# Algebraic Structures[⋆]

Ana Sokolova

Department of Computer Sciences, University of Salzburg

anas@cs.uni-salzburg.at

December 12, 2013

Let $A$ be a set and $n$ a natural number. An (algebraic) *operation* of arity $n$ is a map

$$f\colon A^n \to A.$$

In this text, we focus on operations of arity 2, 1, and 0.

- For $n = 2$, $f\colon A^2 \to A$ is a *binary operation* and is usually written in infix notation, using a binary operation symbol like $\cdot$, $*$, or $+$. Hence, instead of $f(a_1, a_2)$ we write $a_1 f a_2$.
- For $n = 1$, $f\colon A \to A$ is a *unary operation*.
- For $n = 0$, $f\colon A^0 \to A$ is a *nullary operation* or a *constant*.

An algebra (or an algebraic structure) is a set $A$, the *carrier*, together with a set of operations on $A$. In addition, the operations may be required to satisfy a set of equations (identities).

Let us take a closer look at nullary operations and clarify the term "constants". As a matter of convention, $A^0$ is a singleton set, usually denoted as $\{*\}$. Hence, a nullary operation is a function $f\colon \{*\} \to A$ and it is uniquely determined by the image $f(*)$ which is a distinguished element of $A$, i.e., a constant.

## Groupoids, Semigroups, Monoids, Groups

A *groupoid* is an algebra with a single binary operation. Hence, it is a set $A$ together with a binary operation $*\colon A^2 \to A$. We denote such a groupoid by $A(*)$ making both the carrier (the set $A$) and the operation $(*)$ explicit. A groupoid $A(*)$ is a *semigroup* if the binary operation is associative, i.e., the following identity holds:

$$\forall x, y, z \in A.\ x * (y * z) = (x * y) * z \qquad \text{[Associativity]}\ .$$

A groupoid is *commutative* if the binary operation is commutative, i.e.,

$$\forall x, y \in A.\ x * y = y * x \qquad \text{[Commutativity]}\ .$$

A groupoid is a *commutative semigroup* if it is both commutative and associative. A groupoid is *left/right cancellative* if the corresponding of the following two implications holds

$$\forall x, y, z \in A.\ x * y = x * z \Rightarrow y = z \qquad \text{[Left cancellation]}$$

[⋆] Simple lecture notes containing basic definitions and examples of algebraic structures. Meant as a preparation material to the Discrete Mathematics course.

$$\forall x, y, z \in A.\ y * x = z * x \Rightarrow y = z \qquad \text{[Right cancellation]}$$

and it is cancellative if it is both left and right cancellative.

*Example 1.* Finite groupoids are easily presented by so-called Cayley tables, like the following groupoid with carrier $A = \{0, 1, 2\}$.

| $*$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 1 | 1 | 1 |
| 1 | 0 | 1 | 2 |
| 2 | 2 | 2 | 2 |

*Remark 1.* Often, if the binary operation is clear from the context one does not explicitly write it and writes instead $xy$ for $x * y$. Moreover, as usual, if quantifiers are omitted in identities, then the variables are assumed to be *universally* quantified, e.g., commutativity is the law $xy = yx$ (and the variables $x$ and $y$ are implicitly universally quantified).

We say that a groupoid $G(*)$ has a *left/right unit* if the corresponding one of the following two propositions holds:

$$\exists e' \in G.\ \forall x \in G.\ e' * x = x \qquad \text{[Left unit]}$$

$$\exists e" \in G.\ \forall x \in G.\ x * e" = x \qquad \text{[Right unit]}\ .$$

It has a unit if

$$\exists e \in G.\ \forall x \in G.\ e * x = x * e = x \qquad \text{[Unit]}\ .$$

Hence a unit is both a left and a right unit.

The groupoid of Example 1 has a left unit 1. A groupoid may have more than one left unit, or more than one right unit. However, if it has both a right and a left unit, then it has a unique unit as shown next.

