1 Rings

1.1 Definition

Definition 1.1 (Ring)**.** *A ring is a triplet* $(R, +, \times)$*, where*

- R *is a set*
- $+$ *is a binary operation on* R *such that* $(R, +)$ *is an Abelian group.*
- $\times$ *is a binary operation on* R *that satisfies*
    1. $\times$ *is associative, i.e. for all* a, b, c *in* R*, we have*
    $$(a \times b) \times c = a \times (b \times c)$$
    2. $\times$ *distributes on* $+$*, i.e. for all* a, b, c *in* R *we have*
    $$a \times (b + c) = a \times b + a \times c, \quad (b + c) \times a = b \times a + c \times a.$$

Furthermore:

- We denote by 0 the neutral element for $+$.
- If the operation $\times$ is commutative, we say that R is a commutative ring.
- If the operation $\times$ admits a neutral element, we say that R has a unity. Although this is not, strictly speaking, part of our definition, all the rings that we will consider here have a unity - and in fact, in some books the existence of a unity is included in the definition of a ring.

As usual, with the definition of a structure comes the natural definition of the associated sub-structure.

Definition 1.2 (Subring)**.** *Let* $(R, +, \times)$ *be a ring, and* $R' \subset R$ *be a subset of* R*. We say that* R' *is a subring of* R *if* $(R', +, \times)$ *is a ring by itself.*

In practice, to prove that $R' \subset R$ is a subring of R, we check the following properties:

1. $(R', +)$ is a subgroup of $(R, +)$.
2. R' is stable (or "closed") by product, i.e. for all a, b in R', the product $a \times b$ is still in R'.

1.2 Some examples

- The "usual" examples: the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with the usual addition and multiplication are all commutative rings with a unity. In fact $\mathbb{Z}$ is a subring of $\mathbb{Q}$, who is a subring of $\mathbb{R}$, etc.
- The "functional examples": the set $\mathcal{F}$ of all functions from $\mathbb{R}$ to $\mathbb{R}$ can be endowed with a commutative ring structure. We define the sum and product of two functions as follows
$$\forall x \in \mathbb{R}, \quad (f + g)(x) := f(x) + g(x), \quad (f \times g)(x) := f(x) \times g(x).$$
Let us emphasize that when we write $(f+g)(x) := f(x)+g(x)$, the first symbol $+$ denotes the binary operation on $\mathcal{F}$, which is being defined in terms of the usual addition on $\mathbb{R}$, to which the second symbol $+$ corresponds. Inside the ring $\mathcal{F}$ we may find interesting subrings:

- The ring $C^0(\mathbb{R}, \mathbb{R})$ of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. It is a subring of $\mathcal{F}$ because the sum, difference and product of two continuous function is still continuous.
- For all $k \geq 1$, the ring $C^k(\mathbb{R}, \mathbb{R})$ of all functions from $\mathbb{R}$ to $\mathbb{R}$ which are of class C^k, i.e. k times differentiable, and whose k-th derivative is continuous. It is a subring of $\mathcal{F}$ because the sum, difference and product of functions of class C^k is still of class C^k.
- The ring $\mathbb{R}[X]$ of all polynomial functions with real coefficients. We may also look at $\mathbb{Q}[X]$ or $\mathbb{Z}[X]$, and check that $\mathbb{Z}[X]$ is a subring of $\mathbb{Q}[X]$, itself a subring of $\mathbb{R}[X]$.

- The "matrix examples". The set $M_{2,2}(\mathbb{R})$ of 2×2 matrices with real coefficients, with the matrix addition and multiplication, is a ring. Its unity is the identity matrix. Of course, this is **not** a commutative ring. An interesting subring is formed by the "upper triangular" matrices, i.e. the matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \quad a, b, c \in \mathbb{R}.$$

We could also consider the rings $M_{2,2}(\mathbb{Q})$ or $M_{2,2}(\mathbb{C})$, or even $M_{2,2}(\mathbb{Z})$.

1.3 Ring morphisms and ideals

Once the ring structure is defined, we have the usual definition of a ring morphism:

Definition 1.3 (Ring morphism and kernel)**.** *Let $(R, +_R, \times_R)$ and $(S, +_S, \times_S)$ be two rings, and $\varphi : R \to S$ be a map. We say that φ is a ring morphism when*

$$\forall a, b \in R, \quad \varphi(a +_R b) = \varphi(a) +_S \varphi(b), \quad \varphi(a \times_R b) = \varphi(a) \times_S \varphi(b).$$

In other words, φ respects the ring structures of R and S.

