Part 2. Prerequisites and preliminaries

1. Sets

We review some elementary notions from set theory that are required throughout the course. A set is just a collection of objects; the precise definition lies beyond the scope of this course. Not every collection of objects is a set (such as the collection of all sets not containing themselves as elements).

Two sets are equal if and only if they have the same elements.

Example 1.1. The following sets are equal:

- { Styles, Malik, Tomlinson, Horan, Payne };
- { Horan, Styles, Tomlinson, Malik, Payne }.

If X is a set, we write $x \in X$ to indicate that x is an element of X (or x belongs to X). We write $x \notin X$ to indicate that x is not an element of X. The symbol $\varnothing$ denotes the ***empty set***, that is, the set with no elements.

Example 1.2.

- If $X = \{0, 1, 2\}$, then $0 \in X$ but $-1, \pi \notin X$;
- If $X =$ { Paris, New York, London, Berlin }, then Paris $\in X$ but St Andrews $\notin X$;
- If $X =$ { peaches that are apples }, then $X = \varnothing$.

Sets are often specified in the following form:

$$\{\, a \in A \,:\, a \text{ has some property called } P \,\}$$

where A is a set. This should be read as: those elements a belonging to A that have the property P.

Example 1.3.

- { Horan, Styles, Tomlinson, Malik, Payne } = $\{\, x \,:\, x$ is in One Direction $\}$;
- $\{0, 1, 2\} = \{\, x \in \mathbb{Z} \,:\, 0 \leq x \leq 2 \,\}$.

The following sets and the corresponding notation will be used throughout this course:

$\mathbb{N}$**:** the natural numbers $\{1, 2, \ldots\}$;
$\mathbb{Z}$**:** the integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$;
$\mathbb{Q}$**:** the rationals $\{\, p/q \,:\, p, q \in \mathbb{Z},\ q \neq 0 \,\}$;
$\mathbb{R}$**:** the real numbers, such as π, e, $\sqrt{2}$, and all the rationals;
$\mathbb{C}$**:** the complex numbers $\{\, a + bi \,:\, a, b \in \mathbb{R} \,\}$.

Let A and B be sets. Then we write $A \subseteq B$ to indicate that every element of A is an element of B (or A is a ***subset*** of B). We write $A \nsubseteq B$ to indicate that A is not a subset of B, and $A \subsetneq B$ to indicate that A is a subset of B but $A \neq B$. If $A \subsetneq B$, then we say that A is a ***proper subset*** of B.

Example 1.4.

- { Paris, New York, London, Berlin } is a proper subset of the set consisting of World Cities;
- $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$;
- $\{0\} \subsetneq \mathbb{Q}$;
- { Styles, Malik, Tomlinson, Horan, Payne } $\nsubseteq$ { good musicians };
- { peaches that are apples } is a proper subset of {fruit};

The sets

$$A \cap B = \{\, x \,:\, x \in A \text{ and } x \in B \,\}, \quad A \cup B = \{\, x \,:\, x \in A \text{ or } x \in B \,\}$$

are the ***intersection*** and ***union*** of A and B, respectively. If $A \cap B = \varnothing$, then we say that A and B are ***disjoint***.

Example 1.5.

- $\{0, 1, 2\} \cap \{2, 3, 4\} = \{2\}$;
- $\{0, 1, 2\} \cap \{\, x \in \mathbb{R} \,:\, x < 0 \,\} = \varnothing$;
- $\mathbb{Z} = \mathbb{N} \cup \{\, -n \,:\, n \in \mathbb{N} \,\}$;
- $\{\, x \in \mathbb{R} \,:\, x \geq 0 \,\} \cap \{\, x \in \mathbb{Q} \,:\, x \leq 0 \,\} = \{0\}$;

- $\mathbb{Z} \cup \mathbb{Q} = \mathbb{Q}$;
- $\{10, 14, 21\} \cup \{13, 14, 15, 21\} = \{10, 13, 14, 15, 21\}$.

The size of a set A is denoted by $|A|$.

Example 1.6.

- $|\{0, 1, 2\}| = 3$;
- $|\varnothing| = 0$;
- $|\mathbb{R}| = \infty$.

2. Logic

In this section, we briefly describe some aspects of elementary logic which are required in this course.

Validity. You will make use of logic to make **conclusions** based on certain **premisses** or **assumptions**.

Here is a logical argument:

Premiss: James is a responsible person;
Conclusion: James is purple.

Is this a valid argument? No, I am responsible but not purple.

An argument is ***logically valid*** if it has no interpretation such that the premisses are all **true**, and the conclusion is **false**.

Premisses: James is a responsible person, and all responsible people are purple;
Conclusion: James is purple.

