Chapter 7

Permutations

Definitions and notation

Definition (permutation)**.** A **permutation** of a set A is a bijection $\rho\colon A \to A$.

Example (identity permutation)**.** For any set A, the **identity map**, $\mathbb{1}_A$, defined by $\mathbb{1}_A(a) = a$ for all $a \in A$, is a permutation of A.

Definition (the symmetric group S_n)**.** Recall the finite set $\mathbb{N}_n = \{1, 2, \ldots, n\}$.

The **symmetric group on n letters**, denoted S_n, is the set of all permutations of $\mathbb{N}_n$.

The identity permutation in S_n is denoted $\mathbb{1}_n$.

Notation. If $\rho \in S_n$, we can write ρ using **two-line notation** due to Cauchy:

$$\rho = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \rho(1) & \rho(2) & \rho(3) & \ldots & \rho(n) \end{pmatrix}.$$

In particular,

$$\mathbb{1}_n = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}.$$

Example (list of elements of S_3)**.** S_3 consists of

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Question. How many permutations are there of a finite set A?

Theorem 7.1 (the cardinality of S_n)**.** If $|A| = n \geq 1$ then the number of permutations $\rho\colon A \to A$ is $n!$. In particular, $|S_n| = n!$.

Proof. In Chapter 1 we introduced the set $Bij(X,Y)$ of bijections between the set X and the set Y. Permutations of A are exactly the elements of $Bij(A,A)$. By Proposition 1.1, the number of elements of this set is $n!$. □

Recall, if ρ and π are functions $A \to A$, then the composite function is defined by

$$\rho \circ \pi\,(a) = \rho\,(\pi\,(a))$$

for all $a \in A$. Further, if ρ and π are bijections then $\rho \circ \pi$ is a bijection. Hence the composition of permutations is a permutation. We record this in the following

Definition (composition or product, of permutations)**.** Let $\rho,\ \pi \in S_n$. The **composition**, or **product**, of ρ and π is the permutation

$$\rho \circ \pi \in S_n, \qquad (\rho \circ \pi)(a) = \rho(\pi(a)), \qquad \forall a \in \mathbb{N}_n.$$

Alternative notation: we may omit the $\circ$ sign and write $\rho\pi$ for the product $\rho \circ \pi$.

Example (product of permutations is not commutative)**.** The product of permutations is, in general, **not commutative**, meaning that $\rho\pi$ may be different from $\pi\rho$.

To demonstrate this, consider the following example. Let $\rho, \pi \in S_5$ be given by

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} \quad \text{and} \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

Calculate $\rho \circ \pi$.

Solution. To write $\rho \circ \pi$ in the same way we have to see first what π does to a given element of A and then secondly what ρ does to this image. In this example,

$$\begin{array}{lcl}
2 \xleftarrow{\rho} 2 \xleftarrow{\pi} 1 & \quad\text{so}\quad & \rho \circ \pi\,(1) = 2, \\
1 \xleftarrow{\rho} 3 \xleftarrow{\pi} 2 & \quad\text{so}\quad & \rho \circ \pi\,(2) = 1, \\
3 \xleftarrow{\rho} 4 \xleftarrow{\pi} 3 & \quad\text{so}\quad & \rho \circ \pi\,(3) = 3, \\
5 \xleftarrow{\rho} 5 \xleftarrow{\pi} 4 & \quad\text{so}\quad & \rho \circ \pi\,(4) = 5, \\
4 \xleftarrow{\rho} 1 \xleftarrow{\pi} 5 & \quad\text{so}\quad & \rho \circ \pi\,(5) = 4.
\end{array}$$

Thus

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

Note we first looked at π then at ρ, so read $\rho\circ\pi$ **from the right**.

Note also that

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

so that, for instance, $\rho\circ\pi\,(1) = 2$ but $\pi\circ\rho\,(1) = 5$. Thus

$$\rho\circ\pi \neq \pi\circ\rho,$$

which shows that composition of permutations is **not** commutative.

Inverses

Recall, *a bijection always has an inverse*. The inverse of a permutation written in the two row manner can easily be found by **exchanging the rows**, and then **reordering the columns** so that the entries on the upper row appear in the correct order.

