# Number Fields

## Introduction

We are all familiar with the following sets of numbers. What are they? What properties do they have?

- Natural Numbers
- Integers
- Rational Numbers
- Real Numbers
- Complex Numbers

The real question is

*Question* 1. What operations are we able to do in each set of numbers without leaving the set?

For example, within the Natural Numbers, we can always add two numbers and be sure we have a Natural Number. But we cannot always subtract, for instance if we try to take $a - b$ when $b > a$ then we don't get a Natural Number.

*Question* 2. Now that we have thought about which operations we are allowed in each set, let's focus our attention on the Rational Numbers, the Real Numbers, and the Complex numbers. What operations do they have in common?

These three sets of numbers are examples of what we call a Field of Numbers (or a Number Field, or simply a Field).

## Fields of Numbers

A Field $F$ is a set (of numbers) with addition $+$ and multiplication $\cdot$ both defined so that the following are true:

- If $x$ and $y$ are numbers in $F$ then so are $x+y$ and $x \cdot y$.
- $+$ and $\cdot$ are both associative and commutative:

$$\begin{aligned} x+(y+z) &= (x+y)+z \\ x+y &= y+x \\ x\cdot(y\cdot z) &= (x\cdot y)\cdot z \\ x\cdot y &= y\cdot x. \end{aligned}$$

- Multiplication distributes across addition:

$$x\cdot(y+z) = x\cdot y + x\cdot z.$$

- There are two special numbers called 0 and 1 so that:

$$\begin{aligned} x+0 &= x \\ 1\cdot x &= x. \end{aligned}$$

- Every number $x$ has an opposite $-x$ so that

$$x+(-x) = 0.$$

- Every number $x$, except 0, has an inverse $x^{-1}$ so that

$$x\cdot(x^{-1}) = 1.$$

This list of rules, called the "Field Axioms," allows us to decide what is and is not a field, and to make statements about all fields.

*Question* 3. Looking at the Field Axioms, why are neither the set of Natural Numbers nor the set of Integers considered to be fields?

Let's also look at a statement we can make about all fields. This statement will also be useful in deciding that certain things are not fields.

*Theorem* 1. In any field $F$,

$$x\cdot y = 0$$

implies that either $x=0$ or $y=0$.

*Question* 4. Can you prove the above statement?

## Some Nice Fields

The Rationals, Reals, and Complex numbers are all “natural” fields to us. But what are some “simple” fields? Let’s try some finite sets.

*Question* 5. let $F = \{0, 1\}$ be the set with just these two numbers. (Can a field have fewer numbers in it?) Maybe we can make this into a field. Do you have any ideas?

*Question* 6. What is the next natural candidate? Does your idea work here as well?

*Question* 7. What’s next? Does this work too?

*Question* 8. Do you have any conjectures yet? Test them a bit.

## Finite Fields

*Conjecture* 1. $F_p = \{0, 1, 2, \ldots, p-1\}$ can be made into a field using arithmatic modulo $p$ if and only if $p$ is prime.

*Question* 9. Can we prove this conjecture?

## Solving Polynomials in Finite Fields

Consider the polynomial equation

$$x^2 + 1 = 0.$$

Does this equation have any rational solutions? Does it have any real solutions? Does it have any complex solutions? We can now obviously ask:

*Question* 10. Does this equation have any solutions in $F_2$? What about in $F_3$? $F_5$? $F_p$? How many solutions does this equation have in each of these fields?

Let's look at another example. Consider the polynomial equation

$$x^2 - 2 = 0.$$

In which "natural" fields does this equation have solutions?

*Question* 11. If we want to talk about trying to solve this polynomial in finite fields, we should first try to make sense of what the number 2 is in each of these fields. What is "2" in $F_2$? What is "2" in $F_p$?

*Question* 12. Now we can ask: which of the first few finite fields has solutions to the equation $x^2 - 2 = 0$? How many solutions are there?

*Question* 13. Find fields where we can solve the following equations:

$$\begin{aligned} x^3 + 1 &= 0 \\ x^5 + 1 &= 0 \\ x^7 + 1 &= 0 \\ x^{11} + 1 &= 0 \\ x^{13} + 1 &= 0 \end{aligned}$$

How many solutions do we have in each of these cases?

*Question* 14. How many solutions does $x^p + 1 = 0$ have in $F_p$? Can you prove it?

*Question* 15. How about $x^{p-1} - 1 = 0$ in $F_p$? How many solutions?