MATH5735 Modules and Representation Theory Lecture Notes

Joel Beeren

Semester 1, 2012

Contents

1 Why study modules? **4**
1.1 Setup . . . 4
1.2 How do you study modules? . . . 4

2 Rings and Algebras **4**
2.1 Rings . . . 4
2.2 Algebras . . . 5

3 Some examples of Algebras **6**
3.1 Free Algebra . . . 7
3.2 Weyl Algebra . . . 7

4 Module Basics **9**
4.1 Submodules and Quotient Modules . . . 10

5 Module Homomorphisms **11**
5.1 Isomorphism Theorems . . . 12
5.2 Universal property of quotients . . . 13

6 Direct Sums and Products **14**
6.1 Canonical Injections and Projections . . . 14
6.2 Universal Property . . . 15
6.3 Decomposability . . . 16

7 Free Modules and Generators **16**
7.1 Free Modules . . . 16
7.2 Generating Submodules . . . 17

8 Modules over a PID **18**
8.1 Structure theorem for modules over a PID . . . 19
8.2 Elementary Row and Column Operations . . . 20

9 Proof of Structure Theorem **20**

10 Applications of the Structure Theorem **22**
10.1 Endomorphism Ring . . . 23
10.2 Jordan Canonical Forms . . . 24

11 Exact Sequences and Splitting **24**
11.1 Exact Sequences . . . 24
11.2 Splitting . . . 25
11.3 Idempotents . . . 26

12 Chain Conditions **27**
12.1 Submodules and Quotients . . . 27
12.2 Finite Generation . . . 28

13 Noetherian Rings **29**
13.1 Almost Normal Extensions . . . 29
13.2 Hilbert's Basis Theorem . . . 30

14 Composition Series **31**
14.1 Simple Modules . . . 31
14.2 Composition series . . . 31
14.3 Jordan Hölder Theorem . . . 32

15 Semisimple Modules **33**

16 Semisimple rings and Group Representations **35**
16.1 Group Representations . . . 37

17 Maschke's Theorem **38**
17.1 Reynold's Operator . . . 38
17.2 $\mathrm{Hom}_R(M, N)$ . . . 39

18 Wedderburn's Theorem **41**
18.1 Schur's Lemma . . . 41
18.2 Structure Theory . . . 42
18.3 Module Theory . . . 43
18.4 Finite dimensional Semisimple Algebras . . . 44

19 One-dimensional Representations **44**
19.1 Abelianisation . . . 44
19.2 One-dimensional representations . . . 45

20 Centres of Group Algebras **47**
20.1 Centres of Semisimple Rings . . . 47
20.2 Centres of group algebras . . . 48
20.3 Irreducible representations of dihedral groups . . . 49

21 Categories and Functors **50**
21.1 Functors . . . 51
21.2 Hom functor . . . 52

22 Tensor Products I **53**
22.1 Construction of Tensor Products . . . 53
22.2 Universal property of tensor products . . . 53
22.3 Functoriality . . . 54
22.4 Bimodules . . . 54

23 Tensor Products II **55**
23.1 Identity . . . 55
23.2 Distributive Law . . . 56
23.3 Case when R is commutative . . . 57
23.4 Tensor Products of Group Representations . . . 58

24 Characters **58**
24.1 Linear Algebra Recap . . . 58
24.2 Characters . . . 59
24.3 Character Tables . . . 60
24.4 Dual Modules and Contragredient Representation . . . 60
24.5 Hom as tensor product . . . 61

25 Orthogonality **61**
25.1 Characters of $\oplus, \otimes$ . . . 61
25.2 Orthogonality . . . 62
25.3 Decomposing kG-modules into a direct sum of simples . . . 63

26 Example from Harmonic Motion **64**

27 Adjoint Associativity and Induction **64**
27.1 Adjoint Associativity . . . 64
27.2 Induced Modules . . . 66

28 Annihilators and the Jacobson Radical **66**
28.1 Restriction Functor . . . 66
28.2 Annihilators . . . 67
28.3 Jacobson Radical . . . 68

29 Nakayama Lemma and the Wedderburn-Artin Theorem **69**
29.1 NAK Lemma . . . 69
29.2 Properties of the Jacobson Radical . . . 70
29.3 Wedderburn-Artin Theorem . . . 70

30 Radicals and Artinian Rings **71**
30.1 Nilpotence . . . 71
30.2 DCC implies ACC . . . 72
30.3 Computing Some Radicals . . . 72

1 Why study modules?

Modules appear all over mathematics but it is good to keep the following setup in mind. This arises when we have symmetry in a linear context.

1.1 Setup

BIG EXAMPLE HERE (seems unnecessary)

1.2 How do you study modules?

We take our inspiration from linear algebra and study vector spaces. The key theorem of vectorspaces is that any finitely spanned vector space V over the field k has form

$$V \cong k \oplus k \oplus \cdots \oplus k.$$

We seek a similar result for modules – that is, can you write some "finite" modules as a direct sum of ones which are easy to understand? If not, how do you analyse them?

2 Rings and Algebras

2.1 Rings

Definition 2.1. A **ring** R is

(1) An abelian group with group addition denoted $+$ and group zero 0; equipped with

(2) an associative multiplication map $\mu : R \times R \to R$, $(r, r') \mapsto rr'$ satisfying

  (a) (distributive law): for $r, r', s \in R$ we have

$$(r + r')s = rs + r's, \text{ and}$$
$$s(r + r') = sr + sr'.$$

  (b) (multiplicative identity) there is an element $1_R = 1 \in R$ such that

$$1r = r1 = r \quad \forall r \in R.$$

We say R is **commutative** if multiplication is commutative (that is, $rs = sr$ for all $r, s \in R$). The **group of units** is

$$R^* = \{r \in R \mid \exists s \in R.sr = 1 = rs\}.$$

If $R^* = R \setminus \{0\}$ we say R is a **division ring**, and further if R is commutative then it is a field.

Example 2.1. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Q}(i)$ are fields

Example 2.2. $\mathbb{Z}, \mathbb{Z}(i)$ are rings

Example 2.3. For k a field, R a ring, $R[x_1, \ldots, x_n]$ is the polynomial ring in n variables over R, and $k(x_1, \ldots, x_n)$ is the field of rational functions in n variables.

Furthermore, $M_n(R)$ is the ring of $n \times n$ matrices over R, and if V is a vector space then $\text{End}_k(V)$, the set of linear maps $V \to V$ is a ring with pointwise addition and composition for multiplication.

Definition 2.2. Let R be a ring. A subgroup S of the underlying additive group of R is

(1) a **subring** if

- $1_R \in S$; and
- for $s, s' \in S$, we have $ss' \in S$.

(2) an (two-sided) **ideal** if for all $r \in R$, $s \in S$, we have $sr, rs \in S$.

Example 2.4. Let R be a ring. We have the **opposite ring** R^{op} where

$$R^{\text{op}} = \{r^\circ \mid r \in R\}$$

which has the same addition as in R but $r^\circ s^\circ = (sr)^\circ$.

Exercise. Check the ring axioms for R^{op}.

Definition 2.3. Let R be a ring. The **centre** of R is

$$Z(R) = \{z \in R \mid zr = rz \; \forall r \in R\}.$$

Exercise. Check that $Z(R)$ is a subring of R.

Fact 2.1. Let $I \lhd R$ be an ideal of R. Then there is a quotient ring R/I with

- addition: $(r + I) + (r' + I) = (r + r') + I$; and
- multiplication: $(r + I)(r' + I) = rr' + I$.

Definition 2.4. A map of rings $\varphi : R \to S$ is a **ring homomorphism** if (for all $r, r' \in R$)

(1) $\varphi(r + r') = \varphi(r) + \varphi(r')$

(2) $\varphi(rr') = \varphi(r)\varphi(r')$

(3) $\varphi(1_R) = 1_S$

Fact 2.2. Let $\varphi : R \to S$ be a ring homomorphism. Then

- $\text{im}(\varphi) \subseteq S$ is a subring
- $\ker \varphi \lhd R$

2.2 Algebras

Fix a commutative ring R.

Definition 2.5. An R**-algebra** (also called an algebra over R) is a ring A equipped with a ring homomorphism $\iota : R \to Z(A)$.

An R**-subalgebra** is a subring B of A with $Z(\mathbb{R}) \subseteq Z(B)$ (so B is naturally a subalgebra).

Example 2.5. The following are R-algebras:

(1) $R[x_1, \dots, x_n]$ – here we take $\iota : R \to R[x_1, \dots, x_n]$ as the map $r \mapsto r + 0x_1 + \cdots + 0x_n$

(2) $M_n(R)$ – take $\iota : R \to M_n(R)$ by $r \mapsto rI_n$.

Proposition 2.1. Let $A \neq 0$ be an algebra over a field k.

(1) The unit map $\iota : k \to A$ is injective, so we will often consider k as a subring of A by identifying it with $\iota(k)$

(2) A is naturally a vector space over k.

Proof.

(1) k is a field, so $\ker \iota = k$ or 0. We know that $\iota(1_k) = 1_A$ so $\ker \iota = 0$ and hence ι is injective.

(2) We set vector addition to be the same as ring addition, and scalar multiplication the same as ring multiplication by elements of k identified with $\iota(k)$. The vector space axioms then follow from the ring axioms.

□

Definition 2.6. A ring homomorphism $\varphi : A \to B$ of k-algebras is a **k-algebra homomorphism** if it is k-linear.

Definition 2.7. Let G be a group and k a field. Define the vector space

$$kG := \bigoplus_{\sigma \in G} k\sigma$$

of all formal (finite) linear combinations of elements of G. Then kG is a k-algebra called the **group algebra** of G with ring multiplication induced by group multiplication in the following sense:

$$\left(\sum \alpha_{g_i} g_i\right)\left(\sum \beta_{g_j} g_j\right) = \sum_{g \in G}\left(\sum_{g_i g_j = g} \alpha_{g_i}\beta_{g_j} g\right).$$

Exercise. Check the k-algebra axioms for kG.

Exercise. For the cyclic group $G = \{1, \sigma\}$ and field k with $\operatorname{char} k \neq 2$, show that there is a k-algebra isomorphism

$$\begin{aligned} kG &\longrightarrow k \times k \\ 1 &\mapsto (1,1) \\ \sigma &\mapsto (1,-1) \end{aligned}$$

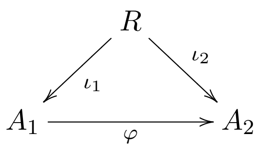
Exercise. Generalise the previous to larger cyclic groups

Exercise. Find a noncommutative ring R with $R \cong R^{\text{op}}$.

3 Some examples of Algebras

Fix a commutative ring R.

Definition 3.1. Let A_1, A_2 be R-algebras with unit maps $\iota_j : R \to A_j$ for $j = 1, 2$. An R-algebra homomorphism (resp. isomorphism) $\varphi : A_1 \to A_2$ is a ring homomorphism (resp. isomorphism) such that the following diagram commutes



(that is, $\iota_2 = \varphi \circ \iota_1$).

Example 3.1. $\mathbb{C}$ is both an $\mathbb{R}$-algebra and a $\mathbb{C}$-algebra (with ι defined as inclusion). Now, the conjugation map

$$\varphi : \mathbb{C} \to \mathbb{C};\ z \mapsto \overline{z}$$

is an $\mathbb{R}$-algebra isomorphism but not a $\mathbb{C}$-algebra isomorphism (as $\iota_2 = \varphi \circ \iota_1 \Leftrightarrow z = \overline{z}$ for all $z \in R$).

3.1 Free Algebra

Let $\{x_i\}_{i\in I}$ be a set of noncommuting variables that commute with scalars in R. Let $R\langle x_i\rangle_{i\in I}$ denote the set of noncommutative polynomials in the x_i's with coefficients in R. That is, expressions of the form

$$\sum_{n\geq 0}\sum_{i_1,\ldots,i_n\in I} r_{i_1}r_{i_2}\ldots r_{i_n}x_{i_1}x_{i_2}\ldots x_{i_n}, \quad r_{i_j}\in R\ \forall j$$

where all but finitely many $r_{i_1},\ldots,r_{i_n}$ are zero.

If $I=\{1,2,\ldots,n\}$, we write $R\langle x_i\rangle_{i\in I}=R\langle x_1,x_2,\ldots,x_n\rangle$.

Proposition 3.1. $R\langle x_i\rangle_{i\in I}$ is an R-algebra when endowed with

(1) ring addition: just add coefficients

(2) ring multiplication: induced by concatenation of monomials

(3) unit map: $R\to R\langle x_i\rangle_{i\in I}$ with $r\mapsto r$, the constant polynomial.

This is called the **free R-algebra** on $\{x_i\}_{i\in I}$.

Proof. Elementary but long and tedious. □

Example 3.2. $A=\mathbb{Z}\langle x,y\rangle$. See

$$\begin{aligned}(2x+xy)(3yx-y^2x) &= 6xyx-2xy^2x+2xy^2x-xy^3x\\ &= 6xyx+xy^2x-xy^3x.\end{aligned}$$

Exercise. For the dihedral group D_n, k a field, show that

$$kD_n\cong\frac{k\langle x,y\rangle}{\langle x^2-1,y^n-1,yx-xy^{n-1}\rangle}.$$

3.2 Weyl Algebra

Let k be a field, V a vector space. Recall that $\operatorname{End}_k(V)$ is the ring of linear maps $T:V\to V$. Then $\operatorname{End}_k(V)$ is also a k-algebra. How? Note that $\alpha\,\mathrm{id}_V$, the scalar multiplication by α map is an element of $\operatorname{End}_k(V)$, so we have the unit map

$$\iota:k\to\operatorname{End}_k(V);\ \alpha\mapsto\alpha\,\mathrm{id}_V.$$

We need to check that $\alpha\,\mathrm{id}_V\in Z(\operatorname{End}_k(V))$ but this is obvious.

Definition 3.2. A **differental operator with polynomial coefficients** is a $\mathbb{C}$-linear map of the form

$$\begin{aligned}D=\sum_{i=0}^n p_i(x)\partial^i:\mathbb{C}[x]&\longrightarrow\mathbb{C}[x]\\ f(x)&\mapsto\sum_{i=0}^n p_i(x)\frac{d^if}{dx^i}\end{aligned}$$

where $p_i(x)\in\mathbb{C}[x]$ for all i.

We denote the set of these operators by A_1 (note that D is an element of the $\mathbb{C}$-algebra $\operatorname{End}_{\mathbb{C}}(\mathbb{C}[x])$). Furthermore, we see that

$$\partial x = x\partial + 1$$

Why? For $p(x) \in \mathbb{C}[x]$, we have

$$\begin{aligned}(\partial x)(p(x)) &= \frac{d}{dx}(xp(x)) \\ &= x\frac{dp}{dx} + p(x) \\ &= (x\partial + 1)(p(x)).\end{aligned}$$

Proposition 3.2. A_1 is a $\mathbb{C}$-subalgebra of $\operatorname{End}_{\mathbb{C}}(\mathbb{C}[x])$. It is called the **(first) Weyl algebra**.

Proof. Note that $\mathbb{C} \subset A_1$, so we check closure axioms. A_1 is clearly closed under addition, and contains 0 and 1. Furthermore, any $D \in A_1$ has the form

$$\sum_{i,j=0}^{N} \alpha_{ij} x^i \partial^j, \quad \alpha_{ij} \in \mathbb{C}$$

so by the distributive law, it suffices to show (exercise)

$$x^{i_1}\partial^{j_1}x^{i_2}\partial^{j_2} \in A_1.$$

However, using the Weyl relation we can push all of the ∂'s to the right of all x's to see that this holds true. □

Proposition 3.3. There is a $\mathbb{C}$-algebra isomorphism

$$\begin{aligned}\varphi : \frac{\mathbb{C}\langle x, y\rangle}{\langle yx - xy - 1\rangle} &\longrightarrow A_1 = \mathbb{C}\langle x, \partial\rangle \\ x + \langle yx - xy - 1\rangle &\mapsto x \\ y + \langle yx - xy - 1\rangle &\mapsto \partial.\end{aligned}$$

Proof. Certainly there is a "substitution homomorphism" $\tilde{\varphi} : \mathbb{C}\langle x, y\rangle \to A_1$ which maps $x \mapsto x$ and $y \mapsto \partial$; and more generally $p(x, y) \mapsto p(x, \partial)$. By the Weyl relation, $\ker\tilde{\varphi} \ni yx - xy - 1$ and so $\ker\tilde{\varphi} \supseteq \langle yx - xy - 1\rangle = I$.

By the universal property of quotients, there is an induced ring homomorphism

$$\varphi : \frac{\mathbb{C}\langle x, y\rangle}{I} \to A_1.$$

This is clearly surjective. We now check that $\ker\varphi = 0$. By the proof of the previous proposition, any nonzero element in A_1 can be written in the form

$$D = \sum_{j=n}^{N} p_j(x)y^j$$

with say $p_n(x) \neq 0$. Then

$$\begin{aligned}[\varphi(D)](x^n) &= \left(\sum_{j=n}^{N} p_j(x)\partial^j\right)(x^n) \\ &= p_n(x)\frac{d^n x^n}{dx^n} + \dots \\ &= n!p_n(x) \neq 0.\end{aligned}$$

So $\varphi(D) \neq 0$ and therefore $\ker\varphi = 0$. □

Exercise. The quaternions can be represented as

$$\mathbb{H} := \frac{\mathbb{R}\langle i, j\rangle}{\langle i^2 - 1, j^2 - 1, ij + ji\rangle}.$$

Show that there is an $\mathbb{R}$-algebra homomorphism $\mathbb{H} \to M_2(\mathbb{C})$ such that

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$
$$j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Hence or otherwise show that $\mathbb{H}$ is a division ring.

4 Module Basics

Fix a ring R.

Definition 4.1. A **(right)** R**-module** is an additive group M equipped with a scalar multiplication map $M \times R \to M : (m, r) \mapsto mr$ such that the following axioms hold (for all $m, m' \in M$, $r, r' \in R$)

(1) $m1 = m$

(2) (associativity) $(mr)r' = m(rr')$

(3) (distributivity) $(m + m')r = mr + m'r$ and $m(r + r') = mr + mr'$

Remark. We can similarly define **left** R-modules.

Example 4.1. For a field k, a right k-module is just a vector space over k with scalars on the right. Here module axioms are equivalent to vector space axioms.

Example 4.2. R itself is a left and right R-module with module addition and scalar multiplication equal to ring addition and multiplication respectively. Note that the module axioms are a consequence of the ring axioms in this case.

Exercise. For any R-module M and $m \in M$ we have

(1) $m0 = 0$

(2) $m(-1) = -m$.

The following tells us that $\mathbb{Z}$-modules are "just" abelian groups.

Proposition 4.1. Let M be an abelian group. There is a unique $\mathbb{Z}$-module structure on it extending the additive group structure.

Proof. (Sketch) We show the $\mathbb{Z}$-module structure is unique by showing how the module axioms completely determine scalar multiplication by $n \in \mathbb{Z}$. If $n > 0$ then axioms (1) and (3) imply that for $m \in M$,

$$\begin{aligned} mn &= m(1 + 1 + \cdots + 1) \\ &= m1 + m1 + \cdots + m1 \\ &= m + m + \cdots + m. \end{aligned}$$

For $n = 0$, we have $m0 = 0$. Also, if $n < 0$ then

$$\begin{aligned} mn &= m((-n)(-1)) \\ &= (m(-n))(-1) \\ &= -(m + \cdots + m) \\ &= -m - m \cdots - m. \end{aligned}$$

□

Exercise. Check that this actually gives a $\mathbb{Z}$-module structure.

Exercise. Explain and prove the following statement: "A right R-module is just a left R^{op}-module". In particular, if R is commutative, so there is a natural isomorphism $R \leftrightarrow R^{\text{op}}$ then left and right modules are the same thing.

Example 4.3. Let $S = M_n(R)$, and let R^n be the set of n-tuples (i.e. row vectors) with entries in R. Then R^n is a right S-module with module addition and scalar multiplication defined by matrix operations.

Exercise. Check the module axioms.

Remark. Similarly, with R^n being column vectors, then R^n is a left S-module.

We can "change scalars" with

Proposition 4.2. Let $\varphi : S \to R$ be a ring homomorphism, M a right R-module. Then M is naturally a right S module with the same additive structure but multiplication defined as

$$ms := m\varphi(s).$$

We denote the S-module by M_S to distinguish it from the original.

Proof. This is an exercise in checking axioms. For example, let $m \in M$, $s, s' \in S$ and see

$$m(s + s') = m\varphi(s + s') = m(\varphi(s) + \varphi(s')) = m\varphi(s) + m\varphi(s') = ms + ms'.$$

□

Corollary 4.1. *For R commutative, any R-algebra A is also a left and right R-module.*

Proof. Follows from proposition 4.2 and example 4.2. □

4.1 Submodules and Quotient Modules

Proposition 4.3. Let M be an R-module. An R-submodule is an additive subgroup N of M which is closed under scalar multiplication. In this case, N is an R-module and we write $N \leq M$. A **right ideal** of R is a submodule of the right module R_R, whereas a **left ideal** of R is a submodule of the left module ${}_RR$.

Exercise. Let $S = M_2(R)$. Then $\left(\begin{smallmatrix} R & 0 \\ R & 0 \end{smallmatrix}\right)$ is a left ideal but not a right ideal.

Remark. An **ideal** is a subset which is both a left and right ideal.

Exercise. The intersection of submodules is a submodule.

Proposition 4.4. Let N be a submodule of M. The quotient abelian group M/N is naturally an R-module with scalar multiplication

$$(m+N)r := mr + N.$$

Proof. First note that multiplication is well defined for if $n \in N$ we have

$$\begin{aligned}(m+n+N)r &= (m+n)r + N \\ &= mr + nr + N \\ &= mr + N\end{aligned}$$

since $nr \in N$. It remains to check the module axioms. □

Exercise. Let R be the Weyl algebra $A_1 = \mathbb{C}\langle x, \partial \rangle$. $M = \mathbb{C}[x]$ is a left R-module with the usual addition and scalar multiplication defined as

$$\left(\sum_i p_i(x)\partial^i\right) p(x) := \sum_i p_i(x)\frac{d^i p(x)}{dx^i}.$$

5 Module Homomorphisms

Fix a ring R.

Definition 5.1. Let M, N be R-modules. A function $\varphi : M \to N$ is an **R-module homomorphism** if it is a homomorphism of abelian groups such that (for all $m \in M,\ r \in R$)

$$\varphi(mr) = \varphi(m)r.$$

In this case we also say φ is **R-linear**. We denote the set of these as $\mathrm{Hom}_R(M, N)$.

Example 5.1. k-module homomorphisms are just k-linear maps.

