1 Algebras

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 $f^A \in F$ are called the fundamental operations of $\mathbf{A}$. (In practice we prefer to write $f$ for $f^A$ 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 $\mathbf{A}$ can be obtained from $\mathbf{B}$ by simply adding more operations.

1.1 Examples

groupoid $\mathbf{A} = \langle A, \cdot \rangle$

An algebra with a single binary operation is called a groupoid. This operation is usually denoted by $+$ or $\cdot$, and we write $a + b$ or $a \cdot b$ (or just $ab$) for the image of $\langle a, b \rangle$ 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 $e \cdot a = a = e$, 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 $a, b \in A$.

ring $\mathbf{A} = \langle A, +, -, 0 \rangle$

A ring is an algebra $\mathbf{A} = \langle A, +, -, 0 \rangle$ such that

R1. $\langle A, +, - \rangle$ is an Abelian group,

R2. $\langle A, \cdot \rangle$ is a semigroup, and

R3. for all $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

A ring with unity (or unital ring) is an algebra $\mathbf{A} = \langle A, +, -, 0, 1 \rangle$, where the reduct $\langle A, +, -, 0 \rangle$ is a ring, and where $1$ is a multiplicative identity; i.e. $a \cdot 1 = 1 \cdot a = a$, for all $a \in A$.

field If $\mathbf{A} = \langle A, +, -, 0, 1 \rangle$ is a ring with unity, an element $r \in A$ is called a unit if it has a multiplicative inverse. That is, $r \in A$ is a unit provided there exists $r^{-1} \in A$ with $r \cdot r^{-1} = r^{-1} \cdot r = 1$. A division ring is a ring in which every non-zero element is a unit, and a field is a division ring in which multiplication is commutative.

---

1. N.B. In this first paragraph, not all of the definitions are entirely precise. Rather, my goal here is to state them in a way that seems intuitive and heuristically useful.

2. This convention creates an ambiguity when discussing, for example, homomorphisms from one algebra, $\mathbf{A}$, to another, $\mathbf{B}$; in such cases we will adhere to the more precise notation $f^A$ and $f^B$, for operations on $A$ and $B$, respectively.
1.2 Vector Spaces, Modules, and Bilinear Algebras

Let \( R = \langle R, +, \cdot, 0, 1 \rangle \) be a ring with unit. An \( R \)-module (sometimes called a left unitary \( R \)-module) is an algebra \( M = \langle M, +, - , 0, f_r \rangle_{r \in R} \) with an Abelian group reduct \( \langle M, +, - , 0 \rangle \), and with unary operations \((f_r)_{r \in R}\) which satisfy the following four conditions for all \( r, s \in R \) and \( x, y \in M \):

\[
\begin{align*}
M1. \quad f_r(x + y) &= f_r(x) + f_r(y) \\
M2. \quad f_{r+s}(x) &= f_r(x) + f_s(x) \\
M3. \quad f_r(f_s(x)) &= f_{rs}(x) \\
M4. \quad f_1(x) &= x.
\end{align*}
\]

If the ring \( R \) happens to be a field, an \( R \)-module is typically called a vector space over \( R \).

Note that condition M1 says that each \( f_r \) is an endomorphism of the Abelian group \( \langle M, +, - , 0 \rangle \). Conditions M2–M4 say: (1) the collection of endomorphisms \((f_r)_{r \in R}\) is itself a ring with unit, where the function composition described in (M3) is the binary multiplication operation, and (2) the map \( r \mapsto f_r \) is a ring epimorphism from \( R \) onto \((f_r)_{r \in R}\).

Part of the importance of modules lies in the fact that every ring is, up to isomorphism, a ring of endomorphisms of some Abelian group. This fact is analogous to the more familiar theorem of Cayley stating that every group is isomorphic to a group of permutations of some set.

Let \( F = \langle F, +, \cdot, 0, 1 \rangle \) be a field. An algebra \( A = \langle A, +, \cdot, 0, f_r \rangle_{r \in F} \) is a bilinear algebra over \( F \) provided \( \langle A, +, \cdot, 0, f_r \rangle_{r \in F} \) is a vector space over \( F \) and for all \( a, b, c \in A \) and all \( r \in F \),

\[
\begin{align*}
(a + b) \cdot c &= (a \cdot c) + (b \cdot c) \\
c \cdot (a + b) &= (c \cdot a) + (c \cdot b) \\
a \cdot f_r(b) &= f_r(a \cdot b) = f_r(a) \cdot b
\end{align*}
\]

If, in addition, \((a \cdot b) \cdot c = a \cdot (b \cdot c)\) for all \(a, b, c \in A\), then \(A\) is called an associative algebra over \(F\). Thus an associative algebra over a field has both a vector space reduct and a ring reduct. An example of an associative algebra is the space of linear transformations (endomorphisms) of any vector space into itself.

1.3 Congruence Relations and Homomorphisms

Let \( A \) be a set. A binary relation \( \theta \) on \( A \) is a subset of \( A^2 = A \times A \). If \( \langle a, b \rangle \in \theta \) we sometimes write \(a \theta b\). The diagonal relation on \( A \) is the set \( \Delta_A = \{ \langle a, a \rangle : a \in A \} \) and the all relation is the set \( \nabla_A = A^2 \). (We write \( \Delta \) and \( \nabla \) when the underlying set is apparent.)

A binary relation \( \theta \) on a set \( A \) is an equivalence relation on \( A \) if, for any \( a, b, c \in A \), it satisfies:

\[
\begin{align*}
E1. \quad \langle a, a \rangle &\in \theta, \\
E2. \quad \langle a, b \rangle \in \theta &\text{ implies } \langle b, a \rangle \in \theta, \text{ and} \\
E3. \quad \langle a, b \rangle \in \theta &\text{ and } \langle b, c \rangle \in \theta \text{ imply } \langle a, c \rangle \in \theta.
\end{align*}
\]

We denote the set of all equivalence relations on \( A \) by \( Eq(A) \).

If \( \theta \in Eq(A) \) is an equivalence relation on \( A \) and \( \langle x, y \rangle \in \theta \), we say that \( x \) and \( y \) are equivalent modulo \( \theta \). The set of all \( y \in A \) that are equivalent to \( x \) modulo \( \theta \) is denoted by \( x/\theta = \{ y \in A : \langle x, y \rangle \in \theta \} \) and we call \( x/\theta \) the equivalence class (or coset) of \( x \) modulo \( \theta \). The set \( \{ x/\theta : x \in A \} \) of all equivalence classes of \( A \) modulo \( \theta \) is denoted by \( A/\theta \). Clearly equivalence classes form a partition of \( A \), which simply means that \( A = \bigcup_{x \in A} x/\theta \) and \( x/\theta \cap y/\theta = \emptyset \) if \( x/\theta \neq y/\theta \).

to be continued...