## 7.3 Cycles

**Definition 7.3.1** *If $\rho$ is a permutation on $A$ then $\rho$* ***fixes*** *$a \in A$ if $\rho(a) = a$ and $\rho$* ***moves*** *$a$ if $\rho(a) \neq a$.*

**Definition 7.3.2** *Let $a_1, a_2, ..., a_r$ be distinct elements in $A$. If $\rho$ is a permutation that fixes all the other elements of $A$ and if*

$$\rho(a_1) = a_2, \rho(a_2) = a_3, \rho(a_3) = a_4, \ldots, \rho(a_{r-1}) = a_r, \rho(a_r) = a_1,$$

*i.e.*

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \ldots \mapsto a_r \mapsto a_1,$$

*then $\rho$ is called a* ***cycle*** *of* ***length*** *$r$, sometimes called an* **r**-***cycle***. *A 2-cycle is called a* ***transposition***.

*The $r$-cycle above will be denoted by*

$$(a_1, a_2, a_3, ..., a_r).$$

**Note** that any $a_i$ can be taken as the "starting point", so

$$(a_1, a_2, a_3, ...., a_r) = (a_2, a_3, ...., a_r, a_1) = .... = (a_r, a_1, ...., a_{r-2}, a_{r-1}).$$

We can take $r = 1$ in the definition to get a 1-cycle, $(a_1)$. But such a cycle fixes all elements of $A$ and is thus the identity. Hence all 1-cycles equal the identity, i.e. $(a) = 1_A$ for all $a \in A$.

**Example 7.3.3** *(i) Two permutations seen before were cycles. Namely, $\rho, \pi \in S_5$,*

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} = (1, 4, 3),$$

*and*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1, 2, 3, 4, 5).$$

*(ii) In $S_3$ all permutations happen to be cycles, namely*

$$1_3, (2, 3), (1, 2), (1, 3), (1, 3, 2) \text{ and } (1, 2, 3).$$

The inverse of a cycle is obtained simply by writing it in reverse order. So in $S_5$,

$$\rho^{-1} = (1,4,3)^{-1} = (3,4,1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix},$$

as seen before. And we can compose cycles written in this notation, remembering to read *from the right*. So, in $S_5$,

$$\rho \circ \pi = (1,4,3) \circ (1,2,3,4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 1 \end{pmatrix},$$

as seen before. Again, we did this by noting that $\pi$ moved 1 to 2 which $\rho$ then fixed. Next $\pi$ moved 2 to 3 which $\rho$ moved onto 1. Continue.

**Example 7.3.4** *In $S_3$ we can represent all possible products in a table*

| $\circ$ | $1_3$ | $(2,3)$ | $(1,2)$ | $(1,3)$ | $(1,3,2)$ | $(1,2,3)$ |
|---|---|---|---|---|---|---|
| $1_3$ | $1_3$ | $(2,3)$ | $(1,2)$ | $(1,3)$ | $(1,3,2)$ | $(1,2,3)$ |
| $(2,3)$ | $(2,3)$ | $1_3$ | $(1,3,2)$ | $(1,2,3)$ | $(1,2)$ | $(1,3)$ |
| $(1,2)$ | $(1,2)$ | $(1,2,3)$ | $1_3$ | $(1,3,2)$ | $(1,3)$ | $(2,3)$ |
| $(1,3)$ | $(1,3)$ | $(1,3,2)$ | $(1,2,3)$ | $1_3$ | $(2,3)$ | $(1,2)$ |
| $(1,3,2)$ | $(1,3,2)$ | $(1,3)$ | $(2,3)$ | $(1,2)$ | $(1,2,3)$ | $1_3$ |
| $(1,2,3)$ | $(1,2,3)$ | $(1,2)$ | $(1,3)$ | $(2,3)$ | $1_3$ | $(1,3,2)$ |

**Note** that because composition of functions is not commutative this table is not symmetric about the leading diagonal (which makes it different to earlier tables we have seen for $(\mathbb{Z}_m, +)$, $(\mathbb{Z}_m, \times)$ and $(\mathbb{Z}_m^*, \times)$).

