Noncommutative algebra 1

Bielefeld University, Summer Semester 2019

William Crawley-Boevey

Introduction

My aim in this course is to cover the following topics:
(1) Basics of rings and modules (for students of differing backgrounds)
(2) Examples and constructions of algebras
(3) Module categories and related properties of modules
(4) Homological algebra: Ext and Tor, global dimension

This is the first course in a master sequence, which continues with:
Noncommutative algebra 2. Representations of finite-dimensional algebras
Noncommutative algebra 3. Geometric methods.

It is also the first part of a sequence to be given by Henning Krause, which will continue with quasi-hereditary algebras and derived categories.

Examples class by Andrew Hubery.

Why study noncommutative algebra?

- Representation theory: to study groups, Lie algebras, algebraic groups, etc., one needs to understand their representations, and for this one should study the group algebra, universal enveloping algebra, Schur algebra, etc.

- Physics: many algebras arise, e.g. for spin in quantum mechanic (Clifford algebras), statistical mechanics (Temperley-Lieb algebras), dimer models (dimer algebras), etc.

- Differential equations: linear differential equations correpond to modules for the ring of differential operators. The notion of a quantum group (which is an algebra, not a group!) arose in the study of integrable systems.

- Topology: The cohomology of a topological space gives a ring. The Jones polynomial for knots came from the representation theory of Hecke algebras.

- Number Theory: a basic object is the Brauer group, classifying central simple algebras. The final step in Wiles and Taylor's proof of Fermat's last theorem involved a different type of Hecke algebra.

- Functional analysis is all about noncommutative algebras, such as C^*-algebras and von Neumann algebras; but it is a different story.

- Linear algebra: Jordan normal form is the classification of f.d. modules for $K[x]$. If you know the Jordan normal form of two $n \times n$ matrices, what can you say about the Jordan normal form of their sum? There is a partial solution using deformed preprojective algebras and representations of quivers.

References. There are many good books on this topic. Some suggestions.
F. W. Anderson and K. R. Fuller, Rings and Categories of Modules, 2nd edition Springer 1992 .
A. J. Berrick and M. E. Keating, Categories and Modules with K-Theory in View, Cambridge University Press 2000.
P. M. Cohn, Algebra 2, 2nd edition Wiley 1989. c.f. also P. M. Cohn, Basic Algebra, 2005.
P. M. Cohn, Algebra 3, 2nd edition Wiley 1991.
B. Farb and R. K. Dennis, Noncommutative Algebra, Springer 1993.
M. Hazewinkel, N. Gubareni and V. V. Kirichenko, Algebras, Rings and Modules, Kluwer 2005.
T.-Y. Lam, A First Course in Noncommutative Rings , Springer 1991.
T.-Y. Lam, Lectures on Modules and Rings, Springer 1999.
J. C. McConnell and J. C. Robson, Noncommutative Noetherian Rings, 2nd edition American Math. Soc. 2001.
M. S. Osborne, Basic Homological Algebra, Springer 2000.
R. S. Pierce, Associative Algebras, Springer 1982.
J. J. Rotman, An Introduction to Homological Algebra, 2nd edition Springer 2009.
J. J. Rotman, Advanced Modern Algebra, American Math. Soc. 2010, or Parts I and 2, 2015 and 2017.
L. Rowen, Ring Theory, Student edition, Acdemic Press 1991.
B. Stenström, Rings of Quotients, Springer 1975.
C. A. Weibel, An Introduction to Homological Algebra, Cambridge University Press 1994.

1 Basics of rings and modules

1.1 Rings

We consider rings R which are *unital*, so there is $1 \in R$ with $r1 = 1r = r$ for all $r \in R$. Examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, $R[x]$ of ring of polynomials in an indeterminate x with coefficients in a ring R, $M_n(R)$ the ring of $n \times n$ matrices with entries in a ring R.

A *subring* of a ring is a subset $S \subseteq R$ which is ring under the same operations, with the same unity as R. A *ring homomorphism* is a mapping $\theta : R \to S$ preserving addition and multiplication and such that $\theta(1) = 1$.

A *(two-sided) ideal* in a ring R is a subgroup $I \subseteq R$ such that $rx \in I$ and $xr \in I$ for all $r \in R$ and $x \in I$. The ideal *generated by* a subset $S \subseteq R$ is

$$(S) = \{\sum_{i=1}^{n} r_i s_i r_i' : n \geq 0, r_i, r_i' \in R, s_i \in S\}.$$

If I is an ideal in R, then R/I is a ring.
Examples: $\mathbb{F}_p = \mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$.

