BASIC STRUCTURES OF ALGEBRA

WAYNE AITKEN

This document gives the definitions of the most common and important structure types used in algebra. Few examples are given, and only properties that follow easily from the definitions are mentioned. It is hoped that this document will serve as a handy reference for those needing a concise, quick source for such definitions.

The definition of each type of structure is divided into two parts: DATA and AXIOMS. The data is a list of objects or information needed to describe the structure, and the axioms describe what needs to be true for the data to qualify as object of the given type.

A common, and reasonable, practice in contemporary mathematics is to give the same name to the structure as a whole and the first, most visible, piece of data for that structure. For example, if G is a group then we also use G to refer to the underlying set of the group. This usually does not lead to confusion, and whenever ambiguity threatens one can add a qualifier, saying, for example, "the group G" in one context and "the set G" in another.

The processes of demonstrating that an object is an example of a certain type of structure is a three step process: (i) describe the data, (ii) show that each piece of data is of the type claimed, and (iii) verify the axioms. Often step (ii) can be skipped when the data is obviously of the correct type. However, step (ii) can turn out to be the most difficult. For example, in most presentations of group theory "closure" is not an axiom for groups, but checking closure is often a critical part of showing that the given product (or sum) is actually a binary operation. As another example, step (ii) sometimes involves showing that a description of a binary operation or other type of function is "well-defined", in other words, that the description really does describe a function of the type claimed.

The only formal prerequisite for this document is a bit of set theory. This document, however, is not an introduction: the reader should have seen several examples of these structures sometime in the past.

1. Terminology and Notation

All interesting algebraic structures use binary operations:

Definition 1.1. If S is a set, then a map $S \times S \to S$ is called a *binary operation*. If a binary operation $S \times S \to S$ is signified by a symbol $*$, then the image of $(a, b) \in S \times S$ under $*$ is typically written $a * b$.

Remark 1.2. If S is a set, then a map $S \to S$ goes by various names: a *unary operation*, a *transformation*, and, if the map is bijective, a *permutation*.

Remark 1.3. We often use *multiplicative notation* for a binary operation $S \times S \to S$. In this case the operation is signified by $\cdot$ and the image of $(a, b) \in S \times S$ under the

Date: December 14, 2005(latest revision: December 14, 2005).

operation is written $a \cdot b$ or simply ab. The operation is then called a *multiplication operation*. The result $a \cdot b$ of the operation is called a *product* (although the term *product* is sometimes used to refer to the operation $\cdot$ itself).

The common alternative is *additive notation*. In this case, the operation is signified by $+$ and the image of $(a, b) \in S \times S$ under the operation is written $a + b$. The operation is then called a *addition operation*. The result $a + b$ of the operation is called a *sum* (although the term *sum* can refer to the operation $+$ itself).

Remark 1.4. The term *map* and *function* are considered synonymous. For maps $f : A \to B$, the adjective *injective* and *one-to-one* are synonymous. The term *one-to-one map* and *injection* are synonymous. For maps $f : A \to B$, the adjective *surjective* and *onto* are synonymous. The term *onto map* and *surjection* are synonymous. A map is said to be *bijective* if it is both injective and surjective. A bijective map is called a *bijection*. Recall, from set theory, that a map has a inverse if and only if it is a bijection.

Definition 1.5. Let $*$ be a binary operation $S \times S \to S$. Then an *identity element* $e \in S$ for $*$ is an element such that $e * a = a * e = a$ for all $a \in S$.

The following is easily proved.

Proposition 1.6. *Let $*$ be a binary operation $S \times S \to S$. Then there is at most one identity element in S for $*$.*

2. Groups

The most important structure type in algebra is the group. Groups often arise from interesting sets of bijections $S \to S$. They also arise from the addition and multiplication operations in number systems.

Definition 2.1. A *group* G is described by the following data and axioms:

Data

(1) A set, called the *underlying set* (denoted here, according to custom, as G).
(2) A binary operation $G \times G \to G$ called the *group operation*. (In what follows, we employ multiplicative notation, although additive notation is also common).

Axioms

(1) (Associativity) For all $a, b, c \in G$,
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$
(2) (Identity) G has an identity element. In other words, there is an identity element for the binary operation of G (which is unique by a previous result).
(3) (Inverse) For all $a \in G$ there is an element b such that $ab = ba = e$ where e is the identity element of G. Such an element b is called the *inverse of* a.

The following makes use of all three axioms.