**Proposition 1.** *If a groupoid $G(*)$ has a left unit $l$ and a right unit $r$, then $l = r$ is a unit of $G(*)$. As a consequence, if a groupoid has a unit, then it has a unique unit.*

*Proof.* Assume $l$ is a left unit of $G(*)$ and $r$ a right unit. Then we have $l = l * r = r$, and clearly this is a unit element. □

A synonym for a unit is *identity element*. In a multiplicative groupoid (operation denoted by $*$ or $\cdot$) with unit, it is common to denote the unit by 1; in an additive groupoid (operation denoted by $+$) with unit, it is usual to denote the unit by 0.

A *monoid* is a semigroup with a unit. To emphesize all operations (also the unit), it is common to write a monoid as a triple, e.g, $(M, +, 0)$ in additive notation or $(M, \cdot, 1)$ in multiplicative notation. A monoid is commutative if the binary operation is commutative; it is (left/right) cancellative if $M(\cdot)$ is a (left/right) cancellative groupoid.

*Example 2.* The following are examples of (commutative) monoids: $(\mathbb{N},\cdot,1)$, $(\mathbb{N},+,0)$, $(\mathbb{Z},\cdot,1)$, $(\mathbb{Z},+,0)$, $(\mathbb{Q},\cdot,1)$, $(\mathbb{Q},+,0)$, $(\mathbb{R},\cdot,1)$, $(\mathbb{R},+,0)$, $(\mathcal{P}(A),\cap,A)$, $(\mathcal{P}(A),\cup,\emptyset)$, for $A$ a given set, as well as $(\{T,F\},\vee,F)$ and $(\{T,F\},\wedge,T)$.

The next definition defines one of the most significant algebraic structures, a group. The theory of groups (and algebra in total) is extremely rich and interesting. For the purpose of this notes, the definition and few examples suffice.

**Definition 1.** *A group $G(\cdot)$ is a set $G$ together with a binary operation $\cdot$ that satisfies the following identities*

$$\begin{aligned} &\textit{[Associativity]} && \forall x,y,z\in G.\ x(yz)=(xy)z\\ &\textit{[Unit]} && \exists e\in G.\ \forall x\in G.\ ex=xe=x\\ &\textit{[Inverse element]} && \forall x\in G.\ \exists x^{-1}\in G.\ xx^{-1}=x^{-1}x=e. \end{aligned}$$

*A group $G(\cdot)$ is commutative or* abelian *if also $\forall x,y\in G.\ xy=yx$.*

Hence, a group is a monoid in which every element is invertible. Note the order of the quantifiers in the unit and inverse laws! The inverse elements are unique, as shown in the following statement.

**Proposition 2.** *Let $(M,\cdot,e)$ be a monoid. If an element $x$ in $M$ is invertible, then there is a unique inverse element, i.e., $xx'=x'x=e\wedge xx"=x"x=e\Rightarrow x'=x"$.*

*Proof.* Let $x$ be invertible and $x'$ and $x"$ be its two inverses, i.e., $xx'=x'x=e$ and $xx"=x"x=e$. Then we have $x'=x'e=x'(xx")=(x'x)x"=ex"=x"$. □

In order to make all operations explicit in the flavor of universal algebra, the following equivalent alternative definition is sometimes preferred.

**Definition 2.** *A group is an algebra $(G,\cdot,(-)^{-1},e)$ with a carrier set $G$ and three operations: a binary operation $\cdot\colon G^2\to G$, a unary operation $(-)^{-1}\colon G\to G$, and constant (nullary operation) $e\in G$ that satisfy the following identities*[1]

$$\begin{aligned} &\textit{[Associativity]} && x(yz)=(xy)z\\ &\textit{[Unit]} && ex=xe=x\\ &\textit{[Inverse element]} && xx^{-1}=x^{-1}x=e. \end{aligned}$$

*As the notation suggests, the image of an element $x\in G$ under the unary operation $(-)^{-1}$ is denoted by $x^{-1}$. In this notation, common elsewhere a well, $(-)$ denotes a hole to be replaced by an argument. A group $(G,\cdot,(-)^{-1},e)$ is commutative or* abelian *if also $xy=yx$.*

Groups are everywhere, some well-known ones are listed in the following example.