## 7.4 Factoring permutations

**Question** If we can compose permutations can we factor them?

**Problem with this Question**. In the last section we factored integers into prime numbers. What is the equivalent of prime numbers for permutations?

**Algorithm** for factorization is best illustrated by an example.

**Example 7.4.1** *In $S_6$ factor*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

**Solution**

1. Take the smallest 'unused' element in $\{1, 2, 3, 4, 5, 6\}$, namely 1. See what $\pi$ does to 1 on repeated applications. It sends 1 to 5. Then $\pi$ sends 5 to 4. Next $\pi$ sends 4 back to 1. Thus we have a cycle $(1, 5, 4)$.

2. Next look at the smallest 'unused' element, i.e not in the cycles already found. In this case it is 2. Then we what happens to 2 under repeated applications of $\pi$, i.e. $2 \longmapsto 6 \longmapsto 2$ and so we get another cycle $(2, 6)$.

3. Repeat by taking the smallest element *not* in these two cycles. We have only one such element 5, and we see this is fixed by $\pi$, and so we get a 1-cycle $(5)$, which we know is the identity. When there is at least one non-identity cycle we can omit the identity $(5)$.

4. When all elements are 'used', i.e. in some cycle, finish.

Hence

$$\pi = (1, 5, 4) \circ (2, 6) \circ (5) = (1, 5, 4) \circ (2, 6) \,.$$

■

So in this way a permutation is factored into cycles, and thus cycles can be considered the equivalent of prime numbers.

**It can be proved** that each new cycle contains no elements in any earlier cycle. We can rewrite this statement using:

**Definition 7.4.2** *Two permutations $\rho$ and $\pi$ of a set $A$ are* ***disjoint*** *if*

*i) every element moved by $\rho$ is fixed by $\pi$ and*

*ii) every element moved by $\pi$ is fixed by $\rho$.*

**Example 7.4.3** *In $S_5$ the cycles $(1, 5, 4)$ and $(2, 6)$ are disjoint. The cycles $(1, 4, 3)$ and $(1, 2, 3, 4, 5)$ are not disjoint.*

The continued application of the factorization method above leads to

**Theorem 7.4.4** *A permutation on a finite set $A$ is a product (composition) of disjoint cycles.*

**Proof** not given, but see Appendix.

You should ask some questions about this algorithm. For example, what happens if we start with a different number, say 2 in place of 1 in the above example? We would get $\pi = (2, 6) \circ (1, 5, 4)$. But we know that composition of permutations is **not** commutative in general so can we have

$$(2, 6) \circ (1, 5, 4) = \pi = (1, 5, 4) \circ (2, 6)?$$

Yes!

**Theorem 7.4.5** *Disjoint permutations on a set commute.*

**Proof** not given in course . ■

Finally it can be shown that the factorization found by this method is unique.

> **Aside** Though the proof is not given here (see the appendix) the idea is similar to the one used to prove that the factorization of integers into primes. Use **strong** induction on the *number of elements moved by the permutation* $\pi$. Write the permutation in two ways as disjoint compositions
>
> $$\pi = \sigma_1 \circ \sigma_2 \circ \sigma_3 \circ ... \circ \sigma_s = \rho_1 \circ \rho_2 \circ \rho_3 \circ ... \circ \rho_t.$$
>
> Look at an element $a$ moved by $\pi$. This must be moved by *exactly* one $\sigma_i$ and $\rho_j$ from each side. Relabel so these are $\sigma_1$ and $\rho_1$. It can be shown that two *cycles* arising from $\pi$ which move the same point must be identical, i.e. $\sigma_1 = \rho_1 = \tau$ say. So we have
>
> $$\tau \circ \sigma_2 \circ \sigma_3 \circ ... \circ \sigma_s = \tau \circ \rho_2 \circ \rho_3 \circ ... \circ \rho_t.$$
>
> Apply $\tau^{-1}$ to both sides to get
>
> $$\sigma_2 \circ \sigma_3 \circ ... \circ \sigma_s = \rho_2 \circ \rho_3 \circ ... \circ \rho_t.$$
>
> The permutation represented here moves fewer elements than did $\pi$ (it no longer moves the elements moved by $\tau$.) So we can now use induction to say that these two decompositions are identical, i.e. $s = t$ and the $\sigma_i$, $2 \le i \le s$ are the same as $\rho_j, 2 \le j \le t = s$ in some order.

