Math 331 Fall 2026, Lecture 1: Number systems and binary operations

website: `https://www.cip.ifi.lmu.de/~grinberg/t/26fa/`

0.1. General

Welcome to Math 331: the first part of a two-quarter sequence on abstract algebra. The website of this course will be

`https://www.cip.ifi.lmu.de/~grinberg/t/26fa/` ;

this is where you can find typeset lecture notes and references. Homework will be submitted (and graded) on Canvas. Homework is to be done by yourself, with no use of AI or outside help (collaboration with your fellow students is allowed, as is use of the MRC). If you collaborate, please acknowledge your coauthors. All homework should be typeset.

1. What is this about?

Abstract algebra is called abstract for a reason: it abstracts some features of objects you know (numbers, matrices, maps, etc.), i.e., isolates them from their context and studies them as independent things, ready to be applied to other contexts. And it is called algebra because it is still fundamentally about algebraic operations, albeit in a more general sense. Indeed, roughly speaking, it is about the same four operations that you have been working with for most of your mathematical life:

- **Middle-to-high-school algebra** is about adding, subtracting, multiplying and dividing numbers.
- **Linear algebra** is about adding, subtracting, multiplying and dividing matrices.[1]
- **Abstract algebra** is about adding, subtracting, multiplying and dividing anything that can be added, subtracted, multiplied and divided. The "anything" here hides quite a lot of fineprint (what exactly makes an operation an "addition"?), and this is exactly what we will be defining in the coming lectures.

[1] The word "dividing" is commonly frowned upon, in favor of "inverting", but the idea is the same. A more serious problem is that matrices cannot be multiplied when their dimensions don't fit together; but let's think about square matrices here. Also, matrices can be scaled.

1.1. A quick overview of number systems

So we will be studying "generalized number systems", even though many of them don't look like numbers at all. But before we come to them, let us recall some of the "number systems" (sets of numbers) we know, in a more-or-less historical order:

- The set $\mathbb{Z}_{>0} = \{1, 2, 3, \ldots\}$ of all positive integers originates in prehistory. (Some of the earliest writing was numbers.)
- The set $\mathbb{Q}_{>0}$ of all positive rational numbers was known to the Babylonians.
- The set $\mathbb{R}_{>0}$ of all positive real numbers was first "discovered" by the Greeks (and possibly the Babylonians before them). Arguably, it was not properly (rigorously) defined until the 19th Century by Dedekind, Cantor, Heine, Méray, Weierstrass and others (who thus founded rigorous real analysis).
- The number 0 and the negative numbers took a surprisingly long time to reach mankind's imagination; I refer to the Wikipedia (zero and negatives) for what we know about their history. Yet, from a modern point of view, they are one of the most natural things (certainly 0, the beginning of all counting). So now we have the number systems $\mathbb{Z}$ (the set of all integers), $\mathbb{Q}$ (the set of all rational numbers) and $\mathbb{R}$ (the set of all real numbers).
- The complex numbers were introduced by Cardano in the 1500s; their set is nowadays called $\mathbb{C}$.
- W. R. Hamilton invented what is now known as the Hamiltonian quaternions in 1843. Their set is denoted by $\mathbb{H}$. Unlike the prior number systems, it is noncommutative – that is, two quaternions a and b can satisfy $ab \neq ba$.
- Then there are two analogues of the complex numbers: the dual numbers $\mathbb{D} = \{a + b\varepsilon \mid a, b \in \mathbb{R}\}$ with $\varepsilon^2 = 0$, and the split complex numbers $\mathbb{S} = \{a + bj \mid a, b \in \mathbb{R}\}$ with $j^2 = 1$. We will not say much about them in this course, but we will see them as examples of rings in the second part of the sequence (Math 332).

There are more "number systems". And there are some things that are quite similar to numbers yet do not commonly get the honor of that name: matrices, for example. Square matrices can be added, subtracted, multiplied and oftentimes inverted; why aren't they called numbers?

What is a number anyway? Where do number systems end? Who decides what a number is?

The modern point of view is that this is not a good question. "Number" is a vague notion not worth defining. The rigorously definable concepts are the specific kinds of numbers, such as integers, rational numbers, real numbers, etc.. (Interestingly, the Greeks did not think of real numbers as numbers but as geometric measurements; so the word has been a floating signifier throughout its history.)

