Moshe Mason Rubin

MATH 330 Homework #1

2 September 2016

1.1 (a) $A \cap B = \{2\}$ as 2 is the only even prime number in $\mathbb{N}$.

(b) $A \cup B = \{2, 3, 4, 5, 6, 7, 8, 10, \cdots\} = \{x : x \in \mathbb{N} \text{ and } (x \text{ is prime or } x \text{ is even})\}$.

(c) $B \cap C = \{5\}$ as 5 is the only multiple of 5 that is prime.

(d) $A \cap (B \cup C) = \{2, 10, 20, 30, \cdots\} = \{2, 10x : x \in \mathbb{N}\}$ as $B \cup C$ is a set containing all multiples of 5 and all prime numbers, so $A \cap (B \cup C)$ is the set of all *even* multiples of 5 and all *even* prime numbers.

1.17 $f : \mathbb{Q} \to \mathbb{Q}$ is a mapping if for every $a \in \mathbb{Q}$ there exists a unique $b \in \mathbb{Q}$ such that $f(a) = b$.

(a) $f(p/q) = \frac{p+1}{p-2}$ is not a mapping because $\frac{1}{2} = \frac{3}{6}$ but $f\left(\frac{1}{2}\right) = \frac{2}{-1} = -2$ and $f\left(\frac{3}{6}\right) = \frac{4}{1} = 4$.

(b) $f(p/q) = \frac{3p}{3q}$ is a mapping because for all $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$, $\frac{p}{q} = \frac{r}{s} \implies f(p/q) = f(r/s)$ as $f(p/q) = \frac{3p}{3q} = \frac{p}{q} = \frac{r}{s} = \frac{3r}{3s} = f(r/s)$. □

(c) $f(p/q) = \frac{p+q}{q^2}$ is not a mapping because $\frac{1}{2} = \frac{2}{4}$ but $f\left(\frac{1}{2}\right) = \frac{3}{2^2} = \frac{3}{4}$ but $f\left(\frac{2}{4}\right) = \frac{6}{4^2} = \frac{3}{8}$.

(d) $f(p/q) = \frac{3p^2}{7q^2} - \frac{p}{q}$ is a mapping because for all $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$, $\frac{p}{q} = \frac{r}{s} \implies f(p/q) = f(r/s)$ as $f(p/q) = \frac{3p^2}{7q^2} - \frac{p}{q} = \frac{3}{7}\left(\frac{p}{q}\right)^2 - \frac{p}{q} = \frac{3}{7}\left(\frac{r}{s}\right)^2 - \frac{r}{s} = \frac{3r^2}{7s^2} - \frac{r}{s} = f(r/s)$. □

1.19 By Theorem 1.4, $f : A \to B$ and $g : B \to C$ are both bijective because they are both invertible. By Theorem 1.3.4, because f and g are bijective, so $g \circ f : A \to C$ is bijective and by Theorem 1.4, it is invertible. So there exists a unique $(g \circ f)^{-1} : C \to A$ such that $(g \circ f)^{-1} \circ (g \circ f) = \mathrm{id}_A$ and $(g \circ f) \circ (g \circ f)^{-1} = \mathrm{id}_C$.

Notice that by Theorem 1.3.1, the assumption that f and g are invertible, and because $\mathrm{id}_B \circ f = f$, $\left(f^{-1} \circ g^{-1}\right) \circ (g \circ f) = f^{-1} \circ \left(g^{-1} \circ g\right) \circ f = f^{-1} \circ (\mathrm{id}_B \circ f) = f^{-1} \circ f = \mathrm{id}_A$. By the same reasoning, $(g \circ f) \circ \left(f^{-1} \circ g^{-1}\right) = g \circ \left(f \circ f^{-1}\right) \circ g^{-1} = (g \circ \mathrm{id}_B) \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_C$. So $f^{-1} \circ g^{-1}$ is the unique function $(g \circ f)^{-1}$ from above and $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$. □

1.25 (a) $x \sim y$ in $\mathbb{R}$ if $x \geq y$ is not an equivalence because it is not symmetric. For example, $10 \sim 5$ but $5 \not\sim 10$.

(b) $m \sim n$ in $\mathbb{Z}$ if $mn > 0$ is an equivalence relation as for all $m \in \mathbb{Z}$, $m \sim m$, $m \sim n \implies n \sim m$, and $m \sim n$ and $n \sim l \implies m \sim l$. This relation describes the first and fourth quadrants of the Cartesian plane (excluding $x = 0$ and $y = 0$).

(c) $x \sim y$ in $\mathbb{R}$ if $|x - y| \leq 4$ is not an equivalence relationship because it is not transitive. For example, $1 \sim 3$ and $3 \sim 7$ but $1 \not\sim 7$.

(d) $m \sim n$ in $\mathbb{Z}$ if $m \equiv n \,(\mathrm{mod} 6)$ is an equivalence relation. It describes the equivalence class $\mathbb{Z}/(\mathrm{mod} 6) := \{[x]_{\mathrm{mod}\ 6} : x \in \mathbb{Z}\}$ where $[x]_{\mathrm{mod}\ 6} := \{y \in \mathbb{Z} | y \equiv x \,(\mathrm{mod} 6)\}$.

2.1 $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n\,(n+1)\,(2n+1)}{6}$

Base case: $\mathbf{n = 1} \to \displaystyle\sum_{k=1}^{1} k^2 = 1^2 = 1$ and $\frac{1(1+1)(2*1+1)}{6} = \frac{1*2*3}{6} = 1$ ✓

Inductive step: Assume $\sum_{\mathbf{k=1}}^{\mathbf{n}} \mathbf{k^2} = \frac{\mathbf{n\,(n+1)\,(2n+1)}}{\mathbf{6}}$ **and show** $\sum_{\mathbf{k=1}}^{\mathbf{n+1}} \mathbf{k^2} = \frac{\mathbf{(n+1)\,[(n+1)+1]\,(2\,[n+1]+1)}}{\mathbf{6}}$.

$$\begin{aligned}
\sum_{k\,=1}^{n+1} k^2 &= \sum_{k=1}^{n} k^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + n^2 + 2n + 1 \quad \text{by inductive hypothesis} \\
&= \frac{(n^2+n)(2n+1)}{6} + n^2 + 2n + 1 = \frac{2n^3+n^2+2n^2+n}{6} + n^2 + 2n + 1 \\
&= \frac{2n^3+3n^2+n}{6} + \frac{6n^2+12n+6}{6} \\
&= \frac{2n^3+9n^2+13n+6}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{(n+1)\,[(n+1)+1]\,(2\,[n+1]+1)}{6}
\end{aligned}$$

So, by induction, for all $n \in \mathbb{N}$, $\sum_{k=1}^{n} k^2 = \frac{n\,(n+1)\,(2n+1)}{6}$. □

2.15 (a) 14 and 39

(i)
$$\begin{aligned}
39 &= 14q + r \quad \rightarrow \quad 39 = 14(2) + 11 \\
14 &= 11q + r \quad \rightarrow \quad 14 = 11(1) + 3 \\
11 &= 3q + r \quad \rightarrow \quad 11 = 3(3) + 2 \\
3 &= 2q + r \quad \rightarrow \quad 3 = 2(1) + \mathbf{1} \\
2 &= 1q + r \quad \rightarrow \quad 2 = 1(2) + 0
\end{aligned}$$

So $\gcd(14, 39) = 1$.

(ii)
$$\begin{aligned}
3 = 2(1) + 1 \quad \Longrightarrow \quad 3 - 2(1) &= 1 \quad \rightarrow \quad 3 - (11 - 3 \cdot 3) = 1 \\
4 \cdot 3 - 11 &= 1 \quad \rightarrow \quad 4(14 - 11) - 11 = 1 \\
4(14) - 5(11) &= 1 \quad \rightarrow \quad 4(14) - 5(39 - 14 \cdot 2) \\
14(\mathbf{14}) - 5(\mathbf{39}) &= 1
\end{aligned}$$

So $(r, s) \in \mathbb{Z}^2$ such that $\gcd(14, 39) = 14r + 39s$ is $(r, s) = (14, -5)$.

(b) 234 and 165

(i)
$$\begin{aligned}
234 &= 165q + r \quad \rightarrow \quad 234 = 165(1) + 69 \\
165 &= 69q + r \quad \rightarrow \quad 165 = 69(2) + 27 \\
69 &= 27q + r \quad \rightarrow \quad 69 = 27(2) + 15 \\
27 &= 15q + r \quad \rightarrow \quad 27 = 15(1) + 12 \\
15 &= 12q + r \quad \rightarrow \quad 15 = 12(1) + \mathbf{3} \\
12 &= 3q + r \quad \rightarrow \quad 12 = 3(4) + 0
\end{aligned}$$

So $\gcd(234, 165) = 3$.

(ii)

$$
\begin{array}{lll}
15 = 12(1) + 3 \implies & 3 = 15 - 12 & \to \quad 3 = 15 - (27 - 15) \\
& 3 = 2(15) - 27 & \to \quad 3 = 2(69 - 2 \cdot 27) - 27 \\
& 3 = 2(69) - 5(27) & \to \quad 3 = 2(69) - 5(165 - 2 \cdot 69) \\
& 3 = 12(69) - 5(165) & \to \quad 3 = 12(234 - 165) - 5(165) \\
& 3 = 12\,(\mathbf{234}) - 17\,(\mathbf{165}) &
\end{array}
$$

So $(r, s) \in \mathbb{Z}^2$ such that $\gcd(234, 165) = 234r + 165s$ is $(r, s) = (12, -17)$.

(c) 1739 and 9923

(i)

$$
\begin{array}{ll}
9923 = 1739q + r & \to \quad 9923 = 1739(5) + 1228 \\
1739 = 1228q + r & \to \quad 1739 = 1228(1) + 511 \\
1228 = 511q + r & \to \quad 1228 = 511(2) + 206 \\
511 = 206q + r & \to \quad 511 = 206(2) + 99 \\
206 = 99q + r & \to \quad 206 = 99(2) + 8 \\
99 = 8q + r & \to \quad 99 = 8(12) + 3 \\
8 = 3q + r & \to \quad 8 = 3(2) + 2 \\
3 = 2q + r & \to \quad 3 = 2(1) + \mathbf{1} \\
2 = 1q + r & \to \quad 2 = 1(2) + 0
\end{array}
$$

So $\gcd(1739, 9923) = 1$.

(ii)

$$
\begin{array}{ll}
1 = 3 - 2 & \to \quad 1 = 3 - (8 - 2 \cdot 3) \\
1 = 3 \cdot 3 - 8 & \to \quad 1 = 3(99 - 12 \cdot 8) - 8 \\
1 = 3 \cdot 99 - 37 \cdot 8 & \to \quad 1 = 3 \cdot 99 - 37(206 - 2 \cdot 99) \\
1 = 77 \cdot 99 - 37 \cdot 206 & \to \quad 1 = 77(511 - 2 \cdot 206) - 37 \cdot 206 \\
1 = 77 \cdot 511 - 191 \cdot 206 & \to \quad 1 = 77 \cdot 511 - 191(1228 - 2 \cdot 511) \\
1 = 459 \cdot 511 - 191 \cdot 1228 & \to \quad 1 = 459(1739 - 1228) - 191 \cdot 1228 \\
1 = 459 \cdot 1739 - 650 \cdot 1228 & \to \quad 1 = 459 \cdot 1739 - 650(9923 - 5 \cdot 1739)
\end{array}
$$

$1 = 3709\,(\mathbf{1739}) - 650\,(\mathbf{9923})$

So $(r, s) \in \mathbb{Z}^2$ such that $\gcd(1739, 9923) = 1739r + 9923s$ is $(r, s) = (3709, -650)$.

(d) 471 and 562

(i)

$$
\begin{array}{ll}
562 = 471q + r & \to \quad 562 = 471(1) + 91 \\
471 = 91q + r & \to \quad 471 = 91(5) + 16 \\
91 = 16q + r & \to \quad 91 = 16(5) + 11 \\
16 = 11q + r & \to \quad 16 = 11(1) + 5 \\
11 = 5q + r & \to \quad 11 = 5(2) + \mathbf{1} \\
5 = 1q + r & \to \quad 5 = 1(5) + 0
\end{array}
$$

So $\gcd(471, 562) = 1$.

