Chapter 1
Set-Theoretic and Combinatorial Background

1.1 Sets and Maps

1.1.1 Sets

I have no desire to include a rigorous introduction to the theory of sets in this book. Perhaps what follows will motivate the interested reader to learn this theory in a special course on mathematical logic. In any case, the common intuitive understanding of a set as an abstract "aggregate of elements" is enough for our purposes. Any set can be imagined geometrically as a collection of points, and we will often refer to the elements of a set as points. By definition, all the elements of a set are distinct. A set X may be considered as having been adequately defined as soon as one can say that a given item is or is not an element of X. If x is an element of a set X, we write $x \in X$. Two sets are *equal* if they consist of the same elements. There is a unique set containing no elements. It is called the *empty set* and is denoted by $\varnothing$. For a finite set X, we write $|X|$ for the total number of elements in X and call it the *cardinality* of X. A set X is called a *subset* of a set Y if each element $x \in X$ also belongs to Y. In this case, we write $X \subset Y$. Note that $\varnothing$ is a subset of every set, and every set is a subset of itself. A subset of a set X that is not equal to X is said to be *proper*.

Exercise 1.1 How many subsets (including the set itself) are there in a finite set of cardinality n?

Given two sets X and Y, the *union* $X \cup Y$ consists of all elements belonging to at least one of them. The union of nonintersecting sets Y, Z is denoted by $Y \sqcup Z$ and called their *disjoint union*. The *intersection* $X \cap Y$ consists of all elements belonging to both sets X, Y simultaneously. The *set difference* $X \smallsetminus Y$ consists of all elements

A.L. Gorodentsev, *Algebra I*, DOI 10.1007/978-3-319-45285-2_1

that belong to X but not to Y. The *direct product*[1] $X \times Y$ consists of all ordered pairs (x, y), where $x \in X$, $y \in Y$.

Exercise 1.2 Check that the intersection can be expressed in terms of the difference as $X \cap Y = X \smallsetminus (X \smallsetminus Y)$. Is it possible to express the difference in terms of the intersection and union?

1.1.2 Maps

A *map* (or *function*) $f : X \to Y$ from a set X to a set Y is an assignment $x \mapsto f(x)$ that relates each point $x \in X$ with some point $y = f(x) \in Y$ called the *image* of x under f or the *value* of f at x. Note that y must be uniquely determined by x and f. Two maps $f : X \to Y$ and $g : X \to Y$ are said to be *equal* if $f(x) = g(x)$ for all $x \in X$. We write $\mathrm{Hom}(X, Y)$ for the set of all maps $X \to Y$.

All points $x \in X$ sent by the map $f : X \to Y$ to a given point $y \in Y$ form a subset of X denoted by

$$f^{-1}(y) \stackrel{\text{def}}{=} \{x \in X \mid f(x) = y\}$$

and called the *preimage* of y under f or the *fiber* of f over y. The preimages of distinct points are disjoint and may consist of arbitrarily many points or even be empty. The points $y \in Y$ with a nonempty preimage form a subset of Y called the *image* of f and denoted by

$$\mathrm{im}(f) \stackrel{\text{def}}{=} \{y \in Y \mid f^{-1}(y) \neq \varnothing\} = \{y \in Y \mid \exists\, x \in X : f(x) = y\}\,.$$

A map $f : X \to Y$ is called *surjective* (or an *epimorphism*) if the preimage of every point $y \in Y$ is nonempty, i.e., if $\mathrm{im}(f) = Y$. We designate a surjective map by a two-headed arrow $X \twoheadrightarrow Y$. A map f is called *injective* (or a *monomorphism*) if the preimage of every point $y \in Y$ contains at most one element, i.e., $f(x_1) \neq f(x_2)$ for all $x_1 \neq x_2$. Injective maps are designated by a hooked arrow $X \hookrightarrow Y$.

Exercise 1.3 List all maps $\{0, 1, 2\} \to \{0, 1\}$ and all maps $\{0, 1\} \to \{0, 1, 2\}$. How many epimorphisms and monomorphisms are there among them in each case?

A map $f : X \to Y$ is called *bijective* or an *isomorphism* if it is simultaneously surjective and injective. This means that for every $y \in Y$, there exists a unique $x \in X$ such that $f(x) = y$. For this reason, a bijection is also called a *one-to-one*

[1] Also called the *Cartesian product* of sets.

correspondence between X and Y. We designate a bijection by an arrow with a tilde over it: $X \xrightarrow{\sim} Y$.

Exercise 1.4 Indicate all bijections, injections, and surjections among the following maps: **(a)** $\mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$, **(b)** $\mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$, **(c)** $\mathbb{Z} \to \mathbb{Z}$, $x \mapsto 7x$, **(d)** $\mathbb{Q} \to \mathbb{Q}$, $x \mapsto 7x$.

A map from X to itself is called an *endomorphism* of X. We write $\operatorname{End}(X) \stackrel{\text{def}}{=} \operatorname{Hom}(X, X)$ for the set of all endomorphisms of X. Bijective endomorphisms $X \xrightarrow{\sim} X$ are called *automorphisms* of X. We denote the set of all automorphisms by $\operatorname{Aut}(X)$. One can think of an automorphism $X \xrightarrow{\sim} X$ as a permutation of the elements of X. The trivial permutation $\operatorname{Id}_X : X \to X$, $x \mapsto x$, which takes each element to itself, is called the *identity map*.

Exercise 1.5 (Dirichlet's Principle) Convince yourself that the following conditions on a set X are equivalent: **(a)** X is infinite; **(b)** there exists a nonsurjective injection $X \hookrightarrow X$; **(c)** there exists a noninjective surjection $X \twoheadrightarrow X$.

