

# Introduction to Groups32

## A group theory calculator

Prof John J Wavrik  
Dept of Mathematics  
Univ of Calif – San Diego

Groups32 contains the tables for the groups of orders 1-32 (there are 144 of them).

|          | <u>A</u> | <u>B</u> | <u>C</u> |
|----------|----------|----------|----------|
| <b>A</b> | <b>A</b> | <b>B</b> | <b>C</b> |
| <b>B</b> | <b>B</b> | <b>C</b> | <b>A</b> |
| <b>C</b> | <b>C</b> | <b>A</b> | <b>B</b> |

It uses the tables to calculate information about these groups. It uses essentially the same methods that you would use by hand – but a computer is much faster than a human at doing this type of computation.

# How much faster than you is a laptop computer?

Let's find out. Here is a routine task:

Check this table for associativity -- time yourself!

|          | <u>A</u> | <u>B</u> | <u>C</u> |
|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        |
| <b>B</b> | B        | C        | A        |
| <b>C</b> | C        | A        | B        |

The computer checks the table so quickly that the only way to get an accurate time is to repeat the computation.

|               |                            |
|---------------|----------------------------|
| 10000 assocx  | Elapsed time: 00:00:00.880 |
| 100000 assocx | Elapsed time: 00:00:08.460 |

|          | <u>A</u> | <u>B</u> | <u>C</u> |
|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        |
| <b>B</b> | B        | C        | A        |
| <b>C</b> | C        | A        | B        |

The computer can do a 3 x 3 table 10,000 times in roughly 1 second.

1. How many seconds would it take you to do this?
2. How long would it take the computer to do a 6 x 6 table 10000 times? (2 seconds is **not** the correct answer)
3. How long would it take you to check a 32 x 32 table for associativity?

- ✓ Computer Speed
- ✓ Group Tables
- ✓ Introduce Groups<sup>32</sup>

**table 1**

|          | <b>A</b> | <b>B</b> | <b>C</b> | <b>D</b> |
|----------|----------|----------|----------|----------|
| <b>A</b> | <b>A</b> | <b>B</b> | <b>C</b> | <b>D</b> |
| <b>B</b> | <b>B</b> | <b>C</b> | <b>D</b> | <b>A</b> |
| <b>C</b> | <b>C</b> | <b>D</b> | <b>A</b> | <b>B</b> |
| <b>D</b> | <b>D</b> | <b>A</b> | <b>B</b> | <b>C</b> |

This is the “multiplication” table for a group having 4 elements. By inspection we see that A is the identity. A and C are their own inverses. B and D are the inverses of each other. (The fact that the group operation is associative cannot be easily seen by inspection.)

**table 1**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <u>A</u> | A        | B        | C        | D        |
| <u>B</u> | B        | C        | D        | A        |
| <u>C</u> | C        | D        | A        | B        |
| <u>D</u> | D        | A        | B        | C        |

**Z mod 4 (+)**

|          | <u>0</u> | <u>1</u> | <u>2</u> | <u>3</u> |
|----------|----------|----------|----------|----------|
| <u>0</u> | 0        | 1        | 2        | 3        |
| <u>1</u> | 1        | 2        | 3        | 0        |
| <u>2</u> | 2        | 3        | 0        | 1        |
| <u>3</u> | 3        | 0        | 1        | 2        |

Compare with the table for addition of integers mod 4. These are essentially the same. If we substitute 0 for A, 1 for B, etc. the table on the left becomes the table on the right.

table 1

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|---|----------|----------|----------|----------|
| A | A        | B        | C        | D        |
| B | B        | C        | D        | A        |
| C | C        | D        | A        | B        |
| D | D        | A        | B        | C        |

table 2

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|---|----------|----------|----------|----------|
| A | A        | B        | C        | D        |
| B | B        | A        | D        | C        |
| C | C        | D        | A        | B        |
| D | D        | C        | B        | A        |

table 3

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|---|----------|----------|----------|----------|
| A | A        | B        | C        | D        |
| B | B        | A        | D        | C        |
| C | C        | D        | B        | A        |
| D | D        | C        | A        | B        |

One of these things  
is not like the others

(but two of these things are kinda the same)

**table 1**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | C        | D        | A        |
| <b>C</b> | C        | D        | A        | B        |
| <b>D</b> | D        | A        | B        | C        |

**table 2**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | A        | D        | C        |
| <b>C</b> | C        | D        | A        | B        |
| <b>D</b> | D        | C        | B        | A        |

**table 3**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | A        | D        | C        |
| <b>C</b> | C        | D        | B        | A        |
| <b>D</b> | D        | C        | A        | B        |

If you think that table 1 and table 3 are like each other, you are right!

