Homework Assignment 6 Solutions

1. 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 $C_G(A) \leq G$.

   Proof. In this an what follows we will freely use that the $x \in C_G(A)$ if and only if $xa = ax$ for all $a \in A$. Then $1a = a1$ so $1 \in C_G(A)$ and it is nonempty. Furthermore, if $x, y \in C_G(A)$, then:

   $$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy),$$

   so that $xy \in C_G(A)$. Finally, if $x \in C_G(A)$ then $xa = ax$. Multiplying on the right *and* left by x^{-1} gives $ax^{-1} = x^{-1}a$ so that $x^{-1} \in C_G(A)$ completing the proof. □

   (b) Deduce the following chain of inclusions.

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

   (*Note:* In class we only defined the normalizer of a subgroup, but we can define the normalizer of a subset the same way: $N_G(A) = \{g \in G : gAg^{-1} = A\}$.)

   Proof. 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 will give two proofs of this fact, starting with a *slicker* one.

   Notice that for two subsets $S, T \subseteq G$, we have that $T \subseteq C_G(S)$ if and only if $ts = st$ for all $t \in T$ and $s \in S$, if and only if $S \subseteq C_G(T)$. Therefore, $x \in C_G(A)$ implies that $A \subseteq C_G(x)$. Since $\langle A \rangle$ is the smallest subgroup of G containing A, we deduce by part (a) that $\langle A \rangle \subseteq C_G(x)$, which in turn implies that $x \in C_G(\langle A \rangle)$, completing the proof.

   Here is a more direct proof of the reverse containment. 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 $hHh^{-1} = H$, so h normalizes H. As $h \in H$ was arbitrary we have $H \leq N_G(H)$. □

(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. □

2. 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. We will use that for any group G, $x \in Z(G) = C_G(G)$ if and only if $C_G(x) = G$ (as in the proof of 1(c)). In particular, to prove that $x \in D_{2n}$ is in the center, we need only check that multiplication commutes with r and with s, since then $r, s \in C_{D_{2n}}(x)$, and therefore so is all of $\langle r, s \rangle = D_{2n}$. 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. □

3. In this exercise we see that we can learn important facts about groups by studying their quotients.

(a) Suppose $H \leq Z(G)$. Show that H is a normal subgroup of G. (In particular, $Z(G)$ is normal).

Proof. Fix $z \in H$ and $g \in G$. It suffices to show $gzg^{-1} \in H$. But since $z \in Z(G)$ we have $gzg^{-1} = gg^{-1}z = z \in H$, so we are done. □

(b) Show that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. If $G/Z(G)$ is cyclic then we can fix a generator: $G/Z(G) = \langle xZ(G)\rangle$. Then the cosets $x^iZ(G)$ for $i \in \mathbb{Z}$ form a partition of G. In particular, fix $a, b \in G$. Then $a = x^iz$ and $b = x^jw$ for $z, w \in Z(G)$. Therefore we can leverage that we can freely commute with z and w, and x^i and x^j commute with eachother to conclude that

$$ab = x^izy^jw = zx^ix^jw = zx^jx^iw = x^jzwx^i = x^jwzx^i = x^jwx^iz = ba.$$

Thus a and b commute, but since they were arbitrary we conclude that G is abelian. □

(c) Let p and q be prime numbers (not necessarily distinct), and G a group of order pq. Show that if G is not abelian, then $Z(G) = \{1\}$.

Proof. Since G is not abelian then $Z(G) \neq G$. If $Z(G) \neq 1$ then by Lagrange's theorem, $Z(G)$ has either order p or q. Assume without loss of generality that it has order q. Then $|G/Z(G)| = |G|/|Z(G)| = p$, so that $G/Z(G)$ has prime order and therefore must be cyclic (by TH1#4(a)). But then by part (b) G must be abelian, a contradiction. □

4. In this exercise we show that if G is a nonabelian group of order 6. We will show $G \cong S_3$.

(a) Show that there is an element $x \in G$ of order 2. (Once we have Cauchy's theorem for nonabelian groups this part becomes easy, but since G has 6 elements, one can do this by inspection using Lagrange's theorem).

Proof. Since G is not abelian, there is no element of order 6. If there is also no element of order 2, then by Lagrange's theorem, $G = \{1, a, b, c, d, e\}$ where the order of a, b, c, d, e are all 3. Then a^{-1} has order 3 as well, so without loss of generality $a^{-1} = b$, and similarly we may assume $c^{-1} = d$. But this implies that $e^{-1} = e$, so that $e^2 = 1$ contradicting that it has order 3. □

(b) Let $x \in G$ have order 2, and let $H = \langle x\rangle$. Show that H is not normal in G. (*Hint:* Show that if H is normal then $H \leq Z(G)$, then apply 3(c) to find a contradiction.)