[1] Since existential quantifiers are not needed now having made the operations explicit, universal quantifiers can be omitted.

*Example 3.* Examples of groups are $(\mathbb{Z}, +, -(-), 0)$, $(\mathbb{Q}, +, -(-), 0)$, $(\mathbb{R}, +, -(-), 0)$, $(\mathbb{Q} \setminus \{0\}, \cdot, 1/(-), 1)$, $(\mathbb{R} \setminus \{0\}, \cdot, 1/(-), 1)$. Convince yourselves that these are indeed groups! Note that the monoid $(\mathbb{N}, +, 0)$ is not a group, since there are no inverse elements with respect to addition. The additive inverse of an element $x$ of a group, in e.g., $(\mathbb{Z}, +, -(-), 0)$, is denoted as usual by $-x$. The monoid $(\mathbb{Z}, \cdot, 1)$ is not a group since there are no inverse elements with respect to multiplication.

Let $A$ be a set and let $P(A)$ denote the set of all permutations on $A$, i.e.,

$$P(A) = \{f \colon A \to A \mid f \text{ is bijective}\}.$$

Then $(P(A), \circ, (-)^{-1}, id_A)$ is a group, known as the group of permutations on $A$. Convince yourself in this as well. Here, as usual, $\circ$ denotes function composition, $f^{-1}$ is the inverse function of a bijection $f$, and $id_A \colon A \to A$ is the identity function mapping every element to itself.

Let $A$ be a set and let $+$ denote the operation of symmetric difference of sets, i.e, for two subsets $B$ and $C$ of $A$, we have

$$B + C = (B \setminus C) \cup (C \setminus B) = (B \cap C^c) \cup (C \cap B^c).$$

Then $(\mathcal{P}(A), +, id_{\mathcal{P}(A)}, \emptyset)$ is a group.

In the sequel we will use both ways to denote a group as convenient. The following simple property shows the relationship between the unary operation (inverse elements) and the binary operation of a group.

**Proposition 3.** *Let $G(\cdot)$ be a group. Then for any $x, y \in G$ it holds that*

$$(xy)^{-1} = y^{-1}x^{-1}.$$

*Proof.* Let $x, y \in G$. We have, applying associativity and unit law,

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$$

and

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e.$$

□

We next show that every group is cancellative.

**Proposition 4.** *Let $G(\cdot)$ be a group, then it is a cancellative groupoid.*

*Proof.* Let $x, y, z \in G$ be such that $xy = xz$. Then $y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$. Similarly , one proves right cancellation. □

### Subalgebras, congruences, quotients

Let $\mathbb{A}$ be an algebra with a carrier $A$ and a set of operations $\Sigma$. A subset $S$ of $A$ is a *subalgebra*, if it is closed under all operations of $\Sigma$.

In particular, for a groupoid $A(\cdot)$ a subset $S \subseteq A$ is a *subgroupoid*, if for all $x, y \in S$ it holds that $xy \in S$.

A subset $S \subseteq M$ is a *submonoid* of a monoid $(M, \cdot, 1)$ if $1 \in M$ and for all $x, y \in S$ it holds that $xy \in S$, i.e., if it contains the unit (closed under the nullary operation) and is a subgroupoid of $M(\cdot)$.

A subset $S \subseteq G$ is a *subgroup* of a group $(G, \cdot, (-)^{-1}, e)$ if it is closed with respect to multiplication, inverse, and unit, i.e., $e \in S$ and for all $x, y \in S$ we have $x^{-1} \in S$ and $xy \in S$.

*Example 4.* For any algebra $\mathbb{A}$ with carrier $A$, we have $A$ is a subalgebra of itself. For any monoid $(M, \cdot, 1)$ the singleton set $\{1\}$ containing the unit is a submonoid. Also for any group $G(\cdot)$ the singleton set $\{e\}$ containing the unit is a subgroup. These subalgebras are called *trivial*.

