A brief review of basic concepts

A few very basic concepts are indispensable for all that follows. They are reviewed here. Later they will be used all the time, usually without any further discussion. Ideally, much of what is discussed here is already known to you from first-year mathematics, at least for special cases. If it is not, don't worry — simply make yourself as familiar with any new concept as possible, and come back later as needed to ponder the details.

Logic

Later in this course, we will introduce and study many different mathematical objects, such as numbers, sequences, functions, derivatives, integrals, etc. Our observations regarding these objects will typically be formulated as **mathematical statements**, often in the form of a **Theorem**, a **Corollary** (i.e. a straightforward consequence of a theorem), a **Lemma** (i.e. an auxiliary observation of independent interest) or a **Proposition** (i.e. a fact stated without proof). Throughout, we will maintain the view that a mathematical statement is either **true** or **false**. For instance, the statement

$$S_1: \quad 5 \text{ is an odd integer}$$

is true, whereas the statement

$$S_2: \quad 4 \text{ is a prime number}$$

is false. Statements of indeterminable logical status such as

$$S_3: \quad \text{Edmonton is a nice city}$$

do not belong in this course.

There are many ways of creating new statements from existing ones. Easiest perhaps is to simply negate a given statement S: The statement $\neg S$ (read: **not** S) is true if S is false and vice versa. If S_1, S_2 are two statements then $S_1 \wedge S_2$ (read: S_1 **and** S_2) is true if both S_1 and S_2 are true, and false otherwise. On the other hand, $S_1 \vee S_2$ (read: S_1 **or** S_2) is true whenever at least one of the two statements is true, and hence false only if both S_1 and S_2 are false. Another statement created from S_1, S_2 is the implication $S_1 \Rightarrow S_2$ (read: S_1 **implies** S_2, or **if** S_1 **then** S_2) which is true unless S_1 is true and, at the same time, S_2 is false. (Note that for false S_1, the statement $S_1 \Rightarrow S_2$ is always true, regardless of the truth

of S_2.) If $S_1 \Rightarrow S_2$ is true then S_1 is also said to be **sufficient** for S_2, and S_2 is **necessary** for S_1. For instance, with

$$S_1: \quad m \geq 5 \text{ is a prime number},$$
$$S_2: \quad m \geq 3 \text{ is an odd integer},$$

clearly $S_1 \Rightarrow S_2$, but $S_2 \not\Rightarrow S_1$, the latter meaning $\neg(S_2 \Rightarrow S_1)$. Finally, the equivalence statement $S_1 \Leftrightarrow S_2$ (read: S_1 **is equivalent to** S_2, or S_1 **if and only if** S_2) is true if S_1 and S_2 are either both true or both false, and false otherwise.

We will often be charged with the task of proving an implication $S_1 \Rightarrow S_2$, that is, demonstrating that $S_1 \Rightarrow S_2$ is true. Since $S_1 \Rightarrow S_2$ is true whenever S_1 is false, all that this really amounts to is showing that S_2 is true whenever S_1 is true. Basically, this can be done in two fundamentally different ways. A **direct proof** would go like this:

`Assume` S_1 `is true. Then ... and therefore ... Hence ...,`
`which in turn shows that` S_2 `is true.`

On the other hand, an **indirect proof** is based on the logical equivalence of $S_1 \Rightarrow S_2$ and $\neg S_2 \Rightarrow \neg S_1$, i.e. on the true statement $(S_1 \Rightarrow S_2) \Leftrightarrow (\neg S_2 \Rightarrow \neg S_1)$. It would go like this:

`Suppose,` S_2 `was false. Then ... and therefore ... Hence ...,`
`and so` S_1 `would be false as well.`

Thus, if S_1 is true then S_2 cannot possibly be false, and hence must be true, that is, $S_1 \Rightarrow S_2$ is true. For a simple concrete example, consider the two statements

$$S_1: \quad m, n \text{ are two positive integers},$$
$$S_2: \quad 2m^2 \neq n^2.$$

To prove $S_1 \Rightarrow S_2$ directly, you would take any positive integers m, n and then, through a combination of brilliant thoughts and calculations, arrive at the conclusion that $2m^2 \neq n^2$. To verify $S_1 \Rightarrow S_2$ indirectly, you would assume that $2m^2 = n^2$ for *some* numbers and then, through an equally brilliant yet presumably very different combination of thoughts, deduce that m, n cannot both be positive integers.

To prove an equivalence statement $S_1 \Leftrightarrow S_2$ (recall, that's "S_1 if and only if S_2"), we will often break it into its two parts $S_1 \Rightarrow S_2$ (the "only if" part) and $S_2 \Rightarrow S_1$ (the "if" part) and deal with each part individually. Also, when formulating statements and proofs, we will make use of the symbols $\exists$ (read: **there exists**) and $\forall$ (read: **for all**). Usage of symbols like $:=$ (or $=:$) means that the expression next to the colon (:) is being *defined* by whatever appears on the right (or left) side of the symbol. Often, *such that* is abbreviated as *s.t.* The end of a proof is indicated by $\square$.

