Moshe Mason Rubin

MATH 330 Homework #4

26 September 2016

Exercise 3.50. Give an example of an infinite group in which every proper sub-group is finite.

Example. Consider the infinite group $(\mathbb{Z}, +)$. Then any sub-group S of $\mathbb{Z}$ such that $S \subsetneq \mathbb{Z}$ is necessarily finite. $\square$

Exercise 3.53. Let H be a sub-group of G and

$$C(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$

Prove that $C(H)$ is a sub-group of G. This subgroups is called the ***centralizer*** of H in G.

Proof. By theorem from class, for $C(H) \subseteq G$ to be a sub-group of G, it is sufficient to show

1. For all $a, b \in C(H)$, $a \circ b \in C(H)$.

2. There exists $e \in C(H)$ such that $a \circ e = a = e \circ a$ for all $a \in C(H)$.

3. For all $a \in C(H)$ there exists $a^{-1} \in C(H)$ such that $a \circ a^{-1} = e = a^{-1} \circ a$.

1. Let $a, b \in C(H)$. Then $a, b \in G$ as $C(H)$ is a subset of G. Furthermore, $h \in G$ as $h \in H$ and H is a sub-group of G. Consider the expression

$$\begin{aligned} h \circ (a \circ b) &= (h \circ a) \circ b && \text{by associativity of elements of } G \\ &= (a \circ h) \circ b && \text{by assumption that } a \in C(H) \\ &= a \circ (h \circ b) && \text{by associativity of elements of } G \\ &= a \circ (b \circ h) && \text{by assumption that } b \in C(H) \\ &= (a \circ b) \circ h && \text{by associativity of elements of } G \end{aligned}$$

So $h \circ (a \circ b) = (a \circ b) \circ h$ for all $h \in H$. So $(a \circ b) \in C(H)$ by definition of $C(H)$. So $C(H)$ is closed under $\circ$.

2. e is an elements of G by assumption that G is a group. H is a sub-group of G means that the same e is identity in H. By definition, the identity e in H commutes with any group element in H. That is, $e \circ h = h \circ e = h$ for all $h \in H$. So $e \circ h = h \circ e \implies e \in C(H)$ by definition of $C(H)$.

3. Let $a \in C(H)$. Then $a \in G$ as $C(H) \subseteq G$. Then $a^{-1} \in G$ by assumption that G is a group. Then

$$\begin{aligned} a \circ h = h \circ a &\implies (a \circ h) \circ a^{-1} = (h \circ a) \circ a^{-1} \\ &\implies a^{-1} \circ \left[(a \circ h) \circ a^{-1}\right] = a^{-1} \circ \left[(h \circ a) \circ a^{-1}\right] \\ &\implies \left(a^{-1} \circ a\right) \circ \left(h \circ a^{-1}\right) = \left(a^{-1} \circ h\right) \circ \left(a \circ a^{-1}\right) \quad \text{by multiple applications of associativity in } G \\ &\implies e \circ \left(h \circ a^{-1}\right) = \left(a^{-1} \circ h\right) \circ e \quad \text{by definition of } a^{-1} \in G \\ &\implies h \circ a^{-1} = a^{-1} \circ h \quad \text{by definition of } e \end{aligned}$$

So $a^{-1} \in C(H)$ by definition. So $a \in C(H)$ implies that $a^{-1} \in C(H)$.

So this shows that $C(H)$ is a sub-group of G. $\square$

Exercise 3.54. Let H be a sub-group of G. If $g \in G$, show that $gHg^{-1} := \left\{g^{-1}hg : h \in H\right\}$ is also a sub-group of G.

Proof. By theorem from class, for $gHg^{-1} \subseteq G$ to be a sub-group of G, it is sufficient to show

1. For all $a, b \in gHg^{-1}$, $a \circ b \in gHg^{-1}$.

2. There exists $e \in gHg^{-1}$ such that $a \circ e = a = e \circ a$ for all $a \in gHg^{-1}$.

3. For all $a \in gHg^{-1}$ there exists $a^{-1} \in gHg^{-1}$ such that $a \circ a^{-1} = e = a^{-1} \circ a$.

Notice that gHg^{-1} is necessarily a subset of G as every element in H is contained in G (by assumption that H is a sub-group of G). So $g, h, g^{-1} \in G$. Furthermore, every element in gHg^{-1} is of the form $g^{-1}hg$, and G is closed by assumption that G is a group. So $gHg^{-1} \subseteq G$.