Combining all the above results gives

**Theorem 7.4.6** *A permutation on a finite set A can be expressed as a product of disjoint cycles* ***uniquely*** *apart from the order of the cycles.*

**Proof** Not given.

## 7.5 Orders of permutations

**Definition 7.5.1**

- *The **positive powers** $\rho^n$ of a permutation are defined inductively by setting $\rho^1 = \rho$ and $\rho^{k+1} = \rho \circ \rho^k$ for all $k \in \mathbb{N}$.*
- *The **negative powers** of a permutation are defined by $\rho^{-n} = (\rho^{-1})^n$ for all $n \in \mathbb{N}$, i.e. taking positive powers (just defined) of the inverse of $\rho$.*
- *Finally, we set $\rho^0 = 1_A$.*

It can be shown by induction that powers satisfy the expected properties of exponents, namely that

$$\rho^{m+n} = \rho^m \circ \rho^n \tag{1}$$

for all $m, n \in \mathbb{Z}$.

The method described above of factorizing a permutation started by taking an element of $A$, repeatedly applying $\rho$ *until you returned to $a$ when you then have a cycle.* This italicized sentence is an assumption, we have to show that repeatedly applying $\rho$ to $a$ does, in fact, gets us back to $a$.

**Lemma 7.5.2** *Let $\rho$ be a permutation on a non-empty finite set. There exists $m \geq 1$ for which $\rho^m = 1_A$.*

**Proof** Consider the set $\{\rho^j : j \geq 0\}$ which is a subset of **all** permutations on $A$. Yet the set of all permutations on $A$ is finite, (if $|A| = n$ then the number of all permutations is $n!$). Thus $\{\rho^j : j \geq 0\}$ is a finite set. Therefore we must have repetition, i.e. $\exists \ell > k \geq 0$ for which $\rho^\ell = \rho^k$. Applying $\rho^{-k}$ to both sides gives

$$\begin{aligned}
\rho^{\ell-k} &= \rho^\ell \circ \rho^{-k} \quad \text{by (1)} \\
&= \rho^k \circ \rho^{-k} \quad \text{since } \rho^\ell = \rho^k \\
&= \rho^{k-k} \quad \text{again by (1)} \\
&= \rho^0 = 1_A \quad \text{by definition.}
\end{aligned}$$

Thus we have found an $m = \ell - k \geq 1$ for which $\rho^m = 1_A$. ■

Hence given a permutation on a finite set $A$ along with $a \in A$ then $\rho^m(a) = a$, so repeated application of $\rho$ on $a$ leads back to $a$ thus giving a cycle. This is as required for our method of factorization.

**Example 7.5.3** *Let* $A = \{1, 2, 3, 4, 5, 6\}$ *and*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

*It is easy to check that* $\pi^6 = 1_A$.

**Be careful**, for a given $a \in A$ we may return to $a$ on repeated application of $\rho$ with a power smaller than the $m$ found above. For example, for $\pi$ above we have $\pi^6 = 1_A$ so, choosing $4 \in A$ this means $\pi^6(4) = 1_A(4) = 4$. But if we apply $\pi$ to 4 only three times we get

$$4 \to 1 \to 5 \to 4.$$

So $\pi^3(4) = 4$.

