Topics in Advanced Algebra

Contents

Preface

These are the lecture notes that were used in a course for advanced undergraduate and graduate students at Warsaw University of Technology in the winter semester 2012/3. The students came from a variety of backgrounds, including both discrete and continuous mathematics, computer science, and physics.

The aim of the course was to provide an introduction to some of the newer topics and modes of thought in algebra that students are likely to encounter in their research careers. Each lecture represents the amount of material that could reasonably be assimilated in a single week. The first six lectures cover what might be called "combinatorial" algebra, based on the category of sets, while the remainder of the course extends the coverage to include "linear" algebra (in the broadest sense), based on the categories of abelian groups, vector spaces, or more generally a category of modules over a ring.

The course is designed both to present the basic definitions of fundamental concepts of contemporary algebra, and to offer deeper insight into selected topics, such as the classification of G-sets for a finite group G, the construction of free groups, the Krasner-Wielandt Theorem, modeling rotations with quaternions, using initial objects for structural specification, the Tarski Fixed Point Theorem, and an existence theorem for final coalgebras. The language of categories is used as a tool to unify the diverse topics of algebra, and to facilitate the translation of content from one context to another.

Thanks are expressed to the Department of Mathematics and Information Sciences of Warsaw Technical University for the gracious hospitality and opportunity to offer these lectures and lecture notes, and to the Fulbright Commission and Iowa State University for the leave and support that made my semester in Warsaw possible.

Jonathan D.H. Smith.

CHAPTER 1

Associativity

1. Functions

1.1. Elementary aspects of functions.

Definition 1.1 (Function notation). Consider a function

$$f\colon X \to Y; x \mapsto xf \tag{1.1}$$

(*a*) Set X is the *domain*;
(*b*) Set Y is the *codomain*;
(*c*) Set $Xf = \{xf \in Y \mid x \in X\}$ is the *image*;
(*d*) Elements x of X are *arguments*;
(*e*) Elements xf of Y are *values* (*of the function f at the argument x*);
(*f*) Function f is *injective*, or an *injection*, if

$$\forall\ x_1, x_2 \in X\ ,\ x_1 f = x_2 f \Longrightarrow x_1 = x_2$$

(*g*) Function f is *surjective*, or a *surjection*, if

$$\forall\ y \in Y\ ,\ \exists\ x \in X\ .\ xf = y$$

(*h*) Function f is *bijective*, or a *bijection*, if it is both injective and surjective.
(*i*) Sets X and Y are *equipollent* or (*set*) *isomorphic*, often written $X \cong Y$ or $|X| = |Y|$, if there is a bijective function with X as domain and Y as codomain.

Remark 1.2. (a) Various authors use the word "range" for the domain, codomain, or image. It is best avoided. The word "image" is sometimes used for specific values of an argument.

(b) The preposition "onto" is used (ungrammatically!) as a synonym for the adjective "surjective."

(c) The (ugly) phrase "one-one" is used as a synonym for the adjective "injective."

(d) Note the basic *algebraic* notation xf for function values, as with $n!$ for example. The *Euler* notation $f(x)$, popular amongst analysts — compare $\Gamma(n+1)$ — will usually be reserved for "dual" situations. Algebraic notation may also be used in superfix form, viz. x^f, as with x^2 for example.

(e) In (elementary) linear algebra, where elements correspond to vectors and functions correspond to matrices, algebraic notation enables one to work with typographically convenient row vectors:

$$\begin{bmatrix} \cdot & \cdot & \cdot \end{bmatrix} \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix} = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

instead of the more awkward column vectors.

1.1.1. The notation (1.1) may be abbreviated, e.g. as $f\colon X \to Y$ or $\mathbb{Z} \to \mathbb{N}; n \mapsto n^2$ or $x \mapsto xf$, if the missing data is irrelevant, or implicit within the context.

1.1.2. A potential function definition may fail because the **domain is too large**:

$$\mathbb{Z} \to \mathbb{R}; n \mapsto \sqrt{n}$$

or because the **codomain is too small**:

$$\mathbb{R} \to \mathbb{Z}; x \mapsto x^2$$

so one should check that a given function is *well-defined*.

Definition 1.3 (Equality of functions). Two functions

$$f_1\colon X_1 \to Y_1; x_1 \mapsto x_1 f_1$$

and

$$f_2\colon X_2 \to Y_2; x_2 \mapsto x_2 f_2$$

are *equal* if:

(a) Their domains are equal: $X_1 = X_2$;
(b) Their codomains are equal: $Y_1 = Y_2$; and
(c) They have the same effect on each element of their common domain: $\forall\ x \in X_1 = X_2\,,\ xf_1 = xf_2$.

1.2. Algebraic aspects of functions.

DEFINITION 1.4. Given functions $f\colon X \to Y$ and $g\colon Y \to Z$, their *composite* is the function written as

$$fg\colon X \to Z; x \mapsto (xf)g$$

in algebraic notation, or as

$$g \circ f\colon X \to Z; x \mapsto g(f(x))$$

in Euler notation.

REMARK 1.5. In algebraic notation, Definition 1.4 amounts to the (*mixed*) *associative law*

$$x(fg) = (xf)g\,, \tag{1.2}$$

where one views the left hand side, for an element x of X, as being defined by the right hand side. One may write

$$x(fg) \longrightarrow (xf)g \tag{1.3}$$

to reflect this reduction of the expression $x(fg)$ to the more basic expression $(xf)g$. Taking the mixed associative law as given, one may simply eliminate all the brackets in (1.2) and write xfg for the common function value.

PROPOSITION 1.6. *Given three functions $f\colon U \to V$, $g\colon V \to W$, and $h\colon W \to X$, the equation*

$$(fg)h = f(gh) \tag{1.4}$$

holds.

PROOF. The equation (1.4), an equality between functions, is established following the guidelines of Definition 1.3. Both sides have common domain U and common codomain X, so one must check for an equal effect on an element u of the common domain U. The one-line proof

$$u((fg)h) = (u(fg))h = ((uf)g)h = (uf)(gh) = u(f(gh)) \tag{1.5}$$

makes four applications of the mixed associative law (1.2). $\square$

DEFINITION 1.7 (The associative law). The equation (1.4) is known as the *associative law* (*for composable functions*).

Remark 1.8. The equation (1.4) is the father of all associative laws, and equation (1.2) is the mother. Whenever you need to prove an associative law, try to reduce it back to these roots.

1.2.1. *Associahedra.* The associative law has many deep connections with geometry, graph theory, and other areas of mathematics. The first step is to disregard the individuality of the letters in (1.3), simply obtaining

$$\cdot(\cdot\cdot) \longrightarrow (\cdot\cdot)\cdot \tag{1.6}$$

as a directed graph, or perhaps as an oriented 1-dimensional complex that corresponds to a 1-dimensional polyhedron, the *associahedron* Y_3. Now one may take the one-line proof (1.5) of Proposition 1.6 (the associative law for composable functions) and arrange it in graphical fashion (Figure 1). The equality between $u(f(gh))$ and $u((fg)h))$ has

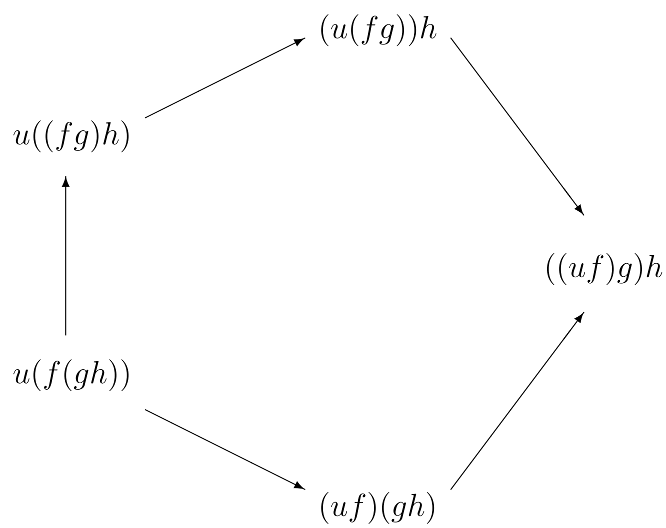


Figure 1. The associahedron Y_4

been directed according to (1.6), as applied to the string fgh. The other equalities, featuring in the one-line proof (1.5), have been directed similarly according to (1.6). Figure 1 may be interpreted as a directed graph, or as an oriented 2-dimensional complex that corresponds to a 2-dimensional polyhedron (pentagon), the *associahedron* Y_4.

1.2.2. Functions may be characterized by their algebraic behavior. The goal is to eliminate any specific mention of elements of the sets involved in concepts such as injectivity or surjectivity.

DEFINITION 1.9. Let $f \colon X \to Y$ be a function.

(a) The function f is a *monomorphism* if:
$$\forall\, W\,,\ \forall\, g_1 \colon W \to X, g_2 \colon W \to X\,,\ g_1 f = g_2 f \Rightarrow g_1 = g_2\,.$$
(b) The function f is an *epimorphism* if:
$$\forall\, Z\,,\ \forall\, h_1 \colon Y \to Z, h_2 \colon Y \to Z\,,\ f h_1 = f h_2 \Rightarrow h_1 = h_2\,.$$
(c) The function f is said to be a (*set*) *isomorphism* if it is both a monomorphism and an epimorphism.
(d) The *identity function* 1_X or id_X on a set X is $1_X \colon x \mapsto x$.
(e) A function $r \colon Y \to X$ is a *right inverse* or a *retraction* for f if
$$fr = 1_X\,. \tag{1.7}$$
(f) The function f is *right invertible* if it has a right inverse.
(g) A function $s \colon Y \to X$ is a *left inverse* or a *section* for f if
$$sf = 1_Y\,. \tag{1.8}$$
(h) The function f is *left invertible* if it has a left inverse.
(i) The function f is *invertible* if it is both right and left invertible.

The role of identity functions is given by the following.

LEMMA 1.10. *If $f : X \to Y$ is a function, then*
$$1_X f = f = f 1_Y\,.$$

Here is an important consequence of the associative law.

PROPOSITION 1.11. *Suppose that a function $f \colon X \to Y$ is invertible. Then if r is any right inverse of f, and s is any left inverse, $r = s$.*

PROOF. Since $fr = 1_X$ and $sf = 1_Y$, one has
$$r = 1_Y r = (sf)r = s(fr) = s1_X = s$$
as a one-line proof. □

Definition 1.12. Suppose that a function $f \colon X \to Y$ is invertible. Then the unique function $Y \to X$ that is both a right and left inverse of f is called the *inverse* f^{-1} of f.

Proposition 1.13. *Let $f \colon X \to Y$ be a function. Then the following conditions are equivalent:*

(a) *f is injective;*
(b) *f is a monomorphism.*

Furthermore, if $X \neq \emptyset$, these conditions are equivalent to

(c) *f is right invertible.*

Proposition 1.14. *Let $f \colon X \to Y$ be a function. Then the following conditions are equivalent:*

(a) *f is surjective;*
(b) *f is an epimorphism.*
(c) *f is left invertible.*

Remark 1.15. The implication (a)$\Rightarrow$(c) in Proposition 1.14 is assumed to be true, as the *Axiom of Choice*.

Proposition 1.16. *Let $f \colon X \to Y$ be a function. Then the following conditions are equivalent:*

(a) *f is bijective;*
(b) *f is an isomorphism.*
(c) *f is invertible.*

Proposition 1.17. *Let $f \colon X \to Y$ and $g \colon Y \to Z$ be functions.*

(a) *If f and g are injective, then so is fg.*
(b) *If f and g are surjective, then so is fg.*
(c) *If f and g are bijective, then so is fg.*

Proof. Part (a) will be proved. For the other parts, see Exercise 6. By Proposition 1.14, f and g are monomorphisms. Consider functions $h_1 \colon W \to X$ and $h_2 \colon W \to X$. Suppose $h_1 fg = h_2 fg$. Since g is a monomorphism, $h_1 f = h_2 f$. Then since f is a monomorphism, $h_1 = h_2$. Thus fg is a monomorphism. □

1.2.3. *Duality.* Comparison of the equivalences in Propositions 1.13 and 1.14 gives a first hint of the far-reaching concept of *duality*. For the time being, it amounts to the correspondences displayed in Table 1. In addition, duality manifests itself by a reversal of composition order, as in the equations (1.2) and (1.3).

TABLE 1. Duality

domain	codomain
surjective	injective
epimorphism	monomorphism
section	retract
left inverse	right inverse
left invertible	right invertible

2. Semigroups, monoids, and groups

2.1. Semigroups, monoids, and groups of functions.

DEFINITION 2.1. For sets X and Y, the set of all functions from X to Y is denoted by Y^X.

DEFINITION 2.2. Let X be a set.

(a) A subset S of X^X is a *semigroup of functions* on the set X if the condition

$$\forall\ f, g \in S\,,\ \ fg \in S$$

of *closure under composition* is satisfied.

(b) A subset S of X^X is a *monoid of functions* on the set X if it is a semigroup of functions, and if the condition

$$1_X \in S$$

of *closure under the identity* is satisfied.

(c) A subset S of X^X is a *group of functions* or a *permutation group* on the set X if it is a monoid of functions on X for which each element is invertible.

DEFINITION 2.3. Let n be a natural number.

(a) Define $\underline{n} = \{i \in \mathbb{N} \mid i < n\}$. Note that $\underline{0} = \varnothing$, and more generally $\underline{n} = \{0, 1, \ldots n-1\}$. The set $\underline{n}$ will be used as the standard n-element set.

(b) The monoid T_n of all functions $f \colon \underline{n} \to \underline{n}$ is the *transformation monoid* of *degree* n.

(c) The group S_n of all invertible functions $f \colon \underline{n} \to \underline{n}$ is called the *symmetric group* of *degree* n.

Example 2.4 (Computable functions). A function $f\colon \mathbb{N} \to \mathbb{N}$ is said to be *computable* if there is a computer program to compute the function value nf given the argument n. Then the set of computable functions is a monoid of functions on $\mathbb{N}$. (See Exercise 10.)

2.2. Abstract semigroups, monoids, and groups.

Definition 2.5. (a) A set A, with a *multiplication* (*operation*)

$$A^2 \to A; (a, b) \mapsto a \cdot b\,,$$

is called a *magma*.

(b) If the *associative law*

$$\forall\ a, b, c \in A\,,\ \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

is satisfied, then $(A, \cdot)$ is an (*abstract*) *semigroup*.

(c) If A is a semigroup with an *identity* (*element*) 1, so that

$$\exists\ 1 \in A\,.\ \forall\ a \in A\,,\ \ a \cdot 1 = a = 1 \cdot a$$

is satisfied, then $(A, \cdot, 1)$ is an (*abstract*) *monoid*.

(d) If $(A, \cdot, 1)$ is a monoid with a function $A \to A; a \mapsto a^{-1}$ such that

$$\forall\ a \in A\,,\ \ a \cdot a^{-1} = 1 = a^{-1} \cdot a$$

is satisfied, then $(A, \cdot, 1)$ is an (*abstract*) *group*.

Remark 2.6. Definition 2.5 is an **abstract** definition. This means that the "multiplication" is capable of interpretation. For example, $(\mathbb{Z}, -)$ is a magma, where the "multiplication" is actually subtraction. When the multiplication of a magma is written as $a \cdot b$, it may often be abbreviated to simple juxtaposition: ab. Another convention uses both $a \cdot b$ and ab, but makes juxtaposition bind stronger than $a \cdot b$. In this convention, the associative law may be written as $ab \cdot c = a \cdot bc$, without brackets.

Proposition 2.7 (Higher associativity). *Let $(A, \cdot)$ be a semigroup. Let n be a positive integer, and let $a_1 a_2 \cdots a_n$ be a string of elements of A of length n. Then there is a unique element a of A such that $a = (a_1[a_2 \dots a_n\}$ in the algebra A for any well-formed parsing $(a_1[a_2 \dots a_n\}$ of the string as a series of $n - 1$ repeated products.*

Proof. For each positive integer n, let A_n denote the set of all possible products $(a_1[a_2 \ldots a_n\}$ of the string $a_1 a_2 \cdots a_n$. Note that $|A_1| = |A_2| = |A_3|$. It will be shown that $|A_n| = 1$ by induction on n. Suppose $|A_k| = 1$ for all positive integers $k < n$. For integers $1 < i < j < n$, consider the products $(a_1 \cdots a_i)(a_{i+1} \cdots a_n)$ and $(a_1 \cdots a_j)(a_{j+1} \cdots a_n)$. Now

$$\begin{aligned}(a_1 \cdots a_j)(a_{j+1} \cdots a_n) &= \Big((a_1 \cdots a_i)(a_{i+1} \cdots a_j)\Big)(a_{j+1} \cdots a_n) \\ &= (a_1 \cdots a_i)\Big((a_{i+1} \cdots a_j)(a_{j+1} \cdots a_n)\Big) \\ &= (a_1 \cdots a_i)(a_{i+1} \cdots a_n)\end{aligned}$$

by induction and the associative law, so $|A_n| = 1$ as required. □

In view of Proposition 2.7, repeated products of elements in a semigroup will normally be written without brackets.

2.2.1. *Monoids of stochastic matrices.*

Definition 2.8. Let m and n be positive integers. Let P be an $m \times n$ matrix with non-negative real entries.

(a) The matrix P is *row-stochastic* if the sum of each row is 1.
(b) The matrix P is *column-stochastic* if the sum of each of its columns is 1.
(c) The matrix P is (*doubly*) *stochastic* if it is both row- and column-stochastic.
(d) An *m-dimensional finite probability distribution* is defined to be a row-stochastic $1 \times m$ matrix.

Lemma 2.9. *Let l, m, n be positive integers. Let A be a row-stochastic $l \times m$ matrix, and let B be a row-stochastic $m \times n$ matrix. Then AB is a row-stochastic $l \times n$ matrix.*

Corollary 2.10. *Suppose that π is an l-dimensional finite probability distribution. Then the product matrix πA is an m-dimensional finite probability distribution.*

Proposition 2.11. *Let n be a positive integer.*

(a) *The set Π_n of all row-stochastic $n \times n$ matrices forms a monoid under matrix multiplication.*
(b) *The set Π^n of all column-stochastic $n \times n$ matrices forms a monoid under matrix multiplication.*

(c) *The set* Π_n^n *of all stochastic* $n \times n$ *matrices forms a monoid under matrix multiplication.*

The proof of Proposition 2.11 is set as Exercise 16.

2.2.2. *Monoids of relations.* Let X be a set. A (*binary*) *relation* V on X is a subset of $X \times X$. The membership $(x, y) \in V$ is often written as $x\ V\ y$.

Definition 2.12. Let X be a set.

(a) The *diagonal* $\widehat{X}$ is the equality relation
$$\{(x, y) \in X \times X \mid x = y\}\,,$$
the image of the *diagonal embedding*
$$\Delta\colon X \to X \times X; x \mapsto (x, x)\,.$$

(b) For binary relations U and V on X, the *relation product* of U and V is the relation
$$U \circ V = \{(x, z) \in X \times X \mid \exists\ y \in X\,.\ (x, y) \in U \text{ and } (y, z) \in V\}$$
on X.

Proposition 2.13. *Let* X *be a set. Then* $\left(2^{X \times X}, \circ, \widehat{X}\right)$ *is a monoid.*

The proof of Proposition 2.13 is set as Exercise 17.

2.3. Invertible elements of monoids.

Definition 2.14. Let $(A, \cdot, 1)$ be a monoid. Let u be an element of A.

(a) The element u is said to be *right invertible* if the condition
$$\exists\ v \in A\,.\ uv = 1$$
is satisfied.

(b) The element u is said to be *left invertible* if the condition
$$\exists\ v \in A\,.\ vu = 1$$
is satisfied.

(c) The element u of A is said to be *invertible*, or a *unit*, if it is both right and left invertible.

Remark 2.15. An element u of a monoid of functions A on a set X is (right, left) invertible in the abstract sense of Definition 2.14 if and only if it is (right, left) invertible in the concrete sense of Definition 1.9.

LEMMA 2.16. *Let u be an element of a monoid $(A, \cdot, 1)$. Then u is a unit if and only if the condition*

$$\exists\, v \in A\,.\; uv = 1 = vu$$

is satisfied.

PROPOSITION 2.17. *Let $(A, \cdot, 1)$ be a monoid. Let A^* be the set of invertible elements of $(A, \cdot, 1)$. Then A^* forms a group $(A^*, \cdot, 1)$.*

DEFINITION 2.18. The group A^* of Proposition 2.17 is called the *group of units* of the monoid A.

EXAMPLE 2.19. In the notation of Definition 2.3, $T_n^* = S_n$.

3. Exercises

(1) (a) Prove $\mathbb{N} \cong \mathbb{Z}$.
 (b) Prove $\mathbb{Z} \cong \mathbb{Q}$.
(2) Draw the 3-dimensional associahedron Y_5 corresponding to all the possible associations of a string of five letters. How many vertices does it have? How many faces (how many squares, how many copies of Y_4)? How many edges (copies of Y_3)?
(3) Prove Propositions 1.13–1.16.
(4) Why are conditions (b) and (c) not equivalent when the function f has an empty domain?
(5) Show that each section is injective. Formulate and prove the dual statement.
(6) Complete the proof of Proposition 1.17.
(7) Give three proofs of Proposition 1.17(b), based on each of the three respective equivalent characterizations of the functions f, g as surjective, epimorphic, and left invertible.
(8) Show that the set of non-decreasing functions forms a monoid of functions on the set of real numbers.
(9) Let n be a natural number. Show that $S_n = n!$ and $|T_n| = n^n$.
(10) Show that the set of computable functions forms a monoid of functions on the set of natural numbers.
(11) Can you show that the set of functions computable in polynomial time forms a monoid of functions on the set of natural numbers?
(12) Let X be a set. Show that the set of left invertible functions $f \colon X \to X$ forms a monoid of functions on X.

(13) Let X be a set. Give an example of a non-empty semigroup S of functions on X which is not a monoid of functions on X.
(14) Explain why $(\mathbb{Q}, /)$ is not a magma.
(15) Explain why $(\mathbb{Z}, -)$ is not a semigroup.
(16) Prove Proposition 2.11.
(17) Let X be a set. Show that $\left(2^{X\times X}, \circ, \widehat{X}\right)$ is a monoid.
(18) Give an example of an element u of a monoid A which is right invertible, but not invertible.
(19) Prove Lemma 2.16.
(20) Let n be a positive integer. Determine the group of units of the monoid Π_n^n of doubly-stochastic matrices.
(21) Let X be a set. Determine the group of units of the relation monoid $\left(2^{X\times X}, \circ, \widehat{X}\right)$ of Proposition 2.13.

CHAPTER 2

Categories

1. Categories

1.1. Definition and examples. While monoids abstract monoids of functions, categories abstract more general systems of functions.

Definition 1.1. A *category* $\mathbf{C} = (\mathbf{C}_0, \mathbf{C}_1)$ consists of two classes, a class $\mathbf{C}_0$ of *objects* and a class $\mathbf{C}_1$ of *morphisms* or *arrows*, together with three functions:

(a) The *identity function*

$$\epsilon\colon \mathbf{C}_0 \to \mathbf{C}_1; X \mapsto 1_X\,;$$

(b) the *tail function* or *domain function*

$$\partial_0\colon \mathbf{C}_1 \to \mathbf{C}_0; f \mapsto f^{\partial_0}\,, \text{ and}$$

(c) the *head function* or *codomain function*

$$\partial_1\colon \mathbf{C}_1 \to \mathbf{C}_0; f \mapsto f^{\partial_1}\,,$$

such that for each object X, one has $1_X\partial_0 = X = 1_X\partial_1$.

Pictorially,

$$f^{\partial_0} \xrightarrow{\quad f \quad} f^{\partial_1} \text{ or } f\colon f^{\partial_0} \to f^{\partial_1}$$

or verbally: f *goes* or *leads* from f^{∂_0} to f^{∂_1}.

For objects X and Y, define $\mathbf{C}(X,Y)$ as the class of all arrows from X to Y. Then for objects U, V, W, X, there is a *composition function*

$$\mathbf{C}(U,V) \times \mathbf{C}(V,W) \to \mathbf{C}(U,W); (f,g) \to fg$$

such that

$$1_U f = f = f 1_V$$

for f in $\mathbf{C}(U, V)$ and the *associative law*

$$(fg)h = f(gh) \tag{1.1}$$

holds for f in $\mathbf{C}(U, V)$, g in $\mathbf{C}(V, W)$, and h in $\mathbf{C}(W, X)$ — Figure 1.

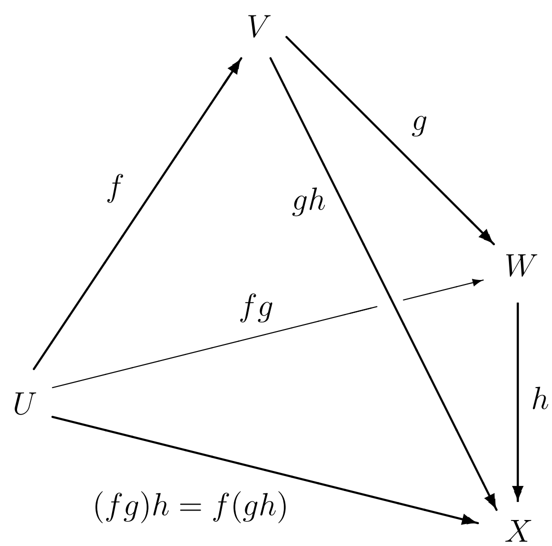


FIGURE 1. The associative law (1.1)

EXAMPLE 1.2. The *category* **Set** *of sets* has the (proper) class of all sets as its object class $\mathbf{Set}_0$. For sets X and Y, one has $\mathbf{Set}(X, Y) = Y^X$, the set of all functions from X to Y. Identities and composition as usual.

EXAMPLE 1.3. The category **Lin** has the class of all real vector spaces as its object class. For real vector spaces U and V, one has $\mathbf{Lin}(U, V)$ as the set of all linear transformations from U to V. Identities and composition as usual.

1.2. Small categories. A category $\mathbf{C}$ is *small* if its object class $\mathbf{C}_0$ is a set. The category of sets is *large*, i.e., not small. However, a category $\mathbf{C}$ is *locally small* if for each pair X, Y of objects of $\mathbf{C}$, the class $\mathbf{C}(X, Y)$ is a set. Thus **Set** is locally small.

EXAMPLE 1.4. Let $(M, \cdot, 1)$ be a monoid. A category $\underline{\underline{M}}$ is defined by taking $\underline{\underline{M}}_0$ as a singleton $\{X\}$, and $\underline{\underline{M}}_1$ as the set M, with $1_M = 1$

and composition of arrows defined by the associative multiplication in the monoid M. Then $\underline{\underline{M}}$ is a small category (with one object and many morphisms).

DEFINITION 1.5. Let V be a relation on a set X.

(a) V is *reflexive* if $\forall\, x \in X\,,\ x\ V\ x$.
(b) The *converse* V' of V is defined by $(x, y) \in V' \Leftrightarrow (y, x) \in V$.
(c) V is *symmetric* if $V = V'$.
(d) V is *antisymmetric* if $\forall\, (x, y) \in V\,,\ (y, x) \in V \Rightarrow x = y$.
(e) V is *transitive* if $\forall\, (x, y), (y, z) \in V\,,\ (x, z) \in V$.
(f) V is an *equivalence relation* if it is reflexive, symmetric and transitive.
(g) (X, V) or V is a *pre-order* or a *quasi-order* if V is reflexive and transitive.
(h) V is an *order relation* if it is reflexive, antisymmetric and transitive.
(i) (X, V) is a (*partially*) *ordered set* or a *poset* if V is an order relation.

EXAMPLE 1.6. For integers d, m, define the divisibility relation

$$d \mid m \quad \Leftrightarrow \quad \exists\, r \in \mathbb{Z}\,.\ m = dr\,.$$

Then $(\mathbb{Z}, \mid)$ is a pre-order, but not a poset, while $(\mathbb{N}, \mid)$ is a poset (see Exercise 3).

PROPOSITION 1.7. *Let X be a set.*

(a) *Suppose that X is the object set of a small category $\mathbf{C}$. Then $V = \{(x, y) \in X^2 \mid \mathbf{C}(x, y) \neq \varnothing\}$ is a pre-order on X.*
(b) *Let (X, V) be a preorder. Then the functions $\epsilon\colon x \mapsto (x, x)$, $\partial_0\colon (x, y) \mapsto x$, and $\partial_1\colon (x, y) \mapsto y$ make (X, V) a category with a uniquely defined composition.*

DEFINITION 1.8 (Equivalence classes). Let E be an equivalence relation on a set X.

(a) For each element x of X, the *equivalence class* x^E is

$$\{y \in X \mid x\ E\ y\}\,.$$

(b) The *quotient set* X^E is

$$\{x^E \mid x \in X\}\,.$$

(c) The (*natural*) *projection* is

$$\operatorname{nat} E\colon X \to X^E; x \mapsto x^E .$$

PROPOSITION 1.9. *Let (X,V) be a preorder.*

(a) *The relation E on X defined by*

$$x\ E\ y \quad \Leftrightarrow \quad x\ V\ y \text{ and } y\ V\ x$$

is an equivalence relation on X.

(b) *The relation*

$$x^E \leq y^E \quad \Leftrightarrow \quad x\ V\ y$$

is a well-defined order relation on the quotient set X^E.

1.2.1. *Concrete and abstract categories.* A category $\mathbf{C}$ is *concrete* if its objects are sets, its morphisms are functions, and the composition in $\mathbf{C}$ is just composition of functions. Thus **Set** and **Lin** are (large) concrete categories.

If M is a monoid of functions on a set X, then the category $\underline{\underline{M}}$ of Example 1.4 is a small concrete category. On the other hand, the category that is constructed from the divisibility preorder $(\mathbb{Z}, |\,)$ by Proposition 1.7(b) is not concrete.

General categories may be described as *abstract*, to signify that they are not (assumed to be) concrete.

1.3. Dual categories. Categories facilitate a precise formulation of duality.

DEFINITION 1.10. Suppose that $\mathbf{C} = (\mathbf{C}_0, \mathbf{C}_1)$ is a category, equipped with identity function ϵ, tail function ∂_0, and head function ∂_1. Then the *dual* or *opposite category* $\mathbf{C}^{\mathsf{op}}$ has object class $\mathbf{C}_0$, morphism class $\mathbf{C}_1$, identity function ϵ, tail function ∂_1, and head function ∂_0. In particular, $\mathbf{C}^{\mathsf{op}}(X,Y) = \mathbf{C}(Y,X)$ for objects X, Y of $\mathbf{C}$ or $\mathbf{C}^{\mathsf{op}}$: the arrows $X \xrightarrow{f} Y$ of $\mathbf{C}^{\mathsf{op}}$ are reversed from arrows $X \xleftarrow{f} Y$ of $\mathbf{C}$.

Consider objects U, V, W of $\mathbf{C}^{\mathsf{op}}$. The composition function

$$\mathbf{C}^{\mathsf{op}}(U,V) \times \mathbf{C}^{\mathsf{op}}(V,W) \to \mathbf{C}^{\mathsf{op}}(U,W); (f,g) \mapsto f \circ g$$

within $\mathbf{C}^{\mathsf{op}}$ is exactly the same function as the composition function

$$\mathbf{C}(V,U) \times \mathbf{C}(W,V) \to \mathbf{C}(W,U); (f,g) \mapsto gf$$

within $\mathbf{C}$.

$\mathbf{C}^{\mathsf{op}}$	$\mathbf{C}$
$\begin{tikzcd} & V \arrow[dr, "g"] & \\ U \arrow[ur, "f"] \arrow[rr, "f \circ g"'] & & W \end{tikzcd}$	$\begin{tikzcd} & V \arrow[dl, "f"'] & \\ U & & W \arrow[ul, "g"'] \arrow[ll, "gf"] \end{tikzcd}$

FIGURE 2. Duality of composition

EXAMPLE 1.11. Let (X, V) be a pre-order category. Then the dual category $(X, V)^{\mathsf{op}}$ is the category determined by the converse preorder (X, V').

1.4. Special morphisms. Generalizing from **Set**:

DEFINITION 1.12. Let $f\colon X \to Y$ be a morphism in a category $\mathbf{C}$.

(a) The morphism f is a *monomorphism* if:

$$\forall\, W\,,\ \forall\, g_1\colon W \to X, g_2\colon W \to X\,,\ g_1 f = g_2 f \Rightarrow g_1 = g_2\,.$$

(b) The morphism f is an *epimorphism* if:

$$\forall\, Z\,,\ \forall\, h_1\colon Y \to Z, h_2\colon Y \to Z\,,\ f h_1 = f h_2 \Rightarrow h_1 = h_2\,.$$

(c) A morphism $r\colon Y \to X$ is a *right inverse* for f if

$$fr = 1_X\,. \tag{1.2}$$

(d) The morphism f is *right invertible* if it has a right inverse.

(e) A morphism $s\colon Y \to X$ is a *left inverse* for f if

$$sf = 1_Y\,. \tag{1.3}$$

(f) The morphism f is *left invertible* if it has a left inverse.

(h) The morphism f is said to be *invertible* or an *isomorphism* if it is both right and left invertible.

Duality: If f is a monomorphism in $\mathbf{C}$, it is an epimorphism in $\mathbf{C}^{\mathsf{op}}$, and so on.

PROPOSITION 1.13. *Suppose that $f\colon x \to y$ is a morphism in a poset category (X, V).*

(a) *f is a monomorphism and an epimorphism.*

(b) *If $x \neq y$, the morphism f is neither right nor left invertible.*

Proposition 1.14. *Let $f\colon X \to Y$ be a morphism in a category* $\mathbf{C}$.

(a) *If f is right invertible, it is a monomorphism.*
(b) *If f is left invertible, it is an epimorphism.*

Proof. (a) If f has right inverse r, and $g_1 f = g_2 f$, then

$$g_1 = g_1 1_X = g_1 f r = g_2 f r = g_2 1_X = g_2\,.$$

The statement (b) is dual to (a). □

Proposition 1.15. *Let $f\colon X \to Y$ and $g\colon Y \to Z$ be morphisms in a category* $\mathbf{C}$.

(a) *If f and g are monomorphisms, then so is fg.*
(b) *If f and g are epimorphisms, then so is fg.*
(c) *If f and g are isomorphisms, then so is fg.*

2. Products

2.1. Cartesian and tensor products. Let X_1 and X_2 be sets. The *cartesian product*

$$X_1 \times X_2 = \{(x_1, x_2) \mid x_i \in X_i\}$$

has *projections*

$$\pi_i\colon X_1 \times X_2 \to X_i; (x_1, x_2) \mapsto x_i \tag{2.1}$$

for $i = 1, 2$.

2.1.1. *Componentwise structure.* If the sets X_1 and X_2 carry algebra structure — semigroup, monoid, group, real vector space, ... — then a similar structure is defined *componentwise* on $X_1 \times X_2$. If X_1 and X_2 are monoids, for example, then $X_1 \times X_2$ has the *componentwise multiplication* $(x_1, x_2)\cdot(y_1, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2)$ and the *componentwise identity* $(1, 1)$.

2.1.2. *Currying.* A function with a product $X \times Y$ as domain is a function of two variables. An important process known as *Currying* in computer science, or *parametrization of a family of functions* in analysis, replaces a function of two variables with a parametrized family of functions of a single variable.

Proposition 2.1. *Let X, Y, Z be sets. Then there is an isomorphism*

$$\mathbf{Set}(X \times Y, Z) \cong \mathbf{Set}(X, \mathbf{Set}(Y, Z)) \tag{2.2}$$

taking a function

$$f\colon X \times Y \to Z; (x,y) \mapsto (x,y)f$$

to a family of functions $f_x\colon Y \to Z; y \mapsto (x,y)f$ *that are parametrized by elements* x *of* X.

2.1.3. *Tensor products of real vector spaces.* There is an analogue of Currying in linear algebra. Let U, V, W be real vector spaces. Recall that the set $\mathbf{Lin}(V, W)$ of linear transformations from V to W inherits a real vector space structure from W. In particular, there is a *zero linear transformation* $0\colon V \to W$ with image $\{0\}$.

There is a vector space $U \otimes V$, called the *tensor product* of U and V, such that there is an isomorphism

$$\mathbf{Lin}(U \otimes V, W) \cong \mathbf{Lin}(U, \mathbf{Lin}(V, W)) \tag{2.3}$$

analogous to the Currying isomorphism (2.7) for sets. To make the analogy precise, suppose that U, V, W have respective bases X, Y, Z. Then (2.3) is a direct consequence of (2.7), taking $U \otimes V$ as the vector space with basis $X \times Y$ (Exercise 14).

2.2. Products in categories.

PROPOSITION 2.2. *Let* X_1 *and* X_2 *be sets. Then for any set* Y, *and for any pair of functions* $f_i\colon Y \to X_i$, *there is a unique function*

$$f_1 \times f_2\colon Y \to X_1 \times X_2; y \mapsto (yf_1, yf_2)$$

such that $(f_1 \times f_2)\pi_i = f_i$, *for* $i = 1, 2$, *using the projections* (2.1).

Here is a picture:

$$\begin{tikzcd} X_1 \times X_2 \arrow[r, "\pi_i"] & X_i \\ Y \arrow[u, dashed, "f_1 \times f_2"] \arrow[ur, "f_i"'] & \end{tikzcd} \tag{2.4}$$

DEFINITION 2.3. Let X_1 and X_2 be objects of a category $\mathbf{C}$. Then an object $X_1 \times X_2$ of $\mathbf{C}$ is said to be a *product* of X_1 and X_2 in the category $\mathbf{C}$ if:

(a) There are *projection* morphisms $\pi_i\colon X_1 \times X_2 \to X_i$ for $i = 1, 2$;
(b) For any object Y and for any pair of morphisms $f_i\colon Y \to X_i$ of $\mathbf{C}$, there is a unique morphism $f_1 \times f_2\colon Y \to X_1 \times X_2$ of $\mathbf{C}$ such that $(f_1 \times f_2)\pi_i = f_i$, for $i = 1, 2$.

Proposition 2.4. *Let (X, V) be a poset category. Then a product $x_1 \times x_2$ of elements x_i of X is a greatest lower bound of x_1 and x_2.*

Proof. Definition 2.3(a) says that $x_1 \times x_2$ is a lower bound for x_1 and x_2, while Definition 2.3(b) says that $x_1 \times x_2$ is greater than (or equal to) any lower bound y for x_1 and x_2. $\square$

Example 2.5. A pair of objects in a category may not have a product: In the "2-crown" poset

$$\begin{tikzcd} x_1 & & x_2 \\ y_1 \arrow[u] \arrow[urr] & & y_2 \arrow[u] \arrow[ull] \end{tikzcd}$$

there is no greatest lower bound of x_1 and x_2.

2.3. Coproducts. Products in the dual $\mathbf{C}^{\mathsf{op}}$ of a category $\mathbf{C}$ may be defined directly within $\mathbf{C}$.

Definition 2.6. Let X_1 and X_2 be objects of a category $\mathbf{C}$. Then an object $X_1 + X_2$ of $\mathbf{C}$ is said to be a *coproduct* or *sum* of X_1 and X_2 in the category $\mathbf{C}$ if:

(a) There are *insertion* morphisms $\iota_i \colon X_i \to X_1 + X_2$ for $i = 1, 2$;
(b) For any object Y and for any pair of morphisms $f_i \colon X_i \to Y$ of $\mathbf{C}$, there is a unique morphism $f_1 + f_2 \colon X_1 + X_2 \to Y$ of $\mathbf{C}$ such that $\iota_i(f_1 + f_2) = f_i$, for $i = 1, 2$.

Here is the picture dual to (2.4):

(2.5)
$$\begin{tikzcd} X_1 + X_2 \arrow[d, dashed, "f_1+f_2"'] & X_i \arrow[l, "\iota_i"'] \arrow[dl, "f_i"] \\ Y & \end{tikzcd}$$

Proposition 2.7. *Let (X, V) be a poset category. Then a coproduct or sum $x_1 + x_2$ of elements x_i of X is a least upper bound of x_1 and x_2.*

Proposition 2.8. *For sets X_1 and X_2, their coproduct in the category* **Set** *is the* disjoint union

$$X_1 + X_2 = \{(x_1, 1) \mid x_1 \in X_1\} \cup \{(x_2, 2) \mid x_2 \in X_2\}$$

with insertions $\iota_i \colon X_i \to X_1 + X_2; x_i \mapsto (x_i, i)$ for $i = 1, 2$.

PROPOSITION 2.9. *Let U and V be real vector spaces. Their coproduct in the category* **Lin** *is the* direct sum $U \oplus V = U \times V$ *with insertions* $\iota_U \colon U \to U \oplus V; u \mapsto (u, 0)$ *and* $\iota_V \colon V \to U \oplus V; v \mapsto (0, v)$. *Thus given a vector space W and linear transformations $f \colon U \to W$, $g \colon V \to W$, there is a unique linear transformation $f \oplus g \colon U \oplus V \to W$ such that $\iota_U(f \oplus g) = f$ and $\iota_V(f \oplus g) = g$.*

REMARK 2.10. (a) Note the use of the special notation $f \oplus g$ rather than $f + g$ in Proposition 2.9, to avoid clashing with the established notation

$$f + g \colon U \to W; u \mapsto uf + ug$$

for given linear transformations $f \colon U \to W$ and $g \colon U \to W$.

(b) In the context of Proposition 2.9, elements (u, v) of $U \times V$ are often written in the form $u \oplus v$.

2.4. Semilattices and lattices.

DEFINITION 2.11. Let $(X, \leq)$ be a poset.

(a) The poset is a *meet semilattice* if for all x, y in X, the greatest lower bound or *meet* $x \wedge y$ exists.
(b) The poset is a *join semilattice* if for all x, y in X, the least upper bound or *join* $x \vee y$ exists.
(c) The poset is a *lattice* if it is both a meet and join semilattice.

EXAMPLE 2.12. The divisibility poset $(\mathbb{N}, |\,)$ is a lattice. For positive integers m and n, the greatest lower bound $m \wedge n$ is the greatest common divisor, while the least upper bound $m \vee n$ is the least common multiple.

EXAMPLE 2.13. The real line $(\mathbb{R}, \leq)$ is a lattice. For real numbers x and y, the greatest lower bound $x \wedge y$ is the minimum, while the least upper bound $x \vee y$ is the maximum.

2.4.1. *Algebraic characterization of semilattices and lattices.*

DEFINITION 2.14. Let $(S, \cdot)$ be a semigroup.

(a) The semigroup is *commutative* if $\forall\ x, y \in S\,,\ xy = yx$.
(b) The semigroup is *idempotent* if $\forall\ x \in S\,,\ xx = x$.
(c) The semigroup is a *semilattice* if it is both idempotent and commutative.

PROPOSITION 2.15. *(a) Let $(S, \wedge)$ be a semilattice. Defining*

$$x \leq_{\wedge}^{\uparrow} y \quad \Leftrightarrow \quad x \wedge y = x$$

yields a meet semilattice $(S, \leq_{\wedge}^{\uparrow})$ or $(S, \leq_{\wedge})$.
(b) Let $(S, \vee)$ be a semilattice. Defining

$$x \leq_{\vee}^{\downarrow} y \quad \Leftrightarrow \quad x \vee y = y$$

yields a join semilattice $(S, \leq_{\vee}^{\downarrow})$ or $(S, \leq_{\vee})$.

REMARK 2.16. If $(S, \cdot)$ is a semilattice, the **meet** semilattice ordering of Proposition 2.15(a) places the product $x \cdot y$ **below** its arguments x, y, while the **join** semilattice ordering of Proposition 2.15(b) places the product $x \cdot y$ **above** its arguments x, y. In other words, the semigroup product $x \cdot y$ becomes a **product** in the **meet** semilattice poset category, and a **coproduct** in the **join** semilattice poset category.

PROPOSITION 2.17. *Let $(S, \wedge)$ and $(S, \vee)$ be semilattices. Then the order relations $\leq_{\wedge}^{\uparrow}$ and $\leq_{\vee}^{\downarrow}$ on S coincide if and only if the* absorption laws

$$x \vee (x \wedge y) = x = x \wedge (x \vee y) \tag{2.6}$$

are satisfied.

Given Proposition 2.17, lattices may be characterized algebraically as sets $(L, \vee, \wedge)$ with two semilattice structures $(L, \vee)$ and $(L, \wedge)$ such that the absorption laws are satisfied (Exercise 18).

2.4.2. *Bounded semilattices and lattices.*

DEFINITION 2.18. Let $(X, \leq)$ be a poset.

(a) An element b of X is an *upper bound* if $\forall\ x \in X\ ,\ x \leq b$. If an upper bound b exists, the poset is *bounded above* by b.
(b) An element b of X is a *lower bound* if $\forall\ x \in X\ ,\ b \leq x$. If a lower bound b exists, the poset is *bounded below* by b.

PROPOSITION 2.19. *Let $(S, \cdot, e)$ be a monoid such that $(S, \cdot)$ is a semilattice. Then the identity element e is an upper bound for the meet semilattice $S, \leq_{\cdot}^{\uparrow}$ and a lower bound for the join semilattice $S, \leq_{\cdot}^{\downarrow}$.*

DEFINITION 2.20. A *bounded lattice* $(L, \vee, \wedge, 0, 1)$ is a lattice $(L, \vee, \wedge)$ with monoids $(L, \vee, 0)$ and $(L, \wedge, 1)$.

2.5. Heyting algebras. Heyting algebras offer poset categories with an analogue of the Currying (2.7).

DEFINITION 2.21. A *Heyting algebra* $(H, \vee, \wedge, \backslash, 0, 1)$ is defined as a bounded lattice $(H, \vee, \wedge, \backslash, 0, 1)$ with an additional binary operation $\backslash$ such that the condition

$$\forall\, x, y, z \in H\,,\ x \wedge y \le z \ \Leftrightarrow x \le y \backslash z \tag{2.7}$$

is satisfied.

EXAMPLE 2.22. Let $(B, \vee, \wedge, \neg, 0, 1)$ be a Boolean algebra, for example the power set $\left(2^X, \cup, \cap, \overline{}, \emptyset, X\right)$ of a set X. Define the *implication* $y \to z = (\neg y) \vee z$. Then $(B, \vee, \wedge, \to, 0, 1)$ is a Heyting algebra.

EXAMPLE 2.23. Let $I = [0, 1]$ be the closed unit interval in the real line. For elements y, z of I, define

$$y \backslash z = \begin{cases} 1 & \text{if } y \le z\,; \\ z & \text{otherwise.} \end{cases}$$

Then with the maximum and minimum operations of Example 2.13, one obtains a Heyting algebra $(I, \vee, \wedge, \backslash, 0, 1)$.

3. Exercises

(1) Let M be a monoid. Show that the multiplication in M is determined completely by the category $\underline{\underline{M}}$ of Example 1.4.
(2) Show that a relation V on X is transitive iff $V \circ V \subseteq V$.
(3) Verify the claims of Example 1.6.
(4) Prove Proposition 1.7
(5) Prove Proposition 1.9
(6) Starting with the divisibility preorder $(\mathbb{Z}, |\,)$, determine which ordered set is produced by Proposition 1.9(b).
(7) If $\mathbf{C}$ is a category, confirm that Definition 1.10 defines $\mathbf{C}^{\mathsf{op}}$ as a category.
(8) Let G be a group, with corresponding category $\underline{\underline{G}}$ as in Example 1.4. Let G^{op} be the group determined by the dual category $\underline{\underline{G}}^{\mathsf{op}}$ as in Exercise 1. Show that the groups G and G^{op} are isomorphic.
(9) Prove Proposition 1.13.

(10) Let $f: U \to V$ be a linear transformation of real vector spaces. If f is a monomorphism in the category **Lin**, show that it is right invertible. [Hint: A linear transformation $g: \mathbb{R} \to U$ is uniquely specified by the element $1g$ in U.]
(11) Prove Proposition 1.15.
(12) Let X_1 and X_2 be sets. Give an example to show that the projection $\pi_2: X_1 \times X_2 \to X_2$ need not be an epimorphism.
(13) (a) If X_1 and X_2 are groups, show that $X_1 \times X_2$, with componentwise structure, is a group.
(b) If X_1 and X_2 are fields, show that $X_1 \times X_2$, with componentwise structure, is not a field.
(14) Prove the existence of the isomorphism (2.3), when the spaces U, V, W have respective bases X, Y, Z.
(15) A set X is said to be a *pointed* set if it has a special element 0_X. A function $f: X \to Y$ between pointed sets is called a *pointed morphism* if $0_X f = 0_Y$. Take $\mathbf{Set}^*$ to be the category of pointed sets and morphisms. For pointed sets X and Y, the morphism set $\mathbf{Set}^*(X,Y)$ is pointed, with $0_{\mathbf{Set}^*(X,Y)}$ as the function having constant value 0_Y. Now let X, Y, Z be finite pointed sets, with respective sizes $1+l, 1+m, 1+n$.
(a) What is the size of the pointed set $\mathbf{Set}^*(Y,Z)$?
(b) If there is a Currying isomorphism

$$\mathbf{Set}^*(X \otimes Y, Z) \cong \mathbf{Set}^*(X, \mathbf{Set}^*(Y,Z)),$$

what is the size of the pointed set $X \otimes Y$?
(16) Prove Proposition 2.8.
(17) Prove Proposition 2.9.
(18) Prove Proposition 2.17.
(19) Let X be a set. Show that the poset $(2^X, \subseteq)$ is a lattice, with intersection as the meet and with union as the join.
(20) Let U be a real vector space. Let $\mathrm{Sb}\, U$ denote the set of subspaces of U.
(a) Show that the poset $(\mathrm{Sb}\, U, \subseteq)$ is a lattice, with intersection as the meet.
(b) How is the join of two subspaces determined?
(21) A lattice L is said to be *distributive* if $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ for all x, y, z in L.
(a) Show that L is distributive if and only if $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ for all x, y, z in L.

(b) Show that for each set X, the lattice $(2^X, \subseteq)$ is distributive.
(c) Show that $(\mathbb{N}, |\,)$ is distributive.
(d) Show that $(\mathbb{R}, \leq)$ is distributive.
(e) Show that $(\mathrm{Sb}\, U, \subseteq)$ (as in Exercise 20) is not distributive if $\dim U > 1$.

(22) Verify Proposition 2.19.
(23) Check the Currying condition (2.7) in the Boolean algebra context of Example 2.22
(24) Check the Currying condition (2.7) in the real closed interval context of Example 2.23
(25) Let $(X, \mathcal{T})$ be a topological space, with set $\mathcal{T}$ of open sets. Show that a binary operation $\backslash$ may be defined on $\mathcal{T}$ to yield a Heyting algebra $(\mathcal{T}, \cup, \cap, \backslash, \emptyset, X)$.

CHAPTER 3

Group actions

1. Representations

1.1. Homomorphisms.

Definition 1.1. Consider a function $f: G \to H$.

(a) If $(G, \cdot)$ and $(H, \cdot)$ are semigroups, the function f is a *semigroup homomorphism* if

$$\forall\, x, y \in G\,,\ xf \cdot yf = (xy)f$$

(i.e., f *preserves the multiplication*).

(b) If $(G, \cdot, 1)$ and $(H, \cdot, 1)$ are monoids, a semigroup homomorphism f is a *monoid homomorphism* if $1f = 1$ (i.e., f *preserves the identity*).

(c) If $(G, \cdot, 1)$ and $(H, \cdot, 1)$ are groups, the function f is a *group homomorphism* if

$$\forall\, x \in G\,,\ (xf)^{-1} = x^{-1}f$$

(i.e., f *preserves the inversion*).

The large concrete categories of semigroup, monoid, and group homomorphisms are respectively denoted **Sgp**, **Mon**, and **Gp**.