Proposition 2.2 (Cancellation Laws)**.** *Let $a, b, c \in G$ where G is a group. If $ac = bc$ then $a = b$. If $ca = cb$ then $a = b$.*

Corollary 2.3. *Let $a \in G$ where G is a group. Then a has a unique inverse.*

Definition 2.4. Let $a \in G$ where G is a group. Then the inverse of a is typically denoted as a^{-1}. However, if we are using additive notation, then the inverse is denoted $-a$. In this case, we write $a - b$ for $a + (-b)$.

If we are using multiplicative notation, then the identity is typically written 1. Thus

$$aa^{-1} = a^{-1}a = 1.$$

If we are using additive notation, then the identity is typically written 0. Thus

$$a + (-a) = a - a = 0 \quad (-a) + a = 0.$$

The following is an easy consequence of the above.

Proposition 2.5. *Let G be a group (written, for convenience, in multiplicative notation). The following hold for all $a, b, c \in G$:*

1. *(One-sided inverses are inverses). If $ab = 1$ then $b = a^{-1}$ and $a = b^{-1}$.*
2. *(Double negatives). $(a^{-1})^{-1} = a$.*
3. *(Inverse of Products). $(ab)^{-1} = b^{-1}a^{-1}$.*
4. *(Uniqueness of Solution). Given $a, b \in G$, each of the following has a unique solution: $ax = b$ and $xa = b$.*
5. *(Inverse of identity). $1^{-1} = 1$.*

3. Abelian Groups

Definition 3.1. An *abelian group* A is a group satifying the following additional axiom (written here with additive notation):

Axiom: (Commutativity) For all $a, b \in A$,

$$a + b = b + a.$$

Note. It is a common convention to use additive notation only for abelian groups. So one finds additive and multiplicative notation used for abelian groups, but usually only multiplicative notation for non-abelian groups.

The following is just earlier results translated into additive notation, except part (4) which uses the commutative property to convert to a standard form.

Proposition 3.2. *Let A be an abelian group written in additive notation. The following hold for all $a, b, c \in A$.*

1. *(Cancellation Law). If $a + c = b + c$ then $a = b$.*
2. *(Inverse). If $a + b = 0$ then $b = -a$.*
3. *(Double Negatives). $-(-a) = a$.*
4. *(Inverse of Sums). $-(a + b) = (-a) + (-b)$.*
5. *(Uniqueness of Solution). Given $a, b \in A$, the equation $a + x = b$ has a unique solution.*
6. *(Inverse of identity). $-0 = 0$.*

4. Rings

Most of the familiar number systems, including the integers, the rational numbers, the real numbers, and the complex numbers are examples of rings. Matrices and polynomials give other basic examples.

Definition 4.1. A *ring* R is described by the following data and axioms:

Data

(1) (Addition) An abelian group R called the *additive group*. As suggested by this terminology, additive notation is used for this group.
(2) (Multiplication) A binary operation $R \times R \to R$ called *multiplication*. Multiplicative notation is typically used for this operation.

Axioms[1]

(1) (Associativity of Multiplication) For all $a, b, c \in R$,
$$a(bc) = (ab)c.$$
(2) (Unity) The multiplication operation has an identity element.[2]
(3) (Distributivity) For all $a, b, c \in R$
$$a(b + c) = ab + ac, \quad \text{and} \quad (b + c)a = ba + ca.$$

Note. The identity element for multiplication is often called the *unity element* of R. It is unique by an earlier result. The unity element is typically denoted by 1.

The following are easy consequence of the definition.

Proposition 4.2. *Let R be a ring. For all $a, b \in R$,*
$$0a = a0 = 0, \quad -(ab) = (-a)b = a(-b), \quad (-1)a = -a \quad (-a)(-b) = ab.$$

Proposition 4.3. *A ring R has exactly one element if and only if $0 = 1$.*

Note. A ring with exactly one element is called a *trivial ring*.

5. Commutative Rings

Most of the familiar rings, including the integers, the rational numbers, the real numbers, the complex numbers, and polynomials rings (usually), are examples of commutative rings. Matrices and quaternions give examples of interesting rings which are not commutative.

Definition 5.1. A *commutative ring* R is a ring satisfying the following additional axiom:

Axiom: (Commutivity of Multiplication) For all $a, b \in R$,
$$ab = ba.$$

6. Integral Domains

Most of the familiar rings, including the integers, the rational numbers, the real numbers, the complex numbers, and most commonly used polynomials rings, are examples of integral domains. Such rings are convenient to work with since one can use familiar cancellation law from traditional algebra.

Definition 6.1. A *integral domain* R is a commutative ring satisfying the following addition axioms.

Axioms

(1) For all $a, b \in R$, if $ab = 0$ then $a = 0$ or $b = 0$.
(2) $0 \neq 1$.

[1]Of course, the data implicitly includes all the group axioms for $+$.

