HOMEWORK 6 SOLUTIONS

Throughout G and H are (arbitrary) groups.

(1) Here are some basic properties of the order of an element for you to prove.

(a) Why can't an element of a group have order 0? (Look at the definition of the order ... there's a word beginning with the letter "p")

Solution. The order of any element is a *positive* integer.

(b) Show that an element of a group has order 1 if and only if it is the identity.

Solution. $g = g^1$. Hence $g^1 = e_G$ if and only if $g = e_G$.

(c) Let $g \in G$. Show that if $g^2 = g^3$, then $g = e$. Generalize this to show that if $g^m = g^n$ where m and n are relatively prime (i.e. have a greatest common divisor equal to 1) then $g = e_G$ **Hint**: Use a theorem proven in class on 2-28.

Solution. For the special case multiply both sides of the equation $g^2 = g^3$ on the left by g^{-2}. For the generalization, recall from the stated class that the assumption guarantees that the order of g divides m and n. But since these two numbers are relatively prime this mean that the order is 1 which implies that $g = e_G$ as desired.

(d) Show that $|g^{-1}| = |g|$.

Solution. $g^n = e_G$ happens if and only if $(g^{-1})^n = (g^n)^{-1} = e_G^{-1} = e_G$.

(e) Show that $q \in \mathbb{H}^*$ has order 4 if and only $q \in \mathbb{S}^2$ (i.e. pure quaternions of length 1).

Solution. Since $1 = q^4 = (q^2)^2$ we must have that q^2 has order 2. But from class (proven on 2-28) we know that this implies that $q^2 = -1$. Brining a q^{-1} to the other side this implies that $q = -q^{-1}$. But from that same class we showed that any element of finite order in $q \in \mathbb{H}^*$ actually lives in $\mathbb{S}^3$. Thus, we know that $q^{-1} = \overline{q}$. Hence $q = -\overline{q}$ which proves that in addition to having length 1, q is pure. Thus q is a purely imaginary quaternion of length 1 as desired.

(2) Recall that the center of G, denoted $Z(G)$ is defined as

$$\{z \in G : gz = zg \quad \forall g \in G\}$$

(i.e. it is the set of elements of G which commute with everybody in G). In the last homework (whether you realized it or not) you proved this was a subgroup of G because you showed it was the kernel of a homomorphism.

(a) Instead give a direct proof of this by using a standard subgroup test (showing closure, etc) to show it is a subgroup.

Solution.

- e_G commutes with every element of G, hence it is in the center.

- Suppose a and b are in $Z(G)$ and let $g \in G$ be arbitrary. Then

$$\begin{aligned}(ab)g &= a(bg)\\ &= a(gb)\\ &= (ag)b\\ &= (ga)b\\ &= (ga)b\\ &= g \cdot (a \cdot b).\end{aligned}$$

  Since g was arbitrary, this implies that $ab \in Z(G)$, hence closure under the product.
- Suppose that $z \in Z(G)$. Then foraan arbitrary $g \in G$ we have

$$\begin{aligned}z^{-1}g &= z^{-1}ge\\ &= z^{-1}gzz^{-1}\\ &= z^{-1}zgz^{-1}\\ &= gz^{-1}.\end{aligned}$$

  Hence $z^{-1} \in Z(G)$, hence closure under inverses.

(b) Since the kernel of any homomorphism is always normal we already know that $Z(G)$ is a *normal* subgroup. Generalize this by showing that any subgroup of $Z(G)$ is also a normal subgroup of G.

Solution. Suppose that $H < Z(G)$ and let $g \in G$ and $h \in H$. Then since $H \subset Z(G)$ we have that $h \in Z(G)$. Thus h commutes with every element of G and in particular it commutes with g. Thus

$$ghg^{-1} = gg^{-1}h = eh = h \in H.$$

Hence H is normal in G.

(c) Show that $Z(G)$ is an abelian group.

Solution. Let $a, b \in Z(G)$ be arbitrary. Since $Z(G) \subset G$ this implies that $b \in G$. Then since $a \in Z(G)$ it commutes with every element of G, in particular it commutes with b. Hence $ab = ba$ and $Z(G)$ is abelian.