Let $a, b \in gHg^{-1}$. Then $a = g^{-1}h_a g$ and $b = g^{-1}h_b g$ for some $h_a, h_b \in H$.

1. Consider

$$\begin{aligned} ab &= \left(g^{-1}h_a g\right)\left(g^{-1}h_b g\right) \\ &= \left(g^{-1}h_a\right)\left(gg^{-1}\right)\left(h_b g\right) \quad \text{by associativity of elements of } G \\ &= \left(g^{-1}h_a\right)(e)\left(h_b g\right) \quad \text{by definition of } g^{-1} \\ &= \left(g^{-1}h_a\right)\left(h_b g\right), \quad \text{by definition of } e \\ &= g^{-1}\left(h_a h_b\right) g \quad \text{by associativity of elements of } G \end{aligned}$$

   and $(h_a h_b) \in H$ as H was assumed to be a sub-group, so H is closed. So $ab = g^{-1}(h_a h_b) g$ is of the form $g^{-1}hg$ for some $h \in H$. So gHg^{-1} is closed.

2. By assumption that H is a sub-group of G, $e \in H$. So $\left(g^{-1}eg\right) \in gHg^{-1}$ and

$$\begin{aligned} g^{-1}eg &= g^{-1}g \quad \text{by definition of } e \\ &= e, \quad \text{by definition of } g^{-1}. \end{aligned}$$

   So $\left(g^{-1}eg\right) \in gHg^{-1}$ and $g^{-1}eg = e$. so $e \in gHg^{-1}$.

3. By Proposition 3.4, if $a = g^{-1}h_a g$ then $a^{-1} = g^{-1}h_a^{-1}g$. So $a^{-1} \in gHg^{-1}$ if $h_a^{-1} \in H$, and h_a^{-1} is necessarily an element of H by assumption that H is a sub-group of G. So $a \in gHg^{-1} \implies a^{-1} \in gHg^{-1}$.

So this shows that gHg^{-1} is a sub-group of G. □

Exercise 4.1. Prove or disprove each of the following statements.

(a) $U(8)$ is cyclic

(b) All of the generators of $\mathbb{Z}_{60}$ are prime.

(c) $\mathbb{Q}$ is cyclic.

(d) If every proper sub-group of a group G is cyclic, then G is a cyclic group.

(e) A group with a finite number of sub-groups is finite.

Proof. (a) $U(8)$ is not cyclic as $U(8) = \{1, 3, 5, 7\}$ and $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. So there does not exist $g \in U(8)$ such that $\langle g \rangle = U(8)$.

(b) 1 is a generator of $\mathbb{Z}_{60}$ as $\langle 1 \rangle := \{n \cdot 1 : n \in \mathbb{Z}\} = \mathbb{Z}_{60}$, so not all generators of $\mathbb{Z}_{60}$ are prime.

(c) Consider $\frac{1}{2} \in \mathbb{Q}$. Then there does not exist an $x \in \mathbb{Q}$ such that $x^n = \frac{1}{2}$ for some $n \in \mathbb{N}$. So $\mathbb{Q}$ is not cyclic.

(d) As demonstrated in Example 5, every proper sub-group of the symmetries of an equilateral triangle S_3 is cyclic, however S_3 itself is not cyclic. So (d) is false.

(e)

□

Exercise 4.2. Find the order of each of the following elements.

(a) $5 \in \mathbb{Z}_12$

(b) $\sqrt{3} \in \mathbb{R}$

(c) $\sqrt{3} \in \mathbb{R}^*$

(d) $-i \in \mathbb{C}^*$

(e) $72 \in \mathbb{Z}_{240}$

(f) $312 \in \mathbb{Z}_{471}$

Proof. (a) $5(5) - 12(2) = 1 \implies 5 \cdot 5 \equiv 1 \pmod{12} \implies |5| = 5$

(b) $\sqrt{3}^n = 1$ for $n \in \mathbb{N}$ is a contradiction. So $|\sqrt{3}| = \infty$.

(c) $\sqrt{3}^n = 1$ for $n \in \mathbb{N}$ is a contradiction. So $|\sqrt{3}| = \infty$.

