Math 355 – PS#1 Solutions
Summer 2, 2012

p.43 #3. Write out the Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$*. How many elements are in each group? Are the groups the same? Why or why not?*

Solution. The symmetries of a rectangle with centroid at the origin and sides parallel to the coordinate axes are generated by reflections σ_x in the x-axis and σ_y in the y-axis. Their square is identity e and their product (in either order) is the rotation ρ of 180° about the origin. Furthermore, $\rho \circ \sigma_y = (\sigma_x \circ \sigma_y) \circ \sigma_y = \sigma_x \circ (\sigma_y \circ \sigma_y) = \sigma_x \circ e = \sigma_x$, and similarly, $\rho \circ \sigma_x = \sigma_y$. Thus the Cayley tables for the symmetries of a rectangle and $(\mathbb{Z}_4, +)$ are:

$\circ$	e	σ_x	σ_y	ρ
e	e	σ_x	σ_y	ρ
σ_x	σ_x	e	ρ	σ_y
σ_y	σ_y	ρ	e	σ_x
ρ	ρ	σ_y	σ_x	e

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

These groups are *not* the same. While each symmetry has square the identity e, the square of 1 and 3 is 2, which is not the identity 0.

p.43 #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.*

Proof. To prove closure we must show that if $a, b \in S$, then $a * b \in S$. We prove the contrapositive: if $a * b \notin S$, either $a \notin S$ or $b \notin S$. But if $a * b \notin S$, then $a * b = a + b + ab = -1$. Adding 1 to both sides and factoring gives $0 = 1 + (-1) = 1 + a + b + ab = (1 + a)(1 + b)$. Hence either $a = -1 \notin S$ or $b = -1 \notin S$. For commutativity, note that $a*b = a+b+ab = b+a+ba = b*a$. To check associativity, let $a, b, c \in S$ and note that $(a * b) * c = (a * b) + c + (a * b) c = (a + b + ab) + c + (a + b + ab) c = a + (b + c + bc) + a (b + c + bc) = a+(b * c)+a (b * c) = a*(b * c)$. There is an identity element, namely 0, since commutativity and the definition of $*$ give $0 * a = a * 0 = a + 0 + a \cdot 0 = a$. For inverses, first note that if $a \in S$, then $\frac{-a}{a+1} \in S$ since $a \neq -1$. But $a * \left(\frac{-a}{a+1}\right) = a + \frac{-a}{a+1} + a\left(\frac{-a}{a+1}\right) = \frac{a(a+1)-a-a^2}{a+1} = 0$, and by commutativity, $\left(\frac{-a}{a+1}\right) * a = a * \left(\frac{-a}{a+1}\right) = 0$. Therefore $a^{-1} = \frac{-a}{a+1}$.

p.43 #25. Let $U(n)$ *be the group of units in* $\mathbb{Z}_n$*. If* $n > 2$*, prove that there is an element* $k \in U(n)$ *such that* $k^2 = 1$ *and* $k \neq 1$*.*

Proof. Note that $(n-1)^2 - 1 = \left(n^2 - 2n + 1\right) - 1 = n(n-2) \equiv 0 \pmod{n}$. Set $k = n - 1$; then $k^2 = 1$ and $k \geq 2$ since $n \geq 3$.

p.43 #29. Prove the right and left cancellation laws for a group G*; i.e., if* $a, b, c \in G$ *then* $ba = ca$ *implies* $b = c$ *and* $ab = ac$ *implies* $b = c$*.*

Proof. If $a \in G$, then $a^{-1} \in G$ since G has inverses. Thus $ba = ca$ implies $b = be = b\left(aa^{-1}\right) = (ba)a^{-1} = (ca)a^{-1} = ce = c$. Similarly, $ab = ac$ implies $b = eb = \left(a^{-1}a\right)b = a^{-1}(ab) = a^{-1}(ac) = ec = c$.

p.43 #31. Show that is G *is a finite group of even order, there is an element* $a \in G$ *such that* $a \neq e$ *and* $a^2 = e$*.*

Proof. Let $G = \{a_1, a_2, \ldots, a_{2n} = e\}$. Since inverses are unique, by Proposition 3.2, each $a_i \in G$ pairs off with its unique inverse a_j. Since $e^2 = e$, the element a_{2n} pairs off with itself. Thus some $a_i \in \{a_1, \ldots, a_{2n-1}\}$ must also pair off with itself so that $a_i^2 = e$.