

Math 416 – Introduction to Abstract Algebra

Chapter 2 – Groups

From last time:

A group is a set G with an operation \circ such that

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

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

5) $a \circ b = b \circ a$

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

$$a = b \pmod n \text{ means } n \mid (a - b)$$

equivalence (mod n)

Division algorithm

given a and b , to find q and r with

a) $a = bq + r$, and

b) $0 \leq r < b$

Euclidean algorithm: to find $\text{GCD}(a, b)$

example: $\text{GCD}(147, 357) = 21$

relation between $a^{-1} \pmod n$, formula $ax = 1 \pmod n$ 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 $4^{-1} \pmod{7}$

$$4x = 1 \pmod{7}$$

$$7 \mid 4x - 1$$

$$4x - 1 = 7y$$

$$4x - 7y = 1$$

$$[x = 2, y = 1 \text{ or } x = 9, y = 5, \text{ or } \dots]$$

$$a = 7, b = 4$$

$$7 = 1 \cdot 4 + 3, p = 1, q [= c] = 3$$

$$b = 4, c = 3$$

$$4 = 1 \cdot 3 + 1, p = 1, q [= d] = 1$$

now, do it backwards

$$1 = 4 - 1 \cdot 3$$

$$3 = 7 - 1 \cdot 4$$

$$1 = 4 - 1 \cdot (7 - 1 \cdot 4)$$

$$= 4 - 1 \cdot 7 + 1 \cdot 4$$

$$= 4 \cdot 2 - 7 \cdot 1$$

$$\text{so } 4 \cdot 2 - 1 = 7 \cdot 1$$

$$\text{and } 7 \mid 4 \cdot 2 - 1$$

$$\text{and } 4 \cdot 2 = 1 \pmod{7}$$

$$\text{so } 4^{-1} = 2 \pmod{7}$$

(Also, use Gallian software ch 2 #1)

Cayley table for multiplication mod 7

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

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.