Mathematics 243, section 3 – Algebraic Structures
Solutions for Problem Set 8
November 16, 2012

'A' Section

1. Consider the 2×2 matrices I_2, S, X, Y, D, T defined by

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Let $G = \{I_2, S, S^2, S^3, X, Y, D, T\}$. Construct the operation table for matrix multiplication on this set and verify that G is a group under this operation.

Solution: The table looks like this (taking the products in order row $\times$ column in all cases):

$\cdot$	I_2	S	S^2	S^3	X	Y	D	T
I_2	I_2	S	S^2	S^3	X	Y	D	T
S	S	S^2	S^3	I_2	D	T	Y	X
S^2	S^2	S^3	I_2	S	Y	X	T	D
S^3	S^3	I_2	S	S^2	T	D	X	Y
X	X	T	Y	D	I_2	S^2	S^3	S
Y	Y	D	X	T	S^2	I_2	S	S^3
D	D	X	T	Y	S	S^3	I_2	S^2
T	T	Y	D	X	S^3	S	S^2	I_2

The table shows that G is closed under matrix multiplication, so this is a binary operation. Matrix multiplication is always associative as we saw before, so this operation is associative. The element I_2 is an identity. Finally, each element has an inverse for matrix multiplication. I, S^2, X, Y, T, D are their own inverses, while $S^{-1} = S^3$ and $(S^3)^{-1} = S$.

2. a. Let $G = \mathbb{Z}_{12}$ under the operation of *addition* modulo 12. Determine the cyclic subgroups $\langle [a] \rangle$ for all $[a] \in \mathbb{Z}_{12}$.

Solution: We have

$$\begin{aligned}
\langle [0] \rangle &= \{[0]\} \\
\langle [1] \rangle &= \mathbb{Z}_{12} = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle \\
\langle [2] \rangle &= \{[0], [2], [4], [6], [8], [10]\} = \langle [10] \rangle \\
\langle [3] \rangle &= \{[0], [3], [6], [9]\} = \langle [9] \rangle \\
\langle [4] \rangle &= \{[0], [4], [8]\} = \langle [8] \rangle \\
\langle [6] \rangle &= \{[0], [6]\}
\end{aligned}$$

b. Conjecture a general formula for the number of elements in $\langle [a] \rangle$ in terms of the integers a and 12. Check out your conjecture on the corresponding list of cyclic subgroups of $\mathbb{Z}_{20}$ constructed in class on November 14.

Solution: The pattern that fits all of these examples is that the number of elements in $\langle [a] \rangle \subseteq \mathbb{Z}_n$ is equal to $n/\gcd(a,n)$. For instance, with $n = 12$ and $a = 10$, we have $\gcd(10,12) = 2$, and $\langle [10] \rangle$ has $12/2 = 6$ elements. Moreover, all the a with the same $\gcd(a,n)$ apparently generate the same cyclic subgroup. *Comment:* These patterns do hold in general and we will prove them shortly.

'B' Section

1. Let

$$G = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

Show that G is a group under the operation of matrix addition.

Solution: We know that $M_{3\times 3}(\mathbb{R})$ is a group under matrix addition. So a sneaky method here is to apply the "shortcut method" of Theorem 3.10 in the text to show that G is a subgroup of $M_{3\times 3}(\mathbb{R})$. G is definitely nonempty since it contains elements for all triples a, b, c of real numbers. Next, if

$$X = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad Y = \begin{pmatrix} 0 & a' & b' \\ 0 & 0 & c' \\ 0 & 0 & 0 \end{pmatrix}$$

are in G, then

$$X - Y = \begin{pmatrix} 0 & a - a' & b - b' \\ 0 & 0 & c - c' \\ 0 & 0 & 0 \end{pmatrix} \in G$$

as well. Therefore G is a subgroup of $M_{3\times 3}(\mathbb{R})$, hence a group.

2. Let

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

Is G is a group under the operation of matrix multiplication. If so, say why; if not say which properties in the definition fail.