The isomorphism theorems (see for example, P.M.Cohn, Algebra, vol. 1).
(1) A homomorphism $\theta : R \to S$ induces an isomorphism $R/\operatorname{Ker}\theta \cong \operatorname{Im}\theta$.
(2) If I is an ideal in R and S is a subring of R then $S/(S \cap I) \cong (S + I)/I$.
(3) If I is an ideal in R, then the ideals in R/I are of the form J/I with J an ideal in R containing I, and $(R/I)/(J/I) \cong R/J$.

The opposite ring R^{op} is obtained from R by using the multiplication $\cdot$, where $r \cdot s = sr$. The transpose defines an isomorphism $M_n(R)^{op} \to M_n(R^{op})$.

A product of rings $\prod_{i \in I} R_i$ is naturally a ring, e.g. $R^n = R \times R \times \cdots \times R$ or $R^I = \prod_{i \in I} R$, the set of functions $I \to R$.

1.2 Modules

Let R be a ring. A *(left) R-module* consists of an additive group M equipped with a mapping $R \times M \to M$ which is an *action*, meaning
- $(rr')m = r(r'm)$ for $r, r' \in R$ and $m \in M$,

- it is distributive over addition, and
- it is unital: $1m = m$ for all m.

An R-module *homomorphism* $\theta : M \to N$ is a map of additive groups with $\theta(rm) = r\theta(m)$ for $r \in R$ and $m \in M$.

A *submodule* of a R-module M is a subgroup $N \subseteq M$ with $rn \in N$ for all $r \in R$, $n \in N$. Given a submodule N of M one gets a quotient module M/N.

The isomorphism theorems for R-modules (see for example P.M.Cohn, Algebra, vol. 2).
(1) A homomorphism $\theta : M \to N$ induces an isomorphism $M/\operatorname{Ker}\theta \cong \operatorname{Im}\theta$.
(2) If L and N are submodules of a module M, then $L/(L \cap N) \cong (L+N)/N$.
(3) If N is a submodule of M, then the submodules of M/N are of the form L/N where L is a submodule of M containing N, and $(M/N)/(L/N) \cong M/L$.

If $\theta : R \to S$ is a ring homomorphism, any S-module ${}_SM$ becomes an R-module denoted ${}_RM$ or ${}_\theta M$ by *restriction*: $r.m = \theta(r)m$.

Dually there is the notion of a *right R-module* with an action $M \times R \to R$. Apart from notation, it is the same thing as a left R^{op}-module. If R is commutative, the notions coincide.

If R and S are rings, then an *R-S-bimodule* is given by left R-module and right S-module structures on the same additive group M, satisfying $r(ms) = (rm)s$ for $r \in R$, $s \in S$ and $m \in M$.

A ring R is naturally an R-R-bimodule. A (two-sided) ideal of R is a sub-bimodule of R. A *left* or *right ideal* of R is a submodule of R as a left or right module.

A product of R-modules $\prod_{i\in I} X_i$ is naturally an R-module. We write X^I for the product of copies of X indexed by a set I, so the set of functions $I \to X$.

The *(external) direct sum* or *coproduct* of modules is:

$$\bigoplus_{i\in I} X_i \left(\text{or } \coprod_{i\in I} X_i \right) = \left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i \colon x_i = 0 \text{ for all but finitely many } i \right\}.$$

One writes $X^{(I)} = \bigoplus_{i\in I} X$.

If the X_i ($i \in I$) are submodules of an R-module X, then addition gives a

homomorphism

$$\bigoplus_{i\in I} X_i \to X, \quad (x_i)_{i\in I} \mapsto \sum_{i\in I} x_i.$$

The image is the *sum* of the X_i, denoted $\sum_{i\in I} X_i$. If this homomorphism is an isomorphism, then the sum is called an *(internal) direct sum*, and also denoted $\bigoplus_{i\in I} X_i$.

If $(m_i)_{i\in I}$ is a family of elements of an R-module M, the submodule *generated by* (m_i) is

$$\sum_{i\in I} Rm_i = \{\sum_{i\in I} r_i m_i : r_i \in R, \text{ all but finitely many zero}\},$$

or equivalently the image of the map $R^{(I)} \to M$, $(r_i) \mapsto \sum_{i\in I} r_i m_i$.

Every module M has a generating set, for example M itself. A module M is *finitely generated* if it has a finite generating set. Equivalently if there is a map from R^n onto M for some $n \in \mathbb{N}$.

A family $(m_i)_{i\in I}$ is an *(R-)basis* for M if it generates M and is R-linearly independent, that is, if

$$\sum_{i\in I} r_i m_i = 0$$

with all but finitely many $r_i = 0$, implies all $r_i = 0$. That is, the map $R^{(I)} \to M$ is bijective. A module M is *free* if it has a basis; equivalently $M \cong R^{(I)}$ for some I.

