COMS10003 Workshop Sheet 10.

Julian Gough 2014-12-1

Introduction

Useful facts

- Definition of a group: given a set X and a map

$$\begin{aligned} X \times X &\rightarrow X \\ (x, y) &\mapsto x \cdot y \end{aligned} \tag{1}$$

then $(X, \cdot)$ is a group if

1. Closure: if $x \in X$ and $y \in X$ then $x \cdot y \in X$.
2. Associativity: if x, y and z are all in X then

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{2}$$

3. Identity: there is an element $e \in X$ such that $x \cdot e = e \cdot x = x$ for all $x \in X$.
4. Inverse: for any element $x \in X$ there is another element x^{-1} such that $x \cdot x^{-1} = x^{-1} \cdot x = e$.

Some common mathematical notation

- Some names for laws governing addition and multiplication.

1. Associative property: rough means you can move the brackets around, holds for both addition and multiplication.

$$\begin{aligned} a(bc) &= (ab)c \\ a + (b + c) &= (a + b) + c \end{aligned} \tag{3}$$

It doesn't hold for division: $(12/4)/3 = 3/3 = 1$ but $12/(4/3) = 36/4 = 9$.

2. Distributive rule: the rule for getting rid of brackets when you have multiplication and addition

$$\begin{aligned} a(b + c) &= ab + ac \\ (a + b)c &= ac + bc \end{aligned} \tag{4}$$

3. Abelian property: the order doesn't matter, holds for addition and multiplication.

$$ab = ba$$

$$a + b = b + a \tag{5}$$

Doesn't hold for division, or matrix multiplication or rotations about different axes.

- How to write maps: above we use a common notation for writing maps

$$\begin{aligned} f : X &\rightarrow Y \\ x &\mapsto f(x) \end{aligned} \tag{6}$$

means that f maps elements in a set X to elements in set Y with x going to $f(x) \in Y$. So, using this notation, if we were defining the floor function we might write

$$\begin{aligned} \lfloor \cdot \rfloor : \mathbf{R} &\rightarrow \mathbf{Z} \\ x &\mapsto \lfloor x \rfloor = \text{the integer you get by rounding down } x \end{aligned} \tag{7}$$

- The four element group we saw in lectures is called $\mathbf{Z}_4$, the one we discuss below, the Klein four-group is often called V_4, the V stands for Vier, the German for four.

Work sheet

1. Work out a multiplication table for $\{[1], [3], [5], [7]\}$ modulo eight. Show it is a group - don't worry about associativity, that follows from the associativity of modular multiplication. In fact, this is the other group with four elements; it is called the Klein four-group.

2. Consider the digit 0, considered as it appears here so it is taller than it is wide, this has flipping over symmetries, flipping it horizonally h, flipping it vertically v and doing both, one after the other, which we will write as hv. You should check hv is the same as as the rotational symmetry, rotation through $\pi = 180°$. Write out a composition 'after' table for this set of symmetries, including e, the symmetry you get by doing nothing. Is this group the Klein four-group V_4 or the four element group $\mathbf{Z}_4$ we saw in lectures.

3. Consider the addition table for $\{[0], [1], [2], [3]\}$ modulo four. Show this is a group - don't worry about associativity, that follows from the associativity of modular addition. What is the identity? Is this group the Klein four-group V_4 or the four element group $\mathbf{Z}_4$ we saw in lectures.

Exercise sheet

1. The group Z_2 can be thought of as the multiplicative group formed by $\{[1], [2]\}$ modulo three. Write out the table.

2. The group Z_2 can be also be thought of as the additive group formed by $\{[0], [1]\}$ modulo two. Write out the table and show it is isomorphic to the table above.

3. Work out the group table for the rotational symmetries of an equilateral triangle.

4. A subgroup of a group is a subset of the group that is a group, the main thing to check is that the subset is closed. Now, using the notation in the lecture notes $\{e, a\}$ in the Z_4 group is not a subgroup since $a^2 = c$ so it isn't closed. Can you find a Z_2 subgroup of Z_4? What about V_4? It has three Z_2 subgroups.

Further study

- One nice story relates to wallpaper groups, they are the group of symmetries of a repeating two-dimensional pattern. It turns out there are only 17 of these; the Wikipedia article has illustrations of patterns with these different symmetries. `http://en.wikipedia.org/wiki/Wallpaper_group`

- The *Futurama* episode *The Prisoner of Benda* involves group theory and one of the writers proved a theorem specifically to use in the episode.

- The problem of finding all possible groups is one of the big problems of twentieth century mathematics, the eventual classification theorem is tens of thousands of pages long. See `http://en.wikipedia.org/wiki/Classification_of_finite_simple_groups`. Important work on this problem was done by John Conway who is known to computer scientists for inventing early cellular automaton called the Game of Life `http://en.wikipedia.org/wiki/John_Horton_Conway`.

Challenge

This week's `projecteuler.net` challenge: try to prove problems with numbers higher than 300.