Proof. Suppose H is normal, so for all $g \in G$, $gxg^{-1} \in H = \{1, x\}$. If $gxg^{-1} = 1$ then $x = 1$, so we must have $gxg^{-1} = x$. This implies that $x \in Z(G)$ and so $H \leq Z(G)$. But since G is nonabelian of order $6 = 2 \cdot 3$, 3(c) says that its center must be trivial. □

(c) Define an action of G on the set $A = G/H$ by *left multiplication*: that is $g \cdot (xH) = gxH$. Show that this defines a well defined group action.

Proof. Although it at first looks like the rule of the action depends on the choice x to represent the coset xH, we can alternatively write

$$gxH = g(xH) = \{gz : z \in xH\},$$

which doesn't actually depend on the choice of x as a representative, so the rule is well defined. To see it is an action we observe that $1 \cdot (xH) = xH$, and $g_1 \cdot (g_2 \cdot (xH)) = g_1g_2xH = (g_1g_2) \cdot (xH)$. □

(d) Consider the action of G on $A = G/H$ by left multiplication. Show that the associated permutation representation is injective. Conclude that $G \cong S_3$.

Proof. The action of G on A gives a permutation representation $\varphi : G \to S_A$, and by HW3 Problem 7, the target is isomorphic to S_3. By HW4 Problem 7(b), $\ker \varphi$ is equal to the kernel G_0 of the action of G on A. Fix some $x \in G_0$. Then in particular, $x \cdot H = H$, so that $x \in H$. This shows that $G_0 \leq H$. Since $|H| = 2$, we see that either $G_0 = H$, or else $G_0 = \{1\}$. But G_0 is normal, and by part (b), H is not. Therefore $G_0 = \{1\}$ and φ is injective. Since $|G| = 6 = |S_3|$, HW1 Problem 5 implies that φ is surjective as well. Therefore φ is an isomorphism and $G \cong S_A \cong S_3$. □

As we start defining more exotic properties of groups we will need to expand our library of finite groups to exhibit some of these interesting properties. We finish with two new examples of finite groups. First up: Quaternions.

Definition 1. *The quaternion group of order 8, denoted Q_8 is the group of the following 8 elements:*

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

subject to the relations:

$$(-1)^2 = 1$$
$$i^2 = j^2 = k^2 = -1,$$
$$(-1)x = -x = x(-1) \text{ for all } x,$$

$$\begin{aligned} ij &= k, & ji &= -k, \\ jk &= i, & kj &= -i, \\ ki &= j, & ik &= -j. \end{aligned}$$

5. Let's establish some basic facts about Q_8. Much of this is worked out in the book.

(a) Write the entire multiplication table for Q_8.

Proof. The group is nonabelian, so we make sure to stick to the convention that in row a and column b we are writing ab (rather than ba),

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

□

(b) Find 2 elements which generate all of Q_8. (*Bonus:* Can you give a presentation of Q_8?)

Proof. Notice that i and j generate everything. Indeed:

$$\begin{array}{lll} -1 = i^2 & -i = i^3 & -j = j^3 \\ 1 = i^4 & k = ij & -k = ji. \end{array}$$

The following is an intuitive presentation, but I want to point out that -1 is tacitly a generator here:

$$\langle i, j \mid i^2 = j^2 = -1, ij = -ji \rangle.$$

This answer is acceptable on this assignment, but not precisely correct. We probably want to assume in our presentation that we don't know what -1 is (i.e., that its square is 1). The correct presentation, that doesn't include -1 secretly is:

$$\langle i, j \mid i^4 = j^4 = 1,\ i^2 = j^2 \text{ and } ji = i^3 j \rangle.$$

Where translating back to the more intuitive notation $i^2 = j^2 = -1$, $ij = k$, and $ji = i^3 j = (i^2)ij = -k$. □

(c) Prove that Q_8 is not isomorphic to D_8.

Proof. The easiest way to see this is to notice that if they were isomorphic, they would need to have the same number of elements of order n for each n. Then we can consider the order of every element in each group.