(d) Show that G is abelian if and only if $Z(G) = G$ (the previous bullet gives you half of this for free).

Solution. If $G = Z(G)$, then G is equal to an abelian group (by the last part) and is thus abelian. On the other hand suppose that G is abelian and let $g \in G$. We want to show that $g \in Z(G)$. To this end let $a \in G$ be arbitrary. Then since G is abelian, $ga = ag$. But this means that $g \in Z(G)$.

(e) Cite a problem from the very first homework assignment which showed that $Z(\mathbb{H}^*)$ is the set of real quaternions.

Solution. You look it up.

(f) Give two proofs of the following: if $G = \langle X \rangle$, then show that g commutes with every element of X implies $g \in Z(G)$ [1] (the converse if obvious since $X \subset G$) . To give the concrete proof follow the following outline:

- Show that assumption guarantees that g commutes with the inverse of every element of X. (What you're really showing is that in general g commutes with $h \in G$ implies that g commutes with h^{-1}. Either cite this in your notes or prove it again).
- Show that the assumption guarantees that g commutes with any power of any element of X (the 1 power is by assumption, the -1 power was the above bullet point).
- Let $w \in G$ be an arbitrary element (hence a word in X), Use the above bullet to show that g commutes with w by writing w out as $x_1^{n_1} \cdots x_m^{n_m}$ and "dragging" (commuting) g by each $x_i^{n_i}$ individually . Perhaps an induction will make this "look" a little cleaner.

For the abstract proof (an abstract proof should never use any (group theoretical) words!)

- Show that $g \in Z(G)$ if and only if $C_G(g) = G$ (the centralizer of $g \in G$ i.e. the set of guys in G who commute with g) (this is simply a rephrasing of definitions).

  Solution. The centralizer of g is the set of elements of G which commute with g. Thus $C_G(g) = G$ if and only if g commutes with every element of G. This is precisely the condition needed for $g \in Z(G)$.

- Show that the assumption that every element of X commutes with g implies that $X \subset C_G(g)$ (again, this completely obvious).

  Solution. If $x \in X$, then the assumption is that x commutes with g, hence $x \in C_G(g)$.

- Either reprove or cite in your notes (the day it was proved) the fact that $C_G(g) < G$ (this is the same place where we proved the first bullet of the concrete proof above). (**Bonus**: Give a "fancy" proof of this by showing that $C_G(g)$ is the set of fixed points of c_g discussed in the previous homework assignment).

  Solution. $gag^{-1} = c_g(a) = a$ which holds if and only if a commutes with g. Hence $C_G(g)$ is the fixed point set of the endomorphism c_g.

- Use the third property of a group generated by a set (**gen3**) and the above bullet to prove that

  $$G = \langle X \rangle < C_G(g) < G$$

  which implies (by basic set theory) $C_G(g) = G$.

  Solution. Since X is a subset of the group $C_G(g)$ we must have that $\langle X \rangle \subset C_G(g)$ by (**gen3**).

[1] This says, among other things that G is abelian if and only if any two elements of X commute

- Conclude from the first bullet point of this sequence that $g \in Z(G)$.

  Solution. We have shown that under the assumptions that $C_G(g) = G$ which by the first bullet point means that $g \in Z(G)$ as desired.

(g) Show that if $G \cong H$, then $Z(G) \cong Z(H)$ (**hint** If φ is an isomorphism between G and H show that $g \in Z(G)$ if and only if $\varphi(g) \in Z(H)$) (thus the isomorphism type, hence the order of the center of any group is an isomorphism invariant).

(3) In this problem, we prove that for any $n > 2$, that $Z(S_n)$ is trivial (i.e. contains only the identity).

(a) For concreteness we first outline the proof for $n = 5$ [2] and from there it should be easy to generalize. Define the elements of S_5 by

$$\begin{aligned} \sigma_1 &= (2\,3\,4\,5) & \sigma_2 &= (1\,3\,4\,5) \\ \sigma_3 &= (1\,2\,4\,5) & \sigma_4 &= (1\,2\,3\,5) \\ \sigma_5 &= (1\,2\,3\,4). \end{aligned}$$

Show that an element τ commutes with σ_i implies that $\tau(i) = i$ (this says that the function ... (yes, elements of S_n are functions) τ maps i to itself.)

