1.3 Subgroups and generating sets

A common approach to understanding algebraic structures is to try to find smaller structures within them that have similar properties. In the case of groups such things are called subgroups.

Example 1.3.1. ***The special linear groups***
Recall that $\mathrm{GL}(3,\mathbb{Q})$*, the set of* 3×3 *matrices that have rational entries and have non-zero determinant, is a group under matrix multiplication. Within this let* $\mathrm{SL}(3,\mathbb{Q})$ *denote the set of elements whose determinant is* 1*. Then*

1. $\mathrm{SL}(3,\mathbb{Q})$ *is closed under matrix multiplication.*
   What is required to show this is that whenever A *and* B *belong to* $\mathrm{SL}(3,\mathbb{Q})$*, then so does their product* AB*. To confirm that this is true we need to look at the defining properties of elements of* $\mathrm{SL}(3,\mathbb{Q})$ *and at how they behave under matrix multiplication.*

   So let $A, B \in \mathrm{SL}(3,\mathbb{Q})$*.*
   This means that A *and* B *are* 3×3 *rational matrices and* $\det(A) = \det(B) = 1$*.*
   Then $\det(AB) = \det(A)\det(B) = 1\times 1 = 1$*.*
   So $AB \in \mathrm{SL}(3,\mathbb{Q})$ *also.*
   (Note that this relies on the multiplicative property of the determinant.)

2. *The identity matrix belongs to* $\mathrm{SL}(3,\mathbb{Q})$ *(since its determinant is 1).*

3. *Suppose that* A *belongs to* $\mathrm{SL}(3,\mathbb{Q})$*. Then so also does* A^{-1}*, since*

$$\det A^{-1} = \frac{1}{\det A} = \frac{1}{1} = 1.$$

It follows that $\mathrm{SL}(3,\mathbb{Q})$ *is itself a group under matrix multiplication. We say that it is a* subgroup *of* $\mathrm{GL}(3,\mathbb{Q})$*.*

Terminology: $\mathrm{SL}(3,\mathbb{Q})$ is called the *special linear group* of 3×3 matrices over $\mathbb{Q}$ with determinant 1. The general linear group includes all invertible matrices; the special linear group only includes those with determinant 1.

Definition 1.3.2. *Let* G *be a group and let* H *be a subset of* G*. Then* H *is called a* subgroup *of* G *if* H *is itself a group under the operation of* G*.*

Every group has a *trivial subgroup* consisting only of the identity element, and every group is a subgroup of itself. A *proper subgroup* is one that is not equal to the whole group.
Not every group has non-trivial proper subgroups. For example, let $\chi = e^{2\pi i/5}$. Then $\chi^5 = 1 \in \mathbb{C}$, so χ is a complex 5th root of unity. The full set of complex fifth roots of unity is

$$\{1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}\} = \{1, \chi, \chi^2, \chi^3, \chi^4\}.$$

These five numbers form a group G_5 under multiplication of complex numbers (note that they occur at the vertices of a regular pentagon in the Argand plane). The full group table is below.

$G_5, \times$	1	χ	χ^2	χ^3	χ^4
1	1	χ	χ^2	χ^3	χ^4
χ	χ	χ^2	χ^3	χ^4	1
χ^2	χ^2	χ^3	χ^4	1	χ
χ^3	χ^3	χ^4	1	χ	χ^2
χ^4	χ^4	1	χ	χ^2	χ^3

Claim: G_5 has no non-trivial proper subgroup.
To see this, take the element χ. Suppose that H is a subgroup of G_5 that contains χ. What else must H contain? Can you show that H must include all of the elements of G_5? Repeat this for each of the other non-identity elements of G_5.

So it is not automatic that a group will have non-trivial proper subgroups. Nevertheless they often do, as in the following examples/exercises.

1. Let D_{2n} be the *dihedral group* consisting of the symmetries of a regular polygon with n sides. So D_{2n} consists of n rotational symmetries and n reflections. The set of rotational symmetries is a subgroup with n elements. To verify this means verifying that

   - The composition of two rotations is a rotation.
   - The inverse of a rotation is a rotation.