Exercise 1.6 Show that $\operatorname{Aut}(\mathbb{N})$ is an uncountable set.[2]

Example 1.1 (Recording Maps by Words) Given two finite sets $X = \{1, 2, \dots, n\}$, $Y = \{1, 2, \dots, m\}$, every map $f : X \to Y$ can be represented by a sequence of its values $w(f) \stackrel{\text{def}}{=} (f(1), f(2), \dots, f(n))$ viewed as an n-letter word in the m-letter alphabet Y. For example, the maps $f : \{1, 2\} \to \{1, 2, 3\}$ and $g : \{1, 2, 3\} \to \{1, 2, 3\}$ defined by the assignments $f(1) = 3, f(2) = 2$ and $g(1) = 1$, $g(2) = 2$, $g(3) = 2$ are represented by the words $w(f) = (3, 2)$ and $w(g) = (1, 2, 2)$ in the alphabet $\{1, 2, 3\}$. Therefore, we get the bijection

$$w : \operatorname{Hom}(X, Y) \xrightarrow{\sim} \{|X| - \text{ letter words in the alphabet Y}\}, \quad f \mapsto w(f).$$

This map takes monomorphisms to words without duplicate letters. Epimorphisms go to words containing the whole alphabet. Isomorphisms go to words in which every letter of the alphabet appears exactly once.

1.1.3 Fibers of Maps

A map $f : X \to Y$ decomposes X into the disjoint union of nonempty subsets $f^{-1}(y)$ indexed by the elements $y \in \operatorname{im}(f)$:

$$X = \bigsqcup_{y \in \operatorname{im}(f)} f^{-1}(y). \tag{1.1}$$

[2] A set is called *countable* if it is isomorphic to $\mathbb{N}$. An infinite set not isomorphic to $\mathbb{N}$ is called *uncountable*.

This viewpoint may be useful when we need to compare cardinalities of sets. For example, if all fibers of the map $f : X \to Y$ have the same cardinality $m = |f^{-1}(y)|$, then

$$|X| = m \cdot |\operatorname{im} f| . \tag{1.2}$$

Proposition 1.1 $|\mathrm{Hom}(X, Y)| = |Y|^{|X|}$ *for all finite sets X, Y.*

Proof Fix an arbitrary point $x \in X$ and consider the *evaluation map*

$$\mathrm{ev}_x : \mathrm{Hom}(X, Y) \to Y , \quad f \mapsto f(x) , \tag{1.3}$$

which takes the map $f : X \to Y$ to its value at x. The maps $X \to Y$ with a prescribed value at x are in bijection with the maps $X \smallsetminus \{x\} \to Y$. Thus, $|\mathrm{ev}_x^{-1}(y)| = |\mathrm{Hom}(X \smallsetminus \{x\}, Y)|$ for all $y \in Y$. Hence, $|\mathrm{Hom}(X, Y)| = |\mathrm{Hom}\,(X \smallsetminus \{x\}\,, Y)\,| \cdot |Y|$ by formula (1.2). In other words, when we add one more point to X, the cardinality of $\mathrm{Hom}(X, Y)$ is multiplied by $|Y|$. ◻

Remark 1.1 In the light of Proposition 1.1, the set of all maps $X \to Y$ is often denoted by

$$Y^X \stackrel{\text{def}}{=} \mathrm{Hom}(X, Y) .$$

Remark 1.2 In the above proof, we assumed that both sets are nonempty. If $X = \varnothing$, then for each Y, there exists just one map $\varnothing \hookrightarrow Y$, namely the empty map, which takes every element of X (of which there are none) to an arbitrary element of Y. In this case, the evaluation map (1.3) is not defined. However, Proposition 1.1 is still true: $1 = |Y|^0$. Note that $\mathrm{Hom}(\varnothing, \varnothing) = \{\mathrm{Id}_\varnothing\}$ has cardinality 1, i.e., $0^0 = 1$ in our current context. If $Y = \varnothing$, then $\mathrm{Hom}(X, \varnothing) = \varnothing$ for every $X \neq \varnothing$. This agrees with Proposition 1.1 as well: $0^{|X|} = 0$ for $|X| > 0$.

Proposition 1.2 *Let* $|X| = |Y| = n$*. We write* $\mathrm{Isom}(X, Y) \subset \mathrm{Hom}(X, Y)$ *for the set of all bijections* $X \xrightarrow{\sim} Y$*. Then* $|\mathrm{Isom}(X, Y)| = n!$*, where* $n! \stackrel{\text{def}}{=} n \cdot (n-1) \cdot (n-2) \cdots 1$*. In particular,* $|\mathrm{Aut}(X)| = n!$.

Proof For every $x \in X$, the restriction of the evaluation map (1.3) to the subset of bijections assigns the surjective map $\mathrm{ev}_x : \mathrm{Isom}(X, Y) \twoheadrightarrow Y$, $f \mapsto f(x)$. The bijections $f : X \xrightarrow{\sim} Y$ with a prescribed value $y = f(x)$ are in one-to-one correspondence with all bijections $X \smallsetminus \{x\} \to Y \smallsetminus \{y\}$. Since the cardinality of $\mathrm{Isom}(X \smallsetminus \{x\}, Y \smallsetminus \{y\})$ does not depend on x, y, we have $|\mathrm{Isom}(X, Y)| = |\mathrm{Isom}((X \smallsetminus \{x\}, Y \smallsetminus \{y\})| \cdot |Y|$ by formula (1.2). In other words, when we add one more point to both X and Y, the cardinality of $\mathrm{Isom}(X, Y)$ is multiplied by $|Y| + 1$. ◻

Remark 1.3 The product $n! = n \cdot (n-1) \cdot (n-2) \cdots 1$ is called *n-factorial*. Since $\mathrm{Aut}(\varnothing) = \{\mathrm{Id}_\varnothing\}$ has cardinality 1, we define $0! \stackrel{\text{def}}{=} 1$.

Example 1.2 (Multinomial Coefficients) To multiply out the expression $(a_1 + a_2 + \cdots + a_m)^n$, we may place the factors in a line:

$$(a_1 + a_2 + \cdots + a_m) \cdot (a_1 + a_2 + \cdots + a_m) \cdots (a_1 + a_2 + \cdots + a_m).$$

Then for each $i = 1, 2, \ldots, n$, we choose some letter a_{ν_i} within the ith pair of parentheses and form the word $a_{\nu_1} a_{\nu_2} \ldots a_{\nu_n}$ from them. After doing this in all possible ways, adding all the words together, and collecting like monomials, we get the sum

$$(a_1 + a_2 + \cdots + a_m)^n = \sum_{\substack{k_1+k_2+\cdots+k_m=n \\ \forall i,\ 0 \leqslant k_i \leqslant n}} \binom{n}{k_1, \ldots, k_m} \cdot a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}\,, \tag{1.4}$$

where each exponent k_i varies over the range $0 \leqslant k_i \leqslant n$, and the total degree of each monomial is equal to $n = k_1 + k_2 + \cdots + k_m$. The coefficient $\binom{n}{k_1, \ldots, k_m}$ of the monomial $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$ is called a *multinomial coefficient*. It equals the number of all n-letter words that can be written with exactly k_1 letters a_1, k_2 letters a_2, etc. To evaluate it precisely, write Y for the set of all such words. Then for each $i = 1, 2, \ldots, n$, mark the k_i identical letters a_i each with different upper index $1, 2, \ldots, k_i$ in order to distinguish these letters from one another. Now write X for the set of all n-letter words written with n distinct marked letters

