Chris Hayduk
Math B4900
Homework 3
9/25/2020

1. **Group actions**

(a) For some fixed $g \in G$, prove that conjugation by $g$ (i.e. the map $G \to G$ defined by $a \mapsto gag^{-1}$) is an automorphism of $G$. Deduce that $a$ and $gag^{-1}$ have the same order (by last week's work), and for any non-empty $S \subseteq G$, the map

$$S \to gSg^{-1} \quad \text{defined by} \quad s \mapsto gsg^{-1}$$

is also a bijection, so that $|gSg^{-1}| = |S|$.
[Recall, even if $A$ and/or $B$ is infinite, we say $|A| = |B|$ exactly when there is a bijection $A \leftrightarrow B$]

*Proof.* Fix $g \in G$. Define $\varphi_g(a) = gag^{-1}$ for every $a \in G$. In order to show that $\varphi_g$ is an automorphism of $G$, we must show that $\varphi_G$ is a bijection from to $G$ to $G$ and that

$$\varphi_g(ab) = \varphi_g(a)\varphi_g(b)$$

for all $a, b \in G$.

First, we have that $\phi_g$ is well-defined. This is true because $G$ is a group, so $gag^{-1} \in G$ for every $a \in G$.

Now fix $a, b \in G$ and suppose $\varphi_g(a) = \varphi_g(b)$. Then we have,

$$\begin{aligned} &\varphi(a) = \varphi(b) \\ \implies &gag^{-1} = gbg^{-1} \end{aligned}$$

Multiplying by $g^{-1}$ on the left and $g$ on the right on both sides of the equal signs yields

$$a = b$$

Hence, $\varphi_g$ is injective.

Now fix $c \in G$. Since $G$ is a group, we have $g^{-1}cg \in G$. Hence this gives us that,

$$\begin{aligned} \varphi_g(g^{-1}cg) &= g(g^{-1}cg)g^{-1} \\ &= c \end{aligned}$$

Since $c$ was arbitrary, this holds for every element in $G$. Hence, $\varphi$ is surjective as well and is thus a bijection from $G$ to $G$.

Now we will check the homomorphism property. Fix $a, b \in G$. Then,

$$\begin{aligned} \varphi_g(ab) &= gabg^{-1} \\ &= ga(g^{-1}g)bg^{-1} \\ &= (gag^{-1})(gbg^{-1}) \\ &= \varphi_g(a)\varphi_g(b) \end{aligned}$$

Hence, $\varphi_g$ is a bijective homorphism and thus an autmorphism of $G$. From problem 2b(iii) on Homework 2, we have that

$$|a| = |gag^{-1}|$$

as a consequence of $\varphi_g$ being an automorphism.

Now for any non-empty $S \subset G$ we consider the map

$$S \to gSg^{-1} \text{ defined by } s \to gsg^{-1}$$

Since every element of $S$ is an element of $G$ and $G$ is a group, we have that $gsg^{-1} \in G$ for every $g \in G$ and $s \in S$. Hence, for every $g$, we have that

$$gSg^{-1} \subset G$$

So our map sends the subsets of $G$ to the subsets of $G$. Let $S, R \in \mathcal{P}(G)\backslash\varnothing$. Suppose $gSg^{-1} = gRg^{-1}$. Then we have

$$\begin{aligned} &(g^{-1}g)S(g^{-1}g) = (g^{-1}g)R(g^{-1}g) \\ &\implies S = R \end{aligned}$$

So our map is injective. Now let $S \in \mathcal{P}(G)\backslash\varnothing$. Observe, that since $G$ is a group, for every $s \in S$, there exists an element $g^{-1}sg \in G$. Hence, we can define the set $R \subset G\backslash\varnothing$ such that every element $r \in R$ is defined to be $g^{-1}sg$ for some $s \in S$. Ensure that each $s$ is used to define exactly one $r$. Then, we have for all $r \in R$,

$$\begin{aligned} grg^{-1} &= g(g^{-1}sg)g^{-1} \\ &= s \end{aligned}$$

Hence, we have that $gRg^{-1} = S$, and so our map is surjective and hence bijective.

Now consider again sets $S, R \in \mathcal{P}(G)\backslash\varnothing$. Then we have

$$\begin{aligned} gSRg^{-1} &= gS(g^{-1}g)Rg^{-1} \\ &= (gSg^{-1})(gRg^{-1}) \end{aligned}$$

So the map is homomorphism and hence and isomorphishm. Thus, again from problem 2b(iii) on Homework 2, we can assert that

$$|S| = |gSg^{-1}|$$

for every $S \in \mathcal{P}(G)\backslash\varnothing$

$\square$

(b) Let $A$ be a non-empty set and let $0 < k \leqslant |A|$. Check that the action of the symmetric group $S_A$ on the set of size $k$ subsets of $A$ by

$$\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$$

satisfies the axioms of group actions. [Similar to the action of $D_{2n}$ on sets from lecture.]

*Proof.* Let $\sigma_1, \sigma_2 \in S_A$ and $a = \{a_1, \cdots a_k\} \subset A$. Then we have,

$$\begin{aligned} \sigma_2 \cdot (\sigma_1 \cdot a) &= \sigma_2 \cdot \{\sigma_1(a_1), \cdots \sigma_1(a_k)\} \\ &= \{\sigma_2(\sigma_1(a)), \cdots, \sigma_2(\sigma_1(a_k))\} \\ &= \{\sigma_2\sigma_1(a), \cdots, \sigma_2\sigma_1(a_k)\} \\ &= \sigma_1\sigma_2 \cdot \{a_1, \cdots, a_k\} \\ &= \sigma_1\sigma_2 \cdot a \end{aligned}$$

We also have,

$$\begin{aligned} 1 \cdot a &= \{1 \cdot a_1, \cdots 1 \cdot a_k\} \\ &= \{a_1, \cdots, a_k\} \\ &= a \end{aligned}$$

Hence, this action satisfies the axioms of group actions. ☐

(c) Let $G$ act on a set $A$. Prove that the relation $\sim$ on $A$ defined by

$$a \sim b \quad \text{if and only if} \quad a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation.