Is this a valid argument? Yes, if the premisses are all true, then the conclusion is also true.

Implications, converses, negations, contrapositives. Premisses can be combined using the following are ***logical terms***:

all, every, some, no, not, and, or, if

In mathematics (unlike in natural language), a statement of the form "if A, then B" means "if A is true, then B is true" and it means "if A is false, then B can be either false or true". A statement of the form "if A, then B" is called an ***implication***.

Example 2.1.

- If $x \in \mathbb{R}$ and $x \geq 0$, then $x > -1$;
- if $n \in \mathbb{N}$ is an even number, then $n/2 \in \mathbb{N}$;
- if $x > 0$, then $x + 1 > 0$.

The ***converse*** of an implication "if A, then B" is "if B, then A". Sometimes the converse of true statement is also true, but it can also be false.

Example 2.2. The following statements are the converses of the examples in Example 2.1:

- if $x \in \mathbb{R}$ and $x > -1$, then $x \geq 0$;
- if $n/2 \in \mathbb{N}$, then n is an even number;
- if $x + 1 > 0$, then $x > 0$.

Which of these statement is true?

- "if $x \in \mathbb{R}$ and $x > -1$, then $x \geq 0$" is ***false*** since $x = -1/2$ has the property that $x > -1$ but not $x \geq 0$. Such an x is called a ***counter example*** to the validity of the statement.
- "if $n/2 \in \mathbb{N}$, then n is an even number" is ***true***, since, in this case, $n = 2 * (n/2)$. This is a ***proof*** that the statement is true.
- "if $x + 1 > 0$, then $x > 0$", again $x = -1/2$ is a counter example to this statement, and so the statement is ***false***.

If an implication and its converse hold, then A and B are said to be ***equivalent***, we also write "A if and only if B".

Example 2.3. We have already seen that $n \in \mathbb{N}$ is even if and only if $n/2 \in \mathbb{N}$.

The ***contrapositive*** of an implication "if A, then B" is the implication "if not B, then not A". The statement "if A is true, then B is true" implies "if B is false, then A is false" (since if B is false and A is true, then the latter implies that B is true but it cannot be both true and false!). It can sometimes be convenient to prove the contrapositive of a statement rather than the statement itself.

Example 2.4. The following statements are the contrapositives of the examples in Example 2.1:

- "if $x \in \mathbb{R}$ and $x < 0$, then $x \leq -1$". This is still ***false***, and $x = -1/2$ is still a counter example;
- "if n is an odd number, then $n/2 \notin \mathbb{N}$." This is still ***true***.
- if "$x \leq 0$, then $x + 1 \leq 0$". This is still ***false***, and $x = -1/2$ is still a counter example.

The ***negation*** of an implication "if A, then B" is "if not A, then not B; more on negations of expressions is in the next subsection.

Quantifiers. The symbol $\forall$ means "for all" or "for every", and the symbol $\exists$ means "there exists". We write $\nexists$ to mean "there does not exist".

What is the difference between the following statements:

(i) $\forall x\ \exists y$;
(ii) $\exists y\ \forall x$?

Try substituting natural language into the expressions:

(i) for all people x there exists a person y who is the mother of x;
(ii) there exists a mother y for all people x.

Expression (i) is true and (ii) is false. A more mathematical example,

(i) for all $x \in \mathbb{N}$ there exists $y \in \mathbb{N}$ such that $y < x$;
(ii) there exists $y \in \mathbb{N}$ such that $y < x$ for all $x \in \mathbb{N}$.

In this example, both statements are false: if $x = 0$, then what is y?

We can also translate from natural language into a logical statement:

Some birds do not fly.

If B is the set of birds and F is the set of birds that fly, then this becomes:

"There exists $x \in B$ such that $x \notin F$" or "$\exists x \in B$ such that $x \notin F$".

Another example:

there is no largest prime number

if P is the set of prime numbers, then this can be written:

$\nexists p \in P$ such that $p \geq x$, $\forall x \in P$.

The ***negation*** of a logical statement such as "$\forall x\ \exists y$ such that A holds" is "$\exists x$ such that A does not hold $\forall y$". For example, "there is a greatest natural number" can be written as "$\exists x \in \mathbb{N}$ such that $x \geq y$, $\forall y \in \mathbb{N}$" and so "there is not a greatest natural number" is "$\forall x \in \mathbb{N}\ \exists y \in \mathbb{N}$ such that $x < y$".

A further example is: "there is no largest prime number" can be written "$\forall p \in P\ \exists x \in P$ such that $p < x$."

