# 6 Subgroups (10/02)

**Definition 6.1** (Subgroups)**.** Let $G$ be a group and let $X$ be a subset of $G$ we say that $X$ is a **subgroup** if the following conditions hold:

(i) $X$ is nonempty,

(ii) if $a \in X$, then $a^{-1} \in X$, and

(iii) if $a, b \in X$, then $ab \in X$.

These conditions imply

(iv) $e \in X$,

**Example 6.2.** The group $\mathbf{Z}$ is a subgroup of $\mathbf{R}$, while $\mathbf{N}$ is not a subgroup of $\mathbf{Z}$ because (ii) fails.

**Example 6.3.** If $V$ is a vector space and $W \subseteq V$ is a subspace, then $W$ is a subgroup of $V$.

**Example 6.4.** The set of positive real numbers $\mathbf{R}_+^\times$ is a subgroup of the group $\mathbf{R}^\times$ of non-zero real numbers under multiplication.

**Remark 6.5.** If $G$ is a group and $X \subseteq G$ is a subgroup, then $X$ is a group. Here, we use condition (iii) to view the restriction of the binary operation from $G$ to $X$ as a binary operation on $X$. Specifically, write $a \cdot_G b$ for the binary operation in $G$ and if $a, b \in X$, define $X \times X \to X$ by $a \cdot_X b = a \cdot_G b$, viewed as an element of $X$. Then, $X$ together with this binary operation is a group.

**Lemma 6.6.** *If $f\colon G \to H$ is a group homomorphism, then the image of $f$, written $\mathrm{im}(f)$ or $f(G)$, is a subgroup of $H$ and $f$ induces a group homomorphism $G \to f(G)$.*

*Proof.* Since $G$ has an identity element $e$, there is an element $f(e) \in f(G)$, so $f(G)$ is nonempty. Similarly, if $x, y \in f(G)$, we can write $x = f(g)$ and $y = f(h)$ for some $g, h \in G$ and hence $xy = f(g)f(h) = f(gh)$, so $xy \in f(G)$ as well. Finally, $x^{-1} = f(g^{-1})$. That the induced function $G \to f(G)$ is a group homomorphism follows from the fact that $f\colon G \to H$ is. □

**Lemma 6.7.** *If $f\colon G \to H$ is an injective group homomorphism, then the induced function $G \to f(G)$ is a group isomorphism.*

*Proof.* It is surjective by definition and injective by hypothesis. □

**Example 6.8** (Subgroup lattice of $S_3$)**.** Figure 1 shows the subgroups of $S_3$ arranged into what is called a subgroup lattice. The lines represent containment. The group on the middle left is isomorphic to $\mathbf{Z}/3$ while the three groups on the middle right are isomorphic to $\mathbf{Z}/2$. These are all of the subgroups because one checks that if a subgroup of $S_3$ has an element of order 2 and an element of order 3, then it is all of $S_3$. Note that two distinct elements of order 2 multiply to an element of order 3.

**Example 6.9** (Subgroup lattice of $\mathbf{Z}/6$)**.** Figure 2 shows the subgroup lattice of $\mathbf{Z}/6$. The middle left subgroup is isomorphic to $\mathbf{Z}/3$ and the middle right to $\mathbf{Z}/2$.

**Theorem 6.10** (Cayley's theorem)**.** *If $G$ is a group, then there is an injective group homomorphism $\ell\colon G \to S_G$, where $S_G$ denotes the group of bijections from the set of elements of $G$ to itself.*

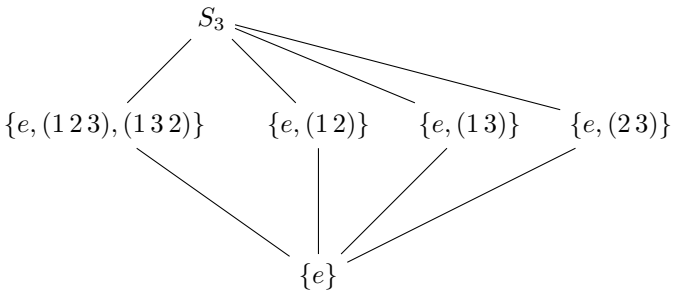


Figure 1: Subgroups of $S_3$.

