1 Algebraic Structures

A (universal) ***algebra*** is a pair

$$\mathbf{A} = \langle A, F \rangle \tag{1.1}$$

where A is a nonempty set and $F = \{f_i : i \in I\}$ is a set of finitary operations on A; that is, $f_i : A^n \to A$ for some $n \in \mathbb{N}$. A common shorthand notation for (1.1) is $\langle A, f_i \rangle_{i \in I}$. The number n is called the ***arity*** of the operation f_i.

Thus, the arity of an operation is the number of operands upon which it acts, and we say that $f \in F$ is an n***-ary*** operation on A if f maps A^n into A. An operation is called *nullary* (or constant) if its arity is zero. *Unary*, *binary*, and *ternary* operations have arities 1, 2, and 3, respectively.

Example 1.1. If $A = \mathbb{R}$ and $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is the map $f(a, b) = a + b$, then $\langle A, f \rangle$ is an algebra with a single binary operation. Many more examples will be given below.

An algebra $\mathbf{A}$ is called ***unary*** if all of its operations are unary. An algebra $\mathbf{A}$ is ***finite*** if $|A|$ is finite and ***trivial*** if $|A| = 1$. Given two algebras $\mathbf{A}$ and $\mathbf{B}$, we say that $\mathbf{B}$ is a ***reduct*** of $\mathbf{A}$ if both algebras have the same universe and $\mathbf{A}$ (resp. $\mathbf{B}$) can be obtained from $\mathbf{B}$ (resp. $\mathbf{A}$) by adding (resp. removing) operations.

A better approach: An ***operation symbol*** f is an object that has an associated arity, which we'll denote $\text{arity}(f)$. A set of operation symbols F is called a ***similarity type***. An algebra of similarity type F is a pair $\mathbf{A} = \langle A, F^{\mathbf{A}} \rangle$, where $F^{\mathbf{A}} = \{f^{\mathbf{A}} : f \in F\}$ and $f^{\mathbf{A}}$ is an operation on A of arity $\text{arity}(f)$.

Example 1.2. Consider the set of integers $\mathbb{Z}$ with operation symbols $F = \{+, \cdot, -, 0, 1\}$, which have respective arities $\{2, 2, 1, 0, 0\}$. The operation $+^{\mathbb{Z}}$ is the usual binary addition, while $-^{\mathbb{Z}}$ is negation: $a \mapsto -a$. The constants $0^{\mathbb{Z}}$ and $1^{\mathbb{Z}}$ are nullary operations. Of course we usually just write $+$ for $+^{\mathbb{Z}}$, etc.

Examples of some general algebraic structures that, historically, have been a central focus of mathematicians over the last century (e.g., groups) are given in Appendix Section A. More examples will be added as we learn about them throughout the semester.

2 Direct Products

The ***Cartesian product*** of two sets A_0 and A_1, denoted $A_0 \times A_1$, is the set of all ordered pairs (a_0, a_1) such that $a_0 \in A_0$ and $a_1 \in A_1$.[1] That is, $A_0 \times A_1 := \{(a_0, a_1) \mid a_0 \in A_0, a_1 \in A_1\}$. More generally, $A_0 \times \cdots \times A_{n-1}$ is the set of all sequences of length n with i^{th} element in A_i. That is,

$$A_0 \times \cdots \times A_{n-1} := \{(a_0, \ldots, a_{n-1}) \mid a_0 \in A_0, \ldots, a_{n-1} \in A_{n-1}\}.$$

[1] For the definition of *ordered pair*, consult the appendix.

Another way to view $A_0 \times \cdots \times A_{n-1}$ is as the set of all functions with domain $\{0, 1, \ldots, n-1\}$ and range $\bigcup_{i=1}^{n-1} A_i$. More generally still, the ***Cartesian product*** of an indexed family of sets, $\{A_i : i \in I\}$, is the set of all functions with domain I and range $\bigcup_{i \in I} A_i$ such that $f(i) \in A_i$. That is,

$$\prod_{i \in I} A_i := \{f : I \to \bigcup_{i \in I} A_i \mid f(i) \in A_i\}.$$

When $A_0 = A_1 = \cdots = A$, we write $A^2 := A \times A$ and $A^n := A \times \cdots \times A$ (n terms), and refer to these as *Cartesian powers* of A.

Question: How do you know $\prod_{i \in I} A_i \neq \varnothing$, even supposing $I \neq \varnothing$ and $A_i \neq \varnothing$ for all $i \in I$.[2]

3 Relations

A ***k-ary relation*** R on a set A is a subset of the Cartesian product A^k. We give some examples of relations below. In these examples, $\mathbb{R}$ denotes the set of real numbers, and letters $a \in \mathbb{R}^2$, $b \in \mathbb{R}^3$ etc. denote tuples (a_0, a_1), (b_0, b_1, b_2), etc.

Example 3.1.

(a) $A = \mathbb{R}$ and $R = \{a \in \mathbb{R}^2 : a = b\} = \{(a, a) : a \in \mathbb{R}\}$.

(b) $A = \mathbb{R}^2$ (the plane) and $R = \{(a, b, c) \in \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 : a, b, c \text{ lie on a line}\}$; i.e. triples of points which are *colinear*.

Note that a 1-ary or ***unary relation*** on a set A is simply a subset of A, a ***binary relation*** is a subset of A^2, a ***ternary relation*** is a subset of A^3, etc. Some binary relations have properties that make them especially useful in a wide variety of applications.