Let $\mathbb{A}$ be an algebra with a carrier $A$ and a set of operations $\Sigma$. An equivalence relation $R$ on the carrier $A$ is a *congruence* of the algebra $\mathbb{A}$ if it conforms with all operations of the algebra, i.e., for any $n$-ary operation $f \in \Sigma$ the following implication holds, for any $a_i, b_i \in A, 1 \leq i \leq n$,

$$a_1 R b_1 \wedge \cdots \wedge a_n R b_n \Rightarrow f(a_1, \ldots, a_n) R f(b_1, \ldots, b_n).$$

In particular, for a groupoid $A(\cdot)$, an equivalence relation $R$ on $A$ is a congruence of the groupoid if for all $x, x', y, y' \in A$ satisfying $xRx'$ and $yRy'$, it holds that $xyRx'y'$. Nullary operations have no impact in the definition of a congruence, hence a congruence of a monoid $(M, \cdot, 1)$ is any congruence of the groupoid $M(\cdot)$.

Let $(G, \cdot, (-)^{-1}, e)$ be a group. An equivalence relation $R$ on $G$ is a congruence of the group if for all $x, x', y, y' \in G$, whenever $xRx'$ and $yRy'$ it holds that $x^{-1}Rx'^{-1}$ and $xyRx'y'$.

Congruences allow for a definition of a quotient algebra: its carrier is the quotient of the carrier consisting of all equivalence classes, and the operations are defined representative-wise. To illustrate this notion, we define the quotient of a group.

Let $G(\cdot)$ be a group and $R$ a congruence relation. Then $G/R(\cdot)$ is a group as well where $G/R = \{[x]_R \mid x \in G\}$ and $[x]_R \cdot [y]_R = [xy]_R$. Actually, this statement is a proposition that requires a proof. First of all, note that the congruence condition ensures that the new operation $\cdot$ on $G/R$ (on classes) is well-defined (independent of the choice of a representative of a class). Then one easily sees that the group identities hold. The unit here is the class of the unit of $G$, i.e., $[e]_R$.

*Example 5.* Consider the additive group of integers $\mathbb{Z}(+)$. Each equivalence $\equiv_n$ (for $n \in \mathbb{N}$) defined as $x \equiv_n y \Leftrightarrow n \mid (x - y)$ is a congruence of $\mathbb{Z}(+)$. It is also a congruence of the multiplicative monoid $(\mathbb{Z}, \cdot, 1)$. Hence, one can define the quotient group modulo-$n$ of $\mathbb{Z}(+)$ usually denoted $\mathbb{Z}_n(+_n)$. In the same way, one can define the quotient multiplicative monoid $(\mathbb{Z}_n, \cdot_n, [1]_{\equiv_n})$.

### Rings and Fields

Two other algebraic structures are very common with a rather developed theory. These are rings and fields.

**Definition 3.** *A* ring *is an algebraic structure with two binary operations $R(+,\cdot)$, called addition and multiplication, respectively, such that $R(+)$ is an abelian group (with unit $0$ and inverse element of an element $x$ denoted by $-x$) and $R(\cdot)$ is a semigroup satisfying the following distributive laws of multiplication with respect to addition:*

$$x(y+z) = xy + xz, \qquad (x+y)z = xz + yz$$

*for all $x, y, z \in R$.*

Just like for groups, one can make all operations in a ring explicit and consider it to be the structure $(R, +, -(-), 0, \cdot)$.

*Example 6.* The structure $\mathbb{Z}(+,\cdot)$ of integers with addition and multiplication is a ring. Also the raionals $\mathbb{Q}(+,\cdot)$ and reals $\mathbb{R}(+,\cdot)$ form rings. Also $\mathbb{Z}_n(+_n, \cdot_n)$ from Example 5 is a ring with operations modulo $n$. Actually, it is the quotient ring of $\mathbb{Z}(+,\cdot)$ under the congruence $\equiv_n$.

Let $G(+)$ be any group in additive notation, with unit 0. Setting $xy = 0$ for all $x, y \in G$ one obtains a ring $G(+,\cdot)$ called the zero-ring.

A subset $S$ of a ring $R$ is a *subring* if $0 \in S$ and for all $x, y \in S$ we have $-x, x+y, xy \in S$.

