1. Notes on the construction of $\mathbb{C}$

Consider the second order polynomial with coefficients $A, B, C \in \mathbb{R}$ with $A \neq 0$,

$$p(x) = Ax^2 + Bx + C.$$

If $B^2 > 4AC$, this equation has two solutions

$$x = \frac{1}{2A}(-B \pm \sqrt{B^2 - 4AC})$$

(one solution with the plus sign, the other with the minus sign). If $B^2 - 4AC = 0$ these two solutions become one solution $x = \frac{-B}{2A}$, while for $B^2 - 4AC < 0$ there is no solution at all, because the square root of a negative number is not defined in $\mathbb{R}$.

Of course, it would be nice if one could avoid this distinction into cases. An idea, which turns out to be very successful, is to introduce a formal symbol i with property $i^2 = -1$, so that -1 will have two square roots $\pm i$. Then the equation $p(x)$ will two solutions even for $B^2 - 4AC < 0$, namely

$$x = \frac{1}{2A}(-B \pm i\sqrt{4AC - B^2}).$$

To make this rigorous, we pass from $\mathbb{R}$ to a larger field $\mathbb{C}$. As a set, we have

$$\mathbb{C} = \mathbb{R} \times \mathbb{R}$$

(the cartesian product), but we will find it convenient to write its elements as

$$a + ib := (a, b), \quad a, b \in \mathbb{R}.$$

One calls such a pair a complex number, with a its *real part* and b its *imaginary part.*

Note that at his point, the *imaginary unit* i doesn't have any particular 'meaning'; it is just a formal symbol – the complex number $a + ib$ is just the same thing as the element (a, b) in the plane.

We introduce addition and multiplication of complex numbers as follows:

$$(a + ib) + (c + id) = (a + b) + i(c + d),$$

$$(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc).$$

Loosely speaking, we add and multiply 'as if' i was an unknown number with $i^2 = -1$. We could have written teh complex numbers as pairs (a, b); the only reason for introducing i was to make the multiplication more intuitive.

These operations extend the addition and multiplication of $\mathbb{R}$, when the latter is identified with the subset of $\mathbb{C}$ consisting of elements of the form $a + i0 = (a, 0)$.

Elements of the form $0 + ia = (0, a) \in \mathbb{C}$ are called 'imaginary numbers', and one such element is the imaginary unit $i = 0 + i1 = (0, 1)$. This element satisfies

$$i^2 = -1$$

by construction. Of course, what makes the whole construction worthwhile is that $\mathbb{C}$ with these operations of addition and multiplication is a field, with neutral elements $0 = 0 + i0$ and $1 = 1 + i0$. The key fact is:

Lemma 1.1. *Every non-zero element of $\mathbb{C}$ has a multiplicative inverse.*

Proof. Consider $a + ib \in \mathbb{C}$ with $a, b \neq 0$. We have that

$$(a + ib)(a - ib) = a^2 + b^2 \neq 0.$$

Using this, it follows that

$$\frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}$$

is a multiplicative inverse to $a + ib$. □

Using this Lemma, one obtains,

Theorem 1.2. *$\mathbb{C} = \mathbb{R} \times \mathbb{R}$ is a field.*

The proof of the remaining field properties amounts to a direct calculation, which we leave as an exercise – you'll find it 'straightforward', but probably not very inspiring.

2. Pensive

Question: Which properties of the field $\mathbb{R}$ did we use in the construction of $\mathbb{C}$? Can we repeat this construction with *any* field F?

Answer: If we were to repeat the construction with $\mathbb{R}$ replaced by a more general field F, we will need to check the existence of multiplicative inverses. The formula for $(a+ib)^{-1}$, provided $a + ib \neq 0$, given in the Lemma does not work if there exists $(a, b) \neq (0, 0)$ with $a^2 + b^2 = 0$. If $a \neq 0$ (resp. $b \neq 0$), this can be written as $(a/b)^2 + 1 = 0$, resp. $(b/a)^2 + 1 = 0$.

So, the construction can be applied to F provided that the equation $x^2 + 1 = 0$ has no solution in F. In particular, we can *not* apply it to $\mathbb{C}$ (since $i^2 + 1 = 0$ in $\mathbb{C}$), to $\mathbb{Z}_2$ (since $1^2 + 1 = 0$ in $\mathbb{Z}_2$) or $\mathbb{Z}_5$ (since $2^2 + 1 = 0$ in $\mathbb{Z}_5$). But it works fine for $F = \mathbb{Z}_3,\ \mathbb{Z}_7,\ \mathbb{Z}_{11}$ and many other examples. So, we now have many new examples of finite fields (with $9,\ 49,\ 121,\ \ldots$ elements).

And what's so special about $x^2 + 1$? Nothing, really. While $x^2 + 1 = 0$ has solutions in $\mathbb{Z}_2$ and $\mathbb{Z}_5$, the equation $x^2 + x + 1 = 0$ does not. You can repeat the construction above by introducing a formal element j with $j^2 + j + 1 = 0$, and in this way get structures of fields on $\mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_5 \times \mathbb{Z}_5$ and some other examples.