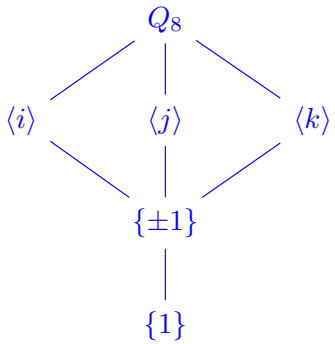
Q_8	order		D_8	order
1	1		1	1
-1	2		r	4
i	4		r^2	2
$-i$	4		r^3	4
j	4		s	2
$-j$	4		sr	2
k	4		sr^2	2
$-k$	4		sr^3	2

In particular, Q_8 only has one element of order 2 whereas D_8 has 5. □

(d) Find all the subgroups of Q_8, and draw them in a lattice ordered by inclusion. (*Hint*: there are 6 total subgroups).

Proof. The nontrivial subgroups (i.e., those which aren't Q_8 and $\{1\}$) must have orders 2 or 4 by Lagranges theorem. The order 2 subgroups must be cyclic, generated by an element of order 2. The only element of order 2 is -1, so the only subgroup of order 2 is $\{\pm 1\}$. As for subgroups of order four, they are either cyclic or isomorphic to the Klein 4 group V_4. But V_4 must be generated by 2 elements of order 2, and Q_8 only has one. Thus each subgroup of order 4 is cyclic. There are 6 elements of order 4, but $-i = i^3$, and similarly for j and k, so there 3 subgroups of order 4 generated by i and j and k.

As $i^2 = j^2 = k^2 = -1$, the subgroup $\{\pm 1\}$ is contained in all of them. Thus the lattice is as follows.



□

(e) Prove that every subgroup of Q_8 is normal. (*Note*: we saw that if a group is abelian, every subgroup is normal. This shows the converse isn't true!)

Proof. Q_8 and $\{1\}$ are automatically normal. Next notice that since $-1 * a = a * -1$ for each $a \in Q_8$. Thus $\{\pm 1\}$ is contained in the center of Q_8 and is therefore normal by 2(a) above.

The cases for $\langle i \rangle, \langle j \rangle$ and $\langle k \rangle$ are completely symmetric, so we just treat the case of $H = \langle i \rangle$. Notice that

$$H \leq N_{Q_8}(H) \leq Q_8.$$

Also $|H| = 4$ and $|N_{Q_8}(H)|$ divides 8 by Lagrange's theorem, so that $N_{Q_8}(H)$ is either H or all of Q_8. Thus if we exhibit one element of the normalizer which is not in H, the normalizer is all of Q_8, which precisely means that $H \trianglelefteq Q_8$. Notice that:

$$jij^{-1} = ji(-j) = (-k)(-j) = kj = -i \in \langle i \rangle.$$

Thus $j \in N_{D_8}(H)$ and we are done. □

(f) Prove that every *proper* subgroup and quotient group of Q_8 is abelian (*Hint*: You can appeal to TH1#4).

Proof. Let H be a proper subgroup or quotient of Q_8. Then by Lagrange's theorem, $|H| = 1, 2$ or 4. In the first case H is the trivial group which is abelian, in the second it is isomorphic to Z_2 which is abelian, and in the third it is isomorphic to either Z_4 or V_4 which are abelian. □

(g) Show that $Q_8/Z(Q_8)$ has order 4. By TH1 it must be isomorphic to Z_4 or V_4. Which one is it? Justify your answer. (*Hint for the second part*: you can do this by hand, but it might be slicker to apply 3(b)).

Proof. It is readily checked using the multiplication table in part (a) that $Z(Q_8) = \{\pm 1\}$. Then

$$|Q_8/Z(Q_8)| = |Q_8|/|\{\pm 1\}| = 8/2 = 4.$$

Then in particular, it is either cyclic or isomorphic to V_4. If it is cyclic, then 3(b) says that Q_8 is abelian, which is false. So the quotient is V_4. □

Let's finish by introducing finite matrix groups. We will need a definition.

Definition 2. *A field is a set F together with two commutative binary operations, $+$ and $\cdot$ (addition and multiplication), such that $(F,+)$ and $(F\setminus\{0\},\cdot)$ are abelian groups, and such that the distributive law holds. That is, for all $a,b,c\in F$ we have:*

$$a\cdot(b+c)=a\cdot b+a\cdot c.$$

For any field we let $F^\times=F\setminus\{0\}$ be its mutliplicative group. A field F is called a finite field if $|F|<\infty$.

It turns out that vector space theory over F is pretty much identical to vector space theory over R. We can define the first matrix group we hope to study.

