MATH 436 Notes: Binary Operations, Monoids and Examples.

Jonathan Pakianathan

September 12, 2003

1 Binary Operations

One of the most basic operations in algebra is that of a binary operation on a set. A binary operation $\star$ on a set S is a mapping $\star : S \times S \to S$. Thus for every pair (a, b) of elements in S we may form a new element $a \star b \in S$. Binary operations are hence like a basic construction rule that enables us to build a new element in the set from any given pair of elements.

However to be useful, such an operation should be relatively easy to work with. Some potential problems are illustrated in the next example:

Example 1.1. *Define* $\star : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *by* $n \star m = 3n + 4m - nm$ *for all* $n, m \in \mathbb{Z}$. *Then one computes that*

$$(2 \star 2) \star 2 = 10 \star 2 = 18$$

and

$$2 \star (2 \star 2) = 2 \star 10 = 26.$$

Thus $(2 \star 2) \star 2 \neq 2 \star (2 \star 2)$. *We hence cannot immediately give meaning to an expression such as* $2 \star 2 \star 2$ *as different interpretations yield different results.*

We see from the last example, that in general when working with a binary product. we cannot uniquely evaluate an expression such as $a \star b \star c$ without being told the order in which the binary (pairwise) multiplications are to be carried out. Of course we could specify this order by inserting brackets but this quickly becomes cumbersome! For example if we were dealing with

a four fold product $a \star b \star c \star d$ there are quite a few ways to do this. For example $(a \star b) \star (c \star d)$ or $a \star ((b \star c) \star d)$ or $a \star (b \star (c \star d))$ among others.

Thus arbitrary binary operations can be hard to work with in algebra. This motivates the following definition:

Definition 1.2. *A semigroup $(S, \star)$ is a set S together with a binary operation $\star : S \times S \to S$ which is* **associative** *i.e.,*

$$(a \star b) \star c = a \star (b \star c)$$

for all $a, b, c \in S$. Thus the expression $a \star b \star c$ is unambiguous in a semigroup.

Even though 3-fold products $a \star b \star c$ are unambiguous in a semigroup $(S, \star)$, it is not apriori clear that higher order products are unambiguous. For example it is not clear that $a \star b \star c \star d$ is well-defined in a semigroup. However it turns out that indeed associativity removes ambiguity in products of any order which is the content of the following proposition, but first a definition:

Definition 1.3. *Given a set S with a binary operation $\star$, a meaningful product for the expression $a_1 \star \cdots \star a_n$ is a bracketing of that expression which exhibits the product as a sequence of binary (pairwise) products. Note since we start with a binary operation, it is only pairwise products that are apriori well-defined.*

Proposition 1.4. *In a semigroup $(S, \star)$, all meaningful products for $a_1 \star \cdots \star a_n$ agree and so the expression $a_1 \star \cdots \star a_n$ is well-defined without the need to insert any bracketing.*

Proof. We proceed by induction on n. For $n = 1, 2$ there is never any ambiguity. The case $n = 3$ follows directly from the definition of associativity. Thus without loss of generality, $n > 3$ and we have shown that any product $a_1 \star \cdots \star a_k$ of $k < n$ elements is unambiguous.

Now consider some meaningful product for $a_1 \star \cdots \star a_n$. Call this meaningful product x. Since x is a sequence of binary products, some pairwise product occurs last and so $x = (a_1 \star \cdots \star a_k) \star (a_{k+1} \star \cdots \star a_n)$ where $k, n-k \geq 1$. Since $k, n-k < n$, the expressions $(a_1 \star \cdots \star a_k)$ and $(a_{k+1} \star \cdots \star a_n)$ are unambiguous by induction. Also by induction, we may express $(a_{k+1} \star \cdots \star a_n)$ as the particular meaningful product $((a_{k+1} \star \cdots \star a_{n-1}) \star a_n)$. Now we compute:

$$\begin{aligned} x &= (a_1 \star \cdots \star a_k) \star ((a_{k+1} \star \cdots \star a_{n-1}) \star a_n) \\ &= ((a_1 \star \cdots \star a_k) \star (a_{k+1} \star \cdots \star a_{n-1})) \star a_n \text{ (Using associativity)} \\ &= (a_1 \star \cdots \star a_{n-1}) \star a_n \text{ (Using the induction hypothesis.)} \end{aligned}$$

Thus all meaningful products x for $a_1 \star \cdots \star a_n$ are equal to the one expression $(a_1 \star \cdots \star a_{n-1}) \star a_n$ and hence are equal. Thus $a_1 \star \cdots \star a_n$ is unambiguous and so by induction, the proposition is proved.