**Definition 7.5.4** *The* ***order*** *or* ***period*** *of a permutation* $\rho$ *of a finite set is the* ***least*** *positive integer* $d$ *such that* $\rho^d = 1_A$.

The order *exists* because we saw earlier that there exists $m \geq 1$ for which $\rho^m = 1_A$. The order of $\rho$ and the $m$ found earlier are related in

**Theorem 7.5.5** *If the order of* $\rho$ *is* $d$ *then* $\rho^m = 1_A$ *if, and only if,* $d|m$.

**Proof** ($\Rightarrow$) Assume $\rho^m = 1_A$. By the division Algorithm write $m = qd + r$ for some integers $q$ and $0 \leq r \leq d - 1$. Then

$$1_A = \rho^m = \rho^{qd+r} = \left(\rho^d\right)^q \rho^r = (1_A)^q \rho^r = \rho^r.$$

But $d$ is the *least* positive integer for which $\rho^d = 1_A$ and thus $r = 0$. That is, $m = qd$ and so $d|m$.

($\Leftarrow$) Assume $d|m$. So $m = dq$ for some $q \in \mathbb{Z}$. But then

$$\rho^m = \left(\rho^d\right)^q = (1_A)^q = 1_A.$$

$\blacksquare$

**Example 7.5.6** *In* $S_4$ *find the orders of*

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \textit{and} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

**Solution**

$$\pi_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1_4,$$

and so the order of $\pi_1$ is 2. But for $\pi_2$

$$\begin{aligned} \pi_2^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \\ \pi_2^3 &= \pi_2 \circ \pi_2^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1_4, \end{aligned}$$

and so the order is 3. ■

But what about finding the order of something a little larger? In $S_7$ consider

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 6 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Then

$$\pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 5 & 7 & 3 & 1 & 2 \end{pmatrix}, \pi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 4 & 6 & 3 & 7 \end{pmatrix}, \dots$$

How long do we have to go on for? What if we had a permutation from $S_{100}$?

Suppose that

$$\pi = \pi_1 \circ \pi_2 \circ .... \circ \pi_m$$

is a decomposition into a product of **disjoint** permutations. Consider the $k$-th power

$$\pi^k = (\pi_1 \circ \pi_2 \circ .... \circ \pi_m)^k .$$

Since the permutations on the right hand side are disjoint the compositions commute, so they can be moved around to give

$$\pi^k = \pi_1^k \circ \pi_2^k \circ .... \circ \pi_m^k.$$

Assume now that $\pi^k = 1_A$, so $\pi^k$ moves **no** elements. Because the permutations are disjoint each of $\pi_1^k$, $\pi_2^k$, ...., $\pi_m^k$ move different elements and so $\pi^k$ moves no elements if, and only if, each of $\pi_1^k$, $\pi_2^k$, ...., $\pi_m^k$ moves no elements, i.e. $\pi_i^k = 1_A$ for all $1 \le i \le m$. Let $d_i$ be the order of $\pi_i$ for each $1 \le i \le m$, then by the Theorem above $\pi_i^k = 1_A$ for all $1 \le i \le m$ iff $d_i | k$ for all $1 \le i \le m$. Finally, in searching for the order of $\pi$ we want the *least* $k$ divisible by all the $d_i$. This leads to

**Definition 7.5.7** *The **lowest common multiple** of integers $m_1, m_2, ..., m_t$, denoted by* $\mathrm{lcm}\,(m_1, m_2, ..., m_t)$ *is the positive integer $f$ that satisfies*

*1)* $m_1|f, m_2|f, ..., m_t|f$,

*2) if* $m_1|k$, $m_2|k$, ..., $m_t|k$ *then* $f|k$.

*In words, (1) says that $f$ is **a** common multiple of the integers, while (2) says that it is the **least** of all possible positive common multiples.*

Compare the definition to that of gcd.

