Homework Assignment 4

Due Friday, February 19

1. Let G be a group and H a *nonempty* subset of G. Let's introduce a few tricks to speed up testing if something is a subgroup.

   (a) *(Subgroup Criterion)* Suppose that for all $x, y \in H$, $xy^{-1} \in H$. Show that H is a subgroup of G.

   Proof. H is nonempty be assumption. Suppose $x \in H$. Then by assumption $xx^{-1} = 1 \in H$. Since $1, x \in H$, then $1x^{-1} = x^{-1} \in H$, so H is closed under inversion. Now fix $x, y \in H$. We have already seen H is closed under inversion so that $x, y^{-1} \in H$, and thus $x(y^{-1})^{-1} = xy \in H$. Therefore H is closed under multiplication so we win. □

   (b) *(Finite Subgroup Criterion)* Show that if H is finite and closed under multiplication, then H is a subgroup of G.

   Proof. H is nonempty and closed under multiplication by assumption. All that remains is to show it is closed under inversion. Since H is closed under multiplication, we know that the set $\{x, x^2, x^3, x^4, \cdots\} \subseteq H$. Since H is finite, we know that the list of powers of x cannot go on forever without repeating (else we would be exhibiting infinitely many different elements of H). Therefore there is some $i < j$ with $x^i = x^j$. In particular, $x^{j-i} = 1$, and $x^{-1} = x^{j-i-1} \in \{x, x^2, x^3, \cdots\} \subseteq H$, and therefore H is closed under inversion. (To be completely precise, one could also have $j - i - 1 = 0$, but then $x^{-1} = 1 = x \in H$ so we're ok.) □

   (c) Suppose now that H is a subgroup of G, and that K is another subgroup of G. Show that if $K \subseteq H$, then $K \leq H$.

   Proof. This is immediate, since K nonempty and closed under multiplication and inversion under the binary operation of G, and H has the same binary operation. □

2. Let G be a group. Let $H, K \leq G$ be two subgroups.

   (a) Show that the intersection $H \cap K$ is a subgroup of G.

   Proof. We first must show $H \cap K$ is nonempty, but as H and K are both subgroups, they both contain 1, and therefore so does $H \cap K$. Next we must show that $H \cap K$ has inverses, so fix an member x. As x is in the subgroup H, so is x^{-1}, and we can similarly argue that $x^{-1} \in K$ as well. Therefore $x^{-1} \in H \cap K$. Finally we must show that if $x, y \in H \cap K$, then so is xy. But $x, y \in H$ implies xy is also because H is a subgroup, and similarly $xy \in K$. Therefore $xy \in H \cap K$, completing the proof. □

   (b) Give an example to show that the union $H \cup K$ need not be a subgroup of G.

   Proof. The even numbers $2\mathbb{Z} = \{\cdots, -4, -2, 0, 2, 4, 6, \cdots\} \leq \mathbb{Z}$ and the multiples of three $3\mathbb{Z} = \{\cdots, -6, -3, 0, 3, 6, 9\} \leq \mathbb{Z}$ are both subgroups of the integers. Their union $2\mathbb{Z} \cup 3\mathbb{Z}$ consists of integers which are either even or mutliples of 3. Thus it contains both 2 and 3. But their sum $2 + 3 = 5$ is not even or a multiple of 3, thus is not in the union. Therefore the union isn't closed under addition, and therefore is not a subgroup. □

(c) Show that $H \cup K$ is a subgroup of G if and only if $H \subset K$ or $K \subset H$.

Proof. If $H \subset K$, then $H \cup K = K$ is a subgroup, and if $K \subset H$ the proof is identical. Conversely, suppose that $H \cup K$ is a subgroup. Suppose for the sake of contradiciton that neither of H or K is contained in the other, so that we can find $h \in H \setminus K$ and $k \in K \setminus H$. As $H \cup K$ is a subgroup that $hk \in H \cup K$, so (without loss of generality) we may assume that $hk \in H$. But then mutliplying by h^{-1} on the left, we have $k \in H$, contrary to our assumption. □

(d) Adjust your proof from part (a) to show that the intersection of an arbitrary collection of subgroups is a subgroup. That is, let $\mathcal{A}$ be a collection of subgroups of G. Show that

$$\bigcap_{H \in \mathcal{A}} H$$

is a subgroup of G. This completes the proof that the subgroup generated by a subset is in fact a subgroup.