Example. $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Q}$ are not free $\mathbb{Z}$-modules.

Lemma. Any proper submodule of a finitely generated module is contained in a maximal proper submodule.

Proof. Apply Zorn's Lemma to the set of proper submodules containing the submodule. Finite generation ensures that the union of a chain of proper submodules is a proper submodule.

1.3 Algebras

Fix a commutative ring K (often a field). An *(unital associative) algebra* over K, or *K-algebra* consists of a ring which is at the same time a K-module, with the same addition, and such that multiplication is a K-module homomorphism in each variable.

To turn a ring R into a K-algebra is the same as giving a homomophism from K to the centre of R, $Z(R) = \{r \in R : rs = sr \text{ for all } s \in R\}$. Given the K-module structure on R, we have the map $K \to Z(R)$, $\lambda \mapsto \lambda 1$. Given a map $f : K \to Z(R)$ we have the K-module structure $\lambda.m = f(\lambda)m$.

A ring is the same thing as a $\mathbb{Z}$-algebra.

Any module for a K-algebra R becomes naturally a K-module via $\lambda.m = (\lambda 1)m$. It can also be considered as a R-K-bimodule.

If R and S are K-algebras, then unless otherwise stated, one only considers R-S-bimodules for which the left and right actions of K are the same.

A *K-algebra homomorphism* is a ring homomorphism which is also a K-module homomorphism, or equivalenty a ring homomorphism which is compatible with the ring homomorphisms from K.

Example 1. Hamilton's quaternions $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$.

If M, N are R-modules, the set of R-module homomorphisms $\mathrm{Hom}_R(M, N)$ becomes a K-module via

$$(\theta + \phi)(m) = \theta(m) + \phi(m), \quad (\lambda\theta)(m) = \lambda\theta(m)(= \theta(\lambda m).$$

But it is not necessarily an R-module, unless R is commutative. For example if we define $r\theta$ for $r \in R$ by $(r\theta)(m) = r\theta(m)$, then for $s \in R$ we have $(r\theta)(sm) = rs\theta(m)$ and $s((r\theta)(m)) = sr\theta(m)$.

Bimodule structures on M or N give module structures on $\mathrm{Hom}_R(M, N)$. For example if M is an R-S-bimodule and N is an R-T-bimodule then $\mathrm{Hom}_R(M, N)$ becomes an S-T-bimodule via $(s\theta t)(m) = \theta(ms)t$.

Example 2. $\mathrm{End}_R(M)$ the set of endomorphisms of an R-module M is a K-algebra.

If R is any K-algebra, then the R-module structures on a K-module M are in 1:1 correspondence with K-algebra homomorphisms $R \to \mathrm{End}_K(M)$.

Example 3. If G is a group, written multiplicatively, the *group algebra* KG is the free K-module with basis the elements of G, and with multiplication given by $g \cdot h = gh$ for $g, h \in G$. Thus a typical element of KG can be written as $\sum_{g \in G} a_g g$ with $a_g \in K$, almost all zero, and

$$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{k \in G} (\sum_{g \in G} a_g b_{g^{-1}k})k.$$

A *representation* of G over K consists of a K-vector space V and a group homomorphism $\rho : G \to \mathrm{GL}(V)$. There is a 1-1 correspondence between representations of G and KG-modules via $\rho(g)(v) = gv$.

Example 4. Given a set X, the *free (associative) algebra* $K\langle X\rangle$ is the free K-module on the set of all words in the letters of X, including the trivial word 1. It becomes a K-algebra by concatenation of words. For example for $X = \{x, y\}$ we write $K\langle x, y\rangle$, and it has basis

$$1, x, y, xx, xy, yx, yy, xxx, xxy, \ldots$$

In case $X = \{x\}$ one recovers the polynomial ring $K[x]$.

If R is any K-algebra, there is a 1:1 correspondence between maps of sets $X \to R$ and K-algebra maps $K\langle X\rangle \to R$.

Thus there is a 1:1 correspondence between $K\langle X\rangle$-module structures on a K-module M and maps of sets $X \to \mathrm{End}_K(M)$.

If X is a subset of R, the K-subalgebra of R *generated* by X is the image of the natural homomorphism $K\langle X\rangle \to R$.

1.4 Exact sequences

Let R be a ring or an algebra. A sequence of modules and homomorphisms

$$\cdots \to L \xrightarrow{f} M \xrightarrow{g} N \to \cdots$$

is said to be *exact* at M if $\mathrm{Im}\, f = \mathrm{Ker}\, g$. It is *exact* if it is exact at every module. A *short exact sequence* is one of the form

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0,$$

so f is injective, g is surjective and $\mathrm{Im}\, f = \mathrm{Ker}\, g$.

