①

M403 - Enrique Areyan - Fall 2013 - HW 3

60/60

(1) Let G be a group.

(a) For each $g \in G$ the centralizer of g is the set

+10

$$C(g) = \{x \in G \mid gx = xg\}.$$

(i) Prove that $C(g)$ is a subgroup of G.

Pf: (I) Let $g \in G$. Let $a, b \in C(g)$. By definition: $ga = ag$ and $gb = bg$ then, From these we get that: $a = gag^{-1}$ and $b = gbg^{-1}$

$$abg = (gag^{-1})(gbg^{-1})g = ga(g^{-1}g)b(g^{-1}g) = (ga)e(be) = gab$$

Hence, $C(g)$ is closed under the group operation.

(II) Let $g \in G$ and let $a \in C(g)$. By definition $ag = ga$, which means $a = gag^{-1}$ by properties of inverses $a^{-1} = (gag^{-1})^{-1} = (g^{-1})^{-1}a^{-1}g^{-1} = ga^{-1}g^{-1}$ and thus, $a^{-1}g = ga^{-1}$, which means that $a^{-1} \in C(g)$.

(I) and (II) means that $C(g)$ is a subgroup of G.

(ii) Compute the centralizers of H and R_2 in D_4.

Solution: For $H \in D_4$. By definition $C(H) = \{x \in D_4 \mid Hx = xH\}$

$IH = HI \Rightarrow I \in C(H)$; $R_1H = D_1 \neq D_2 = HR_1 \Rightarrow R_1 \notin C(H)$

$R_2H = V = HR_2 \Rightarrow R_2 \in C(H)$; $R_3H = D_2 \neq D_1 = HR_3 \Rightarrow R_3 \notin C(H)$

$D_1H = R_1 \neq R_3 = HD_1 \Rightarrow D_1 \notin C(H)$; $D_2H = R_3 \neq R_1 = HD_2 \Rightarrow D_2 \notin C(H)$

$HH = I \Rightarrow H \in C(H)$; $HV = R_2 = VH \Rightarrow V \in C(H)$.

Hence $C(H) = \{I, H, R_2, V\}$.

For $R_2 \in D_4$. Again, by definition $C(R_2) = \{x \in D_4 \mid R_2x = xR_2\}$

$IR_2 = R_2I \Rightarrow I \in C(R_2)$; $R_1R_2 = R_3 = R_2R_1 \Rightarrow R_1 \in C(R_2)$

$R_2R_2 = I \Rightarrow R_2 \in C(R_2)$; $R_2R_3 = R_1 = R_3R_2 \Rightarrow R_3 \in C(R_2)$

$D_1R_2 = D_2 = R_2D_1 \Rightarrow D_1 \in C(R_2)$; $D_2R_2 = D_1 = R_2D_2 \Rightarrow D_2 \in C(R_2)$

$HR_2 = V = R_2H \Rightarrow V \in C(R_2)$; $VR_2 = H = R_2V \Rightarrow V \in C(R_2)$

Hence, $C(R_2) = \{I, R_1, R_2, R_3, D_1, D_2, H, V\} = D_4$

(1) (b) the center of G is the set $Z(G)=\{g\in G \mid gx=xg \text{ for all } x\in G\}$

(i) Prove that $Z(G)$ is a subgroup.

Pf: (I) Let $a,b\in Z(G)$. By definition, $ax=xa$ and $bx=xb$, for all $x\in G$ which means that $a=xax^{-1}$ and $b=xbx^{-1}$, for all $x\in G$.
Let $x\in G$. then $abx=(xax^{-1})(xbx^{-1})x=xa(x^{-1}x)b(x^{-1}x)=(xa)ebe=xab$
therefore, by definition of $Z(G)$ we conclude that $ab\in Z(G)$.
$Z(G)$ is closed under the group operation.

(II) Let $a\in Z(G)$. By definition, $ax=xa$, for all $x\in G$, which means $a=xax^{-1}$, by properties of inverses $a^{-1}=(xax^{-1})^{-1}=(x^{-1})^{-1}a^{-1}x^{-1}=xa^{-1}x^{-1}$
and thus $a^{-1}x=xa^{-1}$, for any $x\in G$. therefore, $a^{-1}\in Z(G)$.

(I) and (II) means that $Z(g)$ is a subgroup of G.