Sets

We are using notions of set theory only in a naive, that is, non-formalistic manner. For us, a **set** is simply a collection of *distinct* objects. The two key features of the notion of a set

are that every set contains each of its elements only once, and that we have to be able to decide (at least theoretically), for every set and every conceivable object we are dealing with, whether or not that object is an element of the set. Typically, upper case characters indicate sets, and lower case characters denote their elements. Two sets are equal precisely if they contain the same elements. The sets we will consider mostly consist of numbers, or of more complicated objects created from numbers. We write $a \in A$ to express that the object a is an element of the set A, and $a \notin A$ to say that it is not. Sets can be defined in many ways, for example by means of an unambiguous verbal description,

$$\begin{aligned} \mathbb{Z} &:= \text{ the set of integers}\,, \\ \mathbb{N} &:= \text{ the set of positive integers}\,, \\ \mathbb{P} &:= \text{ the set of prime numbers}\,, \end{aligned}$$

or by indicating the defining property

$$\begin{aligned} \mathbb{Z} &:= \{k : k \text{ is an integer}\}\,, \\ \mathbb{N} &:= \{n : n \text{ is a positive integer}\} = \{n \in \mathbb{Z} : n > 0\}\,, \\ \mathbb{P} &:= \{p : p \in \mathbb{N} \text{ is a prime number}\}\,, \end{aligned}$$

or sometimes also simply by listing sufficiently many elements,

$$\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}\,, \qquad \mathbb{N} := \{1, 2, 3, 4, 5, \ldots\}\,, \qquad \mathbb{P} := \{2, 3, 5, 7, 11, \ldots\}\,.$$

Note that the order in which elements of a set are displayed is irrelevant. However, some orders may be easier to write, read, and understand than others.

For any two sets A and C, we write $A \cup C$ and $A \cap C$ for their **union** and **intersection**, respectively, that is,

$$A \cup C := \{a : a \in A \ \vee \ a \in C\}\,, \qquad A \cap C := \{a : a \in A \ \wedge \ a \in C\}\,,$$

and $A \setminus C$ for their **difference**

$$A \setminus C := \{a : a \in A \ \wedge \ a \notin C\}\,.$$

The **symmetric difference** of A and C is

$$A \triangle C := (A \setminus C) \cup (C \setminus A) = \{a : a \text{ belongs to exactly one of the sets } A \text{ and } C\}\,.$$

If every element of A is also an element of C, then A is a **subset** of C, in symbols $A \subset C$ or $C \supset A$. Note that $A = C$ precisely if $A \subset C$ and $C \subset A$. To emphasize when A is a **proper** subset of C, that is, $A \subset C$ but $A \neq C$, we sometimes write $A \subsetneq C$. The **empty set** is the set containing no element at all; it is symbolized by $\varnothing$ and is a subset of every set.

For any set A, the set of all subsets of A is denoted by 2^A, that is,

$$2^A = \{B : B \subset A\}\,.$$

(This somewhat clunky notation is motivated by the simple observation that if A has exactly n elements then 2^A has exactly 2^n elements.) For example, if $A = \{a, b\}$ then

$$2^A = \big\{\varnothing, \{a\}, \{b\}, \{a, b\}\big\} .$$

A subset P of 2^A, i.e. a set of subsets of A, is a **partition** of A if every element $a \in A$ is contained in *exactly one* element $B \in P$. For instance, $\{\mathbb{N}_e, \mathbb{N}_o\}$ with

$$\mathbb{N}_e := \{n \in \mathbb{N} : n \text{ even}\} = \{2, 4, 6, 8, 10, \dots\} \quad \text{and} \quad \mathbb{N}_o := \{n \in \mathbb{N} : n \text{ odd}\} = \{1, 3, 5, 7, 9, \dots\}$$

is a partition of $\mathbb{N}$.

Recall that it is irrelevant in which order the elements of a set are displayed. Thus for instance $\{a, b\} = \{b, a\}$ for any $a \in A$, $c \in C$. Often it is important to consider *ordered* pairs (and triples etc.) of elements of sets. To this end, formally define

$$(a, c) := \big\{a, \{a, c\}\big\} \qquad \forall a \in A, c \in C .$$

With this, $(a, c) = (b, d)$ if and only if $a = b$ and $c = d$. Moreover, $(a, c) \neq (c, a)$ unless $a = c$. The object (a, c) is the **ordered pair** with first component a and second component c. The **Cartesian product** of the sets A, C then simply is the set of all ordered pairs,

$$A \times C := \{(a, c) : a \in A, c \in C\} .$$

Relations

So far, we have only considered unstructured sets. Practically every set of any importance in mathematics comes with some additional structure. The simplest forms of structure arise from relations.

