Math 562/662 **Spring 2022**
Homework 2 **Drew Armstrong**

---

1. One Step Subgroup Test. Let $(G, *, \varepsilon)$ be a group and let $H \subseteq G$ be a subset. We say that H is a *subgroup* when the following three conditions are satisfied:

(1) $\varepsilon \in H$,
(2) $a \in H \Rightarrow a^{-1} \in H$,
(3) $a, b \in H \Rightarrow a * b \in H$.

Prove that these three conditions are equivalent to the following single condition:

(4) $a, b \in H \Rightarrow a^{-1} * b \in H$.

Proof. First assume that (1), (2) and (3) hold. Then for any $a, b \in H$ we have $a^{-1} \in H$ by (2) and since $a^{-1}, b \in H$ we have $a^{-1} * b \in H$ by (3). Hence (4) holds.

Conversely, suppose that (4) holds. In this case we will show that (1), (2) and (3) hold. It is important to prove these in a specific order:

(1): For any $a \in H$ we have by (4) that $\varepsilon = a^{-1} * a \in H$.
(2): For any $a \in H$ we have $a, \varepsilon \in H$ by (1) and hence $a^{-1} = a^{-1} * \varepsilon \in H$ by (4).
(3): For any $a, b \in H$ we have $a^{-1}, b \in H$ by (2). Hence by (4) we have

$$a * b = (a^{-1})^{-1} * b \in H.$$

□

2. Congruence Modulo a Subgroup. Let $(G, *, \varepsilon)$ be a group and let $H \subseteq G$ be a subgroup. For any $a, b \in G$ we define the relation of *congruence modulo* H:

$$a \equiv b \bmod H \quad \Longleftrightarrow \quad a^{-1} * b \in H.$$

And for any $a \in G$ we define the *coset of* H *generated by* a:

$$a * H := \{a * h : h \in H\} \subseteq G.$$

(a) Prove that congruence mod H is an equivalence relation on G.
(b) For all $a, b \in G$, prove that a and b are congruent mod H if and only if the cosets that they generate are equal:

$$a \equiv b \bmod H \quad \Longleftrightarrow \quad a * H = b * H.$$

(a): The properties (1), (2) and (3) of subgroups are defined precisely so that this relation is an equivalence:

Reflexive. From (1) we have $a^{-1} * a = \varepsilon \in H$ and hence $a \equiv a \bmod H$ for all $a \in G$.

Symmetric. For all $a, b \in G$ we have

$$\begin{aligned}
a \equiv b \bmod H &\Longrightarrow a^{-1} * b \in H \\
&\Longrightarrow (a^{-1} * b)^{-1} \in H && \text{from (2)} \\
&\Longrightarrow b^{-1} * (a^{-1})^{-1} \in H \\
&\Longrightarrow b^{-1} * a \in H \\
&\Longrightarrow b \equiv a \bmod H.
\end{aligned}$$

Transitive. For all $a, b, c \in G$ we have

$$\begin{aligned}
a \equiv b \text{ and } b \equiv c \bmod H &\implies a^{-1} * b \in H \text{ and } b^{-1} * c \in H \\
&\implies (a^{-1} * b) * (b^{-1} * c) \in H && \text{from (3)} \\
&\implies a^{-1} * (b * b^{-1}) * c \in H \\
&\implies a^{-1} * \varepsilon * c \in H \\
&\implies a^{-1} * c \in H \\
&\implies a \equiv c \bmod H.
\end{aligned}$$

(b): First suppose that we have $a * H = b * H$. Since $\varepsilon \in H$ we have $b = b * \varepsilon \in b * H$, which implies that $b \in a * H$. By definition this means that $b = a * h$ for some $h \in H$, which implies that $a^{-1} * b = h \in H$. We conclude that $a \equiv b \bmod H$, as desired.

Conversely, suppose that we have $a \equiv b \bmod H$, so that $a^{-1} * b \in H$. Let's say $a^{-1} * b = h \in H$, so that $b = a * h$ and $a = b * h^{-1}$. Our goal is to show that $a * H = b * H$ and for this we must prove two inclusions:

- To see that $b * H \subseteq a * H$, consider any element $b * h' \in b * H$, with $h' \in H$. Then since H is a subgroup we have $h * h' \in H$ and hence
$$b * h' = (a * h) * h' = a * (h * h') \in a * H.$$
- To see that $a * H \subseteq b * H$, consider any element $a * h'' \in a * H$, with $h'' \in H$. Then since H is a subgroup we have $h^{-1} * h'' \in H$ and hence
$$a * h'' = (b * h^{-1}) * h'' = b * (h^{-1} * h'') \in b * H.$$

Remark: It follows from (a) and (b) that the group G is **partitioned** into cosets of H. Furthermore, we observe that the function $H \to a * H$ defined by $h \mapsto a * h$ is an invertible function with inverse $g \mapsto a^{-1} * g$. Hence any coset $a * H$ is in bijection with H. If G is finite then H is finite and it follows that any two cosets have the same number of elements. Finally, if G/H is the set of cosets, we conclude that

$$\#G = \#(G/H) \cdot \#H.$$

This is called *Lagrange's Theorem.*

3. Orbit-Stabilizer Theorem. Let $(G, *, \varepsilon)$ be a group and let X be a set. Consider a function $\cdot : G \times X \to X$, which we will denote by $(g, x) \mapsto g \cdot x$. We call this function an *action of G on X* when the following two properties are satisfied:

(i) $\varepsilon \cdot x = x$ for all $x \in X$,

(ii) $a \cdot (b \cdot x) = (a * b) \cdot x$ for all $a, b \in G$ and $x \in X$.