To a ring morphism $\varphi : R \to S$ is associated its kernel

$$\ker \varphi := \{a \in R, \varphi(a) = 0_S\}.$$

Remark 1.4. *A ring morphism from $(R, +_R, \times_R)$ to $(S, +_S, \times_S)$ is in particular a **group morphism** from $(R, +_R)$ to $(S, +_S)$. Its kernel in the sense of "ring morphism" as defined above and its kernel in the sense of "group morphism" as defined previously **are the same object**. In particular, we know that $\ker \varphi$ is a **subgroup** of $(R, +_R)$. It is not difficult to check that it is a **subring** of $(R, +_R, \times_R)$. In fact, we have more!*

Proposition 1.5. *Let $\varphi : R \to S$ be a ring morphism.*

- $\ker \varphi$ *is a subgroup of R.*
- $\ker \varphi$ *"absorbs elements through product": if a is in* $\ker \varphi$ *and b is in R, then $a \times b$ and $b \times a$ are both in* $\ker \varphi$.

Definition 1.6 (Ideal)**.** *Let R be a ring. A subset I of R is an ideal of R if I is a subgroup of R which satisfies:*

- *For all a in I, for all b in R, $a \times b$ is in I (right ideal).*

- *For all a in I, for all b in R, $b \times a$ is in I (left ideal).*
- *For all a in I, for all b in R, $a \times b$ and $b \times a$ are both in I (two-sided ideal).*

Of course, in a commutative ring, there is no distinction between left, right and two-sided ideals.

It follows immediately from Proposition 1.5 and the definition above that the kernel of a ring morphism is always a two-sided ideal.

Proposition 1.7.

1. *The sets $\{0\}$ and R itself are always ideals of R, although not very interesting ones.*
2. *If R has a unity, any ideal containing 1 is equal to R itself. (This is frequently used to prove that some ideal is equal to the whole ring).*

Proof. Proof of 2. if $1 \in I$, and I is e.g. a left ideal, then for all b in R we have $b \times 1 \in I$, but $b \times 1 = b$, so $b \in I$ and I contains all the elements of R. □

Example: evaluation morphisms and their kernel. Let $\mathcal{F}$ be, as above, the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. For any α in $\mathbb{R}$, we consider the map φ_α from $\mathcal{F}$ to $\mathbb{R}$ defined as follows

$$\forall f \in \mathcal{F}, \quad \varphi_\alpha(f) := f(\alpha).$$

Then φ_α is a ring morphism. Its kernel is given by

$$\ker \varphi_\alpha := \{f \in \mathcal{F},\ f(\alpha) = 0\},$$

which is the set of all functions vanishing at α. It is an ideal of $\mathcal{F}$.

1.4 More about ideals

Definition 1.8 (Principal ideals)**.** *Let R be a commutative ring and x be an element of X. The ideal generated by x is defined as the set $\{x \times a, a \in R\}$, and denoted by (x) (or $\langle x \rangle$, depending on the convention).*

Exercise: check that this is indeed an ideal. Of course, if R is not commutative, one should define three notions: left ideal generated by x (sometimes denoted by Rx), right ideal generated by x (sometimes denoted by xR, and two-sided ideal generated by x (sometimes denoted by RxR.

- For any $n \geq 1$, the set $n\mathbb{Z}$ of all multiples of $\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
- In $\mathbb{R}[X]$, for all $k \geq 1$ the set (X^k) of all polynomials which have no coefficient of order $0, 1, 2, \ldots k-1$ is an ideal of $\mathbb{R}[X]$.

Definition 1.9 (Principal ideal)**.** *If an ideal I is of the form (x) for some x in R, we say that I is a principal ideal*

The ideal $6\mathbb{Z}$ is principal. However:

- It is strictly contained in the ideals $2\mathbb{Z}$ and $3\mathbb{Z}$.
- We have $3 \times 2 = 6 \in 6\mathbb{Z}$ even though $2 \notin 6\mathbb{Z}$ and $3 \notin 6\mathbb{Z}$.

