Ring Theory

MATH 40630

Vincent Astier

General remarks:

- In particular if you want to look at past exams:

  This course used to be called MATH40010, Ring Theory, so this is where you should look for past exams.

  But MATH40010 was reduced (not by me) in 2020 from 10 credits and 4 hours per week (and a 3-hour long final exam) to 5 credits and 3 hours per week (and a 2-hour long final exam). In particular I had to cut its content by about 30%.

  So if you look at past exams from MATH40010, some questions will be about topics that we will not see this trimester (mostly questions involving the words “dense”, “density” or “primitive”). Just ignore them.

- Convention for the definitions:

  The terms that are defined in **bold face** are the very important ones, that we will use a lot.

  The terms that are defined, but not in bold face will not be used (much) in this course (and you can even ask me at the exam in case they appear there and you are not too sure).

Contents

Chapter 1

Rings

1.1 Basic notions

Definition 1.1. *A* ***ring*** *is a nonempty set R containing an element 0 and an element 1 and equipped with two binary operations $+$ and $.$ such that:*

1. *$(R, +, 0)$ is an Abelian group;*
2. *$.$ is associative, i.e., for every $a, b, c \in R \quad a.(b.c) = (a.b).c$;*
3. *Left and right distributivity:*
   For every $a, b, c \in R \quad a.(b + c) = a.b + a.c$ and $(a + b).c = a.c + b.c$;
4. *For all $a \in R \quad a.1 = 1.a = a$.*

R is said to be **commutative** *if $ab = ba$ for all $a, b \in R$.*

Remark.
- *In some books, a ring is what we will call a "ring without 1", i.e., a ring that may not contain an element 1 satisfying the last condition.*
- *We will simply write ab for $a.b$.*

If R is a ring, $a \in R$ and $n \in \mathbb{Z}$, we define:

$$na = \begin{cases} a + \cdots + a \quad (n \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a + \cdots + (-a) \quad (n \text{ times}) & \text{if } n < 0 \end{cases}.$$

Definition 1.2. *A subset S of a ring R is called a* **subring** *if $0, 1 \in S$ and S, equipped with the addition and multiplication form R, is itself a ring (with same 0 and 1 as R).*

Remark. *S is a subring of R if and only if $1 \in S$ and if $a, b \in S$ then $-a, a+b, ab \in S$.*

Corollary 1.3. *Let R be a ring. For all $a, b \in R$, $n \in \mathbb{Z}$:*

1. $0a = a0 = 0$.
2. $(-1)a = -a = a(-1)$.
3. $(-a)b = a(-b) = -(ab)$.
4. $(-a)(-b) = ab$.
5. $(na)b = a(nb) = n(ab)$
6. *If* $ab = ba$ *then* $(a+b)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) a^i b^{n-i}$.

Proof. Exercise. □

Definition 1.4. *Let R be a ring.*

1. *$a \in R \setminus \{0\}$ is a left (respectively right)* **zero divisor** *if there exists $b \in R \setminus \{0\}$ such that $ab = 0$ (respectively $ba = 0$).*
2. *$a \in R$ is said to be* **left** *(respectively* **right***)* **invertible** *if there exists $c \in R$ (respectively $b \in R$) such that $ca = 1$ (respectively $ab = 1$).*
   The element c (respectively b) is called a **left inverse** *of a (respectively* **right inverse** *of a).*
   An element which is both left and right invertible is called **invertible** *or a* **unit***. The set of units of R will be denoted by $U(R)$ (the notation $R^\times$ is also common, be careful that it does not mean $R \setminus \{0\}$).*

Corollary 1.5. *Let R be a ring.*

1. *If $a \in U(R)$, then the left and right inverses of a coincide, and are denoted by a^{-1}, the* **inverse** *of a.*
2. *$(U(R), ., 1)$ is a group.*

Definition 1.6. *A ring $R \neq \{0\}$ with no (left or right) zero divisor is called a domain.*
A ring in which every nonzero element is invertible is called a **division ring** *(or a skew field). A* **field** *is a commutative division ring.*

Example.
- *$(\mathbb{Z}, +, ., 0, 1)$ is a domain.*
- *$(\mathbb{R}, +, ., 0, 1)$ and $(\mathbb{C}, +, ., 0, 1)$ are fields.*

- $(M_n(\mathbb{R}), +, ., 0, I_n)$ *is a ring (a noncommutative ring if* $n \geq 2$*).*

- $(\mathbb{Z}/n\mathbb{Z}, +, ., 0, 1)$ *is a commutative ring.*

- $\mathbb{R}[X]$ *is a domain.*

- $\mathbb{Z}/6\mathbb{Z}$ *has zero divisors (for example* $3.2 = 0$*).*

- $\mathbb{Z}/p\mathbb{Z}$ *is a field if* p *is prime:*
  Let $b \in \mathbb{Z}$ *with image* $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$*. We must find the inverse of* b*. Since* p *is prime, we have* $gcd(b, p) = 1$ *and there exists* $u, v \in \mathbb{Z}$ *such that* $bu + pv = 1$*. In* $\mathbb{Z}/p\mathbb{Z}$*, this gives* $\bar{b}\bar{u} + \bar{p}\bar{v} = \bar{1}$*, and (using that* $\bar{p}\bar{v} = \bar{0}$*):* $\bar{b}\bar{u} = 1$*.*
  Since $\mathbb{Z}/p\mathbb{Z}$ *is commutative,* $\bar{b}\bar{u} = \bar{u}\bar{b} = \bar{1}$*, and* $\bar{u}$ *is the inverse of* b*.*

On the topic of division rings, we cite the following important (and famous) result from Wedderburn without proof (we could do it, but it requires spending quite a bit of time on polynomials with coefficients in fields):

Theorem 1.7 (Wedderburn)**.** *A finite division ring is commutative (i.e., is a field).*

Definition 1.8. *Let* R *and* S *be rings. A map* $f : R \mapsto S$ *is a* **morphism (or homomorphism) of rings** *if:*

1. $f(1) = 1$*.*

2. *For all* $a, b \in R$*,* $f(a + b) = f(a) + f(b)$ *and* $f(ab) = f(a)f(b)$*.*

If f *is bijective, then* f *is a called an* **isomorphism***) of rings.*

You will also sometimes find the terminology monomorphism, or embedding (resp. epimorphism) of rings if f *is injective (resp. surjective).*

A morphism of rings from R *to* R *is called an* **endomorphism** *of* R*, and the set of all endomorphisms of rings from* R *to* R *is denoted by* $\mathrm{End}(R)$*.*

The **kernel** *of* f *is*

$$\mathbf{ker}\,(\boldsymbol{f}) = \{x \in R \mid f(x) = 0\}.$$

The **image** *of* f *is*

$$\mathbf{Im}\,(\boldsymbol{f}) = \{f(x) \mid x \in R\}.$$

Two rings R *and* S *are* **isomorphic** *if there is an isomorphism of rings* f *from* R *to* S*. This is denoted by* $\boldsymbol{R \cong S}$ *(or* $R \simeq S$*).*

Example (of morphisms)**.** *1.* $\mathbb{R} \to M_n(\mathbb{R})$*,* $x \mapsto x.I_n$*;*

2. *$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $x \mapsto x + p\mathbb{Z}$;*

3. *$\mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$, is not a morphism since it does not send* 1 *to* 1.

If $f : R \mapsto S$ is a morphism of rings, $\ker(f)$ has some obvious properties, for instance: $0 \in \ker(f)$, and if $a, b \in \ker(f)$ and $r \in R$, then $a + b, ar, ra \in \ker(f)$. In other words, $\ker f$ is an additive subgroup of R, with the additional property that $ar, ra \in \ker f$ whenever $a \in \ker f$ and $r \in R$
This motivates the following definition:

Definition 1.9. *Let R be a ring. A subset I of R is called a* **left** *(respectively* **right***)* **ideal** *of R if:*

1. *I is an additive subgroup of R.*

2. *For every $a \in I$ and every $r \in R$ we have $ra \in I$ (respectively $ar \in I$).*

I is called an **ideal** *(or* **2-sided ideal***) if I is both a left and right ideal.*
An ideal that is different from R is called a **proper** *ideal.*

Remark 1.10.
1. *The definition can be reformulated as follows (easy exercise, do it): I is a left (resp. right) ideal of R if an only if: I is non-empty, and for every $a, b \in I$ and $r \in R$, $a + b$, $ra \in I$ (resp. $a + b$, $ar \in I$).*

2. $\ker(f)$ *is an ideal.*

3. *A left (resp. right) ideal I is proper if and only if $1 \notin I$:*
If $1 \notin I$, then I is necessarily proper. Conversely, suppose I is proper, but $1 \in I$. Then for every $r \in R$, $r = r.1 \in I$ (resp. $r = 1.r \in I$), which gives $I = R$, a contradiction.

4. *Similarly: A left (resp. right) ideal I is proper if and only if I does not contain any invertible element from R (exercise).*

The role of ideals in ring theory can be compared to the role of normal subgroups in group theory (this will become clear in the next few results).

If R is a ring and I is an ideal of R, then I is a normal subgroup of $(R, +, 0)$ since $(R, +, 0)$ is a commutative group.
In particular, the quotient group $(R/I, +, 0 + I)$ is well-defined where:

$$R/I = \{a + I \mid a \in R\}$$

and the sum is defined by

$$(a + I) + (b + I) = (a + b) + I.$$

We can even define a ring structure on R/I:

Theorem 1.11. *Let R be a ring and I and ideal (i.e., 2-sided ideal) of R. Then:*

1. *The additive group R/I can be turned into a ring with the multiplication given by:*

$$(a+I).(b+I) = (ab) + I,$$

and with identity $1+I$.
R/I is called the **quotient ring** *of R by I.*
If R is commutative, then R/I is commutative.

2. *The map* $\begin{array}{rcl} \pi : R & \to & R/I \\ a & \mapsto & a+I \end{array}$ *is a surjective morphism of rings, and* $\ker(\pi) = I$. *π is called the canonical projection from R to R/I.*

Proof. 1. We first check that the multiplication is well-defined, i.e.,:

$$(a+I = a'+I \text{ and } b+I = b'+I) \Rightarrow (ab)+I = (a'b')+I.$$

We have $a' = a+i, b' = b+j$ with $i, j \in I$.
$a'b' = (a+i)(b+j) = ab + aj + ib + ij$, and the last three terms (and hence their sum) are in I since I is an ideal. This gives $a'b'+I = ab+I$. The other properties (associativity, distributivity, identity element) are easy to check.

2. To check that π is a morphism of rings, we use the definitions of sum and product in R/I, namely:

$$(a+b)+I = (a+I)+(b+I) \text{ and } (a.b)+I = (a+I).(b+I).$$

With this $\pi(a+b) = (a+b)+I = (a+I)+(b+I) = \pi(a)+\pi(b)$, $\pi(ab) = (ab)+I = (a+I).(b+I) = \pi(a).\pi(b)$, and $\pi(1) = 1+I$. □

Remark. *1. Why is the quotient ring R/I interesting? If you look back at the definition of quotient of groups, we have:*

$$a+I = b+I \Leftrightarrow \exists i \in I \quad a = b+i$$

which means that the elements a, b from R become identified in R/I when they differ by an element of I. In particular

$$a+I = 0+I \Leftrightarrow a \in I.$$

In other words: going from R to R/I (where the elements are of the form $a+I$), we identify the elements of I with zero (so I “disapears”).

2. *We have seen that if f is a morphism of rings,* $\ker(f)$ *is an ideal. Theorem 1.11 2 gives the converse: every ideal is of the form* $\ker(f)$ *for some morphism of rings f (the π in the theorem).*

3. *The notation $\bar{a}$ for $a + I$ is very common (at least when I is already given, so that there is no ambiguity).*

Proposition 1.12. *Let I be an ideal in a ring R. Then there is a one-to-one correspondence between the ideals of R containing I and the ideals of R/I, given by $J \mapsto \pi(J) = J/I$. Explicitely:*

$$\begin{array}{ccc} \{J \mid J \textit{ ideal of } R,\ I \subseteq J\} & \leftrightarrow & \{K \mid K \textit{ ideal of } R/I\} \\ J & \mapsto & \pi(J) = J/I \\ \pi^{-1}(K) & \leftarrow\!\shortmid & K \end{array}$$

This describes the ideals of R/I using the ideals of R.

Proof. We first show that the map is injective: Let J_1, J_2 be ideals of R containing I, such that $J_1/I = J_2/I$.
Let $a \in J_1$. Then $a + I \in J_1/I = J_2/I$. This implies that there exist $i \in I$ and $b \in J_2$ such that $a + i = j_2$ i.e., $a = j_2 - i$. But $j_2 - i \in J_2$ since $I \subseteq J_2$. This proves $a \in J_2$ and then $J_1 \subseteq J_2$.
Similarly we have $J_2 \subseteq J_1$, which gives $J_1 = J_2$.

We now show that the map is surjective: Let L be an ideal of R/I, and define $J = \pi^{-1}(L)$. We check easily that J is an ideal of R (in fact, if f is a morphism of rings f^{-1}(an ideal) is an ideal), and since π is surjective we have $\pi(J) = L$, i.e., $J/I = L$. □

Lemma 1.13. *If $\{I_k\}_{k\in K}$ are left (resp. right) ideals of a ring R, then $\bigcap_{k\in K} I_k$ is a left (resp. right) ideal of R (i.e., any intersection of left (resp. right) ideals is a left (resp. right) ideal).*

Proof. Exercise. □

Definition/Corollary 1.14. *Let X be a subset of a ring R. The* **ideal generated by X** *, denoted by* $\boldsymbol{(X)}$*, is the intersection of all the ideals containing X, i.e.,:*

$$\boldsymbol{(X)} = \bigcap \{I \mid I \textit{ ideal},\ X \subseteq I\}.$$

It is therefore, by definition, the smallest ideal containing X. The elements of X are called the generators.

We can also define the **left (resp. right) ideal generated by $\boldsymbol{X}$***, by taking the intersection of all the left (resp. right) ideals containing X. They* *will be denoted similarly, by $(X)_\ell$ (for the left ideal) and $(X)_r$ (for the right ideal).*

If $X = \{x_1, \ldots, x_n\}$ then (X) is denoted by $(x_1, \ldots, x_n)$ and is called **finitely generated***. (With similar terminology for the left or right ideals generated by X).*

An ideal (a) generated by a single element $a \in R$ is called principal.

Exercise 1.15. *With notation as in Definition 1.14, we have*

$$(X) = \{\sum_{i=1}^{t} a_i y_i b_i \mid t \in \mathbb{N},\ a_i, b_i \in R,\ y_i \in X\},$$

$$(X)_\ell = \{\sum_{i=1}^{t} a_i y_i \mid t \in \mathbb{N},\ a_i \in R,\ y_i \in X\},$$

$$(X)_r = \{\sum_{i=1}^{t} y_i b_i \mid t \in \mathbb{N},\ b_i \in R,\ y_i \in X\}.$$

We introduce the sums and products of left / right / 2-sided ideals.

Let $A_1, \ldots A_n$ be nonempty subsets of a ring R. We denote by $A_1 + \cdots + A_n$ the set:

$$\{a_1 + \cdots + a_n \mid a_i \in A_i,\ i = 1, \ldots, n\},$$

and by $A_1. \ldots .A_n$ the set:

$$\{\sum_{k=1}^{m} a_{1,k}. \ldots .a_{n,k} \mid m \in \mathbb{N}^*,\ a_{i,k} \in A_i,\ i = 1, \ldots, n,\ k = 1, \ldots, m\}$$

(the set of finite sums of products of the form $a_1. \ldots .a_n$ for $a_i \in A_i$).

