PMATH 347 Groups and Rings, Solutions to Assignment 1

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

(a) $\mathbb{R}^*$ under division.

Solution: $\mathbb{R}^*$ is not a group under $\div$ since $\div$ is not associative; for example $(1\div 2)\div 3 = \frac{1}{6}$ but $1\div(2\div 3) = \frac{3}{2}$.

(b) The set of all subsets of $\{1,2,3,4\}$ under union.

Solution: The set of all subsets of $\{1,2,3,4\}$ under $\cup$ is not a group. To be a group, it must have an identity, say E, and since $A\cup E = A$ for all $A \subseteq \{1,2,3,4\}$, we must have $E = \emptyset$ (the empty set). But then no non-empty set $A \subseteq \{1,2,3,4\}$ can have an inverse B, since $\emptyset \neq A \subseteq A\cup B$.

(c) $\{x\in\mathbb{R}\,\big|\,x^2\in\mathbb{Z}\}$ under addition.

Solution: $S = \{x\in\mathbb{R}|x^2\in\mathbb{Z}\}$ is not a group under $+$, since $+$ is not a well defined binary operation; for example, $1\in S$ and $\sqrt{2}\in S$ but $1+\sqrt{2}\notin S$, since $(1+\sqrt{2})^2 = 3+2\sqrt{2}\notin\mathbb{Z}$ as $\sqrt{2}$ is irrational.

(d) $\big\{(a,b)\in\mathbb{R}^2\big|\,b\neq 0\big\}$ under the operation $*$ defined by $(a,b)*(c,d) = (c+ad, bd)$.

Solution: $\{(a,b)\in\mathbb{R}^2|b\neq 0\}$ is a group under the operation $*$ defined by $(a,b)*(c,d) = (c+ad,bd)$. First note that $*$ is a well defined binary operation since $bd = 0 \Longrightarrow b = 0$ or $d = 0$. Then note that $*$ is associative, since $((a,b)*(c,d))*(f,g) = (c+ad,bd)*(f,g) = (f+cg+adg,bdg) = (a,b)*(f+cg,dg) = (a,b)*((c,d)*(f,g))$. Next note that $(a,b)*(c,d) = (a,b) \iff (c+ad,bd) = (a,b) \iff c+ad = a$ and $bd = b \iff d = 1$ and $c = 0 \iff (c,d) = (0,1)$ and also note that $(0,1)*(a,b) = (a,b)$ and so we see that $(0,1)$ is the identity. Finally note that $(a,b)*(c,d) = (0,1) \iff c+ad = 0$ and $bd = 1 \iff d = 1/b$ and $c = -a/b$ and also that $(-a/b,1/b)*(a,b) = (0,1)$, so we see that $(a,b)^{-1} = (-a/b,1/b)$. This group is not abelian since, for example, $(1,2)*(1,1) = (2,2)$, but $(1,1)*(1,2) = (3,2)$.

2: (a) Let G be a group. Suppose that for all $a, b, c, d, x \in G$, if $axb = cxd$ then $ab = cd$. Show that G is abelian.

Solution: Let $u, v \in G$. Taking $a = d = u$, $b = c = uvu$ and $x = v$, we have $axb = (u)(v)(uvu) = (uvu)(v)(u) = cxd$, and hence $uuvu = ab = cd = uvuu$. Multiplying on the left and on the right by u^{-1} gives $uv = vu$.

(b) Let G be a finite group. Show that there are an odd number of elements $x \in G$ with $x^3 = e$.

Solution: Let $S = \{x \in G \big| x^3 = e, x \neq e\}$. We must show that S has an even number of elements. To do this, we shall show that S can be partitioned into 2-element subsets of the form $\{x, x^2\}$. Note that for $x \in S$ we have $(x^2)^3 = e$ $\big($since $(x^2)^3 = x^6 = (x^3)^2 = e^2 = e\big)$ and we have $x^2 \neq e$ (since if $x^2 = e$ then multiplying both sides on the left by x gives $x^3 = x$, but then since $x^3 = e$ this would give $e = x$) and hence $x^2 \in S$. Also note that for $x \in S$ we have $x^2 \neq x$ $\big($since if $x^2 = x$ then multiplying both sides on the left by x^{-1} gives $x = e\big)$ and hence $\{x, x^2\}$ is a 2-element subset of S. Finally note that for $x, y \in S$, if $y \notin \{x, x^2\}$ then $y^2 \notin \{x, x^2\}$ $\big($since if $y^2 = x$ then squaring both sides gives $y = y^4 = x^2$, and if $y^2 = x^2$ then squaring both sides gives $y = y^4 = x^4 = x\big)$ and hence the distinct 2-element sets $\{x, x^2\}$ are disjoint. Thus S can be partitioned into 2-element subsets, hence S has an even number of elements.