Definition. The **inverse** of a permutation $\rho \in S_n$ is the bijection inverse to ρ. This is the permutation $\rho^{-1} \in S_n$ such that $\rho\circ\rho^{-1} = \rho^{-1}\circ\rho = \mathbb{1}_n$.

Example (finding the inverse in two-line notation)**.** In S_5 find the inverse of

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

Solution.

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

You can check that your answer satisfies the definition of inverse:

$$\begin{aligned} &\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \\ =&\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} = \mathbb{1}_5. \end{aligned}$$

Cycles

Definition (fixed elements, elements that are moved)**.** If ρ is a permutation in S_n then ρ **fixes** $a \in \mathbb{N}_n$ if $\rho(a) = a$ and ρ **moves** a if $\rho(a) \neq a$.

Notation: we write

$$Fix(\rho) = \{a \in \mathbb{N}_n : \rho(a) = a\}$$

for the set of fixed elements of ρ, and

$$Move(\rho) = \mathbb{N}_n \setminus Fix(\rho)$$

for the set of elements that are moved by ρ.

Example (finding the set of elements fixed by a given permutation)**.** In S_5, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$.
Then $Fix(\sigma) = \varnothing$ and $Fix(\tau) = \{2, 3, 4\}$.

Exercise (for students to attempt in their own time)**.** Is there a permutation $\tau \in S_5$ such that $Fix(\tau) = \{1, 2, 3, 4\}$?

Definition (disjoint permutations)**.** Permutations $\sigma, \tau \in S_n$ are **disjoint** if $Move(\sigma) \cap Move(\tau) = \varnothing$.

Lemma 7.2 (disjoint permutations commute)**.** Two disjoint permutations $\sigma, \tau \in S_n$ **commute**, i.e., $\sigma\tau = \tau\sigma$ in S_n.

Proof. Assume that permutations $\sigma, \tau \in S_n$ are disjoint. We need to show that $\sigma(\tau(a)) = \tau(\sigma(a))$ where $a \in \mathbb{N}_n$ is arbitrary. Since a cannot be both in $Move(\sigma)$ and in $Move(\tau)$, one has $\sigma(a) = a$ or $\tau(a) = a$; without loss of generality, assume $\sigma(a) = a$.

We claim that $\tau(a)$ is also fixed by σ. This is true if $\tau(a) = a$, since a is fixed by σ. Otherwise, $\tau(a) \neq a$; the permutation τ is a bijection hence an injection, so, applying τ to both sides, we obtain $\tau(\tau(a)) \neq \tau(a)$. This shows that $\tau(a) \in Move(\tau)$, so $\tau(a) \notin Move(\sigma)$, as claimed.

Now, using the assumption $a = \sigma(a)$, we conclude that $\sigma(\tau(a)) = \tau(a) = \tau(\sigma(a))$. $\square$

Remark. Warning: the converse of the proposition does not hold. If σ, τ commute, i.e., $\sigma\tau = \tau\sigma$, it does not necessarily mean that σ, τ are disjoint. An easy example is: σ commutes with σ for all $\sigma \in S_n$, but σ is not disjoint with σ if $\sigma \neq \mathbb{1}_n$.

Definition (cycle)**.** Let $a_1, a_2, \ldots, a_r$ be *distinct* elements in $\mathbb{N}_n$. If ρ is a permutation that fixes all the other elements of $\mathbb{N}_n$ 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 ρ is called a **cycle** of **length** r, sometimes called an $\boldsymbol{r}$**-cycle**. The r-cycle above will be denoted by

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

Remark (different ways to write the same cycle)**.** Note that any a_i can be taken as the "starting point", so

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

Remark (what are 1-cycles?)**.** We can take $r = 1$ in the definition to get a 1-cycle, (a_1). But such a cycle fixes all elements of $\mathbb{N}_n$ and is thus the identity. Hence all 1-cycles equal the identity, i.e. $(a) = \mathbb{1}_n$ for all $a \in \mathbb{N}_n$.

Definition (transposition)**.** A 2-cycle is called a **transposition**.

Example. (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

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

Example (Finding the inverse in cycle notation)**.** 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.

