Mathematics 243, section 3 – Algebraic Structures
Solutions for Final Examination – December 15, 2012

I. Let $\varphi, \psi : \mathbb{Z} \to \mathbb{Z}$ be the mappings defined

$$\varphi(x) = \begin{cases} 3x+1 & \text{if } x \text{ is odd} \\ x/2 & \text{if } x \text{ is even} \end{cases}$$

$$\psi(x) = \begin{cases} x-1 & \text{if } x \text{ is odd} \\ x+1 & \text{if } x \text{ is even} \end{cases}$$

A) What is the set $\varphi(\{1,2,3,4\})$?

Solution: By definition,

$$\varphi(\{1,2,3,4\}) = \{\varphi(1), \varphi(2), \varphi(3), \varphi(4)\} = \{4,1,10,2\}.$$

B) What is the mapping $\varphi \circ \psi$?

Solution: Since $x-1$ is even if x is odd, while $x+1$ is odd if x is even we have:

$$(\varphi \circ \psi)(x) = \begin{cases} 3(x+1)+1 = 3x+4 & \text{if } x \text{ is even} \\ (x-1)/2 & \text{if } x \text{ is odd} \end{cases}$$

II. Let $A = \{1,2\}$ and let $\mathcal{P} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ (the collection of all subsets of A). Let $*$ be the binary operation on $\mathcal{P}$ defined by $B*C = B-(B\cap C)$. For instance, $\{1,2\}*\{1\} = \{1,2\}-\{1\} = \{2\}$.

A) Compute the rest of the operation table for $*$ on $\mathcal{P}$.

Solution:

$*$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\emptyset$

B) Is $*$ a commutative operation? Is it associative?

Solution: $*$ is not commutative, since for instance $\{1\}*\{1,2\} = \emptyset$, but $\{1,2\}*\{1\} = \{2\}$. It is not associative, since for instance $(\{1,2\}*\{1\})*\{1\} = \{2\}*\{1\} = \{2\}$, but $\{1,2\}*(\{1\}*\{1\}) = \{1,2\} * \emptyset = \{1,2\}$.

C) Is there an identity element for $*$ in $\mathcal{P}$. If so, what is the identity element?

Solution: There is no identity element since no row of the table above consists of the same sets as the column labels. (Note that $\emptyset$ is a right identity, but not a left identity.)

III.

A) Let a, b be integers, at least one of which is nonzero. Show that there is an integer d satisfying the definition of $\gcd(a, b)$ that is contained in the set $S = \{ma + nb \mid m, n \in \mathbb{Z}\}$.

Solution: If one of a, b is zero, say $b = 0$, then $\gcd(a, b) = |a| = (\pm 1)a$, which is an element of S. So now assume that a, b are both nonzero. By adjusting the signs of a, b, we can always produce strictly positive elements in S. Let d be the smallest strictly postive element, which exists by the Well Ordering Principle. We will show that d satisfies the properties of $\gcd(a, b)$. First $d > 0$ is true by construction. Next, we will show $d|a$. By the division algorithm, we have $a = qd + r$ where $0 \leq r < d$. But $a, qd \in S$, so $r = a - qd$ is in S as well. This shows that $r = 0$ since r cannot be strictly smaller than d. Similarly, $d|b$. Now let c be any integer satisfying $c|a$ and $c|b$, so $a = rc$ and $b = sc$ for some integers r, s. Since $d = ma + nb$ for some integers m, n, we have $d = m(rc) + n(sc) = (mr + ns)c$. Hence $c|d$. Therefore d satisfies the properties in the definition of $\gcd(a, b)$

B) Find the integer $d = \gcd(535, 410)$ and express d in the form $d = 535m + 410n$ for some integers m, n.

Solution: By the Euclidean Algorithm

$$\begin{aligned} 535 &= 1 \cdot 410 + 125 \\ 410 &= 3 \cdot 125 + 35 \\ 125 &= 3 \cdot 35 + 20 \\ 35 &= 1 \cdot 20 + 15 \\ 20 &= 1 \cdot 15 + 5. \end{aligned}$$

Therefore $\gcd(535, 410) = 5$, the last nonzero remainder. To find the integers m, n, we use the Extended Euclidean Algorithm table:

	1	0
	0	1
1	1	-1
3	-3	4
3	10	-13
1	-13	17
1	23	-30

Therefore $(535)(23) + (410)(-30) = 5$.

