

The Initial Definitions of Algebra.

Definition 1. (Power of a set) If A is a set and n is a natural number, then $A^n = \{(a_1, \dots, a_n) \mid a_i \in A\}$. Members of A^n are called *n-tuples*. The element a_i is called the *i*th coordinate of (a_1, \dots, a_n) .

To lighten notation we might abbreviate (a_1, \dots, a_n) by \mathbf{a} .

One thing that might be mysterious about Definition 1 is what happens when $n = 0$. There is one 0-tuple of elements of A , and this is independent of the choice of A . The only 0-tuple for any set is the empty set, \emptyset . This can be taken as a convention or even be derived from a refined version of Definition 1. Hence $A^0 = \{\emptyset\}$ for any set A , and in particular $|A^0| = 1$.

Definition 2. (Operation) Let A be a set. An *n-ary operation on A* is a function

$$f: A^n \rightarrow A.$$

The *arity* of f is n .

So, an n -ary operation f accepts an input $\mathbf{a} \in A^n$ (or an n -tuple of inputs from A) and produces an output $f(\mathbf{a})$.

Operations can be 0-ary, 1-ary, 2-ary, etc. It is more common to use the language “nullary, unary, binary, ternary, quaternary/4-ary, 5-ary, etc.”

Again, the most mysterious part of the definition is how to interpret it when $n = 0$. A 0-ary operation on A is a function $f: \{\emptyset\} \rightarrow A$, which does nothing more than select a fixed element $f(\emptyset) \in A$. It is common to treat 0-functions not as functions, but rather as distinguished elements (like $0 \in \mathbb{Z}$).

Definition 3. (Algebra) An *algebra*, or *algebraic structure*, is a structure

$$\mathbb{A} = \langle A; f_1, f_2, \dots \rangle$$

where A is a set and each f_i is an operation on A . A is called the *universe* or *underlying set* of the algebra.

Examples 4. (1) $\mathbb{Z} = \langle \mathbb{Z}; +, -, 0 \rangle$.

(2) $\mathbb{Z} = \langle \mathbb{Z}; \cdot, +, -, 0 \rangle$. This example is different than the preceding one, even though we usually denote them both \mathbb{Z} .

(3) $\mathbb{Q} = \langle \mathbb{Q}; +, -, 0 \rangle$. This is different from all of the above, but is the same “type” as the first example.

(4) $\mathbb{R} = \langle \mathbb{R}; \cdot, +, -, 0 \rangle$. This is different from all of the above, but is the same “type” as the second example.

Identifying the type of an algebra is important if you want to compare two algebras.

Definition 5. A *type* (or *signature*) is a pair $(\mathcal{F}, \text{arity})$ where \mathcal{F} is a set of function symbols and $\text{arity}: \mathcal{F} \rightarrow \{0, 1, 2, \dots\}$ is a function assigning arity.

For the examples above, the types are

- (1) $\mathcal{F} = \{+, -, 0\}$, $\mathbf{arity}(+) = 2$, $\mathbf{arity}(-) = 1$, $\mathbf{arity}(0) = 0$.
- (2) $\mathcal{F} = \{\cdot, +, -, 0\}$, $\mathbf{arity}(\cdot) = 2$, $\mathbf{arity}(+) = 2$, $\mathbf{arity}(-) = 1$, $\mathbf{arity}(0) = 0$.
- (3) $\mathcal{F} = \{+, -, 0\}$, $\mathbf{arity}(+) = 2$, $\mathbf{arity}(-) = 1$, $\mathbf{arity}(0) = 0$.
- (4) $\mathcal{F} = \{\cdot, +, -, 0\}$, $\mathbf{arity}(\cdot) = 2$, $\mathbf{arity}(+) = 2$, $\mathbf{arity}(-) = 1$, $\mathbf{arity}(0) = 0$.

To emphasize, the role of the “type” is to determine whether two algebras can be compared. In any discussion about algebra one typically assumes that all algebras involved have the same type, and thereafter the type plays little role.

Definition 6. (Interpretation) If $f \in \mathcal{F}$ has arity n , and \mathbf{A} is an algebra of type $(\mathcal{F}, \mathbf{arity})$, then the interpretation of the symbol f in \mathbf{A} is the function $f^{\mathbf{A}}: A^n \rightarrow A$ associated with the symbol f .

The difference between f and $f^{\mathbf{A}}$ is essentially this: f is just a symbol, while $f^{\mathbf{A}}$ is a concrete function. (That is, $f^{\mathbf{A}}$ “knows” its operation table.)

Definition 7. (Homomorphism) A *homomorphism* $h: \mathbf{A} \rightarrow \mathbf{B}$ between two algebras of the same type $(\mathcal{F}, \mathbf{arity})$ is a set-function $h: A \rightarrow B$ from the universe of \mathbf{A} to the universe of \mathbf{B} which *preserves* each operation $f \in \mathcal{F}$ in the sense that

$$h(f^{\mathbf{A}}(a, \dots, a_n)) = f^{\mathbf{B}}(h(a_1), \dots, h(a_n)).$$

If the inverse $h^{-1}: B \rightarrow A$ of the set-function $h: A \rightarrow B$ exists, and is a homomorphism,¹ then h is called an *isomorphism*.

Examples/problems:

- (1) Consider $\mathbb{Z} = \langle \mathbb{Z}; +, -, 0 \rangle$ be the additive group of integers. Show that the doubling map

$$h: \mathbb{Z} \rightarrow \mathbb{Z}: n \mapsto 2n$$

is a homomorphism that is not an isomorphism.

- (2) Show that the maps $\mathbb{Z} \rightarrow \mathbb{Z}: n \mapsto n$ and $\mathbb{Z} \rightarrow \mathbb{Z}: n \mapsto -n$ are isomorphisms.

¹More will be said about this later.