2.2 Subgroups

Definition 2.2.1. Let G be a group with operation $*$. We say that H is a *subgroup* of G if $H \subseteq G$ and H is itself a group with the operation on H being also $*$. The notation we use is $H \leq G$. Sometimes we say that G is a *supergroup* of H.

Example 2.2.2. Here are some examples of subgroups.

(i) Let G be any group. Then $G \leq G$ and $\langle e_G \rangle \leq G$.

(ii) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$

(iii) For $k \in \mathbb{N}$ we typically denote the group $(k\mathbb{Z}, +)$ simply by $k\mathbb{Z}$. It is the group consisting of all multiples of k under addition. It is a subgroup of $(\mathbb{Z}, +)$.

Non-Example 2.2.3. Here are some examples of things that are not subgroups.

(i) $(\mathbb{Q}^*, \times) \nleq (\mathbb{R}, +)$
(because the operations do not match)

(ii) $(\mathbb{N}, +) \nleq (\mathbb{Z}, +)$
(because $(\mathbb{N}, +)$ is not a group)

(iii) $\mathrm{GL}(2, \mathbb{R}) \nleq (\mathbb{R}^*, \times)$
(because the set of invertible 2×2 matrices is not a subset of the real numbers)

Theorem 2.2.4. *Let H be a subgroup of G.*

(i) $e_H = e_G$

(ii) For all $h \in H$, the inverse of h in H is equal to the inverse of h in G

Proof. These statements were proved in Algebraic Structures. □

Theorem 2.2.5. (Quick Subgroup Test.) *Let G be a group with operation $*$, and suppose H is a subset of G. Then $(H, *)$ is a subgroup of G if and only if:*

(i) H contains the identity *(i.e. $e_G \in H$)*

(ii) H is closed under $*$ *(i.e. for all $h_1, h_2 \in H$ we have $h_1 * h_2 \in H$)*

(iii) Every element of H has an inverse in H *(i.e. for all $h \in H$ we have $h^{-1} \in H$)*

Proof. Proved in Algebraic Structures (although first point may have been $H \neq \varnothing$). □

Proposition 2.2.6. *Let G be a group and $H \leq G$. Then:*

(i) $|H| = 1$ *if and only if* $H = \langle e_G \rangle$

(ii) If $|G|$ is finite, then $|H| = |G| \iff H = G$.

Proof. You will prove this as an exercise in one of your problem sheets. □

Example 2.2.7. Let G be any group.

(i) $\{e_G\}$ is a subgroup of G.

(ii) G is a subgroup of G.

Definition 2.2.8. The subgroup $\{e_G\}$ of G is often written $\langle e_G \rangle$. It is called *the trivial group*.
If a subgroup H of G is not equal to G then we call it a *proper subgroup* and write $H < G$. If $\{e\} < H < G$ then we say that H is a proper nontrivial subgroup of G.

Example 2.2.9. Let n be a natural number. Recall the *additive group of integers modulo n*, written $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, where $[m]_n$ is the equivalence class of all integers that have remainder m when divided by n. Recall this is a group under the operation $[k]_n \oplus [m]_n = [k+m]_n$. See handout for more details. Note that $\mathbb{Z}_n \nleq (\mathbb{Z}, +)$ because it is not a subset (and the operation $\oplus$ is different to $+$).

2.2.1 Handout for Section 2.2

Definition 2.2.10. Let n be a positive integer, and recall that we can think of integers "modulo n": two integers are equivalent modulo n if they have the same remainder when divided by n.
Being equivalent modulo n is an equivalence relation, so it is a relation that is reflexive, symmetric and transitive.
There are n congruence classes modulo n, which we denote by $[k]_n$ for $k \in \mathbb{Z}$ (sometimes we just write $[k]$). For example, when $n = 5$,

$$[1]_5 = [6]_5 = [-34]_5 = \{\dots, -9, -4, 1, 6, 11, \dots\} \quad \text{and}$$
$$[2]_5 = [7]_5 = [-33]_5 = \{\dots, -8, -3, 2, 7, 12, \dots\},$$