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(k_1)}}_{k_1 \text{ marked letters } a_1}, \underbrace{a_2^{(1)}, a_2^{(2)}, \ldots, a_2^{(k_2)}}_{k_2 \text{ marked letters } a_2}, \ldots, \underbrace{a_m^{(1)}, a_m^{(2)}, \ldots, a_m^{(k_m)}}_{k_m \text{ marked letters } a_m}$$

and containing each letter exactly once. We know from Proposition 1.2 that $|X| = n!$. Consider the *forgetful surjection* $f : X \twoheadrightarrow Y$, which erases all the upper indices. The preimage of every word $y \in Y$ under this map consists of the $k_1! \cdot k_2! \cdots k_m!$ words obtained from y by marking the k_1 letters a_1, k_2 letters a_2, etc. with upper indices in all possible ways. (1.2) on p. 4 leads to

$$\binom{n}{k_1, \ldots, k_m} = \frac{n!}{k_1! \cdot k_2! \cdots k_m!}\,. \tag{1.5}$$

Thus, the expansion (1.4) becomes

$$(a_1 + a_2 + \cdots + a_m)^n = \sum_{\substack{k_1+\cdots+k_m=n \\ \forall i,\ 0 \leqslant k_i \leqslant n}} \frac{n! \cdot a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}}{k_1! \cdot k_2! \cdots k_m!}\,. \tag{1.6}$$

Exercise 1.7 How many summands are there on the right-hand side of (1.6)?

For $m = 2$, we get the following well-known formula[3]:

$$(a+b)^n = \sum_{k=0}^{n} \frac{n! \cdot a^k b^{n-k}}{k!(n-k)!} \,. \tag{1.7}$$

The *binomial coefficient* $\frac{n!}{k!(n-k)!}$ is usually denoted by either $\binom{n}{k}$ or C_n^k instead of $\binom{n}{k,n-k}$. We will use the notation $\binom{n}{k}$. Note that it can be written as

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k \cdot (k-1) \cdots 1} \,,$$

where both the numerator and denominator consist of k decreasing integer factors.

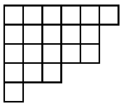
Example 1.3 (Young Diagrams) The decomposition of the finite set $X = \{1, 2, \dots, n\}$ into a disjoint union of nonempty subsets

$$X = X_1 \sqcup X_1 \sqcup X_2 \sqcup \cdots \sqcup X_k \tag{1.8}$$

can be encoded as follows. Renumber the subsets X_i in any nonincreasing order of their cardinalities and set $\lambda_i = |X_i|$. We obtain a nonincreasing sequence of integers

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n) \,, \quad \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k \,, \tag{1.9}$$

called a *partition* of $n = |X|$ or a *shape* of the decomposition (1.8). Partitions are visualized by diagrams like this:



(1.10)

Such a diagram is formed by cellular strips of lengths $\lambda_1, \lambda_2, \dots, \lambda_k$ aligned at the left and of nonincreasing length from top to bottom. It is called *a Young diagram* of the partition λ. We will make no distinction between a partition and its diagram and denote both by the same letter. The total number of cells in the diagram λ is called the *weight* and denoted by $|\lambda|$. The number of rows is called the *length* of the

[3]This is a particular case of the generic *Newton's binomial theorem*, which expands $(1+x)^s$ with an arbitrary α. We will prove it in Sect. 1.2.

diagram and denoted by $\ell(\lambda)$. Thus, the Young diagram (1.10) depicts the partition $\lambda = (6, 5, 5, 3, 1)$ of weight $|\lambda| = 20$ and length $\ell(\lambda) = 5$.

Exercise 1.8 How many Young diagrams can be drawn within a $k \times n$ rectangle?[4]

If we fill the cells of λ by the elements of X (one element per cell) and combine the elements placed in row i into one subset $X_i \subset X$, then we obtain the decomposition (1.8) of shape λ. Since every decomposition of shape λ can be achieved in this way from an appropriate filling, we get a surjective map from the set of all fillings of λ to the set of all decompositions (1.8) of shape λ. All the fibers of this map have the same cardinality. Namely, two fillings produce the same decomposition if and only if they are obtained from each other either by permuting elements within rows or by permuting entire rows of equal length. Let us write m_i for the number of rows of length[5] i in λ. By Proposition 1.2, there are $\prod \lambda_i! = \prod_{i=1}^{n} (i!)^{m_i}$ permutations of the first type and $\prod_{i=1}^{n} m_i!$ permutations of the second type. Since they act independently, each fiber has cardinality $\prod_{i=1}^{n} (i!)^{m_i} m_i!$. Therefore, $n!$ fillings produce

$$\frac{n!}{\prod_{i=1}^{n} m_i! \cdot (i!)^{m_i}} \tag{1.11}$$

different decompositions of a set of cardinality n into a disjoint union of m_1 elements, m_2 subsets of cardinality 2, m_3 subsets of cardinality 3, etc.

1.2 Equivalence Classes

1.2.1 Equivalence Relations

Another way of decomposing X into a disjoint union of subsets is to declare the elements in each subset to be *equivalent*. This can be formalized as follows. A subset $R \subset X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\}$ is called a *binary relation* on X. If $(x_1, x_2) \in R$, we write $x_1 \sim_R x_2$ and say that R relates x_1 with x_2. We omit the letter R from this notation when R is clear from context or is inessential.

For example, the following binary relations on the set of integers $\mathbb{Z}$ are commonly used:

$$\textit{equality} : x_1 \sim x_2, \text{ meaning that } x_1 = x_2; \tag{1.12}$$

$$\textit{inequality} : x_1 \sim x_2, \text{ meaning that } x_1 \leqslant x_2; \tag{1.13}$$

[4] The upper left-hand corner of each diagram should coincide with that of the rectangle. The empty diagram and the whole rectangle are allowed.