   Is the set of reflections in D_{2n} a subgroup? Why or why not?

2. Let S_5 be the group of permutations of the set $\{a, b, c, d, e\}$.
   How many elements are in S_5?
   Let H_1 be the subset of S_5 consisting of those elements that fix a (and permute b, c, d, e). Show that H_1 is a subgroup of S_5. How many elements are in H_1?
   Let H_2 be the subset of S_5 consisting of those elements that fix the set $\{a, b\}$ (this includes those elements that fix both a and b and those that swap a and b). Show that H_2 is a subgroup of S_5. How many elements are in H_2?
   Let H_3 denote the intersection of H_1 and H_2. How many elements does it have? Is it a subgroup of S_5?

3. Let $\mathbb{C}^\times$ denote the group of non-zero complex numbers, under multiplication. The following are some examples of subgroups of $\mathbb{C}^\times$.

   - The set $\mathbb{R}^\times$ of non-zero real numbers.
   - The set $S = \{a + bi \in \mathbb{C} : a^2 + b^2 = 1\}$; S is the set of complex numbers of modulus 1, geometrically it is the unit circle in the complex plane. To see why S is a subgroup of $\mathbb{C}^\times$, you need to confirm that S is closed under multiplication and that it contains the inverse of each of its elements.

   Is the set of *pure imaginary* numbers a subgroup of $\mathbb{C}^\times$? Recall that a complex number is pure imaginary if its real part is zero and its imaginary part is not (e.g. $2i$, $3i$ etc.).

Let G be a group. It is usual to denote the result of combining elements a and b of G by ab (like a product). In the same way we can denote the element of combining a with a by a^2 (same as aa), hence we have a^3 $(= aaa)$, a^4 $(= aaaa)$, etc. We can think of these elements as "positive integer powers" of a.
We also adopt the convention that for every element a of G, a^0 is understood to be the identity element.
Also, a^{-1} is the inverse of a, and we may understand a^{-2} as $a^{-1}a^{-1}$, and so on: $a^{-1}, a^{-2}, a^{-3}, \ldots$ are the positive integer powers of a^{-1}.
Thus for any element a of G we have the full set of "integer powers" of a within G; moreover, they behave as we would like integer powers to behave in the sense that

$$a^r a^s = a^{r+s} \text{ for all } r, s \in \mathbb{Z}.$$

Note: We are not assuming that all of the integer powers of a are necessarily distinct.
Notation: The set of integer powers of an element a of G is often denoted by $\langle a \rangle$:

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, \mathrm{id}, a, a^2, a^3, \ldots\} = \{a^n : n \in \mathbb{Z}\}.$$

Lemma 1.3.3. *For a group* G *and any element* a *of* G, $\langle a \rangle$ *is a subgroup of* G.

Proof. We need to show that

1. $\langle a \rangle$ is closed under the group operation.
   This is clear, the elements of $\langle a \rangle$ are exactly those that have the form a^r for some integer r, and $a^r a^s = a^{r+s}$.

2. $\mathrm{id} \in \langle a \rangle$.
   This is true by definition, since $\mathrm{id} = a^0$.

3. $\langle a \rangle$ contains the inverse of each of its elements.
   To see this, note that for an integer r the inverse of a^r is a^{-r}.

□

Definition 1.3.4. $\langle a \rangle$ *is called the* cyclic subgroup *of* G *generated by* $\langle a \rangle$.
In general, a subgroup of G *is said to be* cyclic *if it is equal to* $\langle a \rangle$ *for some* $a \in G$.

The proof of Lemma 1.3.3 above is very typical of proofs in group theory. The context is a completely abstract group about which we know nothing at all. The Lemma says that given any group, we can choose any element and the set of all powers of that element (and its inverse) in the group will give us a subgroup. We can now apply this lemma to examples, as in the following cases.