Definition 1. Let A, C be sets. Any subset R of $A \times C$ is called a **relation** from A to C. If $A = C$ then R is a relation *on* A. The element $a \in A$ is said to be **related** to $c \in C$ if $(a, c) \in R$.

If R is a relation from A to C then

$$R^{-1} := \{(c, a) : (a, c) \in R\} \subset C \times A$$

is a relation from C to A, called the **inverse relation** of R. For every $c \in C$, the set

$$R_c := \{a \in A : (a, c) \in R\} \subset A$$

is referred to as a **fibre** of R. It is usual to write aRc instead of $(a, c) \in R$. For any $B \subset A$, the **restriction** of R to B, symbolized as $R|_B$, is the relation from B to C given by

$$R|_B := \{(a, c) : aRc \wedge a \in B\} = (B \times C) \cap R .$$

Let R be a relation on a set A. Then R is called

(i) **reflexive** if aRa for every $a \in A$, or equivalently, if $R \supset \{(a,a) : a \in A\}$;

(ii) **symmetric** if aRb precisely if bRa, or equivalently, if $R^{-1} = R$;

(iii) **anti-symmetric** if aRb and bRa together imply that $a = b$;

(iv) **transitive** if aRb and bRc together imply that aRc.

For us, the most important examples of relations are, respectively, equivalence relations, partial orders, and functions.

Definition 2. A relation R on a set A is an **equivalence relation** if it is reflexive, symmetric and transitive.

The two extreme cases of equivalence relations are $R = \{(a,a) : a \in A\}$, where each $a \in A$ is related only to itself, and $R = A \times A$, where each $a \in A$ is related to every $b \in A$. Popular symbols denoting equivalence relations include $\sim$ and $\equiv$. Fibres of equivalence relations are often denoted by $[a]_R$ rather than R_a and referred to as **equivalence classes** of R. For any equivalence relation, you may think of aRc as indicating that a and c are "in some way" the same, with the meaning of "in some way" being made precise by R. It is an easy but important observation that equivalence relations on and partitions of a set are really but two aspects of the same thing.

Lemma 3. *Let A be a set. Then:*

(i) *If R is an equivalence relation on A then $P_R := \{[a]_R : a \in A\} \subset 2^A$, i.e. the set of all equivalence classes of R, is a partition of A.*

(ii) *If P is a partition of A then the relation R_P on A, defined according to*

$$aR_Pb \;:\Leftrightarrow\; \{a,b\} \subset B \text{ for some } B \in P\,,$$

is an equivalence relation on A.

(iii) *With the definitions of P_R as in* (i) *and R_P as in* (ii),

$$R_{P_R} = R \quad \textit{and} \quad P_{R_P} = P\,.$$

Proof. (i) Since R is reflexive, $a \in [a]_R$ for every $a \in A$, hence every $a \in A$ belongs to *at least* one element of P_R. Assume that $a \in [b]_R$ and $a \in [c]_R$ for some $b, c \in A$. Pick any $d \in [b]_R$. Then dRb, bRa, and aRc, hence by transitivity also dRc, i.e. $d \in [c]_R$. Since d was arbitrary, $[b]_R \subset [c]_R$. Reversing the roles of b and c gives $[c]_R \subset [b]_R$. Overall, $[b]_R = [c]_R$. This shows that a is contained in *exactly one* element of P_R, i.e., P_R is a partition.

(ii) Since P is a partition, aR_Pa for every $a \in A$. From $\{a,b\} = \{b,a\}$, it is clear that R_P is symmetric. Also, if $\{a,b\} \subset B \in P$ and $\{b,c\} \subset C \in P$ then $B = C$ since otherwise b would be contained in two different elements of P. Thus $\{a,b,c\} \subset B$, showing that R_P is transitive as well, and hence an equivalence relation.

(iii) From the definitions of R_{P_R} and P_R, we deduce that

$$aR_{P_R}b \Leftrightarrow \exists B \in P_R : \{a,b\} \subset B \Leftrightarrow \exists c \in A : \{a,b\} \subset [c]_R \Leftrightarrow aRb\,,$$

hence $R_{P_R} = R$. On the other hand,

$$\begin{aligned} B \in P_{R_P} &\Leftrightarrow \exists a \in A : B = [a]_{R_P} \\ &\Leftrightarrow \exists a \in A : B = \{c : aR_Pc\} \\ &\Leftrightarrow \exists a \in A : B = \big\{c : \{a,c\} \subset D \text{ for some } D \in P\big\} \\ &\Leftrightarrow \exists D \in P : B = D \\ &\Leftrightarrow B \in P\,, \end{aligned}$$

showing that $P_{R_P} = P$. □

Example 4. Given any $n \in \mathbb{N}$, define a relation $\equiv_n$ on $\mathbb{Z}$ according to

$$k \equiv_n l \ :\Leftrightarrow k - l \text{ is divisible by } n\,.$$

You may want to check that $\equiv_n$ is an equivalence relation. The equivalence classes of $\equiv_n$ are often referred to as the **congruence** (or **residue**) **classes mod** n. Note that there are exactly n such classes as

$$\mathbb{Z}_n := \{[k]_{\equiv_n} : k \in \mathbb{Z}\} = \{[0]_{\equiv_n}, [1]_{\equiv_n}, \ldots, [n-1]_{\equiv_n}\}$$

contains exactly n elements.