(d) $(-i)^4 = (-1)^4 (i)^4 = 1$. So $|-i| = 4$.

(e) $\gcd(72, 240) = 24$ so $|72| = \infty$ as there does not exist $n \in \mathbb{N}$ such that $72 \cdot n \equiv 1 \pmod{240}$.

(f) $\gcd(312, 471) = 3$ so $|312| = \infty$.

□

Exercise 4.4. Find the subgroups of $GL_2(\mathbb{R})$ generated by each of the following matrices.

(a) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

(e) $\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$

(f) $\begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$

Proof. (a) Notice $A^2 = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, $A^3 = A^{-1} = -A$, $A^4 = -A^2$, and $A^5 = A^1 = A$. So $\left\langle \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] \right\rangle = \left\{ \pm \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right], \pm \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \right\}$

(b) Notice $A^{-1} = A$. So $\left\langle \left[\begin{smallmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{smallmatrix}\right] \right\rangle = \left\{ \left[\begin{smallmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{smallmatrix}\right], I_2 \right\}$

(c) Notice

- $A^2 = \left[\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right]$
- $A^3 = A^2 A = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$
- $A^4 = A^3 A = \left[\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right] = -A$
- $A^5 = A^4 A = -A^2$
- $A^6 = A^4 A^2 = -A^3 = I_2$
- $A^7 = A^4 A^3 = -A^4 = A$

So $\left\langle \left[\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right] \right\rangle = \{\pm id, \pm A, \pm A^2\}$.

(d) Notice $A^{-1} = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $A^n = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ for $n \in \mathbb{N}$. So $\left\langle \left[\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right] \right\rangle = \{\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right] : n \in \mathbb{N}\}$.

□

Exercise 4.6. Find the order of every element in the symmetry group of the square, D_4.

Proof. Copy-paste from my last homework, the symmetries of a square are

$\circ$	id	ρ	ρ^2	ρ^3	$\mu_{x=0}$	$\mu_{y=0}$	$\mu_{y=x}$	$\mu_{y=-x}$
id	id	ρ	ρ^2	ρ^3	$\mu_{x=0}$	$\mu_{y=0}$	$\mu_{y=x}$	$\mu_{y=-x}$
ρ	ρ	ρ^2	ρ^3	id	$\mu_{y=x}$	$\mu_{y=-x}$	$\mu_{y=0}$	$\mu_{x=0}$
ρ^2	ρ^2	ρ^3	id	ρ	$\mu_{y=0}$	$\mu_{x=0}$	$\mu_{y=-x}$	$\mu_{y=x}$
ρ^3	ρ^3	id	ρ	ρ^2	$\mu_{y=-x}$	$\mu_{y=x}$	$\mu_{x=0}$	$\mu_{y=0}$
$\mu_{x=0}$	$\mu_{x=0}$	$\mu_{y=-x}$	$\mu_{y=0}$	$\mu_{y=x}$	id	ρ^2	ρ^3	ρ
$\mu_{y=0}$	$\mu_{y=0}$	$\mu_{y=x}$	$\mu_{y=0}$	$\mu_{y=-x}$	ρ^2	id	ρ	ρ^3
$\mu_{y=x}$	$\mu_{y=x}$	$\mu_{x=0}$	$\mu_{y=-x}$	$\mu_{y=0}$	ρ	ρ^3	id	ρ^2
$\mu_{y=-x}$	$\mu_{y=-x}$	$\mu_{y=0}$	$\mu_{y=x}$	$\mu_{x=0}$	ρ^3	ρ	ρ^2	id

So $|id|= 1$, $|\rho|= 4$, and $|\mu_{x=0}|= |\mu_{y=0}|= |\mu_{y=x}|= |\mu_{y=-x}|= 2$. □

Exercise 4.12. Find a cyclic group with exactly one generator. Can you find cyclic groups with exactly two generators? Four generators? How about n generators?

Proof. By Corollary 4.7, the only generator of $\mathbb{Z}_{60}$ is 1 as 1 is the only number < 60 and co-prime to 60.

Z_6 has two generators, 1 and 5 as 1 and 5 are the only numbers < 6 that are co-prime to 6.

Z_8 has two generators, $1, 3, 5$ and 7 as those are the numbers co-prime to 8. □