)}$ denote:

$$\ell(0, \ldots, u_i, \ldots 0) = (u_{1,i}, \ldots, u_{n,i})$$

Let $a'_{j,i}$ be a map sending $u_i \mapsto u_{j,i}$. $x \in M$ $\ell\left(0,\ldots,\overbrace{x}^{i},\ldots 0\right) = a'_{j,i} = j$th component of $\ell\left(0,\ldots,x,\ldots 0\right)$.

We claim $a'_{j,i} \in R'$. If $a \in R$: $a'_{j,i}\left(ax\right) = j$th component of $\ell\left(0,\ldots,ax,\ldots,0\right) = \ell a\left(0,\ldots,x,\ldots 0\right) = a\ell\left(0,\ldots,x,\ldots,0\right) = aa'_{j,i}(x)$ the transition from $\ell a = a\ell$ is because ℓ is R-endomorphism).

$$\begin{aligned} \ell\left(u_1,\ldots,u_n\right) &= \sum_{i=1}^{n}\ell\left(0,\ldots,u_i,\ldots,0\right) \\ &= \sum_{i=1}^{n}\left(a'_{1,i}u_i, a'_{2,i}u_i,\ldots,a'_{n,i}u_i\right) \\ &= \left(\sum_{i=1}^{n}a'_{1,i}u_i,\ldots,\sum_{i=1}^{n}a'_{n,i}u_i\right) \end{aligned}$$

as required. ■

6.1.1 Proof of the theorem

Recall that the theorem states:

Theorem 6.1.4 (*Density theorem for completely reducible modules*)

Let M be a completely reducible R-module.
Denote:

$$\begin{aligned} R' &= \mathrm{End}_R M \\ R'' &= \mathrm{End}_{R'} M = \{\varphi \in \mathrm{End} M \mid \varphi \textit{ commutes with all Rendomorphisms}\} \end{aligned}$$

Let $\{x_1,\ldots,x_n\} \in M$ and $a'' \in R''$ then there exists $a \in R$ s.t. $a''x_i = ax_i$ for all $i \leq i \leq n$.

We want to prove this theorem using the lemmas we've just shown. **Proof:** For $n = 1$ we have $x \in M$ (completely reducible module), $a'' \in R''$. We need $a \in R$ s.t. $a''x = ax$.

Look at $Rx = R$-submodule of M. So by lemma 6.1.2 it is an R''-submodule. So $a''x \in Rx$ so $\exists a \in R$: $a''x = ax$.

For arbitrary n we use the case for $n = 1$ w.r.t module $M^{(n)}$ (and use the lemma 6.1.3).

$M^{(n)}$ is also completely reducible. Let $x_1,\ldots,x_n \in M$, $a'' \in R''$ and define $\varphi \in \mathrm{End}M^{(n)}$: $(x_1,\ldots,x_n) \mapsto (a''x,\ldots,a''x_n)$. φ will be an element of $\mathrm{End}_{\mathrm{End}_R M^{(n)}} M^{(n)}$. Since elements of $\mathrm{End}_R M^{(n)}$ are, by lemma 6.1.3 , defined by matrices of elements in $\mathrm{End}_R M = R'$ and a'' commutes with each a'_{ji} so $\exists a \in R$ s.t.

$$\begin{aligned} \left(ax,\ldots,ax_n\right) = a\left(x_1,\ldots,x_n\right) &= \varphi\left(x_1,\ldots,x_n\right) \\ &= \left(a''x_1,\ldots,a''x_n\right) \end{aligned}$$

■

6.2 Another definition of density

Definition 6.2.1 Let V be a vector space over a division ring Δ, $S \subseteq \mathrm{End}_\Delta V$ =linear transformations on V is called **dense** in $\mathrm{End}_\Delta V$ if given $x_1,\ldots,x_n \in V$ linear independent over Δ and $y_1,\ldots,y_n \in V$ there exists $\varphi \in S$ s.t. $\varphi\left(x_i\right) = y_i$.

Remarks 6.2.2 If V is finite dimensional, the **only** dense set in $\mathrm{End}_\Delta V$ is itself (as taking $x_1,\ldots,x_n$ to be a basis $\exists!\varphi \in \mathrm{End}_\Delta V$ mapping bases to any set of n elements).

