SEPTEMBER 26 NOTES

1. 2.5: The lattice of subgroups of a group

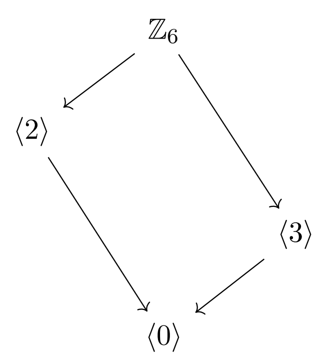
We conclude Chapter 2 with a way of visualizing all subgroups of a given group. This will become very important when we talk about Galois theory in Math 612!

Construction. Let G be a group. For each subgroup of G, plot the subgroups of G vertically, starting with $\{1\}$ at the bottom and G at the top, putting subgroups on the same line if they have the same number of elements. Connect two subgroups $H \leq G$ and $K \leq G$ with a line if $H < K$ and there does not exist a subgroup K' with $H < K' < K$.

Example 1.1. For $G = \mathbb{Z}_6$, we listed all of the subgroups already: The subgroups of $\mathbb{Z}_6$ are:

- (order 6) $\langle 1 \rangle = \langle 5 \rangle = \{0, 1, 2, 3, 4, 5\}$
- (order 3) $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$
- (order 2) $\langle 3 \rangle = \{0, 2\}$
- (order 1) $\langle 0 \rangle = \{0\}$

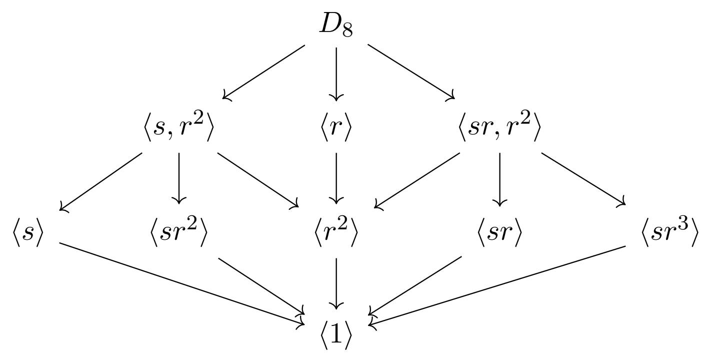
The subgroup lattice is:



Example 1.2. For $G = D_8$, we can list all of the subgroups. (We leave this as an exercise to verify this list is complete. Key input: if a subgroup contains r^i and sr^j for $i = 1, 3$ and $j = 0, 1, 2, 3$, it must be the whole group.)

- (order 8) $\langle r, s \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$
- (order 4) $\langle s, r^2 \rangle = \langle sr^2, r^2 \rangle = \{1, s, r^2, sr^2\}$, and $\langle r \rangle = \langle r^3 \rangle = \{1, r, r^2, r^3\}$, and $\langle sr, r^2 \rangle = \langle sr^3, r^2 \rangle = \{1, sr, r^2, sr^3\}$,
- (order 2) $\langle s \rangle = \{1, s\}$, and $\langle sr^2 \rangle = \{1, sr^2\}$, $\langle r^2 \rangle = \{1, r^2\}$, and $\langle sr \rangle = \{1, sr\}$, and $\langle sr^3 \rangle = \{1, sr^3\}$,
- (order 1) $\langle 1 \rangle = \{1\}$

The subgroup lattice is:



2. 3.1: Quotient groups and homomorphisms

Let $\phi : G \to H$ be a homomorphism. For any $a \in H$, the **fiber** over a, X_a, is the preimage of a:

$$X_a := \phi^{-1}(a) = \{g \in G \mid \phi(g) = a\}.$$

We can visualize this schematically as the fibers of G being the 'vertical' sets that get contracted to the point $a \in H$ (see Dummit and Foote). Using the binary operation in H, we can define a group structure on the set of nonempty fibers by saying $X_a \star X_b = X_{ab}$, where $ab \in H$ is the product of a and b. This construction is one definition of *quotient group*.

The prototypical example is the map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(x) = x \mod n$. The fiber X_a is the set of all $z\mathbb{Z}$ such that $z = a \mod n$, i.e. all elements with remainder a. It makes sense to say $X_a + X_b = X_{a+b}$ because, for $z \in X_a$ and $w \in X_b$, $z = a \mod n$ and $w = b \mod n$, so $z + w = a + b \mod n$.

Before we formally define quotient groups, some reminders:

Let $\phi : G \to H$ be a homomorphism. Then:

(1) $\phi(1_G) = 1_H$
(2) $\phi(g^{-1}) = \phi(g)^{-1}$
(3) for any $n \in \mathbb{Z}$, $\phi(g^n) = \phi(g)^n$
(4) the **kernel** of ϕ is the set $\ker \phi = \{g \in G \mid \phi(g) = 1_H\} = X_{1_H}$. It is a subgroup of G.
(5) the **image** of ϕ is the set $\mathrm{im}\phi = \{\phi(g) \mid g \in G\}$. It is a subgroup of H.