To address these two situations, we introduce two definitions.

Definition 1.10. *Let R be a commutative ring and I be an ideal of R.*

I is said to be a maximal ideal if, for any ideal I' such that $I \subset I'$, we have $I' = I$ or $I' = R$.

I is said to be a prime ideal if, for any a, b in R such that $a \times b \in I$, we must have $a \in I$ or $b \in I$.

For example, $6\mathbb{Z}$ is not maximal because $6\mathbb{Z} \subset 2\mathbb{Z}$ and yet $2\mathbb{Z} \neq 6\mathbb{Z}$ and $2\mathbb{Z} \neq \mathbb{Z}$. It is not prime neither, because $2 \times 3 \in 6\mathbb{Z}$ and yet $2 \notin 6\mathbb{Z}$ and $3 \notin 6\mathbb{Z}$.

1.5 Two constructions

1.5.1 Direct product of rings

Let $(R, +_R, \times_R)$ and $(S, +_S, \times_S)$ be two rings. The Cartesian product $R \times S$ can be endowed with a ring structure $(R \times S, +, \times)$ named the *product ring* and defined as follows: for a, a' in R and b, b' in S, we let

$$(a, b) + (a', b') := (a +_R a', b +_S b'), \quad (a, b) \times (a', b') := (a \times_R a', b \times_S b').$$

The ring $R \times S$ is commutative if and only if both R and S are commutative (proof: exercise).

R and S are both "included" in $R \times S$ as follows: the maps $i_1 : R \to R \times S$ and $i_2 : S \to R \times S$ defined by

$$i_1(a) := (a, 0), \quad i_2(b) := (0, b),$$

are injective ring morphisms.

Conversely, $R \times S$ can be "projected down" onto R or S as follows: the maps $\pi_1 := R \times S \to R$ and $\pi_2 : R \times S \to S$ defined by

$$\pi_1(a, b) := a, \quad \pi_2(a, b) := b,$$

are surjective ring morphisms.

Lemma 1.11. *If R, S are two rings, I is an ideal of R and J is an ideal of S, then $I \times J$ is an ideal of $R \times S$.*

Proof. Exercise. □

1.5.2 Quotient ring

Let $(R, +_R, \times_R)$ be a commutative ring, and I be an ideal of R. In particular, I is a subgroup of R, and it is even a *normal* subgroup of R since $(R, +)$ is always, by definition, an Abelian group. So we can consider the quotient group $(R/I, \overline{+})$.

Question: can R/I be endowed with a ring structure?

Yes! Let $\overline{a}, \overline{b}$ be two elements of R/I, i.e. two equivalence classes for the relation "equal modulo an element of I" on R. We want to define $\overline{a}\overline{\times}\overline{b}$, the natural guess is to let

$$\overline{a}\overline{\times}\overline{b} := \overline{a \times_R b},$$

in other words we define $\overline{a}\overline{\times}\overline{b}$ as the equivalence class of $a \times_R b$ in R.

Question: is this well-defined?

Yes! But as for the quotient group construction, we need to check that the definition above does **not** depend on the choice of a, b among their equivalence class. In order to do that, let

a', b' be such that $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$. By definition of the relation "equal modulo an element of I", it means that there exist i and j in I such that

$$a' = a + i, \quad b' = b + j.$$

Now, let us compute (using the fact that product distributes on sum!)

$$a' \times_R b' = (a + i) \times_R (b + j) = a \times_R b + i \times_R b + a \times_R j + i \times_R j.$$

The last three terms in the right-hand side all belong to I because I is an ideal and i, j are in I. So $a' \times_R b'$ is equal to $a \times_R b$ plus an element of I, which means that they are equivalent modulo I, and have the same equivalence class in R/I, so indeed

$$\overline{a' \times_R b'} = \overline{a \times_R b},$$

and the product operation on R/I is well-defined.

We call $(R/I, \overline{+}, \overline{\times})$ the *quotient ring* of R by the ideal I.

