2. Number systems

We have considered systems of linear equations with coefficients in several different systems of numbers: the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$, the integers $\mathbb{Z}$, and the strange system $\mathbb{Z}/26\mathbb{Z}$. We have seen that linear algebra works identically for the first three, but doesn't seem to work for the last two.

In this section we consider what we need to formulate a linear equation. That is, let R be a set, and let $a_1, \dots a_k \in R$ and $b \in R$. We wish to understand what we need to formulate the following question: Solve

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = b$$

when $x_1, \dots, x_k$ are variable which can only take on values as elements of R.

First, we need a way to multiply elements of R: if x_i is some element in R and a_i is some element in R then we need to form the product a_ix_i. We also need to be able to add the results of these products, so we need to be able to add the elements of R as well.

To add two elements means taking two elements and spitting out a third: thus we model addition by a function $+ : R \times R \longrightarrow R$. For example, if $N = 1, 2, 3, 4, 5, 6, \dots$ is the set of natural numbers, adding 2 and 3 to get 5 is evaluating $+(2, 3) = 5$. However, this notation is unfamiliar, so we will follow the usual convention in mathematics and write $2+3$ instead of $+(2, 3)$[4]. Nevertheless, not every function of two arguments defines an "addition".

In elementary school, addition is typically described by a particular algorithm used to computing sums. However, this algorithm isn't the same as for rational numbers or numbers in $\mathbb{Z}/26\mathbb{Z}$, and thus isn't a good foundation for thinking about addition in other number systems. Instead, we split the discussion into two parts: the properties that the function must satisfy to encode "addition" and the particular form of addition for a particular set of numbers – usually an algorithm for computing the sums. Focusing on the former allows us to prove results that apply to any reasonable system of numbers.

To find the properties that addition should satisfy, we look at the properties of addition in the natural numbers: we know $2 + 3 = 3 + 2$ – and similarly for any two natural numbers – so one property we might require our function to satisfy is $+(x, y) = +(y, x)$ for all x and y in R. That is, we might require our addition to be *commutative*.

Moreover, at this stage, expressions such as $2+3+4$ are undefined since we can't evaluate $+(2, 3, 4)$: we only have $+$ defined as a function of *two* arguments. To find $2 + 3 + 4$ by only adding two numbers at a time, we could compute $(2 + 3) + 4$ or $2 + (3 + 4)$. Depending on our choice of function for $+$, these computations could give different answers. We have no reason to prefer one to the other, however. Of course, in the natural numbers, it doesn't matter which we choose, so we require this of our additions as well. That is, for all x, y, z we must have $(x + y) + z = x + (y + z)$, a property called *associativity*. This takes care of three element sums, but what about more? It turns that commutativity and associativity imply that we get the same result when adding a sequence of

[4]In CS terminology, we will use $+$ as an infix operator rather than a prefix operator

numbers, no matter how we add them. For example,

(Question 2.1) Assuming the $+\colon R\times R \longrightarrow R$ is associative and commutative, and x, y, z, w are all in the domain of $+$, show that the following are all equal

$$x + (y + (z + w)) \qquad (y + x) + (w + z) \qquad (w + (y + x)) + z$$

However, in doing row operations, we also need to subtract. This isn't always possible in the natural numbers, so we switch our model to the addition on the integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. Thus, we will also ask for an *additive identity* element 0, one such that $0 + x = x$ for all x, and that for each x there is an *additive inverse* x^* such that $x + x^* = 0$. Subtracting by x is then implemented as adding x^*.

(Question 2.2) Assuming that $+\colon R\times R \longrightarrow R$ is commutative, why do we not also need to require $x^* + x = 0$ and $x + 0 = x$?

Assume that $+\colon R\times R \longrightarrow R$ is defined on a set R and that this addition is associative, commutative, has an additive identity, and every element has an additive inverse. Write out *step-by-step* proofs of the following, citing the property you use in each step:

(Question 2.3) Show that the additive identity is unique: that is, if $a + x = x$ for all x then $a = 0$. (Hint: must also be true for $x = 0$)

(Question 2.4) Show that the additive inverse for x is unique: that is, if $a + x = 0$ then $a = x^*$.