Definition 3.2. A ***preorder*** on a set A is a binary relation $\leqslant$ that satisfies, for all a, b, and c in A

1. $a \leqslant a$ *(reflexive)*
2. $a \leqslant b$ and $b \leqslant c \implies a \leqslant c$ *(transitive)*

[2] *Answer:* Each f "chooses" an element from each A_i, but when the A_i are all different and I is infinite, we may not be able to do this. The *Axiom of Choice* (Choice) says you can. Gödel proved that Choice is consistent with the other axioms of set theory. Cohen proved that the negation of Choice is also consistent.

Example 3.3. The reachability relation in any directed graph (possibly containing cycles) gives rise to a preorder $\leqslant$, where $x \leqslant y$ if and only if there is a path from x to y in the directed graph. Conversely, every preorder $\leqslant$ on a set A is the reachability relation of a directed graph (simply take elements of A to be the vertices and draw an edge from x to y whenever $x \leqslant y$).

In fact, the significance of preorders stems mainly from the fact that the two most important classes of binary relations happen to be preorders. An *equivalence relation* is a symmetric preorder. A *partial order* is an anti-symmetric preorder.

Definition 3.4. A ***partial order*** on a set A is a relation $\leqslant$ satisfying, for all a, b, and c in A

1. $a \leqslant a$ *(reflexive)*
2. $a \leqslant b$ and $b \leqslant a \implies a = b$ *(anti-symmetric)*
3. $a \leqslant b$ and $b \leqslant c \implies a \leqslant c$ *(transitive)*

Definition 3.5. An ***equivalence relation*** on a set A is a relation R satisfying, for all a, b, and c in A,

1. $a \mathrel{R} a$ *(reflexive)*
2. $a \mathrel{R} b \implies b \mathrel{R} a$ *(symmetric)*
3. $a \mathrel{R} b$ and $b \mathrel{R} c \implies a \mathrel{R} c$ *(transitive)*

We denote the set of all equivalence relations on a set A by $\mathrm{Eq}(A)$.

Example 3.6.

(a) If $A = \mathbb{Z}$ and R is the usual $\leqslant$ relation, then R is a partial order on A. (In fact, $\leqslant$ is a total order on $\mathbb{Z}$ in this case.)

(b) Let X be any set and consider the collection $A = \mathcal{P}(X)$ of all subsets of X. The subset relation $y \subseteq z$ ("y is a subset of z") is a partial order on A.

(c) Let $A = \mathbb{R}^2$ and $R =$ "$\leqslant$ on each component" $= \{(a, b) \in \mathbb{R}^2 \times \mathbb{R}^2 : a_1 \leqslant b_1,\ a_2 \leqslant b_2\}$. Then R is a partial order on A.

(d) If $A = \mathbb{R}^2$ then $R = \{(a, b) \in \mathbb{R}^2 \times \mathbb{R}^2 : a = (a_1, a_2),\ b = (b_1, b_2),\ a_1^2 + a_2^2 = b_1^2 + b_2^2\}$ is an equivalence relation on A. The equivalence classes are circles centered at $(0, 0)$.

A ***partition*** of a set A is a collection $\Pi = \{A_i : i \in I\}$ of non-empty subsets of A such that

$$\bigcup_{i \in I} A_i = A \quad \text{and} \quad A_i \cap A_j = \varnothing \text{ for all pairs } i \neq j \text{ in } I.$$

The A_i are called the "blocks" of the partition.

Every partition Π determines an equivalence relation—namely, the relation R defined by $a\, R\, b$ if and only if a and b are in the same block of Π. Conversely, if R is an equivalence relation on A, we denote the equivalence class of R containing a by $a/R := \{b \in A : a\, R\, b\}$ and the set $A/\theta := \{a/\theta : a \in A\}$ of all θ classes is a partition of A.

4 Relational Structures and Lattices

A ***relational structure*** is a set A and a collection of (finitary) relations on A. A ***partially ordered set***, or ***poset***, is a set A together with a partial order (Sec. 3) $\leqslant$ on it, denoted $\langle A, \leqslant \rangle$.

Let $\langle A, \leqslant \rangle$ be a poset and let B be a subset of the set A. An element a in A is an upper bound for B if $b \leqslant a$ for every b in B. An element a in A is the ***least upper bound*** of B, denoted $\bigvee B$, or ***supremum*** of B ($\sup B$), if a is an upper bound of B, and $b \leqslant c$ for every b in B implies $a \leqslant c$ (i.e., a is the smallest among the upper bounds of B). Similarly, a is a lower bound of B provided $a \leqslant b$ for all b in B, and a is the ***greatest lower bound*** of B ($\bigwedge B$), or ***infimum*** of B ($\inf B$) if a is a lower bound and is above every other lower bound of B.

Let a, c be two elements in the poset A. We say c ***covers*** a, or a is covered by c provided $a \leqslant c$ and whenever $a \leqslant b \leqslant c$ it follows that $a = b$ or $b = c$. We use the notation $a \prec c$ to denote that c covers a.

