Some facts about fields

February 4, 2016

The axioms for a field

A field is a set F equipped with an *addition* operation, which we write as $a + b$, and a *multiplication* operation, which we write as $a \cdot b$. Formally, these are functions:

$$+ : F \times F \to F$$

$$\cdot : F \times F \to F$$

In addition to these operations, we have an *additive identity* $0 \in F$ and a *multiplicative identity* $1 \in F$. Moreover, for any element $a \in F$ we have an element $-a \in F$ called the *additive inverse*, and for any $a \in F$ with $a \neq 0$ we have an element $a^{-1} \in F$ called the *multiplicative inverse*.

The names of the operations and the notation we have used to denote them is very suggestive of addition and multiplication in $\mathbb{R}$ or $\mathbb{C}$. The following rules ensure that the structue of a field recovers much of what we are used to from real and complex numbers:

- *Associativity of addition*

$$a + (b + c) = (a + b) + c$$

- *Commutativity of addition*

$$a + b = b + a$$

- *Law for additive identity*

$$a + 0 = a$$

- *Law for additive inverse*

$$a + (-a) = 0$$

- *Associativity of multiplication*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- *Commutativity of multiplication*

$$a \cdot b = b \cdot a$$

- *Law for multiplicative identity*

$$a \cdot 1 = a$$

- *Law for multiplicative inverse*

$$a \cdot \left(a^{-1}\right) = 1$$

- *Distributivity*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

- *Additive and multiplicative identities are distinct*

$$0 \neq 1$$

Remark. Although the field axioms capture a lot of what we know about real and complex numbers, some of our intuition about these fields does not extend to all fields. For example, there is nothing in the axioms that forces a field to be infinite. Note also that an element can be its own (additive or multiplicative) inverse. Indeed, the element $1 \in F$ is always its own multiplicative inverse, since $1 \cdot 1 = 1$. However, there are other examples: in the field with 5 elements, $F_5 = \{0, 1, 2, 3, 4\}$, we have:

$$4 \cdot 4 = 1$$

Thus, 4 is its own inverse in this field.

Some consequences of the axioms

Here are some simple consequences of the axioms. These statements are true in any field:

1. Multiplicative and additive identities are unique. That is, if $a \cdot b = b$ for every $b \in F$, then $a = 1$. Similarly, if $a + b = b$ for every $b \in F$, then $a = 0$.
2. Multiplicative and additive inverses are unique. That is, if $a \cdot b = a \cdot c = 1$ then $b = c$. Similarly, if $a + b = a + c = 0$ then $b = c$.
3. For any $a \in F$ we have $0 \cdot a = 0$.
4. In any field F we have $(-1) \cdot (-1) = 1$.

Here is a proof of half of Statement 2:

$$\begin{aligned} b &= 0 + b \\ &= (a + c) + b \\ &= a + (c + b) \\ &= a + (b + c) \\ &= (a + b) + c \\ &= 0 + c \\ &= c \end{aligned}$$

Try proving the others.

Ordered Fields

Part of what makes the real numbers pleasant is that any nonzero real number is either positive or negative. This doesn't make sense in every field: for example, what is does it mean to be a positive number in F_5 or $\mathbb{C}$? This property of $\mathbb{R}$ is captured by some additional structure.

An *ordered field* is a field F equipped with a relation $a \leq b$, which satisfies the following conditions:

- *Antisymmetry*
$$(a \leq b) \wedge (b \leq a) \Longrightarrow a = b$$
- *Transitivity*
$$(a \leq b) \wedge (b \leq c) \Longrightarrow a \leq c$$
- *Totality*
$$(a \leq b) \vee (b \leq a)$$
- *Compatibility with addition*
$$(a \leq b) \Longrightarrow (a + c \leq b + c)$$
- *Compatibility with multiplication*
$$(0 \leq a) \wedge (0 \leq b) \Longrightarrow 0 \leq a \cdot b$$

Example. The real numbers $\mathbb{R}$ and the rational numbers $\mathbb{Q}$ form ordered fields. No finite field can be made to form an ordered field, and neither can the complex numbers $\mathbb{C}$.

Algebraically closed fields

A field F is called *algebraically closed* if every polynomial of degree n over F has n roots in F. In other words, if we have any polyomial:

$$f(X) = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \ldots + \alpha_n X^n$$

with $\alpha_i \in F$, we may rewrite it as a product of linear polynomials:

$$f(X) = k(X - a_1)(X - a_2)(X - a_3)\ldots(X - a_n)$$

for $k, a_i \in F$. These a_i are the *roots* or *zeros* of f: we have $f(a_i) = 0$ for any i.

Example. The real numbers $\mathbb{R}$ are not algebraically closed; for instance the polynomial

$$f(X) = X^2 + 1$$

has no roots in $\mathbb{R}$. It does, however, have roots in $\mathbb{C}$, where it can be written:

$$f(X) = (X - i)(X + i)$$

It turns out that $\mathbb{C}$ is algebraically closed; this is sometimes called the fundamental theorem of algebra. Moreover, $\mathbb{C}$ is the *algebraic closure* of $\mathbb{R}$: it is the smallest algebraically closed field that contains $\mathbb{R}$.

Example. No finite field is algebraically closed. This hinges on the observation that there are nontrivial polynomials over finite fields which evaluate to zero everywhere.

Explicitly, let F be a finite field. Then the polynomial below is well-defined, since the product is only over a finite number of elements:

$$f(X) = 1 + \prod_{a \in F} (X - a)$$

This polynomial has no roots in F, because for any $a \in F$ we have:

$$\begin{aligned} f(a) &= 1 + (a - a) \prod_{b \neq a} (b - a) \\ &= 1 + 0 \\ &= 1 \end{aligned}$$