Subgroups

Definition. Let G be a group and H a nonempty subset of G. H is a subgroup if it is closed under taking products and inverses. (The other properties are inherited from G.) In this case, we write $H \leq G$. p.46

Again, this is also something that might seem familiar to you from the topic of vector spaces and subspaces. We can summarize these two closure properties in one, although I personally most often find it easier to check them separately.

Proposition. *A subset H of a group G is a subgroup if and only if* Prop. 1 p.47

(1) $H \neq \emptyset$,

(2) for all $x, y \in H$, we have $xy^{-1} \in H$.

If H is finite, then it suffices to check that H is nonempty and closed under taking products.

Example. Consider the action of a group G on itself, via $g \cdot h = gh$. Then, it is easy to see that this action is faithful. Therefore, we have found an injective homomorphism $\phi : G \to S_G$, or to S_n if $|G| = n$ finite. The image of this homomorphism is a subgroup of S_n. (Show that this is true as an exercise.) And this subrgoup of S_n is isomorphic to G. Since we can do this in general, we see that the symmetric groups S_n contain the structure of all other groups as subgroups.

Now, we will examine a set of subgroups of G that will be very useful later on. In particular, we are going to use normalizers to define so-called normal subgroups. These subgroups are special because we can quotient out by them, which is very similar to division in the natural numbers. It will help us classify groups as products and quotients of one another.

Definition. Let G be a group and A a nonempty subset. The *centralizer* of A in G is defined as p.49

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

We can also describe this as the set of elements that commute with everything in A.

Proposition. *We have $C_G(A) \leq G$.* p.49

Definition. Let G be a group. The *center* of G is defined as p.50

$$Z(G) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in G\} = C_G(G).$$

We can also describe this as the set of elements that commute with everything.

Definition. Let G be a group and A a nonempty subset. The *normalizer* of A in G is defined as p.50

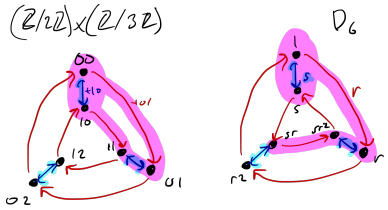
$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

Proposition. *We have $N_G(A) \leq G$.* p.50

We also have that $Z(G) \leq C_G(A) \leq N_G(a) \leq G$.

If we let G act on itself by *conjugation*, i.e. we let $g \cdot h = ghg^{-1}$, then the centralizer of a set A are the elements in G that preserve A pointwise, and the normalizer of A are the elements that preserve A setwise.

Example. We define the group $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z})$ as the set $\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$ where the operation is addition $\pmod 2$ on the first entry and $\pmod 3$ on the second. We let this be generated by $(0,1),(1,0)$ and compare the Cayley diagram to that of D_6.



Look at the sets $A=\{00,01\}$ in $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z})$ or $A=\{1,s\}$ in D_6. In both cases, we can distinguish three blocks that are connected via elements of of A. In the first case, arrows going between blocks agree, but in the second case, they don't. This is why in D_6, we see that r is not in the normalizer of A, since rsr^{-1} is not an element of A. In $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/3\mathbb{Z})$, the subgroup $A=\{00,01\}$ is *normal*, since it turns out that $N_G(A)=G$. Taking group quotients is much like squinting at the picture on the left and seeing a cyclic group of order 3. Since the bundle of 01-arrows agree between the blocks, we can treat it as one big arrow. This is a very handwavy description, but it's just some motivation for the topic of normalizers that we'll return to later.

Example. Consider the quaternion group Q_8. This group is not abelian. We see that $\pm i,\pm j,\pm k$ do not commute with everything, but ± 1 do. Therefore $Z(Q_8)=\{1,-1\}$.

