Mathematics 243, section 1 – Algebraic Structures
Final Examination – December 13, 2006

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

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

A) (10) Is ψ a permutation of $\mathbf{Z}$? Prove your assertion.

Solution : Yes ψ is a permutation, or one-to-one (injective) and onto (surjective) mapping from $\mathbf{Z}$ to itself. Suppose that $\psi(x) = \psi(x')$. Then x and x' must be either both even or both odd, since ψ maps odd integers to even integers, and even integers to odd integers. If x, x' are both even, then $x - 1 = x' - 1$. Adding 1 to both sides yields $x = x'$. Similarly, if x, x' are both odd, then $x + 1 = x' + 1$. Subtracting 1 from both sides shows $x = x'$ in this case too. Hence ψ is injective. ψ is also surjective since if y is even, then $y = \psi(x)$ for the odd number $x = y - 1$. Moreover if y is odd, then $y = \psi(x)$ for the even number $x = y + 1$.

B) (10) What is the mapping $\varphi \circ \psi$?

Solution :
$$(\varphi \circ \psi)(x) = \begin{cases} 1 & \text{if } x \text{ is odd} \\ 3x - 3 & \text{if } x \text{ is even} \end{cases}$$

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 $C + D = (C \cup D) - (C \cap D)$. For instance, $\{1\} + \{1, 2\} = \{1, 2\} - \{1\} = \{2\}$.

A) (15) Compute the rest of the operation table for $+$ on $\mathcal{P}$.

Solution : The complete operation table looks like this:

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

B) (5) Is there an identity element for $+$ in $\mathcal{P}$. If so, what is the identity element?

Solution : Yes. $E = \emptyset$ acts as an identity element here. (Note: In fact from the table above, we can see that $\mathcal{P}$ is even a *group* of order 4 under this operation!)

III. (10) Prove by contradiction: if $A = \{a_1, \ldots, a_n\}$ is a *finite* set and $\varphi : A \to A$ is surjective then φ is also injective.

Solution : Suppose φ is not injective. Then there are two distinct elements of A, say a_i and a_j that satisfy $\varphi(a_i) = \varphi(a_j)$. But then there can be at most $n-1$ distinct elements in the image of φ, so that φ is not onto. This contradiction shows that φ must be surjective.

IV.

A) (5) Let a, b be two integers, at least one of which is nonzero. Give the definition of a gcd of a, b.

Solution : d is a gcd of a, b if $d > 0$, $d|a$ and $d|b$, and if $c|a$ and $c|b$, then $c|d$.

B) (15) Find the integer $d = \gcd(537, 411)$ and express d in the form $d = 537r + 411s$ for some integers r, s.

Solution : Applying the Euclidean algorithm:

$$\begin{aligned}
537 &= 1 \cdot 411 + 126 \\
411 &= 3 \cdot 126 + 33 \\
126 &= 3 \cdot 33 + 27 \\
33 &= 1 \cdot 27 + 6 \\
27 &= 4 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0
\end{aligned}$$

Hence $\gcd(537, 411) = 3$. To find the integers r, s:

	1	0
	0	1
1	1	−1
3	−3	4
3	10	−13
1	−13	17
4	62	−81

This shows $62 \cdot 537 + (-81) \cdot 411 = 3$.

C) (15) Assume that a, b, c are integers, $d = \gcd(a, b)$, $a|c$ and $b|c$. Prove that $ab|cd$.

Solution : Since $d = \gcd(a, b)$, as in part C, there are integers r, s such that $d = ar + bs$, hence $cd = car + cbs$. Since $a|c$, there is an integer q such that $c = qa$, and similarly there is an integer p such that $c = pb$. Substitute as follows:

$$\begin{aligned} cd &= car + cbs \\ &= (pb)ar + qa(bs) \\ &= ab(pr + qs) \end{aligned}$$

Since p, r, s, q are all integers, so is $pr + qs$, and this shows $ab|cd$.

D) (20) An RSA public key cryptographic system has $m = 209$ and encryption exponent $e = 37$. What is the corresponding decryption exponent d?

Solution : Since $209 = 19 \cdot 11$, we want to find d such that $37d \equiv 1 \bmod (19 - 1)(11 - 1) = 180$. Since $\gcd(37, 180) = 1$, such a d exists and we can find it by the same process as in part C:

$$\begin{aligned} 180 &= 4 \cdot 37 + 32 \\ 37 &= 1 \cdot 32 + 5 \\ 32 &= 6 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Then

	1	0
	0	1
4	1	−4
1	−1	5
6	7	−34
2	−15	73

Hence $(-15) \cdot 180 + 73 \cdot 37 = 1$. This says $d = 73$.