Proposition 5.1. $\mathrm{Hom}_R(M, N)$ is an abelian group endowed with group addition

$$(\varphi_1 + \varphi_2)(m) = \varphi_1(m) + \varphi_2(m).$$

Proof. Note that addition is well defined as φ_1, φ_2 are R-linear. Indeed it is additive and for $m \in M, r \in R$ we have

$$\begin{aligned}(\varphi_1 + \varphi_2)(mr) &= \varphi_1(mr) + \varphi_2(mr) \\ &= \varphi_1(m)r + \varphi_2(m)r \\ &= (\varphi_1(m) + \varphi_2(m))r \\ &= (\varphi_1 + \varphi_2)(m)r.\end{aligned}$$

Exercise. Check group axioms.

□

Proposition 5.2. For any R-module M, there is the following isomorphism of abelian groups

$$\begin{aligned}\Phi : M &\longrightarrow \mathrm{Hom}_R(R_R, M) \\ m &\mapsto (\lambda_m : r \mapsto mr)\end{aligned}$$

with inverse

$$\Psi : \varphi \mapsto \varphi(1).$$

Proof. Check λ_m is R-linear so Φ is well defined. The distributive law implies that

$$\lambda_m(r + r') = m(r + r') = mr + mr' = \lambda_m(r) + \lambda_m(r').$$

Associativity gives us

$$\lambda_m(rr') = m(rr') = (mr)r' = \lambda_m(r)r'.$$

Φ is additive by the other distributive law.

It now suffices to check that Ψ is the inverse of Φ. We observe that

$$(\Psi\Phi)(m) = \Psi(\lambda_m) = \lambda_m(1) = m1 = m$$
$$[(\Phi\Psi)(\varphi)](r) = [\Phi(\varphi(1))](r) = \varphi(1)r = \varphi(r)$$

so $\Phi\Psi = \mathrm{id}$. □

Proposition 5.3. As for vector spaces, the composition of R-linear maps is R-linear.

Proof. Exercise. □

Proposition 5.4. Let $\varphi : M \to N$ be a homomorphism of right R-modules. Then

(1) $\ker \varphi \leq M$

(2) $\mathrm{im}(\varphi) \leq N$

Proof. (1) Exercise.

(2) Any element in $\mathrm{im}(\varphi)$ has the form $\varphi(m)$ for $m \in M$. Then for $r \in R$, see

$$\varphi(m)r = \varphi(mr) \in \mathrm{im}(\varphi),$$

so $\mathrm{im}(\varphi)$ is closed under scalar multiplication. We know $\mathrm{im}(\varphi)$ is a subgroup so it must be a submodule.

□

Proposition 5.5. Let $N \leq M$. Then there are module homomorphisms

(1) The **inclusion map** $\iota : N \hookrightarrow M$

(2) the **projection map** $\pi : M \to M/N$ defined by $m \mapsto m + N$.

Proof. Exercise. □

5.1 Isomorphism Theorems

Theorem 5.1 (First Isomorphism Theorem)**.** *Let $\varphi : M \to N$ be an R-module homomorphism. Then the following is a well-defined isomorphism of R-modules:*

$$\bar{\varphi} : \frac{M}{\ker \varphi} \leftrightarrow \mathrm{im}(\varphi)$$
$$m + \ker \varphi \mapsto \varphi(m)$$

Proof. Group theory implies that $\bar{\varphi}$ is a well defined group isomorphism. We need only check $\bar{\varphi}$ is R-linear. But observe

$$\begin{aligned}\bar{\varphi}((m+\ker\varphi)r) &= \bar{\varphi}(mr+\ker\varphi)\\ &= \varphi(mr)\\ &= \varphi(m)r\\ &= \bar{\varphi}(m+\ker\varphi)r.\end{aligned}$$

□

We can similarly conclude

Theorem 5.2. *(1) Let $N, N' \leq M$. Then $N+N' \leq M$ and*

$$\frac{N+N'}{N} \cong \frac{N'}{N\cap N'}$$

(2) Given $M'' \leq M' \leq M$ then

$$\frac{M/M''}{M'/M''} \cong \frac{M}{M'}.$$

Example 5.2. Let R be a ring, and $S = M_2(R)$. Recall that $\begin{pmatrix} R & R\end{pmatrix} \cong R^2$ is a right S-module. Let $m : \begin{pmatrix}1 & 0\end{pmatrix} \in \mathbb{R}^2$ so by proposition (5.2) we get the homomorphism $\lambda_m : s \mapsto \begin{pmatrix}1 & 0\end{pmatrix} s$. It is surjective, so $\operatorname{im}(\lambda_m) = M$, and

$$\ker\lambda_m = \begin{pmatrix} 0 & 0\\ R & R\end{pmatrix}.$$

The first isomorphism theorem gives

$$\frac{M_2(R)}{\ker\lambda_m} \cong \begin{pmatrix} R & R\end{pmatrix}.$$

5.2 Universal property of quotients

Theorem 5.3. *Let $M' \leq M$ and N another R-module. We have a bijection*

$$\begin{aligned}\Psi : \operatorname{Hom}_R\left(M/M', N\right) &\longrightarrow \left\{\varphi \in \operatorname{Hom}_R(M,N) \mid \varphi(M') = 0\right\}\\ \bar{\varphi} &\mapsto \bar{\varphi}\circ\pi.\end{aligned}$$

Proof. Note that Ψ is well defined. It is injective as π is surjective, so we check Ψ is surjective. Let $\varphi \in \operatorname{Hom}_R(M,N)$ with $\varphi(M') = 0$. Then we get the well-defined map

$$\begin{aligned}\bar{\varphi} : M/M' &\longrightarrow N\\ m+m' &\mapsto \varphi(m+M') = \varphi(m).\end{aligned}$$

Exercise. Check that $\bar{\varphi}$ is R-linear.

We note that

$$[\Psi(\bar{\varphi})](m) = \bar{\varphi}(m+M') = \varphi(m+M') = \varphi(m)$$

so $\Psi(\bar{\varphi}) = \varphi$ and thus Ψ is also surjective. □

Example 5.3. What is $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z})$?

The universal property of quotients tells us that these are the homomorphisms

$$\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$$

such that $\varphi(2\mathbb{Z}) = 0$. But proposition (5.2) tells us that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}) = \mathbb{Z}/3\mathbb{Z}$, so we need $a \in \mathbb{Z}/3\mathbb{Z}$ such that $a(2\mathbb{Z}) = 0$. It follows that $a = 0$ as $2 \in (\mathbb{Z}/3\mathbb{Z})^*$.

6 Direct Sums and Products

Let R be a ring, and let $\{M_i\}_{i\in I}$ be a set of (right) R-modules. We recall

$$\prod_{i\in I} M_i = \{(m_i)_{i\in I} \mid m_i \in M_i\}.$$

We also consider the following subset

$$\bigoplus_{i\in I} M_i = \left\{(m_i)_{i\in I} \in \prod_{i\in I} M_i \mid \text{ all but finitely many } m_i \text{ are zero}\right\}.$$

Remark. If $I = \{1, 2, \dots, n\}$ then $\prod M_i = \bigoplus M_i = M_1 \times \cdots \times M_n$, and the elements will be either written as

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} m_1 & \dots & m_n \end{pmatrix}.$$

As usual, M^n denotes $M \times M \times \cdots \times M$.

Proposition 6.1. $\prod_{i\in I} M_i$ is an R-module when endowed with coordinate wise addition and scalar multiplication. This module is called the **direct product**.

$\bigoplus_{i\in I} M_i$ is a submodule of $\prod M_i$ and is called the **direct sum**.

Proof. Check axioms. □

Exercise. $0r = 0$ in any module.

6.1 Canonical Injections and Projections

Proposition 6.2. Let $\{M_i\}_{i\in I}$ be a set of (right) R-modules. Then we have the following R-module homomorphisms for each $j \in I$

(1) **Canonical Injection**:

$$\begin{aligned} \iota_j : M_j &\longrightarrow \bigoplus_{i\in I} M_i \\ m &\mapsto (0, \dots, m, 0, \dots, 0) \end{aligned}$$

(2) **Canonical Projection**:

$$\begin{aligned} \pi_j : \prod_{i\in I} M_i &\longrightarrow M_j \\ (m_i)_{i\in I} &\mapsto m_j \end{aligned}$$

Proof. Check R-linearity. □

6.2 Universal Property

Let $\{M_i\}_{i\in I}$ be as above, and N another R-module. We have the following inverse isomorphisms of abelian groups

(1)

$$\begin{aligned}\operatorname{Hom}_R\left(\bigoplus M_i, N\right) &\overset{\Psi}{\underset{\Phi}{\leftrightarrows}} \prod_{i\in I}\operatorname{Hom}_R(M_i, N)\\ f &\mapsto (f\circ\iota_i)_{i\in I}\\ \left(\tilde{f} : (m_i)\mapsto \sum f_i m_i\right) &\leftarrow\!\shortmid (f_i)_{i\in I}.\end{aligned}$$

(2)

$$\begin{aligned}\operatorname{Hom}_R\left(N, \bigoplus M_i\right) &\overset{\Psi}{\underset{\Phi}{\leftrightarrows}} \prod_{i\in I}\operatorname{Hom}_R(N, M_i)\\ f &\mapsto (\pi\circ f)_{i\in I}\\ (\tilde{f} : n\mapsto (f_i(n))_{i\in I}) &\leftarrow\!\shortmid (f_i)_{i\in I}.\end{aligned}$$

Proof. We do (1) only as (2) is similar. First note that Φ is well defined, $f\circ\iota_i$ is R-linear as it is the composition of R-linear maps.

Exercise. One sees easily that Φ is additive.

It suffices to show that Ψ is an inverse. But observe that

$$\begin{aligned}[(\Psi\Phi)(f)]((m_i)_{i\in I}) &= [\Psi((f\circ\iota_i)_{i\in I})](m_i)_{i\in I}\\ &= \sum_{i\in I}(f\circ\iota_i)(m_i)\\ &= f\left(\sum \iota_i(m_i)\right)\\ &= f((m_i)_{i\in I}).\end{aligned}$$

So $\Psi\Phi = \mathrm{id}$. Furthermore, we have

$$\begin{aligned}[(\Phi\Psi)((f_i)_{i\in I})]_j(m) &= [(\Psi((f_i)_{i\in I}\circ\iota_i))]_j(m)\\ &= \Psi((f_i)_{i\in I})\circ\iota_j(m)\\ &= f_j(m).\end{aligned}$$

So $\Phi\Psi = \mathrm{id}$ and we are done. □

Remark. If $I = \{1, 2, \ldots, n\}$ we usually interpret the map Ψ by

$$\Psi((f_1,\ldots,f_n)) : \begin{pmatrix} m_1\\ \vdots\\ m_n\end{pmatrix} \mapsto \sum_{i=1}^{n} f_i(m_i).$$

That is, $\Psi((f_1,\ldots,f_n))$ is just left multiplication by $(f_1,\ldots,f_n)$ if we write the elements of $\bigoplus M_i$ as column vectors.

Example 6.1. Let R be a ring, $S = M_2(R)$, and recall that $R^2 = \begin{pmatrix} R & R \end{pmatrix}$ is a right S-module. We also have two S-module maps given by left multiplication by

$$\begin{pmatrix} 1 & 0 \end{pmatrix};\ f_1 : S \to R^2$$
$$\begin{pmatrix} 0 & 1 \end{pmatrix};\ f_2 : S \to R^2.$$

We know that

$$\mathrm{Hom}_S\left(S, R^2 \times R^2\right) = \mathrm{Hom}_S\left(S, R^2\right) \times \mathrm{Hom}_S\left(S, R^2\right).$$

We have the S-module map

$$\begin{pmatrix} f_1 \\ f_2 \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \begin{pmatrix} a & b \end{pmatrix} \\ \begin{pmatrix} c & d \end{pmatrix} \end{pmatrix}.$$

We see that $S \cong R^2 \times R^2$ as right S-modules.

6.3 Decomposability

Definition 6.1. We say that a nonzero R-module is **decomposable** if it is isomorphic to the direct sum of two nonzero submodules. Otherwise it is **indecomposable**.

Example 6.2. Let $R = k[x]$. For $n \geq 1$, $\langle x^n \rangle$ is an ideal, and therefore $M = R/\langle x^n \rangle$ is a module which is indecomposable.

Why? From the internal characterisation of direct product groups, we need only show that any two submodules intersect nontrivially. We show indeed that any nonzero $N \leq M$ contains $x^{n-1} + \langle x^n \rangle$. We may suppose that

$$N \ni \alpha_j x^j + \cdots + \alpha_{n-1} x^{n-1} + \langle x^n \rangle, \quad \alpha_j \neq 0 =: n.$$

Then $n\alpha_j^{-1} x^{n-1-j} = x^{n-1} + \langle x^n \rangle$.

7 Free Modules and Generators

7.1 Free Modules

Fix a ring R.

Definition 7.1. A **free module** is one which is isomorphic to a direct sum of copies of R. That is, M is a free module if

$$M \cong \bigoplus_{i \in I} R \ (=: R^I \text{ if } I = \{1, 2, \ldots, n\}.)$$

Proposition 7.1. Let R be a commutative ring, and G a group. Let

$$RG = \bigoplus_{g \in G} gR$$

be the free right (or left) R-module with "basis" the elements of G. The R-module structure on RG extends to an R-algebra structure with multiplication induced by group multiplication, that is,

$$\left(\sum_{g \in G} g r_g\right)\left(\sum_{h \in G} h s_h\right) := \sum_{l \in G} l \left(\sum_{gh = l} r_g s_h\right),$$

and unit map

$$\iota : R \to RG; \quad r \mapsto 1r.$$

This is called the **group algebra**.

Proof. Exercise. ☐

7.2 Generating Submodules

Let M be a module, I an index set. Recall there is a group isomorphism (from the universal property)

$$\mathrm{Hom}_R\left(\bigoplus_{i\in I} R, M\right) \cong \prod_{i\in I} \mathrm{Hom}_R(R, M) \overset{prop5.2}{\cong} \prod_{i\in I} M.$$

We then ask, what is the homomorphism in $\mathrm{Hom}_R\left(R^I, M\right)$ corresponding to $(m_i)_{i\in I} \in \prod_{i\in I} M$?

The answer is called the **universal property for free modules**, and is

$$(m_i)_{i\in I} : (r_i)_{i\in I} \mapsto \sum_{i\in I} m_i r_i.$$

Such an expression of element of M is called a (right) **R-linear combination** of the m_i's.

Example 7.1. We see

$$\mathrm{Hom}_R(R^m, R^n) \cong \prod_{i=1}^{m} R^n = (R^n)^m = M_{nm}(R).$$

Homomorphisms corresponding to $n \times m$ matrices are given by left multiplication.

Example 7.2. Let R be a commutative ring, and G a group. Let H be a subgroup of G.

Exercise. Show RH is an R-subalgebra of RG.

Hence RG is also a (right) RH-module. In fact, it is a *free* RH-module.

Why? For each left coset C of H in G, we pick a representative g_C so $C = g_C H$. The universal property of free modules gives a homomorphism

$$\begin{aligned}(g_C)_{C\in G/H} : \bigoplus_{C\in G/H} (RH) &\longrightarrow RG \\ (a_C)_{C\in G/H} &\mapsto \sum_{C\in G/H} g_C a_C.\end{aligned}$$

Exercise. This is clearly bijective so gives an isomorphism.

Proposition 7.2. Let M be a (right) R-module, and L a subset. The **submodule generated by** L is the set of all R-linear combinations of elements of L. It is a submodule of M, and is denoted $\sum_{l\in L} lR$.

Proof. $\sum lR$ is a submodule as it is the image of the R-linear map

$$(l)_{l\in L} : \bigoplus_{l\in L} R \longrightarrow M$$

given by the universal property of free modules. □

Definition 7.2. Let M be an R-module. A **set of generators** for M is a subset L such that the submodule generated by L is M itself. We also say L **generates** M.

We say M is **finitely generated** if we can take L to be finite, and say M is finite if $|L| = 1$.

Example 7.3. Any module M is generated by the subset M.

Example 7.4. The right (or left) R-module R is cyclic, generated by 1_R.

Corollary 7.1. *Any module is a quotient of a free module by the first isomorphism theorem and the surjectivity of*

$$(m)_{m\in M} : \bigoplus_{m\in M} R \longrightarrow M.$$

Example 7.5. Let $R = \mathbb{C}\langle x, \partial\rangle$ and suppose V is a $\mathbb{C}$-vector space of functions on which polynomial differential operators act (e.g. $V = \mathbb{C}[x]$ or meromorphic functions on $\mathbb{C}$). Suppose $D \in R$ is a differential operator and consider the differential equation $Df = 0$ with solution $f \in V$.

Recall V is a left R-module and so right multiplication by $f \in V$ gives an R-module homomorphism

$$\begin{aligned} \varphi : R &\longrightarrow V \\ D &\mapsto Df. \end{aligned}$$

Since we assumed that $Df = 0$, we know that $D \in \ker\varphi$. Hence $RD \subseteq \ker\varphi$. The universal property of quotients gives an R-module homomorphism

$$\bar{\varphi} : R/RD \longrightarrow V$$

R/RD is a cyclid module generated by $1 + RD$. You can reverse this to see that the solutions to the differential equation $Df = 0$ are given by R-linear maps $R/RD \longrightarrow V$.

Example 7.6. Let $R = k\langle x, y\rangle$ be the ring of polynomials in noncommutative variables x, y over a field k. We know R is cyclic and therefore finitely generated, but the right ideal

$$\sum_{i=0}^{\infty} x^i yR$$

is not finitely generated (exercise).

8 Modules over a PID

Fix a PID R. Recall a PID is a commutative domain where every ideal is generated by a single element. Examples include $\mathbb{Z}$, $\mathbb{Z}[i]$, $k[x]$ for k a field.

Fact 8.1. Every PID is a UFD and we can define a gcd. In fact, for $a, b \in R$, then $\langle \gcd(a, b)\rangle = \langle a, b\rangle$.

Lemma 8.1. Any submodule M of R^n is finitely generated.

Proof. By induction on n, with $n = 0$ automatic.

Suppose that $n > 0$ and let $\pi : R^n \to R$ be the projection onto the first factor (which is a linear map). Let $\iota : M \to R^n$ be inclusion. Consider the linear map $\pi|_M = \pi \circ \iota : M \to R^n \to R$.

$\text{im}(\pi|_M) \lhd R$ so is generated by $\overline{m_0} \in R$ as R is a PID. We pick $m_0 \in M$ such that $\pi(m_0) = \overline{m_0}$. Now, $\ker\pi|_M = \ker\pi \cap M \leq \ker\pi \cong R^{n-1}$. Induction implies that $\ker\pi|_M$ is generated by $m_1, \ldots, m_s$. It suffices to show that $m_0, m_1, \ldots, m_s$ generate M.

Consider $m \in M$. Then $\text{im}(\pi|_M) \ni \pi m = \overline{m_0}r$ for some $r \in R$. Hence

$$\pi(m - m_0 r) = \pi(m) - \pi(m_0)r = \pi(m) - \pi(m) = 0,$$

so $\ker\pi|_M = \ker\pi \cap M \ni m - m_0 r$. But any element of $\ker\pi \cap M$ can be written as $\sum r_i m_i$ so $m = m_0 r + \sum r_i m_i$ and so $m_0, \ldots, m_s$ generate M. □

8.1 Structure theorem for modules over a PID

Theorem 8.1. *Let R be a PID and M a finitely generated R-module. Then*

$$M \cong R^r \oplus \frac{R}{\langle a_1 \rangle} \oplus \frac{R}{\langle a_2 \rangle} \oplus \cdots \oplus \frac{R}{\langle a_s \rangle}$$

for some $a_i \in R$ with $a_1 \mid a_2 \mid \cdots \mid a_s$.

The proof of the theorem occupies the next two sections.

Recall that given a finite set of generators $m_1, \ldots, m_n$ for M we get a surjective homomorphism

$$\pi = \begin{pmatrix} m_1 & m_2 & \ldots & m_s \end{pmatrix} : R^n \to M.$$

Lemma 8.1 implies that $\ker \pi$ is also finitely generated so picking a set of generators for it gives a surjective homomorphism $R^m \to \ker \pi$. The composite map

$$(R^m \to \ker \pi \hookrightarrow R^n) \in \mathrm{Hom}_R\left(R^m, R^n\right)$$

is given by an $n \times m$ matrix over R (by example 7.1). Call this matrix Φ.

Remark. (1) Given a module isomorphism $\Psi : R^n \to R^n$, we get a new surjective isomorphism $\pi\Psi : R^n \to R^n \to M$ which corresponds to a change of basis/generators for M. This has the effect of changing

$$\Phi \mapsto \Psi^{-1}\Phi.$$

(2) Similarly, changing basis in R^m, we can change Φ to $\Phi \circ \Psi$ for some module isomorphism $\Psi : R^m \to R^m$.

(3) The first isomorphism theorem implies that $M \cong R^n / \mathrm{im}(\Phi) = \ker \pi$.

Proposition 8.1. (1) Let S be a ring, N an S-module. The set $\mathrm{Aut}_S(N)$ of module automorphisms $\psi : N \to N$ is a subgroup of the permutation group on N.

(2) Let $GL_n(R) = \{\psi \in M_n(R) \mid \det \psi \in R^*\}$. Then $GL_n(R)$ is a subgroup of $\mathrm{Aut}_R(R^n)$.

Proof. (1) Easy exercise in checking axioms.

(2) Follows from Cramer's rule about the solution to differential equations.

□

This reduces theorem (8.1) to

Theorem 8.2. *Given any $n \times m$ matrix Φ with entries in R, there are $\Psi_l \in GL_n(R)$ and $\Psi_r \in GL_m(R)$ such that*

$$\Psi_l \Phi \Psi_r = \begin{pmatrix} a_1 & 0 & \ldots & & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & a_s & & \vdots \\ 0 & \ldots & \ldots & 0 & \vdots \\ \vdots & & & & \vdots \\ 0 & \ldots & & \ldots & 0 \end{pmatrix}$$

Proof that theorem (8.2) implies theorem (8.1). Remark (3) implies that $M \cong R^n / \operatorname{im}(\Phi)$. By remark (1),(3) as well as proposition 8.1 and theorem 8.2, we can assume that

$$\Phi = \operatorname{diag}\{a_1, \dots, a_s, 0, \dots, 0\}.$$

So

$$\operatorname{im}(\Phi) = \begin{pmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} R \oplus \begin{pmatrix} 0 \\ a_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} R \oplus \cdots \oplus \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_s \\ 0 \\ \vdots \\ 0 \end{pmatrix} R.$$

Exercise. The universal property of free modules and direct products show that we have a surjective R-module homomorphism

$$R^n \longrightarrow R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_s \rangle \oplus R^{n-s}$$
$$(r_1, \dots, r_n) \mapsto (r_1 + \langle a_1 \rangle, \dots, r_s + \langle a_s \rangle, r_{s+1}, \dots, r_n).$$

Furthermore, the kernel of this map is the same as the image of Φ above, so the first isomorphism theorem completes the proof. □

8.2 Elementary Row and Column Operations

One can perform elementary row and column operations (ERO,ECOs) by left (resp. right) multiplication by elements of $GL_n(R)$

(1) row (resp. column) swaps have determinant -1

(2) adding multiples of one row (resp. column) to another has determinant 1

(3) scalar multiplication of a row (resp. column) by μ has determinant μ.