(ii) Compute $Z(D_4)$

Solution: By previous part (a)(ii) we know that $R_2\in Z(D_4)$.
Since $Z(D_4)$ was just proved to be a subgroup we know that $I\in Z(D_4)$
In fact $Z(D_4)=\{e,R_2\}$, since

$R_1H=D_1\neq D_2=HR_1 \Rightarrow R_1\notin Z(D_4)$ and $H\notin Z(D_4)$

$R_3H=D_2\neq D_1=HR_3 \Rightarrow R_3\notin Z(D_4)$

$D_1H=R_1\neq R_3=HD_1 \Rightarrow D_1\notin Z(D_4)$

$D_2H=R_3\neq R_1=HD_2 \Rightarrow D_2\notin Z(D_4)$

$VR_1=D_1\neq D_2=R_1V \Rightarrow V\notin Z(D_4)$

the only elements that commute with every other element are I and R_2

(2) Prove that if G is a group of even order, then G contains an element of order 2.

Pf: the proof will be by contradiction as follow:

the identity element is the unique element of order 1 in any group. therefore, all elements in $G\setminus\{e\}$ have order 2 or more, and $|G\setminus\{e\}| = 2p-$
Suppose for a contradiction that $G\setminus\{e\}$ contains no elements of order 2. this would mean that no element is its own inverse, i.e.,
$\forall a \in G\setminus\{e\}$: $a \neq a^{-1} \iff \theta(a) > 2$. Now, partition the set $G\setminus\{e\}$ as follow
$G\setminus\{e\} = \bigcup_{\substack{\text{distinct} \\ a \in G\setminus\{e\}}} \{a, a^{-1}\}$. for each $a \in G$. Since we assumed that there are no elements which are their own inverse, we will have exactly two elements in each partition. But this would mean that $|G\setminus\{e\}| = 2k$, for k the num of partitions, which contradicts the fact that $|G\setminus\{e\}|$ is an odd number since $|G\setminus\{e\}| = |G| - 1$; $|G|$ even. therefore, there exists at least one element of order 2 in G.

+10

(3) Let G be a group and let $g \in G$ have finite order m.

(a) Prove that if $n|m$, then $\theta(g^n) = m/n$

Pf: If $n|m$ then $m = nk$, for some $k \in \mathbb{Z}$. then, $(g^n)^k = g^{nk} = g^m = e$; but $k = \frac{m}{n}$, so this shows that $(g^n)^{m/n} = e$. Now, suppose there exist $a \in \mathbb{Z}$ with $1 \leq a < \frac{m}{n}$ such that $(g^n)^a = e$. But then $g^{na} = e$, $a < \frac{m}{n} \Rightarrow$ $na < m$, contradicting the fact that $\theta(g) = m$. Hence, there exists no such a and $\theta(g^n) = \frac{m}{n}$.

(b) Prove that if k is an integer and $d = \gcd\{m,k\}$, then $\theta(g^k) = m/d$.

Pf: Since $d|m$ it makes sense to write $(g^k)^{m/d} = (g^m)^{k/d}$, which also makes sense since $d|k$. But then $(g^m)^{k/d} = e^{k/d} = e$. Now, suppose there exists $x \in \mathbb{N}$, with $1 \leq x < \frac{m}{d}$ such that $(g^k)^x = e$. But then $g^{kx} = e$. We have t which means that $m | kx \Rightarrow kx = m \cdot a$, for some $a \in \mathbb{Z}^+$. sin $d|k \Rightarrow k = d \cdot b$ for some $b \in \mathbb{Z}^+$. Hence, $d \cdot b \cdot x = m \cdot a \Rightarrow x = \frac{m}{d} \cdot \frac{a}{b}$, $d|m$, so it has to be that $\frac{a}{b} \geq 1$, and therefore $x \geq \frac{m}{d}$, a contrad
So, there exists no such x and $\theta(g^k) = \frac{m}{d}$.

(3)(c) Prove that if G is a finite group of order p^r where p is a prime, then G contains an element of order p.

