

Solution to Project #1

Math 312-A

Due Tuesday, March 6, 2007

As we fill our table with elements from $\{e, a, b, c\}$, we will force closure on the operation.

Since e is the identity, our multiplication table begins as

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | | | |
| b | b | | | |
| c | c | | | |

We automatically have the identity for our group by doing so.

As we ensure that there are no duplicates in any row or column, we ensure that each row and column contains the identity e . This means that every element has an inverse.

Since we can't have a duplicate in the second row, we have three possible values for aa : e , b , or c .

1. $aa = e$: then the multiplication table becomes

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | | |
| b | b | | | |
| c | c | | | |

Since we can't have duplicates in the second row, ab can't be a or e . Since we can't have duplicates in the third column, ab can't be b . That leaves $ab = c$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | |
| b | b | | | |
| c | c | | | |

Since we can't have duplicates in the second row, $ac = b$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | | | |
| c | c | | | |

Since we can't have duplicates in the third row, ba can't be b . Since we can't have duplicates in the second column, ba can't be a or e . Therefore $ba = c$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | | |
| c | c | | | |

Since we can't have duplicates in the second column, $ca = b$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | | |
| c | c | b | | |

We now have two choices for bb : either $bb = e$ or $bb = a$.

(a) $bb = e$:

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | |
| c | c | b | | |

To avoid duplicates in the third row, we have $bc = a$:

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | | |

To avoid duplicates in the last two columns, we have that $cb = a$ and $cc = e$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

Note that this operation is commutative, and that $c = ab$. Thus every element can be written in the form $a^i b^j$:

$$\begin{aligned}
 e &= a^0 b^0 \\
 a &= a^1 b^0 \\
 b &= a^0 b^1 \\
 c &= a^1 b^1
 \end{aligned}$$

Since the operation is commutative, $(a^i b^j)(a^k b^l) = a^{i+k} b^{j+l}$. This guarantees that we have associativity, since $((a^i b^j)(a^k b^l))(a^m b^n) = a^{i+k+m} b^{j+l+n} = (a^i b^j)((a^k b^l)(a^m b^n))$.

(b) $bb = a$:

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | a | |
| c | c | b | | |

As before, this forces $bc = e$, and then $cb = e$ and $cc = a$:

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | a | e |
| c | c | b | e | a |

Note that $a = b^2$ and $c = ab = b^3$. Therefore $G = \{e, a, b, c\} = \{e, b, a, c\} = \{b^0, b^1, b^2, b^3\}$, we have associativity because $b^i(b^j b^k) = b^{i+j+k} = (b^i b^j)b^k$, and this is a cyclic group of order four.

2. $aa = b$:

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | b | | |
| b | b | | | |
| c | c | | | |

Since the second row can't have duplicates, ac can't be a or b . Since the fourth column can't have duplicates, ac can't be c . Therefore $ac = e$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | b | | e |
| b | b | | | |
| c | c | | | |

Since there can't be any duplicates in the second row, $ab = c$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | | | |
| c | c | | | |

Since there can't be any duplicates in the third row, bc can't be b . Since there can't be any duplicates in the fourth column, bc can't be c or e . Therefore $bc = a$.

| | | | | |
|-----|-----|-----|-----|-----|
| | e | a | b | c |
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | | | a |
| c | c | | | |

Since there can't be any duplicates in the third row, bb can't be b or a . Since there can't be any duplicates in the third column, bb can't be c . Therefore $bb = e$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>b</i> | <i>c</i> | <i>e</i> |
| <i>b</i> | <i>b</i> | | <i>e</i> | <i>a</i> |
| <i>c</i> | <i>c</i> | | | |

Since there can't be any duplicates in the third row, $ba = c$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>b</i> | <i>c</i> | <i>e</i> |
| <i>b</i> | <i>b</i> | <i>c</i> | <i>e</i> | <i>a</i> |
| <i>c</i> | <i>c</i> | | | |

Since there can't be any duplicates in the columns, $ca = e$, $cb = a$, and $cc = b$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>b</i> | <i>c</i> | <i>e</i> |
| <i>b</i> | <i>b</i> | <i>c</i> | <i>e</i> | <i>a</i> |
| <i>c</i> | <i>c</i> | <i>e</i> | <i>a</i> | <i>b</i> |

Note that $b = a^2$ and $c = ab = a^3$, and again we get associativity because $(a^i a^j) a^k = a^{i+j+k} = a^i (a^j a^k)$, and we have a cyclic group of size four: $G = \{e, a, b, c\} = \{a^0, a^1, a^2, a^3\}$.

3. $aa = c$:

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>c</i> | | |
| <i>b</i> | <i>b</i> | | | |
| <i>c</i> | <i>c</i> | | | |

Since we can't have duplicates in the second row, ab can't be a or c . Since we can't have duplicates in the third column, ab can't be b . Therefore $ab = e$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>c</i> | <i>e</i> | |
| <i>b</i> | <i>b</i> | | | |
| <i>c</i> | <i>c</i> | | | |

Since we can't have duplicates in the second row, $ac = b$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>c</i> | <i>e</i> | <i>b</i> |
| <i>b</i> | <i>b</i> | | | |
| <i>c</i> | <i>c</i> | | | |

Since we can't have duplicates in the third row, ba can't be b . Since we can't have duplicates in the second column, ba can't be a or c . Therefore $ba = e$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>c</i> | <i>e</i> | <i>b</i> |
| <i>b</i> | <i>b</i> | <i>e</i> | | |
| <i>c</i> | <i>c</i> | | | |

Since we can't have duplicates in the third row, bc can't be b or e . Since we can't have duplicates in the fourth column, bc can't be c . Therefore $bc = a$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>c</i> | <i>e</i> | <i>b</i> |
| <i>b</i> | <i>b</i> | <i>e</i> | | <i>a</i> |
| <i>c</i> | <i>c</i> | | | |

Since we can't have duplicates in the third row, $bb = c$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>c</i> | <i>e</i> | <i>b</i> |
| <i>b</i> | <i>b</i> | <i>e</i> | <i>c</i> | <i>a</i> |
| <i>c</i> | <i>c</i> | | | |

Since we can't have duplicates in the second, third, and fourth columns, $ca = b$, $cb = a$, and $cc = e$.

| | | | | |
|----------|----------|----------|----------|----------|
| | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>e</i> | <i>e</i> | <i>a</i> | <i>b</i> | <i>c</i> |
| <i>a</i> | <i>a</i> | <i>c</i> | <i>e</i> | <i>b</i> |
| <i>b</i> | <i>b</i> | <i>e</i> | <i>c</i> | <i>a</i> |
| <i>c</i> | <i>c</i> | <i>b</i> | <i>a</i> | <i>e</i> |

Note that $c = a^2$ and that $b = ca = a^3$. We get associativity as before, and $G = \{e, a, b, c\} = \{e, a, c, b\} = \{a^0, a^1, a^2, a^3\}$ is a cyclic group of order 4.