9 Proof of Structure Theorem

Fix a PID R. We need to prove theorem (8.2).

We may as well assume that $\Phi \neq 0$. Then we are reduced to proving

Theorem 9.1. *There are $\Psi_l \in GL_n(R)$, $\Psi_r \in GL_m(R)$ such that the $(1,1)$ entry $\tilde{\Phi_{11}}$ of $\tilde{\Phi} = \Psi_l \Phi \Psi_r$ divides every other entry of $\tilde{\Phi}$.*

Proof that theorem (9.1) implies theorem (8.2). Note (exercise) that $\tilde{\Phi_{11}} \neq 0$. Then by factoring out $\tilde{\Phi_{11}}$ and using EROs and ECOs we can assume

$$\Phi = \tilde{\Phi_{11}} \begin{pmatrix} 1 & 0 \\ 0 & \Phi_1 \end{pmatrix}.$$

Now we use induction on n (or m) and the matrix Φ_1 to get the result. □

Let us now prove theorem (9.1). Using EROs and ECOs we can assume that $\Phi_{11} \neq 0$. Use induction on the number of prime factors of Φ_{11}.

If Φ_{11} is a unit, then theorem (9.1) holds. We need two lemmas.

Lemma 9.1. Let $a \neq 0, b \in R$ and $d = \gcd(a, b)$. Then there is some $\Psi \in GL_2(R)$ with

$$\Psi \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ c \end{pmatrix}$$

with $c \in \langle a, b \rangle = \langle d \rangle$.

Proof. Note that $dR = aR + bR$ so $\exists f, g \in R$ such that $d = af + bg$. Then

$$\Psi = \begin{pmatrix} f & g \\ -\frac{b}{d} & \frac{a}{d} \end{pmatrix}$$

works as $\det \Psi = 1$. □

Lemma 9.2. Let $0 \neq a, b \in R$ and $d = \gcd(a, b)$. Then there are $\Psi_l, \Psi_r \in GL_2(R)$ such that

$$\Psi_l \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \Psi_r = \begin{pmatrix} d & c_1 \\ c_2 & c_3 \end{pmatrix}$$

with $c_i \in \langle d \rangle$.

Proof. As before we have $f, g \in R$ such that $d = af + bg$. Then

$$\Psi_l = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \qquad \Psi_r = \begin{pmatrix} f & -1 \\ 1 & 0 \end{pmatrix}$$

work. □

We now continue the proof of theorem (9.1). Note first that we can assume Φ_{11} divides all entries in its column. Indeed, suppose not and without loss of generality we may assume $\Phi_{11} \nmid \Phi_{21}$. Then by lemma (9.1) there is a $\Phi \in GL_2(R)$ such that

$$\begin{pmatrix} \Phi & 0 \\ 0 & I_{n-2} \end{pmatrix} \begin{pmatrix} \Phi_{11} & \dots \\ \Phi_{21} & \\ \vdots & \end{pmatrix} = \begin{pmatrix} d & * \\ * & * \end{pmatrix}$$

where $d = \gcd(\Phi_{11}, \Phi_{21})$. Then d has fewer prime factors than Φ_{11}, and so we are done by induction.

Similarly using the transpose of lemma (9.1) we can assume Φ_{11} divides all entries in the first row. Applying EROs and ECOs we can assume

$$\Phi = \begin{pmatrix} \Phi_{11} & 0 \\ 0 & \bar{\Phi} \end{pmatrix}.$$

If $\bar{\Phi_{11}}$ does not divide all entries of $\bar{\Phi}$, then we can use EROs and ECOs to ensure that $\Phi_{11} \nmid \Phi_{22}$. Lemma (9.2) implies that there exists $\Psi_l, \Psi_r \in GL_2(R)$ such that

$$\begin{pmatrix} \Psi_l & 0 \\ 0 & I_{n-2} \end{pmatrix} \Phi \begin{pmatrix} \Psi_r & 0 \\ 0 & I_{n-2} \end{pmatrix} = \begin{pmatrix} d & \\ & * \end{pmatrix}$$

where $d = \gcd(\Phi_{11}, \Phi_{22})$ has fewer prime factors than Φ_{11}. This proves theorem (9.1) and hence theorem (8.2) and the structure theorem for finitely generated modules over a PID.

Example 9.1. Let K be the $\mathbb{Z}$ submodule of $\mathbb{Z}^3$ generated by

$$\left\{ \begin{pmatrix} 3 \\ 2 \\ -2 \end{pmatrix}, \begin{pmatrix} 5 \\ 8 \\ 6 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \end{pmatrix} \right\}$$

Write $M = \mathbb{Z}^3/K$ as a direct sum of cyclic modules.

$M = \mathbb{Z}^3/\operatorname{im}(\Phi)$ where

$$\Phi = \begin{pmatrix} 3 & 5 & 4 \\ 2 & 8 & 5 \\ -2 & 6 & 2 \end{pmatrix}.$$

EROs and ECOs reduce this to

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

so $M \cong \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}$.

Example 9.2. Let $M = \mathbb{Z}^2/(\mathbb{Z}\begin{pmatrix} m \\ 1 \end{pmatrix} + \mathbb{Z}\begin{pmatrix} n \\ 2 \end{pmatrix})$ for some $m, n \in \mathbb{Z}$. Show (assuming M is finite) that $|M| = |2m - n|$.

We have $M \cong \mathbb{Z}^2/\operatorname{im}(\Phi)$ where

$$\Phi = \begin{pmatrix} m & n \\ 1 & 2 \end{pmatrix}.$$

Use theorem (8.2) to find $\Psi_l, \Psi_r \in GL_2(\mathbb{Z})$ with

$$\Psi_l \Phi \Psi_r = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

for $a, b \in \mathbb{Z}$.

Then $M \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ and $|M| = |ab| = |\det(\Psi_l \Phi \Psi_r)| = |2m - n|$.

Proposition 9.1. $GL_n(R) = \operatorname{Aut}_R(R^n)$.

Proof. We say in section 8 that $GL_n(\mathbb{R}) \leq \operatorname{Aut}_R(R^n)$. Suppose that $\Phi \in \operatorname{Hom}_R(R^n, R^n)$ and $\det \Phi = \Delta \notin R^*$. Then there are $\Psi_l, \Psi_r \in GL_n(R)$ such that $\Psi_l \Phi \Psi_r$ is diagonal and $\Delta = u a_1 a_2 \dots a_n$ for some $u \in R^*$.

If $\Delta = 0$, then Φ is not injective. If $\Delta \neq 0$ but is not a unit then

$$\frac{R^n}{\operatorname{im}(\Phi)} \cong \frac{R}{a_1 R} \oplus \cdots \oplus \frac{R}{a_n R}.$$

At least one of the a_i's is not a unit so $R/a_i R \neq 0$. So $\operatorname{im}(\Phi) \neq R^n$ and thus Φ is not surjective.

Therefore $\Phi \in \operatorname{Aut}_R(R^n)$. □

10 Applications of the Structure Theorem

Theorem 10.1 (Alternate structure theorem)**.** *Let R be a PID and M a finitely generated R-module. Then M is a direct sum of cyclic modules of the form R or $R/\langle p^n \rangle$ where $p \in R$ is a prime, and $n \in \mathbb{N}$.*

Proof. From the usual structure theorem, we know M is a direct sum of cyclic modules, so we may suppose that $M = R/\langle a\rangle$ for some $a \in R \setminus \{0\}$. Prime factorise $a = p_1^{n_1} p_2^{n_1} \dots p_r^{n_r}$ and use the Chinese Remainder theorem to get a ring isomorphism

$$\frac{R}{\langle a\rangle} \cong \frac{R}{\langle p_1^{n_1}\rangle} \times \cdots \times \frac{R}{\langle p_r^{n_r}\rangle}.$$

This is clearly R-linear as well, so we are done. □

10.1 Endomorphism Ring

Let R be a ring, and M an R-module. Let

$$\mathrm{End}_R(M) = \{\varphi : M \to M \mid \varphi \text{ is } R\text{-linear}\} = \mathrm{Hom}_R(M, M).$$

Proposition 10.1. The abelian group $\mathrm{End}_R(M)$ is a ring when endowed with ring multiplication equal to composition of homomorphisms. It is called the **endomorphism ring** of M and its elements are called **endomorphisms** of M.

Proof. Exercise in checking axioms. □

Definition 10.1. Let R, S be rings. An (R, S)**-bimodule** is a left R-module M which is also a right S-module with the same additive structure such that we have the associative law

$$(rm)s = r(ms).$$

Example 10.1. Let R be a commutative ring, and M a right R-module. It is also a left R-module with the same addition and left multiplication defined as

$$r \cdot m := mr.$$

This makes M an (R, R)-bimodule.

Exercise. Check axioms.

Example 10.2. R itself is a left and right R-module and hence an (R, R)-bimodule.

Proposition 10.2. Let R be a ring, and M a right R-module. Then M is an $(\mathrm{End}_R(M), R)$-bimodule with left multiplication defined by

$$\varphi \cdot m := \varphi(m).$$

Proof. Exercise in checking axioms. □

We now have an alternative view of bimodules:

Proposition 10.3. Let R, S be rings, and M a right R-module, which by proposition (10.1) is an $(\mathrm{End}_R(M), R)$-bimodule.

(1) Given a ring homomorphism
$$\varphi : S \to \mathrm{End}_R(M),$$
the left $\mathrm{End}_R(M)$-module structure on M "restricts" to a left S-module structure by proposition (4.2). This makes M an (S, R)-bimodule.

(2) Any (S, R)-bimodule arises in this fashion.

Proof. (1) Exercise in checking the associative law for bimodules.

(2) Let M be an (S, R)-bimodule. We construct a ring homomorphism $\varphi : S \to \mathrm{End}_R(M)$ by $\varphi(s)$ =left multiplication by s on M. Note $\varphi(s)$ is R-linear.

Exercise. Check φ is a ring homomorphism.

□

10.2 Jordan Canonical Forms

Suppose k is an algebraically closed field, so the primes in $k[x]$ have the form $\beta(x-\alpha)$ with $\alpha \in k, \beta \in k^*$.

Let $X \in M_n(k) = \text{End}_k(k^n)$. We have the substitution homomorphism

$$\Phi : k[x] \longrightarrow M_n(k)$$
$$p(x) \mapsto p(X).$$

Hence proposition (10.2)(1) implies that we get a $(k[x], k)$-bimodule structure on k^n.

Thus by the alternate structure theorem we have an isomorphism of left $k[x]$-modules (also of bimodules)

$$k^n \cong \frac{k[x]}{\langle (x-\alpha_1)^{n_1} \rangle} \oplus \cdots \oplus \frac{k[x]}{\langle (x-\alpha_r)^{n_r} \rangle}.$$

X acts on k^n by left multiplication by x. Therefore the direct sum decomposition above implies that X is similar to a block diagonal matrix, with block sizes $n_1 \times n_1, \dots, n_r \times n_r$.

The ith block with respect to the basis $1, x-\alpha_i, (x-\alpha_i)^2, \dots, (x-\alpha_i)^{n_i-1}$ is in Jordan canonical form.

11 Exact Sequences and Splitting

11.1 Exact Sequences

Fix a ring R.

Definition 11.1. A **complex** of R-modules is a sequence of R-modules and R-module homomorphisms of the form

$$M_\bullet : \cdots \to M_{i-1} \xrightarrow{d_{i-1}} M_i \xrightarrow{d_i} M_{i+1} \to \dots$$

such that $d^2 := d_i d_{i-1} = 0$ for all i.

Remark. $d^2 = 0$ if and only if $d_i(d_{i-1}(M_{i-1})) = 0$ if and only if $\ker d_i \subseteq \text{im}(d_{i-1})$.

Definition 11.2. A complex $M_\bullet : \cdots \to M_{i-1} \to M_i \to \dots$ is **exact** at M_i if $\ker d_i = \text{im}(d_{i-1})$.

We say $M_\bullet$ is exact if it is exact at all M_i.

Example 11.1. Let $R = \mathbb{Z}$. We have the complex of $\mathbb{Z}$-modules

$$\cdots \to \frac{\mathbb{Z}}{4\mathbb{Z}} \xrightarrow{\iota} \frac{\mathbb{Z}}{4\mathbb{Z}} \xrightarrow{\iota} \dots$$

where each stage is the map $n + 4\mathbb{Z} \mapsto 2n + 4\mathbb{Z}$. This is exact.

Example 11.2. (1) $0 \to M \xrightarrow{f} N$ is an exact sequence of R-modules if and only if f is an R-linear injection (as exactness implies $\ker f = 0$).

(2) $M \xrightarrow{g} N \to 0$ is exact if and only if $\text{im}(g) = N$.

(3) Given a submodule $M \leq N$ we get an exact sequence

$$0 \to M \hookrightarrow N \xrightarrow{\pi} N/M \to 0$$

Corollary 11.1. *Consider the sequence of R-modules and R-module homomorphisms*

$$M_\bullet : 0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

Then M is exact if and only if

(1) f is injective

(2) g is surjective

(3) $\ker g = \operatorname{im}(f)$.

In this case, $M'' \cong M/\operatorname{im}(f)$. We say $M_\bullet$ is a ***short exact sequence (SES)****.*

11.2 Splitting

First some motivation. Recall that given R-modules M', M'' we have the canonical injection

$$\iota : M' \to M' \oplus M''$$

and projection

$$\pi : M' \oplus M'' \to M'.$$

Notice that $\pi\iota = \mathrm{id}$.

Proposition 11.1. Consider the R-module homomorphisms $f : M \to N$ and $g : N \to M$ such that $gf = \mathrm{id}_M$.

(1) Then f is injective, g is surjective and we say f is a **split injection** and g is a **split surjection**.

(2) We have a direct sum decomposition

$$\begin{pmatrix} f & \mathrm{id}_{\ker g} \end{pmatrix} : M \oplus \ker g \xrightarrow{\sim} N,$$

and we say M is a direct summand of N.

(3) Given either f or g, we say the other map splits it (e.e. f splits g and g splits f).

Proof. (1) Easy exercise in set theory.

(2) We construct an inverse as follows. First note that

$$\mathrm{id}_N - fg : N \to N$$

has image in $\ker g$. This is because

$$g(\mathrm{id}_N - fg) = g - gfg = g - g = 0.$$

It follows that we can assume $\mathrm{id}_N - fg : N \to \ker g$. We claim that the inverse to $\Phi = \begin{pmatrix} f & \mathrm{id}_{\ker g} \end{pmatrix}$ is

$$\Psi = \begin{pmatrix} g \\ \mathrm{id}_N - fg \end{pmatrix}.$$

To see this, we observe that

$$\begin{aligned} \Phi\Psi &= \begin{pmatrix} f & \mathrm{id}_{\ker g} \end{pmatrix} \begin{pmatrix} g \\ \mathrm{id}_N - fg \end{pmatrix} \\ &= fg + \mathrm{id}|_{\ker g}(\mathrm{id}_N - fg) \\ &= fg + \mathrm{id}_N - fg \\ &= \mathrm{id}_N. \end{aligned}$$

Similarly, we have

$$\begin{aligned}\Psi\Phi &= \begin{pmatrix} g \\ \mathrm{id}_N - fg \end{pmatrix} \begin{pmatrix} f & \mathrm{id}_{\ker g} \end{pmatrix} \\ &= \begin{pmatrix} gf & g\,\mathrm{id}_{\ker g} \\ \mathrm{id}_N f - fgf & (\mathrm{id} - fg)|_{\ker g} \end{pmatrix} \\ &= \mathrm{id}_{M \oplus \ker g}.\end{aligned}$$

□

Corollary 11.2. *Consider a short exact sequence of R-modules*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

(1) f is a split injection if and only if g is a split surjection

(2) in this case, $M \cong M' \oplus M''$ and we say the short exact sequence is ***split****.*

Proof. Exercise. □

Example 11.3.

$$0 \to \frac{\mathbb{Z}}{3\mathbb{Z}} \xrightarrow{2} \frac{\mathbb{Z}}{6\mathbb{Z}} \xrightarrow{g} \frac{\mathbb{Z}}{2\mathbb{Z}} \to 0$$

with $2 : n + 3\mathbb{Z} \mapsto 2n + 6\mathbb{Z}$, and $g : n + 6\mathbb{Z} \mapsto n + 2\mathbb{Z}$. This is a split short exact sequence, where g is split by the "multiplication by 3" map, that is, $h : n + 2\mathbb{Z} \mapsto 3n + 2\mathbb{Z}$.

Exercise. Show that gh =multiplication by 3 which is the identity on $\mathbb{Z}/2\mathbb{Z}$.

Example 11.4.

$$0 \to \frac{\mathbb{Z}}{2\mathbb{Z}} \xrightarrow{2} \frac{\mathbb{Z}}{4\mathbb{Z}} \xrightarrow{\pi} \frac{\mathbb{Z}}{2\mathbb{Z}} \to 0$$

is exact but not split as $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

11.3 Idempotents

Definition 11.3. Let R be a ring, and $e \in R$. e is an **idempotent** if $e^2 = e$.

Exercise. Let M be an (R, S)-bimodule. Show that left multiplication by e

$$\lambda_e : M \to eM$$

is a split surjection of right S-modules. It is split by the inclusion map $eM \hookrightarrow M$.

Show that $M \cong eM \oplus (1 - e)M$.

Exercise. Consider a finite set of idempotents $\{e_1, \ldots, e_n\} \subseteq R$. We say they are **complete** and **orthogonal** if $\sum_i e_i = 1$ and $e_i e_j = 0$ if $i \neq j$.

Show that

$$M \cong e_1 M \oplus \cdots \oplus e_n M.$$

12 Chain Conditions

Let R be a ring, and M a (right) R-module.

Definition 12.1. M is

(1) **noetherian** if it satisfies the **ascending chain condition** (ACC): for any chain of submodules

$$M_1 \leq M_2 \leq \cdots \leq M$$

stabilises in the sense that $M_n = M_{n+1} = \ldots$ for all $n > N$.

(2) **artinian** if it satisfies the **descending chain condition** (DCC): for any chain of submodules

$$M \geq M_1 \leq M_2 \geq \ldots$$

stabilises.

Example 12.1. Let k be a field, and V a finite dimensional vector space. Then V is both noetherian and artinian as any strictly increasing or decreasing chain of subspaces has strictly increasing/decresing dimension.

Example 12.2. Let R be a PID. Then $M = R_R$ is noetherian but not artinian.

Why? Pick a nonzero, non-unit $r \in R$. We obtain a strictly decreasing chain of submodules

$$R \gneq \langle r \rangle \gneq \langle r^2 \rangle \gneq \ldots$$

so R_R is not artinian. However, consider the strictly increasing chain of ideals

$$\langle r_1 \rangle \leq \langle r_2 \rangle \leq \langle r_3 \rangle \leq \ldots$$

so $r_2 \mid r_1$, $r_n \mid r_{n-1}$. Since the number of prime factors will stabilise, M is noetherian.

12.1 Submodules and Quotients

Proposition 12.1. Let R be a ring and N a submodule of an R-module M. Then M is noetherian (resp. artinian) if and only if N and M/N are.

Proof. We only prove the noetherian result. First, suppose that M satisfies the ACC, and therefore N satisfies the ACC trivially. Then let $\pi : M \to M/N$ be the projection map, and consider the chain of submodules

$$\overline{M_1} \leq \overline{M_2} \leq \ldots$$

Exercise. We get an ascending chain of submodules of M

$$\pi^{-1}(\overline{M_1}) \leq \pi^{-1}(\overline{M_2}) \leq \ldots$$

ACC on M implies that for n large enough, this chain stabilises. Now π is surjective so $\pi\pi^{-1}(\overline{M_i}) = \overline{M_i}$, and so the first chain stabilises in M/N and thus the ACC holds for M/N as well.

Conversely, suppose that the ACC holds for N and M/N. Consider a chain of submodules of M

$$M_1 \leq M_2 \leq \ldots$$

We then get induced chains on N and M/N:

$$M_1 \cap N \leq M_2 \cap N \leq \ldots$$
$$\pi(M)1 \leq \pi(M_2) \leq \ldots$$

ACC on N and N/M means that these chains stabilise and we may assume that n is large enough that $M_n \cap N = M_{n+1} \cap N = \ldots$ and $\pi(M_n) = \pi(M_{n+1}) = \ldots$. It now suffices to prove

Claim 12.1. *Suppose given $L_1 \leq L_2 \leq \ldots M$ with $L_1 \cap N = L_2 \cap N$ and $\pi(L_1) = \pi(L_2)$ Then $L_1 = L_2$.*

Proof. It suffices to show that $L_2 \leq L_1$. Pick $m_2 \in L_2$ and we know

$$\pi(m_1) = m_2 + N \in \pi(L_2) = \pi(L_1)$$

so $m_2 + N = m_1 + N$ for some $m_1 \in L_1$. Therefore $m_2 - m_1 \in N \cap L_1 \subseteq L_1$.
It follows that $m_2 = m_1 + (m_2 - m_1) \in L_1$. □

□

Remark. Proposition (12.1) is equivalent to the following statement.
For any short exact sequence of R-modules

$$0 \to M' \to M \to M'' \to 0$$

then M is noetherian (resp. artinian) if and only if M' and M'' are.

Corollary 12.1. *(1) If M_1, M_2 are noetherian (resp. artinian) then so is $M_1 \oplus M_2$.*

(2) If M_1, M_2 are noetherian (resp. artinian) submodules of M, then $M_1 + M_2$ is noetherian (resp. artinian).

Proof. (1) We have a split exact sequence

$$0 \to M_1 \xrightarrow{\iota_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \to 0.$$

(2) We have a surjective homomorphism

$$\begin{aligned} \begin{pmatrix} \iota & \iota \end{pmatrix} : M_1 \oplus M_2 &\to M_1 + M_2 \\ (m_1, m_2) &\mapsto m_1 + m_2, \end{aligned}$$

so (1) and proposition (12.1) give the result.

