Subgroups generated by subsets

For a group G and subset $A \subseteq G$, we have seen that we can find subgroups of G that arise from A, such as $C_G(A)$ and $N_G(A)$. These subgroups do not need to contain A. Perhaps a more natural way to describe a subgroup that arises from A is to take the smallest subgroup of G that contains A, or, alternatively the subgroup of G that consists of the elements A and all other elements that can be expressed in terms of elements of A. As it turns out, these are both valid definitions of a subgroup, and they are in fact equivalent.

We define these two ideas formally as follows:

Definition. The *subgroup generated by* A is defined as p.62

$$\langle A \rangle = \bigcap_{A \subseteq H \leq G} H.$$

If we also define $\overline{A}$ as the set of elements of G that can be expressed as *words* of elements of A:

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \mid n \in \mathbb{Z},\ n \geq 0 \text{ and } a_i \in A,\ \epsilon_i = \pm 1 \text{ for each } i\},$$

where a_is may repeat. Note that 1 is in this set as n may be 0, and an empty product is equal to 1. Then, we have the following proposition.

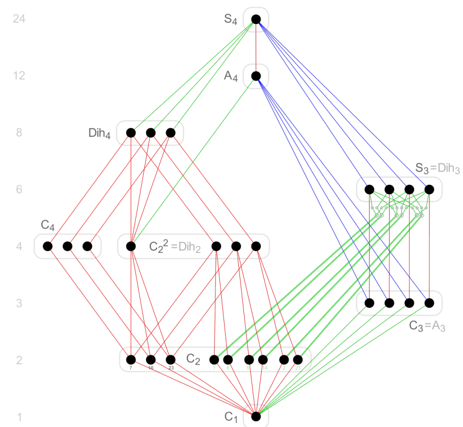
Proposition. $\langle A \rangle = \overline{A}$. Prop. 9 p.63

Note that if $H \leq G$, then $H = \langle H \rangle$, so every subgroup can be described in this way! If we consider the set of subgroups of a group G as a poset under the partial order $\leq$, then we obtain a poset which can be drawn as a Hasse diagram. In this setting, we call such a diagram the *lattice of subgroups* of a group. You can find many examples of these in Section 2.5 in D&F. Sec. 2.5 p.66

Lattice of subgroups

Let G be a group and consider the set of subgroups of G. The subgroup relation $\leq$ defines a *partial order* on this set. (You may want to look this up or refresh your memory if necessary.) The Hasse diagram of this poset is what we call the Lattice of subgroups of G. This lattice gives us yet another way to visualize the structure of a group.

A lattice is a special type of poset, where for any two elements H, K there is a unique smallest element that contains them both, namely $\langle H, k \rangle$, and a unique largest element that is contained in both, namely $H \cap K$ in this case. Section 2.5 shows many examples of lattices of well-known groups. Below is an image of the lattices for S_4 (source: Wikipedia) that shows how it contains groups isomorphic to dihedral and cyclic groups.



Quotient groups

Think of division of integers in the following way. Suppose we want to divide n by k (we'll always assume that $k|n$ when dividing). Take elements of a set of cardinality n and put them in groups of size k. Pack the groups together closely enough so that if you "zoom out", you see n/k groups. This is how we will think of taking quotients of groups, except that we also worry about structure, not just number of elements. It turns out that the study of quotient groups is really the study of homomorphisms. So, we need a few more facts about homomorphisms first. Most of those are already familiar from earlier lectures and homework exercises.

Definition. If ϕ is a homomorphism $\phi : G \to H$, the *kernel* of ϕ is the set p.75

$$\ker \phi = \{g \in G \mid \phi(G) = 1_H\}.$$

Proposition. *Let G and H be groups and let $\phi : G \to H$ be a homomorphism.* Prop. 1 p.75

(1) $\phi(1_G) = 1_H$,

(2) $\phi(g^{-1}) = \phi(g)^{-1}$ *for all* $g \in G$,

(3) $\phi(g^n) = \phi(g)^n$ *for all* $g \in G$,

(4) $\ker \phi$ *is a subgroup of* G,

(5) $\mathrm{im}(\phi)$ *is a subgroup of* H.

Now, we can define quotient groups in terms of kernels of homomorphisms.

Definition. Let $\phi : G \to H$ be a homomorphism with kernel K. The *quotient group G/K* is the group whose elements are the fibers of ϕ with the group operation defined as follows. If $X = \phi^{-1}(a)$ and $Y = \phi^{-1}(b)$ then $XY = \phi^{-1}(ab)$. p.76

Much of the remainder of Section 3.1 is devoted to proving that this quotient group and its binary operation are well-defined.

Definition. For any $N \leq G$ and any $g \in G$ let

$$gN = \{gn \mid n \in N\}, \quad Ng = \{ng \mid n \in N\}$$

called respectively a *left coset* and *right coset* of N in G. Any element of a coset is called a *representative* for the coset.

Now, Proposition 2 and Theorem 3 together help us verify that the definition of quotient groups is well-defined:

Proposition. *Let $\phi : G \to H$ be a homomorphism with kernel K. Let $X \in G/K$ be the fiber above a, i.e. $X = \phi^{-1}(a)$. Then* Prop. 2 p.76

(1) For any $u \in X$, $X = uK$.

(2) For any $u \in X$, $X = Ku$.

Theorem. *Let G be a group and K the kernel of some homomorphism of G to another group. Then the set of left cosets of K in G together with the operation defined by* Thm. 3 p.77

$$uK \circ vK = (uv)K$$

forms the group G/K. (This operation is independent of the choice of representatives u, v.)

Exercises

Exercise 1. Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic. 2.3.11

Exercise 2. Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$. 2.3.19

Exercise 3. Prove that if A is a subset of B, then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subset B$ (proper subset) but $\langle A \rangle = \langle B \rangle$. 2.4.2

Exercise 4. Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 2)(3\ 4)$ is a noncyclic group of order 4. 2.4.6

Exercise 5. Find all elements $x \in D_{16}$ such that $D_{16} = \langle x, s \rangle$. (There are 8 such elements.) 2.5.5

Exercise 6. Let $\phi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\phi^{-1}(E) \leq G$. 3.1.1