2 The ring $\mathbb{Z}$

2.1 $\mathbb{Z}$ as a principal ring

Theorem 1 (Ideals of $\mathbb{Z}$)**.** *Every ideal of $\mathbb{Z}$ is principal, i.e. of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.*

Proof. An ideal of $\mathbb{Z}$ is, in particular, a subgroup of $\mathbb{Z}$, but $\mathbb{Z}$ is cyclic, and we know that all subgroups of a cyclic group is cyclic. So there exists n in $\mathbb{Z}$ such that $I = \langle n \rangle$ (as a subgroup). It is easy to check that $\langle n \rangle = n\mathbb{Z}$ and that $n\mathbb{Z}$ is indeed an ideal.

As a reminder, review the proof that "every subgroup of a cyclic group is cyclic": we introduce n as

$$n := \min \{k \in I, k > 0\},$$

and show that every element of I is a multiple of n, using Euclidean division. □

Proposition 2.1. *Let $n \geq 1$. The following statements are equivalent:*

1. *The ideal $n\mathbb{Z}$ is a maximal ideal.*
2. *The ideal $n\mathbb{Z}$ is a prime ideal.*
3. *n is a prime number.*

Proof. We show

- 2. $\iff$ 3. If n is a prime number, and if $pq \in n\mathbb{Z}$, it means that n divides pq, so n must divide p or q (Gauss's lemma), so $n\mathbb{Z}$ is a prime ideal.
  Conversely, if n is not a prime number and can be written as $n = pq$ for $1 < p, q < n$, then $pq \in n\mathbb{Z}$ and yet $p \notin n\mathbb{Z}$, $q \notin n\mathbb{Z}$ so the ideal $n\mathbb{Z}$ is not prime.
- 1. $\iff$ 3. If n is a prime number, and if $n\mathbb{Z}$ is included in some ideal I, since $\mathbb{Z}$ is principal we know that I is of the form $m\mathbb{Z}$ for some m, but then $n \in n\mathbb{Z} \subset m\mathbb{Z}$ so m divides n, which means $m = 1$ or $m = n$, and thus $m\mathbb{Z} = \mathbb{Z}$ or $m\mathbb{Z} = n\mathbb{Z}$. So indeed $n\mathbb{Z}$ is a maximal ideal.
  Conversely, if n is not a prime number, there exists a number m with $1 < m < n$ which divides m, and thus $n\mathbb{Z} \subset m\mathbb{Z}$, so $n\mathbb{Z}$ is not a maximal ideal.

□

Question: What is the quotient ring $\mathbb{Z}/n\mathbb{Z}$? Nothing but $\mathbb{Z}_n$.

Ideals of $\mathbb{Z} \times \mathbb{Z}$ Let us consider the direct product of $\mathbb{Z}$ by itself, i.e. the ring $\mathbb{Z} \times \mathbb{Z}$. We know a family of ideals of $\mathbb{Z} \times \mathbb{Z}$: all the ideals of the form $n\mathbb{Z} \times m\mathbb{Z}$ for n, m in $\mathbb{Z}$. **Question:** are there more ideals?
No! Let K be an ideal of $\mathbb{Z} \times \mathbb{Z}$. Its respective images by the projections π_1 and π_2 are subgroups (in fact, ideals) of $\mathbb{Z}$, and are thus of the form $m\mathbb{Z}$ and $n\mathbb{Z}$, thus $K \subset m\mathbb{Z} \times n\mathbb{Z}$. Moreover, K contains an element of the form (m, x) for some x and of the form (y, n) for some y. Multiplying the first by $(1, 0)$ and the second by $(0, 1)$, we see that $(m, 0)$ and $(0, n)$ belong to K, and thus K contains $m\mathbb{Z} \times n\mathbb{Z}$. So $K = m\mathbb{Z} \times n\mathbb{Z}$.

3 Rings of functions

Let us start with the following question: what are the ideals of $\mathbb{R}$?

Proposition 3.1. *All the ideals of* $\mathbb{R}$ *are trivial, i.e. are equal to* $\{0\}$ *or* $\mathbb{R}$ *itself.*

Proof. Let I be an ideal of $\mathbb{R}$, and assume that I is not $\{0\}$. Then I contains some $x \neq 0$. Since I is an ideal, it also contains $x \times \frac{1}{x} = 1$. We know that any ideal that contains the unity is the ring itself. □

This is not specific to $\mathbb{R}$, in fact this is true in every *field* (see later).