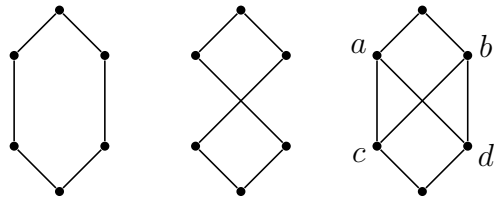
A ***lattice*** is a partially ordered set $\langle L, \leqslant \rangle$ such that for each pair $a, b \in L$ there is a least upper bound, denoted $a \vee b := \text{lub}\{a, b\}$, and a greatest lower bound, denoted $a \wedge b := \text{glb}\{a, b\}$, contained in L. A lattice can also be viewed as an algebra $\langle L, \vee, \wedge \rangle$ where $\vee$, called "join," and $\wedge$, "meet," are binary operations satisfying

1. $x \vee x = x$ and $x \wedge x = x$ *(idempotent)*
2. $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$ *(commutative)*
3. $x \vee (y \vee z) = (x \vee y) \vee z$ *(associative)*
4. $x \vee (y \wedge x) = x$ and $x \wedge (y \vee x) = x$ *(absorbtive)*

Posets in general, and lattices in particular, can be visualized using a so-called ***Hasse diagram***. The Hasse diagram of a poset $\langle A, \leqslant \rangle$ is a graph in which each element of the set A is denoted by a vertex, or "node" of the graph. If $a \prec b$ then we draw the node for b above the node for a, and join them with a line segment. The resulting diagram gives a visual description of the relation $\leqslant$, since $a \leqslant b$ holds iff for

some finite sequence of elements $c_1, \ldots, c_n$ in A we have $a = c_1 \prec c_2 \prec \cdots \prec c_n = b$. Some examples appear in the figures below.

Figure 1: Hasse diagrams



Note that the first two examples in Figure 1 depict the same poset, which illustrates that Hasse diagrams are not uniquely determined. Also, note that the poset represented in the first two diagrams is a lattice. In contrast, the poset depicted in the third diagram is not a lattice since neither $a \wedge b$ nor $c \vee d$ is defined – the sets $\{a, b\}$ and $\{c, d\}$ have upper and lower bounds, but $\{a, b\}$ has no *greatest* lower bound, and $\{c, d\}$ has no *least* upper bound.

5 Subalgebras and Homomorphisms

Suppose $\mathbf{A} = \langle A, F^{\mathbf{A}} \rangle$ is an algebra. We call the nonempty set A the ***universe*** of $\mathbf{A}$. If a subset $B \subseteq A$ is *closed* under all operations in $F^{\mathbf{A}}$, we call B a ***subuniverse*** of A. By closed under all operations we mean the following: for each $f \in F^{\mathbf{A}}$, we have $f(b_0, \ldots, b_{n-1}) \in B$, for all $b_0, \ldots, b_{n-1} \in B$, where $n = \text{arity}(f)$.

If $B \neq \varnothing$ is a subuniverse of $\langle A, F^{\mathbf{A}} \rangle$, and if we let $F^{\mathbf{B}} = \{f \restriction B : f \in F^{\mathbf{A}}\}$, then the algebra $\mathbf{B} = \langle B, F^{\mathbf{B}} \rangle$ is called a ***subalgebra*** of $\mathbf{A}$.[3] If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$, we denote this fact by $\mathbf{B} \leqslant \mathbf{A}$. Similarly, we write $B \leqslant A$ if B is a subuniverse of A. We denote the set of all subalgebras of $\mathbf{A}$ by $\text{Sub}(\mathbf{A})$. Note that universe of an algebra is not allowed to be empty. However, the empty set is a subuniverse.

Theorem 5.1. *If $\mathbf{A}_i \leqslant \mathbf{A}$, $i \in I$, then $\bigcap A_i$ is a subuniverse if it is not empty.*

If S is a nonempty subset of A, the ***subuniverse generated by*** S, denoted $\text{Sg}^{\mathbf{A}}(S)$ or $\langle S \rangle$ is the smallest subuniverse of $\mathbf{A}$ containing the set S. When $\langle S \rangle = A$, we say that S generates A.

Theorem 5.2. *If $S \subseteq A$, then $\text{Sg}^{\mathbf{A}}(S) = \langle S \rangle = \bigcap \{B \leqslant A : S \subseteq B\}$.*

Let $\mathbf{A} = \langle A, F^{\mathbf{A}} \rangle$ and $\mathbf{B} = \langle B, F^{\mathbf{B}} \rangle$ be algebras of the same type, and let $\varphi : A \to B$ be a function. Take an n-ary operation symbol $f \in F$, and suppose that for all $a_1, \ldots a_n \in A$ the following equation holds:

$$\varphi(f^{\mathbf{A}}(a_1, \ldots, a_n)) = f^{\mathbf{B}}(\varphi(a_1), \ldots, \varphi(a_n)).$$

[3]Here $f \restriction B$ denotes restriction of the function f to the set B (see Appendix Sec. B.2).

Then φ is said to *respect the interpretation of* f. If φ respects the interpretation of every $f \in F$, then we call φ a ***homomorphism*** from $\mathbf{A}$ into $\mathbf{B}$, and we write $\varphi \in \mathrm{Hom}(\mathbf{A}, \mathbf{B})$, or simply, $\varphi : \mathbf{A} \to \mathbf{B}$.

Fact: For groups, to check that a map $\varphi : G \to H$ is a homomorphism, it is enough to check that φ respects the interpretation of the binary operation. It follows from this that such a function respects the unary and nulary operations as well. (This was a homework exercise.)