1. In $(\mathbb{Z}, +)$, the operation is addition, and the cyclic subgroup generated by 2 consists of all those elements that can be obtained by adding 2 (or its inverse -2) to itself repeatedly. This subgroup includes 2, $2+2=4$, $2+2+2=6$, etc. It also includes the identity element 0, the inverse -2 of 2, and the elements $(-2)+(-2)=-4$, $(-2)+(-2)+(-2)=-6$, etc.
   The cyclic subgroup of $\mathbb{Z}$ generated by 2 consists of all the even integers.
   Question: What is the cyclic subgroup of $\mathbb{Z}$ generated by 1? By 3?

2. In D_{2n}, let R denote the rotation through $\frac{2\pi}{n}$ about the centroid of the regular polygon. Then the cyclic subgroup generated by R is the group of rotational symmetries of the object. It has n elements.
   If S is one of the reflections in D_{2n} then S is its own inverse and the cyclic subgroup of D_{2n} generated by S consists only of S itself and of the identity element.

3. *Questions*:
   What are the elements of the cyclic subgroup of $\mathbb{C}^\times$ generated by -1?
   What are the elements of the cyclic subgroup of $\mathbb{C}^\times$ generated by i?
   Under what conditions on the complex number z is the subgroup $\langle z \rangle$ of $\mathbb{C}^\times$ a finite group?

Suppose that a is an element of a group G. Then any subgroup of G that contains a must also contain $a^2, a^3, \ldots$, and must also contain a^{-1} and hence $a^{-2}, a^{-3}, \ldots$ as well as the identity element. Hence any subgroup of G that contains the element a must contain $\langle a \rangle$, the cyclic subgroup generated by a. Sometimes it is helpful to think of $\langle a \rangle$ as the set of elements that *must* be in any subgroup that contains a.

Having discussed the concept of the cyclic subgroup of a group that is generated by a particular element, we now move on to the related idea of what it means for a group to be cyclic.

Definition 1.3.5. *A group* G *is said to be* cyclic *if* $G = \langle a \rangle$ *for some* $a \in G$.

Alternative version(s) of definition: A group G is cyclic if it contains an element a with the property that *every* element of G is a "power" of a. A cyclic group is one that is generated by a single element, in the sense that we can start with a single element and produce all the elements of G by (repeatedly) taking powers of that element and its inverse and by multiplying the results of such operations together.

In order to show that a group is cyclic, it is generally necessary to produce an example of a generator for it. It is generally not the case that any element (or any non-identity element) will do this job.

Examples

1. $(\mathbb{Z}, +)$ is an infinite cyclic group, with 1 as a generator.
   (This is saying that every integer is either equal to 0 (the identity in this group) or can be obtained by repeatedly adding 1 or -1 to itself).
   Question: There is one other element that is a generator for $(\mathbb{Z}, +)$ as a cyclic group. What is it?

2. For a natural number n, the group of nth roots of unity in $\mathbb{C}^\times$ is a cyclic group of order n, with (for example) $e^{\frac{2\pi i}{n}}$ as a generator. The elements of this group are the complex numbers of the form $e^{k\frac{2\pi i}{n}}$, where $k \in \mathbb{Z}$.
   Question to think about: What other elements generate this group? The answer to this question is slightly tricky and depends on n.

3. For $n \geqslant 3$, the group of rotational symmetries of a regular n-gon (i.e. a regular polygon with n sides) is a cyclic group of order n, generated (for example) by the rotation through $\frac{2\pi}{n}$ in a counterclockwise direction.

The term *order* appears in the examples above. Here's its definition.

Definition 1.3.6. *The* order *of a finite group is the number of elements in it. A group with infinitely many elements is said to have* infinite order.

It is common practice to denote a cyclic group of order n by C_n, and an infinite cyclic group by C_∞. We might write C_n as $\langle x \rangle$ and think of C_n as being generated by an element x. The elements of C_n would then be

$$\mathrm{id}, x, x^2, \ldots, x^{n-1}.$$

Here it is understood that $x^n = \mathrm{id}$, and that multiplication is defined by

$$x^i \cdot x^j = x^{[i+j]_n},$$

where $[i+j]_n$ denotes the remainder on dividing $i+j$ by n. In this context the multiplication table for $C_4 = \langle x \rangle$ is given below.