Now, let us ask: what are the ideals of $\mathbb{R} \times \mathbb{R}$? Or $\mathbb{R}^N$? We recall that $\mathbb{R} \times \mathbb{R}$ has the structure of a product ring, where

$$(x, y) + (x', y') := (x + x', y + y'), \quad (x, y) \times (x', y') := (x \times x', y \times y').$$

Let K be an ideal of $\mathbb{R} \times \mathbb{R}$. Let I be the image of K by the first projection $\pi_1(x, y) := x$ and let J be the image of K by the second projection $\pi_2(x, y) := y$.

1. I, J are ideals of $\mathbb{R}$, thus they are equal to $\{0\}$ or $\mathbb{R}$. Moreover we have $K \subset I \times J$.
2. Conversely, let (a, b) be in $I \times J$. By definition, a is in the image of π_1, so there exists b' such that (a, b') is in K. But then $(a, 0) = (a, b') \times (1, 0)$ is also in K Similarly, $(0, b)$ is in K. Then $(a, b) = (a, 0) + (0, b)$ is in K. This shows $I \times J \subset K$.

So the ideals of $\mathbb{R} \times \mathbb{R}$ are $\{0\} \times \{0\}$, $\{0\} \times \mathbb{R}$, $\mathbb{R} \times \{0\}$ and $\mathbb{R} \times \mathbb{R}$. **Question:** which one are prime? maximal?

Proposition 3.2. *Let* $N \geq 2$. *The ideals of* $\mathbb{R}^N$ *are of the form* $I_1 \times \cdots \times I_N$ *where* I_k *is either* $\{0\}$ *or* $\mathbb{R}$. *Which one are prime? Maximal? Show that all of them are principal.*

Proof. Homework. □

Now, let S (S as "sequence") be the set of all sequences of real numbers $(u_n)_{n \geq 1}$. We endow it with a commutative ring structure by defining

$$(u + v)_n := u_n + v_n, \quad (u \times v)_n := u_n \times v_n.$$

There is a unity: the sequence constant equal to 1. **Question:** what are the ideals of S?

Claim 1. *Let* I *be an ideal of* S. *If* I *contains a sequence that never vanishes, then* I *is equal to* S *itself.*

Proof. If $u = (u_n)_{n \geq 0}$ is a sequence such that $\forall n, u_n \neq 0$, then the sequence v defined by $v_n = \frac{1}{u_n}$ satisfies $u \times v = 1_S$, so I contains the unity and is thus equal to S itself. □

Thus every sequence in a non-trivial ideal of S must be equal to zero at least once.

Proposition 3.3. *Let Z be a non-empty subset of $\mathbb{N}$. The set $S_0(Z)$ of all sequences u such that*

$$\forall n \in Z, u_n = 0$$

form an ideal of S. It is the principal ideal generated by the sequence v defined by

$$v_n = 0 \text{ if } n \in Z, \quad v_n = 1 \text{ if } n \notin Z.$$

Moreover

$$S_0(Z) \text{ is prime} \iff S_0(Z) \text{ is maximal} \iff Z \text{ is a singleton.}$$

We could hope that all ideals of S are of the form $S_0(Z)$ for some non-empty subset Z, and S would be principal. Unfortunately, here is a counter-example:

Proposition 3.4. *The set J of all sequences that have only finitely many terms not equal to zero is an ideal of J. It is not of the form $S_0(Z)$ for any Z. It is not prime.*

Proof. The fact that J is not prime can be checked with a example: the sequences u, v defined by $u_n = 0$, $v_n = 1$ if n is odd and $u_n = 1$, $v_n = 0$ if n is even, are not elements of J but $u_n \times v_n$ is always 0 and thus $u \times v$ is in J. □

Remark 3.5. *Is the subset "sequences with infinitely many 0 terms" an ideal of S? What about the subset "infinitely many terms not equal to 0"?*

Lemma 3.6 (Bezout's identity)**.** *If R is a commutative ring with unity, if I is a maximal ideal and $p \notin I$, then there exists α in R, i in I such that $\alpha \times p + i = 1$.*

Proof. Let I be a maximal ideal and p be an element of R that does not belong to I. Let $I + (p)$ be the set

$$I + (p) := \{i + \alpha \times p, \, i \in I, \alpha in R\}.$$

Check that this is an ideal, that contains I and is not equal to I. Since I is maximal, this must be R, so it must contain 1, so there exists $i \in I, \alpha in R$ such that $i + \alpha \times p = 1$. □

