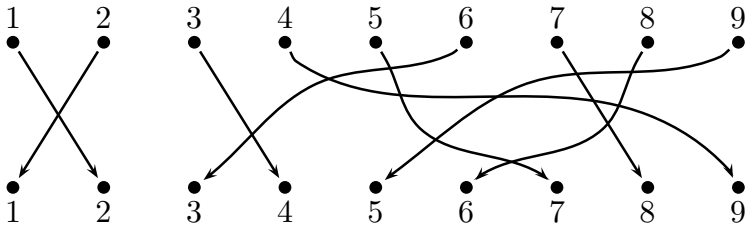
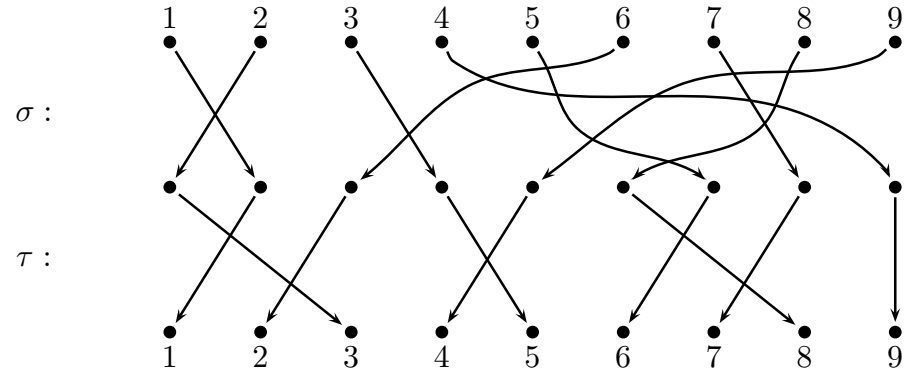
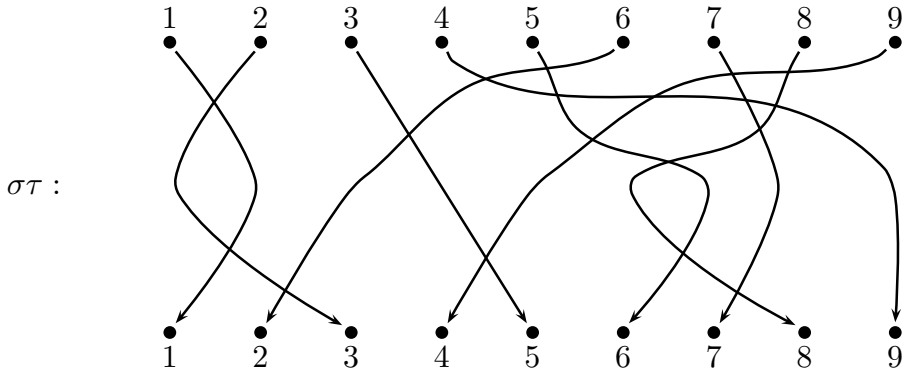
More on permutations

Recall that a permutation of $\{1, 2, \ldots, n\}$ is uniquely determined by specifying what the permutation does to each element $i \in \{1, 2, \ldots, n\}$. In other words, if σ is a permutation of $\{1, 2, \ldots, n\}$, and if you know the values of 1^σ, 2^σ, $\ldots$, n^σ, then you know σ. It can be helpful to associate a permutation with a diagram, in the following way. Draw two rows of n dots, each labelled with the numbers from 1 to n. For each i, draw an arrow that points from the dot labelled i in the first row to the dot labelled i^σ in the second row. Here is such a diagram for the permutation $\sigma = (1, 2)(3, 4, 9, 5, 7, 8, 6) \in \mathrm{Sym}(9)$:



The product of a pair of permutations can be computed from their diagrams. Thus, suppose that we wish to compute $\sigma\tau$, where σ is as above and $\tau = (1, 3, 2)(4, 5)(6, 8, 7)(9)$. (For clarity's sake we have included the fixed point 9 explicitly, but this permutation would usually be written simply as $(1, 3, 2)(4, 5)(6, 8, 7)$.) The method is to draw the diagram for τ below the diagram for σ, combining the second row of σ with the first row of τ, and then simply merge the two diagrams into one by erasing the middle row of dots and joining up the arrows.





