Math 3230 Abstract Algebra I
Section 1.5 Definition of a Group

Slides created by M. Macauley, Clemson (Modified by E. Gunawan, UConn)

`http://egunawan.github.io/algebra`

Abstract Algebra I

The formal definition of a group (Binary operations)

An operation is a method for combining objects. For example, $+$, $-$, $\cdot$, and $\div$. In fact, these are binary operations because they combine two objects into a single object.

Definition

If $*$ is a binary operation on a set S, then $s * t \in S$ for all $s, t \in S$. In this case, we say that S is closed under the operation $*$.

Remarks:

- Combining two group elements (i.e., doing one action followed by the other) is a binary operation. We say that it is a binary operation *on* the group.
- Recall that Rule 4 (from the first lecture) says that any sequence of actions is an action. This ensures that the group is closed under the binary operation.
- Note: Multiplication tables depict the group's binary operation in full.
- Warning: Not every table with symbols in it is going to be the multiplication table for a group.

The formal definition of a group (Associativity)

An operation is called associative if parentheses are permitted anywhere, but required nowhere.

- For example, ordinary addition and multiplication on multiplications are associative.
- However, subtraction of integers is *not* associative:

$$4 - (1 - 2) \neq (4 - 1) - 2.$$

Example

- Give a set and an associative binary operation.
- Give a set and a non-associative binary operation.

The formal definition of a group (Associativity)

Question: Is the operation of combining actions in a group associative?

Recall D_3, the group of symmetries for the equilateral triangle, generated by r (=rotate) and f (=horizontal flip).

Are the following equal?

$$rfr, \qquad (rf)r, \qquad r(fr)$$

Even though we are associating differently, the end result is that *the actions are applied left to right*.

Upshot: We never need parentheses when working with groups, though we may use them for emphasis.

The formal definition of a group

Definition (official)

A set G together with a binary operation $*$ is a group if the following are satisfied:

- The binary operation $*$ is associative.
- There is an identity element $e \in G$. That is, $e * g = g = g * e$ for all $g \in G$.
- Every element $g \in G$ has an inverse, g^{-1}, satisfying $g * g^{-1} = e = g^{-1} * g$.

Remarks

- Depending on context, the binary operation may be denoted by $*$, $\cdot$, $+$, $\circ$, and more.
- As with ordinary multiplication, we frequently omit the symbol altogether and write, e.g., xy for $x * y$.
- We generally only use the $+$ symbol if the group is abelian. Thus, $g + h = h + g$ (always), but in general, $gh \neq hg$. E.g. matrix addition vs multiplication.
- Uniqueness of the identity and inverses is *not* built into the definition of a group, but we can prove these properties.

Examples and non-examples of groups (Part I)

Which of these is a group? It it is a group, give the identity element. If it is not a group, give an explicit reason for why it fails to be a group.

1. All integers $\mathbb{Z}$ under addition $+$ is a group. The identity element is 0. Some possible minimal generating sets are $\{1\}$, $\{-1\}$, $\{4, 5\}$, and $\{7, 12\}$. (But note that $\{9, 12\}$ is *not* a generating set.)
2. All integers $\mathbb{Z}$ under multiplication x is not a group. It satisfies associativity and it has an identity element (1) but not every element has an inverse, for example, there is no integer z such that $5z = 1$.
3. All positive integers under addition.
4. All positive integers under multiplication.
5. All rational numbers $\mathbb{Q}$ under addition.
6. All rational numbers $\mathbb{Q}$ under multiplication.

Examples and non-examples of groups (Part II)

Which of these is a group? It it is a group, give the identity element. If it is not a group, give an explicit reason for why it fails to be a group.

1. All nonzero rational numbers $\mathbb{Q}^*$ under addition.

2. All nonzero rational numbers $\mathbb{Q}^*$ under multiplication.

3. All 2×2 matrices (with real number entries) under addition.

4. All nonzero 2×2 matrices (with real number entries) under multiplication.

5. All 2×2 matrices (with real number entries) which has determinant 1, under multiplication.

Uniqueness of inverses

Theorem

Every element of a group has a *unique* inverse.

Proof

Let g be an element of a group G. By definition, it has at least one inverse.

Suppose that h and k are both inverses of g. This means that $gh = hg = e$ and $gk = kg = e$. (It will suffice to show that $h = k$.) Indeed,

$$\begin{aligned} h &= he \\ &= h(gk) \\ &= (hg)k \\ &= ek \\ &= k\,. \end{aligned}$$

Theorem (HW)

Every group has a *unique* identity element.

You can use a similar technique for the proof.

Uniqueness of the identity (taken from HW)

Theorem (HW)

Every group has a *unique* identity element.

(Instruction: Only use the definition of a group. Don't use other facts)

Proof

By definition, G has at least one identity. Suppose that ...

$\square$