Definition 5. A relation R on a set A is a **partial order** if it is reflexive, anti-symmetric and transitive. If, in addition, any two elements of A are related, that is, if for every $a, c \in A$ either aRc or cRa (or both), then R is a **total** (or **linear**) **order**.

A **partially** (resp. **totally**) **ordered set** is simply a set with a partial (resp. total) order on it. Often, symbols such as $\prec$ or $\leq$ are used to denote partial orders.

Let $(A, \prec)$ be a partially ordered set and $B \subset A$. An element $a \in A$ is a **lower** (resp. **upper**) **bound** of B if $a \prec b$ (resp. $b \prec a$) for all $b \in B$. The set B is **bounded below** (resp. **above**) if there exists a lower (resp. upper) bound of B, and simply **bounded** if it is bounded both below and above. A lower bound $a \in A$ of $B \subset A$ is the **infimum** (or **greatest lower bound**) of B, in symbols $a = \inf B$, if $c \prec a$ for every lower bound c of B. Similarly, an upper bound $a \in A$ of $B \subset A$ with the property that $a \prec d$ for every upper bound d of B is called the **supremum** (or **least upper bound**) of B, in symbols $a = \sup B$. Note that the infimum or supremum of a set $B \subset A$ may not exist, but if it exists it is unique due to anti-symmetry.

Example 6. (i) Let A be a set. Define a relation $\prec$ on 2^A by $B \prec C :\Leftrightarrow B \subset C$. Then $\prec$ is a partial order on 2^A. If A has more than one element, this is not a total order because for any $a \neq b$, neither $\{a\} \subset \{b\}$ nor $\{b\} \subset \{a\}$. Note, however, that every $Q \subset 2^A$ is bounded below by $\varnothing$ and bounded above by A. In fact, it is not hard to verify that

$$\inf Q = \bigcap\nolimits_{B \in Q} B \quad \text{and} \quad \sup Q = \bigcup\nolimits_{B \in Q} B$$

holds for every $Q \subset 2^A$.

(ii) To see that an infimum or supremum of a bounded set may not exist, not even if the ambient set is totally ordered, let A be the set of non-integer rational numbers, that is,

$$A = \left\{ \frac{k}{n} : k \in \mathbb{Z}, n \in \mathbb{N} \right\} \setminus \mathbb{Z}\,,$$

endowed with its usual (total) order. Clearly, the set

$$B = \left\{ \frac{1}{n} : n \in \mathbb{N}, n \geq 2 \right\} = \left\{ \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots \right\} \subset A$$

is bounded below by $-\frac{1}{2}$, say, yet $\inf B$ does not exist. (Why?)

(iii) Define a relation $\prec$ on $\mathbb{N}$ according to

$$m \prec n \;:\Leftrightarrow\; n \text{ is divisible by } m\,.$$

With this, $\prec$ is a partial (but not total) order on $\mathbb{N}$. Every set $B \subset \mathbb{N}$ is bounded below by 1, but B is bounded above only if it has not more than a finite number of elements. (Why?)

Definition 7. Let A, C be sets. A relation R from A to C is a **function** if, for every $a \in A$, the set $\{c \in C : aRc\}$ contains exactly one element.

As in first-year mathematics, you may think of a function R from A to C as a machine ("black box") that, when fed *any* element $a \in A$, produces a *unique* element of C, usually denoted by $R(a)$. Thus $R(a)$ is the unique element of C for which aRc. We will adhere to the tradition according to which functions in calculus are typically denoted by lower case characters such as f, g, etc. To very carefully display a function f from A to C, we write

$$f : \left\{ \begin{array}{ccc} A & \to & C \\ a & \mapsto & f(a) \end{array} \right.$$

but often we simply denote such a function as $f : A \to C$. The set A is called the **domain** of f, and C is its **codomain** (or **target**). The element $f(a) \in C$ can be thought of as the **value** of f at $a \in A$. An especially simple function, on any set A, is the **identity** (**function**) $\mathrm{id}_A : A \to A$, for which $\mathrm{id}_A(a) = a$ for all $a \in A$. Note that in accordance with the definition, we have to be very picky as to when we accept two functions $f : A \to C$ and $g : B \to D$ as being equal: As they are both relations, $f = g$ really means that

$$A = B \quad \wedge \quad C = D \quad \wedge \quad f(a) = g(a)\ \forall a \in A = B\,.$$

If $f : A \to C$ and $B \subset A$ then f, considered as a relation from A to C, can be restricted to B, and the resulting relation $f|_B$ is easily seen to be again a *function* from B to C, not surprisingly referred to as the **restriction** of f to B.