Thus we see that $\sigma\tau = (2,3,5,6)(4,9)$. This diagrammatic approach simply encapsulates the rule that to compute what the product $\sigma\tau$ does to each $i \in \{1, 2, \ldots, n\}$, apply σ first and then apply τ to the result: $i^{\sigma\tau} = (i^{\sigma})^{\tau}$.

Of course, MAGMA is quite good at multiplying permutations.

```
> G:=Sym(8);
> r:=G!(1,4)(2,3)(5,8)(6,7);
> s:=G!(2,4)(5,7);
> t:=G!(2,6)(3,7);
> r*s;
(1, 2, 3, 4)(5, 8, 7, 6)
> s*t;
(2, 4, 6)(3, 7, 5)
> X:={r,s,t};
> XX:={x*y : x,y in X};
> XX;
{
    (1, 4, 3, 2)(5, 6, 7, 8),
    (2, 4, 6)(3, 7, 5),
    Id(G),
    (2, 6, 4)(3, 5, 7),
    (1, 4)(2, 7)(3, 6)(5, 8),
    (1, 2, 3, 4)(5, 8, 7, 6)
}
> X:=X join XX;
> XX:={x*y : x,y in X};
> XX;
{
    (1, 4)(2, 7)(3, 6)(5, 8),
    (1, 6, 5, 2)(3, 4, 7, 8),
    (1, 3, 7)(2, 8, 6),
    (1, 4, 7, 8, 5, 2)(3, 6),
    (1, 2, 5, 6)(3, 8, 7, 4),
    (1, 7, 3)(2, 6, 8),
    (1, 6, 7, 4)(2, 5, 8, 3),
    (1, 2, 5, 8, 7, 4)(3, 6),
    (2, 6)(3, 7),
    (1, 2)(3, 6)(4, 5)(7, 8),
    (2, 4, 6)(3, 7, 5),
    (1, 4)(2, 3)(5, 8)(6, 7),
    (1, 4, 3, 2)(5, 6, 7, 8),
    (2, 6, 4)(3, 5, 7),
    (1, 2, 3, 4)(5, 8, 7, 6),
    (1, 2)(3, 4)(5, 6)(7, 8),
    (3, 5)(4, 6),
    (1, 3)(2, 4)(5, 7)(6, 8),
    (1, 3)(6, 8),
```

```
    (2, 4)(5, 7),
    Id(G),
    (1, 4, 3, 8, 5, 6)(2, 7),
    (1, 4, 7, 6)(2, 3, 8, 5),
    (1, 6, 5, 8, 3, 4)(2, 7)
}
> while not(XX subset X) do
while> X:=X join XX;
while> XX:={x*y : x,y in X};
while> end while;
> #X;
48
```

What we have done with the above MAGMA code is this: starting with the three permutations $r = (1,4)(2,3)(5,8)(6,7)$, $s = (2,4)(5,7)$ and $t = (2,6)(3,7)$ in Sym(8), we have calculated all possible products involving only these permutations as factors. Then, using all these products as well as the original three permutations, we have again calculated all possible products, and continued on in this way until we get nothing new. The last line of MAGMA output tells us that only 48 of the $8! = 40320$ permutations are obtained in this way. (That is, only 48 permutations can be expressed in terms of r, s and t.) This actually indicates that the permutations r, s and t are in some way special, since if the above were repeated with three randomly chosen permutations, it is quite likely that all 40320 would be be obtained. It would take a long time, though, as the example below illustrates. This was carried out using a 233 MHz computer, working with the smaller group Sym(7) rather than Sym(8). The principal feature of the MAGMA code employed is the definition of a function called "closure": given a set `A` of permutations in Sym(7), `closure(A)` returns the set of permutations obtained by the process described above. The code instructs MAGMA to print out, at the end of each loop, the time taken to complete the loop, and the number of permutations obtained thus far.

```
> G:=Sym(7);
> A:={G!(1,2),G!(1,2,3,4,5,6,7)};
> closure:=function(T);
function> X:={Id(G)};
function> XX:=T;
function> while not(XX subset X) do
function|while> t:=Realtime();
function|while> X:=X join XX;
function|while> XX:={x*y : x,y in X};
function|while> print "CPU time =", Cputime(t);
function|while> print "size is now",#X;
function|while> end while;
function> return X;
function> end function;
> closure(A);
CPU time = 0
size is now 3
CPU time = 0
```

```
size is now 6
CPU time = 0
size is now 19
CPU time = 0
size is now 138
CPU time = 105
size is now 2184
CPU time = 560
size is now 5040
{
    (2, 7, 6, 4),
    (1, 7, 5, 3, 6, 4),
   ... 5036 lines omitted ...
    (1, 4, 6, 3, 7)(2, 5),
    (1, 5, 7, 4)(2, 3)
}
> quit;
Total time: 728.000 seconds
```