(b) Show that if τ is in the center, then we have $\tau(i) = i$ all $i = \{1, 2, 3, 4, 5\}$.

(c) Conclude that $\tau = (1)$.

(d) Generalize this in the case for general $n > 2$.

(4) Consider the group

$$G_1 = \langle (3\,6), (2\,4\,6)(1\,3\,5) \rangle \; (< S_6)$$

(as usual we denote the first generator listed, $(3\,6)$ as x and the second generator listed $(2\,4\,6)(1\,3\,5)$ as y.

(a) Show that G_1 is not abelian.

Solution. G_1 is not abelian since x and y do not commute.

(b) Show that $z := (1\,4)(2\,5)(3\,6) \in G_1$. My thought process [3] for this was as follows: (1) xy is a 6-cycle since (you could of course do this the long way by composing functions from right to left)

$$\begin{aligned} xy &= (3\,6)(2\,4\,6)(1\,3\,5) & & \\ &= (3\,6)(6\,2\,4)(1\,3\,5) & & \text{Recycling} \\ &= (3\,6\,2\,4)(1\,3\,5) & & \text{Cut \& Paste} \\ &= (6\,2\,4\;3)(3\,5\,1) & & \text{Recycling} \\ &= (6\,2\,4\,3\,5\,1) & & \text{Cut \& Paste} \end{aligned}$$

(2) any 6-cycle cubed is a 2,2,2-cycle which is the cycle type of our target, z. So a good place to start is by looking at $(xy)^3$.

Solution. I basically gave this one away, $z = (xy)^3$ as can be checked directly.

[2] It should be just as easy to abstract a proof from the case $n = 4$ but 4 is a small enough number that you could possibly "cheat" and prove it by brute force!

[3] You might be able to find a much easier way of doing this, experiment a bit! This was simply the first thing that came to my mind

(c) Show that $z \in Z(G)$ (use the previous problem!) (**Computational hint** Instead of computing xz, zx , yz, and zy you will probably find it easier to use the wonderful formula proven on 2-14 and discussed further on 2-16 pertaining to how to conjugate elements of S_n to show that $xzx^{-1} = z$ and $yzy^{-1} = z$ rather easily).
(d) Use maple or gap to show that this group has order 24.
(e) We already know 3 other groups of order 24, namely $B(\Delta^3)$, S_4, and $\mathbb{Z}_{24}$. Show that G_1 is not isomorphic to any of these groups by using the following hints:
- $B(\Delta^3)$ (as do all groups of quaternions) have at most one element of order two in them (namely the element -1).

  Solution. G_1 has more than 1 element of order 2, namely x and z. Thus the two groups are not isomorphic since they have a different number of elements of order 2.

  Solution. G_1 has a non-trivial center (since z is in it) but S_4 does not (by the previous problem). Thus since the number of elements in the center of a group is an isomorphism invariant, these two groups are not isomorphic.

- $\mathbb{Z}_{24}$ is abelian.

  Solution. And G_1 is not.

(5) Recall that

$$G_2 := B(\square^3) = \left\langle \frac{\sqrt{2}(1+i)}{2}, \frac{\sqrt{2}(1+j)}{2} \right\rangle .$$

(This group has order $2 \cdot 24 = 48$) As usual we denote the first generator x and the second y.
(a) Show that i and j are in G_2. Conclude that $Q_8 < G_2$.

Solution.

$$x^2 = 1/2(1+i)^2 = 1/2(1+2i+i^2) = 1/2(1+2i-1) = i$$

and similarly $y^2 = j$. Thus i and j are words in x and y and are therefore in G_2.

(b) Show that both $\langle i \rangle$ and $\langle j \rangle$ are not normal in G_2.

