PMATH 336 Intro to Group Theory, Solutions to Assignment 1

1: Determine which of the following are groups and which of the groups are abelian.

(a) $G = \{1, 4, 7, 10, 13\}$ under multiplication modulo 15.

Solution: This is not a group because 10 does not have an inverse under multiplication modulo 15.

(b) $G = \{p(x) = ax + b \,|\, a \in U_4, b \in \mathbb{Z}_4\}$ under composition of polynomials.

Solution: We claim that G is a group. If $f(x) = ax+b$ with $a \in U_4$ and $b \in \mathbb{Z}_4$, and $g(x) = cx+d$ with $c \in U_4$ and $d \in \mathbb{Z}_4$, then we have $f(g(x)) = f(cx + d) = a(cx + d) + b = ac\,x + (ad + b)$, and we have $f(g(x)) \in G$ since $ac \in U_4$ and $ad + b \in \mathbb{Z}_4$. Thus the operation is closed. We know that composition is associative. The identity function I is given by $I(x) = 1x + 0$, which is G. Given $f(x) = ax + b$, we can find its inverse $g(x) = cx + d$ by solving $f(g(x)) = I(x)$, that is $ac\,x + (ad + b) = 1x + 0$: we need $ac = 1$, so $c = a^{-1}$, and we need $ad + b = 0$, so $d = -a^{-1}b$, and so the inverse of $f(x) = ax + b$ is given by $g(x) = a^{-1}x - a^{-1}b$, which is in G. Thus G is a group, as claimed. The group G is not abelian since, for example, if $f(x) = 3x$ and $g(x) = x + 1$ then $f(g(x)) = 3x + 3$ but $g(f(x)) = 3x + 1$.

(c) $G = \{x \in \mathbb{R} \,|\, x > 1\}$ under the operation $*$ given by $x * y = xy - x - y + 2$.

Solution: We claim that G is a group. Note first that for all $x, y \in \mathbb{R}$ we have

$$x * y = xy - x - y + 2 = (x - 1)(y - 1) + 1\,.$$

In particular, when $x, y > 1$ we have $x * y = (x - 1)(y - 1) + 1 > (1 - 1)(1 - 1) + 1 = 1$ and so $*$ does indeed give an operation on G. Also, the operation $*$ is associative since

$$(x * y) * z = \big((x - 1)(y - 1) + 1\big) * z = (x - 1)(y - 1)(z - 1) + 1 = x * \big((y - 1)(z - 1) + 1\big) = x * (y * z)\,.$$

The identity is $e = 2$ since we have $x * 2 = (x - 1)(2 - 1) + 1 = x$ and $2 * x = (2 - 1)(x - 1) + 1 = x$. Finally note that the inverse of the $x \in G$ is $y = \frac{1}{x-1} + 1$ (which lies in G since $x > 1$ implies $\frac{1}{x-1} > 0$ and hence $y = \frac{1}{x-1} + 1 > 1$) since then $x * y = (x - 1)(y - 1) + 1 = (x - 1)\big(\frac{1}{x-1}\big) + 1 = 2 = e$ and $y * x = (y - 1)(x - 1) + 1 = \big(\frac{1}{x-1}\big)(x - 1) + 1 = 2 = e$. Thus G is a group, as claimed. The group G is abelian since $x * y = (x - 1)(y - 1) + 1 = (y - 1)(x - 1) + 1 = y * x$.

2: Let G be a group with identity e.

(a) Let $a, b \in G$ with $a^4 = e$ and $ab = ba^2$. Show that $a = e$.

Solution: We have $b = be = ba^4 = (ba^2)a^2 = (ab)a^2 = a(ba^2) = a(ab) = a^2b$. Since $a^2b = b$, we have $a^2 = e$ (by cancellation). Thus $ab = ba^2 = be = b$ and hence $a = e$ (by cancellation).

(b) Let $a, b \in G$ with $a^{16} = b^9$ and $a^{25} = b^{14}$. Show that $a = b$.

Solution: We have $a = a^1 = a^{16\cdot 11 - 25\cdot 7} = (a^{16})^{11}(a^{25})^{-7} = (b^9)^{11}(b^{14})^{-7} = b^{9\cdot 11 - 14\cdot 7} = b^1 = b$.

(c) Let $a, b \in G$ with $|a| = 2$, $b \neq e$ and $ab = b^2a$. Find $|b|$ and $|ab|$.

Solution: Multiply the equation $b^2a = ab$ on the right by a to get $b^2 = aba$ (since $a^2 = e$), then square both sides to get $b^4 = abaaba = abba = a(b^2a) = a(ab) = a^2b = b$. Multiply by b^{-1} to get $b^3 = e$. Since $b \neq e$ we also have $b^2 \neq e$ $\big($since if $b^2 = e$ then multiplying both sides by b gives $b^3 = b$ and hence $e = b\big)$, and so $|b| = 3$. Note that $ab \neq e$ since if we had $ab = e$ we would have $b = eb = a^ab = a(ab) = ae = a$. On the other hand, we have $(ab)^2 = (ab)(ab) = (b^2a)(ab) = b^2a^2b = b^2eb = b^3 = e$, and so $|ab| = 2$.

3: (a) Write out the multiplication table for U_{20}.

Solution: Here is the multiplication table.

	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	1
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	9	1	3
19	19	17	13	11	9	7	3	1

(b) Find the order of each element in U_{20}.