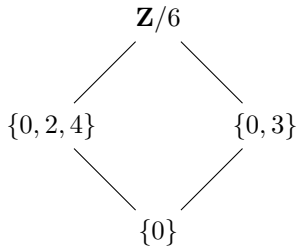


Figure 2: Subgroups of $\mathbf{Z}/6$.

*Proof.* Given $g \in G$, let $\ell_g \colon G \to G$ be defined by $\ell_g(h) = gh$. This is a bijection by the Latin square property, which holds for all groups. Alternatively, $\ell_g(g^{-1}h) = g(g^{-1}h) = h$, and this is a unique solution to $\ell_g(x) = h$. Thus, the assignment $g \mapsto \ell_g$ gives a function $\ell \colon G \to S_G$ where $\ell(g) = f_g$. The claim is that this is an injective group homomorphism. If $\ell_g = \ell_{g'}$ for $g, g' \in G$, then $g = \ell_g(e) = \ell_{g'}(e) = g'$, which proves injectivity. Now, $(\ell_g \circ \ell_{g'})(h) = \ell_g(\ell_{g'}(h)) = \ell_g(g'h) = g(g'h) = (gg')h = \ell_{gg'}(h)$, so $\ell_g \circ \ell_{g'} = \ell_{gg'}$ and the function $\ell$ is a group homomorphism. □

**Remark 6.11.** Cayley's theorem implies every group is a subgroup of a permutation group. However, this can be rather inefficient. For example, the injective group homomorphism $\ell \colon \mathbf{Z}/N \to S_{\mathbf{Z}/N} \cong S_N$ embeds the group $\mathbf{Z}/N$ of order $N$ into a group of order $N!$. What does this embedding look like? It sends $1 \in \mathbf{Z}/N$ to a cycle $c = (0\,1 \cdots N-1)$ (where we use $\{0, \ldots, N-1\}$ instead of $\{1, \ldots, N\}$ since these are the elements of $\mathbf{Z}/N$) and $a \in \mathbf{Z}/N$ to $c^a$.

**Example 6.12.** What about $S_3$? This is a group with 6 elements, so the homomorphism from Cayley's theorem is a group homomorphism $\ell \colon S_3 \to S_6$. Let's label the elements of $S_3$ as:

$$\begin{pmatrix} e & (1\,2) & (1\,3) & (2\,3) & (1\,2\,3) & (1\,3\,2) \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Then, $e$ of $S_3$ gets mapped to the identity element $e$ of $S_6$. A cycle decomposition for $\ell(1\,2)$ is $(1\,2)(3\,6)(4\,5)$.

**Remark 6.13** (Orders and group homomorphisms)**.** If $f \colon G \to H$ is a group homomorphism and $a \in G$ has order $n$, then $f(a)$ has order dividing $n$. Indeed, $f(a)^n = f(a^n) = f(e) = e$. Thus, in the example above $\ell(1\,2)$ has order dividing 2. But, it's clearly not of order 1, so its order must be exactly 2, which means the only cycles appearing in its cycle decomposition are of length 1 or 2.

## 6.1 Exercises

**Exercise 6.1.** Show that if $G$ is a group and $a \in G$ is an element satisfying $a^n = e$ for some integer $n \geqslant 1$, then the order of $a$ divides $n$.

**Exercise 6.2.** Draw the lattice of subgroups for the group $K = \mathbf{Z}/2 \times \mathbf{Z}/2$. (Sample LaTeX code is in Discord.)

**Exercise 6.3.** Draw the lattice of subgroups for the group $\mathbf{Z}/12$.

**Exercise 6.4.** Using Example 6.12, find a cycle decomposition for $\ell(1\,2\,3)$.