Hint. *For part (d), the proof should be very similar to part (a), with only cosmetic modifications. You won't need to use induction. In fact, since $\mathcal{A}$ is could in principle be uncountable, induction won't work without modifications (think about why this is).*

Proof. We first must show $\mathbb{H} = \bigcap_{H \in \mathcal{A}} H$ is nonempty, but since $1 \in H$ for all H, 1 is in their intersection. Next we must show that $\mathbb{H}$ has inverses, so fix an member x. As x is in each $H \in \mathcal{A}$, so is x^{-1}, so that x^{-1} is in the intersection and thus in $\mathbb{H}$. Finally we must show that if $x, y \in \mathbb{H}$, then so is xy. But for each H we know $x, y \in H$, so that $xy \in H$ as well. Since this holds for each H, xy is in the intersection, which is $\mathbb{H}$. □

3. Let G be a group, and let A be a subset of G. Let's establish some facts about centralizers and normalizers.

(a) Let A be a subset of G. Prove that $N_G(A) \leq G$.

Proof. First notice $1A1^{-1} = A$ so that $N_G(A)$ is nonempty. Suppose x normalizes A. Then $xAx^{-1} = A$. Multiplying on the right by x and on the left by x^{-1} we see that $A = x^{-1}Ax$ so that x^{-1} normalizes A. Now let $x, y \in N_G(A)$. Then:

$$xyA(xy)^{-1} = xyAy^{-1}x^{-1} = xAx^{=1} = A.$$

Thus $xy \in N_G(A)$ so $N_G(A)$ is closed under products and we win. □

(b) Deduce the following chain of inclusions.

$$Z(G) \leq C_G(A) \leq N_G(A) \leq G.$$

Proof. Since these are all subgroups of G, by 1(c) we need only show the containments and the fact that they are subgroups comes for free. Let $x \in Z(G)$. If $a \in A$ then $xa = ax$ (since this holds for any element of G), so $x \in C_G(A)$. This shows the first containment. For the second, fix $y \in C_G(A)$. For every $a \in A$, we have $yay^{-1} = a$, so that $yAy^{-1} = A$. Thus $y \in N_G(A)$, proving the second containment.. The final containment is trivial. □

(c) Show that $C_G(A) = C_G(\langle A \rangle)$.

Proof. Notice that if $x \in C_G(\langle A \rangle)$ then $xa = ax$ for all $a \in A$, so the right side is automatically contained in the left. The reverse containment remains

We first show that if x and a commute, then x and a^{-1} do. Indeed, consider $xa = ax$. Multiplying on the right and left by a^{-1} gives the equation $a^{-1}x = xa^{-1}$, as desired. In particular, we see that if $x \in C_G(A)$ and $a \in A$, then $xa^\varepsilon = a^\varepsilon x$ for $\varepsilon = \pm 1$.

Let $a = a_1^{\varepsilon 1} a_2^{\varepsilon^2} \cdots a_n^{\varepsilon_n}$ be an arbirary element of $\langle A \rangle$ (where $a_i \in A$ and $\varepsilon_i = \pm 1$). We hope to show $xa = ax$. We proceed by induction on n. The case $n = 1$ was proved in the previous paragraph. For the general case we assume the analogous relation holds for all expressions of length $n - 1$. Then we compute:

$$ax = (a_1^{\varepsilon 1} a_2^{\varepsilon^2} \cdots a_{n-1}^{\varepsilon_{n-1}})a_n^{\varepsilon_n} x = (a_1^{\varepsilon 1} a_2^{\varepsilon^2} \cdots a_{n-1}^{\varepsilon_{n-1}})xa_n^{\varepsilon_n} = x(a_1^{\varepsilon 1} a_2^{\varepsilon^2} \cdots a_{n-1}^{\varepsilon_{n-1}})a_n^{\varepsilon_n} = xa.$$

This shows any element centralizing A centralizes the subgroup it generates, finishing the proof. □

(d) Give an example to show the analog of part (c) for normalizers is not true. That is, give $A \subseteq G$ where $N_G(A) \neq N_G(\langle A \rangle)$.