Let $f : A \to C$ be a function. For every $B \subset A$, the set

$$f(B) := \{f(b) : b \in B\} \subset C$$

is the **image** of B under f, and for every $D \subset C$, the set

$$f^{-1}(D) := \{a \in A : f(a) \in D\} \subset A$$

is the **pre-image** of D under f. Clearly $f(\varnothing) = f^{-1}(\varnothing) = \varnothing$. Note that f^{-1} may not be a function, in which case $f^{-1}(c)$, unlike $f^{-1}(\{c\})$, may be a meaningless expression. In other words, f^{-1} may make sense only as a *relation* from C to A.

An important aspect of functions is that they can, under appropriate circumstances, be concatenated. Specifically, given functions $f : A \to C$ and $g : D \to F$ with $f(A) \subset D$, a new function, the **composition** of g with f, is defined as

$$g \circ f : \left\{ \begin{array}{ccc} A & \to & F \\ a & \mapsto & g\big(f(a)\big) \end{array} \right.$$

Note that implicit in the usage of the symbol $g \circ f$ is the fact that f is "applied first" and g is "applied last". Also, $f \circ g$ is not defined unless $g(D) \subset A$.

A function $f : A \to C$ is **one-to-one** if $f(a) = f(b)$ for $a, b \in A$ implies that $a = b$, or equivalently, if $f^{-1}(\{c\})$ contains, for every $c \in C$, *at most* one element of A. (In this case, the restriction of f^{-1} to $f(A)$ is a function.) On the other hand, $f : A \to C$ is **onto** if $f(A) = C$, or equivalently, if $f^{-1}(\{c\})$ contains, for every $c \in C$, *at least* one element of A. A function that is both one-to-one and onto is also called a **bijection**. For a bijection $f : A \to C$, the relation f^{-1} is actually a function from C to A, and $f^{-1} \circ f = \mathrm{id}_A$ as well as $f \circ f^{-1} = \mathrm{id}_C$. If $f : A \to C$ is a bijection then, as far as their set-theoretic properties are concerned, the sets A and C are really "the same", up to a "re-labelling" of elements brought about by f. More formally, the relation

$$B \sim D \ :\Leftrightarrow\ \exists \text{ a bijection } g : B \to D$$

is an equivalence relation, and $A \sim C$ by means of f.

Example 8. You probably have seen many functions in first-year mathematics, and you certainly will see many more soon. To emphasize that the properties of a function depend also on its domain and target, consider

$$f : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, \ldots\} \\ k & \mapsto & k^2 \end{array} \right.$$

Since $f(-1) = f(1)$, the function f is not one-to-one. As $2 \notin f(\mathbb{Z})$, it is not onto either. For convenience, let $C := f(\mathbb{Z}) = \{k^2 : k \in \mathbb{Z}\} = \{0, 1, 4, 9, 16, \ldots\}$. The function $f|_{\mathbb{N}_0}$, that is

$$f|_{\mathbb{N}_0} : \left\{ \begin{array}{ccc} \mathbb{N}_0 & \to & \mathbb{N}_0 \\ n & \mapsto & n^2 \end{array} \right.$$

is one-to-one but not onto since $f|_{\mathbb{N}_0}(\mathbb{N}_0) = C \subsetneq \mathbb{N}_0$. On the other hand, the function

$$g : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & C \\ k & \mapsto & k^2 \end{array} \right.$$

is clearly onto while failing to be one-to-one. Finally, the restriction of g to $\mathbb{N}_0$ is a bijection from $\mathbb{N}_0$ to C.

Since $\mathbb{N}_0 \subset \mathbb{Z}$, compositions such as $f \circ f$ and $f \circ f \circ f := f \circ (f \circ f)$ are defined. They are given, respectively, by

$$f \circ f : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{N}_0 \\ k & \mapsto & k^4 \end{array} \right. \quad \text{and} \quad f \circ f \circ f : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{N}_0 \\ k & \mapsto & k^8 \end{array} \right. .$$

Lemma 9. *Let $f : A \to C$ and $g : C \to F$ be functions. Then:*

(i) *If f and g are both one-to-one then $g \circ f$ is one-to one.*

(ii) *If f and g are both onto then $g \circ f$ is onto.*

(iii) *If f and g are both bijections then $g \circ f$ is a bijection.*

(iv) *If $g \circ f$ is one-to-one then f is one-to-one.*

(v) *If $g \circ f$ is onto then g is onto.*

(vi) *If $g \circ f$ is a bijection then f is one-to-one and g is onto.*

Proof. (i) Assume that $g \circ f(a) = g \circ f(b)$ for some a, b. Then $f(a) = f(b)$ because g is one-to-one, and hence $a = b$ as f is one-to-one also. Thus $g \circ f$ is one-to-one.