[2]Some authors do not require the unity axiom, but there is not much to be gained by the added generality. If R satisfies all the axioms except possibly the unity axiom, we will call R a *rng*.

Proposition 6.2. *Let R be a commutative ring. Then R is an integral domain if and only if the set of non-zero elements of R is non-empty and closed under multiplication.*

Proposition 6.3. *Let R be a commutative ring with $0 \neq 1$. Then R is an integral domain if and only if the following cancellation rule holds (for all $a, b, c \in R$):*

$$\text{if } ca = cb \text{ and } c \neq 0 \text{ then } a = b.$$

7. Fields

Number systems, including the rational numbers, the real numbers, and the complex numbers, allow division by any non-zero element. Such number systems are examples of fields. Not all traditional number systems form a field: the ring of integers is not a field.

Definition 7.1. Let u be an element of a ring R. If $w \in R$ is such that $uw = wu = 1$ then w is called a *multiplicative inverse* of u.

Proposition 7.2. *Let R be a ring. Any element $u \in R$ has at most one multiplicative inverse.*

Definition 7.3. Let u be an element of a ring R. The multiplicative inverse of u, if it exists, is written u^{-1}.

Proposition 7.4. *If R is not a trivial ring, then 0 does not have a multiplicative inverse.*

A field is a non-trivial commutative ring that has as many multiplicative inverses as possible:

Definition 7.5. A field F is a commutive ring satisfying the following:

Axioms

(1) Every non-zero element of F has a multiplicative inverse.
(2) $0 \neq 1$.

Proposition 7.6. *Every field is an integral domain.*

So a field can be defined to be an integral domain with the property that every non-zero element has an inverse.

8. The units group of a ring

A ring with its addition operation is a group. The multiplication operation of a ring can also be used to form a group, but in this case one has to restrict to a subset of the ring.

Definition 8.1. Let R be a ring. An unit in R is an element u that has an inverse. The set of units of R is written $R^\times$.

Proposition 8.2. *Let R be a ring. Then $1 \in R^\times$ and $1^{-1} = 1$. If $u \in R^\times$ then $u^{-1} \in R^\times$ and $(u^{-1})^{-1} = u$.*

Proposition 8.3. *Let R be a ring. Then the multiplicative operation $R \times R \to R$ restricts to a binary operation $R^\times \times R^\times \to R^\times$. In fact, if $u, w \in R^\times$ then $(uw)^{-1} = w^{-1}u^{-1}$.*

Proposition 8.4. *Let R be a ring. The set of units $R^\times$ is a group under multiplication. The identity element is* 1.

Definition 8.5. Let R be a ring. The group $R^\times$ is called the *unit group of R*. Obviously if R is a commutative ring, then $R^\times$ is an abelian group.

The following is an alternate characterization for fields:

Proposition 8.6. *Let R be a ring. Then R is a field if and only if (i) $R^\times = R - \{0\}$ and (ii) $R^\times$ is an abelian group.*

9. Modules and Vector Spaces

Definition 9.1. Let R be a ring. An *R-module* M is described by the following data and axioms:

Data

(1) (Additive Group) An abelian group M called the *additive group*. We typically use additive notation for M.
(2) (Scalar Multiplication) A map $R \times M \to M$ called *scalar multiplication*. Typically $a \cdot v$ and av denote the image of (a, v) under this map.

Axioms

(1) (Associativity) For all $a, b \in R$ and $v \in M$,
$$a(bv) = (ab)v.$$
(2) (Unity) For all $v \in M$
$$1v = v.$$
(3) (Distributivity 1) For all $a, b \in R$ and $v \in M$
$$(a + b)v = av + bv.$$
(4) (Distributivity 2) For all $a \in R$ and $u, v \in M$
$$a(u + v) = au + av.$$

Note. We often use the phrase *module over R* instead of *R-module*. If R is understood, then the term *module* may be used as well.

The following is an easy consequence of the definition. (Here 0 sometimes refers to an element of R and sometimes an element of M: context should make it clear what it denoted. Likewise, $-$ has two meanings.)

Proposition 9.2. *Let M be an R-module. For all $a \in R$ and $v \in M$,*
$$0v = 0, \quad a0 = 0, \quad -(av) = (-a)v = a(-v), \quad (-1)v = -v.$$

Remark 9.3. We sometimes use the phrase *left R-module* for R-modules since elements of R are written to the left of elements of the module. We can define the notion of a right R-module in a symmetric manner. This distinction is important if R is a non-commutative ring, but is just a notational distinction if R is a commutative ring (in that case, we can make any right module into a left module by *defining* av to be va).

Remark 9.4. If F is a field, then an F-module is usually called a *vector space over F* or an *F-vector space*.