Thus we see that the following result is not unreasonable.

**Theorem 7.5.8** *Suppose that*

$$\pi = \pi_1 \circ \pi_2 \circ .... \circ \pi_m$$

*is a decomposition into a product of disjoint permutations, then the order of $\pi$ is the least common multiple of the orders of the permutations $\pi_1, \pi_2, ...., \pi_m$.*

**Proof** not given but see the appendix.

**Note** In practice, given a permutation $\pi$ we decompose it into a product of disjoint *cycles.*

**Question** For what permutations is it easy to calculate the order?
**Answer** Cycles.

**Theorem 7.5.9** *The order of a cycle is equal to its length.*

**Proof** Not given, but see the appendix.

**Corollary 7.5.10** *Suppose that*

$$\pi = \sigma_1 \circ \sigma_2 \circ .... \circ \sigma_m$$

*is a decomposition into a product of disjoint cycles, then the order of $\pi$ is the least common multiple of the lengths of the cycles $\sigma_1, \sigma_2, ...., \sigma_m$.*

**Example 7.5.11** *In $S_{12}$ consider*

$$\begin{aligned} \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 3 & 5 & 10 & 2 & 1 & 4 & 9 & 7 & 8 & 12 & 11 \end{pmatrix} \\ &= (4, 10, 8, 9, 7) \circ (2, 3, 5) \circ (1, 6) \circ (11, 12)\,. \end{aligned}$$

*The order equals* $\mathrm{lcm}\,(5, 3, 2, 2) = 30$.

**Example 7.5.12** *What is the largest order of all permutations in $S_{12}$?*

**Solution** Need to find positive integers $a, b, c, ...$ that sum to 12 but for which $\mathrm{lcm}\,(a, b, c, ..)$ is as large as possible. Just search to find $12 = 3 + 4 + 5$, when $\mathrm{lcm}\,(3, 4, 5) = 60$. So, for example

$$\begin{aligned}(1,2,3) \quad &\circ \quad (4,5,6,7) \circ (8,9,10,11,12) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 9 & 10 & 11 & 12 & 8 \end{pmatrix}\end{aligned}$$

has order 60. ■

**Example 7.5.13** $S_8$. *What is the order of*

$$(1,2,4,6,8) \circ (2,3,6) \circ (6,7)?$$

**Solution** CAREFUL, the cycles are not disjoint! We have to write this as a product of disjoint cycles. In fact it equals

$$(1,2,3,8) \circ (4,6,7),$$

now a composition of disjoint cycles. The order is $\mathrm{lcm}\,(4, 3) = 12$. ■

# 8 Groups

## 8.1 Binary Operations

**Question**, why, earlier in the course did we call $(S_n, \circ)$, the set of permutations on $n$ elements under composition, the *Symmetric Group on n elements*?

**Definition 8.1.1** *A **binary operation** on a set $S$ is a function from the ordered pairs of $S \times S$ to $S$. We will denote it in general as $*$, so for each $(a, b) \in S$ the function sends $(a, b) \to a * b$, a value in $S$. Thus*

$$\forall a, b \in S, a * b \in S.$$

*If $C \subseteq S$ we say that $C$ **is closed under** $*$ iff*

$$\forall a, b \in C, a * b \in C.$$

**Example 8.1.2** *$\mathbb{Z}_{20}$ is closed under $\times_{20}$. But $\{[4]_{20}, [8]_{20}, [12]_{20}, [16]_{20}\} \subseteq \mathbb{Z}_{20}$ is also closed, we can draw up a table*

| $\times$ | $[4]_{20}$ | $[8]_{20}$ | $[12]_{20}$ | $[16]_{20}$ |
|---|---|---|---|---|
| $[4]_{20}$ | $[16]_{20}$ | $[12]_{20}$ | $[8]_{20}$ | $[4]_{20}$ |
| $[8]_{20}$ | $[12]_{20}$ | $[4]_{20}$ | $[16]_{20}$ | $[8]_{20}$ |
| $[12]_{20}$ | $[8]_{20}$ | $[16]_{20}$ | $[4]_{20}$ | $[12]_{20}$ |
| $[16]_{20}$ | $[4]_{20}$ | $[8]_{20}$ | $[12]_{20}$ | $[16]_{20}$ |