Replace B by C and C by B in table 1.

Then rearrange the rows and columns.

You will get table 3.

**table 1**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | C        | D        | A        |
| <b>C</b> | C        | D        | A        | B        |
| <b>D</b> | D        | A        | B        | C        |

**table 2**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | A        | D        | C        |
| <b>C</b> | C        | D        | A        | B        |
| <b>D</b> | D        | C        | B        | A        |

**table 3**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | A        | D        | C        |
| <b>C</b> | C        | D        | B        | A        |
| <b>D</b> | D        | C        | A        | B        |

Table 1 and table 3 can be obtained from one another by changing the names of the elements.

In group theory we regard two tables as giving the same group if they can be obtained from each other by renaming the elements.

**table 1**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | C        | D        | A        |
| <b>C</b> | C        | D        | A        | B        |
| <b>D</b> | D        | A        | B        | C        |

**table 2**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | A        | D        | C        |
| <b>C</b> | C        | D        | A        | B        |
| <b>D</b> | D        | C        | B        | A        |

**table 3**

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        |
| <b>B</b> | B        | A        | D        | C        |
| <b>C</b> | C        | D        | B        | A        |
| <b>D</b> | D        | C        | A        | B        |

How can you see that Table 2 cannot be obtained from Table 1 by renaming the elements?

# An Early Theorem

## **Theorem:**

In the table for a group, every element appears exactly once in each row and in each column.

Prove this theorem

I was once asked if this condition is enough:

Suppose that we have a table in which one element is the identity and in which every element appears exactly once in each row and each column. Must this be the table of a group?

The only thing that can fail is associativity.

The answer is NO – and here is an example:

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> | <u>E</u> |
|----------|----------|----------|----------|----------|----------|
| <b>A</b> | A        | B        | C        | D        | E        |
| <b>B</b> | B        | A        | D        | E        | C        |
| <b>C</b> | C        | D        | E        | B        | A        |
| <b>D</b> | D        | E        | A        | C        | B        |
| <b>E</b> | E        | C        | B        | A        | D        |

We check that this operation is not associative

|          | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> | <u>E</u> |
|----------|----------|----------|----------|----------|----------|
| <u>A</u> | A        | B        | C        | D        | E        |
| <u>B</u> | B        | A        | D        | E        | C        |
| <u>C</u> | C        | D        | E        | B        | A        |
| <u>D</u> | D        | E        | A        | C        | B        |
| <u>E</u> | E        | C        | B        | A        | D        |

(BB)C

B(BC)

( )C

B( )



|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> | <u>E</u> |
|---|----------|----------|----------|----------|----------|
| A | A        | B        | C        | D        | E        |
| B | B        | A        | D        | E        | C        |
| C | C        | D        | E        | B        | A        |
| D | D        | E        | A        | C        | B        |
| E | E        | C        | B        | A        | D        |

(BB)C

B(BC)

(A)C

B( )

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> | <u>E</u> |
|---|----------|----------|----------|----------|----------|
| A | A        | B        | C        | D        | E        |
| B | B        | A        | D        | E        | C        |
| C | C        | D        | E        | B        | A        |
| D | D        | E        | A        | C        | B        |
| E | E        | C        | B        | A        | D        |

(BB)C

B(BC)

(A)C

B(D)

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> | <u>E</u> |
|---|----------|----------|----------|----------|----------|
| A | A        | B        | C        | D        | E        |
| B | B        | A        | D        | E        | C        |
| C | C        | D        | E        | B        | A        |
| D | D        | E        | A        | C        | B        |
| E | E        | C        | B        | A        | D        |

(BB)C

B(BC)

(A)C

B(D)

C

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> | <u>E</u> |
|---|----------|----------|----------|----------|----------|
| A | A        | B        | C        | D        | E        |
| B | B        | A        | D        | E        | C        |
| C | C        | D        | E        | B        | A        |
| D | D        | E        | A        | C        | B        |
| E | E        | C        | B        | A        | D        |

(BB)C

B(BC)

(A)C

B(D)

C

E

- ✓ Computer Speed
- ✓ Group Tables
- ✓ Introduce Groups<sub>32</sub>

Groups32 uses an internal set of tables for the groups of orders 1-32 and offers a collection of commands

## Here are the Commands

|        |             |           |             |
|--------|-------------|-----------|-------------|
| CENTER | CENTRALIZER | CHART     | CONJ-CLS    |
| COSETS | EVALUATE    | EXAMPLES  | GENERATE    |
| GROUP  | HELP        | INFO      | ISOMORPHISM |
| LEFT   | NORMALIZER  | ORDERS    | PERMGRPS    |
| POWERS | QUIT        | RESULT    | RIGHT       |
| SEARCH | STOP        | SUBGROUPS | TABLE       |
| X      |             |           |             |

To apply a command, you start typing letters. Once you have typed enough letters to distinguish the command from others, Groups32 will automatically complete the command and ask you to put in numbers or letters as needed.