Lemma 3.7. *If R is a commutative ring with unity, every maximal ideal is prime.*

Proof. Let I be a maximal ideal (not equal to R otherwise there is nothing to prove), let p, q be two elements such that $p \times q \in I$. Assume, by contradiction, that $p \notin I$ and $q \notin I$. Then by the previous result, we know that there exists α, β in R and i, j in I such that

$$\alpha p + i = 1, \quad \beta q + j = 1.$$

But then $(\alpha p + i)(\beta q + j) = 1 = \alpha\beta pq + i\beta q + j\alpha p + ij$, which is a sum of terms in I. Thus $1 \in I$, and I is equal to R, contradiction. □

Questions: What do the quotient rings look like?

4 Rings of matrices

For $n \geq 2$, we let $M_{n,n}(\mathbb{R})$ be the ring of $n \times n$ matrices with real coefficients.

Remark 4.1. *$M_{n,n}$ is **not** commutative.*
Start with $n = 2$, then, for e.g.

$$A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix},$$

we have

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, \quad BA = \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix},$$

and thus $AB \neq BA$.

How to generalize for $n \geq 2$? We find construct an example by hand. Or we can rely on the following "abstract" result:

Lemma 4.2. *For $m \geq n$, the map $\phi : M_{n,n}(\mathbb{R}) \to M_{m,m}(\mathbb{R})$ defined by*

$$\phi(A) := \begin{pmatrix} A & 0_{n,m-n} \\ 0_{m-n,n} & 0_{\mathrm{m-n}} \end{pmatrix},$$

(using block-matrix notation) is a one-to-one ring morphism.
In particular: $M_{n,n}(\mathbb{R})$ is isomorphic to a subring of $M_{m,m}(\mathbb{R})$.

Proof. Exercise. The fact that if there is a one-to-one morphism from R to S, then R is isomorphic to a subring of S (the range of ϕ) was already mentioned in the case of groups. $\square$

In particular, since $M_{2,2}(\mathbb{R})$ is not commutative, then $M_{m,m}(\mathbb{R})$ is not commutative for $m \geq 2$ (why?).

Since we are not dealing with commutative rings R, one has to distinguish between

- Left-ideal I : $\forall a \in I, \forall b \in R, b \times a \in I$
- Right-ideal I : $\forall a \in I, \forall b \in R, a \times b \in I$
- Two-sided ideal: both left and right.

How to find ideals? We still have *principal* ideals, but now of different types. Fix a in R.

- The left-ideal generated by a is $Ra := \{ra, r \in R\}$ (notation Ra with R on the **left**)
- The right-ideal generated by a is $aR := \{ar, r \in R\}$ (notation aR with R on the **right**)

Question, is the subset

$$\{ras, r \in R, s \in R\}$$

a two-sided ideal? Answer: it clearly "absorbs" elements on the left/right but is not clear that it is a subgroup!! To generate a two-sided ideal from a, we need to consider finite linear combinations of elements of the type ras, so in fact we define

$$RaR := \{r_1 a s_1 + \cdots + r_n a s_n, n \geq 1, r_1, \ldots, r_n \in R, s_1, \ldots, s_n \in R\}.$$

Fact: Ra is a left-ideal, aR is a right-ideal, RaR is a two-sided ideal. Proof: exercise.
Question: who are the ideals of the ring $M_{2,2}(\mathbb{R})$?

Remark 4.3. *If I is an ideal (left, right, two-sided) of $M_{2,2}(\mathbb{R})$, then either I is trivial or it contains only **non-invertible** matrices?*

Proof. Same reason than for functions: if A is invertible and in I, then $A \times A^{-1}$ is in I (or $A^{-1} \times A$ if I is a left-ideal) and then the identity is in I and I contains all the matrices. $\square$

The two-sided ideals

Lemma 4.4. *The only two-sided ideals of $M_{2,2}(\mathbb{R})$ are trivial.*

Proof. Let I be a two-sided ideal, and assume it is not trivial, so it contains a matrix A of rank 1 (it cannot contain a matrix of rank 2 because this would be invertible, see above). We now from linear algebra that there exists P, Q (invertible, but here it does not matter) such that

$$PAQ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

and clearly we can also find P', Q' such that

$$P'AQ' = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

since I is a two-sided ideal we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I,$$

and so their sum is in I but this is the identity matrix, so I is trivial. $\square$

Remark 4.5. *We have previously seen an example where all the two-sided ideals where trivial: the case of $\mathbb{R}$ (because it is a "field"). Here we have another example, which is **not** a "field". We say the ring is "simple" (compare to "simple groups" = all normal subgroups are trivial).*

Question: What about left ideals?