It took about 12 minutes to complete. Note that Sym(8) has eight times as many elements as Sym(7), and since the main loop in this (rather unsophisticated) program involves two variables x and y ranging over the entire set, it seems probable that an example involving Sym(8) would take at least 64 times as long—13 hours—to complete.

It should be pointed out that MAGMA can do this in a far more efficient way. If `X` is a subset of `Sym(8)` then the construction `sub < Sym(8) | X >` returns the subgroup generated by `X`. Subgroups are discussed below, but at present all that matters is that `closure(X)`, as defined in the MAGMA code above, is actually the same as the subgroup generated by `X`, and MAGMA can find it almost instantaneously.

```
> S:=Sym(8);
> a:=S!(1,2);
> b:=S!(1,2,3,4,5,6,7,8);
> T:=sub < S | {a, b} >;
> T eq S;
true
> quit;
Total time: 4.000 seconds
```

(The 4.000 seconds was the time it took to paste the instuctions into MAGMA, not the computational time.)

It is not hard to prove that the subgroup generated by $\{(1,2),(1,2,\ldots,n)\}$ is the whole of Sym(n). It took MAGMA less than a minute to confirm this for all n in the range from 2 to 50.

We have yet to prove that Sym(n) is a group; let us turn to this task forthwith.

Proposition. *Multiplication of permutations is associative.*

Proof. Let ρ, σ, $\tau \in \mathrm{Sym}(n)$ be arbitrary. We need to show that $(\rho\sigma)\tau = \rho(\sigma\tau)$. For this it suffices to show that $i^{(\rho\sigma)\tau} = i^{\rho(\sigma\tau)}$ for all $i \in \{1, 2, \ldots, n\}$.

Now by definition, for all $i \in \{1, 2, \ldots, n\}$,

$$i^{(\rho\sigma)\tau} = (i^{(\rho\sigma)})^\tau = ((i^\rho)^\sigma)^\tau,$$

and since we similarly also have that

$$i^{\rho(\sigma\tau)} = (i^\rho)^{\sigma\tau} = ((i^\rho)^\sigma)^\tau,$$

we conclude that $i^{(\rho\sigma)\tau} = i^{\rho(\sigma\tau)}$, as required. □

The essence of the above argument is simply that $(\rho\sigma)\tau$ and $\rho(\sigma\tau)$ are both just ρ followed by σ followed by τ. If you evaluate both sides of the equation using the diagrammatic method explained above, you will find that you effectively do the same thing each time.

Recall that the identity permutation id is defined by $i^{\mathrm{id}} = i$, for all $i \in \{1, 2, \ldots, n\}$,

Proposition. *For all $\sigma \in \mathrm{Sym}(n)$ we have $\mathrm{id}\,\sigma = \sigma = \sigma\,\mathrm{id}$.*

Proof. For all $\sigma \in \mathrm{Sym}(n)$,

$$i^{\mathrm{id}\,\sigma} = (i^{\mathrm{id}})^\sigma = i^\sigma$$

and

$$i^{\sigma\,\mathrm{id}} = (i^\sigma)^{\mathrm{id}} = i^\sigma.$$

So $\mathrm{id}\,\sigma$ and $\sigma\,\mathrm{id}$ have the same effect as σ on all elements $i \in \{1, 2, \ldots, n\}$. □