Definition/Proposition 1.16. *Let $A_1, \ldots, A_n$ be (left, resp. right) ideals in a ring R. Then $A_1 + \cdots + A_n$ and $A_1. \ldots .A_n$ are (left, resp. right) ideals of R.*
$A_1 + \cdots + A_n$ is called the **sum of $A_1, \ldots, A_n$***, and $A_1. \ldots .A_n$ is called the* **product of $A_1, \ldots, A_n$***.*

Proof. For left ideals, and $A_1 + \cdots + A_n$ (the other parts of the proof are similar, and are left as exercise –do it!!–):

1. $A_1 + \cdots + A_n$ is an additive subgroup of R:
   Let $a_1 + \cdots + a_n,\ b_1 + \cdots + b_n \in A_1 + \cdots + A_n$. Then $-a_1 + \cdots + (-a_n) \in A_1 + \cdots + A_n$ (since $-a_i \in A_i$), and $a_1 + \cdots + a_n + b_1 + \cdots + b_n \in A_1 + \cdots + A_n$ (since $a_i + b_i \in A_i$).

2. Product by elements of R (on the left):
   Let $a_1 + \cdots + a_n \in A_1 + \cdots + A_n$ and $r \in R$. Then $r(a_1 + \cdots + a_n) = ra_1 + \cdots + ra_n \in A_1 + \cdots + A_n$ (because $ra_i \in A_i$, since A_i is a left ideal).

Thus $A_1 + \cdots + A_n$ is a left ideal of R. □

Remark. *$A_1 + \cdots + A_n$ is the smallest (left, resp. right) ideal containing $A_1, \dots, A_n$.*[1]

This can be seen as follows (for left ideals), by checking the two properties from the statement:
(1) We have seen that $A_1 + \cdots + A_n$ is a left ideal.
(2) Every left ideal that contains $A_1, \dots, A_n$ contains $A_1 + \cdots + A_n$ (very straightforward from the definition of left ideal).

The smallest left ideal containing $A_1, \dots, A_n$ is by definition $(A_1 \cup \cdots \cup A_n)$, i.e, is

$$\bigcap \{I \mid I \text{ left ideal, } A_1, \dots, A_n \subseteq I\}.$$

We now show that $A_1 + \cdots + A_n$ is contained in any left ideal containing $A_1, \dots, A_n$.
Let I be an ideal containing $A_1, \dots, A_n$. Then $I \ni a_1 + \cdots a_n$, for every $a_i \in A_i$, $i = 1, \cdots, n$. This means $I \supseteq A_1 + \cdots + A_n$, which implies $(A_1 \cup \cdots \cup A_n) \supseteq A_1 + \cdots A_n$. The first one is the smallest ideal containing $A_1, \dots, A_n$, and the second one is an even smaller ideal containing $A_1, \dots, A_n$. This implies $(A_1 \cup \cdots \cup A_n) = A_1 + \cdots A_n$.

Theorem 1.17 (Isomorphism theorems)**.** *We have the following:*

1. *Let $f : R \to S$ be a morphism of rings. Then f induces an isomorphism of rings:*

$$\begin{array}{rcl} \tilde{f} : R/\ker(f) & \to & \operatorname{Im}(f) \\ x + \ker(f) & \mapsto & f(x) \end{array}.$$

   This result is also true for rings without 1.

2. *Let I and J be ideals in a ring R. Then:*

   (a) There is an isomorphism of rings:

$$\begin{array}{rcl} I/(I \cap J) & \to & (I + J)/J \\ x + I \cap J & \mapsto & x + J \end{array}.$$

[1] It means 2 things: (1) that $A_1 + \cdots + A_n$ is a (left, resp. right) ideal, and (2) that any (left, resp. right) ideal containing $A_1, \dots, A_n$ contains $A_1 + \cdots + A_n$ (so is bigger than $A_1 + \cdots + A_n$).

(b) *If $I \subseteq J$, then J/I is an ideal of R/I and there is an isomorphism of rings:*

$$\begin{array}{rcl} (R/I)/(J/I) & \to & R/J \\ (x+I)+J/I & \mapsto & x+J \end{array}.$$

Proof. 1. This is true for the additive Abelian groups $(R,+)$, $(S,+)$ and $(\ker(f),+)$, i.e.,:

$$\begin{array}{rcl} \tilde{f} : R/\ker(f) & \to & \mathrm{Im}(f) \\ x+\ker(f) & \mapsto & f(x) \end{array},$$

is an isomorphism of additive groups.
We only have to check that it is a morphism of rings. Let $a,b \in R$. Then $\tilde{f}((a+\ker(f))(b+\ker(f)) = \tilde{f}(ab+\ker(f)) = f(ab) = f(a)f(b) = \tilde{f}(a+\ker(f))\tilde{f}(b+\ker(f))$, and we also have $\tilde{f}(1+\ker(f)) = f(1) = 1$.

2. (a) Apply the first part for $\begin{array}{rcl} f : I & \to & (I+J)/J \\ x & \mapsto & (x+0)+J \end{array}.$

(b) Apply the first part for $\begin{array}{rcl} f : R/I & \to & R/J \\ x+I & \mapsto & x+J \end{array}.$

□

Definition 1.18. *A ring R is* **simple** *if the only ideals of R are $\{0\}$ and R.*

Important example: A division ring, and in particular a field, is a simple ring, as can be seen using Remark 1.10.4. (do it!! We will see other examples later).

We know consider rings of matrices:

Definition/Proposition 1.19. *Let R be a ring, and let $n \in \mathbb{N}$. The ring of $n \times n$ matrices over R is the set of all $n \times n$ matrices with coefficients in R, equipped with the usual sum and product of matrices. Its identity element is I_n. It is denoted by $\boldsymbol{M_n(R)}$.*

No proof (not hard, but long and not very interesting at all). □

Example. *$M_n(\mathbb{Z})$, $M_n(\mathbb{H})$, $M_n(\mathbb{Z}/n\mathbb{Z})$.*

Proposition 1.20. *Let R be a ring. Then J is an ideal of $M_n(R)$ if and only if J is of the form $M_n(I)$ (the set of $n \times n$ matrices with coefficients in I) for some ideal I of R.*

The proof will require the following lemma, which is obtained by an easy direct computation.

Lemma 1.21. *For $1 \leq r, s \leq n$, let $E_{r,s}$ be the matrix in $M_n(R)$ with 1 as the row r-column s entry and 0 elsewhere.*
Then for every matrix $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(R)$, the matrix $E_{p,r}AE_{s,q}$ is the matrix with a_{rs} as row p-column q entry and 0 elsewhere.

Proof of Proposition 1.20. .

"$\Leftarrow$" Let I be an ideal of R. Then $M_n(I)$ is an additive subgroup of $M_n(R)$ (since I is an additive subgroup of R).
Let $(a_{ij})_{1\leq i,j\leq n} \in M_n(I)$, and $(b_{ij})_{1\leq i,j\leq n} \in M_n(R)$.
Then $(a_{ij})_{1\leq i,j\leq n}(b_{ij})_{1\leq i,j\leq n} = (c_{ij})_{1\leq i,j\leq n}$, with $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. The coefficients of the sum are in I (since I is an ideal and $a_{ik} \in I$), and then $c_{ij} \in I$.
This proves $(c_{ij})_{1\leq i,j\leq n} \in M_n(I)$.
Similarly, $(b_{ij})_{1\leq i,j\leq n}(a_{ij})_{1\leq i,j\leq n} \in M_n(I)$.
$M_n(I)$ is then an ideal of $M_n(R)$.

"$\Rightarrow$" Let J be an ideal of $M_n(R)$ and define:

$$I = \{a \in R \mid a \text{ appears in the top left corner of some matrix in } J\}.$$

I is clearly an ideal of R: take $a, b \in I$ and $r \in R$. Then a (resp. b) appears in the top left corner of some matrix $A \in J$ (resp. $B \in J$), and we see that $a + b$ is given by the matrix $A + B$ (which is in J since J is an ideal), and ra, ar are given by the matrices $(rI_n).A, A.(rI_n)$ (which also are in J, since J is an ideal).

We know check that $J = M_n(I)$ and this is where we use the lemma.

We first prove that $M_n(I) \subseteq J$:
Let $A = (a_{ij})_{1\leq i,j\leq n} \in M_n(I)$, i.e., there exist matrices $A_{ij} \in J$ such that a_{ij} appears in the top left corner of A_{ij}.
Since $A_{ij} \in J$, we will express A using the matrices A_{ij}. Using the previous lemma, we know that the matrix $E_{i,1}A_{ij}E_{1,j}$ contains only zeroes, except for the coordinate (i, j) which is a_{ij}. Moreover, this matrix is in J because $A_{ij} \in J$ and J is an ideal.
Then $A = \sum_{1\leq i,j\leq n} E_{i,1}A_{ij}E_{1,j} \in J$.

To conclude, we check that $J \subseteq M_n(I)$:
Let $A = (a_{ij})_{1\leq i,j\leq n} \in J$. We have to show that $a_{ij} \in I$ for every $1 \leq i, j \leq n$.
But using lemma 1.21 we have:

$$\begin{pmatrix} a_{ij} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & & \cdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} = E_{1,i}AE_{j,1},$$

with $E_{1,i}AE_{j,1} \in J$ since $A \in J$ and J ideal. This gives $a_{ij} \in I$ for every $i, j \in \{1, \ldots, n\}$, and thus $A \in M_n(I)$. □

Remark. *The same statement as Proposition 1.20 but for left or right ideals, is false. See one of the exercise sheets.*

1.2 Hamilton's quaternions

We know that the ring $\mathbb{C}$ is completely determined by:

- $\mathbb{C}$ is a ring.
- $\mathbb{C}$ is $\mathbb{R} \oplus \mathbb{R}i$ as $\mathbb{R}$-vector space.
- $i^2 = -1$ and $ia = ai$ for every $a \in \mathbb{R}$.

This has been generalized (by Hamilton):

Definition 1.22. *The ring $\mathbb{H}$ of (real)* **quaternions** *is the ring determined by:*

- $\mathbb{H}$ *is a ring.*
- $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ *as $\mathbb{R}$-vector space.*
- $i^2 = j^2 = -1$, $ij = -ji = k$, *and i, j, k commute with the elements of $\mathbb{R}$. (Where we say that x commutes with the elements of $\mathbb{R}$ if $xa = ax$ for every $a \in \mathbb{R}$.)*

One can check that the definition of ring is verified (it is a very direct, but long, computation).

We have:

- $ik = i(ij) = i^2 j = -j$.
- $jk = j(ij) = j(-ji) = -j^2 i = i$.
- $ki = (ij)i = (-ji)i = -ji^2 = j$.
- $kj = (ij)j = ij^2 = -i$.
- $k^2 = (ij)(ij) = (ij)(-ji) = -ij^2 i = i^2 = -1$.

For $\alpha = a + bi + cj + dk \in \mathbb{H}$ we define

$$\bar{\boldsymbol{\alpha}} = a - bi - cj - dk,$$

the **conjugate of $\boldsymbol{\alpha}$**, and we have:

$$\begin{aligned}\alpha\bar{\alpha} &= (a+bi+cj+dk)(a-bi-cj-dk)\\ &= a^2-abi-acj-adk+bia-(bi)(bi)-(bi)(cj)-(bi)(dk)\\ &\quad +cja-(cj)(bi)-(cj)(cj)-(cj)(dk)+dka-(dk)(bi)\\ &\quad -(dk)(cj)-(dk)(dk)\\ &= a^2-abi-acj-adk+abi+b^2-bck+bdj+caj+bck+\\ &\quad c^2-cdi+adk-dbj+cdi+d^2\\ &= a^2+b^2+c^2+d^2.\end{aligned}$$

Applying this to $\bar{\alpha}$ we get $\bar{\alpha}\bar{\bar{\alpha}} = \bar{\alpha}\alpha = a^2+b^2+c^2+d^2$, and we then define:

$$\boldsymbol{n(\alpha)} = \bar{\alpha}\alpha = \alpha\bar{\alpha} = a^2+b^2+c^2+d^2,$$

the **norm of $\boldsymbol{\alpha}$**.

Since the norm is the sum of squares of the coefficients of α, computed in $\mathbb{R}$, we get the following important consequence:

If $\alpha \neq 0$ then $n(\alpha) \neq 0$ and thus $n(\alpha)$ has an inverse in $\mathbb{R}$. This gives:

$$(n(\alpha)^{-1}\bar{\alpha})\alpha = n(\alpha)^{-1}(\bar{\alpha}\alpha) = n(\alpha)^{-1}n(\alpha) = 1, \text{ and}$$

$$\alpha(n(\alpha)^{-1}\bar{\alpha}) = (\alpha\bar{\alpha})n(\alpha)^{-1} = n(\alpha)n(\alpha)^{-1} = 1$$

In other words, every nonzero element $\alpha \in \mathbb{H}$ has an inverse, and this inverse is $\alpha^{-1} = n(\alpha)^{-1}\bar{\alpha}$.
$\mathbb{H}$ is then a division ring (but $\mathbb{H}$ is not commutative since $ij = -ji$).

Chapter 2

Modules

Definition 2.1. *Let R be a ring. A (left)* ***R*-module** *M is an additive abelian group $(M, 0, +)$ together with a product*

$$R \times M \to M, \quad (r, m) \mapsto r.m$$

(multiplication on the left by the elements of R), such that, for every $r, s \in R$ and $a, b \in M$:

1. *$r(a + b) = ra + rb$;*

2. *$(r + s)a = ra + sa$;*

3. *$r(sa) = (rs)a$;*

4. *$1.a = a$.*

If R is a field, then a left R-module is called a **vector space** *(over R).*

Remark.
1. *There is also a notion of right R-module, with multiplication by elements of R on the right:*

$$M \times R \to M, \quad (m, r) \mapsto m.r.$$

2. *This is a generalization of the notion of vector space, where the product is by elements of a ring, instead of by elements of a field. It does make a real difference, as we will see.*

Example.
1. *Every vector space.*

2. *Let R be a ring, and $R[X]$ = the ring of polynomials in one variable over R. Then $R[X]$ is an R-module, with:*

$$\begin{array}{rcl} R \times R[X] & \to & R[X] \\ (r, a_0 + a_1 X + \cdots + a_n X^n) & \mapsto & ra_0 + ra_1 X + \cdots + ra_n X^n \end{array}.$$

3. *Let $(G, 0, +)$ be an Abelian group. Then G is a $\mathbb{Z}$-module with:*

$$\mathbb{Z} \times G \to G, \quad (n, g) \mapsto ng.$$

4. *(Important) Let R be a ring, and let I be a left ideal of R. Then I is a (left) R-module with:*

$$R \times I \to I, \quad (r, a) \mapsto ra.$$

Definition 2.2. *Let M be an R-module. A subset N of M is called a* **submodule** *if N is an additive subgroup of M and $rb \in N$ for all $r \in R$, $b \in N$.*

Example. 1. *(Important) R is an R-module. The left ideals of R are exactly the submodules of R (compare the definitions).*

2. *A vector space is a module. A sub-vector space is a submodule.*

Remark. 1. *A submodule is always a module (with the product given by the module).*

2. *Any intersection of submodules is a submodule.*

Definition 2.3. *Let M be an R-module, and let $X \subseteq M$. The intersection of all submodules of M containing X is a submodule which is called the* **submodule generated by X** *(or the span of X). It is the smallest submodule of M containing X.*

Proposition 2.4. *Let M be an R-module, and let $X \subseteq M$. The submodule N generated by X is:*

$$\mathrm{Span}(X) = \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N},\ r_i \in R,\ a_i \in X \textit{ for } i = 1, \cdots, n\}$$

(it is the set of linear combinations of elements of X, with coefficients in R).

Proof. Let $L = \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N},\ r_i \in R,\ a_i \in X \text{ for } i = 1, \cdots, n\}$. L is clearly a submodule of M containing X, so $N \subseteq L$.
We now show that any submodule containing X must contain L. Let K be a submodule containing X. Let $x = \sum_{i=1}^{n} r_i a_i$ with $r_i \in R$ and $a_i \in X$. Since $K \supseteq X$ and K is a submodule we have successively $r_i a_i \in K$ and $\sum_{i=1}^{n} r_i a_i \in K$. This proves that L is included in any submodule containing X, and in particular is included in N.
We then have $L = N$. □

The notion of basis is central for vector spaces. What happens for modules?