6.2.1 Density theorem for primitive rings

Theorem 6.2.3 (***Density theorem for primitive rings***)

R is primitive if and only if R is isomorphic to a dense ring of linear transformation in a vector space over a division ring.

Proof: If R is primitive, we have M irreducible module and representation $\rho : R \to \text{End}M$ with trivial kernel (so M is faithful irreducible module). By Schur's Lemma we know that $\text{End}_R M$ is a division ring which we call Δ. $R \cong \rho(R)$ is a subring of $\text{End}M$ but in fact is a subring of $\text{End}_\Delta M$ as if $\varphi \in \Delta$ and $a \in R$, $x \in M$ then:

$$a\varphi(x) \underbrace{=}_{\varphi \in \text{End}_R M} \varphi(ax)$$

So $R \hookrightarrow \text{End}_\Delta M$. It remains to show that R is dense in $\text{End}_\Delta M$. Let $x_1, \ldots, x_n \in M$ linear independent over Δ and $y_1, \ldots, y_n \in M$ arbitrary. $\exists \ell$ linear transformation in $\text{End}_\Delta M$ s.t. $\ell(x_i) = y_i$, $1 \leq i \leq n$. By our last theorem (Density theorem for completely reducible modules), since M is a completely reducible module as it is irreducible, we have $a \in R$ s.t. $a(x_i) = y_i$, $\leq i \leq n$. So it is dense.

Now, assume $R \cong$dense ring of linear transformation in a vector space M over a division ring Δ. Regard M as an R-module by defining $ax = \rho(a)x$, $x \in M$. M will be irreducible as if $x \in M \neq 0$ and arbitrary $y \in M$. As R is dense, we have $a \in R$ s.t. $ax = y$, so $Rx = M$. M is faithful as ρ is given as an isomorphism. ■

Chapter 7

Structure theorems

7.1 Structure theorem for primitive artinian rings

Theorem 7.1.1 (***Structure theorem for primitive artinian rings***)

The following conditions on a nonzero ring R are equivalent:

1. *R is simple and left-artinian.*
2. *R is primitive and left-artinian.*
3. *$R \cong \mathrm{End}_{\Delta} M$, M is finite dimension vector space over a division ring Δ.*

The $1 \iff 3$ is known as the Wedderburn-Artin theorem for simple artinian rings. Note that we already know that $1 \Rightarrow 2$ as we've seen simple$\Rightarrow$primitive. **Proof:** We first show $2 \Rightarrow 3$:

As in previous theorem, we have M faithful irreducible module, $\Delta = \mathrm{End}_R M$ division ring and $R \cong$dense ring of linear transformations of M over Δ.

If we show M finite dimension then $R \cong \mathrm{End}_{\Delta} M$ as it is dense in $\mathrm{End}_{\Delta} M$.

Now, suppose M infinite dimension over Δ, so we have infinite linear independent set $x_1, \ldots, x_n, \ldots$. Let $I_j = \mathrm{ann}_R\left(x_j\right)$, These are left ideals in R: $I_1 \cap \ldots, \cap I_n = \mathrm{ann}_R\left\{x_1, \ldots, x_n\right\}$. There exists a linear transformation in $\mathrm{End}_{\Delta} M$ sending $x_1, \ldots, x_n$ to 0 and x_{n+1} to a nonzero element. As R is dense in $\mathrm{End}_{\Delta} M$ we have $a \in R$ s.t. $\begin{cases} ax_i = 0 & 1 \leq i \leq n \\ ax_{n+1} \neq 0 \end{cases}$. So $a \in I_1 \cap \ldots \cap I_n$ but $a \notin I_1 \cap \ldots \cap I_{n+1}$. So we get a properly descending sequence of left ideals, contradiction to the artinian property.

We now want to show that $3 \Rightarrow 1$:

Suppose $R = \mathrm{End}_{\Delta} M$, M finite dimensional over a division ring Δ. So by assignment 4 this ring is simple! It is an artinian ring as R finite dimensional over Δ as well! ■

Remarks 7.1.2 $\mathrm{End}_{\Delta} M$ are anti-isomorphic to $M_n(\Delta)$ where $n = \dim_{\Delta} M$. $\varphi \iff A$, $\psi \iff B$ we can show that $\varphi\psi \iff \left(B^T A^T\right)^T$ only if Δ commutative we get $B^T A^T (AB)^T$.