(Question 2.5) Show that if $x + y = z + y$ then $x = z$ (*Hint:* How do we implement subtraction again? But be careful about associativity!)

(Question 2.6) Show that $(x + y)^* = x^* + y^*$. (*Hint:* Show that $(x + y) + (x^* + y^*) = 0$. Why is this enough?

For linear equations, we also want to be need to multiply numbers elements of R. This again is a function $\cdot\colon R\times R \longrightarrow R$ which, to be multiplication, should satisfy some properties. These properties we can lifted from the integers:

(1) $\cdot$ is *commutative* if for all $x, y \in R$, $x \cdot y = y \cdot x$
(2) $\cdot$ is *associative* if for all $x, y, z \in R$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(3) there is a *multiplicative identity* $1 \in R$ if $1 \cdot x = x \cdot 1 = x$ for all $x \in R$

Just as for addition, associativity implies that the product $r_1 r_2 \cdots r_k$ can be computed by taking repeated products of adjacent factors in any order: $(r_1 r_2)(r_3 r_4) = ((r_1 r_2) r_3) r_4$ for example. If $\cdot$ is also commutative, then we can change the order of the factors as well. Similarly, the multiplicative identity is unique.

When we have both an addition and a multiplcation, as in the integers, we also need properties that express how the two operations interact (or else they are independent of each other). In the integers this is done through the distributive property: for all $x, y, z \in R$

$$x \cdot (y + z) = x \cdot y + z \cdot z$$

We give a name to a set with a multiplication and addition with the same properties as in the integers:

Definition 4. *A* commutative ring *is a tuple* $(R, +, \cdot, 1, 0)$ *where* R *is a set,* $0, 1 \in R$*, and* $+ : R \times R \longrightarrow R$*,* $\cdot : R \times R \longrightarrow R$ *are two functions, called addition and multiplication respectively, which satisfy*

- R1. (Associativity of addition and multiplication) $(x+y)+z = x+(y+z)$ *and* $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *for all* $x, y, z \in R$*.*
- R2. (Commutativity of addition and multiplication) $x + y = y + x$ *and* $x \cdot y = y \cdot x$ *for all* $x, y \in R$*.*
- R3. (Additive identity) $0 + x = x$ *for all* $x \in R$*.*
- R4. (Additive inverse) *For each* $x \in R$ *there is a element* $y \in R$ *such that* $x + y = 0$*.*
- R5. (Multiplicative identity) $1 \cdot x = x \cdot 1 = x$ *for all* $x \in R$*.*
- R6. (Distributive) $x \cdot (y + z) = x \cdot y + z \cdot z$ *for all* $x, y, z \in R$*.*

bf Note: This definition is overly restrictive. In particular, there are interesting structures which satisfy almost all of properties $R1 - R6$ above with the exception that multiplication may not be commutative.

Definition 5. *A* non-commutative ring *is a tuple* $(R, +, \cdot, 0)$ *satisfying properties* $R1 - R6$ *above with the exception that multiplication may not be commutative. That is, there can exist* $x, y \in R$ *such that* $x \cdot y \neq y \cdot x$*.*

Linear algebra provides one of the most important examples of a non-commutative ring, but this will be the only one we consider.

Note that the natural numbers with their usual arithmetic, which we denote by $\mathbb{N}$, are not a ring (it satisfies $R1, R2, R5$ and $R7$ though). However, both the integers $\mathbb{Z}$ with their usual arithmetic, and $\mathbb{Z}/26\mathbb{Z}$ with the multiplication and addition as above, are commutative rings.

Convention: From now on, we will use *ring* for a commutative ring, and only include the descriptor when the ring is non-commutative.

(Question 2.7) Let R be a ring. Use the distributive property and $0+0 = 0$ to prove that $0 \cdot x = 0$ for all x.

(Question 2.8) Let $-1 \in R$ be the additive inverse of $1 \in R$. Show that the additive inverse of $x \in X$ equals $(-1) \cdot x$.

Note: Due to the last result, the additive inverse for $x \in R$ will be denoted $-x$.

