Modern Algebra - MATH 5163 - Graded Homework #1 - Fall 2007

Mike Fairchild[1]

Problem 1 (Exercise 1.13). Describe the symmetries of a nonsquare rectangle. Construct the corresponding Cayley table.

SOLUTION: For a nonsquare rectangle, there are only four symmetries. Two reflections: one along a line splitting the rectangle in half horizontally, denoted H, and one along a line splitting the rectangle in half vertically, denoted V (see pictures drawn in next to Cayley table). There are two rotational symmetries: one is a rotation about the center of 0° (the identity transformation), denoted R_0, and the other is a rotation about the center of 180°, denoted R_{180}. Below is the Cayley table.

	R_0	R_{180}	H	V
R_0	R_0	R_{180}	H	V
R_{180}	R_{180}	R_0	V	H
H	H	V	R_0	R_{180}
V	V	H	R_{180}	R_0

Problem 2. Let $\phi : A \to B$ and $\psi : B \to C$ be functions such that $\psi\phi$ is onto. Prove that ψ is onto.

PROOF: Let $c \in C$. Since $\psi\phi$ is onto, there is an $a \in A$ such that $(\psi\phi)(a) = c$. By associativity of function composition, we may write $\psi(\phi(a)) = c$. By the definition of ϕ, we have $\phi(a) = b$ for some $b \in B$. Thus, for this choice of b, we have $\psi(b) = c$. This shows that ψ is onto, since for any $c \in C$ there is a $b \in B$ such that $\psi(b) = c$.

Problem 3 (Exercise 2.24). Construct a Cayley table for $U(12)$.

SOLUTION: $U(12)$ is the set of all positive integers less than 12 and relatively prime to 12. It forms a group under multiplication modulo 12. The positive integers a satisfying $\gcd(a, 12) = 1$ and $1 \leq a < 12$ are $\{1, 5, 7, 11\}$. The Cayley table is shown below.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Problem 4. Consider the group G defined by the Cayley table in problem 17, Chapter 3, page 68.
(a) Find the order of 7.
(b) Find $\langle 7 \rangle$.

[1] http://www.mikef.org/

SOLUTION: (a) By referencing the Cayley table in problem 17, page 68, it is clear that $e = 1$. Also, $7^1 = 7, 7^2 = 5, 7^3 = 7^2 \cdot 7 = 5 \cdot 7 = 3, 7^4 = 7^3 \cdot 7 = 3 \cdot 7 = 1 = e$. Therefore, $|7| = 4$.

(b) By part (a), the cyclic subgroup of G generated by 7 is $\langle 7 \rangle = \{7, 5, 3, 1\}$ (note that $|\langle 7 \rangle| = 4$, agreeing with part (a), as it must by Corollary 1 to Theorem 4.1.)

Problem 5. (a) Let G be an abelian group, and let $H = \{x \in G \mid x^2 = e\}$. (Thus an element g of G is in H precisely when $g^2 = e$). Show that H is a subgroup of G.
(b) Given an example of a (necessarily nonabelian) group G for which $H = \{x \in G \mid x^2 = e\}$ is *not* a subgroup of G.

PROOF: (a) Clearly $e^2 = e$ in any group, and so $e \in H$. Let $a, b \in H$. Then $a^2 = aa = e$, and so $a^{-1} = a$. Hence $a^{-1} \in H$ whenever $a \in H$. Now consider $(ab)(ab)$. That G is abelian and using associativity gives us $(ab)(ab) = (ba)(ab) = b(aa)(b) = beb = bb = e$. Thus $(ab) \in H$. By Theorem 3.2, H is a subgroup of G.

(b) The group D_4 suffices. D_4 is nonabelian, since $HR_{90} = D \neq D' = R_{90}H$. By inspecting the main diagonal of the Cayley table for D_4 on page 33, it is clear that $H = \{R_0, R_{180}, H, V, D, D'\}$ (note the distinction between the group operation H and the subset H of G – it should be clear from the context which is appropriate). However, $HD = R_{90} \notin H$, so H is not closed under the group operation. Therefore, H cannot be a subgroup of D_4.

Problem 6. Let G be a set together with a binary operation (where, as in the definition on page 43, the element assigned to the pair (a, b) is ab). Further suppose that

1. This operation is associative.
2. There is an element $e \in G$ such that $ae = a$ for each $a \in G$.
3. For each $a \in G$, there is an element $b \in G$ such that $ab = e$.

Prove that G is a group. (Note that there is really something to do here, since you are given that the "identity" e works only on the right and that the "inverse" of an element a works only on the right.)

PROOF: The group operation is associative by hypothesis 1, and so (by the definition of a group) it remains to show that the identity works on the left and also each element has a left inverse.

Let $a \in G$. By hypothesis 3, there exists $b \in G$ so that $ab = e$. Then, $b(ab) = be$. By hypothesis 3, b has a right inverse, say $c \in G$. Now write $b(ab)c = (be)c$. Using associativity, we may write $(ba)(bc) = (be)c \Rightarrow (ba)e = bc = e \Rightarrow ba = e$. Therefore, if b is a right inverse of a, it is also a left inverse (hence we may uniquely write $a^{-1} = b$ such that $a^{-1}a = e = aa^{-1}$).

Let $a \in G$. By hypothesis 2, there is an $e \in G$ such that $a = ae$. By hypothesis 3 and the existence of left and right inverses (shown above), there is a $b \in G$ such that $ba = e$. Thus, using associativity, $a = ae = a(ba) = (ab)a = ea$. Hence if e is a right identity it is also a left identity.

Now we have shown that the identity is actually a left and right identity, and that each element has a left and right inverse. Since the operation is associative, the set G satisfying hypotheses 1-3 above is a group, by the definition of a group.