Of course, you can use an unlimited number of $\forall$ and $\exists$, combined in arbitrarily complicated ways. For example,

(i) "$\forall \varepsilon > 0\ \exists \delta > 0$ such that $\forall x \in \mathbb{R}$, $x\delta < \varepsilon$";
(ii) "$\forall \varepsilon > 0$ and $\forall x \in \mathbb{R}\ \exists \delta > 0$ such that $x\delta < \varepsilon$".

Note that (i) is false, and (ii) is true.

3. Numbers, polynomials, and matrices

For the purposes of this section a ***number*** is an element of any of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. If R is any of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, then a ***polynomial*** with coefficients in R is an expression of the form:

$$a_n x^n + \cdots a_1 x^1 + a_0$$

where $a_0, a_1, \ldots, a_n \in R$ for some $n \in \mathbb{N}$. For example, $2x^2 - 5x$ is a polynomial with integer coefficients. If $n \in \mathbb{N}$, then an $n \times n$ ***matrix*** over R is a square array of the form

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,n} \end{pmatrix}$$

where $a_{i,j} \in R$ for all i, j.

What do numbers, polynomials, and matrices have in common?

We can ***add*** numbers, polynomials, and matrices:

$$2 + 2 = 4, \qquad (x^2 - 1) + (3x^2 - 2x + 5) = 4x^2 - 2x + 4, \qquad \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 7 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 9 \\ 8 & 2 \end{pmatrix}.$$

We can ***multiply*** numbers, polynomials, and matrices:

$$3 \times 17 = 51, \qquad x^2 \times x^4 = x^6, \qquad \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 7 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 9 \\ 5 & 22 \end{pmatrix}.$$

[Multiplying matrices involves multiplying and adding numbers.]

We can multiply ***and*** add numbers, polynomials, and matrices:

$$3 \times (2 + 3) = (3 \times 2) + (3 \times 3) = 3 \times 5 = 15, \qquad x^2 \times (x^2 + 1) = (x^2 \times x^2) + (x^2 \times 1)$$

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \times \left(\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix} \right) &= \left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \right) + \left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix} \right) \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} 5 & 5 \\ 5 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 10 & 10 \\ 10 & 10 \end{pmatrix}. \end{aligned}$$

Multiplying is relatively straightforward, if sometimes tedious, but the reverse of multiplication can be really difficult! The reverse of multiplication is ***factorization***.

We can sometimes factorize numbers, polynomials, and matrices, for example:

$$666 = 2 \times 3 \times 3 \times 37.$$

What does this really mean? Why did we chose 2, 3, and 37 as factors? Why not 74 and 9? One reason would be that 2, 3 and 37 are prime numbers, i.e. they cannot be further factorized into a product of natural numbers, while 9 and 74 are not primes. The ***Fundamental Theorem of Arithmetic*** states that every natural number can be factorized uniquely into a product of primes.

What if we are allowed to use rational or real numbers instead of only natural numbers? In this case,

$$666 = \frac{1}{666} \times \frac{1}{2} \times 2^3 \times 3^2 \times \frac{353}{424} \times 37 \times \frac{353}{424}.$$

Are there real numbers which cannot be written as a product of other real numbers? Not really (well, maybe 0 counts).

If we want to factorize a polynomial, what is a good choice for the factors? We might go with a similar definition as for numbers: we want to factorize a polynomial into polynomials which cannot be further factorized into products of polynomials. Such polynomials are called ***irreducible***. Whether a polynomial is irreducible, or not, depends very strongly on the context. For example:

$$x^2 - 2$$

cannot be factorized into a product of polynomials (of smaller degree) with coefficients in $\mathbb{Z}$, but it can be factorized as:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

polynomials with coefficients in $\mathbb{R}$. The ***Fundamental Theorem of Algebra*** states that every non-constant polynomial (with one variable) with coefficients in $\mathbb{C}$ has a factorization into linear polynomials with coefficients in $\mathbb{C}$.

When we consider matrices, life gets even harder. There are many different ways of factorizing matrices, such as the Gram-Schmidt process, the Jordan normal form, and so on.

We can sometimes ***invert*** numbers, polynomials, and matrices and sometimes not: if $x \in \mathbb{R}$, then x^{-1} exists if and only if $x \neq 0$. If $x \in \mathbb{Z}$ and $x \neq \pm 1$, then $x^{-1} \in \mathbb{Q}$ but $x^{-1} \notin \mathbb{Z}$. So we cannot always invert an element of $\mathbb{Z}$ and obtain an element of $\mathbb{Z}$.

The matrix

$$\begin{pmatrix} 10 & 10 \\ 10 & 10 \end{pmatrix}$$

is not invertible, but

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

is invertible.

What about polynomials? Following the example of numbers and matrices, if f is a polynomial, then we want to find another polynomial g such that $fg = 1$. When is this possible? If $f = x^2$, does there exist a polynomial g with $fg = 1$? The answer is ***no***.