Any map $f : M \to N$ gives an exact sequence

$$0 \to \mathrm{Ker}\, f \to M \to N \to \mathrm{Coker}\, f \to 0$$

where $\mathrm{Coker}\, f := M/\,\mathrm{Im}\, f$, and short exact sequences

$$0 \to \mathrm{Ker}\, f \to M \to \mathrm{Im}\, f \to 0, \quad 0 \to \mathrm{Im}\, f \to N \to \mathrm{Coker}\, f \to 0.$$

Snake Lemma. Given a commutative diagram with exact rows

$$\begin{array}{ccccccccc} (0 & \longrightarrow &)L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & & \\ 0 & \longrightarrow & L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N'(& \longrightarrow & 0) \end{array}$$

there is an induced exact sequence

$$(0 \to) \operatorname{Ker}\alpha \to \operatorname{Ker}\beta \to \operatorname{Ker}\gamma \xrightarrow{c} \operatorname{Coker}\alpha \to \operatorname{Coker}\beta \to \operatorname{Coker}\gamma (\to 0).$$

The maps, including the connecting homomorphism c, are given by diagram chasing.

There is also the Five Lemma, and many variations. Maybe we only need:

Corollary. If α and γ are isomorphisms, so is β.

If L and N are modules, one gets an exact sequence

$$0 \to L \xrightarrow{i_L} L \oplus N \xrightarrow{p_N} N \to 0$$

where i_L and p_N are the inclusion and projection maps.

Lemma/Definition. A sequence $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$, is a *split* if it satisfies the following equivalent conditions
(i) f has a *retraction*, a morphism $r : M \to L$ with $rf = 1_L$.
(ii) g has a *section*, a morphism $s : N \to M$ with $gs = 1_N$.
(iii) There is an isomorphism $\theta : M \to L \oplus N$ giving a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \| & & \theta\downarrow & & \| & & \\ 0 & \longrightarrow & L & \xrightarrow{i_L} & L \oplus N & \xrightarrow{p_N} & N & \longrightarrow & 0. \end{array}$$

Proof of equivalence. (i)⇒(iii). Define $\theta(m) = (r(m), g(m))$. The diagram commutes and θ is an isomorphism by the Snake lemma.

(ii)⇒(iii). Define $\phi : L \oplus N \to M$ by $\phi(\ell, n) = f(\ell) + s(n)$. It gives a commutative diagram the other way up, so ϕ is an isomorphism by the Snake lemma, and then take $\theta = \phi^{-1}$.

(iii)⇒(i) and (ii). Define $r = p_L\theta$ and $s = \theta^{-1}i_N$.

1.5 Idempotents

Let K be a commutative ring and let R be a K-algebra (including the case of a ring, with $K = \mathbb{Z}$).

Definitions
(i) An element $e \in R$ is *idempotent* if $e^2 = e$.
(ii) A family of idempotents $(e_i)_{i \in I}$ is *orthogonal* if $e_i e_j = 0$ for $i \neq j$.
(iii) A finite family of orthogonal idempotents $e_1, \ldots, e_n$ is *complete* if $e_1 + \cdots + e_n = 1$.

Examples.
(a) If e is idempotent, then $e, 1 - e$ is a complete set of orthogonal idempotents.
(b) The diagonal unit matrices e^{ii} in $M_n(K)$ are a complete set.

Lemma 1. If M is a left R-module, then
(i) If e is idempotent, then $eM = \{m \in M : em = m\}$. This is a K-submodule of M.
(ii) If (e_i) are orthogonal idempotents, then the sum $\sum_{i \in I} e_i M$ is direct.
(iii) If $e_1, \ldots, e_n$ is a complete family of orthogonal idempotents, then $M = e_1 M \oplus \cdots \oplus e_n M$.

Proof. Straightforward. e.g. for (i), if $em = m$ then $m \in eM$, while if $m \in eM$ then $m = em' = e^2 m' = e(em') = em$.

Proposition (Peirce decomposition). If $e_1, \ldots, e_n$ is a complete family of orthogonal idempotents then $R = \bigoplus_{i,j=1}^{n} e_i R e_j$.

We draw the Peirce decomposition as a matrix

$$R = \begin{pmatrix} e_1Re_1 & e_1Re_2 & \ldots & e_1Re_n \\ e_2Re_1 & e_2Re_2 & \ldots & e_2Re_n \\ \ldots & & & \\ e_nRe_1 & e_nRe_2 & \ldots & e_nRe_n \end{pmatrix}$$

and multiplication in R corresponds to matrix multiplication.