(ii)
$$\begin{aligned}
1 &= 11 - 2 \cdot 5 && \rightarrow && 1 = 11 - 2(16 - 11) \\
1 &= 3 \cdot 11 - 2 \cdot 16 && \rightarrow && 1 = 3(91 - 5 \cdot 16) - 2 \cdot 16 \\
1 &= 3 \cdot 91 - 17 \cdot 16 && \rightarrow && 1 = 3 \cdot 91 - 17(471 - 5 \cdot 91) \\
1 &= 88 \cdot 91 - 17 \cdot 471 && \rightarrow && 1 = 88(562 - 471) - 17 \cdot 471
\end{aligned}$$

$1 = 88(\mathbf{562}) - 105\,(\mathbf{471})$

So $(r, s) \in \mathbb{Z}^2$ such that $\gcd(562, 471) = 562r + 471s$ is $(r, s) = (88, -105)$.

(e) 23,771 and 19,945

(i)
$$\begin{aligned}
23771 &= 19945q + r && \rightarrow && 23771 = 19945(1) + 3826 \\
19945 &= 3826q + r && \rightarrow && 19945 = 3826(5) + 815 \\
3826 &= 815q + r && \rightarrow && 3826 = 815(4) + 566 \\
815 &= 566q + r && \rightarrow && 815 = 566(1) + 249 \\
566 &= 249q + r && \rightarrow && 566 = 249(2) + 68 \\
249 &= 68q + r && \rightarrow && 249 = 68(3) + 45 \\
68 &= 45q + r && \rightarrow && 68 = 45(1) + 23 \\
45 &= 23q + r && \rightarrow && 45 = 23(1) + 22 \\
23 &= 22q + r && \rightarrow && 23 = 22(1) + \mathbf{1} \\
22 &= 1q + r && \rightarrow && 22 = 1(22) + 0
\end{aligned}$$

So $\gcd(23771, 19945) = 1$.

(ii)
$$\begin{aligned}
1 &= 23 - 22 && \rightarrow && 1 = 23 - (45 - 23) \\
1 &= 2 \cdot 23 - 45 && \rightarrow && 1 = 2(68 - 45) - 45 \\
1 &= 2 \cdot 68 - 3 \cdot 45 && \rightarrow && 1 = 2 \cdot 68 - 3(249 - 3 \cdot 68) \\
1 &= 11 \cdot 68 - 3 \cdot 249 && \rightarrow && 1 = 11(566 - 2 \cdot 249) - 3 \cdot 249 \\
1 &= 11 \cdot 566 - 25 \cdot 249 && \rightarrow && 1 = 11 \cdot 566 - 25(815 - 566) \\
1 &= 36 \cdot 566 - 25 \cdot 815 && \rightarrow && 1 = 36(3826 - 4 \cdot 815) - 25 \cdot 815 \\
1 &= 36 \cdot 2836 - 169 \cdot 815 && \rightarrow && 1 = 36 \cdot 3826 - 169(19945 - 5 \cdot 3826) \\
1 &= 881 \cdot 3826 - 169 \cdot 19945 && \rightarrow && 1 = 881(23771 - 19945) - 169 \cdot 19945
\end{aligned}$$

$1 = 811(\mathbf{23771}) - 1050(\mathbf{19945})$

So $(r, s) \in \mathbb{Z}^2$ such that $\gcd(23771, 19945) = 23771r + 19945s$ is $(r, s) = (881, -1050)$.

(f) -4357 and 3754

(i)
$$\begin{aligned}
4357 &= 3754q + r \quad \to \quad 4357 = 3754(1) + 603 \\
3754 &= 603q + r \quad \to \quad 3754 = 603(6) + 136 \\
603 &= 136q + r \quad \to \quad 603 = 136(4) + 59 \\
136 &= 59q + r \quad \to \quad 136 = 59(2) + 18 \\
59 &= 18q + r \quad \to \quad 59 = 18(3) + 5 \\
18 &= 5q + r \quad \to \quad 18 = 5(3) + 3 \\
5 &= 3q + r \quad \to \quad 5 = 3(1) + 2 \\
3 &= 2q + r \quad \to \quad 3 = 2(1) + \mathbf{1} \\
2 &= 1q + r \quad \to \quad 2 = 1(2) + 0
\end{aligned}$$

So $\gcd(-4357, 3754) = 1$.

(ii)
$$\begin{aligned}
1 &= 3 - 2 \quad \to \quad 1 = 3 - (5 - 3) \\
1 &= 2 \cdot 3 - 5 \quad \to \quad 1 = 2(18 - 3 \cdot 5) - 5 \\
1 &= 2 \cdot 18 - 7 \cdot 5 \quad \to \quad 1 = 2 \cdot 18 - 7(59 - 3 \cdot 18) \\
1 &= 23 \cdot 18 - 7 \cdot 59 \quad \to \quad 1 = 23(136 - 2 \cdot 59) - 7 \cdot 59 \\
1 &= 23 \cdot 136 - 53 \cdot 59 \quad \to \quad 1 = 23 \cdot 136 - 53(603 - 4 \cdot 136) \\
1 &= 235 \cdot 136 - 53 \cdot 603 \quad \to \quad 1 = 235(3754 - 6 \cdot 603) - 53 \cdot 603 \\
1 &= 235 \cdot 3754 - 1463 \cdot 603 \quad \to \quad 1 = 235 \cdot 3754 - 1463(4357 - 3754) \\
1 &= 1698(\mathbf{3754}) - 1463(\mathbf{4357}) \iff 1 = 1698(\mathbf{3754}) + 1463(-\mathbf{4357})
\end{aligned}$$

So $(r, s) \in \mathbb{Z}^2$ such that $\gcd(3754, -4357) = 3754r + (-4357)s$ is $(r, s) = (1698, 1463)$.

2.17 (a) Prove that $f_n < 2^n$.

Base case: $\mathbf{n = 1} \to\ f_1 = 1 < 2^1$. ✓

Base case: $\mathbf{n = 2} \to\ f_2 = 1 < 2^2$. ✓

Inductive step: Assume $\mathbf{f_{n-1} < 2^{n-1}}$ and $\mathbf{f_n < 2^n}$ and show that $\mathbf{f_{n+1} < 2^{n+1}}$.

$$\begin{aligned}
&f_{n+1} = f_{n-1} + f_n \text{ and } f_{n-1} < 2^{n-1} \text{ and } f_n < 2^n \\
&\implies f_{n-1} + f_n = f_{n+1} \\
&< 2^n + 2^{n-1} \\
&= 2^{n-1}(2 + 1) \\
&= 3 \cdot 2^{n-1} \\
&< 4 \cdot 2^{n-1} \\
&= 2^{n+1}
\end{aligned}$$

So, by induction, for all $n \in \mathbb{N}$, $f_n < 2^n$. □

(b) Prove that $f_{n+1}f_{n-1} = f_n^2 + (-1)^n, n \geq 2$.

Base case: $\mathbf{n = 2}$ $f_3 f_1 = f_2^2 + (-1)^2 \implies 2 \cdot 1 = 1 + 1 \implies 2 = 2$ ✓

Inductive step: Assume $\mathbf{f_{n+1}f_{n-1} = f_n^2 + (-1)^n}$ and show $\mathbf{f_{n+2}f_n = f_{n+1}^2 + (-1)^{n+1}}$.

$$
\begin{aligned}
f_{n+1}f_{n-1} &= f_n^2 + (-1)^n \quad \text{by induction hypothesis} \\
&\implies -f_{n+1}f_{n-1} = -f_n^2 + (-1)^{n+1} \\
&\implies -f_{n+1}\left(f_{n+1} - f_n\right) = -f_n^2 + (-1)^{n+1} \quad \text{by definition of Fibonacci numbers} \\
&\implies f_n f_{n+1} - f_{n+1}^2 = -f_n^2 + (-1)^{n+1} \\
&\implies f_n f_{n+1} + f_n^2 = f_{n+1}^2 + (-1)^{n+1} \\
&\implies f_n\left(f_{n+1} + f_n\right) = f_{n+1}^2 + (-1)^{n+1} \\
&\implies f_n f_{n+2} = f_{n+1}^2 + (-1)^{n+1}
\end{aligned}
$$

So for all $n \in \mathbb{N}$ such that $n \geq 2$, $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$. □

(c) Prove that $f_n = \frac{\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n}{2^n\sqrt{5}}$.

Base case: $\mathbf{n = 1}$ $\rightarrow$ $\frac{\left(1+\sqrt{5}\right)^1 - \left(1-\sqrt{5}\right)^1}{2\sqrt{5}} = \frac{2\sqrt{5}}{2\sqrt{5}} = 1$. ✓

Base case: $\mathbf{n = 2}$ $\rightarrow$ $\frac{\left(1+\sqrt{5}\right)^2 - \left(1-\sqrt{5}\right)^2}{2^2\sqrt{5}} = \frac{1+2\sqrt{5}+5-\left(1-2\sqrt{5}+5\right)}{4\sqrt{5}} = \frac{4\sqrt{5}}{4\sqrt{5}} = 1$. ✓

Inductive step: Assume $\mathbf{f_n = \frac{\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n}{2^n\sqrt{5}}}$ and $\mathbf{f_{n+1} = \frac{\left(1+\sqrt{5}\right)^{n+1} - \left(1-\sqrt{5}\right)^{n+1}}{2^{n+1}\sqrt{5}}}$ and show that $\mathbf{f_{n+2} = \frac{\left(1+\sqrt{5}\right)^{n+2} - \left(1-\sqrt{5}\right)^{n+2}}{2^{n+2}\sqrt{5}}}$.

$f_{n+2} = f_n + f_{n+1}$ by definition of Fibonacci numbers

$$
\begin{aligned}
f_n + f_{n+1} &= \frac{\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n}{2^n\sqrt{5}} + \frac{\left(1+\sqrt{5}\right)^{n+1} - \left(1-\sqrt{5}\right)^{n+1}}{2^{n+1}\sqrt{5}} \quad \text{by inductive hypothesis} \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n\left(1 + \frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^n\left(1 + \frac{1-\sqrt{5}}{2}\right)\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n\left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^n\left(\frac{3-\sqrt{5}}{2}\right)\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n\left[\frac{1}{4}\left(6+2\sqrt{5}\right)\right] - \left(\frac{1-\sqrt{5}}{2}\right)^n\left[\frac{1}{4}\left(6-2\sqrt{5}\right)\right]\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^n\left(\frac{1-\sqrt{5}}{2}\right)^2\right] \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right] \\
&= \frac{\left(1+\sqrt{5}\right)^{n+2} - \left(1-\sqrt{5}\right)^{n+2}}{2^{n+2}\sqrt{5}} = f_{n+2}
\end{aligned}
$$

(d) Show that $\lim_{n\to\infty} f_n/f_{n+1} = \frac{\sqrt{5}-1}{2}$.

Let $x = \lim_{n\to\infty}$

$$
\begin{aligned}
\lim_{n\to\infty}\frac{f_n}{f_{n+1}} &= \lim_{n\to\infty}\frac{f_{n+2} - f_{n+1}}{f_{n+1}} \\
&= \lim_{n\to\infty}\frac{f_{n+2}}{f_{n+1}} - 1 \\
&\implies \lim_{n\to\infty}\frac{f_n}{f_{n+1}} = \lim_{n\to\infty}\frac{f_{n+2}}{f_{n+1}} - 1
\end{aligned}
$$

Moshe Mason Rubin

MATH 330 Homework #2

9 September 2016

2.8 $(fg)^{(n)}(x) = \sum_{k=1}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x)$.

