PMATH 336 Introduction to Group Theory, Solutions to the Exercises for Chapter 1

1: (a) Write down the multiplication table for U_{18}.

Solution:

	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

(b) Find the order of each element in U_{18}.

Solution: We tabulate powers of each element a until we reach n such that $a^n = 1$. :

a	a^2	a^3	a^4	a^5	a^6
1					
5	7	17	13	11	1
7	13	1			
11	13	17	7	5	1
13	7	1			
17	1				

The table shows that $|1| = 1$, $|5| = |11| = 6$, $|7| = |13| = 3$ and $|17| = 2$.

2: Determine which of the following are groups.

(a) $X = \{(x, y) \in \mathbb{R}^2 \big| x^2 = y^2\}$ under vector adition.

Solution: This is not a group because vector addition is not an operation on X (X is not closed under $+$), for example $(1, 1) \in X$ and $(1, -1) \in X$ but $(1, 1) + (1, -1) = (1, 0) \notin X$.

(b) $G = \{1, 3, 5, 7, 9\}$ under multiplication modulo 10.

Solution: This is not a group. If it were, then the identity would have to be 1, but then 5 has no inverse.

(c) $\mathbb{R}$ under the operation $*$ given by $x * y = x + y + 1$.

Solution: This is a group. The operation $*$ is associative since $(x*y)*z = (x+y+1)*z = x+y+z+2$ and $x * (y * z) = x * (y + z + 1) = x + y + z + 2$. To find the identity e, we solve $x * e = x$, that is $x + e + 1 = x$ to get $e = -1$. To find the inverse of $x \in \mathbb{R}$, we solve $x * y = e$, that is $x + y + 1 = -1$, to get $y = -x - 2$.

(d) $H = \{1, 2, 4, 8, 16\}$ under the operation $*$ given by $a * b = \gcd(a, b)$.

Solution: This is not a group. If it were, then the identity would have to be 16, since $\gcd(a, 16) = a$ for all $a \in H$. But then 16 is the only element in H with an inverse, since for $a, b \in H$, $\gcd(a, b) = 16 \Longrightarrow a = b = 16$.

3: Let G be a group with identity e. Prove each of the following statements.

(a) If $(\forall a, b, c \in G \ \ ab = ca \Rightarrow b = c)$ then G is abelian.

Solution: Suppose that for all $a, b, c \in G$ we have $ab = ca \Longrightarrow b = c$ (so we can cancel an a on the left with an a on the right). Then since $aba = aba$, we can cancel the a on the left with the a on the right to get $ba = ab$.

(b) If $(\forall a, b \in G \ \ (ab)^2 = a^2b^2)$ then G is abelian.

Solution: Suppose that for all $a, b \in G$ we have $(ab)^2 = a^2b^2$. Then from $abab = aabb$, cancel the a on the left to get $bab = abb$, and then cancel the b on the right to get $ba = ab$.

(c) If $(\forall a \in G \ \ a^2 = e)$ then G is abelian.

Solution: Suppose that for all $a \in G$ we have $a^2 = e$. Then in particular, given $a, b \in G$ we have $aa = e$, $bb = e$ and $abab = e$. Multiply the equation $abab = e$ on the left by a to get $aabab = a$, use the fact that $aa = e$ to get $bab = a$, then multiply on the right by b to get $babb = ab$ and use $bb = e$ to get $ba = ab$.