(a) For any element $x \in X$ we define the set $\text{Stab}(x) := \{a \in G : a \cdot x = x\} \subseteq G$, called the *stabilizer of x*. Prove that this set is a subgroup of G.

(b) For any element $x \in X$ we define the set $\text{Orb}(x) := \{g \cdot x : g \in G\} \subseteq X$, called the *orbit of x*. Prove that there exists a bijection $\text{Orb}(x) \leftrightarrow G/\text{Stab}(x)$ between elements of the orbit and cosets of the stabilizer. [Hint: Send the element $g \cdot x \in \text{Orb}(x)$ to the coset $g * \text{Stab}(x)$. Check that this is well-defined and bijective.]

(c) If G is finite, combine (b) with Lagrange's Theorem to prove that
$$\#G = \#\text{Orb}(x)\#\text{Stab}(x) \quad \text{for any } x \in X.$$

(a): We must show that (1), (2) and (3) hold.

(1): From (i) we have $\varepsilon \cdot x = x$ for all $x \in X$, and hence $\varepsilon \in \mathrm{Stab}(x)$.

(2): For any $a \in \mathrm{Stab}(x)$, it follows from (i), (ii) and (1) that

$$a^{-1} \cdot x = a^{-1} \cdot (a \cdot x) = (a^{-1} * a) \cdot x = \varepsilon \cdot x = x,$$

and hence $a^{-1} \in \mathrm{Stab}(x)$.

(3): For any $a, b \in \mathrm{Stab}(x)$, it follows from (ii) that

$$(a * b) \cdot x = a \cdot (b \cdot x) = a \cdot x = x,$$

and hence $a * b \in H$.

Remark: We could also have used the one step subgroup test.

(b): We want to define a bijection from $\mathrm{Orb}(x)$ to the set of cosets $G/\mathrm{Stab}(x)$. I claim that the following function does the trick:

$$\begin{array}{cccc} \varphi : & \mathrm{Orb}(x) & \to & G/\mathrm{Stab}(x) \\ & g \cdot x & \mapsto & g * \mathrm{Stab}(x). \end{array}$$

First observe that the function φ is well-defined:

$$\begin{aligned} a \cdot x = b \cdot x &\Longrightarrow a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (b \cdot x) && \\ &\Longrightarrow x = (a^{-1} * b) \cdot x && \text{(i) and (ii)} \\ &\Longrightarrow a^{-1} * b \in \mathrm{Stab}(x) && \\ &\Longrightarrow a * \mathrm{Stab}(x) = b * \mathrm{Stab}(x) && \text{from 2(b)} \\ &\Longrightarrow \varphi(a \cdot x) = \varphi(b \cdot x). && \end{aligned}$$

Next we observe that the function φ is surjective by definition because any coset has the form $g \in \mathrm{Stab}(x)$ for some $g \in G$, and hence $g * \mathrm{Stab}(x) = \varphi(g \cdot x)$. Finally, we observe that φ is injective:

$$\begin{aligned} \varphi(a \cdot x) = \varphi(b \cdot x) &\Longrightarrow a * \mathrm{Stab}(x) = b * \mathrm{Stab}(x) && \\ &\Longrightarrow a^{-1} * b \in \mathrm{Stab}(x) && \text{from 2(b)} \\ &\Longrightarrow x = (a^{-1} * b) \cdot x && \\ &\Longrightarrow a \cdot x = a \cdot [(a^{-1} * b)] \cdot x && \\ &\Longrightarrow a \cdot x = b \cdot x && \text{from (i) and (ii)} \end{aligned}$$

Remark: We could have proved simultaneously that φ is well-defined and injective by observing that each of the implications in the argument is reversible. I only avoided this for pedagogical reasons.

