6. Subgroups

Consider the chain of inclusions of groups

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

where the law of multiplication is ordinary addition.

Then each subset is a group, and the group laws are obviously compatible. That is to say that if you want to add two integers together, it does not matter whether you consider them as integers, rational numbers, real numbers or complex numbers, the sum always comes out the same.

Definition 6.1. *Let G be a group and let H be a subset of G. We say that H is a **subgroup** of G, if the restriction to H of the rule of multiplication and inverse makes H into a group.*

Notice that this definition hides a subtlety. More often than not, the restriction to $H \times H$ of m the rule of multiplication of G, won't even define a rule of multiplication on H itself, because there is no a priori reason for the product of two elements of H to be an element of H.

For example suppose that G is the set of integers under addition, and H is the set of odd numbers. Then if you take two elements of H and add them, then you **never** get an element of H, since you will always get an even number.

Similarly, the inverse of H need not be an element of H. For example take H to be the set of natural numbers. Then H is closed under addition (the sum of two positive numbers is positive) but the inverse of every element of H does not lie in H.

Definition 6.2. *Let G be a group and let S be subset of G.*

*We say that S is **closed** under multiplication, if whenever a and b are in S, then the product of a and b is in S.*

*We say that S is **closed** under taking inverses, if whenever a is in S, then the inverse of a is in S.*

For example, the set of even integers is closed under addition and taking inverses. The set of odd integers is not closed under addition (in a big way as it were) and it is closed under inverses. The natural numbers are closed under addition, but not under inverses.

Proposition 6.3. *Let H be a non-empty subset of G.*

Then H is a subgroup of G if and only if H is closed under multiplication and taking inverses. Furthermore, the identity element of H is the identity element of G and the inverse of an element of H is equal to the inverse element in G.

If G is abelian, then so is H.

Proof. If H is a subgroup of G, then H is closed under multiplication and taking inverses by definition.

So suppose that H is closed under multiplication and taking inverses. Then there is a well defined product on H. We check the axioms of a group for this product.

Associativity holds for free. Indeed to say that the multiplication on H is associative, is to say that for all g, h and $k \in H$, we have

$$(gh)k = g(hk).$$

But g, h and k are elements of G and the associative rule holds in G. Hence equality holds above and multiplication is associative in H.

We have to show that H contains an identity element. As H is non-empty we may pick $a \in H$. As H is closed under taking inverses, $a^{-1} \in H$. But then

$$e = aa^{-1} \in H$$

as H is closed under multiplication. So $e \in H$. Clearly e acts as an identity element in H as it is an identity element in G. Suppose that $h \in H$. Then $h^{-1} \in H$, as H is closed under taking inverses. But h^{-1} is clearly the inverse of h in H as it is the inverse in G.

Finally if G is abelian then H is abelian. Just follow a similar argument to the proof of associativity. □

Example 6.4. *(1) The set of even integers is a subgroup of the set of integers under addition. By* (6.3) *it suffices to show that the even integers are closed under addition and taking inverses, which is clear.*

(2) The set of natural numbers is not a subgroup of the group of integers under addition. The natural numbers are not closed under taking inverses.

(3) The set of rotations of a regular n-gon is a subgroup of the group D_n of symmetries of a regular n-gon. By (6.3) *it suffices to check that the set of rotations is closed under multiplication and inverse. Both of these are obvious. For example, suppose that R_1 and R_2 are two rotations, one through θ radians and the other through ϕ. Then the product is a rotation through $\theta + \phi$. On the other hand the inverse of R_1 is rotation through $2\pi - \theta$.*

(4) The group D_n of symmetries of a regular n-gon is a subgroup of the set of invertible two by two matrices, with entries in $\mathbb{R}$. Indeed any symmetry can be interpreted as a matrix. Since we have already seen that the set of symmetries is a group, it is in fact a subgroup.

(5) *The following subsets are subgroups:*

$$M_{m,n}(\mathbb{Z}) \subset M_{m,n}(\mathbb{Q}) \subset M_{m,n}(\mathbb{R}) \subset M_{m,n}(\mathbb{C}),$$

under addition.