Proof. Let $G = D_{2n}$ for $n \geq 3$. Notice that if we conjugate r by s we get

$$srs^{-1} = r^{-1}ss^{-1} = r^{-1}.$$

Therefore let $A = \{r, s\}$ (just the two element set, not the subgroup they generate).

$$sAs^{-1} = \{srs^{-1}, sss^{-1}\} = \{r^{-1}, s\} \neq A.$$

Therefore $s \notin N_G(A)$. Of course, $\langle A \rangle = \langle r, s \rangle = G$, and $N_G(G) = G \ni s$, so this gives our example. (Notice this also gives an example where $A \not\subseteq N_G(A)$. The next exercise shows this can't happen if A is a subgroup). □

(e) Show that if H is a subgroup of G, then $H \leq N_G(H)$.

Proof. Recall that $N_G(H) = \{g \in G : gHg^{-1} = H\}$. Let $h \in H$. Then for every $x \in H$ we have $hxh^{-1} \in H$ as it is the product of three elements of H. Therefore (applying 7(b) below) $hHh^{-1} = H$, so h normalizes H. As $h \in H$ was arbitrary we have $H \subseteq N_G(H)$, so that $H \leq N_G(H)$ by 1(c). □

(f) Show that $H \leq C_G(H)$ if and only if H is abelian.

Proof. H centralizes H if and only if for all $x, y \in H$, $xy = yx$. This is precisely what it means for H to be abelian. □

4. Compute the center of the dihedral group. Explicitly, let n be an integer ≥ 3. Compute $Z(D_{2n})$. (Note: you will need to split into the two cases, where n is even or n is odd).

Proof. By 3(c), to see if an element $x \in D_{2n}$ is in the center, we need only check if multiplication commutes with r and with s, If $x = sr^i$ we have:

$$xr = sr^{i+1} \qquad \text{and} \qquad rx = rsr^i = sr^{i-1}.$$

Therefore if $xr = rx$ we deduce that $r^2 = 1$, but $n \geq 3$ so this equality does not hold. Therefore reflections are never in the center of D_{2n} If $x = r^i$ is a rotation then $xr = rx$. We next check how it commutes with s:

$$sx = sr^i \qquad \text{and} \qquad xs = sr^{-i}.$$

So if $xs = sx$ then we deduce $r^{2i} = 1$. As we may assume $0 \leq i < n$ we have $i = 0$ or $i = n/2$. Thus if n is even we have $Z(D_{2n}) = \{1, r^{n/2}\}$ and if n is odd we have $Z(D_{2n}) = \{1\}$ since we cannot take fractional powers of r. □

5. In this exercise we study products of finite cyclic groups. Recall that we denote by Z_n the cyclic group of order n (written multiplicatively).

   (a) Prove that $Z_2 \times Z_2$ is not a cyclic group.

   Proof. Notice that $|Z_2 \times Z_2| = 4$. Therefore if it were cyclic, it would need a generator x of order 4. But notice that if $x = (a, b)$ then $x^2 = (a^2, b^2) = (1, 1)$ since a, b have order ≤ 2 as elements of Z_2. Therefore $|x| \leq 2$ so x cannot generate the entire group. □

   (b) Prove that $Z_2 \times Z_3 \cong Z_6$. Conclude that $Z_2 \times Z_3$ is a cyclic group.