□

From now on, we will be working primarily with associative products and so will consider expressions such as $a_1 \star \cdots \star a_n$ with no further comment. Now even with an associative product, it is important to keep the order of the elements fixed in general, thus $a \star b \neq b \star a$ in general. Some semigroups have the additional property that we may ignore the order of elements in a product and we give this a name next:

Definition 1.5. *A semigroup $(S, \star)$ is commutative (equivalently Abelian) if $a \star b = b \star a$ for all $a, b \in S$.*

Besides associativity, it is often convenient to have an identity element to work with, this motivates the next definition:

Definition 1.6. *A monoid $(M, \star)$ is a semigroup with an identity element e, which satisfies $m \star e = m = e \star m$ for all $m \in M$.*

Let us now consider some examples:

Example 1.7. *The set $\mathbb{Z}$ of integers is a monoid under the usual addition operation $+$. Since $n+m = m+n$, this monoid is commutative. The identity element e is 0. Since $n + m = n + k \implies m = k$ we say that $(\mathbb{Z}, +)$ has the cancellation property, which we define formally later.*

The set of natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$ is a subset of $\mathbb{Z}$ which is a monoid under $+$ in its own right. We say that $(\mathbb{N}, +)$ is a submonoid of $(\mathbb{Z}, +)$. It inherits the commutativity and cancellation properties automatically from $\mathbb{Z}$.

The set $S = \{n \in \mathbb{N} | n \geq 5\}$ is a subsemigroup of $\mathbb{Z}$ but not a submonoid as it does not contain the identity element 0.

On the other hand, the set $T = \{n \in \mathbb{N} | n \leq 5\}$ is not a subsemigroup of $\mathbb{Z}$ as $+$ does not induce a binary operation on T, since for example $3, 4 \in T$ but $3 + 4 \notin T$. We say that T fails to be closed under $+$.

Definition 1.8. *A semigroup $(S, \star)$ has the left cancellation property if $a \star b = a \star c \implies b = c$ for all $a, b, c \in S$. It has the right cancellation property if $b \star a = c \star a \implies b = c$ for all $a, b, c \in S$. (Of course in the Abelian case, both notions coincide).*

Example 1.9 (Monoid of $n \times n$ matrices). *Let $Mat_n(\mathbb{R}) = \{\mathbb{A} | \mathbb{A}$ is a $n \times n$ matrix with real entries$\}$. $Mat_n(\mathbb{R})$ is a monoid under matrix multiplication. This follows as matrix multiplication is associative, i.e,*

$$(\mathbb{AB})\mathbb{C} = \mathbb{A}(\mathbb{BC})$$

and there is an identity element e namely $e = \mathbb{I}$, the identity matrix. Since $\mathbb{AB} \neq \mathbb{BA}$ in general for $n \geq 2$, this monoid is non-Abelian when $n \geq 2$.

If we let $\mathbb{A} = \begin{pmatrix} 5 & 0 \\ 6 & 0 \end{pmatrix}$, $\mathbb{B} = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}$ $\mathbb{C} = \begin{pmatrix} 0 & 0 \\ 1 & 3 \end{pmatrix}$ then an easy computation shows $\mathbb{AC} = \mathbb{BC}$ even though $\mathbb{A} \neq \mathbb{B}$ so $Mat_n(\mathbb{R})$ does not have right cancellation. A similar example shows that it does not have left cancellation either.

Similar comments apply to $Mat_n(\mathbb{C})$ the monoid of $n \times n$ matrices with complex entries.

In a monoid, we may define the concept of inverses:

Definition 1.10. *Let $(M, \star)$ be a monoid with identity element e. Then if $f \star g = e$ we say that g is a right inverse for f or equivalently that f is a left inverse for g. If $f \star g = e = g \star f$ then we call g a two-sided inverse for f. Any element f with a two-sided inverse will be called a unit of M.*

The first part of the following proposition should remind the reader of our discussion of functions in the previous section:

Proposition 1.11. *Let $(M, \star)$ be a monoid. Then*
(a) If g has a two-sided inverse, it is unique. We will thus denote it by g^{-1}.
(b) If g is a unit, so is g^{-1} and $(g^{-1})^{-1} = g$.
(c) If g_1 and g_2 are units, then so is $g_1 \star g_2$ and $(g_1 \star g_2)^{-1} = g_2^{-1} \star g_1^{-1}$.
(d) The identity e is a unit and $e^{-1} = e$.