08/07/2014

Chapter 8

Hilbert's Nullstellensatz

8.1 Definition

Let $F \subseteq E$ be fields. $R = F[X_1, \ldots, X_n]$.

Definition 8.1.1 Given $\vec{x} = (x_1, \ldots, x_n) \in E^n$ denote $f(\vec{x}) = f(x_1, \ldots, x_n)\,,\ f \in R$. Given $Q \subset R$ denote:

$$\mathrm{Zer}\,(Q) = \{\vec{x} \in E^n \mid\ f\,(\vec{x} = 0\ \forall f \in Q)\} = \text{Variety determined by } Q$$

Definition 8.1.2 A set $A \subseteq E^n$ is called algebraic if it is of the form $\mathrm{Zer}\,(Q)$ for some $Q \subset R$.

Example 8.1.3 () $\mathrm{Zer}\,(\{0 = 0_R\}) = E^n$.

Example 8.1.4 () $\mathrm{Zer}\,(R) = \varnothing$.

Example 8.1.5 () If $E = F$, then $\{(x_1, \ldots, x_n)\} = \mathrm{Zer}\,(\{X_i - x_i \mid 1 \leq i \leq n\})$.

Example 8.1.6 () $R = \mathbb{Q}\,[X, Y]$, . Then:

$$\mathrm{Zer}\left(\left\{Y - X^2\right\}\right) = \text{parabola } y = x^2\text{in } \mathbb{R}^2$$

Lemma 8.1.7

The collection of algebraic sets in E^n is closed under finite unions and arbitrary intersections.

Proof: If $A_\alpha = \mathrm{Zer}\,(Q_\alpha)$ then:

$$\bigcap A_\alpha = \mathrm{Zer}\left(\bigcup Q_\alpha\right)$$

$\mathrm{Zer}\,(Q_1) \cup \mathrm{Zer}\,(Q_2) = \mathrm{Zer}\,(\{f \cdot g \mid\ f \in Q_1, g \in Q_2\})$. ■

Definition 8.1.8 Zariski Topology on E^n: Closed sets $=$ algebraic sets.

Theorem 8.1.9

If $F \subseteq \overline{F} \subseteq E$. If A algebraic set over F in $\overline{F}^n$ then there exists a unique algebraic set B in E^n s.t. $B \cap \overline{F}^n = A$.

Remarks 8.1.10 B doesn't have to be equal to A. For example, consider the zero polynomial.

We shall prove this theorem later, first we will see some corollaries.

Corollary 8.1.11

If $S \subseteq E^n$ be a nonempty algebraic set over F. $F \subseteq E$, E algebraic closed. Then S contains a point all of whose coordinates are algebraic over F.

Proof: (of the corollary)

Suppose $S \cap \overline{F}^n = \varnothing$.

Then S and $\varnothing$ are 2 distinct sets over F in E^n with equal intersections. Contradiction to the uniqueness in thm, taking $A = \varnothing$. ■

Definition 8.1.12 Let $A \subseteq E^n$. $\mathrm{Pol}\,(A) = \{f \in R \mid \ f\,(\vec{x}) = 0 \ \vec{x} \in A\}$ (or $I\,(A)$)

Lemma 8.1.13

If A is algebraic then:
$\mathrm{Zer}\,(\mathrm{Pol}\,(A)) = A$.

Remarks 8.1.14 $\mathrm{Zer}\,(\mathrm{Pol}\,(A)) \supseteq A$ always, even if A is not algebraic.

Proof: If $\vec{x} \in A$, $f\,(\vec{x}) = 0$ for all $f \in \mathrm{Pol}\,(A)$ so $\vec{x} \in \mathrm{Zer}\,(\mathrm{Pol}\,(A))$.

Now show the converse.