□

12.2 Finite Generation

Proposition 12.2. An R-module M is noetherian if and only if every submodule is finitely generated.

Proof. Suppose M is infinitely generated. If suffices to construct a strictly ascending chain of finitely generated submodules inductively: set $M_0 = 0$ and

$$M_n = \sum_{i=1}^{n} f_i R$$

where f_{n+1} is any element of $M \setminus M_n$ (this is possible because M is infinitely generated but M_n is finitely generated). Putting

$$M_{n+1} = M_n + f_{n+1} R.$$

Conversely, consider an ascending chain of submodules

$$M_1 \leq M_2 \leq \ldots$$

Exercise.

$$M' := \bigcup_{i \geq 1} M_i$$

is a submodule.

Therefore it is finitely generated by say $m_1, \dots, m_r$. Hence we can pick n large enough so $M_n \ni m_1, \dots, m_r$. Thus

$$M' = \sum_{i=1}^{r} m_i R = M_n = M_{n+1} = \dots$$

so the ACC holds. □

13 Noetherian Rings

Definition 13.1. A ring R is (right) noetherian (resp. artinian) if the module R_R is noetherian (resp. artinian).

Example 13.1. Let k be a field. Then any finite dimensional k-algebra A is right and left notherian and artinian.

Furthermore, any PID is noetherian, but $k\langle x, y\rangle$ is not noetherian or artinian.

Proposition 13.1. Let R be a right noetherian ring.

(1) An M-module M is noetherian if and only if M is finitely generated.

(2) Every submodule of a finitely generated R-module is itself finitely generated.

Proof. (1) $\Rightarrow$ (2) by proposition (12.1), so it remains to prove (1). The forward direction follows from proposition (12.2). Conversely, if M is finitely generated, there exists elements $m_1, \dots, m_n \in M$ with $M = m_1 R + \dots + m_n R$. Each $m_i R$ is noetherian as it is a quotient of R_R, and hence M is noetherian by corollary (12.1). □

Exercise. If R is right noetherian, so is R/I for every $I \lhd R$.

13.1 Almost Normal Extensions

Definition 13.2. Let S and R be rings such that R is a subring of S. We say S is an **almost normal extension** of R with **almost normal generator** a if

(1) $R + aR = R + Ra$, so (exercise: induction)

$$R + aR + a^r R + \dots + a^d R = R + Ra + \dots + Ra^d$$

that is, any "right" polynomial in a (with coefficients in R) of degree $\leq d$ is also a left polynomial in a with degree $\leq d$.

(2) $S = \bigcup_{d \geq 0} R + Ra + \dots + Ra^d$

We then write $S = R\langle a\rangle$.

Example 13.2. Let R be a ring. Then $R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])\,[x_n]$ is an almost normal extension of $R[x_1, \dots, x_{n-1}]$ with almost normal generator x_n.

Example 13.3. Consider the Weyl algebra $\mathbb{C}\langle x, \partial\rangle = \mathbb{C}[x]\langle\partial\rangle$ – this is an almost normal extension of $\mathbb{C}[x]$ with almost normal generator ∂.

Why? We know (by the Weyl relation) $\partial x = x\partial + 1$ and so $\mathbb{C}[x] + \partial\mathbb{C}[x] = \mathbb{C}[x]\partial + \mathbb{C}[x]$.

13.2 Hilbert's Basis Theorem

Theorem 13.1 (Hilbert)**.** *Let R be a right noetherian ring and let $S = R\langle a\rangle$ be an almost normal extension with almost normal generator a. The S is right noetherian.*

Proof. By proposition (12.2), it suffices to show that any right ideal $I \lhd S$ is finitely generated. We consider the set of "degree j leading coefficients"

$$I_j := \left\{ r_j \in R \mid \sum_{i=0}^{j} r_i a^i \in I \right\} \subseteq R$$

for each $j \geq 0$.

Note that $I_j \subseteq I_{j+1}$ since I is closed under right multiplication by a.

Claim 13.1. *I_j is also a right ideal of R.*

Proof. Let $r_j \in I_j$, so we have some $\sum_{i=0}^{j} r_i a_i \in I$. Note that I_j is an additive subgroup because I is. Now, let $r \in R$. Definition 13.2(1) implies that $ra^j = a^j r' +$ lower order terms in a. Then

$$\begin{aligned} I \ni \sum_{i=0}^{j} r_i r_i a^i r' &= r_j a^j r' + \text{ lower order terms} \\ &= r_j r a^j + O(a^{j-1}) \end{aligned}$$

and so $r_j r \in I_j$. □

ACC on R_R implies that for d large enough, we have $I_d = I_{d+1} = \dots$. Note

$$I^{\leq d} = (R + Ra + \cdots + Ra^d) \cap I = (R + aR + \cdots + a^d R) \cap I$$

is a finitely generated R-module since it is a submodule of the noetherian module $R+\cdots+Ra^d$. Thus we can find $f_1, \dots, f_s \in I^{\leq d}$ with $f_1 R + \cdots + f_s R = I^{\leq d}$. It suffices to show that $I' := f_1 S + \cdots + f_s S \supseteq I$, since $I \supset I'$.

Define

$$I'_j := \left\{ r_j \in R \mid \sum_{i=0}^{j} r_i a^i \in I' \right\} \subset I_j.$$

But

$$I' \cap (R + \cdots + a^d R) \geq (f_1 R + \cdots + f_s R) \cap (R + aR + \cdots + a^d R) = I \cap (R + aR + \cdots + a^d R) \quad (13.1)$$

and so $I'_d = I_d = I_{d+1} = I'_{d+1}$ so $I'_t = I_t$ for $t \geq d$. We now show

$$r = r_t a^t + r_{t-1} a^{t-1} + \cdots + r_0 \in I$$

is in I' by induction on t.

If $t \leq d$, then this holds by (13.1). Otherwise, we know $I'_t = I_t$ so there exists $\sum_{i=0}^{t} r'_i a^i \in I'$ with $r'_t = r_t$. Then $r - r' \in I \cap (R + \cdots + Ra^{t-1})$ so we are done by induction. □

Corollary 13.1. *If R a noetherian ring, so is $R[x_1, \dots, x_n]$. Furthermore, the Weyl algebra is noetherian.*

14 Composition Series

14.1 Simple Modules

Let R be a ring.

Definition 14.1. An R-module $M \neq 0$ is called **simple** or **irreducible** if the only submodules of M are 0 and M itself.

A right ideal $I \lhd R$ is **maximal** if the only ideal strictly containing I is R. We say I is **minimal** if the only ideals contained in I are 0 and I.

Proposition 14.1. A right module M is simple if and only if $M \cong R/I$ for some maximal $I \lhd R$.

Proof. Suppose M is simple, and pick $m \in M \setminus \{0\}$. Consider the homomorphism $\lambda_m : R \to M$ which maps $r \mapsto mr$. Note that λ_m is surjective as $\text{im}(\lambda_m)$ is a nonzero submodule of the simple module M. The first isomorphism theorem implies that $M \cong R/I$ for some $I = \ker \lambda_m$. Now, I is maximal, for if not we can find an ideal I' with $I \lneq I' \lneq R$. This gives a nontrivial submodule of M corresponding to I'/I.

The converse is clear by reversing the above argument. □

Example 14.1. Let R be a PID. Simple modules correspond to $R/\langle p\rangle$ for some $p \in R$ prime.

Example 14.2. Let R be the Weyl algebra $\mathbb{C}\langle x, \partial\rangle$, and M the left R-module $\mathbb{C}[x]$. Then M is simple for given a submodule N containing some nonzero element, say $p(x) = p_n x^n + \cdots + p_0 \neq 0$, then $N \ni \frac{1}{p_n n!}\frac{d}{dx^n}p(x) = 1$, so $N = M$.

14.2 Composition series

Definition 14.2. Let M be an R-module. A **composition series** is a chain of submodules

$$0 < M_1 < M_2 < \cdots < M_n = M$$

such that M_{i+1}/M_i is simple for all i.

In this case, we call M_{i+1}/M_i the **composition factors** of M and say M has **finite length**.

Example 14.3. Let $R = k[x]$, and $M = k[x]/\langle x^2\rangle$. Then M has composition series

$$0 < \frac{\langle x\rangle}{\langle x^2\rangle} < M.$$

Thus

$$\frac{k[x]/\langle x^2\rangle}{\langle x\rangle/\langle x^2\rangle} \cong \frac{k[x]}{\langle x\rangle}$$

is simple. Also, we have the isomorphism

$$\frac{k[x]}{\langle x\rangle} \cong \frac{\langle x\rangle}{\langle x^2\rangle}$$

that maps $1 \mapsto x + \langle x^2\rangle$. Therefore the composition series has a repeated composition factor, $k[x]/\langle x\rangle$.

14.3 Jordan Hölder Theorem

Theorem 14.1. *Let M be an R-module with two composition series*

$$0 < M_1 < M_2 < \cdots < M_n = M \tag{14.1}$$

and

$$0 < M_1' < M_2' < \cdots < M_m' = M. \tag{14.2}$$

*Then $n = m$ (called the **length** of M). Also, there exists a permutation σ of $\{1, \dots, n\}$ such that*

$$\frac{M_i}{M_{i-1}} \cong \frac{M'_{\sigma(i)}}{M'_{\sigma(i-1)}},$$

that is, the composition factors are equal up to isomorphism.

Proof. By induction on n with the case $n = 0$ clear.

Suppose that $n \geq 1$. Note that we have the following composition series for M/M_1:

$$0 = \frac{M_1}{M_1} < \frac{M_2}{M_1} < \cdots < \frac{M}{M_1} \tag{14.3}$$

which has the same composition factors as (14.1) except one copy of M_1 is removed.

We construct another composition series for M/M_1 as follows. Note that M_1 is simple, so for any i, we have $M_i' \cap M_1$ is either 0 or all of M_1, in which case $M_i' \supseteq M_1$. Hence we can find a j such that $M_j' \cap M_1 = 0$ but $M_{j+1}' \cap M_1 = M_1$. Note $(M_1 + M_j')/M_j'$ is a nonzero submodule of M_{j+1}'/M_j' and so must equal it.

Hence

$$\begin{aligned} M_1 &\cong \frac{M_1}{M_1 \cap M_j'} \\ &\cong \frac{M_1 + M_j'}{M_j'} \\ &\cong \frac{M_{j+1}'}{M_j'}. \end{aligned}$$

It suffices by induction to now prove

Claim 14.1. *We have the following composition series for M/M_1*

$$0 < \frac{M_1' + M_1}{M_1} < \frac{M_2' + M_1}{M_1} < \cdots < \frac{M_j' + M_1}{M_1} = \frac{M_{j+1}'}{M_1} < \cdots < \frac{M}{M_1} \tag{14.4}$$

and this has the same composition factors as (14.2) except one copy of $M_{j+1}'/M_j' \cong M_1$ is removed.

Proof. For $i > j$, we have

$$\frac{M_{i+1}'/M_1}{M_i'/M_1} \cong \frac{M_{i+1}'}{M_i'} \text{ simple.}$$

For $i \leq j$, we have composition factors

$$\begin{aligned} \frac{(M'_{i+1} + M_1)/M_1}{(M'_i + M_1)/M_1} &\cong \frac{M'_{i+1} + M_1}{M'_1 + M_1} \\ &\cong \frac{M'_{i+1} + (M'_i + M_1)}{M'_i + M_1} \\ &\cong \frac{M'_{i+1}}{M'_{i+1} \cap (M'_i + M_1)} \\ &\cong \frac{M'_{i+1}}{M'_i}. \end{aligned}$$

If $m \in M'_{i+1}$ and $m = m_i + m_1$ with $m_i \in M'_i$ and $m_1 \in M_1$, then

$$m - m_i = m_1 \in M'_{i+1} \cap M_1 = 0$$

and so $m_1 = 0$, $m \in M'_i$ and we are done. □

□

Exercise. If $M_1, \ldots, M_n$ are simple, find a composition series for $M_1 \oplus \cdots \oplus M_n$.

Remark. Any simple module is noetherian and artinian.

Exercise. Show M has finite length if and only if M is noetherian and artinian.

15 Semisimple Modules

Let R be a ring.

Proposition 15.1. A (right) R-module M is **semisimple** if any of the following equivalent conditions hold

(1) Any submodule $M' \leq M$ is a direct summand

(2) Any surjective homomorphism $M \to M''$ is split

(3) Any short exact sequence of the form

$$0 \to M' \to M \to M'' \to 0$$

splits.

Proof. Easy exercise. □

Example 15.1. Let $R = k[x]$, with k a field. Then $k[x]/\langle x^2 \rangle$ is not semisimple because

$$0 \to \frac{\langle x \rangle}{\langle x^2 \rangle} \hookrightarrow M \to \frac{k[x]}{\langle x^2 \rangle} \to 0$$

is not split. However,

$$M = \frac{k[x]}{\langle x(x-1) \rangle} \cong \frac{k[x]}{\langle x \rangle} \oplus \frac{k[x]}{\langle x-1 \rangle}$$

is semisimple (as the direct summands are semisimple).

Lemma 15.1. Let M be a semisimple module, and $N \leq M$. Then N is semisimple.

Proof. Let $N' \leq N \leq M$. As M is semisimple, the map $N' \hookrightarrow M$ is split by $\pi : M \to N'$. Restrict π to N, and hence $\pi|_N : N \to N'$ also splits $N' \hookrightarrow N$, so by proposition (15.1)(1) N is also semisimple. □

Lemma 15.2. Let $M \neq 0$ be a cyclic module. Then there exists a quotient M/N which is simple.

Proof. M cyclic implies that $M = mR$ for some $m \in M$. We thus find a surjective homomorphism $R \xrightarrow{m} M$. The first isomorphism theorem then implies that we can assume $M = R/I$ for some right ideal I. Zorn's lemma tells us that we can find a right ideal J such that

(1) $J \supseteq I$;

(2) $1 \neq J$; and

(3) J is maximal with respect to these properties.

Call this maximal J J_{max}. Indeed, let $\mathscr{S}$ be the set of such J, then given an increasing chain of right ideals in $\mathscr{S}$

$$I \subseteq J_1 \subseteq J_2 \subseteq \dots$$

we have

$$J_\infty = \bigcup_{i \in \mathbb{N}} J_i$$

is an upper bound in $\mathscr{S}$ since

Exercise. J_∞ is a right ideal which satisfies the properties above.

The maximality of J_{max} implies that any right ideal strictly containing J_{max} contains 1 and therefore is R.

Hence

$$\frac{R/I}{J_{max}/I} \cong \frac{R}{J_{max}}$$

is the desired simple quotient. □

Lemma 15.3. Let $N \leq M$. Then there exists a submodule $N' \leq M$ such that

(a) N' is a direct sum of simple modules

(b) $N \cap N' = 0$

(c) for any simple submodule $N_s \leq M$ we have

$$(N + N') \cap N_s \neq 0.$$

Proof. Let $\{N_s\}_{s \in S}$ be the set of simple submodules of M and $\mathscr{S} \subset \mathcal{P}(S)$ be the set of $J \subseteq S$ such that

(1) $N_J := \sum_{j \in J} N_j$ is a direct sum in the sense that the natural map

$$\bigoplus_{j \in J} N_j \longrightarrow \sum N_j$$

is an isomorphism.

(2) $N \cap N_J = 0$.

By Zorn's lemma

Exercise. $\mathscr{S}$ has a maximal element, say J_{max}.

We wish to show $N' = N_{J_{max}}$ satisfies the lemma. Note that (1) and (2) give (a) and (b). We need only check (c) so suppose instead that there exists a simple module N_s with

$$(N + N') \cap N_s = 0. \tag{15.1}$$

We will show that $J' = J_{max} \cup \{S\}$ contradicts the maximality of J_{max}. Note that $N_s \cap N' = N_S \cap N_{J_{max}} = 0$, so

$$N_{J'} = N_S \oplus N'$$

so (1) holds. We show (2) holds for J', that is, $N \cap N_{J'} = 0$.

Suppose instead that $(N_S + N') \cap N \ni n = n_S + n'$, Since (c) is assumed to be false, $n - n' = n_s \in (N + N') \cap N_S$ so $n - n' = n_s = 0$. This means that $n = n' \in N \cap N' = 0$ by (b). This is a contradiction, so $(N_S + N') \cap N = 0$. □

Theorem 15.1. *The following are equivalent for an R-module M*

(1) M is semisimple

(2) $M \cong \bigoplus M_j$ *with* M_j *simple for all* j.

Proof. Suppose that M is semisimple. By lemma (15.3) with $N = 0$ we get a direct sum of simples $N' \leq M$ such that

$$N' \cap N_S = 0$$

for N_S simple. It suffices to show that $M = N'$. Proposition (15.1) implies that $M = N' \oplus N''$ for some $N'' \leq M$. Pick $n'' \in N'' \setminus \{0\}$, so the submodule $n''R$ is also semisimple by lemma (15.1). By lemma (15.2), $n''R$ has a simple quotient N'''. The semisimplicity of $n''R$ implies that it has a submodule N_S isomorphic to N'''. But $N_S \cap N' \subseteq N'' \cap N' = 0$, so (c) in lemma (15.3) is violated.

Conversely, Let $N \leq M$, N' be as in lemma (15.3). It suffices to show $M = N' + N$ for we know $N \cap N' = 0$.

Suppose $M \neq N + N'$, so there exists $M_j \leq N + N'$. But M_j is simple, and therefore $(N + N') \cap M_j = 0$. This contradicts (c) in lemma (15.3), so $N + N' = M$. □

Exercise. Let $R = \mathbb{Z}[x]$. Show that $R/\langle 6x \rangle$ is not semisimple, but $R/\langle 6, x \rangle$ is.

16 Semisimple rings and Group Representations

Proposition 16.1. A ring R is semisimple if either of the following equivalent conditions hold

(1) Any short exact sequence of right R-modules

$$0 \to M' \to M \to M'' \to 0$$

splits

(2) R_R is semisimple.

Proof. It is clear that (1) $\Rightarrow$ (2) on setting $M = R_R$. For (2) $\Rightarrow$ (1), (2) and theorem (15.1) imply that any free module is a direct sum of simple modules and so is semisimple. Any M is a quotient of a free module F, and the semisimplicity of F implies that M is isomorphic to a summand of F so is semisimple by lemma (15.1). $\square$

Example 16.1. Let D be a division ring. Then D is right and left semisimple since ${}_DD$ and D_D are simple and therefore semisimple.

More generally,

Proposition 16.2. Let D be a division ring and $R = M_n(D)$. Then

(1) D^n is a simple right R-module

(2) $M_n(D)$ is semisimple.

Proof. (1) Consider $N \le D^n$ which is nonzero. It suffices to show $N = D^n$.
Pick $(\alpha_1, \dots, \alpha_n) \in N$ with $\alpha_i \neq 0$. Let $\varphi \in M_n(D)$ with α_i^{-1} in the $(1, i)$th entry and zeroes elsewhere. Then $N \ni (\alpha_1, \dots, \alpha_n)\varphi = (1, 0, \dots, 0)$ and so

$$N \ni (1, 0, \dots, 0) \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ * & * & * & * \end{pmatrix} = (\beta_1, \dots, \beta_n) \in D^n.$$

So $N = D^n$ and D^n must be simple.

(2) $R = M_n(D)$ is right semisimple because R_R has the following direct sum decomposition into simple modules (using (1))

$$M_n(D) = \begin{pmatrix} D & \dots & D \\ \vdots & \ddots & \vdots \\ D & \dots & D \end{pmatrix} = \begin{pmatrix} D^n \\ 0 \\ \vdots \\ 0 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 0 \\ \vdots \\ 0 \\ D^n \end{pmatrix} \cong D^n \oplus \cdots \oplus D^n.$$

Similarly R is left semisimple.

$\square$

Proposition 16.3. Let $R_1, \dots, R_n$ be rings, and $R = R_1 \times \cdots \times R_n$ their product. Then

(1) Given R_i-modules M_i for each i, we obtain an R-module structure on

$$M = M_1 \times \cdots \times M_n$$

with scalar multoplication defined by

$$(m_1, \dots, m_n)(r_1, \dots, r_n) := (m_1 r_1, \dots, m_n r_n).$$

(2) Conversely, every R-module has this form (the M_i are called the **components** of M).

Proof. (1) Check module axioms.

(2) We give a sketch proof in the case $n = 2$. Let $R = R_1 \times R_2$, and consider the nonunital subrings $\begin{pmatrix} 1 & 0 \end{pmatrix} R = R_1 \times \{0\} \cong R_1$ and $\begin{pmatrix} 0 & 1 \end{pmatrix} R \cong R_2$. Let M be an R-module, and $M_1 = M \begin{pmatrix} 1 & 0 \end{pmatrix}$, $M_2 = M \begin{pmatrix} 0 & 1 \end{pmatrix}$.

Exercise. Note M_1 is a module over $R_1 = \begin{pmatrix}1 & 0\end{pmatrix} R$ "since"

$$\begin{aligned} M_1R_1 &= M\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} R \\ &= M\begin{pmatrix}1 & 0\end{pmatrix} R \\ &= MR\begin{pmatrix}1 & 0\end{pmatrix} \\ &= M\begin{pmatrix}1 & 0\end{pmatrix} \\ &= M_1. \end{aligned}$$

Similarly, M_2 is an R_2-module.

it now suffices to show

$$\begin{aligned} \varphi : M_1 \times M_2 &\longrightarrow M \\ (m_1, m_2) &\mapsto m_1 + m_2 \end{aligned}$$

is an R-module isomorphism by showing

Exercise. (a) $M_1 + M_2 = M$ since given any $m \in M$ we have $m = m\begin{pmatrix}1 & 1\end{pmatrix} = m\begin{pmatrix}1 & 0\end{pmatrix} + m\begin{pmatrix}0 & 1\end{pmatrix}$

(b) $M_1 \cap M_2 = 0$ since given $m \in M_1 \cap M_2$, $m \in M_1 \Rightarrow m1_{R_1} = m\begin{pmatrix}1 & 0\end{pmatrix}$ and $m \in M_2 \Rightarrow m = m1_{R_2} = m\begin{pmatrix}0 & 1\end{pmatrix}$. It follows that $m\begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = m = 0$.

(c) Show φ is actually R-linear.

□

Corollary 16.1. *Any finite product $R = R_1 \times \cdots \times R_n$ of semisimple rings is also semisimple.*

Proof. Each $R_i \cong \bigoplus_{j=1}^{i_r} M_{i_j}$ for simple R_i-modules M_{i_j}.

Exercise. Note that these sums are finite as 1 must have a nonzero component in each M_{i_j}.