Let $\sigma \in \mathrm{Sym}(n)$. As we noted in our earlier discussion of permutations, the function $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ given by $i \mapsto i^\sigma$ (for all i) is one-to-one and onto. It is a general fact that any function that is one-to-one and onto has an inverse. Explicitly, if $f\colon X \to Y$ is one-to-one and onto then its inverse is the function $g\colon Y \to X$ such that $g(y) = x$ if and only if $f(x) = y$ (for all $x \in X$ and $y \in Y$). The inverse function is also one-to-one and onto. Applied to σ, this tells us that there is a permutation $\sigma^{-1} \in \mathrm{Sym}(n)$ with the property that $j^{\sigma^{-1}} = i$ if and only if $i^\sigma = j$, for all $i, j \in \{1, 2, \ldots, n\}$. In other words σ^{-1} takes j to i if and only if σ takes i to j. Thus σ^{-1} is obtained by reversing all the cycles of σ.

For example, if σ is the permutation $(1, 5, 2)(3, 7, 6, 4)(9, 10) \in \mathrm{Sym}(10)$, then σ^{-1} is $(1, 2, 5)(3, 4, 6, 7)(9, 10)$.

Of course, if one reverses all the cycles, and then reverses them all again, the result is the original permutation. So $(\sigma^{-1})^{-1} = \sigma$ (for all permutations σ).

Definition. If σ is a permutation of $\{1, 2, \ldots, n\}$ then the *inverse* of σ is the permutation σ^{-1} of $\{1, 2, \ldots, n\}$ such that $j^{\sigma^{-1}} = i$ for all $i, j \in \{1, 2, \ldots, n\}$ satisfying $i^\sigma = j$.

Proposition. *Let $\sigma \in \mathrm{Sym}(n)$, and let $\sigma^{-1} \in \mathrm{Sym}(n)$ be defined as above. Then $\sigma\sigma^{-1} = \mathrm{id}$.*

Proof. Let $i \in \{1, 2, \ldots, n\}$ be arbitrary, and write $j = i^\sigma$. Then by the definition of σ^{-1} we have $j^{\sigma^{-1}} = i$, and so

$$i^{\sigma\sigma^{-1}} = (i^\sigma)^{\sigma^{-1}} = j^{\sigma^{-1}} = i.$$

So $\sigma\sigma^{-1}$ fixes every $i \in \{1, 2, \ldots, n\}$, and hence $\sigma\sigma^{-1} = \mathrm{id}$. □

Applying this result with σ^{-1} in place of σ tells us that $\sigma^{-1}(\sigma^{-1})^{-1} = \mathrm{id}$; that is, $\sigma^{-1}\sigma = \mathrm{id}$, since $(\sigma^{-1})^{-1} = \sigma$.

Our last three propositions tell us that permutation multiplication defines an associative operation on $\mathrm{Sym}(n)$, that this operation has an identity element, and that every element of $\mathrm{Sym}(n)$ has an inverse with respect to this operation. In other words, we have proved the following theorem.

Theorem. $\mathrm{Sym}(n)$ *is a group under the operation of permutation multiplication.*

Subgroups

It is quite possible for a subset of a group to itself be a group. We have already encountered several examples of this phenomenon. For example, by the theorem proved above, Sym(4), the set of all permutations of $\{1, 2, 3, 4\}$, is a group. By identifying the symmetries of a square with permutations we found that the subset $H = \{\mathrm{id}, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,3), (1,2)(3,4), (2,4), (1,4)(2,3)\}$ of Sym(4) is also a group under the operation determined by permutation multiplication. Similarly, the set of all nonzero complex numbers is a group under multiplication, and the subset $\{1, i, -1, -i\}$ is also a group with respect to an operation given by multiplication. We shall give more examples below.

Suppose that S is a set equipped with a binary operation $*$, and let T be a subset of S. It is clearly not necessarily the case that $*$ determines an operation on T. If x and y are elements of T then they are also elements of S, and so $x * y$ is defined. However, it is in S and not necessarily in T. The rule $(x, y) \mapsto x * y$ constitutes a binary operation on T if and only if T is closed under $*$, in the sense of the following definition.

Definition. Let $*$ be an operation on a set S, and let T be a subset of S. We say that T is *closed* under $*$ if $xy \in T$ for all x and y such that $x \in T$ and $y \in T$. When T is closed under $*$ the operation on T given by the rule $(x, y) \mapsto x * y$ (for all x, $y \in T$) is called the operation on T *inherited* from the operation $*$ on S.