Pf: Let G be a group such that $|G|=p^r$, where p is prime. Consider an element $a\in G$ such that $a\neq e$. Then, $O(a)$, call it $O(a)=n$, must be such that $n|p^r$ (by Lagrange's theorem, considering $\langle a\rangle=n$, $n>1$ then $p^r=nq$, for some $q\in\mathbb{N}$. Thus, $n=\frac{p^r}{q}$. Since p is a prime, q must be a power of p and hence $n=p^m$, $1\leq m\leq r-1$. Therefore, $O(a)=p^m$, $1\leq m\leq r-1$. Now, let us consider the element $b=a^{p^{m-1}}$. Claim: the order of b is p. Pf (of claim): First, note that $b^p=(a^{p^{m-1}})^p=a^{p^m}=e$, since $O(a)=p^m$. Moreover, suppose there exist an integer K, with $1\leq K<p$, such that $b^K=e$. But then $b^K=(a^{p^{m-1}})^K=a^{Kp^{m-1}}=e$, but $Kp^{m-1}<p^m$, since $K<p$, which contradicts the fact that $O(a)=p^m$. Therefore, there exists no such K, and we conclude that $O(b)=p$. (END of Pf of claim)

Since b is clearly an element in G, since it is a power of a, we have found an element in G of order p.

+10

(4)(a) Let G be an abelian group and let $x,y\in G$. Let $O(x)=m$ and $O(y)=n$. Prove that if m and n are relatively prime then $O(xy)=mn$.

Pf: First note that:

$$\begin{aligned}(xy)^{mn}&=x^{mn}y^{mn} &&\text{since G is abelian}\\&=(x^m)^n(y^n)^m &&\text{Power rule}\\&=e^n e^m &&\text{since } O(x)=m \text{ and } O(y)=n\\&=e\cdot e=e &&\text{By properties of the identity}\end{aligned}$$

+10

Now, let $d=O(xy)$.

By our previous calculation and theorem proved in class, it must be that $d|m\cdot n$. Moreover, consider $e=((xy)^d)^m=(xy)^{dm}=(x^m)^d y^{md}=e^d y^{md}=y^{md}$. Hence, $n|md$. Likewise: $e=((xy)^d)^n=(xy)^{dn}=x^{dn}(y^n)^d=x^{nd}\cdot e^d=x^{nd}$, thus, $m|nd$. So we have that $n|md$ and $m|nd$. But n, m are relatively prime so $n|d$ and $m|d$, which means $d=n\cdot a$ and $d=m\cdot b$ for some integers a, b. But we have $d|m\cdot n\Rightarrow m\cdot n=d\cdot c$, for some c

Hence, combining these equations we get that $m \cdot n | d$, and together $d | m \cdot n$ and $m \cdot n | d$ imply that $d = \pm m \cdot n$; but d is an order of an element and by definition this is a positive number. therefore $d = m.n.$ and so $O(xy) = m.n.$

(b) Prove that the stament of part (a) is false for arbitrary groups.

Solution: Consider S_3 and two of its elements: $(1,2)$ and $(1,2,3)$. then, $O((12)) = 2$ since $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$ and

$$O((123)) = 3 \text{ since } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

the order of these two elements are relatively prime. However,

$$(1\,2)(1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

the order of this element is 2; i.e., $O((13)) = 2$ since

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Since S_3 is an arbitrary group, in particular not abelian, the statement in part (a) is false, as this example shows: $O((12)) = 2$ and $O((123)) = 3$ and $\gcd(2,3) = 1$ But $O((12)\circ(123)) = O((13)) = 2 \neq 2 \cdot 3 = 6 = O((12))\,O((123))$.

(c) Let G be an abelian group of order 6. Prove that G is cyclic.

Pf: Let G be an abelian group s.t $|G| = 6$.

this proof will work as follow:

(i) Prove that G has at least one element of order 2.

(ii) Prove that G has at least one element of order 3.

(iii) Use part (a) and (i), (ii) to conclude that there exists an element of order 6, i.e., a generator.

Before we begin, note that for any $g \neq e$, $|\langle g \rangle| \mid |G| = 6 \Rightarrow$
$|\langle g \rangle| = O(g) = 2, 3$ or 6. Moreover, an element of order 6 would
mean a generator.

(i) Suppose for a contradiction that all elements are of order 3.
Pick $g \in G$, $g \neq e$. Consider $\langle g \rangle = \{e, g, g^2\}$. Since $|G| = 6$, there exist
$h \in G$, $g \neq h$. Consider $\langle h \rangle = \{e, h, h^2\}$. this groups do not share any
element except the identity, and so consider $G = \{e, g, g^2, h, h^2, t\}$,
but t by assumption has order 3, which would mean that t^2 is also
in G but then $|G| = 7 > 6 = |G|$, a contradiction. therefore, we either
have an element of order 6 and we are done, or we have at least
one element of order 2.