Example (Finding composition of cycles)**.** We can compose cycles written in cycle notation, remembering to read *from the right.* So, in S_5,

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

as seen before. Again, we did this by noting that π moved 1 to 2 which ρ then fixed. Next π moved 2 to 3 which ρ moved to 1. Continue.

At the moment, we obtain an answer in two-line notation only.

Example. In S_3 we can represent all possible products in a table

$\circ$	$\mathbb{1}_3$	$(2,3)$	$(1,2)$	$(1,3)$	$(1,3,2)$	$(1,2,3)$
$\mathbb{1}_3$	$\mathbb{1}_3$	$(2,3)$	$(1,2)$	$(1,3)$	$(1,3,2)$	$(1,2,3)$
$(2,3)$	$(2,3)$	$\mathbb{1}_3$	$(1,3,2)$	$(1,2,3)$	$(1,2)$	$(1,3)$
$(1,2)$	$(1,2)$	$(1,2,3)$	$\mathbb{1}_3$	$(1,3,2)$	$(1,3)$	$(2,3)$
$(1,3)$	$(1,3)$	$(1,3,2)$	$(1,2,3)$	$\mathbb{1}_3$	$(2,3)$	$(1,2)$
$(1,3,2)$	$(1,3,2)$	$(1,3)$	$(2,3)$	$(1,2)$	$(1,2,3)$	$\mathbb{1}_3$
$(1,2,3)$	$(1,2,3)$	$(1,2)$	$(1,3)$	$(2,3)$	$\mathbb{1}_3$	$(1,3,2)$

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 $(\mathbb{Z}_m^*, \times)$.

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 analogue of prime factorisation for permutations?

Algorithm for factorisation **into disjoint cycles** is best illustrated by an example.

Example. 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 π does to 1 on repeated applications. It sends 1 to 5. Then π sends 5 to 4. Next π 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 work out what happens to 2 under repeated applications of π, 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 3, and we see this is fixed by π, and so we get a 1-cycle (3), which we know is the identity. When there is at least one non-identity cycle we can omit the identity (3).

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

Hence

$$\pi = (1,5,4) \circ (2,6) \circ (3) = (1,5,4) \circ (2,6)\,.$$

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

It can be proved that each new cycle contains no elements in any earlier cycle. That is, the new cycle is **disjoint** from all the earlier cycles.

The factorisation method above can be formalised as follows.

Theorem 7.3. Every permutation in S_n can be expressed as a product of disjoint cycles **uniquely** up to a reordering of the cycles.

Proof. No formal proof given, but you should master the factorisation algorithm above. $\square$

Order of a permutation

Definition.

- The **positive powers** ρ^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 $\rho^{-n} = \left(\rho^{-1}\right)^n$ for all $n \in \mathbb{N}$, i.e. taking positive powers (just defined) of the inverse of ρ.
- Finally, we set $\rho^0 = \mathbb{1}$.

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

Claim. $\rho^{m+n} = \rho^m \circ \rho^n$ for all $m,n \in \mathbb{Z}$. $\square$

Corollary 7.4. Powers of a permutation ρ commute: $\rho^m \rho^n = \rho^n \rho^m$ for all $m,n \in \mathbb{Z}$.

Proof. By Claim 7, both sides are equal to ρ^{m+n}. $\square$

Now, the method described above of factorising a permutation started by taking an element of A, repeatedly applying ρ *until you returned to a when you then have a cycle*. This italicised sentence is an assumption: we have to show that repeatedly applying ρ to a does, in fact, gets us back to a. This follows, for example, from the next Lemma.

Lemma 7.5. Let ρ be a permutation in S_n. There exists $m \geq 1$ for which $\rho^m = \mathbb{1}_n$.

Proof. Consider the set $\{\rho^j : j \geq 0\} \subseteq S_n$. The set S_n of all permutations of $\mathbb{N}_n$ is finite (the number of all permutations is $n!$), hence $\{\rho^j : j \geq 0\}$ is a finite set. Therefore we must have repetition, i.e. $\exists \ell > k \geq 0$ for which $\rho^\ell = \rho^k$. Pre-multiplying both sides by ρ^{-k}, we obtain

$$\begin{aligned}
\rho^{\ell-k} &= \rho^\ell \circ \rho^{-k} && \text{by Claim 7} \\
&= \rho^k \circ \rho^{-k} && \text{since } \rho^\ell = \rho^k \\
&= \rho^{k-k} && \text{again by 7} \\
&= \rho^0 = \mathbb{1}_n && \text{by definition.}
\end{aligned}$$

Thus we have found an $m = \ell - k \geq 1$ for which $\rho^m = \mathbb{1}_n$. $\square$

This result motivates the following

Definition (order of a permutation)**.** The **order** of a permutation $\rho \in S_n$ is the **least** positive integer d such that $\rho^d = \mathbb{1}_n$.