We come now to this week's main concept.

Definition. A subset H of a group G is called a *subgroup* of G if the following conditions are satisfied:

SG1) $xy \in H$ for all x, $y \in H$;
SG2) $e \in H$, where e is the identity element of G;
SG3) for all x, if $x \in H$ then $x^{-1} \in H$.

The following theorem justifies the use of the term "subgroup" for this concept.

Theorem. *A subgroup of a group is a group under the inherited operation.*

Proof. Let H be a subgroup of G. Since (SG1) says that H is closed under the group operation of G, we know that H inherits an operation from this operation on G. So our task is to show that the group axioms are satisfied.

Since G is a group, we know (by (G1)) that $x(yz) = (xy)z$ for all x, y, $z \in G$. Since H is a subset of G, anything that holds for all elements of G certainly holds for all elements of H. So $x(yz) = (xy)z$ for all x, y, $z \in H$, which shows that the inherited operation is associative. Thus H satisfies (G1).

By (SG2) we know that the identity element e of G lies in the subset H. It is easy to see that this element of H satisfies the requirements of the group axiom (G2). Firstly,

since $ex = x = xe$ holds for all $x \in G$, it certainly holds for all $x \in H$. Secondly, by (SG3), if x is an arbitrary element of H then x^{-1} (the inverse of x in G) is in the subset H, and so there is a $y \in H$—namely, $y = x^{-1}$—satisfying $xy = e = yx$. So (G2) holds in H, and hence H is a group. □

Examples of subgroups

(1) The set $H = \{\mathrm{id}, (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,3), (1,2)(3,4), (2,4), (1,4)(2,3)\}$ is a subgroup of $G = \mathrm{Sym}(4)$. (See above.)

(2) The set $\{1, i, -1, -i\}$ is a subgroup of the multiplicative group of nonzero complex numbers. (See above.)

(3) Let $\mathcal{G}$ be the set of 2×2 matrices over $\mathbb{R}$ with nonzero determinant. As we noted last week, $\mathcal{G}$ is a group under matrix multiplication. Let $\mathcal{H} = \{\, A \in G \mid \det A = 1 \,\}$. We can check that $\mathcal{H}$ is a subgroup of $\mathcal{G}$. Firstly, if A, $B \in \mathcal{H}$ then $\det A = \det B = 1$, and so $\det(AB) = (\det A)(\det B) = 1$, showing that $AB \in \mathcal{H}$. So it follows that $\mathcal{H}$ is closed under matrix multiplication. Secondly, the identity element of $\mathcal{G}$ is the 2×2 identity matrix $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, which has determinant 1. So (SG2) holds. Thirdly, if $A \in \mathcal{H}$ then A^{-1} exists (since $\det A \neq 0$), and $(\det A)(\det A^{-1}) = \det(AA^{-1}) = 1$. Since $\det A = 1$ it follows that $\det A^{-1} = 1$ also, so that $A^{-1} \in \mathcal{H}$. We conclude that (SG3) also holds, as required.

(4) The set $\mathbb{C}$ (consisting of all complex numbers) is a group under addition. Identifying real numbers with complex numbers whose imaginary part is zero permits us to regard $\mathbb{R}$ as a subset of $\mathbb{C}$. Since the sum of two real numbers is real, $\mathbb{R}$ is an additively closed subset of $\mathbb{C}$. The zero element of $\mathbb{C}$ lies in $\mathbb{R}$ (since the imaginary part of 0 is 0), and the negative of every element of $\mathbb{R}$ is also in $\mathbb{R}$. So $\mathbb{R}$ is a subgroup of $\mathbb{C}$.

(5) The set $\mathbb{Z}$ of all integers is a subset of $\mathbb{R}$ (and hence also of $\mathbb{C}$). The sum of two integers is an integer; so $\mathbb{Z}$ is closed under addition. The real number 0 is an integer; so the zero element of $\mathbb{R}$ lies in the subset $\mathbb{Z}$. An the negative of every integer is also an integer. So $\mathbb{Z}$ is a subgroup of $\mathbb{R}$. The same reasoning shows equally that $\mathbb{Z}$ is a subgroup of $\mathbb{C}$. (Note that it is implicit throughout this example that the operation is the usual arithmetic operation of addition. Of course, other operations can be defined on these sets, and they may or may not make the sets into groups. And if some other operation makes $\mathbb{R}$ into a group, $\mathbb{Z}$ may or may not be a subgroup.)