(ii) Observe first that generally, by definition,

$$g \circ f(A) = \{g \circ f(a) : a \in A\} = \big\{g\big(f(a)\big) : a \in A\big\} = \{g(c) : c \in f(A)\} = g\big(f(A)\big) .$$

With $f(A) = C$ and $g(C) = F$, it follows that $g \circ f(A) = g(C) = F$, i.e., $g \circ f$ is onto.

(iii) This is obvious from (i) and (ii).

(iv) Suppose f was not one-to-one. Then $f(a) = f(b)$ for some $a, b \in A$ with $a \neq b$. But then $g \circ f(a) = g \circ f(b)$, contradicting the fact that $g \circ f$ is one-to-one.

(v) Suppose g was not onto. Then $g(C) \subsetneq F$ and hence $g \circ f(A) = g\big(f(A)\big) \subset g(C) \subsetneq F$, which contradicts the fact that $g \circ f$ is onto.

(vi) This is clear from (iv) and (v). □

Recall that if $a, b \in A$ then the sets $\{a, b\}$, $\{a, a, b\}$ and $\{a, a, b, b\}$, for instance, are all identical. Thus, to select elements from a set *with repetitions being allowed* the concept of subsets is not appropriate. Functions can be used to elegantly overcome this problem. To see how, simply let I be a set and $a : I \to A$ a function, and write $a(i)$ as a_i. With this, a_i is, for every $i \in I$, an element of A, and we can have $a_i = a_j$ for as many different $i, j \in I$ as we like. Instead of $a : I \to A$, we write $(a_i)_{i \in I}$ and call it a **family** in A with **index set** I. The set of *all* families in A with index set I is denoted by A^I, i.e.

$$A^I = \{a : a \text{ is a function from } I \text{ to } A\} .$$

Note that if I has exactly two elements, e.g. $I = \{\heartsuit, \spadesuit\}$, then A^I is essentially the same as $A \times A$, or more formally, the function

$$f : \left\{ \begin{array}{ccc} A^I & \to & A \times A \\ a & \mapsto & \big(a(\heartsuit), a(\spadesuit)\big) \end{array} \right.$$

is a bijection. By analogy, we define, for every $n \in \mathbb{N}$,

$$A^n := \underbrace{A \times A \times \ldots \times A}_{n \text{ copies of } A} := A^{\{1,2,\ldots,n\}}\,.$$

Thus A^n is the set of all maps $a : \{1, 2, \ldots, n\} \to A$ or, up to a "re-labelling" of all elements by means of a bijection, the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in A$ for all $i = 1, 2, \ldots n$.

A very useful application of families pertains to subsets of a given set A. A family $(B_i)_{i\in I}$ of subsets of A is simply a map $B : I \to 2^A$, and the set-theoretic operations $\cup$ and $\cap$ can be extended to such families:

$$\bigcup_{i\in I} B_i := \{a \in A : a \in B_i \text{ for at least one } i \in I\}\,,$$
$$\bigcap_{i\in I} B_i := \{a \in A : a \in B_i \text{ for all } i \in I\}\,.$$

Finally, it is worth spelling out how functions interact with operations on (families of) sets.

Lemma 10. *Let $f : A \to C$ be a function, and $(B_i)_{i\in I}$ and $(D_j)_{j\in J}$ be families of subsets of A and C, respectively, with index sets I and J. Then:*

(i) $f\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f(B_i)$;

(ii) $f\left(\bigcap_{i\in I} B_i\right) \subset \bigcap_{i\in I} f(B_i)$;

(iii) $f^{-1}\left(\bigcup_{j\in J} D_j\right) = \bigcup_{j\in J} f^{-1}(D_j)$;

(iv) $f^{-1}\left(\bigcap_{j\in J} D_j\right) = \bigcap_{j\in J} f^{-1}(D_j)$.

Proof. (i) We show that the set on the left is contained in the one on the right, and vice versa. If $c \in f\left(\bigcup_{i\in I} B_i\right)$ then $c = f(a)$ for some $a \in \bigcup_{i\in I} B_i$. Hence $c = f(a) \in f(B_i)$ for some $i \in I$, that is, $c \in \bigcup_{i\in I} f(B_i)$. Conversely, if $c \in \bigcup_{i\in I} f(B_i)$ then $c \in f(B_i)$ for some $i \in I$, meaning that $c = f(a)$ for some $i \in I$ and $a \in B_i$. Thus $a \in \bigcup_{i\in I} B_i$, and so $c = f(a) \in f\left(\bigcup_{i\in I} B_i\right)$.