[5] Note that the equality $|\lambda| = n = m_1 + 2m_2 + \cdots + nm_n$ forces many of the m_i to vanish.

$$\textit{divisibility} : x_1 \sim x_2, \text{ meaning that } x_1 \mid x_2; \tag{1.14}$$

$$\textit{congruence modulo } n : x_1 \sim x_2, \text{ meaning that } x_1 \equiv x_2 \pmod{n}. \tag{1.15}$$

(The last of these is read "x_1 is congruent to x_2 modulo n" and signifies that n divides $x_1 - x_2$.)

Definition 1.1 A binary relation $\sim$ is called an *equivalence relation* or simply an *equivalence* if it satisfies the following three properties:

$$\begin{aligned} \textit{reflexivity}: &\ \forall\, x \in X, \quad x \sim x\,; \\ \textit{transitivity}: &\ \forall\, x_1, x_2, x_3 \in X, \quad x_1 \sim x_2 \ \&\ x_2 \sim x_3 \quad \Rightarrow \quad x_1 \sim x_3\,; \\ \textit{symmetry}: &\ \forall\, x_1, x_2 \in X, \quad x_1 \sim x_2 \iff x_2 \sim x_1\,. \end{aligned}$$

In the above list of binary relations on $\mathbb{Z}$, (1.12) and (1.15) are equivalences. Relations (1.13) and (1.14) are not symmetric.[6]

If X is decomposed into a disjoint union of subsets, then the relation $x_1 \sim x_2$, meaning that x_1, x_2 belong to the same subset, is an equivalence relation. Conversely, given an equivalence relation R on X, let us introduce the notion of an *equivalence class* of x as

$$[x]_R \stackrel{\text{def}}{=} \{z \in X \mid x \sim_R z\} = \{z \in X \mid z \sim_R x\}\,,$$

where the second equality holds because R is symmetric.

Exercise 1.9 Verify that any two classes $[x]_R$, $[y]_R$ either coincide or are disjoint.

Thus, X decomposes into a disjoint union of distinct equivalence classes. The set of these equivalence classes is denoted by X/R and called the *quotient* or *factor set* of X by R. The surjective map sending an element to its equivalence class,

$$f : X \twoheadrightarrow X/R\,, \quad x \mapsto [x]_R\,, \tag{1.16}$$

is called the *quotient map* or *factorization map*. Its fibers are exactly the equivalence classes. Every surjective map $f : X \twoheadrightarrow Y$ is the quotient map modulo the equivalence defined by $x_1 \sim x_2$ if $f(x_1) = f(x_2)$.

Example 1.4 (Residue Classes) Fix a nonzero $n \in \mathbb{Z}$ and write $\mathbb{Z}/(n)$ for the quotient of $\mathbb{Z}$ modulo the congruence relation (1.15). The elements of $\mathbb{Z}/(n)$ are called *residue classes* modulo n. The class of a number $z \in \mathbb{Z}$ is denoted by $[z]_n$ or simply by $[z]$ when the value of n is clear from context or is inessential.

[6] They are *skew-symmetric*, i.e., they satisfy the condition $x_1 \sim x_2 \ \&\ x_2 \sim x_1 \Rightarrow x_1 = x_2$; see Sect. 1.4 on p. 13.

The factorization map

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n), \quad z \mapsto [z]_n,$$

is called *reduction modulo n*. The set $\mathbb{Z}/(n)$ consists of the n elements $[0]_n, [1]_n, \dots, [n-1]_n$, in bijection with the residues of division by n. However, it may sometimes be more productive to think of residue classes as subsets in $\mathbb{Z}$, because this allows us to vary the representation of an element depending on what we need. For example, the residue of division of 12^{100} by 13 can be evaluated promptly as follows:

$$\left[12^{100}\right]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = \left[(-1)^{100}\right]_{13} = [1]_{13}.$$

Exercise 1.10 Prove the consistency of the above computation, i.e., verify that the residue classes $[x+y]_n$ and $[xy]_n$ do not depend on the choice of elements $x \in [x]_n$ and $y \in [y]_n$ used in their representations.

Thus, the quotient set $\mathbb{Z}/(n)$ has a well-defined addition and multiplication given by

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n, \quad [x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n. \tag{1.17}$$

1.2.2 Implicitly Defined Equivalences

Given a family of equivalence relations $R_\nu \subset X \times X$, the intersection $\bigcap R_\nu \subset X \times X$ is again an equivalence relation. Indeed, if each set $R_\nu \subset X \times X$ contains the diagonal $\Delta = \{(x,x) \mid x \in X\} \subset X \times X$ (reflexivity), goes to itself under reflection $(x_1, x_2) \leftrightarrows (x_2, x_1)$ (symmetry), and contains for every pair of points $(x,y), (y,z) \in R_\nu$ the point (x,z) as well (transitivity), then the intersection $\bigcap R_\nu$ will inherit the same properties. Therefore, for every subset $S \subset X \times X$, there exists a unique equivalence relation $\overline{S} \supset S$ contained in all equivalence relations containing S. It is called the equivalence relation *generated* by S and can be described as the intersection of all equivalence relations containing S. A more constructive description is given in the next exercise.

Exercise 1.11 Check that x is related to y by $\overline{R}$ if and only if there exists a finite sequence of points $x = z_0, z_1, z_2, \dots, z_n = y$ in X such that for each $i = 1, 2, \dots, n$, either (x_{i-1}, x_i) or (x_i, x_{i-1}) belongs to R.

However, such an implicit description may be quite ineffective even for understanding whether there are any inequivalent points at all.

