8. Algebraic deficiencies of rationals

At first sight, the rationals appear to have most of the algebraic properties needed for daily operations with numbers. Indeed, they allow for addition, multiplication as well as the inverse operations of subtraction and division (by non-zero numbers). However, once other natural operations are introduced, problems arise.

Recall that (natural) powers are defined in any ordered field $(F, +, 0, \cdot, 1, \leqslant)$ recursively as

$$\forall b \in F\colon \quad b^0 := 1 \ \wedge \ \big(\forall n \in \mathbb{N}_F\colon b^{n+1} := b \cdot b^n\big) \tag{8.1}$$

With these in hand we can ask for solutions to polynomial equations such as

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{8.2}$$

for some natural $n \in \mathbb{N}_F$ and *coefficients* $a_0, \ldots, a_n \in F$, where we began to adopt the convention that the multiplication sign $\cdot$ can be omitted when no confusion arises. The simplest non-trivial case of (8.2) is arguably the quadratic equation

$$x^2 = a. \tag{8.3}$$

By the Pythagorean theorem, a positive x solving this equation gives the length of the hypothenuse in the right triangle whose legs-squared add up to a. (This remains relevant to present day: Builders use the right triangle with sides of lengths 3, 4 and 5 to check that walls meet in the corner at the right angle.)

Since the square of any number is non-negative (prove this from axioms of the field!), (8.3) has no solution for $a < 0$. However, a solution clearly exists for some positive $a \in \mathbb{Q}$, e.g., $a = 4$ or $a = \frac{4}{9}$. Unfortunately, as was noted already by ancient Greeks, there are also positive $a \in \mathbb{Q}$ for which (8.3) admits no rational solution:

Lemma 8.1 (Euclid) $\quad \forall x \in \mathbb{Q}\colon x^2 \neq 2$

Proof. Suppose, on the way to a contradiction, that there is $x \in \mathbb{Q}$ with $x^2 = 2$. Since x is rational, we have $x = \tilde{p}/\tilde{q}$ for some non-zero $\tilde{p}, \tilde{q} \in \mathbb{Z}$ (note that the square of zero is zero). Note that by multiplying both $\tilde{p}$ and $\tilde{q}$ by -1, we may achieve this with $\tilde{q} > 0$. Now take q to be the smallest number in

$$\big\{\tilde{q} \in \mathbb{N} \smallsetminus \{0\}\colon (\exists \tilde{p} \in \mathbb{Z}\colon \tilde{p} = x \cdot \tilde{q})\big\} \tag{8.4}$$

We checked a moment ago that this set is non-empty and so, by a homework problem, the minimal number exists. Then set $p := x \cdot q$.

From $x^2 = 2$ we then get $(p/q)^2 = 2$ and so $p^2 = 2q^2$. Since the square of and odd number is odd (prove this!), we get

$$p \text{ is even.} \tag{8.5}$$

But then there exists $r \in \mathbb{Z} \smallsetminus \{0\}$ such that $p = 2r$ and so $q^2 = 2r$. Hence we also get

$$q \text{ is even.} \tag{8.6}$$

But this contradicts our assumption that q is a minimal element in (8.4) because $q/2$ is a member of that set as well. Hence $x^2 = 2$ has no solution in $\mathbb{Q}$. □

The subsequent arguments in this section use the following definitions:

Definition 8.2 *Given non-zero integers $m, n \in \mathbb{Z}$, we say that "m divides n" with notation $m|n$ if $n/m \in \mathbb{Z}$. In short,*

$$m|n \;:=\; (\exists k \in \mathbb{Z}\colon\; n = k \cdot m) \tag{8.7}$$

Given $m, n \in \mathbb{Z} \setminus \{0\}$, the greatest common divisor *$gcd(m, n)$ of m and n is the largest natural that divides both m and n. For each $p \in \mathbb{N}$ we also define*

$$p \text{ is a prime } :=\; p \in \mathbb{N} \setminus \{0, 1\} \;\wedge\; \big(\forall q \in \mathbb{N} \setminus \{0, 1\}\colon q|p \Rightarrow q = p\big) \tag{8.8}$$

We will show that $\gcd(m, n)$ exists for all non-zero integers m and n later in this course and/or homework assignment.