But still, there is a real question to be asked here: What do the above number systems have in common, and what other objects share these commonalities?

This is what abstract algebra is about.

So what makes a number, or, rather, what makes a number system? All the above number systems have operations $+$ (addition), $-$ (subtraction), $\cdot$ (multiplication) and $/$ (division), even though the operations $-$ and $/$ are not always defined in some of the systems (for example, $a - b$ and a/b are not always defined in $\mathbb{Z}_{>0}$, and $n/0$ is never defined). So it makes sense to focus on the operations $+$ and $\cdot$, and view $-$ and $/$ as their partially-defined "undo operations". Let us see what we know about $+$ and $\cdot$ on some of our number systems:

1. **Associativity of addition:** We have $(a+b)+c = a+(b+c)$ for all numbers a, b, c.

2. **Associativity of multiplication:** We have $(ab)\,c = a\,(bc)$ for all numbers a, b, c. (When the operation symbol is not written, always read a $\cdot$, as usual in algebra.)

3. **Commutativity of addition:** We have $a + b = b + a$ for all numbers a, b.

4. **Commutativity of multiplication:** We have $ab = ba$ for all numbers a, b. (This holds for all the above number systems, except for $\mathbb{H}$; it also does not hold for matrices.)

5. **Identity element of addition:** There exists a number – called 0 – that satisfies $a + 0 = 0 + a = a$ for each number a. (This holds for all "modern" number systems, but not for $\mathbb{Z}_{>0}$, $\mathbb{Q}_{>0}$ and $\mathbb{R}_{>0}$.)

6. **Identity element of multiplication:** There exists a number – called 1 – that satisfies $a1 = 1a = a$ for each number a.

7. **Annihilation:** We have $a0 = 0a = 0$ for each number a. (Here and in the following, "0" and "1" mean the 0 and the 1 from the previous two properties.)

8. **Distributivity I:** We have $a\,(b+c) = ab + ac$ for all numbers a, b, c.

9. **Distributivity II:** We have $(a+b)\,c = ac + bc$ for all numbers a, b, c.

10. **Existence of additive inverses:** For each number a, there exists a number a' such that $a + a' = a' + a = 0$. (This does not hold for $\mathbb{Z}_{>0}$, $\mathbb{Q}_{>0}$ and $\mathbb{R}_{>0}$. The number a' is denoted by $-a$ and called the **negative** or the **additive inverse** of a. This allows us to define subtraction by $a - b = a + b'$.)

11. **Existence of multiplicative inverses:** For each number $a \neq 0$, there exists a number a' such that $aa' = a'a = 1$. (This holds for $\mathbb{Q}$, for $\mathbb{R}$, for $\mathbb{C}$ and for $\mathbb{H}$, but not for $\mathbb{Z}$, for $\mathbb{D}$, for $\mathbb{S}$ and for many other number systems. This number a' is denoted by a^{-1} or $\dfrac{1}{a}$ and called the **reciprocal** or the **multiplicative inverse** of a. This allows us to define division by $\dfrac{a}{b} = ab'$.)

12. **Absence of zero-divisors:** If a and b are two nonzero numbers, then $ab \neq 0$. (This holds for all the above number systems except for $\mathbb{D}$ and $\mathbb{S}$. It also fails for matrices.)

13. **Ordering:** There is a total order on the number system (i.e., numbers can be compared by size) that "behaves well" (this means, e.g., that $a \leq b$ implies $a + c \leq b + c$ and $ac \leq bc$ for every $c \geq 0$ and so on). (This is true for $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{Q}$ but not for $\mathbb{C}$.)

As you can already see, these properties (called **axioms**) are not universal; some number systems satisfy more of them than others do. And there are many more axioms that we can think of (for example, any real number has a cube root, but most number systems do not satisfy this). The idea is now to define "number systems" as sets with two operations $+$ and $\cdot$ that satisfy some of the above axioms. More precisely, for each selection of axioms, we want to know both

1. examples of number systems that satisfy these axioms, and

2. general properties that all such number systems have (i.e., theorems that can be deduced from the axioms).

These are the daily bread of an algebraist.

In this quarter-long course, we will only cover "number systems" with one operation ($+$ or $\cdot$ or whatever else we call it). There is already a lot of interesting things to say about them. Then, systems with two operations $+$ and $\cdot$ will be covered in Math 332.