Notice $\binom{n}{k} + \binom{n}{k-1} := \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n+1-k)} = n!\left[\frac{n+1-k}{k!(n+1-k)!} + \frac{k}{k!(n+1-k)!}\right] = \frac{n!(n+1)}{k!(n-k+1)!} =: \binom{n+1}{k}$. So

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k} \tag{1}$$

Base Case $\mathbf{n = 1}$ $\rightarrow fg^{(1)} = \sum_{k=0}^{1} \binom{1}{k} f^{(k)}(x)\, g^{(n-k)}(x) = \binom{1}{0} f' g(x) + \binom{1}{1} f g'(x) = f'g + fg'$ which is true by product rule. ✓

Inductive step: Assume $(\mathbf{fg})^{(n)}(\mathbf{x}) = \sum_{\mathbf{k=1}}^{\mathbf{n}} \binom{\mathbf{n}}{\mathbf{k}} \mathbf{f^{(k)}(x) g^{(n-k)}(x)}$ and show $(\mathbf{fg})^{(n+1)}(\mathbf{x}) = \sum_{\mathbf{k=1}}^{\mathbf{n+1}} \binom{\mathbf{n+1}}{\mathbf{k}} \mathbf{f^{(k)}(x) g^{(n+1-k)}(x)}$.

$$\begin{aligned}
(fg)^{(n+1)}(x) &= \left[(fg)^{(n)}(x)\right]' \\
&= \left[\sum_{k=1}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x)\right]' \qquad \textit{by inductive hypothesis} \\
&= \left[\binom{n}{0} f g^{(n)} + \binom{n}{1} f' g^{(n-1)} + \binom{n}{2} f'' g^{(n-2)} + \cdots + \binom{n}{n-2} f^{(n-2)} g'' + \binom{n}{n-1} f^{(n-1)} g' \right. \\
&\qquad \left. + \binom{n}{n} f^{(n)} g\right]' \\
&= \binom{n}{0} f' g^{(n)} + \binom{n}{0} f g^{(n+1)} + \binom{n}{1} f'' g^{(n-1)} + \binom{n}{1} f' g^{(n)} + \binom{n}{2} f''' g^{(n-2)} \\
&\quad + \binom{n}{2} f'' g^{(n-1)} + \cdots + \binom{n}{n-2} f^{(n-1)} g'' + \binom{n}{n-2} f^{(n-2)} g''' + \binom{n}{n-1} f^{(n)} g' \\
&\quad + \binom{n}{n-1} f^{(n-1)} g'' + \binom{n}{n} f^{(n+1)} g + \binom{n}{n} f^{(n)} g' \qquad \textit{by base case} \\
&= \binom{n}{0} f g^{(n+1)} + \left(\binom{n}{0} + \binom{n}{1}\right) f' g^{(n)} + \left(\binom{n}{1} + \binom{n}{2}\right) f'' g^{(n-1)} + \cdots \\
&\quad + \left(\binom{n}{n-2} + \binom{n}{n-1}\right) f^{(n-1)} g'' + \left(\binom{n}{n-1} + \binom{n}{n}\right) f^{(n)} g' + \binom{n}{n} f^{(n+1)} g \\
&= \binom{n}{0} f g^{(n+1)} + \binom{n+1}{1} f' g^{(n)} + \binom{n+1}{2} f'' g^{(n-1)} + \cdots \\
&\quad + \binom{n+1}{n-1} f^{(n-1)} g'' + \binom{n+1}{n} f^{(n)} g' + \binom{n}{n} f^{(n+1)} g \qquad \textit{by equation (1)} \\
&= \binom{n+1}{0} f g^{(n+1)} + \binom{n+1}{1} f' g^{(n)} + \binom{n+1}{2} f'' g^{(n-1)} + \cdots + \binom{n+1}{n-1} f^{(n-1)} g'' \\
&\quad + \binom{n+1}{n} f^{(n)} g' + \binom{n+1}{n+1} f^{(n+1)} g, \quad \text{as } \binom{n}{0} = \binom{n+1}{0} = \binom{n}{n} = \binom{n+1}{n+1} = 1 \\
&= \sum_{k=1}^{n+1} \binom{n+1}{k} f^{(k)}(x) g^{(n+1-k)}(x)
\end{aligned}$$

So for all $n \in \mathbb{N}$, $(fg)^{(n)}(x) = \sum_{k=1}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x)$. □

2.27 Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

By Theorem 2.4, $\gcd(a, b) = 1 \implies$ there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b) = 1$.

$a|bc \implies$ there exists $k \in \mathbb{Z}$ such that $ak = bc$ by definition. So

$$\begin{aligned} ax + by = 1 &\implies acx + bcy = c \\ &\implies acx + aky = c \quad \text{as } ak = bc \\ &\implies a(cx + ky) = c \end{aligned}$$

Because $(cx + ky) \in \mathbb{Z}$, so $a|c$ by definition.

Lemma to 2.31 Let $x \in \mathbb{Z}$ such that $2|x^2$, then $2|x$.

Consider for a contradiction that $2|x^2$ but $2 \nmid x$. Then x must be of the form $x = 2c + 1$ for some $c \in \mathbb{Z}$ by the Remainder Theorem and assumption that $2 \nmid x$. Then $x^2 = c^2 + 2c + 1 = 2(c^2 + c) + 1 = 2c' + 1$. But $2 \nmid (2c' + 1)$, which is a contradiction to the assumption that $2|x^2$. So $2|x^2 \implies 2|x$.

2.31 Show $\sqrt{2} \notin \mathbb{Q}$.

Assume for a contradiction that $\sqrt{2} = \frac{p}{q}$, a fraction is lowest terms such that p and q share no divisors. Then $2 = \frac{p^2}{q^2}$.

$$\begin{aligned} 2 = \frac{p^2}{q^2} &\implies 2q^2 = p^2 \\ &\implies 2|p^2 \quad \text{by definition of divides} \\ &\implies 2|p \quad \text{by lemma to 2.31} \\ &\implies \text{There exists } k \in \mathbb{Z} \text{ such that } 2k = p \quad \text{by definition of divides} \end{aligned}$$

So,

$$\begin{aligned} 2q^2 = p^2 &\implies 2q^2 = (2k)^2 \quad \text{as } p = 2k \\ &\implies 2q^2 = 4k^2 \\ &\implies q^2 = 2k^2 \\ &\implies 2|q^2 \quad \text{by definition of divides} \\ &\implies 2|q \quad \text{by lemma to 2.31} \end{aligned}$$

But $2|p$ and $2|q$ is a contradiction as p and q were assumed to be co-prime. So our assumption that $\sqrt{2}$ can be written as a fraction is incorrect and $\sqrt{2} \notin \mathbb{Q}$. □

3.1 Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $3x \equiv 2 \pmod 7$

Notice $3 \cdot 5 \equiv 15 \equiv 1 \pmod 7$. So $3x \equiv 2 \pmod 7 \implies 5 \cdot 3x \equiv 5 \cdot 2 \pmod 7 \implies 15x \equiv 10 \pmod 7 \implies$ $\boxed{x \equiv 3 \pmod 7}$

(b) $5x + 1 \equiv 13 \pmod{23}$

Notice that $\gcd(23, 5) = 1$:

$$\begin{aligned} 23 = 5q + r &\quad \to \quad 23 = 5(4) + 3 \\ 5 = 3q + r &\quad \to \quad 5 = 3(1) + 2 \\ 3 = 2q + r &\quad \to \quad 3 = 2(1) + \mathbf{1} \\ 2 = 1q + r &\quad \to \quad 2 = 1(2) + 0 \end{aligned}$$

Furthermore, $3 - 2 = 1 \implies 3 - (5 - 3) = 1 \implies 2(3) - 5(1) = 1 \implies 2(23 - 5 \cdot 4) - 5 = 1 \implies 2 \cdot 23 - 9 \cdot 5 = 1 \implies 23|(1 + 9 \cdot 5) \implies -9 \cdot 5 \equiv 1 \pmod{23}$.

So $5x + 1 \equiv 13 \pmod{23} \implies 5x \equiv 12 \pmod{23} \implies -9 \cdot 5x \equiv -9 \cdot 12 \pmod{23} \implies -45x \equiv -108 \pmod{23} \implies$ $\boxed{x \equiv 7 \pmod{23}}$

(c) $5x + 1 \equiv 13 \pmod{26}$

Notice $\gcd(5, 26) = 1$ and $26 - 5(5) = 1 = \gcd(5, 26)$. So $5x + 1 \equiv 13 \pmod{26} \implies 5x \equiv 12 \pmod{26} \implies -5(5) \equiv -5(12) \pmod{26} \implies \boxed{x \equiv 18 \pmod{26}}$

(d) $9x \equiv 3 \pmod{5}$

Notice $\gcd(9, 5) = 1$ and $9(4) + 5(-7) = 1 = \gcd(9, 5)$. So $9x \equiv 3 \pmod{5} \implies 4 \cdot 9x = 4 \cdot 3 \pmod{5} \implies \boxed{x \equiv 12 \equiv 2 \pmod{5}}$

(e) $5x \equiv 1 \pmod{6}$

Notice $\gcd(5, 6) = 1$ and $6 - 5 = 1 = \gcd(5, 6)$. So $5x \equiv 1 \pmod{6} \implies -5x \equiv -1 \pmod{6} \implies \boxed{x \equiv 5 \pmod{6}}$

(f) $3x \equiv 1 \pmod{6}$

By Proposition 3.1.6, $\gcd(3, 6) \neq 1 \implies$ there exists no $b \in \mathbb{Z}_n$ such that $3b = 1 \pmod{6}$. So this equation has no solutions.

3.2 Which of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group?

(a) is not a group. a is the element such that $a \circ x = x$ for all $x \in G$, however, $x \circ a \neq x$,so (a) is not a group.

(b) is a group.

(c) is a group.

(d) is not a group because it is not associative. For example, $(b \circ c) \circ d$ should equal $b \circ (c \circ d)$, but $(b \circ c) \circ d = d$ and $b \circ (c \circ d) = a$

3.3 Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$.

1. Rotations of a rectangle:

$\circ$	id	ρ_{180°	μ_y	μ_x
id	id	ρ_{180°	μ_y	μ_x
ρ_{180°	ρ_{180°	id	μ_x	μ_y
μ_y	μ_y	μ_x	id	ρ_{180°
μ_x	μ_x	μ_y	ρ_{180°	id

2. $(\mathbb{Z}_4, +)$:

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

3.6 Give a multiplication table for the group $U(12)$.

$U(n) = \{x \in \mathbb{Z}_n | \gcd(n, x) = 1\} \implies U(12) = \{1, 5, 7, 11\}$.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

3.7 Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

An *abelian group* is a group G such that $a * b = b * a$ for all $a, b \in G$.

Associative For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

$$\begin{aligned}(a * b) * c &= (a * b) + c + (a * b)c \quad \text{by definition of } a * b \\ &= (a + b + ab) + c + (a + b + ab)c \quad \text{by definition of } a * b \\ &= a + b + c + ab + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + (b * c) + a(b * c) \quad \text{by definition of } a * b \\ &= a * (b * c) \quad \text{by definition of } a * b\end{aligned}$$

Identity element There exists an element $e \in G$ such that for any $a \in G$, $e * a = a * e = a$.

For any a, let $b = 0$. Then $a * b = a + 0 + a(0) = a = 0 + a + 0(a) = b * a$. So $b = 0$ is the identity element such that $a * 0 = 0 * a$ for all $a \in G$.

Inverse element For each element $a \in G$ there exists an $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

We know from above that $e = 0$. So given $a \in G$,

$$\begin{aligned}a + b + ab &= 0 \\ &\implies b(1 + a) + a = 0 \\ &\implies b = \frac{-a}{1 + a}\end{aligned}$$

which is defined for all $x \in S$. So $b = \frac{-a}{1+a}$ is the unique inverse element a^{-1} to each a such that $a * a^{-1} = a^{-1} * a = e$.