Lemma 8.1 readily generalizes to $x^n = p$ having no rational solution for any $p \in \mathbb{N}$ prime and any $n \in \mathbb{N}$ different from 0 and 1. The mathematicians of middle ages (and even ancient Greeks, who knew of the right triangle with legs of unit length and the hypothenuse whose length is not a rational number) were quite aware of this problem and so they invented the notion of a *radical*. The idea is to introduce a new element into the existing number system that is defined as a solution of the polynomial equation $x^n = a$ for some a in the number system.

For instance, $\sqrt{2}$ is defined to be the positive number that solves the equation $x^2 = 2$, while $\sqrt[5]{7}$ is the number that solves $x^5 = 7$. The process can be iterated, which means that once $\sqrt{2}$ is already in our number system, we define $\sqrt{2 + \sqrt{2}}$ to be a positive solution to the equation $x^2 = 2 + \sqrt{2}$ which then resolves into $(x^2 - 2)^2 = 2$ and thus

$$x^4 - 4x^2 + 2 = 0. \tag{8.9}$$

A natural question is then: Which expressions involving radicals are rational and which are not? Some insight into this question is offered by:

Theorem 8.3 (Rational root test) *Suppose $x \in \mathbb{Q}$ solves*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \tag{8.10}$$

where $a_0, \ldots, a_n \in \mathbb{Z}$ and $a_0, a_n \neq 0$. Then

$$\exists p, q \in \mathbb{Z} \setminus \{0\}\colon \quad x = \frac{p}{q} \;\wedge\; \gcd(p, q) = 1 \;\wedge\; p|a_0 \;\wedge\; q|a_n \tag{8.11}$$

In words, x can be written as the ratio $\frac{p}{q}$ of two non-zero integers with no non-trivial common divisors such that p divides a_0 and q divides a_n.

Proof. Write x as p/q where $p, q \in \mathbb{Z}$ with $q > 0$ and $\gcd(p, q) = 1$. (Again, this is achieved by taking a representation with smallest positive q.) Since $a_0 \neq 0$ we have $x \neq 0$ and so $p \neq 0$. Substituting $x = p/q$ into (8.10) and multiplying the whole equation by q^n then yields

$$a_n p^n = -q\big[a_{n-1} p^{n-1} + a_{n-2} p^{n-2} q + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}\big] \tag{8.12}$$

The square bracket is an integer and so q divides $a_n p^n$. But the fact that $\gcd(p, q) = 1$ then forces $q|a_n$ as claimed. The proof that $p|a_0$ is similar and thus omitted. □

To demonstrate this on an example, the theorem implies that any rational solution to (8.9) is an integer that divides 2, which leaves $-2, -1, 1, 2$ as only possible candidates. As none of these solves (8.9), we conclude $\sqrt{2 + \sqrt{2}} \notin \mathbb{Q}$.

However, not all expressions involving radicals are necessarily non-rational: Obviously, $\sqrt{4}$ is rational but so is $\sqrt{7+2\sqrt{3}}-\sqrt{3}$ because

$$\sqrt{7+2\sqrt{3}}-\sqrt{3}=\sqrt{(2+\sqrt{3})^2}-\sqrt{3}=2+\sqrt{3}-\sqrt{3}=2. \tag{8.13}$$

While Theorem 8.3 is typically used to rule out rational roots, it in fact outputs a finite set of numbers as possible candidates for rational roots and so, if one of these solves (8.10), it gives us a rational root if one exists. However, using this for expressions as in (8.13) is not practical as the main point there is to show that the expression simplifies.

A formal way to add the radical $\sqrt{2}$ to the field of rationals is by introducing the set

$$\left\{a+b\sqrt{2}\colon\, a,b\in\mathbb{Q}\right\} \tag{8.14}$$

The addition on these is defined canonically

$$(a+b\sqrt{2})+(\tilde{a}+\tilde{b}\sqrt{2}):=(a+\tilde{a})+(b+\tilde{b})\sqrt{2}, \tag{8.15}$$

while multiplication is defined as

$$(a+b\sqrt{2})\cdot(\tilde{a}+\tilde{b}\sqrt{2}):=\left(a\cdot\tilde{a}+2\cdot b\cdot\tilde{b}\right)+(a\cdot\tilde{b}+\tilde{a}\cdot b)\sqrt{2}. \tag{8.16}$$