Definition 2.5. *Let M be an R-module, and let $X \subseteq M$. We say that:*

1. *X is* **linearly independent** *if*

$$\begin{gathered}\forall n \in \mathbb{N}, \quad \forall x_1, \ldots, x_n \in X \textit{ all different}, \quad \forall r_1, \ldots r_n \in R \\ r_1 x_1 + \cdots + r_n x_n = 0 \Rightarrow r_1 = \cdots = r_n = 0.\end{gathered}$$

2. *X* **generates** *M (or X is a set of* **generators** *of M) if*

$$\begin{gathered}\forall a \in M \quad \exists n \in \mathbb{N} \quad \exists x_1, \ldots, x_n \in X \quad \exists r_1, \ldots r_n \in R \\ a = r_1 x_1 + \cdots + r_n x_n.\end{gathered}$$

   (i.e., $\mathrm{Span}(X) = M$*).*

3. *X is a* **basis** *of M if X is linearly independent and X generates M.*

It is possible to define the sum and direct sum of modules, exactly as for vector spaces. We recall the definitions here. Make sure you are comfortable with them, and have a look at your linear algebra course if necessary, because we will use direct sums a lot.

Definition 2.6. *Let M be an R-module, and let M_i, $i \in I$, be submodules of M.*

1. *M is* **the sum of the submodules** *M_i, $i \in I$ if each $x \in M$ can be written as a finite sum of elements of the submodules M_i, $i \in I$. We write* $\boldsymbol{M = \sum_{i \in I} M_i}$*.*

2. *M is* **the direct sum of the submodules** *M_i, $i \in I$ if each $x \in M$ can be written in a unique way as finite sum of elements of the submodules M_i, $i \in I$. We write* $\boldsymbol{M = \bigoplus_{i \in I} M_i}$*.*

Remark. *It $M = \sum_{i \in I} M_i$, then $M = \bigoplus_{i \in I} M_i$ if and only if for every finite subset J of I and every $k \in I \setminus J$ we have $M_k \cap \sum_{j \in J} M_j = \{0\}$.*

DANGER:

In general you cannot work with bases in modules as you do with bases in vector spaces, as the following example shows:

Consider $\mathbb{Z}$ as a $\mathbb{Z}$-module (with usual sum and product in $\mathbb{Z}$). Let $a \in \mathbb{Z}$, $a > 1$.

Then the submodule generated by a is $\mathbb{Z}.a = \{na \mid n \in \mathbb{Z}\} \neq \mathbb{Z}$. We see that

$\{a\}$ does not generate $\mathbb{Z}$.
We also clearly see that $\{a\}$ is linearly independent.

Consider now $b \in \mathbb{Z}$, $b \neq 0$. Then $\{a, b\}$ is not linearly independent: Indeed $b \cdot a + (-a) \cdot b = 0$ and the coefficients of this linear combination (b and $-a$) are not both 0.

We can also check that the submodule generated by $\{a, b\}$ is:

$$\mathbb{Z}.d = \{nd \mid n \in \mathbb{Z}\},$$

where $d = \gcd(a, b)$ (see exercise sheets) which is different from $\mathbb{Z}$ if $d > 1$.

Recapitulating, we have:

- **$\{a\}$ is linearly independent but cannot be completed to a basis of $\mathbb{Z}$.**
- **If $gcd(a, b) = 1$ with $a, b > 1$, then $\{a, b\}$ generates $\mathbb{Z}$, $\{a, b\}$ is not linearly independent, but no proper subset of $\{a, b\}$ generates $\mathbb{Z}$.**

However, modules over a division ring behave correctly:

Lemma 2.7. *Let M be an R-module, with R a division ring. Then any maximal linearly independent subset X of M is a basis*[1].

Proof. Let N be the submodule generated by X. By definition, X is a basis of N, and the proof is finished if $N = M$.
Suppose $N \neq M$, take $a \in M \setminus N$ and consider $X \cup \{a\}$:
If we prove that $X \cup \{a\}$ is linearly independent, this will contradict "X maximal" and we will have $N = M$.
Suppose $ra + r_1x_1 + \cdots + r_nx_n = 0$, with $r, r_1, \ldots r_n \in R$, $x_1, \ldots .x_n \in X$. We distinguish two cases:

- If $r = 0$, then $r_1x_1 + \cdots + r_nx_n = 0$, which gives $r_1 = \cdots = r_n = 0$ since X is linearly independent.
- If $r \neq 0$, we get $a = r^{-1}(r_1x_1 + \cdots + r_nx_n)$. In particular we have $a \in N$, a contradiction. This case is impossible. □

Theorem 2.8. *Let M be a module over a division ring R. Then:*

1. *Every linearly independent subset of M is contained in a basis of M (in particular, every non-zero module has a basis).*

[1] X maximal linearly independent means 2 things: That X is linearly independent, and that any subset strictly larger than X is not linearly independent

2. *Every set of generators of M contains a basis of M.*

3. *Any two bases of M have the same cardinality.*

Proof. 1. Let $S = \{m_i\}_{i\in I}$ be a linearly independent subset of M, and let $A = \{T \subseteq M \mid S \subseteq T,\ T \text{ is linearly independent}\}$. A, with the (partial) order given by the inclusion ($T_1 \leq T_2$ iff $T_1 \subseteq T_2$) is a partially ordered set. We will apply Zorn's lemma to A:
A is non-empty since $S \in A$.
Let $B \subseteq A$ be a chain in A We want to find an upper bound of B in A. Let $T_B = \bigcup_{T\in B} T$. We first check that $T_B \in A$: Let $n \in \mathbb{N}$ and $x_1, \dots x_n \in T_B$. By definition of T_B there exist $T_1, \dots, T_n \in B$ such that $x_i \in T_i$ for $i = 1, \dots, n$.
Since B is a chain, one of the T_i contains the others, say T_1. We then have $x_1, \dots, x_n \in T_1$, and since T_1 is linearly independent, $\{x_1, \cdots, x_n\}$ is linearly independent.
This shows that T_B is linearly independent, i.e., $T_B \in A$. And by definition of T_B, it is necessarilly an upper bound of B.

Zorn's lemma then applies and gives a maximal element T_m in A: T_m is linearly independent and is not contained in any bigger linearly independent subset of M.

We now show that T_m generates M:
Let N be the submodule generated by T_m, and suppose $N \neq M$.
Choose $x \in M \setminus N$. We show that $T_m \cup \{x\}$ is linearly independent:
Let $n \in \mathbb{N}$ and $x_1, \dots, x_n \in T_m$, $r, r_1, \dots, r_n \in R$ such that $rx + r_1x_1 + \cdots + r_nx_n = 0$. We deduce $rx = (-r_1)x_1 + \cdots + (-r_nx_n)$, and we distinguish between 2 cases:

- If $r = 0$ then $r_1x_1 + \cdots + r_nx_n = 0$, which gives (since T_m is linearly independent): $r_1 = \cdots = r_n = 0$.
- If $r \neq 0$ then $x = r^{-1}(-r_1)x_1 + \cdots + r^{-1}(-r_n)x_n \in M$, a contradiction. This case is impossible.

Thus the first case is the only possibility, we have $r = r_1 = \cdots = r_n = 0$. $T_m \cup \{x\}$ is linearly independent, which contradicts the fact that T_m is maximal.

2. Exercise. The idea of the proof goes as follows: Let X be a set of generators of M. Use Zorn's lemma to find a maximal linearly independent subset of X. This is a basis.

3. No proof.

□

Definition 2.9. *Let M and N be R-modules over a ring R. A map $f : M \to N$ is a R-module* **homomorphism** *(or* **morphism of $\boldsymbol{R}$-modules***) if for all $a, b \in M$, for all $r \in R$:*

$$f(a+b) = f(a) + f(b) \text{ and } f(ra) = rf(a).$$

f is a monomorphism (resp. epimorphism, **isomorphism***) if f is a morphism and is injective (resp. surjective, bijective).*
The **kernel** *of f is*

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

The **image** *of f is*

$$\mathbf{Im}\,(\boldsymbol{f}) = \{f(x) \mid x \in M\} \quad (= f(M)).$$

$\mathrm{End}_{\boldsymbol{R}}\,\boldsymbol{M}$ *denotes the set of all morphisms of R-modules from M to M (such a morphism is called an* **endomorphism***).*
Two modules M and N are **isomorphic** *if there is an isomorphism of modules f from M to N. This is denoted by $M \cong N$ (or $M \simeq N$).*

Remark.

- $\ker(f)$, $\mathrm{Im}(f)$ *are submodules of M, N.*
- *If L is a submodule of M, then $f(L)$ is a submodule of N. If P is a submodule of N, then $f^{-1}(P)$ is a submodule of M.*
- $\ker(f) = \{0\} \Leftrightarrow f$ *injective .*
- *You all know the notation $M \to N$ to indicate a map from M to N. The notation $M \xrightarrow{\sim} N$ is used to indicate an isomorphism (it is used for rings, modules, groups, etc and means an isomorphism of rings, modules, groups, etc).*

Remark 2.10.

1. *R^n is an R-module.*
2. *$\mathrm{End}_R\,M$ is always a ring, under the following operations, for $f, g \in \mathrm{End}_R\,M$:*
   - *$(f+g)(m) = f(m) + g(m) \quad \forall m \in M$. tem $fg = f \circ g$, i.e., $(fg)(m) = (f \circ g)(m) \quad \forall m \in M$.*

   The identity is the identity map from M to M.

3. *If M has a basis $\{u_1, \ldots, u_n\}$ then M is isomorphic to R^n by:*

$$R^n \xrightarrow{\phi} M, \quad (r_1, \ldots, r_n) \mapsto r_1u_1 + \cdots + r_nu_n.$$

And

$$\operatorname{End}_R R^n \xrightarrow{\sim} \operatorname{End}_R M, \quad f \mapsto \phi \circ f \circ \phi^{-1}.$$

Theorem 2.11. *Let N be a submodule of an R-module M. Then the quotient group M/N is an R-module with the action of R on M/N defined by:*

$$R \times M/N \to M/N, \quad (r, a + N) \mapsto ra + N.$$

The map

$$\pi : M \to M/N, \quad a \mapsto a + N$$

is a surjective morphism of R-modules, with kernel N. π is usually called the canonical projection and M/N is called the **quotient** *of M by N.*

Proof. Similar to the corresponding one for rings. □

Theorem 2.12 (Isomorphism theorems)**.** *We have the following:*

1. *Let $f : M \to N$ be a morphism of modules. Then f induces an isomorphism of modules:*

$$\tilde{f} : M/\ker(f) \to \operatorname{Im}(f), \quad a + \ker(f) \mapsto f(a).$$

2. *Let A and B be submodules of M. Then:*

   (a) *There is an isomorphism of modules:*

$$A/(A \cap B) \to (A + B)/B, \quad x + A \cap B \mapsto x + B.$$

   (b) *If $A \subseteq B$, then B/A is a submodule of M/A and there is an isomorphism of modules:*

$$(M/A)/(B/A) \to M/B, \quad (x + A) + B/A \mapsto x + B.$$

Proof. Similar to the corresponding one for rings. □

Proposition 2.13. *Let M be an R-module and let N be a submodule of M. There is a one-to-one correspondance between the submodules of M containing N and the submodules of M/N, given by (if $\pi : M \to M/N$ denotes the canonical projection):*

$$\begin{array}{rcl} \{\textit{submodules of } M \textit{ containing } N\} & \mapsto & \{\textit{submodules of } M/N\} \\ L & \mapsto & \pi(L) \\ \pi^{-1}(P) & \leftarrow\!\shortmid & P \end{array} .$$

Proof. Similar to the corresponding one for rings (proposition 1.12). □

Definition 2.14. *A nonzero R-module M is* **simple** *if the only submodules of M are $\{0\}$ and M.*

(Sometimes the terminology "irreducible" can be found, but it is also used for other meanings, so we will avoid it.)

Remark. *If M is simple, then M is generated by any nonzero element:*
If $m \in M \setminus \{0\}$, then the submodule generated by m is non-zero, and then must be M (this submodule is $R.m$).

Definition 2.15. *Let R be a ring.*

- *An ideal (resp. left, right ideal) I in R is said to be* **maximal** *if I is different from R and for every ideal (resp. left, right ideal) J of R:*

  $$I \subseteq J \Rightarrow (J = I \text{ or } J = R).$$

  In words: J is not R and the only (left, right two-sided) ideal strictly larger than J is R.

- *An ideal (resp. left, right ideal) I in R is said to be* **minimal** *if I is different from $\{0\}$ and for every ideal (resp. left, right ideal) J of R:*

  $$J \subseteq I \Rightarrow (J = \{0\} \text{ or } J = I).$$

  In words: I is not $\{0\}$ and that only ideal strictly smaller than I is $\{0\}$.

A ring may have several maximal (or minimal) ideals. Examples:

- Let $R = \mathbb{Z}$. For $a, b \in \mathbb{Z}$, the ideal (a, b) generated by a, b is $(gcd(a, b)) = \mathbb{Z}.gcd(a, b)$, the ideal generated by $gcd(a, b)$.
  Then, if p is a prime, $(p) = \mathbb{Z}.p$ is maximal (so $\mathbb{Z}$ has a lot of maximal ideals):
  Let I be an ideal such that $\mathbb{Z}.p \subsetneqq I$. Take $a \in I \setminus \mathbb{Z}.p$. Then $(a, p) \subseteq I$. But $(a, p) = (gcd(a, p)) = (1) = \mathbb{Z}$. This proves that $I = \mathbb{Z}$.

- Let $S = \mathbb{Z}/2\mathbb{Z}$ be the ring of integers modulo 2, and let $R = S \times S$, with product and sum coordinate by coordinate (see Appendix A). S is a ring, and the subsets $\{0\} \times S$ and $S \times \{0\}$ are ideals of R. They are clearly both minimal (since they only contain 2 elements.)

Lemma 2.16. *A ring R has at least one maximal ideal (resp. maximal left, maximal right ideal).*

Proof. Consider $\mathcal{E} = \{I \text{ proper ideal of } R\} = \{I \text{ ideal of } R \mid 1 \notin I\}$, with the order given by the inclusion, and use Zorn's lemma (easy exercise). □

Proposition 2.17. *A left R-module M is simple if and only if $M \cong R/L$ for some maximal left ideal L of R.*

Proof. "⇒" We have $M = R.m$ for some $m \in M$, $m \neq 0$.
Define

$$f : R \to M, \quad r \mapsto r.m.$$

It is a morphism of R-modules. f is surjective, so induces an isomorphism from $R/\ker f$ to M (by the isomorphism theorem). We show that $\ker f$ is a maximal left ideal of R: Let J be a left ideal of R with $\ker f \subseteq J$. Then $f(J)$ is a submodule of M, so is equal to $\{0\}$ or M. In the first case we get $J = \ker f$, in the second case $J = R$, which shows that $\ker f$ is a maximal left ideal of R.
"⇐" Let ϕ be the isomorphism from M to R/L, and let N be an R-submodule of M. Then $\phi(N)$ is a submodule of R/L. In particular $\phi(N)$ is of the form J/L for some left ideal J of R, $J \supseteq L$ (see proposition 1.12).
Since L is maximal we have $J = L$ or $J = R$. If $J = L$ then $\phi(N) = \{0\}$, i.e., $N = \{0\}$. If $J = R$ then $\phi(N) = R/L$, i.e., $N = M$. □

Proposition 2.18 (Schur's lemma)**.** *If M is a simple R-module, then $\operatorname{End}_R M$ is a division ring.*

Proof. We have to show that every non-zero element $f \in \operatorname{End}_R M$ has an inverse. Let $f \in \operatorname{End}_R M \setminus \{0\}$.
$\operatorname{Im} f$ is a submodule of M, and so is $\{0\}$ or M (since M is simple). The first case is impossible because $f \neq 0$. We then have $\operatorname{Im} f = M$, i.e., f surjective.
$\ker f$ is a submodule of M, and so is $\{0\}$ or M (since M is simple). The second case is impossible because $f \neq 0$. We then have $\ker f = \{0\}$, i.e., f injective.
f is then bijective, and so has an inverse, which is easily checked to be an element of $\operatorname{End}_R M$. □

We conclude this part on modules by recalling the link between endomorphisms and square matrices.

