Math 31 – Homework 4 Solutions

1. Determine whether each of the following subsets is a subgroup of the given group. If not, state which of the subgroup axioms fails.

(a) The set of real numbers $\mathbb{R}$, viewed as a subset of the complex numbers $\mathbb{C}$ (under addition).

(b) The set $\pi\mathbb{Q}$ of rational multiples of π, as a subset of $\mathbb{R}$ (under addition).

(c) The set of $n \times n$ matrices with determinant 2, as a subset of $\mathrm{GL_n}(\mathbb{R})$.

(d) The set $\{i, m_1, m_2, m_3\} \subset D_3$ of reflections of the equilateral triangle, along with the identity transformation.

Solution. (a) Yes, $\mathbb{R}$ is a subgroup of $\mathbb{C}$. The sum of any two real numbers is real, $0 \in \mathbb{R}$, and if $a \in \mathbb{R}$, then $-a \in \mathbb{R}$.

(b) Yes, $\pi\mathbb{Q}$ is a subgroup of $\mathbb{R}$ under addition. The verification is almost identical to the argument that we gave in class to show that $\mathbb{Q}$ is a subgroup of $\mathbb{R}$.

(c) No, this set is not a subgroup of $\mathrm{GL_n}(\mathbb{R})$, since it is not closed. If A and B both have determinant 2, then $\det(AB) = 4$, so $AB \in \mathrm{GL_n}(\mathbb{R})$. It is also easy to see that this set does not contain the identity matrix, and that none of its elements possess inverses within the set.

(d) No, this is not a subgroup of D_3. It contains the identity by definition, and each element is its own inverse, but the set is not closed. For example, we saw that $m_1 m_2 = r_1$.

2. We proved in class that every subgroup of a cyclic group is cyclic. The following statement is almost the converse of this:

"Let G be a group. If every *proper* subgroup of G is cyclic, then G is cyclic."

Find a counterexample to the above statement.

Proof. We actually mentioned in class that the Klein 4-group, V_4, is a counterexample. All of its proper subgroups are cyclic, but V_4 is not itself cyclic. Another example would be the dihedral group D_3. Every proper subgroup has order 1, 2, or 3, and is thus cyclic. However, D_3 is not cyclic. (It is not even abelian.)

3. [Saracino, #5.10] Prove that any subgroup of an abelian group is abelian.

Proof. Let G be an abelian group, and suppose that $H \leq G$. We need to check that for any $a, b \in H$, we have $ab = ba$. Well, $a, b \in H \subseteq G$, so

$$ab = ba,$$

since G is abelian. Therefore, H is abelian as well. $\square$

4. [Saracino, #5.14] Let G be a group. If H and K are subgroups of G, show that $H \cap K$ is also a subgroup of G.

Proof. Suppose that $a, b \in H \cap K$. Then $a, b \in H$, so $ab \in H$ since H is a subgroup. Similarly, $a, b \in K$, so $ab \in K$. Then $ab \in H \cap K$, so $H \cap K$ is closed. Since H and K are both subgroups, $e \in H$ and $e \in K$, hence $e \in H \cap K$. Finally, if $a \in H \cap K$, then $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$. Therefore, $H \cap K \leq G$.

Alternatively, we could use the subgroup criterion that we proved in class. Suppose that $a, b \in H \cap K$. Then $ab^{-1} \in H$ and $ab^{-1} \in K$, since H and K are both subgroups, so $ab^{-1} \in H \cap K$. Since a and b are arbitrary elements of $H \cap K$, it follows that $H \cap K \leq G$ by the subgroup criterion. $\square$

5. Let r and s be positive integers, and define

$$H = \{nr + ms : n, m \in \mathbb{Z}\}.$$

(a) Show that H is a subgroup of $\mathbb{Z}$.

(b) We saw in class that every subgroup of $\mathbb{Z}$ is cyclic. Therefore, $H = \langle d \rangle$ for some $d \in \mathbb{Z}$. What is this integer d? Prove that the d you've found is in fact a generator for H.

Proof. (a) We can verify directly that $H \leq \mathbb{Z}$. If $nr + ms, nt + mu \in H$, then

$$(nr + ms) + (nt + mu) = n(r + t) + m(s + u),$$

which is again in H. Thus H is closed. Also, $0 = n \cdot 0 + m \cdot 0 \in H$, and if $nr + ms \in H$, then

$$-(nr + ms) = n(-r) + m(-s) \in H,$$

so H is indeed a subgroup of $\mathbb{Z}$.

