SOME HISTORICAL CONTEXT

We begin[1] with the abstract definition of a group;

Definition 1. *A* group *is an ordered pair (G, μ), where G is a set and $\mu : G \times G \to G$ is a binary operation, satisfying the following axioms:*

(1) (associativity) $\mu(\mu(a, b), c) = \mu(a, \mu(b, c))$ for any $a, b, c \in G$
(2) (identity) there exists $e \in G$ such that for any $a \in G$ we have $\mu(a, e) = \mu(e, a) = a$
(3) (inverses) for any $a \in G$, there is an element $a^{-1} \in G$ such that $\mu(a, a^{-1}) = \mu(a^{-1}, a) = e$.

As we saw in class, a few basic examples are:

- the integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, with the binary operation $\mu : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by ordinary addition of integers
- the nonzero rational numbers $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$, with the binary operation given by ordinary multiplication of rational numbers
- the nonzero complex numbers $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$, with the binary operation given by multiplication of complex numbers, etc.

We also saw that $\mathbb{Z}$ equipped with ordinary multiplication is *not* a group, since most elements do not have an inverse within the integers.

Another very important family of groups are the *permutation groups*. Recall that for $n \in \mathbb{Z}_{\geq 1}$, S_n is the set of permutations of the set $\{1, \dots, n\}$, i.e. invertible maps from the set $\{1, \dots, n\}$ to the set $\{1, \dots, n\}$. The natural binary operation $\mu : S_n \times S_n \to S_n$ is given the composition of set maps, i.e. for $f, g \in S_n$, we define $\mu(f, g) \in S_n$ to be the permutation characterized by $\mu(f, g)(k) = (f \circ g)(k) = f(g(k))$ for any $k \in \{1, \dots, n\}$. We have $|S_n| = n!$ (i.e. S_n is a set whose number of elements is $n!$). Also, for $n \geq 3$, the group S_n is *nonabelian*, meaning that the binary operation is not always commutative, i.e. $\mu(f, g) \neq \mu(g, f)$ for some elements $f, g \in S_n$. We will be encountering permutation groups a lot throughout the course. In fact, we will see that, in a certain sense, every group is a subgroup of permutation group (this result is known as Cayley's theorem).

At this early stage in the course, you should be asking yourself:

Question 2. *Why is this definition of a group a "good" one, or the "right" one? Why should you care?*

It is not possible to answer this question in a few sentences. Hopefully, an answer will begin to unfold over the course of the semester. As we will see, this abstract definition of a group leads to a beautifully self-consistent theory admitting many nontrivial results. We will be seeing a great many diverse examples of groups which all satisfy this definition. We will also see that there are some surprisingly deep structural theorems about groups.

Date: September 5, 2019.

[1]Note: in this document and subsequent ones there will likely be plenty of typos and possibly more serious errors. If anything causes confusion, I appreciate you letting me know so that I can correct it for the benefit of others.

Although we will not focus on many applications in this course, there are certainly too many to innumerate. At least in my view, groups are the mathematically precise way of encapsulating the concept of "symmetry". Any time symmetry is important, groups are likely to be important as well.

For the time being I would like to give a few words of historical context. It is important to wonder: how did humanity arrive at this definition of a group? In fact, it took a very long time and a great many brilliant minds. Roughly speaking, up through the 18th century, algebra was primarily about solving explicit algebraic equations. These equations often had a concrete geometric interpretation, in the spirit of say Euclidean geometry. In the 19th century, a transition occurred. Mathematicians began to realize that solving equations is often not possible, and that perhaps this approach is too simplistic. Instead, they began to seek more structure, and slowly arrived at such abstract concepts as groups, rings, fields, modules, representations, and so on. From the 20th century onward, algebra has been primarily about understanding these abstract structures. The primary goals are now to prove nontrivial theorems about these structures, and to better how they interrelate with each other and also with other areas of mathematics and science. Below, I will try to briefly describe how this transition came about. For more details, I recommend the very interesting (and quite readable) book "A History of Algebra" by B.L. van der Waerden. There is also a very nice short article "The Evolution of Group Theory: a Brief Survey" by Israel Kleiner, which should be readily available online. Any inaccuracies or misrepresentations in the exposition below are my own.