Remark 1.2. More generally, a function between algebraic structures is a *homomorphism* if it preserves those structures. For example, vector space homomorphisms are linear transformations. A bijective function between algebraic structures A and B is an *isomorphism*; one then writes $A \cong B$.

The following lemma is very useful.

Lemma 1.3. *If a function $f: (G, \cdot, 1) \to (H, \cdot, 1)$ between groups is a semigroup homomorphism, then it is a group homomorphism.*

1.1.1. *The First Isomorphism Theorem for Sets.* In Theorem 1.6 below, an arbitrary function $f\colon X \to Y$ is decomposed as $f = sbj$, with a surjection s, a bijection b, and an injection j.

DEFINITION 1.4. The (*relation*) *kernel* or *relation kernel* $\ker f$ of f is the equivalence relation on X defined by

$$x_1 \ker f\ x_2 \quad \Leftrightarrow \quad x_1 f = x_2 f$$

for elements x_1, x_2 of the domain X of f.

REMARK 1.5. To distinguish from the relation kernel, the kernel subspace of a linear transformation f is written as $\operatorname{Ker} f$. Then a similar convention applies in other contexts (groups, rings, etc.).

THEOREM 1.6 (First Isomorphism Theorem for Sets). *Let $f\colon X \to Y$ be a function. With the surjection*

$$s = \operatorname{nat}\ker f\colon X \to X^{\ker f}; x \mapsto x^{\ker f}$$

and the injection

$$j\colon Xf \to Y; xf \mapsto xf\,,$$

there is a well-defined bijection (set isomorphism)

$$b\colon X^{\ker f} \to Xf; x^{\ker f} \mapsto xf$$

such that $f = sbj$.

$$\begin{tikzcd}
x \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & xf \\
& X \arrow[r, "f"] \arrow[d, "s"'] & Y & \\
& X^{\ker f} \arrow[r, "b"'] & Xf \arrow[u, "j"'] & \\
x^{\ker f} \arrow[rrr, mapsto] & & & xf \arrow[uuu, mapsto]
\end{tikzcd}$$

1.1.2. *The First Isomorphism Theorem for Algebras.* Suppose that $f\colon X \to Y$ is a homomorphism of algebraic structures. Then a refined version of Theorem 1.6 applies.

THEOREM 1.7 (First Isomorphism Theorem for Algebras). *Suppose that $f\colon X \to Y$ is a homomorphism. The surjective homomorphism*

$$s = \mathrm{nat}\,\mathrm{ker} f\colon X \to X^{\ker f}; x \mapsto x^{\ker f}$$

and the injective homomorphism

$$j\colon Xf \to Y; xf \mapsto xf$$

compose with a well-defined algebra isomorphism

$$b\colon X^{\ker f} \to Xf; x^{\ker f} \mapsto xf$$

to yield $f = sbj$.

REMARK 1.8. Applied to a linear transformation $f\colon X \to Y$ between finite-dimensional real vector spaces, Theorem 1.7 implies the relation $\dim X = \dim \mathrm{Ker}\, f + \dim Xf$ (Exercise 3).

1.2. Semigroup representations. Let X be a set. Recall the semigroup of functions $(X^X, \cdot)$ under composition.

DEFINITION 1.9 (Semigroup representations). Let M be a semigroup.

(a) A homomorphism $r\colon M \to X^X; m \mapsto m^r$ is called a (*right*) (*semigroup*) *representation* of M (on X).
(b) A right representation r is *faithful* if the function r is injective.
(c) A homomorphism $l\colon M \to \left(X^X\right)^{\mathsf{op}}; m \mapsto m^l$ is called a (*left*) (*semigroup*) *representation* of M (on X).
(d) A left representation l is *faithful* if the function l is injective.

PROPOSITION 1.10 (Mixed associative laws). *Let X be a set and let M be a semigroup.*

(a) *Consider a right representation $r\colon M \to X^X; m \mapsto m^r$ of M. Then the* mixed associative law

$$\forall\ x \in X\,,\ \forall\ m, n \in M\,,\ (xm^r)n^r = x(mn)^r \tag{1.1}$$

holds.

(b) *Consider a left representation $l\colon M \to X^X; m \mapsto m^l$ of M. Then the* mixed associative law

$$\forall\ x \in X\,,\ \forall\ m, n \in M\,,\ (m^l \circ n^l)(x) = (mn)^l(x) \tag{1.2}$$

holds.

(c) *A function* $r\colon M \to X^X$ *is a right representation if the mixed associative law* (1.1) *holds.*
(d) *A function* $l\colon M \to X^X$ *is a left representation if the mixed associative law* (1.2) *holds.*

Proposition 1.10 shows how algebraic and Euler function notations are natural in their respectively dual contexts. Using the "wrong" notation for the context inserts extra twists in the mixed associative laws.

1.2.1. *Currying.* A right representation of a semigroup M on a set X has been defined as a semigroup homomorphism $r\colon M \to X^X$. As an element of $\mathbf{Set}(M, \mathbf{Set}(X, X))$, the function r may be Curried to

$$\rho\colon X \times M \to X; (x, m) \mapsto xm^r\,.$$

The mixed associative law (1.1) encodes as the commutative diagram

$$\begin{tikzcd} X \times M \times M \arrow[r, "\rho\times 1_M"] \arrow[d, "1_X\times\nabla"'] & X \times M \arrow[d, "\rho"] \\ X \times M \arrow[r, "\rho"'] & X \end{tikzcd} \tag{1.3}$$

in the category **Set**, with

$$\nabla\colon M \times M \to M; (m, n) \mapsto mn$$

as the semigroup multiplication.

1.3. Some examples.

Example 1.11 (Homotheties). Let U be a real vector space. Then there is a representation $(\mathbb{R}, \cdot) \to U^U$, under which a real number (or "scalar") λ is represented by the *homothety* that multiplies each vector in U by the constant scale factor λ.

Definition 1.12. Let s be an element of a magma $(S, \cdot)$.
(a) The *right multiplication* by s is the mapping

$$R(s)\colon S \to S; x \mapsto x \cdot s$$

in S^S.
(b) The *left multiplication* by s is the mapping

$$L(s)\colon S \to S; x \mapsto s \cdot x$$

in S^S.

PROPOSITION 1.13. *Suppose that* $(S, \cdot)$ *is a semigroup. Then there is a right representation*

$$R \colon S \to S^S; s \mapsto R(s)$$

of S *on* S.

PROOF. The mixed associative law $xR(s)R(t) = xR(st)$, given elements x, s, t of S, follows from the associative law $(xs)t = x(st)$. $\square$

DEFINITION 1.14. The representation R of Proposition 1.13 is known as the *right regular representation* of the semigroup $(S, \cdot)$.

1.3.1. *Induced representations.*

DEFINITION 1.15. Let $f \colon M \to N$ be a semigroup homomorphism. Let $r \colon N \to X^X$ be a right representation of N on a set X. The composite homomorphism $fr \colon M \to X^X$ is called the (*right*) *representation* of M on X *induced* by f.

EXAMPLE 1.16 (The flip-flop). Consider the set $\underline{2} = \{0, 1\}$ of bits. The set $S = \{\mathrm{id}_{\underline{2}}, c_0, c_1\}$, with *constant* or *reset* functions $c_i \colon \underline{2} \to \underline{2}$ having image $\{i\}$ for $i \in \underline{2}$, forms a semigroup (Exercise 9). The right representation of S induced by the inclusion

$$S \hookrightarrow \underline{2}^{\underline{2}}; f \mapsto f$$

is called the *flip-flop*. Along with right regular representations of finite simple groups, it is one of the key components in the Krohn-Rhodes theory analysing finite semigroups, as a generalization of the Jordan-Hölder decomposition for groups [**2**].

1.4. Monoid and group actions. If X is a set and M is a monoid, then (right or left) *monoid representations* of M on X are defined by monoid homomorphisms $M \to X^X$ or $M \to (X^X)^{\mathsf{op}}$ in place of the semigroup homomorphisms of §1.2. Proposition 1.10(c)(d) has its corresponding analogue:

PROPOSITION 1.17. *Let* X *be a set and let* M *be a monoid.*

(a) *A function* $r \colon M \to X^X$ *is a right monoid representation if the mixed associative law* (1.1) *holds, and if* $x1^r = x$ *for all* $x \in X$.
(b) *A function* $l \colon M \to X^X$ *is a left monoid representation if the mixed associative law* (1.2) *holds, and if* $1^l(x) = x$ *for all* $x \in X$.

Definition 1.18. Let X be a set, and let M be a group.

(a) A group homomorphism $r\colon M \to X!; m \mapsto m^r$ is called a (*right*) *permutation representation* of M (on X).

(c) A group homomorphism $l\colon M \to (X!)^{\mathsf{op}}; m \mapsto m^l$ is called a (*left*) *permutation*) *representation* of M (on X).

Lemma 1.3 implies the following.

Proposition 1.19. *Let X be a set and let M be a group.*

(a) *A function $r\colon M \to X!$ is a right permutation representation if the mixed associative law* (1.1) *holds.*

(b) *A function $l\colon M \to X!$ is a left permutation representation if the mixed associative law* (1.2) *holds.*

Theorem 1.20 (Cayley's Theorem). *Let $(G, \cdot, 1)$ be a group. Then there is a faithful right permutation representation*

$$R\colon G \to G!; g \mapsto R(g)$$

of G on G.

Definition 1.21. The representation R of Theorem 1.20 is known as the *right regular permutation representation* of the group $(G, \cdot, 1)$.

1.5. Dual representations.

Proposition 1.22. *Let X and Y be sets. Let M be a semigroup. Let $r\colon M \to X^X$ be a right representation of M on X. Then*

$$x(m^l f) = (xm^r)f\,,$$

for $x \in X$, $m \in M$, and $f\colon X \to Y$, defines a left representation l of M on Y^X.

Proof. By Proposition 1.10, the mixed associative law

$$(m^l \circ n^l)(f) = (mn)^l f \tag{1.4}$$

must be verified for $f \in Y^X$ and $m, n \in M$. The functions on each side of (1.4) have the same domain X and codomain Y. Then for an element x of X, one has

$$\begin{aligned} x(m^l \circ n^l)(f) &= x\big(m^l\left(n^l f\right)\big) = (xm^r)(n^l f) \\ &= xm^r n^r f = \big(x(mn)^r\big)f = x\big((mn)^l f\big)\,, \end{aligned}$$

so the two sides of (1.4) represent equal functions. $\square$

DEFINITION 1.23. In the context of Proposition 1.22, one says that the left representation l of M on Y^X is *dual* to the right representation r of M on X.

REMARK 1.24. Proposition 1.22 and Definition 1.23 both have their analogues for monoid and group permutation representations.

2. Sets with action

This section puts a new slant on representations. The emphasis moves to the underlying set of a representation, described as a set with a semigroup, monoid, or group *action*.

2.1. Representations as algebras.

DEFINITION 2.1. Let X be a set.

(a) The set X is said to be a (*right*) S-*act* (X, S, r) or (X, S) for a semigroup S if S has a right representation r on X.
(b) The set X is said to be a (*right*) M-*set* (X, M, r) or (X, M) for a monoid M if M has a right representation r on X.
(c) The set X is said to be a (*right*) G-*set* (X, G, r) or (X, G) for a group G if G has a right permutation representation r on X.

REMARK 2.2. (a) Left S-acts, M-sets, and G-sets are defined dually.

(b) The specific representation r that appears in the different parts of Definition 2.1 is often suppressed, being understood in a given context. One then writes xs rather than xs^r for $x \in X$, $s \in S$, and so on.

2.1.1. *Intertwining.* For a fixed semigroup S, monoid M, or group G, one may consider S-acts, M-sets, or G-sets as algebraic structures on the underlying set X. An S-act homomorphism or S-*homomorphism* $\varphi\colon (X_1, S, r_1) \to (X_2, S, r_2)$ is a function $\varphi\colon X_1 \to X_2$ such that the *intertwining* diagram

(2.1)
$$\begin{tikzcd} X_1 \arrow[r, "\varphi"] \arrow[d, "s^{r_1}"'] & X_2 \arrow[d, "s^{r_2}"] \\ X_1 \arrow[r, "\varphi"'] & X_2 \end{tikzcd}$$

commutes for all elements s of S. The language is extended with terms such as *M-homomorphism*, *G-isomorphism*, and so on. It is often convenient to denote the respective categories of S-acts, M-sets, or G-sets as $\underline{\underline{S}}$, $\underline{\underline{M}}$, and $\underline{\underline{G}}$.

2.1.2. *Closed subsets.* Suppose that a set X has algebraic structure. A subset Y of X is a *subalgebra* if it is itself an algebra under the operations on X, or in other words, if it is closed under all the operations of the structure. For S-acts, M-sets, or G-sets, the respective subalgebras are called S-subsets, M-subsets, or G-subsets.

2.2. ***G*-sets.** Let G be a given group. In a model for much of algebra, the goal is to analyze and classify all G-sets. In particular, given finite G-sets X and Y, one would like an algorithm to decide whether X and Y are isomorphic.

2.2.1. *Orbits.*

Definition 2.3. Let (X, G) or X be a G-set.

(a) The G-set X is *irreducible* or *transitive* if it has no proper, non-empty G-subsets.
(b) An irreducible, non-empty G-subset of X is an *orbit*.
(c) The G-set X is *decomposable* if it can be expressed as a disjoint union $X = Y + Z$ of non-empty G-subsets.
(d) The G-set X is *indecomposable* if it is not decomposable.

Irreducibility implies indecomposability. The converse is true.

Lemma 2.4. *An indecomposable G-set is irreducible.*

Proof. Suppose that Y is a proper, non-empty G-subset of a G-set X. Since Y is proper and non-empty, its complement $\overline{Y}$ in X is proper and non-empty. Consider an element x of $\overline{Y}$, and an element g of G. Then $xg \in Y$ would imply $x = xgg^{-1} \in Yg^{-1} = Y$, a contradiction. Thus $xg \in \overline{Y}$, and $X = Y + \overline{Y}$ with proper, non-empty G-subsets Y and $\overline{Y}$. □

The set of orbits of a (right) G-set (X, G) is written as X/G. Note that for $x \in X$, the element x lies in the orbit $xG = \{xg \mid g \in G\}$.

Proposition 2.5. *Let (X, G) be a G-set. Then (X, G) is the disjoint union $\sum X/G$ of its orbits.*

Proof. If two irreducible G-subsets of (X, G) have a non-trivial intersection, then they coincide, since their intersection is a G-subset of (X,G). Thus the union $\bigcup X/G$ of the orbits is the disjoint union $\sum X/G$. Suppose that this disjoint union does not cover all of X, say with $x \in X \smallsetminus \sum X/G$. Then $x \in xG \subseteq \sum X/G$, a contradiction. $\square$

Example 2.6 (Conjugacy). The group G acts on itself by the so-called *conjugacy representation*

$$T\colon G \mapsto G!; g \mapsto L(g)^{-1}R(g)\,. \tag{2.2}$$

The orbits of the right G-set (G,G,T) are the *conjugacy classes* of G. More generally, two subsets A, B of G are said to be *conjugate* if $AT(g) = B$ for some element g of G.

2.2.2. *Homogeneous spaces.* Given Proposition 2.5, the next step is to determine which G-sets may appear as orbits. Let H be a subgroup of G. The insertion $H \hookrightarrow G$ of H in G, combined with the left regular representation $L\colon G \to G!$ of G, induces a left representation

$$L\colon H \to G!; h \mapsto L(h)$$

of H. The non-empty irreducible left H-subsets of this action are the *right cosets* $Hx = \{hx \mid h \in H\}$ of the various elements x of G.

Definition 2.7 (Homogeneous spaces). Suppose that H is a subgroup of a group G.

(a) Define $H\backslash G = \{Hx \mid x \in G\}\,.$
(b) The *homogeneous space* $H\backslash G$ is the right G-set $(H\backslash G, G)$ with action

$$g\colon H\backslash G \to H\backslash G; Hx \mapsto Hxg \tag{2.3}$$

for g in G.

Example 2.8. The map $G \to \{1\}\backslash G; x \mapsto \{x\}$ gives a G-isomorphism from the right regular representation of G to the homogeneous space $(\{1\}\backslash G, G)$ of the trivial subgroup.

Remark 2.9. The arguments of the functions g in (2.3) are right cosets. Moving down one level in the **element** $<$ **set** $<$ **set of sets** hierarchy, one obtains mutually inverse functions

$$g\colon Hx \to Hxg; y \mapsto yg$$

and

$$g^{-1}\colon Hxg \to Hx; z \mapsto zg^{-1}\,.$$

Thus the various right cosets of H are isomorphic as sets. When H is finite, this means that the cosets all have $|H|$ elements. If G is finite,

$$|G| = |H| \cdot |H\backslash G|, \tag{2.4}$$

so $|H|$ divides $|G|$. This is *Lagrange's Theorem.*

Definition 2.10. Let x be an element of a G-set X. Then the *stabilizer* or "isotropy subgroup" is $G_x = \{g \in G \mid xg = x\}$.

Lemma 2.11. *The stabilizer is a subgroup of G.*

Proposition 2.12. *Let (X, G) be an irreducible G-set.*

(a) *If x and y are elements of X, then the stabilizer subgroups G_x and G_y are conjugate.*
(b) *For each element x of X, the G-set (X, G) is G-isomorphic to the homogeneous space $G_x\backslash G$ of G.*

Proof. (a) Since the orbit xG is a non-empty G-subset of the irreducible G-set X, it is the improper subset $xG = X$. Thus $y \in G$, so $y = xg$ for some element g of G. For $s \in G_x$, one has $yg^{-1}sg = xsg = xg = y$. Then $g^{-1}G_xg \subseteq G_y$. Conversely, for $t \in G_y$, one has $x(gtg^{-1}) = x$, so $gtg^{-1} \in G_x$ and $t \in g^{-1}G_xg$. Thus $G_y \subseteq g^{-1}G_xg$ and $G_y = g^{-1}G_xg$.

(b) Consider the surjective G-set homomorphism

$$\varphi\colon (G, G) \to (X, G); g \mapsto xg$$

from the right regular representation (G, G). For a general element g of G, one has $g^{\ker\varphi} = \{h \in G \mid xg = xh\} = \{h \in G \mid hg^{-1} \in G_x\} = G_xg$. Thus $G^{\ker\varphi} = G_x\backslash G$ and $G\varphi = X$. The First Isomorphism Theorem for Algebras (1.7) provides the G-set isomorphism $b\colon G_x\backslash G \to (X, G)$. $\square$

2.2.3. *Isomorphism of homogeneous spaces.* The final step in our program is to determine when two homogeneous spaces are isomorphic as G-sets.

Proposition 2.13. *Let H and K be subgroups of G. Then there is a G-homomorphism $\varphi\colon (H\backslash G, G) \to (K\backslash G, G)$ if and only if there is an element f of G such that $H \subseteq f^{-1}Kf$.*

PROOF. Suppose there is a G-homomorphism $\varphi\colon H\backslash G \to K\backslash G$. Suppose $H\varphi$ is the coset Kf of K, for some element f of G. Then for each element h of H, the intertwining (2.1) shows that

$$Kf = H\varphi = Hh\varphi = H\varphi h = Kfh\,,$$

so that $fhf^{-1} \in K$ and $h \in f^{-1}Kf$. Thus $H \subseteq f^{-1}Kf$.

Conversely, suppose $H \subseteq f^{-1}Kf$. Then the function

$$\varphi\colon H\backslash G \to K\backslash G; Hx \mapsto Kfx$$

is well-defined. Indeed, for elements x, x' of G, suppose $Hx = Hx'$. Then $x'x^{-1} \in H \subseteq f^{-1}Kf$, so $f^{-1}Kfx = f^{-1}Kfx'$ and $Kfx = Kfx'$. Finally, φ is a G-homomorphism, since $Hxg\varphi = Kfxg = Hx\varphi g$ for elements x and g of G. □

COROLLARY 2.14. (a) *The homogeneous spaces $H\backslash G$ and $K\backslash G$ are isomorphic if and only if there are group elements f and g such that $g^{-1}Kg \subseteq H \subseteq f^{-1}Kf$.*

(b) *Suppose that G is finite. Then the homogeneous spaces $H\backslash G$ and $K\backslash G$ are isomorphic if and only if the groups H and K are conjugate.*

PROOF. (a) The inverse isomorphism $\varphi^{-1}\colon K\backslash G \to H\backslash G$ yields a group element g with $K \subseteq gHg^{-1}$. The result follows.

(b) If G is finite, one has $|G|/|H| = |H\backslash G| = |K\backslash G| = |G|/|K|$ by (2.4), whence $|H| = |K|$. The desired equality $H = f^{-1}Kf$ follows. □

REMARK 2.15. In an infinite group G, one may have a subgroup H and an element f with a proper containment $H \subset f^{-1}Hf$. See Exercise 18.

2.3. The class of all actions.

DEFINITION 2.16. Let (X, M, r) and (Y, N, s) be monoid actions.

(a) An *action morphism*

$$(\varphi, f)\colon (X, M, r) \to (Y, N, s) \tag{2.5}$$

is a pair consisting of a monoid homomorphism $f\colon M \to N$ and an M-homomorphism $\varphi\colon (X, M, r) \to (Y, M, fs)$.

(b) The action morphism (2.5) is a *similarity* if f is a monoid isomorphism and φ is an M-isomorphism. In this case the M-set X and the N-set Y are said to be *similar*.

The category $(\mathbf{Set}; \mathbf{Mon})$ has object class the class of all monoid actions, and morphism class the class of all action morphisms.

2.3.1. *Restriction and induction.* If M is a submonoid of a monoid N, and (Y, N, s) is an N-set, the *restriction* $(Y, N, s){\downarrow}^N_M$ or $Y{\downarrow}^N_M$ of (Y, N, s) to M is the M-set induced by the insertion $j \colon M \hookrightarrow N$.

PROPOSITION 2.17. *Let (X, M, r) be a right M-set. Define a relation V on $X \times N$ by*

$$(x_1, n_1)\ V\ (x_2, n_2) \ \Leftrightarrow\ \exists\, x \in X, m \in M\ .\ x_1 = x_2 m \text{ and } n_2 = mn_1\,.$$

Let E be the smallest equivalence relation on $X \times M$ that contains V. Then a right representation s of N is well-defined by

$$(x, n')^E n^s = (x, n'n)^E$$

for $x \in X$ and $n, n' \in N$.

REMARK 2.18. Consider the situation of Proposition 2.17.

(a) The relation V is a pre-order. Then two elements $(x, n), (x', n')$ of $X \times N$ are related by E if and only if there is a natural number k and elements (x_i, n_i) of $X \times N$ such that $(x, n) = (x_0, n_0)$, $(x', n') = (x_{2k}, n_{2k})$, and $(x_{2j}, n_{2j})\ V\ (x_{2j+1}, n_{2j+1})$, $(x_{2j+1}, n_{2j+1})\ V'\ (x_{2j+2}, n_{2j+2})$ for $0 \le j < k$.

(b) If N is a group, then $V = E$.

DEFINITION 2.19. The N-set $\big((X \times N)^E, N, s\big)$ of Proposition 2.17 is called the N-set $(X, M, r){\uparrow}^N_M$ or $X{\uparrow}^N_M$ *induced* by the M-set (X, M, r).

PROPOSITION 2.20. *Let M be a submonoid of a monoid N. For an M-set (X, M, r) and an N-set (Y, N, s), there is an isomorphism*

$$\underline{\underline{N}}(X{\uparrow}^N_M, Y) \cong \underline{\underline{M}}(X, Y{\downarrow}^N_M)$$

of corresponding morphism sets.

2.3.2. *Wreath products.* Let (X, M, r) and (Y, N, s) be right monoid representations. Consider the left representation (M^Y, N, l) dual to (Y, N, s), with

$$y(n^l f) = (yn^s)f$$

for $y \in Y$, $n \in N$, and $f \colon Y \to M$ (compare §1.5). Let $e \colon Y \to M$ be the constant function with image $\{1\}$. Note that M^Y is a monoid, with a *pointwise product* defined by the product

$$y(f \cdot f') = yf \cdot yf'$$

in the monoid M for $y \in Y$ and $f, f' \in M^Y$. The identity element of the monoid M^Y is the constant function e.

PROPOSITION 2.21. *Define a product on the set* $M^Y \times N$ *by*

$$(f, n)(f', n') = (f \cdot n^l f', nn')$$

for $f, f' \in M^Y$ *and* $n, n' \in N$. *Then* $M^Y \times N$ *is a monoid, with identity element* $(e, 1)$.

DEFINITION 2.22. The monoid $M^Y \times N$ of Proposition 2.21 is defined as the *wreath product monoid* $M \wr (Y, N, s)$ or $M \wr (Y, N)$.

PROPOSITION 2.23. *The wreath product monoid* $M \wr (Y, N, s)$ *has a right representation* $r \wr s$ *on* $X \times Y$ *given by*

$$(x, y)(f, n)^{r \wr s} = \big(x(yf)^r, yn^s\big)$$

for $x \in X$, $y \in Y$, $f\colon Y \to M$ *and* $n \in N$.

DEFINITION 2.24. The action $r \wr s$ of Proposition 2.23 is defined as the *wreath product action* of $M \wr (Y, N)$ on $X \times Y$.

3. Exercises

(1) Prove Lemma 1.3.
(2) Is a semigroup homomorphism between monoids necessarily a monoid homomorphism? Justify your answer.
(3) Let $f\colon U \to V$ be a linear transformation between real vector spaces of finite dimension.
   (a) Show that $\operatorname{Ker} f = 0^{\ker f}$ is a subspace of U.
   (b) Suppose that a basis C of $\operatorname{Ker} f$ extends to a basis $B \dot{\cup} C$ (disjoint union) of U. Show that $\{b + \operatorname{Ker} f \mid b \in B\}$ is a basis for $U^{\ker f}$.
   (c) Use the First Isomorphism Theorem to conclude that the equality $\dim U - \dim \ker f = \dim Uf$ holds.
(4) Prove Proposition 1.10.
(5) Show that the homothety representation of the semigroup $(\mathbb{R}, \cdot)$ in Example 1.11 is faithful if $\dim U > 0$.
(6) For a semigroup $(S, \cdot)$, show that left multiplications provide a left representation $L\colon S \to S^S; s \mapsto L(s)$.
(7) Show that a magma $(S, \cdot)$ is associative iff the commutativity condition

$$\forall\ s, t \in S\,,\ R(s)L(t) = L(t)R(s)$$

is satisfied.

(8) Give an example of a semigroup $(S, \cdot)$ for which the right regular representation is not faithful.

(9) Show that the set S of Example 1.16 forms a semigroup of functions on $\underline{2}$.

(10) Prove Cayley's Theorem.

(11) In the context of Proposition 1.22, show the right representation r of M is faithful if $|Y| > 1$ and the left representation l is faithful.

(12) Let S be a semigroup. For an S-homomorphism

$$\varphi \colon (X_1, S, r_1) \to (X_2, S, r_2)\,,$$

show that the relation $\ker \varphi$ is an S-subset of $(X_1 \times X_1, S, r)$ with $(x, x')s^r = (xs^{r_1}, x's^{r_1})$ for $x, x' \in X_1$ and $s \in S$.

(13) Give an example of a monoid M and an M-set (X, M) such that X is indecomposable, but not irreducible.

(14) Confirm that (2.2) yields a right representation of the group G.

(15) Determine the conjugacy classes of the symmetric group S_3.

(16) Verify Lemma 2.11.

(17) Let $\mathrm{Sb}(G)$ be the set of subgroups of a given group G. Show that the relation

$$H \ V \ K \quad \Leftrightarrow \quad \exists\, f \in G\,.\ H \subseteq f^{-1}Kf$$

is a preorder on $\mathrm{Sb}(G)$.

(18) Let G be the group of invertible 2×2 real matrices. Let p be a prime number. Consider the element

$$g = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}$$

of G, and the subset

$$H = \left\{ \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \;\middle|\; m \in \mathbb{Z} \right\}$$

of G.

(a) Show that H is a subgroup of G.

(b) Show that

$$g^{-n}Hg^{n} = \left\{ \begin{bmatrix} 1 & mp^{-n} \\ 0 & 1 \end{bmatrix} \;\middle|\; m \in \mathbb{Z} \right\}$$

for each integer n.

(c) Show that there is a properly nested sequence

$$\ldots \subset g^2Hg^{-2} \subset gHg^{-1} \subset H \subset g^{-1}Hg \subset g^{-2}Hg^2 \subset \ldots$$

of conjugates of H.

(d) Show that the homogenous space $(H\backslash G)$ is faithful.

(19) Let M and N be monoids. Consider an M-set (X, M, r) and an N-set (Y, N, s).

(a) Show that there is an action t of $M \times N$ on $X \times Y$ given by $(x, y)(m, n)^t = (xm^r, yn^s)$ for $x \in X$, $y \in Y$, $m \in M$, and $n \in N$.

(b) Show that $(X \times Y, M \times N, t)$ is the product of (X, M, r) and (Y, N, s) in the category $(\mathbf{Set}; \mathbf{Mon})$.

(c) Do (X, M, r) and (Y, N, s) have a coproduct in the category $(\mathbf{Set}; \mathbf{Mon})$?

(20) Verify Proposition 2.17, at least in the case where N is a group.

(21) Prove Proposition 2.20.

(22) Verify Proposition 2.21.

(23) Verify Proposition 2.23.

(24) Let M be the 2-element cyclic group $\mathbb{Z}/_2$, and let C_2 be the right regular representation of M.

(a) Show that $M \wr C_2$ is (isomorphic to) the Sylow 2-subgroup H of the symmetric group S_4.

(b) Let $(\underline{4}, H)$ be the restriction to H of the action of S_4 on $\underline{4}$. Show that $(\underline{4}, H)$ is similar to the wreath product action of $M \wr C_2$ on $C_2 \times C_2$.

CHAPTER 4

Free groups and monoids

1. Free groups

Let X be a set. Let V be a (real) vector space with basis X. Consider the insertion $\eta_X \colon X \to V; x \mapsto x$ of the subset X into V. Then for each real vector space U, each function $f \colon X \to U$ has a unique linear extension $\overline{f} \colon U \to V$, defined by

$$(\lambda_1 x_1 + \cdots + \lambda_r x_r)\overline{f} = \lambda_1 x_1 f + \cdots + \lambda_r x_r f$$

for scalars $\lambda_1, \ldots, \lambda_r$ and elements $x_1, \ldots, x_r$ of X. The fact that $\overline{f}$ is an extension of f is expressed by the equation $\eta_X \overline{f} = f$. The fact that $\overline{f}$ is the unique linear extension of f is expressed conventionally by the commuting diagram

(1.1)
$$\begin{tikzcd}
V \arrow[dr, dashed, "\overline{f}"] & \\
X \arrow[u, "\eta_X"] \arrow[r, "f"'] & U
\end{tikzcd}$$

where the dashed format of the arrow labeled $\overline{f}$ records the existence and uniqueness of that function.

The vector space V with basis X may be described as the *free vector space* over the set X in the context of the diagram (1.1). In this context, it is best to think of V as the space

$$V = \left\{ \sum_{i=1}^{r} \lambda_i x_i \;\middle|\; r \in \mathbb{N},\ x_1, \ldots, x_r \in X,\ \lambda_1, \ldots, \lambda_r \in \mathbb{R} \right\} \tag{1.2}$$

of all linear combinations of elements of the set X. Note that the vector 0 corresponds to the “empty” linear combination with $r = 0$ in (1.2).

1.1. Free abelian groups. Let X be a set. The *free abelian group* $\mathbb{Z}X$ over X is defined by a property analogous to the property expressed by the diagram (1.1). Specifically, define Λ or

$$\mathbb{Z}X = \left\{ \sum_{i=1}^{r} n_i x_i \;\middle|\; r \in \mathbb{N},\ x_1, \dots, x_r \in X,\ n_1, \dots, n_r \in \mathbb{Z} \right\} \tag{1.3}$$

as a subset of the vector space V in (1.2). Note that $(\mathbb{Z}X, +, 0)$ is an abelian subgroup of the abelian group $(V, +, 0)$. Also, note that the function $\eta_X \colon X \to V; x \mapsto x$ of (1.1) allows its codomain to be cut down to yield a new function $\eta_X \colon X \to \mathbb{Z}X; x \mapsto x$.

(1.4)
$$\begin{tikzcd} \mathbb{Z}X \arrow[dr, dashed, "\overline{f}"] & \\ X \arrow[u, "\eta_X"] \arrow[r, "f"'] & A \end{tikzcd}$$

Proposition 1.1. *Let A be an abelian group. Then for each function $f \colon X \to A$, there is a unique group homomorphism*

$$\overline{f} \colon \mathbb{Z}X \to A; \sum_{i=1}^{r} n_i x_i \mapsto \sum_{i=1}^{r} n_i (x_i f)$$

such that $\eta_X \overline{f} = f$.

It is sometimes convenient to refer to the subset (1.3) of the free vector space V on X as a *lattice* Λ, a discrete set of position vectors carrying the free abelian group structure. (Compare Exercise 3.) One then reserves the notation $\mathbb{Z}X$ for the group structure itself, which may be considered as a group of translation vectors. The right regular representation of $\mathbb{Z}X$ given by Cayley's Theorem is then written as $(\Lambda, \mathbb{Z}X)$.

1.2. Automata and free monoids.

1.2.1. *Dynamical systems and automata.* One defines a *dynamical system* (X, T) to be a set X (called the *state space*) equipped with a function $T \colon X \to X$, the *evolution operator*. If an element x of the state space represents the state of a physical system at a given time, then xT is the state of the system one time unit later. The dynamical system is *reversible* if $T \colon X \to X$ is bijective.

More generally, an *automaton* (X, E) is a set X (again called the *state space*) equipped with a set E of functions $e\colon X \to X$, known as (*elementary*) *events*. If the system is in a state x, and event e occurs, then the system *transitions* to state xe. By convention of the model, the system is subject to no more than one event at any given time.

An automaton (X, E) may be described by a labeled graph (with loops), the *transition diagram*. For each event e, each state x is the tail of a directed edge $x \xrightarrow{e} xe$. If an event e does not change a state x, one may choose to omit the corresponding loop labeled e at x, thereby obtaining the transition diagram as a directed graph without loops.

1.2.2. *Free monoids.* Let A be a set, described in the current context as an *alphabet*. For brevity, encode a tuple $(a_1, \dots, a_n)$ from a direct power A^n as a string $a_1 \dots a_n$, thus interpreting A^n as the set of *words of length* n in the alphabet A. In particular, write the singleton A^0 as $\{1\}$, so that 1 is the *empty word*.

Now define A^* to be the disjoint union $\sum_{n \in \mathbb{N}} A^n$. A monoid $(A^*, \cdot, 1)$ is defined on A^* by the *concatenations*

$$A^m \times A^n \to A^{m+n}; (a_1 \dots a_m, b_1 \dots b_n) \mapsto a_1 \dots a_m b_1 \dots b_n$$

for positive integers m, n. On the strength of the proposition below, the monoid A^* becomes the *free monoid* on the set A, with the function $\eta_A\colon A \to A^*; a \mapsto a$ inserting letters as words of length 1.

(1.5)
$$\begin{tikzcd} A^* \arrow[dr, dashed, "\overline{f}"] & \\ A \arrow[u, "\eta_A"] \arrow[r, "f"'] & M \end{tikzcd}$$

PROPOSITION 1.2. *Let M be a monoid. For each function $f\colon A \to M$, there is a unique monoid homomorphism*

$$\overline{f}\colon A^* \to M; a_1 a_2 \dots a_r \mapsto (a_1 f)(a_2 f) \dots (a_r f)$$

such that $\eta_A \overline{f} = f$.

COROLLARY 1.3. *Let (X, E) be an automaton. Then for the insertion $j\colon E \hookrightarrow X^X; e \mapsto e$, the extension $\overline{j}\colon E^* \to X^X$ yields a representation of E^* on X.*

REMARK 1.4. In the context of Corollary 1.3, words from E^* may be described as *compound events* of the automaton (X, E), to distinguish from the elementary events in the alphabet E.

1.2.3. *Free semigroups.* Given a set A, the set A^+ of words of positive length with letters from the alphabet A forms a subsemigroup of A^*. This semigroup is known as the *free semigroup* on the set A, since analogues of (1.5) and Proposition 1.2 may be formulated (Exercise 4).

DEFINITION 1.5. A subset C of A^+ is a *code* over the alphabet A if

$$\forall\ 0 < m, n \in \mathbb{Z}\,,\ \forall\ c_1, \dots, c_m, d_1, \dots, d_n \in C\,,$$
$$c_1 \dots c_m = d_1 \dots d_n\ \Rightarrow\ m = n\,,\ c_1 = d_1\,,\ \dots, c_m = d_m\,.$$

1.3. Action on trees. Let X be a set. The goal is to construct a group XG, together with a function $\eta_X \colon X \to XG$, such that for each function $f \colon X \to M$ from X to a group M, there is a unique group homomorphism $\overline{f} \colon XG \to M$ such that $\eta_X \overline{f} = f$:

$$\begin{tikzcd} XG \arrow[dr, dashed, "\overline{f}"] & \\ X \arrow[u, "\eta_X"] \arrow[r, "f"'] & M \end{tikzcd} \tag{1.6}$$

The group XG is known as the *free group* over the set X.

The free abelian group $\mathbb{Z}X$ over X, constructed in §1.1, emerged with a representation $(\Lambda, \mathbb{Z}X)$ by translation vectors acting on the lattice Λ of point vectors. The construction of the free group is similar, but more complex. The free group will be described by the action of an automaton, whose state space will be (the vertex set of) a tree Γ. Figure 1 illustrates the tree for the free group over the two-element set $\{x_1, x_2\}$.

Given the set X, let $A = X + XJ$ be the disjoint union of two copies of the set X. The insertions are $x \mapsto x$ and $x \mapsto x^J$. Define the map $J \colon A \to A$ with $J^2 = 1_A$ by $J \colon x \mapsto x^J$. Let Γ denote the subset of the free monoid A^* consisting of those words in the alphabet A in which no letter a is immediately followed by a^J. For $x_1, x_2 \in X$, the word $x_1 x_2^J x_1 x_2$ lies in Γ, but the word $x_1 x_2^J x_2 x_1$ does not.

The automaton (Γ, A) will now be constructed. Consider an element a^J of A. The state space Γ decomposes into two parts: the set

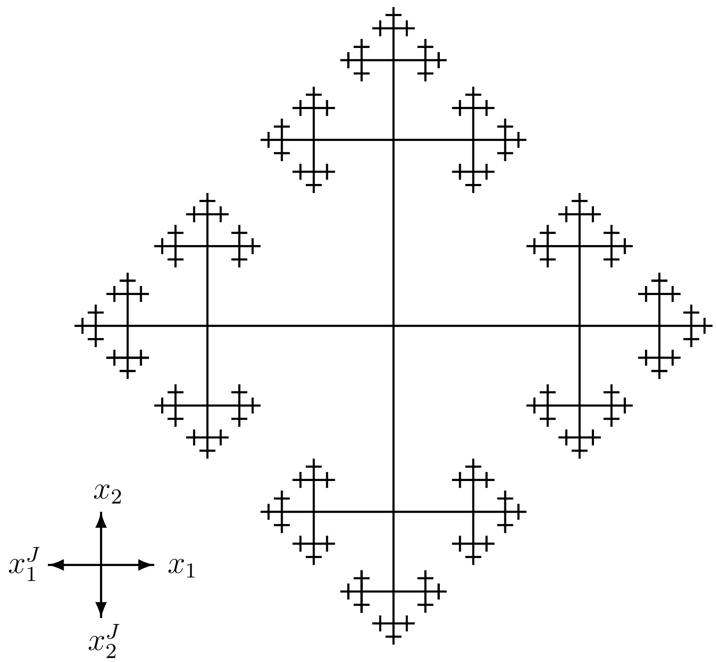


Figure 1. Tree structure for the free group on two generators.

Γ_a of words ending in a, and its complement $\overline{\Gamma}_a$. The elementary event a^J then acts as follows:

$$a^J\colon \begin{cases} pa \mapsto p & \text{for } pa \in \Gamma_a\,; \\ q \mapsto qa^J & \text{for } q \in \overline{\Gamma}_a\,. \end{cases}$$

This elementary action is invertible, and its two-sided inverse is the action of a.

Since the composition of bijections is bijective, compound actions of the automaton (Γ, A) also biject. The inverse of the compound action of a word $a_1 \dots a_n$ in A^* is the compound action of the word $a_n^J \dots a_1^J$. Thus the image of A^* under the representation $r\colon A^* \to \Gamma^\Gamma$ given by Corollary 1.3 is actually a subgroup of $\Gamma!$. This subgroup is defined to be the free group XG. Thus the representation yields a monoid homomorphism

$$r\colon A^* \to XG\,.$$

Furthermore, there is the insertion $\eta_X\colon X \to XG; x \mapsto x^r$.

1.4. The free group XG on the set X.

1.4.1. *Group equivalence.* Let $u = a_1 \dots a_m$ and v be words in A^*, with letters $a_1, \dots, a_m$. The word v is said to be (obtained from u by) an *elementary reduction* of u if $a_i a_{i+1} = aa^J$ for some $1 \le i < m$ and a in A, and then $v = a_1 \dots a_{i-1} a_{i+2} \dots a_m$. Successive application of at most $\lfloor m/2 \rfloor$ elementary reductions to u reduces it to a word in Γ that is the result $1u^r$ of acting on 1 in Γ by the compound event u of A^*. Two words u, v in A are said to be *group equivalent* if and only if $1u^r = 1v^r$. Note that group equivalence is an equivalence relation, the relation kernel of the function $A^* \to \Gamma; u \mapsto 1u^r$. Moreover, Γ is a full set of representatives for the equivalence classes. The element $1u^r$ of Γ is called the (*completely*) *reduced form* or *normal form* of u.

1.4.2. *Extension to a homomorphism.* Let $f \colon X \to M$ be a function from the set X to a group M. The extension $\overline{f}$ of (1.6) will be constructed. Initially, the function extends to $f \colon A \to M$ by $x^J f = (xf)^{-1}$ for $x \in X$. By the free monoid property (1.5), there is a unique monoid homomorphism $f' \colon A^* \to M$ extending $f \colon A \to M$. If $u = saa^J t$ and $v = st$ in A^*, then

$$\begin{aligned} uf' &= saa^J tf' \\ &= sf' \cdot af \cdot a^J f \cdot tf' \\ &= sf' \cdot af \cdot (af)^{-1} \cdot tf' \\ &= sf' \cdot tf' = stf' = vf' , \end{aligned}$$

so that group-equivalent words u, v in A^* have the same images uf', vf' in the group M.

LEMMA 1.6. *The set Γ of A^* carries a well-defined group structure*

$$p \cdot q = pq^r \tag{1.7}$$

that makes it isomorphic to the group XG.

PROOF. In the considerations above, interpret the function $f \colon X \to M$ as $\eta_X \colon X \to XG; x \mapsto x^r$. Then for u, v in Γ, the group-equivalence $1u^r = 1v^r$ implies $u\eta'_X = v\eta'_X$, so that $pu^r = pv^r$ for all p in Γ. In other words, the map

$$\theta \colon XG \to \Gamma; u^r \mapsto 1u^r \tag{1.8}$$

is injective. Since $p = 1p^r$ for p in Γ, the map θ of (1.8) is also surjective. With the product in Γ defined by (1.7), the map θ becomes a group isomorphism. Indeed, one has

$$(p^r q^r)\,\theta = (pq)^r\theta = 1(pq)^r = 1p^r q^r = pq^r = p\cdot q = 1p^r \cdot 1q^r = p^r\theta\cdot q^r\theta$$

for general elements p^r and q^r of XG, with p and q in Γ. □

Now consider the monoid homomorphism $f'\colon A^*\to M$. Then for p and q in Γ, one has $pf'\cdot qf' = pqf' = pq^r f' = (p\cdot q)f'$. Thus the monoid homomorphism $f'\colon A^*\to M$ restricts to a group homomorphism $f'\colon(\Gamma,\cdot,1)\to M$. Finally, define

$$\overline{f} = \theta f'\colon XG\to\Gamma\to M \tag{1.9}$$

as the composite group homomorphism. Since $x\eta_X\overline{f} = x^r\theta f' = 1x^r f' = xf' = xf$ for x in X, the homomorphism (1.9) gives the required extension of $f\colon X\to M$.

2. Free commutative semigroups and partitions

2.1. Free commutative monoids. Let X be a set. There are many ways to build a free commutative monoid $\mathbb{N}X$ on X. Mimicking §1.1, one may take

$$\mathbb{N}X = \left\{\sum_{i=1}^{r} n_i x_i \;\middle|\; r\in\mathbb{N},\ x_1,\dots,x_r\in X,\ n_1,\dots,n_r\in\mathbb{N}\right\} \tag{2.1}$$

as a subset of the vector space V in (1.2). Note that $(\mathbb{N}X,+,0)$ is a submonoid of the commutative monoid $(V,+,0)$. Also, note that the function $\eta_X\colon X\to V; x\mapsto x$ of (1.1) allows its codomain to be cut down to yield a new function $\eta_X\colon X\to\mathbb{N}X; x\mapsto x$.

$$\begin{tikzcd} \mathbb{N}X \arrow[dr, dashed, "\overline{f}"] & \\ X \arrow[u, "\eta_X"] \arrow[r, "f"'] & M \end{tikzcd} \tag{2.2}$$

Proposition 2.1. *Let M be a commutative monoid. Then for each function $f\colon X\to M$, there is a unique monoid homomorphism*

$$\overline{f}\colon\mathbb{N}X\to M;\sum_{i=1}^{r} n_i x_i\mapsto\prod_{i=1}^{r}(x_i f)^{n_i}$$

such that $\eta_X\overline{f} = f$.

2.1.1. *Other interpretations.* A natural-number linear combination

$$n_1x_1 + \cdots + n_rx_r$$

appearing in (2.1) may be interpreted as a *multiset*

$$\Big\langle \overbrace{x_1, \dots, x_1}^{n_1 \text{ times}}, \dots, \overbrace{x_r, \dots, x_r}^{n_r \text{ times}} \Big\rangle \tag{2.3}$$

where the particular order in which elements appear is irrelevant (just as in ordinary sets), but where the multiplicity of occurrence of each element *is* counted. The empty linear combination 0 corresponds to the empty multiset $\langle\ \rangle$. The free monoid operation, addition of linear combinations, is taken as a union for multisets. Thus

$$\langle 1, 1, 1, 2\rangle \cup \langle 1, 3\rangle = \langle 1, 1, 1, 1, 2, 3\rangle\,,$$

for example. Sometimes, the multiset (2.3) is written with a *power notation* as $x_1^{n_1} \dots x_r^{n_r}$. In this convention, the monoid operation (just juxtaposition) is taken multiplicatively, and zero-th powers give the identity element of the monoid.

By (2.2), the constant function $f\colon X \to \mathbb{N}; x \mapsto 1$ extends to a monoid homomorphism $\overline{f}\colon \mathbb{N}X \to \mathbb{N}$. The value $|S|$ of $\overline{f}$ at a multiset S is known as the *size* of the multiset. For example, $|\langle 1, 1, 1, 2\rangle| = 4$.

2.2. Free commutative semigroups. Let X be a set. The set of non-zero elements of the free commutative monoid $(\mathbb{N}X, +, 0)$ forms the *free commutative semigroup* X^{c} on X. As usual, there are appropriate analogues of (2.2) and Proposition 2.1:

$$\begin{tikzcd} X^{\mathsf{c}} \arrow[dr, dashed, "\overline{f}"] & \\ X \arrow[u, "\eta_X"] \arrow[r, "f"'] & S \end{tikzcd} \tag{2.4}$$

Proposition 2.2. *Let S be a commutative semigroup. Then for each function $f\colon X \to S$, there is a unique semigroup homomorphism*

$$\overline{f}\colon X^{\mathsf{c}} \to S; \sum_{i=1}^{r} n_ix_i \mapsto \prod_{i=1}^{r} (x_if)^{n_i}$$

such that $\eta_X\overline{f} = f$.

REMARK 2.3. The other interpretations of free commutative monoid elements discussed in §2.1.1 apply in particular to the non-identity elements, as free commutative semigroup elements.

2.3. Integer partitions. Denote the singleton semigroup $(\{1\}, \cdot)$ by 1. As in §2.2, the free commutative semigroup 1^{c} may be identified with the semigroup $(\mathbb{Z}^+, +)$ of positive integers under addition. Thus the free commutative semigroup over $\mathbb{Z}^+$ is 1^{cc}. Elements λ of 1^{cc} are called *integer partitions*.

In accord with Remark 2.3, various notations for integer partitions are used, such as the *sum form*, e.g., $4+2+2+1$, or the *product form*, e.g., $4^1 2^2 1^1$ or $4^1 3^0 2^2 1^1$, or the *multiset form* $\langle 4, 2, 2, 1\rangle$. The elements of the multiset are called the *parts* of the partition.

The constant function $1^{\mathsf{c}} \to 1^{\mathsf{c}}$ with image 1 extends to a semigroup homomorphism $1^{\mathsf{cc}} \to 1^{\mathsf{c}}$ whose values $|\lambda|$ give the *length* of a partition λ, the size of the multiset or the number of parts. For example, the length of the partition $4 + 2 + 2 + 1$ is 4.

The identity function $\mathrm{id}_{1^{\mathsf{c}}} \colon 1^{\mathsf{c}} \to 1^{\mathsf{c}}$ also extends to a semigroup homomorphism $\overline{\mathrm{id}_{1^{\mathsf{c}}}} \colon 1^{\mathsf{cc}} \to 1^{\mathsf{c}}$, whose values give the *sum* of a partition. For example, the sum of the partition $4 + 2 + 2 + 1$ is 9. For a partition λ, the functional relationship $\lambda\, \overline{\mathrm{id}_{1^{\mathsf{c}}}} = n$ is written as $\lambda \vdash n$.

2.3.1. *Segre characteristics.* Elements of 1^{ccc} are multisets of multisets of positive integers. They are known as *Segre characteristics*. Note that a classically written Segre characteristic such as [(22)3(11)] denotes the multiset $\langle\langle 2, 2\rangle, \langle 3\rangle, \langle 1, 1\rangle\rangle$ of multisets.

Segre characteristics are used to specify the blocks in the Jordan normal form of a matrix over an algebraically closed field, such as the field of complex numbers. For example, the Jordan normal form

$$
\begin{bmatrix}
\begin{bmatrix}\lambda_1 & 1 \\ & \lambda_1\end{bmatrix} & & & & \\
& \begin{bmatrix}\lambda_1 & 1 \\ & \lambda_1\end{bmatrix} & & & \\
& & \begin{bmatrix}\lambda_2 & 1 & \\ & \lambda_2 & \\ & & \lambda_2\end{bmatrix} & & \\
& & & \begin{bmatrix}\lambda_3\end{bmatrix} & \\
& & & & \begin{bmatrix}\lambda_3\end{bmatrix}
\end{bmatrix}
$$

corresponds to the Segre characteristic [(22)3(11)].

2.4. Conjugacy classes of symmetric groups. One of the primary algebraic applications of integer partitions is the specification of the conjugacy classes in a symmetric group S_n for a positive integer n.

Let p be a permutation of $\underline{n}$, i.e., an element of S_n. The set of powers
$$p^{\mathbb{Z}} = \{p^r \mid r \in \mathbb{Z}\}$$
forms a subgroup of S_n. The $p^{\mathbb{Z}}$-set $\underline{n}$ decomposes as a disjoint union of orbits. If the respective orbit sizes are $n_1 \geq n_2 \geq \ldots \geq n_l$, then $n_1 + n_2 + \ldots + n_l$ is the sum form of a partition of n, the so-called *cycle type* of p.