Solution: We know that $GL_3(\mathbb{R})$ is a group under matrix multiplication. So a sneaky method here is to apply the "shortcut method" of Theorem 3.10 in the text to show that G is a subgroup of $GL_3(\mathbb{R})$. G is definitely nonempty since it contains elements for all triples a, b, c of real numbers. Next, if

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad Y = \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}$$

are in G, then

$$Y^{-1} = \begin{pmatrix} 1 & -a' & a'c' - b' \\ 0 & 1 & -c' \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence

$$XY^{-1} = \begin{pmatrix} 1 & a - a' & a'c' - b' - ac' + b \\ 0 & 1 & c - c' \\ 0 & 0 & 1 \end{pmatrix} \in G$$

as well. Therefore G is a subgroup of $GL_3(\mathbb{R})$, hence a group.

3. Let G be a group, and consider the relation R on G defined by $xRy \leftrightarrow y = axa^{-1}$ for some $a \in G$. (If xRy is true, the a that works in the equation will depend on x, y.) R is called the *conjugacy* relation on G.

   a. Show that conjugacy is an equivalence relation on G.

   Solution: For all $x \in G$, we have xRx since $x = exe^{-1}$. Therefore R is reflexive. If xRy, then $y = axa^{-1}$. If we multiply both sides of this equality by a^{-1} on the left and a on the right, we get $x = a^{-1}ya = a^{-1}y(a^{-1})^{-1}$. It follows that yRx is also true, so R is symmetric. Finally, if xRy and yRz, then $y = axa^{-1}$ and $z = byb^{-1}$ for some $a, b \in G$. Substituting, we get $z = b(axa^{-1})b^{-1} = (ba)x(ba)^{-1}$ by associativity and the reverse order law for inverses. Therefore R is transitive.

   b. Show that G is an abelian group if and only if the equivalence classes for the conjugacy relation satisfy $[x] = \{x\}$ for all $x \in G$.

   Solution: We have $[x] = \{x\}$ if and only if $x = axa^{-1}$ for all $a \in G$, or equivalently if and only if $xa = ax$. This is true for all classes $[x]$ if and only if $xa = ax$ for all a and all x in G. That is the same as saying the operation in G is commutative, or that G is an abelian group.

   c. More generally, show that if $[x] = \{x\}$ for some element $x \in G$, then $xa = ax$ for all $a \in G$ and conversely. The set of such elements x is called the *center* of G: The center is the subset of G defined by:

   $$Z(G) = \{x \in G \mid xa = ax \text{ for all a in } G\}.$$

   Solution: One direction is essentially the same as the argument for part of the proof of part b, except we are no longer assuming that $[x] = \{x\}$ holds for all $x \in G$, just for some particular $x \in G$. This proof is "reversible," so it can be phrased like this:

$$\begin{aligned}
[x] = \{x\} &\Leftrightarrow x = axa^{-1} \text{ for all } a \in G \\
&\Leftrightarrow xa = axa^{-1}a \text{ for all } a \in G \\
&\Leftrightarrow xa = ax(a^{-1}a) \text{ for all } a \in G, \text{ by associativity} \\
&\Leftrightarrow xa = axe \text{ for all } a \in G, \text{ by definition of inverse} \\
&\Leftrightarrow xa = ax \text{ for all } a \in G, \text{ by definition of identity element.}
\end{aligned}$$

Hence $[x] = \{x\}$ if and only if $x \in Z(G)$, the center of G.

d. Show that the center of G (as defined in part c) is a subgroup of G.

Solution: We again use the criterion of Theorem 3.10: $Z(G)$ is not empty since it always contains the identity element $e \in G$ – recall $ex = x = xe$ for all $x \in G$. Next, let $x, y \in Z(G)$, then $xa = ax$ and $ya = ay$ for all $a \in G$. But then $y^{-1}yay^{-1} = y^{-1}ayy^{-1}$ as well so $ay^{-1} = y^{-1}a$ for all $a \in G$. Hence by associativity and this last observation, for all $a \in G$:

$$(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1}).$$

This shows $xy^{-1} \in Z(G)$, so $Z(G)$ is a subgroup of G.

e. Let $x \in G$ be a fixed element and define $C_x = \{a \in G \mid x = axa^{-1}\}$. Show that C_x is a subgroup of G (C_x is called the *centralizer of* x).