Remark. The order of a permutation **exists**, because by Lemma 7.5, it is the least element of a non-empty set of natural numbers.

Example (Powers of a permutation via disjoint cycles)**.** Let

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

Write π as a product of disjoint cycles. Hence find π^2, π^3, π^4, π^5, π^6.

Solution. Using the algorithm above to factorise π into disjoint cycles, we obtain

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

Now, since disjoint cycles commute, we can swap $(1, 5, 4)$ and $(2, 6)$ in the following calculation:

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

We observe that the permutation $(1,5,4)^2$ maps the elements 1, 5 and 4 as follows:

$$1 \mapsto 5 \mapsto 4, \qquad 5 \mapsto 4 \mapsto 1, \qquad 4 \mapsto 1 \mapsto 5$$

where each arrow is one application of the cycle $(1,5,4)$; elements other than 1, 5 and 4 are fixed by $(1,5,4)^2$. We conclude that

$$(1,5,4)^2 = (1,4,5).$$

We can similarly find the square of the transposition $(2,6)$:

$$(2,6)^2 = \mathbb{1}.$$

We arrive at

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

Arguing in the same way, we find

$$\begin{aligned}
\pi^3 &= (1,5,4)^3(2,6)^3 = \mathbb{1}(2,6) = (2,6),\\
\pi^4 &= (1,5,4)^4(2,6)^4 = (1,5,4)\mathbb{1} = (1,5,4),\\
\pi^5 &= (1,5,4)^5(2,6)^5 = (1,4,5)(2,6),\\
\pi^6 &= (1,5,4)^6(2,6)^6 = \mathbb{1}\mathbb{1} = \mathbb{1}.
\end{aligned}$$

Note, writing π as disjoint cycles makes it easier to compute π^k. We found that the order of π is 6.

Remark (how to find the order of a permutation?)**.** Computing all the successive powers of π until we obtain identity is inefficient if we only want to find the order of π. What if we had a permutation from S_{100}? How many powers would we have to compute? Can the order be anywhere near $100!$ (greater than the number of electrons in observable universe)?

Question. Is there a better way to find the order from disjoint cycles?

We first answer the question for permutations for which the order is easy to find: cycles.

Lemma 7.6 (order of a cycle)**.** A cycle of length r has order r.

Sketch of proof. To simplify the notation, instead of a cycle $(a_1, a_2, \ldots, a_r)$ we will use the cycle $\pi = (1,2,\ldots,r)$. Note that $\pi(1) = 2$, $\pi^2(1) = \pi(2) = 3$, etc; using induction, one shows that $\pi^k(1) = 1 + k$ *if* $k < r$. This means that $\pi^k \neq \mathbb{1}$ if $k < r$.

On the other hand we have $\pi^r(1) = \pi(\pi^{r-1}(1)) = \pi(r) = 1$. Moreover, for all i, $1 \le i \le r$, we have $\pi^r(i) = \pi^r(\pi^{i-1}(1))$ which equals $\pi^{i-1}(\pi^r(1)) = \pi^{i-1}(1) = i$. This shows that $\pi^r = \mathbb{1}$. Hence r is the least positive integer with this property, that is, the order of π. $\square$

Remark (powers of a cycle are not necessarily cycles)**.** One should be aware that powers of a cycle may not be cycles: e.g., $(1,2,3,4)^2 = (1,3)(2,4)$.

Question. If a permutation ρ has order d, we know that by definition of order $\rho^d = \mathbb{1}$. What other powers ρ^m of ρ are equal to the identity?

Proposition 7.7 (powers of ρ that are identity)**.** If the order of ρ is d then, for any $m \in \mathbb{Z}$, $\rho^m = \mathbb{1}$ if, and only if, $d \mid m$.