So

$$R_R = \left(\bigoplus_{j=1}^{i_1} M_{1_j} \times 0 \times \cdots \times 0\right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{i_n} 0 \times \cdots \times 0 \times M_{n_j}\right)$$

is a decomposition of R_R into a direct sum of simple modules. □

16.1 Group Representations

Let G be a group, and R a commutative ring.

Definition 16.1. An (R-linear) **representation** of G is a group homomorphism

$$\rho : G \longrightarrow \mathrm{Aut}_R(V)$$

for some R-module V.

Remark. (1) $\mathrm{Aut}_R(V)$ is a subgroup of the permutation group of V so the group representation above gives a G-set such that each $g \in G$ acts linearly on V.

Exercise. Given any G-set such that every $g \in G$ acts linearly on V, we obtain a group representation.

Such G-sets are called G-modules.

(2) (a) Given any left RG-module M, we may consider it an (RG, R)-bimodule with right action of R equal to the left action. This is well defined as $R \subseteq Z(RG)$.

(b) Proposition (10.2) implies that such an (RG, R)-bimodule structure is equivalent to giving the right R-module M and a ring homomorphism

$$\Phi : RG \longrightarrow \text{End}_R(M)$$

(c) Given such an R-algebra homomorphism we obtain by restriction a group representation

$$\rho : G \to \text{Aut}_R(M).$$

Conversely, any such group representation extends linearly to an R-algebra homomorphism $RG \to \text{End}_R(M)$.

Exercise. Let $G = \langle\sigma\rangle$ be a cyclic group of order n, and $A = \mathbb{C}G$, $M = \mathbb{C}$. We have the group representation

$$\rho : G \to \text{Aut}_A(\mathbb{C}) = \mathbb{C}^*$$

defined by $\sigma \mapsto \omega$, some nth root of unity.

This gives by remark (2) a $\mathbb{C}G$-module with left action

$$\left(\sum_{i=0}^{n-1} \alpha_i \sigma^i\right) \alpha := \sum_{i=0}^{n-1} \alpha_i \omega^i \alpha.$$

17 Maschke's Theorem

17.1 Reynold's Operator

Let G be a finite group of order n, and R a commutative ring such that $n \in R^*$. For example, it R is a field then this condition just means $\text{char}\, R \nmid n$.

Let M be a left RG-module.

Proposition 17.1. The **fixed submodule** of M is

$$M^G := \{m \in M \mid gm = m \ \forall g \in G\}.$$

This is an R-submodule of M.

Proof. Exercise in checking axioms. □

Note that M can be viewed as an (RG, R)-bimodule with right R-action the same as the left action. Consider the element

$$e = \frac{1}{|G|} \sum_{g \in G} g \in RG$$

which is well defined since $|G| \in R^*$.

Now consider the right R-linear map induced by left multoplication by e,

$$(\cdot)^\natural : M \longrightarrow M.$$

This is called the **Reynold's operator**.

Lemma 17.1. (1) $\text{im}((\cdot)^\natural) \subseteq M^G$

(2) The induced map $(\cdot)^\natural : M \to M^G$ splits the inclusion map $\iota : M^G \hookrightarrow M$ (that is, $(\cdot)^\natural$ projects onto M^G).

Proof. (1) Let $m \in M$, $g \in G$. Then

$$\begin{aligned} gm^\natural &= g\frac{1}{|G|}\sum_{h\in G} hm \\ &= \frac{1}{|G|}\sum_{h\in G} ghm \\ &= \frac{1}{|G|}\sum_{h'\in G} h'm \\ &= m^\natural. \end{aligned}$$

So $m^\natural \in M^G$ and (1) holds.

(2) We need to check $(\cdot)^\natural \circ \iota : M^G \hookrightarrow M \to M^G$ is the identity on M^G. Let $m \in M^G$, then

$$\begin{aligned} (\iota m)^\natural &= m^\natural \\ &= \frac{1}{|G|}\sum_{g\in G} gm \\ &= \frac{1}{|G|}|G|m \text{ since } m \in M^G \\ &= m. \end{aligned}$$

So $(\cdot)^\natural \circ \iota = \mathrm{id}_{M^G}$ and $\natural$ splits ι.

□

17.2 $\mathrm{Hom}_R(M, N)$

Let R be a commutative ring, G a finite group and M, N R-modules.

Proposition 17.2. The abelian group $\mathrm{Hom}_R(M, N)$ has the structure of an R-module with scalar multiplication defined by

$$(rf)(m) := rf(m) = f(rm)$$

for $r \in R, f \in \mathrm{Hom}_R(M, N)$ and $m \in M$.

Proof. Exercise in checking axioms. □

Proposition 17.3. Suppose now that M, N are RG-modules, corresponding to R-linear group representations $\rho_M : G \to \mathrm{Aut}_R(M)$ and $\rho_N : G \to \mathrm{Aut}_R(N)$.

Then $H := \mathrm{Hom}_R(M_R, N_R)$ is a left RG-module with corresponding group representation

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{Aut}_R(H_R) \\ g &\mapsto \big((M \to N) \ni f \mapsto \rho_N(g) \circ f \circ \rho_M(g^{-1}) \in (M \to M \to N \to N)\big). \end{aligned}$$

Proof. It suffices to show ρ is a well defined group homomorphism.

(1) Note $\rho_N(g) \circ f \circ \rho_M(g^{-1}) \in H$ since it is a composition of R-linear maps

(2) Also $\rho(g) : f \mapsto \rho_N(g) \circ f \circ \rho_M(g^{-1})$ is in $\mathrm{Aut}_R(H)$ since it is clearly invertible (with inverse $\rho(g^{-1})$) and it is clearly (exercise) R-linear.

(3) ρ is a group homomorphism, for given $g, h \in G$ we have for all $f \in H$,

$$\begin{aligned}[\rho(gh)](f) &= \rho_N(gh) \circ f \circ \rho_M(h^{-1}g^{-1}) \\ &= \rho_N(g) \circ \rho_N(h) \circ f \circ \rho_M(h^{-1}) \circ \rho_M(g^{-1}) \\ &= \rho(g)(\rho(h)f) \\ &= (\rho(g)\rho(h))(f).\end{aligned}$$

□

Lemma 17.2. Let M, N be RG-modules. A function $f : M \to N$ is RG-linear if and only if it is R-linear and for all $g \in G$, $m \in M$,

$$f(gm) = gf(m).$$

Proof. The forward direction is clear. For the converse, it suffices to check

$$f\left(\left(\sum_{g\in G} r_g g\right) m\right) = \left(\sum_{g\in G} r_g g\right) f(m).$$

But

$$\begin{aligned}f\left(\left(\sum_{g\in G} r_g g\right) m\right) &= f\left(\sum_{g\in g} r_g gm\right) \\ &= \sum_{g\in G} r_g f(gm) \\ &= \left(\sum_{g\in G} r_g g\right) f(m).\end{aligned}$$

□

Proposition 17.4. Let M, N be RG-modules. Then

$$\mathrm{Hom}_R(M, N)^G = \mathrm{Hom}_{RG}(M, N).$$

Proof. Let $f \in \mathrm{Hom}_R(M, N)$ and $g \in G$. Then

$$\begin{aligned}gf = f &\Leftrightarrow [\rho(g)]f = f \\ &\Leftrightarrow f \circ \pi_M(g)\rho_N(g) \circ f \\ &\Leftrightarrow \forall m \in M,\ f(gm) = gf(m).\end{aligned}$$

Lemma (17.2) then implies that $f \in \mathrm{Hom}_R(M, N)^G \Leftrightarrow f \in \mathrm{Hom}_{RG}(M, N)$. □

Theorem 17.1 (Maschke)**.** *Let G be a finite group, k a field such that $\operatorname{char} k \nmid |G|$. Then kG is left (and right) semisimple.*

Proof. Consider the inclusion of kG-modules

$$\iota : N \to M.$$

It suffices to show that ι splits.

Now k is a field and therefore is semisimple, so there is a k-module splitting $\pi : M \to N \in \mathrm{Hom}_k(M, N)$. Proposition (17.3) and lemma (17.1) imply that $\pi^\natural \in \mathrm{Hom}_k(M, N)^G = \mathrm{Hom}_{kG}(M, N)$. It now suffices to show $\pi^\natural$ splits ι, that is,

$$\pi^\natural \circ \iota = \mathrm{id}_N .$$

Let $n \in N$, then

$$\begin{aligned}
\pi^\natural(\iota(n)) &= \pi^\natural(n) \\
&= \left[\left(\frac{1}{|G|}\sum_{g\in G} g\right)\pi\right](n) \\
&= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}n) \\
&= \frac{1}{|G|}\sum_{g\in G} gg^{-1}n \\
&= \frac{1}{|G|}\sum_{g\in G} n \\
&= n.
\end{aligned}$$

So $\pi^\natural \circ \iota = \mathrm{id}_N$ and therefore $\pi^\natural$ splits ι and hence kG is left semisimple. □

Exercise. Let $G = \langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$ act on the vector space V of real valued functions on $\mathbb{R}$ by

$$(\sigma f)(x) := f(-x).$$

V is an $\mathbb{R}G$-module. Explore the Reynold's operator and the fixed submodule in this case.

18 Wedderburn's Theorem

Let R be a ring.

18.1 Schur's Lemma

Lemma 18.1 (Schur)**.** Let M, N be simple R-modules.

(1) Any R-module homomorphism $\varphi : M \to N$ is either 0 or invertible

(2) $\mathrm{End}_R(M)$ is a division ring

Proof. It is clear that (1) implies (2) as every nonzero element of $\mathrm{End}_R(M)$ is invertible by (1). So it remains to prove (1).

Suppose $\varphi : M \to N$ is not the zero map. Then $\mathrm{im}(\varphi) \le N$ is nonzero, so we must have $\mathrm{im}(\varphi) = N$ as N is simple. Also, $\ker\varphi \le M$ and $\ker\varphi \ne M$ so $\ker\varphi = 0$ and thus φ is injective. So φ is an isomorphism. □

18.2 Structure Theory

Lemma 18.2. The isomorphism of abelian groups

$$\begin{aligned}\Phi : E &\longrightarrow \mathrm{End}_R(R) = \mathrm{Hom}_R(R_R, R_R)\\ r &\mapsto (\lambda_r : s \mapsto rs)\end{aligned}$$

is an isomorphism of rings.

Proof. Just note that $\lambda_1 = \mathrm{id}_R = 1_{\mathrm{End}_R(R)}$ and for $r, s \in R$, we have

$$\Phi(rs) = \lambda_{rs} = \lambda_r \lambda_s = \Phi(r)\Phi(s).$$

□

Theorem 18.1 (Wedderburn)**.** *Let R be a right semisimple ring. Then*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

where the D_i are division rings, and $r, n_i \in \mathbb{Z}$.

Proof. Theorem (15.1) implies that

$$R_R \cong V_1^{n_1} \oplus V_2^{n_2} \oplus \cdots \oplus V_r^{n_r}$$

for some simple nonisomorphic modules V_i.

Exercise. The sum is finite because the image of 1 in each component must be nonzero.

Schur's lemma implies that

$$\mathrm{Hom}_R(V_i, V_j) = \begin{cases} 0 & i \neq j \\ D_i & i = j \end{cases}$$

where D_i is a division ring.

Now, lemma (18.2) implies that we have the following ring isomorphisms

$$\begin{aligned}R &\cong \mathrm{End}_R(R_R)\\ &= \mathrm{End}_R(V_1^{n_1} \oplus \cdots \oplus V_r^{n_r})\\ &\cong \bigoplus_{i,j=1}^{r} \mathrm{Hom}_R\left(V_i^{n_i}, V_j^{n_j}\right) \text{ by the universal property of } \oplus\\ &= M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r).\end{aligned}$$

□

Remark. The $M_{n_i}(D_i)$ are called the **simple** or **Wedderburn components** of R. They are well defined by the following addendum:

Addendum 18.1. *The numbers n_i and division rings D_i are uniquely determined by R up to isomorphism and permutation.*

Proof. Continuing the above notation, suppose also that

$$R \cong M_{n'_1}(D'_1) \times \cdots \times M_{n'_s}(D'_s)$$

for some division rings D'_i. Then (abusing notation)

$$R_R = \left(D'^{n'_1}_1\right)^{n'_1} \oplus \cdots \oplus \left(D'^{n'_s}_s\right)^{n'_s}.$$

The Jordan-Hölder theorem implies that (on reindexing) we may suppose $n_i = n'_i$ and $V_i \cong (D'_i)^{n'_i}$ (and $r = s$).

To show $D'_i \cong D_i$, we use

Lemma 18.3. For $R = M_n(D)$ with D a division ring, we have

$$\mathrm{End}_R\left(D^n\right) = D.$$

Proof. Note that $\mathrm{End}_R\left(D^n\right)$ is a subring of $\mathrm{End}_D\left(D^n\right) = M_n(D)$.

Exercise. Show it is the subring of scalar matrices.

□

□

Corollary 18.1. *A right semisimple ring is left semisimple and conversely a left semisimple ring is right semisimple.*

Proof. If R is right semisimple, then $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ where D_i are division rings. These are left semisimple.

For the converse, we can apply the left hand version of Wedderburn's theorem, or note

Exercise. R is left semisimple if and only if R^{op} is right semisimple.

So left semisimplicity implies right semisimplicity. □

Scholium 1. Any semisimple ring is noetherian and artinian.

18.3 Module Theory

Corollary 18.2. *Let $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ where the D_i are all division rings.*

(1) The only simple modules up to isomorphism are $D_1^{n_1}, \ldots, D_r^{n_1}$

(2) Any R-module is a direct sum of these simples.

Proof. (1) $\Rightarrow$ (2) since R is semisimple, so it remains to prove (1).

Let M be a simple right R-module. Proposition (14.1) implies that we know $M \cong R/I$ for some maximal ideal I.

Now M is a composition factor for R since any composition series for I gives one for R. But $R_R \cong \bigoplus (D_i^{n_i})^{n_i}$ so the composition factors are all of the form $D_i^{n_i}$. □

Definition 18.1. For $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ with each D_i a division ring, the components of any R-module are called **isotypic components.**

18.4 Finite dimensional Semisimple Algebras

Let k be an algebraically closed field, and R a finite dimensional k-algebra.

Lemma 18.4. If R is a division ring, then $R = k$.

Proof. Exercise (or note for $r \in R$, $k[r] \subset R$ is a finite field extension of k). □

Corollary 18.3. *Let R be a semisimple k-algebra whose simple modules have dimension $n_1, \ldots, n_r$. Then*

$$\dim kR = n_1^2 + \cdots + n_r^2.$$

Proof. By Wedderburn's theorem and lemma (18.4) we know $R \cong M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ so the simples are $k^{n_1}, \ldots, k^{n_r}$. Then

$$\dim kR = \dim \prod M_{n_i}(k) = \sum n_i^2.$$

□

Example 18.1. Let $G = S_3$, the symmetric group on three symbols. Maschke's theorem implies that $\mathbb{C}G$ is semisimple, so $\mathbb{C}G \cong \prod_{i=1}^{r} M_{n_i}(\mathbb{C})$, where

$$n_1^2 + \cdots + n_r^2 = \dim_{\mathbb{C}} \mathbb{C}G = |G| = 6.$$

The only possibilities are

$$6 = 1^2 + \cdots + 1^2 \text{ or}$$
$$6 = 1^2 + 1^2 + 2^2.$$

But $\mathbb{C}G \ncong \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C}$, as $\mathbb{C}^6$ is commutative but $\mathbb{C}G$ is not. So

$$\mathbb{C}G \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}).$$

It follows that there are exactly three simple $\mathbb{C}G$-modules up to isomorphism.

19 One-dimensional Representations

19.1 Abelianisation

Let G be a group.

Definition 19.1. Let $g, h \in G$. The **commutator** of g and h is

$$[g, h] = g^{-1}h^{-1}gh.$$

The subbgroup of G generated by these is called the **commutator subgroup** and is denoted $[G, G]$.

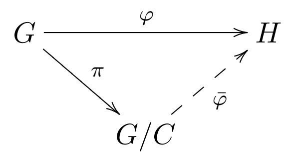
Lemma 19.1. (1) $C := [G, G] \trianglelefteq G$

(2) G/C is an abelian group called the **abelianisation** of G (denoted G_{ab})

(3) Let H be any abelian group and $\varphi : G \to H$ any group homomorphsim. Then

$$\ker \varphi \supseteq C = [G, G]$$

so there is a commutative diagram of the form



(that is, $\varphi = \bar{\varphi} \circ \pi$).

Proof. (1) Let $f, g, h \in G$. Then

$$\begin{aligned} f^{-1}[g,h]f &= f^{-1}g^{-1}h^{-1}ghf \\ &= (f^{-1}g^{-1}f)(f^{-1}h^{-1}f)(f^{-1}gf)(f^{-1}hf) \\ &= [f^{-1}gf, f^{-1}hf] \\ &\in [G, G] \end{aligned}$$

so $f^{-1}[g,h]f \in [G,G]$ and hence $[G,G] \trianglelefteq G$.

(2) We have

$$\begin{aligned} (gC)(hC) &= gh(h^{-1}g^{-1}hg)C \\ &= hgC \\ &= hCgC \end{aligned}$$

so G/C is abelian.

(3) It suffices to show $\varphi([g,h]) = 1_H$. But

$$\varphi(g^{-1}h^{-1}gh) = \varphi(g)^{-1}\varphi(h)^{-1}\varphi(g)\varphi(h) = 1$$

since H is abelian.

□

19.2 One-dimensional representations

Let k be a field.

Lemma 19.2. The isomorphism classes of one-dimensional kG-modules are in one-to-one correspondence with group representations of the form

$$\rho : G \to \mathrm{Aut}_k(k) = k^* = GL_1(k)$$

that is, one-dimensional representations.

Proof. Suppose we have a one-dimensional kG-module V. It corresponds to a group representation of the form

$$\rho_V : G \to \mathrm{Aut}_k(V) \cong k^*$$

with the isomorphism given by the map $\alpha \in k^* \mapsto \lambda_\alpha$, the multiplication by α map. This one-dimensional representation depends only on the isomorphism class of V, for if $\varphi : V \to W$ is a kG-module isomorphism then for any $v \in V,\ g \in G$ we have

$$\varphi(gv) = g\varphi(v).$$

Therefore

$$\varphi(\rho_V(g)v) = \rho_W(g)\varphi(v) \tag{19.1}$$

and hence $V \cong W \Rightarrow \rho_V = \rho_W$.

Conversely, if $\rho_V = \rho_W$ then by (19.1) any vector space isomorphism is an isomorphism of kG-modules. We also know any one-dimensional representation arises from the above since there is a kG-module structure on k associated to any one-dimensional representation

$$\rho : G \to k^* = \mathrm{Aut}_k\left(k\right).$$

□

Exercise. Extend this to n-dimensional kG-modules as follows.

An n-dimensional representation is a group representation of the form

$$\rho : G \longrightarrow \mathrm{Aut}_k\left(k^n\right) \cong GL_n(k).$$

We put an equivalence relation on the representations by $\rho_1 \sim \rho_2$ if $\rho_1 = c_A \circ \rho_2 : G \xrightarrow{\rho_2} GL_n(k) \to GL_n(k)$ where c_A is conjugation by some matrix $A \in GL_n(k)$.

Equivalence classes of n-dimensional representations correspond to the isomorphism classes of n-dimensional kG-modules.

Corollary 19.1. *The isomorphism classes of one-dimensional modules correspond to the elements of the abelian group* $\mathrm{Hom}_{\mathbb{Z}}\left(G_{ab}, k^*\right)$.

Proof. Use lemmas (19.1)(3) and (19.2). □

Remark. (1) If G is finite and you know to write

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_r\mathbb{Z}$$

then we know

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}}\left(G, k^*\right) &= \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{i=1}^{r} \mathbb{Z}/a_i\mathbb{Z}, k^*\right)\\ &= \prod_{i=1}^{r} \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/a_i\mathbb{Z}, k^*\right)\\ &= \prod_{i=1}^{r} \mu_{a_i,k}\end{aligned}$$

where $\mu_{a_i,k}$ is the subgroup of a_ith roots of unity in k. The last equality follows by the universal property of quotients and the fact

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, k^*\right) = k^*$$

so then $\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/a_i\mathbb{Z}, k^*\right)$ are those $\alpha \in k^*$ with $\alpha^{a_i} = 1$.

(2) The zero in $\mathrm{Hom}_{\mathbb{Z}}(G_{ab}, k^*)$ is the trivial representation $\rho : G \mapsto 1_k$.

Corollary 19.2. *Let k be an algebraically closed field with $\operatorname{char} k \nmid |G|$, and G a finite group. Then*

$$kG \cong \prod_{i=1}^{|G_{ab}|} k \times \prod_{j=1}^{s} M_{n_j}(k)$$

where all $n_j \geq 2$.

Proof. Follows from section 18 and the fact that the number of one-dimensional representations is

$$|\mathrm{Hom}_{\mathbb{Z}}(G_{ab}, k^*)| = |G_{ab}|$$

□

Example 19.1. Let $G = A_4$, the alternating group on four symbols. Then $|A_4| = 12$. Let

$$H := \{(12)(34), (13)(24), (14)(23)\} \subset A_4$$

Exercise. This is a normal subgroup of A_4 by computation or Sylow's theorem.

In fact

Exercise. Show $H = [G, G]$

and so $G_{ab} = G/H \cong \mathbb{Z}/3\mathbb{Z}$. It follows that $|G/H| = 3$. Hence the one-dimensional representations over $\mathbb{C}$ are the elements of $\mathrm{Hom}_{\mathbb{Z}}(G_{ab}, \mathbb{C}^*)$, and there are $|G_{ab}| = 3$ of these. They are

$$\rho_0 : G \longrightarrow 1 \qquad \begin{aligned} \rho_1 : G &\longrightarrow \mathbb{C}^* \\ H &\mapsto 1 \\ (123) &\mapsto e^{2\pi i/3} \\ (123)^2 &\mapsto e^{4\pi i/3} \end{aligned} \qquad \begin{aligned} \rho_2 : G &\longrightarrow \mathbb{C}^* \\ H &\mapsto 1 \\ (123) &\mapsto e^{4\pi i/3} \\ (123)^2 &\mapsto e^{2\pi i/3} \end{aligned}$$

Since $\dim_{\mathbb{C}} \mathbb{C}G = |G| = 12$, corollary (19.2) implies that

$$\mathbb{C}G \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M_3(\mathbb{C}).$$

Therefore there are 4 simple $\mathbb{C}G$-modules up to isomorphism – three with dimension 1 and one with dimension 3.

Exercise. Figure out the three-dimensional representation.