(b) We claim that H is generated by $d = \gcd(n, m)$. To prove this, we need to check that $H = \langle d \rangle$. First, note that since $d \mid n$ and $d \mid m$, $d \mid nr + ms$ for any $r, s \in \mathbb{Z}$. That is, any element of H is a multiple of d, so

$$H \subset \langle d \rangle = d\mathbb{Z}.$$

We also need to check that $d\mathbb{Z} \subset H$, and it is enough to show that $d \in H$. (Remember that any subgroup containing d must also contain the cyclic subgroup that it generates.) For this, we just need to remember Bézout's lemma/Extended Euclidean algorithm, which says that there are integers $x, y \in \mathbb{Z}$ such that

$$nx + my = \gcd(n, m) = d.$$

Therefore, $d \in H$, so $H = d\mathbb{Z}$. $\square$

6. Let X be a set, and recall that S_X is the group consisting of the bijections from S to itself, with the binary operation given by composition of functions. (If X is finite, then S_X is just the symmetric group on n letters, where X has n elements.) Given $x_1 \in X$, define

$$H = \{f \in S_X : f(x_1) = x_1\}.$$

Show that $H \leq S_X$.

Proof. First note that the identity function $i \in S_X$ belongs to H, since $i(x) = x$ for all $x \in X$. Also, if $f, g \in H$, then

$$f \circ g(x_1) = f(g(x_1)) = f(x_1) = x_1,$$

since f and g both fix x_1. Therefore, $f \circ g \in H$, so H is closed under composition. Finally, if $f \in S_X$, then

$$f^{-1}(x_1) = f^{-1}(f(x_1)) = i(x_1) = x_1,$$

since $f(x_1) = x_1$. Therefore, $f^{-1} \in H$, and H is a subgroup of S_X. (This subgroup is called the **stabilizer** of x_1.) $\square$

7. [Saracino, #5.22] Let G be a group. Define

$$Z(G) = \{a \in G : ax = xa \text{ for all } x \in G\}.$$

In other words, the elements of $Z(G)$ are exactly those which commute with *every* element of G. Prove that $Z(G)$ is a subgroup of G, called the **center** of G.

Proof. Suppose that $a, b \in Z(G)$. Then $ax = xa$ and $bx = xb$ for all $x \in G$, and for any $x \in G$ we have

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab),$$

so $ab \in Z(G)$. Therefore, $Z(G)$ is closed. Also, we certainly have $ex = xe = x$ for all $x \in G$, so $e \in Z(G)$. Finally, if $a \in Z(G)$, then

$$a^{-1}x = ((a^{-1}x)^{-1})^{-1} = (x^{-1}a)^{-1} = (ax^{-1})^{-1},$$

since a commutes with every element of G. Continuing, we have

$$(ax^{-1})^{-1} = xa^{-1},$$

so $a^{-1}x = xa^{-1}$, and $a^{-1} \in Z(G)$. Therefore, $Z(G)$ is a subgroup of G. $\square$

8. Show that if H and K are subgroups of an *abelian* group G, then

$$\{hk : h \in H \text{ and } k \in K\}$$

is a subgroup of G.

Proof. Define

$$HK = \{hk : h \in H \text{ and } k \in K\}.$$

Let $a, b \in HK$. Then $a = h_1k_1$ and $b = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Now we have

$$ab = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2),$$

where we have used the fact that G is abelian to interchange h_2 and k_1. Since $H \leq G$, $h_1h_2 \in H$, and similarly, $k_1k_2 \in K$, so $ab \in HK$. Therefore, HK is closed. Since H and K are both subgroups of G, $e \in H$ and $e \in K$, so $e = ee \in HK$. Finally, suppose that $a = hk \in HK$. Then

$$a^{-1} = (hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1},$$

again since G is abelian. Since $h^{-1} \in H$ and $k^{-1} \in K$, $a^{-1} \in HK$. Therefore, $HK \leq G$.