Proof. By the Division Theorem, the integer m can be written as $m = dq + r$ where $q \in \mathbb{Z}$ and $0 \le r < d$. We do this because we know that any product of dth powers of ρ gives the identity. Then

$$\rho^m = \rho^{dq}\rho^r = (\rho^d)^q\rho^r = \mathbb{1}^q\rho^r = \rho^r.$$

If $\rho^m = \mathbb{1}$, then $\rho^r = \mathbb{1}$. This is impossible for *positive* remainder r, as in this case $0 < r < d$ but by definition d is the **least** positive integer with this property. Hence $r = 0$, meaning $d \mid m$.

Vice versa, if $d \mid m$, then $r = 0$ and $\rho^m = \rho^0 = \mathbb{1}$. □

We are almost ready to state the result about the order of an arbitrary permutation. It depends on the following

Definition. The **lowest common multiple** of positive integers $m_1, m_2, \ldots, m_t$, denoted by

$$\operatorname{lcm}(m_1, m_2, \ldots, m_t),$$

is the least positive integer f such that $m_1 \mid f$, $m_2 \mid f, \ldots, m_t \mid f$.

Remark (Properties of lcm)**.**

1. The lcm of positive integers $m_1, m_2, \ldots, m_t$ **exists**.

   Indeed, lcm is the least element of the set of all positive common multiples of $m_1, \ldots, m_t$. This set is not empty: for example, the product $m_1 \ldots m_t$ is in the set. Every non-empty set of positive integers contains a least element.

2. The lcm **may not be equal to the product** of the given numbers.

   For example, $\operatorname{lcm}(4,6) = 12$ not 24.

3. The least common multiple **divides any other common multiple**.

   Indeed, assume that k is a common multiple, i.e. $m_1 \mid k$, $m_2 \mid k, \ldots, m_t \mid k$. Let $f = \operatorname{lcm}(m_1, m_2, ..., m_t)$. Write $k = fq + r$ where $0 \le r < f$. Then each m_i divides both k and f hence divides $r = k - fq$. So r is a common multiple, but f is the **least positive** common multiple, yet $r < f$. Hence r cannot be positive. The only remaining possibility is $r = 0$ so that $f \mid k$.

Exercise. Compare the definition of lcm to that of gcd.

Theorem 7.8 (Calculating the order by factorisation)**.** Suppose that

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

is a decomposition into a product of **disjoint** permutations. Then

$$\mathrm{order}(\pi) = \mathrm{lcm}\left(\mathrm{order}(\pi_1), \ldots, \mathrm{order}(\pi_m)\right).$$

Proof. Consider the kth power

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

Since the permutations on the right hand side are disjoint, by Lemma 7.2 the compositions **commute**, so the permutations can be moved around to give

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

Assume now that $\pi^k = \mathbb{1}$, so π^k moves **no** elements. Because the permutations are disjoint each of π_1^k, $\pi_2^k, \ldots, \pi_m^k$ move different elements and so π^k moves no elements if, and only if, each of π_1^k, $\pi_2^k, \ldots, \pi_m^k$ moves no elements. That is,

$$\pi^k = \mathbb{1} \qquad \Longleftrightarrow \qquad \forall i,\ 1 \le i \le m,\ \pi_i^k = \mathbb{1}.$$

Denote by d_i the order of π_i. By Proposition 7.7 $\pi_i^k = \mathbb{1}$ for all $1 \le i \le m$ iff $d_i \mid k$ for all $1 \le i \le m$.

Finally, in searching for the order of π we want the *least* k divisible by all the d_i. By definition, this is exactly $\mathrm{lcm}(d_1, \ldots, d_m)$. □

Remark. Although the Theorem is true for any set of disjoint permutations, in practice, given a permutation π we decompose it into a product of disjoint **cycles**.

Corollary. 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 π is the least common multiple of the lengths of the cycles $\sigma_1, \sigma_2, \ldots, \sigma_m$.