C_4	id	x	x^2	x^3
id	id	x	x^2	x^3
x	x	x^2	x^3	id
x^2	x^2	x^3	id	x
x^3	x^3	id	x	x^2

Note: The philosophy here is that all cyclic groups of order n (or 4) really look the same, so we might as well have one notation C_n for them. Once we give a name to a generator, like x, we can write out the multiplication table as for C_4 above. In this context, we don't care what sort of object x is, whether it is a number, a matrix, a function, a permutation or whatever. The group of nth roots of unity in $\mathbb{C}$ and the group of rotational symmetries of the regular n-gon might be regarded as particular manifestations of C_n in algebra and geometry. Later we will have the language to make all of this precise.

We might ask how many elements of C_n are actually generators of it as a cyclic group and how this number depends on n. The answer is not immediately obvious. Of course (provided $n > 1$) the identity element is never a generator of C_n and so the answer is at most $n - 1$. In the case of C_4, we can use the table above to look at the set of powers of each element and see if they include the whole group. We find

- Powers of x: x, x^2, x^3, id - the whole group.
- Powers of x^2: x^2 and id only - not the whole group.
- Powers of x^3: x^3, x^2, x, id - the whole group.

So two of the four elements of C_4 generate it as a cyclic group. What about C_5? What about C_6?

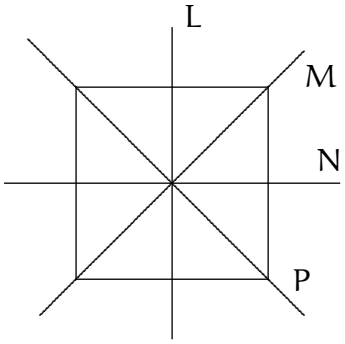
Theorem 1.3.7. *Suppose that* x *is a generator of* C_n*. Then the elements of* C_n *that generate it as a cyclic group are exactly those elements of the form* x^i *where* $\gcd(i, n) = 1$*. The number of these is* $\phi(n)$*.*

We won't prove Theorem 1.3.7 in these notes, but in order to investigate it, have a look at some examples, like the group of 6th, 7th or 8th roots of unity in $\mathbb{C}^\times$. See if you can convince yourself that this theorem is true and why.
Recall: For a natural number n, $\phi(n)$ is the number of integers in the range $1, \ldots, n$ that are relatively prime to n.

We finish this section by remarking that the cyclic subgroup generated by a particular element is a special case of a more general phenomenon. Suppose that G is a group and that S is a subset (not necessarily a subgroup) of G. Then we can define *the subgroup of* G *generated by* S. This is denoted by $\langle S \rangle$ and it consists of all the elements of G that can be obtained by starting with the identity and the elements of S and their inverses, and multiplying these elements together in all possible ways. So $\langle S \rangle$ is the smallest subgroup of G that contains S.

Definition 1.3.8. *If* $\langle S \rangle$ *is all of* G*, we say that* S *is a* generating set *of* G*.*

Problems As usual let D_8 denote the group of symmetries of the square (below).



Let T_L, T_M, T_N, T_P denote the reflections in the indicated lines, and let R_t denote the anticlockwise rotation through $t°$.

1. Show that the subgroup of D_8 generated by R_{180} and T_L is not all of D_8. (For example it does not contain R_{90}).

2. Show that D_8 can be generated by R_{90} and by any one of the reflections.

3. Show that $\{T_L, T_M\}$ is a generating set for D_8.

4. More generally, show that the group D_{2n} of symmetries of the regular n-gon can be generated by the counterclockwise rotation through $\frac{2\pi}{n}$ and any one reflection.
   This last one might be tricky - remember that by having the rotation through $\frac{2\pi}{n}$ in your generating set, you get all the rotations for free. What needs to be shown is that you can get all the reflections by composing the one reflection that is in your symmetry group with rotations. If in doubt, start with the equilateral triangle, the square and the regular pentagon.