As A algebraic, there exists $Q \subseteq R$ s.t. $A = \mathrm{Zer}\,(Q)$. If $f \in Q$ then $f\,(\vec{x}) = 0$ for all $\vec{x} \in A$. So $f \in \mathrm{Pol}\,(A)$, so $Q \subseteq \mathrm{Pol}\,(A)$.

Clearly, for any $B, C \subseteq R$:

$$B \subseteq C \to \mathrm{Zer}\,(B) \supseteq \mathrm{Zer}\,(C)$$

Applying it to $Q \subseteq \mathrm{Pol}\,(A)$ we get that:

$$A = \mathrm{Zer} Q \supseteq \mathrm{Zer}\,(\mathrm{Pol}\,(A))$$

which completes the proof. ■

Remarks 8.1.15 $\mathrm{Pol}\,(A)$ is always an ideal.
So the lemma implies that every algebraic set is of the form $\mathrm{Zer}\,(I)$ for some ideal I in R.

Corollary 8.1.16

Every algebraic set is of the form $\mathrm{Zer}\,(Q)$ where Q is a finite set of polynomials.

Proof: By the Hilbert's basis theorem (which we won't prove in class, but it can be found in Isaacs: Graduate Algebra page 434).

If R is noetherian then so is $R\,[x]$.

And inductively we get that $F\,[X_1, \ldots, X_n]$ is noetherian, F is a field.

So we have that our ring $R = F\,[x_1, \ldots, x_n]$ is noetherian.

So if A is an algebraic set and $A = \mathrm{Zer}\,(I)$. $I \triangleleft R$ then I is finitely generated by a finite set Q in R and $A = \mathrm{Zer}\,(Q)$. ■

8.2 The Nullstellensatz

Theorem 8.2.1 (*Nullstsllensatz*)

Let $R \supseteq F$, E is algebraic closed.
Let I ben an ideal in $R = F\,[X_1, \ldots, X_n]$ then $\mathrm{Pol}\,(\mathrm{Zer}\,(I)) = \sqrt{I}$.

$$\sqrt{I} = \mathrm{Nilrad}\,(I) = \{f \in R \mid \ \exists n \in \mathbb{N} \ f^n \in I\}$$

Remarks 8.2.2 $\sqrt{I} \subseteq \operatorname{Pol}(\operatorname{Zer}(I))$ as if $f \in R$ and $f^n \in I$ then for $\vec{x} \in \operatorname{Zer}(I)$, $f^n(\vec{x}) = (f(\vec{x}))^n = 0$. So as $\vec{x} \in E^n$ we must have $f(\vec{x}) = 0$ so $f \in \operatorname{Pol}(\operatorname{Zer}(I))$.

First we show the weak Nullstellensatz:

Theorem 8.2.3 (*The weak Nullstellensatz*)

If I is a proper ideal of $R = F[X_1, \dots, X_n]$, $F \subseteq E$ and E is algebraic closed then: $\operatorname{Zer}(I) \neq \varnothing$.

Proof: Direct proof: $I \underset{\neq}{\triangleleft} R$ (proper). There exists by Zorn a maximal ideal M of R containing I.

So ${}^{R}/_{M} = \overline{R}$ is a field. Clearly $M \cap F = \{0\}$ (as M contains no units). So we have an embedding of F in $\overline{R}$: $F \subseteq \overline{R}$.

Let $\alpha_i = X_i + M$. $R = F[X_i, \dots, X_n]$. So $\overline{R} = F[\alpha_1, \dots, \alpha_n]$.

So as $\overline{R}$ is a field we get that the α_i are algebraic over F. $F \subseteq \overline{R} \subseteq E$.

We claim $(\alpha_1, \dots, \alpha_n) \in \overline{R}^n \subseteq E^n$ is in fact an element of $\operatorname{Zer}(I)$ as if $f \in I$:

$$f(\alpha_1, \dots, \alpha_n) = f(X_1 + M, \dots, X_n + M) = \overline{f(X_1, \dots, X_n)} = \overline{0}$$

as $f \in I \subseteq M$. ■

We shall now prove the Nullstellensatz: **Proof:** Remains to show:

$$\operatorname{Pol}(\operatorname{Zer}(I)) \subseteq \sqrt{I}$$

Let $f \in \operatorname{Pol}(\operatorname{Zer}(I))$. Need to show $\exists n \in \mathbb{N}$: $f^n \in I$. Let T be a new indeterminate. Look at the ring $S = R[T] = F[X_1, \dots, X_n, T]$.

