SEPTEMBER 14 NOTES

1. 1.7: Group actions

From last time:

Definition 1.1. Let A be a set. An **action** of a group G on a set A is a map $G \times A \to A$, written as $(g, a) \mapsto g \cdot a$, such that:

(1) for all $g_1, g_2 \in G$ and $a \in A$, $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, and
(2) for all $a \in A$, $1 \cdot a = a$.

In this case, we say the group G **acts** on A.

Example 1.2. Later in the course, we will often have a group G act *on itself*. The most common examples are the **left regular action** of G acting on G by $g \cdot a = ga$ for all $g, a \in G$ and **conjugation**: G acting on itself by $g \cdot a = gag^{-1}$ for all $g, a \in G$. You will explore these more in your homework, and we will use groups acting on themselves to prove many results (e.g. Lagrange's Theorem, the class equation, Sylow's Theorems, ...).

We will come back to actions later today.

2. 2.1: Subgroups

Definition 2.1. A **subgroup** of a group G is a subset $H \subset G$ such that:

(1) H is nonempty,
(2) H is closed under products, i.e. $x, y \in H$ implies $xy \in H$, and
(3) H is closed under inverses, i.e. $x \in H$ implies $x^{-1} \in H$.

If H is a subgroup of G, we denote this by $H \leq G$. If H is a *proper* subgroup (meaning $H \neq G$), we denote this by $H < G$.

Subgroups of G are in fact just subsets of G that are groups with the binary operation of G: this is associative because it is in G, contains at least one element x and by (3) contains x^{-1}, so contains the identity $1 = xx^{-1}$ by (2), and contains the inverse of every element by (3).

Example 2.2. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ because the sum of any two integers (resp. rational numbers) is an integer (resp. rational number) and the additive inverse of any integer (resp. rational number) is an integer (resp. rational number).

Example 2.3. Let $G = D_{2n}$ and let $H = \{1, r, r^2, \dots, r^{n-1}\}$. Because the product of any two rotations is again a rotation, and the inverse of any rotation is a rotation, H is a subgroup of G.

If instead $H = \{1, s, sr, \dots, sr^{n-1}\}$, then H is not a subgroup, because $(s)(sr) = r \notin H$.

Example 2.4. The set of even integers is a subgroup of $\mathbb{Z}$: the sum and additive inverse of an even number is again even.

Example 2.5. If G is a group and $x \in G$ is any element, the **subgroup generated by** x is the set

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\} = \{\dots, x^{-1}, 1, x, x^2, \dots\}.$$

This is indeed a subgroup: the product of two powers of x is again a power of x and the inverse of a power of x is again a power of x.

Proposition 2.6. *A subset H of a group G is a subgroup if and only if $H \neq \emptyset$ and for all $x, y \in H$, $xy^{-1} \in H$.*

Proof. If H is a subgroup of G, then these properties hold by requirements (1), (2), (3) to be a subgroup.

Now suppose $H \neq \emptyset$ and for all $x, y \in H$, $xy^{-1} \in H$. We must show H satisfies requirements (1),(2),(3). (1) holds by assumption. To show (3), assume $x \in H$ is any element. If $y = x$, we know $xx^{-1} = 1 \in H$ so the identity is in H, and therefore $1x^{-1} \in H$, so $x^{-1} \in H$. Finally, to show (2), note that we just showed for any element $z \in H$, $z^{-1} \in H$, so if $x, y \in H$, then $x, y^{-1} \in H$, and therefore $x(y^{-1})^{-1} = xy \in H$. Therefore, H is a subgroup. □

Proposition 2.7. *If G is a finite group, then H is a subgroup if and only if H is nonempty and H is closed under products.*

Proof. If H is a subgroup, it is nonempty and closed under products by definition.

For the converse, we must show that H nonempty and closed under products implies it is closed under inverses. Let $x \in H$ be any element. Because G is finite, there are only finitely many distinct elements $x, x^2, x^3, \ldots$ so there must exist $a, b \in \mathbb{Z}^+$ with $b > a$ such that $x^a = x^b$, i.e. $1 = x^{b-a}$ (which proves $1 \in H$). Therefore, $xx^{b-a-1} = 1$ so $x^{-1} = x^{b-a-1}$. In particular, $x^{b-a-1} \in H$ so $x^{-1} \in H$. □

On your homework, you will prove many of the subsets we have already encountered are subgroups:

Example 2.8. If $\phi : G \to H$ is a homomorphism, then $\ker \phi$ is a subgroup of G and $\mathrm{im}\phi$ is a subgroup of H.

We will introduce several more subgroups in the next section.

3. 2.2: Centralizers, normalizers, stabilizers, and kernels

In what follows, G will denote a group and A will denote a nonempty set.