THEOREM 2.4. *Suppose $\lambda \vdash n$. Then the set of all permutations of $\underline{n}$ with cycle type λ forms a conjugacy class C_λ of S_n. Indeed,*
$$S_n = \sum_{\mu \vdash n} C_\mu$$
is the orbit decomposition of S_n under the conjugacy action.

REMARK 2.5. The proof of Theorem 2.4 is assigned as Exercise 18. Recall that on a $p^{\mathbb{Z}}$-orbit $\{x_i \mid i \in \mathbb{Z}/_k\}$ of length k, a permutation p acts as a cycle $(x_0\ x_1\ \ldots\ x_{k-1})\colon x_i \mapsto x_{i+1}$ of length k. Two cycles $(x_0\ x_1\ \ldots\ x_{k-1})$ and $(y_0\ y_1\ \ldots\ y_{k-1})$ of length k are conjugate by a permutation with $x_i \mapsto y_i$ for $i \in \mathbb{Z}/_k$. A permutation of cycle type $n_1 + n_2 + \ldots + n_l$ may be constructed as the product of disjoint cycles of respective lengths $n_1, n_2, \ldots, n_l$.

3. Exercises

(1) Verify Proposition 1.1.
(2) Suppose that there is a set bijection $b\colon X \to Y$. Show that the free abelian groups $\mathbb{Z}X$ and $\mathbb{Z}Y$ are isomorphic.
(3) For the respective choices

Square lattice:
$$\{(1,0),(0,1)\}$$
Rectangular lattice:
$$\{(1,0),(0,2)\}$$
Rhombic lattice:
$$\{(0,2),(1,1)\}$$

Oblique lattice:

$$\{(0,3),(1,1)\}$$

Triangular lattice:

$$\left\{(0,1)\,,\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right)\right\}$$

of the set X, draw the lattice Λ underlying the free abelian group $\mathbb{Z}X$ in the plane.

(4) Formulate and prove the freeness claims of §1.2.3.

(5) Show that $\{0,01,10\}$ is not a code over $\{0,1\}$.

(6) Given an alphabet A of size at least 3, fix one particular element, and call it the *comma*. A *comma code* C is a subset of A^* consisting of words, in each of which the comma appears just once, namely at the end. Show that C is a code over A.

(7) A word v in A^* is said to appear as a *proper suffix* in a word w if there is a word u in A^+ such that $w = uv$. A subset C of A^* is a *suffix code* if no element of C appears as a proper suffix of another. Show that a suffix code is a code over A.

(8) Consider the context of §1.4.1. Suppose that a word u of length m is group equivalent to 1. Show that m is even.

(9) For a singleton set X, show that $\mathbb{Z}X$ and XG are isomorphic.

(10) Show that a bijection $b\colon X \to Y$ extends to an isomorphism $\overline{b}\colon XG \to YG$.

(11) Let $X = \{x_1, x_2\}$. Consider a function $f\colon X \to S_3$ in which x_1f has order 2 and x_2f has order 3. Determine the respective function values under the extension $\overline{f}\colon XG \to S_3$ for reduced words of length less than 4 in the alphabet $\{x_1, x_2, x_1^{-1}, x_2^{-1}\}$.

(12) Let M be a group. Let $\{H_i \mid i \in I\}$ be a set of subgroups of M. Show that the intersection

$$\bigcap\{H_i \mid i \in I\} = \{x \in M \mid \exists\, i \in I\,.\, x \in H_i\}$$

is a subgroup of M.

(13) Let X be a subset of a group M. Let $j\colon X \hookrightarrow M$ be the inclusion of X in M. Consider the homomorphic extension $\overline{j}\colon XG \to M$. The image of $\overline{j}$ is called the *subgroup* $\langle X\rangle$ of M *generated* by X.

(a) Show directly that $\langle X\rangle$ is a subgroup of M.

(b) Show that $\langle X\rangle$ is the intersection of the set of subgroups of M that contain X.

(14) Show that the inclusion $P \hookrightarrow \mathbb{Z}^+$ of the set P of prime numbers in the set of positive integers extends to a monoid isomorphism $\mathbb{N}P \to (\mathbb{Z}^+, \cdot, 1)$. This is the classical Fundamental Theorem of Arithmetic.

(15) List all 7 partitions that sum to 5.

(16) Derive Euler's formula

$$\sum_{n=1}^{\infty} p(n)x^n = \prod_{m=1}^{\infty}(1-x^m)^{-1}$$

for the number $p(n)$ of partitions of a positive integer n.

(17) List all the possible Segre characteristics for the Jordan normal forms of 4×4-matrices over $\mathbb{C}$.

(18) Prove Theorem 2.4.

(19) For the partition $\lambda = n_1 + \ldots + n_l$ of a positive integer n, determine the size of the conjugacy class C_λ in S_n.

(20) In the group S_4, determine which unions of conjugacy classes form subgroups of S_4.

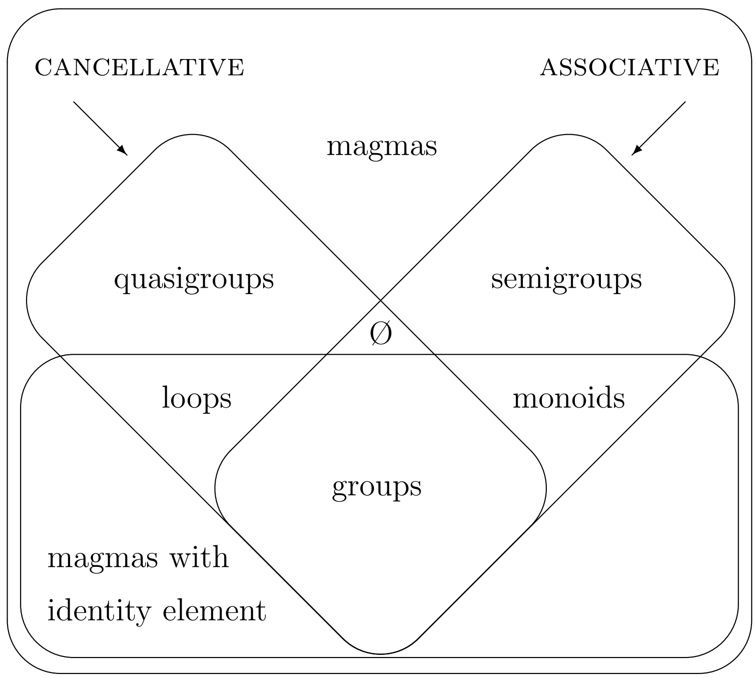
CHAPTER 5

Quasigroups and loops

1. Quasigroups and loops

1.1. Combinatorial quasigroups and loops.

1.1.1. *Magmas: Cancellativity versus associativity.*



1.1.2. *Right and left quasigroups.*

Definition 1.1. Let $(Q, \cdot)$ be a magma.

(a) The magma $(Q, \cdot)$ is said to be a (*combinatorial*) *right quasigroup* if the right multiplication

$$R(q)\colon Q \to Q; x \mapsto xq$$

is bijective for each element q of Q.

(b) The magma $(Q, \cdot)$ is said to be a (*combinatorial*) *left quasigroup* if the left multiplication

$$L(q)\colon Q \to Q; x \mapsto qx$$

is bijective for each element q of Q.

(c) The magma $(Q, \cdot)$ is said to be a (*combinatorial*) *quasigroup* if both the left multiplication $L(q)$ and right multiplication $R(q)$ are bijective for each element q of Q.

(d) A (non-empty) quasigroup $(Q, \cdot)$ is a *loop* if it has an element e such that the equations

$$e \cdot x = x = x \cdot e \tag{1.1}$$

hold for all x in Q. In this case, e is said to be the *identity element* of the loop $(Q, \cdot, e)$.

Lemma 1.2. *The identity element of a loop is unique*

Proof. If e and f are identity elements, then $e = e \cdot f = f$. □

Example 1.3 (Left projections give right quasigroups). Let X be a set. Define $x \cdot y = x$ for $x, y \in X$. Then $(X, \cdot)$ is an associative right quasigroup.

Example 1.4. Each group $(G, \cdot)$ is an associative quasigroup. The empty quasigroup $(\emptyset, \cdot)$ is (vacuously) associative. Each non-empty, associative quasigroup is a group (Exercise 2).

Example 1.5. Under subtraction, the integers form a non-associative quasigroup, but not a loop (Exercise 3). Similarly, for each positive integer n, the set $\mathbb{Z}/_n$ of integers modulo n forms a quasigroup under subtraction.

1.2. Equational quasigroups. Definition 1.1 gave a combinatorial specification of quasigroups. That definition is unsuitable for algebraic purposes: an alternative (Definition 1.7) is required.

1.2.1. *Right and left divisions.* Consider the equation $x \cdot b = c$ or $xR(b) = c$ in a right quasigroup $(Q, \cdot)$, with x as an unknown. Since $R(b)$ is surjective, a solution x exists. On the other hand, since $R(b)$ is injective, the solution x is unique. The solution $x = cR(b)^{-1}$ is written as $x = c/b$, and described as c *divided by* b or c *over* b or c *slash* b.

Dually, the unique solution $y = cL(a)^{-1}$ to $a \cdot y = c$ in a left quasigroup $(Q, \cdot)$ is written as $y = a \backslash c$, described verbally as *a dividing into c* or *a under c* or *a backslash c*.

If x and y are elements of a group $(Q, \cdot)$, then $x/y = xy^{-1}$ and $x \backslash y = x^{-1}y$.

In order to reduce the number of brackets in quasigroup expressions, multiplication denoted by juxtaposition will bind stronger than any explicitly written multiplications or divisions. For example, one may write the associative law as $xy \cdot z = x \cdot yz$, while the left hand side of (1.2) below may be written as xy/y.

PROPOSITION 1.6. *Let $(Q, \cdot)$ be a magma.*

(a) *If $(Q, \cdot)$ is a right quasigroup, then the identities*

$$(x \cdot y)/y = x = (x/y) \cdot y \tag{1.2}$$

are satisfied in Q.

(b) *If $(Q, \cdot)$ is a left quasigroup, then the identities*

$$x \backslash (x \cdot y) = y = x \cdot (x \backslash y) \tag{1.3}$$

are satisfied in Q.

1.2.2. *Equational quasigroups and loops.*

DEFINITION 1.7. (a) An algebra $(Q, \cdot, /)$ is a(n *equational*) *right quasigroup* if the identities (1.2) are satisfied.

(b) An algebra $(Q, \cdot, \backslash)$ is said to be a(n *equational*) *left quasigroup* if the identities (1.3) are satisfied.

(c) An algebra $(Q, \cdot, /, \backslash)$ is a(n *equational*) *quasigroup* if the identities (1.2) and (1.3) are satisfied.

(d) An algebra $(Q, \cdot, /, \backslash, 1e)$ is a(n *equational*) *loop* if the identities (1.2), (1.3), and (1.1) are satisfied.

REMARK 1.8. Proposition 1.6 implies that each combinatorial right quasigroup $(Q, \cdot)$ yields an equational right quasigroup $(Q, \cdot, /)$. The left and two-sided cases are similar.

PROPOSITION 1.9. (a) *An equational right quasigroup $(Q, \cdot, /)$ forms a combinatorial right quasigroup $(Q, \cdot)$.*

(b) *An equational left quasigroup $(Q, \cdot, \backslash)$ forms a combinatorial left quasigroup $(Q, \cdot)$.*

(c) *An equational quasigroup* $(Q, \cdot, /, \backslash)$ *forms a combinatorial quasigroup* $(Q, \cdot)$.

PROOF. In (1.2), the first equation shows that $R(y)$ is injective. The second shows that $R(y)$ is surjective. Similarly, (1.3) shows that $L(x)$ is bijective. $\square$

With the algebraic definitions, one may speak of right, left, and two-sided quasigroup or loop homomorphisms, subquasigroups, and so on. Similarly, the First Isomorphism Theorem applies to quasigroup and loop homomorphisms. Exercise 6 exhibits a surjective magma homomorphism from a combinatorial quasigroup to a magma which is not a combinatorial quasigroup.

1.3. Multiplication groups. Let $(Q, \cdot, /)$ be a right quasigroup. The *right multiplication group* $\mathrm{RMlt}(Q, \cdot, /)$ or $\mathrm{RMlt}\, Q$ of Q is the subgroup

$$\langle R(q) \mid q \in Q \rangle_{Q!}$$

of the permutation group $Q!$ generated by the set $\{R(q) \mid q \in Q\}$ of right multiplications by elements of Q. Similarly, the *left multiplication group* $\mathrm{LMlt}(Q, \cdot, \backslash)$ or $\mathrm{LMlt}\, Q$ of Q is the subgroup

$$\langle L(q) \mid q \in Q \rangle_{Q!}$$

of the permutation group $Q!$ generated by the set $\{L(q) \mid q \in Q\}$ of left multiplications by elements of Q. The (*two-sided*) *multiplication group* $\mathrm{Mlt}(Q, \cdot, /, \backslash)$ or $\mathrm{Mlt}\, Q$ of a quasigroup $(Q, \cdot, /, \backslash)$ is the subgroup

$$\langle L(q), R(q) \mid q \in Q \rangle_{Q!}$$

of the permutation group $Q!$ generated by the set $\{L(q), R(q) \mid q \in Q\}$ of all multiplications by elements of Q.

EXAMPLE 1.10. Let A be an abelian group. Then

$$L\colon A \to \mathrm{Mlt}\, A; x \mapsto L(x)$$

is a group isomorphism.

PROPOSITION 1.11. *Let* Q *be a group, with center*

$$Z = \{z \in Q \mid \forall\ x \in Q\,,\ zx = xz\}\,.$$

(a) *There are group isomorphisms*

$$R\colon Q \to \mathrm{RMlt}\, Q; q \mapsto R(q)$$

and

$$\Gamma\colon Q \to \mathrm{LMlt}\, Q; q \mapsto L(q)^{-1}\,.$$

(b) *There is a group homomorphism*

$$\Delta\colon Z \to \mathrm{LMlt}\, Q \times \mathrm{RMlt}\, Q; z \mapsto (L(z)^{-1}, R(z))\,.$$

(c) *There is a group homomorphism*

$$T\colon \mathrm{LMlt}\, Q \times \mathrm{RMlt}\, Q \to \mathrm{Mlt}\, Q; (L(x), R(y)) \mapsto L(x)^{-1}R(y)\,.$$

(d) *The group kernel of T is $Z\Delta$, so*

$$\mathrm{Mlt}\, Q \cong (\mathrm{LMlt}\, Q \times \mathrm{RMlt}\, Q)/Z\Delta\,.$$

DEFINITION 1.12. Let n be a positive integer. Then the *dihedral group* D_n of *degree* n is the multiplication group of the quasigroup $(\mathbb{Z}/_n, -)$ of integers modulo n under subtraction.

PROPOSITION 1.13. *For each positive integer n,*

$$D_n = \{L(r), R(r) \mid r \in (\mathbb{Z}/_n, -)\}\,.$$

In particular, $|D_n| = 2n$ for $n > 1$.

1.4. Quasigroup homotopies. Because (equational) quasigroups are algebras, the concept of a quasigroup homomorphism is standard. In many contexts, however, a more general notion is required.

DEFINITION 1.14. Let $(Q, \cdot, /, \backslash)$ and $(Q', \cdot, /, \backslash)$ be quasigroups.

(a) A triple

$$(f_1, f_2, f_3)\colon Q \to Q'$$

of functions from Q to Q' is a (*quasigroup*) *homotopy* if

$$x^{f_1} \cdot y^{f_2} = (xy)^{f_3}$$

for all x, y in Q.

(b) A homotopy $(f_1, f_2, f_3)\colon Q \to Q'$ is an *isotopy* if the functions f_1, f_2, f_3 are bijective. In this case, the quasigroups Q and Q' are said to be *isotopic*.

(c) An isotopy $(f_1, f_2, f_3)\colon Q \to Q'$ is said to be *principal* if $f_3 = \mathrm{id}_Q$ (so in particular the underlying sets of the quasigroups Q and Q' coincide). In this case, the quasigroups $(Q, \cdot, /, \backslash)$ and $(Q', \cdot, /, \backslash)$ are said to be *principally isotopic*.

REMARK 1.15. Note that a homotopy $(f_1, f_2, f_3)\colon Q \to Q'$ is a quasigroup homomorphism iff its three components f_1, f_2, f_3 coincide.

EXAMPLE 1.16. The triple $(1, -1, 1)\colon (\mathbb{Z}/_n, -) \to (\mathbb{Z}/_n, +)$ of scalar multiplications is a principal isotopy.

The following proposition gives constructions of certain quasigroups.

PROPOSITION 1.17. *Let $(Q', \cdot, /, \backslash)$ be a quasigroup. Let Q be a set. Consider a triple (f_1, f_2, f_3) of bijections $f_i\colon Q \to Q'$. Then there is a unique quasigroup structure on Q such that $(f_1, f_2, f_3)\colon Q \to Q'$ is an isotopy.*

The quasigroup structure built on Q by Proposition 1.17 is called the *quasigroup induced* by the homotopy (f_1, f_2, f_3). The proof of the proposition is assigned as Exercise 12. Here is a typical application.

EXAMPLE 1.18. The quasigroup structure $(\mathbb{R}, \circ)$ induced from the abelian group $(\mathbb{R}, +, 0)$ by the scalar multiple isotopy $(\frac{1}{2}, \frac{1}{2}, 1)$ is called the *arithmetic mean* quasigroup (Figure 1).

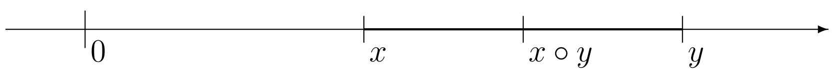


FIGURE 1. The arithmetic mean $x \circ y$ of x and y.

PROPOSITION 1.19. *Let $(Q, \cdot, /, \backslash)$, $(Q', \cdot, /, \backslash)$, and $(Q'', \cdot, /, \backslash)$ be quasigroups. Let $(f_1, f_2, f_3)\colon Q \to Q'$ and $(g_1, g_2, g_3)\colon Q' \to Q''$ be homotopies. Then the composite $(f_1g_1, f_2g_2, f_3g_3)\colon Q \to Q''$ is a homotopy.*

As a consequence of Proposition 1.19, one may define a large category $\mathbf{Qtp}$, with $\mathbf{Qtp}_0$ as the class of quasigroups. For quasigroups Q and Q', the morphism class $\mathbf{Qtp}(Q, Q')$ is the set of homotopies from Q to Q'. The category $\mathbf{Qtp}$ is contrasted with the category $\mathbf{Q}$ of homomorphisms between quasigroups.

The following decomposition of isotopies is often useful.

$$\begin{tikzcd}
P \arrow[r, "{(f,g,h)}"] \arrow[dr, "{(fh^{-1},gh^{-1},\mathrm{id}_P)}"'] & Q \\
& P' \arrow[u, "{(h,h,h)}"']
\end{tikzcd}$$

PROPOSITION 1.20. *Suppose that the triple* $(f, g, h)\colon P \to Q$ *is a quasigroup isotopy. Induce a quasigroup structure* P' *on the underlying set* P *by the isomorphism* (h, h, h)*. Then the isotopy* (f, g, h) *decomposes as the product of the principal isotopy* $(fh^{-1}, gh^{-1}, \mathrm{id}_P)$ *with the isomorphism* (h, h, h)*.*

2. Applications of quasigroups and loops

2.1. Latin squares. A *Latin square*, as on the left of Figure 2, is an $n \times n$ array, for some positive integer n, containing a multiset of n symbols, each with multiplicity n, such that each symbol appears precisely once in each row and in each column of the array.

1	3	2	5	6	4
3	2	1	6	4	5
2	1	3	4	5	6
4	5	6	1	2	3
5	6	4	2	3	1
6	4	5	3	1	2

$\cdot$	1	2	3	4	5	6
1	1	3	2	5	6	4
2	3	2	1	6	4	5
3	2	1	3	4	5	6
4	4	5	6	1	2	3
5	5	6	4	2	3	1
6	6	4	5	3	1	2

FIGURE 2. A Latin square gives a quasigroup.

Such a Latin square may be given a (left) border of row names, and a (top) border of column names, to yield the multiplication table of a quasigroup, as on the right of Figure 2. In the quasigroup, the product $x \cdot y$ is given by the element appearing in the table in the row labeled x and the column labeled y. The bijectivity of $L(x)$ corresponds to the unique occurrence of each symbol in the row labeled x. The bijectivity of $R(y)$ corresponds to the unique occurrence of each symbol in the column labeled y. Permutations of the row and column labels lead to multiplication tables of principally isotopic quasigroups.

2.1.1. *Latin squares as experimental designs.* The classic application of Latin squares is in the design of statistical experiments. For example, suppose that a consumer organization wishes to test 6 different brands of tires, on 6 different cars, with 6 different drivers. Rather than trying all $6 \times 6 \times 6 = 216$ different combinations, the organization could follow the design given by the right hand side of Figure 2. In this design, which only requires 36 tests instead of 216, tire brand x would be tested on car y by driver $x \cdot y$. The Latin square property avoids biased results, for example where a certain brand would be favored by being tested only by the most careful drivers.

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	1	4	3	0	2
2	2	0	4	1	3
3	3	2	0	4	1
4	4	3	1	2	0

FIGURE 3. A noncommutative loop of order 5.

2.1.2. *Latin squares as quasigroup specifications.* Latin squares provide a direct way to construct certain quasigroups. For example, one may ask whether every quasigroup is isotopic to a group. For quasigroups of order less than 5, this is indeed the case. However, one may use a Latin square to present the multiplication table of a loop of order 5 that is not commutative (Figure 3). Since there are no groups of order 5 which are not commutative, this loop is not isomorphic to a group. It follows that this loop is not isotopic to a group, either (compare Exercise 16).

2.2. Loop transversals. Let G be a group. If N is a normal subgroup of G, the set of cosets of N in G forms a group under multiplication. Quasigroups and loops may be used to obtain quotients by subgroups that are not necessarily normal.

2.2.1. *Right loops.* A right quasigroup $(Q, \cdot, /)$ is said to be a *right loop* if it contains a two-sided identity element e such that (1.1) holds. Note that for a set X with $|X| > 1$, the left-projection right quasigroup of Example 1.3 does not contain a two-sided identity element.

Now let H be a subgroup of a group G. Let T be a *right transversal* to H in G, a set of representatives for the right cosets of H in G.

Suppose that T is *normalized* in the sense that $1 \in T$, so 1 represents H itself. An *error function*

$$\varepsilon\colon G \to T; g \mapsto g^\varepsilon$$

is well-defined by $g \in Hg^\varepsilon$, so that g^ε is the unique representative in T for the right coset of H that contains g. It is also convenient to define a *decoding function* $\delta\colon G \to H; g \mapsto g^\delta$ by

$$g = g^\delta g^\varepsilon\,. \tag{2.1}$$

Note that $1^\delta = 1^\varepsilon = 1$. Moreover, $h^\delta = h$ and $h^\varepsilon = 1$ for $h \in H$, while $t^\delta = t$ and $t^\varepsilon = t$ for $t \in T$.

Proposition 2.1. *Let T be a normalized right transversal from a group G to a subgroup H. Then*

$$t * u = (tu)^\varepsilon \quad \textit{and} \quad t||u = (t/u)^\varepsilon$$

define a right loop structure $(T, *, ||, 1)$.

Proof. The respective right quasigroup identities (1.2) in $(T, *, ||)$ are verified by

$$H(t * u)/u \ni (tu)/u = t \in Ht\,,$$

so that $(t * u)||u = t$, and by

$$H(t||u)u \ni (t/u) \cdot u = t \in Ht\,,$$

so that $(t||u) * u = t$. The equations

$$1 * t = (1t)^\varepsilon = t^\varepsilon = t = t^\varepsilon = (t1)^\varepsilon = t * 1$$

verify (1.1). □

2.2.2. *Loop transversals.* Under certain circumstances, the right loop of Proposition 2.1 may become a two-sided loop. In this case, the normalized transversal T is described as a *loop transversal*. Thus T is a loop transversal if and only if, for each ordered pair (t, u) of elements of T, the equation

$$t * x = u$$

has a unique solution x in T.

Example 2.2. Let T be a normalized right transversal to a normal subgroup N of a group G. Then there is a right loop isomorphism

$$(T, *, ||, 1) \to (N\backslash G, \cdot, /, N); t \mapsto Nt$$

with $N(t * u) = Ntu = Nt \cdot Nu$ for $t, u \in T$. Thus T is a loop transversal.

PROPOSITION 2.3. *Let T be a normalized right transversal to a subgroup H of a group G. Then T is a loop transversal if and only if it is a right transversal to each conjugate $g^{-1}Hg$ of H in G.*

2.3. Loop transversal codes. Let n be a positive integer. Let A be a *binary* (communication) *channel of length n*, the set $\underline{2}^n$ of bit strings of length n. The channel A inherits a componentwise abelian group structure from $(\mathbb{Z}/_2, +, 0)$. Let C be a subgroup of A, known as the *code*. By Lagrange's Theorem, $|C| = 2^k$ for some integer $0 \leq k \leq n$ known as the *dimension* of the code. Words chosen from C, so-called *codewords*, are sent through the channel A from transmitter to receiver, but are subject to corruption during the transmission. A transmitted codeword c may be received as a word x in A that is not necessarily a codeword. In a well-designed code, there is a *decoding function* $\delta \colon A \to C$, assigning a most likely transmitted codeword x^δ to each received word x from the channel. The difference $x^\varepsilon = x - x^\delta$ is the (most likely) *error*. In a good channel, the error strings (of length n) are "close to zero" in the sense that almost all of their bits are zeroes.

Loop transversals may be used to design good codes, and indeed the terminology of §2.2 was chosen with this application in mind. Let T be a normalized transversal to a code C, as a subgroup of the abelian group A. By Proposition 2.3, the transversal T will be a loop transversal, since conjugation is trivial in an abelian group. In coding applications, the transversal T represents the set of errors to be corrected. The equation $g = g^\delta g^\varepsilon$ of (2.1) is implemented as $x = c + (x - c)$. The loop structure $(T, *)$ on T, actually an abelian group structure, is given by a group isomorphism

$$s \colon (T, *) \to (\underline{2}^{n-k}, +, 00\ldots0)$$

known as the *syndrome* of the code. If the error set T includes the set

$$B = \{e_1 = 00\ldots01, e_2 = 00\ldots10, \ldots, e_{n-1} = 01\ldots00, e_n = 10\ldots00\},$$

of *basic errors*, then the error x^ε of a received word $x = \sum_{i=1}^n b_i e_i$ is $\left(\sum_{i=1}^n b_i e_i^s\right) s^{-1}$.

EXAMPLE 2.4 (A repetition code). Suppose $n = 3$ and $k = 1$, with error set $T = \{000, 001, 010, 100\}$ and code $\{000, 111\}$. The syndrome is given by

$$s\colon e_1 \mapsto 01, e_2 \mapsto 10, e_3 \mapsto 11\,.$$

The received word $101 = e_3 + e_1$ has error $(11 + 01)s^{-1} = 10s^{-1} = e_2 = 010$, and is thus decoded to $101 - 010 = 111$.

EXAMPLE 2.5 (Hamming codes). Suppose $n = 2^r - 1$ for a positive integer r. Suppose $T = B \cup \{0\ldots0\} \subset \underline{2}^n$. Note that $|T| = 2^r$. Suppose that the syndrome of e_m (for $1 \le m < 2^r$) is the length-r binary representation of the integer m. Then any error from T may be corrected. The case $r = 2$ is Example 2.4. Consider the case where $r = 3$, with received word $x = 1000101 = e_7 + e_3 + e_1$. The syndrome is $111 + 011 + 001 = 101$, the binary representation of 5, so the likely error was $e_5 = 0010000$. The received word 1000101 is decoded to $1000101 - 0010000 = 1010101$.

3. Exercises

(1) Give an example of an associative left quasigroup with three elements. Verify that the example has the claimed properties.

(2) Let $(G,\cdot)$ be a non-empty, associative quasigroup. Prove:

$$\exists\ e \in G\,.\ \forall\ x \in G\,,\ e \cdot g = g = g \cdot e\,.$$

Conclude that $(G,\cdot,e)$ is a group.

(3) Show that $(\mathbb{Z},-)$ is a quasigroup that is not associative, and that possesses no identity element.

(4) Show that $\mathbb{Z}$ is the smallest subquasigroup of $(\mathbb{Z},-)$ containing the element 1.

(5) Prove Proposition 1.6.

(6) Let P be the set of polynomials with real coefficients, considered as a magma $(P,\cdot)$ with

$$p(x) \cdot q(x) = p(x) + q'(x)\,.$$

Let Q be the set of sequences $q = (q_0(x), q_1(x), \ldots)$ of real polynomials such that $q_n(x) = q'_{n+1}(x)$ for each natural number n, equipped with the componentwise multiplication from P.

(a) Show that $(Q,\cdot)$ is a combinatorial quasigroup.

(b) Show that $(P,\cdot)$ is not a combinatorial quasigroup.

(c) Show that

$$f\colon Q \to P; (q_0(x), q_1(x), \dots) \mapsto q_0(x)$$

is a surjective magma homomorphism.

(7) Show that the identities

$$x = y/(x\backslash y) \quad \text{and} \quad x = (y/x)\backslash y$$

hold in a quasigroup $(Q, \cdot, /, \backslash)$.

(8) Let $(Q, \cdot)$ be a quasigroup. Show that $(Q, /)$ and $(Q, \backslash)$ are quasigroups.

(9) Give an example of a group G for which

$$L\colon G \to \operatorname{Mlt} G; x \mapsto L(x)$$

is not a group homomorphism.

(10) Prove Proposition 1.11.

(11) Prove Proposition 1.13. In particular, compute the products $L(x)L(y), L(x)R(y), R(x)L(y), R(x)R(y)$ for $x, y \in \mathbb{Z}/_n$.

(12) Prove Proposition 1.17.

(13) Is the quasigroup $(\mathbb{R}, \circ)$ of Example 1.18 associative?

(14) Give a geometric interpretation to the quasigroup structure $(\mathbb{R}, \circ)$ induced from the abelian group $(\mathbb{R}, +, 0)$ by the scalar multiple isotopy $(2, -1, 1)$.

(15) Let a and b be elements of a quasigroup $(Q, \cdot, /, \backslash)$. Show that

$$x \circ y = (x/b) \cdot (a\backslash y)$$

defines a loop $(Q, \circ, a \cdot b)$ that is principally isotopic to the quasigroup $(Q, \cdot, /, \backslash)$.

(16) Let L be a loop that is isotopic to a group G. Show that the loop L is isomorphic to the group G. [Hint: Use Proposition 1.20 to reduce to the case of a principal isotopy from a loop structure to a group structure on a given set.]

(17) Can the pattern

$$\begin{bmatrix} & & 1 & & & \\ & 2 & & & & \\ 3 & & & & 2 & \\ & & 5 & & & 1 \\ & & & & & 3 \\ & & & & & 4 \end{bmatrix}$$

be completed to a 6×6 Latin square with entries from the set $\{1, 2, 3, 4, 5, 6\}$?

(18) Prove Proposition 2.3.

(19) Let Q be a non-empty quasigroup, with multiplication group G. Define the mapping

$$\rho \colon Q \times Q \to G; (x, y) \mapsto R(x\backslash x)^{-1} R(x\backslash y) .$$

Let e be a fixed element of Q, and let G_e be the stabilizer of e in G. Show that $T = \{\rho(e, q) \mid q \in Q\}$ is a normalized loop transversal to G_e in G.

(20) Let n be a positive integer. Consider the following sets of $n \times n$ real matrices:
  (a) The set P_n of positive definite symmetric matrices;
  (b) The *orthogonal group* $\mathsf{O}_n(\mathbb{R})$ of matrices of determinant ± 1;
  (c) The *general linear group* $\mathsf{GL}_n(\mathbb{R})$ of invertible matrices.

Use polar decomposition to show that the set P_n forms a loop transversal to the subgroup $\mathsf{O}_n(\mathbb{R})$ of the group $\mathsf{GL}_n(\mathbb{R})$.

(21) In special relativity, show that the set of boosts forms a loop transversal to the group of spatial rotations in the Lorentz group.

(22) Consider the Hamming code of length 7.
  (a) Determine all 8 codewords.
  (b) Decode the received word 1101000.

CHAPTER 6

Symmetry

1. Symmetry

1.1. Relations. Let X be a set. For each positive integer k, a *k-ary relation* R on X is a subset of X^k. For $k = 1, 2, 3, 4$, "k-ary" becomes *unary, binary, ternary, quaternary*.

Definition 1.1. Let X be a set. Consider $1 < k \in \mathbb{Z}$.

(a) A k-ary relation γ on X is said to be *antireflexive* when each element $(x_1, \dots, x_k)$ of γ contains no repeated components, i.e., if $\forall\ (x_1, \dots, x_k) \in \gamma\,,\ |\{x_1, \dots, x_k\}| = k$.

(b) The largest antireflexive k-ary relation $[X]_k$ on X is called the *k-ary diversity relation* on X.

Let k, n be integers, with $1 < k$. The *falling factorial* is defined as

$$[n]_k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)\,.$$

Note that $n! = [n]_n$. Then for a set X with $|X| = n$, note $\big|[X]_k\big| = [n]_k$ (Exercise 1).

1.1.1. *Graphs.* Let E be a subset of the binary diversity relation on a set V. Then (V, E) is a *directed graph* with *vertex set* V and *edge set* E. A containment $(v_1, v_2) \in E$ is drawn as $v_1 \longrightarrow v_2$. If the relation E is symmetric, then (V, E) is a(n *undirected*) *graph*. In this case, the containment $(v_1, v_2) \in E$ is drawn as $v_1 \,\text{——}\, v_2$.

1.1.2. *Relational structures and algebras.*

Definition 1.2. (a) A (*relational*) *signature* or *type* is a function $\sigma \colon \Gamma \to \mathbb{Z}^+$, with codomain the set $\mathbb{Z}^+$ of positive integers.

(b) Given a relational signature σ, a *relational structure* (X, Γ) *of type* σ is a set X with a set $\{\gamma_X \mid \gamma \in \Gamma\}$ of relations, such that each relation γ_X has arity $\gamma\sigma$.

Remark 1.3. (a) In Definition 1.2(b), one informally writes γ rather than γ_X if the set X is clear in the context.

(b) Directed and undirected graphs (V, E) may be viewed as examples of relational structures $(V, \{\eta\})$ with signature $\sigma\colon \{\eta\} \to \{2\}$.

Definition 1.4. (a) The *graph* of a function $f\colon A \to B$ (not to be confused with the definition of §1.1.1!) is the subset

$$\operatorname{gr} f = \{(a, af) \in A \times B \mid a \in A\}$$

of $A \times B$.

(b) A (*functional*) *signature* or *type* is a function $\tau\colon \Omega \to \mathbb{N}$. The domain Ω of τ is called the *operator domain*, and its elements are called *operators*.

(c) Given a functional signature τ, a τ-*algebra* or *algebra* (X, Ω) *of type* τ is a set X with a function

$$\omega\colon X^{\omega\tau} \to X; (x_1, \dots, x_{\omega\tau}) \mapsto x_1 \dots x_{\omega\tau}\omega\,,$$

a so-called $\omega\tau$-*ary operation*, for each operator $\omega \in \Omega$.

Remark 1.5. In Definition 1.4(c), "k-ary" becomes *nullary, unary, binary, ternary, quaternary* respectively for $k = 0, 1, 2, 3, 4$.

Example 1.6. For $\tau\colon \mu \mapsto 2, \iota \mapsto 1, \epsilon \mapsto 0$, a group $(G, \cdot, 1)$ becomes a τ-algebra with $xy\mu = x \cdot y$ and $x\iota = x^{-1}$ for $x, y \in G$, and $\epsilon\colon G^0 \to \{1\}$.

Proposition 1.7. *Suppose that (X, Ω) is an algebra of functional type $\tau\colon \Omega \to \mathbb{N}$. Then there is a relational structure $(X, \operatorname{Gr}\Omega)$ of relational signature $\sigma\colon \operatorname{Gr}\Omega \to \mathbb{Z}^+$ with $\operatorname{Gr}\Omega = \{\operatorname{gr}\omega \mid \omega \in \Omega\}$ and $(\operatorname{gr}\omega)\sigma = \omega\tau + 1$ for $\omega \in \Omega$. The algebra (X, Ω) is completely determined by the relational structure $(X, \operatorname{Gr}\Omega)$.*

Example 1.8. Let $(X, \cdot)$ be a magma, construed as an algebra of binary type $\mu \mapsto 2$. Then the corresponding relation

$$\operatorname{gr}\mu = \{(x, y, x \cdot y) \in X^3 \mid x, y \in X\}$$

is the *multiplication table* of $(X, \cdot)$.

1.1.3. *Homomorphisms of relational structures.*

Definition 1.9. Let (X, Γ) and (Y, Γ) be relational structures of given type σ.

(a) A function $f\colon X \to Y$ is a *homomorphism* $f\colon (X,\Gamma) \to (Y,\Gamma)$ if $\forall\ \gamma \in \Gamma\,,\ \forall\ (x_1,\dots,x_{\gamma\sigma}) \in X^{\gamma\sigma}\,,$

$$(x_1,\dots,x_{\gamma\sigma}) \in \gamma_X \ \Rightarrow\ (x_1 f,\dots,x_{\gamma\sigma} f) \in \gamma_Y\,.$$

(b) An *automorphism* of the relational structure (X,Γ) is a bijective homomorphism $f\colon (X,\Gamma) \to (X,\Gamma)$.

(c) The set $\mathrm{Aut}(X,\Gamma)$ of all automorphisms of (X,Γ) is called the *automorphism group* of the relational structure (X,Γ).

The terminology of Definition 1.9(c) is justified as follows.

Proposition 1.10. *Consider relational structures (X,Γ), (Y,Γ) and (Z,Γ) of given type σ.*

(a) *Suppose that $f\colon (X,\Gamma) \to (Y,\Gamma)$ and $g\colon (Y,\Gamma) \to (Z,\Gamma)$ are homomorphisms. Then so is $fg\colon (X,\Gamma) \to (Z,\Gamma)$.*

(b) *The set $\mathrm{Aut}(X,\Gamma)$ forms a subgroup of $X!$.*

The formal equivalents of Definition 1.9 for algebras are as follows.

Definition 1.11. Let (X,Ω) and (Y,Ω) be algebras of given type τ.

(a) A function $f\colon X \to Y$ is a *homomorphism* $f\colon (X,\Omega) \to (Y,\Omega)$ if

$$\forall\ \omega \in \Omega\,,\ \forall\ (x_1,\dots,x_{\omega\tau}) \in X^{\omega\tau}\,,\ x_1 \dots x_{\omega\tau}\omega f = x_1 f \dots x_{\omega\tau} f\omega\,.$$

(b) A bijective homomorphism $f\colon (X,\Omega) \to (X,\Omega)$ is said to be an *automorphism* of the algebra (X,Ω).

(c) The set $\mathrm{Aut}(X,\Omega)$ of all automorphisms of (X,Ω) is called the *automorphism group* of the algebra (X,Ω).

Proposition 1.12. *Let (X,Ω) and (Y,Ω) be algebras of given type τ, with corresponding relational structures $(X,\mathrm{Gr}\,\Omega)$ and $(Y,\mathrm{Gr}\,\Omega)$. Then a function $f\colon X \to Y$ is a homomorphism $f\colon (X,\mathrm{Gr}\,\Omega) \to (X,\mathrm{Gr}\,\Omega)$ of relational structures iff it is a homomorphism $f\colon (X,\Omega) \to (X,\Omega)$ of algebras.*

1.2. Permutation groups. Let G be a group, and let (X,G,r) or (X,G) be a G-set. The G-set is said to be *faithful* (or "effective") if the representation $r\colon G \to X!$ is injective. In this case, G is called a *permutation group* of *degree* $|X|$ on X, or a *symmetry group* on X. It will often be identified with its image G^r in $X!$.

EXAMPLE 1.13. Let Q be a quasigroup. Then the right, left, and two-sided multiplication groups of Q are permutation groups on Q.

EXAMPLE 1.14. Let n be a positive integer. The symmetric group S_n is a permutation group of $\underline{n}$. By the First Isomorphism Theorem, each permutation group of degree n is similar to a subgroup of S_n on the set $\underline{n}$.

EXAMPLE 1.15. Let n be a positive integer. The cyclic group C_n, the multiplication group of $(\mathbb{Z}/_n, +)$, is a permutation group of $\underline{n}$.

EXAMPLE 1.16. Let n be a positive integer. The dihedral group D_n, the multiplication group of $(\mathbb{Z}/_n, -)$, is a permutation group of $\underline{n}$.

Suppose that (X, Γ) is a relational structure. Then $\big(X, \mathrm{Aut}(X, \Gamma)\big)$ is a permutation group on X. For a finite set X, the Krasner-Wielandt Theorem (§1.3) provides the converse statement: Each permutation group on X is the automorphism group of a relational structure on X.

1.2.1. *Action on powers.* Let (X, G, r) be a G-set for a group G. Let k be a natural number. Then the k-th power G-set (X^k, G) yields a representation r_k of G with

$$g^{r_k}\colon (x_1, \ldots, x_k) \mapsto (x_1 g, \ldots, x_k g)$$

or simply $(x_1, \ldots, x_k)g = (x_1 g, \ldots, x_k g)$ for $x_1, \ldots, x_k \in X$ and $g \in G$.

LEMMA 1.17. *If $k > 0$ and (X, G, r) is faithful, then r_k is faithful.*

DEFINITION 1.18. Let (X, G) be a G-set. Then the orbits of G on (X^2, G) are known as the *orbitals* of (X, G).

1.2.2. *Transitivity.* For a given group G, the actions on powers provide a classification of G-sets.

DEFINITION 1.19. Let G be a group. Then for each positive integer k, a G-set (X, G) is said to be *k-transitive* if the k-ary diversity relation $[X]_k$ is an irreducible G-subset of (X^k, G).

Note that a G-set (X, G) is 1-transitive if and only if it is transitive (or irreducible).

EXAMPLE 1.20. Let n be a positive integer. Then the action $(\underline{n}, S_n)$ of Example 1.14 is n-transitive.

EXAMPLE 1.21. Consider the *real projective line*, the set $\mathsf{PG}(1, \mathbb{R})$ of 1-dimensional subspaces of the real vector space $\mathbb{R}^2$. Consider the general linear group $\mathsf{GL}_2(\mathbb{R})$ of dimension 2, the set of invertible 2×2 real matrices. Since $\mathsf{GL}_2(\mathbb{R})$ is the automorphism group of the vector space $\mathbb{R}^2$, it is represented as a group of permutations of $\mathsf{PG}(1, \mathbb{R})$. Then the $\mathsf{GL}_2(\mathbb{R})$-set $\big(\mathsf{PG}(1, \mathbb{R}), \mathsf{GL}_2(\mathbb{R})\big)$ is 3-transitive (Exercise 11).

PROPOSITION 1.22. *Let G be a group, and let (X, G) be an irreducible G-set with element e. Let G_e be the stabilizer of e in G. Then (X, G) is 2-transitive if and only if the G_e-set $\big(X \smallsetminus \{e\}, G_e\big)$ is irreducible.*

PROOF. It may be shown that the function

$$[X]_2/G \to (X \smallsetminus \{e\})/G_e; R \mapsto e^R$$

is a well-defined bijection (Exercise 1.22). □

1.3. The Krasner-Wielandt Theorem. Let G be a group. Recall that the set of orbits of a (right) G-set (Y, G) is written as Y/G. Note that for $y \in Y$, the element y lies in the orbit $yG = \{yg \mid g \in G\}$.

THEOREM 1.23 (Krasner-Wielandt Theorem). *Let G be a permutation group on a set X of finite cardinality n. For $1 \leq k \leq n$, consider the set X^k/G of orbits of G on X^k.*

(a) *For all $1 \leq k < n$, the automorphism group* $\mathrm{Aut}(X, X^{k+1}/G)$ *is a subgroup of* $\mathrm{Aut}(X, X^k/G)$.
(b) *For some $1 \leq k \leq n$, the automorphism group* $\mathrm{Aut}(X, X^k/G)$ *coincides with G.*

PROOF. (a) For each subgroup H of $X!$, note that there is an injective H-homomorphism

$$D \colon X^k \to X^{k+1}; (x_1, x_2, \ldots, x_k) \mapsto (x_1, x_1, x_2, \ldots, x_k)\,.$$

Now D induces a map

$$X^k/G \to X^{k+1}/G; \gamma \mapsto \gamma D\,.$$

Consider γ in X^k/G and f in $\mathrm{Aut}(X, X^{k+1}/G)$. Then the image γD is an $\langle f \rangle$-subset of $(X^k D, \langle f \rangle)$ so γ is an $\langle f \rangle$-subset of $(X^k, \langle f \rangle)$. It follows that f lies in $\mathrm{Aut}(X, X^k/G)$.

(b) First note that G is a subgroup of $\mathrm{Aut}(X, X^n/G)$. Conversely, establish a bijection $b \colon \{1, 2, \ldots, n\} \to X$, and consider the orbit $(1b, 2b, \ldots, nb)G \in X^n/G$. For f in $\mathrm{Aut}(X, X^n/G)$, one has

$$(1b, 2b, \ldots, nb)Gf = (1b, 2b, \ldots, nb)G\,.$$

In particular,

$$\exists\ g \in G\,.\ (1b, 2b, \dots, nb)f = (1b, 2b, \dots, nb)g\,.$$

Then $f = g \in G$, and $\mathrm{Aut}(X, X^n/G) \leq G$. $\square$

Definition 1.24. If $G = \mathrm{Aut}(X, X^k/G)$ in the context of the Krasner-Wielandt Theorem, then the permutation group G on X is said to be *k-closed*.

Example 1.25. For a positive integer n, the symmetric group S_n on $\underline{n}$ is 1-closed.

The philosophy behind the Krasner-Wielandt Theorem, specifying a permutation group as the group of all symmetries of certain relations, may apply equally to infinite groups.

Example 1.26. Fix a positive integer n as a *dimension.* Then the n-dimensional *Euclidean group* $\mathsf{E}_n(\mathbb{R})$ is the group of all permutations of $\mathbb{R}^n$ that preserve the binary *distance relations*

$$\left\{(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^n \times \mathbb{R}^n \;\middle|\; d^2 = \sum_{i=1}^{n}(x_i - y_i)^2\right\}$$

for each positive real number d.

1.4. Permutation characters and Burnside's lemma.

Definition 1.27. Let G be a group, and let (X, G) be a G-set.

(a) An element x of X is a *fixed point* of a group element g in the action (X, G) if $xg = x$.
(b) For $g \in G$, the *fixed point set* $X_g = \{x \in X \mid xg = x\}$.
(c) If X is finite, the *permutation character* π_X on G is defined as the function π or

$$\pi_X \colon G \to \mathbb{N}; g \mapsto |X_g|$$

that counts the number of fixed points of each element of G.

Theorem 1.28 (Burnside's Lemma). *Let G be a finite group, and let (X, G) be a finite G-set. Then*

$$|X/G| = \frac{1}{|G|}\sum_{g \in G} \pi_X(g)\,.$$

Thus the number of orbits in (X, G) is equal to the average number of fixed points.

Proof. First note that

$$\sum_{g\in G}(X_g\times\{g\}) = \{(x,g)\in X\times G \mid xg=x\} = \sum_{x\in X}(\{x\}\times G_x)\ .$$

Thus

$$\begin{aligned}\sum_{g\in G}\pi_X(g) &= \sum_{g\in G}|X_g| = \sum_{x\in X}|G_x| \\ &= \sum_{x\in X}\frac{|G|}{|xG|} = |G|\sum_{x\in X}\frac{1}{|xG|} \\ &= |G|\sum_{Y\in X/G}\sum_{x\in Y}\frac{1}{|xG|} = |G|\sum_{Y\in X/G}\sum_{x\in Y}\frac{1}{|Y|} \\ &= |G|\sum_{Y\in X/G}1 = |G|\cdot|X/G|\,.\end{aligned}$$

Division by $|G|$ yields the desired result. □

1.4.1. *Counting orbits in powers.* Let G be a group. If (X,G) and (Y,G) are G-sets, and g is an element of G, then

$$(X\times Y)_g = \{(x,y)\in X\times Y \mid (x,y)g=(x,y)\} = X_g\times Y_g\,.$$

Thus if X and Y are finite, $\pi_{X\times Y}(g)=\pi_X(g)\cdot\pi_Y(g)$. In particular, $\pi_{X^k}(g)=\pi_X(g)^k$ for natural numbers k. If G is also finite, Burnside's Lemma yields

$$|X^k/G| = \frac{1}{|G|}\sum_{g\in G}\pi_X(g)^k$$

for $k\in\mathbb{N}$. These formulas are summarized in the generating function

$$\begin{aligned}p(z) = \sum_{k=0}^{\infty}|X^k/G|z^k &= \frac{1}{|G|}\sum_{k=0}^{\infty}\sum_{g\in G}\pi_X(g)^k z^k \\ = \frac{1}{|G|}\sum_{g\in G}\sum_{k=0}^{\infty}(z\pi_X(g))^k &= \frac{1}{|G|}\sum_{g\in G}\frac{1}{1-z\pi(g)}\end{aligned}$$

known as the *Poincaré series*.

EXAMPLE 1.29. Consider the dihedral action $D_{2n} = \mathrm{Mlt}(\mathbb{Z}/_{2n}, -)$ of even degree. The permutation character is computed as follows:

$$\pi(g) = \begin{cases} 2n & \text{for } g = R(0)\,; \\ 0 & \text{for } g = R(q),\ 0 \neq q \in \mathbb{Z}/_{2n}\,; \\ 2 & \text{for } g = L(q),\ q \in 2\mathbb{Z}/_{2n}\,; \\ 0 & \text{for } g = L(q),\ q \in 1 + 2\mathbb{Z}/_{2n}\,. \end{cases}$$

Then

$$\begin{aligned} p(z) &= \frac{3n - 1 + n(1-2z)^{-1} + (1-2nz)^{-1}}{4n} \\ &= 1 + z + \sum_{k=2}^{\infty} 2^{k-2}(1 + n^{k-1})z^k\,. \end{aligned}$$

In particular, there are $1+n$ orbits on $(\mathbb{Z}/_{2n})^2$. Two of these have size $2n$, namely $(0,0)D_{2n}$ and $(0,n)D_{2n}$. Since the maximum size of any orbit is $|D_{2n}| = 4n$, each of the remaining orbits must have size $4n$. For example, $(0,1)D_{2n}$ is a symmetric, antireflexive relation determining the simple, undirected graph with edge set $\{x, x+1 \mid x \in \mathbb{Z}/2n\}$. Note that D_{2n} is the automorphism group of this graph, and thus the action D_{2n} is 2-closed (compare Exercise 13).

2. Symmetric and alternating groups

2.1. Generating symmetric groups. Recall the *cycle notation* for permutations of a set X: For a positive integer k and an element $(x_0, \dots, x_{k-1})$ of the diversity relation $[X]_k$, with coordinates indexed by elements of the abelian group $(\mathbb{Z}/_k, +, 0)$ of residues modulo k, the function $(x_0\ x_1\ \dots\ x_{k-1})\colon X \to X$, a *cycle of length* k, is defined by

$$y \mapsto \begin{cases} x_{i+1} & \text{if } \exists\ i \in \mathbb{Z}/_k\,.\ y = x_i\,; \\ y & \text{if } y \notin \{x_0, \dots, x_{k-1}\}\,. \end{cases}$$

Cycles of length 2 are *transpositions*.

LEMMA 2.1. *Let X be a set, with a bijection $f\colon X \to X$ and a cycle $(x_0\ x_1\ \dots\ x_{k-1})$.*

(a) $f^{-1}(x_0\ x_1\ \dots\ x_{k-1})f = (x_0 f\ x_1 f\ \dots\ x_{k-1} f)\,.$
(b) $(x_0\ x_1\ \dots\ x_{k-1}) = (x_0\ x_1)(x_0\ x_2)\dots(x_0\ x_{k-1})\,.$

PROPOSITION 2.2. *Let n be a positive integer. Recall $S_n = \underline{n}!$.*

(a) *The set*

$$\{(r-1\ r) \mid 0 < r < n\} \tag{2.1}$$

of transpositions generates S_n.