Example 5.3. Let $\mathbf{G} = \langle G, \cdot, ^{-1}, e\rangle$ be a finite group of order n. Take the set G (the elements of $\mathbf{G}$) and consider the group of all permutations of these elements. We will denote this group by $\mathrm{Sym}(G) = \langle S, \circ, ^{-1}, \mathrm{id}\rangle$. Fix an element $a \in G$ and recall that the function $\lambda_a : G \to G$, defined by $\lambda_a(g) = a \cdot g$, is a permutation of the set G. That is, λ_a belongs to the permutation group $\mathrm{Sym}(G)$. The function $\lambda : G \to \mathrm{Sym}(G)$ defined by $a \mapsto \lambda_a$ is a group homomorphism.[4] To see this, fix $a, b \in G$. We must show that the permutation $\lambda(a \cdot b) = \lambda_{ab}$ is the same as the permutation $\lambda(a) \circ \lambda(b) = \lambda_a \circ \lambda_b$. Indeed, for all $g \in G$,

$$\begin{aligned} \lambda_{ab}(g) &= (a \cdot b) \cdot g = a \cdot (b \cdot g) \qquad (\textit{associativity}) \\ &= a \cdot \lambda_b(g) = \lambda_a(\lambda_b(g)) \\ &= (\lambda_a \circ \lambda_b)(g). \end{aligned}$$

6 Isomorphism Theorems

This section covers the group theoretic versions of what are sometimes called the *Noether isomorphism theorems*.[5] Analogs of these theorems exist for other algebraic structures (such as rings). More generally the theorems can be stated in a way that makes them true for all algebraic structures.

To keep the presentation simple, we begin by stating the special versions of the theorems that apply to groups. However, in anticipation of the more general versions to come, we introduce some terminology that will make the transition to a more general context smoother. For now the reader will have to trust that carrying around this slightly heavier baggage at the start will pay off in the end.

6.1 The kernel: equivalence relation or subgroup?

Let A and B be sets and let $\varphi : A \to B$ be a function. We say that a pair $(a_0, a_1) \in A^2$ belongs to the ***kernel*** of φ, and we write $(a_0, a_1) \in \ker \varphi$, just in case $\varphi(a_0) = \varphi(a_1)$.

[4] Note that the function is given, for each $a \in G$, by $\lambda(a) = \lambda_a$.

[5] Emmy Noether (23 Mar 1882 – 14 Apr 1935), was an influential German mathematician known for her groundbreaking contributions to abstract algebra and theoretical physics. Ring theoretic versions of Noether's isomorphism theorems appeared in her 1927 paper [2].

Thus, to every function $\varphi : A \to B$ there corresponds a binary relation on A given by

$$(a_0, a_1) \in \ker \varphi \qquad \Longleftrightarrow \qquad \varphi(a_0) = \varphi(a_1).$$

The proof of the next proposition is an easy exercise.

Proposition 6.1. $\ker \varphi$ *is an equivalence relation on the domain of* φ.

Exercise 1. Prove proposition 6.1.

Each equivalence relation R on a set A partitions that set into "blocks" or *equivalence classes*. Given an element $a_1 \in A$, we denote the equivalence class containing a_1 by a_1/R, or by $[a_1]$ when the latter seems more convenient. Thus, a few alternative ways to write the equivalence class of R that contains a_1 are as follows:

$$a_1/R = \{a_2 \in A \mid a_1 \; R \; a_2\} = \{a_2 \in A \mid (a_1, a_2) \in R\} = [a_1].$$

The set of all equivalence classes of a given relation R is denoted by A/R. That is,

$$A/R = \big\{[a] : a \in A\big\}.$$

Example 6.2. Suppose $A = \{w, x, y, z\}$ and $B = \{0, 1, 2\}$ and let $\varphi : A \to B$ be defined by $\varphi(w) = 2$, $\varphi(x) = 0$, and $\varphi(y) = 1 = \phi(z)$. Let $R \subseteq A^2$ denote the kernel of φ. Then,

$$R = \{(a_0, a_1) \mid \varphi(a_0) = \varphi(a_1)\} = \{(w, w), (x, x), (y, y), (y, z), (z, y), (z, z)\},$$

and

$$[w] = \{w\}, \qquad [x] = \{x\}, \qquad [y] = \{y, z\}, \qquad [z] = \{y, z\}.$$

The set A/R of all equivalence classes of R is

$$A/R = \{[w], [x], [z]\}.$$

The point is that φ maps y and z to the same element, so the kernel "collapses" these points into a single class, which we can represent either by $[y]$ or by $[z]$. The choice is arbitrary, since they both denote the same equivalence class, namely $\{y, z\}$.

Example 6.3. Suppose $\varphi : G \to H$ is a group homomorphism. As above, the kernel of φ is

$$\ker \varphi = \{(x, y) \in G \times G : \varphi(x) = \varphi(y)\} \tag{6.1}$$

Since $\ker \varphi$ is an equivalence relation, G is partitioned into equivalence classes of $\ker \varphi$. Let K_φ denote the equivalence class of $\ker \varphi$ that contains the identity element e_G of G. That is,

$$K_\varphi = e_G/\ker \varphi = \{x \in G : (x, e_G) \in \ker \varphi\} = \{x \in G : \varphi(x) = \varphi(e_G)\} = [e_G].$$

Since φ is a homomorphism, $\varphi(e_G) = e_H$. Therefore,

$$K_\varphi = \{x \in G : \varphi(x) = e_H\} = \varphi^{-1}(\{e_H\}).$$

Exercise 2. Let $\varphi : G \to H$ be a group homomorphism.