Example 1.5 (Fractions) The set of rational numbers $\mathbb{Q}$ is usually introduced as the set of *fractions* a/b, where $a, b \in \mathbb{Z}$, $b \neq 0$. By definition, such a fraction is an equivalence class of the pair $(a,b) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus 0)$ modulo the equivalence generated by the relations

$$(a, b) \sim (ac, bc) \quad \text{for all } c \in \mathbb{Z} \smallsetminus 0\,, \tag{1.18}$$

which assert the equality of the fractions $a/b = (ac)/(bc)$. The relations (1.18) do not themselves form an equivalence relation. Indeed, if $a_1b_2 = a_2b_1$, then the leftmost element in the two-step chain

$$(a_1, b_1) \sim (a_1b_2, b_1b_2) = (a_2b_1, b_1b_2) \sim (a_2, b_2)$$

may not be related to the rightmost one directly by (1.18). For example, $3/6$ and $5/10$ produce equal fractions and are not directly related. Thus, the equivalence generated by (1.18) must contain the relations

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{for all} \quad a_1b_2 = a_2b_1\,. \tag{1.19}$$

Exercise 1.12 Verify that the relations (1.19) are reflexive, symmetric, and transitive.

Hence, relations (1.19) give a complete explicit description for the equivalence generated by relations (1.18).

1.3 Compositions of Maps

1.3.1 Composition Versus Multiplication

A *composition* of maps $F : X \to Y$ and $g : Y \to Z$ is a map

$$g \circ f : X \to Z\,, \quad x \mapsto g\big(f(x)\big)\,.$$

The notation $g \circ f$ is usually shorted to gf, which should not be confused with a product of numbers. In fact, the algebraic properties of compositions differ from those used in numeric computations. The composition of maps is not commutative: $fg \neq gf$ in general. When fg is defined, gf may not be. Even if both compositions are well defined, say for endomorphisms $f, g \in \mathrm{End}(X)$ of some set X, the equality $fg = gf$ usually fails.

Exercise 1.13 Let two lines ℓ_1, ℓ_2 in the plane cross at the point O. Write σ_1 and σ_2 for the reflections (i.e., axial symmetries) of the plane in these lines. Describe explicitly the motions $\sigma_1\sigma_2$ and $\sigma_2\sigma_1$. How should the lines be situated in order to get $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Cancellation of common factors also fails. Generically, neither $fg = fh$ nor $gf = hf$ implies $g = h$.

Example 1.6 (Endomorphisms of a Two-Element Set) The set $X = \{1, 2\}$ has four endomorphisms. Let us record maps $f : X \to X$ by two-letter words $(f(1), f(2))$ as in Example 1.1 on p. 3. Then the four endomorphisms X are $(1, 1)$,$(1, 2) = \mathrm{Id}_X$,$(2, 1)$,$(2, 2)$. The compositions fg are collected in the following multiplication table:

$f \diagdown g$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$
$(1,2)$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(2,1)$	$(2,2)$	$(2,1)$	$(1,2)$	$(1,1)$
$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$

(1.20)

Note that $(2, 2) \circ (1, 1) \neq (1, 1) \circ (2, 2)$, $(1, 1) \circ (1, 2) = (1, 1) \circ (2, 1)$, whereas $(1, 2) \neq (2, 1)$ and $(1, 1) \circ (2, 2) = (2, 1) \circ (2, 2)$, whereas $(1, 1) \neq (2, 1)$.

The only nice property of numeric multiplication shared by the composition of maps is *associativity*: $(hg)f = h(gf)$ for every triple of maps $f : X \to Y$, $g : Y \to Z$, $h : Z \to T$. Indeed, in each case, we have $x \mapsto h(g(f(x)))$.

Lemma 1.1 (Left Inverse Map) *The following conditions on a map $f : X \to Y$ are equivalent:*

1. *f is injective;*
2. *there exists a map $g : Y \to X$ such that $gf = \mathrm{Id}_X$ (any such g is called a left inverse to f);*
3. *for any two maps $g_1, g_2 : Z \to X$ such that $fg_1 = fg_2$, the equality $g_1 = g_2$ holds.*

Proof We verify the implications $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1)$. Let f be injective. For $y = f(x)$, put $g(y) = x$. For $y \notin \operatorname{im} f$, define $g(y)$ arbitrarily. Then $g : Y \to X$ satisfies (2). If (2) holds, then the left composition of both sides of the equality $fg_1 = fg_2$ with g leads to $g_1 = g_2$. Finally, if $f(x_1) = f(x_2)$ for some $x_1 \neq x_2$, then (3) is not satisfied for $g_1 = \mathrm{Id}_X$ and $g_2 : X \xrightarrow{\sim} X$ that swaps x_1, x_2 and leaves all the other points fixed. □

1.3.2 Right Inverse Map and the Axiom of Choice

A feeling of harmony calls for the right counterpart of Lemma 1.1. We expect that the following conditions on a map $f : X \to Y$ should be equivalent:

(1) f is surjective;
(2) there exists a map $g : Y \to X$ such that $fg = \mathrm{Id}_Y$;
(3) for any two maps $g_1, g_2 : Z \to X$ such that $g_1 f = g_2 f$, the equality $g_1 = g_2$ holds.

If these conditions hold, we shall call the map g from (2) a *right inverse* to f. Another conventional name for g is a *section* of the surjective map f, because every map g

satisfying (2) just selects some element $g(y) \in f^{-1}(y)$ in the fiber of f over each point $y \in Y$ simultaneously for all $y \in Y$. In rigorous set theory, which we try to avoid here, there is a special *selection axiom*, called the *axiom of choice*, postulating that every surjective map of sets admits a section. Thus, implication (1) $\Rightarrow$ (2) is part of the rigorous definition of a set. The proof of the implication (2) $\Rightarrow$ (3) is completely symmetric to the proof from Lemma 1.1: compose both sides of $g_1 f = g_2 f$ with g from the right and obtain $g_1 = g_2$. Implication (3) $\Rightarrow$ (1) is proved by contradiction: if $y \notin \operatorname{im} f$, then (1) fails for $g_1 = \mathrm{Id}_Y$ and every $g_2 : Y \to Y$ that takes y to some point in $\operatorname{im} f$ and leaves all other points fixed. Therefore, the above three properties, symmetric to those of Lemma 1.1, are equivalent as well.

1.3.3 Invertible Maps

If a map $f : X \xrightarrow{\sim} Y$ is bijective, then the preimage $f^{-1}(y) \subset X$ of a point $y \in Y$ consists of exactly one point. Therefore, the prescription $y \mapsto f^{-1}(y)$ defines a map $f^{-1} : Y \to X$ that is simultaneously a left and right inverse to f, i.e., it satisfies the equalities

$$f \circ f^{-1} = \mathrm{Id}_Y \quad \text{and} \quad f^{-1} \circ f = \mathrm{Id}_X . \tag{1.21}$$

The map f^{-1} is called a (*two-sided*) *inverse* to f.