   Proof. For simplicity we use the identification $Z_n = \mathbb{Z}/n\mathbb{Z}$ and write additively. I claim $(\overline{1}, \overline{1})$ generates $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Indeed, since $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}| = 6$ it suffices to show that $|(\overline{1}, \overline{1})| = 6$. Suppose that for some $n > 0$ we have $n(\overline{1}, \overline{1}) = (\overline{n}, \overline{n}) = (0, 0)$. This implies that $2|n$ and that $3|n$. In particular we have $6|n$. Thus the smallest n can be is 6. As $(\overline{6}, \overline{6}) = (0, 0)$ we have $|(\overline{1}, \overline{1})| = 6$ completing the proof. □

   Those two examples really cover all the bases. Use the intuition you gained from them to prove the following classification result.

   (c) Show that $Z_n \times Z_m$ is cyclic if and only if $\gcd(n, m) = 1$. (Hint: recall that up to isomorphism there is only one cyclic group of order N for every positive integer N).

   Proof. The real heavy lifting here is done because $\gcd(m, n) = 1$ if and only if $\text{lcm}(m, n) = mn$. I will state and prove this here as a lemma, but it is rather well known and elementary so I am ok with it being used without proof.

   Lemma 1. *Let $a, b \in \mathbb{Z}$ be positive integers. then*

   $$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

   In particular, $\gcd(a, b) = 1$ *if and only if* $\text{lcm}(a, b) = ab$.

Proof. By the fundamental theorem of arithmetic we have prime factorizations

$$\begin{aligned} a &= p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n} \\ b &= p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}, \end{aligned}$$

where we allow α_i or β_i to be 0 so that the p_i are the same. Then it is clear that,

$$\begin{aligned} \gcd(a,b) &= p_1^{\min(\alpha_1,\beta_1)}p_2^{\min(\alpha_2,\beta_2)}\cdots p_n^{\min(\alpha_n,\beta_n)} \\ \operatorname{lcm}(a,b) &= p_1^{\max(\alpha_1,\beta_1)}p_2^{\max(\alpha_2,\beta_2)}\cdots p_n^{\max(\alpha_n,\beta_n)}. \end{aligned}$$

Thus the product is

$$gcd(a,b)\cdot \operatorname{lcm}(a,b) = p_1^{\alpha_1+\beta_1}p_2^{\alpha_2+\beta_2}\cdots p_n^{\alpha_n+\beta_n} = ab,$$

and we win. □

With this in hand we can proof the classification result. As in part (b) we identify Z_n with $\mathbb{Z}/n\mathbb{Z}$ and write additively. First suppose that $\gcd(n,m) = 1$. Then $(\overline{1},\overline{1})$ is a generator for $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. Indeed, if $a > 0$ and

$$a(\overline{1},\overline{1}) = (\overline{a},\overline{a}) = (0,0)$$

then $n|a$ and $m|a$, so that $\operatorname{lcm}(m,n) = mn$ divides a. Thus

$$|(\overline{1},\overline{1})| = mn = |\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}|,$$

so $(\overline{1},\overline{1})$ generates the group and so it is cyclic of order mn.

Conversely, suppose that $\gcd(n,m)\neq 1$. Then $l = \operatorname{lcm}(m,n) < mn$. Therefore for any $(\overline{a},\overline{b})\in\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$, we have $l(\overline{a},\overline{b}) = (\overline{la},\overline{lb}) = (0,0)$ so that $|(\overline{a},\overline{b})|\leq l < mn$ and it cannot be a generator. Therefore $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ cannot be cyclic. □

6. For $n\geq 2$ let $G = S_n$ be the symmetric group equipped with it's natural action on $\Omega_n = \{1,2,\cdots,n\}$ by permutations. For $i\in\Omega_n$, let $G_i = \{\sigma\in G|\sigma(i) = i\}$ be the stabilizer of i. Describe an isomorphism between G_i and S_{n-1}.