(b) *The set* $\{(0\ 1), (0\ 1\ \dots\ n-1)\}$ *generates* S_n.

PROOF. (a) By Lemma 2.1(b), and the decomposition of an arbitrary element of S_n as a product of disjoint cycles, it suffices to show that each transposition $(r\ s)$ may be expressed as a product of elements of (2.1). Now by Lemma 2.1(b),

$$(0\ s) = \big((1\ 2)(2\ 3)\dots(s-1\ s)\big)^{-1}(0\ 1)\big((1\ 2)(2\ 3)\dots(s-1\ s)\big)\,.$$

Then again by Lemma 2.1(b),

$$(r\ s) = \big((0\ 1)(1\ 2)\dots(r-1\ r)\big)^{-1}(0\ s)\big((0\ 1)(1\ 2)\dots(r-1\ r)\big)\,.$$

(b) Since

$$(r-1\ r) = (0\ 1\ \dots\ n-1)^{1-r}(0\ 1)(0\ 1\ \dots\ n-1)^{r-1}$$

by Lemma 2.1(b), each element of the generating set (2.1) is generated by elements of the set $\{(0\ 1), (0\ 1\ \dots\ n-1)\}$. $\square$

2.2. Alternating groups. For $1 < n \in \mathbb{Z}$, consider the *sign function*

$$\varepsilon \colon S_n \to \{\pm 1\};\ f \mapsto \frac{\prod_{0\le i<j<n}(X_{if} - X_{jf})}{\prod_{0\le i<j<n}(X_i - X_j)}\,. \tag{2.2}$$

LEMMA 2.3. *For* $1 < n \in \mathbb{Z}$, *the sign function* $\varepsilon \colon S_n \to (\{\pm 1\}, \cdot, 1)$ *is a group homomorphism.*

PROOF. For $f, g \in S_n$, one has

$$\begin{aligned}
f^\varepsilon g^\varepsilon &= \frac{\prod_{0\le i<j<n}(X_{if} - X_{jf})}{\prod_{0\le i<j<n}(X_i - X_j)} \cdot \frac{\prod_{0\le i<j<n}(X_{ig} - X_{jg})}{\prod_{0\le i<j<n}(X_i - X_j)} \\
&= \frac{\prod_{0\le i<j<n}(X_{if} - X_{jf})}{\prod_{0\le i<j<n}(X_i - X_j)} \cdot \frac{\prod_{0\le i<j<n}(X_{ifg} - X_{jfg})}{\prod_{0\le i<j<n}(X_{if} - X_{jf})} \\
&= \frac{\prod_{0\le i<j<n}(X_{ifg} - X_{jfg})}{\prod_{0\le i<j<n}(X_i - X_j)} = (fg)^\varepsilon\,,
\end{aligned}$$

so ε is a semigroup homomorphism between the two groups. $\square$

Definition 2.4. For $1 < n \in \mathbb{Z}$, the *alternating group* A_n of *degree* n is the group kernel $\operatorname{Ker} \varepsilon$ of the sign function (2.2).

Elements of A_n are described as *even* permutations, while elements of $S_n \smallsetminus A_n$ are *odd*. Transpositions are odd. More generally, Lemma 2.1(b) shows that cycles of even length are odd, while cycles of odd length are even. The following result, whose proof is relegated to Exercise 16, lists some properties of alternating groups.

Proposition 2.5. *Suppose* $1 < n \in \mathbb{Z}$.

(a) *A permutation of* $\underline{n}$ *is even if and only if it is a product of an even number of transpositions.*
(b) *The set of all* 3*-cycles is a generating set for the alternating group* A_n.
(c) *The action* $(\underline{n}, A_n)$ *is* $(n-1)$*-transitive.*
(d) $|A_n| = n!/2$.

2.3. Cayley graphs.

Definition 2.6. Let C be a subset of a quasigroup Q. The (*right*) *Cayley graph* of Q over C is the transition diagram of the automaton with state space Q and event set $\{R(c) \mid c \in C\}$.

For $1 < n \in \mathbb{Z}$, the Cayley graph of S_n over the set

$$\{t_r = (r-1\ r) \mid 0 < r < n\}$$

of transpositions from (2.1) is of especial interest. Note that

$$t_r t_s = t_s t_r$$

or

$$(r-1\ r)(s-1\ s) = (s-1\ s)(r-1\ r)$$

if $|r-s| > 1$ and $0 < r, s < n$, while

$$t_r t_{r+1} t_r = t_{r+1} t_r t_{r+1}$$

or

$$\begin{aligned}(r-1\ r)(r\ r+1)(r-1\ r) &= (r-1\ r+1)\\ &= (r\ r+1)(r-1\ r)(r\ r+1)\end{aligned}$$

for $0 < r < n-1$.

EXAMPLE 2.7. The right Cayley graph of S_3 over $\{(0\ 1), (1\ 2)\}$ is

$$\begin{tikzcd}
& (0\ 2) \arrow[dl, dash, "(0\ 1)"'] \arrow[dr, dash, "(1\ 2)"] & \\
(0\ 2\ 1) \arrow[d, dash, "(1\ 2)"'] & & (0\ 1\ 2) \arrow[d, dash, "(0\ 1)"] \\
(0\ 1) \arrow[dr, dash, "(0\ 1)"'] & & (1\ 2) \arrow[dl, dash, "(1\ 2)"] \\
& 1 &
\end{tikzcd}$$

2.3.1. *Group presentations.* The description of S_3 in Example 2.7 may be summarized in the so-called *presentation*

$$S_3 = \langle t_1, t_2 \mid t_1^2 = t_2^2 = 1,\ t_1t_2t_1 = t_2t_1t_2\rangle\,.$$

This means that the group S_3 is generated by elements t_1 and t_2 that satisfy the equations $t_1^2 = t_2^2 = 1$ and $t_1t_2t_1 = t_2t_1t_2$. More generally, for $3 < n \in \mathbb{Z}$, there is a presentation

$$\begin{aligned} S_n = \langle t_1, \dots, t_{n-1} \mid t_1^2 = \ldots = t_{n-1}^2 = 1,& \\ t_rt_{r+1}t_r = t_{r+1}t_rt_{r+1} \text{ for } 0 < r < n-1,& \\ t_rt_s = t_st_r \text{ for } |r-s| > 1 \text{ and } 0 < r, s < n\rangle\,.& \end{aligned}$$

The related infinite groups with presentations

$$B_3 = \langle t_1, t_2 \mid\ t_1t_2t_1 = t_2t_1t_2\rangle$$

and

$$\begin{aligned} B_n = \langle t_1, \dots, t_{n-1} \mid t_rt_{r+1}t_r = t_{r+1}t_rt_{r+1} \text{ for } 0 < r < n-1,& \\ t_rt_s = t_st_r \text{ for } |r-s| > 1 \text{ and } 0 < r, s < n\rangle& \end{aligned}$$

for $3 < n \in \mathbb{Z}$ are known as *braid groups*. For $2 < n \in \mathbb{Z}$, the dihedral group D_n of degree n is often presented as

$$D_n = \langle r, s \mid r^n = s^2 = 1, s^{-1}rs = r^{-1}\rangle \tag{2.3}$$

with $r = R(1)$ and $s = L(0)$ in $D_n = \mathrm{Mlt}\,(\mathbb{Z}/_n, -)$.

In order to gain some understanding of the structure of a group given by a presentation, one may use the coset enumeration procedure that was initiated by Todd and Coxeter [**4**, Chapter 2]. Nevertheless, there may be no algorithm to decide whether a group given by a certain presentation is trivial or not, since one may encode undecidable problems like the Halting Problem for Turing machines into group presentations [**1**]. For this reason, the direct specification of dihedral groups as multiplication groups is preferable to presentations such as (2.3).

3. Exercises

(1) Let X be a finite set. If $|X| = n$, and $1 < k \in \mathbb{Z}$, show that $\big|[X]_k\big| = [n]_k$.

(2) Prove Proposition 1.7. [Hint: When $\omega\colon X^0 \to X$ is a nullary operation with image $\{e\}$, the graph $\operatorname{gr}\omega$ is the subset $\{e\}$ of X. Recall the set isomorphism $X^0 \times X \to X; (*, x) \mapsto x$.]

(3) Let $(Q, \cdot)$ be a combinatorial quasigroup, with multiplication table $T = \{(x_1, x_2, x_3) \mid x_1, x_2 \in Q\}$.

   (a) Show that

$$\{(x_1, x_3, x_2) \mid (x_1, x_2, x_3) \in T\} \tag{3.1}$$

   is the multiplication table of $(Q, \backslash)$.

   (b) Express the multiplication table of $(Q, /)$ in a form that is analogous to (3.1).

(4) Determine the automorphism groups of the undirected graph

$$\begin{tikzcd} A \arrow[r, dash] \arrow[d, dash] & B \arrow[d, dash] \\ C \arrow[r, dash] & D \end{tikzcd}$$

and the following directed graphs:

$$\text{(a)}\ \begin{tikzcd} A \arrow[r] & B \\ C \arrow[u] \arrow[r] & D \arrow[u] \end{tikzcd} \qquad \text{(b)}\ \begin{tikzcd} A \arrow[r] & B \arrow[d] \\ C \arrow[u] \arrow[r] & D \end{tikzcd} \qquad \text{(c)}\ \begin{tikzcd} A \arrow[r] & B \arrow[d] \\ C \arrow[u] & D \arrow[l] \end{tikzcd} .$$

Give your answers as certain sets of permutations expressed as products of disjoint cycles, or as one of the similar groups from Examples 1.14–1.16.

(5) Verify Proposition 1.12.

(6) Let G be a group. Let (G, G) be the right regular representation of G. Show that the action $\big(G, \mathrm{Aut}(G, G)\big)$ is the left regular representation of G.

(7) Consider the inclusion $\underline{n} \hookrightarrow \mathbb{N}$ for each natural number n. Show that $\bigcup_{n=1}^{\infty} S_n$ is a subgroup of $\mathbb{N}!$. Is it a normal subgroup?

(8) Prove Lemma 1.17.

(9) Complete the proof of Proposition 1.22.

(10) A function $f\colon \mathbb{R} \to \mathbb{R}$ is said to be *affine* if there are real numbers m and c such that $\forall\ x \in \mathbb{R}\,,\ xf = mx + c$. The number m is known as the *slope*, and the number c is known as the *y-intercept*. Let G be the set of all affine functions with non-zero slope.
  (a) Show that G is a group of permutations of $\mathbb{R}$.
  (b) Show that the G-set $(\mathbb{R}, G)$ is 2-transitive.

(11) Show that $\big(\mathsf{PG}(1, \mathbb{R}), \mathsf{GL}_2(\mathbb{R})\big)$ (in Example 1.21) is 3-transitive. [Hints:
  (a) Right multiplication by an invertible matrix $\begin{bmatrix} d & -b \\ -c & d \end{bmatrix}$ takes the line $\{\mathbf{x} \mid \mathbf{x}\mathbf{u}^T = 0\}$ orthogonal to a vector $\mathbf{u}$ to the line orthogonal to $A\mathbf{u}$ with $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.
  (b) If $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$, then the linear system $\begin{Bmatrix} e = \lambda a + \mu b \\ f = \lambda c + \mu d \end{Bmatrix}$ has a solution (λ, μ). Consider sending the triple of distinct lines orthogonal to $(1, 0), (0, 1), (1, 1)$ respectively to the triple of distinct lines orthogonal to $(\lambda a, \lambda c), (\mu b, \mu d), (e, f)$.]

(12) For an element g of a group G, the *centralizer* is the subset
$$C_G(g) = \{x \in G \mid xg = gx\}\,.$$
  (a) Show that $C_G(g)$ is a subgroup of G.
  (b) If G is finite, show that $\frac{1}{|G|} \sum_{g \in G} |C_G(g)|$ is the number of conjugacy classes in G.

(13) For $n > 1$, show that the dihedral group D_{2n} of even degree $2n$ is not 1-closed.

(14) Repeat the analysis of Example 1.29 for dihedral groups D_{2n+1} of odd degree.

(15) Prove Lemma 2.1.

(16) Prove Proposition 2.5.

(17) (a) Determine the orders of the conjugacy classes in A_5.
 (b) Show that no proper non-singleton union of conjugacy classes containing 1 has order dividing 60.
 (c) Conclude that A_5 is *simple*: it contains no proper, non-trivial normal subgroups.

(18) Draw the right Cayley graph of S_4 over $\{(0\ 1), (1\ 2), (2\ 3)\}$.

(19) Draw the right Cayley graph of the degree-4 dihedral group $D_4 = \mathrm{Mlt}(\mathbb{Z}/_4, -)$ over $\{R(1), L(0)\}$.

(20) Show that there is a homomorphism

$$B_3 \to \mathsf{GL}_2(\mathbb{Z}/_2); t_1 \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, t_2 \mapsto \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

into the group of invertible 2×2 matrices with entries in $\mathbb{Z}/_2$.

CHAPTER 7

Linear mathematics

1. Abelian groups and rings

1.1. Abelian groups. Generally, abelian groups A will now be written in additive notation $(A, +, 0)$, with unary negation as inversion and a zero element as identity. Powers are written as multiples. Recall that each subgroup C of an abelian group A is normal, so an abelian quotient group $A/C = \{a + C \mid a \in A\}$ is always well-defined, with addition $(a_1{+}C){+}(a_2{+}C) = (a_1{+}a_2){+}C$, negation $-(a{+}C) = -a{+}C$, zero element $0 = C$, and (*natural*) *projection* $A \to A/C; a \mapsto a + C$. The trivial (abelian) group $\{0\}$ is often written simply as 0. For any abelian group A, there is a unique homomorphism $0 \to A$ and a unique homomorphism $A \to 0$.

1.1.1. *Exact sequences.*

Definition 1.1. Let $h \colon A \to B$ be a homomorphism of abelian groups.

(a) The *group kernel* of h is the subgroup

$$\operatorname{Ker} h = \{a \in A \mid ah = 0\}$$

of the domain A, together with the injection

$$\operatorname{Ker} h \to A\,. \tag{1.1}$$

(b) The *image* of h is the subgroup

$$\operatorname{Im} h = \{ah \in B \mid a \in A\}$$

of the codomain B.

(c) The *cokernel* of h is the quotient group

$$\operatorname{Coker} h = B/\operatorname{Im} h$$

of the codomain B, together with the projection

$$B \to \operatorname{Coker} h\,. \tag{1.2}$$

In Definition 1.1, note the duality between the injection $\operatorname{Ker} h \to A$ and the projection $B \to \operatorname{Coker} h$.

Definition 1.2. Consider a sequence

$$A_0 \longrightarrow \dots \xrightarrow{f_{n-2}} A_{n-1} \xrightarrow{f_{n-1}} A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} \cdots \longrightarrow A_N$$

of abelian group homomorphisms.

(a) The sequence is said to be *exact at* A_n if $\operatorname{Im} f_{n-1} = \operatorname{Ker} f_n$.
(b) The sequence is said to be *exact* whenever it is exact at each intermediate group $A_1, \dots, A_{N-1}$.

Proposition 1.3 (Extended First Isomorphism Theorem). *Suppose that $h\colon A \to B$ is a homomorphism of abelian groups. Then there is an exact sequence*

$$0 \longrightarrow \operatorname{Ker} h \longrightarrow A \xrightarrow{h} B \longrightarrow \operatorname{Coker} h \longrightarrow 0$$

with the injection (1.1) *and projection* (1.2).

1.1.2. *Groups of homomorphisms.* For sets X and Y, the morphism class $\mathbf{Set}(X, Y)$ of functions from X to Y is a set. Let $\underline{\underline{\mathbb{Z}}}$ denote the category of abelian groups and homomorphisms. For abelian groups A and B, the set $\underline{\underline{\mathbb{Z}}}(A, B)$ is an abelian group, a subgroup of the power group B^A with componentwise operations. The zero 0 of $\underline{\underline{\mathbb{Z}}}(A, B)$ is the composite $A \to 0 \to B$. The identity function on the abelian group A is written as 1 in $\underline{\underline{\mathbb{Z}}}(A, A)$.

Proposition 1.4. *Suppose that A, B, C, A_i are abelian groups (for i in an index set I).*

(a) *There is an abelian group isomorphism $\underline{\underline{\mathbb{Z}}}(\mathbb{Z}, A) \cong A$.*
(b) *There is an abelian group isomorphism*

$$\underline{\underline{\mathbb{Z}}}(C, A \times B) \cong \underline{\underline{\mathbb{Z}}}(C, A) \times \underline{\underline{\mathbb{Z}}}(C, B)\,.$$

(c) *There is an abelian group isomorphism*

$$\underline{\underline{\mathbb{Z}}}\Big(C, \prod_{i \in I} A_i\Big) \cong \prod_{i \in I} \underline{\underline{\mathbb{Z}}}(C, A_i)\,.$$

1.1.3. *Biproducts.* Suppose that $A_1, \dots, A_m, C$ are abelian groups, with homomorphisms $f_i\colon A_i \to C$ for $1 \le i \le m$. Consider the *insertions*

$$\iota_j\colon A_j \to \prod_{i=1}^m A_i; a_j \mapsto (0, \dots, 0, \overbrace{a_j}^{\text{Slot}j}, 0, \dots, 0) \tag{1.3}$$

for $1 \le j \le m$. Then

$$\sum_{i=1}^m f_i\colon \prod_{i=1}^m A_i \to C; (a_1, \dots, a_m) \mapsto \sum_{i=1}^m a_i f_i$$

is the unique homomorphism $f\colon \prod_{i=1}^m A_i \to C$ such that $\iota_j f = f_j$ for each $1 \le j \le m$. In other words, the product $\prod_{i=1}^m A_i$, with the insertions ι_i, is the *coproduct* of the groups A_i, $1 \le i \le m$. For this reason, the product $\prod_{i=1}^m A_i$ is described as the *biproduct* or *external direct sum* $\bigoplus_{i=1}^m A_i$ of the groups A_i (and occasionally as the *internal direct sum* of its embedded subgroups $A_i\iota_i$).

1.1.4. *Matrices.* Let $A_1, \dots, A_m$ and $B_1, \dots, B_n$ be abelian groups. Each element f of $\underline{\underline{\mathbb{Z}}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$ determines an *$m \times n$-matrix*

$$[f] = \begin{bmatrix} \iota_1 f \pi_1 & & \dots & & \iota_1 f \pi_n \\ & \dots & \iota_i f \pi_j & \dots & \\ \iota_m f \pi_1 & & \dots & & \iota_m f \pi_n \end{bmatrix} \tag{1.4}$$

with *(i,j)-entries* $\iota_i f \pi_j\colon A_i \to B_j$. Conversely, each $m \times n$-matrix

$$F = \begin{bmatrix} f_{11} & & \dots & & f_{1n} \\ & \dots & f_{ij} & \dots & \\ f_{m1} & & \dots & & f_{mn} \end{bmatrix}$$

with entries $f_{ij} \in \underline{\underline{\mathbb{Z}}}(A_i, B_j)$ determines a unique homomorphism

$$f\colon \bigoplus_{i=1}^m A_i \to \bigoplus_{j=1}^n B_j$$

whose matrix (1.4) is F (Exercise 8).

1.1.5. *Coproducts.* Let I be an arbitrary index set. Consider abelian groups A_i for $i \in I$. A coproduct of the groups A_i is constructed within the product $\prod_{j \in I} A_j$. Given i in I, an insertion $\iota_i \colon A_i \to \prod_{j \in I} A_j$ is defined as the product $\prod_{j \in I} \delta_{ij} \colon A_i \to \prod_{j \in I} A_j$ of the homomorphisms $\delta_{ij} \in \underline{\underline{\mathbb{Z}}}(A_i, A_j)$ with $\delta_{ii} = 1$ and $\delta_{ij} = 0$ for $i \neq j$ — compare (1.3). Then the *coproduct* $\coprod_{j \in I} A_j$ is defined as the subgroup of $\prod_{j \in I} A_j$ generated be the subset $\bigcup \{A_i \iota_i \mid i \in I\}$. Given homomorphisms $f_i \colon A_i \to C$ for $i \in I$, with common codomain C, a unique homomorphism $\sum_{i \in I} f_i$ or $f \colon \coprod_{j \in I} A_j \to C$, with $\iota_i f = f_i$ for $i \in I$, is defined by

$$f \colon \sum_{j=1}^{n} a_{i_j} \mapsto \sum_{j=1}^{n} a_{i_j} f_{i_j}$$

for $a_{i_j} \in A_{i_j}$, $1 \leq j \leq n$. Note that $\coprod_{j \in I} A_j$ is a proper subgroup of $\prod_{j \in I} A_j$ if infinitely many of the groups A_i are non-trivial (compare Exercise 13).

1.2. Rings. Suppose that A is an abelian group. Then the linear analogue of the set X^X of all functions on a set X is the set $\underline{\underline{\mathbb{Z}}}(A, A)$ of homomorphisms from A to A. Such homomorphisms are known as *endomorphisms*, and $\underline{\underline{\mathbb{Z}}}(A, A)$ is written as $\operatorname{End} A$. As noted in §1.1.2, there is a componentwise abelian group structure $(\operatorname{End} A, +, 0)$. On the other hand, $\operatorname{End} A$ is a submonoid of $(A^A, \cdot, 1)$.

Definition 1.5. Let $(S, +, 0)$ be an abelian group.

(a) If there is a semigroup structure $(S, \cdot)$ such that all the right multiplications

$$R(s) \colon S \to S; x \mapsto xs \tag{1.5}$$

and left multiplications

$$L(s) \colon S \to S; x \mapsto sx \tag{1.6}$$

by elements s of S are endomorphisms of $(S, +, 0)$, then S is said to be a (*non-unital*) *ring* $(S, +, \cdot)$.

(b) If there is a monoid structure $(S, \cdot, 1)$ such that $(S, +, \cdot)$ is a non-unital ring, then S is said to be a (*unital*) *ring* $(S, +, \cdot, 1)$.

(c) A ring $(S, +, \cdot)$ is *commutative* whenever the semigroup $(S, \cdot)$ is commutative.

In Definition 1.5(a), the endomorphism conditions on the right and left multiplications are described as *right* and *left distributivity*.

EXAMPLE 1.6. For an abelian group A, the set $\operatorname{End} A$ forms a unital ring $(\operatorname{End} A, +, \cdot, 1)$. Indeed, for elements $a \in A$ and $r, s, t \in \operatorname{End} A$, one has

$$a(r+s)t = (ar+as)t = art + ast = a(rs+st)$$

and

$$at(r+s) = atr + ats = a(tr+ts)\,,$$

so $(r+s)t = rs + rt$ and $t(r+s) = tr + ts$ as required.

EXAMPLE 1.7. Let A be an abelian group. Define $a \cdot b = 0$ for all $a, b \in A$. Then $(A, +, \cdot)$ is a non-unital ring, known as a *zero ring*.

DEFINITION 1.8. Let S be a unital ring.

(a) S is a(n *integral*) *domain* if $(S \smallsetminus \{0\}, \cdot, 1)$ is a commutative monoid.
(b) S is a *skewfield* if $(S \smallsetminus \{0\}, \cdot, 1)$ is a group.
(c) S is a *field* if $(S \smallsetminus \{0\}, \cdot, 1)$ is a commutative group.

EXAMPLE 1.9. (a) $\mathbb{Z}$ forms an integral domain.
(b) $\mathbb{R}$ and $\mathbb{C}$ form fields.
(c) $\mathbb{Z}/_n$ forms a field iff n is prime.

DEFINITION 1.10. Let S or $(S, +, 0)$ be a ring. Then the *opposite ring* S^{op} is the ring $(S, +, \circ)$ with $x \circ y = y \cdot x$ for $x, y \in S$.

1.2.1. *Matrix rings.* Let S be a ring. For positive integers m and n, the set of all $m \times n$-matrices with entries in S is written as S^n_m. As an implementation of the power S^{mn}, the set S^n_m has componentwise ring structure. The componentwise product is called the *Hadamard product*. On the other hand, the usual matrix multiplication (compare Exercise 9) gives a product $S^n_m \times S^p_n \to S^p_m$ for positive integers m, n, p. Equipped with this product and componentwise addition, the set S^n_n of all $n \times n$-matrices over S forms a ring $(S^n_n, +, \cdot)$, known as the $n \times n$ *matrix ring* over S. If S is unital, then $(S^n_n, +, \cdot, I_n)$ is unital with the $n \times n$ *identity matrix* having 1 in each diagonal entry and 0 in each off-diagonal position.

1.2.2. *The algebra of rings.* Since rings are algebras, the usual algebraic notions apply. It is sometimes necessary to distinguish carefully between the unital and non-unital cases when discussing subrings and ring homomorphisms, although the distinction is often left implicit.

DEFINITION 1.11. Let S be a ring.

(a) A subgroup J of $(S, +, 0)$ is said to be an *ideal*, written $J \lhd S$, if the *absorption properties*
$$\forall\ j \in J\,,\ \forall\ s \in S\,,\ js \in J \text{ and } sj \in J$$
are satisfied.

(b) The *ring kernel* of a ring homomorphism $f\colon S \to T$ is the group kernel $\operatorname{Ker} f = \{s \in S \mid sf = 0\}$.

PROPOSITION 1.12. *Let S be a ring.*

(a) *Each ring kernel in S is an ideal of S.*

(b) *For $J \lhd S$, the quotient group S/J has a well-defined multiplication making the group projection*
$$S \to S/J; s \mapsto s + J$$
a ring homomorphism.

DEFINITION 1.13. Let S be a ring.

(a) The *trivial* ideal is $\{0\}$ and the *improper* ideal is S.

(b) The ring S is *simple* if its only ideals are trivial or improper.

PROPOSITION 1.14. *Let S be a commutative, unital ring. Then S is a field if and only if it is simple and non-trivial.*

2. Modules

Modules over a ring are the linear analogues of sets with a semigroup or monoid action. In particular, abelian groups are modules over $\mathbb{Z}$, while real vector spaces are modules over $\mathbb{R}$.

2.1. Unital modules.

DEFINITION 2.1. Let S be a ring.

(a) If A is an abelian group with a non-unital ring homomorphism
$$r\colon S \to \operatorname{End} A; s \mapsto (A \to A; a \mapsto as)\,, \tag{2.1}$$
then A is said to be a (*non-unital*) (*right*) *S-module*.

(b) If A is an abelian group with a non-unital ring homomorphism

$$l\colon S^{\mathsf{op}} \to \operatorname{End} A; s \mapsto (A \to A; a \mapsto sa)\,, \tag{2.2}$$

then A is said to be a (*non-unital*) *left* S-*module*.

(c) If (2.1) is a unital ring homomorphism, then A is said to be a (*unital*) (*right*) S-*module*.

(d) If (2.2) is a unital ring homomorphism, then A is said to be a (*unital*) (*left*) S-*module*.

(e) An abelian group homomorphism $f\colon (A,+,0) \to (B,+,0)$ is a (*right* or *left*) S-*module homomorphism* $f\colon (A,+,S) \to (B,+,S)$ if it is a (right or left) S-set homomorphism.

(f) If K is a field, then a K-module is called a *vector space* over K, and K-module homomorphisms are often described as *linear transformations*.

EXAMPLE 2.2. Let S be a ring. Consider the matrix notation of §1.2.1. Then for positive integers m and n, the abelian group S^n_m becomes a left S^m_m-module and a right S^n_n-module under the usual matrix multiplication.

For a (unital) ring S, the category of (unital) right S-modules and homomorphisms is written as $\mathbf{Mod}_S$ or $\underline{\underline{S}}$. [This is the reason for the notation introduced in §1.1.2 for the category of abelian groups.] The category of (unital) left S-modules and homomorphisms is written as ${}_S\mathbf{Mod}$. For a commutative ring S, there is no essential distinction between left and right S-modules.

In many aspects of linear algebra over the field $\mathbb{R}$ of real numbers, the only relevant property of $\mathbb{R}$ is the field property. Thus the results and concepts of elementary linear algebra (bases, linear independence, dimension, etc.) apply equally to vector spaces over a general field K.

2.1.1. *The algebra of modules.* For a ring S, a set A that is both an abelian group and a right S-set is a right S-module if and only if $(a + b)s = as + bs$ for elements a, b in A and "scalars" $s \in S$. Since S-modules are algebras, the usual algebraic notions apply. If H is a submodule of a module A, then the group quotient A/H carries a well-defined S-module structure — with $(a+H)s = as+H$ for $a \in A$, $s \in S$ — such that the projection $A \to A/H; a \mapsto a + H$ becomes an S-module homomorphism. All the definitions of §1.1.1 (cokernels, exact sequences, ...) carry over, so the Extended First Isomorphism Theorem (Proposition 1.3) holds for S-modules (Exercise 20).

Given S-modules A_i (for i in an index set I), the product $\prod_{i\in I} A_i$ is the product both of the abelian groups A_i and the S-sets A_i. In other words, given S-homomorphisms $f_i \colon C \to A_i$ with common domain C, there is a unique S-homomorphism $f \colon C \to \prod_{i\in I} A_i$ such that $f\pi_i = f_i$ for each $i \in I$. Now the abelian group coproduct $\coprod_{i\in I} A_i$ is an S-subset of the S-set $\prod_{i\in I} A_i$, and thus an S-module. It is the *coproduct* of the S-modules A_i: Given S-homomorphisms $f_i \colon A_i \to C$ with common codomain C, there is a unique S-homomorphism $f \colon \coprod_{i\in I} A_i \to C$ such that $\iota_i f = f_i$ for each $i \in I$. If there are only finitely many non-trivial modules A_i, then the product and coproduct coincide to give the *biproduct* $\bigoplus_{i\in I} A_i$. In particular, the matrix notation of §1.1.4 applies to elements of $\underline{\underline{\mathbb{S}}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$.

2.1.2. *Schur's Lemma.* Suppose that S is a unital ring. For S-homomorphisms $f \colon A \to B$ and $g \colon A \to B$, the sum $f + g$ is an S-homomorphism. Thus $\underline{\underline{S}}(A, A)$ is an abelian subgroup of $\underline{\underline{Z}}(A, A)$.

Definition 2.3. A unital right S-module A is *simple* if it has no proper, non-trivial submodules.

Proposition 2.4 (Schur's Lemma). *Let A be a simple S-module. Then $\underline{\underline{S}}(A, A)$ is a skewfield.*

Proof. Consider an S-homomorphism $f \colon A \to A$. If the submodule $\operatorname{Ker} f$ is non-trivial, one has $\operatorname{Ker} f = A$ and $f = 0$. Otherwise, $\operatorname{Ker} f = \{0\}$ and f is injective. Since $f \neq 0$, the submodule $\operatorname{Im} f$ of A is non-trivial. Thus $\operatorname{Im} f = A$ and f is surjective. Thus f is invertible, and $f^{-1} \in \underline{\underline{S}}(A, A)$. □

2.2. Free and projective modules.

2.2.1. *Free modules.* Let S be a ring. An S-module F is said to be a *free module* over a set X if there is a function $\eta_X \colon X \to F$ such that each function $f \colon X \to A$ to an S-module A extends uniquely to an S-homomorphism $\overline{F} \colon F \to A$ such that $\eta_X f = \overline{f}$.

(2.3)
$$\begin{tikzcd} F \arrow[dr, dashed, "\overline{f}"] & \\ X \arrow[u, "\eta_X"] \arrow[r, "f"'] & A \end{tikzcd}$$

Specifically, one speaks of free right and left S-modules in the respective contexts of right and left S-modules.

PROPOSITION 2.5. *Let S be a unital ring.*

(a) *With scalar multiplications* (1.5) *for $s \in S$, the ring S becomes a unital right S-module, written as S or S_S.*
(b) *With $\eta_{\{x\}} \colon \{x\} \to S_S; x \mapsto 1$, the module S_S becomes a free unital right S-module over a singleton $\{x\}$.*
(c) *With scalar multiplications* (1.6) *for $s \in S$, the ring S becomes a unital left S-module, written as S or ${}_SS$.*
(d) *With $\eta_{\{x\}} \colon \{x\} \to_S S; x \mapsto 1$, the module ${}_SS$ becomes a free unital left S-module over $\{x\}$.*

DEFINITION 2.6. Let S be a unital ring.

(a) A submodule of S_S is called a *right ideal* of S.
(b) A submodule of ${}_SS$ is called a *left ideal* of S.

If S_S is playing the role of the free right S-module over $\{x\}$, as in Proposition 2.5(b), it is convenient to write it as $xS = \{xs \mid s \in S\}$ with $x1 = x$ and an S-module isomorphism $S \to xS; s \mapsto xs$, taking $\eta_{\{x\}} \colon \{x\} \to xS; x \mapsto x$.

COROLLARY 2.7. *Let X be a set. Then the coproduct $\sum_{x \in X} xS$ is the free right S-module over X, with*

$$\eta_X \colon X \to \sum_{x \in X} xS; x \mapsto x\eta_{\{x\}}\iota_x .$$

Given a function $f \colon X \to A$ from X to an S-module A, the map

$$\overline{f} \colon \sum_{x \in X} xS \to A; \sum_{j=1}^{n} x_j s_j \mapsto \sum_{j=1}^{n} x_j f s_j$$

is the unique S-homomorphic extension of $f \colon X \to A$.

2.2.2. *Projective modules.*

DEFINITION 2.8. Let S be a unital ring. A S-module P is said to be *projective* if for each S-homomorphism $f \colon P \to B$ and surjective S-homomorphism $s \colon A \to B$, there is an S-homomorphism $\overline{f} \colon P \to A$ such that $\overline{f}s = f$. Each such homomorphism $\overline{f}$ is called a *lifting* of f from B to A.

Definition 2.8 may be illustrated as follows:

(2.4)
$$\begin{tikzcd}
& A \arrow[d, "s"] \\
P \arrow[ur, dashed, "\overline{f}"] \arrow[r, "f"'] & B \arrow[d] \\
& 0
\end{tikzcd}$$

The right hand side of the picture is understood as an exact sequence, expressing the surjectivity of s — compare Definition 1.2(a). Note that the lifting $\overline{f}$ of f is not required to be unique.

Proposition 2.9. *Let S be a unital ring.*

(a) *A free S-module is projective.*
(b) *An S-module P is projective if and only if there is a free S-module F with an isomorphism $F \cong P \oplus Q$.*

Proof. For (a), suppose that P is free over X. Consider the situation of (2.4). Let $r \colon B \to A$ be a retract for $s \colon A \to B$. Then $\overline{f} \colon P \to A$ is the unique homomorphic extension of the restriction of fr to $X\eta_X$. The proof of (b) is left as Exercise 22. $\square$

Example 2.10. By Proposition 2.9(b), the $(\mathbb{Z}\times\mathbb{Z})$-module $\mathbb{Z}\times\{0\}$ is projective (but not free).

2.3. Duality.

Proposition 2.11. *Consider a unital ring S and an abelian group G.*

(a) *Let A be a right S-module. Then the abelian group $\underline{\underline{\mathbb{Z}}}(A, G)$, with scalar multiplications defined by the mixed associative law*
$$a(s\alpha) = (as)\alpha$$
for $a \in A$, $s \in S$, $\alpha \in \underline{\underline{\mathbb{Z}}}(A, G)$, is a left S-module.

(a) *Let B be a left S-module. Then the abelian group $\underline{\underline{\mathbb{Z}}}(B, G)$, with scalar multiplications defined by the mixed associative law*
$$(\beta s)(b) = \beta(sb)$$
for $b \in A$, $s \in S$, $\beta \in \underline{\underline{\mathbb{Z}}}(B, G)$, is a right S-module.

Definition 2.12. The modules $A^T = \underline{\underline{\mathbb{Z}}}(A, G)$ and $B^T = \underline{\underline{\mathbb{Z}}}(B, G)$ of Proposition 2.11 are known as the modules *dual* to the respective modules A and B.

Example 2.13. Given S-modules A_i (for i in an index set I), there is an abelian group isomorphism

$$\theta\colon \underline{\underline{\mathbb{Z}}}\Big(\coprod_{i\in I} A_i, G\Big) \to \prod_{i\in I} \underline{\underline{\mathbb{Z}}}(A_i, G)\,,$$

where $\big(\sum_{i\in I} f_i\big)\theta$ is determined by its projections $\big(\sum_{i\in I} f_i\big)\theta\pi_j = f_j$ for $j \in I$. Now for $s \in S$, one has

$$\big(s\sum_{i\in I} f_i\big)\theta\pi_j = \big(\sum_{i\in I} sf_i\big)\theta\pi_j = sf_j\,,$$

whence $\big(s\sum_{i\in I} f_i\big)\theta = s\big((\sum_{i\in I} f_i)\theta\big)$, and θ becomes a left S-module homomorphism. In other words, the dual $\big(\coprod_{i\in I} A_i\big)^T$ of the coproduct is (isomorphic to) the product $\prod_{i\in I} A_i^T$ of the duals.

Example 2.14. Let S be a unital ring, and let G be the abelian group $(S, +, 0)$. Consider the free right S-module S_S of Proposition 2.5(a). Define

$$R\colon S \to S_S^T; t \mapsto \big(R(t)\colon S \to S; s \mapsto st\big)\,.$$

For $x, s, t \in S$, one has $x\big(sR(t)\big) = (xs)R(t) = (xs)t = x(st) = xR(st)$ and $t = 1R(t)$. Thus R is a left S-module homomorphism embedding the free left S-module ${}_SS$ of Proposition 2.5(c) as a submodule of the dual S_S^T.

2.3.1. *Dual homomorphisms.* Fix a unital ring S and an abelian group G. Let $f\colon A \to B$ be a homomorphism of right S-modules. Then, as illustrated below,

$$\begin{tikzcd}
A \arrow[rrrr, "f"] \arrow[ddrr, bend right] & & & & B \arrow[ddll, bend left] \\
& f\beta & & \beta \arrow[ll, mapsto, "f^T"'] & \\
& & G & &
\end{tikzcd}$$

a map $\underline{\underline{Z}}(f, G)$ or f^T is defined as $f^T \colon B^T \to A^T; \beta \mapsto f\beta$. This map, which is a left S-module homomorphism (Exercise 26), is defined as the *dual* of the S-homomorphism f. Given a further S-homomorphism $g \colon B \to C$, one has $(fg)^T = g^T f^T$. Dual homomorphisms are often written with Eulerian notation, so that this relationship takes the form $(fg)^T = f^T \circ g^T$. In general, duality in linear mathematics means applying the construction $\underline{\underline{Z}}(\_, G)$.

2.3.2. *Transposes of matrices.* Fix a unital ring S and an abelian group G. For given right S-modules $A_1, \dots, A_m$ and $B_1, \dots, B_n$, consider an element f of $\underline{\underline{S}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$. Recall that f has a matrix $[f]$ as in §1.1.4, with (i,j)-entries f_{ij} or $\iota_i f \pi_j \colon A_i \to B_j$. By Example 2.13, one obtains

$$\begin{aligned}\left(\bigoplus_{i=1}^m A_i\right)^T &= \underline{\underline{S}}\left(\bigoplus_{i=1}^m A_i, G\right) = \underline{\underline{S}}\left(\coprod_{i=1}^m A_i, G\right) \\ &\cong \prod_{i=1}^m \underline{\underline{S}}(A_i, G) = \bigoplus_{i=1}^m \underline{\underline{S}}(A_i, G) = \bigoplus_{i=1}^m A_i^T\end{aligned}$$

and $\left(\bigoplus_{j=1}^n B_j\right)^T \cong \bigoplus_{j=1}^n B_j^T$, the isomorphisms being homomorphisms of left S-modules. Thus f^T, which *a priori* is an element of the group

$$\underline{\underline{\mathbb{Z}}}\left(\left(\bigoplus_{j=1}^n B_j\right)^T, \left(\bigoplus_{i=1}^m A_i\right)^T\right),$$

becomes an element of $\underline{\underline{\mathbb{Z}}}\left(\bigoplus_{j=1}^n B_j^T, \bigoplus_{i=1}^m A_i^T\right)$. Two questions then arise: What is the $n \times m$-matrix $[f^T]$ of f^T, and what relationship does that matrix $[f^T]$ bear to the $m \times n$-matrix $[f]$ of f?

To answer these questions, consider $\beta_j \in B_j^T$ for $1 \le j \le n$ and $1 \le i \le m$ in the following commutative diagram:

$$\begin{tikzcd}
\bigoplus_{i=1}^m A_i \arrow[rr, "f"] \arrow[dr, "f\pi_j\beta_j"] & & \bigoplus_{j=1}^n B_j \arrow[dl, "\pi_j\beta_j"'] \arrow[dd, "\pi_j"] \\
& G & \\
A_i \arrow[uu, "\iota_i"] \arrow[ur, "\iota_i f\pi_j\beta_j"'] & & B_j \arrow[ul, "\beta_j"]
\end{tikzcd}$$

Then under the composite $B_j^T \xrightarrow{\iota_j} \bigoplus_{k=1}^n B_k \xrightarrow{f^T} \bigoplus_{h=1}^m A_h \xrightarrow{\pi_i} A_i^T$, the element β_j maps to $\iota_i f \pi_j \beta_j = f_{ij}\beta_j = f_{ij}^T(\beta_j)$. Thus:

THEOREM 2.15. *If* $f \in \underline{\underline{S}}\left(\bigoplus_{i=1}^m A_i, \bigoplus_{j=1}^n B_j\right)$ *has* $m \times n$*-matrix* $[f_{ij}]$*, the dual homomorphism* $f^T \in \underline{\underline{\mathbb{Z}}}\left(\bigoplus_{j=1}^n B_j^T, \bigoplus_{i=1}^m A_i^T\right)$ *has an* $n \times m$*-matrix whose* (j,i)*-entry is the dual* f_{ij}^T *of the* (i,j)*-entry* f_{ij} *of* $[f]$*.*

In Theorem 2.15, the $n \times n$-matrix $[f^T]$ is called the *transpose* of the $m \times n$-matrix $[f]$.

3. Exercises

(1) Let $h\colon A \to B$ be a homomorphism of abelian groups.
   (a) Prove that h is injective if and only if $\operatorname{Ker} h = 0$.
   (b) Prove that h is surjective if and only if $\operatorname{Coker} h = 0$.
   (b) Prove that h is an isomorphism if and only if the sequence $0 \to A \xrightarrow{h} B \to 0$ is exact.

(2) Let $0 \to A \to B \to C \to 0$ be an exact sequence of finite abelian groups. Prove that $\log|A| - \log|B| + \log|C| = 0$.

(3) Let $0 \to A_0 \to A_1 \to \cdots \to A_n \to 0$ an exact sequence of finite abelian groups. Prove that $\sum_{i=0}^n (-1)^i \log|A_i| = 0$.

(4) Prove the Extended First Isomorphism Theorem (Proposition 1.3).

(5) Give an example of groups G and H such that the set of group homomorphisms from G to H is not a subgroup of the power H^G (with componentwise operations).

(6) Prove Proposition 1.4.

(7) Let $A_1, \dots, A_m, C$ be abelian groups. Show that

$$\underline{\underline{\mathbb{Z}}}\left(C, \bigoplus_{i=1}^m A_i\right) \cong \prod_{i=1}^m \underline{\underline{\mathbb{Z}}}(C, A_i)$$

and

$$\underline{\underline{\mathbb{Z}}}\left(\bigoplus_{i=1}^m A_i, C\right) \cong \prod_{i=1}^m \underline{\underline{\mathbb{Z}}}(A_i, C)\,.$$

(8) Prove the claim of §1.1.4.

(9) Let $A_1, \dots, A_m$, $B_1, \dots, B_n$, and $C_1, \dots, C_p$ be abelian groups. Consider homomorphisms

$$f\colon \bigoplus_{i=1}^{m} A_i \to \bigoplus_{j=1}^{n} B_j \quad \text{and} \quad g\colon \bigoplus_{j=1}^{n} B_j \to \bigoplus_{k=1}^{p} C_k$$

with matrices $[f]$ and $[g]$. Determine the matrix $[fg]$ of

$$fg\colon \bigoplus_{i=1}^{m} A_i \to \bigoplus_{k=1}^{p} C_k$$

in terms of the entries f_{ij} and g_{jk}.

(10) Let $A, A_1, \dots, A_m$ be abelian groups. Show that the group A is the biproduct of $A_1, \dots, A_m$ if and only if there are homomorphisms $p_i\colon A \to A_i$ and $j_i\colon A_i \to A$ for $1 \le i \le m$ such that:
(a) $\forall\ 1 \le h, i \le m\,,\ j_h p_i = \delta_{hi} 1_{A_i}$;
(b) $1_A = \sum_{i=1}^{m} p_i j_i$ in $\underline{\underline{\mathbb{Z}}}(A, A)$.

(11) An exact sequence, with three groups sandwiched between zero groups, is called a *short exact sequence*. Let

$$0 \to A \xrightarrow{\ j\ } E \xrightarrow{\ p\ } Q \to 0$$

be a short exact sequence of abelian groups. In this context, E is called an *extension* of A by Q. Show that the following three conditions are equivalent:
(a) The surjection $p\colon E \to Q$ has a section $s\colon Q \to E$ that is a homomorphism;
(b) The injection $j\colon A \to E$ has a retract $r\colon E \to A$ that is a homomorphism;
(c) The extension E is the internal direct sum of $\operatorname{Im} j$ and $\operatorname{Coker} j$.

(If these conditions hold, the extension and the exact sequence are said to *split*).

(12) Let B be an abelian group. Consider subgroups B_i of B, with i in an index set I. Show that the subgroup of B generated by $\bigcup\{B_i \mid i \in I\}$ is

$$\left\{ \sum_{j=1}^{n} b_{i_j} \;\middle|\; n \in \mathbb{N}\,,\ 1 \le j \le n\,,\ i_j \in I\,,\ b_{i_j} \in B_{i_j} \right\}.$$

(13) For each natural number n, let A_n be a copy of the abelian group $\mathbb{Z}/_2$ of bits or integers modulo 2 under addition. Show that the set $\coprod_{n\in\mathbb{N}} A_n$ is countable, while the set $\prod_{n\in\mathbb{N}} A_n$ is uncountable.

(14) If a positive integer n is composite, show that $\mathbb{Z}/_n$ is not an integral domain.

(15) Complete the verification of the claims of §1.1.5.

(16) Let A be a zero ring. Show that the 2×2 matrix ring A^2_2 is commutative.

(17) Prove Proposition 1.12, and formulate the First Isomorphism Theorem for Rings.

(18)
  (a) Prove Proposition 1.14.
  (b) Give an example of a simple, non-trivial commutative ring which is not a field.

(19) Let S be a field. For $1 < n \in \mathbb{Z}$, show that S^n_n is a simple, non-trivial unital ring which is not a skewfield. [Hint: For $1 \leq k, l \leq n$, consider the *elementary matrices* E^{kl} with i, j-entry $[E^{kl}]_{ij} = \delta_{ik}\delta_{jl}$.]

(20) Let S be a unital ring. Formulate and prove the Extended First Isomorphism Theorem for right S-modules.

(21)
  (a) Prove Proposition 2.5 and Corollary 2.7.
  (b) Formulate and prove the analogue of Corollary 2.7 for left S-modules.

(22) Complete the proof of Proposition 2.9.

(23) An element e of a ring S is said to be *idempotent* if $ee = e$. Suppose that e is an idempotent element of a unital ring S.
  (a) Show that $eS = \{es \mid s \in S\}$ is a right ideal of S.
  (b) Show that eS is a projective right S-module.

(24) Let A be a finitely generated abelian group. Use the structure theory for such groups to show that if A is projective, then it is free.

(25) Prove Proposition 2.11.

(26) Suppose that $f: A \to B$ is a right S-homomorphism. Show that $f^T: B^T \to A^T$ is a left S-homomorphism.

(27) For $1 < n \in \mathbb{Z}$, consider the abelian group $\mathbb{Z}/_n$ as a $\mathbb{Z}$-module. Let G be the *circle group*, the group $\{z \in \mathbb{C} \mid z\overline{z} = 1\}$ of complex numbers of unit modulus. Show that $\mathbb{Z}/_n$ is isomorphic with its dual $\mathbb{Z}/_n^T$.

CHAPTER 8

Matrix constructions

1. Skewfields and number fields

1.1. Complex numbers. Complex numbers arose from the need to adjoin a square root i of -1 to the field $\mathbb{R}$ of real numbers.

1.1.1. *Scalar matrices.* Let S be a unital ring. Let n be a positive integer. The unital ring S^n_n of $n \times n$-matrices over S has multiplicative identity I_n. Consider the injective unital ring homomorphism

$$\eta \colon S \to S^n_n ; s \mapsto sI_n \,.$$

The image $\{sI_n \mid s \in S\}$ of η is the set of *scalar matrices*. It is convenient to identify the ring S with this image, e.g. writing $I_n = 1$.

1.1.2. *Constructing complex numbers.* Let S be a commutative, unital ring. Consider the element

$$i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{1.1}$$

of S^2_2. In the right $\mathbb{R}^2_2$-set $\mathbb{R}^2_1$, the actions $[1\ 0] \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = [0\ 1]$ and $[0\ 1] \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = [-1\ 0]$ show that the matrix i implements a counter-clockwise rotation by $\pi/2$. Since negation of two-dimensional vectors is the same as rotation by π, one obtains $i^2 = -1$. Define the set of *complex numbers* as

$$\mathbb{C} = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \;\middle|\; x, y \in \mathbb{R} \right\} \tag{1.2}$$

or

$$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\} \,. \tag{1.3}$$

The proof of the following result is assigned as Exercise 2.

LEMMA 1.1. *Let S be a ring. For* $\alpha = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ *in* S_2^2, *define*

$$S[\alpha] = \left\{ \begin{bmatrix} x + ya_{11} & ya_{12} \\ ya_{21} & x + ya_{22} \end{bmatrix} \;\middle|\; x, y \in S \right\}.$$

Then if S is commutative, $S[\alpha]$ forms a commutative subring of S_2^2.

DEFINITION 1.2. The ring $\mathbb{Z}[i]$ is called the *ring of Gaussian integers*.

PROPOSITION 1.3. *The set $\mathbb{C}$ of complex numbers forms a field.*

PROOF. By Lemma 1.1, $\mathbb{C} = \mathbb{R}[i]$ forms a commutative subring of $\mathbb{R}_2^2$. Note the equation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} I_2 \tag{1.4}$$

which holds in S_2^2 for any commutative, unital ring S. Now

$$\det \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = x^2 + y^2$$

is 0 iff $x = y = 0$, so $\mathbb{C}$ is a field. □

COROLLARY 1.4. *Let S be a field where the equation $x^2 + y^2 = 0$ has only the trivial solution $x = y = 0$. Then $S[i]$ forms a field.*

EXAMPLE 1.5. The ring $\mathbb{Z}/_3[i]$ forms a field, whereas $\mathbb{Z}/_5[i]$ does not.

1.1.3. *Complex number terminology.* Because complex numbers were developed before matrices, they have their own terminology. Here is a dictionary to translate into matrix terms.

Matrix $Z = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$	Complex number $z = x + iy$	Value
$\sqrt{\det Z} = \sqrt{ZZ^T}$	Absolute value $\|z\|$	$\sqrt{x^2+y^2}$
Z^T	Complex conjugate $\overline{z}$	$x - iy$
$\frac{1}{2}\mathrm{tr}\, Z = \frac{1}{2}(Z + Z^T)$	Real part $\mathrm{Re}\, z = \frac{1}{2}(z + \overline{z})$	x
$\frac{1}{2i}(Z - Z^T)$	Imaginary part $\mathrm{Im}\, z = \frac{1}{2i}(z - \overline{z})$	y

REMARK 1.6. Since $\mathbb{C}$ is commutative, matrix transposition/complex conjugation provides an automorphism of $\mathbb{C}$, defined by preserving $\mathbb{R}$ and mapping $i \mapsto -i$. In quantum mechanics, which is based on $\mathbb{C}$, this automorphism models time reversal.