Definition 2.19. *Let R be a ring. The* **opposite ring R^{op}** *is the ring defined by:*

- *R^{op} has the same elements as R and the same addition.*
- *The multiplication $\times^{op}$ in R^{op} is defined by $a \times^{op} b = ba$ (where the product on the right-hand side is computed in R).*

Remark.

- *If R is a division ring, then R^{op} is a division ring.*
- *If R is commutative, we have $R^{op} = R$.*

Theorem 2.20. *If M is an R-module isomorphic to R^n (i.e., M has a basis with n elements), then $\operatorname{End}_R M \cong M_n(R^{op})$.*

Proof. We only do it for $n = 2$ (the general case is similar) and $M = R^2$ (the result for a general M follows from the third part of Remark 2.10). Let

$$\begin{array}{rcl} \Phi : \operatorname{End}_R R^2 & \to & M_2(R^{op}) \\ f & \mapsto & \begin{pmatrix} f(\begin{pmatrix}1\\0\end{pmatrix}) & f(\begin{pmatrix}0\\1\end{pmatrix}) \end{pmatrix}, \end{array}$$

where $f(\begin{pmatrix}1\\0\end{pmatrix})$ and $f(\begin{pmatrix}0\\1\end{pmatrix})$ are elements of R^2 seen as column vectors (expressed in a fixed basis of R^2). We check that Φ is an isomorphism of rings. Let $f \in \operatorname{End}_R R^2$. Assume $\Phi(f) = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$. Then

$$\begin{aligned} f(\begin{pmatrix}u\\v\end{pmatrix}) &= f(u\begin{pmatrix}1\\0\end{pmatrix}) + vf(\begin{pmatrix}0\\1\end{pmatrix})) \\ &= u\begin{pmatrix}a_1\\a_2\end{pmatrix} + v\begin{pmatrix}b_1\\b_2\end{pmatrix} \\ &= \begin{pmatrix}ua_1 + vb_1\\ua_2 + vb_2\end{pmatrix} \end{aligned} \tag{2.1}$$

which shows that f is completely determined by $\Phi(f)$, so Φ is bijective.

It is clear that $\Phi(\mathrm{Id}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\Phi(f + g) = \Phi(f) + \Phi(g)$ whenever $f, g \in \operatorname{End}_R R^2$.

Consider now $g \in \operatorname{End}_R R^2$ with $\Phi(g) = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{pmatrix}$. We have

$$\begin{array}{rcl} f \circ g(\begin{pmatrix}1\\0\end{pmatrix}) & = & f(\begin{pmatrix}\alpha_1\\\alpha_2\end{pmatrix}) \\ & = & f(\alpha_1\begin{pmatrix}1\\0\end{pmatrix} + \alpha_2\begin{pmatrix}0\\1\end{pmatrix}) \\ & = & \alpha_1 f(\begin{pmatrix}1\\0\end{pmatrix}) + \alpha_2 f(\begin{pmatrix}0\\1\end{pmatrix}) \\ & = & \begin{pmatrix}\alpha_1 a_1 + \alpha_2 b_1\\ \alpha_1 a_2 + \alpha_2 b_2\end{pmatrix} \end{array}$$

and

$$\begin{aligned} f\circ g(\begin{pmatrix}0\\1\end{pmatrix}) &= f(\begin{pmatrix}\beta_1\\\beta_2\end{pmatrix}) \\ &= \begin{pmatrix}\beta_1a_1+\beta_2b_1\\\beta_1a_2+\beta_2b_2\end{pmatrix}, \end{aligned}$$

from which follows

$$\Phi(f\circ g)=\begin{pmatrix}\alpha_1a_1+\alpha_2b_1 & \beta_1a_1+\beta_2b_1\\\alpha_1a_2+\alpha_2b_2 & \beta_1a_2+\beta_2b_2\end{pmatrix}.$$

Now a product of matrices in $M_2(R)$ would give us

$$\Phi(f)\Phi(g)=\begin{pmatrix}a_1 & b_1\\a_2 & b_2\end{pmatrix}\begin{pmatrix}\alpha_1 & \beta_1\\\alpha_2 & \beta_2\end{pmatrix}=\begin{pmatrix}a_1\alpha_1+b_1\alpha_2 & a_1\beta_1+b_1\beta_2\\a_2\alpha_1+b_2\alpha_2 & a_1\beta_1+b_2\alpha_2\end{pmatrix},$$

which is not what we want.
But a product of matrices in $M_2(R^{op})$ gives

$$\begin{aligned} \Phi(f)\Phi(g) &= \begin{pmatrix}a_1 & b_1\\a_2 & b_2\end{pmatrix}\begin{pmatrix}\alpha_1 & \beta_1\\\alpha_2 & \beta_2\end{pmatrix} \\ &= \begin{pmatrix}a_1\times^{op}\alpha_1+b_1\times^{op}\alpha_2 & a_1\times^{op}\beta_1+b_1\times^{op}\beta_2\\a_1\times^{op}\alpha_1+b_2\times^{op}\alpha_2 & a_1\times^{op}\beta_1+b_2\times^{op}\alpha_2\end{pmatrix} \\ &= \begin{pmatrix}\alpha_1a_1+\alpha_2b_1 & \beta_1a_1+\beta_2b_1\\\alpha_1a_2+\alpha_2b_2 & \beta_1a_2+\beta_2b_2\end{pmatrix}, \end{aligned}$$

which is what we want. □

Remark. *If you want to then use matrices to compute the values of f, you have to do this is R^{op}, indeed:*

- *If you compute in R, you get for $f(\begin{pmatrix}u\\v\end{pmatrix})$:*

  $$\Phi(f)\begin{pmatrix}u\\v\end{pmatrix}=\begin{pmatrix}a_1u+b_1v\\a_2u+b_2v\end{pmatrix},$$

  which is not the correct result (compare with 2.1 above).

- *If you compute in R^{op}, you get for $f(\begin{pmatrix}u\\v\end{pmatrix})$:*

  $$\begin{aligned} \Phi(f)\begin{pmatrix}u\\v\end{pmatrix} &= \begin{pmatrix}a_1\times^{op}u+b_1\times^{op}v\\a_2\times^{op}u+b_2\times^{op}v\end{pmatrix} \\ &= \begin{pmatrix}ua_1+vb_1\\ua_2+vb_2\end{pmatrix}, \end{aligned}$$

  which is the desired result.

2.1 Chain conditions

Definition 2.21. *A family of subsets $\{C_i\}_{i\in I}$ in a set C is said to satisfy the* **ascending chain condition** *(***ACC** *for short) if there does not exist an infinite strictly increasing chain:*

$$C_{i_1} \subsetneqq C_{i_2} \subsetneqq \cdots \subsetneqq C_{i_k} \subsetneqq \cdots$$

of elements of $\{C_i\}_{i\in I}$.
An equivalent condition is:
For any ascending chain $C_{i_1} \subseteq C_{i_2} \subseteq \cdots \subseteq C_{i_k} \subseteq \cdots$, of elements of $\{C_i\}_{i\in I}$, there exists $n \in \mathbb{N}$ such that $C_{i_n} = C_{i_{n+1}} = C_{i_{n+2}} = \cdots$.

There is a corresponding notion for descending chains:

Definition 2.22. *A family of subsets $\{C_i\}_{i\in I}$ in a set C is said to satisfy the* **descending chain condition** *(***DCC** *for short) if there does not exist an infinite strictly descending chain:*

$$C_{i_1} \supsetneqq C_{i_2} \supsetneqq \cdots \supsetneqq C_{i_k} \supsetneqq \cdots$$

of elements of $\{C_i\}_{i\in I}$.
An equivalent condition is:
For any descending chain $C_{i_1} \supseteq C_{i_2} \supseteq \cdots \supseteq C_{i_k} \supseteq \cdots$, of elements of $\{C_i\}_{i\in I}$, there exists $n \in \mathbb{N}$ such that $C_{i_n} = C_{i_{n+1}} = C_{i_{n+2}} = \cdots$.

Example.

- *If V is a finite-dimensional vector space, then the following are equivalent (easy exercise, do it):*

  1. *The dimension of V is finite;*
  2. *The set of all subspaces of V satisfies the ACC;*
  3. *The set of all subspaces of V satisfies the DCC.*

  Since we don't have a well-behaved notion of dimension for R-modules, we will use this by analogy, and consider the notions of ACC or DCC for the set of submodules as a substitute (intuitively) to having finite dimension. Be careful that for the set of subsmodules of a given module, satisfying the ACC is not equivalent to satisfying the DCC.

- *If C is a finite set, every family $\{C_i\}_{i\in I}$ of subsets of C satisfies both the ACC and the DCC.*

- *The ideals of $\mathbb{Z}$ are of the form $a.\mathbb{Z}$ for $a \in \mathbb{Z}$, and $a.\mathbb{Z} \subseteq b.\mathbb{Z}$ if and only if b divides a. This implies that the set of ideals of $\mathbb{Z}$ satisfies the ACC (you can only divide a given element of $\mathbb{Z}$ a finite number of times).*

  Remark that the set of ideals of $\mathbb{Z}$ does not satisfy the DCC, because (for example) $\mathbb{Z} \supsetneqq 2.\mathbb{Z} \supsetneqq 2^2.\mathbb{Z} \supsetneqq 2^3.\mathbb{Z} \cdots$.

  Finally, observe that the ideals of $\mathbb{Z}$ are exactly the submodules of $\mathbb{Z}$ (when $\mathbb{Z}$ is seen as a $\mathbb{Z}$-module).

Definition 2.23. 1. *A ring R is* **left** *(resp.* **right***)* **Noetherian** *if the set of left (resp. right) ideals of R satisfies the ACC (i.e., there is no infinite strictly increasing chain of left (resp. right) ideals).*
R is **Noetherian** *if it is both left and right Noetherian.*

2. *A ring R is* **left** *(resp.* **right***)* **Artinian** *if the set of left (resp. right) ideals of R satisfies the DCC (i.e., there is no infinite strictly descending chain of left (resp. right) ideals).*
R is **Artinian** *if it is both left and right Artinian.*

There is also a notion of Noetherian and Artinian modules (where Noetherian means the set of submodules satifies the ACC, and Artinian means the set of submodules satisfies the DCC).

Example. 1. *Using the example after definition 2.22, we know that $\mathbb{Z}$ is Noetherian but not Artinian.*

2. *A division ring D is both Noetherian and Artinian, because the only (left, right) ideals of D are $\{0\}$ and D.*

3. *A finite ring is both Noetherian and Artinian.*

We saw that every ring has a maximal left ideal. It is not true that every ring has a minimal left ideal ($\mathbb{Z}$ gives a counter-example), but it is the case if R is Artinian:

Proposition 2.24. *If R is a ring such that $R \neq \{0\}$ and R satisfies the DCC on left ideals (*i.e. *R is left Artinian), then R has a minimal left ideal.*

Proof. Assume that R has no minimal left ideal. Pick any non-zero left ideal J_1 of R. Since J_1 is not minimal, there is a non-zero left ideal J_2 such that $J_2 \subsetneqq J_1$. Again, J_2 is not minimal, so there is a non-zero left ideal J_3 such that $J_3 \subsetneqq J_2$. If we keep doing this, we get an infinite strictly decreasing chain of left ideals of R:

$$J_1 \supsetneqq J_2 \supsetneqq J_3 \supsetneqq \cdots$$

contradicting the fact that R is left Artinian. □

(This space was taken by an older version of the proof of Proposition 2.24)

We give the next two results without proof, as examples of constructions that preserve the "Noetherian" and/or "Artinian" properties:

Proposition 2.25. *If R is left (resp. right) Noetherian, then $M_n(R)$ is left (resp. right) Noetherian.*
If R is left (resp. right) Artinian, then $M_n(R)$ is left (resp. right) Artinian.

Remark. *The proof of this proposition cannot be done using proposition 1.20, because proposition 1.20 gives informations about ideals (i.e., two-sided ideals), but the "Artinian" and "Noetherian" properties deal with left or right ideals.*

Theorem 2.26 (Hilbert basis theorem)**.** *If R is a commutative Noetherian ring, then so is $R[x]$ (and thus $R[x_1, \ldots, x_n]$).*

2.2 Composition series

If M is a module, the notions of ACC and DCC on the set of all submodules of M provide a kind of intuitive subsitute to the property "M has finite dimension".

We will try to be a bit more precise and get a substitute to "M has dimension n", and this can be done using the notion of composition series.

Definition 2.27. *Let M be an R-module.*

1. *A* **series** *S of M is a finite chain of submodules of M:*
$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n.$$
Its **length** *is the number of proper inclusions.*
Its **factors** *are the quotient modules M_i/M_{i-1}, for $i = 1, \ldots, n$*
Its set of modules is $\mathcal{M}(S) = \{M_0, \ldots, M_n\}$.

2. *Let S and T be two series of M. T is a* **refinement** *of S if $\mathcal{M}(S) \subseteq \mathcal{M}(T)$, and a proper refinement if $\mathcal{M}(S) \subsetneqq \mathcal{M}(T)$.*

3. *A* **composition series** *of a module M is a series of M that has no proper refinement (i.e., and it is an easy exercise, a series starting with $\{0\}$ and ending with M, in which every nonzero factor module is simple).*

Remark. 1. *Not every module has a composition series. For instance, let M be an infinite dimensional vector space over a field K. Then M is a K-module and has no composition series (for dimension reasons).*

2. *Let M be a finite-dimensional vector space, with basis $\{u_1, \ldots, u_n\}$. Then M has a composition series of length n:*
$$\{0\} \subsetneqq \mathrm{Span}\{u_1\} \subsetneqq \mathrm{Span}\{u_1, u_2\} \subsetneqq \cdots \subsetneqq \mathrm{Span}\{u_1, \ldots, u_{n-1}\} \subsetneqq M.$$
Actually, the following holds (easy exercise, do it):
The dimension of M is n if and only if M has a composisien series of length n.

Lemma 2.28. *Let R be a ring, let M be an R-module and let M' be a proper submodule of M. Assume that M has a composition series of length n. Then M' has a composition series of length less than n.*

Proof. Let $\{0\} = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_n = M$ be a composition series of M. We consider the following series of M':
$$\{0\} = (M_0 \cap M') \subseteq (M_1 \cap M') \subseteq \cdots \subseteq (M_n \cap M') = M'. \tag{2.2}$$

We first observe that the quotient $(M_{i+1} \cap M')/(M_i \cap M')$ is isomorphic to the submodule $P_i = [(M_{i+1} \cap M') + M_i]/M_i$ of M_{i+1}/M_i (the isomorphism is defined as follows, for $x \in M_{i+1} \cap M'$: $x + (M_i \cap M') \mapsto (x + 0) + M_i$; easy exercise).

Since M_{i+1}/M_i is simple, the submodule P_i is equal to $\{0\}$ or M_{i+1}/M_i (and in this later case $(M_{i+1} \cap M') + M_i = M_{i+1}$). So we have two possibilities for each i:

- $(M_{i+1} \cap M')/(M_i \cap M') = \{0\}$;
- $(M_{i+1} \cap M')/(M_i \cap M')$ is simple and $(M_{i+1} \cap M') + M_i = M_{i+1}$.

Reformulating these two possibilities, we obtain, for each i, either

- $(M_{i+1} \cap M') = (M_i \cap M')$, or
- $(M_{i+1} \cap M')/(M_i \cap M')$ is simple and $(M_{i+1} \cap M') + M_i = M_{i+1}$.

Note that this proves that the series (2.2) is a composition series (all the proper inclusions in the series give a simple quotient).