Proof. **Part (a):** Let h and h' be two two-sided inverses for g, then by associativity we have:

$$h = h \star e = h \star (g \star h') = (h \star g) \star h' = e \star h' = h'$$

and so $h = h'$. Thus the two-sided inverse for g is unique when it exists and we will call it g^{-1}.
part (b): The identity $g \star g^{-1} = e = g^{-1} \star g$ exhibits g as a two-sided inverse for g^{-1} from which (b) follows.
part (c): We compute

$$(g_1 \star g_2) \star (g_2^{-1} \star g_1^{-1}) = g_1 \star e \star g_1^{-1} = g_1 \star g_1^{-1} = e$$

and similarly $(g_2^{-1} \star g_1^{-1}) \star (g_1 \star g_2) = e$. Thus $g_2^{-1} \star g_1^{-1}$ is a two-sided inverse for $g_1 \star g_2$ and hence is $(g_1 \star g_2)^{-1}$.
part (d): Follows from $e \star e = e$. □

The next example shows the preponderence of nonunits which behave badly in general monoids:

Example 1.12 (Monoid of Functions). *Fix a set S and define $M(S) = \{f : S \to S\}$ to be the monoid of all functions with domain and codomain equal to S. This is a monoid under the composition of functions (which we have seen is associative) and with identity $e = 1_S$, the identity function for S.*

We have seen that if $f \in M(S)$ is not injective it has no left inverse and if it is not surjective it has no right inverse. As an exercise in Homework 1 will show, there can also be examples of f with infinitely many distinct left inverses and no right inverse or vice versa.

It is also simple to check that in general $M(S)$ is non-Abelian if $|S| \geq 3$ and fails to have cancellation if $|S| \geq 2$.

The final example will have applications later in the course:

Example 1.13 (Free monoids). *Let A be a set, usually called an alphabet. Then the free monoid on A, denoted $W(A)$ is the set of all finite words on this alphabet, i.e., strings of the form $a_1 a_2 \ldots a_n$ for an integer $n \geq 1$. We also include an "empty word" denoted $\hat{e}$. The monoid operation $\star$ is that of concatenation of words. This operation has identity element $\hat{e}$.*

For example if $A = \{a, b, c, \ldots, z\}$ is the standard roman alphabet then if we take $x_1 = abra, x_2 = cadabra \in W(A)$, we compute $x_1 \star x_2 = abracadabra$.

For another example if $A = \{0, 1\}$ then $W(A)$ is the set of all binary strings of finite length. If $x_1 = 011001$ and $x_2 = 11001$ then $x_1 \star x_2 = 01100111001$ while $x_2 \star x_1 = 11001011001$. Thus $W(A)$ is non-Abelian in general.

The monoid $W(A)$ is crucial in the abstract study of languages and grammars carried out for example in areas of computer science. For example, the abstract definition of a language L over an alphabet A is as a subset of $W(A)$. (See for example Rosen's "Discrete Mathematics and its Applications")

2 Groups

We have seen in the previous section, that working with monoids can be complicated by the fact that cancellation does not hold in general. Furthermore, elements might not have an inverse, and even in the case that they have a one-sided inverse, it may not be unique. This motivates the definition of one of the fundamental algebraic objects whose study will occupy us for awhile:

Definition 2.1. *A group G is a monoid $(M, \star)$ such that every element g has a two-sided inverse. Since we have seen that such a two-sided inverse will be unique, we will commonly denote it by g^{-1}.*

It is obvious from the definition, that the problem of inverses is solved in a group. The next proposition shows that all groups also have the cancellation property. From now on, we will omit explicit mention of the binary operation in a group G if it is understood and will write $g_1 g_2$ for $g_1 \star g_2$.

Proposition 2.2 (Cancellation holds in groups). *Let G be a group then G has both the left and right cancellation properties.*

Proof. Suppose $a, b, c \in G$ such that $ab = ac$. Since a^{-1} exists in G we may multiply both sides of the equation by it on the left. Thus we find $a^{-1}ab = a^{-1}ac$ which gives $b = c$. Thus G has the left cancellation property. The right cancellation property is proved similarly. □

We now proceed to give some examples:

Example 2.3. *The set of integers $\mathbb{Z}$ is an Abelian group under addition. The inverse of n is denoted $-n$. In the future we will often use $+$ to denote the group operation in an Abelian group and will also usally refer to the inverse of g as $-g$ rather than g^{-1} in this case.*

One important source of examples is the following proposition:

Proposition 2.4 (Group of Units). *Given a monoid $(M, \star)$, the set of units of M, denoted $U(M)$, forms a group under $\star$.*

Proof. This follows from Proposition 1.11. □

Example 2.5 (General Linear Groups). *In the monoid $Mat_n(\mathbb{R})$, the group of units is called the real general linear group. It is denoted by $GL_n(\mathbb{R})$ and so $GL_n(\mathbb{R}) = \{\mathbb{A} | \mathbb{A}$ a $n \times n$ matrix such that $\mathbb{A}^{-1}$ exists $\}$.*
Equivalently $GL_n(\mathbb{R}) = \{\mathbb{A} | \mathbb{A}$ a $n \times n$ matrix such that $det(\mathbb{A}) \neq 0\}$. Here "det" is the determinant function.