1.1.4. *The one-dimensional unit sphere.*

DEFINITION 1.7. The subset

$$\{z \in \mathbb{C} \mid 1 = |z|\}$$

of $\mathbb{C}$ is called the *one-dimensional unit sphere* S^1.

PROPOSITION 1.8. *The one-dimensional unit sphere S^1 is a subgroup of the (commutative) group of units $\mathbb{C}^*$.*

PROOF. The matrix equation $\det AB = \det A \det B$ yields the complex number formula

$$|z_1 z_2| = |z_1| \cdot |z_2| \,, \tag{1.5}$$

while the matrix equation $\det A^T = \det A$ yields the complex number formula $|\overline{z}| = |z|$ (compare §1.1.3). It follows that S^1 is closed under multiplication and inversion. □

REMARK 1.9. The equation (1.5), written in the equivalent form

$$|z_1|^2 \cdot |z_2|^2 = |z_1 z_2|^2$$

or

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + y_1 x_2)^2 \tag{1.6}$$

for elements x_j, y_k of a general commutative ring S, shows that the product of two sums of two squares is again a sum of two squares. In the form (1.6), it is known as the *Two Squares Identity*.

Let θ be a real number. Consider the series

$$\begin{aligned}\exp(i\theta) &= \sum_{k=0}^{\infty}\frac{(i\theta)^k}{k!} = \sum_{k=0}^{\infty}\frac{(i\theta)^{2k}}{(2k)!} + \sum_{k=0}^{\infty}\frac{(i\theta)^{2k+1}}{(2k+1)!} \\ &= \sum_{k=0}^{\infty}(-1)^k\frac{\theta^{2k}}{(2k)!} + i\sum_{k=0}^{\infty}(-1)^k\frac{\theta^{2k+1}}{(2k+1)!} \\ &= \cos\theta + i\sin\theta = \begin{bmatrix}\cos\theta & \sin\theta \\ -\sin\theta & \cos\theta\end{bmatrix}\end{aligned} \tag{1.7}$$

representing a counter-clockwise rotation by an angle θ (in radians). Note $\det\exp(i\theta) = \cos^2\theta + \sin^2\theta = 1$, so $\exp(i\theta) \in S^1$. Indeed,

$$S^1 = \left\{ \begin{bmatrix}\cos\theta & \sin\theta \\ -\sin\theta & \cos\theta\end{bmatrix} \;\middle|\; \theta \in \mathbb{R} \right\}.$$

PROPOSITION 1.10. *There is a surjective group homomorphism*

$$(\mathbb{R}, +, 0) \to S^1; \theta \mapsto \exp(2\pi i\theta) \tag{1.8}$$

with group kernel $(\mathbb{Z}, +, 0)$*, so* $\mathbb{R}/\mathbb{Z} \cong S^1$.

Note that the semigroup isomorphism property of (1.8) yields the addition formulae for the sine and cosine functions.

1.1.5. *Roots of unity.* Just as S^1 contains the square roots $\pm i$ of 1, it also contains other roots of unity. Indeed, for a given positive integer r, the complex number

$$\zeta_r = \exp(2\pi i/r) = \begin{bmatrix}\cos\frac{2\pi i}{r} & \sin\frac{2\pi i}{r} \\ -\sin\frac{2\pi i}{r} & \cos\frac{2\pi i}{r}\end{bmatrix} = \cos\frac{2\pi i}{r} + i\sin\frac{2\pi i}{r}$$

satisfies $\zeta_r^r = 1$.

1.2. Number fields.

DEFINITION 1.11. A (n *algebraic*) *number field* is a field K, containing $\mathbb{Q}$, such that K has a finite basis as a vector space over $\mathbb{Q}$.

EXAMPLE 1.12. The ring $\mathbb{Q}[i]$ of *Gaussian rationals* is an algebraic number field. Indeed, the nonzero elements of $\mathbb{Q}[i]$ are invertible in $\mathbb{C}$, and (1.4) shows that $\mathbb{Q}[i]$ is closed under these inverses. The set $\{1, i\}$ forms a basis for $\mathbb{Q}[i]$ over $\mathbb{Q}$.

PROPOSITION 1.13. *Let n be a positive integer whose square root $\sqrt{n}$ is irrational. Then setting*

$$\sqrt{n} = \begin{bmatrix} 0 & n \\ 1 & 0 \end{bmatrix}, \tag{1.9}$$

the set

$$\mathbb{Q}\big[\sqrt{n}\,\big] = \left\{ \begin{bmatrix} x & ny \\ y & x \end{bmatrix} \;\middle|\; x, y \in \mathbb{Q} \right\}$$

is an algebraic number field with $\mathbb{Q}$-basis $\{1, \sqrt{n}\,\}$.

PROOF. First note that

$$\begin{bmatrix} 0 & n \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & n \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix} = n\,,$$

so the notation (1.9) is justified. Lemma 1.1 shows that $\mathbb{Q}\big[\sqrt{n}\,\big]$ is a commutative ring. Now

$$\det \begin{bmatrix} x & ny \\ y & x \end{bmatrix} = x^2 - ny^2 = 0$$

iff $x^2 = ny^2$. A nontrivial, rational solution x, y to this equation would imply that $\sqrt{n}$ is rational. Thus each nonzero element of $\mathbb{Q}\big[\sqrt{n}\,\big]$ is an invertible matrix. By (1.4), the inverse lies in $\mathbb{Q}\big[\sqrt{n}\big]$, so $\mathbb{Q}\big[\sqrt{n}\,\big]$ becomes a field. $\square$

COROLLARY 1.14. *Let n be a non-square element of a field S. Let*

$$\sqrt{n} = \begin{bmatrix} 0 & n \\ 1 & 0 \end{bmatrix}.$$

Then $S\big[\sqrt{n}\,\big]$ forms a field.

EXAMPLE 1.15. The ring $\mathbb{Z}/_5\big[\sqrt{2}\,\big]$ forms a field.

1.3. Quaternions. Let S be a unital ring. Define the matrices

$$i = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \; j = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \; k = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

in S_4^4. Since the relations

$$i^2 = j^2 = k^2 = -1 \tag{1.10}$$

and

$$ij = k,\ jk = i,\ ki = j; \qquad ji = -k,\ kj = -i,\ ik = -j \tag{1.11}$$

are satisfied (Exercise 9), one has the following.

PROPOSITION 1.16. *Let S be a commutative, unital ring. Let $S[i, j, k]$ denote the subset $\{t + xi + yj + zk \mid t, x, y, z \in S\} =$*

$$\left\{ \begin{bmatrix} t & x & y & z \\ -x & t & -z & y \\ -y & z & t & -x \\ -z & -y & x & t \end{bmatrix} \middle| \, t, x, y, z \in S \right\}$$

of S_4^4. Then $S[i, j, k]$ is a subring of S_4^4.

LEMMA 1.17. *Consider elements t, x, y, z of a commutative, unital ring S.*

(a) *The product*

$$\begin{bmatrix} t & x & y & z \\ -x & t & -z & y \\ -y & z & t & -x \\ -z & -y & x & t \end{bmatrix} \begin{bmatrix} t & -x & -y & -z \\ x & t & z & -y \\ y & -z & t & x \\ z & y & -x & t \end{bmatrix}$$

of the matrix $t + xi + yj + zk$ with its transpose is the scalar matrix $t^2 + x^2 + y^2 + z^2$.

(b) *One has* $\det(t + xi + yj + zk) = (t^2 + x^2 + y^2 + z^2)^2$.

(c) *The* Four Squares Identity

$$\begin{aligned}(t_1^2 + x_1^2 + y_1^2 + z_1^2)&(t_2^2 + x_2^2 + y_2^2 + z_2^2) \\ &= (t_1t_2 - x_1x_2 - y_1y_2 - z_1z_2)^2 + (t_1x_2 + t_2x_1 + y_1z_2 - y_2z_1)^2 \\ &\quad + (t_1y_2 + t_2y_1 - x_1z_2 + x_2z_1)^2 + (t_1z_2 + t_2z_1 + x_1y_2 - x_2y_1)^2\end{aligned}$$

holds for elements t_h, x_h, y_h, z_h of S.

PROOF. Part (a) is verified by direct computation. For part (b), set $X = t + xi + yj + zk$ and $s = t^2 + x^2 + y^2 + z^2$. By (a), one has $XX^T = sI_4$. Then $(\det X)^2 = \det X \det X^T = \det(XX^T) = \det(sI_4) = s^4$. Part (c) is a consequence of (b) and the matrix identity $\det X_1 \det X_2 = \det(X_1X_2)$, setting $X_h = t_h + x_hi + y_hj + z_hk$. $\square$

THEOREM 1.18. *The ring $\mathbb{H} = \mathbb{R}[i, j, k]$ is a skewfield.*

REMARK 1.19. The choice of the letter "H" commemorates Hamilton.

COROLLARY 1.20. *Let S be a field where the equation $t^2 + x^2 + y^2 + z^2 = 0$ has only the trivial solution $t = x = y = z = 0$. Then $S[i, j, k]$ forms a skewfield that is not commutative.*

PROOF. Note $x \neq -x$ for a nonzero element of S, since $t^2 + x^2 + y^2 + z^2 = 0$ has the nontrivial solution $t = x = y = z = 1$ in $\mathbb{Z}/_2$. Then $ij = k \neq -k = ji$ in $S[i, j, k]$, so $S[i, j, k]$ is not commutative. □

DEFINITION 1.21. Elements $t + xi + yj + zk$ of the skewfield $\mathbb{H}$ are known as *quaternions*. The real number t is the *real part*, and $xi + yj + zk$ is the *imaginary part*, of a quaternion $t + xi + yj + zk$. A quaternion with zero real part is said to be *purely imaginary*.

1.3.1. *Quaternions and Euclidean space.* Consider a purely imaginary quaternion $\mathbf{x} = xi + yj + zk$. Lemma 1.17(b) shows that $\det \mathbf{x} = |\mathbf{x}|^4$ with the Euclidean norm $|\mathbf{x}| = \sqrt{x^2 + y^2 + z^2}$. Then for quaternions $t_h + \mathbf{x}_h = t_h + x_h i + y_h j + z_h k$, the matrix product in $\mathbb{H}$ becomes

$$(t_1 + \mathbf{x}_1)(t_2 + \mathbf{x}_2) = (t_1 t_2 - \mathbf{x}_1 \cdot \mathbf{x}_2) + (t_1 \mathbf{x}_2 + t_2 \mathbf{x}_1 + \mathbf{x}_1 \times \mathbf{x}_2) \tag{1.12}$$

making use of the usual dot or scalar product $\mathbf{x}_1 \cdot \mathbf{x}_2$ and cross or vector product $\mathbf{x}_1 \times \mathbf{x}_2$ for vectors $\mathbf{x}_h$ from three-dimensional Euclidean space. Using distributivity and the way scalar matrices behave, it suffices to remember just the fragment

$$\mathbf{x}_1 \mathbf{x}_2 = -\mathbf{x}_1 \cdot \mathbf{x}_2 + \mathbf{x}_1 \times \mathbf{x}_2$$

of (1.12). The set of purely imaginary quaternions is written as $\mathbb{R}^3 \subset \mathbb{H}$.

1.3.2. *The three-dimensional unit sphere.*

DEFINITION 1.22. The subset

$$\{t + xi + yj + zk \in \mathbb{H} \mid t^2 + x^2 + y^2 + z^2 = 1\}$$

of $\mathbb{H}$ is called the *three-dimensional unit sphere* S^3. Elements of S^3 are described as *unit quaternions*.

PROPOSITION 1.23. *The three-dimensional unit sphere S^3 is a subgroup of the group of units $\mathbb{H}^*$.*

PROOF. By the Four Squares Identity, S^3 is closed under multiplication. Lemma 1.17(a) shows that S^3 is closed under inversion. □

DEFINITION 1.24. The subgroup S^3 of $\mathbb{H}^*$ is known as the *spin group* Spin_3.

1.3.3. *Complex numbers in the quaternions.* Suppose that $\mathbf{w}$ is a purely imaginary unit quaternion. (One may take $\pm i, \pm j$ or $\pm k$ as examples.) Then (1.12) yields

$$(u_1 + v_1\mathbf{w})(u_2 + v_2\mathbf{w}) = (u_1u_2 - v_1v_2) + (u_1v_2 + v_1u_2)\mathbf{w}$$

for $u_h, v_h \in \mathbb{R}$. In other words,

$$\mathbb{C}_{\mathbf{w}} = \{u + v\mathbf{w} \in \mathbb{H} \mid u, v \in \mathbb{R}\}$$

provides an implementation of the complex number field $\mathbb{C}$ in $\mathbb{H}$. In particular, (1.7) yields the element

$$\exp(\mathbf{w}\theta) = \cos\theta + \mathbf{w}\sin\theta \tag{1.13}$$

of $\mathbb{C}_{\mathbf{w}}$. Note that $\exp(\mathbf{w}\theta)$ is a unit quaternion, and indeed

$$S^3 = \{\exp(\mathbf{w}\theta) \mid \ \theta \in \mathbb{R}\,,\ \mathbf{w} \in S^3 \cap \mathbb{R}^3 \subset \mathbb{H}\} \tag{1.14}$$

(Exercise 14).

1.3.4. *Rotations in Euclidean space.* Let $\mathbf{w}$ be a purely imaginary unit quaternion, and consider the quaternion $\exp(\mathbf{w}\theta/2)$. For an element $\mathbf{x}$ of $\mathbb{R}^3 \subset \mathbb{H}$, one has

$$\begin{aligned}
\exp(-\mathbf{w}\theta/2)\mathbf{x}\exp(\mathbf{w}\theta/2) &= \left(\cos\frac{\theta}{2} - \mathbf{w}\sin\frac{\theta}{2}\right)\mathbf{x}\left(\cos\frac{\theta}{2} + \mathbf{w}\sin\frac{\theta}{2}\right) \\
&= \left(\mathbf{w}\cdot\mathbf{x}\sin\frac{\theta}{2} + \mathbf{x}\cos\frac{\theta}{2} - (\mathbf{w}\times\mathbf{x})\sin\frac{\theta}{2}\right)\left(\cos\frac{\theta}{2} + \mathbf{w}\sin\frac{\theta}{2}\right) \\
&= \mathbf{w}\cdot\mathbf{x}\sin\frac{\theta}{2}\cos\frac{\theta}{2} + (\mathbf{w}\cdot\mathbf{x})\mathbf{w}\sin^2\frac{\theta}{2} \\
&\quad + \mathbf{x}\cos^2\frac{\theta}{2} - \mathbf{x}\cdot\mathbf{w}\cos\frac{\theta}{2}\sin\frac{\theta}{2} + (\mathbf{x}\times\mathbf{w})\cos\frac{\theta}{2}\sin\frac{\theta}{2} \\
&\quad - (\mathbf{w}\times\mathbf{x})\sin\frac{\theta}{2}\cos\frac{\theta}{2} - \big((\mathbf{w}\times\mathbf{x})\times\mathbf{w}\big)\sin^2\frac{\theta}{2} \\
&= (\mathbf{w}\cdot\mathbf{x})\mathbf{w}\sin^2\frac{\theta}{2} + \mathbf{x}\cos^2\frac{\theta}{2} + (\mathbf{x}\times\mathbf{w})\sin\theta \\
&\quad + \big((\mathbf{w}\cdot\mathbf{x})\mathbf{w} - (\mathbf{w}\cdot\mathbf{w})\mathbf{x}\big)\sin^2\frac{\theta}{2} \\
&= \mathbf{x}\cos\theta + (\mathbf{x}\times\mathbf{w})\sin\theta + 2(\mathbf{w}\cdot\mathbf{x})\mathbf{w}\sin^2\frac{\theta}{2}\,, \qquad (1.15)
\end{aligned}$$

which again is an element of $\mathbb{R}^3 \subset \mathbb{H}$. In other words, the quaternion $\exp(\mathbf{w}\theta/2)$ determines the transformation

$$T(\exp(\mathbf{w}\theta/2))\colon \mathbb{R}^3 \to \mathbb{R}^3; \mathbf{x} \mapsto \exp(-\mathbf{w}\theta/2)\mathbf{x}\exp(\mathbf{w}\theta/2) \qquad (1.16)$$

of Euclidean space. For $\mathbf{x}$ orthogonal to $\mathbf{w}$, one has

$$\mathbf{x}T(\exp(\mathbf{w}\theta/2)) = \mathbf{x}\cos\theta + (\mathbf{x}\times\mathbf{w})\sin\theta\,,$$

corresponding to a rotation by an angle of θ about the axis determined by the vector $\mathbf{w}$. On the other hand, setting $\mathbf{x} = \mathbf{w}$ in (1.15) gives

$$\mathbf{w}T(\exp(\mathbf{w}\theta/2)) = \mathbf{w}\left(\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2}\right) + 2\mathbf{w}\sin^2\frac{\theta}{2} = \mathbf{w}\,,$$

so that $T(\exp(\mathbf{w}\theta/2))$ fixes $\mathbf{w}$. Again, this is the action of a rotation about $\mathbf{w}$. Since $\mathbb{R}^3$ is spanned by $\mathbf{w}$ and vectors orthogonal to $\mathbf{w}$, one obtains the following important result.

THEOREM 1.25. *For an angle θ and a purely imaginary unit quaternion $\mathbf{w}$, the operation* (1.16) *implements a rotation by θ about the axis $\mathbf{w}$.*

COROLLARY 1.26. *There is a surjective group homomorphism*

$$T\colon \mathsf{Spin}_3 \to \mathsf{SO}_3$$

from the spin group to the group SO_3 of rotations of $\mathbb{R}^3$.

2. Octonions

2.1. Zorn vector-matrices. Let S be a commutative, unital ring. A *Zorn vector-matrix* over S is a 2×2 matrix

$$z = \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \tag{2.1}$$

in which α and β are scalars from S, while $\mathbf{a}$ and $\mathbf{b}$ are 3-dimensional row vectors from S_1^3. The vector-matrix

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is the *Zorn identity matrix*.

DEFINITION 2.1. The *Zorn vector-matrix algebra* $\mathsf{Zorn}(S)$ over the ring S is the set of all Zorn vector-matrices over S, with componentwise S-module structure. A (non-associative) product of two Zorn vector-matrices is given as

$$\begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \cdot \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} = \begin{bmatrix} \alpha\gamma + \mathbf{a}\cdot\mathbf{d} & \alpha\mathbf{c} + \delta\mathbf{a} - \mathbf{b}\times\mathbf{d} \\ \gamma\mathbf{b} + \beta\mathbf{d} + \mathbf{a}\times\mathbf{c} & \mathbf{b}\cdot\mathbf{c} + \beta\delta \end{bmatrix} \tag{2.2}$$

using the usual vector or cross product

$$[a_1\ a_2\ a_3] \times [b_1\ b_2\ b_3] = \left[\ \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} \quad \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} \quad \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}\ \right]$$

of row vectors. The real Zorn vector-matrix algebra $\mathsf{Zorn}(\mathbb{R})$ is known as the algebra of *split octonions*.

2.1.1. *Scalar Zorn vector-matrices.* For an element λ of S, note that
$$\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}\cdot\begin{bmatrix}\alpha & \mathbf{a}\\ \mathbf{b} & \beta\end{bmatrix}=\begin{bmatrix}\lambda\alpha & \lambda\mathbf{a}\\ \lambda\mathbf{b} & \lambda\beta\end{bmatrix}=\begin{bmatrix}\alpha & \mathbf{a}\\ \mathbf{b} & \beta\end{bmatrix}\cdot\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}.$$
Thus there is a homomorphic embedding
$$\eta\colon S\to \mathsf{Zorn}(S); \lambda\mapsto \lambda I=\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix}$$
(compare §1.1.1). The image $\{\lambda I \mid \lambda\in S\}$ of η is the set of *scalar matrices*. It is convenient to identify the ring S with this image, e.g. writing $I=1$.

2.1.2. *Trace and norm.* The *trace* of the Zorn vector-matrix (2.1) is the ring element
$$\mathrm{Tr}(z)=\alpha+\beta.$$
The *Zorn conjugate* of the Zorn vector-matrix (2.1) is the Zorn vector-matrix
$$z'=\begin{bmatrix}\beta & -\mathbf{a}\\ -\mathbf{b} & \alpha\end{bmatrix}.$$
The *norm* or *Zorn determinant* of the Zorn vector-matrix (2.1) is the ring element
$$\mathrm{N}(z)=\begin{vmatrix}\alpha & \mathbf{a}\\ \mathbf{b} & \beta\end{vmatrix}=\alpha\beta-\mathbf{a}\cdot\mathbf{b}$$
defined using the usual scalar product
$$\mathbf{a}\cdot\mathbf{b}=[a_1\ a_2\ a_3]\cdot[b_1\ b_2\ b_3]=a_1b_1+a_2b_2+a_3b_3$$
of row vectors.

PROPOSITION 2.2. *Each Zorn vector matrix z satisfies the quadratic equation*
$$X^2-\mathrm{Tr}(z)X+\mathrm{N}(z)=0 \tag{2.3}$$
together with its Zorn conjugate.

PROOF. The satisfaction of (2.3) follows from
$$z+z'=\mathrm{Tr}(z)$$
and
$$z\cdot z'=\mathrm{N}(z).$$
(Note the identification of scalars with the corresponding Zorn scalar matrices.) □

2.1.3. *The Moufang identity.* The Zorn vector-matrix algebra over a ring S may be directly verified to satisfy the (*third*) *Moufang identity*

$$zx \cdot yz = (z \cdot xy)z \tag{2.4}$$

(Exercise 18). A loop satisfying (2.4) is said to be a *Moufang loop*. A loop is said to be *diassociative* if each subloop generated by two elements is associative. The major classical result about Moufang loops is Moufang's Theorem, stating that Moufang loops are diassociative.

The norm in the Zorn vector-matrix algebra $\mathsf{Zorn}(S)$ is described as *multiplicative*, in the sense that

$$\mathrm{N}(x)\mathrm{N}(y) = \mathrm{N}(xy) \tag{2.5}$$

for x, y in $\mathsf{Zorn}(S)$ (compare Exercise 21). For each element t of S, let $\mathrm{M}_t(S)$ be the set of Zorn vector-matrices over S whose norm is t.

PROPOSITION 2.3. *Under the multiplication* (2.2)*, the set* $\mathrm{M}_1(S)$ *of Zorn vector-matrices of norm* 1 *over a field S forms a Moufang loop* $(\mathrm{M}_1(S), \cdot, I)$*.*

PROOF. The multiplicativity (2.5) of the norm shows that $\mathrm{M}_1(S)$ is closed under multiplication. Consider the bilinear form

$$\langle z \,|\, t\rangle = \mathrm{N}(z+t) - \mathrm{N}(z) - \mathrm{N}(t)$$

given by the norm on the vector-matrix algebra, namely

$$\left\langle \begin{bmatrix} \alpha & \mathbf{a} \\ \mathbf{b} & \beta \end{bmatrix} \middle| \begin{bmatrix} \gamma & \mathbf{c} \\ \mathbf{d} & \delta \end{bmatrix} \right\rangle = \alpha\delta + \beta\gamma - \mathbf{a}\cdot\mathbf{d} - \mathbf{b}\cdot\mathbf{c}\,. \tag{2.6}$$

From (2.6) it is apparent that the bilinear form is nondegenerate. Now multiplication on the left or right by an element x of norm one preserves the nondegenerate form. For example,

$$\begin{aligned} \langle zx \,|\, tx\rangle &= \mathrm{N}\big((z+t)x\big) - \mathrm{N}(zx) - \mathrm{N}(tx) \\ &= \mathrm{N}(z+t)\mathrm{N}(x) - \mathrm{N}(z)\mathrm{N}(x) - \mathrm{N}(t)\mathrm{N}(x) \\ &= \mathrm{N}(z+t) - \mathrm{N}(z) - \mathrm{N}(t) = \langle z \,|\, t\rangle\,. \end{aligned}$$

The right and left multiplications by x are representable by orthogonal matrices. This implies that the multiplications are invertible, making $\mathrm{M}_1(S)$ a loop. □

For a prime power q, let $\mathrm{M}_1(q)$ denote the loop $\mathrm{M}_1(\mathsf{F}_q)$ over the finite field F_q of order q. The group $\{\pm 1\}$ of scalars acts by multiplication on $\mathrm{M}_1(q)$, so that the orbits are the classes of a loop congruence on $\mathrm{M}_1(q)$. Let $\mathrm{M}(q)$ denote the corresponding quotient. Paige showed that the Moufang loops $\mathrm{M}(q)$ are simple [**7**]. Subsequently, using work of Doro [**5**] and the classification of finite simple groups, Liebeck showed that up to isomorphism, the $\mathrm{M}(q)$ are the only nonassociative finite simple Moufang loops [**6**].

2.1.4. *Split octonions and special relativity.* Just as the quaternions $\mathbb{H}$ contain a copy of Euclidean space (§1.3.1), the split octonions $\mathsf{Zorn}(\mathbb{R})$ contain a copy of Minkowski space-time. Indeed, a 4-vector $(t, \mathbf{r})$ may be identified with the element

$$\begin{bmatrix} t & -\mathbf{r} \\ \mathbf{r} & -t \end{bmatrix}$$

of $\mathsf{Zorn}(\mathbb{R})$ whose norm is the square $-t^2+\mathbf{r}\cdot\mathbf{r}$ of the Minkowski norm of $(t, \mathbf{r})$, in units chosen so the speed of light $c = 1$. Maxwell's equations reduce to a single equation in the split octonions (Exercise 22).

2.2. Octonions. Consider the 3-dimensional unit vectors

$$\mathbf{u}_1 = [1\ 0\ 0], \quad \mathbf{u}_2 = [0\ 1\ 0], \quad \mathbf{u}_3 = [0\ 0\ 1]$$

over a commutative, unital ring S. In the complex Zorn vector-matrix algebra $\mathsf{Zorn}(\mathbb{C})$, consider the elements $e_0 = 1$,

$$e_4 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, e_j = \begin{bmatrix} 0 & -\mathbf{u}_j \\ \mathbf{u}_j & 0 \end{bmatrix}, \text{ and } e_{4+j} = \begin{bmatrix} 0 & i\mathbf{u}_j \\ i\mathbf{u}_j & 0 \end{bmatrix}$$

for $1 \le j \le 3$. Note that $e_j^2 = -1$ for $1 \le j \le 7$. Then the algebra $\mathbb{R}$ of real numbers forms the real span of the subset $\{e_0\}$ of $\mathsf{Zorn}(\mathbb{C})$. The algebra $\mathbb{C}$ of complex numbers forms the real span of the subset $\{e_0, e_1\}$ of $\mathsf{Zorn}(\mathbb{C})$. The algebra $\mathbb{H}$ of quaternions forms the real span of the subset $\{e_0, e_1, e_2, e_3\}$ of $\mathsf{Zorn}(\mathbb{C})$: indeed $e_1e_2 = e_3 = -e_2e_1$, etc. — compare (1.11). Now

$$e_je_k \in \{\pm e_{j*k}\}$$

for $0 \le j, k \le 7$, the product $*$ being given by componentwise addition of the bit strings of length 3 that give the binary representations of the elements of $\underline{8}$. For example, $e_4e_5 \in \{\pm e_1\}$, since $100 * 101 = 001$. Then the real span of the subset

$$\{e_0, \dots, e_7\}$$

of $\mathsf{Zorn}(\mathbb{C})$ forms an 8-dimensional real algebra $\mathbb{K}$, the *Cayley numbers* or *octonions*. The norms of octonions are real. The argument of the proof of Proposition 2.3 shows that the set S^7 of nonzero octonions of norm 1 forms a Moufang loop under multiplication. (Geometrically, this set is a 7-sphere.) It follows that the set $\mathbb{K}^*$ of nonzero octonions also forms a Moufang loop.

The properties of the algebras considered may be summarized as follows:

Dimension d	Algebra	Property	Unit sphere S^{d-1}
1	$\mathbb{R}$	ordered	cyclic group
2	$\mathbb{C}$	commutative	abelian group
4	$\mathbb{H}$	associative	group
8	$\mathbb{K}$	Moufang	Moufang loop

3. Exercises

(1) Let S be a unital ring, and let n be a positive integer. Show that
$$\{A \in S_n^n \mid \forall\ B \in S_n^n\,,\ AB = BA\}$$
is the set of scalar matrices.

(2) Verify Lemma 1.1. [Hint: This may be done computationally, or conceptually using a ring homomorphism to S_2^2 from the commutative polynomial ring $S[X]$ over an indeterminate X.]

(3) Exhibit two nonzero elements u, v of $\mathbb{Z}/_5[i]$ such that $uv = 0$.

(4) Let k be a positive integer. Show that $\mathbb{Z}/_{2k+1}[i]$ is a field if and only if k is odd.

(5) Consider the circle group S^1.
   (a) For each positive integer n, exhibit an element x of S^1 with order n.
   (a) Exhibit an element x of S^1 with infinite order.

(6) The dual of the concept of "projective" is *injective*.
   (a) Formulate the defining property for an abelian group to be injective.
   (b) Show that $(\mathbb{Q}, +, 0)$ is injective.
   (c) Show that the subgroup $\mathbb{Q}/\mathbb{Z}$ of S^1 is injective.

(7) Let n be a positive integer whose square root $\sqrt{n}$ is irrational. Consider the matrix $\sqrt{-n} = \begin{bmatrix} 0 & -n \\ 1 & 0 \end{bmatrix}$.

(a) Show that
$$\begin{bmatrix} 0 & -n \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -n \\ 1 & 0 \end{bmatrix} = -n\,.$$

(b) Show that the set
$$\mathbb{Q}\big[\sqrt{-n}\,\big] = \left\{ \begin{bmatrix} x & -ny \\ y & x \end{bmatrix} \;\middle|\; x, y \in \mathbb{Q} \right\}$$
is an algebraic number field with $\mathbb{Q}$-basis $\{1, \sqrt{-n}\,\}$.

(8) Let n be a positive integer whose square root $\sqrt{n}$ is irrational. Let m be a positive integer. Show that the fields $\mathbb{Q}\big[\sqrt{n}\,\big]$ and $\mathbb{Q}\big[\sqrt{m^2 n}\,\big]$ are isomorphic.

(9) Verify the relations (1.10) and (1.11).

(10) Using the notation of §1.3, let Q_8 be the *quaternion group* group generated by the invertible matrices j and k in $\mathbb{Z}_4^4$.

(a) Show that Q_8 is not commutative.

(b) Show that each subgroup of Q_8 is normal.

(c) Show that Q_8 is not isomorphic to the dihedral group D_4 of degree 4.

(11) Use the Four Squares Identity to show that if each prime integer is a sum of four integral squares, then each positive integer is a sum of four integral squares.

(12) Let p be a prime number. Show that the equation
$$t^2 + x^2 + y^2 + z^2 = 0$$
always has a non-trivial solution in the field $\mathbb{Z}/_p$. [Hint: Every finite skewfield is commutative.] Can you conclude that every prime number is a sum of four integral squares?

(13) For which purely imaginary unit quaternions $\mathbf{w}$, $\mathbf{w}'$ do the subsets $\mathbb{C}_{\mathbf{w}}$ and $\mathbb{C}_{\mathbf{w}'}$ of $\mathbb{H}$ coincide?

(14) (a) Show that (1.13) is a unit quaternion.

(b) Prove (1.14).

(15) Design a rotation taking the vector $\frac{3}{5}i + \frac{4}{5}j$ to $\frac{5}{13}j + \frac{12}{13}k$.

(16) Let θ be an angle, and let $\mathbf{w}$ be a purely imaginary unit vector in $\mathbb{H}$.

(a) Show that $T(\exp(\mathbf{w}\theta/2))$ maps $S^3 \cap \mathbb{R}^3$ to itself.

(b) If $T(\exp(\mathbf{w}\theta/2))\colon \mathbf{x} \mapsto \mathbf{y}$ for purely imaginary unit vectors $\mathbf{x}$ and $\mathbf{y}$, show that

$$(u + v\mathbf{x}) \mapsto \exp(-\mathbf{w}\theta/2)(u + v\mathbf{x})\exp(\mathbf{w}\theta/2)$$

gives an isomorphism of $\mathbb{C}_{\mathbf{x}}$ with $\mathbb{C}_{\mathbf{y}}$.

(17) Prove Corollary 1.26.

(18) Give a computational verification of the Moufang identity (2.4).

(19) Show that the order of the simple Moufang loop $M(q)$ is given by $q^3(q^4-1)/\gcd\{q+1,2\}$ for each prime power q.

(20) Show that a loop Q satisfies the Moufang identity if and only if $\big(L(z), R(z), L(z)R(z)\big)\colon Q \to Q$ is an isotopy for each element z of Q.

(21) Give a computational verification of (2.5).

(22) Pick units so that the dielectric constant and permeability take the value 1. Defining the differential operator vector-matrix

$$D = \begin{bmatrix} -\frac{\partial}{\partial t} & \nabla \\ \nabla & -\frac{\partial}{\partial t} \end{bmatrix},$$

the field matrix

$$F = \begin{bmatrix} 0 & -\mathbf{E} + \mathbf{B} \\ \mathbf{E} + \mathbf{B} & 0 \end{bmatrix},$$

and the 4-current

$$J = \begin{bmatrix} \rho & -\mathbf{j} \\ \mathbf{j} & -\rho \end{bmatrix},$$

show that Maxwell's equations may be written as the single equation $DF = J$ in the split octonions.

CHAPTER 9

Functors and adjunctions

1. Functors

1.1. Graph maps.

1.1.1. *Quivers.* Quivers generalize directed graphs, and may be viewed as categories without a composition structure.

Definition 1.1. A *quiver* $C = (C_0, C_1, \partial_0, \partial_1)$ (or "graph") consists of two classes C_0, C_1 and two maps $\partial_0 \colon C_1 \to C_0$, $\partial_1 \colon C_1 \to C_0$.

(a) Elements of C_0 are called *vertices*, *points*, or *objects*.
(b) Elements of C_1 are called *edges*, *arrows*, or *morphisms*.
(c) The map ∂_0 is variously called the *tail* or *domain map*.
(d) The map ∂_1 is variously called the *head* or *codomain map*.

An edge f is often depicted in the form $f \colon x \to y$ or $x \xrightarrow{f} y$ to indicate that $f^{\partial_0} = x$ and $f^{\partial_1} = y$. For a given pair (x, y) of vertices, set

$$C(x, y) = \{f \in C_1 \mid f^{\partial_0} = x\,, f^{\partial_1} = y\}. \tag{1.1}$$

The quiver C is said to be *small* if the classes C_0 and C_1 are sets. The quiver is *locally small* if the class (1.1) is a set for each pair (x, y) of vertices. Usually, quivers are implicitly assumed to be locally small.

Example 1.2. Let (V, E) be a directed graph. Then the maps

$$\partial_i \colon E \to V ; (v_0, v_1) \mapsto v_i$$

for $i = 0, 1$ yield a quiver $(V, E, \partial_0, \partial_1)$.

1.1.2. *Graph maps.*

Definition 1.3. A *graph map* $F : D \to C$ from a quiver D to a quiver C consists of two functions, a *vertex map* or *object part* $F_0 \colon D_0 \to C_0$ and an *edge map* or *morphism part* $F_1 \colon D_1 \to C_1$, such that for each pair x, y of vertices of D, the map F_1 restricts to

$$F_1 : D(x, y) \to C(xF_0, yF_0). \tag{1.2}$$

The respective suffices 0 and 1 on the object and morphism parts are usually suppressed.

Example 1.4. Suppose that (V_i, E_i) are directed graphs for $i = 1, 2$, having corresponding relational structures $(V_i, \{\eta\})$ of signature $\sigma\colon \{\eta\} \to \{2\}$. Then a graph homomorphism f, a homomorphism

$$f\colon (V_1, \{\eta\}) \to (V_2, \{\eta\})$$

of relational structures, yields a graph map F with

$$F_0\colon V_1 \to V_2; v \mapsto vf$$

and

$$F_1\colon E_1 \to E_2; (v, v') \mapsto (vf, v'f)\,.$$

Note that the domains of the restrictions (1.2) are either singletons or empty in this case.

Example 1.5. Let D be a quiver.

(a) The *identity map* $1_D : D \to D$ on D comprises the respective identity maps 1_{D_0} and 1_{D_1} on the vertex and edge classes.
(b) If C is a category, and c is an object of C, then the *constant map* $[c] : D \to C$ takes each vertex of the quiver D to c and each arrow of the quiver D to 1_c.

1.2. Natural transformations.

1.2.1. *Commuting diagrams.*

Definition 1.6. Let D be a quiver.

(a) A pair (f, g) of edges in D is described as *composable* when $f^{\partial_1} = g^{\partial_0}$, i.e., if the head of f is the tail of g:

$$f^{\partial_0} \xrightarrow{f} f^{\partial_1} = g^{\partial_0} \xrightarrow{g} g^{\partial_1}\,.$$

(b) A (*non-trivial*) *path* in D is a non-empty sequence $e_1, \dots, e_l$ of edges such that each pair (e_1, e_2), $\dots$, (e_{l-1}, e_l) is composable.

Definition 1.7. Let C be a category.

(a) A *diagram* in C is a graph map $F\colon D \to C$ with codomain C.
(d) The diagram is said to *commute* if for each pair

$$(e_1, \dots, e_l)\,, \quad (f_1, \dots, f_m)$$

of paths in D with common starting point $e_1^{\partial_0} = f_1^{\partial_0}$ and end point $e_l^{\partial_1} = f_m^{\partial_1}$, the composite morphisms

$$e_1^F \dots e_l^F \quad \text{and} \quad f_1^F \dots f_m^F$$

in C agree.

1.2.2. *Natural transformations.* Given two diagrams $F : D \to C$ and $G : D \to C$ with common domain quiver D and codomain category C, a *natural transformation* $\tau : F \to G$ is a vector having a component $\tau_x : xF \to xG$ in $C(xF, xG)$ for each vertex x of D, such that the *naturality property* $f^F \tau_y = \tau_x f^G$ is satisfied for each edge $f : x \to y$ of D. The naturality corresponds to the commuting of the diagram in C on the right-hand side of the picture

(1.3)

$$\boxed{\text{In } D} \qquad \begin{array}{c} x \\ {\scriptstyle f}\big\downarrow \\ y \end{array} \qquad \Bigg| \qquad \begin{array}{ccc} xF & \xrightarrow{\tau_x} & xG \\ {\scriptstyle f^F}\big\downarrow & & \big\downarrow{\scriptstyle f^G} \\ yF & \xrightarrow{\tau_y} & yG \end{array} \qquad \boxed{\text{In } C}$$

for every arrow $f : x \to y$ in D displayed on the left-hand side of the picture.

EXAMPLE 1.8. Let D be a quiver. If $h : a \to b$ is a morphism of a category C, then the *constant* natural transformation $[h] : [a] \to [b]$ has the morphism $h : a \to b$ as its component at each vertex x of D.

1.3. Functors.

DEFINITION 1.9. Let D and C be categories.

(a) A (*covariant*) *functor* $F : D \to C$ is a graph map satisfying the *functoriality properties* $1_x F = 1_{xF}$ for all objects x of D and

$$(fg)^F = f^F g^F \tag{1.4}$$

for all composable pairs (f, g) of D.

(b) A *contravariant functor* $F : D \to C$ is a covariant functor from D to C^{op}.

EXAMPLE 1.10. Let (X, V) and (X', V') be poset categories.

(a) The object part of a functor $F : (X, V) \to (X', V')$ is an *order-preserving* map, i.e. $(x, y) \in V$ implies $(xF, yF) \in V'$.

(b) The object part of a contravariant functor $F\colon (X,V) \to (X',V')$ is an *order-reversing* map, i.e. $(x,y) \in V$ implies $(yF, xF) \in V'$.

EXAMPLE 1.11 (Forgetful functors). Let $\mathbf{C}$ be a category of algebras and homomorphisms. Then the *forgetful functor* $G\colon \mathbf{C} \to \mathbf{Set}$ assigns the underlying set to each algebra, and the underlying function to each homomorphism.

Let C be a category. Then the *identity functor* 1_C on C has object part 1_{C_0} and morphism part 1_{C_1}. If $F\colon D \to C$ and $F'\colon C \to B$ are functors, then so is the composite $FF'\colon D \to B$.

2. Adjunctions

If $F\colon D \to C$ and $G\colon C \to D$ are mutually inverse functions, then $1_D = FG$ and $GF = 1_C$. The concept of an adjunction provides an analogous relationship for functors.

2.1. Left and right adjoints. Let C and D be categories. Then an *adjunction* $(F, G, \eta, \varepsilon)$ consists of the following data:

- a *left adjoint* functor $F : D \to C$,
- a *right adjoint* functor $G : C \to D$,
- a *unit* natural transformation $\eta : 1_D \to FG$, and
- a *counit* natural transformation $\varepsilon : GF \to 1_C$,

such that

$$\eta_x^F \varepsilon_{xF} = 1_{xF} \quad \text{and} \quad \eta_{yG}\varepsilon_y^G = 1_{yG} \tag{2.1}$$

for all objects x of D and for all objects y of C.

Such an adjunction is often summarized by the isomorphism

$$F \text{ on left} \longrightarrow \boxed{C(xF, y) \cong D(x, yG)} \longleftarrow G \text{ on right} \tag{2.2}$$

for objects x of D and y of C, under which a morphism $g\colon xF \to y$ maps to $\eta_x g^G$, while a morphism $f\colon x \to yG$ maps to $f^F\varepsilon_y$. In particular, η_x corresponds to 1_{xF} and ε_y corresponds to 1_{yG}.

2.1.1. *Free algebras.*

EXAMPLE 2.1. For a characteristic example of an adjunction, take C to be the category $\mathbf{Mon}$ of monoids and monoid homomorphisms, with D as the category $\mathbf{Set}$ of sets. The right adjoint is the underlying set functor $G : \mathbf{Mon} \to \mathbf{Set}$, while the left adjoint $F\colon \mathbf{Set} \to \mathbf{Mon}$

takes a set X, considered as an alphabet, to the free monoid X^* of words in the alphabet X (with the empty word as the identity element). Words are multiplied by concatenation. The general adjunction (2.2) takes the form

$$\mathbf{Mon}(XF, M) \cong \mathbf{Set}(X, MG) \tag{2.3}$$

for a monoid M. The component $\eta_X \colon X \to X^*$ at a set X embeds letters (elements) from X into X^* as one-letter words. For a monoid M, the counit $\varepsilon_M : M^* \to M$ takes a word in the alphabet M to the product of its letters computed in the monoid M. Under the isomorphism (2.3), a monoid homomorphism $g \colon XF \to M$ or $g \colon X^* \to M$ is mapped to its restriction to the set X of one-letter words. Conversely, a function $f \colon X \to M$ from a set X to (the underlying set of) a monoid M is mapped to its canonical extension to a monoid homomorphism from X^* to M.

Example 2.2. The constructions of Example 2.1 carry over when the category **Mon** of monoids is replaced by a more general category C of algebras and homomorphisms. Suppose that for each set X, a free algebra XF has been constructed. Then for each algebra A from C, and for each function $f \colon X \to A$, there is a unique homomorphism $\overline{f} \colon XF \to A$ such that $\eta_X \overline{f} = f$. Up to now, this situation has been illustrated by diagrams of the following form:

$$\begin{tikzcd} XF \arrow[dr, dashed, "\overline{f}"] & \\ X \arrow[u, "\eta_X"] \arrow[r, "f"'] & A \end{tikzcd} \tag{2.4}$$

Now while the arrow $\overline{f}$ is a morphism in $\mathbf{C}$, the arrows η_X and f are morphisms in **Set**, although their respective codomains are indicated in (2.4) by objects from the category $\mathbf{C}$. For added precision, diagrams like (2.4) are replaced by the adjunction isomorphism

$$\mathbf{C}(XF, A) \cong \mathbf{Set}(X, AG) \tag{2.5}$$

featuring the forgetful functor $G \colon \mathbf{C} \to \mathbf{Set}$ of Example 1.11. The function η_X is written as the morphism $\eta_X \colon X \to XFG$ in **Set**, the component at X of the natural transformation η. The extension from f to $\overline{f}$ in diagram (2.4) becomes an extension from $f \colon X \to AG$ to

$\overline{f}\colon XF \to A$, the application

$$\overline{f} \longleftarrow\!\!\!\dashv f$$

or $f \mapsto f^F \varepsilon_A$ of the isomorphism (2.5). The image $f^F\colon XF \to YF$ of a function $f\colon X \to Y$ under the *free algebra functor* F is given from (2.4) as the unique homomorphic extension $\overline{f\eta_Y}$ of the function $f\eta_Y\colon X \to YFG$:

$$\begin{tikzcd} XF \arrow[drr, dashed, "f^F"] & & \\ X \arrow[u, "\eta_X"] \arrow[r, "f"'] & Y \arrow[r, "\eta_Y"'] & YF \end{tikzcd}$$

The counit component $\varepsilon_A\colon AGF \to A$ at an algebra A is given by:

$$\begin{tikzcd} AGF \arrow[dr, dashed, "\varepsilon_A"] & \\ AG \arrow[u, "\eta_{AG}"] \arrow[r, "1_{AG}"'] & A \end{tikzcd} \tag{2.6}$$

— compare the left hand side of (2.1), and see Exercise 9.

2.2. Currying and tensor products.

2.2.1. *Currying revisited.*

PROPOSITION 2.3. *Let Y be a set. Consider the functors*

$$F_Y\colon \mathbf{Set} \to \mathbf{Set}; Z \mapsto Z \times Y$$

(object part) and

$$G_Y\colon \mathbf{Set} \to \mathbf{Set}; (f\colon X \to X') \mapsto (X^Y \to X'^Y; g \mapsto gf)$$

(morphism part). Then the currying isomorphism

$$\mathbf{Set}(Z \times Y, X) \cong \mathbf{Set}(Z, \mathbf{Set}(Y, X)) \tag{2.7}$$

becomes the adjoint relationship

$$\mathbf{Set}(ZF_Y, X) \cong \mathbf{Set}(Z, XG_Y)$$

between F_X and G_Y.

2.2.2. *Bilinear functions and tensor products.* Let S be a commutative, unital ring, with the corresponding category $\underline{\underline{S}}$ of S-modules.

Definition 2.4. Consider S-modules X, Y, Z.

(a) A function $f \in \mathbf{Set}(Z \times Y, X)$ is *bilinear* if its curried version in $\mathbf{Set}(Z, \mathbf{Set}(Y, X))$ actually lies in $\underline{\underline{S}}(Z, \underline{\underline{S}}(Y, X))$. In other words, the curried functions

$$f_y \colon Z \to X; z \mapsto (y, z)f$$

for $y \in Y$ and

$$f_z \colon Y \to X; y \mapsto (y, z)f$$

for $z \in Z$ are both linear (i.e., S-module homomorphisms).

(b) The set of bilinear functions from $Z \times Y$ to X is written as $\underline{\underline{S}}(Z, Y; X)$.

For the general proof of the following proposition, see [**10**, III, §3.6]. For the case where X, Y, Z are vector spaces over a field S, compare Chapter 2, Exercise 14.

Proposition 2.5. *Let Y be an S-module. Then the functor*

$$G_Y \colon \underline{\underline{S}} \to \underline{\underline{S}}; (f \colon X \to X') \mapsto (\underline{\underline{S}}(Y, X) \to \underline{\underline{S}}(Y, X'); g \mapsto gf)$$

(morphism part) has a left adjoint $F_Y \colon \underline{\underline{S}} \to \underline{\underline{S}}; Z \mapsto Z \otimes Y$.

Definition 2.6. The module $Z \otimes Y$ is called the (S-*module*) *tensor product* of Z and Y.

Corollary 2.7. *Let X, Y, Z be S-modules. Then each bilinear function $f \colon Z \times Y \to X$ determines a unique linear function $f \colon Z \otimes Y \to X$.*

2.3. Galois connections. A *Galois connection* is an adjunction

$$(F \colon D \to C, G \colon C \to D, \eta, \varepsilon) \tag{2.8}$$

where the categories C and D are poset categories $(C. \leq)$, $(D, \leq)$. The isomorphism relationship (2.2) reduces to

$$\forall\, x \in D\,,\ \forall\, y \in C\,, \quad x^F \leq y \ \Leftrightarrow\ x \leq y^G\,.$$

The existence of the unit and counit reduces to

$$\begin{cases} \text{(a)} \quad \forall\, x \in D\,,\ x \leq x^{FG}; \\ \text{(b)} \quad \forall\, y \in C\,,\ y^{GF} \leq y. \end{cases}$$

The identities (2.1) reduce to

$$\begin{cases} \text{(a)} \quad \forall\, x \in D\,,\ x^F = x^{FGF}; \\ \text{(b)} \quad \forall\, y \in C\,,\ y^{GFG} = y^G. \end{cases} \tag{2.9}$$

EXAMPLE 2.8. Let $f\colon A \to B$ be a function. Define

$$F\colon (2^A, \subseteq) \to (2^B, \subseteq); X \mapsto Xf$$

and

$$G\colon (2^B, \subseteq) \to (2^A, \subseteq); Y \mapsto f^{-1}Y$$

with the *inverse image* $f^{-1}Y = \{x \in A \mid xf \in Y\}$. Since

$$Xf \subseteq Y \ \Leftrightarrow\ X \subseteq f^{-1}Y\,,$$

the functors F and G yield a Galois connection.

2.3.1. *Galois correspondence.* In a Galois connection (2.8), elements of the subsets DF of C and CG of D are described as *closed*. One obtains induced posets $(DF, \leq)$ and $(CG, \leq)$. By (2.9), the restricted functors $F\colon CG \to DF$ and $G\colon DF \to CG$ yield mutually inverse isomorphisms. The isomorphism

$$(DF, \leq) \cong (CG, \leq)$$

is known as a *Galois correspondence*.

2.3.2. *Polarities.*

DEFINITION 2.9. Let I and J be sets. A subset α of $I \times J$ is known as a *relation between* the sets I and J. One often writes $x\ \alpha\ y$ for $(x, y) \in \alpha$.

EXAMPLE 2.10. Let n be a positive integer. The *orthogonality relation*

$$\mathbf{x} \perp \mathbf{u} \ \Leftrightarrow\ \mathbf{xu} = 0$$

is a relation between the space $\mathbb{R}^n_1$ of n-dimensional row vectors $\mathbf{x}$ and the space $\mathbb{R}^1_n$ of n-dimensional column vectors $\mathbf{u}$.

Suppose that α is a relation between I and J. Consider the poset categories $(2^I, \subseteq)$ and $(2^J, \supseteq)$. Define

$$F\colon (2^I, \subseteq) \to (2^J, \supseteq); X \mapsto \{y \in J \mid \forall\ x \in X,\ x\ \alpha\ y\}$$

and

$$G\colon (2^J, \supseteq) \to (2^I, \subseteq); Y \mapsto \{x \in I \mid \forall\ y \in Y,\ x\ \alpha\ y\}$$

Since

$$X^F \supseteq Y \;\Leftrightarrow\; [\,\forall\, x \in X\,,\ \forall\, y \in Y\,,\ x\ \alpha\ y\,] \;\Leftrightarrow\; X \subseteq Y^G\,,$$

the functors F and G form a Galois connection, known as the *polarity* determined by the relation α.

Definition 2.11. Let G be a group, and let X be a G-set. Consider the subset

$$\{(x, g) \in X \times G \mid xg = x\} \tag{2.10}$$

of $X \times G$ used in the proof of Burnside's Lemma (Theorem 1.28 in Chapter 6) as a relation between X and G.