Proposition 1.3 *The following properties of a map $f : X \to Y$ are equivalent:*

(1) *f is bijective;*
(2) *there exists a map $g : Y \to X$ such that $f \circ g = \mathrm{Id}_Y$ and $g \circ f = \mathrm{Id}_X$;*
(3) *there exist maps $g', g'' : Y \to X$ such that $g' \circ f = \mathrm{Id}_X$ and $f \circ g'' = \mathrm{Id}_Y$.*

If f satisfies these properties, then $g = g' = g'' = f^{-1}$, where f^{-1} is the map defined before formula (1.21).

Proof If (1) holds, then $g = f^{-1}$ satisfies (2). Implication (2) $\Rightarrow$ (3) is obvious. Conversely, if (3) holds, then $g' = g' \circ \mathrm{Id}_Y = g' \circ (f \circ g'') = (g' \circ f) \circ g'' = \mathrm{Id}_X \circ g'' = g''$. Therefore, (2) holds for $g = g' = g''$. Finally, let (2) hold. Then for every $y \in Y$, the preimage $f^{-1}(y)$ contains $g(y)$, because $f(g(y)) = y$. Moreover, every $x \in f^{-1}(y)$ equals $g(y)$: $x = \mathrm{Id}_X(x) = g(f(x)) = g(y)$. Hence, f is bijective, and $g = f^{-1}$. □

1.3.4 Transformation Groups

Let X be an arbitrary set. A nonempty subset $G \subset \operatorname{Aut} X$ is called a *transformation group* of X if $\forall\, g_1, g_2 \in G$, $g_1 g_2 \in G$ and $\forall\, g \in G$, $g^{-1} \in G$. Note that every transformation group automatically contains the identity map Id_X, because $\mathrm{Id}_X = g^{-1} g$ for every $g \in G$. For a finite transformation group G, its cardinality $|G|$ is called the *order* of G. Every transformation group $H \subset G$ is called a *subgroup* of G. Every transformation group is a subgroup of the group $\mathrm{Aut}(X)$ of all automorphisms of X.

Example 1.7 (Permutation Groups) For $X = \{1, 2, \dots, n\}$, the group $\mathrm{Aut}(X)$ is denoted by S_n and called the nth *symmetric group* or the *permutation group* of n elements. By Proposition 1.2, $|S_n| = n!$. We will indicate a permutation $\sigma \in S_n$ by the row $(\sigma_1, \sigma_2, \dots, \sigma_n)$ of its values $\sigma_i = \sigma(i)$, as in Example 1.1. For example,

$$\sigma = (3, 4, 2, 1) \quad \text{and} \quad \tau = (2, 3, 4, 1)$$

encode the maps

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 2 & 1 \end{array} \quad \text{and} \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

The compositions of these maps are recorded as $\sigma\tau = (4, 2, 1, 3)$ and $\tau\sigma = (4, 1, 3, 2)$.

Exercise 1.14 For the six elements of the symmetric group S_3, write a multiplication table similar to that from formula (1.20) on p. 11.

Example 1.8 (Abelian Groups) A group G in which every two elements $f, g \in G$ commute, i.e., satisfy the relation $fg = gf$, is called *commutative* or *abelian*. Examples of abelian groups are the group T of parallel displacements of the Euclidean plane and the group SO_2 of the rotations of the plane about some fixed point. For every integer $n \geqslant 2$, rotations by integer multiples of $2\pi/n$ form a finite subgroup of SO_2 called the *cyclic group* of order n.

1.4 Posets

1.4.1 Partial Order Relations

A binary relation[7] $x \leqslant y$ on a set Z is called a *partial order* if, like an equivalence relation, it is reflexive and transitive,[8] but instead of symmetric, it is *skew-symmetric*, which means that $x \leqslant y$ and $y \leqslant x$ imply $x = y$. If some partial order is given, we

[7] See Sect. 1.2 on p. 7.

[8] See Definition 1.1 on p. 8.

write $x < y$ if $x \leqslant y$ and $x \neq y$. A partial order on Z is called a *total order* if for all $x, y \in Z$, $x < y$ or $x = y$ or $y < x$ holds. For example, the usual inequality of numbers provides the set of integers $\mathbb{Z}$ with a total order, whereas the divisibility relation $n \mid m$, meaning that n divides m, is a partial but not total order on $\mathbb{Z}$. Another important example of a nontotal partial order is the one provided by inclusions on the set $\mathcal{S}(X)$ of all subsets in a given set X.

Exercise 1.15 (Preorder) Let a set Z be equipped with a reflexive transitive binary relation[9] $x \precsim y$. We write $x \sim y$ if both $x \precsim y$ and $y \precsim x$ hold simultaneously. Verify that $\sim$ is an equivalence relation and that on the quotient set $Z/\sim$, a partial order is well defined by the rule $[x] \leqslant [y]$ if $x \precsim y$.

A set P equipped with a partial order is called a *partially ordered set*, or *poset* for short. If the order is total, we say that P is totally ordered. Every subset X of a poset P is certainly a poset with respect to the order on P. Totally ordered subsets of a poset P are called *chains*. Elements $x, y \in Z$ are called *incompatible* if neither $x \leqslant y$ nor $y \leqslant x$ holds. Otherwise, x, y are said to be *compatible*. Thus, a partial order is total if and only if every two elements are compatible. Note that two incompatible elements have to be distinct.

A map $f : M \to N$ between two posets is called *order-preserving*[10] if for all $x, y \in M$, the inequality $x \leqslant y$ implies the inequality $f(x) \leqslant f(y)$. Posets M, N are said to be *isomorphic* if there is an order-preserving bijection $M \xrightarrow{\sim} N$. We write $M \simeq N$ in this case. A map f is called *strictly increasing* if for all $x, y \in M$, the inequality $x < y$ implies the inequality $f(x) < f(y)$. Every injective order-preserving map is strictly increasing. The converse is true for maps with totally ordered domain and may fail in general.

An element $y \in P$ is called an *upper bound* for a subset $X \subset P$ if $x \leqslant y$ for all $x \in X$. Such an upper bound is called *exterior* if $y \notin X$. In this case, the strong inequality $x < y$ holds for all $x \in X$.