Commutative For all $a, b \in G$, $a * b = b * a$.

$$\begin{aligned}a * b &= a + b + ab \\ &= b + a + ab \quad \text{by commutative property of addition} \\ &= b + a + ba \quad \text{by commutative property of multiplication} \\ &= b * a \quad \text{by definition}\end{aligned}$$

So $(S, *)$ is an abelian group. □

3.10 Prove that the set of matrices of the form $\left[\begin{smallmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right]$ is a group under matrix multiplication. Matrix multiplication in the Heisenberg group is defined by

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x + x' & y + y' + xz' \\ 0 & 1 & z + z' \\ 0 & 0 & 1 \end{bmatrix}$$

Associative For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

$$
\begin{aligned}
(a \cdot b) \cdot c &= \begin{bmatrix} 1 & a_x b_y & a_y b_y + a_x b_z \\ 0 & 1 & a_z + b_z \\ 0 & 0 & 1 \end{bmatrix} \cdot c \quad \text{by definition} \\
&= \begin{bmatrix} 1 & a_x + b_x + c_x & a_y + b_y + c_y + a_x b_z + a_x c_z + b_x c_z \\ 0 & 1 & a_z + b_z + c_z \\ 0 & 1 & 1 \end{bmatrix} \quad \text{by definition} \\
&= \begin{bmatrix} 1 & a_x + (b_x + c_x) & a_y + (b_y + c_y + b_x c_z) + a_x (b_z + c_z) \\ 0 & 1 & a_z + (b_z + c_z) \\ 0 & 0 & 1 \end{bmatrix} \\
&= a \cdot \begin{bmatrix} 1 & b_x + c_x & b_y + c_y + b_x c_z \\ 0 & 1 & b_z + c_z \\ 0 & 0 & 1 \end{bmatrix} \quad \text{by definition} \\
&= a \cdot (b \cdot c) \quad \text{by definition}
\end{aligned}
$$

Identity element There exists an element $e \in G$ such that for any $a \in G$, $e \cdot a = a \cdot e = a$.

Let $e = I_3 = \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$. Then

$$
\begin{aligned}
\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & x + 0 & y + 0 + x(0) \\ 0 & 1 & z + 0 \\ 0 & 1 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 + x & 0 + y + 0(z) \\ 0 & 1 & 0 + z \\ 0 & 1 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}
\end{aligned}
$$

So $e = I_3$ is the identity element such that $e \cdot a = a = a \cdot e$ for all $a \in G$.

Inverse element For each element $a \in G$ there exists an $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

For each $a = \left[\begin{smallmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right] \in G$, it's inverse a^{-1} is given by the inverse matrix of a, $a^{-1} = \left[\begin{smallmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{smallmatrix}\right]$ (by linear algebra),

as

$$\begin{aligned}
a \cdot a^{-1} &= \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & x+(-x) & y+(xz-y)+x(-z) \\ 0 & 1 & z+(-z) \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3 \\
&= \begin{bmatrix} 1 & (-x)+x & (xz-y)+y+(-x)z \\ 0 & 1 & (-z)+z \\ 0 & 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \\
&= a^{-1} \cdot a
\end{aligned}$$

So $a^{-1} = \left[\begin{smallmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{smallmatrix}\right]$ is the unique inverse element to each a such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

So the set of matrices of the form $\left[\begin{smallmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right]$ is a group under matrix multiplication. □

Moshe Mason Rubin

MATH 330 Homework #3

19 September 2016

Exercise 3.8. Give an example of two elements A and B in $GL_2(\mathbb{R})$ with $AB \neq BA$.

Solution. Let $A = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right]$. Then $A, B \in GL_2(\mathbb{R})$ as A^{-1} and B^{-1} are given by $A^{-1} = \left[\begin{smallmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{smallmatrix}\right]$ and $B^{-1} = \left[\begin{smallmatrix} -4 & 3 \\ \frac{7}{2} & -\frac{5}{2} \end{smallmatrix}\right]$. However,

$$AB = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix} \neq \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix} = BA$$

So $BA \neq AB$ for $A = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right]$. □

Exercise 3.12. Let $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on $\mathbb{Z}_2^n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)\,.$$

Prove that $\mathbb{Z}_2^n$ is a group under this operation.

Proof:

Associative Let $a, b, c \in \mathbb{Z}_2^n$ such that $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n)$, and $c = (c_1, c_2, \ldots, c_n)$. Then

$$\begin{aligned}
(a+b)+c &= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) + c \quad \text{by definition of } a+b \\
&= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2, \ldots, (a_n + b_n) + c_n) \quad \text{by definition of a+b} \\
&= (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), \ldots, a_n + (b_n + c_n)) \quad \text{by associativity of real addition} \\
&= a + (b_1 + c_1, b_2 + c_2, \ldots, b_n + c_n) \quad \text{by definition of } a+b \\
&= a + (b + c) \quad \text{by definition of } a+b
\end{aligned}$$

So $+$ is associative in $\mathbb{Z}_2^n$.

Identity For $a \in \mathbb{Z}_2^n$ let b be given by $b = (0, 0, \ldots, 0)$. Then $b \in \mathbb{Z}_2^n$ as $0 \in \mathbb{Z}_2$. Then

$$\begin{aligned}
a + b &= (a_1 + 0, a_2 + 0, \ldots, a_n + 0) \quad \text{by definition of } a+b \\
&= (a_1, a_2, \ldots, a_n) \quad \text{as 0 is the additive identity in } \mathbb{Z}_2^n \\
&= a \quad \text{by definition of } a \qquad (1) \\
&= (0 + a_1, 0 + a_2, \ldots, 0 + a_n) \quad \text{as 0 is the additive identity in } \mathbb{Z}_2^n \\
&= b + a \quad \text{by definition of } a+b \qquad (2)
\end{aligned}$$

So (1) and (2) imply that $a + b = a = b + a$ for $b \in \mathbb{Z}_2^n$ given by $b = (0, 0, \ldots, 0)$. So there exists an identity in $\mathbb{Z}_2^n$ under $+$.

Inverse For $a \in \mathbb{Z}_2^n$ let $b = a$. Then

$$\begin{aligned}
a + b &= ([a_1 + b_1]_2, [a_2 + b_2]_2, \ldots, [a_n + b_n]_2) \quad \text{by definition of } a+b \\
&= ([2a_1]_2, [2a_2]_2, \ldots, [2a_n]_2) \quad \text{as } a_i = b_i \text{ for } i \in (\mathbb{Z} \cap [1, n]) \\
&= (0, 0, \ldots, 0) \quad \text{as } [2k]_2 = 0 \text{ for all } k \in \mathbb{Z}. \text{ Notice } (0, 0, \ldots, 0) \text{ is the additive inverse from above.} \qquad (3) \\
&= ([2a_1]_2, [2a_2]_2, \ldots, [2a_n]_2) = ([b_1 + a_1]_2, [b_2 + a_2]_2, \ldots [b_n + a_n]_2) \quad \text{as } a_i = b_i \text{ for } i \in (\mathbb{Z} \cap [1, n]) \\
&= b + a \quad \text{by definition of } a+b \qquad (4)
\end{aligned}$$

So (3) and (4) imply that for all $a \in \mathbb{Z}_2^n$, a is its own inverse element under $+$.

So $(\mathbb{Z}_2^n, +)$ is a group. □

Exercise 3.15. Prove or disprove that every group containing six elements is abelian.

Counterexample. Consider the group $D_3 = \{id, \rho, \rho^2, \tau_A, \tau_B, \tau_C\}$ which contains exactly 6 elements with $id = \left(\begin{smallmatrix} a & b & c \\ a & b & c \end{smallmatrix}\right)$, $\rho = \left(\begin{smallmatrix} a & b & c \\ b & c & a \end{smallmatrix}\right)$, $\rho^2 = \left(\begin{smallmatrix} a & b & c \\ c & a & b \end{smallmatrix}\right)$, $\tau_A = \left(\begin{smallmatrix} a & b & c \\ a & c & b \end{smallmatrix}\right)$, $\tau_B = \left(\begin{smallmatrix} a & b & c \\ c & b & a \end{smallmatrix}\right)$, and $\tau_C = \left(\begin{smallmatrix} a & b & c \\ b & a & c \end{smallmatrix}\right)$. D_3 is *not* abelian. For example,

$$\begin{aligned}\tau_A\tau_B &= \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \\ &= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \rho\end{aligned}$$

but

$$\begin{aligned}\tau_B\tau_A &= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \\ &= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \rho^2\end{aligned}$$

So D_3 is an example of a group containing 6 elements that is not abelian. □

Exercise 3.26. Prove that the inverse of $g_1g_2\cdots g_n$ is $g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}$.

Proof. **Base case $\mathbf{n = 2}$** If $n = 2$ then $g_2^{-1}g_1^{-1}$ is the inverse of g_1g_2 as

$$\begin{aligned}(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) &= g_1\left(g_2g_2^{-1}\right)g_1^{-1} \quad \text{by associativity} \\ &= g_1(e)g_1^{-1} \quad \text{by definition of } g_2^{-1} \\ &= g_1g_1^{-1} \quad \text{by definition of } e \\ &= e \quad \text{by definition of } g_1^{-1} \qquad (5) \\ &= g_2^{-1}g_2 \quad \text{by definition of } g_2^{-1} \\ &= g_2^{-1}(e)g_2 \quad \text{by definition of } e \\ &= g_2^{-1}\left(g_1^{-1}g_1\right)g_2 \quad \text{by definition of } g_1^{-1} \\ &= \left(g_2^{-1}g_1^{-1}\right)(g_1g_2) \qquad (6)\end{aligned}$$

So (5) and (6) imply that $\left(g_2^{-1}g_1^{-1}\right)$ is unique inverse element such that $(g_1g_2)\left(g_2^{-1}g_1^{-1}\right) = e = \left(g_2^{-1}g_1^{-1}\right)(g_1g_2)$.

Assume $(\mathbf{g_1g_2\cdots g_n})^{-1} = \mathbf{g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}}$ for some $\mathbf{n} \in \mathbb{N}$ and show that $(\mathbf{g_1g_2\cdots g_ng_{n+1}})^{-1} = \mathbf{g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}}$:

Consider

$$\begin{aligned}(g_1g_2\cdots g_{n-1}g_ng_{n+1})\left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) &= (g_1g_2\cdots g_{n-1}g_n)\left(g_{n+1}g_{n+1}^{-1}\right)\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) \quad \text{by associativity} \\ &= (g_1g_2\cdots g_{n-1}g_n)(e)\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) \quad \text{by definition of } g_{n+1}^{-1} \\ &= (g_1g_2\cdots g_{n-1}g_n)\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) \quad \text{by definition of } e \\ (g_1g_2\cdots g_{n-1}g_ng_{n+1})\left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) &= e \quad \text{by inductive hypothesis} \qquad (7) \\ &= g_{n+1}^{-1}g_{n+1} \quad \text{by definition of } g_{n+1}^{-1} \\ &= \left(g_{n+1}^{-1}\right)(e)(g_{n+1}) \quad \text{by definition of } e \\ &= \left(g_{n+1}^{-1}\right)\left(\left(g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right)(g_1g_2\cdots g_{n-1}g_n)\right)(g_{n+1}) \\ &\quad \text{by inductive hypothesis} \\ (g_1g_2\cdots g_{n-1}g_ng_{n+1})\left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right) &= \left(g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}\right)(g_1g_2\cdots g_{n-1}g_ng_{n+1}) \quad \text{by associativity} \qquad (8)\end{aligned}$$

So by **Base case**, (7), and (8), $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$ and $(g_1g_2\cdots g_n)^{-1} = g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1} \implies (g_1g_2\cdots g_ng_{n+1})^{-1} = g_{n+1}^{-1}g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}$.

So the inverse of $g_1g_2\cdots g_n$ is $g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1}$ for all $n \in \mathbb{N}$. □

Exercise 3.30. Show that if $a^2 = e$ for all elements a in a group G, then G must be abelian.