**Example 8.1.3** *1.*

2. *The set of all permutations on a set of $n$ elements is closed under composition $\circ$.*

3. *For each $m \geq 1$ the set $\mathbb{Z}_m$ (of congruence classes mod $m$) is closed under multiplication modulo $m$.*

4. *For each $m \geq 1$ the set $\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$ (of invertible congruence classes mod $m$) is closed under multiplication modulo $m$.*

**Example 8.1.4** *(**Only given if time**) Earlier we introduced bijections*

$$\rho_a : \mathbb{Z}_m^* \to \mathbb{Z}_m^*, \rho_a([r]_m) = [ar]_m,$$

*for each $[a]_m \in \mathbb{Z}_m^*$. In the particular case of $m = 8$ we found four permuta-*

*tion, written in cycle form as*

$$\rho_1 = 1_{\mathbb{Z}_8^*},\ \rho_3 = (1,3) \circ (5,7)\,,\ \rho_5 = (1,5) \circ (3,7)\ \text{ and } \rho_7 = (1,7) \circ (3,5)\,.$$

*These are just four of the 24 possible permutations on the four elements* $\{1,3,5,7\}$. *Yet*

$$\begin{aligned}\rho_b \circ \rho_a ([r]_8) &= \rho_b (\rho_a ([r]_8)) = \rho_b ([ar]_8) \\ &= [b\,(ar)]_8 = [(ba)\,r]_8 \\ &= \rho_{ba} ([r]_8)\,.\end{aligned}$$

*Hence* $\rho_b \circ \rho_a = \rho_{ba}$. *Thus* $\{\rho_1, \rho_2, \rho_3, \rho_4\}$ *is a closed set of permutations in which case we can draw up their multiplication table*:

| $\circ$ | $\rho_1$ | $\rho_3$ | $\rho_5$ | $\rho_7$ |
|---|---|---|---|---|
| $\rho_1$ | $\rho_1$ | $\rho_3$ | $\rho_5$ | $\rho_7$ |
| $\rho_3$ | $\rho_3$ | $\rho_1$ | $\rho_7$ | $\rho_5$ |
| $\rho_5$ | $\rho_5$ | $\rho_7$ | $\rho_1$ | $\rho_3$ |
| $\rho_7$ | $\rho_7$ | $\rho_5$ | $\rho_3$ | $\rho_1$ |

A binary operation might satisfy certain properties that we have seen before (PJE p.18 for real numbers and p.71 for sets).

**Definition 8.1.5** *(i) A binary operation is* ***commutative*** *if,*

$$\forall a, b \in S, a * b = b * a,$$

*(ii) A binary operation is* ***associative*** *if,*

$$\forall a, b, c \in S, (a * b) * c = a * (b * c)\,.$$

**Definition 8.1.6** *Given a set $S$ and binary operation $*$ on $S$ we say that $e \in S$ is an* ***identity*** *if, for all $a \in S$,*

$$e * a = a \quad \text{and} \quad a * e = a.$$

We have to check both $e * a$ and $a * e$ since we are not assuming that $*$ is commutative.

**Example 8.1.7** $\{[4]_{20}\,, [8]_{20}\,, [12]_{20}\,, [16]_{20}\,, \times\}$. *Looking back at the table above we see that the identity is* $[16]_{20}$.

This last example is important, it shows that we get identities different to 1 and 0!

