12. Subgroups

Definition. Let $(G, *)$ be a group. A subset H of G is called a subgroup if it satisfies the following conditions:

(i) $e \in H$

(ii) H is closed under $*$: if $x, y \in H$, then $x * y \in H$

(iii) H is closed under inversion: if $x \in H$, then $x^{-1} \in H$

The following result explains the conceptual importance of this definition:

Claim 12.1. *Let $(G, *)$ be a group and H a subset of G. Then H is a subgroup of $G \iff H$ itself is a group with respect to the operation $*$.*

Idea of proof. Conditions (i), (ii) and (iii) are equivalent to saying that the pair $(H, *)$ satisfies axioms (G2), (G0) and (G3), respectively. Note that the remaining axiom (G1) (associativity) holds automatically. Indeed, since G is a group, we have $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$, and the same surely remains true under additional restriction $x, y, z \in H$. □

We now give a few examples of subgroups.

Example 1. *Let $G = (\mathbb{Z}, +)$ and $H = 2\mathbb{Z}$ (even integers).*

Let us check that H is a subgroup. We have

(i) The identity element of G is 0 and $0 = 2 \cdot 0 \in H$.

(ii) If $x, y \in H$, then $x = 2u$ and $y = 2v$ for some $u, v \in \mathbb{Z}$, so $x + y = 2(u + v) \in H$ as well. Thus H is closed under group operation.

(iii) Recall that the group inversion in this case is additive inversion. Let $x \in H$. Then $x = 2u$ for some $u \in \mathbb{Z}$, so $-x = -(2u) = 2(-u) \in H$. Thus H is closed under inversion.

In exactly the same way one can check that $n\mathbb{Z}$ (where n is any fixed integer) is a subgroup of G. It turns out that G does not have any other subgroups (this will be one of homework problems).

Example 2. *Let $G = (\mathbb{Z}_{10}, +)$. Describe all subgroups of G.*

In this example we just give an answer, so far without proof (formal justification will be given in Lecture 14). It is easy to check that G has (at least) four subgroups: G itself, $\{[0], [5]\}$, $\{[0], [2], [4], [6], [8]\}$ and $\{[0]\}$. It takes a bit more work to show that there are no other subgroups in G.

Note that the set of "multiples of 3" in $\mathbb{Z}_{10}$, namely the set $S = \{[3], [6], [9]\}$ is NOT a subgroup since $[9] + [3] = [2] \notin S$.

Example 3. *Let* $G = GL_2(\mathbb{R}) = \{A \in Mat_2(\mathbb{R}) : \det(A) \neq 0\}$. *Recall from Lecture 10 that* G *is a group with respect to the usual matrix multiplication. Let* $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) : c = 0 \right\}$, *that is,* H *is the set of all matrices in* $GL_2(\mathbb{R})$ *whose* $(2,1)$*-entry is* 0. *We claim that* H *is a subgroup.*

Proof: (i) The identity element of G is the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Its $(2,1)$-entry is 0, so $I \in H$.

(ii) Take any $g, h \in G$. Thus, $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ and $h = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ for some $a, b, d, x, y, z \in \mathbb{R}$. Then $gh = \begin{pmatrix} ax & ay + bz \\ 0 & dz \end{pmatrix}$ also has zero $(2,1)$-entry, so $gh \in H$.

(iii) Finally to prove that H is closed under inversion we use the formula for inverse in $GL_2(F)$ from HW#5.6. According to that formula, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} \frac{d}{D} & -\frac{b}{D} \\ -\frac{c}{D} & \frac{a}{D} \end{pmatrix} \text{ where } D = ad - bc.$$

In particular, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, then $c = 0$, whence $-\frac{c}{D} = 0$ and therefore $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in H$.

12.1. **Cyclic subgroups.** We now discuss some general constructions of subgroups. Consider the following question:

Question. *Let* $(G, *)$ *be a group and* a *an element of* G. *What is the smallest subgroup of* G *containing* a*?*

To answer this question assume that H is any subgroup of G which contains a and let us try to determine which other elements besides a must be contained in H.

First of all we must have $e \in G$. Since H is closed under $*$ and $a \in H$, we must have $a^2 = a * a \in H$, $a^3 = (a^2) * a \in H$ etc. (to be precise we define a^2 as the element $a * a$, a^3 as the element $(a^2) * a$ etc.) We also know that H must contain a^{-1}, hence it must also contain elements $a^{-2} = a^{-1} * a^{-1}$, $a^{-3} = (a^{-2}) * a^{-1}$ etc. Thus, H must contain a^k for every $k \in \mathbb{Z}$ (where we set $a^0 = e$).