(a) The right adjoint

$$(2^G, \supseteq) \to (2^X, \subseteq); H \mapsto \bigcap_{h \in H} X_h$$

in the polarity determined by (2.10) is known as the *fixed-point functor*.

(a) The left adjoint

$$(2^X, \subseteq) \to (2^G, \supseteq); Y \mapsto \bigcap_{y \in Y} G_y$$

in the polarity determined by (2.10) is known as the *stabilizer functor*.

There is an interesting correspondence between G-subsets of X and normal subgroups of G in the context of Definition 2.11.

Proposition 2.12. *Let G be a group, and let X be a G-set.*

(a) *Suppose that Y is a G-subset of X. Then $\bigcap_{y \in Y} G_y$ is a normal subgroup of G.*

(b) *Suppose that N is a normal subgroup of G. Then $\bigcap_{n \in N} X_n$ is a G-subset of X.*

Proof. (a) For $g \in G$, $n \in \bigcap_{y \in Y} G_y$, and $y \in Y$, one has

$$yg^{-1}ng = yg^{-1} = y\,,$$

so $g^{-1}ng \in \bigcap_{y \in Y} G_y$.

(b) For $g \in G$, $y \in \bigcap_{n \in N} X_n$, and $n \in N$, one has

$$ygn = ygng^{-1}g = yg\,,$$

so $yg \in \bigcap_{n \in N} X_n$. $\square$

2.3.3. *Galois theory.* The classical application of the polarity that was introduced in Definition 2.11 is to the action of a so-called "Galois group" on a field.

DEFINITION 2.13. Let A be a field that contains a field K as a unital subring.

(a) Let $\mathrm{Aut}_K A$ denote the group of all ring automorphisms of A that leave each element of K fixed. Then $\mathrm{Aut}_K A$ is known as the *Galois group* of A over K.
(b) A field C that contains K, and is a subring of A, is known as an *intermediate field*.

The following result is the *Fundamental Theorem of Galois Theory*. For a proof, see [**10**, III, §3.3].

THEOREM 2.14. *Let K be a field. Let A be a field containing K, such that the dimension $\dim_K A$ of A as a vector space over K is finite. Let G be the Galois group of A over K. Consider the polarity introduced in Definition 2.11 for the G-set A. Suppose that K is a closed subset of A.*

(a) *The group G is finite, with $|G| = \dim_K A$.*
(b) *Each subgroup of G is a closed subset of G.*
(c) *Each intermediate field C is a closed subset of A.*
(d) *The Galois correspondence yields a bijection between the set of subgroups of G and the set of intermediate fields.*
(e) *If C is an intermediate field, then the dimension of C over K is $|G|/|\bigcap_{y\in C} G_y|$.*
(f) *If H is a subgroup of G, then the order of H is the dimension of A over $\bigcap_{h\in H} A_h$.*

EXAMPLE 2.15. Let n be a positive integer. Let $\mathbb{Q}[\zeta_n]$ be the smallest subfield of $\mathbb{C}$ that contains the n-th root of unity $\exp(2\pi i/n)$. Then the Galois group of $\mathbb{Q}[\zeta_n]$ over $\mathbb{Q}$ is the cyclic group $(\mathbb{Z}/_n, +, 0)$. The intermediate fields have the form $\mathbb{Q}[\zeta_r]$ for each divisor r of n.

3. Exercises

(1) Suppose that C is a poset category. Show that each diagram $F\colon D \to C$ commutes.
(2) Suppose that D is a quiver. Define $D\Pi_1$ to be the disjoint union of the class D_0 and the class $D\Pi_1^+$ of paths in D. Define

$d_0 \colon D\Pi_1 \to D$ as the disjoint union of the identity $D_0 \to D_0$ and the map

$$D\Pi_1^+ \to D_0; (e_1, \ldots, e_l) \mapsto e_1^{\partial_0}.$$

Define $d_1 \colon D\Pi_1 \to D$ as the disjoint union of the identity $D_0 \to D_0$ and the map

$$D\Pi_1^+ \to D_0; (e_1, \ldots, e_l) \mapsto e_l^{\partial_1}.$$

Define a composition of non-trivial paths by

$$\big((e_1, \ldots, e_l), (f_1, \ldots, f_m)\big) \mapsto (e_1, \ldots, f_m)$$

when $e_m^{\partial_1} = f_1^{\partial_0}$ in D. Show that there is a unique way to extend these partial data to yield a category $D\Pi = (D, D\Pi_1)$. This category is known as the *path category* of the quiver D.

(3) A quiver D is said to be *discrete* if D_1 is empty. Determine the path category $D\Pi$ of a discrete quiver D.

(4) Let (X, V) be a poset. An element (x, y) of V is a *covering pair* if $|\{z \in X \mid x \leq z \leq y\}| = 2$. Let $C(X, V)$ be the set of covering pairs of (X, V), equipped with the projections

$$\pi_i \colon C(X, V) \to X; (x_0, x_1) \mapsto x_i\,.$$

The quiver $\big(X, C(X, V), \pi_0, \pi_1\big)$ is called the *Hasse diagram* of (X, V). Show that (X, V) is the path category of its Hasse diagram.

(5) For the natural transformation $[h]$ of Example 1.8, draw the naturality diagram (1.3).

(6) Let M and N be monoids, with corresponding single-object categories $\underline{\underline{M}}$ and $\underline{\underline{N}}$.
  (a) Show that a monoid homomorphism $f \colon M \to N$ yields a functor $F \colon \underline{\underline{M}} \to \underline{\underline{N}}$ with $mF = mf$ for each morphism m of $\underline{\underline{M}}$.
  (b) Show that a functor $F \colon \underline{\underline{M}} \to \underline{\underline{N}}$ yields a monoid homomorphism $f \colon M \to N$ with $mf = mF$ for each element m of M.

(7) Give an example of lattices L, L' and an order-preserving map $F \colon (L, \leq) \to (L', \leq)$ such that $F \colon (L, \vee, \wedge) \to (L', \vee, \wedge)$ is not a lattice homomorphism.

(8) Consider the context of Example 2.1.
  (a) For each monoid M, verify that $\eta_M \varepsilon_M^G = 1_M$.

(b) For each set X, verify that $\eta^F_X \varepsilon_{X^*} = 1_{X^*}$.

(9) In Example 2.2, draw the precise, categorical diagram that implements the left hand side of (2.1) for $y = A$, and note how it differs from the more informal diagram (2.6).

(10) In the context of Example 2.2, take $\mathbf{C}$ to be the category $\mathbf{Lin}$ of real vector spaces and linear transformations. What is the component ε_V of the counit ε at a vector space V?

(11) Consider the categories $\mathbf{Mon}$ of monoids and $\mathbf{Gp}$ of groups. Let $U \colon \mathbf{Gp} \to \mathbf{Mon}$ be the functor that forgets the inversion in a group. Recalling the notation M^* for the group of units in a monoid M, verify the adjunction relationship

$$\mathbf{Mon}(GU, M) \cong \mathbf{Gp}(G, M^*)$$

for a group G and monoid M.

(12) An adjunction $(F \colon C \to D, G \colon D \to C, \eta, \varepsilon)$ is said to provide an *equivalence* between the categories C and D if the components η_x and ε_y of the unit and counit are always isomorphisms. Let $\underline{\mathbb{N}}$ be the category with object set $\{\underline{n} \mid n \in \mathbb{N}\}$, taking all functions between the various sets $\underline{n}$ as morphisms. Let $\mathbf{FinSet}$ denote the category of finite sets and functions between them. Show that there is an equivalence between $\underline{\mathbb{N}}$ and $\mathbf{FinSet}$.

(13) Let M be a submonoid of a monoid N, with corresponding categories $\underline{\underline{M}}$ and $\underline{\underline{N}}$ of actions. Show that there is an adjunction between induction $\uparrow^N_M \colon \underline{\underline{M}} \to \underline{\underline{N}}$ and restriction $\downarrow^N_M \colon \underline{\underline{N}} \to \underline{\underline{M}}$ — compare Chapter 3, Proposition 2.20.

(14) Consider the context of Proposition 2.3.
(a) Identify the morphism part of F_Y.
(b) Determine the unit and counit for the adjunction between F_Y and G_Y.

(15) Prove Corollary 2.7. [Hint: Apply the composition

$$\underline{\underline{S}}(Z, Y; X) \cong \underline{\underline{S}}(Z, \underline{\underline{S}}(Y, X)) \cong \underline{\underline{S}}(Z \otimes Y, X)$$

of the Currying isomorphism with the adjointness relation from Proposition 2.5.]

(16) Let $(H, \vee, \wedge, \backslash, 0, 1)$ be a Heyting algebra, also considered as a poset category $(H, \leq)$. Then for each element y of H, show

that the functors

$$S(y)\colon H \to H; x \mapsto x \wedge y$$

and

$$R(y)\colon H \to H; z \mapsto y \backslash z$$

form a Galois connection.

(17) Consider the polarity determined by the orthogonality relation of Example 2.10. Show that the closed subsets are subspaces.

(18) Let G be a group. Consider the polarity determined by the *commutation* relation $\{(x, y) \in G^2 \mid xy = yx\}$ on G.
  (a) Show that the closed elements are subgroups of G.
  (b) For the case $G = S_4$, determine which subgroups are closed.

(19) Show that $\mathbb{Q}$ is not a closed subfield of $\mathbb{R}$.

(20) Determine the Galois group of $\mathbb{Z}/_5[\sqrt{2}]$ over $\mathbb{Z}/_5$.

CHAPTER 10

Structural specifications

1. Initial objects

1.1. Initial and terminal objects.

Definition 1.1. Let $\mathbf{C}$ be a category.

(a) An object $\perp$ of $\mathbf{C}$ is *initial* if $|\mathbf{C}(\perp, X)| = 1$ for all $X \in \mathbf{C}_0$.
(b) An object $\top$ of $\mathbf{C}$ is *terminal* if $|\mathbf{C}(X, \top)| = 1$ for all $X \in \mathbf{C}_0$.
(a) An object 0 of $\mathbf{C}$ is a *zero object* if it is both initial and terminal.

Example 1.2. (a) The empty set is initial in **Set**, while any singleton set is terminal.

(b) In the category of right modules over a ring S, the trivial S-module is a zero object.

(c) In a poset category, an initial object is a lower bound, and a terminal object is an upper bound. (Compare Chapter 2, Definition 2.18.)

The concepts of initial and terminal objects are dual:

Proposition 1.3. *If $\perp$ is an initial object of a category $\mathbf{C}$, then it is a terminal object in $\mathbf{C}^{\mathsf{op}}$.*

Initial objects are specified uniquely up to isomorphism:

Proposition 1.4. *Any two initial objects of a category are isomorphic.*

Proof. Let $\perp_1$ and $\perp_2$ be initial objects in a category. Consider the following diagram

$$\begin{tikzcd}
\perp_2 \arrow[r] \arrow[dr] & \perp_1 \arrow[d] \arrow[dr] & \\
& \perp_2 \arrow[r] & \perp_1
\end{tikzcd}$$

in which each arrow is uniquely specified since its domain is initial. The diagram commutes, since each path in the diagram starts from an initial object. The right hand triangle shows that $\perp_1 \to \perp_2$ is right invertible, while the left hand triangle shows that $\perp_1 \to \perp_2$ is left invertible. $\square$

Corollary 1.5. *Any two terminal objects of a category are isomorphic, and any two zero objects of a category are isomorphic.*

Proposition 1.4 means that mathematical objects may be specified uniquely up to isomorphism as initial objects of certain categories. For example, the ring of integers is uniquely specified as the initial object of the category of unital rings (Exercise 7).

1.2. Slice categories and comma categories. If one is to apply the uniqueness of initial objects, it is necessary to design special categories.

1.2.1. *Slice categories.*

Definition 1.6. Let x be an object of a category C.

(a) The *slice category* C/x of C*-objects over* x has objects which are C-morphisms $p\colon a \to x$ with codomain x. A morphism in $(C/x)(p\colon a \to x, q\colon b \to x)$ is a C-morphism $f\colon a \to b$ such that the diagram

$$\begin{tikzcd} a \arrow[rr, "f"] \arrow[dr, "p"'] & & b \arrow[dl, "q"] \\ & x & \end{tikzcd}$$

commutes. The identity at $p\colon a \to x$ is 1_a.

(b) The *slice category* x/C of C*-objects under* x has objects which are C-morphisms $p\colon x \to a$ with domain x. A morphism in $(x/C)(p\colon x \to a, q\colon x \to b)$ is a C-morphism $f\colon a \to b$ such that the diagram

$$\begin{tikzcd} & x \arrow[dl, "p"'] \arrow[dr, "q"] & \\ a \arrow[rr, "f"'] & & b \end{tikzcd}$$

commutes. The identity at $p\colon x \to a$ is 1_a.

Example 1.7. Let x be an object of a poset category $(X, \leq)$. Then X/x is the *down-set* $x^{\geq} = \{a \in X \mid x \geq a\}$, as a poset category with the order induced from $(X, \leq)$.

Example 1.8. Let $\top$ be a singleton set, a terminal object of **Set**. Then the slice category $\top/\mathbf{Set}$ is the category of *pointed sets*, sets with a selected element. (Compare Chapter 2, Exercise 15.) Morphisms of pointed sets are functions which preserve the pointed element.

1.2.2. *Comma categories.* Comma categories provide a more flexible generalization of slice categories.

Definition 1.9. Consider functors $D \xrightarrow{S} C \xleftarrow{T} E$.

(a) The *comma category* $(S \downarrow T)$ has objects $(d, f \colon dS \to eT, e)$ in $D_0 \times C_1 \times E_0$, often abbreviated just to $f \colon dS \to eT$.

(b) An $(S \downarrow T)$-*morphism*

$$(g, h) \colon (d, f \colon dS \to eT, e) \to (d', f' \colon d'S \to e'T, e')$$

is an element (g, h) of $D_1(d, d') \times E_1(e, e')$ such that the diagram

$$\begin{tikzcd} dS \arrow[r, "gS"] \arrow[d, "f"'] & d'S \arrow[d, "f'"] \\ eT \arrow[r, "hT"'] & e'T \end{tikzcd} \tag{1.1}$$

in C commutes.

In many cases, one of the functors S or T in a comma category $(S \downarrow T)$ is taken to be a constant functor, whose domain is the category $\mathbf{1}$ with just one object 1 and one morphism 1_1.

Example 1.10. Let x be an object of a category C, with constant functor $[x] \colon \mathbf{1} \to C$.

(a) The slice category C/x is the comma category $(1_C \downarrow [x])$.

(b) The slice category x/C is the comma category $([x] \downarrow 1_C)$.

1.3. Units in adjunctions. Consider an adjunction

$$(F \colon D \to C, G \colon C \to D, \eta, \varepsilon)\,. \tag{1.2}$$

Proposition 1.11. *Let x be an object of D, with constant functor $[x] \colon \mathbf{1} \to D$. Then the component $\eta_x \colon x \to xFG$ is an initial object of the comma category $([x] \downarrow G)$.*

PROOF. The comma category $([x] \downarrow G)$ starts with the functors

$$\mathbf{1} \xrightarrow{[x]} D \xleftarrow{G} C\,.$$

Let $h\colon x \to yG$ be an object of $([x] \downarrow G)$. Suppose that

$$(1_1, k) \in \mathbf{1}(1,1) \times C(xF, y)$$

is a $([x] \downarrow G)$-morphism from $\eta_x\colon x \to xFG$ to $h\colon x \to yG$. Then the diagram

(1.3)
$$\begin{tikzcd} & x \arrow[dl, "\eta_x"'] \arrow[dr, "h"] & \\ xFG \arrow[rr, "kG"'] & & yG \end{tikzcd}$$

in D commutes, as an instance of the diagram (1.1). However, the adjunction isomorphism

$$C(xF, y) \cong D(x, yG)$$

sends $k\colon xF \to y$ to $\eta_x k^G$. By the commuting of (1.3), $\eta_x k^G = h$. Thus there is a unique C-morphism $k\colon xF \to y$ such that (1.3) commutes. Correspondingly, there is a unique $([x] \downarrow G)$-morphism $(1_1, k)$ from $\eta_x\colon x \to xFG$ to $f\colon x \to yG$. □

Dual to Proposition 1.11 is the following result. Its proof is relegated to Exercise 12.

PROPOSITION 1.12. *Let y be an object of C, with constant functor $[y]\colon \mathbf{1} \to C$. Then the component $\varepsilon_y\colon yGF \to y$ is a terminal object of the comma category $(F \downarrow [y])$.*

COROLLARY 1.13. *Consider the adjunction* (1.12).

(a) *The unit $\eta\colon 1_D \to FG$ is uniquely determined by the functors F and G.*
(b) *The counit $\varepsilon\colon GF \to 1_C$ is uniquely determined by the functors F and G.*

PROOF. (a) Apply Proposition 1.11 and the uniqueness of initial objects. Note that specification of the comma category $([x] \downarrow G)$ only involves the functor G.

(a) Apply Proposition 1.12 and the uniqueness of terminal objects. □

1.4. Recognizing adjunctions. Consider a functor $G\colon C \to D$. In §1.3, the existence of an adjunction

$$(F\colon D \to C, G\colon C \to D, \eta, \varepsilon)$$

implied that for each object x of D, the comma category $([x] \downarrow G)$ had an initial object. The converse result is the topic of this section. The idea of the proof mimics the discussion of Example 2.2 in Chapter 9.

Theorem 1.14. *Let $G\colon C \to D$ be a functor. Then G has a left adjoint if, for each object x of D, the comma category $([x] \downarrow G)$ has an initial object.*

Proof. For each object x of D, let $\eta_x\colon x \to xFG$ be the initial object of $([x] \downarrow G)$, where xF is an object in C mapping to the codomain of η_x under the object part of the functor G. This defines a function $F_0\colon D_0 \to C_0; x \mapsto xF$ which will become the object part of the functor $F\colon D \to C$.

Given a D-morphism $f\colon x' \to x$, the C-morphism $f^F\colon x'F \to xF$ is defined as the C-morphism yielding the unique $([x'] \downarrow G)$-morphism $(1_1, f^F)$ from $\eta'_x\colon x' \to x'FG$ to $f\eta_x\colon x' \to xFG$, i.e. making the diagrams

$$\begin{tikzcd} & x' \arrow[dl, "\eta'_x"'] \arrow[dr, "f\eta_x"] & \\ x'FG \arrow[rr, "fFG"'] & & xFG \end{tikzcd}$$

or

(1.4)
$$\begin{tikzcd} x' \arrow[r, "\eta'_x"] \arrow[d, "f"'] & x'FG \arrow[d, "fFG"] \\ x \arrow[r, "\eta_x"'] & xFG \end{tikzcd}$$

in D commute. It is straightforward to verify that F is a functor (Exercise 13). The diagram (1.4) then shows that η is a natural transformation from 1_D to FG.

Now for x in D_0 and y in C_0, define

$$\varphi^x_y\colon C(xF, y) \to D(x, yG); g \mapsto \eta_x g^G\,.$$

For an element h of $D(x, yG)$, define $h\psi^y_x$ to be the unique element k of $C(xF, y)$ yielding an $([x] \downarrow G)$-morphism $(1_1, k)$ from $\eta_x\colon x \to xFG$

to $h\colon x \to yG$ — compare (1.3). Then φ_y^x and ψ_x^y are mutually inverse, so the desired isomorphism

$$C(xF, y) \cong D(x, yG)$$

is obtained. □

Corollary 1.15. *Let $F\colon D \to C$ be a functor. Then F has a right adjoint if, for each object y of C, the comma category $(C \downarrow [y])$ has a terminal object.*

Proof. This is dual to Theorem 1.14. □

2. Algebras in categories

2.1. Categories with products. Let $\mathbf{C}$ be a category. Definition 2.3 of Chapter 2 defined products $X_0 \times X_1$ of pairs of objects $X_0, X_1 \in \mathbf{C}_0$.

Definition 2.1. Suppose that $X_i \in \mathbf{C}_0$ for i in an index set I. Then the *product* $\prod_{i\in I} X_i$ is an object of $\mathbf{C}$ equipped with *projections*

$$\pi_i\colon \prod_{j\in I} X_j \to X_i$$

for each i in I, such that given $\mathbf{C}$-morphisms $f_i\colon Y \to X_i$ for $i \in I$, there is a unique morphism

$$\prod_{j\in I} f_j\colon Y \to \prod_{j\in I} X_j$$

such that $\left(\prod_{j\in I} f_j\right)\pi_i = f_i$ for $i \in I$.

Example 2.2. (a) If I is empty, the product is just a terminal object.

(b) Let $X = \{x_i \mid i \in I\}$ be a subset of $\mathbb{R}$ that is bounded below. Then in the poset category $(\mathbb{R}, \leq)$, the product $\prod_{j\in I} x_j$ is the infimum $\inf X$.

(c) If there is an object X such that $X_i = X$ for all $i \in I$, then the product $\prod_{i\in I} X_i$ is the I-th *power* X^I.

2.1.1. *Algebras in categories.* Suppose that $\mathbf{C}$ is a category in which the product $\prod_{i\in I} X_i$ exists whenever I is finite. (One describes $\mathbf{C}$ as a *category with finite products*.) In Chapter 1, Definition 2.5 defined magmas, semigroups, monoids, and groups as objects in the category **Set** equipped with extra structure.

DEFINITION 2.3. Let A be an object of $\mathbf{C}$.

(a) The *diagonal* $\Delta\colon A \to A^2$ is defined by

$$\begin{tikzcd} A & A^2 \arrow[l, "\pi_0"'] \arrow[r, "\pi_1"] & A \\ & A \arrow[ul, "1_A"] \arrow[u, "\Delta"'] \arrow[ur, "1_A"'] & \end{tikzcd}$$

using the product property of $A^2 = A \times A$.

(b) If there is a morphism $\mu\colon A^2 \to A$, then A is a *magma* in $\mathbf{C}$.

(c) If further, the *associativity* diagram

$$\begin{tikzcd} A^3 \arrow[r, "1_A\times\mu"] \arrow[d, "\mu\times 1_A"'] & A^2 \arrow[d, "\mu"] \\ A^2 \arrow[r, "\mu"'] & A \end{tikzcd}$$

commutes, then A is a *semigroup* in $\mathbf{C}$.

(d) If further, there is a morphism $\eta\colon \top \to A$ with composite

$$\begin{tikzcd} A \arrow[rr, "\upsilon"] \arrow[dr] & & A \\ & \top \arrow[ur, "\eta"'] & \end{tikzcd}$$

such that

$$\begin{tikzcd} A^2 \arrow[r, "\upsilon\times 1_A"] & A^2 \arrow[d, "\mu"] & A^2 \arrow[l, "1_A\times\upsilon"'] \\ & A \arrow[ul, "\Delta"] \arrow[ur, "\Delta"'] & \end{tikzcd}$$

commutes, then A is a *monoid* in $\mathbf{C}$.

(e) If, further, there is an *inversion* morphism $S\colon A \to A$ such that

$$\begin{tikzcd} A^2 \arrow[r, "S\times 1_A"] & A^2 \arrow[d, "\mu"] & A^2 \arrow[l, "1_A\times S"'] \\ A \arrow[u, "\Delta"] \arrow[r, "\upsilon"'] & A & A \arrow[u, "\Delta"'] \arrow[l, "\upsilon"] \end{tikzcd}$$

commutes, then A is a *group* in $\mathbf{C}$.

Remark 2.4. If $(A, \cdot, 1)$ is a group, then $\mu\colon (a_0, a_1) \mapsto a_0 \cdot a_1$ and $S\colon a \mapsto a^{-1}$, along with the selection of the identity element of A by $\eta\colon \top \to A$ (compare Exercise 2), make A a group in the category **Set** of sets.

Example 2.5. Let **Top** be the category consisting of topological spaces and continuous maps (compare §2.4.1). A group in the category **Top** is a *topological group*.

2.1.2. *Commutative magmas.*

Definition 2.6. Let A be an object in a category $\mathbf{C}$ that has finite products. Then the *twist* is the morphism $\tau\colon A^2 \to A^2$ defined by the application

$$\begin{tikzcd} A & A^2 \arrow[l, "\pi_0"'] \arrow[r, "\pi_1"] & A \\ & A \arrow[ul, "\pi_1"] \arrow[u, "\tau"] \arrow[ur, "\pi_0"'] & \end{tikzcd}$$

of the product property.

Example 2.7. If A is a set, then

$$\tau\colon A^2 \to A^2; (a_0, a_1) \mapsto (a_1, a_0)\,.$$

Definition 2.8. Let (A, μ) be a magma in a category $\mathbf{C}$ that has finite products. Then the magma is said to be *commutative* if the diagram

$$\begin{tikzcd} A^2 \arrow[rr, "\tau"] \arrow[dr, "\mu"'] & & A^2 \arrow[dl, "\mu"] \\ & A & \end{tikzcd}$$

commutes. A commutative group A in a category is described as *abelian*, with *addition* $\mu\colon A^2 \to A$, *negation* $S\colon A \to A$, and *zero morphism* $\eta\colon \top \to A$.

2.2. Pullbacks.

DEFINITION 2.9. Given arrows $f\colon X \to Z$ and $g\colon Y \to Z$ in a category $\mathbf{C}$, their *pullback* is an object $X \times_Z Y$ of $\mathbf{C}$, equipped with *projection* arrows $p\colon X \times_Z Y \to X$ and $q\colon X \times_Z Y \to Y$ satisfying $pf = qg$, such that for each object T of C and arrows $h\colon T \to X$, $k\colon T \to Y$ satisfying $hf = kg$, there is a unique arrow $h \times_Z k\colon T \to X \times_Z Y$ such that $(h \times_Z k)p = h$ and $(h \times_Z k)q = k$. The pullback is usually displayed as in the following diagram:

(2.1)
$$\begin{tikzcd}
 & Y \arrow[dr, "g"] & \\
X \times_Z Y \arrow[ur, "q"] \arrow[dr, "p"'] & T \arrow[l, dashed, "h \times_Z k"'] \arrow[u, "k"'] \arrow[d, "h"] & Z \\
 & X \arrow[ur, "f"'] &
\end{tikzcd}$$

EXAMPLE 2.10. In the category $\mathbf{Set}$ of sets, the pullback $X \times_Z Y$ is realized as $\{(x, y) \in X \times Y \mid xf = yg\}$, with the projections

$$p\colon X \times_Z Y \to X; (x, y) \mapsto x$$

and

$$q\colon X \times_Z Y \to Y; (x, y) \mapsto y\,.$$

In categories of algebras and homomorphisms, the same construction works.

The following proposition (with proof assigned as Exercise 18) shows how the pullback generalizes the product.

PROPOSITION 2.11. *Suppose that X and Y are objects of a category $\mathbf{C}$ with terminal object $\top$. Then the pullback $X \times_\top Y$ is the product $X \times Y$.*

2.2.1. *Products in slice categories.* Let Q be an object of a category $\mathbf{C}$. If the category $\mathbf{C}$ has pullbacks, then the slice category $\mathbf{C}/Q$ has finite products: The product of two objects $p_0 : E_0 \to Q$ and $p_1 : E_1 \to Q$ is the pullback $p\colon E_0 \times_Q E_1 \to Q$ as in

(2.2)
$$\begin{tikzcd}
E_0 \times_Q E_1 \arrow[r, "\pi_1"] \arrow[d, "\pi_0"'] \arrow[dr, "p"] & E_1 \arrow[d, "p_1"] \\
E_0 \arrow[r, "p_0"'] & Q
\end{tikzcd}$$

with the composite morphism $p = \pi_0 p_0 = \pi_1 p_1$ to Q.

2.3. Split extensions and modules.

DEFINITION 2.12. Let M be an abelian group. Then for a group G, the abelian group M is a (*right*) *G-module* if it is a right G-set whose representation $r\colon G \to M!$ restricts to $r\colon G \to \operatorname{End} M$.

EXAMPLE 2.13. Let n be a positive integer.

(a) The abelian group $\mathbb{R}^n_1$ of n-dimensional row vectors is a right module for the *general linear group* $\mathsf{GL}_n(\mathbb{R})$ of invertible $n \times n$ real matrices. (Compare Chapter 6, Example 1.21.)
(b) More generally, for any commutative unital ring S, the additive group S^n_1 is a right module over the group $(S^n_n)^*$ of invertible $n \times n$ matrices over S.

2.3.1. *Split extensions.*

DEFINITION 2.14. Let M be a right module over a group Q. Then the *split extension* $E = Q \ltimes M$ is the set $Q \times M$ equipped with the product

$$(q_1, m_1)(q_2, m_2) = (q_1 q_2, m_1 q_2 + m_2)\,. \tag{2.3}$$

The split extension comes equipped with the projection

$$p : E \to Q; (q, m) \mapsto q \tag{2.4}$$

and the insertion η_Q or

$$\eta : Q \to E; q \mapsto (q, 0), \tag{2.5}$$

both of which are group homomorphisms (Exercise 20).

EXAMPLE 2.15. For each positive integer n, the split extension

$$\mathsf{GA}_n(\mathbb{R}) = \mathsf{GL}_n(\mathbb{R}) \ltimes \mathbb{R}^n_1$$

is known as the *general affine group*. Compare Exercise 22.

EXAMPLE 2.16. For each positive integer n, the *orthogonal group* $\mathsf{O}_n(\mathbb{R})$ is the subgroup $\{A \in \mathsf{GL}_n(\mathbb{R}) \mid AA^T = I_n\}$ of $\mathsf{GL}_n(\mathbb{R})$. Then the *Euclidean group* $\mathsf{E}_n(\mathbb{R})$ is the subgroup $\mathsf{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n_1$ of the general affine group. (Compare Chapter 5, Exercise 20 and Chapter 6, Example 1.26.)

Consider the category $\mathbf{Gp}$ of groups. If M is a module over a group Q, the projection $p : E \to Q$ of (2.4) is an abelian group in the slice category $\mathbf{Gp}/Q$. The addition (compare Definition 2.8) is

$$+ : E \times_Q E \to E; \big((q, m_1), (q, m_2)\big) \mapsto (q, m_1 + m_2)$$

and the zero morphism is given by the group homomorphism η of (2.5), determining the morphism

$$\begin{tikzcd} Q \arrow[r, "\eta"] \arrow[d, "1_Q"'] & E \arrow[d, "p"] \\ Q \arrow[r, "1_Q"'] & Q \end{tikzcd} \tag{2.6}$$

from the terminal object $1_Q : Q \to Q$ of the slice category $\mathbf{Gp}/Q$.

2.3.2. *Modules.* Given a module M over a group Q, the split extension $p : Q \ltimes M \to Q$ of (2.4) is an abelian group in the slice category $\mathbf{Gp}/Q$. For q in Q, the conjugation action of the element q^η on the normal subgroup $p^{-1}\{1\}$ of $Q \ltimes M$ is given by

$$(q, 0)^{-1}(1, m)(q, 0) = (1, mq), \tag{2.7}$$

thereby reflecting the action of Q on the module M.

Conversely, suppose that $p : E \to Q$ is an abelian group in the slice category $\mathbf{Gp}/Q$, with addition $+ : E \times_Q E \to E$ and zero morphism as in (2.6). Let M denote the inverse image $p^{-1}\{1\}$ of the identity element 1 of Q under p. For elements m_1 and m_2 of M, the pair (m_1, m_2) lies in the pullback $E \times_Q E$, and the image $m_1 + m_2$ of the pair (m_1, m_2) under the addition again lies in M. In this way, the set M receives an abelian group structure. In analogy with (2.7), each element q of Q acts on M by

$$q\colon m \mapsto (q^\eta)^{-1} m q^\eta,$$

making M a right Q-module.

THEOREM 2.17. *Modules over a group Q are equivalent to abelian groups $p : E \to Q$ in the slice category $\mathbf{Gp}/Q$ of groups over Q.*

3. Exercises

(1) Show that the trivial group is a zero object in the category of groups.

(2) Suppose that a category C has a terminal object $\top$. Define a *point* of an object a of C to be a morphism $\top \to a$. Show that in **Set**, the points of an object A coincide with the elements of the set A.
(3) Let $\mathbf{C}$ be the category of all sets with at least two elements, and all functions between them. Show that $\mathbf{C}$ has no initial or terminal objects.
(4) Give an example of a poset category with no initial or terminal objects.
(5) Prove Proposition 1.3.
(6) Derive Corollary 1.5 from Proposition 1.4.
(7) Let S be a unital ring. Show that there is a unique unital ring homomorphism $\mathbb{Z} \to S$.
(8) Let x be an object of a category C.
  (a) Verify the category axioms for the slice category C/x.
  (b) Show that $(C^{\mathsf{op}}/x)^{\mathsf{op}} = x/C$.
(9) Suppose that $(X, \leq)$ is a poset category. Show that $(X, \leq)$ is isomorphic to the concrete category C with $C_0 = \{x^{\geq} \mid x \in X\}$ and $C(x^{\geq}, y^{\geq}) = \{x^{\geq} \hookrightarrow y^{\geq}\}$ for $x \leq y$ in X.
(10) Identify pointed sets as algebras with a single, nullary operation.
(11) Let **Ring** be the category of unital rings. Then an object $\varepsilon\colon R \to \mathbb{Z}$ of the slice category $\mathbf{Ring}/\mathbb{Z}$ is an *augmentation* of the ring R. Show that $p(X) \mapsto p(1)$ gives an augmentation of the integral polynomial ring $\mathbb{Z}[X]$.
(12) Prove Proposition 1.12.
(13) In the proof of Theorem 1.14, verify that F is a functor.
(14) Verify the claim of Example 2.2(b).
(15) Let $\mathbf{C}$ be a category with finite products.
  (a) Let $\mathbf{C}^2$ be the quiver with $(\mathbf{C}^2)_0 = \mathbf{C}_0 \times \mathbf{C}_0$ and
  $$\mathbf{C}^2\big((X,Y),(X',Y')\big) = \mathbf{C}(X,X') \times \mathbf{C}(Y,Y')$$
  for $X, X', Y, Y' \in \mathbf{C}_0$. Show that $\mathbf{C}^2$ is a category.
  (b) Let X_0 and X_1 be objects of $\mathbf{C}$. Let $\mathbf{C}\Delta/(X_0, X_1)$ be the subquiver of the slice category $\mathbf{C}^2/(X_0, X_1)$ whose object class consists of all objects of the form $(Y, Y) \to (X_0, X_1)$ for $Y \in \mathbf{C}_0$, and whose morphism class is formed by all morphisms $(f, f)\colon (Y, Y) \to (Z, Z)$ for $f\colon Y \to Z$ in $\mathbf{C}_1$. Show that $\mathbf{C}\Delta/(X_0, X_1)$ is a category.

(c) Show that $(\pi_0, \pi_1)\colon (X_0 \times X_1, X_0 \times X_1) \to (X_0, X_1)$ is a terminal object of $\mathbf{C}\Delta/(X_0, X_1)$.

(d) Conclude that products are uniquely specified up to isomorphism.

(16) Let $\mathbf{C}$ be a category with a terminal object $\top$.

(a) For $A \in \mathbf{C}_0$, show that the product $A \times \top$ exists in $\mathbf{C}$.

(b) Consider the functor $F_\top\colon \mathbf{C} \to \mathbf{C}; A \mapsto A \times \top$ (compare Chapter 9, Proposition 2.3.) Show that there is a natural transformation $\lambda\colon 1_{\mathbf{C}} \to F_\top$ whose component

$$\lambda_A\colon A \to A \times \top$$

at each object A of $\mathbf{C}$ is an isomorphism.

(17) Show that a group in the category of groups is abelian.

(18) Prove Proposition 2.11.

(19) Verify the claims of §2.2.1.

(20) Check that the maps (2.4) and (2.5) are group homomorphisms. In particular, check that E is a group.

(21) In the context of Definition 2.14, define

$$r\colon E \to M! \tag{3.1}$$

by $m'(q,m)^r = m'q + m$ for $m', m \in M$ and $q \in Q$. Show that (3.1) gives a permutation action of E on M.

(22) Show that

$$\mathsf{GL}_n(\mathbb{R}) \ltimes \mathbb{R}^n_1 \to \mathsf{GL}_{n+1}(\mathbb{R}); (A, \mathbf{x}) \mapsto \begin{bmatrix} 1 & \mathbf{x} \\ & A \end{bmatrix}$$

provides an injective group homomorphism from the general affine group to the general linear group one dimension higher.

(23) Let S be the ring of integers modulo 2.

(a) What is the order of the group $(S^2_2)^* \ltimes S^2_1$ (compare with Example 2.13)?

(b) How does the group $(S^2_2)^* \ltimes S^2_1$ compare to the symmetric group of degree 4?

(24) Let $\theta\colon \mathbb{R}^2_1 \to \mathbb{R}^2_1$ be a transformation of the plane that preserves lengths. Show that $\theta \in \mathsf{E}_2(\mathbb{R})$, with the action of the Euclidean group $\mathsf{E}_2(\mathbb{R})$ on the plane $\mathbb{R}^2_1$ given by (3.1).

CHAPTER 11

Limits and colimits

1. Limits and colimits

1.1. Limits.

1.1.1. *Functor categories.*

Definition 1.1. Let D and C be categories.

(a) The class of all functors $F\colon D \to C$ is denoted by $\left(C^D\right)_0$.
(b) The class of all natural transformations $\tau\colon F \to G$ between objects of $\left(C^D\right)_0$ is denoted by $\left(C^D\right)_1$.
(c) Given an element $F\colon D \to C$ of $\left(C^D\right)_0$, the *identity natural transformation* 1_F has components $(1_F)_x : xF \to xF$ at each vertex x of D.
(d) Given natural transformations $\tau_1\colon F_0 \to F_1$ and $\tau_2\colon F_1 \to F_2$ between objects of $\left(C^D\right)_0$, the *composite* natural transformation $\tau_1\tau_2\colon F_0 \to F_2$ is defined by its components $(\tau_1\tau_2)_x = (\tau_1)_x(\tau_2)_x$ at each vertex x of D.
(e) Then $C^D = \left(\left(C^D\right)_0, \left(C^D\right)_1\right)$ is known as a *functor category*.

Example 1.2. Let G be a group that is realized as a category G with a single object X, and a morphism g for each group element g (compare Chapter 2, Example 1.4). Consider the category $\underline{\underline{\mathbb{Z}}}$ of abelian groups. Then the functor category $\underline{\underline{\mathbb{Z}}}^G$ is the category of G-modules. Indeed, given a functor $r\colon G \to \underline{\underline{\mathbb{Z}}}$ with $Xr = M$, each morphism g^r (for $g \in G$) is an automorphism of the abelian group M, and the functoriality of r means that $mg^r h^r = m(gh)^r$ for $g, h \in G$.

Example 1.3. A poset is *discrete* if it has the form $(I, =)$ for a set I. Then for $\underline{2} = \{0, 1\}$ construed as a discrete poset category, the functor category $C^{\underline{2}}$ has an object class consisting of pairs (x_0, x_1) of objects of C, and a morphism class consisting of pairs $(f_0\colon x_0 \to y_0, f_1\colon x_1 \to y_1)$ of morphisms of C.

1.1.2. *Limits.*

Definition 1.4. Let J and $\mathbf{C}$ be categories, and let $F\colon J \to \mathbf{C}$ be a functor.

(a) The *diagonal functor* $\Delta\colon \mathbf{C} \to \mathbf{C}^J$ sends each object X of $\mathbf{C}$ to the constant functor $[X]\colon J \to \mathbf{C}$. Each morphism $f\colon X \to Y$ of $\mathbf{C}$ is sent to the natural transformation $[f]\colon [x] \to [y]$ with component $[f]_j = f$ at each object j of J.
(b) Let $[F]$ be the constant functor $[F]\colon \mathbf{1} \to \mathbf{C}$. Then the *limit* $\varprojlim F$ of F is a terminal object of the comma category $(\Delta \downarrow [F])$.

The comma category $(\Delta \downarrow [F])$ in Definition 1.4(b) is built on the pair

$$\mathbf{C} \xrightarrow{\Delta} \mathbf{C}^J \xleftarrow{[F]} \mathbf{1}$$

of functors whose common codomain is the functor category $\mathbf{C}^J$.

- An object $(Y, Y\Delta \to F, 1)$ of the comma category $(\Delta \downarrow [F])$ consists of a natural transformation $f\colon [Y] \to F$, specified by its components $f_j\colon Y \to jF$ at each object j of J.
- In particular, the terminal object $\varprojlim F$ of the comma category $(\Delta \downarrow [F])$ consists of an object of $\mathbf{C}$ itself, informally denoted as $\varprojlim F$, together with a natural transformation

  $$\pi\colon [\varprojlim F] \to F\,,$$

  specified by its components $\pi_j\colon \varprojlim F \to jF$ for each object j of J. These components are known as *projections*.
- The terminality of $\varprojlim F$ means that for each object Y of $\mathbf{C}$ with morphisms $f_j\colon Y \to jF$ for $j \in J_0$, there is a unique comma category morphism

  $$(\varprojlim f, 1_1) \in \mathbf{C}(Y, \varprojlim F) \times \mathbf{1}(1,1)$$

  such that the diagrams

$$\begin{tikzcd} {[Y]} \arrow[r, "{[\varprojlim f]}"] \arrow[d, "f"'] & {[\varprojlim F]} \arrow[d, "\pi"] \\ F \arrow[r, "1_F"'] & F \end{tikzcd} \quad \text{or} \quad \begin{tikzcd} Y \arrow[rr, "\varprojlim f"] \arrow[dr, "f_j"'] & & \varprojlim F \arrow[dl, "\pi_j"] \\ & jF & \end{tikzcd} \tag{1.1}$$

commute (in the second case, for each object j of J). (For the first diagram, compare (1.1) in Chapter 10).

1.1.3. *Products and pullbacks as limits.* Products of pairs of objects are implemented as limits in which the index category J is the discrete poset category $\underline{2}$ of Example 1.3. More generally, an arbitrary product $\prod_{i\in I} X_i$ is implemented as a limit in which the index category J is the discrete poset category I given by the set I.

Example 1.5. Let J be the join semilattice poset category with Hasse diagram $0 \longrightarrow 0+1 \longleftarrow 1$. Then for a functor $F\colon J \to \mathbf{C}$ with $jF = X_j$ for $j \in J_0$, the limit $\varprojlim F$ is the pullback $X_0 \xleftarrow{\pi_0} X_0 \times_{X_{0+1}} X_1 \xrightarrow{\pi_1} X_1$. Note that $\pi_{0+1}\colon X_0 \times_{X_{0+1}} X_1 \to X_{0+1}$ is the composite $\pi_0(0 \to 0+1)^F = \pi_1(1 \to 0+1)^F$. The diagram

$$\begin{tikzcd}
 & X_1 \arrow[dr, "(1\to 0+1)F"] & \\
Y \arrow[ur, bend left, "f_1"] \arrow[r, "\varprojlim f"'] \arrow[dr, bend right, "f_0"'] & \varprojlim F \arrow[u, "\pi_1"'] \arrow[r, "\pi_{0+1}"'] \arrow[d, "\pi_0"] & X_{0+1} \\
 & X_0 \arrow[ur, "(0\to 0+1)F"'] &
\end{tikzcd}$$

summarizes this case of the right-hand diagrams in (1.1).

1.1.4. *Equalizers.* Let $\|$ or *parallel* denote the category

$$\begin{tikzcd}
0 \arrow[loop left] \arrow[r, shift left] \arrow[r, shift right] & 1 \arrow[loop right]
\end{tikzcd}$$

with a parallel pair of non-identity arrows. Thus a functor $F\colon \| \to \mathbf{C}$ corresponds to a *parallel pair of arrows* $X_0 \underset{f_1}{\overset{f_0}{\rightrightarrows}} X_1$ in the category $\mathbf{C}$. The limit $\varprojlim F$ is a morphism $e\colon E \to X_0$ such that

$$\begin{tikzcd}
D \arrow[d, dashed, "\varprojlim d"'] \arrow[dr, "d"] & & \\
E \arrow[r, "e"'] & X_0 \arrow[r, shift left, "f_0"] \arrow[r, shift right, "f_1"'] & X_1
\end{tikzcd}$$

commutes, i.e., such that $ef_0 = ef_1$, and such that $d\colon D \to X_0$ with $df_0 = df_1$ implies the existence of a unique morphism $\varprojlim d\colon D \to E$

with $(\varprojlim d)e = d$. The limit E is known as the *equalizer* of f_0 and f_1. In the category of sets, or concrete categories of algebras, one may take e as the insertion of the subset

$$E = \{x \in X_0 \mid xf_0 = xf_1\}$$

into X_0.

1.2. Colimits. Colimits are the duals of limits.

DEFINITION 1.6. Let J and $\mathbf{C}$ be categories, and let $F\colon J \to \mathbf{C}$ be a functor, with $[F]$ as the constant functor $[F]\colon \mathbf{1} \to C$. Then the *colimit* $\varinjlim F$ of F is an initial object of the comma category $([F] \downarrow \Delta)$.

The comma category $([F] \downarrow \Delta)$ in Definition 1.6 is built on the pair

$$\mathbf{1} \xrightarrow{[F]} \mathbf{C}^J \xleftarrow{\Delta} \mathbf{C}$$

of functors whose common codomain is the functor category $\mathbf{C}^J$.

- An object $(1, F \to Y\Delta, Y)$ of the comma category $([F] \downarrow \Delta)$ consists of a natural transformation $f\colon F \to [Y]$, specified by its components $f_j\colon jF \to Y$ at each object j of J.
- In particular, the initial object $\varinjlim F$ of the comma category $([F] \downarrow \Delta)$ consists of an object of $\mathbf{C}$ itself, informally denoted as $\varinjlim F$, together with a natural transformation

$$\iota\colon F \to [\varinjlim F]\,,$$

  specified by its components $\iota_j\colon jF \to \varinjlim F$ for each object j of J. These components are known as *insertions*.
- The initiality of $\varinjlim F$ means that for each object Y of $\mathbf{C}$ with morphisms $f_j\colon jF \to Y$ for $j \in J_0$, there is a unique comma category morphism

$$(1_1, f) \in \mathbf{1}(1,1) \times \mathbf{C}(\varinjlim F, Y)$$

such that the diagrams

$$\begin{tikzcd} F \arrow[r, "1_F"] \arrow[d, "\iota"'] & F \arrow[d, "f"] \\ {[\varinjlim F]} \arrow[r, "{[\varinjlim f]}"'] & {[Y]} \end{tikzcd} \qquad \text{or} \qquad \begin{tikzcd} & jF \arrow[dl, "\iota_j"'] \arrow[dr, "f_j"] & \\ \varinjlim F \arrow[rr, "\varinjlim f"'] & & Y \end{tikzcd} \tag{1.2}$$

commute (in the second case, for each object j of J).

REMARK 1.7. Limits are also known as "projective limits" (because they come with projections) or "inverse limits," and may be written as "lim." Colimits, which may be written as "colim," are also known as "inductive limits" or "direct limits."

REMARK 1.8. As a mnemonic for the direction of the arrow under limit and colimit symbols, one may think of the projections $jF \xleftarrow{\pi_j} \varprojlim F$ coming out of limits and the insertions $jF \xrightarrow{\iota_j} \varinjlim F$ going in to colimits.

1.2.1. *Coproducts.* Coproducts of pairs of objects are just colimits in which the index category J is the discrete poset category $\underline{2}$ considered in Example 1.3. More generally, an arbitrary coproduct $\coprod_{i\in I} X_i$ or $\sum_{i\in I} X_i$ is a colimit in which the index category J is the discrete poset category I given by the set I.

EXAMPLE 1.9. (a) If I is empty, the coproduct $\coprod_{i\in I} X_i$ is just an initial object.

(b) Let $X = \{x_i \mid i \in I\}$ be a subset of $\mathbb{R}$ that is bounded above. Then in the poset category $(\mathbb{R}, \leq)$, the coproduct $\sum_{j\in I} x_j$ is the supremum $\sup X$.

(c) If there is an object X such that $X_i = X$ for all $i \in I$, then the coproduct $\sum_{i\in I} X_i$ is the I-th *multiple* IX.

1.2.2. *Pushouts.*

DEFINITION 1.10. Let J be the meet semilattice poset category with Hasse diagram $0 \longleftarrow 0\cdot 1 \longrightarrow 1$. Then for a functor $F\colon J \to \mathbf{C}$ with $jF = X_j$ for $j \in J_0$, the *pushout*

$$X_0 \xrightarrow{\iota_0} X_0 +_{X_{0\cdot 1}} X_1 \xleftarrow{\iota_1} X_1 \tag{1.3}$$

is the colimit $\varinjlim F$.

In the pushout (1.3), the composite $(0\cdot 1\to 0)^F\iota_0=(0\cdot 1\to 1)^F\iota_1$ is the insertion $\iota_{0\cdot 1}\colon X_{0\cdot 1}\to X_0+_{X_{0\cdot 1}}X_1$. The diagram

$$\begin{tikzcd}
 & X_1 \arrow[d, "\iota_1"] \arrow[dr, bend left, "f_1"] & \\
X_{0\cdot 1} \arrow[ur, bend left, "(0\cdot 1\to 1)F"] \arrow[r, "\iota_0+1"'] \arrow[dr, bend right, "(0\cdot 1\to 0)F"'] & X_0+_{X_{0\cdot 1}}X_1 \arrow[r, "\varinjlim f"'] & Y \\
 & X_0 \arrow[u, "\iota_0"] \arrow[ur, bend right, "f_0"'] &
\end{tikzcd}$$

summarizes this case of the right-hand diagrams in (1.2).

1.2.3. *Coequalizers.* For a functor $F\colon \| \to \mathbf{C}$ yielding a parallel pair of arrows $X_1 \underset{f_1}{\overset{f_0}{\rightrightarrows}} X_0$ in a category $\mathbf{C}$, the colimit $\varinjlim F$ is known as a *coequalizer*. It is a morphism $q\colon X_0\to Q$ such that

$$\begin{tikzcd}
 & & P \\
X_1 \arrow[r, shift left, "f_0"] \arrow[r, shift right, "f_1"'] & X_0 \arrow[ur, "p"] \arrow[r, "q"'] & Q \arrow[u, dashed, "\varinjlim p"']
\end{tikzcd}$$

commutes, i.e., such that $f_0q=f_1q$, and such that $p\colon X_0\to P$ with $f_0p=f_1p$ implies the existence of a unique morphism $\varinjlim p\colon Q\to P$ with $q(\varinjlim p)=p$.

2. Applications

Limit and colimits pervade mathematics.

2.1. Coequalizers.

2.1.1. *Equivalence relations.* Let X be a set, and let B be a binary relation on X. The projections

$$\pi_i\colon B\to X;(x_0,x_1)\mapsto x_i$$

for $i=0,1$ furnish a parallel pair $B \underset{\pi_1}{\overset{\pi_0}{\rightrightarrows}} X$ of arrows in the category **Set**. Let V be the equivalence relation *generated* by B, the smallest equivalence relation on X containing B. Then the natural projection

$$\operatorname{nat} V\colon X\to X^V;x\mapsto x^V\,, \tag{2.1}$$

with $x^V = \{y \in X \mid x\ V\ y\}$ and $X^V = \{x^V \mid x \in X\}$, is the coequalizer of $B \underset{\pi_1}{\overset{\pi_0}{\rightrightarrows}} X$ in **Set** (Exercise 11).