V. (20) Prove by mathematical induction: for all real numbers a, b and all $n \geq 1$:

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

Solution : The statement is clear in the base case $n = 1$. So assume that

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

Then

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

which is what we wanted to show.

VI. (20) Consider the set of all 2×2 matrices with real entries:

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

Show that $M_{2\times 2}(\mathbf{R})$ is a group under matrix *addition*:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}.$$

Solution : G is closed under sums since from the above, if a, b, c, d, e, f, g, h in $\mathbf{R}$, then the sum matrix is also an element of $M_{2\times 2}(\mathbf{R})$. Matrix sums are associative since if $A = (a_{ij}), B = (b_{ij})$ and $C = (c_{ij})$, then the entry in row i and column j in the sum $(A+B)+C$ is $(a_{ij}+b_{ij})+c_{ij} = a_{ij}+(b_{ij}+c_{ij})$, using the associativity of $+$ in $\mathbf{R}$. Hence $(A+B)+C = A+(B+C)$. The zero matrix $Z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is an identity element for matrix sums. Finally if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in G, then the additive inverse of A is $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$.

VII. All parts of this question refer to the group $G = \mathbf{Z}_{27}$, in which the operation is addition mod 27.

A) (5) Find all generators for G.

Solution : The generators are the classes $[x]$ with $\gcd(x, 27) = 1$, so

$$[x] = [1], [2], [4], [5], [7], [8], [10], [11], [13], [14], [16], [17], [19], [20], [22], [23], [25], [26]$$

B) (5) Find the elements of the cyclic subgroup $\langle [21] \rangle$ in G.

Solution : By our general theorems on subgroups of cyclic groups, this is the same subgroup as $\langle [3] \rangle$ since $\gcd(21, 27) = 3$. Hence

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

C) (5) Find all elements of G of order 9.

Solution : These are the same as the generators of $\langle [3] \rangle = \langle [21] \rangle$ from part B:

$$[3], [6], [12], [15], [21], [24].$$

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

Solution : Write K for $\ker(\varphi)$. $K \neq \emptyset$ because we know $\varphi(e_G) = e_H$, so $e_G \in K$. If $x, y \in K$, then since φ is a group homomorphism $\varphi(xy) = \varphi(x)\varphi(y) = e_H e_H = e_H$. Hence $xy \in K$ so K is closed under products. Finally, let $x \in K$ and recall that since φ is a group homomorphism $\varphi(x^{-1}) = (\varphi(x))^{-1}$ for all $x \in G$. If $x \in K$, then this says $\varphi(x^{-1}) = (e_H)^{-1} = e_H$. Hence K is closed under inverses too, and K is a subgroup of G.

B) (5) Let $c \in H$, and let $a, b \in \varphi^{-1}(\{c\})$, (the inverse image under the mapping φ). Prove that $ab^{-1} \in \ker(\varphi)$.

Solution : From the given information, $\varphi(a) = \varphi(b) = c$. Hence by the group homomorphism properties.

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)(\varphi(b))^{-1} = cc^{-1} = e_H$$

Hence by definition, $ab^{-1} \in K = \ker(\varphi)$.

C) (5) Prove that φ is injective if and only if $\ker(\varphi) = \{e_G\}$.

Solution : If φ is injective, there is only one element that maps to e_H, namely e_G. Hence $K = \ker(\varphi) = \{e_G\}$ (and nothing else). Conversely, if $K = \ker(\varphi) = \{e_G\}$ and $\varphi(a) = \varphi(b)$ for $a, b \in G$, then reasoning as in part B, but "working backwards"

$$e_H = \varphi(a)(\varphi(b))^{-1} = \varphi(ab^{-1})$$

Hence $ab^{-1} \in K = \{e_G\}$. This implies $ab^{-1} = e_G$ so $a = b$. It follows that φ is injective.

IX. (10) Let G be a group, and let $x, y \in G$. The conjugacy relation R on G is defined as follows. We say x and y are *conjugate* in G, xRy, if there exists an $a \in G$ such that $y = axa^{-1}$. Show that the conjugacy relation is an equivalence relation on G.

Solution : R is reflexive: We have $x = exe^{-1}$, so xRx for all $x \in G$ (take $a = e$ in the definition).

R is symmetric: If xRy, then $y = axa^{-1}$ for some $a \in G$. But then $x = a^{-1}ya = byb^{-1}$ if we write $b = a^{-1}$. Hence yRx.

R is transitive: If xRy and yRz, then $y = axa^{-1}$ and $z = byb^{-1}$ for some $a, b \in G$ (not necessarily the same). Then if we substitute for y in the second equation,

$$z = b(axa^{-1})b^{-1} = (ba)x(a^{-1}b^{-1}) = (ba)x(ba)^{-1}$$

(reverse order law for inverses). This shows yRz.