20 Centres of Group Algebras

20.1 Centres of Semisimple Rings

Proposition 20.1. Let $R = R_1 \times \cdots \times R_r$. Then

$$Z(R) = Z(R_1) \times \cdots \times Z(R_r).$$

Proof. $z = (z_1, \ldots, z_r) \in Z(R)$ if and only if for any $(r_1, \ldots, r_r) \in R$ we have $(z_1, \ldots, z_r)(r_1, \ldots, r_r) = (r_1, \ldots, r_r)(z_1, \ldots, z_r)$. Therefore we must have $z_i r_i = r_i z_i$ for all i, and so $z_i \in Z(R_i)$. □

Proposition 20.2. Let R be a ring. Then $Z(M_n(R)) = Z(R)$.
[Note: the right hand side of the equality is technically $Z(R)1_{M_n(R)}$.]

Proof. Easy exercise – check commutativity with row and column swaps. □

Corollary 20.1. *Let k be an algebraically closed field and A a finite dimensional semisimple k-algebra. Then*

$$\dim_k Z(A) = \#(\textit{Wedderburn components of } A) = \#(\textit{isomorphism classes of simple } kG\textit{-modules}).$$

Proof. Wedderburn's theorem implies that $A \cong \prod_{i=1}^{r} M_{n_i}(k)$. Then propositions (20.1) and (20.2) imply that

$$\begin{aligned} Z(A) &= \prod_{i=1}^{r} Z(k) \\ &= \prod_{i=1}^{r} k \end{aligned}$$

so $\dim_k Z(A) = \#(\text{Wedderburn components of } A)$. □

20.2 Centres of group algebras

Let R be a commutative ring, and G a group.

Lemma 20.1.

$$Z(RG) = \{z \in RG \mid zg = gz \ \forall g \in G\}.$$

Proof. We see $\subseteq$ so we check the other inclusion, so assume $z \in RG$ commutes with every $g \in G$. Consider an arbitrary element of RG, $\sum r_g g$. Then

$$\begin{aligned} z \sum_{g \in G} r_g g &= \sum_{g \in G} z r_g g \\ &= \sum_{g \in G} r_g z g \\ &= \sum_{g \in G} r_g g z \\ &= \left(\sum_{g \in G} r_g g \right) z. \end{aligned}$$

□

Let $C \subset G$ be a conjugacy class and $\Sigma_C = \sum_{g \in C} g$.

Proposition 20.3. $Z(RG) = \bigoplus_C R\Sigma_C$ where C ranges over all conjugacy classes of G.

Proof. By lemma (20.1),

$$\begin{aligned}
z = \sum r_g g \in Z(RG) &\Leftrightarrow zh = hz \; \forall h \in G \\
&\Leftrightarrow \sum_{g \in G} r_g g = \sum_{g \in G} r_g h^{-1} g h \; \forall h \in G \\
&\Leftrightarrow \sum_{g \in G} r_g g = \sum_{l \in G} r_l l \text{ where } l = h^{-1} g h \\
&\Leftrightarrow \forall g, h \in G \text{ we have } r_g = r_{hgh^{-1}} \\
&\Leftrightarrow \text{for each conjugacy class, there is a scalar } r_C \in R \\
&\quad\;\; \text{such that } r_g = r_C \text{ for all } g \in C \\
&\Leftrightarrow z = \sum_C r_c \Sigma_C.
\end{aligned}$$

□

Corollary 20.2. *Let k be an algebraically closed field and G a finite group with $\operatorname{char} k \nmid G$. Then*

$$\#(\textit{simple } kG\textit{-modules up to isomorphism}) = \#(\textit{conjugacy classes of } G).$$

Proof. Maschke's theorem implies that kG is semisimple, so corollary (20.1) implies that $\dim_k Z(kG)$ is equal to the number of simple kG-modules. But proposition (20.3) implies that $\dim_k Z(kG)$ is equal to the number of conjugacy classes of G, so we are done. □

20.3 Irreducible representations of dihedral groups

Let

$$G = D_n = \langle \sigma, \tau \mid \sigma^n = 1 = \tau^2, \; \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$$

be the dihedral group of order $2n$ with $n \geq 3$ odd. We will work over $k = \mathbb{C}$.

First step is to find G_{ab}. See

$$[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau = \sigma^{-2}$$

which generates $\langle \sigma \rangle$ since n is odd. Hence $\langle \sigma \rangle \subseteq [G, G]$, but $G/\langle \sigma \rangle \cong \mathbb{Z}/2\mathbb{Z}$ is abelian, so $\langle \sigma \rangle = [G, G]$ and $G_{ab} = \mathbb{Z}/2\mathbb{Z}$.

The one-dimensional complex representations correspond to elements of

$$\operatorname{Hom}_{\mathbb{Z}} (G_{ab}, \mathbb{C}^*) \cong \{\pm 1\}.$$

Thus the representations are

$$\begin{aligned} \rho_0 : G &\longrightarrow 1 \\ \langle \sigma \rangle &\mapsto 1 \\ \langle \tau \rangle &\mapsto 1 \end{aligned} \qquad\qquad \begin{aligned} \rho_{-1} : G &\longrightarrow \mathbb{C}^* \\ \langle \sigma \rangle &\mapsto 1 \\ \langle \tau \rangle &\mapsto -1. \end{aligned}$$

We now find the conjugacy classes. $\sigma\tau\sigma^{-1} = \tau\sigma^{-2}$ shows (exercise) that all reflections $\tau, \tau\sigma, \ldots, \tau\sigma^{n-1}$ are conjugate.

The other conjugacy classes are

$$\left\{\sigma, \sigma^{-1}\right\}, \; \left\{\sigma^2, \sigma^{-2}\right\}, \ldots, \left\{\sigma^{(n-1)/2}, \sigma^{(n+1)/2}\right\}.$$

There are $(n-1)/2+2=(n+3)/2$ conjugacy classes. It then follows that there are $(n+3)/2$ simple $\mathbb{C}G$-modules. Furthermore, we have

$$\dim_{\mathbb{C}} \mathbb{C}D_n = 2n = 2 + \left(\frac{n-1}{2}\right)\cdot 4 = 1^2+1^2+\underbrace{2^2+2^2+\cdots+2^2}_{(n-1)/2 \text{ terms}}.$$

Thus corollary (20.2) implies that

$$\mathbb{C}D_n \cong \mathbb{C}\times\mathbb{C}\times\prod_{i=1}^{\frac{n-1}{2}} M_2(\mathbb{C}).$$

There are two one-dimensional simple $\mathbb{C}D_n$-modules, all of the others are dimension 2. These two-dimensional simples are given by representations as follows for $j=1,\ldots,\frac{n-1}{2}$

$$\begin{aligned}\pi_j : G &\longrightarrow GL_2(\mathbb{C})\\ \sigma &\mapsto \begin{pmatrix} e^{2\pi ij/n} & 0\\ 0 & e^{-2\pi ij/n}\end{pmatrix}\\ \tau &\mapsto \begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}.\end{aligned}$$

Note that these are simple because they are not direct sums of one-dimensionals. Also, they are nonisomorphic because the eigenvalues of $\rho_j(\sigma)$ differ (see exercise in section 19).

Exercise. Do this for n even.

21 Categories and Functors

Definition 21.1. A **category** $\mathscr{C}$ consists of the following data:

(1) A class $\operatorname{Obj}\mathscr{C}$ of **objects**

(2) A collection of sets $\operatorname{Hom}_{\mathscr{C}}(X,Y)$, one for each ordered pair $X,Y\in\operatorname{Obj}\mathscr{C}$ whose elements are called **morphisms** (from $X\to Y$), denoted by $\varphi : X\to Y$.

(3) A collection of mappings, one for each ordered triple $X,Y,Z\in\operatorname{Obj}\mathscr{C}$, with

$$\begin{aligned}\operatorname{Hom}_{\mathscr{C}}(X,Y)\times\operatorname{Hom}_{\mathscr{C}}(Y,Z) &\longrightarrow \operatorname{Hom}_{\mathscr{C}}(X,Z)\\ (\varphi,\psi)&\mapsto \psi\varphi=\psi\circ\varphi\end{aligned}$$

called the **composition** of φ,ψ.

These data also satisfy the following conditions:

(a) The sets $\operatorname{Hom}_{\mathscr{C}}(X,Y)$ are piecewise distinct

(b) The composition of morphisms is associative: $(\xi\psi)\varphi=\xi(\psi\varphi)$ for any $\varphi : X\to Y,\ \psi : Y\to Z,\ \xi : Z\to W$.

(c) For any $X\in\operatorname{Obj}\mathscr{C}$, $\exists$ an identity morphism $\mathrm{id}_X : X\to X$ such that $(\mathrm{id}_X)\varphi=\varphi$ and $\psi(\mathrm{id}_X)=\psi$ whenever these compositions are defined.

Example 21.1. **Grp** is the category of groups with

- Obj $\underline{\textbf{Grp}}$: the class of all groups
- $\text{Hom}_{\underline{\textbf{Grp}}}(G, H)$: group homomorphisms from G to H
- composition: composition of group homomorphisms.

Example 21.2. $\underline{\textbf{Ring}}$, the category of rings

Example 21.3. Let R be a ring. We then have two induced categories

- R-$\underline{\textbf{mod}}$: the category of left R-modules
- $\underline{\textbf{mod}}$-R: the category of right R-modules

Example 21.4. Let R be a commutative ring. We then have the category R-$\underline{\textbf{alg}}$ of R-algebras.

Example 21.5. $\underline{\textbf{Top}}$, the category of topological spaces.

21.1 Functors

Definition 21.2. A **covariant functor** F from category $\mathscr{C}$ to category $\mathscr{D}$ (notated $F : \mathscr{C} \to \mathscr{D}$) consists of the following data:

(1) A mapping from Obj $\mathscr{C}$ to Obj $\mathscr{D}$ denoted by $X \mapsto FX$

(2) For each $X, Y \in \text{Obj}\,\mathscr{C}$, a function

$$F : \text{Hom}_{\mathscr{C}}(X, Y) \longrightarrow \text{Hom}_{\mathscr{D}}(FX, FY).$$

These data also satisfy the following conditions:

(a) $F(\psi\varphi) = F\psi F\varphi$ for any $\varphi, \psi \in \text{Mor}(\mathscr{C})$ defined

(b) $F(\text{id}_X) = \text{id}_{FX}$ for all $X \in \text{Obj}\,\mathscr{C}$

If F is a functor, we also say F is **functorial**.

Example 21.6 (Group algebra functor)**.** Fix R a commutative ring. We have the following covariant functor

$$F : \underline{\textbf{Grp}} \longrightarrow R - \underline{\textbf{alg}}$$

defined by the mappings

- Objects: for $G \in \underline{\textbf{Grp}}$, have $FG = RG$, the group algebra over R
- Morphisms: for $\varphi : G \to H$ we have

$$\begin{aligned} F\varphi : RG &\longrightarrow RH \\ \sum r_g g &\mapsto \sum r_g \varphi(g). \end{aligned}$$

We need $F\varphi$ to be an R-algebra map, that is

$$F : \text{Hom}_{\underline{\textbf{Grp}}}(G, H) \longrightarrow \text{Hom}_{R-\underline{\textbf{alg}}}(RG, RH)$$

It is clear that φ is R-linear so we check that products are preserved:

$$\begin{aligned}
F\varphi\left((\sum_g r_g g)(\sum_h s_h h)\right) &= F\varphi\left(\sum_{k\in G}\sum_{gh=k}(r_g s_h)k\right) \\
&= \sum_{k\in G}\left(\sum_{gh=k} r_g s_h\right)\varphi(k) \\
&= \sum_{k\in G}\left(\sum_{gh=k} r_g s_h\right)\varphi(g)\varphi(h) \\
&= \left(\sum_g r_g\varphi(g)\right)\left(\sum_h s_h\varphi(h)\right) \\
&= F\varphi(\sum r_g g)F\varphi(\sum s_h h).
\end{aligned}$$

Exercise. Check F is a functor.

Definition 21.3. A **contravariant functor** $F : \mathscr{C} \to \mathscr{D}$ is defined similarly to definition (21.2) except (2) is replaced with

($2'$) For each $X, Y \in \operatorname{Obj}\mathscr{C}$, a function

$$F : \operatorname{Hom}_{\mathscr{C}}(X,Y) \longrightarrow \operatorname{Hom}_{\mathscr{D}}(FY,FX)$$

and (a) is replaced with

(a') $F(\varphi\psi) = F(\psi)F(\varphi)$ for any $\varphi,\psi \in \operatorname{Mor}(\mathscr{C})$ defined.

Remark. Let R, S be rings. Note that R-$\underline{\textbf{mod}}$ (and $\underline{\textbf{mod}}$-R) have the additional property that for $M, N \in \operatorname{Obj} R$-$\underline{\textbf{mod}}$,

$$\operatorname{Hom}_{R-\underline{\textbf{mod}}}(M,N) = \operatorname{Hom}_R(M,N)$$

are abelian groups, so a functor $F : R$-$\underline{\textbf{mod}} \longrightarrow S$-$\underline{\textbf{mod}}$ is **additive** if all of the morphism maps are group homomorphisms.

21.2 Hom functor

Let R be a ring, and $M, M', N \in \underline{\textbf{mod}}$-$R$. We define a contravariant additive functor

$$F_n = \operatorname{Hom}_R(-,N) : \underline{\textbf{mod}} - R \longrightarrow \underline{\textbf{mod}} - \mathbb{Z}$$

by

- $F_n(M) = \operatorname{Hom}_R(M,N)$, and
- $$\begin{aligned}
F_N \operatorname{Hom}_R\left(M,M'\right) &\longrightarrow \operatorname{Hom}_{\mathbb{Z}}\left(\operatorname{Hom}_R\left(M',N\right), \operatorname{Hom}_R(M,N)\right) \\
\varphi &\mapsto \left((M' \xrightarrow{f} N) \mapsto (M \xrightarrow{\varphi} M' \xrightarrow{f} N)\right).
\end{aligned}$$

Proposition 21.1. $F_n = \operatorname{Hom}_R(-,N)$ is indeed a contravariant additive functor. We also say $\operatorname{Hom}_R(M,N)$ is functorial in M.

Similarly, $\operatorname{Hom}_R(M,N)$ is covariantly functorial in N.

Proof. Mainly exercise. □

22 Tensor Products I

22.1 Construction of Tensor Products

Let R be a ring, $M \in \underline{\textbf{mod}}\text{-}R$ and $N \in R\text{-}\underline{\textbf{mod}}$. We wish to construct an abelian group $M \otimes_R N$.

We start by considering the free $\mathbb{Z}$-module $\mathbb{Z}(M \times N)$ with free generators (m, n) as m, n vary over M, N. Consider the subgroup K generated by elements of the form below, where $m, m' \in M$, $n, n' \in N$ and $r \in R$

(a) $(m + m', n) - (m, n) - (m', n)$

(b) $(m, n + n') - (m, n) - (m, n')$

(c) $(mr, n) - (m, rn)$

Definition 22.1. The **tensor product** of M and N is the abelian group $M \otimes_R N = \mathbb{Z}(M \times N)/K$.

We denote the image of (m, n) in $M \otimes_R N$ by $m \otimes n$ and call it an **elementary tensor**. (a),(b),(c) above give the following relations

(1) $(m + m') \otimes n = m \otimes n + m' \otimes n$

(2) $m \times (n + n') = m \otimes n + m \otimes n'$

(3) $mr \otimes n = m \otimes rn$.

Remark.

$$0_M \otimes n = 0 \otimes n + 0 \otimes n \Longrightarrow 0 \otimes n = 0.$$

Example 22.1. $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

We see this as $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$ is generated by elementary tensors

$$a \otimes b = a \otimes 4b = 2a \otimes 2b = 0 \otimes 2b = 0.$$

22.2 Universal property of tensor products

Definition 22.2. Let $M \in \underline{\textbf{mod}}\text{-}R$, $N \in R\text{-}\underline{\textbf{mod}}$ and A an abelian group. A function $\varphi : M \times N \to A$ is **mid-linear** if for $m, m' \in M$, $n, n' \in N$ and $r \in R$ we have

(1) $\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)$

(2) $\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')$

(3) $\varphi(mr, n) = \varphi(m, rn)$.

Example 22.2.

$$\iota_\otimes : M \times N \longrightarrow M \otimes_R N$$
$$(m, n) \mapsto m \otimes n$$

is mid-linear by definition (22.1).

Proposition 22.1 (Universal property)**.** With the above notation, there are inverse bijections

$$\begin{array}{ccc} & \varphi \longmapsto (\tilde{\varphi} : m \otimes n \mapsto \varphi(m, n)) & \\ \{\text{mid-linear } \varphi : M \times N \to A\} & \underset{\Psi}{\overset{\Phi}{\longleftrightarrow}} & \{\text{abelian group homs } \tilde{\varphi} : M \otimes_R N \to A\} \\ & \varphi = \tilde{\varphi} \circ \iota_\otimes \longleftarrow \tilde{\varphi}. & \end{array}$$

Proof. Note first that by the universal property of free modules we have a group homomorphism $\tilde{\tilde{\varphi}} : \mathbb{Z}(M \times N) \to A$ such that $(m, n) \mapsto \varphi(m, n)$. By the universal property of quotients, we need $\tilde{\tilde{\varphi}}(K) = 0$ where K is as in definition (22.1). But this follows precisely because φ is mid-linear. So Φ is well defined.

Exercise. Check Ψ is well defined, that is, $\tilde{\varphi} \circ \iota_{\otimes}$ is indeed mid-linear.

We now check $\Psi\Phi = \text{id}$.

$$\begin{aligned} [(\Psi\Phi)\varphi]\,(m, n) &= [(\Phi\varphi) \circ \iota_{\otimes}]\,(m, n) \\ &= (\Phi\varphi)(m \otimes n) \\ &= \varphi(m, n) \end{aligned}$$

so $\Psi\Phi(\varphi) = \varphi$ and $\Psi\Phi = \text{id}$.

Exercise. Check $\Phi\Psi = \text{id}$.

□

22.3 Functoriality

Let R be a ring, $M, M' \in$ **mod**-R, $N \in R$-**mod**. Consider an R-linear map $\varphi : M \to M'$ and the induced homomorphism

$$\begin{aligned} \varphi \otimes_R N : M \otimes_R N &\longrightarrow M' \otimes_R N \\ m \otimes n &\longmapsto \varphi(m) \otimes n \end{aligned}$$

Note that this is a homomorphism by the universal property as we can check the mid-linearity of

$$\begin{aligned} \bar{\varphi} : M \times N &\longrightarrow M' \otimes_R N \\ (m, n) &\longmapsto \varphi(m) \otimes n. \end{aligned}$$

Proposition 22.2. $M \otimes_R N$ is covariantly functorial and additive in both M and N.

Proof. We have $1_M \otimes_R N = 1_{M \otimes_R N}$. Furthermore, given $M \xrightarrow{\varphi} M' \xrightarrow{\varphi'} M''$, we have

$$(\varphi'\varphi) \otimes_R N : M \otimes_R N \to M'' \otimes_R N = (\varphi' \otimes_R N)(\varphi \otimes_R N) : M \otimes_R N \to M' \otimes_R N \to M'' \otimes_R N.$$

Exercise. Check additivity, and the case for N.

□

22.4 Bimodules

Proposition 22.3. Let $R, S, T \in$ **Ring**, $M \in$ **mod**-R, $N \in R$-**mod**.

(1) If M is an (S, R)-bimodule, then $M \otimes_R N$ is a left S-module with multiplication $s(m \otimes n) = sm \otimes n$

(2) If M is an (R, T)-bimodule, then $M \otimes_R N$ is a right T-module, with multiplication $(m \otimes n)t = m \otimes nt$.

If both (1) and (2) occur, then $M \otimes_R N$ is an (S, T)-bimodule.

Proof. Mainly exercise in checking module axioms. Alternatively, (1) and (2) can be proven along the following lines.

Note $\lambda_s : M \to M$ given by left multiplication by s is a homomorphism $M_R \to M_R$. By functoriality, we have the induced homomorphism of abelian groups

$$\lambda_s \otimes N : M \otimes_R N \longrightarrow M \otimes_R N$$

giving left multiplication by s on $M \otimes_R N$. Functoriality and additivity imply the module axioms, and we are done. □

23 Tensor Products II

23.1 Identity

Let R be a ring, and recall R is an (R, R)-bimodule.

Proposition 23.1. Let $M \in R$-**mod**.

(1) Then there are inverse left R-**mod** isomorphisms

$$\begin{aligned} m &\longmapsto 1 \otimes m \\ M &\overset{\Phi}{\underset{\Psi}{\longleftrightarrow}} R \otimes_R M \\ rm &\longleftarrow r \otimes m \end{aligned}$$

(2) If M is an (R, S)-bimodule for some ring S then Φ, Ψ are right S-linear.

Proof. We check Ψ is well defined by the universal property for tensor products, that is, check

$$\begin{aligned} \tilde{\Psi} : R \times M &\longrightarrow M \\ (r, m) &\longmapsto rm \end{aligned}$$

is mid-linear. $\tilde{\Psi}$ is clearly additive in r and m by the distributive law, and for $r' \in R$ we have

$$(rr', m) \overset{\tilde{\Psi}}{\longmapsto} (rr')m \overset{\tilde{\Psi}}{\longleftarrow} (r, r'm).$$

Now we check Ψ, Φ are inverses: for $r \in R,\ m \in M$

$$\Phi\Psi(r \otimes m) = \Phi(rm) = 1 \otimes rm = r \otimes m$$

so $\Phi\Psi = \text{id}$. Similarly $\Psi\Phi = \text{id}$.

Exercise. Check R-linearity and S-linearity in case (2).

□

Remark. Similarly, $N \otimes_R R \cong N$ for $N \in$ **mod**-R.

23.2 Distributive Law

Let $\{M_i\}_{i\in I}$ be a set of right R-modules, and $N \in R$-$\underline{\textbf{mod}}$. Recall that we have the canonical injection

$$\begin{aligned}\iota_j : M_j &\longrightarrow \bigoplus_{i\in I} M_i \\ m &\longmapsto (0,\dots,0,m,0,\dots).\end{aligned}$$

Functoriality implies that we have the R-linear map

$$\iota_j \otimes N : M_j \otimes N \longrightarrow \left(\bigoplus_{i\in I} M_i\right) \otimes N$$

for each $j \in I$. Furthermore, the universal property of $\oplus$ gives the map

$$\Phi : \bigoplus_{i\in I}(M_i \otimes N) \longrightarrow \left(\bigoplus_{i\in I} M_i\right) \otimes N.$$

Proposition 23.2. (1) Φ above is an isomorphism.

(2) If all M_i are (S,R)-bimodules so is $\bigoplus M_i$ and Φ is left S-linear

(3) If N is an (R,T)-bimodule then Φ is right T-linear.