1. Prove that K_φ is a normal subgroup of G.

2. Recall that an equivalence on G partitions G into disjoint equivalence classes. Show that the equivalence classes of $\ker \varphi$ are precisely the left cosets of K_φ in G; that is $\ker \varphi$ partitions G into the disjoint union,

$$G = K_\varphi \cup g_1 K_\varphi \cup g_2 K_\varphi \cup \cdots .$$

A note on terminology. Our textbook, and most other elementary books on classical algebra, calls the subgroup K_φ described above the "kernel" of φ. This terminology is useful in the context of certain special classes of algebraic structures, such as groups or rings. However, to treat algebraic structures more generally requires the definition of kernel given in (6.1). Since the two definitions of "kernel" serve different purposes, and since neither is dispensible, we must agree on a convention that will allow us to speak about these two notions without causing confusion. From now on,

- "kernel relation" and $\ker \varphi$ will refer to the equivalence relation defined in (6.1);
- "kernel subgroup" and K_φ will refer to the equivalence class of $\ker \varphi$ containing the identity.

We refrain from using the term "kernel" without qualification, unless it is obvious that we are referring to an equivalence relation and not a subgroup (or vice-versa).

To summarize, if $\varphi : G \to H$ is a function from a set G to a set H, then the ***kernel relation*** is $\ker \varphi = \{(x, y) \in G \times G : \varphi(x) = \varphi(y)\}$. In the special case when G and H are groups and $\varphi : G \to H$ is a group homomorphism, then we may speak of the ***kernel subgroup***, $K_\varphi = \{x \in G : \varphi(x) = e_H\}$.

6.2 Group Isomorphism Theorems

Theorem 6.4 (First Isomorphism Theorem)**.** *Suppose $\varphi : G \to H$ is a group homomorphism. Then,*

1. *$K_\varphi = \varphi^{-1}(\{e_H\})$ is a normal subgroup of G;*
2. *the image of G under φ is a subgroup of H;*
3. *the factor group G/K_φ is isomorphic to the image of G under φ.*

In other terms, if $\varphi : G \to H$ is a homomorphism, then

$$K_\varphi \triangleleft G, \quad \varphi(G) \leqslant H, \quad G/K_\varphi \cong \varphi(G).$$

Exercise 3. Suppose N is a normal subgroup of G. Prove that the function $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a group epimorphism with kernel subgroup $K_\pi = N$.

Exercise 4. Prove the First Isomorphism Theorem.

Exercise 5. Suppose K and L are normal subgroups of G. Prove that $G/K \cap L$ is isomorphic to a subgroup of $G/K \times G/L$ (the external direct product),[6] and compute the index of this subgroup in $G/K \times G/L$, in terms of $[G : K]$, $[G : L]$, and $[G : KL]$.

Theorem 6.5 (Second Isomorphism Theorem)**.** *Let G be a group with subgroups H and N, and suppose that N is a normal subgroup of G. Then*

1. *HN is a subgroup of G;*
2. *$H \cap N$ is a normal subgroup of H;*
3. *$HN/N \cong H/H \cap N$.*

Exercise 6. Prove the Second Isomorphism Theorem.

Exercise 7. Let G be a nonabelian simple group. Let S_n be the symmetric group of all permutations on an n-element set, and let A_n be the alternating group.

1. Show that if G is a subgroup of S_n, n finite, then G is a subgroup of A_n.
2. Let H be a proper subgroup of G, and, for $g \in G$, let λ_g be the map of the set of left cosets of H onto themselves defined by $\lambda_g(xH) = gxH$. Show that the map $g \mapsto \lambda_g$ is a monomorphism (injective homomorphism) of G into the group of permutations of the set of left cosets of H.
3. Let H be a subgroup of G of finite index n and assume $n > 1$ (so $H \neq G$). Show that G can be embedded in A_n. (That is, show that G is isomorphic to a subgroup of A_n.
4. If G is infinite, it has no proper subgroup of finite index.

Theorem 6.6 (Correspondence Theorem)**.** *Let N be a normal subgroup of a group G. Then the map $H \mapsto H/N$ is a one-to-one correspondence between the set of subgroups of G that contain N and the set of subgroups of G/N. That is,*

$$\mathrm{Sub}(G) \ \ni \ H \ \longleftrightarrow \ H/N \ \in \ \mathrm{Sub}(G/N).$$

Moreover, the normal subgroups of G containing N correspond to normal subgroups of G/N.

[6]Note that the expression $G/K \cap L$ can only be interpreted as $G/(K \cap L)$, since $(G/K) \cap L$ doesn't make sense.

Proof. Let H be a subgroup of G containing N. Since N is normal in H, H/N makes sense. Let aN and bN be elements of H/N. Then $(aN)(b^{-1}N) = ab^{-1}N \in H/N$; hence, H/N is a subgroup of G/N.

Let S be a subgroup of G/N. This subgroup is a set of cosets of N. If $H = \{g \in G : gN \in S\}$, then for $h_1, h_2 \in H$, we have that $(h_1N)(h_2N) = h_1h_2N \in S$ and $h_1^{-1}N \in S$. Therefore, H must be a subgroup of G. Clearly, H contains N. Therefore, $S = H/N$. Consequently, the map $H \mapsto H/N$ is onto.

Suppose that H_1 and H_2 are subgroups of G containing N such that $H_1/N = H_2/N$. If $h_1 \in H_1$, then $h_1N \in H_1/N$. Hence, $h_1N = h_2N \subset H_2$ for some h_2 in H_2. However, since N is contained in H_2, we know that $h_1 \in H_2$ or $H_1 \subset H_2$. Similarly, $H_2 \subset H_1$. Since $H_1 = H_2$, the map $H \mapsto H/N$ is one-to-one.

Suppose that H is normal in G and N is a subgroup of H. Then it is easy to verify that the map $G/N \to G/H$ defined by $gN \mapsto gH$ is a homomorphism. The kernel of this homomorphism is H/N, which proves that H/N is normal in G/N.