Note: the equivalence classes with respect to this relation are called **orbits**.

*Proof.* We need to check that this relation is reflexive, symmetric, and transitive. We will start with reflexivity. Since $G$ is a group, then $1 \in G$ and so we have

$$a = 1 \cdot a$$

Hence, we have $a \sim a$. Now let $a, b \in A$ and suppose $a \sim b$. Then,

$$a = g \cdot b$$

for some $g \in G$. Since $G$ is a group, we have $g^{-1} \in G$ and hence

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b)$$

By properties of group actions, we can write

$$\begin{aligned} g^{-1} \cdot a &= (g^{-1}g) \cdot b \\ &= b \end{aligned}$$

So we have that $b \sim a$ since $g^{-1} \in G$. Hence, the relation is symmetric.

Now let $a, b, c \in A$. Suppose $a \sim b$ and $b \sim c$. Then we have,

$$a = g_1 \cdot b$$

and

$$b = g_2 \cdot c$$

for some $g_1, g_2 \in G$. We can use our equation for $b$ and the properties of group action to rewrite $a$ as

$$a = (g_1 g_2) \cdot c$$

Since $g_1 g_2 \in G$, we have that $a \sim c$ and so the relation is transitive. Hence, this is an equivalence relation. $\square$

(d) Describe the orbits of the action of $S_4$ on 2-element subsets of $\{1,2,3,4\}$ (as in problem 1b).

*Answer.* The two element subsets of $\{1,2,3,4\}$ are: $\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$

We have,

$$\begin{aligned}
(2\ 3) \cdot \{1,2\} &= \{1,3\} \\
(3\ 4) \cdot \{1,3\} &= \{1,4\} \\
(1\ 2) \cdot \{1,4\} &= \{2,4\} \\
(3\ 4) \cdot \{2,4\} &= \{2,3\} \\
(2\ 3) \cdot \{2,4\} &= \{3,4\}
\end{aligned}$$

From the above equations, we have

$$\begin{aligned}
\{1,2\} &\sim \{1,3\} \\
&\sim \{1,4\} \\
&\sim \{2,4\} \\
&\sim \{2,3\}, \{3,4\}
\end{aligned}$$

Hence, by transitivity, all of two element subsets of $\{1,2,3,4\}$ belong to the same equivalence class under this relation. Thus, there is only one orbit for this relation.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

2. **Cyclic groups**

(a) If $x$ is an element of a finite group $G$ and $|x| = n = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show $|x| = |G|$ does not imply $G = \langle x \rangle$ if $G$ is an infinite group.

*Proof.* Suppose $G$ is a group with finite order and $x \in G$. Also suppose that $|x| = |G|$.

Now suppose there exists $y \in G$ such that $y \neq x^k$ for some $k \in \mathbb{Z}$. Note that since we know $|x| = n$, we can list out a subset of the elements in $G$. Hence, we have

$$\{1, x, x^2, \cdots, x^{n-1}, y\} \subset G$$

However, note that $\{1, x, x^2, \cdots, x^{n-1}, y\} = n + 1 > |G|$. But since this is a subset of $G$, we have that,

$$|\{1, x, x^2, \cdots, x^{n-1}, y\}| \leqslant G$$

So we have a contradiction and thus, this $y \neq x^k$ cannot exist. Hence, $G = \langle x \rangle$.

Now consider the infinite group $(\mathbb{R}, +)$. We have that $|\mathbb{R}| = \infty = |2|$. However, $\mathbb{R} \neq \langle 1 \rangle$ because $1 \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition, so $\mathbb{R} \backslash \mathbb{Z}$ is not generated by $\langle 1 \rangle$. $\square$

(b) Write $Z_{63} = \langle x \rangle$. For which integers $a$ does the map $\psi_a$ defined by

$$\psi_a : \bar{1} \to x^a$$

extend to a *well defined homomorphism* from $\mathbb{Z}/147\mathbb{Z}$ to $Z_{63}$? Can $\psi_a$ ever be a surjective homomorphism? [Take care to remember that the binary operation on the left is + and the binary operation on the right is $\times$: if the image of $\bar{1}$ is $x^a$, then the image of $\bar{1} + \bar{1} + \cdots + \bar{1} = \ell\bar{1}$ is $(x^a)^\ell$.]

*Answer.*

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(c) For $a \in \mathbb{Z}$, define

$$\sigma_a : Z_n \to Z_n \quad \text{by} \quad \sigma_a(x) = x^a \text{ for all } x \in Z_n.$$

Show that $\sigma_a$ is an automorphism of $Z_n$ if and only if $(a, n) = 1$.

*Proof.* Suppose that $\sigma_a$ is an automorphism of $Z_n$. Then $\sigma_a$ is a bijective homomorphism from $Z_n \to Z_n$. $\square$

(d) Under what circumstances does there exist a non-trivial homomorphism $\varphi : Z_n \to G$? [Note: $\varphi$ need not be injective or surjective; just well-defined, and not the map $g \mapsto 1$ for all $g$.]

(e) For which $n \in \mathbb{Z}_{\geqslant 1}$ is $(\mathbb{Z}/2^n\mathbb{Z})^\times$ cyclic? [Hint: Try to find more than one subgroup of order 2. Why would this prove $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is *not* cyclic? Start by doing some examples.]

(f) Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.