Remark. If e is an idempotent, then eRe is an algebra with the same operation as R, with unit element e. Since the unit element is not the same as for R, it is not a subalgebra of R. Sometimes called a *corner algebra*.

Lemma 2. For M a left R-module, we have $\mathrm{Hom}_R(R, M) \cong M$ as R-modules, and if $e \in R$ is idempotent, then $\mathrm{Hom}_R(Re, M) \cong eM$ as K-modules.

In particular, $R \cong \mathrm{End}_R(R)^{op}$ (if we used right modules, we wouldn't need the opposite here) and $eRe \cong \mathrm{End}_R(Re)^{op}$.

Proof. Send $\theta : R \to M$ to $\theta(1)$ and $m \in M$ to $r \mapsto rm$, etc.

1.6 Hom spaces and decompositions

Let R be a K-algebra (including the case of R a ring with $K = \mathbb{Z}$).

Lemma 1. Given modules X, Y and families of modules X_i, Y_i $(i \in I)$, there are natural isomorphisms

$$\mathrm{Hom}_R(X, \prod_i Y_i) \cong \prod_i \mathrm{Hom}_R(X, Y_i),$$
$$\mathrm{Hom}_R(\bigoplus_i X_i, Y) \cong \prod_i \mathrm{Hom}_R(X_i, Y).$$
$$\mathrm{Hom}_R(X, \bigoplus_i Y_i) \cong \bigoplus_i \mathrm{Hom}_R(X, Y_i) \text{ for } X \text{ finitely generated}$$

Proof. Straightforward.

Lemma 2. In the algebra $\mathrm{End}_R(X_1 \oplus \cdots \oplus X_n)$, the projections onto the X_i give a complete family of orthogonal idempotents, and the Peirce decomposition is

$$\mathrm{End}_R(X_1 \oplus \cdots \oplus X_n) \cong \begin{pmatrix} \mathrm{Hom}(X_1, X_1) & \mathrm{Hom}(X_2, X_1) & \dots & \mathrm{Hom}(X_n, X_1) \\ \mathrm{Hom}(X_1, X_2) & \mathrm{Hom}(X_2, X_2) & \dots & \mathrm{Hom}(X_n, X_2) \\ \dots & & & \\ \mathrm{Hom}(X_1, X_n) & \mathrm{Hom}(X_2, X_n) & \dots & \mathrm{Hom}(X_n, X_n) \end{pmatrix}.$$

In particular, $\mathrm{End}_R(X^n) \cong M_n(\mathrm{End}_R(X))$.

Proof. Straightforward.

A module M is *indecomposable* if it is non-zero and in any decomposition into submodules $M = X \oplus Y$, either $X = 0$ or $Y = 0$.

Lemma 3. A module M is indecomposable if and only if $\mathrm{End}_R(M)$ has no non-trivial idempotents (other than 0 and 1).

Proof. An idempotent endomorphism e gives $M = \mathrm{Im}\, e \oplus \mathrm{Ker}\, e$. A decomposition $M = X \oplus Y$ gives $e =$ projection onto X.

Theorem (Specker, 1950). $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$ is a free $\mathbb{Z}$-module with basis $(\pi_i)_{i\in\mathbb{N}}$ where $\pi_i(a) = a_i$.

Proof. (cf. Scheja and Storch, Lehrbuch der Algebra, Teil 1, 2nd edition, Satz III.C.4, p230) It is clear that the π_i are linearly independent. Let (e_i) be the standard basis of $\mathbb{Z}^{(\mathbb{N})} \subset \mathbb{Z}^{\mathbb{N}}$. Let $h : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$, and let $b_i = h(e_i)$. Let (c_n) be a sequence of positive integers such that c_{n+1} is a multiple of c_n and

$$c_{n+1} \geq n + 1 + \sum_{i=0}^{n} |c_i b_i|.$$

Let $c = h((c_n))$.

For each $m \in \mathbb{N}$ there is $y_m \in \mathbb{Z}^{\mathbb{N}}$ with

$$(c_n) = \sum_{i=0}^{m} c_i e_i + c_{m+1} y_m.$$

Applying h gives

$$c = \sum_{i=0}^{m} c_i b_i + c_{m+1} h(y_m),$$

so

$$|c - \sum_{i=0}^{m} c_i b_i| = c_{m+1} |h(y_m)|$$

is either 0 or $\geq c_{m+1}$. But if $m \geq |c|$, then

$$|c - \sum_{i=0}^{m} c_i b_i| \leq |c| + \sum_{i=0}^{m} |c_i b_i| < c_{m+1}.$$

Thus $c = \sum_{i=0}^{m} c_i b_i$ for all $m \geq |c|$. But this implies $b_i = 0$ for all $i > |c|$. Then the linear form $h - \sum_{i=0}^{|c|} b_i \pi_i$ vanishes on all of the standard basis elements e_i.