Solution. The first group, $\langle i\rangle$, is $\{1,-1,i,-i\}$ and the second is $\{1,-1,j,-j\}$. But

$$\begin{aligned} yiy^{-1} &= \left(\frac{\sqrt{2}(1+j)}{2}\right) i \left(\frac{\sqrt{2}(1+j)}{2}\right)^{-1} \\ &= \left(\frac{\sqrt{2}(1+j)}{2}\right) i \left(\frac{\sqrt{2}(1-j)}{2}\right) \\ &= \left(\frac{\sqrt{2}(1+j)}{2}\right) \left(\frac{\sqrt{2}(1+j)}{2}\right) i \\ &= \left(\frac{\sqrt{2}(1+j)}{2}\right)^{2} i \\ &= ji \\ &= -k. \end{aligned}$$

which is not in $\langle i\rangle$. Hence $\langle i\rangle$ is not normal. Similarly $xjx^{-1}=k$ (this time no negative sign!) which is not in $\langle j\rangle$ proving that $\langle j\rangle$ is not normal in G_2.

(c) Show however that Q_8 is normal in G_2.

Solution. Since i is a power of x and j is a power of y the only non-trivial cases that we need to check to use "the normal subgroup check using generators" are xjx^{-1} and yiy^{-1}. But we showed in the previous part that the first equals $k=ij$ and the second equals $-k=ji$. Hence in either case the conjugate is still in Q_8, and we can conclude that Q_8 is a normal subgroup of G_2.

(6) Define

$$G_3 = \langle (1\,5)(3\,7), (1\,2\,3\,8)(4\,5\,6\,7)\rangle\,.$$

(We'll be able to show later that this group has order 16. For now you could use maple or gap to verify this.) As usual we denote the first generator x and the second y.

(a) Show that G_3 is not abelian.

Solution. Again, x and y do not commute, so the group is not abelian.

(b) Show both $z := (2\,6)(4\,8)$ and $w := (1\,5)(2\,6)(3\,7)(4\,8)$ are in G_3.

Solution. $z = yxy^{-1}$ and $w = xz$.

(c) Show that both y^2 and w are in the center of G.

Solution. Since y^2 is a power of y we only need to check that x commutes with y^2. First we note that $y^2 = (1\,3)(2\,8)(4\,6)(5\,7)$. So using the formula of conjugation in S_n we see that

$$\begin{aligned} xy^2x^{-1} &= ((1\,5)(3\,7))\ \ (1\,3)(2\,8)(4\,6)(5\,7)\ \ ((1\,5)(3\,7))^{-1} \\ &= (5\,7)(2\,8)(4\,6)(1\,3) \\ &= (1\,3)(2\,8)(4\,6)(5\,7) \qquad \text{(can switch order of dij perm)} \\ &= y^2. \end{aligned}$$

As desired. To show that $w \in Z(G_3)$ we could do the same thing, but let's be a little sneakier. Note that since y^2 is central we have that

$$x = y^2 x y^{-2} = yyxy^{-1}y^{-1} = yzy^{-1}.$$

Moreover, since x and z are disjoint cycles, x and z commute. Since $w = xz$ we also have that x commutes with w (product of two elements commuting with x also commutes with x). Thus we only need to show that y commutes with w:

$$\begin{aligned} ywy^{-1} &= yxzy^{-1} \\ &= yxy^{-1}yzy^{-1} \\ &= zx \qquad \text{since } yzy^{-1} = x \\ &= xz \qquad \text{since } xz = zx \\ &= w \end{aligned}$$

as desired.

(d) Show that the group $\langle x, z \rangle$ is a normal subgroup of G_3.

Solution. The only non-trivial thing that we need to check to apply the "the normal subgroup check using generators" is yxy^{-1} and yzy^{-1}. But we have already shown that the first equals z and the second equals x. In particular both conjugates are in $\langle x, z \rangle$ which implies that this subgroup is normal as desired.

(e) Recall that BD_4 and D_8 are groups of order 16. Is either isomorphic to G_3? Why or why not?

Solution. Neither are isomorphic to G_3. For starters, BD_4 isn't because it has only 1 element of order 2 (as do all quaternion groups) (namely -1) and G_3 has more than 1 (it has at least x and z ... it also has y^2 and w, but the second we get more than 1 we don't care anymore!). At the same time D_8 has only 1 non-trivial element in its center, namely rotation by 180 degrees, but we have seen that G_3 has more than 1, namely y^2 and w (as well as $y^2 w$, but again the second we get more than 1 we no longer care).

(7) Suppose that a and b are two distinct, commuting elements of order 2 (in any group). Show that $\langle a, b \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.