In this lecture, we shall introduce the basic ideas of the field of mathematics known as "modern algebra" (or as "abstract algebra" or simply as "algebra"). We will only have time to scratch the surface of this vast and beautiful subject; if you want to learn more, the following texts are both excellent introductions:

- I. Herstein, *Topics in Algebra* (1975)
- M. Artin, *Algebra* (1993).

At the end of this lecture, we will describe just one application of algebra to computer science—secret sharing schemes.

Groups and Fields

A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation satisfying the following properties:

- there exists an element $e \in G$ such that for all $x \in G$, $e \cdot x = x \cdot e = x$,
- for every element $x \in G$, there exists an element $x^{-1} \in G$ such that $x \cdot x^{-1} = x^{-1} \cdot x = e$, and
- for all elements $x, y, z \in G$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

The element $e \in G$ is called the *identity element* of G. If the operation $\cdot$ is commutative—i.e., if $x \cdot y = y \cdot x$ for all $x, y \in G$—then we say that G is an *abelian* group.

Examples:

1. The set of integers $\mathbb{Z}$, with the operation of addition $(+)$, is an abelian group. The integers with the operation of multiplication is not a group, however (why not?).
2. The set of real numbers $\mathbb{R}$ with the operation of addition is an abelian group, and the set $\mathbb{R} \setminus \{0\}$, with the operation of multiplication, is also an abelian group. Note that the set $\mathbb{R}$, again with multiplication as the operation, is not a group. The same statements hold for the rational numbers $\mathbb{Q}$ and the complex numbers $\mathbb{C}$.
3. The set of integers mod n—which we denote by $\mathbb{Z}/n\mathbb{Z}$—is a group under (modular) addition. $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication (why not?).
4. The set of integers relatively prime to n, taken mod n—which we denote by $(\mathbb{Z}/n\mathbb{Z})^*$—is a group under multiplication but not under addition (why not?).

You should take the time to verify, axiom-by-axiom, that these sets are indeed groups. (We shall engage in the usual abuse of language by referring to "the group G" when the operation is understood.)

The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are very special groups, as you might have already noticed: they are the canonical examples of algebraic objects known as *fields*. Formally, a field is a triple $(F,+,\cdot)$, where F is a set and $+$ and $\cdot$ are binary operations on F satisfying the following properties:

- $(F,+)$ is an abelian group with identity element $0 \in F$,
- $(F \setminus \{0\},\cdot)$ is an abelian group with identity element $1 \in F$, and
- for all $x,y,z \in F$, $x\cdot(y+z) = x\cdot y + x\cdot z$.

The fields that we will most be interested in are *finite fields*, i.e., fields $(F,+,\cdot)$ such that F is a finite set. ($\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, with the standard operations, are all infinite fields.)

We observed above that $\mathbb{Z}/n\mathbb{Z}$ is always an abelian group under addition and that $(\mathbb{Z}/n\mathbb{Z})^*$ is an abelian group under multiplication. From these two facts, we see easily that if $n = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field (you should make sure that you are fully convinced that this is true). This field is often denoted $GF(p)$ (for "Galois Field") by computer scientists and $\mathbb{F}_p$ by mathematicians.

Conversely, we claim that if $\mathbb{Z}/n\mathbb{Z}$ is a field, then n must be prime. To see this, suppose that $\mathbb{Z}/n\mathbb{Z}$ is a field. Every nonzero element of a field has a multiplicative inverse, so every nonzero element $x \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse. Now we proved before that the equation $ax \equiv 1 \pmod{n}$ has a solution a if and only if $\gcd(x,n) = 1$, so we know that $\gcd(x,n) = 1$ for all x such that $1 \le x < n-1$, and this is equivalent to the statement that n is prime.

Polynomials

We developed most of the properties of polynomials that we'll need in past homeworks (cf. homework 4, in particular), which we briefly recall now:

- A polynomial of degree n over a field F has at most n roots (you proved this by induction).
- A polynomial P of degree n is uniquely determined by any $n+1$ distinct pairs (x_i, y_i) such that $P(x_i) = y_i$ (this follows immediately from the previous property).

In the following, we shall be working over some arbitrary field $\mathbb{F}$. Suppose that we are given the value of a polynomial $P(x)$ of degree n at $n+1$ points: $P(a_i) = b_i$ for $i = 1 \; to \; n+1$, where $a_i, b_i \in \mathbb{F}$. How do we reconstruct the unique polynomial $P(x)$ of degree n satisfying these $n+1$ constraints?

Consider the following polynomials of degree n:

For $i = 1,2,\ldots,n+1$, define

$$\Delta_i(x) = \left(\prod_{j\neq i}(a_i - a_j)\right)^{-1} \prod_{j\neq i}(x - a_j).$$

Notice that $\Delta_i(a_i) = 1$ and for $1 \le j \le n+1,\ j \neq i\ \Delta(a_j) = 0$. It follows that the desired polynomial $P(x) = \sum_{i=1}^{n+1} b_i \Delta_i(x)$.

The process we have just gone through—explicitly constructing a polynomial that passes through a number of given points—is called *Lagrange interpolation*.

If $n = 3$, and $a_i = i$, for instance, then

$$\Delta_1(x) = ((1-2)(1-3))^{-1}(x-2)(x-3) = 2^{-1}(x-1)(x-2)$$
$$\Delta_2(x) = ((2-1)(2-3))^{-1}(x-1)(x-3) = (-1)^{-1}(x-1)(x-3)$$
$$\Delta_3(x) = ((3-1)(3-2))^{-1}(x-1)(x-2) = 2^{-1}(x-1)(x-2).$$

Secret Sharing

Suppose the U.S. government finally decides that a nuclear strike can be initiated only if at least $k > 1$ major officials agree to it (what a "major official" is doesn't really matter to us). We want to devise a scheme such that (1) any group of k of these officials can pool their information to figure out the launch code and initiate the strike but (2) no group of $k-1$ or fewer can conspire to find the code. How can we accomplish this?

Suppose that there are n officials and that launch code is some natural number s. Let q be a prime number larger than n and s —we will work over $GF(q)$ from now on.

Now pick a random polynomial P of degree $k-1$ such that $P(0) = s$ and give the pair $(1, P(1))$ to the first official, $(2, P(2))$ to the second, ..., $(n, P(n))$ to the nth. Then

- Any k officials, having the values of the polynomial at k points, can use Lagrange interpolation to find P, and once they know what P is, they can compute $P(0) = s$ to learn the secret.
- Any group of $k-1$ officials has no information about P. All they know is that there is a polynomial of degree $k-1$ passing through their $k-1$ points such that $P(0) = s$. However, for each possible value $P(0) = b$, there is a unique polynomial that is consistent with the information of the $k-1$ officials, and satisfies the constraint that $P(0) = b$.