(ii) If $c \in f\left(\bigcap_{i\in I} B_i\right)$ then $c = f(a)$ where $a \in B_i$ for all $i \in I$. Consequently, $c = f(a) \in f(B_i)$ for all $i \in I$, that is, $c \in \bigcap_{i\in I} f(B_i)$. (Think of an example for which the reverse inclusion in (ii) does not hold.)

(iii) Observe that $a \in f^{-1}\left(\bigcup_{j\in J} D_j\right)$ if and only if $f(a) \in D_j$, or equivalently $a \in f^{-1}(D_j)$ for some $j \in J$, which in turn is equivalent to $a \in \bigcup_{j\in J} f^{-1}(D_j)$.

(iv) Analogously to (iii), $a \in f^{-1}\left(\bigcap_{j\in J} D_j\right)$ if and only if $f(a) \in D_j$, or equivalently $a \in f^{-1}(D_j)$ for all $j \in J$, and the latter is equivalent to $a \in \bigcap_{j\in J} f^{-1}(D_j)$. □

Groups

Let G be a set. A function from $G \times G$ to G is also called a **binary operation** on G. Usually, symbols like $*$, $\circ$, etc. are used to denote binary operations, and the value of $*$, say,

at $(a,b) \in G \times G$ is denoted by $a*b$, instead of the correct but prohibitively clumsy $*\big((a,b)\big)$. Binary operations abound in mathematics. Some sets have more than one natural binary operation defined on them. However, a most fundamental concept involving *one* binary operation is the following.

Definition 11. A **group** is a set G, together with a binary operation $*$, a function $i_G : G \to G$, and a distinguished element $e_G \in G$ such that:

(i) The operation $*$ is **associative**, that is,

$$(a*b)*c = a*(b*c) \quad \forall a,b,c \in G\,;$$

(ii) The element e_G is (**left-**)**neutral**, that is,

$$e_G * a = a \quad \forall a \in G\,;$$

(iii) For every $a \in G$, the element $i_G(a)$ is (**left-**)**inverse** to a, that is,

$$i_G(a) * a = e_G \quad \forall a \in G\,.$$

A group is **Abelian** (or **commutative**) if, in addition,

(iv) The operation $*$ is commutative, that is,

$$a*b = b*a \quad \forall a,b \in G\,.$$

Traditionally, groups are denoted by upper case characters G, H, etc., and we will adhere to this tradition. If precision is important, a group will be referred to in the form $(G, *, i_G, e_G)$, but often the ingredients i_G and e_G, and perhaps even $*$, will be clear from the context or not specifically relevant, in which case we will use short phrases like "Let $(G,*)$ be a group" or "For every group G" etc.

The axioms of a group have been chosen in a minimalist way and may not appear substantial. However, many other properties can be derived from them. Here are a few simple consequences. Throughout, let $(G, *, i_G, e_G)$ be a group.

(v) By associativity, brackets do not matter at all and therefore will not be used, except where they increase readability. For instance, given any $a,b,c,d \in G$,

$$\big(a*(b*c)\big)*d = \big((a*b)*c\big)*d = (a*b)*(c*d) = a*\big(b*(c*d)\big) = a*\big((b*c)*d\big)\,.$$

Thus the expression $a*b*c*d$ is defined unambiguously.

(vi) For every $a \in G$, the element $i_G(a)$ is also right-inverse, that is,

$$a * i_G(a) = e_G \quad \forall a \in G\,.$$

Indeed, for every $a \in G$,

$$\begin{aligned} a * i_G(a) &= e_G * a * i_G(a) = i_G\big(i_G(a)\big) * i_G(a) * a * i_G(a) = i_G\big(i_G(a)\big) * e_G * i_G(a) \\ &= i_G\big(i_G(a)\big) * i_G(a) = e_G\,. \end{aligned}$$

(vii) The element e_G is also right-neutral, that is,

$$a * e_G = a \quad \forall a \in G\,.$$

With (vi), this follows immediately from

$$a * e_G = a * i_G(a) * a = e_G * a = a \quad \forall a \in G\,.$$

(viii) The element e_G is the only left-neutral element in G since if $\widetilde{e}_G$ is also left-neutral then, with (vii), $\widetilde{e}_G = \widetilde{e}_G * e_G = e_G$.

(ix) For every $a \in G$, the element $i_G(a)$ is the only element of G that is left-inverse to a, since if $j \in G$ is also left-inverse to a then

$$j = j * e_G = j * a * i_G(a) = e_G * i_G(a) = i_G(a)\,.$$

To summarize, every group G contains a uniquely determined element e_G, referred to as the **neutral element** of G, which is both left- and right-neutral. Moreover, for every $a \in G$ there is a unique element $i_G(a)$ which is both left- and right-inverse to a. It is common practice to write $i_G(a)$ as a^{-1} and refer to it as the **inverse** of $a \in G$. As (vi) has shown, $(a^{-1})^{-1} = a$ for every $a \in G$. Two more simple consequences of the group axioms are as follows:

(x) If $a, b \in G$ then $b^{-1} * a^{-1} * a * b = b^{-1} * e_G * b = b^{-1} * b = e_G$, showing that

$$(a * b)^{-1} = b^{-1} * a^{-1} \quad \forall a, b \in G\,.$$

(xi) Given any $a, b \in G$, there exists a unique $x \in G$ with $a * x = b$, and a unique $y \in G$ satisfying $y * a = b$.