You might wonder if these properties are enough to encode addition and multiplication, even for the integers. Once we know how to represent the integers using decimal notation (a particular property of the integers) the general properties above compel the addition and multiplication to behave in a specific way:

$$37 \times 43 = 37 \cdot (4 \cdot 10 + 3) = (37 \cdot 4) \cdot 10 + 37 \cdot 3$$

Here we have used the decimal expansion, distributivity, and associativity properties. In fact, this is the basis for the multiplication algorithm taught in US schools: multiply 37 by 3, write it on one line, then, on the next line, write $37 \cdot 4$ shifted over by 1 space (which is the same as multiplication

by 10). Furthermore, to compute $37 \cdot 4$ we use

$$\begin{aligned} 37 \cdot 4 &= (3 \cdot 10 + 7) \cdot 4 \\ &= (3 \cdot 4) \cdot 10 + 7 \cdot 4 \\ &= (1 \cdot 10 + 2) \cdot 10 + 2 \cdot 10 + 8 \\ &= 1 \cdot 10^2 + (2 + 2) \cdot 10 + 8 \end{aligned}$$

where the $(2 + 2)$ corresponds to a carry of 2 in the usual algorithm.

Thus, the *properties* defining addition and multiplication in a general ring allow us to derive the algorithm for addition and multiplication in the *particular* setting of integers, once we have represented the integers by decimal expansions. If we instead represented the natural numbers as the Romans did, we could use these same properties (and the basic additions I + I = II and so forth) to *derive* the correct algorithms for addition and multiplication when using Roman numerals (However, the Roman numerals weren't built around arithmetic, so these algorithms won't be nice: quick, add LXIV and MCI!).

As another benefit we can use these properties to find other algorithms for computing addition and multiplication. Even in the integers, there are other algorithms for computing sums and products. Indeed, in modern cryptography we need to multiply integers with thousands of digits, and the fastest method known for multiplying such large integers is decidely NOT the method you learned in school – it is to cleverly use discrete fast Fourier transforms. We can show that this works because of the properties above.

Finally, by separating out the properties from the algorithms, we can generalize to considering addition and multiplication on other sets, such as the modular arithmetic we used in $\mathbb{Z}/26\mathbb{Z}$. Anything we have proven using the general properties must automatically be valid, and we don't need to provide a particular argument for each number system: for example, the additive identity will be unique since that only required commutativity and the existence of an additive identity.

We consider two types of commonly used rings:

First, let $d > 0$ be an integer and let $\mathbb{Z}/d\mathbb{Z}$ be the set $\{0, 1, \ldots, d-1\}$ equipped with multiplication and addition as in $\mathbb{Z}/26\mathbb{Z}$: take the sum or product as in $\mathbb{Z}$ and then take the remainder after dividing by d.

There is a map $\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}$ which comes from taking the remainder of $x \in \mathbb{Z}$ when dividing by d. More formally, we say $x \cong y \mod d$ if d divides $x - y$. Then there is one and only one $r \in \{0, 1, \ldots, d-1\}$ for which $x \cong r \mod d$, and this number is what we mean by "the remainder of x when divided by d".

(Question 2.9) Show that if $x, y, z \in \mathbb{Z}$ and $x \cong y \mod d$ (that is x and y have the same remainder when divided by d) then $x + z$ and $y + z$ will as well, and so will $x \cdot z$ and $y \cdot z$.

(Question 2.10) Use the result from the previous question and that $\mathbb{Z}$ is a commutative ring, to show that $\mathbb{Z}/d\mathbb{Z}$ is a commutative ring.

