Homework 4

Aleck Zhao

October 6, 2016

Section 2.2: Groups

13. If G is any group, define $\alpha : G \to G$ by $\alpha(g) = g^{-1}$. Show that α is injective and surjective.

Proof. To show α is injective, consider g_1 and g_2 such that $\alpha(g_1) = \alpha(g_2)$. Then $g_1^{-1} = g_2^{-1}$, and left multiplying by $g_2 g_1$, we have

$$\begin{aligned} g_2 g_1 g_1^{-1} &= g_2 g_1 g_2^{-1} \\ g_2 &= g_2 g_1 g_2^{-1} \\ g_2 g_2 &= g_2 g_1 g_2^{-1} g_2 \\ g_2 g_2 &= g_2 g_1 \end{aligned}$$

and by the cancellation law, we have $g_2 = g_1$, so α is injective, as desired.

To show α is surjective, we must show that for all $g \in G$, there exists a $g_0 \in G$ such that $\alpha(g_0) = g$. Since $gg^{-1} = 1$ it follows that $(g^{-1})^{-1} = g$, so then $g_0 = g^{0-1}$ will satisfy this, and since G is a group, every element has an inverse, so α is surjective, as desired.

□

Section 2.3: Subgroups

2. If H is a subset of a group G, show that H is a subgroup if and only if H is nonempty and $ab^{-1} \in H$ whenever $a \in H$ and $b \in H$.

Proof. If H is a subgroup, then H must contain at least $1 \in G$, so H is nonempty. Then if $a, b \in H$, we have $b^{-1} \in H$ so $ab^{-1} \in H$ since H is a subgroup, as desired.

For the other direction, if H is nonempty, then suppose it contains at least 1 element. If it has 1 element, say a, then $aa^{-1} = 1 \in H$ which is the trivial subgroup. On the other hand, if H contains more than 1 element, for $a, b \in H$, we have $ab^{-1} \in H$. Since we know $1 \in H$ it follows that if $b \in H$ then $1 \cdot b^{-1} = b^{-1} \in H$ is the inverse of a which is also contained in H. Thus since $a, b^{-1} \in H$, we have $a(b^{-1})^{-1} = ab \in H$. Thus H is a subgroup, as desired.

□

5. (a) If G is an abelian group, show that $H = \{a \in G | a^2 = 1\}$ is a subgroup of G.

Proof. Clearly $1 \cdot 1 = 1$ so $1 \in H$. Then consider $a, b \in H$ so that $a^2 = b^2 = 1$. Then $aabb = 1$ and since G is abelian, we have $(ab)(ab) = 1$, so $(ab)^2$ so $ab \in H$ as well. Finally, if $a \in H$ then $a^2 = 1$ so $a = a^{-1}$, thus $(a^{-1})^2 = 1$ so $a^{-1} \in H$. Thus H is a subgroup as desired. □

(b) Give an example where H is not a subgroup.

Solution. When G is not abelian, then H is not necessarily a subgroup. For example, consider the group $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ where H is then $\{\varepsilon, \tau, \tau\sigma, \tau\sigma^2\}$. However, we have $\tau(\tau\sigma) = \sigma \notin H$ so H is not a subgroup. □

8. If X is a nonempty subset of a group G, let $\langle X \rangle$ be the set of all products of powers of elements of X; more formally

$$\langle X \rangle = \left\{ x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} \mid m \geq 1, x_i \in X \right\}$$

(a) Show that $\langle X \rangle$ is a subgroup of G that contains X.