Proof. Mainly exercise.

Recall we have the canonical projection

$$\begin{aligned}\pi_j : \prod_{i\in I} M_i &\longrightarrow M_j \\ (m_i)_{i\in I} &\longmapsto m_j.\end{aligned}$$

The universal property of the direct product gives map and functoriality of $-\otimes N$ give

$$\left(\prod_{i\in I} M_i\right) \otimes N \longrightarrow \prod_{i\in I}(M_i \otimes N).$$

Exercise. Show that this restricts to a map

$$\left(\bigoplus_{i\in I} M_i\right) \otimes_R N \longrightarrow \bigoplus_{i\in I}(M_i \otimes_R N)$$

which is inverse to Φ.

Exercise. Check S,T-lienarity in cases (2) and (3).

□

Remark. For $M \in \underline{\textbf{mod}}$-$R$, $\{N_i\}_{i\in I} \subseteq R$-$\underline{\textbf{mod}}$, we have similarly that

$$M \otimes_R \left(\bigoplus_{i\in I} N_i\right) \xrightarrow{\sim} \bigoplus_{i\in I}(M \otimes_R N_i).$$

Example 23.1. Complexification of a real vector space $V = \bigoplus_{i=1}^{n} \mathbb{R}e_i$. Its complexification is the $\mathbb{C}$-module $\mathbb{C} \otimes_{\mathbb{R}} V$.

Note that $\mathbb{C}$ is a $(\mathbb{C}, \mathbb{R})$-bimodule. Now

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} V &= \mathbb{C} \otimes_{\mathbb{R}} \left(\bigoplus_{i=1}^{n} \mathbb{R}e_i \right) \\ &= \bigoplus_{i=1}^{n} (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}e_i) \\ &= \bigoplus_{i=1}^{n} \mathbb{C}(1 \otimes e_i) \end{aligned}$$

as $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}e_i \cong \mathbb{C}$ by proposition (23.1).

23.3 Case when R is commutative

Now let R be a commutative ring, and M, N left R-modules. R commutative implies that we can think of M, N as (R, R)-bimodules with left multiplication equal to right multiplication. Hence we can define the (R, R)-bimodule $M \otimes_R N$.

However, for $r \in R,\ m \in M,\ n \in N$ we have

$$r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn) = m \otimes (nr) = (m \otimes n)r$$

so we always have that left multiplication by r is equal to right multiplication. Thus we get no more information than a left module.

Remark. An UPSHOT of the discussion above is that tensor products of left/right R-modules are left/right R-modules.

Corollary 23.1. *$R^n \otimes_R R^m \cong R^{nm}$.*

More precisely,

$$\left(\bigoplus_{i=1}^{n} Re_i \right) \otimes_R \left(\bigoplus_{j=1}^{m} Rf_j \right) \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m} R(e_i \otimes f_j)$$

for e_i, f_j free generators.

Now, consider R-linear endomorphisms $\varphi : R^n \to R^n$ and $\psi : R^m \to R^m$ given by matrices $(\varphi_{ij}) \in M_n(R)$ and $(\psi_{ij}) \in M_m(R)$. Functoriality of $\otimes$ gives a new R-linear endomorphism

$$\begin{aligned} \varphi \otimes \psi : R^n \otimes_R R^m &\longrightarrow R^n \otimes_R R^m \\ a \otimes b &\longmapsto \varphi(a) \otimes \psi(b). \end{aligned}$$

We can represent this with some matrix $((\varphi \otimes \psi)_{ij}) \in M_{nm}(R)$.

Proposition 23.3.

$$\operatorname{tr}\left((\varphi \otimes \psi)_{ij}\right) = \operatorname{tr}(\varphi_{ij}) \operatorname{tr}(\psi_{ij}).$$

Proof. Use the free basis from corollary (23.1), that is, $\{e_i\}_{i=1}^{n}$ and $\{f_j\}_{j=1}^{m}$. Then observe

$$\begin{aligned} (\varphi \otimes \psi)(e_i \otimes f_j) &= \varphi(e_i) \otimes \psi(f_j) \\ &= \left(\sum_{u=1}^{n} \varphi_{ui} e_u \right) \otimes \left(\sum_{v=1}^{m} \psi_{vj} f_v \right). \end{aligned}$$

The coefficient of $e_i \otimes f_j$ here is $\varphi_{ii}\psi_{jj}$. Therefore

$$\begin{aligned}\operatorname{tr}((\varphi \otimes \psi)_{ij}) &= \sum_{i=1}^{n}\sum_{j=1}^{m} \varphi_{ii}\psi_{jj} \\ &= \sum_{i=1}^{n}\varphi_{ii}\sum_{j=1}^{m}\psi_{jj} \\ &= \operatorname{tr}(\varphi_{ij})\operatorname{tr}(\psi_{ij}).\end{aligned}$$

□

23.4 Tensor Products of Group Representations

Let R be a commutative ring, and G a group.

Proposition 23.4. Given two group representations $\rho_V : G \to \operatorname{Aut}_R(V)$ and $\rho_W : G \to \operatorname{Aut}_R(W)$, we get a new group representation

$$\rho_{V\otimes_R W} : G \longrightarrow \operatorname{Aut}_R(V \otimes_R W)$$

defined by

$$\rho_{V\otimes_R W}(g) = \rho_V(g) \otimes_R \rho_W(g).$$

This is called the **tensor product representation** and the RG-module $V \otimes_R W$ is called the **tensor product**.

Proof. For $g, h \in G$ we check $\rho_{V\otimes_R W}$ is multiplicative.

$$\begin{aligned}\rho_{V\otimes_R W}(gh) &= \rho_V(gh) \otimes \rho_W(gh) \\ &= \rho_V(g)\rho_V(h) \otimes \rho_W(g)\rho_W(h) \\ &\overset{\text{ex}}{=} (\rho_V(g) \otimes \rho_W(g)) \circ (\rho_V(h) \otimes \rho_W(h)) \\ &= \rho_{V\otimes_R W}(g) \circ \rho_{V\otimes_R W}(h).\end{aligned}$$

[Note: the exercise follows from functoriality]. □

Exercise. Show that the set of one-dimensional representations of G over k form a group under $\otimes$ which is essentially equal to the group

$$\hat{G} = \operatorname{Hom}_{\mathbb{Z}}(G_{ab}, k^*).$$

24 Characters

24.1 Linear Algebra Recap

Fix a field k.

Lemma 24.1. Let $T \in M_n(k)$ and $U \in GL_n(k)$. Then

$$\operatorname{tr}(T) = \operatorname{tr}(U^{-1}TU).$$

Proof.
$$\det(U^{-1}TU - \lambda I) = \det(U^{-1}(T - \lambda I)U) = \det(T - \lambda I).$$
□

Corollary 24.1. *Let V be a finite dimensional k-space, and $\varphi : V \to V$ a linear map. Then the* ***trace*** *of φ, $\operatorname{tr}(\varphi) := \operatorname{tr}(T)$ is independent of the matrix T representing it (with respect to any basis for V in both the domain and codomain).*

Addendum 24.1. *Given a linear isomorphism $\psi : V \to V$ then*
$$\operatorname{tr}(\psi^{-1}\varphi\psi) = \operatorname{tr}(\varphi)$$
because both $\psi^{-1}\varphi\psi$ and φ can be represented by the same matrix.

Lemma 24.2. Let V be a finite dimensional k-space, and suppose $V = V_1 \oplus V_2$. The linear projection onto V_1, that is, $\varphi : V_1 \oplus V_2 \mapsto V_1 \hookrightarrow V_1 \oplus V_2$ has trace $\operatorname{tr}\varphi = \dim V_1$.

Proof. Exercise – show that you can find a matrix representing it of the form
$$\begin{pmatrix} I_{\dim V_1} & 0 \\ 0 & 0 \end{pmatrix}$$
□

24.2 Characters

Let G be a group and V a finite dimensional kG-module with corresponding group representation $\rho_V : G \to \operatorname{Aut}_k(V)$. Note we have $\rho_V(g) : V \to V$ is linear for all $g \in G$.

Definition 24.1. The **character** of V (or ρ_V) is the function
$$\begin{aligned} \chi_V : G &\longrightarrow k \\ g &\longmapsto \operatorname{tr}(\rho_V(g)). \end{aligned}$$

We say χ_V is **irreducible** if V is an irreducible (that is, simple) kG-module.

Fact 24.1.
$$\chi_V(1) = \operatorname{tr}(\rho_V(1)) = \operatorname{tr}(\mathrm{id}_V) = \dim V.$$

Characters are invariants of kG-modules in the following sense:

Proposition 24.1. Let $\varphi : V \xrightarrow{\sim} W$ be an isomorphism of finite dimensional kG-modules. Then $\chi_V = \chi_W$.

Proof. The kG-linearity of φ implies that for all $g \in G$, $v \in V$ we have $\varphi(gv) = g(\varphi(v))$. So $\varphi(\rho_V(g)) = \rho_W(g)\varphi$ and therefore $\rho_V(g) = \varphi^{-1}\rho_W(g)\varphi$. It follows by the addendum that $\chi_V = \chi_W$. □

Definition 24.2. A function $\chi : G \to k$ is a **class function** if it is constant on conjugacy classes. The set of these will be denoted $F_k(g)$. Hence given a conjugacy class $C \subseteq G$ we can define
$$\chi(C) = \chi(g) \text{ for } g \in C.$$

Corollary 24.2. *Characters are class functions.*

Proof. Given a character χ_V, for $g, h \in G$ we have

$$\rho_V(h^{-1}gh) = \rho_V(h^{-1})\rho_V(g)\rho_V(h).$$

The addendum implies that $\chi_V(h^{-1}gh) = \chi_V(g)$. □

Example 24.1. Let

$$G = S_3 = D_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle.$$

Consider the irreducible kG-module V given by the representation

$$\begin{aligned} \rho_V : G &\longrightarrow GL_2(k) \\ \sigma &\longmapsto \begin{pmatrix} e^{2\pi i/3} & 0 \\ 0 & e^{-2\pi i/3} \end{pmatrix} \\ \tau &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

See

$$\begin{aligned} \chi_V(1) = \dim V = 2 \\ \chi_V(\sigma) = \chi_V(\sigma^2) = 2\cos\frac{2\pi}{3} = 1 \\ \chi_V(\tau) = \chi_V(\sigma\tau) = \chi_V(\sigma^2\tau) = 0. \end{aligned}$$

24.3 Character Tables

Definition 24.3. Suppose now G is finite, and k is algebraically closed with $\operatorname{char} k \nmid |G|$. Let $C_1, \dots, C_r$ be the conjugacy classes of G, and $\chi_1, \dots, \chi_r$ the irreducible characters.

The **character table** for G is the $r \times r$-matrix

$$X = (\chi_i(C_j))_{i,j=1}^r$$

Example 24.2. Let $G = S_3 = D_3$.

	Conjugacy Classes		
Irreducible characters	1	$\{\sigma, \sigma^2\}$	$\{\tau, \sigma\tau, \sigma^2\tau\}$
trivial $= \chi_1$	1	1	1
det $= \chi_2$	1	1	-1
χ_V	2	1	0

Table 1: Character table for $D_3 = S_3$

24.4 Dual Modules and Contragredient Representation

Recall we have the trivial representation

$$\rho_0 : G \longrightarrow 1 \hookrightarrow k^*$$

which makes k a left kG-module.

Definition 24.4. Given a kG-module V, the **dual module** is the kG-module $V^* = \operatorname{Hom}_k(V, k)$.

Exercise. Let $V = k^n$, and consider the inner product $\langle \mathbf{v}, \mathbf{v}' \rangle := \mathbf{v}^T\mathbf{v}' \in k$.

(1) Show that the map $\Phi : V \to V$ defined by $\mathbf{v} \mapsto \langle \mathbf{v}, - \rangle$ is a linear isomorphism

(2) Let $\Psi : V \to V$ be a linear map (so it is a matrix). Then show that
$$\langle \mathbf{v}, \Psi \mathbf{v'} \rangle = \langle \Psi^T \mathbf{v}, \mathbf{v'} \rangle.$$
Hence the natural induced map
$$\begin{aligned} \Psi^* : V^* &\longrightarrow V^* \\ (f : V \to k) &\longmapsto (f \circ \Psi : V \to V \to k) \end{aligned}$$
is represented by the matrix Ψ^T.

Proposition 24.2. Let V be a finite dimensional left kG-module, and let $g \in G$. Then
$$\chi_{V^*}(g) = \chi_V(g^{-1}).$$

Proof. By the definition of V^*, we have $\rho_{V^*}(g) = \rho_V(g^{-1})^* = \rho_V(g^{-1})^T$. Taking traces gives
$$\chi_{V^*}(g) = \chi_V(g^{-1}).$$
□

24.5 Hom as tensor product

Proposition 24.3. Let V, W be finite dimensional left kG-modules. Then there is an isomorphism of kG-modules
$$\begin{aligned} \Phi : W \otimes_k V^* &\longrightarrow \mathrm{Hom}_k (V, W) \\ w \otimes f &\longmapsto (v \mapsto f(v)w). \end{aligned}$$

Proof. Exercise. Check Φ is an isomorphism of vector spaces and now note that with the above notation, for $g \in G$
$$\begin{aligned} [\Phi(g(w \otimes f))](v) &= \Phi(gw \otimes (f \circ \rho_V(g^{-1}))v \\ &= f(g^{-1}v)gw \\ &= g(f(g^{-1}v)w) \\ &= [g\Phi(w \otimes f)](v). \end{aligned}$$
□

25 Orthogonality

25.1 Characters of $\oplus, \otimes$

Let k be a field, G a group and V, W finite dimensional left kG-modules.

Lemma 25.1. For any $g \in G$,

(1) $\chi_{V \oplus W} = \chi_V(g) + \chi_W(g)$

(2) $\chi_{V \otimes W} = \chi_V(g)\chi_W(g)$

Proof. (1) Just take the trace of
$$\rho_{V \oplus W}(g) = \begin{pmatrix} \rho_V(g) & 0 \\ 0 & \rho_W(g) \end{pmatrix}$$
and the result follows.

(2) Follows from proposition (23.2) [since $\rho_{V \otimes W} = \rho_V(g) \otimes \rho_W(g)$].

□

25.2 Orthogonality

For the rest of this section, assume k is an algebraically closed field and $hk \nmid |G| < \infty$ (so kG is finite dimensional and semisimple by Maschke's theorem).

For V, W left kG-modules, recall $\mathrm{Hom}_k(V, W)$ is also a kG-module. Hence given $a \in kG$ we have the linear map $\lambda_a : \mathrm{Hom}_k(V, W) \to \mathrm{Hom}_k(V, W)$ defined by left multiplication by a.

From section 17 we know if $e = \frac{1}{|G|}\sum_{g \in G} g$ then the Reynold's operator λ_e is a projection onto $\mathrm{Hom}_k(V, W)^G = \mathrm{Hom}_{kG}(V, W)$.

Theorem 25.1 (First orthogonality relation)**.** *Let V, W be simple left kG-modules, and χ_V, χ_W their characters. Then*

$$\frac{1}{|G|}\sum_{g \in G} \chi_V(g^{-1})\chi_W(g) \overset{(*)}{=} \dim_k\left(\mathrm{Hom}_k(V, W)^G\right) \overset{Schur}{=} \begin{cases} 1 & V \cong W \\ 0 & V \ncong W. \end{cases}$$

Proof. Schur's lemma implies that it suffices to prove $(*)$. We have

$$\begin{aligned} \dim_k\left(\mathrm{Hom}_k(V, W)^G\right) &= \mathrm{tr}\left(\lambda_e : \mathrm{Hom}_k(V, W) \to \mathrm{Hom}_k(V, W)\right) \text{ [lemma 24.2]} \\ &= \frac{1}{|G|}\sum_{g \in G} \mathrm{tr}\left(\lambda_g : \mathrm{Hom}_k(V, W) \to \mathrm{Hom}_k(V, W)\right) \\ &= \frac{1}{|G|}\sum_{g \in G} \mathrm{tr}\left(\lambda_g : V^* \otimes W \to V^* \otimes W\right) \text{ [prop 24.3]} \\ &= \frac{1}{|G|}\sum_{g \in G} \chi_{V^* \otimes W}(g) \\ &= \frac{1}{|G|}\sum_{g \in G} \chi_{V^*}(g)\chi_W(g) \text{ [lemma 25.1]} \\ &= \frac{1}{|G|}\sum_{g \in G} \chi_V(g^{-1}\chi_W(g) \text{ [prop 24.2]} \end{aligned}$$

□

Theorem 25.1 suggests defining the following inner product (that is, mid-k-linear map) on $F_k(G) \times F_k(G)$:

$$\langle \chi, \chi' \rangle := \frac{1}{|G|}\sum_{g \in G} \chi(g^{-1})\chi'(g).$$

Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G, and $C_1, \ldots, C_r$ the conjugacy classes. Theorem 25.1 can be restated as

Corollary 25.1. *$\{\chi_1, \ldots, \chi_r\}$ is an orthonormal basis for the r-dimensional space of class functions $F_k(G)$.*

There is another orthogonality relation.

Recall that $X = (\chi_i(C_j))_{i,j=1}^r$ is the character table. Let

$$\Gamma = \begin{pmatrix} |C_1| & 0 & \dots & 0 \\ \vdots & |C_2| & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & |C_r| \end{pmatrix}$$

$$Y = (\chi_i(C_j^{-1}))_{i,j=1}^r.$$

Then $X, \Gamma, Y \in M_r(k)$.

Exercise. (1) If $k = \mathbb{C}$, $Y = \overline{X}^T$

(2) Theorem 25.1 can be rewritten as

$$X\Gamma Y = |G| I_r$$

(3) $\Gamma Y X = |G| I_r$

Then we have

Theorem 25.2 (Second orthogonality relation)**.**

$$\frac{1}{|G|} \sum_{l=1}^{r} \chi_l(C_i^{-1}) \chi_l(C_j) = \delta_{ij}.$$

25.3 Decomposing kG-modules into a direct sum of simples

Theorem 25.3. *Let k be an algebraically closed field with $\operatorname{char} k = 0$. Let V be a finite dimensional kG-module. Then χ_V determines the isomorphism class of V as follows:*

(1) $\chi_V = \sum_i n_i \chi_I$ *where the Fourier coefficients are given by*

$$n_i = \langle \chi_V, \chi_i \rangle$$

(2) $V \cong \bigoplus_{i=1}^r V_i^{n_i}$ *where V_i is the simple kG-module with character χ_i.*

Proof. Easy. We know $V \cong \bigoplus V_i^{n_i}$ for some $n_i \in \mathbb{N}$, but lemma (25.1)(1) implies that $\chi_V = \sum n_i \chi_i$. Part (1) (and hence (2)) follows from orthogonality. □

Proposition 25.1. Let k be an algebraically closed field, $\operatorname{char} k = 0$ and V a finite dimensional kG-module. Then V is simple if and only if

$$\langle \chi_V, \chi_V \rangle = 1.$$

Proof. Write $\chi_V = \sum n_i \chi_i$, then

$$\langle \chi_V, \chi_V \rangle = \sum n_i^2.$$

This is 1 if and only if all $n_i = 0$ except one. □

$g \in C_i$ $\lvert C_i \rvert$	1 1	(12)(34) 3	(123) 4	(132) 4
χ_0	1	1	1	1
χ_1	1	1	ω	ω^2
χ_2	1	1	ω^2	ω
χ_3	$3 = \dim V_i$	a	b	c

Table 2: Character table for A_4

Example 25.1. $G = A_4 \leq S_3$.

Let $\omega = e^{2\pi i/3}$. We saw before what all of the one-dimensional representations of A_4 are, these give the first three rows of the character table below.

Using orthogonality, we can deduce the values for the three-dimensional character χ_3. We know

$$\langle \chi_0, \chi_3 \rangle = 0 \Longrightarrow 3 + 3a + 4b + 4c = 0$$
$$\langle \chi_1, \chi_3 \rangle = 0 \Longrightarrow 3 + 3a + 4\omega^2 b + 4\omega c = 0$$
$$\langle \chi_2, \chi_3 \rangle = 0 \Longrightarrow 3 + 3a + 4\omega b + 4\omega^2 c = 0$$

From these, we deduce $a = -1$, $b = c = 0$.

26 Example from Harmonic Motion

OMITTED

27 Adjoint Associativity and Induction

To keep track of scalars acting on modules we let ${}_R M$ denote a left R-module, N_S a right S-module and ${}_R L_S$ an (R, S)-bimodule.

27.1 Adjoint Associativity

Let R, S, T be rings, M, N modules with scalars given in the above notation.

Proposition 27.1. (1) The abelian group $\operatorname{Hom}_R({}_R M_S, {}_R N)$ is a left S-module with scalar multiplication given by

$$(s\varphi)(m) := \varphi(ms)$$

(2) Similarly $\operatorname{Hom}_R({}_R M, {}_R N_T)$ is a right T-module with scalar multiplication

$$(\varphi t)(m) := \varphi(m)t$$

(3) $\operatorname{Hom}_R({}_R M_S, {}_R N_T)$ is an (S, T)-bimodule.

Proof. Exercise: this can be proved using the functoriality of $\operatorname{Hom}_R(-, -)$ of just checking module axioms directly. □

For a subring S of a ring R, recall we have an (R, S)-bimodule ${}_R R_S$.

Proposition 27.2. The isomorphism of abelian groups from section 5

$$\begin{aligned}\Phi : {}_S\operatorname{Hom}_R({}_RR_S, {}_RM) &\longrightarrow M\\ \varphi &\longmapsto \varphi(1)\end{aligned}$$

is S-linear.

Proof. Just check S-linearity. We know Φ is additive so consider $s \in S$, so we have

$$\begin{aligned}\Phi(s\varphi) &= (s\varphi)(1)\\ &= \varphi(s)\\ &= s\varphi(1)\\ &= s\Phi(\varphi).\end{aligned}$$

□

Theorem 27.1 (Adjoint Associativity)**.** *Let R, S, T be rings and consider modules ${}_RB_S$, ${}_SM$ and ${}_RN$.*

(1) The following is an isomorphism of groups

$$\begin{aligned}\Phi : \operatorname{Hom}_R({}_RB_S \otimes_S {}_SM, {}_RN) &\longrightarrow \operatorname{Hom}_S({}_SM, {}_S\operatorname{Hom}_R({}_RB_S, {}_RN))\\ \varphi &\longmapsto (m \mapsto \varphi(- \otimes m))\end{aligned}$$

(2) If M is an (S,T)-bimodule, this map is left T-linear. If N is an (R,T)-bimodule, then this map is right T-linear.

Proof. Purely formal but long and tedious and mainly left as an exercise.

