Algebra

Adam Yin

A glossary reference for Algebra and related terms. [1] [2]

Glossary

Cayley's Theorem Every group G is isomorphic to a subgroup of the symmetric group acting on G.
Note: The same can be stated about monoids and monoid actions.

Equivariant Map is a function that commutes with the action of the group on either its domain or codomain. Thus, for a group G and an equivariant map $\phi : S \to T$ for sets S and T:

$$\forall g \in G, \forall s \in S, g\phi(s) = \phi(gs)$$

Field is a set F of two or more elements, together with the two operations called addition ($+$) and multiplication ($\bullet$) and satisfies the following axioms:

(A_1) Closure: $a,b \in F \Rightarrow a+b \in F$

(A_2) Associative Law: $a,b,c \in F \Rightarrow (a+b)+c = a+(b+c)$

(A_3) (Additive) Identity: $\exists 0 \in F$ such that $0+a = a+0 = a, \forall a \in F$

(A_4) (Additive) Inverse: $a \in F \Rightarrow \exists -a \in F$ such that $a+(-a) = (-a)+a = 0$

(A_5) Commutative Law: $a,b \in F \Rightarrow a+b = b+a$

(M_1) Closure: $a,b \in F \Rightarrow a \bullet b \in F$

(M_2) Associative Law: $a,b,c \in F \Rightarrow (a \bullet b) \bullet c = a \bullet (b \bullet c)$

(M_3) (Multiplicative) Identity: $\exists 1 \in F$ such that $1 \bullet a = a \bullet 1 = a, \forall a \in F$

(M_4) (Multiplicative) Inverse: $a \in F, a \neq 0 \Rightarrow \exists a^{-1} \in F$ such that $a \bullet a^{-1} \bullet a = a \bullet a^{-1} = 1$

(M_5) Commutative Law: $a,b \in F \Rightarrow a \bullet b = b \bullet a$

(D_1) Left Distributive Law: $a,b,c \in F \Rightarrow a \bullet (b+c) = a \bullet b + a \bullet c$

(D_2) Right Distributive Law: $a,b,c \in F \Rightarrow (b+c) \bullet a = b \bullet a + c \bullet a$

With the following algebraic properties:

1. The identity elements 0 and 1 are unique
2. The following cancellation laws hold:

$$(1)\ a+b = a+c \Rightarrow b+c,\ (2)\ a \bullet b = a \bullet c, a \neq 0 \Rightarrow b = c$$

3. The inverse elements $-a$ and a^{-1} are unique.
4. For every $a,b \in F$

$$(1)\ a \bullet 0 = 0,\ (2)\ a \bullet (-b) = (-a) \bullet b = -(a \bullet b),\ (3)\ (-a) \bullet (-b) = a \bullet b$$

Subtraction: is defined as $b - a \equiv b + (-a)$
Division: (by a non-zero element) is defined as $\frac{b}{a} \equiv b \bullet a^{-1}$

Group Action is a way of interpreting elements of group "acting" on some space, thus if G is a group and X is a set, the action of G on X is a group homomorphism from G to the symmetry group on X. The group action $\alpha : G \times X \to X$ may be defined as follows:

- $\alpha(1,x) = x$ where 1 is the identity in G for any $x \in X$
  Also written as: $1x = x$
- $\alpha(gh,x) = \alpha(g,\alpha(h,x))$ for all $g,h \in G, x \in X$
  Also written as: $(gh)x = g(hx)$

Note: A similar construct can be defined for monoids.
Note: One way to think of group actions would be the set X is a *state space* and elements of G acting on X induces *transitions* from one state to another.

Identity Element An element $e \in \Omega$ is said to be an **identity element** under the binary operator o if and only if $\forall a \in \Omega$:

$$a \circ e = e \circ a = a$$

In order for e to be an **identity element**, e must statisfy the following:

1. $e \in \Omega$
2. $\forall a \in \Omega, a \circ e = a$
3. $\forall a \in \Omega, e \circ a = a$

ie: the identity element e must be in Ω and commute with every element in Ω.
Note: if the binary operator $\circ$ is abelian, only conditions 1. and 2. or 3. is necessary.
To prove, let $a \in \Omega$ be arbitrary but fixed. Compute $a \circ x$, $x \circ a$ and solve for x where $a \circ x = x \circ a$. Show that $x \in \Omega$ does not depend on a. Conclude $e = x$ is an identity element in Ω under the binary operator $\circ$.
Theorem: If Ω is closed under the $\circ$ binary operation and e is an identity element under $\circ$, then e is unique

Inverse Element An element $a \in \Omega$ is said to have an **inverse element** $a^{-1} \in \Omega$ under the binary operator $\circ$ if and only if:

$$a \circ a^{-1} = a^{-1} \circ a = e$$

where e is the identity element in Ω.

To prove, determine the identity element e and let $a \in \Omega$ be arbitrary but fixed. Compute $a \circ x$, $x \circ a$, solve for x where $a \circ x = e = x \circ a$ and show that $x \in \Omega$. Conc that $a^{-1} = x$ is the inverse of the element a under the binary operator $\circ$.
Theorem: Let o be an associative binary operator. If Ω is closed under $\circ$ and $a^{-1} \in \Omega$ whenever $a \in \Omega$, then a^{-1} is unique
Theorem: If Ω is closed under $\circ$ and $a^{-1} \in \Omega$ whenever $a \in \Omega$, then $(a^{-1})^{-1} = a$

Ring is a non-empty set together with two operations that satisfy all the axioms of a field except (M_3), (M_4) and (M_5).

Example: $\mathbb{Z}$, the set of integers under addition and multiplication is a ring but not a field.

References

[1] Charles Wells Michael Barr. *Category Theory for Computing Science*. Reprints in Theory and Applications of Categories #22. 2013.

[2] Lipschutz S. *Theory and applications of general topology*. Schaum's outlines. 1965.