An element $m^* \in X$ is called *maximal* in X if for all $x \in X$, the inequality $m^* \leqslant x$ implies $x = m^*$. Note that such an element may be incompatible with some $x \in X$, and therefore it is not necessarily an upper bound for X. A poset may have many different maximal elements or may not have any, like the poset $\mathbb{Z}$. If X is totally ordered, then the existence of a maximal element forces such an element to be unique. *Minimal elements* are defined symmetrically: $m_* \in X$ is called *minimal* if $\forall\, x \in X$, $m_* \leqslant x \Rightarrow x = m_*$, and the above discussion for maximal elements carries over to minimal elements with the obvious changes.

[9]Every such relation is called *a partial preorder* on $\mathbb{Z}$.

[10]Also *nondecreasing* or *nonstrictly increasing* or a *homomorphism of posets*.

1.4.2 Well-Ordered Sets

A totally ordered set W is called *well ordered* if every subset $U \subset W$ has a minimal element.[11] For example, the set $\mathbb{N}$ of positive integers is well ordered by the usual inequality between numbers. All well-ordered sets share one of the most important properties of the positive integers: they allow proofs by induction. If some statement $\Sigma = \Sigma(w)$ depends on an element w running through a well-ordered set W, then $\Sigma(w)$ holds for all $w \in W$ as soon the following two statements are proven:

(1) $\Sigma(w_*)$ holds for the minimal element w_* of W;
(2) for every $x \in W$, if $\Sigma(w)$ holds for all $w < x$, then $\Sigma(x)$ holds.

This is known as the *principle of transfinite induction*.

Exercise 1.16 Verify the principle of transfinite induction.

Let us write $[y) \stackrel{\text{def}}{=} \{w \in W \mid w < y\}$ for the set of all elements strictly preceding y in a well-ordered set W and call it the *initial segment* of W preceding y. Note that y is uniquely determined by $[y)$ as the minimal element in $W \smallsetminus [y)$. For the minimal element w_* of the whole of W, we set $[w_*) \stackrel{\text{def}}{=} \varnothing$. We write $U \leqslant W$ if $U \simeq [w)$ for some $w \in W$, and write $U < W$ if $U \leqslant W$ and $U \not\simeq W$. As good training in the use of the principle of transfinite induction, I strongly recommend the following exercise.

Exercise 1.17 For any two-well ordered sets U, W, either $U < W$ or $U \simeq W$ or $W < U$ holds.

Classes of isomorphic well-ordered sets are called *cardinals*. Thus, the set $\mathbb{N}$ can be identified with the set of all finite cardinals. All the other cardinals, including $\mathbb{N}$ itself, are called *transfinite*.

1.4.3 Zorn's Lemma

Let P be a poset. We write $\mathcal{W}(P)$ for the set of all well-ordered (by the partial order on P) subsets $W \subset P$. Certainly, $\mathcal{W}(P) \neq \varnothing$, because all one-point subsets of P are within $\mathcal{W}(P)$. We also include $\varnothing$ as an element of $\mathcal{W}(P)$.

Lemma 1.2 *For every poset P, there is no map $\beta : \mathcal{W}(P) \to P$ sending each $W \in \mathcal{W}(P)$ to some exterior upper bound of W.*

Proof Let such a map β exist. We will say that $W \in \mathcal{W}(P)$ is β-stable if $\beta([y)) = y$ for all $y \in W$. For example, the set $\big\{\beta(\varnothing),\ \beta\big(\{\beta(\varnothing)\}\big),\ \beta\big(\{\beta(\varnothing),\ \beta(\{\beta(\varnothing)\})\}\big)\big\}$ is β-stable, and it certainly can be enlarged by any amount to the right. For any two β-stable sets $U, W \in \mathcal{W}(P)$ with common minimal element, either $U \subset W$ or $W \subset U$

[11] Such an element is unique, as we have seen above.

holds, because the minimal elements $u \in U \smallsetminus (U \cap W)$ and $w \in W \smallsetminus (U \cap W)$ are each the β-image of the same initial segment $[u) = [w) \subset U \cap W$ and therefore must be equal.

Exercise 1.18 Check that the union of all β-stable sets having the same minimal element $p \in P$ is well ordered and β-stable.

Let U be some union from Exercise 1.18. Then $\beta(U)$ cannot be an exterior upper bound for U, because otherwise, $U \cup \{\beta(U)\}$ would be a β-stable set with the same minimal point as U, which forces it to be a subset of U. Contradiction. □

Corollary 1.1 (Zorn's Lemma I) *Suppose that every well-ordered subset in a poset P has an upper bound, not necessarily exterior. Then there exists a maximal element in P.*

Proof Assume the contrary. Then for all $x \in P$ there exists $y > x$. Hence, the axiom of choice allows us to choose some *exterior* upper bound[12] $b(W)$ for every $W \in \mathcal{W}(P)$. The resulting map $W \mapsto b(W)$ contradicts Lemma 1.2. □

Exercise 1.19 (Bourbaki–Witt Fixed-Point Lemma) Under the assumption of Corollary 1.1, show that every map $f : P \to P$ such that $f(x) \geqslant x$ for all $x \in X$ has a fixed point, i.e., that there exists $p \in P$ such that $f(p) = p$.

Definition 1.2 (Complete Posets) A partially ordered set is said to be *complete* if every totally ordered (with respect to the order on P) subset in P has an upper bound, not necessarily exterior.

Lemma 1.3 (Zorn's Lemma II) *Every complete poset P has a maximal element.*

Proof Every complete poset surely satisfies the assumption of Corollary 1.1. □

Problems for Independent Solution to Chap. 1

Problem 1.1 Find the total number of maps from a set of cardinality 6 to a set of cardinality 2 such that every point of the target set has at least two elements in its preimage.

Problem 1.2 Let X, Y be finite sets, $|X| \geqslant |Y|$. How many right inverse maps does a given surjection $X \twoheadrightarrow Y$ have? How many left inverse maps does a given injection $Y \hookrightarrow X$ have?