Proof. Let $a, b \in G$. Then $(a \circ b) \in G$ by the assumption that G is a group. Then $a, b, (a \circ b) \in G \implies a^2 = b^2 = (a \circ b)^2 = e$ by the assumption that $a^2 = e$ for all elements a in G. Then

$$
\begin{aligned}
(a \circ b)^2 = e &\implies (a \circ b) \circ (a \circ b) = e \quad \text{by definition of exponentiation} \\
&\implies (b \circ a) \circ [(a \circ b) \circ (a \circ b)] = (b \circ a) \circ e \quad \text{by Proposition 3.2 (that } e \text{ is unique) and definition of } e, \text{ as } (b \circ a) \in G \\
&\implies [(b \circ a) \circ (a \circ b)] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by associativity of elements of } G \\
&\implies [((b \circ a) \circ a) \circ b] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by associativity of elements of } G \\
&\implies [(b \circ (a \circ a)) \circ b] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by associativity of elements of } G \\
&\implies [(b \circ e) \circ b] \circ (a \circ b) = (b \circ a) \circ e \quad \text{by assumption that } a \circ a = e \text{ for all } a \in G \\
&\implies [b \circ b] \circ (a \circ b) = b \circ a \quad \text{by definition of } e \\
&\implies e \circ (a \circ b) = b \circ a \quad \text{by assumption that } a \circ a = e \text{ for all } a \in G \\
&\implies a \circ b = b \circ a \quad \text{by definition of } e
\end{aligned}
$$

So for any $a, b \in G$, the definition of G implies that $(a \circ b)^2 \in G$. So $(a \circ b)^2 = e$ because $(a \circ b)^2 \in G$. We have shown that $(a \circ b)^2 = e \implies a \circ b = b \circ a$ for all $a, b \in G$. So if $a^2 = e$ for all elements $a \in G$ then G must be abelian. □

Exercise 3.35. Compute the subgroups of the symmetry of a square.

Proof. The symmetries of a square are given by $\rho = \left(\begin{smallmatrix} a & b & c & d \\ b & c & d & a \end{smallmatrix}\right)$, $\rho^2 = \left(\begin{smallmatrix} a & b & c & d \\ c & d & a & b \end{smallmatrix}\right)$, $\rho^3 = \left(\begin{smallmatrix} a & b & c & d \\ d & a & b & c \end{smallmatrix}\right)$, $\rho^4 = id = \left(\begin{smallmatrix} a & b & c & d \\ a & b & c & d \end{smallmatrix}\right)$, $\mu_{x=0} = \left(\begin{smallmatrix} a & b & c & d \\ d & c & b & a \end{smallmatrix}\right)$, $\mu_{y=0} = \left(\begin{smallmatrix} a & b & c & d \\ b & a & d & c \end{smallmatrix}\right)$, $\mu_{y=x} = \left(\begin{smallmatrix} a & b & c & d \\ c & b & a & d \end{smallmatrix}\right)$, and $\mu_{y=-x} = \left(\begin{smallmatrix} a & b & c & d \\ a & d & c & b \end{smallmatrix}\right)$. Then the sub-groups are the trivial sub-groups:

$$\langle id \rangle = \{id\} \tag{9}$$

and

$$\langle D_8 \rangle = \left\{\rho, \rho^2, \rho^3, \mu_{x=0}, \mu_{y=0}, \mu_{y=x}, \mu_{y=-x}, id\right\} \tag{10}$$

and the proper non-trivial sub-groups:

$$\langle \rho \rangle = \left\langle \rho^3 \right\rangle = \left\{\rho, \rho^2\rho^3, id\right\} \tag{11}$$
$$\left\langle \rho^2 \right\rangle = \left\{\rho^2, id\right\} \tag{12}$$
$$\langle \mu_{x=0} \rangle = \{\mu_{x=0}, id\} \tag{13}$$
$$\langle \mu_{y=0} \rangle = \{\mu_{y=0}, id\} \tag{14}$$
$$\langle \mu_{y=x} \rangle = \{\mu_{y=x}, id\} \tag{15}$$

and

$$\langle \mu_{y=-x} \rangle = \{\mu_{y=-x}, id\}. \tag{16}$$

Furthermore,

$$\left\langle \rho^2 \right\rangle \cup \langle \mu_{x=0} \rangle \cup \langle \mu_{y=0} \rangle = \left\{\rho^2, \mu_{x=0}, \mu_{y=0}\right\} \tag{17}$$

and

$$\left\langle \rho^2 \right\rangle \cup \langle \mu_{y=x} \rangle \cup \langle \mu_{y=-x} \rangle = \left\{\rho^2, \mu_{y=x}, \mu_{y=-x}\right\} \tag{18}$$

are proper sub-groups as $id \in$ (17) and $id \in$ (18), any element in (17) and (18) is its own inverse, and (17) and (18) are closed under composition as can be seen in the Cayley table below.

Besides by theorem from class that $g \in D_8$ implies that $\langle g \rangle := \{g^n | n \in \mathbb{N}\}$ is a subgroup of D_8 it is clear from the Cayley table that each of these forms a sub-group of D_8, including (17) and (18):

$\circ$	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

□

Exercise 3.40. Prove that

$$G = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are both not } 0 \right\}$$

is a sub-group of $\mathbb{R}^*$ under the group operation of multiplication.

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

1. For all $h_1, h_2 \in G$, $h_1 \cdot h_2 \in G$.
2. There exists $e \in G$ such that $h_1 \cdot e = h_1 = e \cdot h_1$ for all $h_1 \in G$.
3. For all $h_1 \in G$ there exists $h_1^{-1} \in G$ such that $h_1 \cdot h_1^{-1} = e = h_1^{-1} \cdot h_1$.

1. To show G is closed, take $h_1, h_2 \in G$. Clearly $h_1 \neq 0$ and $h_2 \neq 0$ so $h_1 \cdot h_2 \neq 0$. So

$$\begin{aligned} h_1 \cdot h_2 &= \left(a_1 + b_1\sqrt{2}\right) \cdot \left(a_2 + b_2\sqrt{2}\right) \\ &= a_1a_2 + a_1b_2\sqrt{2} + b_1a_2\sqrt{2} + 2b_1b_2 \quad \text{by the distributive property} \\ &= (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \quad \text{by distributive, associative laws} \end{aligned}$$

   and $\left[(a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}\right] \in G$.

2. To show the multiplicative identity is in G, take $a = 1$ and $b = 0$. Then $1 + 0\sqrt{2} \in G$ and $1 + 0\sqrt{2} = 1$ and 1 is the multiplicative identity in $\mathbb{R}^*$.

3. To show that each element in G has an inverse, given $h_1 = a + b\sqrt{2}$ its inverse is given by $h_1^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ as

$$\begin{aligned}
&h_1 \cdot h_1^{-1} = h_1^{-1} \cdot h_1 \quad \text{because multiplication is commutative in } \mathbb{R}^* \\
&h_1^{-1} \cdot h_1 = \left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right)\left(a + b\sqrt{2}\right) \\
&= \left(\frac{a - b\sqrt{2}}{a^2-2b^2}\right)\left(a + b\sqrt{2}\right) \\
&= \frac{a^2 - ab\sqrt{2}}{a^2-2b^2} + \frac{ab\sqrt{2} - 2b^2}{a^2-2b^2} \quad \text{by distributive law} \\
&= \frac{a^2-2b^2}{a^2-2b^2} \\
&= 1
\end{aligned}$$

and 1 is the multiplicative identity. Notice that the inverse is well defined: $h_1^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \neq 0$ as not both a and b are zero. Furthermore, the denominator is not zero as $a^2 - 2b^2 = 0 \implies a = b\sqrt{2}$ which violates the assumption that $a, b \in \mathbb{Q}$. So $\left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right) \in G$ exists and is well defined.

So we have shown that G is a sub-group of $\mathbb{R}^*$ under multiplication. □

Exercise 3.43. List the sub-groups of the quaternion group, Q_8.

Proof. By definition, $Q_8 := \{\pm 1, \pm I, \pm J, \pm K\}$ such that $I^2 = J^2 = K^2 = -1$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$ and $IK = -J$. Then the sub-groups of Q_8 are $\langle 1\rangle = \{1\}$, $\langle -1\rangle = \{-1, 1\}$, $\langle I\rangle = \{I, -1, -I, 1\}$, $\langle J\rangle = \{J, -1, -J, 1\}$, $\langle K\rangle = \{K, -1, -K, 1\}$, and $\langle Q_8\rangle = \{\pm 1, \pm I, \pm J, \pm K\}$ □

Exercise 3.44. Prove that the intersection of two sub-groups of a group G is also a sub-group of G.

Proof. Let $H_1, H_2 \in G$ be sub-groups of G. Consider $H_1 \cap H_2 = \Gamma$.
By theorem from class, for $\Gamma \subseteq G$ to be a sub-group of G, it is sufficient to show

1. For all $g_1, g_2 \in \Gamma$, $g_1 \circ g_2 \in \Gamma$.
2. There exists $e \in \Gamma$ such that $g_1 \circ e = g_1 = e \circ g_1$ for all $g_1 \in \Gamma$.
3. For all $g_1 \in \Gamma$ there exists $g_1^{-1} \in G$ such that $g_1 \circ g_1^{-1} = e = g_1^{-1} \circ g_1$.

1. Let $g_1, g_2 \in \Gamma$. Then $g_1, g_2 \in H_1$ and $g_1, g_2 \in H_2$ as $\Gamma = H_1 \cap H_2$. Then $g_1 \circ g_2 \in H_1$ and $g_1 \circ g_2 \in H_2$ by the assumption that H_1 and H_2 are sub-groups of G.
   $g_1 \circ g_2 \in H_1$ and $g_1 \circ g_2 \in H_2 \implies g_1 \circ g_2 \in \Gamma$ by definition of Γ. So $g_1, g_2 \in \Gamma \implies g_1 \circ g_2 \in \Gamma$. So Γ is closed under $\circ$.
2. $e \in H_1$ and $e \in H_2$ by the assumption that H_1 and H_2 are sub-groups. Then $e \in \Gamma$ by definition of Γ. So $e \in \Gamma$. This also proves that $\Gamma \neq \emptyset$.
3. Let $g_1 \in \Gamma$. Then $g_1 \in H_1$ and $g_1 \in H_2$ by definition of Γ. Then $g_1^{-1} \in H_1$ and $g_1^{-1} \in H_2$ by assumption that H_1 and H_2 are sub-groups of G. So $g_1^{-1} \in H_1$ and $g_1^{-1} \in H_2 \implies g_1^{-1} \in \Gamma$. So $g_1 \in \Gamma \implies g_1^{-1} \in \Gamma$.

So we have shown that Γ is a sub-group of G under $\circ$. □

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. □

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. □

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. □

Moshe Mason Rubin

MATH 330 Homework #5

3 October 2016

Exercise 4.14. Let

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

be elements in $GL_2(\mathbb{R})$.Show that A and B have finite orders but AB does not.

Proof. Notice

$$A^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

and

$$\begin{aligned} A^4 = A^2A^2 &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = id \end{aligned}$$

so A is of order 4. Notice

$$\begin{aligned} B^3 &= \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \\ &= \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = id \end{aligned}$$

So B is of order 3.

Notice $AB = \left[\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right]$

Claim. $(AB)^n = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ for $n \in \mathbb{N}$, so AB is of infinite order as this would imply there is no $n \in \mathbb{N}$ such that $(AB)^n = id$.

By induction:

Base case $n = 2$:

$$\begin{aligned} (AB)^2 &= \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

So the hypothesis holds for $n = 2$. ✓

Inductive step Assume $(AB)^n = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ for some fixed $n \in \mathbb{N}$ and show that $(AB)^{n+1} = \left[\begin{smallmatrix} 1 & -(n+1) \\ 0 & 1 \end{smallmatrix}\right]$:

$$\begin{aligned}(AB)^{n+1} &= (AB)^n (AB) \\ &= \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -1-n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -(n+1) \\ 0 & 1 \end{bmatrix} \quad \checkmark\end{aligned}$$

So $(AB)^n = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ for $n \in \mathbb{N}$.

So AB is of infinite order as this would imply there is no $n \in \mathbb{N}$ such that $(AB)^n = id$. □

Exercise 4.18. Calculate each of the following expressions.

(a) $(1+i)^{-1}$ (c) $\left(\sqrt{3}+i\right)^5$ (e) $\left(\frac{1-i}{2}\right)^4$ (g) $(-2+2i)^{-5}$

(b) $(1+i)^6$ (d) $(-i)^{10}$ (f) $\left(-\sqrt{2}-\sqrt{2}i\right)^{12}$

Proof. Recall that *Euler's Formula* that $Ae^{i\theta} = A(\cos\theta + i\sin\theta)$ for $A \in \mathbb{R}$, $\theta \in [0, 2\pi]$.