A ring has a unit 1 if the multiplicative semigroup $R(\cdot)$ has a unit 1, i.e., if $(R, \cdot, 1)$ is a monoid.

**Proposition 5.** *If $R$ is a ring with a unit $1$ and at least two different elements, then $0 \neq 1$.*

*Proof.* Assume towards a contradiction that $0 = 1$ and let $x \in R$ be arbitrary. We first show that $x \cdot 0 = 0 = 0 \cdot x$. We have

$$x \cdot 0 + 0 = x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$$

and since we are in an additive group, we can cancel out $x \cdot 0$ and get $0 = x \cdot 0$. Similarly one proves that $0 \cdot x = 0$. Now, using that $0 = 1$, we have $x = x \cdot 1 = x \cdot 0 = 0$ contradicting the assumption that $R$ has at least two different elements. □

A ring is commutative if the multiplicative semigroup $R(\cdot)$ is commutative. A ring is an *integral domain* if it is a commutative ring with unit and has no divisors of zero, i.e., $xy = 0 \Rightarrow x = 0 \vee y = 0$. An example of an integral domain is the ring of integers $\mathbb{Z}(+,\cdot)$. For $n \geq 2$, it is not difficult to show that $\mathbb{Z}_n(+,\cdot)$ is an integral domain if and only if $n$ is a prime number.

**Definition 4.** *A* field *is a commutative ring with a unit in which every non-zero element is invertible. In other words, an algebraic structure $F(+,\cdot)$ is a field if $F(+)$ is an additive group and $F \setminus \{0\}(\cdot)$ is a multiplicative group, where as usual $0$ denotes the unit of the additive group.*

*Example 7.* The rationals $\mathbb{Q}(+,\cdot)$ form a field. Also the reals $\mathbb{R}(+,\cdot)$ do. The latter is a so-called complete field, a condition based on the notion of order on a given field.

## Homomorphisms

A very important notion in algebra (and in other areas of mathematics and computer science where there is a structure to deal with) is the one of a homomorphism, a structure preserving mapping. We present the general definition first and instantiate it then to define groupoid homomorphism, group homomorphism, and ring homomorphism as examples.

Let $\mathbb{A}$ be an algebra with a carrier set $A$ and a set of operations $\Sigma$. Let $\mathbb{B}$ be another algebra of the same type (operations "in" $\Sigma$ as well) with carrier $B$. Let $f$ be an arbitrary operation in $\Sigma$ of arity $n$. Finally, let $f_{\mathbb{A}}$ denote the corresponding operation of $\mathbb{A}$ and $f_{\mathbb{B}}$ the one of $\mathbb{B}$. Then a *homomorphism* is a mapping $h\colon A \to B$ which preserves the operations, i.e.,

$$h(f_{\mathbb{A}}(a_1, \ldots, a_n)) = f_{\mathbb{B}}(h(a_1), \ldots, h(a_n))$$

for all $a_1, \ldots, a_n \in A$.

*Remark 2.* We never made this explicit so far but, as it is evident of the homomorphism definition, a (universal) algebra is given by a carrier set and a set of operational symbols $\Sigma$ of which each is interpreted by a concrete arity-matching operation on the carrier set. Most of the notions introduced so far (in particular homomorphism, subalgebra, or congruence) apply to such a general notion of an algebra. This is the topic of study of an area called universal algebra. It focuses on abstract notions and results that algebras have in common.

More concretely, let $G_1(*)$ and $G_2(\cdot)$ be two groupoids. A mapping $h\colon G_1 \to G_2$ is a (groupoid) homomorphism if and only if for all $x, y \in G_1$ we have

$$h(x * y) = h(x) \cdot h(y).$$

Regarding Remark 2, we see here that a groupoid is an algebra with one binary operation that is interpreted by $*$ in $G_1$ and by $\cdot$ in $G_2$.