---

[12]To be more precise (see Sect. 1.3.2 on p. 11), let $I \subset \mathcal{W} \times P$ consist of all pairs (W, c) such that $w < c$ for all $w \in W$. Then the projection $\pi_1 : I \to \mathcal{W}$, $(W, c) \mapsto W$, is surjective, because by the assumption of the lemma, for every W, there exists some upper bound d, and then we have assumed that there exists some $c > d$. Take $b : \mathcal{W} \to P$ to be the composition $\pi_2 \circ g$, where $g : \mathcal{W} \to I$ is any section of π_1 followed by the projection $\pi_2 : I \to P$, $(W, c) \mapsto c$.

Problem 1.3 How many distinct "words" (i.e., strings of letters, not necessarily actual words) can one get by permuting the letters in the words:

(a) `algebra`, **(b)** `syzygy`, **(c)** $\underbrace{\texttt{aa...a}}_{\alpha}\underbrace{\texttt{bb...b}}_{\beta}$,

(d) $\underbrace{\texttt{a}_1\texttt{a}_1\ldots\texttt{a}_1}_{\alpha_1}\underbrace{\texttt{a}_2\texttt{a}_2\ldots\texttt{a}_2}_{\alpha_2}\ldots\underbrace{\texttt{a}_m\texttt{a}_m\ldots\texttt{a}_m}_{\alpha_m}$?

Problem 1.4 Expand and collect like terms in **(a)** $(a_1+a_2+\cdots+a_m)^2$, **(b)** $(a+b+c)^3$.

Problem 1.5 Given $m, n \in \mathbb{N}$, how many solutions does the equation $x_1+x_2+\cdots+x_m = n$ have in **(a)** positive, **(b)** nonnegative, integers $x_1, x_2, \ldots, x_m$?

Problem 1.6 Count the number of monomials in n variables that have total degree[13] **(a)** exactly d, **(b)** at most d.

Problem 1.7 Is $1000!/\left(100!^{10}\right)$ an integer?

Problem 1.8 For a prime $p \in \mathbb{N}$, show that every binomial coefficient $\binom{p}{k}$ with $1 \leqslant k \leqslant (p-1)$ is divisible by p.

Problem 1.9 Evaluate the sums: **(a)** $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}$, **(b)** $\binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots$, **(c)** $\binom{k}{k}+\binom{k+1}{k}+\cdots+\binom{k+n}{k}$, **(d)** $\binom{n}{1}+2\binom{n}{2}+\cdots+n\binom{n}{n}$, **(e)** $\binom{n}{0}+2\binom{n}{1}+\cdots+(n+1)\binom{n}{n}$, **(f)** $\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^n\binom{n}{n}$, **(g)** $\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2$.

Problem 1.10 For given $m, n \in \mathbb{N}$, count the total number of **(a)** arbitrary, **(b)** bijective, **(c)** strictly increasing, **(d)** injective, **(e)** nonstrictly increasing, **(f)** nonstrictly increasing and surjective, **(g)** surjective maps $\{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$.

Problem 1.11 Count the total number of Young diagrams **(a)** of weight 6, **(b)** of weight 7 and length at most 3, **(c)** having at most p rows and q columns.

Problem 1.12* (by L. G. Makar-Limanov). A soda jerk is whiling away the time manipulating 15 disposable cups stacked on a table in several vertical piles. During each manipulation, he removes the topmost cup of each pile and stacks these together to form a new pile. What can you say about the distribution of cups after 1000 such manipulations?

Problem 1.13 Given four distinct cups, four identical glasses, ten identical sugar cubes, and seven cocktail straws each in different color of the rainbow, count the number of distinct arrangements of **(a)** straws between cups, **(b)** sugar between cups, **(c)** sugar between glasses, **(d)** straws between glasses. **(e)** Answer the same questions under the constraint that every cup or glass must have at least one straw or sugar cube (possibly one or more of each) in it.

Problem 1.14 The sides of a regular planar n-gon lying in three-dimensional space are painted in n fixed different colors, one color per side, in all possible ways. How many different painted n-gons do we get if two colored n-gons are considered the same if one can be obtained from the other by some motion in three-space?

---

[13] The *total degree* of the monomial $x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$ equals $\sum_{i=1}^{n} m_i$.

Problem 1.15 How many different necklaces can be made from 5 red, 7 blue, and 11 white otherwise identical glass beads?

Problem 1.16 All the faces of a regular **(a)** cube, **(b)** tetrahedron, are painted using six fixed colors (different faces in distinct colors) in all possible ways. How many different painted polyhedra do we get?

Problem 1.17 How many different knick-knacks do we get by gluing pairs of the previously painted **(a)** cubes, **(b)** tetrahedra face to face randomly?

Problem 1.18 Show that Zorn's lemma, Lemma 1.3, is equivalent to the axiom of choice. More precisely, assume that Lemma 1.3 holds for every poset P and prove that every surjective map $f : X \twoheadrightarrow Y$ admits a section. Hint: consider the set of maps $g_U : U \to X$ such that $U \subset Y$ and $fg_U = \mathrm{Id}_U$; equip it with a partial order, where $g_U \leqslant g_W$ means that $U \subset W$ and $g_W|_U = g_U$; verify that Lemma 1.3 can be applied; prove that every maximal g_U has $U = Y$.

Problem 1.19 (Hausdorf's Maximal Chain Theorem) Use Lemma 1.3, Zorn's lemma, to prove that every chain in every poset is contained in some maximal (with respect to inclusion) chain. Hint: consider the set of all chains containing a given chain; equip it with the partial order provided by inclusion; then proceed as in the previous problem.

Problem 1.20 (Zermelo's Theorem) Write $\mathcal{S}(X)$ for the set of all nonempty subsets in a given set X including X itself. Use the axiom of choice to construct a map $\mu : \mathcal{S}(X) \to X$ such that $\mu(Z) \in Z$ for all $Z \in \mathcal{S}(X)$. Write $\mathcal{W}(X)$ for the set of all $W \in \mathcal{S}(X)$ possessing a well ordering such that $\mu(W \smallsetminus [w)) = w$ for all $w \in W$. Verify that $\mathcal{W}(X) \neq \varnothing$, and modify the proof of Lemma 1.2 on p. 15 to show that $X \in \mathcal{W}(X)$. This means that *every set can be well ordered*.

Springer

http://www.springer.com/978-3-319-45284-5

Algebra I
Textbook for Students of Mathematics
Gorodentsev, A.L.
2016, XX, 564 p. 79 illus., 42 illus. in color., Hardcover
ISBN: 978-3-319-45284-5