(a) $(1+i)^{-1}$ is given by $\frac{1}{2} - \frac{1}{2}i$ as $(1+i)\left(\frac{1}{2} - \frac{1}{2}i\right) = \frac{1}{2} - \frac{1}{2}i + \frac{1}{2}i + \frac{1}{2} = 1$. So $\boxed{\frac{1}{2} - \frac{1}{2}i = (1+i)^{-1}}$.

(b) By *Euler's Formula*, $1 + i = \sqrt{2}e^{\frac{i\pi}{4}}$, so

$$\begin{aligned}(1+i)^6 &= \left(\sqrt{2}e^{\frac{i\pi}{4}}\right)^6 \\ &= \sqrt{2}^6 e^{\frac{6i\pi}{4}} \\ &= 8e^{\frac{3i\pi}{2}} \\ &= 8\left(\cos\left(\frac{3\pi}{2}\right) + i\sin\left(\frac{3\pi}{2}\right)\right) \quad \text{by } \textit{Euler's Formula} \\ &= -8i, \quad \text{as } \cos\left(\tfrac{3\pi}{2}\right) = 0 \text{ and } \sin\left(\tfrac{3\pi}{2}\right) = -1\end{aligned}$$

So $\boxed{(1+i)^6 = -8i}$.

(c) By *Euler's Formula*, $\sqrt{3} + i = 2e^{\frac{i\pi}{6}}$, so

$$\begin{aligned}\left(\sqrt{3}+i\right)^5 &= \left(2e^{\frac{i\pi}{6}}\right)^5 \\ &= 2^5 e^{\frac{5i\pi}{6}} \\ &= 32\left(\cos\left(\frac{5\pi}{6}\right) + i\sin\left(\frac{5\pi}{6}\right)\right) \quad \text{by } \textit{Euler's Formula} \\ &= 32\left(-\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) \quad \text{as } \cos\left(\tfrac{5\pi}{6}\right) = -\tfrac{\sqrt{3}}{2} \text{ and } \sin\left(\tfrac{5\pi}{6}\right) = \tfrac{1}{2} \\ &= 16i - 16\sqrt{3}\end{aligned}$$

So $\boxed{\left(\sqrt{3}+i\right)^5 = 16i - 16\sqrt{3}}$.

(d)

$$\begin{aligned}(-i)^{10} &= (-1)^{10}(i)^{10} \\ &= (-1)^2 (i)^2 \quad \text{as } (-1)^m = (-1)^{(m \bmod 2)} \text{ and } i^n = i^{(n \bmod 4)} \\ &= (1)(-1) \\ &= -1\end{aligned}$$

So $\boxed{(-i)^{10} = -1}$.

(e) By *Euler's Formula*, $\frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i = \frac{\sqrt{2}}{2}e^{\frac{7i\pi}{4}}$, so

$$\begin{aligned}\left(\frac{1-i}{2}\right)^4 &= \left(\frac{\sqrt{2}}{2}e^{\frac{7i\pi}{4}}\right)^4 \\ &= \left(\frac{\sqrt{2}}{2}\right)^4 e^{7i\pi} \\ &= \frac{1}{4}e^{i\pi} \quad \text{as we restrict } \theta \text{ to } 0 \le \theta \le 2\pi \\ &= \frac{1}{4}(\cos(\pi) + i\sin(\pi)) \\ &= -\frac{1}{4}\end{aligned}$$

So $\boxed{\left(\frac{1-i}{2}\right)^4 = -\frac{1}{4}}$.

(f) By *Euler's Formula*, $-\sqrt{2} - \sqrt{2}i = 2e^{\frac{5i\pi}{4}}$, so

$$\begin{aligned}\left(-\sqrt{2} - \sqrt{2}i\right)^{12} &= \left(2e^{\frac{5i\pi}{4}}\right)^{12} \\ &= 2^{12}e^{\frac{60i\pi}{4}} \\ &= 4096e^{15i\pi} \\ &= 4096e^{i\pi} \quad \text{as we restrict } \theta \text{ to } 0 \le \theta \le 2\pi \\ &= -4096 \quad \text{as } e^{i\pi} = -1 \text{ from above}\end{aligned}$$

So $\boxed{\left(-\sqrt{2} - \sqrt{2}i\right)^{12} = -4096}$.

(g) By *Euler's Formula*, $-2 + 2i = 2\sqrt{2}e^{\frac{3i\pi}{4}}$, so

$$\begin{aligned}(-2+2i)^{-5} &= \left(2\sqrt{2}e^{\frac{3i\pi}{4}}\right)^{-5} \\ &= \left(2\sqrt{2}\right)^{-5}\left(e^{\frac{3i\pi}{4}}\right)^{-5} \\ &= \frac{\sqrt{2}}{256}e^{\frac{-15i\pi}{4}} \\ &= \frac{\sqrt{2}}{256}e^{\frac{i\pi}{4}} \quad \text{as we restrict } \theta \text{ to } 0 \le \theta \le 2\pi \\ &= \frac{\sqrt{2}}{256}\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right) \quad \text{by } \textit{Euler's Formula}, \text{ as } \sin\left(\tfrac{\pi}{4}\right) = \cos\left(\tfrac{\pi}{4}\right) = \tfrac{1}{\sqrt{2}} \\ &= \frac{1}{256} + \frac{1}{256}i\end{aligned}$$

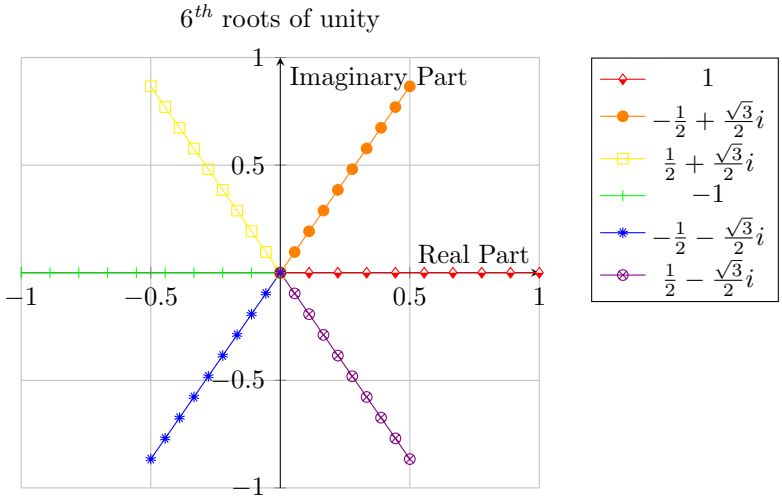
So $\boxed{(-2+2i)^{-5} = \frac{1}{256} + \frac{1}{256}i}$. □

Exercise 4.20. List and graph that 6^{th} roots of unity. What are the generators of this group? What are the primitive 6^{th} roots of unity?

Proof. By Theorem 4.11, the 6^{th} roots of unity are given by $z = \cos\left(\frac{k\pi}{3}\right) + i\sin\left(\frac{k\pi}{3}\right)$ for $k = 0, 1, 2, 3, 4, 5$. So the 6^{th} roots of unity are

1. $\cos(0) + i\sin(0) = 1$
2. $\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right) = \frac{1}{2} + \frac{\sqrt{3}}{2}i$
3. $\cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$
4. $\cos(\pi) + i\sin(\pi) = -1$
5. $\cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$
6. $\cos\left(\frac{5\pi}{3}\right) + i\sin\left(\frac{5\pi}{3}\right) = \frac{1}{2} - \frac{\sqrt{3}}{2}i$

Only $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\frac{1}{2} - \frac{\sqrt{3}}{2}i$ are primitive 6^{th} roots of unity as $1^1 = 1$, $\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^3 = 1$, $(-1)^2 = 1$, and $\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)^3 = 1$ for the other roots. So $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\frac{1}{2} - \frac{\sqrt{3}}{2}i$ are the generators of this group. □



Exercise 4.23. Let $a, b \in G$. Prove the following statements.

(a) The order of a is the same as the order of a^{-1}.

(b) For all $g \in G$, $|a| = |g^{-1}ag|$.

(c) The order of ab is the same as the order of ba.

Proof.

(a)

- Assume $a \in G$ is of finite order $k \in \mathbb{N}$. Then $a^k = 1$ by definition. Then

$$\begin{aligned}\left(a^{-1}\right)^k &= a^{-k} \quad \text{by Theorem 3.8.2} \\ &= \left(a^k\right)^{-1} \quad \text{by Theorem 3.8.2} \\ &= (1)^{-1} \quad \text{by assumption that } a \text{ is of order } k \\ &= 1\end{aligned}$$

  So $\left(a^{-1}\right)^k = 1$. So a^{-1} is of order k.

- Assume a is of infinite order. Then there does not exist $k \in \mathbb{N}$ suck that $a^k = 1$. Now, assume we wish to find $n \in \mathbb{N}$ such that $\left(a^{-1}\right)^n = 1$. Then

$$\begin{aligned}\left(a^{-1}\right)^n = 1 &\implies a^{-n} = 1 \quad \text{by Theorem 3.8.2} \\ &\implies (a^n)^{-1} = 1 \\ &\implies (a^n)^{-1} = (a^n)(a^n)^{-1} \quad \text{by definition of } (a^n)^{-1} \\ &\implies 1 = a^n \quad \text{by right multiplying by } a^n\end{aligned}$$

  But $a^n \neq 1$ for all $n \in \mathbb{N}$ by assumption that $|a| = \infty$. So $\left(a^{-1}\right)^n \neq 1$ for all $n \in \mathbb{N}$, so $|a^{-1}| = \infty$.

So $|a| = |a^{-1}|$. □

(b) I will show $|a| = |g^{-1}ag|$ for all $g \in G$ using the following claim:

Claim. $\left(g^{-1}ag\right)^k = g^{-1}a^kg$ for $k \in \mathbb{N}$.

By induction:

Base Case $n = 2$:

$$\begin{aligned}\left(g^{-1}ag\right)^2 &= \left(g^{-1}ag\right)\left(g^{-1}ag\right)\\ &= \left(g^{-1}a\right)\left(gg^{-1}\right)(ag) \quad \text{by associative property}\\ &= \left(g^{-1}a\right)(ag) \quad \text{by definition of } g^{-1}\\ &= g^{-1}a^2g \quad \text{by associative property}\end{aligned}$$

So the hypothesis holds for $n = 2$. ✓

Inductive step Assume $\left(g^{-1}ag\right)^k = g^{-1}a^kg$ for some fixed $k \in \mathbb{N}$ and show that $\left(g^{-1}ag\right)^{k+1} = g^{-1}a^{k+1}g$:

$$\begin{aligned}\left(g^{-1}ag\right)^{k+1} &= \left(g^{-1}ag\right)^k\left(g^{-1}ag\right)\\ &= \left(g^{-1}a^kg\right)\left(g^{-1}ag\right) \quad \text{by inductive hypothesis}\\ &= \left(g^{-1}a^k\right)\left(gg^{-1}\right)(ag) \quad \text{by associative property}\\ &= \left(g^{-1}a^k\right)(ag) \quad \text{by definition of } g^{-1}\\ &= g^{-1}a^{k+1}g \quad ✓\end{aligned}$$

So $\left(g^{-1}ag\right)^k = g^{-1}a^kg \implies \left(g^{-1}ag\right)^{k+1} = g^{-1}a^{k+1}g$. So $\left(g^{-1}ag\right)^k = g^{-1}a^kg$ for all $k \in \mathbb{N}$. □

Now, consider that $|a| = n$ for some $n \in \mathbb{N}$. Then $a^n = 1$ by definition. Then

$$\begin{aligned}a^n = n &\implies a^n = gg^{-1}\\ &\implies a^ng = g\left(g^{-1}g\right) \quad \text{by associative property}\\ &\implies a^ng = g, \quad \text{by definition of } g^{-1}\\ &\implies g^{-1}a^ng = g^{-1}g\\ &\implies g^{-1}a^ng = 1\\ &\implies \left(g^{-1}ag\right)^n = 1 \quad \text{by above claim that } \left(g^{-1}ag\right)^k = g^{-1}a^kg\end{aligned}$$

So $\left(g^{-1}ag\right)^n = 1$. So $|g^{-1}ag| = |a|$ for all $g \in G$. □

(c) Notice $ab = b^{-1}(ba)b$. So

$$\begin{aligned}|ab| &= |b^{-1}(ba)b|\\ &= |ba| \quad \text{by (b)}\end{aligned}$$

So $|ab| = |ba|$. □

Exercise 4.30. Suppose that G is a group and let $a, b \in G$. Prove that if $|a| = m$ and $|b| = n$ with $\gcd(m, n) = 1$, then $\langle a\rangle \cap \langle b\rangle = \{e\}$.