It remains to show that if $g \in \mathrm{Hom}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$ vanishes on all the e_i, then it is zero. Suppose given $(c_i) \in \mathbb{Z}^{\mathbb{N}}$. Expanding $c_i = c_i(3-2)^{2i}$, we can write $c_i = v_i 2^i + w_i 3^i$ for some $v_i, w_i \in \mathbb{Z}$. Then $g((c_i)) = g((v_i 2^i)) + g((w_i 3^i))$. Now for any m, $(v_i 2^i) = \sum_{i=0}^{m-1} v_i 2^i e_i + 2^m z_m$ for some $z_m \in \mathbb{Z}^{\mathbb{N}}$. Thus $g((v_i 2^i)) \in 2^m \mathbb{Z}$. Thus $g((v_i 2^i)) = 0$. Similarly for w. Thus $g((c_n)) = 0$.

Corollary. $\mathbb{Z}^{\mathbb{N}}$ is not a free $\mathbb{Z}$-module.

Proof. Say $\mathbb{Z}^{\mathbb{N}} \cong \mathbb{Z}^{(I)}$. Since $\mathbb{Z}^{\mathbb{N}}$ is uncountable, I must be. Certainly it must be infinite. Then $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) \cong \mathrm{Hom}(\mathbb{Z}^{(I)}, \mathbb{Z}) \cong (\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}))^I \cong \mathbb{Z}^I$, which is also uncountable. But $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$ is a free $\mathbb{Z}$-module with countable basis, so it is countable.

1.7 Simple and semisimple modules

Let R be an algebra. A module S is *simple* (or irreducible) if it has exactly two submodules, namely $\{0\}$ and S. It is equivalent that S is non-zero and any non-zero element is a generator. In particular the simple modules are the quotients R/I with I a maximal left ideal.

Examples.
(i) The simple $\mathbb{Z}$-modules are $\mathbb{Z}/p\mathbb{Z}$ for p prime.
(ii) If D is a division ring, that is every non-zero element is invertible, then ${}_DD$ is a simple D-module.
(iii) K^n considered as column vectors becomes a simple $M_n(K)$-module.

Schur's Lemma. Any homomorphism between simple modules must either be zero or an isomorphism, so if S is simple, $\mathrm{End}_R(S)$ is a division ring. Moreover if R is a K-algebra, with K an algebraically closed field, and S is finite-dimensional over K, then $\mathrm{End}_R(S) = K$.

Proof. The last part holds because any f.d. division algebra D over an algebraically closed field is equal to K. Namely, if $d \in D$ then left multiplication by D gives a linear map $D \to D$, and it must have an eigenvalue λ. Then $d - \lambda 1$ is not invertible, so must be zero, so $d \in K1$.

Theorem/Definition. A module M is said to be *semisimple* (or completely reducible) if it satisfies the following equivalent conditions.
(a) M is isomorphic to a direct sum of simple modules.
(b) M is a sum of simple modules.
(c) Any submodule of M is a direct summand.

Sketch. For fuller details see P.M.Cohn, Algebra 2, §4.2.

(a) implies (b) is trivial. Assuming (b), say $M = \sum_{i \in I} S_i$ and that N is a submodule of M, one shows by Zorn's lemma that $M = N \oplus \bigoplus_{i \in J} S_i$ for some subset J or I. This gives (a) and (c).

The property (c) is inherited by submodules $N \subseteq M$, for if $L \subseteq N$ and

$M = L \oplus C$ then $N = L \oplus (N \cap C)$. Let N be the sum of all simple submodules. It has complement C, and if non-zero, then C has a non-zero finitely generated submodule F. Then F has a maximal proper submodule P. Then P has a complement D in F, and $D \cong F/P$, so it is simple, so $D \subseteq N$. But $D \subseteq C$, so its intersection with N is zero.

Corollary 1. Any submodule or quotient of a semisimple module is semisimple.

Proof. We showed above that condition (c) passes to submodules. Now if M is semisimple and M/N is a quotient, then N has a complement C in M, and $M/N \cong C$, so it is semisimple.

Corollary 2. If K is a field, or more generally a division ring, every K-module is free and semisimple (hence the theory of vector spaces).

Proof. K is a simple K-module, and it is the only simple module up to isomorphism, since if S is a simple module and $0 \neq s \in S$ then the map $K \to S$, $r \mapsto rs$ must be an isomorphism. Thus free = semisimple. The result follows.