(c) Let G be a non-empty finite set with a binary operation $* : G \times G \to G$ with the following properties:

(1) associativity: for all $a, b, c \in G$ we have $(a * b) * c = a * (b * c)$,
(2) right cancellation: for all $a, b, c \in G$, if $a * c = b * c$ then $a = b$, and
(3) left cancellation: for all $a, b, c \in G$, if $c * a = c * b$ then $a = b$.

Show that G is group under $*$.

Solution: For $a, b \in G$, we write $a * b$ as ab. Because we have right-cancellation, it follows that for all $c \in G$, the right-multiplication map $R_c : G \to G$ given by $R_c(a) = ac$ is injective. Since G is finite, R_c is bijective for all $c \in G$. Similarly, because we have left cancellation, it follows that L_c is bijective for all $c \in G$, where $L_c(a) = ca$.

Fix $u \in G$. Since L_u is bijective, we can choose $e \in G$ so that $ue = u$. We claim that $ea = a$ for all $a \in G$. Let $a \in G$ and say $ea = b$. Then we have $ua = (ue)a = u(ea) = ub$ and hence $a = b$ by left-cancellation. Thus $ea = a$ for all $a \in G$, as claimed. In particular, we have $ee = e$. We claim that $ae = a$ for all $a \in G$. Let $a \in G$, and say $ae = b$. Then $ae = a(ee) = (ae)e = be$ and so $a = b$ by right-cancellation. Thus $ae = a$ for all $a \in G$ as claimed. This shows that the element e acts as a (2-sided) identity element for G.

It remains to show that for every $a \in G$ there exists $b \in G$ such that $ab = e = ba$. Let $a \in G$. Since L_a is bijective we can choose $b \in G$ so that $ab = e$, and since R_a is bijective we can choose $c \in G$ so that $ca = e$. Then we have $c = ce = c(ab) = (ca)b = eb = b$.

3: Let R be a ring with 1.

(a) Let $a, b \in R$. Suppose that $a^3 = a$ and $ab + ba = 1$. Show that $a^2 = 1$.

Solution: We have $a = a \cdot 1 = a(ab + ba) = a^2 b + aba$, and we have $a = 1 \cdot a = (ab + ba)a = aba + ba^2$, and so $a^2 b = a - aba = ba^2$. Since $ab + ba = 1$, and $a^3 = a$ and $a^2 b = ba^2$, we have

$$a^2 = a^2 \cdot 1 = a^2(ab + ba) = a^3 b + a^2 ba = ab + ba^2 a = ab + ba^3 = ba + ab = 1.$$

(b) Let $a, b \in R$. Suppose that a and b and $a + b$ are units. Show that $a^{-1} + b^{-1}$ is a unit.

Solution: We have

$$a(a^{-1} + b^{-1})b = a\,a^{-1}b + a\,b^{-1}b = b + a = a + b.$$

It follows that

$$\begin{aligned}&(a^{-1} + b^{-1})\big(b(a + b)^{-1}a\big) = a^{-1}a(a^{-1} + b^{-1})b\,(a + b)^{-1}a = a(a + b)(a + b)^{-1}a = 1 \text{ and}\\ &\big(b(a + b)^{-1}a\big)(a^{-1} + b^{-1}) = b(a + b)^{-1}a(a^{-1} + b^{-1})b\,b^{-1} = b(a + b)^{-1}(a + b)b^{-1} = 1\end{aligned}$$

and so $a^{-1} + b^{-1}$ is invertible with two-sided inverse $b(a + b)^{-1}a$.

(c) Show that if $a^2 = a$ for all $a \in R$ then R is commutative.

Solution: Suppose that $a^2 = a$ for all $a \in R$. Let $a \in R$. Then

$$a + a = (a + a) \cdot (a + a) = a \cdot a + a \cdot a + a \cdot a + a \cdot a = a + a + a + a.$$

Subtracting $a + a$ from both sides gives $a + a = 0$. This proves that $a + a = 0$ for all $a \in R$.

Now let $a, b \in R$. Then

$$a + b = (a + b) \cdot (a + b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b = a + a \cdot b + b \cdot a + b = (a \cdot b + b \cdot a) + a + b.$$

Subtract $a + b$ from both sides to get $ab + ba = 0$. Thus

$$ab = ab + 0 = ab + (ab + ba) = (ab + ab) + ba = 0 + ba = ba.$$

4: (a) Find $\left|GL_2(\mathbb{Z}_4)\right|$.

Solution: Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}^4$. We have $A \in GL_2(\mathbb{Z}_4)$ when $\det A \in U(4)$, that is when $ad - bc = 1$ or 3. There are 16 possibilities for the first row (a, b) of A, since there are 4 choices for a and 4 for b. Fix the first row (a, b).

