Math 561/661 **Fall 2023**
Homework 2 **Drew Armstrong**

---

1. One Step Subgroup Test. Let $(G, *, \varepsilon)$ be a group and let $H \subseteq G$ be a subset. Consider the following four properties:

(S1) $\varepsilon \in H$,
(S2) For all $a \in H$ we have $a^{-1} \in H$,
(S3) For all $a, b \in H$ we have $a * b \in H$,
(S4) For all $a, b \in H$ we have $a * b^{-1} \in H$.

Prove that (S4) holds if and only if all three of (S1), (S2), (S3) hold.

Proof. If (S1), (S2), (S3) hold then (S4) clearly holds. Conversely, suppose that (S4) holds. In this case we will show that (S1), (S2) and (S3) hold. We will prove them in this order.

(S1): We will assume that the set H is non-empty. (Sorry I forgot to mention this.) Pick any element $a \in H$. Then from (S4) we have $\varepsilon = a * a^{-1} \in H$.

(S2): From (S1) we have $\varepsilon \in H$. Then for any $b \in H$, (S4) implies $b^{-1} = \varepsilon * b^{-1} \in H$.

(S3): Consider any $a, b \in H$. From (S2) we know that $b^{-1} \in H$. Then from (S4) we have

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

2. Homomorphism and Isomorphism. Consider two groups $(G, *, \varepsilon_G)$ and $(H, \bullet, \varepsilon_H)$. A function $\varphi : G \to H$ is called a *homomorphism* if it satisfies the following condition:

$$\varphi(a * b) = \varphi(a) \bullet \varphi(b) \quad \text{for all } a, b \in G.$$

(a) If $\varphi : G \to H$ is a homomorphism, prove that $\varphi(\varepsilon_G) = \varepsilon_H$.
(b) If $\varphi : G \to H$ is a homomorphism, prove that $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$.
(c) Let $\varphi : G \to H$ be a homomorphism and suppose the inverse function φ^{-1} exists. Prove that the function $\varphi^{-1} : H \to G$ is also a homomorphism. It follows that invertible homomorphisms are the same as isomorphisms. [Hint: Given $a, b \in H$, apply the function φ to the group element $\varphi^{-1}(a) * \varphi^{-1}(b) \in G$.]

(a): Let $\varphi : G \to H$ be a homomorphism. For any group element $a \in H$ we have

$$\varphi(a) = \varphi(a * \varepsilon_G) = \varphi(a) \bullet \varphi(\varepsilon_G).$$

Since H is a group, the inverse $\varphi(a)^{-1} \in H$ exists. Multiplying the previous equation on the left by $\varphi(a)^{-1}$ gives

$$\begin{aligned} \varphi(a) \bullet \varphi(\varepsilon_G) &= \varphi(a) \\ \varphi(a)^{-1} \bullet \varphi(a) \bullet \varphi(\varepsilon_G) &= \varphi(a)^{-1} \bullet \varphi(a) \\ \varphi(\varepsilon_G) &= \varepsilon_H. \end{aligned}$$

(b): Let $\varphi : G \to H$ be a homomorphism. For any element $a \in G$ we have

$$\varphi(a) \bullet \varphi(a^{-1}) = \varphi(a * a^{-1}) = \varphi(\varepsilon_G) = \varepsilon_H,$$

where the last step follows from part (a). Then multiplying on the left by the element $\varphi(a)^{-1} \in H$ (which exists because H is a group), we obtain

$$\varphi(a) \bullet \varphi(a^{-1}) = \varepsilon_H$$

$$\begin{aligned} \varphi(a)^{-1} \bullet \varphi(a) \bullet \varphi(a^{-1}) &= \varphi(a)^{-1} \bullet \varepsilon_H \\ \varphi(a^{-1}) &= \varphi(a)^{-1}. \end{aligned}$$

(c): Let $\varphi : G \to H$ be a homomorphism and assume that the function φ^{-1} exists. Then for any elements $a, b \in H$ we have

$$\begin{aligned} \varphi[\varphi^{-1}(a) * \varphi^{-1}(b)] &= \varphi[\varphi^{-1}(a)] \bullet [\varphi^{-1}(b)] \\ &= a \bullet b. \end{aligned}$$

Finally, applying φ^{-1} to both sides gives

$$\varphi^{-1}(a \bullet b) = \varphi^{-1}\left[\varphi[\varphi^{-1}(a) * \varphi^{-1}(b)]\right] = \varphi^{-1}(a) * \varphi^{-1}(b),$$

as desired.

