

EMAT10001 Lecture 7.

Conor Houghton 2013-11-10

Preface

These are outline notes for lecture 7; this lecture introduces group theory. As usual there is a bounty of between 20p and £2 for errors, you can tell me at the end of a lecture or email me at `conor.houghton@bristol.ac.uk`. A manicule (☞ or ☞) is used to indicate that a proof, derivation or piece of material has been omitted from the lecture but will be covered in the workshop.

Introduction

This lecture is about group theory; group theory is a huge subject with a myriad of diverse applications. Here, though, we will only touch on it and the main message is one about abstraction. In mathematics we can start in one place, here, modular arithmetic, codify the structure, examine how the structure unfolds and then apply it to other sorts of problems and to other applications, often ones that are very different to the one we started with.

Equivalence classes

Say we are working in modular arithmetic, for example as part of cryptography and we are presented with a problem, say to solve

$$3x \equiv 1 \pmod{8} \quad (1)$$

Now we would immediately apply the Euclid algorithm

$$\begin{aligned} 8 &= 2 \cdot 3 + 2 \\ 3 &= 2 + 1 \end{aligned} \quad (2)$$

so $1 = 3 - 2$ and $1 = 3 - (8 - 2 \cdot 3)$ so $1 = 3 \cdot 3 - 8$ and $3^{-1} \equiv 3 \pmod{8}$. We can check this

$$3 \cdot 3 = 9 \equiv 1 \pmod{8}. \quad (3)$$

Now, at this stage we are used to the idea that $3^{-1} \equiv 3 \pmod{8}$ means that $3^{-1} \equiv 11 \pmod{8}$ as well, because $3 \equiv 11 \pmod{8}$ and we can check

$$3 \cdot 11 = 33 \equiv 1 \pmod{8} \quad (4)$$

In the same way to know all about modular arithmetic modulo eight we only need to look at the numbers from zero to seven, everything else can be worked out from them using the modular properties, so

$$19 \cdot 11 = 209 \equiv 1 \pmod{8} \quad (5)$$

since $209 = 26 \cdot 8 + 1$ but we could just as easily go

$$19 \cdot 11 \equiv 3 \cdot 3 \equiv 1 \pmod{8} \quad (6)$$

because $19 \equiv 11 \equiv 3 \pmod{8}$.

The idea of equivalence classes is to deal with this. If you have an equivalence relation, \sim say, on some set X and $x \in X$ then *the equivalence class of x* often written $[x]$ is the set of x and all things equivalent to it

$$[x] = \{y | y \sim x\} \quad (7)$$

So here our equivalence relation is equivalence modulo eight then, for example

$$[3] = \{y | y \equiv 3 \pmod{8}\} = \{3 + 8k | k \in \mathbf{Z}\} = \{\dots - 13, -5, 3, 11, 19, \dots\} \quad (8)$$

and we call ‘3’ a representative of the equivalence class $[3]$.

Now, when we are interested in arithmetic modulo eight we look at the relationship between the equivalence classes, so

$$[3] \cdot [3] = [3 \cdot 3] = [1] \pmod{8} \quad (9)$$

and that stands in for

$$3 \cdot 3 \equiv 1 \pmod{8} \quad (10)$$

as well as

$$19 \cdot 11 \equiv 1 \pmod{8} \quad (11)$$

and the whole mess of different representations of the same modular product. Of course, this depends on equivalence classes ‘playing nice’ with addition. The mathematical way to say this is that addition is *well defined* with respect to this equivalence relation

$$[a] + [b] = [a + b] \quad (12)$$

no matter which representatives a and b we use. We won’t go too much into that today, but we proved, or at least discussed, lemmas that show that addition and multiplication are well defined with respect to the modulus.

Groups

Now lets look at multiplication modulo five; we will ignore $[0]$ for reasons that will become clear

\cdot	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[4]$	$[3]$	$[2]$	$[1]$

This looks quite hard to read because of all the brackets, so lets use some other symbols, say $e = [1]$, $[1]$ is the *identity*, multiplying by $[1]$ doesn't change anything and e is often used for identity, and $[2] = a$, $[3] = b$ and $[4] = c$, then the multiplication table becomes

\cdot	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

This multiplication table has lots of the properties you might expect a multiplication table to have. Formally, we say a set X is a *group* if there is a map \cdot that maps two elements x and y to a third element $x \cdot y$ and

- If x and y are two elements of the set X then $x \cdot y$ is also an element.
- It is associative: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- There is an *identity* element, $e \in X$ such that $x \cdot e = e \cdot x = x$ for all elements $x \in X$.
- Every element of X has an inverse, so, for all $x \in X$ there exists an element $x^{-1} \in X$ such that $x \cdot x^{-1} = x^{-1} \cdot x = e$.

Here, \cdot is multiplication modulo five and the set X is

$$X = \{[1], [2], [3], [4]\} \quad (13)$$

If we had included $[0]$ we would not have gotten a group because $[0]$ has no inverse.

Now, we said at the outset that groups occur in a huge number of different context. Here is another one. Imagine the rotational symmetries of a square. If you have a square you can rotate it by $\pi/2 = 90^\circ$ clockwise around the center line, or by $\pi = 180^\circ$ or by $3\pi/2 = 270^\circ$; all of these are symmetries, as is not rotating it at all. Now lets call rotating by no degrees R_0 and refer to rotating by 90° as R_{90} , rotating by 180° as R_{180} and rotating by 270° as R_{270} . You can compose these, if you rotate by 90° after already rotating by 90° you are doing R_{90} after R_{90} , and this is the same as doing R_{180} all in one go. We write

$$R_{180} = R_{90} \circ R_{90} \quad (14)$$

and, as another example,


$$R_0 = R_{90} \circ R_{270} \quad (15)$$

where we read \circ as 'after' where we use that rotating by 360° is the same as not rotating at all. In the same way we can make up the multiplication table

\circ	R_0	R_{90}	R_{270}	R_{180}
R_0	R_0	R_{90}	R_{270}	R_{180}
R_{90}	R_{90}	R_{180}	R_0	R_{270}
R_{270}	R_{270}	R_0	R_{180}	R_{90}
R_{180}	R_{180}	R_{270}	R_{90}	R_0

Of course, it doesn't matter what order I write the rows and columns, I wrote it in the order I did with R_{270} in-between R_{90} and R_{180} for later convenience.

It would be easy to check that this is a group, however, there is a stronger result: it is the same group. If you replace R_0 with e , R_{90} with a , R_{270} with b and R_{180} with c this is exactly the same as the group we looked at before. This is an example of a *group isomorphism*; the two groups are the same up to a change in the symbols used. We say the group of rotational symmetries of a square is isomorphic to the multiplicative group modulo five.

This is an example of two seemingly different things being the same when looked at abstractly. In fact, in a sense, there aren't that many different groups, with four elements, there are two: the one above and another called the *Klein four group* .