On the other hand, it is not hard to show (see § 3.2) that the set $\{a^k : k \in \mathbb{Z}\}$ is a subgroup of G. We let $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ and call $\langle a \rangle$ the cyclic subgroup generated by a. According to the above discussion, $\langle a \rangle$ is the smallest subgroup of G which contains a.

Note that verification of the fact that $\langle a \rangle$ is a subgroup boils down to the following identities which are known as *exponent laws* and important in their own right.

Theorem (Exponent laws)**.** *Let G be a group and $a \in G$. Then for any $i, j \in \mathbb{Z}$ we have $a^i \cdot a^j = a^{i+j}$ and $(a^i)^{-1} = a^{-i}$.*

Proof. See § 3.2. □

We now look at some specific examples of cyclic subgroups.

Example 4. *Let $G = (\mathbb{R} \setminus \{0\}, \cdot)$, nonzero real numbers with multiplication. Compute $\langle 2 \rangle$, the cyclic subgroup generated by 2.*

By definition $\langle 2 \rangle = \{2^k : k \in \mathbb{Z}\} = \{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\}$.

Example 5. *Let $G = (\mathbb{Z}, +)$, integers with addition.*

In this example we do not want to use notation a^k to avoid confusion with usual multiplication in $\mathbb{Z}$. Indeed, a^k in our general notation means that we start with a and apply the group operation k times, but the operation in this example is addition, so a^k should be replaced by $ka = \underbrace{a + \ldots + a}_{k \text{ times}}$.

Thus, for every $a \in \mathbb{Z}$ we have $\langle a \rangle = \{ka : k \in \mathbb{Z}\}$, the set of all multiples of a.

Example 6. *Let $G = (\mathbb{Z}_{10}, +)$ and $a = [3]$.*

As in the previous example, we can say that $\langle [3] \rangle = \{k[3] : k \in \mathbb{Z}\}$. This is a correct answer, but it is not given in the most explicit form. Indeed, as we saw in an earlier example, $\mathbb{Z}_{10}$ has only four subgroups, so $\langle [3] \rangle$ must equal one of these subgroups. To determine which one we compute elements of $\langle [3] \rangle$ explicitly one at a time. Since by definition $(k+1)[3] = k[3] + [3]$ for all k, we have $0[3] = [0]$, $1[3] = [3]$, $2[3] = [3] + [3] = [6]$, $3[3] = [6] + [3] = [9]$, $4[3] = [9] + [3] = [12] = [2]$, $5[3] = [2] + [3] = [5]$, $6[3] = [5] + [3] = [8]$, $7[3] = [8] + [3] = [11] = [1]$, $8[3] = [1] + [3] = [4]$, $9[3] = [4] + [3] = [7]$. We can stop at this point since the above computation already shows that $\langle [3] \rangle$ contains all elements of $G = \mathbb{Z}_{10}$ (and $\langle [3] \rangle$ cannot be larger than $\mathbb{Z}_{10}$). Thus we conclude that $\langle [3] \rangle = \mathbb{Z}_{10}$.

We will show in Lecture 14 that given an element $[a] \in \mathbb{Z}_n$ we have $\langle [a] \rangle = \mathbb{Z}_n \iff a$ and n are coprime.

12.2. **Defining subgroups by constraints.** Another general method of constructing subgroups is to take the set of all elements of a given group satisfying certain constraint (typically some equation). The subgroup H in Example 3 is a special case of this construction. Of course, in general there is no guarantee that the given constraint will give us a subgroup.

In the example below we use multiplicative notation.

Example 7. *Let G be a group and fix $a \in G$. Define*

$$C(a) = \{x \in G : xa = ax\},$$

the set of all elements of G which commute with a. The set $C(a)$ is called the centralizer of a. We claim that $C(a)$ is a subgroup of G.

Proof: (i) By axiom (G2) we have $ea = ae = a$, so $e \in C(a)$.

(ii) Take any $g, h \in C(a)$. This means that $ga = ag$ and $ha = ah$. We need to use these equalities to show that $gh \in C(a)$, that is, $(gh)a = a(gh)$. The computation below proves this:

$$(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$$

where the first, third and fifth equalities hold by associativity, the second one uses $ah = ha$ and the fourth one uses $ga = ag$.

Note: As mentioned in the last lecture, we do not really need to write parentheses when doing computations in groups (thanks to associativity), but here we do this anyway to clearly illustrate the steps.

Thus, we showed that $C(a)$ is closed under group operation.

(iii) The last part ($C(a)$ is closed under inversion) is left as a homework exercise.