(ii) Suppose for a contradiction that all elements are of order 2. then,
Consider the set $\{e, g_1, g_2, g_3\}$, where $g_1 \neq g_2$ and $g_3 = g_1 g_2$.
all elements contain inverses since each is its own inverse ($O(g_i) = 2$)
Moreover, this is a closed set since: $g_3 = g_1 g_2 \Leftrightarrow g_2 g_3 = g_2 g_1 g_2 = g_1$
$\Leftrightarrow g_2 g_3 = g_1 = g_3 g_2$ using the fact that G is abelian. Likewise,
$g_3 = g_1 g_2 \Leftrightarrow g_1 g_3 = g_3 g_1 = g_1^2 g_2 = g_2 \Leftrightarrow g_1 g_3 = g_2 = g_3 g_1$
Since this is a closed set with every element having inverses, it is a
subgroup. But $|\{e, g_1, g_2, g_3\}| = 4 \nmid 6$, in contradiction with Lagrange's
theorem. therefore, not all elements have order 2. So either we have
an element of order 6 and we are done, or we have at least one
element of order 3.

(iii) Parts (i) and (ii) provide the existence of at least one
element of order 2, call it x and one element of order 3,
call it y. then, by part (a), $O(xy) = 2 \cdot 3 = 6$, which means
that xy is a generator for G and thus, G is cyclic.

(5) Prove that if m is the H-order of g then for all integers k, $g^k \in H$ if and only if $m \mid k$.

Pf: Let G be a finite group. Let H be a subgroup of G. Let $g \in G$ and m be its H-order.

($\Rightarrow$) Suppose that for all integers k, $g^k \in H$. In particular, for $k=1$ we have that $g^1 \in H$. this means that $m=1$, the smallest positive integer. But then $k = k \cdot 1 \Rightarrow 1 \mid k$, for any $k \in \mathbb{Z}$. therefore, $m=1$ is the H-order and is such that $m \mid k$ for any k.

($\Leftarrow$) Suppose that $m \mid k$, for any $k \in \mathbb{Z}$. then $k = m \cdot p$, for $p \in \mathbb{Z}$. and so:

$$g^k = g^{m \cdot p} = (g^m)^p \in H,$$ since $g^m \in H$ by definition of H-order and subgroups are closed under the group operation: $g^m \cdot g^m \in H$, $(g^m g^m) g^m$ ..., $\underbrace{g^m \cdots g^m}_{p \text{ times}} = (g^m)^p \in H$. So any power of g^m is in H, showing the result.

---

(6) Let H be a subgroup of a group G.

(a) Prove that if $g \in G$, then gHg^{-1} is a subgroup of G.

+10

Pf: Let $g \in G$.

(i) Let $x, y \in gHg^{-1}$. then $x = gh_1g^{-1}$ for some $h_1 \in H$ and $y = gh_2g^{-1}$ for some $h_2 \in H$. then, So let

$$xy = (gh_1g^{-1})(gh_2g^{-1}) = (gh_1(g^{-1}g)h_2g^{-1}) = g(h_1h_2)g^{-1}.$$

By properties of closure of subgroups, $h_3 \in H$ which means $h_3 = h_1h_2$. therefore, that $xy = gh_3g^{-1} \Rightarrow xy \in gHg^{-1}$.

(ii) Let $z \in gHg^{-1}$. then $z = ghg^{-1}$ for some $h \in H$. therefore,

$$z^{-1} = (ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1} \Rightarrow z^{-1} = gh^{-1}g^{-1};$$ and since $h \in H \Rightarrow h^{-1} \in H$; so we can conclude that $z^{-1} \in gHg^{-1}$.

(i) and (ii) imply that gHg^{-1} is a subgroup of G.

M403 - Enrique Areyan - Fall 2013 - HW 3

(6) (b) Prove that if $g_1, g_2 \in G$ and $g_1H = g_2H$, then $g_1Hg_1^{-1} = g_2Hg_2^{-1}$

Pf: Let $g_1, g_2 \in G$. Suppose that $g_1H = g_2H$.

($\subseteq$) Let $x \in g_1Hg_1^{-1}$. then $x = g_1hg_1^{-1}$, for some $h \in H$.