   Proof. Reording the elements of Ω_n, we may assume that $i = n$. Then an element of G_n is just a permutation of $1,2,\cdots,n-1$, keeping n fixed. In particular, this gives an action on $\{1,\cdots,n-1\}$ which int turn gives a permutation representation $G_n\to S_{n-1}$. It is surjective as any permutation of $1,\cdots,n-1$ can be extended to a permutation of $1,\cdots,n$ keeping n fixed, and it is injective because $\sigma\in G_n$ automatically fixes n, if it it fixes $1,\cdots,n-1$, it must be the identity permutation. □

7. In this problem we will introduce the following very important class of subgroups. A subgroup $H\leq G$ is called *normal* if $N_G(H) = G$. Recall that this means, for $x\in G$, the set $xHx^{-1} = H$. If H is a normal subgroup, we write $H\trianglelefteq G$.

   (a) Let H be a subgroup, and $x\in G$. Give a bijection between H and xHx^{-1}.

Proof. Define a function $\varphi : H \to xHx^{-1}$ which takes $h \mapsto xhx^{-1}$. This has the obvious inverse $\varphi^{-1} : xHx^{-1} \to H$ given by $h' \mapsto x^{-1}h'x$. To see that this lands in the right place, if $h' \in xHx^{-1}$, then $h' = xhx^{-1}$ for some $h \in H$. Thus

$$\varphi^{-1}h' = x^{-1}(xhx^{-1})x = h \in H.$$

□

(b) Part (a) makes it easy to check if something is normal. In particular, suppose that for every $h \in H$, the element $xhx^{-1} \in H$ for every $x \in G$. Show that H is normal.

Proof. (I didn't end up using (a), seems easier to do directly). By assumption, $xHx^{-1} \subseteq H$. Given $h \in H$, $x^{-1}hx \in H$ as well, so that $x(x^{-1}hx)x^{-1} \in xHx^{-1}$ so that $H \subseteq xHx^{-1}$. This shows $xHx^{-1} = H$ and so $x \in N_G(H)$. Since x was arbitrary $N_G(H) = G$ and so H is normal. □

(c) Let $\varphi : G \to G'$ be a homomorphism with kernel K. Show that K is a normal subgroup of G.

Proof. Fix $x \in G$. For any $k \in K$, we comptue:

$$\varphi(xkx^{-1}) = \varphi(x)\varphi(k)\varphi(x)^{-1} = \varphi(x)\varphi(x)^{-1} = 1.$$

Thus $xkx^{-1} \in K$. Since x was arbitrary, $K \trianglelefteq G$ by part (b). □

(d) Give an example of a subgroup that is not normal. Conclude that not every subgroup can be the kernel of some homomorphism.

Proof. Consider $\langle s \rangle \leq D_8$. Notice that $rsr^{-1} = sr^2 \notin \langle s \rangle$. This shows $r \notin N_{D_8}(\langle s \rangle)$, so that in particular $\langle s \rangle$ cannot be normal. If $\langle s \rangle$ were the kernel of some homomorphism, by part (c) it would have to be normal, so there is no homomorphism $\varphi D_8 \to H$ with kernel $\langle s \rangle$. □

8. Let's study the converse of the previous question. We will give an intrinsic definitnion of quotient groups along the way. A lot of this problem is covered in class (with some details for you to fill in), but I think it is very important to work through these constructions carefully for yourself. This should feel very similar to the construction of $\mathbb{Z}/n\mathbb{Z}$.

Recall the following definition from class: Let $K \leq G$ be a subgroup. For $x, y \in G$ we say that x and y are congruent mod K, $x \equiv y \mod K$ if $y^{-1}x \in K$ (or equivalently if $x = yk$ for some $k \in K$).

(a) Show that congruence modulo K is an equivalence relation on G. Observe that the the equivalence classes of congruence mod K are the sets

$$xK = \{xk : k \in K\}.$$

We call these the *cosets* of K.

Proof. First we notice that it is reflexive. Indeed, $xx^{-1} = 1 \in K$. Now suppose $x \equiv y$, so that $x = yk$ for some $k \in K$. Then $y = xk^{-1}$ and $k^{-1} \in K$, so that $y \equiv x$. Finally, suppose $x \equiv y$ and $y \equiv z$. Then $xy^{-1}, yz^{-1} \in K$ so their product $xy^{-1}yz^{-1} = xz^{-1} \in K$, and thus $x \equiv z$.