(6) *The following subsets are subgroups:*

$$\mathrm{GL}_n(\mathbb{Q}) \subset \mathrm{GL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{C}),$$

under multiplication.

(7) *It is interesting to enumerate the subgroups of D_3. At one extreme we have D_3 and at the other extreme we have $\{I\}$. Clearly the set of rotations is a subgroup, $\{I, R, R^2\}$. On the other hand $\{I, F_i\}$ forms a subgroup as well, since $F_i^2 = I$. Are these the only subgroups?*

Suppose that H is a subgroup that contains R. Then H must contain R^2 and I, since H must contain all powers of R. Similarly if H contains R^2, it must contain $R^4 = (R^2)^2$. But $R^4 = R^3R = R$.

Suppose that in addition H contains a flip. By symmetry, we may suppose that this flip is $F = F_1$. But $RF_1 = F_3$ and $FR = F_2$. So then H would be equal to G.

The final possibility is that H contains two flips, say F_1 and F_2. Now $F_1R = F_2$, so

$$R = F_1^{-1}F_2 = F_1F_2.$$

So if H contains F_1 and F_2 then it is forced to contain R. In this case $H = G$ as before.

Here are some examples, which are less non-trivial.

Definition-Lemma 6.5. *Let G be a group and let $g \in G$ be an element of G.*

*The **centraliser** of $g \in G$ is defined to be*

$$C_g = \{\, h \in G \,|\, hg = gh \,\}$$

Then C_g is a subgroup of G.

Proof. $e \in C_g$ so that the centraliser is non-empty.

By (6.3) it therefore suffices to prove that C_g is closed under multiplication and taking inverses.

Suppose that h and k are two elements of C_g. We show that the product hk is an element of C_g. We have to prove that $(hk)g = g(hk)$.

$$\begin{aligned}
(hk)g &= h(kg) && \text{by associativity} \\
&= h(gk) && \text{as } k \in C_g \\
&= (hg)k && \text{by associativity} \\
&= (gh)k && \text{as } h \in C_g \\
&= g(hk) && \text{by associativity.}
\end{aligned}$$

Thus $hk \in C_g$ and C_g is closed under multiplication.

Now suppose that $h \in G$. We show that the inverse of h is in G. We have to show that $h^{-1}g = gh^{-1}$. Suppose we start with the equality

$$hg = gh.$$

Multiply both sides by h^{-1} on the left. We get

$$h^{-1}(hg) = h^{-1}(gh),$$

so that simplifying we get

$$g = (h^{-1}g)h.$$

Now multiply both sides of this equality by h^{-1} on the right,

$$gh^{-1} = (h^{-1}g)(hh^{-1}).$$

Simplifying we get

$$h^{-1}g = gh^{-1}$$

which is what we want. Thus $h^{-1} \in C_g$. Thus C_g is closed under taking inverses and C_g is a subgroup by (6.3). □

Lemma 6.6. *Let G be a group and let H be a non-empty finite set, closed under multiplication.*

Then H is a subgroup of G.

Proof. It suffices to prove that H is closed under taking inverses.

Let $a \in H$. If $a = e$ then $a^{-1} = e$ and this is obviously in H.

So we may assume that $a \neq e$.

Consider the powers of a,

$$a, a^2, a^3, \ldots.$$

As H is closed under products, it is obviously closed under powers (by an easy induction argument). As H is finite and this is an infinite sequence, we must get some repetitions, and so for some m and n distinct positive integers

$$a^m = a^n.$$

Possibly switching m and n, we may assume $m < n$. Cancelling the above equation, we get

$$a^{n-m} = e.$$

(Note that we can cancel since G is a group but both sides of this equation are in fact in H; compare this with the fact one can cancel in the natural numbers, since they sit inside the integers.)

As $a \neq e$, $n - m \neq 1$. Set $k = n - m - 1$. Then $k > 0$. If we put $b = a^k \in H$ then

$$ba = a^k a = a^{n-m-1}a = a^{n-m} = e.$$

Similarly

$$ab = e.$$

Thus b is the inverse of a. Thus H is closed under taking inverses and so H is a subgroup of G by (6.3). $\square$