Conversely, suppose that H/N is normal in G/N. The homomorphism given by

$$G \to G/N \to \frac{G/N}{H/N}$$

has kernel H. Hence, H must be normal in G. □

Notice that in the course of the proof of Theorem 6.6, we have also proved the following theorem.

Theorem 6.7 (Third Isomorphism Theorem)**.** *Let $N \leqslant H \leqslant G$ be a chain of groups and suppose N and H are both normal in G. Then,*

$$G/H \cong \frac{G/N}{H/N}.$$

Example 6.8. Fix two integers $m, n \in \mathbb{Z}$. By the Third Isomorphism Theorem,

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}).$$

Since $|\mathbb{Z}/mn\mathbb{Z}| = mn$ and $|\mathbb{Z}/m\mathbb{Z}| = m$, we have $|m\mathbb{Z}/mn\mathbb{Z}| = n$.

7 Quotient Algebras

Let $\mathbf{A} = \langle A, F\rangle$ be an algebra. Recall, F denotes the set of operation symbols, and to each operation symbol $f \in F$ there corresponds an arity, and the set of arities determines the similarity type of the algebra. (We might do better to denote the algebra by $\langle A, F^{\mathbf{A}}\rangle$, since the algebra is not defined until we have associated to each operation symbol $f \in F$ an actual operation $f^{\mathbf{A}}$ on A, but this is a technical point, and we will often denote two algebras of the same similarity type as $\langle A, F\rangle$ and $\langle B, F\rangle$ with the understanding that the meaning of F depends on the context.)

Let $\theta \in \operatorname{Con}\mathbf{A}$ be a congruence relation. The ***quotient algebra*** $\mathbf{A}/\theta$ is an algebra with the same similarity type as $\mathbf{A}$, with universe $A/\theta = \{a/\theta : a \in A\}$, and operation symbols F, where for each (k-ary) symbol $f \in F$ the operation $f^{\mathbf{A}/\theta}$ is defined as follows: for $(a_1/\theta, \dots, a_k/\theta) \in (A/\theta)^k$,

$$f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_k/\theta) = f^{\mathbf{A}}(a_1, \dots, a_k)/\theta.$$

(As mentioned above, F denotes the set of operation symbols of the similarity type of the algebra, and it is "overloaded" in the sense that we write $\mathbf{A} = \langle A, F\rangle$ and $\mathbf{A}/\theta = \langle A/\theta, F\rangle$, and for each $f \in F$ the corresponding operation in these algebras is interpreted appropriately—i.e., as $f^{\mathbf{A}}$ or $f^{\mathbf{A}/\theta}$.)

8 Direct Products of Algebras

Above we defined direct products of sets. We now define direct products of algebras. Let $\mathbf{A} = \langle A, F\rangle$ and $\mathbf{B} = \langle B, F\rangle$ be two algebras of the same similarity type. The ***direct product*** $\mathbf{A} \times \mathbf{B}$ is an algebra of the same type as $\mathbf{A}$ and $\mathbf{B}$, with universe $A \times B = \{(a, b) : a \in A, b \in B\}$, and operation symbols F. To each (k-ary) symbol $f \in F$ corresponds an operation $f^{\mathbf{A}\times\mathbf{B}}$ defined as follows: for $((a_1, b_1), \dots, (a_k, b_k)) \in (A \times B)^k$,

$$f^{\mathbf{A}\times\mathbf{B}}((a_1, b_1), \dots, (a_k, b_k)) = (f^{\mathbf{A}}(a_1, \dots, a_k), f^{\mathbf{B}}(b_1, \dots, b_k)). \tag{8.1}$$

This definition can be easily extended to the direct product $\prod \mathbf{A}_i$ of any collection of algebras $\{\mathbf{A}_i : i \in I\}$, and we leave it to the reader to write down the defining property of the operations, which is completely analogous to (8.1).

If all the algebras are isomorphic we sometimes call $\prod \mathbf{A}_i$ the ***direct power*** of $\mathbf{A}$. When the set I is finite, say, $I = 1, 2, \dots, n$, we have alternative notations for the direct power, namely,

$$\prod \mathbf{A}_i = \mathbf{A}_1 \times \mathbf{A}_2 \times \cdots \times \mathbf{A}_n = \mathbf{A}^n.$$

The constructions of this section and the preceding one are often combined to give direct products of quotient algebras. For instance, if θ_1 and θ_2 are two congruences of $\mathbf{A}$, the algebra $\mathbf{A}/\theta_1 \times \mathbf{A}/\theta_2$ has the same similarity type as $\mathbf{A}$, and its universe is

$$A/\theta_1 \times A/\theta_2 = \{(a/\theta_1, b/\theta_2) : a, b \in A\}.$$

Define $\mathbf{A}_1 := \mathbf{A}/\theta_1$ and $\mathbf{A}_2 := \mathbf{A}/\theta_2$. The operation symbols of the algebra $\mathbf{A}_1 \times \mathbf{A}_2$ are again F, and to each (k-ary) symbol $f \in F$ corresponds an operation $f^{\mathbf{A}_1\times\mathbf{A}_2}$ defined as follows: and for $((a_1/\theta_1, b_1/\theta_2), \dots, (a_k/\theta_1, b_k/\theta_2)) \in (A_1 \times A_2)^k$,

$$\begin{aligned} f^{\mathbf{A}_1\times\mathbf{A}_2}((a_1/\theta_1, b_1/\theta_2), \dots, (a_k/\theta_1, b_k/\theta_2)) &= (f^{\mathbf{A}_1}(a_1/\theta_1, \dots, a_k/\theta_1), f^{\mathbf{A}_2}(b_1/\theta_2, \dots, b_k/\theta_2)) \\ &= (f^{\mathbf{A}}(a_1, \dots, a_k)/\theta_1, f^{\mathbf{A}}(b_1, \dots, b_k)/\theta_2). \end{aligned}$$