Proof. We have $1 \in \langle X \rangle$ if we take all the $k_i = 0$. Next, if two elements

$$\begin{aligned} a &= x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} \\ b &= x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \end{aligned}$$

are in $\langle X \rangle$, then we have

$$\begin{aligned} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} ab &= \left(x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} \right) \left(x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \right) \\ &= x_1^{k_1+i_1} x_2^{k_2+i_2} \cdots x_m^{k_m+i_m} \\ &= x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m} \end{aligned}$$

which is in $\langle X \rangle$ as well. Then if a is as above, its inverse is given by

$$a^{-1} = x_1^{-k_1} x_2^{-k_2} \cdots x_m^{-k_m}$$

which in particular is in $\langle X \rangle$ as well. Thus $\langle X \rangle$ is a subgroup of G, and it contains X because for each x_i in X, we can represent x_i with $k_i = 1$ and all other $k_j = 0$. □

(b) Show that $\langle X \rangle \subseteq H$ for every subgroup H such that $X \subseteq H$. Thus, $\langle X \rangle$ is the *smallest* subgroup of G that contains X, and is called the **subgroup generated** by X.

Proof. Let $X = \{x_1, x_2, \cdots, x_m\} \subset H$. Then since each of $x_i \in H$, it must be that $x_i^2 \in H$ and by induction $x_i^{k_i} \in H$ for any k_i. Thus since each of $x_1^{k_1}, x_2^{k_2}, \cdots, x_m^{k_m} \in H$, it must be that their product $x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} \in H$ as well for all k_i. This is exactly $\langle X \rangle$, so it follows that $\langle X \rangle \subseteq H$, with equality when $X = H$. □

13. (a) If G is a group, show that $H = \{(g, g) | g \in G\}$ is a subgroup of $G \times G$.

Proof. Since $1 \in G$ is the identity, we have $g \cdot 1 = g$, so $(g, f) \cdot (1, 1) = (g, f)$ for all $(g, f) \in G \times G$ thus $(1, 1)$ is the identity in $G \times G$ as well and is in H.
Since G is a group, if $g, h \in G$, we have $g + h \in G$. Next, if $(g, g), (h, h) \in H$, then $(g, g) \cdot (h, h) = (g + h, g + h) \in H$ as well.
Finally, since G is a group, if $g \in G$, its inverse $g^{-1} \in G$ as well. Thus if $(g, g) \in H$, its inverse is given by $(g^{-1}, g^{-1}) \in H$, so H is a subgroup, as desired. □

(b) Determine the groups G such that $H = \left\{(g, g^{-1}) | g \in G\right\}$ is a subgroup of $G \times G$.

Solution. If $(g, g^{-1}), (f, f^{-1}) \in H$, then the binary operation on them

$$(g, g^{-1}) \cdot (f, f^{-1}) = (gf, g^{-1}f^{-1}) = (gf, (fg)^{-1})$$

must also be in H in order for H to be a subgroup. Therefore, we must have $gf = fg$, so H is a subgroup if and only if $\boxed{G \text{ is abelian.}}$

□

22. Find $Z[GL_2(\mathbb{R})]$.

Solution. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$ be an arbitrary matrix, and let $Z = \begin{bmatrix} h & i \\ j & k \end{bmatrix} \in GL_2(\mathbb{R})$ be a center. Then we have

$$AZ = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} h & i \\ j & k \end{bmatrix} = \begin{bmatrix} ah + bj & ai + bk \\ ch + dj & ci + dk \end{bmatrix}$$
$$ZA = \begin{bmatrix} h & i \\ j & k \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ah + ic & bh + id \\ aj + ck & bj + dk \end{bmatrix}$$

If $AZ = ZA$, then we must have $ah + bj = ah + ic \implies bj = ci$ for all $b, c \in \mathbb{R}$. Since we have no control over what b and c are, it must be that $i = j = 0$. Then we must have $ai + bk = bk = bh + id = bh$ and $ch + dj = ch = aj + ck = ck$. Thus, we $h = k$, and the group of centers is given by the general form

$$Z\left(GL_2(\mathbb{R})\right) = \boxed{\left\{ \begin{bmatrix} h & 0 \\ 0 & h \end{bmatrix} \middle| h \in \mathbb{R} \right\}}$$

□

Section 2.4: Cyclic Groups and the Order of an Element

6. If G is a group and $g \in G$, show that $\langle g \rangle = \langle g^{-1} \rangle$.

Proof. For some $f \in \langle g \rangle$, we have $f = g^k$ for some $k \in \mathbb{Z}$. Then $f = (g^{-k})^{-1} = (g^{-1})^{-k} \in \langle g^{-1} \rangle$ so it follows that $g \in \langle g^{-1} \rangle$, thus $\langle g \rangle \subset \langle g^{-1} \rangle$.