1.8 Jacobson radical

Theorem/Definition. The *(Jacobson) radical* $J(R)$ of R is the ideal in R consisting of all elements x satisfying the following equivalent conditions.
(i) $xS = 0$ for any simple left module S.
(ii) $x \in I$ for every maximal left ideal I
(iii) $1 - ax$ has a left inverse for all $a \in R$.
(iv) $1 - ax$ is invertible for all $a \in R$.
(i')-(iv') The right-hand analogues of (i)-(iv).

Proof (i) implies (ii). If I is a maximal left ideal in R, then R/I is a simple left module, so $x(R/I) = 0$, so $x(I + 1) = I + 0$, so $x \in I$.

(ii) implies (iii). If there is no left inverse, then $R(1 - ax)$ is a proper left ideal in R, so contained in a maximal left ideal I by Zorn's Lemma. Now $x \in I$, and $1 - ax \in I$, so $1 \in I$, so $I = R$, a contradiction.

(iii) implies (iv) $1 - ax$ has a left inverse u, and $1 + uax$ has a left inverse v. Then $u(1 - ax) = 1$, so $u = 1 + uax$, so $vu = 1$. Thus u has a left and right inverse, so it is invertible and these inverses are equal, and are themselves

invertible. Thus $1 - ax$ is invertible.

(iv) implies (i). If $s \in S$ and $xs \neq 0$, then $Rxs = S$ since S is simple, so $s = axs$ for some $a \in R$. Then $(1 - ax)s = 0$, but then $s = 0$ by (iv).

(iv) implies (iv'). If b is an inverse for $1 - ax$, then $1 + xba$ is an inverse for $1 - xa$. Namely $(1 - ax)b = b(1 - ax) = 1$, so $axb = b - 1 = bax$, and then $(1 + xba)(1 - xa) = 1 + xba - xa - xbaxa = 1$, and $(1 - xa)(1 + xba) = 1 - xaxba - xa + xba = 1$.

Example. The maximal (left) ideals in $\mathbb{Z}$ are $p\mathbb{Z}$, p prime, so $J(\mathbb{Z}) = \bigcap_p \mathbb{Z}p = 0$.

Notation. If M is an R-module and I an ideal in R, we write IM fot the set of sums of products im. The powers of an ideal are defined inductively by $I^1 = I$ and $I^{n+1} = II^n$. An ideal is *nilpotent* if $I^n = 0$ for some n, or equivalently $i_1 \dots i_n = 0$ for all $i_1, \dots, i_n \in I$. An ideal I is *nil* if every element is nilpotent.

Lemma 1. For an ideal I, we have I nilpotent $\Rightarrow$ I nil $\Rightarrow$ $I \subseteq J(R)$.

Proof. The first implication is clear. If $x \in I$ and $a \in R$ then $ax \in I$, so $(ax)^n = 0$ for some n. Then $1 - ax$ is invertible with inverse $1 + ax + (ax)^2 + \dots + (ax)^{n-1}$. Thus $x \in J(R)$.

Lemma 2. If I is a nil ideal in a ring R, then any idempotent in R/I lifts to one in R.

Proof. There is a formal power series $p(x) = a_1 x + a_2 x^2 + \dots$ with integer coefficients satisfying

$$(1 + 4x)p(x)^2 - (1 + 4x)p(x) + x = 0.$$

Namely, either solve recursively for the a_i, or use the formula for a quadratic,

$$p(x) = \frac{1 - \sqrt{1 - 4\frac{x}{1+4x}}}{2},$$

expand as a power series, and observe that the coefficients are integers.

Now an idempotent in R/I lifts to an element $a \in R$ with $b = a^2 - a \in I$. Since b is nilpotent and commutes with a, the element $e = a(1 - 2p(b)) + p(b)$ makes sense and

$$e^2 - e = a^2(1 - 2p(b))^2 + 2ap(b)(1 - 2p(b)) + p(b)^2 - a(1 - 2p(b)) - p(b).$$

Writing $a^2 = a + b$ and collecting terms, this becomes

$$a[(1-2p(b))^2 + 2p(b)(1-2p(b)) - (1-2p(b)] + b(1-2p(b))^2 + p(b)^2 - p(b)]$$

$$= (1+4b)p(b)^2 - (1+4b)p(b) + b = 0.$$

Nakayama's Lemma. Suppose M is a finitely generated R-module.
(i) If $J(R)M = M$, then $M = 0$.
(ii) If $N \subseteq M$ is a submodule with $N + J(R)M = M$, then $N = M$.

