Lecture 1: Introduction to abstract algebra

Rajat Mittal

IIT Kanpur

Please look at the course policies mentioned in the course homepage. Most importantly, any immoral behavior like cheating and fraud will be punished with extreme measures and without any exception.

1 What is this course about?

Take a look at the following questions.

- Give a number n which leaves a remainder of 20 when divided by 23 and 62 when divided by 83.
- How many different necklaces can you form with 2 black beads and 8 white beads? How many necklaces can you form with blue, green and black beads?
- What are the last two digits of of a^{40} when a is not divisible by 2 or 5?
- We know that there is an explicit formula for the roots of quadratic equation $ax^2+bx+c=0$, $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. Similarly there are explicit formulas for degree 3 and degree 4 equations. Why don't we have something for degree 5?
- When does the equations of the form $x-y=z$ make sense? If x is a natural number or an integer or a matrix or an apple or a permutation?

When we look at these questions, they seem unrelated and seem to have no common thread. Mathematicians realized long time back that problems in algebra, number theory and even geometry can be solved using very similar techniques. They were interested in finding out the common element among these proofs and were interested in searching for more domains where such techniques are applicable. It turns out that there is a single mathematical theory which can help us understand these questions in a single framework and give us answers to these seemingly non-related topics.

The mathematical framework which ties these questions together is called *abstract algebra*. Not surprisingly, given the name, the course is going to be about *abstract algebra*.

Exercise 1. What does *abstract* mean?

Note 1. The exercises given in the course notes are practice problems with the exception of this particular introduction. The exercises given in this particular document are to motivate the study of abstract algebra. You should try to think about them but remember that there are no clear answers.

We will precisely study the mathematical structures which can represent numbers, matrices, permutations, geometric objects under different parameters. The first step would be to define these mathematical (algebraic) structures like groups, rings and fields. The next step is to find properties of these algebraic structures. Finally we will also see how these properties give so many beautiful results in different areas of mathematics.

Lets start with a more basic question,

Exercise 2. What does *algebra* mean?

1.1 Arithmetic and algebra

Most of the people when asked the above question, think about numbers, equations and operations between them. So lets make the previous question more precise. What is the difference between arithmetic and algebra? Arithmetic is the study of numbers and the operations (like addition, subtraction, multiplication) between them. Algebra, intuitively, talks about equations, variables, symbols and relations between them.

The primary difference is the use of variables, which can stand for an unknown or a group of numbers. These variables are somewhat abstract but really help us in manipulating equations and solving them. It would be too cumbersome to write things in words instead of using equations and variables.

Exercise 3. Give an example where using a variable helps you to write a statement concisely.

Now we know what algebra is, lets talk about *abstract* part of it.

1.2 Abstraction

All of us like numbers (or at least understand the importance of it). One of the reason is that numbers are very well-behaved. In other words, there are so many nice properties that it is easy to manipulate and work with numbers. Lets look at one of the most fundamental properties,

Theorem 1. *Fundamental theorem of arithmetic: Every integer greater than* 1 *can be uniquely expressed as the product of primes up to different orderings.*

Since this property is so useful, we should ask, are there other objects which satisfy similar theorems.

Exercise 4. Do we have unique factorization theorem for matrices or permutations.

There is a very important methodology to generalize given proofs. You look at the proof and figure out the crucial step and properties which make the proof work. So one way to approach this question would be, carefully look at the proof of the theorem and figure out the properties of integers we have used at different step. Then check if another mathematical object satisfies the same properties.

In other words, *any* mathematical object which satisfies these properties will also have a unique factorization theorem. The abstract object which has all these properties can be given an appropriate name. This is similar to variables. As variables can take different values, this abstract object can be assigned different mathematical objects.

We will turn this method upside down. We will consider some basic properties and give a name to the abstract structure which satisfies these "basic properties".

Exercise 5. Who decides these basic properties?

Using these "basic properties" we will come up with multiple theorems like the unique factorization theorem above. By the above discussion any mathematical object (from arithmetic, algebra, geometry or anywhere else) which has these "basic properties" will satisfy all the theorems too. Hence in one shot we will get theorems in diverse areas.

You are already familiar with one such abstract structure, *set*. A collection of objects is called set and it needs no other property to be satisfied.

Exercise 6. What kind of theorems can you prove for sets?

In the course we will look at the collection of objects (sets) with certain composition properties. These will give rise to groups, rings etc.. The first such abstraction we will study is group.

Exercise 7. Should we choose as many basic properties as possible or as less basic properties as possible?