Example (calculating the order by factorising into disjoint cycles)**.** In S_{12} consider

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

To find the order of π, write π as a product of **disjoint** cycles:

$$\pi = (4, 10, 8, 9, 7) \circ (2, 3, 5) \circ (1, 6) \circ (11, 12).$$

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

Example (largest order in S_{12})**.** What is the *largest* order of all permutations in S_{12}?

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

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

has order 60.

Example (finding the order when cycles are not disjoint)**.** In S_8, what is the order of

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

Solution. CAREFUL, the cycles are not disjoint! We have to write this as a product of disjoint cycles. The way we do this is similar to factorising a permutation given in two-row notation. We start with 1 and note that an element is not moved by a cycle or a product of cycles where it does not appear. So, for example,

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

giving $\pi(1) = 2$. Continue:

$$\begin{aligned} 1 &\xrightarrow{(1,2,4,6,8)\circ(2,3,6)\circ(6,7)} 2 \\ &\xrightarrow{(1,2,4,6,8)\circ(2,3,6)\circ(6,7)} 3 \\ &\xrightarrow{(1,2,4,6,8)\circ(2,3,6)\circ(6,7)} 8 \\ &\xrightarrow{(1,2,4,6,8)\circ(2,3,6)\circ(6,7)} 1, \end{aligned}$$

completing the first cycle $(1,2,3,8)$. Now start with 4:

$$\begin{aligned} 4 &\xrightarrow{(1,2,4,6,8)\circ(2,3,6)\circ(6,7)} 6 \\ &\xrightarrow{(1,2,4,6,8)\circ(2,3,6)\circ(6,7)} 7 \\ &\xrightarrow{(1,2,4,6,8)\circ(2,3,6)\circ(6,7)} 4. \end{aligned}$$

Finally, 5 is fixed by π so will not appear in the decomposition into disjoint cycles. We obtain

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

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

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 letters*?

Definition (binary operation)**.** A **binary operation** on a set S is a function from the set $S \times S$ of ordered pairs 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

$$\forall c, d \in C,\ c * d \in C.$$

Example.

- $+$, $-$, $\times$ are binary operations on the set $\mathbb{Z}$ of integers. / (divide) is not a binary operation on $\mathbb{Z}$.
- Furthermore, if $m \geq 1$, then $+$, $-$, $\times$ are binary operations on the finite set $\mathbb{Z}_m$ of congruence classes mod m. The subset $\mathbb{Z}_m^*$ of $\mathbb{Z}_m$, which consists of *invertible* congruence classes, is closed under $\times$ but not under $+$.
- If $n \geq 1$, the set $\mathit{Fun}(\mathbb{N}_n, \mathbb{N}_n)$ of all functions from $\mathbb{N}_n$ to itself has binary operation $\circ$ (composition). The set S_n of all *permutations* of $\mathbb{N}_n$ is a subset of $\mathit{Fun}(\mathbb{N}_n, \mathbb{N}_n)$ closed under $\circ$.
- If A is a set, then $\cup$, $\cap$, $\setminus$ are binary operations on the power set $\mathcal{P}(A)$.

Exercise. Show that the subset $\{\varnothing, A\}$ of $\mathcal{P}(A)$ is closed under all the three operations $\cup$, $\cap$ and $\setminus$.

Example. $\mathbb{Z}_{20}$ 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

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

A binary operation may (or may not) satisfy the following important properties.

Definition. (i) A binary operation $*$ on S is **commutative** if,

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

(ii) A binary operation $*$ on S is **associative** if,

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

(iii) A binary operation $*$ on S has an **identity** $e \in S$ if

$$\forall a \in S,\ e * a = a \text{ and } a * e = a.$$

Remark (two checks for identity)**.** In the definition of an identity, we have to check both $e * a$ and $a * e$ since we are not assuming that $*$ is commutative.

Example. On the set $\mathbb{Z}$:

- $+$, $\times$ are commutative and associative;
- $+$ has identity 0: $\forall a \in \mathbb{Z}\ 0 + a = a + 0 = a$;
- $\times$ has identity 1: $\forall a \in \mathbb{Z}\ 1 \times a = a \times 1 = a$;
- the binary operation $-$ on $\mathbb{Z}$ is not commutative, not associative and has no identity.

On the set S_n of permutations:

- $\circ$ is associative; $\circ$ is not commutative for $n \geq 3$; $\circ$ has identity $\mathbb{1}_n$.