APPENDIX

A Examples of Algebraic Structures

Recall from above that an *algebra* $\mathbf{A}$ is an ordered pair $\mathbf{A} = \langle A, F \rangle$ where A is a nonempty set and F is a family of finitary operations on A. The set A is called the universe of $\mathbf{A}$, and the elements $f^{\mathbf{A}} \in F$ are called the fundamental operations of $\mathbf{A}$. (In practice we prefer to write f for $f^{\mathbf{A}}$ when this doesn't cause ambiguity.The *arity* of an operation is the number of operands upon which it acts, and we say that $f \in F$ is an *n-ary* operation on A if f maps A^n into A. An operation $f \in F$ is called a *nullary* operation (or constant) if its arity is zero. *Unary*, *binary*, and *ternary* operations have arity 1, 2, and 3, respectively. An algebra $\mathbf{A}$ is called *unary* if all of its operations are unary. An algebra $\mathbf{A}$ is *finite* if $|A|$ is finite and *trivial* if $|A| = 1$. Given two algebras $\mathbf{A}$ and $\mathbf{B}$, we say that $\mathbf{B}$ is a *reduct* of $\mathbf{A}$ if both algebras have the same universe and $\mathbf{A}$ is obtained from $\mathbf{B}$ by simply adding more operations.

Below is a list of a few of the most basic algebraic structures. A list of *many* more can be found at http://www.math.chapman.edu/~jipsen/structures/doku.php/index.html.

magma $\mathbf{A} = \langle A, \cdot \rangle$
An algebra with a single binary operation is called a *magma* (or groupoid or binar). This operation is usually denoted by $+$ or $\cdot$, and we write $a + b$ or $a \cdot b$ (or just ab) for the image of (a, b) under this operation, and call it the sum or product of a and b, respectively.

semigroup $\mathbf{A} = \langle A, \cdot \rangle$
A groupoid for which the binary operation is associative is called a *semigroup*. That is, a semigroup is a groupoid with binary operation satisfying $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in A$.

monoid $\mathbf{A} = \langle A, \cdot, e \rangle$
A *monoid* is a semigroup along with a *multiplicative identity* e. That is, $\langle A, \cdot \rangle$ is a semigroup and e is a constant (nullary operation) satisfying $e \cdot a = a \cdot e = a$, for all $a \in A$.

group $\mathbf{A} = \langle A, \cdot, ^{-1}, e \rangle$
A *group* is a monoid along with a unary operation $^{-1}$ called *multiplicative inverse*. That is, the reduct $\langle A, \cdot, e \rangle$ is a monoid and $^{-1}$ satisfies $a \cdot a^{-1} = a^{-1} \cdot a = e$, for all $a \in A$. An *Abelian group* is a group with a commutative binary operation, which we usually denote by $+$ instead of $\cdot$. In this case, we write 0 instead of e to denote the *additive identity*, and $-$ instead of $^{-1}$ to denote the *additive inverse*. Thus, an Abelian group is a group $\mathbf{A} = \langle A, +, -, 0 \rangle$ such that $a + b = b + a$ for all $a, b \in A$.

B Prerequisites

This section gives a brief review of some elementary definitions and facts from set theory. See Enderton [1] for more details.

B.1 Tuples and Relations

Most of us probably have a good idea of what is meant by an "ordered pair," (x, y). It consists of two elements (or sets) x and y, listed in a particular order. How to make this notion mathematically precise is not quite so obvious. According to [1], in 1921 Kazimierz Kuratowski gave us the definition in general use today: given two sets x and y, the ***ordered pair*** (x, y) is defined to be the set $\{\{x\}, \{x, y\}\}$. It is not too hard to prove that this definition captures our intuitive idea of ordered pair—namely, (x, y) uniquely determines both what x and y are, and the order in which they appear. Indeed, it is a theorem (Theorem 3A of [1]) that $(u, v) = (x, y)$ iff $u = x$ and $v = y$.

A ***binary relation*** is a set of ordered pairs. Thus, if X is a set, a binary relation R on X is simply a subset of the Cartesian product, that is,

$$R \subseteq X \times X := \{(x_1, x_2) : x_1, x_2 \in X\}.$$

For a binary relation R, we sometimes write $x\, R\, y$ in place of $(x, y) \in R$. For example, in the case of the order relation $\leqslant$ on the set $\mathbb{R}$ of real numbers, $\leqslant$ is defined to be the set

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} : x \text{ is less than or equal to } y\},$$

and we usually write $x \leqslant y$ to mean that the pair (x, y) belongs to the relation $\leqslant$. Of course, we could write $(x, y) \in \leqslant$, but the "infix" notation $x \leqslant y$ is often preferred for binary relations.