3. Powers of a Cycle. Consider the "standard 12-cycle" in cycle notation:

$$c := (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12) \in S_{12}.$$

Compute the first twelve powers $c, c^2, c^3, \ldots, c^{12}$ and express each of them in cycle notation. Try to guess what the k-th power of an n-cycle looks like.
We have

$$\begin{aligned} c &= (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12), \\ c^2 &= (1, 3, 5, 7, 9, 11)(2, 4, 6, 8, 10, 12), \\ c^3 &= (1, 4, 7, 10)(2, 5, 8, 11)(3, 6, 9, 12), \\ c^4 &= (1, 5, 9)(2, 6, 10)(3, 7, 11)(4, 8, 12), \\ c^5 &= (1, 6, 11, 4, 9, 2, 7, 12, 5, 10, 3, 8), \\ c^6 &= (1, 7)(2, 8)(3, 9)(4, 10)(5, 11)(6, 12), \\ c^7 &= (1, 8, 3, 10, 5, 12, 7, 2, 9, 4, 11, 6), \\ c^8 &= (1, 9, 5)(2, 10, 6)(3, 11, 7)(4, 12, 8), \\ c^9 &= (1, 10, 7, 4)(2, 11, 8, 5)(3, 12, 9, 6), \\ c^{10} &= (1, 11, 9, 7, 5, 3)(2, 12, 10, 8, 6, 4), \\ c^{11} &= (1, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2), \\ c^{12} &= (1)(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12) = \varepsilon. \end{aligned}$$

You may observe the following general phenomenon: If c is an n-cycle then for any integer $k \in \mathbb{Z}$ the permutation c^k is a product of cycles, each of length $n/\gcd(k, n)$. We will prove this later.

4. Order of an Element. Let $(G, *, \varepsilon)$ be a group and let $g \in G$ be any element. Recall that there is a unique way to define group elements $g^n \in G$ for all integers $n \in \mathbb{Z}$ so that

- $g^1 = g$,
- $g^{m+n} = g^n * g^m$ for all $m, n \in \mathbb{Z}$.

This notation satisfies $g^0 = \varepsilon$ and $(g^n)^{-1} = g^{-n}$ for all $n \in \mathbb{Z}$.

(a) Let $\langle g \rangle \subseteq G$ be the smallest subgroup of G that contains the element g. Prove that

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

[Hint: Show that the set on the right is a subgroup of G.]

(b) If $\langle g \rangle$ is a finite set, prove that there exists some $n \geq 1$ such that $g^n = \varepsilon$.

(c) Let $\langle g\rangle$ be a finite set and let $m \geq 1$ be the **smallest positive integer** satisfying $g^m = \varepsilon$. In this case, prove that $\langle g\rangle$ has exactly m elements:

$$\langle g\rangle = \{\varepsilon, g, g^2, \ldots, g^{m-1}\}.$$

This m is called the *order* of the element $g \in G$. If the set $\langle g\rangle$ is infinite then we will say that g has *infinite order*. [Hint: For each integer $k \in \mathbb{Z}$ there exist **unique** integers $q, r \in \mathbb{Z}$ satisfyiing $k = qm + r$ and $0 \leq r < m$.]

(a): Let $\langle g\rangle \subseteq G$ be the smallest subgroup of G that contains the element g. Let $P = \{g^n : n \in \mathbb{Z}\}$ be the set of integer powers of g. I claim that $\langle g\rangle = P$.

To see this we must prove that $\langle g\rangle \subseteq P$ and $P \subseteq \langle g\rangle$. For the first statement, we observe that P is a subgroup of G since for any two powers $g^m, g^n \in P$ we also have[1]

$$g^m * (g^n)^{-1} = g^m * g^{-n} = g^{m-n} \in P.$$

Then since P is a subgroup of G containing $g = g^1$, it must contain the smallest such subgroup. That is, we must have $\langle g\rangle \subseteq P$.