Let $G_1(*, (-)^{-1}, e_1)$ and $G_2(\cdot, (-)^{-1}, e_2)$ be two groups. A map $h\colon G_1 \to G_2$ is a (group) homomorphism if for all $x, y \in G_1$ we have

$$h(x * y) = h(x) \cdot h(y), \;\; h(x^{-1}) = (h(x))^{-1}, \;\; \text{and} \;\; h(e_1) = e_2.$$

**Proposition 6.** *Let $G_1(*, (-)^{-1}, e_1)$ and $G_2(\cdot, (-)^{-1}, e_2)$ be two groups. A mapping $h\colon G_1 \to G_2$ is a (group) homomorphism if and only if for all $x, y \in G_1$ we have $h(x * y) = h(x) \cdot h(y)$ and $h(e_1) = e_2$.*

*Proof.* The one direction is obvious. For the other direction, assume $h\colon G_1 \to G_2$ satisfies $h(e_1) = e_2$ and for all $x, y \in G_1$ we have $h(x * y) = h(x) \cdot h(y)$. Let $x \in G_1$. Then

$$h(x) \cdot h(x^{-1}) = h(x * x^{-1}) = h(e_1) = e_2$$

and

$$h(x^{-1}) \cdot h(x) = h(x^{-1} * x) = h(e_1) = e_2$$

showing that $(h(x))^{-1} = h(x^{-1})$. Hence, $h$ is a group homomorphism. □

At this point we can define a ring homomorphism as follows. Let $R_1(+_1, \cdot_1)$ and $R(+_2, \cdot_2)$ be two rings. A mapping $h\colon R_1 \to R_2$ is a (ring) homomorphism if it is a group homomorphism from $R_1(+_1)$ to $R_2(+_2)$ and a groupoid homomorphism from $R_1(\cdot_1)$ to $R_2(\cdot_2)$. In other words, using Proposition 6, if $0_1$ is the zero of $R_1(+_1, \cdot_1)$ and $0_2$ the zero of $R_2(+_2, \cdot_2)$, then a mapping $h\colon R_1 \to R_2$ is a (ring) homomorphism if for all $x, y \in R_1$

$$h(x +_1 y) = h(x) +_2 h(y), \;\; h(0_1) = 0_2, \;\; \text{and} \;\; h(x \cdot_1 y) = h(x) \cdot_2 h(y).$$

Some special homomorphisms are of particular importance. An algebra homomorphism $h$ is a *monomorphism* (or an embedding) if it is an injective function; it is an *epimorphism* if it is a surjective function; and, it is an isomorphism if it is bijective. Two algebras $\mathbb{A}$ and $\mathbb{B}$ are *isomorphic*, notation $\mathbb{A} \cong \mathbb{B}$, if there is an isomorphism between them.

*Example 8.* The following two groups $G_1(*)$ and $G_2(\cdot)$ are isomorphic. Note that the unit of $G_1$ is 0 and the unit of $G_2$ is $a$.

| $G_1(*)$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $G_2(\cdot)$ | a | b |
|---|---|---|
| a | a | b |
| b | b | a |

Here, of course, $G_1 = \{0, 1\}$ and $G_2 = \{a, b\}$. The isomorphism is $i\colon G_1 \to G_2$ given by $i(0) = a$ and $i(1) = b$.

We end these notes with an important isomorphism theorem, which we give without a proof. The interested reader can do the proof herself (it amounts to checking all conditions) or read it in any standard algebra textbook. The theorem applies to universal algebra but we just formulate it for groups.

**Theorem 1.** *Let $G_1(*, (-)^{-1}, e_1)$ and $G_2(\cdot, (-)^{-1}, e_2)$ be two groups and $h\colon G_1 \to G_2$ a (group) homomorphism. Then the following three statements hold*

*(1)* $\ker(h) = \{(x, y) \mid h(x) = h(y)\} \subseteq G_1 \times G_1$
*is a congruence of* $G_1(*, (-)^{-1}, e_1)$*,*

*(2)* $h(G_1)$ *is a subgroup of* $G_2$*, and*

*(3)* $G_1/\ker(h) \cong h(G_1)$.

*where* $G_1/\ker(h)$ *denotes the quotient group of* $G_1(*, (-)^{-1}, e_1)$ *under the congruence* $\ker(h)$*. Since the operations of a quotient group and a subgroup are canonical, we do not write them in (3).*