Similarly, if $h \in \langle g^{-1} \rangle$, then $h = (g^{-1})^n$ for some $n \in \mathbb{Z}$. Then $h = g^{-n}$ so $h \in \langle g \rangle$, thus $\langle g^{-1} \rangle \subset \langle g \rangle$, so in fact $\langle g \rangle = \langle g^{-1} \rangle$, as desired.

□

7. Let $o(g) = 20$ in a group G. Compute

   (a) $o(g^2)$

   Answer. Since $o(g) = 20$, that means $g^{20} = 1$. Then $(g^2)^{10} = g^{20} = 1$, so $o(g^2) = \boxed{10.}$

   (b) $o(g^8)$

   Answer. Since $o(g) = 20$, that means $g^{20} = 1$. Then $(g^8)^5 = g^{40} = (g^{20})^2 = 1$, so $o(g^8) = \boxed{5.}$.

   (c) $o(g^5)$

   Answer. Since $o(g) = 20$, that means $g^{20} = 1$. Then $(g^5)^4 = g^{20} = 1$, so $o(g^5) = \boxed{4.}$

   (d) $o(g^3)$

   Answer. Since $o(g) = 20$, that means $g^{20} = 1$. Then $(g^3)^{20} = (g^{20})^3 = 1$, so $o(g^3) = \boxed{20.}$

10. (a) If $gh = hg$ in a group and $o(g)$ and $o(h)$ are finite, show that $o(gh)$ is finite.

   Proof. Let $o(g) = n$ and $o(h) = m$, so that $g^n = h^m = 1$. Then $(g^n)^m = 1 = (h^m)^n$ so the product $g^{mn}h^{mn} = 1$. Since $gh = hg$, we have $(gh)^{mn} = 1$, thus $o(gh)$ must divide mn. Since mn is finite, it follows that $o(gh)$ must be finite too. □

   (b) Show that (a) fails if $gh \neq hg$ by considering $g = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $h = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$.

   Proof. We have $g^4 = I$ so $o(g) = 4$, and $h^3 = I$ so $o(h) = 3$ so $o(g)$ and $o(h)$ are both finite. Now,

$$gh = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

   and we claim that

$$(gh)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

   for all $n \geq 1$, which we show by induction. The base case $n = 1$ is already given. Next, suppose this holds for arbitrary k. Then

$$(gh)^k(gh) = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix} = (gh)^{k+1}$$

   so the claim is proved. In particular, $n \neq 0$ for any $n \geq 1$, so $(gh)^n \neq I$ for any n, thus $o(gh) = \infty$. □

18. If $G = \langle g \rangle$ and $H = \langle h \rangle$, show that $G \times H = \langle (g,1), (1,h) \rangle$

Proof. Consider some $(a,b) \in G \times H$, so that $a \in \langle g \rangle$ and $b \in \langle h \rangle$. That means $a = g^i$ and $b = h^j$ where $i, j \in \mathbb{Z}$. Then the element (g^i, h^j) can be represented as the product $(g^i, 1) \cdot (1, h^j) = [(g,1)]^i \, [(1,h)]^j$ so

$$(a,b) = (g^i, h^j) \in \langle (g,1), (1,h) \rangle$$

and thus $G \times H \subset \langle (g,1), (1,h) \rangle$.

Next, for some element in $\langle (g,1), (1,h) \rangle$, we can express it in the form $(g,1)^n \cdot (1,h)^m$ for some $n, m \in \mathbb{Z}$. This is exactly

$$(g,1)^n \cdot (1,h)^m = (g^n, 1) \cdot (1, h^m) = (g^n, h^m)$$

which is an element of the Cartesian product $\langle g \rangle \times \langle h \rangle$. Thus $\langle (g,1), (1,h) \rangle \subset G \times H$, so in fact $G \times H = \langle (g,1), (1,h) \rangle$, as desired. □