(c): If G is finite then the subgroup $\mathrm{Stab}(x) \subseteq G$ is finite Lagrange's Theorem gives

$$\#G = \#(G/\mathrm{Stab}(x)) \cdot \#\mathrm{Stab}(x).$$

But from the Orbit-Stabilizer Theorem we know that the sets $\mathrm{Orb}(x)$ and $G/\mathrm{Stab}(x)$ have the same number of elements, hence

$$\#G = \#\mathrm{Orb}(x) \cdot \#\mathrm{Stab}(x).$$

4. The Alternating Group, Part 2. Consider the following polynomial in n variables:

$$\delta(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j) \in \mathbb{Q}[x_1, \ldots, x_n].$$

Recall that the symmetric group S_n acts on the ring of polynomials by permuting variables: For all $\sigma \in S_n$ and $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ we define

$$(\sigma \cdot f)(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in \mathbb{Q}[x].$$

(a) Prove that for any transposition $t \in S_n$ we have $t \cdot \delta = -\delta$.
(b) Use part (a) to prove that the stabilizer of δ is the alternating group:

$$\mathrm{Stab}(\delta) = A_n.$$

(c) Now use the Orbit-Stabilizer Theorem to prove that

$$\#A_n = \frac{1}{2}\#S_n = \frac{1}{2}n!.$$

[Hint: Show that $\mathrm{Orb}(\delta)$ has size 2.]

(a): I realized this is too hard so I told you not to prove it. For any $\sigma \in S_n$ we have

$$\sigma \cdot \delta = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}).$$

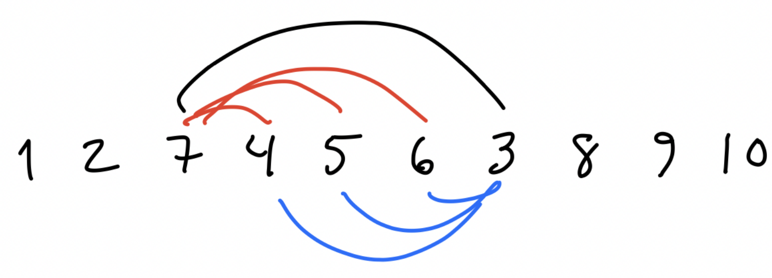
When $\sigma(i) < \sigma(j)$ the factor $x_{\sigma(i)} - x_{\sigma(j)}$ occurs in both δ and $\sigma \cdot \delta$. But when $\sigma(i) > \sigma(j)$ the factor $x_{\sigma(j)} - x_{\sigma(i)} = -(x_{\sigma(i)} - x_{\sigma(j)})$ occurs in δ. This means that $\sigma \cdot \delta = \pm\delta$, where the sign is determined by the number of pairs $i < j$ such that $\sigma(i) > \sigma(j)$. Such a pair $i < j$ is called an *inversion* of σ. If $\mathrm{inv}(\sigma)$ denotes the number of inversions of σ then we see that

$$\sigma \cdot \delta = (-1)^{\mathrm{inv}(\sigma)}\delta.$$

Thus our goal is to show that any transposition $t \in S_n$ has an **odd number of inversions**. In fact, I claim that the transposition $(k\ell) \in S_n$, with $k < \ell$, has exactly $2(\ell - k - 1) + 1$ inversions, which come in three kinds:

- The pair $k < \ell$ is an inversion.
- Each pair $k < j$ (with $j < \ell$) is an inversion. There are $\ell - k - 1$ of these.
- Each pair $j < \ell$ (with $k < j$) is an inversion. There are $\ell - k - 1$ of these.

To see this it's best to draw a picture. The inversions of σ correspond to pairs of numbers $\sigma(i)$ and $\sigma(j)$ in the one-line notation where the larger number is on the left. Thus we need to count such pairs in the one-line notation for the transposition $(k\ell) \in S_n$. Here's the picture for $(37) \in S_{10}$:



(b): You showed on a previous homework that every permutation $\sigma \in S_n$ can be expressed in the form $\sigma = t_1 \circ t_2 \circ \cdots \circ t_k$, where $t_1, \ldots, t_k \in S_n$ are transpositions. In this case, part (a) and property (ii) of group actions imply that

$$(*) \qquad \sigma \cdot \delta = t_1 \cdot (t_2 \cdot (t_3 \cdot (\cdots t_k \cdot \delta)) = (-1)^k\delta.$$

The transpositions t_i and the number k are not unique. However, we see that the *parity* of k (i.e., the evenness or oddness) is unique. Indeed, if σ is a composition of an even number transpositions then $(*)$ says that $\sigma \cdot \delta = \delta$ and if σ is a product of an odd number of transpositions then $(*)$ says that $\sigma \cdot \delta = -\delta$. But since $\delta \neq -\delta$, this implies that no permutation can simultaneously be a composition of an even and an odd number of transpositions. By definition, A_n is the set of permutations that are a composition of an even number of transpositions. Hence it follows that

$$A_n = \{\sigma \in S_n : \sigma \cdot \delta = \delta\} = \mathrm{Stab}(\delta).$$

(c): In part (b) we observed that $\sigma \cdot \delta = \pm\delta$ for all $\sigma \in S_n$, and in part (a) we found that both of these possibilities do indeed occur. Thus we have

$$\mathrm{Orb}(\delta) = \{\sigma \cdot \delta : \sigma \in S_n\} = \{\delta, -\delta\}.$$

Finally, we conclude from the Orbit-Stabilizer Theorem that

$$\begin{aligned} \#S_n &= \#\mathrm{Orb}(\delta)\#\mathrm{Stab}(\delta) \\ n! &= 2\#A_n \\ \#A_n &= n!/2. \end{aligned}$$