For a relation R, we define the ***domain*** of R ($\operatorname{dom} R$) and the ***range*** of R ($\operatorname{ran} R$) by

$$\begin{aligned} x \in \operatorname{dom} R &\iff \exists y\ (x, y) \in R, \\ x \in \operatorname{ran} R &\iff \exists t\ (t, x) \in R. \end{aligned}$$

We can extend the definition of ordered pairs and define an *ordered triple* recursively, as follows:

$$(x, y, z) = ((x, y), z).$$

Similarly we can form *ordered quadruples*:

$$(x_1, x_2, x_3, x_4) = ((x_1, x_2, x_3), x_4) = (((x_1, x_2), x_3), x_4).$$

Inductively, for each $n \in \mathbb{N}$, if we assume the notion of ordered k-tuple, $(x_1, \ldots, x_k)$, has been defined for $k < n$, we can form *ordered n-tuples* as follows:

$$(x_1, \ldots, x_{n-1}, x_n) = ((x_1, \ldots, x_{n-1}), x_n).$$

It is convenient for reasons of uniformity to define also the 1-tuple $(x) = x$. We define an n-ary relation on A to be a set of ordered n-tuples with all components in A. Thus a binary (2-ary) relation on A is just a subset of $A \times A$. And a ternary (3-ary) relation on A is a subset of $(A \times A) \times A$. There is, however, a terminological quirk here. If $n > 1$, then any n-ary relation on A is actually a binary relation, but a unary (1-ary) relation on A is just a subset of A.

A relation R on a set A is called ***reflexive*** iff $x\,R\,x$ for all $x \in A$; ***symmetric*** iff whenever $x\,R\,y$ then also $y\,R\,x$; ***transitive*** iff whenever $x\,R\,y$ and $y\,R\,z$, then also $x\,R\,z$. A relation is an ***equivalence relation*** iff it is a binary relation that is reflexive, symmetric, and transitive. Given a set A, we denote the set of all equivalence relations on A by $\mathrm{Eq}(A)$.

B.2 Functions

A ***function*** (or mapping) is a relation F such that for each x in $\operatorname{dom} F$ there is only one y such that $x\,F\,y$.

The following operations are most commonly applied to functions, are sometimes applied to relations, but can actually be defined for arbitrary sets A, F, and G.

(a) The ***inverse*** of F is the set

$$F^{-1} = \{(u, v) \mid v\,F\,u\} = \{(u, v) \mid (v, u) \in F\}.$$

(b) The ***composition*** of F and G is the set

$$F \circ G = \{(u, v) \mid \exists t\,(u\,G\,t\ \&\ t\,F\,v)\} = \{(u, v) \mid \exists t\ ((u, t) \in G\ \&\ (t, v) \in F)\}.$$

(c) The ***restriction*** of F to A is the set

$$F \restriction A = \{(u, v) \mid u\,F\,v\ \&\ u \in A\} = \{(u, v) \mid (u, v) \in F\ \&\ u \in A\}.$$

(d) The ***image*** of A under F is the set

$$F[A] = \operatorname{ran}(F \restriction A) = \{v \mid (\exists u \in A)\ (u, v) \in F\}.$$

$F[A]$ can be characterized more simply when F is a function and $A \subseteq \operatorname{dom} F$; in this case

$$F[A] = \{F(u) \mid u \in A\}.$$

In each case we can easily apply a subset axiom to establish the existence of the desired set. Specifically,

$$F^{-1} \subseteq \operatorname{ran} F \times \operatorname{dom} F, \quad F \circ G \subseteq \operatorname{dom} G \times \operatorname{ran} F, \quad F \restriction A \subseteq F, \quad F[A] \subseteq \operatorname{ran} F.$$

(A more detailed justification of the definition of F^{-1} would go as follows: By a subset axiom there is a set B such that for any x,

$$x \in B \quad \Longleftrightarrow \quad x \in \operatorname{ran} F \times \operatorname{dom} F \;\&\; \exists u\, \exists v\, (x = (u, v) \;\&\; (v, u) \in F).$$

It then follows that

$$x \in B \quad \Longleftrightarrow \quad \exists u\, \exists v\, (x = (u, v) \;\&\; (v, u) \in F).$$

This unique set B we denote by F^{-1}.)

Example B.1. Let

$$F = \{(\varnothing, a), (\{\varnothing\}, b)\}.$$

Observe that F is a function. We have $F^{-1} = \{(a, \varnothing), (b, \{\varnothing\})\}$. Thus, F^{-1} is a function iff $a \neq b$. The restriction of F to $\varnothing$ is $\varnothing$, but $F \restriction \{\varnothing\} = \{(0, a)\}$. Consequently, $F[\{\varnothing\}] = \{a\}$, in contrast to the fact that $F(\{\varnothing\}) = b$.

Theorem B.2. *Assume that $F : A \to B$, and that A is nonempty.*

(a) There exists a function $G : B \to A$ (a "left inverse") such that $G \circ F$ is the identity function id_A on A iff F is one-to-one.

(b) There exists a function $H : B \to A$ (a "right inverse") such that $F \circ H$ is the identity function id_B on B iff F maps A onto B.

Axiom of Choice 1. For any relation R there is a function $H \subseteq R$ with $\operatorname{dom} H = \operatorname{dom} R$.

With this axiom we can prove the sufficiency direction of part (b) of the Theorem above: take H to be a function with $H \subseteq F^{-1}$ and $\operatorname{dom} H = \operatorname{dom} F^{-1} = B$. Then H does what we want: Given any $y \in B$, we have $(y, H(y)) \in F^{-1}$ hence $(H(y), y) \in F$, and so $F(H(y)) = y$. □

References

[1] Herbert Enderton. *Elements of set theory.* Academic Press, 1977.

[2] Emmy Noether. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. *Mathematische Annalen*, 96:26–61, 1927.