Proof. Notice $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $\langle b\rangle = \{e, b, b^2, \ldots, b^{m-1}\}$. We want to show e is the only element these two sets have in common.

Suppose not: Suppose $a^{n_0} = b^{m_0}$ for some $n_0, m_0 \in \mathbb{N}$ such that $0 < n_0 < n$ and $0 < m_0 < m$. Then

$$\begin{aligned} a^{n_0} = b^{m_0} &\implies (a^{n_0})^n = (b^{m_0})^n \\ &\implies a^{n_0 n} = b^{m_0 n} \quad \text{by Theorem 3.8.2} \\ &\implies e = b^{m_0 n} \quad \text{by Proposition 4.5, as } n|(m_0 n) \\ &\implies m|(m_0 n) \quad \text{by Proposition 4.5} \\ &\implies m|m_0 \quad \text{by } \textbf{Exercise 2.27} \text{ from homework 2, as } \gcd(m,n) = 1 \text{ by assumption} \end{aligned}$$

and $m|m_0$ is contradiction as we assumed $0 < m_0 < m$. So $a^{n_0} \neq b^{m_0}$ for any n_0, m_0. So $\langle a\rangle$ and $\langle b\rangle$ have no elements in common except e. So $\langle a\rangle \cap \langle b\rangle = \{e\}$. □

Exercise 5.1. Write the following permutations in cycle notation.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

Solution.

(a) (12453) (b) $(14)(35)$ (c) $(13)(25)$ (d) (24) □

Exercise 5.2. Compute each of the following.

(a) $(1345)(234)$

(b) $(12)(1253)$

(c) $(143)(23)(24)$

(d) $(1423)(34)(56)(1324)$

(e) $(1254)(13)(25)$

(f) $(1254)(13)(25)^2$

Solution.

(a) $(1351)(24)$

(b) (253)

(c) $(14)(23)$

(d) $(12)(56)$

(e) (1324)

(f) (13254) □

Exercise 5.3. Express the following permutations as products of transpositions and identify them as even or odd.

(a) (14356)

(b) $(156)(234)$

(c) $(1426)(142)$

(d) $(17254)(1423)(154632)$

(e) (142637)

Solution. Recall that

$$(a_1, a_2, \ldots, a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2)$$

(a) $(14356) = (16)(15)(13)(14)$ and is even.

(b) $(156)(234) = (16)(15)(24)(23)$ and is even.

(c) $(1426)(142) = (1246) = (16)(14)(12)$ and is odd.

(d) $(17254)(1423)(154632) = (14672) = (12)(17)(16)(14)$ and is even.

(e) $(142637) = (17)(13)(16)(12)(14)$ and is odd. □

Exercise 5.5. List all of the sub-groups of S_4. Find each of the following sets.

(a) $\{\sigma \in S_4 : \sigma(1) = 3\}$

(b) $\{\sigma \in S_4 : \sigma(2) = 2\}$

(c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$

Proof. The elements of S_4 are given by

e	(12)	$(12)(34)$	$(123) = (13)(12)$	$(1234) = (14)(13)(12)$
	(13)	$(13)(24)$	$(132) = (12)(13)$	$(1243) = (13)(14)(12)$
	(14)	$(14)(23)$	$(124) = (14)(12)$	$(1423) = (13)(12)(14)$
	(23)		$(142) = (12)(14)$	$(1324) = (14)(12)(13)$
	(24)		$(134) = (14)(13)$	$(1432) = (12)(13)(14)$
	(34)		$(143) = (13)(14)$	$(1342) = (12)(14)(13)$
			$(234) = (24)(23)$	
			$(243) = (23)(24)$	

Then the sub-groups of S_4 are given by

1. $\langle e \rangle = \{e\}$
2. $\langle (12) \rangle = \{e, (12)\}$
3. $\langle (13) \rangle = \{e, (13)\}$
4. $\langle (14) \rangle = \{e, (14)\}$
5. $\langle (23) \rangle = \{e, (23)\}$
6. $\langle (24) \rangle = \{e, (24)\}$
7. $\langle (34) \rangle = \{e, (34)\}$
8. $\langle (12)(34) \rangle = \{e, (12)(34)\}$
9. $\langle (13)(24) \rangle = \{e, (13)(24)\}$
10. $\langle (14)(23) \rangle = \{e, (14)(23)\}$
11. $\langle (123) \rangle = \{e, (123), (132)\}$
12. $\langle (124) \rangle = \{e, (124), (142)\}$
13. $\langle (134) \rangle = \{e, (134), (143)\}$
14. $\langle (234) \rangle = \{e, (234), (243)\}$
15. $\langle (1234) \rangle = \{e, (1234), (13)(24), (1432)\}$
16. $\langle (1243) \rangle = \{e, (1243), (14)(23), (1342)\}$
17. $\langle (1423) \rangle = \{e, (1423), (12)(43), (1324)\}$
18. $\langle (12), (34) \rangle = \{e, (12), (34), (12)(34)\}$
19. $\langle (13), (24) \rangle = \{e, (13), (24), (13)(24)\}$
20. $\langle (14), (23) \rangle = \{e, (14), (23), (14)(23)\}$
21. S_4
22. I know there are more but I'm not totally sure the best way to compute "all sub-groups"

(a) $\{\sigma \in S_4 : \sigma(1) = 3\} = \{(13), (13)(24), (132), (134), (1324), (1342)\}$

(b) $\{\sigma \in S_4 : \sigma(2) = 2\} = \{e, (13), (14), (34), (134), (143)\}$

(c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\} = \{(13), (134)\}$

□

Moshe Mason Rubin

MATH 330 Homework #6

10 October 2016

Exercise 5.8. Show that A_{10} contains an element of order 15.

Proof. Consider $\sigma \in A_{10} \subset S_{10}$ given by $\sigma = (12345)(678)$, the product of two disjoint cycles. Then $\sigma \in A_{10}$ as σ is the product of two even permutations and Theorem 5.7 states A_{10} is a sub-group of S_{10}, therefore closed. Notice $(12345)^{-1} = (12345)^4$ and $(678)^{-1} = (678)^2$, and clearly $(12345)^{-1} \neq (678)^n$ and $(678)^{-1} \neq (12345)^m$ for any $(n, m) \in \mathbb{Z}^2$. Because $|A_{10}| = \frac{10!}{2}$ is finite, $|\sigma| \neq \infty$ as $\sigma^n \in A_{10}$ for all $n \in \mathbb{Z}$ by Theorem 5.7 that A_n is a sub-group of S_n. Then

$$\begin{aligned}
\sigma^{15} &= [(12345)(678)]^{15} \\
&= (12345)^{15}(678)^{15} \quad \text{by Proposition 5.2 (that disjoint cycles commute) and Theorem 3.8.3} \\
&= \left[(12345)^5\right]^3 \left[(678)^3\right]^5 \quad \text{by Theorem 3.8.2} \\
&= (id)^3 (id)^5 \\
&= id
\end{aligned}$$

So $\sigma = (12345)(678) \in A_{10}$ is an element of A_{10} of order 15. □

Exercise 5.13. Let $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ be the product of disjoint cycles. Prove that the order of σ is the least common multiple of the lengths of the cycles $\sigma_1, \ldots, \sigma_m$.

Proof. Let $|\sigma| = k$. So

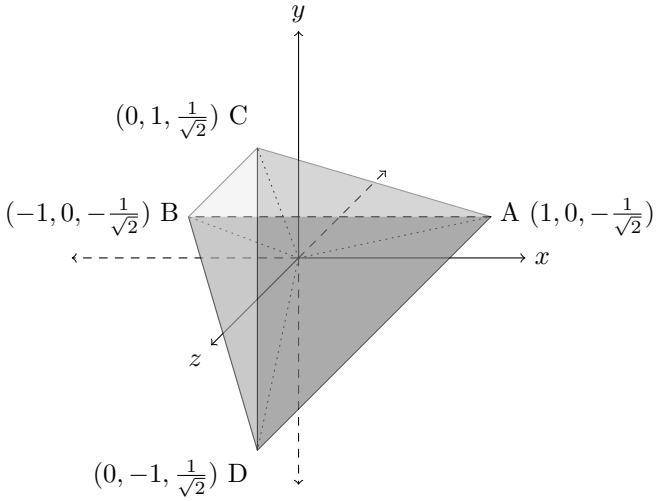
$$\begin{aligned}
\sigma^k &= (\sigma_1 \cdots \sigma_m)^k \\
&= \sigma_1^k \cdots \sigma_m^k \quad \text{by Proposition 5.2 (that disjoint cycles commute) and Theorem 3.8.3} \\
&= id \quad \text{because } \sigma^k = id \text{ as } |\sigma| = k
\end{aligned}$$

So $\sigma_i^k = id$ for $i \in ([1, m] \cap \mathbb{Z})$. So if So $\sigma_i^k = id$ then k must be a common multiple of the length of each σ_i. So the smallest k (that is, the order of σ) must be equal to the least common divisor of lengths of $\sigma_1, \ldots \sigma_m$ by definition of least common multiple. □

Exercise 5.16. Find all group of rigid motions of a tetrahedron. Show that this is the same group as A_4.

Proof.

A regular tetrahedron centered at $(0, 0, 0)$ with each face an equilateral triangle of side length $\frac{\sqrt{6}}{2}$



Consider the position of face $ACD \to A'C'D'$ for each rigid motion of the tetrahedron. The point A may assume 4 distinct locations. Once A is fixed, C may assume one of 3 remaining distinct locations. Once A and C are chosen, D may assume only 1 distinct location. So the order is $4 \times 3 \times 1 = 12$. The group of rigid rotations is given by $\rho_A = \left(\begin{smallmatrix} A & B & C & D \\ A & D & B & C \end{smallmatrix}\right)$, $\rho_A^2 = \left(\begin{smallmatrix} A & B & C & D \\ A & C & D & B \end{smallmatrix}\right)$, $\rho_B = \left(\begin{smallmatrix} A & B & C & D \\ C & B & D & A \end{smallmatrix}\right)$, $\rho_B^2 = \left(\begin{smallmatrix} A & B & C & D \\ D & B & A & C \end{smallmatrix}\right)$, $\rho_C = \left(\begin{smallmatrix} A & B & C & D \\ B & D & C & A \end{smallmatrix}\right)$, $\rho_C^2 = \left(\begin{smallmatrix} A & B & C & D \\ D & A & C & B \end{smallmatrix}\right)$, $\rho_D = \left(\begin{smallmatrix} A & B & C & D \\ C & A & B & D \end{smallmatrix}\right)$, $\rho_D^2 = \left(\begin{smallmatrix} A & B & C & D \\ B & C & A & D \end{smallmatrix}\right)$, $\rho_{AB,BC} = \left(\begin{smallmatrix} A & B & C & D \\ B & A & D & C \end{smallmatrix}\right)$, $\rho_{AC,BD} = \left(\begin{smallmatrix} A & B & C & D \\ C & D & A & B \end{smallmatrix}\right)$, $\rho_{AD,BC} = \left(\begin{smallmatrix} A & B & C & D \\ D & C & B & A \end{smallmatrix}\right)$, and $id = \left(\begin{smallmatrix} A & B & C & D \\ A & B & C & D \end{smallmatrix}\right)$. By Proposition 5.8, $A_4 \subset S_4$ is of order $\frac{4!}{2} = 12$ and A_4 is given by

$$\begin{aligned} A_4 &= \{id, (12)(13), (12)(14), (12)(34), (13)(12), (13)(14), (13)(24), (14)(12), (14)(13), (14)(23), (23)(24), (24)(23)\} \quad \text{by definition} \\ &= \{(24)(23), (23)(24), (14)(13), (13)(14), (14)(12), (12)(14), (13)(12), (12)(13), (12)(34), (13)(34), (14)(23), id\} \quad \text{by reordering} \\ &= \{(234), (243), (134), (143), (124), (142), (123), (132), (12)(34), (13)(24), (14)(23), id\} \quad \text{as } (a_i a_k)(a_i a_j) = (a_i a_k a_j). \end{aligned}$$