Conversely, we must show that every power of g is in $\langle g\rangle$. Since $\langle g\rangle$ is by definition a subgroup that contains g we must have $\varepsilon = g^0 \in \langle g\rangle$ and $g^1 = g \in \langle g\rangle$. Now assume for induction that $g^n \in \langle g\rangle$. Since $g \in \langle g\rangle$ and since $\langle g\rangle$ is closed under $*$, this implies that $g^{n+1} = g^n * g \in \langle g\rangle$. Hence $g^n \in \langle g\rangle$ for all integers $n \geq 0$. Finally, since $\langle g\rangle$ is closed under inversion, we have $g^{-n} = (g^n)^{-1} \in \langle g\rangle$ for all $n \geq 0$. In conclusion, we have $P \subseteq \langle g\rangle$.

(b): Suppose that $\langle g\rangle$ is a finite set. From part (a) this means that the list of powers

$$\ldots, g^{-2}, g^{-1}, \varepsilon, g, g^2, \ldots$$

contains some repetition. That is, we must have $g^k = g^\ell$ for some integers $k < \ell$. Multiplying both sides of this equation by the inverse element $(g^k)^{-1} = g^{-k}$ gives

$$\begin{aligned} g^\ell &= g^k \\ g^\ell * g^{-k} &= g^k * g^{-k} \\ g^{\ell-k} &= \varepsilon, \end{aligned}$$

with $\ell - k \geq 1$.

(c): Let $\langle g\rangle$ be finite. Then from part (b) there exists a **smallest positive integer** m satisfying $g^m = \varepsilon$. In this case I claim that that the m group elements $\varepsilon, g, \ldots, g^{m-1}$ are distinct and that every element of $\langle g\rangle$ is in this list. To see that every element of $\langle g\rangle$ has the form g^r for some $0 \leq r < m$, we consider an arbitrary integer power g^n. Then there exists a quotient and remainder $q, r \in \mathbb{Z}$ such that

$$\begin{cases} n = qm + r, \\ 0 \leq r < m. \end{cases}$$

In this case we have

$$g^n = g^{r+qm} = g^r * g^{qm} = g^r * (g^m)^q = g^r * \varepsilon^q = g^r.$$

To see that the list $\varepsilon, g, \ldots, g^{m-1}$ contains no repetition, suppose for contradiction that we have $g^k = g^\ell$ for some integers $0 \leq k < \ell \leq m-1$. But then multiplying both sides by g^{-k} gives $g^{\ell-k} = \varepsilon$ with $1 \leq \ell - k < m$, **contradicting the minimality of** m.

[1] The identity $(g^m)^n = g^{mn}$ holds any integers m, n. This can be proved by induction.

5. Join of Two Subgroups. Let G be a group and let $H, K \subseteq G$ be subgroups. Recall that the subgroup generated by the union $H \cup K$ is called the *join*:

$$\begin{aligned} H \vee K &:= \langle H \cup K \rangle \\ &:= \text{ the intersection of all subgroups that contain } H \cup K. \end{aligned}$$

(a) If $(G, +, 0)$ is abelian, we define the *sum* of H and K as follows:

$$H + K := \{h + k : h \in H, k \in K\}.$$

Prove that this is a subgroup.

(b) If $(G, +, 0)$ is abelian, use part (a) to prove that $H \vee K = H + K$.

(c) If $(G, *, \varepsilon)$ is non-abelian, show that the following set is **not** necessarily a subgroup, and hence it does not coincide with the join:

$$H * K := \{h * k : h \in H, k \in K\}.$$

[Hint: The smallest non-abelian group is S_3.]

(a): Let $(G, +, 0)$ be abelian and let $H, K \subseteq G$ be subgroups. I claim that the set $H + K = \{h + k : h \in H, k \in K\}$ is also a subgroup. To see this, consider any two elements $h_1 + k_1$ and $h_2 + k_2$ of $H + K$. Since H is a subgroup we have $h_1 - h_2 \in H$ and since K is a subgroup we have $k_1 - k_2 \in K$. Finally, since the operation $+$ is commutative, we have $k_1 - h_2 = -h_2 + k_1$ and hence

$$(h_1 + k_1) - (h_2 + k_2) = (h_1 - h_2) + (k_1 - k_2) \in H + K.$$

(b): Continuing from part (a), let $H \vee K$ be the smallest subgroup of G that contains the set $H \cup K$. I claim that $H \vee K = H + K$. On the one hand, we know from (a) that $H + K$ is a subgroup of G. And we know that $H + K$ contains all elements of the form $h = h + 0$ and $k = 0 + k$ for $h \in H$ and $k \in K$. Hence $H + K$ contains the set $H \cup K$. By minimality it follows that $H \vee K \subseteq H + K$.