Solution: The idea of the proof is similar to that of the proof of part d. First, C_x is not empty since C_x contains at least the identity element. Let $a, b \in C_x$. Then $x = axa^{-1} = bxb^{-1}$. It also follows by multiplying both sides of the equality $x = bxb^{-1}$ by b^{-1} on the left and b on the right that $b^{-1}xb = x$. But then by the reverse order law and associativity,

$$(ab^{-1})x(ab^{-1})^{-1} = ab^{-1}xba^{-1} = a(b^{-1}xb)a^{-1} = axa^{-1} = x.$$

It follows that $ab^{-1} \in C_x$, so C_x is a subgroup by Theorem 3.10.

f. Let $G = \mathcal{S}(A)$ be the group of permutations of $A = \{a, b, c\}$. Using the names for the elements of this group we introduced in Problem Set 3, find all of the equivalence classes for the conjugacy relation on G (there are three of them), determine the centralizer of each element of G, and the center of G. How are the sizes of the equivalence class of x and the number of elements of the centralizer of x related in each case?

Solution: Recall that $\mathcal{S}(A) = \{I_A, R_a, R_b, R_c, C_1, C_2\}$. Computing we find that there are exactly three conjugacy classes:

$$\begin{aligned}
[I_A] &= \{I_A\} \\
[R_a] &= \{R_a, R_b, R_c\} = [R_b] = [R_a] \\
[C_1] &= \{C_1, C_2\}
\end{aligned}$$

To start, since I_A is the identity element of this group, which commutes with every element, it follows from part c above, that $[I_A] = \{I_A\}$. The rest can be read off from the operation table you derived in Problem Set 3. For example,

$$R_b = R_c \circ R_a \circ R_c^{-1},$$

so $R_b \in [R_a]$. Similarly

$$R_c = R_b \circ R_a \circ R_b^{-1},$$

so $R_c \in [R_a]$. On the other hand conjugating C_1 or C_2 by any element of $\mathcal{S}(A)$ always yields either C_1 or C_2, so those elements form another conjugacy class. The centralizers are as follows:

$$\begin{aligned} C_{I_A} &= \mathcal{S}(A) \\ C_{C_1} = C_{C_2} &= \{I_A, C_1, C_2\} \\ C_{R_a} &= \{I_A, R_a\} \\ C_{R_b} &= \{I_A, R_b\} \\ C_{R_c} &= \{I_A, R_c\}. \end{aligned}$$

(For instance, from the group table for $\mathcal{S}(A)$, we see I, C_1, C_2 all commute with C_1, but $R_a \circ C_1 = R_b \neq R_c = C_1 \circ R_a$, $R_b \circ C_1 = R_c \neq R_a = C_1 \circ R_b$, and $R_c \circ C_1 = R_a \neq R_b = C_1 \circ R_c$. These computations show that none of R_a, R_b, R_c are in the centralizer of C_1.) In each case, the product of the size of the conjugacy class times the order of the centralizer equals $6 = |\mathcal{S}(A)|$. (Equivalently, the size of the conjugacy class of x is $\frac{6}{|C_x|}$ in each case.)

4. Let H and K be subgroups of a group G.

   a. Show that $H \cap K$ is also subgroup of G.

   Solution: Both H and K contain e, so $H \cap K \neq \emptyset$. Next, let $x, y \in H \cap K$, then $xy^{-1} \in H$ since H is a subgroup. Similarly $xy^{-1} \in K$ since K is a subgroup. Thus $xy^{-1} \in H \cap K$. It follows that $H \cap K$ is a subgroup of G by Theorem 3.10.

   b. Find an example where $H \cup K$ *is* a subgroup of G and one where $H \cup K$ *is not* a subgroup of G.

   Solution: Consider the subgroups $H = \{I_A, R_a\}$ and $K = \{I_A, R_b\}$ of $\mathcal{S}(A)$ from question 3f above. $H \cup K$ is not a subgroup of $\mathcal{S}(A)$ because $H \cup K$ is not closed under composition $R_a \circ R_b = C_1 \notin H \cup K$. On the other hand if $H = K$, then $H \cup K = H = K$ is a subgroup.