(6) The set E consisting of all even integers is closed under addition, contains zero, and contains the negatives of all of its elements. So E is a subgroup of $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, under addition. By similar arguments, the set of all multiples of 4 is readily seen to be a subgroup of E, of $\mathbb{Z}$, of $\mathbb{R}$ and of $\mathbb{C}$. In general, the set of all integer multiples of any number x is a subgroup of $\mathbb{C}$, and if x' is an integer multiple of x then the group consisting of the integer multiples of x' is a subgroup of the group of integer multiples of x.

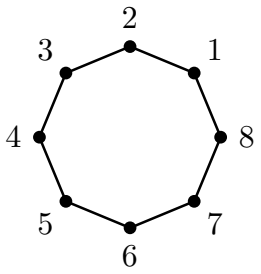
(7) The sets $\{1\}$, $\{1, -1\}$ and $\{1, i, -1, -i\}$ are all subgroups of the group $\{1, i, -1, -i\}$ (under multiplication). (Note that just as every set is regarded as a subset of itself, so every group is regarded as a subgroup of itself.

(8) If G is any group and e the identity element of G then the sets $\{e\}$ and G are both subgroups of G.

Definition. Let H be subgroup of a group G. We say that H is a *nontrivial* subgroup if $H \neq \{e\}$ (where e is the identity element). We say that H is a *proper* subgroup of G if $H \neq G$.

Cyclic groups

Consider a regular n-sided polygon, with vertices labelled with the numbers from 1 to n, and consider all of its rotational symmetries. Let σ be the anticlockwise rotation through the angle $\theta = 2\pi/n$ radians. For an octagon, labelled as in the diagram, it can be seen that σ corresponds to the permutation $(1, 2, 3, 4, 5, 6, 7, 8)$. In general, σ



corresponds to $(1, 2, \ldots, n) \in \mathrm{Sym}(n)$. Clearly σ^2 is the anticlockwise rotation through 2θ, σ^3 the anticlockwise rotation through 3θ, and so on. In particular, σ^n is the rotation through $n\theta = 2\pi$, which is the same as the identity transformation (the rotation through 0 radians). Thus σ has exactly n distinct powers, and it is also clear that these are all the rotational symmetries of the polygon.

Groups in which every element is a power of some fixed element are called *cyclic groups*. The group of all rotational symmetries of a regular n-sided polygon is a cyclic group of order n. The multiplication table of a cyclic group of order n has a particularly simple form, shown here in the case $n = 8$.

	e	σ	σ^2	σ^3	σ^4	σ^5	σ^6	σ^7
e	e	σ	σ^2	σ^3	σ^4	σ^5	σ^6	σ^7
σ	σ	σ^2	σ^3	σ^4	σ^5	σ^6	σ^7	e
σ^2	σ^2	σ^3	σ^4	σ^5	σ^6	σ^7	e	σ
σ^3	σ^3	σ^4	σ^5	σ^6	σ^7	e	σ	σ^2
σ^4	σ^4	σ^5	σ^6	σ^7	e	σ	σ^2	σ^3
σ^5	σ^5	σ^6	σ^7	e	σ	σ^2	σ^3	σ^4
σ^6	σ^6	σ^7	e	σ	σ^2	σ^3	σ^4	σ^5
σ^7	σ^7	e	σ	σ^2	σ^3	σ^4	σ^5	σ^6

The pattern involved should be clear.

Observe that we can also use complex numbers to give another construction of a cyclic group of order n. Define $\zeta = \cos\theta + i\sin\theta \in \mathbb{C}$, where (as above) $\theta = 2\pi/n$. By DeMoivre's Theorem, $\zeta^k = \cos(k\theta) + i\sin(k\theta)$, for each integer k. In particular, $\zeta^n = \cos(2\pi) + i\sin(2\pi) = 1$. Clearly ζ has exactly n distinct powers, and they satisfy the same multiplication table as the powers of σ above.