Conversely, we must show that $H + K \subseteq H \vee K$. To see this, note that for all elements $h \in H$ and $k \in K$ we have $h \in H \vee K$ and $k \in H \vee K$ because $H \vee K$ contains the set $H \cup K$. Furthermore, since $H \vee K$ closed under addition we must have $h + k \in H \vee K$. Hence every element of $H + K$ is in $H \vee K$.

(c): Consider the symmetric group $S_3 = \{\varepsilon, (12), (13), (23), (123), (132)\}$ and the (cyclic) subgroups $H = \{\varepsilon, (12)\}$ and $K = \{\varepsilon, (23)\}$. By definition we have[2]

$$\begin{aligned} H \circ K &= \{\varepsilon \circ \varepsilon, (12) \circ \varepsilon, \varepsilon \circ (23), (12) \circ (23)\} \\ &= \{\varepsilon, (12), (23), (123)\}. \end{aligned}$$

But this set is **not** a subgroup of S_3. Indeed, the inverse $(123)^{-1} = (132)$ is not in the set. Since $H \vee K$ is by definition a subgroup of S_3, it follows that $H \circ K \neq H \vee K$. (In this case, $H \vee K$ is the whole group.)

6. Two Groups with Eight Elements. There are two different non-abelian groups with eight elements, called the *dihedral group* D_8 and the *quaternion group* Q_8. We will use multiplicative notation with identity element called "1".

[2] In this case the group operation $*$ is functional composition.

(a) The dihedral group has elements $D_8 = \{1, r, r^2, r^3, f, rf, r^2f, r^3f\}$ subject to the relations

$$r^4 = f^2 = rfrf = 1.$$

Write out the full 8×8 group table.

(b) The quaternion group has elements $Q_8 = \{1, i, j, k, e, ei, ej, ek\}$ subject to the relations

$$i^2 = j^2 = k^2 = ijk = e, \quad e^2 = 1, \quad \text{and} \quad ae = ea \text{ for all } a \in Q_8.$$

Write out the full 8×8 group table. [If you want you can write e as "-1" and write the elements ei, ej, ek as $-i, -j, -k$, respectively.]

(c) Prove that D_8 and Q_8 are **not isomorphic**. [Hint: Isomorphic groups have the same number of elements of each order. Count the elements of order 2.]

(a): Here is the group table of D_8:

$\cdot$	1	r	r^2	r^3	f	rf	r^2f	r^3f
1	1	r	r^2	r^3	f	rf	r^2f	r^3f
r	r	r^2	r^3	1	rf	r^2f	r^3f	f
r^2	r^2	r^3	1	r	r^2f	f^3f	f	rf
r^3	r^3	1	r	r^2	r^3f	f	rf	r^2f
f	f	r^3f	r^2f	rf	1	r^3	r^2	r
rf	rf	f	r^3f	r^2f	r	1	r^3	r^2
r^2f	r^2f	rf	f	r^3f	r^2	r	1	r^3
r^3f	r^3f	r^2f	rf	f	r^3	r^2	r	1

(b): Here is the group table of Q_3:

$\cdot$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

(c): To show that D_8 and Q_8 are not isomorphic we will look at the orders of their elements.[3] Here are the orders of the elements of D_8:

g	1	r	r^2	r^3	f	rf	r^2f	r^3f
$\#\langle g\rangle$	1	4	2	4	2	2	2	2

And here are the orders of the elements of Q_8:

g	1	i	j	k	-1	$-i$	$-j$	$-k$
$\#\langle g\rangle$	1	4	4	4	2	4	4	4

The group D_8 has five elements of order 2 but the group Q_8 has just one element of order 2, hence these groups cannot be isomorphic.

[3] If $\varphi : G \to H$ is a group isomorphism then $g \in G$ and $\varphi(g) \in H$ have the same order because $\varphi(g^n) = \varphi(g)^n$ for all $n \in \mathbb{Z}$ and $\varphi(a) = \varepsilon_H$ if and only if $a = \varepsilon_G$.