Example. $\{[4]_{20}, [8]_{20}, [12]_{20}, [16]_{20}, \times\}$. This binary operation is commutative and associative. 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 7.9 (identity, if exists, is unique)**.** 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 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 (invertible element)**.** Let S be a set with a binary operation $*$ and identity $e \in S$. We say that an element $a \in S$ is **invertible** if there exists $b \in S$ such that

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

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

Example. Show that in $(\mathbb{Z}_6, \times)$ the element $[2]_6$ has no inverse.

Solution. Assume for contradiction that $[2]_6$ has an inverse, say $[b]_6$. Then

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

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

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

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 is to look at $(\mathbb{Z}_m^*, \times)$ where we have simply thrown away all the elements that don't have an inverse!

Lemma 7.10 (inverse under an associative $*$ is unique)**.** 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, consider the equation

$$b * (a * c) = (b * a) * c.$$

The left-hand side evaluates to $b * e = b$ since c is an inverse of a and $a * c = e$.

The right-hand side evaluates to $e * c = c$ since b is an inverse of a and $b * a = e$.

But the left-hand side equals the right-hand side, by associativity. Thus $b = c$ and the inverse is unique. □

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

Groups

Definition. Given a set G and binary operation $*$ on G we say that $(G, *)$ is a **group** if $*$ obeys the following rules:

G1. G is closed under $*$, [*this is part of the definition of binary operation*]

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.

$$\forall a \in G, \ \exists a^{-1} \in G : \ a * a^{-1} = a^{-1} * a = e.$$

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

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

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 ($\dagger$) holds in *any* group:

Proposition 7.11. Assume that $(G, *)$ is a group. If $x, y \in G$ then

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

Notice how the order of factors has changed.

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

Next note that

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

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 by Lemma 7.10 so the two inverses we have here must be equal, i.e. $(x * y)^{-1} = y^{-1} * x^{-1}$. $\square$

Question. We now understand why $(S_n, \circ)$ is a *group*. But why do we call the *symmetric* group?

Answer. In general, *symmetries* are bijections from a set X to itself which preserve some given structure on the set X.

The set $\mathbb{N}_n$ has no specific structure we want to preserve, so "symmetries" of the set $\mathbb{N}_n$ are simply all bijections $\mathbb{N}_n \to \mathbb{N}_n$.

But groups arise everywhere symmetries are involved, and it is especially instructive to look at symmetries of geometric shapes.

Consider, as an example, $n = 4$. Think of a square in the plane, centred at the origin, with vertices at $(1, 1)$, $(-1, 1)$, $(-1, -1)$ and $(1, -1)$, labelled clockwise by 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. Each symmetry of the square can be represented by an element of S_4.

Exercise. What are the permutations that represent the other symmetries of the square?

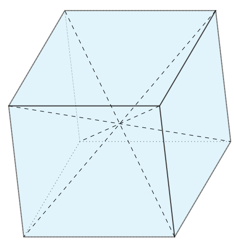
Every symmetry of the square is represented by a permutation from S_4 but this does not exhaust *all* of S_4. Give an example of a permutation in S_4 which does **not** represent a symmetry of the square.

Exercise (symmetries of a regular tetrahedron)**.** Imagine a regular tetrahedron in the three-dimensional space, with vertices labelled 1, 2, 3 and 4. Symmetries of the tetrahedron are all possible rotations and reflections of the space which take the tetrahedron to itself — but the four vertices possibly change places (are permuted), so again a symmetry is written as a permutation of $\{1, 2, 3, 4\}$.

Show that, unlike for the square, **every** permutation in S_4 represents a symmetry of the regular tetrahedron.

The next and final exercise is more advanced and requires spatial thinking — try it:

Exercise. Consider a **cube** in the 3D space. Look at the **rotations** of the cube: these are symmetries of the cube which take the cube to itself, moving it as a solid body, without reflections. Show that there are 24 rotations of the cube. Label the four **main diagonals** of the cube (i.e., the diagonals which pass through the centre of the cube) as 1, 2, 3, 4 and show that every element of S_4 viewed as a permutation of the four diagonals represents one, and only one, rotation of the cube.



THE END