So we only have to check that the length of the series (2.2) is less than n, i.e., that $(M_{i+1} \cap M') = (M_i \cap M')$ for at least one i. Assume it is not the case, i.e., $(M_{i+1} \cap M')/(M_i \cap M')$ is simple and $(M_{i+1} \cap M') + M_i = M_{i+1}$ for every $i = 0, 1, \ldots, n$. We prove by induction on i that it implies $M_i \subseteq M'$, a contradiction for $i = n$:
If $i = 0$ we clearly have $M_0 = \{0\} \subseteq M'$.
Supposing by induction that $M_i \subseteq M'$, we obtain $M' \cap M_{i+1} = (M' \cap M_{i+1}) + M_i$. Since by induction hypothesis we have $(M' \cap M_{i+1}) + M_i = M_{i+1}$, we get $M' \cap M_{i+1} = M_{i+1}$, which means $M_{i+1} \subseteq M'$. □

Remark. *If M is an R-module with a composition series of length 0, then $M = \{0\}$.*

Indeed, let M_1 be a composition series of M of length 0. Then $M_1 = M$ (otherwise this composition series would have the proper refinement $M_1 \subsetneq M$) and $M_1 = \{0\}$ (otherwise it would have the proper refinement $\{0\} \subsetneq M_1$).

Theorem 2.29. *Let R be a ring and let M be an R-module.*

1. *M has a composition series if and only if M is Artinian and Noetherian.*

2. *If M has a composition series of length n, then every series of M has length at most n and can be refined to a composition series.*

Proof. 1. "$\Leftarrow$" First observe that a module satisfying the ACC on submodules always contains a maximal proper submodule (the proof is similar to that of proposition 2.24).
We then choose a maximal proper submodule M_1 of M, a maximal proper submodule M_2 of M_1, and so on...
By the DCC on submodules, there is $k \in \mathbb{N}$ such that $M_k = M_\ell$ for every $\ell \geq k$. But this can only happen if $M_k = \{0\}$. Then $M \supsetneq M_1 \supsetneq \cdots \supsetneq M_{k-1} \supsetneq \{0\}$ is a composition series for M.
"$\Rightarrow$" It follows from the next item.

2. Let $N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_k = M$ be a series of M. We show by induction on n that $k \leq n$. This is clear if $n = 0$ since in this case $M = \{0\}$. By lemma 2.28, N_{k-1} has a composition series of length at most $n - 1$, so by induction the length of the series $N_0 \subsetneqq \cdots \subsetneqq N_{k-1}$ is at most $n - 1$, so the length of $N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_k = M$ is less than n.

   Let $\mathcal{S}$ be a series of M. Knowing that every series of M has length at most n, we can then take a series of M that is a refinement (not necessarilly proper) of $\mathcal{S}$ and is of maximal length. This last property implies that it is a composition series. □

Remark. *In particular if M has a composition series, then any two composition series of M have the same length:*

Let $\mathcal{S}_1$ be a composition series of length n_1 and $\mathcal{S}_2$ be a composition series of length n_2. Then $n_1 \leq n_2$ and $n_2 \leq n_1$, so $n_1 = n_2$.

It is actually possible to obtain the following two results (which we will not need) about composition series.

Definition 2.30. *Two series of M are equivalent if there is a bijection between their sets of nonzero factor modules, so that corresponding factor modules are isomorphic.*

Theorem 2.31 (Schreier)**.** *Any two series of a module have equivalent refinements.*

Theorem 2.32 (Jordan-Hölder)**.** *Any two composition series of a module are equivalent.*

Proof. It follows at once from the Schreier theorem since a composition series has no proper refinement. □

Remark. *Conversely, the Schreier theorem follows easily out of the Jordan-Hölder theorem with the help of theorem 2.29.*

Chapter 3

Semisimple modules and rings

3.1 Semisimplicity

Definition 3.1. Semisimple modules *are defined by any of the equivalent conditions presented in the next proposition.*

Proposition 3.2. *Let M be an R-module. The following are equivalent:*

1. *M is a direct sum of simple submodules.*
2. *M is a sum of simple submodules.*
3. *Every submodule of M is a direct summand (i.e., for every submodule N of M, there is a submodule P of M such that $M = N \oplus P$).*

Proof. 1. $\Rightarrow$ 2. is clear.
2. $\Rightarrow$ 1. and 3.: By hypothesis we have $M = \sum_{i\in I} S_i$, where the S_i are simple submodules of M.
Let N be a submodule of M, and consider

$$\begin{aligned}\mathcal{S} = \{J \subseteq I \mid\ & \text{all sums in the following expression are direct} \\ & \qquad \text{sums: } N + \sum_{i\in J} S_i\} \\ = \{J \subseteq I \mid N \cap \sum_{i\in J} S_i &= \{0\} \wedge [S_j \cap (N + \sum_{i\in J, i\neq j} S_i) = \{0\}\ \forall j \in J]\}.\end{aligned}$$

Applying Zorn's lemma (exercise: check that the hypotheses are satisfied), we find a maximal element J of $\mathcal{S}$. Note that by choice of J the sum $N + \sum_{i\in J} S_i$ is direct, i.e., equal to $N \oplus \bigoplus_{i\in J} S_i$. In particular we now only have to prove that $N + \sum_{i\in J} S_i = M$ to get 3.

Assume $N + \sum_{i\in J} S_i \subsetneq M$. Then there is $k \in I$ such that $S_k \nsubseteq N + \sum_{i\in J} S_i$. It follows:

$$(N + \sum_{i\in J} S_i) \cap S_k \subsetneq S_k, \text{ and thus}$$

$$(N + \sum_{i\in J} S_i) \cap S_k = \{0\}$$

since S_k is simple.
This means that the sum $N + \sum_{i\in J\cup\{k\}} S_i$ is direct, contradicting the choice of J.

The case $N = \{0\}$ yields $M = \bigoplus_{i\in J} S_i$.

3. $\Rightarrow$ 2.: With start by proving the following.
Claim: Any non-zero cyclic (=generated by one element only, so of the form Ra for some $a \in M$) submodule of M contains a simple submodule.
Proof of the claim: The map $\phi : R \to Ra$, $r \mapsto ra$ is a module homomorphism from the left R-module R to the left R-module Ra. Its kernel is a left ideal of R, which is then contained in a maximal left ideal L of R. Then $\phi(L) = La$ is a maximal submodule of Ra (easy exercise), and therefore the quotient module Ra/La is simple (easy exercise again). We now use the hypothesis: By 3. La is a direct summand in M, i.e., there is a submodule N of M such that $M = La \oplus N$. It follows easily that $Ra = La \oplus (Ra \cap N)$, which yields $Ra \cap N \cong Ra/La$ as R-module, so $Ra \cap N$ is simple. End of the proof of the claim.

Let now N be the sum of all simple submodules of M. Then $M = N \oplus N'$ for some submodule N' of M. We check that $N' = \{0\}$: Otherwise N' contains a cyclic submodule of M (take any $a \in N\setminus\{0\}$ and consider Ra). By the above claim, N then contains a simple submodule S, so $S \subseteq N$, which contradicts $N \cap N' = \{0\}$. □

Proposition 3.3. 1. *A direct sum of semisimple R-modules is semisimple.*

2. *Every submodule of a semisimple R-module is semisimple.*

3. *Every quotient module of a semisimple R-module is semisimple.*

Proof. Since it follows rather easily from proposition 3.2, we only present a sketch of the proof.

1. This one is obvious.

2. Use the (easy; exercise) fact that if M is a module and S, T and A are submodules of M such that $M = S \oplus T$ and S submodule of A, then $A = S \oplus (T \cap A)$.

3. If M is semisimple and N is a submodule of M, then $M = N \oplus P$ for some submodule P of M. P is semisimple by 2. and $M/N \cong P$. □

Definition 3.4. *A ring R is called* **semisimple** *if every left R-module is semisimple.*

Remark 3.5. *Every R-module is isomorphic to a quotient of a direct sum of copies of the R-module R:*

Let M be an R-module. Then the map $f : \bigoplus_{m \in M} R \to M$, $(r_m)_{m \in M} \mapsto \sum_{m \in M} r_m \cdot m$ is a surjective morphism of R-module (observe that the sum makes sense, since by definition of $\bigoplus_{m \in M} R$ only finitely many of the elements in the tuple $(r_m)_{m \in M}$ are non-zero, so it is a finite sum). By the isomorphism theorem for modules, we get $\bigoplus_{m \in M} R / \ker f \cong M$.

Proposition 3.6. *For a ring R, the following statements are equivalent:*

1. *R is semisimple.*

2. *The left R-module R is semisimple.*

3. *R is a direct sum of minimal left ideals.*

4. *R is a direct sum of finitely many minimal left ideals.*

Proof. 1. $\Rightarrow$ 2. Clear.
2. $\Rightarrow$ 1. By proposition 3.3, since every left R-module is a isomorphic to a quotient of a direct sum of copies of R (by remark 3.5).
2. $\Rightarrow$ 3. and 4. By definition of semisimplicity, R is a direct sum of simple submodules, and a simple submodule of R is a minimal left ideal of R. So $R = \bigoplus_{i \in I} L_i$, where the L_i are minimal left ideals of R. But such a direct sum is always finite. Indeed, consider the element $1 \in R$. We have $1 = \sum_{j \in J} e_i$, where J is a finite subset of I and $e_j \in L_j$, for every $j \in J$.
Consider now $x \in L_k$, for some $k \notin J$. Then $x \cdot 1 = x$, i.e., $\sum_{j \in J} x e_j = x$. Since $x \in L_k$ and $x e_j \in L_j$, the fact that the L_i are in direct sum gives us $x = 0$, so $L_k = \{0\}$ for every $k \notin J$. □

Be careful: There is no obvious direct link between simple and semisimple rings. The simple condition is about 2-sided ideals, while the semisimple condition is about minimal left ideals (or minimal right ideals, cf. Remark 3.17).

We have actually seen some semisimple rings:

Proposition 3.7. *Let D be a division ring and let $n \in \mathbb{N}$. Then $M_n(D)$ is a direct sum of minimal left ideals (and thus is semisimple).*

Proof. Let L_i be the set of matrices in $M_n(D)$ whose entries are zero outside the ith column. L_i is a left ideal of $M_n(D)$ and $R = L_1 \oplus \cdots \oplus L_n$. That $L_1, \dots, L_n$ are minimal ideals is left as exercise (show that if I is an ideal that is included in L_1 and $I \neq \{0\}$, then $I = L_1$). □

Exercise 3.8. *Let R be a ring and let I, J be left ideals of R such that $R = I \oplus J$. Then there are two idempotents $e, f \in R$ such that*

$$I = Re, \quad J = Rf, \quad 1 = e + f.$$

(An element x in a ring is called an idempotent if $x^2 = x$.)

Hint: Start by writing $1 = e + f$ with $e \in I$ and $f \in J$.

3.2 The structure of semisimple rings

Proposition 3.9. *Let $\{R_i\}_{i \in I}$ be a nonempty family of rings and let $\prod_{i \in I} R_i$ be the direct product of the abelian groups $(R_i, +)$, $i \in I$.*

1. *$\prod_{i \in I} R_i$ is a ring, with product defined by $(a_i)_{i \in I}(b_i)_i \in I = (a_i b_i)_{i \in I}$. If 1_i denotes the identity of R_i (for $i \in I$), then $(1_i)_{i \in I}$ is the identity of $\prod_{i \in I} R_i$;*

2. *If R_i is commutative for every $i \in I$, then $\prod_{i \in I} R_i$ is commutative;*

3. *For each $k \in I$ the canonical projection $\pi_k : \prod_{i \in I} R_i \to R_k$ given by $(a_i)_{i \in I} \mapsto a_k$ is a surjective morphism of rings.*

Proof. Exercise. □

Definition 3.10. *The ring $\prod_{i \in I} R_i$ defined in proposition 3.9 is called the (direct)* **product of the rings** *R_i, $i \in I$.*

Proposition 3.11. *Let $R_1, \dots, R_n$ (for some $n \in \mathbb{N}$) be semisimple rings. Then $\prod_{i=1}^n R_i$ is semisimple.*

Proof. Exercise. □

Remark. *Using proposition 3.7 we then see that if $D_1, \dots, D_n$ are division rings and $k_1, \dots, k_n \in \mathbb{N}$, then $M_{k_1}(D_1) \times \cdots \times M_{k_n}(D_n)$ is semisimple. We will see in theorem 3.16 that the converse also holds.*

Let $A_1, \dots, A_m$, $B_1, \dots, B_n$ be R-modules and let $A = \bigoplus_{i=1}^m A_i$, $B = \bigoplus_{j=1}^n B_j$. We describe the morphisms of R-modules $\phi : B \to A$.
For $j = 1, \dots, n$ let λ_j be the canonical inclusion of B_j into $\bigoplus_{\ell=1}^n B_\ell$.
For $i = 1, \dots, m$ let π_i be the canonical projection from $\bigoplus_{\ell=1}^m A_\ell$ onto A_i.

Let $x \in \bigoplus_{j=1}^n B_j$ and write it as $x = x_1 + \dots + x_n$ with $x_j \in B_j$ for $j = 1, \dots, n$. Since ϕ is R-linear, we have $\phi(x) = \phi(x_1) + \dots + \phi(x_n)$. In other words ϕ is uniquely determined by $\phi \circ \lambda_1, \dots, \phi \circ \lambda_n$.

Now, each morphism $\phi \circ \lambda_j$ has values in $\bigoplus_{i=1}^m A_i$, so is uniquely determined by its m coordinates in $A_1, \dots, A_m$. In other words, $\phi \circ \lambda_i$ is uniquely determined by $\pi_1 \circ \phi \circ \lambda_j, \dots, \pi_m \circ \phi \circ \lambda_j$.

We then just proved that ϕ is uniquely determined by the collection of morphisms of R-modules $\phi_{ij} = \pi_i \circ \phi \circ \lambda_j : B_j \to A_i$. We sum it up and prove a bit more in the next proposition.

Proposition 3.12. *With the notation introduced since definition 3.10:*
There is a bijection between morphisms of R-modules $\phi : \bigoplus_{j=1}^n B_j \to \bigoplus_{i=1}^m A_i$ and $m \times n$ matrices $(\phi_{ij})_{i=1,\dots,m \ j=1,\dots,n}$ of homomorphisms of R-modules $\phi_{ij} : B_j \to A_i$.
Moreover, if $\phi' : \bigoplus_{j=1}^n B_j \to \bigoplus_{i=1}^m A_i$ and if $\psi : \bigoplus_{k=1}^\ell C_k \to \bigoplus_{j=1}^n B_j$ are morphisms of R-modules, then

1. *the matrix corresponding to $\phi + \phi'$ is the sum of the matrices corresponding to ϕ and ϕ';*

2. *the matrix corresponding to $\phi \circ \psi$ is the product of the matrices corresponding to ϕ and ψ.*

Proof. The first part was proved before the statement of the proposition, and the part concerning the sum is obvious. We then only check the last statement.
Let μ_k be the canonical injection from C_k to $\bigoplus_{i=1}^\ell C_i$ and let p_j be the canonical projection from $\bigoplus_{\ell=1}^n B_\ell$ onto B_j. Since $\sum_{j=1}^n \lambda_j \circ p_j$ is the identity on $\bigoplus_{j=1}^n B_j$ we have

$$\pi_i \circ \phi \circ \psi \circ \mu_k = \pi_i \circ \phi \circ (\sum_{j=1}^n \lambda_j \circ p_j) \circ \psi \circ \mu_k = \sum_{j=1}^n \phi_{ij} \circ \psi_{jk}. \qquad \square$$

Remark. *What happens if $A = R^n$ and $B = R^n$?*

Then a morphism of R-modules $\phi : B \to A$ corresponds to an $m \times n$ matrix of elements of $\mathrm{End}_R R$. *By theorem 2.20, we know that* $\mathrm{End}_R R \cong R^{op}$. *By proposition 3.12 we then have* $\mathrm{End}_R(R^n) \cong M_n(R^{op})$.