C) Assume that a, b, c are integers, $d = \gcd(a, b)$, $a|c$ and $b|c$. Prove that $(ab)|(cd)$.

Solution: By part A above we have $d = ma + nb$ for some integers m, n. Moreover $c = ra$ and $c = sb$ for some integers r, s. Therefore substituting for c in each term and using distributivity, we have

$$cd = c(ma + nb) = mca + mnb = m(sb)a + n(ra)b = ab(ms + nr)$$

It follows that $ab|cd$.

D) An RSA public key cryptographic system has $m = 187$ and encryption exponent $e = 31$. What is the corresponding decryption exponent d?

Solution: $m = 187 = 11 \cdot 17$ so the two primes used to construct the RSA system are $p = 11$ and $q = 17$. Hence $(p-1)(q-1) = 160$, and we need to find $[d]$ with $[31][d] = [1]$ in $\mathbb{Z}_{160}$. We apply the Euclidean Algorithm again:

$$160 = 5 \cdot 31 + 5$$
$$31 = 6 \cdot 5 + 1.$$

Then

$$\begin{array}{ccc} & 1 & 0 \\ & 0 & 1 \\ 5 & 1 & -5 \\ 6 & -6 & 31 \end{array}$$

Therefore $(-6)(160) + (31)(31) = 1$. Hence $d = 31$. (This is another case like the one on the review sheet for the final where $d = e$.)

IV. Prove by mathematical induction: for all real numbers a, b and all $n \geq 1$:

$$\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ na^{n-1}b & a^n \end{pmatrix}.$$

Solution: With $n = 1$, there is nothing to prove. Assume that

$$\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}^k = \begin{pmatrix} a^k & 0 \\ ka^{k-1}b & a^k \end{pmatrix}$$

and compute

$$\begin{aligned} \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}^{k+1} &= \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}^k \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \\ &= \begin{pmatrix} a^k & 0 \\ ka^{k-1}b & a^k \end{pmatrix} \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \\ &= \begin{pmatrix} a^{k+1} & 0 \\ (k+1)a^k b & a^{k+1} \end{pmatrix}, \end{aligned}$$

which is what we wanted to show.

V. Consider the set of all 2×2 matrices with real entries:

$$M_{2\times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\},$$

which is a group under matrix *addition*. Show that

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

is a subgroup of $M_{2\times 2}(\mathbb{R})$.

Solution: In words, H is the set of all 2×2 matrices with zeroes in the first column. H is clearly nonempty since it contains matrices for all choices of $a, b \in \mathbb{R}$ in the second column. Let $A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ and $B = \begin{pmatrix} 0 & a' \\ 0 & b' \end{pmatrix}$ be two arbitrary elements of H. We have

$$A - B = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} - \begin{pmatrix} 0 & a' \\ 0 & b' \end{pmatrix} = \begin{pmatrix} 0 & a - a' \\ 0 & b - b' \end{pmatrix}.$$

Since the matrix $A - B$ also has zeroes in the first column, it belongs to H. Hence by the "shortcut" method (Theorem 3.10), H is a subgroup of $M_{2\times 2}(\mathbb{R})$.

VI. All parts of this question refer to the group $G = \mathbb{Z}_{36}$, in which the operation is addition mod 36.

A) Find all generators for G.

Solution: The generators for G are the $[a]$ with $\gcd(a, 36) = 1$, so the elements of

$$\{[1], [5], [7], [11], [13], [17], [19], [23], [25], [29], [31], [35]\}.$$

B) Find the elements of the cyclic subgroup $\langle [21] \rangle$ in G.

Solution: We have

$$\langle [21] \rangle = \{[0], [21], [6], [27], [12], [33], [18], [3], [24], [9], [30], [15]\}.$$

(This is the same as $\langle [3] \rangle$, since $3 = \gcd(21, 36)$.)

C) Find all elements of G of order 9.

Solution: We want all the $[a]$ for which $\gcd(a, 36) = 4$. These are the classes in

$$\{[4], [8], [16], [20], [28], [32]\}.$$

(These are the multiples of $[4]$ by k such that $\gcd(k, 9) = 1$. The number of them is $\varphi(9) = 6$.)

VII. Let G be a group with operation $*$ and let $a \in G$. Let $\ell_a : G \to G$ be the mapping defined by $\ell_a(x) = a * x$. Show that ℓ_a is always a one-to-one and onto mapping.