2.1.2. *Group presentations.* Group presentations were discussed in Chapter 6, §2.3.1. A presentation

$$Q = \langle x_1, \dots, x_n \mid u_1 = v_1, \dots, u_r = v_r \rangle \tag{2.2}$$

of a group Q by generators $x_1, \dots, x_n$ subject to the relations

$$u_1 = v_1, \dots, u_r = v_r\,,$$

where the u_i and v_i are elements of the free group F on the set

$$\{x_1, \dots, x_n\}\,,$$

means that Q is being described as a coequalizer in the category **Gp** of groups. Specifically, let R be the free group on a set $\{y_1, \dots, y_r\}$. Define group homomorphisms

$$f_0 \colon R \to F; y_1 \mapsto u_1, \dots, y_r \mapsto u_r$$

and

$$f_1 \colon R \to F; y_1 \mapsto v_1, \dots, y_r \mapsto v_r$$

using the freeness of R on $\{y_1, \dots, y_r\}$. Then Q is the coequalizer $q \colon F \to Q$ of the parallel pair $R \underset{f_1}{\overset{f_0}{\rightrightarrows}} F$ in **Gp**. Indeed, $f_0 q = f_1 q$ implies that for $1 \le i \le r$, one has $y_i f_0 q = y_i f_1 q$ or $u_i q = v_i q$, meaning that the relation $u_i = v_i$ holds in Q. Furthermore, if the relations $u_i = v_i$ hold in a group P generated by $\{x_1, \dots, x_n\}$, then there is a homomorphism $p \colon F \to P$ with $f_0 p = f_1 p$. The group homomorphism $\varinjlim p \colon Q \to P$ with $q(\varinjlim p) = p$ then shows that P is a quotient of Q, so Q is the largest group satisfying the relations given in the presentation. It is uniquely specified by the presentation (2.2), since coequalizers, as examples of colimits, which in turn are examples of initial objects, are uniquely specified.

2.1.3. *Regular epimorphisms.* In many concrete categories, and even in categories of algebras and homomorphisms, the underlying function of an epimorphism may not necessarily be surjective.

Example 2.1. Consider the category **Ring** of unital rings. Then the inclusion $j \colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism (Exercise 14), even though the underlying function is not surjective.

The concept of a regular epimorphism is intended to address this problem.

PROPOSITION 2.2. *Consider a category* **C**. *Suppose that* $q\colon X_0 \to Q$ *is the coequalizer in* **C** *of a parallel pair* $X_1 \overset{f_0}{\underset{f_1}{\rightrightarrows}} X_0$. *Then* q *is an epimorphism.*

PROOF. Consider morphisms $f, g\colon Q \to P$ with $qf = qg$, say

$$qf = qg = p\,. \tag{2.3}$$

Now $f_0p = f_0qf = f_1qf = f_1p$, so by the coequalizer property, there is a unique morphism $\varinjlim p\colon Q \to P$ with $q(\varinjlim p) = p$. Thus (2.3) yields $f = \varinjlim p = g$. $\square$

DEFINITION 2.3. A *regular epimorphism* in a category **C** is a coequalizer $q\colon X_0 \to Q$ of a parallel pair $X_1 \overset{f_0}{\underset{f_1}{\rightrightarrows}} X_0$ of arrows in **C**.

Regular epimorphisms are often obtained as follows.

DEFINITION 2.4. Let $f\colon X \to Y$ be a morphism in a category **C**.

(a) The *kernel pair* of f is the pullback $\ker f$ of $X \xrightarrow{f} Y \xleftarrow{f} X$.
(b) The morphism f is said to be an *effective epimorphism* if it is the coequalizer of its kernel pair $\ker f \overset{\pi_0}{\underset{\pi_1}{\rightrightarrows}} X$.

REMARK 2.5. In **Set**, or concrete categories of algebras like **Gp**, **Ring**, or **Lin**, the First Isomorphism Theorem shows that each morphism f may be factorized as the product $f = em$ of an effective epimorphism e and a monomorphism m.

2.2. Coproducts.

2.2.1. *Disjoint unions of sets.* In the category of sets, the coproduct $\coprod_{i\in I} X_i$ is given by the disjoint union. One realization is as the union $\bigcup_{i\in I}(X_i \times \{i\})$, with insertions

$$\iota_j\colon X_j \to \bigcup_{i\in I}(X_i \times \{i\})\,; x \mapsto (x, j)$$

for $j \in I$. Of course, all the possible realizations are isomorphic.

2.2.2. *Coproducts of free algebras.* Let $\mathbf{A}$ be a category of algebras, with underlying set functor $G\colon \mathbf{A} \to \mathbf{Set}$. The forgetful functor G has a left adjoint $F\colon \mathbf{Set} \to \mathbf{A}$, assigning the free algebra XF over X to each set X. Comparing the defining properties, one sees that the free algebra $(X+Y)F$ over the disjoint union $X+Y$ of sets X and Y is the coproduct $XF * YF$ of the free algebras XF over X and YF over Y. The homomorphic insertions $\iota_X\colon XF \to (X+Y)F$ and $\iota_Y\colon YF \to (X+Y)F$ are the respective unique homomorphic extensions of the composite functions $X \to (X+Y) \xrightarrow{\eta_{X+Y}} (X+Y)FG$, $Y \to (X+Y) \xrightarrow{\eta_{X+Y}} (X+Y)FG$. Now consider homomorphisms $f\colon XF \to A$ and $g\colon YF \to A$, with restriction functions $f|_X\colon X \to AG$ and $g|_Y\colon Y \to AG$. Then the function $f|_X + g|_Y\colon X+Y \to AG$ extends to a unique coproduct homomorphism $f * g\colon (X+Y)F \to A$.

2.2.3. *Free products of groups.* Coproducts $G * H$ of groups G, H, known as *free products*, may be described in terms of presentations. Suppose that

$$G = \langle x_1, \dots, x_m \mid s_1 = t_1, \dots, s_q = t_q \rangle$$

and

$$H = \langle y_1, \dots, y_n \mid u_1 = v_1, \dots, u_r = v_r \rangle$$

are respective presentations of G and H, with disjoint generating sets $\{x_1, \dots, x_m\}$ and $\{y_1, \dots, y_n\}$. Then $G * H =$

$$\langle x_1, \dots, x_m, y_1, \dots, y_n \mid s_1 = t_1, \dots, s_q = t_q, u_1 = v_1, \dots, u_r = v_r \rangle$$

is a presentation of the free product $G * H$.

EXAMPLE 2.6. Let H^2 denote the *upper half-plane* $\{x + iy \in \mathbb{C} \mid y > 0\}$. Then the *modular group* Γ is the subgroup of H^2! generated by the elements

$$S\colon z \mapsto -1/z$$

and

$$T\colon z \mapsto z + 1$$

which satisfy the relations

$$S^2 = 1 \quad \text{and} \quad (ST)^3 = 1 \tag{2.4}$$

(see Exercise 17.) Indeed, there is a presentation

$$\Gamma = \langle S, T \mid S^2 = 1, (ST)^3 = 1 \rangle$$

or

$$\Gamma = \langle S, U \mid S^2 = 1, U^3 = 1 \rangle$$

with $U = ST$ [**9**, Chapter 7]. Thus Γ is the free product $C_2 * C_3$ of the cyclic groups

$$C_2 = \langle S \mid S^2 = 1 \rangle$$

and

$$C_3 = \langle U \mid U^3 = 1 \rangle$$

(given in terms of presentations).

2.3. Directed colimits. Recall that a poset category J is a join semilattice if each pair of objects has a coproduct, a least upper bound. More weakly, a poset category J is said to be (*upwards*) *directed* if each pair of objects has an upper bound.

EXAMPLE 2.7. The poset with Hasse diagram

$$\begin{tikzcd}
 & z & \\
y_1 \arrow[ur] & & y_2 \arrow[ul] \\
x_1 \arrow[u] \arrow[urr] & & x_2 \arrow[u] \arrow[ull]
\end{tikzcd}$$

is upwards directed, but does not form a join semilattice.

DEFINITION 2.8. Let $\mathbf{C}$ be a category, and let J be a directed poset. Then the colimit $\varinjlim F$ of a functor $F \colon J \to \mathbf{C}$ is described as a *directed colimit*.

The following proposition (which is typical of analogues for more general algebras) gives an illustration of the use of directed colimits.

PROPOSITION 2.9. *Let V be a vector space over a field K. Let J be the poset of finite-dimensional subspaces of V, ordered by containment. Let $F \colon J \to \underline{\underline{K}}$ send a containment $X \subseteq Y$ to the linear inclusion $X \hookrightarrow Y$. Then the directed colimit of F is V.*

EXAMPLE 2.10. Consider $\mathbb{R}$ as a vector space over its subfield $\mathbb{Q}$. Then $\mathbb{R}$ is the directed colimit of its finite-dimensional $\mathbb{Q}$-subspaces.

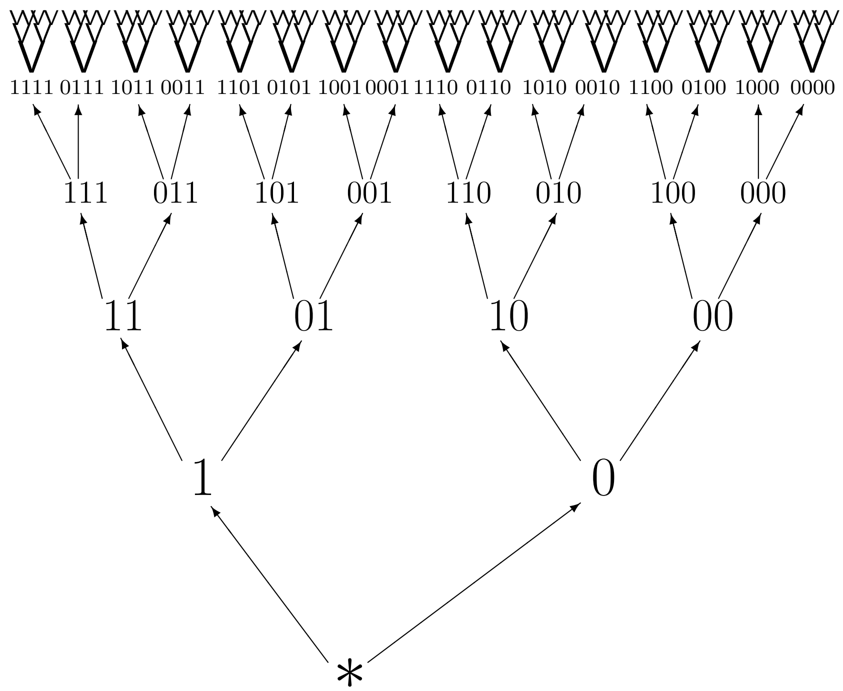


FIGURE 1. 2-adic integers as paths in the binary tree.

2.4. p-adic integers. Let p be a prime number. For given natural numbers n and r, there is a unital ring homomorphism

$$\rho_n^{n+r}\colon \mathbb{Z}/p^{n+r}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}; x + p^{n+r}\mathbb{Z} \mapsto x + p^n\mathbb{Z}$$

given by reduction modulo p^n. Consider the functor

$$F\colon (\mathbb{N}, \geq) \to \mathbf{Ring}$$

with $(n+r, n)F = \rho_n^{n+r}$ for natural numbers n and r.

DEFINITION 2.11. The limit $\varprojlim F$ is the ring $\mathbb{Z}_p$ of *p-adic integers*.

One may realize $\mathbb{Z}_p$ as the set of sequences

$$(x_1 + p\mathbb{Z}, x_2 + p^2\mathbb{Z}, x_3 + p^3\mathbb{Z}, \dots) \tag{2.5}$$

such that $\forall\ 0 < n \in \mathbb{N}\,,\ x_{n+1} + p^n\mathbb{Z} = x_n + p^n\mathbb{Z}$. (See Figure 1 for the case $p = 2$.) The ring operations are performed componentwise. In particular, since each residue coprime to p is invertible in each quotient $\mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$, each p-adic number (2.5) with $x_1 \not\equiv 0 \mod p$ is invertible in $\mathbb{Z}_p$. For example, the inverse of 3 or $(1, 3, 3, 3, 3, \dots)$ in $\mathbb{Z}_2$ is $(1, 3, 3, 11, 11, \dots)$ in $\mathbb{Z}_2$. Similarly, one may solve certain algebraic equations within the rings $\mathbb{Z}_p$ (compare Exercise 21).

3. Exercises

(1) In the context of Definition 1.1, verify that C^D is a category.

(2) Let M be a monoid, realized as a category with a single object. Show that the functor category $\mathbf{Set}^M$ is essentially the category of M-sets. [Hint: Interpret the intertwining diagram (compare (2.1) in Chapter 3) as a naturality condition.]

(3) Let J be a category with an initial object $\perp$. For each functor $F\colon J \to \mathbf{C}$, show that $\varprojlim F = \perp F$.

(4) Show that a pullback $X \times_Z Y$ may be expressed as the equalizer of a parallel pair $X \times Y \rightrightarrows Z$ of arrows from the product $X \times Y$.

(5) Suppose that finite products exist in a category $\mathbf{C}$. Show that the equalizer of a parallel pair $X_0 \underset{f_1}{\overset{f_0}{\rightrightarrows}} X_1$ of arrows in $\mathbf{C}$ is the pullback of $X_0 \xrightarrow{1_A \times g} X_0 \times X_1 \xleftarrow{1_A \times f} X_0$.

(6) Let C be a poset category. Show that equalizer morphisms $e\colon E \to X_0$ in C are identities.

(7) Justify the claim of the final sentence of §1.1.4.

(8) Let G be a group, realized as a category. Show that a parallel pair of distinct morphisms f_0, f_1 of G has no equalizer.

(9) Let V be a finite-dimensional real vector space. Consider the endomorphism monoid $\operatorname{End} V$ as a category. Show that the equalizer e of a pair of morphisms f_0, f_1 is the projection from V to the null space $\operatorname{Ker}(f_0 - f_1)$ of $f_0 - f_1$.

(10) Pullbacks were used to build products in slice categories $\mathbf{C}/Q$. Can you use pushouts to build coproducts in slice categories $Q/\mathbf{C}$?

(11) Show that (2.1) is the coequalizer of the parallel pair $B \underset{\pi_1}{\overset{\pi_0}{\rightrightarrows}} X$ in §2.1.1.

(12) Let $f\colon A \to B$ be a homomorphism of abelian groups. Show that the cokernel $B \to \operatorname{Coker} f$ is the coequalizer of the parallel pair $A \underset{0}{\overset{f}{\rightrightarrows}} B$.

(13) Show that the coequalizer property of presentations discussed in §2.1.2 may be used to conclude that the symmetric group S_n of positive degree n is a quotient of the braid group B_n.

(14) Show that the inclusion $j\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ is an epimorphism in the category of unital rings and homomorphisms.

(15) Suppose that $e\colon E \to X_0$ is the equalizer of a pair $X_0 \underset{f_1}{\overset{f_0}{\rightrightarrows}} X_1$ of parallel arrows. Show that e is a monomorphism.

(16) Let $f\colon X \to Y$ be a function. Describe the kernel pair

$$\ker f \underset{\pi_1}{\overset{\pi_0}{\rightrightarrows}} X$$

of f in the category **Set**.

(17) In the modular group Γ, show that S and T satisfy the relations (2.4).

(18) Show that the modular group Γ is a quotient of the braid group B_3. [Hint: Consider the generators $t_1t_2t_1$ and t_1t_2 of B_3.]

(19) Verify Proposition 2.9.

(20) Show that every group is obtained as the directed colimit of its finitely generated subgroups.

(21) Show that -1 has a square root in the ring $\mathbb{Z}_5$ of 5-adic integers.

(22) Can you justify the computation $-1 = 1 + 2 + 2^2 + 2^3 + \dots$ in the ring $\mathbb{Z}_2$ of 2-adic integers?

CHAPTER 12

Continuity

1. Continuity

1.1. Preserving limits and colimits. Suppose that $F\colon J \to C$ and $R\colon C \to D$ are functors. Consider the limit diagrams

$$\varprojlim F \xrightarrow{\pi_j} jF \tag{1.1}$$

for F in C and

$$\varprojlim\,(FR) \xrightarrow{\varpi_j} jFR \tag{1.2}$$

for FR in D, as well as the colimit diagrams

$$jF \xrightarrow{\iota_j} \varinjlim F \tag{1.3}$$

for F in C and

$$jFR \xrightarrow{i_j} \varinjlim\,(FR) \tag{1.4}$$

for FR in D.

Definition 1.1. (a) Suppose that F has a limit (1.1). The functor R *preserves* the limit of F if $(\varprojlim F)R \xrightarrow{\pi_j R} jFR$ is a limit of FR in D.

(b) Suppose that F has a colimit (1.3). Then the functor R *preserves* the colimit of F if $jFR \xrightarrow{\iota_j R} (\varinjlim F)R$ is a colimit of FR in D.

Remark 1.2. The preservation property expressed in Definition 1.1(a) is often summarized by the equation

$$\varprojlim\,(FR) = (\varprojlim F)R\,.$$

Dually,

$$\varinjlim (FR) = (\varinjlim F)R$$

summarizes Definition 1.1(b).

EXAMPLE 1.3. Let $U\colon \mathbf{Gp} \to \mathbf{Set}$ be the usual forgetful functor from groups to sets.

(a) Suppose that $G_1 \times G_2$ is a product of groups. Then one has $(G_1 \times G_2)U = G_1U \times G_2U$. Thus U preserves the product of two groups.
(b) Recall that the modular group Γ is the coproduct $C_2 * C_3$ of the respective cyclic groups of orders 2 and 3. (See Chapter 11, Example 2.6.) However, ΓU is an infinite set, so it is not the disjoint union of the finite sets C_2U and C_3U. Thus U does not preserve the coproduct $C_2 * C_3$.

EXAMPLE 1.4. Let $G\colon \mathbf{Set} \to \mathbf{Gp}$ be the free group functor.

(a) Suppose that $X_1 + X_2$ is the disjoint union of sets X_1 and X_2. Then $(X_1 + X_2)G = X_1G * X_2G$, so G preserves the coproduct of two sets.
(b) Let X be a singleton set. Then $XG \cong (X \times X)G \cong \mathbb{Z}$, but $(X \times X)G \cong \mathbb{Z} \not\cong \mathbb{Z} \times \mathbb{Z} \cong XG \times XG$, so G does not preserve the product $X \times X$.

1.1.1. *Exactness and continuity.* If J and C are categories, limits of functors $F\colon J \to C$ in C are classified according to the nature of the category J. Specifically, $\varprojlim F$ is:

- *small* if J is small;
- *finite* if J is finite;
- *directed* if J is directed.

A similar classification applies to colimits. (Compare Chapter 11, Definition 2.8.) This classification extends to categories and functors.

DEFINITION 1.5. Let C be a category.

(a) C is *complete* if all small limits exist in C.
(b) C is *cocomplete* if all small colimits exist in C.
(c) C is *left exact* if all finite limits exist in C.
(d) C is *right exact* if all finite colimits exist in C.

DEFINITION 1.6. Let $R\colon C \to D$ be a functor.

(a) R is *continuous* if it preserves all small limits in C.
(b) R is *cocontinuous* if it preserves all small colimits in C.
(c) R is *left exact* if it preserves all finite limits in C.
(d) R is *right exact* if it preserves all finite colimits in C [1].

Example 1.7 (Distributive lattices). Let $(L, \vee, \wedge, 0, 1)$ be a bounded lattice. For an element x of L, consider the multiplication

$$S(x)\colon L \to L; y \mapsto x \wedge y\,.$$

Note that $S(x)\colon L \to L$ is a functor. Since the only nontrivial colimits in a poset category are coproducts, the multiplications $S(x)$ for $x \in L$ are right exact if and only if

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

for $x, y, z \in L$, i.e., if and only if the lattice is *distributive*.

1.2. Continuity and adjunction.

1.2.1. *Limits as adjoints.*

Proposition 1.8. *Let J and C be categories. Suppose that for each functor $F\colon J \to C$, the limit $\varprojlim F$ exists in C. Then the functor*

$$[\quad]\colon C \to C^J; X \mapsto [X]$$

is left adjoint to the functor

$$\varprojlim\colon C^J \to C; F \mapsto \varprojlim F\,.$$

Proof. For the adjunction isomorphism

$$C^J([Y], F) \cong C(Y, \varprojlim F)\,, \tag{1.5}$$

note that a natural transformation $f\colon [Y] \to F$ with components $f_j\colon Y \to jF$ corresponds to a unique C-morphism $\varprojlim f\colon Y \to \varprojlim F$. Conversely, a C-morphism $l\colon Y \to \varprojlim F$ determines a unique natural transformation $f\colon [Y] \to F$ with components $f_j = l\pi_j$ for j in J, such that $l = \varprojlim f$. $\square$

Corollary 1.9. *Let J and C be categories, with a functor $F\colon J \to C$. The isomorphism* (1.5) *holds for each object Y of C if and only if the functor F has a limit.*

[1] See Exercise 10 for a justification of the terminology of Definition 1.6(d).

PROOF. The existence of the limit is equivalent to the existence of a unique C-morphism $\varprojlim f\colon Y \to \varprojlim F$ for each given natural transformation $f\colon [Y] \to F$. $\square$

1.2.2. *Continuity of right adjoints.*

PROPOSITION 1.10. *Suppose that a functor $R\colon C \to D$ has a left adjoint $S\colon D \to C$. Then R is continuous.*

PROOF. Suppose that a functor $F\colon J \to C$ with small domain has a limit $\varprojlim F$ in C. For each object X of C, an isomorphism

$$C^J\big([XS], F\big) \cong D^J\big([X], FR\big) \tag{1.6}$$

is provided by the adjunction isomorphism

$$C(XS, jF) \cong D(X, jFR)$$

for each object j of J, sending the component h_j of an element of the left hand side of (1.6) to the corresponding component of a natural transformation from the right hand side. Now consider the string of isomorphisms

$$\begin{aligned} D^J\big([X], FR\big) &\cong C^J\big([XS], F\big) \\ &\cong C(XS, \varprojlim F) \cong D\big(X, (\varprojlim F)R\big) \end{aligned} \tag{1.7}$$

coming respectively from (1.6), (1.5), and the adjunction. Considering the isomorphism between the extremes of (1.7), Corollary 1.9 then shows that $\varprojlim (FR) = (\varprojlim F)R$, as required. $\square$

COROLLARY 1.11. *Suppose that a functor $S\colon D \to C$ has a right adjoint $R\colon C \to D$. Then S is cocontinuous.*

1.3. Tensor products of modules. Suppose that S is a unital, commutative ring. Let $\underline{\underline{S}}$ be the category of unital S-modules. Recall the adjunction

$$\underline{\underline{S}}(Z \otimes Y, X) \cong \underline{\underline{S}}(Z, \underline{\underline{S}}(Y, X))$$

that defines the tensor product $Z \otimes Y$ of S-modules Z and Y, with left adjoint $F_Y\colon \underline{\underline{S}} \to \underline{\underline{S}}; Z \mapsto Z \otimes Y$ (compare Chapter 9, Proposition 2.5), as well as the isomorphism

$$\underline{\underline{S}}(Z \otimes Y, X) \cong \underline{\underline{S}}(Z, Y; X) \tag{1.8}$$

with the set of bilinear functions from $Z \times Y$ to an S-module X. Setting $X = Z \otimes Y$ in (1.8) yields a bilinear function

$$\otimes\colon Z \times Y \to Z \otimes Y; (z, y) \mapsto z \otimes y \tag{1.9}$$

corresponding to $1_{Z\otimes Y}$ on the left. Elements of the image of (1.9) inside $Z \otimes Y$ are described as *primitive*. The primitive elements may form a proper subset of $Z \otimes Y$ (Exercise 7).

The isomorphism $Z \times Y \cong Y \times Z$ yields the commutative law

$$Z \otimes Y \cong Y \otimes Z$$

for tensor products. The cocontinuity of F_Y given by Corollary 1.11 implies the distributive law

$$Y \otimes \sum_{i\in I} Z_i \cong \sum_{i\in I} Y \otimes Z_i \tag{1.10}$$

for modules Y and Z_i with i in an arbitrary index set I.

PROPOSITION 1.12. *There is a natural transformation* $\lambda\colon F_S \to 1_{\underline{\underline{S}}}$ *with isomorphic components* $\lambda_Z\colon Z \otimes S \to Z; z \otimes s \mapsto zs$.

PROOF. For S-modules Z and X, one has isomorphisms

$$\underline{\underline{S}}(Z \otimes S, X) \cong \underline{\underline{S}}(Z, \underline{\underline{S}}(S, X)) \cong \underline{\underline{S}}(Z, X)\,, \tag{1.11}$$

where the latter isomorphism follows from the two mutually inverse isomorphisms

$$X \to \underline{\underline{S}}(S, X); x \mapsto (S \to X; 1 \mapsto x)$$

and

$$\underline{\underline{S}}(S, X) \to X; f \mapsto 1f$$

given by the freeness of the S-module S on $\{1\}$. Comparing the extreme ends of (1.11), the isomorphism $Z \otimes S \cong Z$ is given by the uniqueness of adjoints. $\square$

PROPOSITION 1.13. *Tensor products of free modules are free.*

PROOF. Recall that the free S-module on a set I is the coproduct $\sum_{i\in I} S$ of copies of the free module S indexed by I. For sets I and J, the isomorphisms

$$\sum_{i\in I} S \otimes \sum_{j\in J} S \cong \sum_{(i,j)\in I\times J} S \otimes S \cong \sum_{(i,j)\in I\times J} S$$

are given by the distributive law (1.10) and Proposition 1.12. $\square$

Proposition 1.14. *Let X be an S-module. Let K be an ideal of S.*

(a) *There are mutually inverse isomorphisms*

$$X \otimes (S/K) \to X/(XK); x \otimes (s+K) \mapsto xs + XK$$

and

$$X/(XK) \to X \otimes (S/K); x + XK \mapsto x \otimes 1\,.$$

(b) *In particular,*

$$S/K \otimes S/L \cong S/(K+L)$$

with $K + L = \{k + l \mid k \in K, l \in L\}$ for a second ideal L of S.

Proposition 1.14 is especially useful for computing tensor products of abelian groups. For instance,

$$\mathbb{Z}/_m \otimes \mathbb{Z}/_n \cong \mathbb{Z}/_d \tag{1.12}$$

with positive integers m and n, if $\gcd\{m,n\} = d$ (Exercise 9).

2. Existence of adjoints

2.1. Complete lattices.

Proposition 2.1. *Let $(X, \leq)$ be a poset, construed as a category. Then the following conditions are equivalent:*

(a) *For each function $A\colon J \to X; j \mapsto x_j$, the greatest lower bound*

$$\prod\{x_j \mid j \in J\}$$

exists;

(b) *For each function $A\colon J \to X; j \mapsto x_j$, the least upper bound*

$$\sum\{x_j \mid j \in J\}$$

exists.

Proof. Suppose that (a) holds. Let $A\colon J \to X; j \mapsto x_j$ be a function. Define

$$U = \{u \in X \mid \forall\ j \in J\,,\ x_j \leq u\}\,,$$

the set of upper bounds of the image JA. Let $I\colon U \hookrightarrow X; u \mapsto u$ be the inclusion function. By (a), the product $\prod U$ exists. Consider $x_j \in JA$. Now

$$\forall\, u \in U\,,\ x_j \leq u \quad \Rightarrow \quad x_j \leq \prod U\,,$$

so $\prod U$ is an upper bound for JA. Suppose that u is an upper bound for JA. On the other hand, if u is an upper bound for JA, one has $u \in U$, and so $\prod U \leq u$. Thus $\prod U$ is the least upper bound for JA. The implication (b) $\Rightarrow$ (a) is dual to (a) $\Rightarrow$ (b). ☐

Definition 2.2. A poset that satisfies the equivalent conditions of Proposition 2.1 is called a *complete lattice*.

2.2. Tarski's Fixed Point Theorem.

Theorem 2.3. *Let $(X, \leq)$ be a complete lattice. Let $T\colon X \to X$ be a functor (order-preserving map). Consider the set*

$$X_T = \{x \in X \mid xT = x\}$$

of fixed points of T. Then the induced poset $(X_T, \leq)$ is a complete lattice.

Proof. Let A be a subset of X_T. Define

$$B = \{b \in X \mid \forall\, a \in A\,,\ a \leq bT \leq b\}\,.$$

Let g be the greatest lower bound $\prod B$ of B in X. Then for $b \in B$, one has $g \leq b$, and so $gT \leq bT \leq b$. Thus gT is a lower bound for B, and therefore $gT \leq g$.

Next, let l be the least upper bound $\sum A$ of A in X. Then

$$(\forall\, a \in A\,,\ \forall\, b \in B\,,\ a \leq bT) \Rightarrow (\forall\, b \in B\,,\ l \leq bT \leq b) \Rightarrow l \leq g\,.$$

Thus g is an upper bound for A in X, i.e.

$$\forall\, a \in A\,,\ a \leq g\,.$$

Applying T yields

$$\forall\, a \in A\,,\ aT = a \leq gT \leq g\,,$$

so $g \in B$. Applying T again yields

$$\forall\, a \in A\,,\ aT = a \leq gT^2 \leq gT\,,$$

so $gT \in B$. Since $g = \prod B$, one has $g \leq gT$. Thus $gT = g \in X_T$. This means that g, which was an upper bound for A in X, is actually an upper bound for A in X_T.

If u is any upper bound for A in X_T, then

$$(\forall\ a \in A\,,\ a \leq uT \leq u) \Rightarrow u \in B \Rightarrow g \leq u\,.$$

Thus g, the greatest lower bound for B in X, is the least upper bound for A in X_T. $\square$

COROLLARY 2.4. *Consider functions $f\colon A \to B$ and $g\colon B \to A$.*

(a) **Banach Decomposition Theorem.** *One has disjoint union decompositions $A = A_1 + A_2$ and $B = B_1 + B_2$ with $A_1 f = B_1$ and $B_2 g = A_2$.*

(b) **Cantor-Schröder-Bernstein Theorem.** *If f and g inject, then A and B are isomorphic.*

PROOF. (a) Consider the following four functors:

$$\begin{aligned}
S_1&\colon (2^A, \subseteq) \to (2^B, \subseteq); Y \mapsto Yf\,;\\
S_2&\colon (2^B, \subseteq) \to (2^B, \supseteq); Z \mapsto B \smallsetminus Z\,;\\
S_3&\colon (2^B, \supseteq) \to (2^A, \supseteq); Z \mapsto Zg\,;\\
S_4&\colon (2^A, \supseteq) \to (2^A, \subseteq); Y \mapsto A \smallsetminus Y\,.
\end{aligned}$$

Their composite $T\colon (2^A, \subseteq) \to (2^A, \subseteq)$ is a functor on the complete lattice $(2^A, \subseteq)$, and thus has a fixed point A_1, i.e.,

$$A_1 = A_1 T = A_1 S_1 S_2 S_3 S_4\,.$$

Now set $A_2 = A_1 S_1 S_2 S_3$, $B_2 = A_1 S_1 S_2$, and $B_1 = A_1 S_1$.

(b) The disjoint union $(f\colon A_1 \to B_1) + (g^{-1}\colon A_2 \to B_2)$ is a bijection from A to B. $\square$

2.3. Existence of adjoints on posets. Proposition 1.10 showed that if a functor R is a right adjoint, then it is continuous. The following result gives the converse for poset categories, if the domain of R is a complete lattice.

PROPOSITION 2.5. *A continuous functor $R\colon A \to B$ from a complete lattice to a poset has a left adjoint $S\colon B \to A$.*

PROOF. Define

$$S\colon B \to A; x \mapsto \prod\{z \in A \mid x \leq z^R\}\,.$$

Note that for $x_1, x_2 \in A$, one has

$$x_1 \leq x_2 \Rightarrow \{z \in A \mid x_1 \leq z^R\} \supseteq \{z \in A \mid x_2 \leq z^R\}$$
$$\Rightarrow \prod\{z \in A \mid x_1 \leq z^R\} \leq \prod\{z \in A \mid x_2 \leq z^R\} \Rightarrow x_1^S \leq x_2^S\,,$$

so S is a functor. Then for the adjointness, one has the unit relationship

$$x \leq \prod\{z^R \mid z \in A\,,\ x \leq z^R\} = \Big(\prod\{z \mid z \in A\,,\ x \leq z^R\}\Big)^R = x^{SR}$$

for x in B, the first equality holding by the continuity of R. Dually,

$$y^{RS} = \prod\{z \in A \mid y^R \leq z^R\} \leq y$$

for y in A. □

Dually, one has the following:

COROLLARY 2.6. *A cocontinuous functor $S\colon B \to A$ from a complete lattice to a poset has a right adjoint $R\colon A \to B$.*

2.4. Complete Heyting algebras. Consider a bounded lattice $(L, \vee, \wedge, 0, 1)$. Recall that L is distributive if and only if the functors

$$S(x)\colon L \to L; y \mapsto x \wedge y$$

are right exact for all x in L (Example 1.7). If L is a complete lattice, and the functors $S(x)$ are cocontinuous for all x in L, i.e.

$$\forall\ J \subseteq L\,,\ x \wedge \sum\{y \mid y \in J\} = \sum\{x \wedge y \mid y \in J\} \tag{2.1}$$

for all x in L, then L is called a *completely distributive lattice*. However, Corollary 2.6 shows that each $S(y)$ has a right adjoint

$$R(y)\colon L \to L; z \mapsto y\backslash z$$

namely with

$$L\big(xS(y), z\big) \cong L\big(x, zR(y)\big)$$

or

$$x \wedge y \leq z \quad \Leftrightarrow \quad x \leq y\backslash z\,,$$

so that $(L, \vee, \wedge, \backslash, 0, 1)$ forms a *complete Heyting algebra*.

EXAMPLE 2.7. Let X be a set. With the Boolean implication

$$U \to V = (X \smallsetminus U) \cup V\,,$$

the power set 2^X forms a complete Heyting algebra $(2^X, \cup, \cap, \to, \emptyset, X)$. (Compare Chapter 2, Example 2.22.)

2.4.1. *Topology.* Let X be a set. Let T be a complete sublattice of 2^X for which the inclusion $T \hookrightarrow 2^X$ is a cocontinuous bounded lattice homomorphism. Then T is a complete Heyting algebra. Indeed, the complete distributive law (2.1) in T is inherited from 2^X. Such a sublattice T of 2^X is called a *topology* on the set X, and the pair (X, T) is a *topological space*. Elements of T are called *open subsets of X in the topology T*.

Let (X, T) and (Y, U) be topological spaces Consider a function $f\colon X \to Y$, and the right adjoint

$$f^{-1}\colon (2^Y, \subseteq) \to (2^X, \subseteq); Z \mapsto f^{-1}Z \tag{2.2}$$

to the functor

$$(2^X, \subseteq) \to (2^Y, \subseteq); W \mapsto Wf \tag{2.3}$$

(compare Exercise 13). The function f is said to be *continuous* if f^{-1} restricts to a functor $f^{-1}\colon (U, \subseteq) \to (T, \subseteq)$. The large concrete category **Top** has topological spaces as its objects and continuous maps as its morphisms. It is the domain of a forgetful functor

$$U\colon \mathbf{Top} \to \mathbf{Set}$$

sending a space (X, T) to its underlying set X.

2.5. Freyd's Adjoint Functor Theorem.

Definition 2.8. Let K be a set of objects in a (possibly large) category C. Then K is said to *dominate* C if each object of C is the codomain of a C-morphism whose domain lies in K.

Note that if C has an initial object $\perp$, then $\{\perp\}$ dominates C. A poset category is dominated by the set of minimal elements of the poset. More trivially, a small category C is dominated by its object set C_0.

In order to motivate the following definition, recall that a functor $G\colon C \to D$ has a left adjoint if for each object X of D, the comma category $([X] \downarrow G)$ has an initial object. (Compare Theorem 1.14 in Chapter 10.)

Definition 2.9. A functor $G\colon C \to D$ is said to satisfy the *solution set condition* if for each object X of D, the comma category $([X] \downarrow G)$ possesses a dominating set.

Freyd's Adjoint Functor Theorem gives a very powerful converse to Proposition 1.10, and a broad generalization of Proposition 2.5:

THEOREM 2.10. *Suppose that C is a complete, locally small category. If a continuous functor $G\colon C \to D$ satisfies the solution set condition, then it has a left adjoint.*

For the proof of Freyd's Adjoint Functor Theorem, see [**10**, §III.3.5].

3. Exercises

(1) Let U and V be finite-dimensional real vector spaces. Specify a functor $S\colon \mathbf{Set} \to \mathbf{Lin}$ such that the equation
$$\dim(U \oplus V) = \dim U + \dim V$$
may be interpreted to express the fact that S preserves certain coproducts.

(2) Let $*\colon \mathbf{Mon} \to \mathbf{Gp}$ be the functor sending a monoid to its group of units. Show that $*$ preserves products.

(3) Let $\mathcal{P}^{<\infty}\mathbb{N}$ be the set of subsets of $\mathbb{N}$ whose complement is finite. Consider $(\mathcal{P}^{<\infty}\mathbb{N}, \subseteq)$ as a poset category.
 (a) Show that finite products exist in $\mathcal{P}^{<\infty}\mathbb{N}$.
 (b) Show that infinite products may not exist in $\mathcal{P}^{<\infty}\mathbb{N}$.

(4) In the adjunction of Proposition 1.8, determine the unit and counit.

(5) Formulate the duals of Proposition 1.8 and Corollary 1.9.

(6) Suppose that X_i, for $1 \le i \le 3$, are unital modules over a unital, commutative ring S. Verify the associative law
$$(X_1 \otimes X_2) \otimes X_3 \cong X_1 \otimes (X_2 \otimes X_3)$$
for tensor products.

(7) Let K be a finite field of order q. Consider the row vector spaces $Z = K_1^2$ and $Y = K_1^3$.
 (a) Show that $|Z \times Y| = q^5$.
 (b) Show that $|Z \otimes Y| = q^6$.
 (c) Conclude that the tensor product $Z \otimes Y$ has elements which are not primitive.

(8) Specify the inverse of the mapping λ_Z in Proposition 1.12.

(9) Derive (1.12) from Proposition 1.14.

(10) Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \tag{3.1}$$

be an exact sequence of abelian groups. Let Y be an abelian group. Show that

$$A \otimes Y \xrightarrow{fF_Y} B \otimes Y \xrightarrow{gF_Y} C \otimes Y \longrightarrow 0 \tag{3.2}$$

is an exact sequence of abelian groups.

[According to the terminology of Definition 1.6(d), the functor F_Y, as a left adjoint, is right exact. The exactness in (3.2) of the image of the right hand end of the original sequence (3.1) is the motivation for this terminology.]

(11) Let S be a unital, commutative ring.
   (a) For positive integers m and n, prove that
   $$S^m_m \otimes S^n_n \cong S^{mn}_{mn}\,.$$
   (b) For matrices $[x_{ij}]$ in S^m_m and $[y_{kl}]$ in S^n_n, prove that the element $[x_{ij}] \otimes [y_{kl}]$ of $S^m_m \otimes S^n_n$ corresponds to $[x_{ij}y_{kl}]$ in S^{mn}_{mn} under the isomorphism of (a).

(12) Perform the Banach decomposition for the pair of functions $f\colon \mathbb{Z} \to \mathbb{Z}; n \mapsto 2n$ and $g\colon \mathbb{Z} \to \mathbb{Z}; n \mapsto 3n$.

(13) Show that (2.2) is a functor that is right adjoint to (2.3).

(14) Let X be a set.
   (a) Show that $\{\emptyset, X\}$ forms a topology (which is known as the *indiscrete topology* on X).
   (b) Show 2^X forms a topology (the *discrete topology* on X).
   (c) Show that $U\colon \mathbf{Top} \to \mathbf{Set}$ is left adjoint to an *indiscrete topology functor* which sends a set X to the space X with the indiscrete topology.
   (d) Show that $U\colon \mathbf{Top} \to \mathbf{Set}$ is right adjoint to a *discrete topology functor* which sends a set X to the space X with the discrete topology.
   (e) Conclude that the forgetful functor $U\colon \mathbf{Top} \to \mathbf{Set}$ is both continuous and cocontinuous.

(15) Let Y be a subset of a topological space (X, T). Show that

$$U = \{Z \subseteq Y \mid \exists\ G \in T\,.\ Z = G \cap Y\}$$

is a topology on Y (the *subspace topology* on Y).

(16) Let $(X, \leq)$ be a poset. Show that the set

$$x^{\geq} = \{a \in X \mid x \geq a\}$$

of downsets (for $x \in X$) forms a topology on X (known as the *Alexandrov topology*). (Compare Chapter 10, Example 1.7.)

(17) Let X be a set. Let $(B, \cap, X)$ be a submonoid of $(2^X, \cap, X)$. Show that $\{Y \subseteq X \mid \forall\ y \in Y\ ,\ \exists\ Z \in B\ .\ y \in Z \subset Y\}$ is a topology on X (the *topology spanned* or *generated by the base* B). [Let S be a subset of 2^X. Let $(\langle S \rangle, \cap, X)$ be the submonoid of $(2^X, \cap, X)$ generated by S. Then the topology spanned by the base $\langle S \rangle$ is called the *topology spanned by the subbase* S.]

(18) Let $G \colon C \to D$ be a functor with small domain and codomain.
   (a) Show that R satisfies the solution set condition.
   (b) Interpret Proposition 2.5 as a special case of Theorem 2.10.

CHAPTER 13

Algebras and coalgebras

1. Algebras

1.1. Endofunctors and their algebras.

1.1.1. *Unital rings.* Let A be a unital ring, so that A has an additive group structure and a multiplicative monoid structure. The structure lies in the binary operations $+\colon A^2 \to A$, $\cdot\colon A^2 \to A$; unary operation $-\colon A \to A$, and nullary operations $0\colon A^0 \to A$, $1\colon A^0 \to A$. These operations can be packed into a single sum function or "structure map" $\alpha\colon 2A^2 + A + 2A^0 \to A$. The domain of the structure map, namely $2A^2 + 1A^1 + 2A^0$, is the image AT of the set A under a "polynomial functor" $T\colon \mathbf{Set} \to \mathbf{Set}; X \mapsto 2X^2 + 1X^1 + 2X^0$. Given unital rings A and B encoded by structure maps $\alpha_A\colon AT \to A$ and $\alpha_B\colon BT \to B$, a function $f\colon A \to B$ is a unital ring homomorphism iff the diagram

$$\begin{tikzcd} AT \arrow[r, "\alpha_A"] \arrow[d, "fT"'] & A \arrow[d, "f"] \\ BT \arrow[r, "\alpha_B"'] & B \end{tikzcd}$$

commutes.

1.1.2. *Endofunctors and polynomial functors.* Let $\mathbf{C}$ be a category. A functor $T\colon \mathbf{C} \to \mathbf{C}$ is called an *endofunctor* on $\mathbf{C}$.

Definition 1.1. Let $\mathbf{C}$ be a category with all arbitrary small sums (coproducts) and finite products. Then an endofunctor T on $\mathbf{C}$ is called a *polynomial functor* of *type* τ if there is a *signature* function $\tau\colon \Omega \to \mathbb{N}$ with *operator domain* Ω such that

$$XT = \sum_{n\in\mathbb{N}} |\tau^{-1}\{n\}| X^n \tag{1.1}$$

for each object X of $\mathbf{C}$.

REMARK 1.2. For a natural number n in (1.1), the coefficient $|\tau^{-1}\{n\}|$ of X^n may be infinite. In all cases, the summand $|\tau^{-1}\{n\}|X^n$ denotes the sum of a family of copies of X^n indexed by the set $\tau^{-1}\{n\}$ of *n-ary operators* ω. (Compare Exercise 1.)

1.1.3. *Algebras for an endofunctor.*

DEFINITION 1.3. Let T be an endofunctor on a category $\mathbf{C}$.

(a) A *T-algebra* is an object A of $\mathbf{C}$ equipped with a $\mathbf{C}$-morphism α or $\alpha_A \colon AT \to A$ known as the *structure map*.

(b) A *T-algebra morphism* between T-algebras $\alpha_A \colon AT \to A$ and $\alpha_B \colon BT \to B$ in $\mathbf{C}$ is a $\mathbf{C}$-morphism $f \colon A \to B$ such that the diagram

$$\begin{tikzcd} AT \arrow[r, "\alpha_A"] \arrow[d, "fT"'] & A \arrow[d, "f"] \\ BT \arrow[r, "\alpha_B"'] & B \end{tikzcd}$$

commutes.

(c) The category of T-algebras and morphisms is written as ${}^T\mathbf{C}$.

(d) An initial object I of ${}^T\mathbf{C}$ is known as an *initial T-algebra*.

(e) The *canonical forgetful functor* $U_T \colon {}^T\mathbf{C} \to \mathbf{C}$ sends an object $\alpha_A \colon AT \to A$ to A.

1.1.4. *Examples.*

EXAMPLE 1.4. Let S be a set. Consider the polynomial endofunctor

$$T \colon \mathbf{Set} \to \mathbf{Set}; X \mapsto X \times S$$

on the category of sets.

(a) A T-algebra $\alpha_A \colon A \times S \to A$ is an automaton with set S of elementary events, and with the transition $a \xrightarrow{s} (a, s)\alpha_A$ from a state a under the action of an elementary event s (compare Chapter 4, §1.2.1).

(b) If S is a semigroup with multiplication $m \colon S \times S \to S$, then a T-algebra $\alpha_A \colon A \times S \to A$ is a right S-set if the diagram

$$\begin{tikzcd} AT^2 \arrow[r, "1_A \times m"] \arrow[d, "\alpha_A T"'] & AT \arrow[d, "\alpha_A"] \\ AT \arrow[r, "\alpha_A"'] & A \end{tikzcd} \quad \text{or} \quad \begin{tikzcd} A \times S \times S \arrow[r, "1_A \times m"] \arrow[d, "\alpha_A \times 1_S"'] & A \times S \arrow[d, "\alpha_A"] \\ A \times S \arrow[r, "\alpha_A"'] & A \end{tikzcd}$$

commutes

(c) If there is a natural transformation $\mu\colon T^2 \to T$ such that the diagram

$$\begin{tikzcd} AT^3 \arrow[r, "\mu_{AT}"] \arrow[d, "\mu_A T"'] & AT^2 \arrow[d, "\mu_A"] \\ AT^2 \arrow[r, "\mu_A"'] & AT \end{tikzcd}$$

commutes for all A, then $\mu_\top\colon S \times S \to S$ (with $\top$ terminal in **Set**) is a semigroup multiplication. In that case, a T-algebra $\alpha_A\colon A \times S \to A$, for which the version

$$\begin{tikzcd} AT^2 \arrow[r, "\mu_A"] \arrow[d, "\alpha_A T"'] & AT \arrow[d, "\alpha_A"] \\ AT \arrow[r, "\alpha_A"'] & A \end{tikzcd}$$

of the diagram of (b) commutes, is a right S-set.

Example 1.5. Let $\mathbf{C}$ be a category of algebras (such as groups, abelian groups, S-modules) satisfying some given set of identities. Consider the adjunction

$$(F\colon \mathbf{C} \to \mathbf{Set}, G\colon \mathbf{Set} \to \mathbf{C}, \eta, \varepsilon)$$

between the forgetful functor G and free algebra functor F. Take the endofunctor $FG\colon \mathbf{Set} \to \mathbf{Set}$. Then for each algebra A in $\mathbf{C}$, the image $\varepsilon_A G\colon AGFG \to AG$ under G of the counit component $\varepsilon_A\colon AGF \to A$ is the structure map of an FG-algebra AG.

Example 1.6. Let A be a non-unital ring. The bilinear multiplication

$$m_A\colon A \times A \to A; (x, y) \mapsto xy$$

yields an abelian group homomorphism

$$\mu_A\colon A \otimes A \to A; x \otimes y \mapsto xy\,.$$

Thus with the tensor square endofunctor $T\colon \underline{\underline{\mathbb{Z}}} \to \underline{\underline{\mathbb{Z}}}; A \to A \otimes A$, one obtains the structure map $\mu_A\colon AT \to A$ of a T-algebra. Conversely, if a T-algebra $\mu_A\colon AT \to A$ satisfies the *associative law*

$$\begin{tikzcd} A \otimes A \otimes A \arrow[r, "1_A \otimes \mu_A"] \arrow[d, "\mu_A \otimes 1_A"'] & A \otimes A \arrow[d, "\mu_A"] \\ A \otimes A \arrow[r, "\mu_A"'] & A \end{tikzcd}$$

then A is a non-unital ring.

1.2. Signatures and algebras. Suppose that $\tau\colon \Omega \to \mathbb{N}$ is a signature or type. Define $\Omega_n = \tau^{-1}\{n\}$ for each natural number n. Then the corresponding polynomial endofunctor is

$$T\colon \mathbf{Set} \to \mathbf{Set}; X \mapsto \sum_{n \in \mathbb{N}} X^n \times \Omega_n$$

or

$$T\colon \mathbf{Set} \to \mathbf{Set}; X \mapsto \sum_{\omega \in \Omega} X^{\omega\tau} \tag{1.2}$$

on the category of sets (compare (1.1) and Exercise 1). Recall the definition of a τ-algebra (X, Ω) (compare Chpater 6, Definition 1.4).

PROPOSITION 1.7. *For a given signature $\tau\colon \Omega \to \mathbb{N}$, the concepts of T-algebra and τ-algebra coincide.*

PROOF. If (X, Ω) is a τ-algebra, the structure map $\alpha_X\colon XT \to X$ is the sum of functions

$$X^{\omega\tau} \times \{\omega\} \to X; (x_1, \dots, x_{\omega\tau}, \omega) \mapsto x_1 \dots x_{\omega\tau}\omega$$

indexed by elements ω of the set Ω.

Conversely, suppose that $\alpha_X\colon XT \to X$ is a T-algebra. Let ω be an element of Ω, with insertion

$$\iota_\omega\colon X^{\omega\tau} \to XT$$

into the coproduct. Then the commutative diagram

$$\begin{tikzcd} X^{\omega\tau} \arrow[rr, "\iota_\omega"] \arrow[dr, "\omega"'] & & XT \arrow[dl, "\alpha_X"] \\ & X & \end{tikzcd}$$

gives a corresponding $\omega\tau$-ary operation $\omega\colon X^{\omega\tau} \to X$ on X.

Finally, note that a function $f\colon X \to Y$ between the underlying sets X, Y of algebras is a homomorphism of T-algebras if and only if it is a homomorphism of τ-algebras. $\square$

1.2.1. *Initial algebras.* For the polynomial functor T in (1.2), an initial object I_T of the category ${}^T\mathbf{Set}$ of T-algebras will be constructed in this paragraph.

Recall that a *subalgebra* of a τ-algebra (X, ω) is a subset Y of X such that

$$\forall\, \omega \in \Omega\,,\ \forall\, (y_1, \ldots, y_{\omega\tau}) \in Y^{\omega\tau}\,,\ y_1 \ldots y_{\omega\tau}\omega \in Y\,. \tag{1.3}$$

LEMMA 1.8. *Let (X, ω) be a τ-algebra. Then with the order relation $\subseteq$ of set-theoretical containment, the set $\mathrm{Sb}(X, \Omega)$ of subalgebras of (X, Ω) forms a complete lattice.*

PROOF. Let J be a subset of $\mathrm{Sb}(X, \Omega)$. The set-theoretic intersection

$$\bigcap\{Y \mid Y \in J\}$$

is the greatest lower bound $\prod J$ of J in the poset $(\mathrm{Sb}(X, \Omega), \subseteq)$. $\square$

DEFINITION 1.9. Let S be a subset of a τ-algebra (X, Ω). Then the intersection

$$\bigcap\{Y \in \mathrm{Sb}(X, \Omega) \mid S \subseteq Y\}$$

is the *subalgebra* $\langle S\rangle$ of (X, Ω) *generated* by the subset S.

PROPOSITION 1.10. *Let Ω^* be the free monoid on the alphabet Ω. Define the structure (Ω^*, Ω) of a τ-algebra on Ω^* with the operation*

$$\omega\colon (\Omega^*)^{\omega\tau} \to \Omega^*; (a_1, \ldots, a_{\omega\tau}) \mapsto a_1 \ldots a_{\omega\tau}\omega$$

for each operator ω in Ω. Then the subalgebra $I_T = \langle \Omega_0\rangle$ of (Ω^*, Ω) generated by the set Ω_0 of nullary operators is an initial T-algebra.