The set of all congruency classes modulo n is $\mathbb{Z}_n = \{[0]_n, [1]_5, \dots, [n-1]_5\}$. Each integer lies in precisely one of these classes.
There is a natural operation on $\mathbb{Z}_n$ under which it forms a group: for $[a]_n, [b]_n \in \mathbb{Z}_n$, define

$$[a]_n \oplus [b]_n = [a+b]_n.$$

For example, when $n = 5$:

$$[2]_5 \oplus [1]_5 = [2+1]_5 = [3]_5 \quad \text{and}$$
$$[3]_5 \oplus [2]_5 = [3+2]_5 = [5]_5 = [0]_5.$$

The group $\mathbb{Z}_n$ is called *the additive group of integers modulo n.*

2.3 Cyclic groups

Definition 2.3.1. If G be a group with operation $*$, and $g \in G$ and $n \in \mathbb{N}$. Recall:

$$g^n = g * g * \cdots * g \ (n \text{ times}).$$

Also $g^0 = e_G$ and $g^{-n} = (g^n)^{-1}$. You should also check that $g^n g^m = g^{n+m}$ holds for $n, m \in \mathbb{Z}$.

Now we define

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

to be the set of all integer powers of g. It is a group under the operation $*$ (exercise—check this!).

Hence $\langle g \rangle \leq G$. It is called the *cyclic group generated by* g.

We say G is *cyclic* if there exists some $g \in G$ for which $G = \langle g \rangle$. In this case we say that the element g *generates* G.

Warning! Be careful with the notation g^n means $g * g * \cdots * g$ (n times) and sometimes $*$ will mean e.g. addition.

Later in the course we will use the notation $\langle \cdots \rangle$ again in a more powerful way.

Proposition 2.3.2. *If G is a group and $g \in G$, then $|\langle g \rangle| = o(g)$.*

Proof. You will prove this for finite groups as one of your exercises. The proof for infinite groups easy: it is obvious that $o(g)$ is finite if and only if $\langle g \rangle$ is finite. □

Example 2.3.3. Here are some examples of cyclic subgroups of some groups you know.

(i) In the group $(\mathbb{Z}, +)$ the subgroup $\langle 2 \rangle$ is equal to $2\mathbb{Z}$ (i.e. the group of even integers under addition).

(ii) In the group S_5, the subgroup $\langle (1\,2)(3\,4\,5) \rangle$ has 6 elements. Let $a = (1\,2)(3\,4\,5)$, then $a^6 = e$ and so,

$$\langle a \rangle = \{e, a, a^2, a^3, a^4, a^5\} = \{e, (1\,2)(3\,4\,5), (3\,5\,4), (1\,2), (3\,4\,5), (1\,2)(3\,5\,4)\}.$$

(iii) In the group $\mathrm{GL}(2, \mathbb{R})$, the cyclic subgroup $\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ contains only two elements. What are they?

Example 2.3.4. Here is an example of a cyclic group.

$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$, so $(\mathbb{Z}, +)$ is cyclic and is generated by 1.

Proof: Fix $n \in \mathbb{N}$. We will show that $n, -n, 0 \in \langle 1 \rangle$, from which it follows immediately that $(\mathbb{Z}, +) = \langle 1 \rangle$. Now that $n = 1 + 1 + \cdots + 1 = 1 * 1 * \cdots * 1 = 1^n$. Hence $n \in \langle 1 \rangle$. Furthermore $n + (-n) = 0 = e$, so $-n = n^{-1} = (1^n)^{-1}$. By Theorem 2.1.11 (vi) we know $(1^n)^{-1} = 1^{-n} \in \langle 1 \rangle$. Hence $-n \in \langle 1 \rangle$. Finally, we note that $0 = 1^0 \in \langle 1 \rangle$.

Non-Example 2.3.5. Here is an example of a group that is not cyclic.

$(\mathbb{Q}^*, \times)$ is not cyclic.

Proof: Suppose it is cyclic. Then there exist nonzero $a, b \in \mathbb{Q}$ such that every nonzero rational number can be written as $(a/b)^n = a^n/b^n$ for some $n \in \mathbb{Z}$. This is clearly false—for example if $p, q > \max(a, b)$ are primes then $p/q \in \mathbb{Q}^*$ can't be written in the form a^n/b^n.

Definition 2.3.6. This is an important example of a cyclic group. For $n \in \mathbb{N}$, the cyclic group generated by the n-cycle $(1\ 2\ \ldots\ n)$ is called *the cyclic group of order* n and is denoted by C_n. In other words:

$$C_n = \langle (1\ 2\ \ldots\ n) \rangle.$$

Since the n-cycle is an element of S_n, we have that $C_n \leq S_n$.