Corollary 3.13. *Let S be a simple R-module and let $D = \operatorname{End}_R S$. Then $\operatorname{End}_R S^n \cong M_n(D)$, for all $n \in \mathbb{N}$ (S^n is the direct sum of n copies of S).*

Proposition 3.14. *Let R be a semisimple ring, written $R = I_1 \oplus \cdots \oplus I_n$ with $I_1, \ldots, I_n$ minimal left ideals (see proposition 3.6). Then every simple R-module is isomorphic to one of $I_1, \ldots, I_n$.*

Proof. Let S be a simple R-module. We have $S \cong \operatorname{Hom}_R(R, S)$, from which follows $\operatorname{Hom}_R(R, S) \neq \{0\}$. Since $R \cong I_1 \oplus \cdots \oplus I_k$, by proposition 3.12 we know $\operatorname{Hom}_R(R, S) \cong \operatorname{Hom}_R(I_1, S) \times \cdots \times \operatorname{Hom}_R(I_n, S)$, so this last product of rings is non-zero. It means that there is $j \in \{1, \ldots, n\}$ such that $\operatorname{Hom}_R(I_j, S) \neq \{0\}$. Since both I_j and S are simple R-modules, the only morphisms between them are the zero morphism and isomorphisms. So I_j and S are isomorphic. □

Proposition 3.15. *Let $S_1, \ldots, S_k$ be simple R-modules, and let $n_1, \ldots, n_k \in \mathbb{N}$. Assume that $S_1, \ldots, S_k$ are pairwise non isomorphic. Let $M = S_1^{n_1} \oplus \cdots \oplus S_k^{n_k}$ and let D_i be the division ring $\operatorname{End}_R S_i$ for $i = 1, \ldots, k$.*
Then $\operatorname{End}_R M \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$.

Proof. By proposition 3.12, $\operatorname{End}_R M$ is isomorphic to a ring of $k \times k$ matrices of the form $(f_{ij})_{1 \leq i,j \leq k}$, where $f_{ij} : S_j^{n_j} \to S_i^{n_i}$ is a morphism of R-modules.

If $i \neq j$, by proposition 3.12 again: f_{ij} is represented by a matrix of morphisms of R-modules from S_j to S_i. Since both S_j and S_i are simple R-modules, the only morphisms of R-modules between them are isomorphisms or the zero map. Since S_j and S_i are not isomorphic by hypothesis, f_{ij} is the zero map (whenever $i \neq j$).

It follows that the matrix $(f_{ij})_{1 \leq i,j \leq k}$ is a diagonal matrix, whose diagonal entries are in $\operatorname{End}_R S_i^{n_i}$. So

$$\operatorname{End}_R M \cong \operatorname{End}_R S_1^{n_1} \times \cdots \times \operatorname{End}_R S_k^{n_k},$$

and using corollary 3.13 we obtain the result. □

Theorem 3.16 (Wedderburn-Artin)**.** *A ring R is semisimple if and only if it is isomorphic to a direct product $M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$, for some $k, n_1, \ldots, n_k \in \mathbb{N}$ and some division rings $D_1, \ldots, D_k$.*

Proof. Let R be a semisimple ring. By proposition 3.6

$$R = I_1 \oplus \cdots \oplus I_k,$$

where the I_ℓ are minimal left ideals of R, and in particular simple R-modules of R. Regrouping together the R-modules I_i that are isomorphic to each other we obtain

$$R \cong S_1^{n_1} \oplus \cdots \oplus S_\ell^{n_\ell},$$

where $S_1, \dots, S_n$ are pairwise non isomorphic simple R-modules.
It follows, by proposition 3.15:

$$\operatorname{End}_R R \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_\ell}(\Delta_\ell),$$

for some division rings $\Delta_1, \dots, \Delta_\ell$. Finally, since $\operatorname{End}_R R \cong R^{op}$ and $(R^{op})^{op} \cong R$ we obtain

$$\begin{aligned} R &\cong (M_{n_1}(\Delta_1) \times \cdots \times M_{n_\ell}(\Delta_\ell))^{op} \\ &\cong M_{n_1}(\Delta_1)^{op} \times \cdots \times M_{n_\ell}(\Delta_\ell)^{op} \\ &\cong M_{n_1}(\Delta_1^{op}) \times \cdots \times M_{n_\ell}(\Delta_\ell^{op}). \end{aligned}$$ □

Remark 3.17. *We defined semisimple rings in terms of left modules, simple (left-)submodules, and minimal left ideals, so we could call it left-semisimple. We can similarly define right-semisimple by using right R-modules, simple right-submodules, and minimal right ideals, and we can re-do this whole chapter for this notion of right-semisimple, and we will get the exact same Wedderburn-Artin theorem, which does not depend on "left" or "right". So these two notions of left and right-semisimple ring coincide, which is why we just say semisimple*

Corollary 3.18. *Every semisimple ring is left Artinian, left Noetherian, right Artinian, right Noetherian.*

Proof. By proposition 3.6 $R = I_1 \oplus \cdots \oplus I_k$, where $k \in \mathbb{N}$ and $I_1, \dots, I_k$ are minimal left ideals of R, i.e., minimal submodules of the left R-module R. It follows easily that

$$\{0\} \subsetneq I_1 \subsetneq I_1 \oplus I_2 \subsetneq \cdots \subsetneq I_1 \oplus \cdots \oplus I_{k-1} \oplus R$$

is a composition series for R. We can now apply theorem 2.29 to the left R-module R to get the conclusion about left-Noetherian and left-Artinian.

The statements about right Artinian and right Noetherian follow from Remark 3.17: redoing the same argument with "right" semisimple will get that a semisimple ring is right Artinian and right Noetherian. □

3.3 The structure of simple rings

Lemma 3.19. *Let R be a ring and let $f : R \to R$ be a morphism of R-modules. If I is a minimal left ideal of R, then $f(I)$ is either $\{0\}$ or a minimal left ideal of R.*

Proof. Assume that $f(I) \neq \{0\}$ and let J be a left ideal of R such that $J \subseteq f(I)$. Then $f^{-1}(J) \cap I$ is a left ideal of R included in I. So $f^{-1}(J) \cap I = \{0\}$ or $f^{-1}(J) \cap I = I$. In the first case $J = \{0\}$ and in the second case $I \subseteq f^{-1}(J)$, so $J = f(I)$. □

Lemma 3.20. *Let R be a ring with a minimal left ideal L, and let S be the sum of all minimal left ideals of R. Then S is a 2-sided ideal of R.*

Proof. By definition, S is a left ideal of R, so we only have to check that if $x \in S$ and $r \in R$, then $xr \in S$. Again by definition of S, we have $x = a_1 + \cdots + a_t$ where each a_s belongs to some minimal left ideal I_s for $s = 1, \ldots, t$. Since $xr = a_1r + \cdots + a_tr$, we will be done if we show that each a_sr is zero or belongs to a minimal left ideal of R.

But $a_sr \in I_sr$, which is either 0 or a minimal left ideal of R by Lemma 3.19 (use the morphism of R-modules $f(z) = zr$ from R to R). □

Remark. *By definition of semisimple, the ideal S in the previous lemma is the largest "semisimple part" of R. Obviously, we will have $S = R$ when R is semisimple (cf. Proposision 3.6).*

The ideal S is often called the socle of the ring R.

Theorem 3.21. *(Wedderburn-Artin) Let R be a simple ring. The following are equivalent:*

1. *R is left Artinian;*
2. *R is semisimple;*
3. *R has a minimal left ideal;*
4. *R is isomorphic to $M_n(D)$ for some $n \in \mathbb{N}$ and some division ring D.*

Proof. We first record the implications that have already been proved:

- 1 implies 3 follows from Proposition 2.24 (even for a general ring R).
- 2 implies 3 by Proposition 3.6
- 2 implies 1 by Corollary 3.18.

The equivalence of 2 and 4 is clear by Theorem 3.16 (indeed, if R is a product of more than one matrix ring, then it will have proper 2-sided ideals, for instance $M_{n_1}(D_1) \times \{0\} \times \cdots \times \{0\}$, which is impossible).

Finally, 3 implies 2: Let S be the sum of all minimal left ideals of R. It is a 2-sided ideal of R by Lemma 3.20, and is non-zero since R has at least one minimal left ideal. Therefore $S = R$, and the conclusion follows since S is semisimple by definition. □

Corollary 3.22. *Let R be a finite ring. Then R is simple if and only if R is isomorphic to $M_n(F)$ for some finite field F and some integer $n \in \mathbb{N}$.*

Proof. It follows immediately from Theorem 3.21 and Theorem , since R, and thus D, is finite. □

Observe that, by Theorem 3.21, a simple ring is semisimple if and only if it is Artinian. And there are simple rings that are not Artinian, hence not semisimple. An example can be obtained as follows:

If R is a ring and M is a maximal ideal of R, then R/M is simple. If we can find such an R and M such that R/M is not Artinian, we will have that R/M is not semisimple. Let K be a field and let V be an infinite-dimensional K-vector space. Let $R = \operatorname{End}_K V$. Then

$$M := \{f \in R \mid \dim(\operatorname{Im} f) \text{ is finite}\}$$

is a maximal ideal of R, and R/M is not Artinian. Hence R/M is simple but not semisimple. (Exercise, it might end up in one of the exercise sheets.)

We have seen that simple Artinian rings are of the form $M_n(D)$ for some $n \in \mathbb{N}$ and some division ring D. We conclude this chapter by some results on such rings and their simple modules.

Let $V = D^n$. Then V is a left R-module with the action

$$R \times V \to V, \quad (A, v) \mapsto A \cdot v.$$

We have

Proposition 3.23. *1. V is a simple R-module;*

2. Any simple R-module is isomorphic to V.

Proof:

1. Let M be a non-zero R-submodule of D^n, and let $m \in M$, $m \neq 0$. Then $R \cdot m \subseteq M$, but $R \cdot m = D^n$ (simple linear algebra exercise). So $M = D^n$.

2. Let $\{e_1, \ldots, e_n\}$ be any basis of D^n and define

$$\xi : R \to V \oplus \cdots \oplus V, \quad A \mapsto (A \cdot e_1, \ldots, A \cdot e_n).$$

It is not very hard to check that ξ is an isomorphism of R-modules (linear algebra exercise).

Let M be a simple R-module, and let $m \in M$, $m \neq 0$. We define $\lambda : R \to M$, $\lambda(r) = rm$, and we define

$$\tau : V \oplus \cdots \oplus V \overset{\xi^{-1}}{\to} R \overset{\lambda}{\to} M.$$

We obtain in this way n morphism of R-modules τ_i (for $i = 1, \dots, n$):

$$V \overset{\text{id}}{\to} 0 \oplus \cdots \oplus 0 \oplus V \oplus 0 \oplus \cdots \oplus 0 \to R \overset{\lambda}{\to} M$$

(where the second map is the restriction of ξ^{-1}), and we have $\tau = \tau_1 + \cdots + \tau_n$.

Since $\tau \neq 0$, one of the τ_i is non zero, say $\tau_1 \neq 0$. It follows that τ_1 is an isomorphism since both V and M are simple R-modules. □

Lemma 3.24. *Let $R \cong M_n(D)$ with notation as above. Then and*

1. *V and $M_n(D)$ can be seen as an R-modules;*
2. *V is simple as R-module;*
3. *the R-modules R and $V \oplus \cdots \oplus V$ are isomorphic;*
4. *$D^{op} \cong \operatorname{End}_R V$.*

Proof. Let $\lambda : R \to M_n(D)$ be an isomorphism. Using this isomorphism, every $M_n(D)$-module M can be seen as an R-module by defining the product:

$$r \cdot m = \lambda(r) \cdot m,$$

for $r \in R$ and $m \in M$. A direct simple verification shows that the R-submodules of M are exactly the same as the $M_n(D)$-submodules of M. The first two statements follow immediately from this.

For the third statement, a direct verification shows that the map λ is an isomorphism of R-modules from R to $M_n(D)$, and the result follows since $M_n(D) \cong V \oplus \cdots \oplus V$ (as $M_n(D)$-modules, but the definition of direct sum only depends on the sum, so it is also statisfied if we look at them as R-modules).

We check the final statement. We must associate, to every element of D^{op}, an element of $\operatorname{End}_R V$. Let $d \in D^{\text{op}}$, and define

$$\mu_d : V \to V, \quad \mu_d(v) = v \cdot d.$$

We have $\mu_d(v_1+v_2) = \mu_d(v_1)+\mu_d(v_2)$ and, for $r \in R$, $\mu_d(r\cdot v) = \mu_d(\lambda(r)\cdot v) = \lambda(r) \cdot v \cdot d = \lambda(r) \cdot \mu_d(v) = r \cdot \lambda_d(v)$, so $\lambda_d \in \operatorname{End}_R V$. We only have to show that the map

$$\mu : D \to \operatorname{End}_R V, \quad d \mapsto \mu_d$$

is an isomorphism of rings, i.e., that it is a morphism: $\mu_{d_1+d_2} = \mu_{d_1} + \mu_{d_2}$, $\mu_{d_1 \times^{\mathrm{op}} d_2} = \mu_{d_1} \circ \mu_{d_2}$, and $\mu_1 = \mathrm{Id}$ (this is left as an exercise), and that it is bijective. The injectivity is easy, for the surjectivity, let $f \in \mathrm{End}_R V$. If we write

$$f(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}) = \begin{pmatrix} d \\ * \\ \vdots \\ * \end{pmatrix},$$

then (written for $R = M_n(D)$ to simplify the notation; for the general case, the map λ also comes in):

$$\begin{aligned} f(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}) &= f(\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}) \\ &= \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} f(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}) \\ &= \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} d \\ * \\ \vdots \end{pmatrix} \\ &= \begin{pmatrix} a_1 d \\ \vdots \\ a_n d \end{pmatrix} \\ &= \mu_d(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}). \end{aligned}$$

□

Proposition 3.25. *If D, D' are division rings and $n, n' \in \mathbb{N}$ then $M_n(D) \cong M_{n'}(D')$ if and only if $n = n'$ and $D \cong D'$.*

Proof. Let $V' = (D')^n$. Using the previous lemma, we get that V and V' are simple R-modules, and that

$$V \oplus \cdots \oplus V \cong V' \oplus \cdots \oplus V'$$

as R-modules. The direct sum on the left-hand side gives a composition series of length n, while the direct sum on the right-hand side gives a composition series of length n'. Therefore $n = n'$.

Since R is simple and V, V' are simple R-modules, we get by Proposition 3.23 that V and V' are isomorphic R-modules. It follows that $\operatorname{End}_R V \cong \operatorname{End}_R V'$ and we get from Lemma 3.24 that $D \cong D'$. □

Chapter 4

The Jacobson radical

4.1 Definition and first properties

Definition 4.1. *The* **Jacobson radical** *of a ring R is the intersection of all maximal left ideals of R:*

$$\boldsymbol{J(R)} = \bigcap\{M \mid M \textit{ maximal left ideal of} R\}.$$

In the next few results we will see in particular that this definition is left-right symmetric, i.e., that $J(R)$ is also equal to the intersection of all the maximal right ideals of R.

We first observe that the definition makes sense:

Lemma 4.2. *Let R be a ring. Every left (resp. right, 2-sided) ideal of R is contained in a maximal left (resp. right, 2-sided) ideal of R. In particular, R contains at least one maximal left (resp. right, 2-sided) ideal.*

Proof. (For left ideals) Let I be a left ideal of R, and consider:

$$\begin{aligned} E &= \{J \mid J \text{ left ideal of } R,\ J \supseteq I,\ J \neq R\} \\ &= \{J \mid J \text{ left ideal of } R,\ J \supseteq I,\ 1 \notin J\}. \end{aligned}$$

E, with the order given by the inclusion, is a partially ordered set. Apply Zorn's lemma to find a maximal element of E. □

Definition 4.3. *Let M be an R-module, and let $B \subseteq M$. The (left)* **annihilator** *of B in R is:*

$$\operatorname{Ann}_R B = \{r \in R \mid rb = 0 \quad \forall b \in B\}.$$

This is a left ideal of R (easy exercise).