It is easy to check that $GL_n(\mathbb{R})$ is non-Abelian when $n \geq 2$.

Similar comments hold for the complex general linear group $GL_n(\mathbb{C})$.

Example 2.6 (Permutation Groups). *Let S be a set and let $M(S)$ be the monoid of functions with domain and codomain equal to S under composition of functions. The units of $M(S)$ are exactly the bijections $f : S \to S$. This group of units is called the permutation group of S (equivalently the symmetric group of S), and is denoted $\Sigma(S)$.*

Thus $\Sigma(S) = \{f : S \to S | f$ is a bijection $\}$.

2.1 Symmetric group on n letters

A very important example of a group G that we will consistently use to illustrate many concepts is a special case of Example 2.6.

If $S = \{1, 2, \ldots, n\}$ is a finite set of size n, then we will denote $\Sigma(S)$ by Σ_n. Σ_n is frequently called the symmetric group on n letters.

We need some notation to work with elements σ of Σ_n.

The simplest notation is array notation which lays out the permutation σ as an array with two rows, the top row being the domain, and the bottom the corresponding images under σ in the codomain.

For example in Σ_6, the array $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$ describes the permutation $\sigma : 1 \to 3, 2 \to 6, 3 \to 4, 4 \to 1, 5 \to 5, 6 \to 2$.

This notation though can be cumbersome to work with so usually one works with cycle notation which we describe next.

Let us illustrate the basic concept with the example σ above. If we compute the orbit of 1, i.e. what happens as we compute $1, \sigma(1), \sigma(\sigma(1)), \ldots$ we find that we get the following "cycle": $1 \to 3 \to 4 \to 1$. We would have basically got the same cycle if we computed the orbit of 3 or 4 instead. On the other hand when we compute the orbit of 2 or 6 we get the cycle $2 \to 6 \to 2$ which is disjoint from the original one.

Thus we may adopt a cycle notation for σ which exhibits the cycles of σ. In this case we write $\sigma = (1,3,4)(2,6)(5)$. When there is no confusion, we will drop cycles of length one and so we write $\sigma = (1,3,4)(2,6)$. Notice given the cycle notation for σ, one can recover the array notation and so no information is lost.

Of course since $(1,3,4), (3,4,1)$ and $(4,1,3)$ all describe the same cycle we may use any of these interchangably. However the cycle $(1,3,4)$ is **different** from the cycle $(1,4,3)$ as in the latter 1 is sent to 4 not 3, thus the reader should be careful. There is also no importance to the order of the cycles themselves in this notation (we will come back to this point later). Thus we can equally well write $\sigma = (6,2)(3,4,1)$ for the permutation σ above.

Now we explain why this works generally. Let $\sigma \in \Sigma_n$ be some general permutation. Let us look at the orbit of some number j: $j, \sigma(j), \sigma(\sigma(j)), \ldots$. Since we are working with a finite set of numbers $\{1, \ldots, n\}$, we conclude there is a first (smallest) integer $k \geq 1$ so that $\sigma^k(j) = \sigma^s(j)$ for some $0 \leq s < k$. Now $s \geq 1$ is impossible as $\sigma(\sigma^{s-1}(j)) = \sigma^s(j) = \sigma(\sigma^{k-1}(j))$ and only one input can be sent to the output $\sigma^s(j)$ as σ is injective. Thus we see that $\sigma^k(j) = j$ and so the orbit of j forms a cycle. It is easy to see that if we look at the orbit of a number not on this cycle, that it again forms another cycle which has to be disjoint from this first one, again by injectivity of σ.

Thus the orbits of $\sigma \in \Sigma_n$ again break up into disjoint cycles and we may hence use cycle notation to describe σ as in our first example.

As practice in using this notation, let us show that Σ_3 is non-Abelian.

Let $a = (1,2)$ and $b = (2,3)$ in Σ_3. Let us compute $a \star b$ in cycle notation. Now $a \star b$ is composition so we apply b first and then a. b takes $1 \to 1$ and then a takes $1 \to 2$ so $a \star b$ does $1 \to 2$. Similarly one computes $a \star b : 2 \to 3, 3 \to 1$. Thus $(1,2) \star (2,3) = (1,2,3)$. On the other hand one computes that $(2,3) \star (1,2) = (1,3,2)$. Thus since the cycles $(1,2,3)$ and $(1,3,2)$ are different, we see that Σ_3 is non-Abelian. A simple count shows that $|\Sigma_n| = n!$ (we will provide a more conceptual proof later). Thus $|\Sigma_3| = 3! = 6$. The reader may check that the following is an explicit complete listing of all permutations on 3 letters using the cycle notation we have developed:

$$\Sigma_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}.$$