2 Groups (09/22)

Algebraic structures are sets equipped with additional structures, often binary operations, which satisfy certain properties and are viewed as being part of the data of the algebraic structure.

Definition 2.1 (Magmas)**.** A **magma** M is a pair $(S, \cdot)$ where S is a set and $\cdot$ is a binary operation on S. The binary operation could also be written as $+$ or $\bullet$ or $\star$, etc.

Notation 2.2. It is very convenient to write M for the magma *and* the underlying set. So, a magma M will be a set M equipped with a binary operation on M. This is an abuse of notation, but is harmless and will make everything a bit prettier.

Remark 2.3. While a set has varying binary operations, a magma has a single binary operation which is singled out and viewed as fixed.

Definition 2.4 (Types of magmas)**.** In general, one can say that a magma is commutative, associative, unital, and so forth if its binary operation has that property. In many cases, magmas possessing these properties have special names.

(a) A **semigroup** is an associative magma.

(b) A **monoid** is a unital semigroup (a unital associative magma).

(c) A **group** is a monoid which has inverses (a unital associative magma with inverses).

(d) An **abelian group** is a group whose underlying magma is commutative.[1]

(e) A **quasigroup** is a magma with the Latin square property.

(f) A **loop** is a unital quasigroup.

This course will focus on the theory of groups, although monoids are also sometimes useful.

Definition 2.5. A **finite group** is a group whose underlying set is finite.

Example 2.6. The set $\mathbf{N} = \{0, 1, 2, \cdots\}$ of natural numbers is a commutative monoid under addition. It is not a group.

Example 2.7. The set $\mathbf{Z} = \{0, \pm 1, \pm 2, \cdots\}$ of integers under addition is an abelian group. Unless otherwise specified, when we speak of $\mathbf{Z}$ we will always mean this particular group.

Warning 2.8. There is another natural binary operation on $\mathbf{Z}$: multiplication. Under this operation, $(\mathbf{Z}, \cdot)$ is a commutative monoid, but it is not a group. Taken together, the triple $(\mathbf{Z}, +, \cdot)$ forms a **ring**: a set with an abelian group structure under $+$, a monoid structure under $\cdot$, and where $+$ and $\cdot$ interact in a prescribed way via the **distributivity laws**: $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$. This particular ring is commutative because the multiplicative monoid is. These algebraic structures are the subject of the second quarter of this sequence.

Example 2.9. The sets $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, and $\mathbf{R}^n$ under (vector) addition are abelian groups.

Example 2.10. If k is a field and V is a k-vector space, then addition makes V into an abelian group.

Example 2.11. If $G = \{e\}$ is a set with a single element, e, then the unique binary operation on G (specified by $e \cdot e = e$) makes G into a group (with identity element e).

[1] One could call these commutative groups, but for historical reasons, abelian groups are used instead.

Example 2.12. The empty set $\emptyset$ also admits a unique binary operation $\emptyset \times \emptyset \to \emptyset$. It is commutative, associative, and has the Latin square property, but is not unital as unitality asserts the existence of an element. So, it is a semigroup and a quasigroup, but it is not a group.

Now, we introduce two of the most important examples of groups: addition modulo N and symmetric groups.

Lemma 2.13. *Fix a positive integer $N \geqslant 1$. Let $\mathbf{Z}/N$ be the set $\{0, 1, \ldots, N-1\}$. The binary operation on $\mathbf{Z}/N$ defined by letting $a +_N b = r$ where r is the unique integer in $\{0, \ldots, N-1\}$ such that $a + b \equiv r \mod N$ makes $\mathbf{Z}/N$ into an abelian group.*

Proof. The existence and uniqueness of c follows from the fact that for $c \in \mathbf{Z}$ there are unique integers q and $r \in \{0, \ldots, N-1\}$ such that $c = qN + r$ (this is often called **Euclidean division**). Applying this to $c = a + b$ (where the sum is computed in $\mathbf{Z}$) produces q and r such that $a + b = qN + r$. We define $a +_N b = r$. This operation is commutative since $a + b = b + a = qN + r$, so $a +_N b = b +_N a$ and unital since $a + 0 = 0 + a = 0 \cdot N + a = a$ for $a \in \{0, \ldots, N-1\}$, so $a +_N 0 = 0 +_N a = a$. The inverse of a is computed by finding $r \in \{0, \ldots, N-1\}$ such that $-a = qN + r$. Then, $0 = a + r = a + qN + r$ is divisible by N so that $a + r = N$ and hence $a + r = (q+1)N + 0$, so $a +_N r = 0$. Thus, $+_N$ has inverses. For associativity, suppose that $a + b = q_0 N + r_0$ and $b + c = q_1 N + r_1$, where $r_0, r_1 \in \{0, \ldots, N-1\}$. Then, assume that $r_0 + c = q_2 N + r_2$ and $a + r_1 = q_3 N + r_3$ for $r_2, r_3 \in \{0, \ldots, N-1\}$. Then, by associativity of addition on $\mathbf{Z}$,

$$(q_1 + q_3)N + r_3 = a + q_1 N + r_1 = a + b + c = q_0 N + r_0 + c = (q_0 + q_1)N + r_2.$$

By uniqueness of the remainder, we must have $r_3 = r_2$, so that $a +_N (b +_N c) = (a +_N b) +_N c$, which proves associativity and finally that $\mathbf{Z}/N$ is an abelian group. $\square$

Notation 2.14. We will typically write $a + b \equiv c \mod N$ instead of $a +_N b = c$ when working in $\mathbf{Z}/N$.

Example 2.15. The Cayley table of $\mathbf{Z}/3$ was already introduced in Remark 1.8. We reproduce it here for convenience.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table 1: The Cayley table of $\mathbf{Z}/3$.

2.1 Exercises

Exercise 2.1. An associative loop is a group. Show that there exist non-associative loops.

Exercise 2.2. Let G be a group and fix $a \in G$. Prove that $(a^{-1})^{-1} = a$.

Exercise 2.3. Let G be a group and fix $a, b \in G$. Prove that $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Exercise 2.4. Let G be a group with identity element e and fix $a \in G$ and $n \in \mathbf{Z}$. Set $a^0 = e$. For $n > 0$, define a^n inductively by $a^n = a \cdot a^{n-1}$. For $n < 0$, define $a^n = (a^{-n})^{-1}$. One has $a^m \cdot a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for $m, n \in \mathbf{Z}$. Prove that if G is abelian, then $(a \cdot b)^n = a^n \cdot b^n$ for all $a, b \in G$.

Exercise 2.5. Let G be a finite group with identity element e. Show that there exists an integer $n > 0$ such that $a^n = e$ for all $a \in G$.