Definition 2.1. Let $\phi : G \to H$ be a homomorphism with kernel K. The **quotient group** G/K ('G mod K') is the group

$$G/K = \{X_a \mid a \in H\}$$

with $X_a \star X_b := X_{ab}$.

This may be quite different than the definition you've seen before. To relate them, we introduce more notation and observations.

Proposition 2.2. *Let $\phi : G \to H$ be a homomorphism with kernel K. Let $X = \phi^{-1}(a)$ for $a \in H$. Then:*

(1) For any $u \in X$, $X = \{uk \mid k \in K\}$ and
(2) for any $u \in X$, $X = \{ku \mid k \in K\}$.

Proof. We prove only (1). Let $uK = \{uk \mid k \in K\}$. For any $k \in K$, we have $\phi(k) = 1$, and $u \in X$, so $\phi(u) = a$, and therefore $\phi(uk) = \phi(u)\phi(k) = a1 = a$, so $uk \in X$. Therefore, $uK \subset X$.

Now, let $x \in X$ be any element. Let $k = u^{-1}x$ and note that $\phi(k) = \phi(u^{-1}x) = \phi(u)^{-1}\phi(x) = a^{-1}a = 1$ so $k \in K$. Because $x = uk$, we have shown $x \in uK$ so $X \subset uK$. Therefore, $X = uK$. □

These sets uK are very important so have their own name.

Definition 2.3. Let $H \leq G$ be any subgroup and $g \in G$. The **left coset** of H with respect to g is

$$gH = \{gh \mid h \in H\}.$$

The **right coset** is

$$Hg = \{hg \mid h \in H\}.$$

We can use the language of cosets to define a quotient group without using the homomorphism ϕ at all.

Theorem 2.4. *Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set of left cosets of K forms a group G/K with binary operation $uKvK = (uv)K$.*

Proof. Note that, by the previous proposition, the fibers of ϕ are exactly the cosets of K, so the set G/K is the same as our previous definition. Let us show that this binary operation is well-defined and the same as above. First, let X and Y be fibers so $X = \phi^{-1}(a)$ and $Y = \phi^{-1}(b)$. Let $Z = \phi^{-1}(ab)$ so $XY = Z$. Let u and v be arbitrary representatives of X and Y, i.e. $X = uK$ and $Y = vK$. To show our new binary operation $uKvK = (uv)K$ is well defined, we need to show that $uvK = Z$, which is implied by saying $uv \in Z$ (by the previous proposition). By definition, $\phi(u) = a$ and $\phi(v) = b$, so we have $\phi(uv) = \phi(u)\phi(v) = ab$ so $uv \in Z$. Therefore, $Z = uvK$. □

Example 2.5. The morphism $\phi : \mathbb{Z} \to \mathbb{Z}_n$ has kernel $\langle n \rangle$. The cosets of $\langle n \rangle$ are exactly the sets $0 + \langle n \rangle$, $1 + \langle n \rangle$, $2 + \langle n \rangle$, ... $n - 1 + \langle n \rangle$. The group of cosets has binary operation determined by just adding the first number: $u + \langle n \rangle + v + \langle n \rangle = (u + v) + \langle n \rangle$.

Sometimes Dummit and Foote denotes cosets by $\overline{u}$ instead of uK for simplicity, so the previous example we could write the cosets as $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

More on cosets:

Proposition 2.6. *Let H be any subgroup of G. The set of left cosets form a partition of G, meaning for every $g \in G$, g appears in some coset of H, and for two different elements $u, v \in G$, either $uH = vH$ or $uH \cap vH = \emptyset$. Furthermore, $uH = vH$ if and only if $v^{-1}u \in H$.*

Proof. Because $e \in H$, for any $g \in G$, $g = ge \in gH$, so every $g \in G$ appears in some coset of H. Now, suppose $u, v \in G$. If $uH \cap vH = \emptyset$, we have nothing to prove. Suppose $uH \cap vH \neq \emptyset$ and let $x \in uH \cap vH$. Then, $x = uh_1$ and $x = vh_2$ for some $h_1, h_2 \in H$. In particular, $uh_1 = vh_2$, so $u = vh_2h_1^{-1}$. Because $h_2h_1^{-1} \in H$, we have $u \in vH$. Therefore, for any $uh \in uH$, $uh = v(h_2h_1^{-1}h) \in vH$ so $uH \subset vH$. Similarly, we can show $vH \subset uH$ so $vH = uH$.

Note that we showed $u \in vH$ in the course of the proof, so $u = vh$ for some $h \in H$, so $v^{-1}u = h \in H$. Similarly, if $v^{-1}u = h \in H$, then by the proof $uH \subset vH$. Finally, if $v^{-1}u = h \in H$, then $u^{-1}v = h^{-1} \in H$, so $vH \subset uH$. Therefore, $v^{-1}u \in H$ if and only if $uH = vH$. □