Exercise.

- Check Φ is well defined, that is
  - $\varphi(- \otimes m)$ is R-linear
  - $m \mapsto \varphi(- \otimes m)$ is S-linear
- Check Φ is aditive
- Use the universal property to construct an inverse Ψ to Φ as follows:

  Suppose given S-linear map $\psi : M \to \operatorname{Hom}_R(B, N)$. We get a mid-$S$-linear map

  $$\begin{aligned}\tilde{\varphi} : B \otimes M &\longrightarrow N\\ (b, m) &\longmapsto [\psi(m)](b).\end{aligned}$$

  Indeed, this is clearly additive in m and b, and

  $$\begin{aligned}\tilde{\varphi}(bs, m) &= [\psi(m)](bs)\\ &= [s(\psi(m))](b)\\ &= [\varphi(sm)](b)\\ &= \tilde{\varphi}(b, sm).\end{aligned}$$

- Check $\Psi = \Phi^{-1}$
- Check linearity in the case (2).

□

27.2 Induced Modules

Let k be a field, G a group and H a subgroup of G. kH is a subring of kG, and we also get the bimodule ${}_{kG}kG_{kH}$.

Definition 27.1. Let V be a left kH-module. The **induced module** is the kG-module

$$ {}_{kG}kG_{kH} \otimes_{kH} V =: \mathrm{Ind}_H^G (V) . $$

Corollary 27.1 (Frobenius reciprocity)**.** *With this notation,*

$$ \mathrm{Hom}_{kG} (kG \otimes_{kH} V, {}_{kG}W) = \mathrm{Hom}_{kH} (V, {}_{kH}W) . $$

Proof. Use theorem 27.1 and proposition 27.2. □

Example 27.1. Consider the dihedral group

$$ G = D_n = \langle \sigma, \tau \mid \sigma^n = 1 = \tau^2, \tau\sigma = \sigma^{-1}\tau \rangle. $$

Let $H = \langle \sigma \rangle$.

Suppose we are given a one-dimensional $\mathbb{C}H$-module $V = \mathbb{C}v$. Hence $\sigma v = \omega v$ for some nth root of unity ω. What is $\mathrm{Ind}_H^G (V) = \mathbb{C}G \otimes_{\mathbb{C}H} V$? Observe

$$ \begin{aligned} \mathbb{C}G \otimes_{\mathbb{C}H} V &= (\mathbb{C}G \otimes_{\mathbb{C}H} V) \oplus (\tau\mathbb{C}H \otimes_{\mathbb{C}H} V) \\ &= (1 \otimes V) \oplus (\tau \otimes V) \end{aligned} $$

as $\mathbb{C}$-spaces. Therefore $W = \mathrm{Ind}_H^G (V)$ is two-dimensional with $\mathbb{C}$-basis $\{1 \otimes v, \tau \otimes v\}$.

What is $\rho_W : G \longrightarrow GL_2(\mathbb{C})$ with respect to this basis?

We note that τ swaps $1 \otimes v$ with $\tau \otimes v$ so

$$ \rho_W(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . $$

Furthermore, we have

$$ \begin{aligned} \sigma(1 \otimes v) &= \sigma \otimes v = 1 \otimes \sigma v = 1 \otimes \omega v = \omega(1 \otimes v) \\ \sigma(\tau \otimes v) &= (\sigma\tau \otimes v) = \tau\sigma^{-1} \otimes v = \tau \otimes \omega^{-1} v = \omega^{-1}(\tau \otimes v) \end{aligned} $$

so

$$ \rho_W(\sigma) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} . $$

If $\omega \neq \omega^{-1}$ these give the two-dimensional simple $\mathbb{C}G$-modules.

28 Annihilators and the Jacobson Radical

28.1 Restriction Functor

Let R be a ring, $I \lhd R$ and consider the canonical quotient map $\pi : R \longrightarrow R/I$.

Recall from section 5 (using the universal property of quotients) that we have a "restriction" functor

$$ \begin{aligned} \rho : \underline{\mathbf{mod}} - R/I &\longrightarrow \underline{\mathbf{mod}} - R \\ M &\mapsto M_R \end{aligned} $$

where the R-module structure on M is given by

$$ mr := m\pi(r) = m(r + I). $$

Exercise. This is an additive functor.

Proposition 28.1. The restriction functor ρ identifies the class of (right) R/I-modules with the class of right R-modules such that $MI = 0$.

Proof. Suppose $M \in \underline{\mathbf{mod}}\text{-}R/I$. Then it is clear $M_R I = 0$.

Conversely, suppose $M_R \in \underline{\mathbf{mod}}\text{-}R$ such that $M_R I = 0$. We get an R/I-module on the underlying abelian group M of M_R by defining $m(r + I) := mr$, which is well defined because $M_R I = 0$. □

28.2 Annihilators

Definition 28.1. Let R be a ring, $M \in \underline{\mathbf{mod}}\text{-}R$, $I \trianglelefteq R$, $N \subseteq M$. We say I **annihilates** N if $NI = 0$.

[Note that $NI = \{\sum_i m_i r_i \mid m_i \in N,\ r_i \in I\}$].

The **right annihilator** of N in R is

$$r\operatorname{ann}_R(N) = \operatorname{ann}_R(N) = \{r \in R \mid nr = 0\ \forall n \in N\}$$

that is, the maximal subset of R which annihilates N.

Proposition 28.2. With the above notation,

(1) $\operatorname{ann}_R(N)$ is a right ideal of R

(2) If N is a submodule then $\operatorname{ann}_R(N)$ is an ideal.

Proof. Just need to check closure axioms. Let $n \in N$, $r', r'' \in \operatorname{ann}_R(N)$, $r \in R$.

(1)
- $n0 = 0 \Longrightarrow 0 \in \operatorname{ann}_R(N)$
- $n(r' + r'') = 0 \Longrightarrow r' + r'' \in \operatorname{ann}_R(N)$
- $n(-r') = -nr' = 0 \Longrightarrow -r' \in \operatorname{ann}_R(N)$
- $n(r'r) = 0r = 0 \Longrightarrow r'r \in \operatorname{ann}_R(N)$

(2) Since $nr \in N$ we have $n(rr') = (nr)r' = 0$ so $rr' \in \operatorname{ann}_R(N)$.

□

Example 28.1. Consider the product of rings $R = R_1 \times \cdots \times R_n$. Let $I = 0 \times R_2 \times \cdots \times R_n$ be the kernel of the projection map $\pi_1 : R \to R_1$ (and therefore an ideal of R).

Recall every R-module has the form $M_1 \times \cdots \times M_n$ for R_i-modules M_i. Those of the form $M_1 \times 0 \times \cdots \times 0$ are annihilated by I.

Example 28.2. Let $N_R, N'_R \leq M_R$. Suppose I annihilates N and I' annihilates N'. Then $I \cap I'$ annihilates $N + N'$.

Indeed, see that given any $r \in I \cap I'$, $n \in N$, $n' \in N'$ we have

$$(n + n')r = nr + nr' = 0.$$

Lemma 28.1. Let $M \in \underline{\mathbf{mod}}\text{-}R$.

(1) Given any $m \in M$ we have $mR \cong R/\operatorname{ann}_R(m)$.

(2) Suppose M is simple. Then for any $m \in M \setminus \{0\}$, $\operatorname{ann}_R(M)$ is a maximal right ideal. Conversely, any maximal right ideal $I \lhd R$ is the annihilator of $1 + I \in R/I$ in the simple module R/I.

Proof. (1) ⇒ (2) exercise.

For (1) use the first isomorphism theorem on $R \xrightarrow{\lambda_M} M$. □

28.3 Jacobson Radical

Theorem 28.1. *Let R be a ring.*

(1) The following subsets of R are equal:

$$J_1 = \bigcap_S \operatorname{ann}_R(S) \text{ for } S \text{ ranging over all simple } R\text{-modules}$$
$$J_2 = \bigcap_I I \text{ for } I \text{ ranging over all maximal right ideals of } R$$

(2) The common subset $J_1 = J_2$ in (1) is an ideal, called the ***Jacobson radical*** *of R and is denoted $J(R)$ (or sometimes $\operatorname{rad} R$).*

(3) Via the restriction functor $\rho : \underline{\textbf{mod}}\text{-}R/J(R) \longrightarrow \underline{\textbf{mod}}\text{-}R$, the semisimple R-modules are precisely the semisimple $R/J(R)$ modules.

Proof. Proposition (28.2)(2) implies (2). Furthermore, proposition (28.1) implies (3). It remains to prove (1). But we have

$$\begin{aligned} J_1 &= \bigcup_S \operatorname{ann}_R(S) \\ &= \bigcup_S \bigcup_{s\in S} \operatorname{ann}_R(s) \\ &= \bigcup_{S, s\in S\setminus\{0\}} \operatorname{ann}_R(s) \\ &= \bigcup_{I \ max} I \\ &= J_2. \end{aligned}$$

□

Definition 28.2. Say R is **semiprimitive** if $J(R) = 0$.

Example 28.3. $\mathbb{Z}$ is seimprimitive as

$$J(\mathbb{Z}) = \langle 2\rangle \cap \langle 3\rangle \cap \cdots = 0.$$

Definition 28.3. Let R be a ring and $r \in R$. We say r is **nilpotent** if $r^n = 0$ for some $n > 0$. Similarly, $S \subseteq R$ is nilpotent if $S^n = 0$ for some n.

Proposition 28.3. Let R be a ring, $I \subseteq R$ be a nilpotent right ideal. Then $I \subseteq J(R)$.

Proof. It suffices to show $I \subseteq \operatorname{ann}_R(S)$ for any simple R-module S.

Note that SI is a submodule of S so by simplicity is either 0 or S. Suppose by way of contradiction that $SI = S$. Pick n large enough so $I^n = 0$, then

$$S = SI = SI^2 = \cdots = SI^n = 0$$

which is a contradiction. So $SI = 0$ and therefore $I \subseteq \operatorname{ann}_R(S)$ as required. □

Example 28.4. Let G be a finite group, k a field with $\operatorname{char} k \mid G$. Consider $\Sigma = \sum_{g \in G} g$. Note that for any $h \in G$ we have
$$h\Sigma = \Sigma = \Sigma h.$$
Therefore, $k\Sigma$ is an ideal of kG. Also, $(k\Sigma)^2 = k\Sigma^2 = k|G|\Sigma = 0$, so $k\Sigma$ is nilpotent, and $J(kG) \supseteq k\Sigma$.

Exercise. Consider rings R, S and (R, S)-bimodule B. We have the ring
$$\begin{pmatrix} R & B \\ 0 & S \end{pmatrix}$$
with entrywise addition and matrix multiplication (which is well defined as B is an (R, S)-bimodule).

Then
$$\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix}$$
is a nilpotent ideal.

29 Nakayama Lemma and the Wedderburn-Artin Theorem

Fix a ring R.

29.1 NAK Lemma

Lemma 29.1. Let I be a right ideal of R. Then every element of $1 + I$ has a right inverse in R if and only if $1 + I \subset R^*$.

Proof. The reverse direction is clear as two-sided inverses are trivially right inverses as well.

We prove the forward direction. Suppose $r \in I$, so $1 + r$ has right inverse $1 + s \in R$. Then
$$1 = (1 + r)(1 + s) = 1 + r + s + rs$$
so $s = -r - rs \in I$. Therefore $1 + s$ has right inverse, say $1 + r'$. Byt then
$$(1 + r) = (1 + r)(1 + s)(1 + r') = (1 + r').$$
Hence $(1 + s)$ is also a left inverse of $1 + r' = 1 + r$, and so $1 + r \in R^*$. □

Lemma 29.2 (Nakayama-Azumaya-Krull (NAK))**.** Let M be a finitely generated R-module and I a right ideal of R such that $1 + I \subseteq R^*$. If $MI = M$ then $M = 0$ – that is, $MI \subsetneq M$ unless $M = 0$.

Proof. By induction on the number of generators n with $n = 0$ being what we wish to show.

Suppose $M = m_1R + \cdots + m_nR$. If $MI = M \ni m_n = m_1r_1 + \cdots + m_nr_n$ with $r_i \in I$. So
$$m_n(1 - r_n) = m_1r_1 + \cdots + m_{n-1}r_{n-1}.$$
But $-r_n \in I$ so $1 - r_n \in R^*$ by the assumption. Therefore
$$m_n = m_1r_1(1 - r_n)^{-1} + \cdots + m_{n-1}r_{n-1}(1 - r_n)^{-1}$$
so M is generated by $m_1, \ldots, m_{n-1}$ and we are done by induction. □

Corollary 29.1. *Let I be a right ideal of R such that $1 + I \in R^*$. For any simple right R-module M we have $MI = 0$. In particular, $I \subseteq J(R)$.*

Proof. Simplicity of M implies that $MI = 0$ or M. Nakayama's lemma then tells us that $MI = 0$. □

29.2 Properties of the Jacobson Radical

Proposition 29.1. $1 + J(R) \subseteq R^*$.

Proof. Let $r \in J(R)$, and suppose by way of contradiction that $1 + r$ is not invertible. Then lemma 29.1 implies that it doesn't have a right inverse, and so $(1 + r)R \subsetneq R$.

Zorn's lemma implies that there is a maximal right ideal I which contains $(1 + r)R$. But now $I \supseteq J(R)$ so $I \ni r, 1 + r \implies I \ni 1$ which contradicts the maximality of I. □

Theorem 29.1. *The Jacobson radical is equal to any of the subsets listed below*

$$\begin{aligned} J_a(R) &= \bigcap_{S \text{ left simple}} \operatorname{ann}_R(S) \\ J_b(R) &= \bigcap_{I \text{ left maximal}} I \\ J_c(R) &= \text{ the largest right (or left or two-sided) ideal such that } 1 + I \subseteq R^*. \end{aligned}$$

Proof. $J_a(R) = J_b(R)$ by the same proof as in theorem (28.1). Corollary (29.1) and proposition (29.1) imply that $J(R)$ is a maximal right (or left) ideal satisfying $1 + I \subseteq R^*$. It is two-sided so the three subsets in (3) are all equal to $J(R)$.

Left-right symmetry in (3) gives $J_a(R) = J(R)$. □

29.3 Wedderburn-Artin Theorem

Theorem 29.2 (Wedderburn-Artin)**.** *A ring R is semisimple if and only if it is semiprimitive and is (right) artinian.*

Proof. Suppose that R is semisimple, so $R_R = \bigoplus_{j=1}^n I_j$ where I_j are simple right R-modules (that is, minimal right ideals). Since I_j is artinian, so is R_R.

Note $M_j := \sum_{i \neq j} I_i$ is a maximal right ideal as $R/M_j \cong I_j$ which is simple. It follows that

$$J(R) \subseteq \bigcap_{j=1}^n M_j = 0.$$

For the converse, we note that the descending chain condition and semiprimitivity of R imply the following facts

(a) Any right ideal I contains a minimal right ideal I'

(b) Any minimal right ideal I of R is a direct summand of R_R

Why? $J(R) = \bigcap_L L$ where L ranges over all maximal right ideals. Thus there is a maximal right ideal L such that $I \cap L \subsetneq I$. But I is simple, so $I \cap L = 0$. Also, L is maximal and so $I + L = R$ and therefore $R = I \oplus L$.

We wish to show R_R is a direct sum of simple modules by constructing two sequences of ideals $I_n,\ I'_n$ such that

(i) $R_R \cong I_n \oplus I'_n$

(ii) I_n is the internal direct sum of minimal right ideals

(iii) $I'_n \supsetneq I'_{n+1}$.

Given these sequences, the descending chain condition implies that eventually $I'_n = 0$ for large enough n, so $R_R = I_n$ is a direct sum of simples. To generate the sequences, we start with $I_0 = 0$ so $I'_0 = R$. Assume that I_n, I'_n are defined. Fact (a) implies that we can find a minimal right ideal I''_n contained in I'_n. Fact (b) then implies that the inclusion map $I''_n \hookrightarrow R_R$ splits, and so the inclusion $I''_n \hookrightarrow I'_n$ also splits. Hence

$$I'_n = I''_n \oplus I'_{n+1}$$

for some ideal I'_{n+1}. Define $I_{n+1} = I_n \oplus I''_n$ and we are done. □

Definition 29.1. A ring R is **simple** if it has no nontrivial ideals (that is, the only two-sided ideals are 0 and R).

Proposition 29.2. A ring R is simple (right) artinian if and only if $R \cong M_n(D)$ for some division ring D.

Proof. Suppose R is a simple artinian ring. Then simplicity implies that $J(R) = 0$ so the Wedderburn-Artin theorem implies that R is semisimple.

The wedderburn theorem then implies that $R \cong \prod_{i=1}^{n} M_{n_i}(D_i)$ for division rings D_i. Simplicity then implies that $n = 1$ (else $M_{n_1}(D_1) \times 0 \times \cdots \times 0$ is a nontrivial ideal).

Proof of the converse is an exercise in the computation of ideals. □

30 Radicals and Artinian Rings

30.1 Nilpotence

Theorem 30.1. *Let R be a (right) artinian ring. Then $J(R)$ is the unique largest nilpotent right ideal of R.*

Proof. Proposition (28.3) implies that any nilpotent right ideal is contained in $J(R)$ so it suffices to show $J(R)$ is nilpotent. The DCC implies that for n large enough, we have

$$J(R)^n = J(R)^{n+1} = \dots$$

Suppose $J(R)$ is not nilpotent, so $J(R)^{n+1} \neq 0$ (that is, $J(R)J(R)^n \neq 0$). Hence DCC implies that we can find a right ideal I satisfying

$$IJ(R)^n \neq 0 \tag{30.1}$$

such that I is minimal amongst right ideals satisfying (30.1). Pick $x \in I$ such that $xJ(R)^n \neq 0$. Then $xR \subseteq I$ and $xRJ(R)^n \neq 0$ so $xR = I$.

Also, $0 \neq IJ(R)^n \leq I$ and

$$(IJ(R)^n)J(R)^n = IJ(R)^{2n} = IJ(R) \neq 0$$

(this comes from the fact that the minimality of I implies that $I = IJ(R)^n$). Now, the Nakayama lemma and the fact that I is finitely generated (by x) imply that $I = 0$, a contradiction. □

Lemma 30.1. Let R be a ring, and I an ideal contained in $J(R)$. Then

$$J(R/I) = J(R)/I.$$

Proof. This is clear from the definition of $J(R/I)$ and $J(R)$ as an intersection of maximal right (or left) ideals. □

Corollary 30.1. *Let R be a (right) artinial ring. Then the Jacobson radical is the only nilpotent ideal I with R/I semisimple.*

Proof. We know $J(R)$ is nilpotent. Also, lemma (30.1) implies that $J(R/J(R)) = J(R)/J(R) = 0$, so $R/J(R)$ is semiprimitive. Furthermore, as R is artinian, so is $R/J(R)$. The Wedderburn-Artin theorem then implies that $R/J(R)$ is semisimple.

Suppose conversely that $I \lhd R$ is nilpotent, and R/I is semisimple. We know $I \subseteq J(R)$. Also, the nilpotency of $J(R)$ implies that $J(R)/I \lhd R/I$ is nilpotent. But R/I is semisimple, and therefore has no nonzero nilpotent ideals (as any such is contained in $J(R/I)$). Therefore $J(R)/I = 0$ and thus $J(R) = I$. □

30.2 DCC implies ACC

Theorem 30.2 (Hopkins-Levitzki)**.** *Let R be a right artinian ring. Then R is also right noetherian.*

Proof. Theorem (30.1) implies that we have a sequence of ideals

$$R > J(R) > J(R)^2 > \cdots > J(R)^n = 0.$$

It suffices to show each quotient $M_i = J(R)^i/J(R)^{i+1}$ is a noetherian right R-module.

Note that $J(R)$ annihilates M_i so M_i is an $R/J(R)$-module. Now, the Wedderburn-Artin theorem implies that $R/J(R)$ is semisimple. So M_i is a direct sum of simple $R/J(R)$-modules (which correspond to simple R-modules). But M_i is also an artinian module, so this is a (exercise) finite direct sum. Now, simple modules are noetherian so M_i is as well. □

30.3 Computing Some Radicals

Example 30.1. Let R_1, R_2 be simple artinian rings and consider the (R_1, R_2)-bimodule ${}_{R_1}B_{R_2}$ such that B_{R_2} is artinian.

Exercise. Then

$$R = \begin{pmatrix} R_1 & B \\ 0 & R_2 \end{pmatrix}$$

is artinian because it is right artinian over $\begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix}$.

Then $J = \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix}$ is a nilpotent ideal and

$$R/J = \begin{pmatrix} R_1 & 0 \\ 0 & R_2 \end{pmatrix} \cong R_1 \times R_2$$

which is semisimple.

Corollary (30.1) implies that $J = J(R)$.

A consequence of this is that the subring $R = \begin{pmatrix} M_2(k) & M_2(k) \\ 0 & M_2(k) \end{pmatrix}$ of $M_4(k)$ has Jacobson radical $\begin{pmatrix} 0 & M_2(k) \\ 0 & 0 \end{pmatrix}$.

Definition 30.1. Let R be a ring, and $x \in R$. We say x is **normal** if $xR = Rx$.
In this case, xR is a two-sided ideal.

Remark. Let $x \in R$ be normal and nilpotent. Then xR is a nilpotent ideal.
Why? Suppose $x^n = 0$, then

$$(xR)^n = xRxR \dots xR = x^2R^2xRxR \dots xR = x^nR = 0.$$

Example 30.2. Let k be a field, $\zeta \in k$ be a primitive nth root of unity. We let

$$R = \frac{k\langle x, y\rangle}{\langle yx - \zeta xy, x^n, y^n - \alpha\rangle}$$

for some $\alpha \in k$ such that $y^n - \alpha \in k[y]$ is irreducible. We then want to find $J(R)$.

R is finite dimensional over k with spanning set $\left\{x^iy^j\right\}_{i,j=0}^{n-1}$, so R is artinian.
Now $x \in R$ is nilpotent and is normal because by using $yx - \zeta xy = 0$ we camn write any $p(x, y)x$ as $xq(x, y)$ for some $q(x, y) \in R$. Thus $Rx \subseteq xR$. A similar argument gives $xR \subseteq Rx$ and so x is normal.
The remark then implies that $xR \subseteq J(R)$.

Claim 30.1. $xR = J(R)$.

This follows because

$$\begin{aligned} R/xR &= \frac{k\langle x, y\rangle}{\langle yx - \zeta xy, x^n, y^n - \alpha, x\rangle} \\ &= \frac{k[y]}{\langle y^n - \alpha\rangle} \end{aligned}$$

which is a field. This is semisimple so corollary (30.1) implies $xR = J(R)$.