The second type we will need is the ring of polynomials with coefficients in a ring R. A polynomial is a function $p : R \longrightarrow R$ of the form

$$p(x) = p_0 + p_1\, x + p_2\, x^2 + \cdots + p_n x^n$$

for $p_i \in R$, $p_n \neq 0$, and some $n \in \mathbb{N} \cup \{0\}$. It is convenient to rewrite these somewhat differently, as infinite series

$$p(x) = p_0 + p_1\, x + p_2\, x^2 + \cdots + p_n x^n + 0\, x^{n+1} + 0\, x^{n+2} + \cdots = \sum_{i=0}^{\infty} p_i\, x^i$$

where all the terms after a certain point (x^n in this example) have coefficient $p_i = 0$. The highest n for which x^n has non-zero coeffcient is called the *degree* of the polynomial, and is denoted $\deg p(x)$. We take the degree of 0, the polynomial with all 0 coefficients, to be $-\infty$. Then,

Definition 6. *Let R be a ring. Then the set of polynomials with coefficients in R is*

$$R[x] = \Big\{ \sum_{i=0}^{\infty} p_i\, x^i \;\Big|\; \exists n \in \mathbb{N} \cup \{0\} \text{ such that } p_N = 0 \text{ for all } N > n \Big\}$$

equipped with the addition

$$\left(\sum_{i=0}^{\infty} p_i\, x^i \right) + \left(\sum_{i=0}^{\infty} q_i\, x^i \right) = \sum_{i=0}^{\infty} \big(p_i + q_i\big)\, x^i$$

and multiplication

$$\left(\sum_{i=0}^{\infty} p_i\, x^i \right) \cdot \left(\sum_{i=0}^{\infty} q_i\, x^i \right) = \sum_{i=0}^{\infty} \left(\sum_{r=0}^{i} p_r q_{i-r} \right) x^i$$

(Question 2.11) Verify that the infinite series (in i) on the right of the expressions defining addition and multiplication do give polynomials – that is, all the coefficients above some cutoff are always 0.

(Question 2.12) What are the identities 0 and 1 in $R[x]$?

(Question 2.13) Verify that that $R[x]$ has the properties of a commutative ring, omitting the verification of associativity of multiplication (which is true, but a bear to check directly)

3. Fields

While we can formulate systems of linear equations, matrices, and such, with coefficients in any *ring*, R, we have seen that the method of Gaussian elimination, and all the usual results of linear algebra, only work when we can also divide. This isn't always possible – for example, in the integers $\mathbb{Z}$ – so we will add another property:

Definition 7. *An element $r \in R$ is a* unit *if there is an element $s \in R$ such that $rs = 1$. The element s is called a* multiplicative inverse *for r. The set of all units in R is denoted $R^\times$*

(Question 3.1) If $r \cdot s = 1$ and $r \cdot s' = 1$ show that $s = s'$. That is, multiplicative inverses are unique! (Remember, R is commutative!)

Thus the multiplicative inverse for $r \in R$ is unique, and we will denote it by r^{-1}.

(Question 3.2) If u and v are units in R, show that uv and u^{-1} are units in R.

(Question 3.3) What is $\mathbb{Z}^\times$? What is $\big(\mathbb{Z}/6\mathbb{Z}\big)^\times$? $\big(\mathbb{Z}/3\mathbb{Z}\big)^\times$?

(Question 3.4) Explain why $\mathbb{Q}^\times = \mathbb{Q}\backslash\{0\}$

(Question 3.5) What are $\mathbb{R}^\times$ and $\mathbb{C}^\times$.

So, in the rationals $\mathbb{Q}$, every (non-zero) number q has a *multiplicative* inverse, q^{-1}. Rings with this property are a *VERY special* type:

Definition 8. *A* field *is a ring $F = (F, +, \cdot, 1, 0)$ such that every non-zero element has a multiplicative inverse: for each $x \in F\backslash\{0\}$ there is a element $x^{-1} \in F$ such that $x \cdot x^{-1} = x^{-1}x = 1$.*

Basic linear algebra works over *any* field, without modification.

Note: The rationals are a subset of the real numbers $\mathbb{R}$, and the additions and multiplications correspond: we get the same sum whichever we use to compute it. The rationals are then a *subfield* of $\mathbb{R}$. The real numbers, in turn, sit inside another field: the complex numbers $\mathbb{C}$. The complex numbers have a specific property that makes them extremely useful:

Theorem 9 (Fundamental Theorem of Algebra)**.** *The complex numbers $\mathbb{C}$ are* algebraically closed. *That is, given any polynomial $p(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots a_1 z + a_0$ ($n \geq 0$) there is a complex number $r \in \mathbb{C}$ such that $p(r) = 0$.*

As a consequence of this theorem, any polynomial with complex coefficients can be completely factored into linear factors. This is not true in the rationals, since $p(x) = x^2 - 2$ has rational coefficients but irrational, real roots. It is also not true in the real numbers since $p(x) = x^2 + 1$ has real coefficients, but no real roots.