Proof. (i) Suppose $M \neq 0$. Let $m_1, \ldots, m_n$ be generators with n minimal. Since $J(R)M = M$ we can write $m_n = \sum_{i=1}^n r_i m_i$ with $r_i \in J(R)$. This writes $(1-r_n)m_n$ in terms of the others. But $1 - r_n$ is invertible, so it writes m_n in terms of the others. Contradiction.

(ii) Apply (i) to M/N.

Lemma/Definition. R is a *local ring* if it satisfies the following equivalent conditions.
(i) $R/J(R)$ is a division ring.
(ii) The non-invertible elements of R form an ideal (which is $J(R)$).
(iii) There is a unique maximal left ideal in R (which is $J(R)$).

Proof. (i) implies (ii). The elements of $J(R)$ are not invertible, so it suffices to show that any $x \notin J(R)$ is invertible. Now $J(R) + x$ is an invertible element in $R/J(R)$, say with inverse $J(R) + a$. Then $1 - ax, 1 - xa \in J(R)$. But this implies ax and xa are invertible, hence so is x.

(ii) implies (iii). Clear.

(iii) implies (i). Assuming (iii), $J(R)$ is the unique maximal left ideal, so $\overline{R} = R/J(R)$ is a simple R-module, and so a simple $\overline{R}$-module. Then $\overline{R} \cong \mathrm{End}_{\overline{R}}(\overline{R})^{op}$, which is a division ring by Schur's Lemma.

Examples. (a) The set $R = \{q \in \mathbb{Q} : q = a/b, b \text{ odd}\}$ is a subring of $\mathbb{Q}$. The ideal $(2) = \{q \in \mathbb{Q} : q = a/b, a \text{ even}, b \text{ odd}\}$ is the set of all non-invertible elements. Thus R is local and $J(R) = (2)$.
(b) The set of upper triangular matrices with equal diagonal entries is a subalgebra of $M_n(K)$, e.g.

$$\left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} : a, b, c, d \in K \right\}$$

The set of matrices with $a = 0$ form a nil ideal I, so $I \subseteq J(R)$. The map sending such a matrix to a defines an isomorphism $R/I \cong K$. Thus $I = J(R)$ and $R/J(R) \cong K$ so R is local.
(c) The ring $M_n(K)$ has no 2-sided ideals other than 0 and $M_n(K)$, but it is not local.

1.9 Finite-dimensional algebras

In this section K is a field, and we consider f.d. algebras and modules.

Wedderburn's Theorem/Definition. A f.d. algebra R is *semisimple* if the following equivalent conditions hold
(i) $J(R) = 0$.
(ii) R is semisimple as an R-module.
(iii) Every R-module is semisimple.
(iv) Every short exact sequence of R-modules is split.
(v) $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ with the D_i division algebras.

Proof. If (i) holds, then since $J(R) = 0$ the intersection of the maximal left ideals is zero. Since R is f.d., a finite intersection of them is zero, say $I_1 \cap \cdots \cap I_n = 0$. Then the map $R \to (R/I_1) \oplus \ldots (R/I_n)$ is injective. Thus (ii).

If (ii) then $R = \bigoplus_{i \in I} S_i$. Now for $j \in I$ the sum $M_j = \bigoplus_{i \neq j} S_i$ is a maximal left ideal in R, and $\bigcap_{j \in I} M_j = 0$, giving (i).

Now (ii) implies that every free module is semisimple, and since any module is a quotient of a free module, (iii) follows.

The equivalence of (iii) and (iv) is easy, using that a short exact sequence $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ is split if and only if $\operatorname{Im} f$ is a direct summand of M, and that a module is semisimple if and only if every submodule is a direct summand.

If (iii) holds then we can write ${}_RR$ as a finite direct sum of simples, and collecting terms we can write

$$R \cong S_1 \oplus \cdots \oplus S_1 \oplus S_2 \oplus \cdots \oplus S_2 \oplus \cdots \oplus S_r \oplus \cdots \oplus S_r$$

where $S_1, \ldots, S_n$ are non-isomorphic simples, and there are n_i copies of each S_i. The Peirce decomposition of the endomorphism ring of this direct sum

gives $\mathrm{End}_R(R) \cong \prod_{i=1}^{n} M_{n_i}(\mathrm{End}_R(S_i))$. Now use Schur's lemma and take the opposite ring to get (v).

If (v) holds, say $R \cong \prod_{i=1}^{n} M_{n_i}(D_i)$ then $R = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{n_i} I_{ij}$ where I_{ij} is the left ideal in $M_{n_i}(D_i)$ consisting of matrices which are zero outside the jth column. This is isomorphic to the module consisting of column vectors $D_i^{n_i}$, and for D_i a division algebra, this is a simple module, giving (ii).