Al-Khwarizmi. The word "algebra" comes from the arabic "al-jabr", which is roughly translated into "the reunion of broken parts". An important early treatise on algebra was written by al-Khwarizmi (780-850), who was a Persian born in present day Uzbekistan and did most of his important work in Bagdad (the center of the scientific Arab word in that period). The term al-jabr roughly refered to the idea of adding equal terms to both sides of an equation in order to eliminate negative terms. As an example from al-Khwarizmi's treatise, given the equation

$$x^2 = 40x - 4x^2,$$

one can perform al-jabr to reduce this to $5x^2 = 40x$. However, it's important to realize that for much of history these types of algebraic equations were written out in sentences rather than symbolically, e.g. al-Khwarizmi writes the equation $x^2 = 40x - 4x^2$ as (after translating to English) "a square, which is equal to forty things minus four squares". Our modern symbolic notation is often attribute to René Descartes, who wrote his important treatise around 1637.

The solution to the general quadratic equation $ax^2 + bx + c = 0$ was known since ancient times. By completing the square, one arrives at the (in)famous formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Note that for most of history, only the positive real-valued solutions would have been acknowledged.

Given the enormous important of the quadratic formula, it is natural to ask for a similar formula for the general cubic equation

$$ax^3 + bx^2 + cx + d = 0.$$

We might as well divide by a and consider instead the equation $x^3 + ax^2 + bx + c = 0$. This turns out to be quite a bit trickier. We next turn to Italy.

Scipione del Ferro. As far as we know, Scipione del Ferro (1465-1526), who lived in Bologna, Italy, was the first to solve the general cubic equation. Here is his idea:
Step 1: The first step (which I believe was already well-known), is to make the change of variable $x' = x + a/3$. This makes the quadratic term disappear. Indeed, the equation $x^3 + ax^2 + bx + c = 0$ becomes

$$(x' - a/3)^3 + a(x' - a/3)^2 + b(x' - a/3) + c = 0.$$

Using the binomial expansion formula, we have

$$(x' - a/3)^3 = (x')^3 + 3(x')^2(-a/3) + 3(x')(-a/3)^2 + (-a/3)^3$$

and

$$(x' - a/3)^2 = (x')^2 - 2(x')(a/3) + (-a/3)^2,$$

and so we see that the two quadratic terms $3(x')^2(-a/3)$ and $a(x')^2$ cancel each other.
Step 2: It therefore suffices to consider an equation of the form $x^3 + px + q = 0$. For concreteness, let's consider the example

$$x^3 + 6x - 20 = 0.$$

Now del Ferro's trick is to put $x = u - v$, where u and v are two new variables. Then $x^3 + 6x - 20 = 0$ becomes

$$(u - v)^3 + 6(u - v) - 20 = 0,$$

which can be written as

$$u^3 - v^3 - 3uv(u - v) + 6(u - v) - 20 = 0.$$

This equation will be satisfied provided that we have

$$\begin{cases} 3uv = 6 \\ u^3 - v^3 = 20. \end{cases}$$

To achieve this, note that the first equation implies $uv = 2$, and hence $u^3v^3 = 8$. Since we now know the product and sum of u^3 and v^3, we can easily solve for u and v, and hence for x. For example, after making the substitution $v^3 = 8/u^3$, the second equation gives

$$(u^3)^2 - 8 = 20(u^3),$$

so we can solve for u^3 using the quadratic formula. The final result is

$$x = \sqrt[3]{\sqrt{108} + 10} - \sqrt[3]{\sqrt{108} - 10}.$$

Incidentally, this number is equal to 2, which one can easily check is a root of $x^3 + 6x - 20$ (although a typical cubic equation will not have integer solutions).

For some reason, Scipione del Ferro did not publish this monumental discovery, and told only a few close friends and colleagues.

Niccolo Tartaglia. Niccolo Tartaglia (1499 - 1557) was born in Brescia, Italy and lived in Venice. He was a famous teacher of mathematics and apparently the first to translate Eucld and Archimedes into Italian. In 1535, he was challenged to a mathematics competition by a student of Scipione del Ferro by the name of Fiore. Both of them would try to solve 30 mathematics problems, and the loser would have to pay for 30 banquets. This style of challenging another mathematician was apparently common in those days. As it turns out, all 30 problems were examples of the form $x^3 + px + q = 0$. In a moment of inspiration, Tartaglia rediscovers del Ferro's insight, and manages to solve them all. He is so proud of his discovery that he renounces the 30 banquets. For some reason, Tartaglia also does not publish his method.

Gerolamo Cardano. Gerolamo Cardano (1501-1576) was a prominent doctor, astrologer, philosopher, and mathematician living in Milan. Having heard of Tartaglia's discovery, he convinces Tartaglia to come to Milan and stay in his house. He promises to introduce Tartaglia to the military commander of Milan so that Tartaglia can demonstrate some of his military inventions. When Tartaglia arrives, Cardano persuades him to reveal his secret of the cubic. Tartaglia does, but only under the condition that Cardano swears an oath of secrecy, which takes place on March 25, 1539.