Solution: We make a table of powers modulo 20, and on the last row we indicate the order of each element.

x	1	3	7	9	11	13	17	19
x^2	1	9	9	1	1	9	9	1
x^3	1	7	3	9	11	17	13	19
x^4	1	1	1	1	1	1	1	1
$\lvert x\rvert$	1	4	4	2	2	4	4	2

(c) Solve $x^3y^6 = 3$ for $x, y \in U_{20}$.

Solution: Let $x, y \in U_{20-}$. From the above table of powers, we have $y^6 = y^2 \in \{1, 9\}$. When $y \in \{1, 9, 11, 19\}$ we have $y^2 = y^2 = 1$ so that $x^3y^6 = 3 \iff x^3 = 3 \iff x = 7$. When $y \in \{3, 7, 13, 17\}$ we have $y^6 = y^2 = 9$ so that $x^3y^6 = 3 \iff 9x^3 = 3 \iff 9 \cdot 9\,x^3 = 9 \cdot 3 \iff x^3 = 7 \iff x = 3$. Thus the solutions are the pairs $(x, y) = (1, 7)$, $(9, 7)$, $(11, 7)$, $(19, 7)$, $(3, 3)$, $(7, 3)$, $(13, 3)$ and $(17, 3)$.

4: When R is a commutative ring (with identity), the set $M_n(R)$ of $n\times n$ matrices with entries in R is a ring (with identity) under matrix addition and matrix multiplication. The subsets $GL_n(R)=\{A\in M_n(R)\,\big|\,\det A\neq 0\}$, $SL_n(R)=\{A\in M_n(R)\,\big|\,\det A=1\}$, $O_n(R)=\{A\in M_n(R)\,\big|\,A^TA=I\}$ and $SO_n(R)=\{A\in O_n(R)\,\big|\,\det A=1\}$ are groups (with identity) under matrix multiplication.

(a) Find $\big|SL_2(\mathbb{Z}_5)\big|$.

Solution: For a matrix in $GL_2(\mathbb{Z}_5)$, the two rows are linearly independent, so the first row cannot be zero, and the second row cannot be a multiple of the first; there are $5^2-1=24$ choices for the first row and $5^2-5=20$ choices for the second row, and so we have $|GL_2(\mathbb{Z}_5)|=24\cdot 20=480$.

For each matrix A in $SL_2(\mathbb{Z}_5)$, we obtain 4 matrices in $GL_2(\mathbb{Z}_5)$ by multiplying the first row of A by 1,2,3 or 4, and hence $|SL_2(\mathbb{Z}_5)|=\frac{1}{4}|GL_2(\mathbb{Z}_5)|=120$.

We mark that the above argument shows more generally that for p prime we have

$$\big|SL_n(\mathbb{Z}_p)\big|=\tfrac{1}{p-1}(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})\,.$$

(b) Find every element of order 2 in $SL_2(\mathbb{Z}_5)$.

Solution: Let $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$. We have $A\in SL_2(\mathbb{Z}_5)$ and $A^2=I\iff\det A=1$ and $A=A^{-1}\iff$ $\det A=1$ and $\begin{pmatrix}a&b\\c&d\end{pmatrix}=\frac{1}{\det A}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}=\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\iff ad-bc=1, a=d, b=-b, c=-c\iff$ $a^2=ad=1,\ a=d, b=c=0\iff A=\begin{pmatrix}a&0\\0&a\end{pmatrix}$ with $a^2=1$. In $\mathbb{Z}_5$ we have $a^2=1\iff a\in\{1,4\}$, so the only elements $A\in SL_2(\mathbb{Z}_5)$ with $A^2=1$ are $A=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ and $\begin{pmatrix}4&0\\0&4\end{pmatrix}$. Thus the only element $A\in SL_2(\mathbb{Z}_5)$ with $|A|=2$ is $A=\begin{pmatrix}4&0\\0&4\end{pmatrix}$.

(c) Find $\big|O_2(\mathbb{Z}_5)\big|$ and $\big|SO_2(\mathbb{Z}_5)\big|$.

Solution: If $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in O_2(\mathbb{Z}_5)$ then we have $A^TA=I$, that is $\begin{pmatrix}a^2+c^2&ab+cd\\ab+cd&b^2+d^2\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Since $a^2+c^2=1$, where a and b are in $\mathbb{Z}_5$ (so that $0^2=0,\ 1^2=4^2=1$ and $2^2=3^2=4$) we must have $\begin{pmatrix}a\\c\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}4\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}$ or $\begin{pmatrix}0\\4\end{pmatrix}$. Similarly $\begin{pmatrix}b\\d\end{pmatrix}$ is one of these 4 vectors. Also, we must have $ab+cd=0$ so for example, when $\begin{pmatrix}a\\c\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$, $\begin{pmatrix}b\\d\end{pmatrix}$ must be equal to $\begin{pmatrix}0\\1\end{pmatrix}$ or $\begin{pmatrix}0\\4\end{pmatrix}$. We have $O_2(\mathbb{Z}_5)=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&4\end{pmatrix},\begin{pmatrix}4&0\\0&1\end{pmatrix},\begin{pmatrix}4&0\\0&4\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\4&0\end{pmatrix},\begin{pmatrix}0&4\\1&0\end{pmatrix},\begin{pmatrix}0&4\\4&0\end{pmatrix}\right\}$. The determinants of these matrices are all 1 or 4, and $SO_2(\mathbb{Z}_5)=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}4&0\\0&4\end{pmatrix},\begin{pmatrix}0&1\\4&0\end{pmatrix},\begin{pmatrix}0&4\\1&0\end{pmatrix}\right\}$. Thus $\big|O_2(\mathbb{Z}_5)\big|=8$ and $\big|SO_2(\mathbb{Z}_5)\big|=4$.