There are may other fields besides these, although these are the most likely for you to have encountered. The first example below are representatives of another important type of field: the finite fields.

(Question 3.6) Show that when $d > 2$ is *NOT* prime, then there are numbers $a, b \neq 0$ in $\mathbb{Z}/d\mathbb{Z}$ such that $a \cdot b = 0$. Explain why a cannot have a multiplicative inverse.

(Question 3.7) When p is prime, it turns out that the set

$$\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$$

is a field.

(1) Write out the multiplication table for the elements of $\mathbb{Z}/p\mathbb{Z}$ for $p = 2, 3, 5, 7$ and verify that every non-zero element has a multiplicative inverse.
(2) Pick an $a \in \{1, 2, \ldots, p-1\} = (\mathbb{Z}/p\mathbb{Z})^*$. Show that if $b \in (\mathbb{Z}/p\mathbb{Z})^*$ as well, then $a \cdot b \in (\mathbb{Z}/p\mathbb{Z})^*$ (where we take the product in $\mathbb{Z}/p\mathbb{Z}$). Show that the map $b \longrightarrow a \cdot b$ is a *injection* $(\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ and therefore, by counting elements, that there is one, and only one, element $c \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a \cdot c = 1$ in $\mathbb{Z}/p\mathbb{Z}$. (*Hint:* You may assume the following fact: if a prime p divides a product $n \cdot m$ of integers then p either divides one (or both) if n and m)

(Question 3.8) Solve the following system of equations over the field $\mathbb{F} = \mathbb{Z}/5\mathbb{Z}$. How many solutions does the system have?

$$\begin{aligned} 1\,a + 2\,b + 4\,c + 3\,d &= 2 \\ 4\,a + 3\,b + 2\,c + 2\,d &= 2 \\ 2\,a + 4\,b + 4\,c + 1\,d &= 3 \end{aligned}$$

(Question 3.9) Try to prove that $\mathbb{C}$ is a field by directly verifying the properties of the definition from our rules for multiplication and addition. You will need some computation to verify that multiplication is associative.

(Question 3.10) Let $\mathbb{Q}[i] = \left\{ q_1 + iq_2 \in \mathbb{C} \,\middle|\, q_1, q_2 \in \mathbb{Q} \right\}$. Prove that $\mathbb{Q}[i]$ is a field, where the addition, multiplication, additive identity, and multiplicative identity are the same as in $\mathbb{C}$. (Note: you already know the operations on $\mathbb{C}$ form a field, so first convince yourself that this will follow if you can just show that products and sums of elements of $\mathbb{Q}[i]$ are in $\mathbb{Q}[i]$, inverses of elements of $\mathbb{Q}[i]$ are in $\mathbb{Q}[i]$, identities are in $\mathbb{Q}[i]$ etc.)

(Question 3.11) Let $\mathbb{F}[i] = \left\{ f_1 + if_2 \,\middle|\, f_1, f_2 \in \mathbb{F} \right\}$ where $\mathbb{F}$ is a field. Define addition and multiplication by

$$\begin{aligned} (f_1 + i\,f_2) + (g_1 + i\,g_2) &= (f_1 + g_1) + i(f_2 + g_2) \\ (f_1 + i\,f_2) \cdot (g_1 + i\,g_2) &= (f_1 g_1 - f_2 g_2) + i(f_1 g_2 + g_1 f_2) \end{aligned}$$

In addition, let $0 = 0_F + i\,0_F$ and $1 = 1_F + i\,0_F$.

(1) Prove that $\mathbb{F}[i]$ is a ring
(2) Prove that $\mathbb{Z}/3\mathbb{Z}[i]$ is a field
(3) Show that $\mathbb{Z}/5\mathbb{Z}[i]$ is *NOT* a field. (Hint: Show that $1 + 2i$ has no multiplicative inverse!.)