Of course, complex numbers are commonly associated with points in the Cartesian plane, the number $x + iy$ corresponding to the point with coordinates (x, y). The points corresponding to the powers of ζ lie on the unit circle, at the vertices of a regular n-sided polygon. Moreover, multiplying a complex number by ζ corresponds geometrically to applying a rotation about the origin through an angle of θ. So our two examples of cyclic groups of order n are very closely related to one another.

We have been talking about powers of elements, without having defined the concept. We should correct this omission. Observe first that if $*$ is an associative binary operation

on a set S, then all possible bracketings of an extended product $a_1 * a_2 * \cdots * a_n$ give the same element of S. For example,

$$\begin{aligned} a_1 * (a_2 * (a_3 * a_4)) = a_1 * ((a_2 * a_3) * a_4) = (a_1 * (a_2 * a_3)) * a_4 \\ = ((a_1 * a_2) * a_3) * a_4 = (a_1 * a_2) * (a_3 * a_4) \end{aligned}$$

by several applications of the asociative law. The general result can be proved by a straightforward induction, which we omit. It is convenient and customary to omit the brackets from such products. (Note, however, that the order of the factors must be preserved, unless it happens that the operation satisfies the commutative law, $a*b = b*a$.) Now if n is any positive integer we define the n-th power of $a \in S$ by $a^n = a_1 * a_2 * \cdots * a_n$, where $a_i = a$ for each i. If the set S has an identity element e, we define $a^0 = e$. And if the element a has an inverse, we define $a^{-n} = (a^{-1})^n$, for all positive integers n.

Given the above definitions, it is not hard to use mathematical induction to prove the familiar exponent laws $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$, which hold for all $a \in S$ and all integers m and n for which they make sense. (That is, m and n must be positive unless S has an identity element, are only allowed to be negative if a has an inverse.)

If the operation is written as addition, it is customary to use a different notation: $a + a + \cdots + a$ (where there are n terms) is written as na rather than a^n, and called a "multiple" of a rather than a "power". The exponent laws become $ma + na = (m + n)a$ and $n(ma) = (nm)a$.

Cyclic groups can have infinitely many elements. Consider, for example, the following set of rational numbers:

$$T = \{ \ldots, (3/2)^3, (3/2)^2, 3/2, 1, 2/3, (2/3)^2, (2/3)^3, \ldots \}.$$

It is readily checked that T is a subgroup of the multiplicative group of nonzero rational numbers; moreover, T is cyclic, since it can be described as $\{ (2/3)^k \mid k \in \mathbb{Z} \}$, the set of all powers of the element $2/3$. (Note that negative powers are included.) Distinct integers k give rise to distinct numbers $(2/3)^k$; so the number of elements of T is infinite.

The additive group of all integers is the standard example of an infinite cyclic group. All integers are multiples of the integer 1.

It is not hard to see that if G is any infinite cyclic group then there is a natural one-to-one correspondence between the elements of G and the integers. Specifically if G consists of the powers of the element g then the one-to-one correspondence is given by $g^n \leftrightarrow n$ for all $n \in \mathbb{Z}$.

Cyclic subgroups

If G is any group and $x \in G$ then the set of all powers of x is subgroup of G, called the *cyclic subgroup generated by* x, and denoted by $\langle x \rangle$.

For example, if $G = \mathrm{Sym}(4)$ and $x = (1, 2, 3, 4)$ then the powers of x are as follows:

$$x^0 = \mathrm{id}, \qquad , x^1 = (1, 2, 3, 4), \qquad x^2 = (1, 3)(2, 4), \qquad x^3 = (1, 4, 3, 2).$$

It is easily seen that if $n \in \mathbb{Z}$ lies outside the set $\{0, 1, 2, 3\}$ then $x^n = x^m$ for a some $m \in \{0, 1, 2, 3\}$. Specifically, m is the least nonnegative integer such that $n - m$ is a multiple of 4. For example, $x^4 = x^0 = \mathrm{id}$ and $x^{-1} = x^3$.

In the group $G = \mathrm{Sym}(3)$, the cyclic subgroup generated by the element $(2, 3)$ is $\langle (2, 3) \rangle = \{\mathrm{id}, (2, 3)\}$, since $(2, 3)^2 = \mathrm{id}$.