Suppose we want to study only the things about matrices, polynomials, and numbers that can be deduced from the properties of addition and multiplication? More specifically, suppose we only want study the consequences of those properties of addition and multiplication that are common to matrices, polynomials, and numbers. This is essentially what **abstract algebra** is, the study of those properties common to matrices, polynomials, and numbers.

We could study matrices, polynomials, and numbers, separately, but this would be wasteful, and so we will **abstract** away from the particular examples and only study the consequences of the rules of addition and multiplication, which are common to matrices, polynomials, and numbers.

If we do this, then we obtain the following definition.

Definition 3.1. A ***ring*** is a set R together with $+$ and $*$ satisfying the axioms:

(i) $r + s \in R$ for all $r, s \in R$;
(ii) $r + (s + t) = (r + s) + t$ for all $r, s, t \in R$;
(iii) there exists $0 \in R$ such that $r + 0 = 0 + r = r$ for all $r \in R$;
(iv) for all $r \in R$ there exists $-r \in R$ such that $r + (-r) = 0 = (-r) + r$;
(v) $r + s = s + r$ for all $r, s \in R$;
(vi) $r * s \in R$ for all $r, s \in R$;
(vii) $r * (s * t) = (r * s) * t$ for all $r, s, t \in R$;
(viii) $(r + s) * t = r * t + s * t$ and $r * (s + t) = r * s + r * t$ for all $r, s, t \in R$.

The prototypical example of a ring is $\mathbb{Z}$. Further examples are: $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, the polynomials with coefficients in any of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, and the $n \times n$ matrices with entries in any of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. There are many further rings besides. In fact, if R is any ring, then the polynomials with coefficients in R are also a ring. The set of $n \times n$ matrices with entries in R, $n \in \mathbb{N}$, is also a ring.

Here is an example of a ring which is not one of the types we have already seen.

Example 3.2. The quaternions are defined to be the set $\mathbb{H} = \{\, a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \,:\, a, b, c, d \in \mathbb{R} \,\}$ with addition

$$(a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}) + (b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}) = (a_1 + b_1) + (a_2 + b_2)\mathbf{i} + (a_3 + b_3)\mathbf{j} + (a_4 + b_4)\mathbf{k}$$

and multiplication

$$\begin{aligned}(a_1+a_2\mathbf{i}+a_3\mathbf{j}+a_4\mathbf{k})*(b_1+b_2\mathbf{i}+b_3\mathbf{j}+b_4\mathbf{k}) &= (a_1b_1-a_2b_2-a_3b_3-a_4b_4)+(a_1b_2+a_2b_1+a_3b_4-a_4b_3)\mathbf{i} \\ &\quad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)\mathbf{j} + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)\mathbf{k}.\end{aligned}$$

Sometimes the quaternions are denoted Q_8 or $\mathbf{H}$.

The above multiplication is rather cumbersome. It is often more useful to multiply elements of $\mathbb{H}$ together as if they are polynomials (with real coefficients and indeterminants **i, j,** and **k**) and then apply the rules given in the following table:

*	1	**i**	**j**	**k**
1	1	**i**	**j**	**k**
i	**i**	-1	**k**	**-j**
j	**j**	**-k**	-1	**i**
k	**k**	**j**	**-i**	-1

By rather laborious calculations it is possible to show that $\mathbb{H}$ together with the addition and multiplication defined above satisfy the ring axioms. Thus $\mathbb{H}$ is a ring.

One the ring axioms, says that $r+s=s+r$ for all $r,s\in R$. Why did we not include $r*s=s*r$ for all $r,s\in R$? This is not a common feature of numbers, polynomials, and matrices, that's why. For example,

$$\begin{pmatrix}3&4\\1&2\end{pmatrix}*\begin{pmatrix}1&1\\1&2\end{pmatrix}=\begin{pmatrix}7&11\\3&5\end{pmatrix}\neq\begin{pmatrix}4&6\\5&8\end{pmatrix}=\begin{pmatrix}1&1\\1&2\end{pmatrix}*\begin{pmatrix}3&4\\1&2\end{pmatrix}.$$

Why did we not include that every element should be invertible in the ring axioms? This is not a common feature of numbers, polynomials, and matrices, that's why. For example, we saw earlier that not every integer is invertible, most polynomials are not invertible, and many matrices are not.

A ring where $r*s=s*r$ for all $r,s\in R$ and every element is invertible has a special name, it is called a ***field***. For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not. Satisfying ten axioms, as they do, they are rather special types of rings.

We will begin our study of abstract algebra by looking at some objects which are closely related to rings and fields, but which only satisfy four of the axioms.