Math 416 – Introduction to Abstract Algebra

Chapter 2 – Groups

From last time:

A group is a set G with an operation ° such that

1) the operation ° is closed on G
   that is, if a and b are in G, then so is a ° b
2) the operation ° is associative
   that is, (a ° b) ° c = a ° (b ° c)
3) there is an identity element in G. Call it e
   that is, e ° a = a ° e = a, for every a in G
4) every element a in G has an inverse, call it a⁻¹, such that a ° a⁻¹ = e ° a⁻¹ = e

A group does not have to be commutative (we call it “abelian”). If it is, then it means

5) a ° b = b ° a

9/13 – HW #1 due: Ch 1, p. 37 # 2, 3, 12, 13, 16, 20, 22
9/18 – HW #2 due: Ch 2, p. 53 # 1, 2, 3, 6, 7, 13, 16, 22, 25, 26
Online Quiz Zero – technical problems continue

Review of modular arithmetic (see “Modular arithmetic) pages 8-14)

addition and additive inverses

a = b mod n means n | (a – b)

equivalence (mod n)

Division algorithm

given a and b, to find q and r with
a) a = bq + r, and
b) 0 ≤ r < b

Euclidean algorithm: to find GCD(a, b)

example: GCD(147,357) = 21

relation between a⁻¹ (mod n), formula ax = 1 mod n and formula ax + ny = 1

requirement that a and n be relatively prime
How to solve \( ax + ny = 1 \) (see theorems 0.1 and 0.2, pages 4-7)

**Example:** find \( 4^{-1} \pmod{7} \)

\[
4x = 1 \pmod{7} \\
7 \mid 4x - 1 \\
4x - 1 = 7y \\
4x - 7y = 1 \\
\text{[ } x = 2, y = 1 \text{ or } x = 9, y = 5, \text{ or } ... \text{ ]}
\]

\[
a = 7, \ b = 4 \\
7 = 1*4 + 3, \ p = 1, \ q \ [= c] = 3 \\
b = 4, \ c = 3 \\
4 = 1*3 + 1, \ p = 1, \ q \ [= d] = 1
\]

Now, do it backwards

\[
1 = 4 - 1*3 \\
3 = 7 - 1*4 \\
1 = 4 - 1*(7 - 1*4) \\
= 4 - 1*7 + 1*4 \\
= 4*2 - 7*1
\]

So \( 4*2 - 1 = 7*1 \)

And \( 7 \mid 4*2 - 1 \)

And \( 4*2 = 1 \pmod{7} \)

So \( 4^{-1} = 2 \pmod{7} \) *(Also, use Gallian software ch 2 #1)*

Cayley table for multiplication mod 7

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

How to read inverses off the Cayley table

Make a Cayley table for multiplication mod 10

Entries are numbers less than 10 relatively prime to 10,

\( 1, 3, 7, 9 \)

Name of group is \( U_{10} \), the *Group of units.*

Theorem 2.1: Uniqueness of the identity: In a group \( G \), there is only one identity element.

Proof strategy: Typical of uniqueness proofs: suppose there are two, and derive a contradiction, in this case, that the two things are equal.

Fact review: if \( e \) is an identity, and \( a \) is any element, then \( ea = a \) and \( ae = e \).
Proof: Suppose that $e'$ and $e''$ are both identities.

Since $e'$ is an identity, $e'e'' = e''$
Since $e''$ is an identity, $e'e'' = e'$.

By transitivity, $e' = e''$, and there weren’t really two different identities.

QED

Theorem 2.2: cancellation: In a group, $G$, both left and right cancellation laws hold.

That is,

if $ba = ca$, then $b = c$ (right cancellation), and
if $ab = ac$, then $b = c$ (left cancellation)

Proof plan: direct deduction. Suppose they hypothesis, and deduce the consequences

Proof: (of left cancellation only. Right cancellation is very similar)

suppose $ab = ac$.

a has an inverse, call it $a'$. Then $a'(ab) = a'(ac)$ multiplying both sides on the left by $a'$

$(a'a)b = (a'a)c$ associative law

$eb = ec$ property of inverses

$b = c$ property of identities

QED

Theorem 2.3: uniqueness of inverses: An element $a$ has only one inverse.

Proof plan: suppose there were two, and show they are the same.

Proof: Suppose $a'$ and $a''$ were both inverses of $a$.

Then $aa' = e$ and $aa'' = e$ (properties of inverses)
so $aa' = aa''$ transitivity
so $a' = a''$ left cancellation

and the two inverses are in fact equal.

QED

Theorem 2.4: The inverse of $ab$ is $b'a'$ (not necessarily $a'b'$)

Proof: (direct) $(ab)(b'a') = a(bb')a' = aea' = aa' = e$

so $b'a'$ is an inverse of $ab$ (property of inverses)

so $b'a'$ is the inverse of $ab$ Theorem 2.3

QED

remark on the use of $^{-1}$ as an inverse notation in “multiplicative” groups and multiples in additive groups.