### **Example:**

The CHART command will list groups of various orders. There are other commands that begin with the letter "C" but this is the only one which begins with "CH". Once you type "C" and "H" the command is completed for you.

G1>> CH

You type in the letters C and H

(your input is shown in red)

G1>> CHART      Order of Groups (1-32 or 0) Number

Groups32 completes the CHART command for you.

It then informs you that you can put in a number from 1-32 if you want to see a list of groups of a specific order, or put in the number 0 if you want a listing of all groups.

```
G1>> CHART    Order of Groups (1-32 or 0) Number 8
      10     11     12     13*    14*
      There are 5 Groups of order 8
      3 abelian and 2 non-abelian
```

If you put in the number 8, the program shows you that there are a total of 5 groups of order 8. The groups numbered 10, 11 and 12 are abelian (commutative) while those numbered 13 and 14 are non-abelian.

# Helpful Hints

- Type `H` (for Help) at any time and you will get the list of commands.
- Type `INFO` or `X` and then a command and you will get information about that command (the command will not execute).

G1>> HELP

CENTER

CENTRALIZER

CHART

CONJ-CLS

COSETS

EVALUATE

EXAMPLES

GENERATE

GROUP

HELP

INFO

ISOMORPHISM

LEFT

NORMALIZER

ORDERS

PERMGRPS

POWERS

QUIT

RESULT

RIGHT

SEARCH

STOP

SUBGROUPS

TABLE

X

G1>> X

This will provide information about the next command you use. INFO and X do the same thing but X is quicker to use.

G1>> CHART

This prints a chart of all groups of a given order.

The groups are numbered 1 to 144 and are grouped by order. An asterisk indicates that the group is not abelian.

Input of 0 for the order gives all groups.

# A Short Sample Session

A separate "Sample Session" file goes through many of the commands in Groups32. You should go through this file while running Groups32 and try things for yourself.

However - here is a quick sample

```
G1>> CHART    Order of Groups (1-32 or 0) Number 4
      4      5
      There are 2 Groups of order 4
      2 abelian and 0 non-abelian
```

There are two essentially different tables for groups of order 4. Both represent abelian groups. The groups are number 4 and number 5.

G1>> TABLE for Group Number 4

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|---|----------|----------|----------|----------|
| A | A        | B        | C        | D        |
| B | B        | C        | D        | A        |
| C | C        | D        | A        | B        |
| D | D        | A        | B        | C        |

G4>> TABLE for Group Number 5

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|---|----------|----------|----------|----------|
| A | A        | B        | C        | D        |
| B | B        | A        | D        | C        |
| C | C        | D        | A        | B        |
| D | D        | C        | B        | A        |

Table 4

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|---|----------|----------|----------|----------|
| A | A        | B        | C        | D        |
| B | B        | C        | D        | A        |
| C | C        | D        | A        | B        |
| D | D        | A        | B        | C        |

Table 5

|   | <u>A</u> | <u>B</u> | <u>C</u> | <u>D</u> |
|---|----------|----------|----------|----------|
| A | A        | B        | C        | D        |
| B | B        | A        | D        | C        |
| C | C        | D        | A        | B        |
| D | D        | C        | B        | A        |

We have seen these tables before and noted that they are essentially different.

```
G5>> ORDERS    for Group Number 4
```

```
Group number 4 of Order 4
```

```
1 elements of order 1:    A
```

```
1 elements of order 2:    C
```

```
2 elements of order 4:    B D
```

```
G4>> ORDERS    for Group Number 5
```

```
Group number 5 of Order 4
```

```
1 elements of order 1:    A
```

```
3 elements of order 2:    B C D
```

```
0 elements of order 4:
```

Notice that the number of elements of various orders are different. Thus the tables cannot be obtained from each other by renaming the elements.

## **Theorem:**

If two groups are isomorphic (i.e. they give the same table if the elements are suitably named) then they must have the same number of elements of each order.

## Question:

Is the converse true? If two groups have the same number of elements of each order, must the groups be isomorphic?

# Conclusion

The commands in Groups32 cover topics that occur in most introductory courses in abstract algebra – but not, of course at the beginning. Once you have learned about some of these topics, it should be easy to discover how to use Groups32 to do computations.

I should note that the original version of Groups32 is programmable, there are more advanced commands that can be loaded in, and the user can also write commands which can be added to the system.