Definition 3.1. If A is a subset of G, the **centralizer** $C_G(A)$ is the set

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

Equivalently,

$$C_G(A) = \{g \in G \mid ga = ag \text{ for all } a \in A\}.$$

In other words, the centralizer of A is the set of elements of G that commute with every element of A.

Proposition 3.2. *For any nonempty subset A of G, $C_G(A)$ is a subgroup of G.*

Proof. First, note that $C_G(A) \neq \emptyset$ because $1 \in C_G(A)$. To prove it is a subgroup, we must then show that if $x, y \in C_G(A)$, then x^{-1} and $xy \in C_G(A)$. Suppose $x \in C_G(A)$, so for all $a \in A$, $xax^{-1} = a$. Multiplying on the left by x^{-1} and the right by x, we obtain $a = x^{-1}ax$, or $a = x^{-1}a(x^{-1})^{-1}$. This holds for any $a \in A$, and therefore $x^{-1} \in C_G(A)$ so the centralizer is closed under inverses.

Now suppose $x, y \in C_G(A)$, so for all $a \in A$, $xax^{-1} = a$ and $yay^{-1} = a$. We compute:

$$\begin{aligned}(xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

which proves that $xy \in C_G(A)$ so the centralizer is closed under products. Therefore, $C_G(A)$ is a subgroup of G. □

Remark 3.3. If $A = \{a\}$ is a single element of G, we denote $C_G(A)$ by $C_G(a)$. Because powers of a commute with each other, $\langle a \rangle \subset C_G(a)$, i.e. $a^n \in C_G(a)$ for all $n \in \mathbb{Z}$.

Example 3.4. If G is abelian, then for any nonempty subset A of G, $C_G(A) = G$ (every element of G commutes with any element of A, by definition).

Definition 3.5. The **center** of a group G is the set $Z(G)$ of elements

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

The center is the set of elements that commute with all elements of G.

By definition, $Z(G) = C_G(G)$ so it is a subgroup of G. In general, for any A subset of G, $Z(G) \subset C_A(G)$.

Definition 3.6. If $g \in G$ is an element of a group and A is a nonempty subset of G, then $gAg{-}1 = \{gag^{-1} \mid a \in A\}$. The **normalizer** of A in G is the set

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

If you have seen *normal subgroups* before, this may look familiar.

Note that if $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$, so $gAg^{-1} = A$, which implies that $C_G(A) \subset N_G(A)$.

Proposition 3.7. *$C_G(A) \leq N_G(A)$ and $N_G(A) \leq G$.*

Proof. Exercise. □

Example 3.8. Let $G = D_8$. Then, $Z(G) = \{1, r^2\}$. We show this by demonstrating that these elements commute with all elements of D_8, and by exhibiting an example to show that no other elements commute with everything.

Write $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Recall that $r^k s = sr^{4-k}$.

First, $1 \in Z(G)$ by definition. Also, $r^2 \in Z(G)$ because $r^2 r^j = r^{2+j} = r^j r^2$ for any $j \in \mathbb{Z}$, and $r^2 sr^j = sr^{4-2} r^j = sr^2 r^j = sr^j r^2$ for any $j \in \mathbb{Z}$.

Now, $r, r^3 \neq Z(G)$ because $sr \neq rs = sr^3$, and $sr^3 \neq r^3 s = sr$. Also, $s \neq Z(G)$ again because $sr \neq rs$. Similarly, $sr^j \neq Z(G)$ because $sr^j r = sr^{j+1} \neq rsr^j = sr^{3+j}$. Therefore, no other elements of D_8 can be in the center so $Z(D_8) = \{1, r^2\}$.

Tying this back in to group actions, we have the following additional subgroups.

Definition 3.9. If G is a group acting on a set A and $a \in A$ is any element, the **stabilizer** of a is the set

$$G_a = \{g \in G \mid g \cdot a = a\}.$$

Proposition 3.10. *For any $a \in A$, G_a is a subgroup of G.*

Proof. Exercise. □

Definition 3.11. If G is a group acting on a set A the **kernel** of the action is the set

$$\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}.$$

Proposition 3.12. *The kernel of a group action is a subgroup of G.*

Proof. Exercise. □

Every example in the first half of this section is a special case of kernel or stabilizer.

Example 3.13. Let $S = \mathcal{P}(G)$ be the set of all subsets of G. Then, G acts on S by conjugation: for any $B \subset G$,

$$g \cdot B = gBg^{-1} \subset G.$$

Then, by definition, for a subset A of G, $N_G(A) = G_A$ is the stabilizer of A under this action.

Next, for any $A \subset G$, we can consider $N_A(G)$ acting on A by conjugation: for $g \in N_A(G)$, $g \cdot a = gag^{-1}$. (Because $g \in N_A(G), g \cdot a$ is indeed an element of A.) Then, the centralizer of A, $C_G(A)$, is exactly the kernel of this action.