Definition 3. *Let F be a field. If M,N are matrices with entries in F, we can compute their product MN and the determinant $\det(M)\in F$ using the same formulas as if $F=\mathbb{R}$. Then the general linear group of degree n over F is,*

$$GL_n(F)=\{A\mid A \text{ is an } n\times n \text{ matrix with entries in } F \text{ and } \det(A)\neq 0\}.$$

You may use the following fact without proof (since it is a standard result of linear algebra).

Proposition 1. *The set $GL_n(F)$ can be identified with the set of linear bijections $F^n\to F^n$, and matrix multiplication corresponds to composition of functions. In particular, $GL_n(F)$ is a group under matrix multiplication.*

6. It turns out that we have seen examples of finite fields already.

   (a) Let p be a prime number. Show that $\mathbb{Z}/p\mathbb{Z}$ with the operations $+$ and $\times$ is a field. This is the *finite field of order p* and will be denoted by $\mathbb{F}_p$.

   Proof. We already have seen that $\mathbb{Z}/p\mathbb{Z}$ is an abelian group under addition. Furthermore, by the extended Euclidean algorithm we know that an integer has a multiplicative inverse mod p if and only if it is coprime to p, so that every element of $\mathbb{Z}/p\mathbb{Z}\setminus\{0\}$ has a multiplicative inverse, making it an abelian group under multiplication. Finally, multiplication and addition are inherited from the same operations on $\mathbb{Z}$ which satisfy the distributive law. □

   (b) Show that if n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not a field.

   Proof. There are multliple ways to see that $\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ is not an abelian group under multiplication. For example, it isn't even closed under mutliplication. Take $n=ab$ for $1<a,b<n$. Then $\overline{a}\overline{b}=\overline{0}\notin\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$, so multiplication isn't even a binary operation.

   Another proof is the following: by the extended Euclidean algorithm, $a\in\mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(a,n)=1$. Therefore, letting $a|n$ and $a\neq 1$, we have $a\in\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ without a multiplicative inverse. □

7. Now let's study $GL_2(\mathbb{F}_p)$.

(a) Prove that $|GL_2(\mathbb{F}_2)| = 6$.

Proof. We will do parts (a) and (b) together, listing all the elements to see that there are 6 of them. A general matrix looks like

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Notice first that a and b can't both be 0. In each case, we fix (a, b) and leverage the fact that (c, d) must not be a multiple of (a, b). There are 3 cases, each with two possibilities. First, $a = 1$ and $b = 0$.

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

The case wehre $a = 0$ and $b = 1$ is similar.

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad D = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Finally, we have the case $a = b = 1$.

$$E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad F = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Thus there are six elements. □

(b) Write all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.

Proof. $A = I$ is the identity element and therefore has order 1. One can compute directly that $B^2 = C^2 = E^2 = I$ are the identity as well, thus they have order 2. But notice that $D^2 = F$ and that F^2 is D. Nevertheless, we notice that $F = D^{-1}$ so that $DF = FD = I$ so that $D^3 = F^3 = I$ so that they have order 3. □

(c) Show that $GL_2(\mathbb{F}_2)$ is not abelian. Conclude that it is isomorphic to S_3.

Proof. We can check directly that $BC = D$ and that $CB = F$. Therefore $GL_2(\mathbb{F}_2)$ is a nonabelian group of order 6, and therefore isomorphic to S_3 by 4(d). □

(d) Generalizing part (a), show that if p is prime then

$$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.$$

Proof. Fix some:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We want to count how many choices of (a, b, c, d) we have. We will use the fact that $\det A \neq 0$ if and only if $(a, b) \neq (0, 0)$ and (c, d) is not a multiple of (a, b). Let's notice that the total number should be the product of the choices for (a, b) with the choices for (c, d) having fixed (a, b). Let's begin by counting the number of choices for (a, b). They must be selected from $\mathbb{F}_p$, so that we have p choices each for a and p choices for

b, giving p^2 total choices. Of course, they cannot both be 0, $p^2 - 1$ allowable ones. Now all we have to say is that (c, d) is not a multiple of (a, b). That is, there are p^2 choices for (c, d), but p of them are $(\lambda a, \lambda b)$ for all the different $\lambda \in \mathbb{F}_p$. In particular, there are $p^2 - p$ allowable choices. Thus the total is:

$$(p^2 - 1)(p^2 - p) = p^4 - p^3 - p^2 + p.$$

□