Lemma 4.6. *Let I be a non trivial left-ideal of $M_{2,2}(\mathbb{R})$. For any A_1, A_2 in I, we must have*

$$\ker A_1 \cap \ker A_2 \neq \{0\}.$$

Proof. Since I is not trivial, A_1, A_2 have rank at most 1. Assume they both have rank 1 (otherwise there is nothing to prove), but $\ker A_1 \cap \ker A_2 = \{0\}$.

Let u, v such that $\ker A_1 = \mathbb{R}u, \ker A_2 = \mathbb{R}v$, and by assumption u, v are not colinear, hence they form a basis. We have

$$A_1 u = 0, A_1 v = \alpha u + \beta v, \quad A_2 u = \gamma u + \delta v, A_2 v = 0.$$

- If $\beta = 0$, but $\alpha \neq 0$ multiply A_1 on the left by the matrix C such that

$$Cu = \frac{1}{\alpha} v, Cv = 0,$$

then CA_1 sends u to 0 and v to v

- If $\beta \neq 0$, multiply A_1 on the left by the matrix C such that

$$Cu = 0, Cv = \frac{1}{\beta} v,$$

then CA_1 sends u to 0 and v to v.
- Idem for A_2.

Since I is a left-ideal, we obtain that (written in a certain basis)

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I,$$

so the identity is in I, hence I is trivial. □

Proposition 4.7. *If I is a non-trivial left-ideal of $M_{2,2}(\mathbb{R})$, then*

$$\bigcap_{M \in I} \ker M$$

is a subspace F of dimension 1, and I is the left-ideal of matrices whose kernel contains F.

Proof. It follows from the previous lemma. Why? □

Remark 4.8. *This is a principal ideal. Can you find a generator? Complete F into a basis of $\mathbb{R}^2$ (by adding a vector) and consider the matrix written*

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

in this basis. Then any matrix in the ideal can be written as

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Exercise: extend the result to $n \geq 3$, and to right-ideals.

5 Polynomials

Definition 5.1. *If R is a ring, we define the ring of polynomials with coefficients in R, denoted by $R[X]$, as the set of all sequences of elements of R that are eventually equal to 0, so*

$$R[X] := \{P = \{a_k\}_{k \geq 0},\ a_k \in R \forall k\, a_k = 0 \text{ for } k \text{ large enough}\}.$$

We define the degree of P as

$$\deg(P) := \max\{k, a_k \neq 0\}.$$

Given a sequence of coefficients $\{a_k\}_{k\geq 0}$, we usually write

$$P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_k X^k + \ldots a_{\deg(P)} X^{\deg(P)} = \sum_{k=0}^{\deg(P)} a_k X^k.$$

We define two operations $+$ and $\times$ on $R[X]$, cf. Textbook section 17.1. If R is a commutative ring with unity, then so is $R[X]$. In the sequel, we will focus on $\mathbb{C}[X]$, polynomials with coefficients in $\mathbb{C}$.

Ideals? Let us consider the "evaluation morphisms": fix z in $\mathbb{C}$ and define $\Phi_z : \mathbb{C}[X] \to \mathbb{C}$ by

$$\Phi_z(P) := P(z).$$

Its kernel is the set of all polynomials vanishing at z, it is an ideal of $\mathbb{C}[X]$. More ideals?

Lemma 5.2. *Let R, S_1, S_2 be three rings, let φ_1 be a ring morphism from R to S_1 and φ_2 be a ring morphism from R to S_2. Then the map (φ_1, φ_2) defined by*

$$r \mapsto (\varphi_1, \varphi_2)(r) := (\varphi_1(r), \varphi_2(r))$$

is a ring morphism from R to $S_1 \times S_2$ and its kernel is the intersection $\ker \varphi_1 \cap \ker \varphi_2$.