Notice this matches the set A_4 as listed in Chapter 5, **Example 8.**

Since the order of the rigid motions of a tetrahedron equals the order of A_4, to show that the two groups are equivalent we must show that every rigid motion of a tetrahedron is the product even number of permutations. Label A, B, C, D as $1, 2, 3, 4$ respectively. Then

- (234) corresponds to ρ_A ((243) to ρ_A^2)
- (124) corresponds to ρ_C ((142) to ρ_C^2)
- (12)(34) corresponds to $\rho_{AB,BC}$
- (14)(23) corresponds to $\rho_{AD,BC}$
- (134) corresponds to ρ_B ((143) to ρ_B^2)
- (123) corresponds to ρ_D ((132) to ρ_D^2)
- (13)(24) corresponds to $\rho_{AC,BD}$
- The identity id corresponds to itself

Notice every rigid motion of is the product of an even number of permutations as for each $x \in \{\text{group of rigid motions of a tetrahedron}\}$, $x \in A_4$. So the group of rigid motions of a tetrahedron is the same as A_4 as

$$\begin{aligned} \{\text{group of rigid motions of a tetrahedron}\} &= \left\{\rho_A, \rho_A^2, \rho_B, \rho_B^2, \rho_C, \rho_C^2, \rho_D, \rho_D^2, \rho_{((AB)(BC))}, \rho_{((AC)(BD))}, \rho_{((AD)(BC))}\right\} \\ &\quad \text{from way above} \\ &= \{(234), (243), (134), (143), (124), (142), (123), (132), (12)(34), (13)(24), (14)(23), id\} \\ &\quad \text{from above} \\ &= \{id, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \\ &\quad \text{by reordering} \\ &= A_4 \quad \text{as listed in Chapter 5, } \textbf{Example 8.} \text{ and above} \end{aligned}$$

□

Exercise 5.19. Prove that D_n is non-abelian for $n \geq 3$.

Proof. By Theorem 5.10, we know that the group D_n consists of all products of the two elements r and s satisfying the relations

$$\begin{aligned} r^n &= id \\ s^2 &= id \\ srs &= r^{-1} \end{aligned}$$

for $n \geq 3$.

Let $n \geq 3$ and label r, s such that $r^n = id$ and $s^2 = id$, which is certainly possible by Theorem 5.10. Now assume for a contradiction of D_n is abelian. Then

$$\begin{aligned} srs = (sr)s &= (rs)s \quad \text{by assumption that } D_3 \text{ is abelian} \\ &= r(ss) = rs^2 \quad \text{by associativity of elements in } D_n \text{ as } D_n \text{ is a sub-group of } S_n \text{ by Theorem 5.9} \\ &= r(id) \quad \text{by Theorem 5.15 and chose of } s \in D_n \\ &= r \end{aligned}$$

However $srs = r$ is a contradiction to Theorem 5.10 that $srs = r^{-1}$ as this would imply

$$\begin{aligned} rr^{-1} = id &\implies r(srs) = id \quad \text{by Theorem 5.10} \\ &\implies r(r) = id \quad \text{by calculation above that } srs = r \\ &\implies r^2 = id \end{aligned}$$

and $r^2 = id$ cannot happen for $r \in D_n$ for $n \geq 3$ as r is necessarily of order n and $2 < n$. So our original assumption that D_n is abelian must be false, so D_n must be non-abelian for $n \geq 3$. □

Exercise 5.23. If σ is a cycle of odd length, prove that σ^2 is also a cycle.

Proof. Let $\sigma = (\sigma_1, \ldots, \sigma_k)$ for some odd integer k. Then σ may be written as $\sigma = (\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)$, a finite product of transpositions. Then

$$\begin{aligned} \sigma^2 &= \left((\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)\right)^2 \\ &= \left[(\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)\right]\left[(\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)\right] \quad \text{by definition of exponentiation} \end{aligned}$$

Then σ^2 is given by $\sigma^2(\sigma_\ell) = \sigma(\sigma(\sigma_\ell)) = \sigma(\sigma_{\ell+1}) = \sigma_{\ell+2}$ for $\ell = 1, 2, \ldots, k-2$. So $\sigma^2 : \sigma_1 \mapsto \sigma_3$, and $\sigma^2 : \sigma_3 \mapsto \sigma_5$, and eventually we will arrive at $\sigma^2 : \sigma_{k-2} \mapsto \sigma_k$ as k is an odd number. Then $\sigma^2(\sigma_k) = \sigma(\sigma_1) = \sigma_2$. $\sigma^2(\sigma_\ell) = \sigma(\sigma(\sigma_\ell)) = \sigma(\sigma_{\ell+1}) = \sigma_{\ell+2}$ for $\ell = 1, 2, \ldots, k-2$. So $\sigma^2 : \sigma_2 \mapsto \sigma_4$, and $\sigma^2 : \sigma_4 \mapsto \sigma_6$, and eventually we will arrive at $\sigma^2 : \sigma_{k-3} \mapsto \sigma_{k-1}$ as k is an odd number so $k-3$ is even. Then $\sigma_{k-1} \mapsto \sigma_1$ as $\sigma_1 \mapsto \sigma_3$ as before. So $\sigma^2 = (\sigma_3, \sigma_5, \ldots, \sigma_{k-2}, \sigma_k, \sigma_2, \sigma_4, \ldots, \sigma_{k-1}, \sigma_1)$ is a cycle. □

Exercise 5.26. Prove that any element in S_n can be written as a finite product of the following permutations.

(a) $(12), (13), \ldots, (1n)$ (b) $(12), (23), \ldots, (n-1, n)$ (c) $(12), (12\ldots n)$

Proof. Let $\sigma \in S_n$.

(a) Then by Theorem 5.3, σ can be written as the product of disjoint cycles $\sigma = a_1 a_2 \cdots a_k$. For $i = 1, \ldots k$, let $a_i = (\alpha_{i_1}, \ldots, \alpha_{i_\ell})$. Then $a_i : \alpha_{i_m} \mapsto \alpha_{i_{m+1}}$ for $m = 1, \ldots, \ell - 1$ and $a_i : \alpha_{i_\ell} \mapsto \alpha_1$. Consider $a_i' = (\alpha_{i_1} a_{i_\ell})(a_{i_1} a_{i_{\ell-1}}) \cdots (a_{i_1} a_{i_3})(a_{i_1} a_{i_2})$, which is a product of $(12), (13), \ldots, (1n)$. Then $a_i' : \alpha_{i_m} \mapsto \alpha_{i_{m+1}}$ for $m = 1, \ldots, \ell - 1$ and $a_i' : \alpha_{i_\ell} \mapsto \alpha_1$. So $a_i = a_i'$ for all i. So

$$\begin{aligned} \sigma &= a_1 a_2 \cdots a_k \\ &= a_1' a_2' \cdots a_k' \quad \text{as } a_i = a_i' \\ &= \left((a_{1_1} a_{1_\ell}) \cdots (a_{1_1} a_{1_2})\right)\left((a_{2_1} a_{2_\ell}) \cdots (a_{2_1} a_{2_2})\right) \cdots \left((a_{k_1} a_{k_\ell}) \cdots (a_{k_1} a_{k_2})\right) \end{aligned}$$

which is a product of $(12), (13), \ldots, (1n)$ □

Exercise 6.1. Suppose that G is a finite group with an element g of order 5 and an element h of order 7. Why must $|G| \geq 35$?

Proof. Let $g = (g_1 g_2 g_3 g_4 g_5)$ and $h = (h_1 h_2 h_3 h_4 h_5 h_6 h_7)$. By Corollary 6.6, the orders of g and h, (5 and 7 respectively) must divide the number of elements in G, so $|G|$ is 35 at least, or larger. □

Exercise 6.3. Prove or disprove: Every sub-group of the integers has finite index.

Proof. This is false. Let $H = \{1\}$. Then H is a sub-group of $\mathbb{Z}$ and $[\mathbb{Z} : H] = \#\mathcal{L}_H = \#\{g \cdot 1 : g \in \mathbb{Z}\} = \infty$ □

Exercise 6.5. List the left and right co-sets of the sub-groups in each of the following.

(a) $\langle 8\rangle$ in $\mathbb{Z}_{24}$ (b) $\langle 3\rangle$ in $U(8)$ (d) A_4 in S_4 (f) D_4 in S_4

Solution.

(a) The left and right co-sets of $\langle 8\rangle$ in $\mathbb{Z}_{24}$ are the same as addition is commutative in $\mathbb{Z}_{24}$. So the left and right co-set are

$$\begin{array}{rcrcrcr}
0+\langle 8\rangle & = & 8+\langle 8\rangle & = & 16+\langle 8\rangle & = & \{0,8,16\} \\
1+\langle 8\rangle & = & 9+\langle 8\rangle & = & 17+\langle 8\rangle & = & \{1,9,17\} \\
2+\langle 8\rangle & = & 10+\langle 8\rangle & = & 18+\langle 8\rangle & = & \{2,10,18\} \\
3+\langle 8\rangle & = & 11+\langle 8\rangle & = & 19+\langle 8\rangle & = & \{3,11,19\} \\
4+\langle 8\rangle & = & 12+\langle 8\rangle & = & 20+\langle 8\rangle & = & \{4,12,20\} \\
5+\langle 8\rangle & = & 13+\langle 8\rangle & = & 21+\langle 8\rangle & = & \{5,13,21\} \\
6+\langle 8\rangle & = & 14+\langle 8\rangle & = & 22+\langle 8\rangle & = & \{6,14,22\} \\
7+\langle 8\rangle & = & 15+\langle 8\rangle & = & 23+\langle 8\rangle & = & \{6,14,22\}
\end{array}$$

(b) The left and right co-sets of $\langle 3\rangle$ in $U(8)$ are the same as multiplication is commutative in $\mathbb{Z}_8$. $U(8) = \{1,3,5,7\}$ and $\langle 3\rangle = \{1,3\}$, so the left and right co-sets are:

$$\begin{aligned}
1\cdot\{3,1\} &= \{3,1\} \\
3\cdot\{3,1\} &= \{1,3\} \\
5\cdot\{3,1\} &= \{7,5\} \\
7\cdot\{3,1\} &= \{5,7\}
\end{aligned}$$

(d) The order of A_4 in S_4 is 2, so the left co-sets equals the right co-sets. So the left and right co-sets of

$$A_4 = \{(234),(243),(134),(143),(124),(142),(123),(132),(12)(34),(13)(24),(14)(23),id\}$$

are

$$\begin{aligned}
A_4 &= \{(234),(243),(134),(143),(124),(142),(123),(132),(12)(34),(13)(24),(14)(23),id\} \\
(12)A_4 &= \{(1234),(1243),(1342),(1432),(24),(14),(23),(34),(1324),(1423),(12)\}
\end{aligned}$$

(f) From Chapter 5 **Example 9.**, $D_4 = \{(1234),(13)(24),(1432),id,(24),(13),(12)(34),(14)(32)\}$. So the left co-sets are

$$\begin{aligned}
D_4 &= \{(1234),(13)(24),(1432),id,(24),(13),(12)(34),(14)(32)\} \\
(12)D_4 &= \{(12),(234),(2413),(143),(34),(1423),(132),(124)\} \\
(14)D_4 &= \{(14),(123),(1342),(243),(1243),(23),(134),(142)\}
\end{aligned}$$

□