Lodovico Ferrari. Lodovico Ferrari was born in 1522 in Bologna and became Cardano's servant at the age of 14. As he was extremely bright, Cardano started to teach him mathematics. Later, Ferrari makes an enormous discovery. Namely, he figures out how to solve the general quartic equation $x^4 + ax^3 + bx^2 + cx = 0$. His idea is roughly the following, which is explained in Cardano's book "Args Magna, sive de regulis algebraicis", printed in 1545. Incidentally, by a similar trick to before, it is always possible to remove the cubic term by a simple change of variables. Now let us consider the example

$$x^4 + 6x^2 - 60x + 36 = 0.$$

By a little manipulation, this equation can be written in the form

$$(x^2 + 6 + C)^2 = 6x^2 + 60x + 2Cx^2 + 12C + C^2,$$

for any constant C. If the right hand side happens to be a perfect square, then we can take the square roots of both sides to arrive at a quadratic equation for x, which we know how to solve. So the key is to pick C such that the right hand side is a perfect square. This happens precisely when the discriminant (i.e. $b^2 - 4ac$ in the context of the quadratic formula) is zero, so we must have

$$60^2 - 4(6 + 2C)(12C + C^2) = 0.$$

This is a cubic equation for C, which at this point in time Cardano knows how to solve!

So together, Cardano and Ferrari can now solve a general quartic equation. But there's a problem: their solution relies on the solution of the cubic equation, and Cardano is sworn to secrecy! However, in 1543, Cardano and Ferrari to go Bologna to pursue a rumor that del Ferro has already known how to solve the cubic before Tartaglia. They are shown some of del Ferro's posthumous papers, and see his solution to the cubic written out clearly. They therefore decide to publish their work, citing both del Ferro and Tartaglia for the solution of the cubic. Needless to say, Tartaglia is furious. In retaliation, his publishes the text of the oath.

Lagrange. Lagrange (1736 - 1813, also Italian) made important early contributions to what is now group theory. The solution of the quintic equation $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ resisted efforts. In the above solutions of the cubic and quartic equations, one introduces a trick to arrive at an auxiliary equation of lower degree. However, similar efforts for the quintic appeared to always result in an auxiliary equation of *higher* degree. It turns outs to be very fruitful to study the effect of permuting the roots of a polynomial, and this sheds light on why these tricks for the cubic and quartic work.

Abel. Niels Henrik Abel (1802 - 1829) was a brilliant Norwegian mathematician. In 1824, at age 22, after initially thinking he could solve the quintic equation, he managed to prove that the general quintic equation cannot be solved by radicals. His work makes use of the earlier work of Lagrange and Cauchy. Roughly speaking, his result says that there is no analogue of the quadratic formula for the equation $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$, which would give the roots by applying the usual arithmetic operations to the coefficients a, b, c, d, e, allowing ourselves also to iteratively extract nth roots. Group theory had still not quite been born, but note that abelian groups are named after Abel.

Galois. Galois was born in 1811 near Paris and died 20 years later in a (politically motivated) dual. Knowing his premature end was near, Galois wrote up his ideas as best he could. It would be many decades before his important insights were truly appreciated. The main outcome of his work is a conceptual proof of Abel's theorem in terms of a theory which is nowadays called Galois Theory. The starting point of Galois theory is to associate to each polynomial a group, called its "Galois group". The Galois group of a polynomial is a certain subgroup of the group of permutations of its roots. Galois was the first to introduce the term "group", although his definition was still rather specific to permutation groups and their subgroups. As Galois realized, one can then translate the solvability of a polynomial equation by radicals into a purely group theoretic property of its Galois group. Galois theory connects groups to another important object in abstract algebra: fields. This will be covered in the second semester of this course.

Many others. Many others contributed to the birth of group theory, and I cannot give a full historical account here. After Galois, Augustin-Louis Cauchy (1789-1857, French) and Arthur Cayley (1821 -1895, British) developed a full-blown theory of permutation groups. In a 1854 paper, Cayley was perhaps the first to give an abstract definition of a group, although his definition only applies to finite groups and is not explicit about the existence of inverses. Note that such abstractions were not necessarily well-received by the mathematical community at the time. Walther von Dyck (1856 - 1934, German) is credited with giving the first full modern definition of a group. Felix Klein (1849 - 1925, German) made many important early contributions to groups of geometric transformations. Sophus Lie (1842 - 1899, Norwegian) initiated the study of what are now called Lie groups (which, while examples of groups, are mostly beyond the scope of this course). Of course, this is only the very beginning of the theory of groups.