Detnote by $I[T] = \{g \in S \mid \text{ coeffs of } g \text{lie in } I\}$. This is clearly an ideal in S. Look at the ideal: $J = I[T] + (1 - T \cdot f) S$. We claim: $J = S$.

Suppose not, then J is a proper ideal and we can use the weak Nullstellensatz with respect to S. So applying the weak Nullstellensatz to $S = F[X_1, \dots, X_n, T]$ we have that $\operatorname{Zer}(J) \neq \varnothing$. So we have $(\alpha_1, \dots, \alpha_n, \beta) \in E^{n+1}$ in $\operatorname{Zer}(J)$.

$I \subseteq J$ so $\vec{\alpha} = (\alpha_1, \dots, \alpha_n) \in \operatorname{Zer} I$ $f \in \operatorname{Pol}(\operatorname{Zer}(I))$ so also $f(\vec{\alpha}) = 0$ but then as $1 - Tf \in J$ we get $1 \in J$ contradiction.

So we have:

$$S = I[T] + (1 - Tf) S$$

In particular, we have $u \in I[T]$, $v \in S = R[T]$.

$$1 = u + (1 - Tf) v$$

The above can be regarded as an identity over field of fraction of R: R^*.

$\frac{1}{f} \in R^*$ substitute in $1 = u + (1 - Tf) v$ in place of T:

$$1 = u\left(\frac{1}{f}\right) + \left(1 - \frac{1}{f} f\right) v \left(\frac{1}{f}\right)$$

So $u\left(\frac{1}{f}\right) = 1$.

Denote: $u(T) = a_n T^n + \ldots + a_1 T + a_0$, $a_i \in I$.

$$1 = a_n \frac{1}{f^n} + \ldots + a_1 \frac{1}{f} + a_0$$

$$f_n = \underbrace{a_n + a_{n-1} f + \ldots + a_1 f^{n-1} + a_0 f^n}_{\in I}$$

So $f^n \in I$ or $f \in \sqrt{I}$. ■

8.3 Leftovers

We now want to prove 8.1.9:

Theorem 8.3.1

$F \subseteq \overline{F} \subseteq E$, E algebraic closed. We had $A \subseteq \overline{F}^n$ algebraic set.
We want to show there exists a unique $B \subseteq E^n$ s.t. $B \cap \overline{F}^n = A$.

Proof: Let $\mathrm{Zer}_E, \mathrm{Zer}_F$ be the zero set function in E and F respectively. Define $B = \mathrm{Zer}_E\left(\mathrm{Pol}\left(A\right)\right)$.
$B \cap \overline{F}^n = \mathrm{Zer}_{\overline{F}}\left(\mathrm{Pol}\left(A\right)\right) = A$.

It remains to show uniqueness. Suppose $C \subseteq F^n$, $C \cap \overline{F}^n = A$. Again using lemma:

$$\begin{aligned} C &= \mathrm{Zer}_E\left(\mathrm{Pol}\left(C\right)\right) \\ A &= C \cap \overline{F}^n = \mathrm{Zer}_{\overline{F}}\left(\mathrm{Pol}\left(C\right)\right) \end{aligned}$$

Now, use the Nullstellensatz in $\overline{F}$:

$$\mathrm{Pol}\left(\mathrm{Zer}_{\overline{F}}\left(I\right)\right) = \sqrt{I}$$

Taking $I = \mathrm{Pol}\left(C\right)$ we then get:

$$\sqrt{I} = \mathrm{Pol}\left(\mathrm{Zer}_{\overline{F}}\left(\mathrm{Pol}\left(C\right)\right)\right) = \mathrm{Pol}\left(A\right)$$

Again in E by the Nullstellensatz:

$$I = \mathrm{Pol}\left(C\right) = \mathrm{Pol}\left(\mathrm{Zer}_E\left(I\right)\right) = \sqrt{I}$$

So:

$$\mathrm{Pol}\left(A\right) = \mathrm{Pol}\left(C\right)$$

■