Solution: Let $x, y \in G$. If $\ell_a(x) = \ell_a(y)$, then $a * x = a * y$. Since G is a group, though, it contains an inverse for a. We can multiply that on both sides of the equation above (on the left). Then by associativity, $(a^{-1} * a) * x = (a^{-1} * a) * y$, which shows $x = y$. This shows that ℓ_a is one-to-one. Now let $y \in G$ be arbitrary. The equation $y = \ell_a(x) = a * x$ is true for $x = a^{-1} * y$. Therefore ℓ_a is onto.

VIII. Let G and H be groups with identity elements e_G and e_H respectively, and let $\varphi : G \to H$ be a group homomorphism.

A) Show that $\ker(\varphi)$ is a subgroup of G.

Solution: $\ker(\varphi) = \{x \in G \mid \varphi(x) = e_H\}$. We know that this is nonempty, since $\varphi(e_G)\ e_H$. Hence $e_G \in \ker(\varphi)$. Next, let x, y be two arbitrary elements of $\ker(\varphi)$. Since φ is a group homomorphism, we have

$$\begin{aligned}\varphi(x * y^{-1}) &= \varphi(x) * \varphi(y^{-1}) \\ &= \varphi(x) * \varphi(y)^{-1} \\ &= e_H * (e_H)^{-1} \\ &= e_H.\end{aligned}$$

Hence $\ker(\varphi)$ is a subgroup of G by the "shortcut" criterion.

B) Let $c \in H$, and let $a, b \in \varphi^{-1}(\{c\})$, (the inverse image under the mapping φ). Prove that $a *_G b^{-1} \in \ker(\varphi)$.

Solution: By the same reasoning as above, if $\varphi(a) = c = \varphi(b)$,

$$\begin{aligned}\varphi(a *_G b^{-1}) &= \varphi(a) *_H \varphi(b^{-1}) \\ &= \varphi(a) *_H \varphi(b)^{-1} \\ &= c *_H c^{-1} \\ &= e_H.\end{aligned}$$

Therefore $a *_G b^{-1} \in \ker(\varphi)$.

1. C) Let G be a group and let H be a subgroup of G. Define a relation called *congruence modulo* H on G by this rule:

$$x \equiv y \bmod H \Leftrightarrow xy^{-1} \in H.$$

Show that congruence mod H is an equivalence relation.

Solution: Congruence mod H is reflexive since for all $x \in G$, $xx^{-1} = e_G \in H$. If $x \equiv y \bmod H$, then $xy^{-1} \in H$. This implies $(xy^{-1})^{-1} = yx^{-1}$ is in H since H is a subgroup, hence closed under inverses. Therefore $y \equiv x \bmod H$ too, and congruence mod H is symmetric. Finally, if $x \equiv y \bmod H$ and $y \equiv z \bmod H$, then $xy^{-1} \in H$ and $yz^{-1} \in H$. It follows that $(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xz^{-1}$ is in H since H is a subgroup and hence closed under products. Therefore $x \equiv z \bmod H$, and congruence mod H is transitive.

Extra Credit – From the 2012 Putnam Exam: Let $*$ be a commutative and associative binary operation on a set S. Assume that for every $x, y \in S$, there exists some $z \in S$ such that $x * z = y$. (The z may depend on x and y.) Show that if $a, b, c \in S$ and $a * c = b * c$, then $a = b$.

Solution: Letting $x = a * c = b * c$ and $y = a$, the given information says there exists some $w \in S$ such that

$$(a * c) * w = a = (b * c) * w. \tag{1}$$

Similarly, with $x = b * c = a * c$ and $y = b$, there exists some $u \in S$ such that

$$(b * c) * u = b = (a * c) * u. \tag{2}$$

By associativity and commutativity, and using (2) and then (1),

$$(a * c) * w * c * u = ((a * c) * u) * (c * w) = b * (c * w) = (b * c) * w = a.$$

But on the other hand using (1) and then (2),

$$(a * c) * w * c * u = (b * c) * w * c * u = ((b * c) * w) * (c * u) = a * (c * u) = (a * c) * u = b.$$

Therefore $a = b$. (There are many other correct ways to solve this one as well. This is just the first proof I found as I was thinking about the problem! For instance, you can "cook up" an identity element and inverses from the given information. However, you cannot use things like the existence of inverses without *proving* that they exist.)