Note that $g_1 \cdot e = g_1$; since $e \in H \Rightarrow g_1 \in g_1H \Rightarrow g_1 \in g_2H \Rightarrow g_1 = g_2h_1$ for some $h_1 \in H$. But then $g_1^{-1} = h_1^{-1}g_2^{-1}$. Replacing this equations in our equation for x we get: $x = g_1hg_1^{-1} = (g_2h_1)h(h_1^{-1}g_2^{-1}) = g_2(h_1hh_1^{-1})g_2^{-1}$

But $h, h_1, h_1^{-1} \in H \Rightarrow h_1hh_1^{-1} = h_2 \in H$, hence $x = g_2h_2g_2^{-1}$, which means that $x \in g_2Hg_2^{-1}$.

($\supseteq$) let $y \in g_2Hg_2^{-1}$. then $y = g_2hg_2^{-1}$, for some $h \in H$.

Like before: $g_2e = g_2$; since $e \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H \Rightarrow g_2 = g_1h_1$, for some $h_1 \in H$. But then $g_2^{-1} = h_1^{-1}g_1^{-1}$. Replacing for y:

$y = g_2hg_2^{-1} = (g_1h_1)h(h_1^{-1}g_1^{-1}) = g_1(h_1hh_1^{-1})g_1^{-1}$. But $h, h_1, h_1^{-1} \in H \Rightarrow$ $h_1hh_1^{-1} = h_2 \in H$, hence $x = g_1h_2g_1^{-1}$, which means that $y \in g_1Hg_1^{-1}$.

Now, assume G is finite.

(6)(c) Prove that if $g \in G$, then $|gHg^{-1}| = |H|$.

Pf: It suffices to show a bijection between gHg^{-1} and H to show that they have the same size.

Define $\varphi: gHg^{-1} \to H$ by $\varphi(x) = g^{-1}xg$. Note that this is a well defined function since $x \in gHg^{-1} \Rightarrow x = ghg^{-1}$, for some $h \in H$ and thus $\varphi(x) = \varphi(ghg^{-1}) = g^{-1}(ghg^{-1})g = h \in H$. this function is 1-1 and onto.

1-1: Let $x, y \in gHg^{-1}$. Suppose that $\varphi(x) = \varphi(y) \iff g^{-1}xg = g^{-1}yg \iff x = y$

onto: Let $y \in H$. Consider the element $gyg^{-1} \in gHg^{-1}$. then:

$$\varphi(gyg^{-1}) = g^{-1}(gyg^{-1})g = (g^{-1}g)y(g^{-1}g) = y.$$

therefore, φ is 1-1 and onto. the sets gHg^{-1} and H have the same cardinality.

M403 - Enrique Areyan - Fall 2013 - HW3

(6)(d) Prove that if $G = \bigcup_{g \in G} gHg^{-1}$ then $H = G$.

Pf: First note that this is a case where G is finite. Hence, let $|G| = n$, for $n \in \mathbb{N}$, $n > 1$ ($n = 1$ is trivial $G = \langle e \rangle$).

By part (6)(a), for $g \in G$: gHg^{-1} is a subgroup of G.

By part (6)(b), if $g_1, g_2 \in G$ and $g_1 H = g_2 H$ then $g_1 H g_1^{-1} = g_2 H g_2^{-1}$

By part (6)(c), if $g \in G$ then $|gHg^{-1}| = |H|$.

therefore, in this case $G = \bigcup_{g \in G} gHg^{-1}$ consists of all distincts subgroups form by taking elements of g and constructing gHg^{-1}.

Hence,

$$G = \bigcup_{g \in G} gHg^{-1} = \bigcup_{\substack{\text{distinct} \\ \text{representatives} \\ g \in G}} gH$$

But then, let us count the elements in these sets. Note that since $G \subseteq H$, then G is finite $|G| = n$ and H is a subgroup of G has to be finite $|H| = m$. then

$$n = |G| = \left| \bigcup_{g \in G} gHg^{-1} \right| = \left| \bigcup_{\substack{\text{distinct} \\ \text{representative} \\ g \in G}} gH \right| \overset{\text{by part (b) \& (c)}}{=} |H| = m \implies n = m.$$

which means that G and H have the same cardinality. But these are finite sets, one contain in the other therefore, they must be equal $H = G$.