Note that the fact that G is abelian is crucial here. The result is not true in general for nonabelian groups. $\square$

9. [Saracino, #5.20] We will see in class that if p is a prime number, then the cyclic group $\mathbb{Z}_p$ has no proper subgroups as a consequence of Lagrange's theorem. This problem will have you investigate a "converse" to this result.

(a) If G is a finite group which has no proper subgroups (other than $\{e\}$), prove that G must be cyclic.

(b) Extend the result of (a) by showing that if G has no proper subgroups, then G is not only cyclic, but

$$|G| = p$$

for some prime number p.

Proof. (a) Suppose that G has no proper subgroups. If $G = \{e\}$, then G is cyclic, so let's assume that G contains more than one element. Let $a \in G$ with $a \neq e$. Then $|a| > 1$, and a generates a subgroup $\langle a \rangle$ of G with order greater than 1. But G contains no proper subgroups, so we must have $\langle a \rangle = G$. That is, a generates G, and G is cyclic.

(b) We have already established that G is cyclic, so we simply need to prove that G has prime order. We saw in class that the subgroups of any finite cyclic group correspond exactly to the divisors of $|G|$. Since G has no proper subgroups other than e, $|G|$ cannot have any proper divisors. In other words, $|G|$ is prime. $\square$

Hard

10. [Saracino, #5.25 and 5.26] Let G be a group, and let H be a subgroup of G.

(a) Let a be some fixed element of G, and define

$$aHa^{-1} = \{aha^{-1} : h \in H\}.$$

This set is called the **conjugate** of H by a. Prove that aHa^{-1} is a subgroup of G.

(b) Define the **normalizer** of H in G to be

$$N(H) = \{a \in G : aHa^{-1} = H\}.$$

Prove that $N(H)$ is a subgroup of G.

Proof. To prove (a), we'll use the subgroup criterion. Let $x, y \in aHa^{-1}$. We will show that $xy^{-1} \in aHa^{-1}$. We have $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$ for some $h_1, h_2 \in H$, so

$$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1}.$$

Since H is a subgroup, $h_1h_2 \in H$, and it follows that $ah_1h_2a^{-1} \in aHa^{-1}$. That is, $xy^{-1} \in aHa^{-1}$, so aHa^{-1} is a subgroup of G.

(b) Clearly the identity element of G belongs to $N(H)$, since

$$eHe^{-1} = \{ehe^{-1} : h \in H\} = \{h : h \in H\} = H.$$

Now let $a \in N(H)$. We will show that $a^{-1} \in N(H)$ as well. First observe that if $h \in H$, then we can write

$$h = aka^{-1}$$

for some $k \in H$, since $aHa^{-1} = H$. Then

$$a^{-1}ha = a^{-1}(aka^{-1})a = k,$$

which belongs to H. Therefore, $a^{-1}Ha \subseteq H$. On the other hand, suppose that $h \in H$. Then we have

$$h = (a^{-1}a)h(a^{-1}a) = a^{-1}(aha^{-1})a.$$

But $aha^{-1} \in H$, so it follows that $h \in a^{-1}Ha$. Thus $H \subseteq a^{-1}Ha$, so $a^{-1} \in N(H)$.

Finally, suppose that $a, b \in N(H)$, so $aHa^{-1} = H$ and $bHb^{-1} = H$. Then for any $h \in H$, we have

$$(ab)h(ab)^{-1} = abhb^{-1}a^{-1} = a(bhb^{-1})a^{-1}.$$

Since $b \in N(H)$, $bhb^{-1} \in H$. Moreover, $a \in N(H)$, so $a(bhb^{-1})a^{-1} \in H$. Therefore, $(ab)H(ab)^{-1} \subseteq H$. On the other hand, we need to show that $H \subseteq (ab)H(ab)^{-1}$ as well. Well, if $h \in H$, then $h = ak_1a^{-1}$ for some $k \in H$, since $aHa^{-1} = H$. Similarly, we can write $k_1 = bk_2b^{-1}$ for some $k_2 \in H$, since $b \in N(H)$. Therefore,

$$h = ak_1a^{-1} = a(bk_2b^{-1})a^{-1} = (ab)k_2(ab)^{-1},$$

so $h \in (ab)H(ab)^{-1}$. Thus $H \subseteq (ab)H(ab)^{-1}$, and $ab \in N(H)$. It follows that $N(H) \leq G$. $\square$