What is the normalizer of the set $A=\{i,j,k\}$? We know this must contain $Z(Q_8)=\{1,-1\}$. We have

$$iAi^{-1}=\{iii^{-1},iji^{-1},iki^{-1}\}=\{-iii,-iji,-iki\}=\{i,-j,-k\}\neq A.$$

Similarly, $jAj^{-1}\neq A$ and $kAk^{-1}\neq A$, and same for $-i,-j,-k$. Therefore $N_{Q_8}(A)=\{1,-1\}$. Since $Z(Q_8)\leq C_{Q_8}(A)\leq N_{Q_8}(A)$, we also see that $C_{Q_8}(A)=\{1,-1\}$.

Definition. If G is a group acting on a set S, then we define the stabelizer of $s\in S$ as the set p.51

$$G_s=\{g\in G\mid g\cdot s=s\}.$$

Clearly the kernel will always be a subset of any stabilizer.

Proposition. *We have $G_s\leq G$.* p.51

Cyclic groups and subgroups

As we have seen a couple of times, For any group G and element $x\in G$, we can generate a cyclic subgroup of G by taking the set $\{x^k\mid k\in\mathbb{Z}\}$. If $|x|=n$ is finite, this is the set $\{1,x,\ldots,x^{n-1}\}$. In fact, we can define cyclic groups this way, as groups that are generated by a single element. p.54

The following two propositions are very useful when dealing with cyclic groups or subgroups. We have already proven most of both of them in homework exercises, but now we have not used the Euclidean Algorithm before.

Proposition. *If $H=\langle x\rangle$, then $|H|=|x|$. Specifically* Prop. 2 p.55

(1) *if* $|H| = n < \infty$, *then* $x^n = 1$ *and* $1, x, \ldots, x^{n-1}$ *are all distinct elements of* H, *and*

(2) *if* $|H| = \infty$, *then* $x^n \neq 1$ *for all* $n \neq 0$ *and* $x^a \neq x^b$ *for all* $a \neq b \in \mathbb{Z}$.

Proposition. *Let* G *be an arbitrary group,* $x \in G$ *and let* $m, n \in \mathbb{Z}$. *If* $x^n = x^m = 1$, *then* $x^d = 1$ *where* $d = (m, n)$. *This implies that if* $x^m = 1$ *for some* $m \in \mathbb{Z}$, *then* $|x|$ *divides* m. Prop. 3 p.55

In class, we will go over the proof for this Proposition using the Euclidean Algorithm.
In class, we have defined cyclic groups in various ways, such as rotations of a polygon, or as additive groups $\mathbb{Z}$ (infinite)or $\mathbb{Z}/n\mathbb{Z}$ (finite). As it turns out, they are structurally equivalent as long as they have the same number of elements. We will go over the proof (via explicit mapping) in class.

Theorem. *Any two cyclic groups of the same order are isomorphic.* Thm. 4 p.56

The following theorem summarizes the structure of subgroups of the cyclic groups.

Theorem. *Let* $H = \langle x \rangle$ *be a cyclic group.* Thm. 7 p.58

(1) *Every subgroup of* H *is cyclic.*

(2) *If* $|H| = \infty$, *then for any distinct nonnegative integers* a *and* b, $\langle x^a \rangle \neq \langle x^b \rangle$.

(3) *If* $|H| = n < \infty$, *then for each positive integer* a *dividing* n *there is a unique subgroup of* H *of order* a.

Exercises

Exercise 1. Show that for any subset A of a group G, $N_G(A)$ is a subgroup of G.

Exercise 2. Show that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$. 2.2.2

Exercise 3. Let H be a subgroup of G. 2.2.6

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

Exercise 4. Let $n \geq 3$. Show that $Z(D_{2n}) = \{1\}$ if n is odd, and $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$. 2.2.7

Exercise 5. Find all generators for $\mathbb{Z}/202\mathbb{Z}$. 2.3.4

Exercise 6. If x is an element of a finite group G and $|x| = |G|$, show that $G = \langle x \rangle$. Give an example to show that this need not be true if G is an infinite group. 2.3.2