Proposition 4.4. *Let M be an R-module, and let N be a submodule of M. Then $\operatorname{Ann}_R N$ is a 2-sided ideal of R.*

Proof. We already know that it is a left ideal, so we only have to show that for every $a \in \operatorname{Ann}_R N$ and $r \in R$, $ar \in \operatorname{Ann}_R N$. Let $m \in N$. Then $(ar)m = a(rm) = 0$ since $rm \in N$ (N is a submodule) and $a \in \operatorname{Ann}_R N$. □

Lemma 4.5. *Let R be a ring. For $y \in R$ the following are equivalent:*

1. *$y \in J(R)$.*
2. *$1 - xy$ is left-invertible for every $x \in R$.*
3. *$y.M = \{0\}$ for every simple R-module M.*
4. *$y \in \bigcap\{\operatorname{Ann}_R M \mid M$ simple R-module$\}$.*

Proof. We first remark that 4 is simply a reformulation of 3:

$$3 \Leftrightarrow y \in \bigcap\{\operatorname{Ann}_R M \mid M \text{ simple } R\text{-module } \}.$$

We consider now the other equivalences.

$1 \Rightarrow 2$. Suppose $1 - xy$ is not left-invertible, for some $x \in R$. Define $I = R.(1 - xy)$. I is different from R since $1 \notin I$, and I is a left ideal. So $I \subseteq L$ for some L maximal left ideal of R.
We have $1 - xy \in I \subseteq L$, i.e., $1 - xy = \ell \in L$. But $y \in L$ by hypothesis, and then $xy \in L$. This implies $1 = \ell + xy \in L$, and then $L = R$, a contradiction.

$2 \Rightarrow 3$. Assume there exists a simple R-module M such that $yM \neq \{0\}$. In particular there exists $m \in M$ such that $ym \neq 0$.
Consider $R.(ym)$, the R-submodule generated by ym. It is nonzero since $ym \neq 0$. Since M is a simple R-module, we get $R.(ym) = M$.
In particular there exists $r \in R$ such that $rym = m$, which implies $(1 - ry)m = 0$. But $1 - ry$ is left-invertible by hypothesis, and if we multiply this equation on the left by its left-inverse, we have $m = 0$, a contradiction.

$3 \Rightarrow 1$. Let L be a maximal left ideal of R. R/L is an R-module (with product $R \times R/L \to R/L$, $(r, a + L) \mapsto ra + L$), which is simple (exercise: it is because L is a maximal left ideal of R, i.e., a maximal left submodule of the R-module R). By hypothesis we have $y.R/L = \{0\}$, and in particular $y(1 + L) = 0$, i.e., $y + L = 0$, which means $y \in L$. □

Corollary 4.6. *Let R be a ring. Then:*

$$J(R) = \bigcap\{\operatorname{Ann}_R M \mid M \textit{ simple } R\textit{-module}\}.$$

In particular $J(R)$ is a 2-sided ideal of R.

Lemma 4.7. *Let R be a ring, and let $y \in R$. The following are equivalent:*

1. $y \in J(R)$.

2. $\forall x, z \in R \quad 1 - xyz \in U(R)$.

Proof. *2.* $\Rightarrow$ *1.* By taking $z = 1$, we have *2.* from lemma 4.5, which means (by part *1.* of lemma 4.5) $y \in J(R)$.
1. $\Rightarrow$ *2.* Let $y \in J(R)$ and $x, z \in R$. Since $J(R)$ is an ideal, $yz \in J(R)$. So by lemma 4.5, $1 - xyz$ is left invertible, so there exists $u \in R$ such that $u(1 - xyz) = 1$ $(\star)$.
Since $J(R)$ is an ideal, $xyz \in J(R)$. By *2.* in lemma 4.5, $1 + u(xyz)$ is left-invertible.
But $(\star)$ gives $u(xyz) = u - 1$, so we have $1 + u(xyz) = u$ is left-invertible. This implies $u \in U(R)$ since u is also right invertible by $(\star)$. This suffices to show that $1 - xyz = u^{-1}$ and then belongs to $U(R)$ (since for an element of $U(R)$ the right and left inverses coincide, and are in $U(R)$). □

Remark. *From lemma 4.5 and 4.7 we have:*

$$\begin{array}{c} \forall x \in R \quad 1 - xy \textit{ is left invertible} \\ \Downarrow \\ \forall x, z \in R \quad 1 - xyz \textit{ is invertible,} \end{array}$$

which looks much stronger.

Corollary 4.8. *$J(R)$ is the intersection of all maximal right ideals of R.*

Proof. It relies on the fact that second condition in Lemma 4.7 does not involve left or right:

Let $J'(R)$ be the intersection of all maximal right ideals of R. We can re-write Lemma 4.5 for $J'(R)$ instead of R, and we will obtain that $y \in J'(R)$ if and only if for every $x, z \in R$ we have $1 - xyz \in U(R)$. □

Corollary 4.9. *$J(R)$ is the largest left ideal $I \subseteq R$ such that $1 + I \subseteq U(R)$. (In the sense that any such ideal is included in $J(R)$.)*

Proof. Let I be a left ideal such that $1 + I \subseteq U(R)$. Let $y \in I$ and $x \in R$. Since I is a left ideal, $-xy \in I$, and then, by hypothesis, $1 - xy \in U(R)$. Since this is true for every $x \in R$ we have $y \in J(R)$ by Lemma 4.5. This proves $I \subseteq J(R)$. □

Definition 4.10. *An element a of a ring R is* **nilpotent** *if $a^n = 0$ for some $n \in \mathbb{N}$.*
A left (reps. right, two-sided) ideal I of R is **nil** *if every element of I is nilpotent; I is* **nilpotent** *if $I^n = \{0\}$ for some $n \in \mathbb{N}$.*

An easy example of nilpotent element can be found in $M_2(\mathbb{R})$ with $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, because $a^2 = 0$.

Remark. *We have*

$$\begin{aligned} I^n &= I.I.\cdots.I \quad (n\ \textit{times}) \\ &= \{\sum_{i=1}^{m} a_{i,1}.\cdots.a_{i,n} \mid m \in \mathbb{N},\ a_{i,k} \in I\} \\ &\textit{(see definition page 11).} \end{aligned}$$

This gives:

$$\begin{aligned} I\ \textit{nilpotent} &\overset{def}{\Leftrightarrow} \exists n \in \mathbb{N} \quad I^n = \{0\} \\ &\Leftrightarrow \forall a_1, \cdots, a_n \in I \quad a_1.\cdots.a_n = 0 \\ &\Rightarrow \forall a \in I \quad a^n = 0. \end{aligned}$$

So I nilpotent implies I nil. (The converse is false! See exercise sheets.)

Theorem 4.11. *Let R be a ring and let I be a nil left ideal of R. Then $I \subseteq J(R)$.*

Proof. Let $a \in I$. a is nilpotent and there exits $n \in \mathbb{N}$ such that $a^n = 0$. Define $r = -a + a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1}$. Then:

$$\begin{aligned} r + a + ra &= a^2 - a^3 + \cdots + (-1)^{n-1}a^{n-1} - a^2 + a^3 + \cdots + (-1)^{n-2}a^{n-1} \\ &= 0. \end{aligned}$$

This implies $(1 + r)(1 + a) = 1 + r + a + ra = 1$. We also get in a similar way: $(1 + a)(1 + r) = 1$. We have proved $1 + a \in U(R)$ for every $a \in I$, i.e., $1 + I \subseteq U(R)$, and by corollary 4.9 we get $I \subseteq J(R)$. □

Proposition 4.12. *If R is a left Artinian ring (i.e., satisfies the descending chain condition on left ideals), then $J(R)$ is nilpotent.*

Proof. Let $J = J(R)$ and consider:

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots$$

It is a descending chain of left ideals, and since R is left Artinian, there exists $k \in \mathbb{N}$ such that $J^i = J^k$ for every $i \geq k$.
We prove that $J^k = \{0\}$ (which will give J nilpotent):
Suppose $J^k \neq \{0\}$. Then $J^{2k} = J^k \neq \{0\}$. Consider:

$$E = \{L \text{ left ideal of } R \mid J^k L \neq \{0\}\},$$

with the order given by the reversed inclusion (i.e., $L_1 \geq L_2$ if and only if $L_1 \subseteq L_2$). E is nonempty because $J^k \in E$. Using that R is left Artinian, we can verify that E satisfies the hypothesis of Zorn's lemma (see the proof of proposition 2.24), and by applying it we get a minimal element I_0 of E.
Since $I_0 \in E$, we have $J^k I_0 \neq \{0\}$ and there exists $a \in I_0$, $a \neq 0$, such that $J^k a \neq \{0\}$.

$J^k a$ is a left ideal of R and $J^k a \in E$ (since $J^k(J^k a) = J^{2k} a = J^k a \neq \{0\}$). But we also have $J^k a \subseteq I_0$ since $a \in I_0$ and I_0 is a left ideal. Since I_0 is minimal in E, this implies $J^k a = I_0$.
Using $a \in I_0$, we get $r \in J^k$ such that $ra = a$.

We have $r \in J^k \subseteq J$, so by lemmas 4.5 and 4.7, $1 - r \in U(R)$. Let $\alpha \in R$ be such that $\alpha(1-r) = 1$. We then have $\alpha(1-r)a = 1.a = a$, but we also have:

$$\begin{aligned}\alpha(1-r)a &= (\alpha - \alpha r)a\\ &= \alpha a - \alpha r a\\ &= \alpha a - \alpha a\\ &= 0.\end{aligned}$$

This gives $a = 0$, a contradiction. □

Corollary 4.13. *If R is a left Artinian ring then:*

1. *If I is a nil left ideal of R, then I is nilpotent.*
2. *$J(R)$ is the unique maximal nilpotent left ideal of R.*

Proof. It is an immediate consequence of theorem 4.11 and proposition 4.12. □

Remark. *Proposition 4.12 and corollary 4.13 apply in particular to finite rings, since a finite ring as necessarilly left Artinian.*

4.2 Links with semisimplicity

Theorem 4.14. *Let R be a ring. The following statements are equivalent:*

1. *R is semisimple.*
2. *R is left Artinian and $J(R) = \{0\}$.*
3. *R is left Artinian and has no nonzero nilpotent ideal.*

Proof. The equivalence of 2 and 3 follows at once from proposition 4.12 and corollary 4.13.
"1 $\Rightarrow$ 2" Assume R is semisimple. Then R is left Artinian by Corollary 3.18.

Consider now the left ideal $J(R)$. Since $J(R)$ is also an R-submodule of R, there is a submodule P of R such that $R = J(R) \oplus P$ as R-module. By exercise 3.8, there are idempotents $e, f \in R$ such that $e \in J(R)$, $f \in P$, $1 = e + f$, $J(R) = Re$ and $P = Rf$. Since $e \in J(R)$, by proposition 4.5, $f = 1 - e$ has a left inverse $u \in R$. Since f is an idempotent ($f^2 = f$) we obtain

$$1 = uf = uf^2 = (uf)f = f,$$

from which follows $e = 0$, and therefore $J(R) = J(R)e = \{0\}$.

"2 $\Rightarrow$ 1" We first show that if I is a minimal left ideal of R, then I is a direct summand of R:
Since $I \neq \{0\}$ we have $I \not\subseteq J(R)$. Since $J(R)$ is the intersection of all maximal left ideals of R, there is a maximal left ideal L of R not containing I.
Since I is minimal, it is a simple left R-module, so $I \cap L$ is either $\{0\}$ or I. Thesecond possibility means $I \subseteq L$, which is impossible. So $I \cap L = \{0\}$. The maximality of L gives $R = I + L$, and so we have $R = I \oplus L$.
We now use the Artinian property to repeat this process until we get the whole ring R:
Choose a minimal left ideal I_1 of R (it exists since R is Artinian, see proposition 2.24). As we just saw, $R = I_1 \oplus B_1$ for some left ideal B_1. In the same way, B_1 contains a minimal left ideal I_2 of R, and $B_1 = I_2 \oplus B_2$, where B_2 is a left ideal of R. It follows $R = I_1 \oplus I_2 \oplus B_2$.
We continue this process, which must stop at some point because R is left Artinian and the sequence of left ideals

$$B_1 \supsetneq B_2 \supsetneq \cdots$$

is strictly decreasing. Since the only way for this sequence to stop decreasing it for some B_k to be equal to $\{0\}$, we get $k \in \mathbb{N}$ such that $B_k = \{0\}$, which gives

$$R = I_1 \oplus I_2 \oplus \cdots \oplus I_k,$$

proving that R is semisimple. □

The Jacobson radical can be used to investigate properties of left Artinian rings: If R is left Artinian, then so is $R/J(R)$. But $J(R/J(R)) = \{0\}$ (see exercise sheets), so $R/J(R)$ is semisimple, which means that we have a good description of it. We can then use it to get results about R. The following three results are examples of this.

Proposition 4.15. *Let R be a left Artinian ring. Then a left R-module M is semisimple if and only if $J(R) \cdot M = \{0\}$.*

Proof. Let $J = J(R)$. By Corollary 4.6 we have $JS = \{0\}$ for every simple left R-module S, since $J \subseteq \operatorname{Ann}_R S$. It yields $JM = \{0\}$ for every semisimple left R-module M.

Conversely, assume $JM = \{0\}$. Then the product $R/J \times M \to M$, $(r + J, m) \mapsto rm$ is well-defined and defines a structure of R/J-module on M. Moreover the R/J-module M and the R-module M have the same submodules (easy verification).

Now R/J is still left Artinian (easy) and we have $J(R/J) = \{0\}$ (exercise). By theorem 4.14 we know that R/J is semisimple. In particular M is semisimple as R/J-module, i.e., every R/J-submodule of the R/J-module M is a direct summand. But it is easy to check that the R/J-submodules of M are exactly the R-submodules of M (look at the definition of the product by elements of R/J), so every R-submodule of the R-module M is a direct summand, i.e., M is semisimple. □

Theorem 4.16 (Hopkins-Levitzki)**.** *Let R be a left Artinian ring. Then for a R-module M the following properties are equivalent:*

1. *M is Noetherian.*

2. *M is Artinian.*

3. *M is of finite length.*

Proof. Step 1: If M is semisimple 1, 2 and 3 are all equivalent, since a Noetherian or Artinian module cannot be the direct sum of infinitely many simple submodules.

Step 2: Consider now the general case, and let $J = J(R)$. Since R is left Artinian, there is $n \in \mathbb{N}$ such that $J^n = \{0\}$ ($J(R)$ is nilpotent, see proposition 4.12). Let M be Noetherian (or Artinian). We have a descending sequence of submodules of M:

$$M \supseteq JM \supseteq \cdots \supseteq J^n M = \{0\}.$$

For every $i \in \{1, \ldots, n-1\}$, $J^i M$ is Noetherian (or Artinian) and therefore $J^i M/J^{i+1}M$ is also Noetherian (or Artinian). But $J \cdot (J^i M/J^{i+1}M) = 0$ so by proposition 4.15, the R-module $J^i M/J^{i+1}M$ is semisimple. Hence by Step 1 every $J^i M/J^{i+1}M$ has a composition series, and then M has a composition series. □

Corollary 4.17 (Hopkins)**.** *Every left Artinian ring is left Noetherian.*

Proof. Take $M = R$ in theorem 4.16. □

Appendix A

Products of rings

Let R and S be rings. We define the (direct) product of the rings R and S, denoted $R \times S$ as follows:

- $R \times S = \{(r, s) \mid r \in R,\ s \in S\}$ (so, as a set, $R \times S$ is simply the cartesian product of R and S);

- $0_{R\times S} = (0_R, 0_S)$ (we will simply write $0 = (0, 0)$);

- $1_{R\times S} = (1_R, 1_S)$ (we will simply write $1 = (1, 1)$);

- For all $r_1, r_2 \in R$ and $s_1, s_2 \in S$:

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2),$$

$$(r_1, r_2) \cdot (s_1, s_2) = (r_1 \cdot s_1, r_2 \cdot s_2).$$

It is quite easy to check that $R \times S$ is itself a ring.