The equivalence classes are the cosets xK essentially by definition. But it is worth explicitly pointing out that this means that $y \in xK$ if and only if $xK = yK$. This isn't too hard to compute directly (indeed, it is essentially what we did in the previous paragraph), but it is an immediate consequence of the fact that these sets form a partition of G. □

(b) Suppose $K \trianglelefteq G$. If $x \equiv x_1 \mod K$ and $y \equiv y_1 \mod K$, show $xy \equiv x_1y_1 \mod K$. (You will need normality here. Be careful not to assume your group is abelian).

Proof. We use that $xx_1^{-1}, yy_1^{-1} \in K$. Say $yy_1^{-1} = k$ and $xx_1^{-1} = \ell$ for $k, \ell \in K$. We then compute:

$$xy(x_1y_1)^{-1} = xyy_1^{-1}x_1 = xkx_1^{-1} = x_1\ell kx_1^{-1} \in K,$$

since ℓk is in K which is normal, so when we conjugate it by x_1 it remains in K.

Alternatively, one could use the characterization that $x \equiv x_1$ if and only if $xK = x_1K$ (and similarly for y), and that we proved in class that if K is normal, $gK = Kg$ for all g. Then observe that:

$$x_1y_1K = x_1y_1KK = x_1Ky_1K = xKyK = xyKK = xyK.$$

□

(c) Define G/K to be the set of cosets of K.

$$G/K = \{xK : x \in G\}.$$

If K is normal, show that the operation $(xK)(yK) = xyK$ is a well defined binary operation making G/K into a group. What is the identity element? (Note: You already did the work to show it's well defined.)

Proof. The multiplication operation is well defined by part (c). To be completely explicit (perhaps moreso than necessary), if $x_1K = xK$ and $y_1K = yK$, then $x_1 \equiv x$ and $y_1 \equiv y$, so that $x_1y_1 \equiv xy$ so that $x_1y_1K = xyK$.

Since multiplication is computed using the group law of G, we immediately get that $1K$ is the identity, that $(xK)^{-1} = x^{-1}K$, and that associativity holds. □

(d) Suppose K is a normal subgroup. Let $\pi : G \to G/K$ be the map $x \mapsto xK$. Show that π is a group homomorphisms with kernel K. This is often called *the natural projection.*

Proof. Notice that:

$$\pi(x)\pi(y) = (xK)(yK) = xyK = \pi(xy),$$

so we get that it is a homomorphism. It is surjective because any coset is the image of any representative: $xK = \pi(x)$. Finally, $\pi(x) = 1$ if and only if $xK = 1K$, if and only if $x \in K$ (applying part (a), or noticing that $x = 1k$ for some $k \in K$). This implies that $\ker \pi = 1$ and we win. □

(e) Suppose that G/K is a group under the operation described in part (c). Show that K must be normal (*Hint:* Rather than trying to explicitly compute things with elements, use the then natural projection together with 7(c)).

Proof. Notice that the only place we used where K was normal in part (d) was in applying part (c) to know that G/K is a group. In particular, if we assume G/K is a group, the same argument goes through and so $\pi : G \to G/K$ is a homomorphism with kernel K. Since K is the kernel of a homomorphism, it is normal by 7(c). □

(f) Putting everything together, conclude the following are equivalent for a subgroup $K \leq G$.

(i) K is normal in G.

(ii) K is the kernel of a homomorphism.

(iii) G/K is a group.

Hint. *You've already done all the work for this. Each implication should be easily accessible appealing to something proven in question 7 or 8.*

Proof. We've done it all already:
(i)$\Longrightarrow$(ii) is 8(d).
(ii)$\Longrightarrow$(i) is 7(c).
(i)$\Longrightarrow$(iii) is 8(c).
(iii)$\Longrightarrow$(i) is 8(e).
Therefore we see (ii)$\Leftrightarrow$(i)$\Leftrightarrow$(iii) and we win. □