To see this, simply note that $x = a^{-1} * b$ solves $a * x = b$, and

$$x = e_G * x = a^{-1} * a * x = a^{-1} * b$$

shows that it is indeed the only solution. The claim regarding y is proved completely analogously.

Example 12. (i) The set $\mathbb{Z}$ of integers with the usual addition is an Abelian group, with neutral element $e_{\mathbb{Z}} = 0$ and inverses $k^{-1} = -k$.

(ii) Recall the definition of $\mathbb{Z}_n$ from Example 4. You may want to confirm that

$$[k]_{\equiv_n} \oplus [l]_{\equiv_n} := [k + l]_{\equiv_n} \quad \forall k, l \in \mathbb{Z}$$

is a binary operation on $\mathbb{Z}_n$ that turns the latter into an Abelian group, with neutral element $e_{\mathbb{Z}_n} = [0]_{\equiv_n}$, and inverses $([k]_{\equiv_n})^{-1} = [-k]_{\equiv_n}$.

(iii) On $\mathbb{Z}$, the usual multiplication is an associative and commutative binary operation, and 1 is a neutral element. Clearly, $(\mathbb{Z}, \cdot)$ is not a group, as $0 \cdot k = 0$ for every $k \in \mathbb{Z}$, and

hence 0 does not have an inverse. Note that with $G := \mathbb{Z}\backslash\{0\}$, the usual multiplication still is an associative and commutative binary operation on G. However, $(G, \cdot)$ is not a group either as $2 \in G$ for instance does not have an inverse. On the other hand, $(\{-1, 1\}, \cdot)$ is a group.

(iii) Let $A \neq \varnothing$ be a set. Denote by $\pi(A)$ the set of all bijections from A to itself, that is,

$$\pi(A) = \{f : A \to A : f \text{ is a bijection}\}.$$

The binary operation $f * g := g \circ f$ turns $\pi(A)$ into a group, with neutral element $e_{\pi(A)} = \mathrm{id}_A$ and inverses $i_{\pi(A)}(f) = f^{-1}$. Especially when A is finite, $\pi(A)$ is often referred to as the **group of permutations** of A. Observe that $(\pi(A), \circ)$ is Abelian precisely if A contains no more than two elements.

In view of the extremely important examples (i) and (ii) above, in an Abelian group G the binary operation is usually denoted by $+$, the neutral element by 0, and the inverse of $a \in G$ is written as $-a$.

Definition 13. Let $(G, *, i_G, e_G)$ be a group. A set $H \subset G$ is a **subgroup** of G if H is itself a group when endowed with the binary operation $*|_{H\times H}$.

Lemma 14. *Let G be a group, and $\varnothing \neq H \subset G$. Then H is a subgroup if and only if $a * b^{-1} \in H$ for every $a, b \in H$.*

Proof. Assume first that H is a subgroup. Since for every $b \in H$,

$$e_H = e_H * e_G = e_H * b * b^{-1} = b * b^{-1} = e_G,$$

$e_G \in H$, and if $c \in H$ is (left-)inverse to b then $c = c * e_G = c * b * b^{-1} = e_H * b^{-1} = e_G * b^{-1} = b^{-1}$. In other words, $b^{-1} \in H$ and therefore also $a * b^{-1} \in H$ whenever $a, b \in H$.

Conversely, with any $b \in H$, the elements $b * b^{-1} = e_G$ and $e_G * b^{-1} = b^{-1}$ also belong to H, which shows that H is a subgroup. □

As seen above, $e_G \in H$ whenever H is a subgroup of G. Every group containing more than one element has at least two subgroups, namely $\{e_G\}$ and G itself; they are sometimes referred to as **trivial** subgroups. Also, if G is Abelian then each of its subgroups is Abelian as well.

Example 15. (i) The set $2\mathbb{Z} := \{2k : k \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.

(ii) In every Abelian group $(G, +)$, the set $\{a \in G : a + a = 0\}$ is a subgroup. (Check this.)

(iii) Given any set $A \neq \varnothing$ and any $a \in A$, the set of bijections of A that leave a fixed, i.e.

$$\mathrm{Fix}_a := \{f : A \to A \text{ is a bijection with } f(a) = a\} \subset \pi(A),$$

is a subgroup of $(\pi(A), \circ)$.