PROOF. Let (X, Ω) be a τ-algebra. For each nullary operator ω, let x_ω be the element of X selected by the nullary operation $\omega\colon X^0 \to X$. A unique homomorphism $f\colon I_T \to X$ is defined by induction on the lengths of the words in I_T. For words of length 1, the homomorphism property forces

$$f\colon \Omega_0 \to X; \omega \mapsto x_\omega\,.$$

Longer words from I_T end in an element ω of Ω, and then

$$f\colon a_1 \ldots a_{\omega\tau}\omega \mapsto a_1 f \ldots a_{\omega\tau} f\omega$$

is the inductive step in the construction of the unique homomorphism $f\colon I_T \to (X, \Omega)$. $\square$

Corollary 1.11. *Let S be a set. Let $S+T$ be the polynomial functor*

$$S+T\colon \mathbf{Set} \to \mathbf{Set}; X \mapsto (S+\Omega_0) + \sum_{0<n\in\mathbb{N}} X^n \times \Omega_n\,.$$

Then the initial algebra I_{S+T} is the free T-algebra over S in ${}^T\mathbf{Set}$.

Proof. Let $f\colon S \to X$ be a function from S to the underlying set X of a τ-algebra (X, Ω). Construe X as an $(S+T)$-algebra by defining nullary operations $s\colon X^0 \to X$ with singleton image $\{sf\}$ for each element s of S. Then the $(S+T)$-homomorphism $f\colon I_{S+T} \to X$ defined by Proposition 1.10 is the unique T-homomorphism $f\colon I_{S+T} \to X$ extending $f\colon S \to X$. $\square$

Corollary 1.12. *Let $T\colon \mathbf{Set} \to \mathbf{Set}$ be a polynomial endofunctor. Then the canonical forgetful functor*

$$U_T\colon {}^T\mathbf{Set} \to \mathbf{Set}$$

of Definition 1.3(e) has a left adjoint.

2. Coalgebras

2.1. Endofunctors and their coalgebras. Coalgebras are dual to algebras. Recall the format $\alpha_A\colon AT \to A$ for the structure map of an algebra.

Definition 2.1. Let T be an endofunctor on a category $\mathbf{C}$.

(a) A T-*coalgebra* is an object A of $\mathbf{C}$ equipped with a $\mathbf{C}$-morphism α or $\alpha_A\colon A \to AT$ known as the *structure map*.

(b) A T-*coalgebra morphism* between T-coalgebras $\alpha_A\colon A \to AT$ and $\alpha_B\colon B \to BT$ in $\mathbf{C}$ is a $\mathbf{C}$-morphism $f\colon A \to B$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\alpha_A} & AT \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle fT} \\ B & \xrightarrow[\alpha_B]{} & BT \end{array}$$

commutes.

(c) The category of T-coalgebras and morphisms is written as ${}_T\mathbf{C}$.
(d) A terminal object F of ${}_T\mathbf{C}$ is known as a *final T-coalgebra*.
(e) The *canonical forgetful functor* $U_T\colon {}_T\mathbf{C} \to \mathbf{C}$ sends an object $\alpha_A\colon A \to AT$ to A.

Intuitively, while algebras describe how a collection of objects may be combined to make a new object, coalgebras describe how a single object breaks up into component parts.

2.1.1. *Examples.*

EXAMPLE 2.2 (Comultiplication). On the category of abelian groups, consider the tensor square endofunctor $T\colon \underline{\underline{\mathbb{Z}}} \to \underline{\underline{\mathbb{Z}}}; A \to A \otimes A$ of Example 1.6. Consider the ring $\mathbb{Z}[X]$ of polynomials over $\mathbb{Z}$ in a single indeterminate X. For each natural number n, define

$$\Delta\colon X^n \mapsto \sum_{r=0}^{n} X^r \otimes X^{n-r}\,. \tag{2.1}$$

Note how the individual primitive elements being summed on the right hand side of (2.1) represent the various factorizations of the power X^n as a product of two powers X^r and X^{n-r}. Now since $\mathbb{Z}[X]$ is a free $\mathbb{Z}$-module over the set $\{X^n \mid n \in \mathbb{N}\}$, there is a unique extension of the assignments (2.1) to an abelian group homomorphism

$$\Delta\colon \mathbb{Z}[X] \to \mathbb{Z}[X] \otimes \mathbb{Z}[X]$$

known as a *comultiplication*. Then $\Delta\colon \mathbb{Z}[X] \to \mathbb{Z}[X]T$ is the structure map of a T-coalgebra.

EXAMPLE 2.3 (Deterministic automata). Let S be a set. Consider the endofunctor

$$T\colon \mathbf{Set} \to \mathbf{Set}; X \mapsto X^S$$

on the category of sets. Note that this endofunctor is polynomial if and only if S is finite. Let

$$\alpha_A\colon A \to A^S$$

be a T-coalgebra. Dually to Example 1.4(a), consider A as the state space of an automaton. Then for each state a, the image $a\alpha_A$ of a under the structure map α_A is the function

$$a\alpha_A\colon S \to A; s \mapsto as$$

sending each elementary event s from S to the effect as that it has on the given state a.

EXAMPLE 2.4 (Probabilistic automata). Let S be a set. Example 2.3 showed how a deterministic automaton may be modeled by a coalgebra. There, if the automaton, in state a, was subject to elementary event s from S, then the automaton moved deterministically to a new state as. Now for a set X, let $X\Pi$ denote the set of finitely supported probability distributions on X. Consider the (nonpolynomial) endofunctor

$$T\colon \mathbf{Set} \to \mathbf{Set}; X \mapsto X\Pi^S$$

on the category of sets. Let

$$\alpha_A\colon A \to A\Pi^S$$

be a T-coalgebra. As in Example 2.3, one may again consider A as the state space of an automaton. However, this time the automaton is probabilistic. For each state a, the image $a\alpha_A$ of a under the structure map α_A is the function

$$a\alpha_A\colon S \to A\Pi; s \mapsto p_s$$

sending each elementary event s from S to the probability distribution p_s on A for the effect of s on a.

EXAMPLE 2.5 (Finite Markov chains). If $|S| = 1$ and $0 < |A| < \infty$ in Example 2.4, then a T-coalgebra

$$\alpha_A\colon A \to A\Pi^S$$

is a *finite Markov chainMarkov chain*. For each element a of A, the probability distribution $a\alpha_A$ on A may be described by a row vector. The $|A|$ row vectors together constitute a square row-stochastic matrix of degree $|A|$ that specifies the Markov chain (compare Chapter 1, Definition 2.8).

2.2. Graphs and homomorphisms. For a set X, let $X\mathcal{P}$ denote the set of subsets of X. For a function $f\colon X \to Y$, define

$$f\mathcal{P}\colon X\mathcal{P} \to Y\mathcal{P}; S \mapsto Sf\,.$$

Then $\mathcal{P}\colon \mathbf{Set} \to \mathbf{Set}$ is a functor, the *covariant power set functor* (Exercise 6).

Let (V,E) be an undirected graph (compare Chapter 6, §1.1.1). For a vertex u, the set

$$u^E = \{v \in V \mid (u,v) \in E\}$$

is the *neighborhood* of u. The graph (V,E) determines a $\mathcal{P}$-coalgebra V whose structure map

$$\alpha_V \colon V \to V\mathcal{P}; u \mapsto u^E \tag{2.2}$$

sends a vertex to its neighborhood. Conversely, the structure map (2.2) determines the graph structure on the set V, since one has

$$(u,v) \in E \quad \text{if and only if} \quad v \in u\alpha_V$$

for a pair u, v of vertices.

2.2.1. *Coalgebra homomorphisms of graphs.* Let (V,E) and (W,F) be graphs, with $\mathcal{P}$-coalgebras $\alpha_V \colon V \to V\mathcal{P}$ and $\alpha_W \colon W \to W\mathcal{P}$. Consider a function $f \colon V \to W$. Then f is a $\mathcal{P}$-coalgebra homomorphism if and only if the diagram

$$\begin{tikzcd} V \arrow[r, "\alpha_V"] \arrow[d, "f"'] & V\mathcal{P} \arrow[d, "f\mathcal{P}"] \\ W \arrow[r, "\alpha_W"'] & W\mathcal{P} \end{tikzcd} \tag{2.3}$$

commutes. Thus for all vertices v of V, one has

$$v^E f = v f^F .$$

This equation means two things:

(1) Each edge $v \,\text{—}\, v'$ of (V,E) is mapped under f to an edge $vf \,\text{—}\, v'f$ of (W,F);
(2) For a vertex vf in the subset Vf of W, each edge $vf \,\text{—}\, w$ in (W,F) is the image $vf \,\text{—}\, v'f$ of an edge $v \,\text{—}\, v'$ of (V,E).

However, in graph theory, a function $f \colon V \to W$ is said to be a *graph homomorphism* if and only if just the first of these two conditions is satisfied. In other words, the coalgebra homomorphism condition (2.3) is too strong for graph theory applications. (See Exercises 10, 11 for coalgebraic characterizations of graph homomorphisms.)

2.3. Final coalgebras. The following result is the *Lambek Lemma*. (Compare Exercise 5 for the dual, algebraic version.)

THEOREM 2.6. *Let $T\colon \mathbf{C} \to \mathbf{C}$ be an endofunctor. Let $\alpha_F\colon T \to FT$ be a final coalgebra. Then the structure map α_F is an isomorphism.*

PROOF. Consider the following commutative diagram:

$$\begin{tikzcd}
F \arrow[rrr, "\alpha_F"] \arrow[dr, "\alpha_F"] \arrow[dd, "1_F"'] & & & FT \arrow[dl, "\alpha_F T"'] \arrow[dd, "1_{FT}"] \\
& FT \arrow[r, "\alpha_F T"] \arrow[dl, "k"'] \arrow[drr, dashed, "1_{FT}"'] & FTT \arrow[dr, "kT"] & \\
F \arrow[rrr, "\alpha_F"'] & & & FT
\end{tikzcd}$$

- The commuting of the upper rhombus is trivial.
- The commuting of the lower rhombus expresses the fact that there is a unique T-coalgebra homomorphism $k\colon FT \to F$ to the final algebra F from the algebra FT (whose structure map is the image $\alpha_F T$ of α_F under F.
- The commuting of the left-hand and right-hand triangles follows from the fact that 1_F is the unique T-coalgebra morphism from F to the final coalgebra F.
- The commuting triangle above the dotted arrow is a reflection (in kT) of the right-hand triangle.

The commuting of the left-hand triangle yields $\alpha_F k = 1_F$, while the commuting of the triangle below the dotted arrow yields $k\alpha_F = 1_{FT}$. Thus the structure map α_F, having k as a two-sided inverse, is an isomorphism. $\square$

COROLLARY 2.7. *For the covariant power set functor $\mathcal{P}\colon \mathbf{Set} \to \mathbf{Set}$ of §2.2, there is no final $\mathcal{P}$-coalgebra.*

PROOF. No set is isomorphic to its power set. (Compare Exercise 12.) $\square$

2.3.1. *An existence theorem for final coalgebras.*

THEOREM 2.8. *Let $T\colon \mathbf{C} \to \mathbf{C}$ be an endofunctor on a category $\mathbf{C}$ with a terminal object E. Let $L\colon (\mathbb{N}, \geq) \to \mathbf{C}$ be the functor with* *image*

$$E \xleftarrow{j} ET \xleftarrow{jT} ET^2 \xleftarrow{jT^2} ET^3 \xleftarrow{jT^3} \dots \tag{2.4}$$

in $\mathbf{C}$*, where* $j\colon ET \to E$ *is the unique morphism from* ET *to the terminal object* E *in* $\mathbf{C}$*. If the limit* $\varprojlim L$ *of* L *exists in* $\mathbf{C}$*, and is preserved by* T*, then* $\varprojlim L$ *carries the structure of a final* T*-coalgebra.*

Proof. The image of the functor $LT\colon (\mathbb{N}, \geq) \to \mathbf{C}$ consists of all but the leftmost arrow of (2.4). However, that leftmost arrow is just the unique morphism to the terminal object E of $\mathbf{C}$. Thus $\varprojlim L \cong \varprojlim(LT)$. On the other hand, $\varprojlim(LT) \cong (\varprojlim L)T$, since the limit $\varprojlim L$ of L is preserved by T. Thus $\varprojlim L \cong (\varprojlim L)T$: There is an isomorphism $\alpha_{\varprojlim L}\colon \varprojlim L \to (\varprojlim L)T$ giving the structure map of a T-coalgebra. This T-coalgebra will be shown to be final.

Let $\alpha_X\colon X \to XT$ be a T-coalgebra. Since E is terminal in $\mathbf{C}$, there is a unique $\mathbf{C}$-morphism $k\colon X \to E$. Consider the following commutative diagram:

$$\begin{tikzcd}
X \arrow[r, "\alpha_X"] \arrow[d, "k"'] & XT \arrow[r, "\alpha_X T"] \arrow[d, "kT"'] & XT^2 \arrow[r, "\alpha_X T^2"] \arrow[d, "kT^2"'] & XT^3 \arrow[r, "\alpha_X T^3"] \arrow[d, "kT^3"'] & \dots \\
E & ET \arrow[l, "j"] & ET^2 \arrow[l, "jT"] & ET^3 \arrow[l, "jT^2"] & \dots \arrow[l, "jT^3"]
\end{tikzcd} \tag{2.5}$$

The left-hand square commutes because its paths end at the terminal object E. Subsequent squares commute because they are the successive images of commuting squares under the functor T.

A natural transformation τ in the functor category morphism class $\mathbf{C}^{(\mathbb{N},\geq)}\big([X], L\big)$ is defined by components

$$\tau_n = \alpha_X \alpha_X^T \alpha_X^{T^2} \dots \alpha_X^{T^{n-1}} k^{T^n}$$

for natural numbers n, the paths from X to ET^n in (2.5). Naturality is guaranteed by the commuting of (2.5). Since the limit of L exists, there is an isomorphism

$$\mathbf{C}^{(\mathbb{N},\geq)}\big([X], L\big) \cong \mathbf{C}(X, \varprojlim L)$$

(recall Chapter 12, Corollary 1.9). Suppose thet $t\colon X \to \varprojlim L$ is the $\mathbf{C}$-morphism corresponding to τ under this isomorphism. The

C-morphism t is the unique T-coalgebra morphism from X to $\varprojlim L$ (Exercise 14). $\square$

REMARK 2.9. If **C** in Theorem 2.8 is the category of sets, then $\varprojlim L$ is constructed by a set of sequences, in analogy with the set (2.5) of sequences that constructed the p-adic integers in Chapter 11.

3. Exercises

(1) If $\mathbf{C} = \mathbf{Set}$ in Remark 1.2, show that

$$|\tau^{-1}\{n\}|X^n \cong \tau^{-1}\{n\} \times X^n \,.$$

(2) Consider the endofunctor

$$T\colon \underline{\underline{\mathbb{Z}}} \to \underline{\underline{\mathbb{Z}}}; A \to (A \otimes A) \oplus \mathbb{Z}$$

on the category of abelian groups. Present a structure map $\alpha\colon AT \to A$ that encodes the structure of a unital ring A.

(3) Let S be a commutative ring. Consider the endofunctor

$$T\colon \underline{\underline{\mathbb{Z}}} \to \underline{\underline{\mathbb{Z}}}; A \to A \otimes S$$

on the category of abelian groups. Taking the analogy provided by Example 1.4, show how to construe S-modules as T-algebras.

(4) If X is a set, define $X\Lambda^2$ to be the set of two-element subsets of X.
   (a) Show how to extend Λ^2 to a functor

$$T\colon \mathbf{Set} \to \mathbf{Set}; X \mapsto X + X\Lambda^2 \,.$$

   (b) Explain how to interpret a T-algebra $\alpha_A\colon AT \to A$ as a commutative magma.

(5) Let $T\colon \mathbf{C} \to \mathbf{C}$ be an endofunctor. Let $\alpha_I\colon IT \to I$ be an initial algebra. Show that α_I is an isomorphism. [This result is known as the *Lambek Lemma*.]

(6) In §2.2, verify that $\mathcal{P}$ forms a functor.

(7) Show that $\mathcal{P}$-coalgebras $\alpha_X\colon X \to X\mathcal{P}$ are equivalent to sets X with a binary relation $R \subseteq X \times X$.

(8) Suppose that $\alpha_A\colon A \to A\mathcal{P}$ is a $\mathcal{P}$-coalgebra. Explain how to interpret the coalgebra α_A as a *non-deterministic dynamical system*, in which a state may transition to any one of a number of states at each discrete time step.

(9) Let $\alpha_V \colon V \to V\mathcal{P}$ be a $\mathcal{P}$-coalgebra. Under what conditions does α_V become the structure map (2.2) of a graph structure (V, E) on V?

(10) Let $\alpha_V \colon V \to V\mathcal{P}$ and $\alpha_W \colon W \to W\mathcal{P}$ be $\mathcal{P}$-coalgebras. Define a function $f \colon V \to W$ to be a *lower $\mathcal{P}$-morphism* if

$$\forall\ v \in V\ ,\ v\alpha_V f^{\mathcal{P}} \subseteq vf\alpha_W\ .$$

(a) Confirm that each $\mathcal{P}$-coalgebra morphism $f \colon V \to W$ is a lower $\mathcal{P}$-morphism.

(b) If $\alpha_V \colon V \to V\mathcal{P}$ and $\alpha_W \colon W \to W\mathcal{P}$ are $\mathcal{P}$-coalgebras given by graphs (V, E) and (W, F), show that a function $f \colon V \to W$ is a graph homomorphism if and only if it is a lower $\mathcal{P}$-morphism.

[See [**3**] for further details.]

(11) Consider the category $\mathbf{Set}^{\underline{2}}$ (compare Chapter 11, Example 1.3). Define a functor

$$G \colon \mathbf{Set}^{\underline{2}} \to \mathbf{Set}^{\underline{2}}; (V, E) \mapsto (\top, V \times V)$$

with the terminal object $\top$ of $\mathbf{Set}$ as the singleton $\{\varnothing\}$.

(a) If (V, E) is a graph, consider the projections

$$\pi_i \colon E \to V; (v_0, v_1) \mapsto v_i$$

for $i = 0, 1$. Show that the entire graph structure (V, E) is encoded by the structure map

$$\alpha_{(V,E)} \colon (V, E) \to (V, E)G; (v, e) \mapsto \big(\varnothing, (e\pi_0, e\pi_1)\big)$$

of a G-coalgebra.

(b) Suppose that (V, E) and (W, F) are graphs, determining corresponding G-coalgebras $\alpha_{(V,E)} \colon (V, E) \to (V, E)G$ and $\alpha_{(W,F)} \colon (W, F) \to (W, F)G$. Consider a given ($\mathbf{Set}^{\underline{2}}$)-morphism $(f, g) \colon (V, E) \to (W, F)$. Show that (f, g) is a G-coalgebra homomorphism if and only if $e\pi_i f = eg\pi_i$ for $e \in E$ and $i = 0, 1$.

[This approach is attributed to Andrea Corradini [**8**].]

(12) Suppose that there is a surjection $f \colon A \to 2^A$ from a set A to its power set. Consider the subset

$$B = \{x \in A \mid x \notin xf\}$$

of A, and an element b of A with $B = bf$.

(a) Show $b \in B\ \Rightarrow b \notin B$.

   (b) Show $b \notin B \Rightarrow b \in B$.
   (c) Conclude that there is no surjection $f: A \to 2^A$.
   (d) Prove the inequality $n < 2^n$ for each natural number n.

(13) Suppose that S is a set with at least two elements. Consider the functor

$$T: \mathbf{Set} \to \mathbf{Set}; X \mapsto X^S$$

of Example 2.3. Show that a final T-coalgebra structure cannot be sustained on a finite set with more than one element.

(14) Complete the proof of Theorem 2.8 by verifying the final claim.

(15) Dualize Theorem 2.8 to obtain a sufficient condition for the existence of initial algebras.

CHAPTER 14

Hopf algebras

1. Bialgebras

1.1. Algebras and coalgebras over a ring. Let R be a commutative, unital ring. For an R-module Z, there are isomorphisms

$$\lambda_Z \colon Z \otimes R \to Z; z \otimes r \mapsto zr$$

and

$$\rho_Z \colon R \otimes Z \to Z; r \otimes z \mapsto zr$$

(compare §1.3 and Exercise 8 in Chapter 12). For a second S-module Y, there is an isomorphism τ or

$$\tau_{Y,Z} \colon Y \otimes Z \to Z \otimes Y; y \otimes z \mapsto z \otimes y$$

known as the *twist*.

Definition 1.1. Let R be a commutative, unital ring.

(a) An *R-algebra* is an R-module A with a *multiplication* ∇_A or $\nabla \colon A \otimes A \to A$ and a *unit* η_A or $\eta \colon R \to A; 1 \mapsto 1_A$ that are R-module homomorphisms such that the diagrams

$$(1.1) \qquad \begin{tikzcd} A \otimes A \otimes A \arrow[r, "1_A \otimes \nabla"] \arrow[d, "\nabla \otimes 1_A"'] & A \otimes A \arrow[d, "\nabla"] \\ A \otimes A \arrow[r, "\nabla"'] & A \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \otimes A \arrow[dr, "\nabla"] & A \otimes R \arrow[l, "1_A \otimes \eta"'] \arrow[d, "\lambda_A"] \\ R \otimes A \arrow[u, "\eta \otimes 1_A"] \arrow[r, "\rho_A"'] & A \end{tikzcd}$$

commute.

(b) Dually, an *R-coalgebra* is an R-module C that is equipped with a *comultiplication* Δ_C or $\Delta \colon C \to C \otimes C$ and a *counit* ε_C or $\varepsilon \colon C \to R$ that are R-module homomorphisms such that the diagrams

$$
\begin{tikzcd}
C \otimes C \otimes C & C \otimes C \arrow[l, "1_C \otimes \Delta"'] \\
C \otimes C \arrow[u, "\Delta \otimes 1_C"] & C \arrow[l, "\Delta"] \arrow[u, "\Delta"']
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
C \otimes C \arrow[r, "1_A \otimes \varepsilon"] \arrow[d, "\varepsilon \otimes 1_C"'] & C \otimes R \\
R \otimes C & C \arrow[l, "\rho_C^{-1}"] \arrow[u, "\lambda_C^{-1}"'] \arrow[ul, "\Delta"']
\end{tikzcd}
\tag{1.2}
$$

commute. The left-hand diagram in (1.2) is said to express *coassociativity*, while the right-hand diagram is described as expressing *counitality*.

(c) An R-algebra A is *commutative* if the diagram

$$
\begin{tikzcd}
A \otimes A \arrow[rr, "\tau"] \arrow[dr, "\nabla"'] & & A \otimes A \arrow[dl, "\nabla"] \\
& A &
\end{tikzcd}
$$

commutes.

(c) Dually, an R-coalgebra C is *cocommutative* if the diagram

$$
\begin{tikzcd}
C \otimes C & & C \otimes C \arrow[ll, "\tau"'] \\
& C \arrow[ul, "\Delta"] \arrow[ur, "\Delta"'] &
\end{tikzcd}
$$

commutes.

1.1.1. *Examples.*

Example 1.2. The polynomial ring $\mathbb{Z}[X]$ in a single indeterminate X has a comultiplication given by

$$\Delta\colon X^n \mapsto \sum_{r=0}^{n} X^r \otimes X^{n-r}$$

(compare Chapter 13, Example 2.2). Together with the counit

$$\varepsilon\colon \mathbb{Z}[X] \to \mathbb{Z}; p(X) \mapsto p(0)\,,$$

$\mathbb{Z}[X]$ forms a cocommutative $\mathbb{Z}$-coalgebra (Exercise 3). Dually, under the tensorized version

$$\nabla\colon \mathbb{Z}[X] \otimes \mathbb{Z}[X] \to \mathbb{Z}[X]; p(X) \otimes q(X) \mapsto p(X)q(X)$$

of the usual multiplication, and with the unit given by the insertion

$$\eta\colon \mathbb{Z} \to \mathbb{Z}[X]\colon n \mapsto n$$

of integers as constant polynomials, $\mathbb{Z}[X]$ also forms a commutative $\mathbb{Z}$-algebra.

EXAMPLE 1.3. Let R be a commutative, unital ring. Let RX be the free R-module on the set X (compare Chapter 7, §2.2.1). Under the *grouplike* comultiplication Δ or

$$\Delta_{RX} \colon RX \to RX \otimes RX; x \mapsto x \otimes x \tag{1.3}$$

for x in X, and with the counit

$$\varepsilon \colon RX \to R; x \mapsto 1\,,$$

RX forms a cocommutative R-coalgebra that is known as the *grouplike R-coalgebra* on the set X (Exercise 5).

1.1.2. *Homomorphisms.*

DEFINITION 1.4. Let R be a commutative ring.

(a) An R-module homomorphism $f \colon A \to B$ between R-algebras A and B is a *homomorphism* if the diagrams

$$\begin{tikzcd} A \arrow[d, "f"'] & A \otimes A \arrow[l, "\nabla_A"'] \arrow[d, "f\otimes f"] \\ B & B \otimes B \arrow[l, "\nabla_B"] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \arrow[d, "f"'] & R \arrow[l, "\eta_A"'] \arrow[d, "1_R"] \\ B & R \arrow[l, "\eta_B"] \end{tikzcd}$$

commute.

(b) The *kernel* $\operatorname{Ker} f$ of an R-algebra homomorphism $f \colon A \to B$ is the group or module kernel $f^{-1}\{0_B\}$.

(c) An R-module homomorphism $f \colon D \to C$ between R-coalgebras D and C is a *homomorphism* if the diagrams

$$\begin{tikzcd} C \arrow[r, "\Delta_C"] & C \otimes C \\ D \arrow[u, "f"] \arrow[r, "\Delta_D"'] & D \otimes D \arrow[u, "f\otimes f"'] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} C \arrow[r, "\varepsilon_C"] & R \\ D \arrow[u, "f"] \arrow[r, "\varepsilon_D"'] & R \arrow[u, "1_R"'] \end{tikzcd}$$

commute.

(d) Let $f \colon D \to C$ be an R-coalgebra homomorphism. Then the *kernel* $\operatorname{Ker} f$ is the group or module kernel $f^{-1}\{0_C\}$.

The formulation and proof of the (standard) First Isomorphism Theorem for R-algebras are relegated to Exercise 7. The formulation may make use of the following.

DEFINITION 1.5. Let J be an R-submodule of an R-algebra A.

(a) J is a *left ideal* if $(A \otimes J)\nabla_A \subseteq J$.
(b) J is a *right ideal* if $(J \otimes A)\nabla_A \subseteq J$.
(c) J is an *ideal* if $(J \otimes A + A \otimes J)\nabla_A \subseteq J$.

1.1.3. *Coideals.*

DEFINITION 1.6. Let K be an R-submodule of an R-coalgebra D.

(a) K is a *left coideal* if $K\Delta_D \subseteq D \otimes K$.
(b) K is a *right coideal* if $K\Delta_D \subseteq K \otimes D$.
(c) K is a *coideal* if $K\varepsilon_D = \{0\}$ and $K\Delta_D \subseteq K \otimes D + D \otimes K$.

PROPOSITION 1.7. *Let R be a commutative, unital ring. Let $f : D \to C$ be an R-coalgebra homomorphism. Then*

$$\mathrm{Ker}(f \otimes f) = (\mathrm{Ker}\, f) \otimes D + D \otimes (\mathrm{Ker}\, f) \tag{1.4}$$

if R is a field or if f is surjective.

For a proof of Proposition 1.7 in the case where R is a field, see Exercise 8.

COROLLARY 1.8. *Let R be a commutative, unital ring, and let K be the kernel of an R-coalgebra homomorphism $f : D \to C$.*

(a) *If f is surjective, then K is a coideal of D.*
(b) *If R is a field, then K is a coideal of D.*

REMARK 1.9. In general, the kernel of a coalgebra homomorphism need not form a coideal. (Compare Exercise 10.)

PROPOSITION 1.10. *Let K be a coideal of a coalgebra D. Then the quotient module D/K inherits a coalgebra structure within which the specifications*

$$(d+K)\Delta_{D/K} = d\Delta_D + (K \otimes D + D \otimes K) \quad \textit{and} \quad (d+K)\varepsilon_{D/K} = d\varepsilon_D$$

are well-defined.

1.1.4. *Tensor products.* Tensor products of R-algebras form R-algebras. Dually, tensor products of R-coalgebras form R-coalgebras.

DEFINITION 1.11. Let R be a commutative, unital ring.

(a) Given R-algebras A and B, the following composite

$$A \otimes B \otimes A \otimes B \xrightarrow{1_A \otimes \tau_{B,A} \otimes 1_B} A \otimes A \otimes B \otimes B \xrightarrow{\nabla_A \otimes \nabla_B} A \otimes B$$

defines a *tensor product multiplication* $\nabla_{A \otimes B}$.

(b) Given R-algebras A and B, the composite

$$R \xrightarrow{\Delta_R} R \otimes R \xrightarrow{\eta_A \otimes \eta_B} A \otimes B\,,$$

where the first map is given by the grouplike comultiplication (1.3) for R free on $\{1\}$, defines a *tensor product unit* $\eta_{A\otimes B}$.

(c) For R-coalgebras C and D, the composite

$$C \otimes D \otimes C \otimes D \xleftarrow{1_C \otimes \tau_{C,D} \otimes 1_D} C \otimes C \otimes D \otimes D \xleftarrow{\Delta_C \otimes \Delta_D} C \otimes D$$

defines a *tensor product comultiplication* $\Delta_{C\otimes D}$.

(d) For R-coalgebras C and D, the composite

$$R \xleftarrow{\nabla_R} R \otimes R \xleftarrow{\varepsilon_C \otimes \varepsilon_D} C \otimes D\,,$$

where the left hand map is given by the multiplication λ_R on the commutative ring R, defines a *tensor product counit* $\varepsilon_{C\otimes D}$.

Proposition 1.12. (a) *The tensor product of two R-algebras is an R-algebra.*

(b) *The tensor product of two R-coalgebras is an R-coalgebra.*

1.2. Bialgebras. The appearance of the grouplike comultiplication Δ_R in Definition 1.11(b) for tensor product algebras, and the regular multiplication ∇_R in Definition 1.11(d) for tensor product coalgebras, suggests that R-algebras and R-coalgebras are intimately related. The following result gives further confirmation.

Proposition 1.13. *Let R be a commutative, unital ring (R, ∇_R, η_R). Take R as the grouplike coalgebra over the set $\{1\}$. Let B be both an R-algebra and an R-coalgebra. Then the following conditions are equivalent:*

(a) *The comultiplication $\Delta_B \colon B \to B \otimes B$ and counit $\varepsilon_B \colon B \to R$ are R-algebra homomorphisms;*

(b) *The multiplication $\nabla_B \colon B \otimes B \to B$ and unit $\eta_B \colon R \to B$ are R-coalgebra homomorphisms;*

(c) *The diagram*

$$
\begin{tikzcd}
R \otimes R \arrow[r, "\nabla"] & R & & R \arrow[ll, "1_R"'] \arrow[dl, "\eta"] \arrow[r, "\Delta"] & R \otimes R \arrow[d, "\eta\otimes\eta"] \\
B \otimes B \arrow[u, "\varepsilon\otimes\varepsilon"] \arrow[rr, "\nabla"] \arrow[d, "\Delta\otimes\Delta"'] \arrow[ddrrrr, dashed] & & B \arrow[ul, "\varepsilon"] \arrow[rr, "\Delta"] & & B \otimes B \\
B \otimes B \otimes B \otimes B \arrow[rrrr, "1_B\otimes\tau\otimes 1_B"'] \arrow[urrrr, dashed] & & & & B \otimes B \otimes B \otimes B \arrow[u, "\nabla\otimes\nabla"']
\end{tikzcd}
$$

commutes.

Remark 1.14. For the proof of Proposition 1.13, see Exercise 13. As a hint, the dotted arrows in the diagram of Proposition 1.13(c) indicate the comultiplication and multiplication on the tensor square $B \otimes B$.

Definition 1.15. An R-algebra and coalgebra B that satisfies the equivalent conditions of Proposition 1.13 is known as an R-*bialgebra*. Module homomorphisms between bialgebras are described as *bialgebra homomorphisms* if they are simultaneously R-algebra and coalgebra homomorphisms.

Definition 1.16. A submodule J of a bialgebra B is a *bi-ideal* if it is both an ideal and a coideal.

Proposition 1.17. *If J is a bi-ideal of a bialgebra B, then the quotient B/J carries a natural bialgebra structure that makes the projection $p\colon B \to B/J$ a bialgebra homomorphism.*

2. Hopf algebras

2.1. Antipodes.

2.1.1. *Convolution algebras.* Let R be a commutative, unital ring, with category $\underline{\underline{R}}$ of R-modules. Suppose that A is an R-algebra and C is an R-coalgebra. Consider the set $\underline{\underline{R}}(C, A)$ of R-module homomorphisms from C to A.

Definition 2.1. For f, g in $\underline{\underline{R}}(C, A)$, the composite

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{f\otimes g} A \otimes A \xrightarrow{\nabla} A$$

is called the *convolution product* $f * g\colon C \to A$ of f and g.

Proposition 2.2. *Under the convolution product, the set* $\underline{\underline{R}}(C, A)$ *forms a monoid*

$$\left(\underline{\underline{R}}(C, A), *, \varepsilon_C \eta_A\right)$$

with $\varepsilon_C \eta_A \colon C \to A$ *as identity element.*

Corollary 2.3. *If* B *is a bialgebra, the endomorphism ring* $\mathrm{End}_R B$ *of the* R*-module* B *is a monoid*

$$(\mathrm{End}_R B, *, \varepsilon_B \eta_B)$$

under the convolution product.

2.1.2. *Antipodes.*

Definition 2.4. Let B be an R-bialgebra. Then an *antipode* for B is defined as an inverse $S \colon B \to B$ to id_B in the convolution monoid $(\mathrm{End}_R B, *, \varepsilon_B \eta_B)$.

The uniqueness of inverses in monoids shows that if an antipode exists, then it is unique.

Proposition 2.5. *Let* R *be a commutative, unital ring. Let* B *be an* R*-bialgebra. Then* $S \colon B \to B$ *is an antipode if and only if the diagram*

$$\begin{tikzcd}
 & B \otimes B \arrow[rr, "S\otimes 1_B"] & & B \otimes B \arrow[dr, "\nabla"] & \\
B \arrow[ur, "\Delta"] \arrow[rr, "\varepsilon_B"] \arrow[dr, "\Delta"'] & & R \arrow[rr, "\eta_B"'] & & B \\
 & B \otimes B \arrow[rr, "1_B\otimes S"'] & & B \otimes B \arrow[ur, "\nabla"'] &
\end{tikzcd}$$

commutes.

Proof. Commuting of the upper pentagon in the diagram is equivalent to S being a left inverse for 1_B or id_B under the convolution product. Dually, commuting of the lower pentagon in the diagram is equivalent to S being a right inverse. $\square$

2.2. Hopf algebras.

2.2.1. *Basic definitions.*

DEFINITION 2.6. Let R be a commutative, unital ring. Then a *Hopf algebra* (over R) is an R-bialgebra with an antipode S.

DEFINITION 2.7. A Hopf algebra is said to be *commutative* if its algebra is commutative, and *cocommutative* if its coalgebra is cocommutative.

Just as each semigroup homomorphism between groups is a group homomorphism[1], it transpires that bialgebra homomorphisms between Hopf algebras preserve the additional antipode structure.

PROPOSITION 2.8. *Let $f\colon H \to K$ be a bialgebra morphism between Hopf algebras*

$$(H, \nabla_H, \Delta_H, \eta_H, \varepsilon_H, S_H)$$

and

$$(K, \nabla_K, \Delta_K, \eta_K, \varepsilon_K, S_K)\,.$$

Then $\begin{tikzcd} H \arrow[r, "S_H"] \arrow[d, "f"'] & H \arrow[d, "f"] \\ K \arrow[r, "S_K"'] & K \end{tikzcd}$ *commutes.*

PROOF. Consider the maps

$$\underline{\underline{R}}(H,H) \to \underline{\underline{R}}(H,K); g \mapsto gf \tag{2.1}$$

and

$$\underline{\underline{R}}(K,K) \to \underline{\underline{R}}(H,K); h \mapsto fh\,. \tag{2.2}$$

These are convolution monoid homomorphisms (Exercise 16). Then

$$\begin{aligned}(S_H f)*f &= (S_H f) * (\mathrm{id}_H f) = (S_H * \mathrm{id}_H)f = (\varepsilon_H \eta_H)f = \varepsilon_H \eta_K \\ &= f(\varepsilon_K \eta_K) = f(\mathrm{id}_K * S_K) = (f\mathrm{id}_K) * (fS_K) = f * (fS_K)\,,\end{aligned}$$

so the left inverse $S_H f$ of f equals the right inverse fS_K of f in the convolution monoid $\big(\underline{\underline{R}}(H,K), *, \varepsilon_H\eta_K\big)$. □

DEFINITION 2.9. A bialgebra homomorphism between Hopf algebras is called a *Hopf algebra homomorphism*. Bijective Hopf algebra homomorphisms are *Hopf algebra isomorphisms*.

[1]Compare Chapter 3, Lemma 1.3

The following useful result is stated without proof.

PROPOSITION 2.10. *For a Hopf algebra* $(H, \nabla_H, \Delta_H, \eta_H, \varepsilon_H, S_H)$, *the antipode*

$$S\colon (H, \nabla_H, \Delta_H, \eta_H, \varepsilon_H, S_H) \to (H, \tau\nabla_H, \tau\Delta_H, \eta_H, \varepsilon_H, S_H)$$

is a homomorphism.

2.2.2. *Classical examples.*

EXAMPLE 2.11 (Group algebras). Let G be a finite group. Let $\mathbb{C}G$ be a complex vector space with basis G. Extend the group multiplication $G \times G \to G$ to a bilinear map $m\colon \mathbb{C}G \times \mathbb{C}G \to \mathbb{C}G$, yielding a $\mathbb{C}$-algebra multiplication $\nabla\colon \mathbb{C}G \otimes \mathbb{C}G \to \mathbb{C}G$. Taking $\eta_{\mathbb{C}G}\colon \mathbb{C} \to \mathbb{C}G; 1 \mapsto 1_G$ as the unit, one obtains a $\mathbb{C}$-algebra known as the *complex group algebra* of G. In conjunction with the grouplike coalgebra structure on G, and the antipode $S\colon \mathbb{C}G \to \mathbb{C}G; g \mapsto g^{-1}$, the group algebra $\mathbb{C}G$ forms a cocommutative Hopf algebra.

EXAMPLE 2.12 (Dual group algebras). Let G be a finite group. Let $\mathbb{C}^G$ be the space of complex-valued functions defined on G, with pointwise (commutative) algebra structure. This space is spanned by the functions

$$\delta_g\colon G \to \mathbb{C}; h \mapsto \begin{cases} 1 & \text{if } h = g\,; \\ 0 & \text{otherwise.} \end{cases}$$

With comuliplication $\Delta\colon \delta_g \mapsto \sum_{hk=g} \delta_h \otimes \delta_k$, counit $\varepsilon\colon \delta_h \mapsto 1_G\delta_h$, and antipode $S\colon \delta_g \mapsto \delta_{g^{-1}}$, the *dual group algebra* $\mathbb{C}^G$ forms a commutative Hopf algebra.

EXAMPLE 2.13 (Tensor algebras). Let R be a commutative, unital ring. Let V be the free R-module RX over X. The *tensor algebra* XT over X is the R-algebra

$$XT = \sum_{n \in \mathbb{N}} \overbrace{V \otimes \ldots \otimes V}^{n \text{ factors}} \tag{2.3}$$

with the product (for $x_i, y_j \in X$) given by

$$\nabla\colon (x_1 \otimes \ldots \otimes x_r) \otimes (y_1 \otimes \ldots \otimes y_s) \mapsto x_1 \otimes \ldots \otimes x_r \otimes y_1 \otimes \ldots \otimes y_s$$

and unit $\eta\colon R \hookrightarrow XT$ embedding R as the summand for $n = 0$ in (2.3). Under the specifications

$$\Delta\colon x \mapsto x \otimes 1 + 1 \otimes x\,, \quad \varepsilon\colon x \mapsto 0\,, \quad S\colon x \mapsto -x$$

for $x \in X$, it becomes a cocommutative Hopf algebra.

DEFINITION 2.14. Let x be an element of a Hopf algebra.

(a) x is *grouplike* if $\Delta\colon x \mapsto x \otimes x$ and $x\varepsilon = 1$.
(b) x is *primitive* if $\Delta\colon x \mapsto x \otimes 1 + 1 \otimes x$ (and $x\varepsilon = 0$).

A Hopf algebra is *classical* if it is commutative or cocommutative. All the Hopf algebra examples presented so far are classical.

2.3. A non-classical example. This paragraph will present a class of Hopf algebras, the Taft algebras, which are neither commutative nor cocommutative. Some preparation is needed.

2.3.1. *Quantum combinatorics.* Consider the integral polynomial ring $\mathbb{Z}[X]$ over an indeterminate X. Define the *quantum natural numbers*

$$(n)_X = 1 + X + X^2 + \ldots + X^{n-1}$$

for natural numbers n. Define the *quantum factorials*

$$(0)^!_X = 1$$

and

$$(n)^!_X = (n)_X(n-1)_X \ldots (2)_X(1)_X$$

for positive integers n. Define the *quantum binomial coefficients*

$$\binom{n}{k}_X = \frac{(n)^!_X}{(n-k)^!_X(k)^!_X}$$

for $0 \leq k \leq n \in \mathbb{N}$.

PROPOSITION 2.15. *The quantum binomial coefficients lie in* $\mathbb{Z}[X]$.

PROOF. The result follows by induction on n, with *boundary conditions*

$$\binom{n}{0}_X = 1 = \binom{n}{n}_X$$

for $n \in \mathbb{N}$ and the *quantum Pascal triangle identity*

$$X^k\binom{n}{k}_X + \binom{n}{k-1}_X = \binom{n+1}{k}_X \tag{2.4}$$

for $1 \leq k \leq n$. $\square$

LEMMA 2.16. *Consider* $1 < N \in \mathbb{N}$. *Let* R *be a field with a primitive* N*-th root of unity* ζ*, so that* $\zeta^N = 1$*, but* $\zeta^r \neq 1$ *for* $1 \leq r < N$ *(compare Chapter 8, §1.1.5). Then* $\binom{N}{k}_\zeta = 0$ *for* $0 < k < N$.

PROOF. In the field R, one has $0 = 1 - \zeta^N = (1-\zeta)(n)_\zeta$. Now $1 \neq \zeta$, so $(n)_\zeta = 0$. Since $(n)_\zeta$ appears as a factor in each of the quantum binomial coefficients $\binom{N}{k}_\zeta$ for $0 < k < N$, these quantities vanish as claimed. □

Now let R be a commutative, unital ring. Suppose that A is an R-algebra.

DEFINITION 2.17. Let q be an element of R. An ordered pair (x, y) of elements of A is said to *q-commute* if $xy = qyx$.

PROPOSITION 2.18 (The Quantum Binomial Theorem). *Let* q *be an element of a commutative, unital ring* R*. Let* (x, y) *be an ordered pair of* q*-commuting elements of an* R*-algebra* A*. Then*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k}_q y^k x^{n-k}$$

for each natural number n.

PROOF. Use induction on n and the quantum Pascal triangle identity (2.4). □

2.3.2. *Taft algebras.*

EXAMPLE 2.19. Consider $1 < N \in \mathbb{N}$. Let R be a field with a primitive N-th root of unity ζ. Consider the R-algebra T generated by a cyclic group $\{g^l \mid 0 \leq l < N\}$ of grouplike elements, and an element x, such that $x^N = 0$ and the pair (x, g) ζ-commutes. Thus T has basis $B = \{g^l x^m \mid 0 \leq l, m < N\}$. A non-classical Hopf algebra structure is erected on T.

The coalgebra structure is given on T by $x\Delta = 1 \otimes x + x \otimes g$. Requiring $\Delta\colon T \to T \otimes T$ to be an algebra homomorphism yields $(g\Delta)^N = 1$, and makes the ordered pair $(x\Delta, g\Delta)$ ζ-commute. By the componentwise algebra structure on primitive elements of the tensor square $T \otimes T$, the pair $(1 \otimes x, x \otimes g)$ ζ-commutes. Thus

$$\begin{aligned}(x\Delta)^N = (1 \otimes x + x \otimes g)^N &= \sum_{k=0}^{N} \binom{N}{k}_\zeta (x \otimes g)^k (1 \otimes x)^{N-k} \\ &= (1 \otimes x)^N + (x \otimes g)^N = 1 \otimes x^N + x^N \otimes g^N = 0\end{aligned}$$

by Proposition 2.18 and Lemma 2.16. It follows that Δ is a well-defined algebra homomorphism. The counit is given by

$$\varepsilon \colon g^l x^m \mapsto \begin{cases} 1 & \text{if } m = 0; \\ 0 & \text{if } 0 < m < N \end{cases}$$

on the basis B. The antipode is specified by $xS = -\zeta^{-1} g^{-1} x$. Further details may be found in [**11**].

3. Exercises

(1) Show that unital rings are the same as $\mathbb{Z}$-algebras. In particular, given a unital ring A, how is the unit $\eta \colon \mathbb{Z} \to A$ defined?

(2) Consider the skewfield $\mathbb{H}$ of quaternions.
  (a) Does $\mathbb{H}$ form an $\mathbb{R}$-algebra?
  (b) Does $\mathbb{H}$ form a $\mathbb{C}$-algebra?

(3) Verify that the comultiplication and counit on $\mathbb{Z}[X]$ given in Example 1.2 make it into a $\mathbb{Z}$-coalgebra. [Hint: In checking coassociativity and counitality, explain why it suffices to chase a monomial X^n around the diagrams in (1.2).]

(4) Just as an algebra multiplication may be written in elementary fashion as

$$\nabla \colon A \otimes A \to A; x \otimes y \mapsto xy\,,$$

so a coalgebra comuliplication may be written in the elementary *Sweedler notation* as

$$\Delta \colon C \to C \otimes C; x \mapsto x^L \otimes x^R\,,$$

with the understanding that $x^L \otimes x^R$ may denote a sum of primitive elements of the tensor square $C \otimes C$, as in Example 1.2. Write the axioms (1.2) in Sweedler notation.

(5) Verify that the comultiplication and counit on RX given in Example 1.3 make it into an R-coalgebra.

(6) Let A be a unital ring. Show that a subset J of A is a left, right, or (two-sided) ideal of A if and only if it satisfies the corresponding conditions of Definition 1.5 for $R = \mathbb{Z}$.
(7) Formulate, and then prove, the First Isomorphism Theorem for R-algebras.
(8) Let R be a field. Suppose that $f\colon D \to C$ is an R-coalgebra homomorphism. Let $\{e_k \mid k \in K\}$ be a basis for $\operatorname{Ker} f$. Extend to a basis $\{e_i \mid i \in I\}$ of D. Show that

$$\{e_i \otimes e_j \mid i, j \in I;\ i \in K \text{ or } \ j \in K\}$$

is a common basis for the spaces on each side of (1.4).
(9) Derive Corollary 1.8 from Proposition 1.7.
(10) Let $D = \mathbb{Z} \oplus \mathbb{Z}/_2 \oplus \mathbb{Z}$ with generators

$$d_0 = [1\ 0\ 0]\,,\ d_1 = [0\ 1\ 0]\,,\ d_2 = [0\ 0\ 1]\,.$$

Let $C = \mathbb{Z} \oplus \mathbb{Z}/_4$ with generators $c_0 = [1\ 0]\,,\ c_1 = [0\ 1]\,.$
 (a) Show that there is a $\mathbb{Z}$-coalgebra structure defined on D by $d_i\varepsilon_D = \delta_{0i}$ and

$$\begin{aligned}\Delta_D\colon d_0 &\mapsto d_0 \otimes d_0\,,\\ d_1 &\mapsto d_0 \otimes d_1 + d_1 \otimes d_0\,,\\ d_2 &\mapsto d_0 \otimes d_2 + d_1 \otimes d_1 + d_2 \otimes d_0\,.\end{aligned}$$

 (b) Show that there is a $\mathbb{Z}$-coalgebra structure defined on C by $c_i\varepsilon_C = \delta_{0i}$ and

$$\Delta_C\colon c_0 \mapsto c_0 \otimes c_0\,,\ c_1 \mapsto c_0 \otimes c_1 + c_1 \otimes c_0\,.$$

 (c) Show that a coalgebra homomorphism is defined by the abelian group homomorphism with

$$f\colon D \to C; d_0 \mapsto c_0\,,\ d_1 \mapsto 2c_1\,,\ d_2 \mapsto 0\,.$$

 (d) Show that f has group kernel $K = d_2\mathbb{Z}$.
 (e) Show that $d_2 \in K$, but $d_2\Delta_D \notin K \otimes D + D \otimes K$, so that K is not a coideal of D.
(11) Verify Proposition 1.10.
(12) Verify Proposition 1.12.
(13) Verify Proposition 1.13.
(14) Verify Proposition 2.2.
(15) Let C be an R-coalgebra.

(a) Show that the dual $C^* = \underline{\underline{R}}(C, R)$ is an algebra under the convolution product.

(b) Show that C^* is commutative iff C is cocommutative.

(16) In the proof of Proposition 2.8, verify that the maps (2.1) and (2.2) are homomorphisms of convolution monoids.

(17) In the group algebra structure of Example 2.11, confirm that the diagrams in Propositions 1.13 and 2.5 commute. [Hint: It suffices to chase basis elements such as g or $g \otimes h$ round the diagrams.]

(18) Verify that the dual group algebra of Example 2.12 forms a Hopf algebra.

(19) In the tensor algebra of Example 2.13, compute $(u \otimes v \otimes w)\Delta$ for elements u, v, w of V.

(20) Show that the set of grouplike elements of a Hopf algebra H forms a group under ∇_H.

(21) Show that the set of primitive elements of a Hopf algebra H is closed under the *commutator* $[x, y] = x \otimes y\nabla - y \otimes x\nabla$.

(22) Show that $(n)_1^! = n!$ and $\binom{n}{k}_1 = \binom{n}{k}$ for natural numbers n.

Bibliography

[1] S.I. Adyan, "Unsolvability of some algorithmic problems in the theory of groups" (Russian), *Trudy Moskov. Mat. Obshch.* **6** (1957), 231–298.

[2] M.A. Arbib (ed.), *Algebraic Theory of Machines, Languages, and Semigroups*, Academic Press, New York, NY, 1968.

[3] K.O. Chung and J.D.H. Smith, "Weak homomorphisms and graph coalgebras," *Arabian Journal of Science and Engineering* **33** (2008), 107–122.

[4] H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Discrete Groups*, Springer, Berlin, 1957.

[5] Doro, S., "Simple Moufang loops," *Math. Proc. Camb. Phil. Soc.* **83** (1978), 377–392.

[6] Liebeck, M.W., "The classification of finite simple Moufang loops," *Math. Proc. Camb. Phil. Soc.* **102**, 33–47.

[7] Paige, L.J., "A class of simple Moufang loops," *Proc. Amer. Math. Soc.* **7** (1956), 471–482.

[8] J.J.M.M. Rutten, "Universal coalgebra: a theory of systems," *Theoretical Computer Science* **249** (2000), 3–80.

[9] J.-P. Serre, *A Course in Arithmetic*, Springer, New York, 1973.

[10] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.

[11] E. Taft, "The order of the antipode of finite-dimensional Hopf algebra," *Proceedings of the National Academy of Sciences* **68** (1971), 2631–2633.

Index