**Note** the use of the word "an" in the definition. But

**Lemma 8.1.8** *Suppose that* $*$ *is a binary operation on a set* $S$ *and that* $(S, *)$ *has an identity. The identity is unique.*

**Proof** Suppose that $e$ and $f$ are two identities on $S$. Then

$$\begin{aligned} e &= e * f \text{ since } f \text{ is an identity (used here on the right),} \\ &= f \text{ since } e \text{ is an identity (used here on the left).} \end{aligned}$$

■

So we can now talk about "the" identity.

If, in the multiplication table for $(S, *)$, we can find an element whose row (**and** whose column) is identical to the heading row (respectively heading column), then we have found the identity.

**Definition 8.1.9** *Let* $S$ *be a set with a binary operation* $*$ *and an identity element* $e \in S$. *We say that an element* $a \in S$ *is* ***invertible*** *if there exists* $b \in S$ *such that*

$$a * b = e \text{ and } b * a = e.$$

*We say that* $b$ *is the* ***inverse*** *of* $a$, *and normally write* $b$ *as* $a^{-1}$.

**Example 8.1.10** *In* $(\mathbb{Z}_6, \times)$ *the element* $[2]_6$ *has no inverse.*

**Solution If** $[2]_6$ had an inverse, i.e. $[b]_6$ then

$$[2]_6 \, [b]_6 = [1]_6 \, .$$

Multiply both sides by $[3]_6$ to get

$$[6]_6 \, [b]_6 = [3]_6 \, , \quad \text{i.e.} \quad [0]_6 = [3]_6 \, ,$$

since $[6]_6 = [0]_6$, a contradiction. ■

The problem here is that $6 = 2 \times 3$ is composite. We have got round this in two ways in this course. First we can look at $(\mathbb{Z}_p, \times)$ with $p$ prime, when every non-zero element has an inverse. The second way it to look at $(\mathbb{Z}_m^*, \times)$ where we have simply thrown away all the elements that don't have an inverse!

If, for an $i \in S$ we can look in its row in the multiplication table and find the identity in column $j$, say, **and** find in row $j$ the identity in column $i$ then $i$ and $j$ are inverse to each other. If we can do this for every $i \in S$ then every element will have an inverse.

**Example 8.1.11** $\{[4]_{20}, [8]_{20}, [12]_{20}, [16]_{20}, \times\}$

| $\times$ | $[4]_{20}$ | $[8]_{20}$ | $[12]_{20}$ | $[16]_{20}$ |
|---|---|---|---|---|
| $[4]_{20}$ | $[16]_{20}$ | $[12]_{20}$ | $[8]_{20}$ | $[4]_{20}$ |
| $[8]_{20}$ | $[12]_{20}$ | $[4]_{20}$ | $[16]_{20}$ | $[8]_{20}$ |
| $[12]_{20}$ | $[8]_{20}$ | $[16]_{20}$ | $[4]_{20}$ | $[12]_{20}$ |
| $[16]_{20}$ | $[4]_{20}$ | $[8]_{20}$ | $[12]_{20}$ | $[16]_{20}$ |

Since the identity is $[16]_{20}$ we note

$$\begin{aligned} [4]_{20} \times [4]_{20} &= [16]_{20} \quad \text{so } [4]_{20}^{-1} = [4]_{20}, \\ [8]_{20} \times [12]_{20} &= [16]_{20} \quad \text{so } [8]_{20}^{-1} = [12]_{20}, \\ [12]_{20} \times [8]_{20} &= [16]_{20} \quad \text{so } [12]_{20}^{-1} = [8]_{20}. \end{aligned}$$

(The inverse of the identity is always itself!)