More generally, if $\{R_i\}_{i\in I}$ is a collection of rings (which can be infinite), we define the product of the R_i to be

- $\prod_{i\in I} R_i = \{(r_i)_{i\in I} \times r_i \in R_i \text{ for every } i \in I\}$ (so, as a set, $\prod_{i\in I} R_i$ is simply the cartesian product of the R_i, $i \in I$);

- $0 = (0_{R_i})_{i\in I}$;

- $1 = (1_{R_i})_{i\in I}$;

- For all $(a_i)_{i\in I},\ (b_i)_{i\in I} \in \prod_{i\in I} R_i$:

$$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I},$$

$$(a_i)_{i\in I} \cdot (b_i)_{i\in I} = (a_i \cdot b_i)_{i\in I}.$$

Again, it is straightforward to check that $\prod_{i\in I} R_i$ is a ring.

Appendix B

Zorn's lemma

B.1 The axiom of choice

Let $\{A_i\}_{i\in I}$ be a family of non-empty sets (with I also non-empty). We would like to know if $\prod_{i\in I} A_i \neq \emptyset$.

The naive answer if to say that $\prod_{i\in I} A_i$ is obviously not empty:
Since $A_i \neq \emptyset$, it contains some element a_i. Then the element $(a_i)_{i\in I}$ belongs to $\prod_{i\in I} A_i$, which is therefore non-empty.

However, what this reasonning says is "we pick one element in each A_i", which leads to the following question: Can we really do it if I is infinite? Obviously we cannot do it "by hand" if I is infinite. So accepting that $\prod_{i\in I} A_i$ is not empty means accepting the existence of some procedure that chooses an element in each A_i, whithout necessarilly being able to describe it explicitely.

The axiom of choice: The product of a non-empty familly of non-empty sets is non-empty.

In this course, and in many other areas of mathematics, we will work under the hypothesis that the axiom of choice is true. (It is actually possible to make this choice. If you take a course on set theory, you will see that the axiom of choice is consistent with the usual axioms of set theory, i.e. that you can assume it holds. It means that it is possible to do mathematics under the hypothesis that the axiom of choice holds. Some people however prefer to avoid using it.)

There are several statements that are equivalent to the axiom of choice, in the sense that you can prove them out of the axiom of choice, and that you can prove the axiom of choice out of any of them. One of then is Zorn's lemma (see below), which we mostly use in this course to show the existence of maximal ideals in rings.

There are many other statements equivalent to the axiom of choice (for instance the fact that every vector space has a basis). While the axiom of choice itself and many of its equivalent statements seem natural enough, some others are really counter-intuitive, and justify why some people try to avoid using the axiom of choice.
Possibly the most famous example of such a counter-intuitive statement is the Banach-Tarski paradox: Using the axiom of choice, it is possible to decompose a ball in $\mathbb{R}^3$ of radius 1 into 5 different pieces, which can then be put back together by rotations and translations to give 2 balls of radius 1. The "trick" is that these pieces are so complicated that they don't have a "volume" (more precisely, if you are curious, they are nonmeasurable, cf. any course on measure theory or integration theory).

B.2 Zorn's lemma

Definition B.1. *A set X is called* **partially ordered** *if there is a relation $\leq$ on X such that, for every $a, b, c \in X$*

1. *$(a \leq b$ and $b \leq c) \to a \leq c$;*
2. *$(a \leq b$ and $b \leq a) \to a = b$.*

We also say that $\leq$ is a partial order on X.

X is **totally ordered** *if X is partially ordered by $\leq$ and, for every $a, b \in X$, $a \leq b$ or $b \leq a$.*
We also say that $\leq$ is a total order on X.

Example. 1. *The usual order $\leq$ on $\mathbb{R}$ or $\mathbb{Z}$ is a total order.*

2. *Let S be a non-empty set and let $X = P(S)$ the set of all subsets of S. Let $\leq$ be the inclusion, i.e. for $A, B \in X$ (which means A, B subsets of S) we define $A \leq B$ if and only if $A \subseteq B$.*
Then $\subseteq$ is a partial order on X:
$(A \subseteq B$ and $B \subseteq C) \Rightarrow A \subseteq C$;
$(A \subseteq B$ and $B \subseteq A) \Rightarrow A = B$.
It is not in general a total order, because we can have subsets A, B of S such that $A \nsubseteq B$ and $B \nsubseteq A$.

3. *More generally, any set of subsets is partially ordered by inclusion.*

4. *Similarly, we can consider on $X = P(S)$ the reverse inclusion, i.e. we define $A \leq B$ if and only if $B \subseteq A$. It is easy to check that the reverse inclusion is also a partial order on $P(S)$.*

5. *A graphic representation that also gives plenty of examples.*
   We represent the elements of X by dots, and put edges between them in such a way that

$$x \leq y \text{ if and only if}$$
$$\text{there is a path constantly going up from } x \text{ to } y.$$

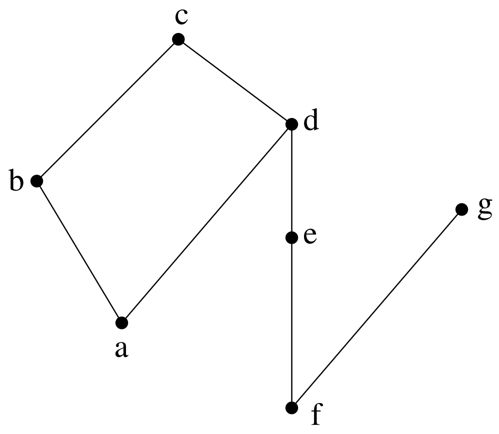


Figure B.1: A partial order on $\{a, b, c, d, e, f, g\}$

In this example we have $a \leq b$, $e \leq c$, $f \leq g\dots$
But $a \not\leq e$, $e \not\leq a$, $f \not\leq b\dots$

Definition B.2. *Let X be a partially ordered set and let $a \in X$.*

1. (a) *a is* **maximum** *(in X) if*

$$\forall x \in X \;\; x \leq a$$

(a is greater than or equal to every element of X).

   (b) *a is* **minimum** *(in X) if*

$$\forall x \in X \;\; a \leq x$$

(a is smaller than or equal to every element of X).

2. (a) *a is* **maximal** *(in X) if*

$$\forall x \in X \;\; x \geq a \Rightarrow x = a$$

(there is no element larger than a).

(b) a is **minimal** *(in X) if*

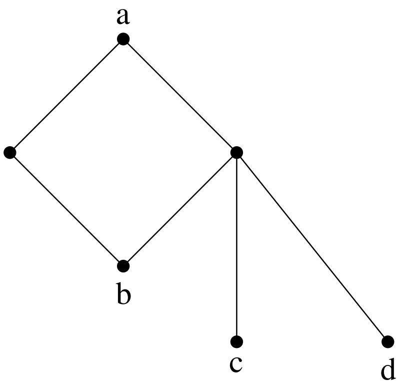
$$\forall x \in X \;\; x \leq a \Rightarrow x = a$$

(there is no element smaller than a).

Note that a maximum element is always maximal, and that a minimum element is always minimal.
If there is a maximum element, it is unique, and if there is a minimum element it is unique.

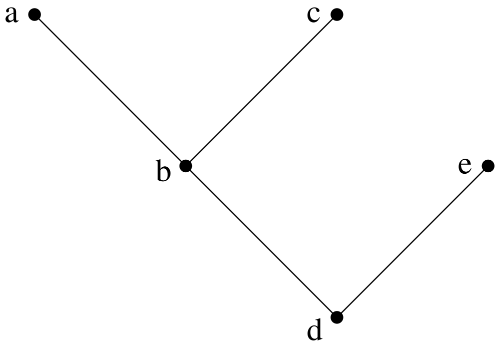
Example. *1. In figure B.1: c and g are maximal. a and f are minimal. There are no maximum or minimum elements.*

2. In the following figure



a is maximum, b, c and d are minimal. There are no minimum elements, and a is the unique maximal element.

In the figure



a, c and e are maximal, and there are no maximum elements. d is minimum (and minimal) and there are no other minimal elements.

Definition B.3. *Let X be a partially ordered set and let $C \subseteq X$. C is called a* **chain** *if C is totally ordered by the order from X. In other words:*

$$\forall a, b \in C \ a \leq b \text{ or } b \leq a.$$

Theorem B.4 (Zorn's lemma)**.** *Let X be a partially ordered set such that*

1. *X is not empty;*

2. *Whenever C is a chain in X, there is $a \in X$ such that $C \leq a$ (i.e. for every $x \in C$, $x \leq a$).*

Then X has at least one maximal element.

Remark. *It can also be used to prove the existence of minimal elements, because of the following observation:*
If X is partially ordered by $\leq$, then X is also partially ordered by $\leq'$, where:

$$a \leq' b \text{ if and only if } b \leq a.$$

B.2.1 Application: Every non-zero ring has a maximal (proper) left ideal

Let R be a ring, $R \neq \{0\}$. Recall that a left ideal I of R is called maximal if $I \neq R$ and for every left ideal J of R we have

$$I \subseteq J \Rightarrow (J = I \text{ or } J = R).$$

Let

$$X = \{J \subseteq R \mid J \text{ left ideal of } R, \ J \neq R\}.$$

Since X consists of subsets of R, it is partially ordered by inclusion. Observe that I is a maximal left ideal of R if and only if I is maximal in X for the partial order $\subseteq$.

Therefore, to prove the existence of a maximal ideal, we just need to check the hypotheses of Zorn's lemma.

1. To show that X is non-empty, we have to find an element of X, i.e. a proper left ideal of R. The simplest one is the ideal $\{0\}$.

2. Let C be a chain in X, i.e. $C = \{J_k\}_{k \in K}$ such that, for every $J_r, J_s \in C$, $J_r \subseteq J_s$ or $J_s \subseteq J_r$.
   Let $J' = \bigcup\{J_k \mid k \in K\}$. It is easy to check (exercise) that J' is a

left ideal of R. Moreover it is also a proper ideal of R (exercise again; hint: a left (or right, or 2-sided) ideal is proper if and only if it does not contain 1).

Since $J_r \subseteq J'$ for every $J_r \in C$, the second hypothesis of Zorn's lemma is satisfied.

You can show in the same way that every non-zero ring has a maximal right ideal, and a maximal 2-sided ideal.

The same kind of idea is used to show that every vector space has a basis, by showing that every vector space contains a maximal linearly independent subset, which is then a basis (Zorn's lemma is only required for vector spaces of infinite dimension). Actually the statement "every vector space has a basis" is equivalent to Zorn's lemma.

Appendix C

Maschke's theorem

Let F be a field. Let us go back for one second to $F[X]$ the ring of polynomials with indeterminate X. Its elements are of the form

$$\sum_{i\in\mathbb{N}} a_i X^i,$$

where the a_i are in F and only a finite number of them are non-zero. In other words, $F[X]$ is the F-vector space with a basis labelled by the elements X^i, for $i \in \mathbb{N}$.

It is turned into a ring by defining a product as follows

1. If $i, j \in \mathbb{N}$, then $X^i X^j = X^{i+j}$.

2. If $a \in F$ and $i \in \mathbb{N}$, then $X^i a = aX^i$.

3. The product is linear in each entry, so that

$$(\sum_{i\in\mathbb{N}} a_i \cdot X^i) \cdot (\sum_{j\in\mathbb{N}} b_j \cdot X^j) = \sum_{i,j\in\mathbb{N}} a_i b_j \cdot X^{i+j}.$$

We now do the same thing, but where we use the elements of a group as indeterminates:

Let F be a field and let G be a group (written multiplicatively, with identity element 1_G). We denote by $F[G]$ the vector space over F having a basis labelled by the elements of G. It means that an element of $F[G]$ has a unique expression in the form

$$\sum_{g\in G} a_g \cdot g,$$

where $a_g \in F$ and only a finite number of the coefficients a_g are non-zero. Equivalently, you can consider the elements of $F[G]$ as polynomials where the elements of G are used as the indeterminates.

The sum is defined in the natural way in both cases (and gives the same results), and $F[G]$, equipped with this sum, is an Abelian group.

We define a product on $F[G]$ in 3 steps:

1. If $g, h \in G$, then the product of g by h is $F[G]$ is the basis element / indeterminate gh (product computed in G).
2. If $a \in F$ and $g \in G$, then $ag = ga$.
3. The product in linear in each entry, so that
$$(\sum_{g\in G} a_g \cdot g) \cdot (\sum_{h\in G} b_h \cdot h) = \sum_{g,h\in G} a_g b_h \cdot (gh).$$

In other words: You compute the product as usual, using that the elements of F and G commute, and you "regroup" the part in F and the part in G. For instance:

$$\begin{aligned}(a_1g_1 + a_2g_2)(b_1h_1 + b_2h_2) = (a_1b_1)(g_1h_1) + (a_1b_2)(g_1h_2) + (a_2b_1)(g_2h_1) + \\ (a_2b_2)(g_2h_2).\end{aligned}$$

So: It is very similar to how you compute with polynomials.

Definition C.1. *With this sum and product, the set $F[G]$ is a ring with $1 = 1_F \cdot 1_G$. The ring $F[G]$ is called the* **group ring** *of G over F.*

Remark C.2. *Let R be a ring and let M be an R-module. Let N be a submodule of M and let $f : M \to N$ be a morphism of R-modules such that f is the identity on N (i.e., $f(x) = x$ for every $x \in N$). Then $M = N \oplus \ker f$.*

Indeed: If $m \in M$, then $m = f(x) + (x - f(x))$, and a direct computation shows that $x - f(x) \in \ker f$ (use that $f(f(x)) = f(x)$ since $f(x) \in N$). Furthermore, if $x \in N \cap \ker f$, then $f(x) = 0$ and also $f(x) = 0$, so $x = 0$.

Theorem C.3 (Maschke, 1898)**.** *Let F be a field and let G be a finite group. If $\operatorname{char} F$ does not divide $|G|$ then $F[G]$ is a semisimple ring.*

(Actually this implication is an equivalence, but we only prove one direction.)

Proof. We show that if V is an $F[G]$-module and V is an $F[G]$-submodule of V, then W is a direct summand in V. It will show that every $F[G]$-module is semisimple, i.e., that $F[G]$ is semisimple.

We first observe that since $F \subseteq F[G]$, V is also an F-vector space, and W is a subspace of V. Therefore, there is a subspace W' of V such that $V = W \oplus W'$ as F-vector spaces. Let $f : V \to W$ be the projection with kernel W'. It is an F-linear map and the restriction of f to W is the identity. We modify f to obtain a morphism of $F[G]$-modules as follows:

Define $\mu : V \to V$ by

$$\mu(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} f(gv),$$

for every $v \in V$. ($|G|$ is invertible in F by hypothesis.) Observe that $f(gv) \in W$. Since W is an $F[G]$-module we get $g^{-1}f(gv) \in W$ and $\frac{1}{|G|} g^{-1} f(gv) \in W$. Therefore μ is a map from V to W. Furthermore, if $v \in W$, we have

$$\mu(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} g v = v,$$

so that μ is the identity map on W.

Finally, μ is an $F[G]$-morphism: It is easy to check that $\mu(v + v') = \mu(v) + \mu(v')$ and that μ is F-linear. So we still have to check that for $h \in G$ and $v \in V$, $\mu(hv) = h\mu(v)$:

$$\begin{aligned}
\mu(hv) &= \frac{1}{|G|} \sum_{g \in G} g^{-1} f(ghv) \\
&= \frac{1}{|G|} \sum_{g' \in G} hg'^{-1} f(g'v) \\
&\quad \text{(where } g' = gh) \\
&= h\mu(v).
\end{aligned}$$

We can now use Remark C.2 to conclude. □

Using this result, what we learned about semisimpe rings can be used to study groups. This is part of Group Reprensentation Theory.

Remark C.4. *It is possible to show that if G is infinite, then $F[G]$ is never semisimple.*