Writing $0+0\sqrt{2}$ for the zero element and $1+0\sqrt{2}$ for the unit element, we then check that the inverse to $a+b\sqrt{2}$ under addition is

$$-(a+b\sqrt{2})=-a+(-b)\sqrt{2} \tag{8.17}$$

while that under multiplication is

$$(a+b\sqrt{2})^{-1}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2} \tag{8.18}$$

where we noted that $\forall a,b\in\mathbb{Q}\colon\, a^2-2b^2\neq 0$ by Lemma 8.1. For convenience of expression, we also wrote rationals as fractions instead of invoking inverse elements. (Lemma 8.1 also guarantees that the representation of any element of (8.14) using two rationals a and b is unique.) We thus conclude that (8.14) is a field containing $\mathbb{Q}$. With some additional work, we can even give (8.14) the structure of an ordered field.

Formally, the field (8.14) can be regarded as a linear vector space over the field $\mathbb{Q}$ with basis $\{1,\sqrt{2}\}$. Thanks to (8.14) being also a field, the procedure can thus be iterated and other radicals gradually added. This leads to the formal description of a solution of polynomial equations "in radicals."

Definition 8.4 *Let $P(x)$ be a polynomial in x with rational coefficients. We say that the equation $P(x)=0$ admits a solution* in radicals *if there exists $m\in\mathbb{N}$ and fields $F_0,F_1,\ldots,F_m$ such that:*

(1) $F_0=\mathbb{Q}$

(2) $\forall i=0,\ldots,m-1\ \exists z\in F_{i+1}\ \exists a\in F_i\ \exists k\in\mathbb{N}\colon$

$$z^k=a\ \wedge\ F_{i+1}=\{b_0+b_1z+\cdots+b_{k-1}z^{k-1}\colon\, b_0,\ldots,b_{k-1}\in F_i\} \tag{8.19}$$

(3) $\exists x\in F_m\colon\, P(x)=0$

The reason why all powers less than k-th are listed on the right of (8.19) is that only then the set is closed under multiplication. Additional conditions are needed to ensure that the set in (8.19) is a field (e.g., if $z^j \in F_i$ for some $j < k$ then we may have $b_0 + b_1 z + \cdots + b_{k-1} z^{k-1} = 0$ without all $b_0, \ldots, b_{k-1}$ vanishing) but the statement does not care about these as we assume that F_{i+1} is a field to begin with.

Translating Definition 8.4 into more laymen terms, we are trying to find a sequence of symbols of the form $\sqrt[k]{a}$ — that is, solutions to equations of the kind $x^k = a$ — where a is expressed as a polynomial in all symbols obtained thus far, so that, when this process terminates, we are able to write a solution of the polynomial equation $P(x) = 0$ of interest. Or, even more simply, a solution in radicals is that which uses only a finite number of additions, multiplications (which includes subtractions and divisions, of course) and taking roots of any degree.

Besides the quadratic equation (the case $n = 2$ in (8.10)), a solution in radicals turns out to be possible for the *cubic* equation (the case $n = 3$ in (8.10)) and the *quartic* equation (the case $n = 4$ in (8.10)) thanks to the classical solutions due to L. Ferrari (quartic equation, solved in 1540) and G. Cardano (cubic equation, solved in 1545). Unfortunately, as shown by P. Ruffini in 1799 (in a somewhat controversial 100-page paper) and N.H. Abel in 1824 (in a 6-page paper), this fails for some quintic equations, e.g.,

$$x^5 - x - 1 = 0. \tag{8.20}$$

(Being a quintic, this equation does have at least one real root.) Soon after this (in 1830) E. Galois developed tools to determine whether a given polynomial equation admits a solution in radicals, thus founding what is now called Galois theory.

With the process of gradually adding radicals to rationals failing to describe the solutions to even some basic polynomial equations, we may try to take a more abstract approach and consider simply all numbers that (quite loosely) solve *some* polynomial equation (8.10) for *some* non-trivial integer coefficients. (We will need to define the reals first to make this precise.) Such numbers are called *algebraic*. Unfortunately, as it turns out, even these are not sufficient to give us important numbers such as π, or the Euler number e that are fundamental for analysis. It follows (and this is the punchline of this section) that we will have to approach the reals using different means than just algebra. This is what we will do next.