**Lemma 8.1.12** *Assume that the binary operation $*$ on $S$ is associative. Assume that $(S, *)$ has an identity $e$ and $a \in S$ has an inverse. Then the inverse is unique.*

**Proof** If an element $a$ has two inverses, $b, c \in S$ say, then

$$\begin{aligned} a * b &= e \quad \text{and} \quad b * a = e \\ a * c &= e \quad \text{and} \quad c * a = e. \end{aligned}$$

From these we keep $b * a = e$ and $a * c = e$. These pieces of information are combined in the following way,

$$\begin{aligned} b &= b * e = b * (a * c) \quad \text{since } c \text{ is an inverse of } a, \\ &= (b * a) * c \quad \text{by associativity}, \\ &= e * c \quad \text{since } b \text{ is an inverse of } a, \\ &= c. \end{aligned}$$

Thus $b = c$ and the inverse is unique. ■

So we can now talk about "the" inverse of an (invertible) element.

## 8.2 Groups

**Definition 8.2.1** *Given a set $G$ and binary operation $*$ we say that $(G, *)$ is a **group** if, and only if,*

G1 *$G$ is closed under $*$,*

G2 *$*$ is associative on $G$,*

G3 *$(G, *)$ has an identity element, i.e.*

$$\exists e \in G : \forall a \in G, e * a = a * e = a,$$

G4 *every element of $(G, *)$ has an inverse, i.e.*

$$\forall a \in G, \exists a' \in G : a * a' = a' * a = e.$$

*We say that $(G, *)$ is a **commutative** or **abelian** group (after Niels Abel) if, and only if, it is a group and $*$ is commutative.*

**Recall** that in the course we showed that $\mathbb{Z}_n^*$ is closed under multiplication. This was done by taking $[a]_n, [b]_n \in \mathbb{Z}_n^*$ and showing that

$$([a]_n [b]_n)^{-1} = [b]_n^{-1} [a]_n^{-1}. \tag{2}$$

What is important here is *not* the value of the inverse but that the product $[a]_n [b]_n$ *has* an inverse. For this implies $[a]_n [b]_n \in \mathbb{Z}_n^*$ as required for closure.

But it can be shown that (2) holds in *any* group.

**Proposition 8.2.2** *Assume that $(G, *)$ is a group. If $x, y \in G$ then*

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Notice how the order has changed.

**Proof** First note that $(x * y)^{-1}$ is, by definition, an inverse of $x * y$.

Next note that

$$\begin{aligned}
(x * y) * \left(y^{-1} * x^{-1}\right) &= \left((x * y) * y^{-1}\right) * x^{-1} \\
&\qquad \text{using } * \text{ is associative} \\
&= \left(x * \left(y * y^{-1}\right)\right) * x^{-1} \\
&\qquad \text{again using } * \text{ is associative} \\
&= (x * e) * x^{-1} \\
&= x * x^{-1} \\
&= e.
\end{aligned}$$

So $(x * y) * (y^{-1} * x^{-1}) = e$. It is similarly shown that $(y^{-1} * x^{-1}) * (x * y) = e$. Together these mean that $y^{-1} * x^{-1}$ is an inverse of $x * y$.

Yet the inverse in a group is unique so the two inverses we have here must be equal, i.e. $(x * y)^{-1} = y^{-1} * x^{-1}$. ■

**Question** But why do we call $(S_n, \circ)$ the *symmetric* group?

Consider, as an example, $n = 4$. Think of a square in the plane, center at the origin, with vertices at $(1, 1)$, $(-1, 1)$, $(-1, -1)$ and $(1, -1)$, labelled clockwise, 1,2,3 and 4. What symmetries does the square have? It has rotational symmetries about the origin. If we rotate by $\pi/2$ in the clockwise direction we see that corners map $1 \to 2$, $2 \to 3$, $3 \to 4$ and $4 \to 1$. So this rotation can be represented by the cycle $(1, 2, 3, 4)$.

In the other direction what would $(1, 2) \circ (3, 4)$ represent? It would be a reflection in a line through the origin.

**For Student:** What are the permutations that represent the other symmetries of the square?

In this way we see that $S_4$ contains the symmetries of the square. Hence the use of the word "symmetry" in the name of $(S_n, \circ)$.