If $a = 1$ then $ad - bc = d - bc$, so $A \in GL_2(\mathbb{Z}_4)$ when $d - bc = 1$ or 3. For any choice of c, there two values of d for which $A \in GL_2(\mathbb{Z}_4)$, namely $d = 1 + bc$ and $d = 3 + bc$. Thus when $a = 1$ there are $4 \cdot 2 = 8$ choices for (c, d) such that $A \in GL_2(\mathbb{Z}_4)$.

If $a = 3 = -1$, then $ad - bc = -b - bc$, so for every choice of c there are two choices of d for which $A \in GL_2(\mathbb{Z}_4)$, namely $d = -1 - bc$ and $d = -3 - bc$. Thus when $a = 3$ there are again 8 choices of (c, d) for which $A \in GL_2(\mathbb{Z}_4)$.

We have shown that when a is odd there are 8 choices of (c, d) for which $A \in GL_2(\mathbb{Z}_4)$. Similarly, when b is odd, then there will be 8 choices of (c, d) for which $A \in GL_2(\mathbb{Z}_4)$.

On the other hand, when a and b are both even, the determinant $\det A = ad - bc$ will also be even, so $A \notin GL_2(\mathbb{Z}_4)$.

Of the 16 possibilities for the first row (a, b), there are 4 for which a and b are both even, namely $(a, b) = (0, 0)$, $(0, 2)$, $(2, 0)$ and $(2, 2)$, and there are 12 for which either a or b is odd. Thus the total number of matrices in $GL_2(\mathbb{Z}_4)$ is equal to $12 \cdot 8 = 96$, that is $\left|GL_2(\mathbb{Z}_4)\right| = 96$.

(b) List every element in each conjugacy class in $GL_2(\mathbb{Z}_2)$.

Solution: Let $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $C = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $D = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $E = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ so that

$$GL_2(\mathbb{Z}_2) = \{I, A, B, C, D, E\}.$$

We make a multiplication table (showing the value of XY for each pair A, B) and then we use the multiplication table to help make a conjugation table (showing the value of XYX^{-1} for each pair X, Y).

$X\backslash Y$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	C	B	E	D
B	B	D	I	E	A	C
C	C	E	A	D	I	B
D	D	B	E	I	C	A
E	E	C	D	A	B	I

$X\backslash Y$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	I	A	E	D	C	B
B	I	E	B	D	C	A
C	I	B	E	C	D	A
D	I	E	A	C	D	B
E	I	B	A	D	C	E

The conjugacy classes are the sets of matrices of each column of the conjugation table, that is $Cl(I) = \{I\}$, $Cl(A) = \{A, B, E\}$ and $Cl(C) = \{C, D\}$.

(c) Find the number of elements in the conjugacy class of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ in $GL_2(\mathbb{Z}_3)$.

Solution: Recall from linear algebra that for a field F, two matrices $A, B \in M_n(F)$ are similar when there exists a matrix $P \in GL_n(F)$ such that $B = PAP^{-1}$. For $A, B \in GL_n(F)$, we see that A and B are similar if and only if they are conjugate, in which case we write $A \sim B$. Also recall that when $A \sim B$ we have $\det A = \det B$ and $f_A(x) = f_B(x)$ where $f_A(x)$ denotes the characteristic polynomial of A. Finally, recall that when $A \in M_n(F)$ has n distinct eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_n$, we have $A \sim D$ where D is the diagonal matrix with diagonal entries $\lambda_1, \lambda_2, \cdots, \lambda_n$.

For $D = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $M_2(\mathbb{Z}_3)$, we have

$$\begin{aligned} A \sim D &\iff f_A(x) = f_D(x) \\ &\iff x^2 - (a+d)x + (ad - bc) = x^2 + 2 \\ &\iff a + d = 0 \text{ and } ad - bc = 2 = -1 \\ &\iff d = -a \text{ and } bc = 1 - a^2 \end{aligned}$$

When $a = 0$ we have $bc = 1 - a^2 \iff bc = 1 \iff (b, c) \in \{(1,1), (2,2)\}$ and when $a \in \{1, 2\}$ we have $bc = 1 - a^2 \iff bc = 0 \iff (b, c) \in \{(0,0), (0,1), (0,2), (1,0), (2,0)\}$. Thus there are exactly 12 matrices $A \in M_2(\mathbb{Z}_3)$ which are similar to D, and for each of these we have $\det A = \det D = 2$ so that $A \in GL_2(\mathbb{Z}_3)$. To be explicit, we have $Cl(D) = \left\{ \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 2 \\ 0 & 1 \end{smallmatrix}\right) \right\}$.