It follows from the lemma that the only possible rational solutions of the equation $u^3 - 2 = 0$ are $u = \pm 1$ or $u = \pm 2$, all four of which are quickly seen not to be solutions. Similarly, the only possible solutions of the second and third equations are $u = \pm 1$, which are also seen not to work. We may conclude that solutions to these three equations cannot be expressed by means of rational operations alone, but there remains the possibility that they can be expressed with the help of square roots.

Over the years, many people have tried their hand at problems **I** and **II**. For example, the much envied Casanova worked on doubling the cube and, even today, there are still many determined angle trisectors. However, in 1837, Pierre Wantzel (1814–1848) showed that none of $\sqrt[3]{2}$, $2\cos 20°$, and $2\cos(370°/7)$ can be expressed in terms of rational operations and square roots and, therefore, that problems **I**, **II** and **IV** cannot be solved by ruler and compass constructions.

To give a simple exposition of why this is so, we shall introduce a more modern concept, that of a field. For our purposes, a *field* is a set of numbers, real or complex, which contains the number 1 and which is closed under the rational operations. (There are other fields, but we shall not need them here.) In particular, the rationals form a field $\mathbf{Q}$ and so does $\mathbf{Q}[\sqrt{2}]$, the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational. More generally, if F is any field, then so is $F[\sqrt{c}]$, where c is a given element of F, by which we understand the set of all numbers of the form $a + b\sqrt{c}$ with $a, b \in F$.

It is clear that $F[\sqrt{c}]$ is closed under addition, subtraction and multiplication. To show that it is also closed under division, we assume that $\sqrt{c}$ is not in F, otherwise there would be nothing to prove, and that $a + b\sqrt{c} \neq 0$. We calculate

$$\frac{1}{a+b\sqrt{c}} = \frac{1}{a+b\sqrt{c}} \times \frac{a-b\sqrt{c}}{a-b\sqrt{c}} = \frac{a-b\sqrt{c}}{a^2-b^2c} = \frac{a}{a^2-b^2c} + \frac{-b}{a^2-b^2c}\sqrt{c},$$

which is again of the form $a' + b'\sqrt{c}$ with $a', b' \in F$. A small argument is necessary to check that $a^2 - b^2c \neq 0$.

We can now say that a real number u is constructible with ruler and compass, equivalently, expressible by rational operations and square roots, if and only if there exists a sequence of fields

$$\mathbf{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$$

such that $F_{k+1} = F_k[\sqrt{c_k}]$ with $c_k \in F_k$ and $u \in F_n$.

Proposition 15.2. *Suppose $f(x) = x^3 + a_2x^2 + a_1x + a_0$ is a cubic polynomial with coefficients in a field F. Suppose further that the equation $f(x) = 0$ has a solution in $F[\sqrt{c}]$ with $c \in F$. Then it already has a solution in F.*

Proof: Let $x_1 = a + b\sqrt{c}$ be the given solution with $a, b \in F$. Then

$(x_1 - a)^2 = b^2c$, hence $x_1^2 + px_1 + q = 0$ with $p, q \in F$. Dividing $f(x)$ by the polynomial $x^2 + px + q$, we obtain

$$f(x) = (x^2 + px + q)(x + d) + (ex + f),$$

where the quotient is $x + d$ with $d \in F$ and the remainder is $ex + f$ with $e, f \in F$. Since $f(x_1) = 0$ and $x_1^2 + px_1 + q = 0$, we deduce that $ex_1 + f = 0$. If $e \neq 0$, then $x_1 = -f/e \in F$ and we need look no further. If $e = 0$, then also $f = 0$, hence $x + d$ is a factor of $f(x)$. But then $f(-d) = 0$ and so $x_2 = -d \in F$ is the required solution.

Corollary 15.3. *If a number expressible by rational operations and square roots satisfies a cubic equation with rational coefficients, then this equation must have a rational solution.*

Proof: Suppose the cubic equation $f(x) = 0$ has no rational solution. Then, by Proposition 15.2 with $F = \mathbf{Q}$, it has no solution in $\mathbf{Q}[\sqrt{c_1}]$ with $c_1 \in \mathbf{Q}$. Again, by the Proposition with $F = \mathbf{Q}[\sqrt{c_1}]$, it has no solution in $\mathbf{Q}[\sqrt{c_1}][\sqrt{c_2}]$ with $c_2 \in \mathbf{Q}[\sqrt{c_1}]$. Continuing in this way, we see that it has no solution in $\mathbf{Q}[\sqrt{c_1}] \cdots [\sqrt{c_n}]$ for any n, where $c_k \in \mathbf{Q}[\sqrt{c_1}] \cdots [\sqrt{c_{k-1}}]$ for $1 < k \leq n$. Thus it has no solution expressible by rational operations and square roots.

Since the cubic equations

$$u^3 - 2 = 0, \quad u^3 - 3u - 1 = 0, \quad u^3 + u^2 - 2u - 1 = 0$$

have no rational solutions, as we verified earlier, we can now infer from Corollary 15.3 that they have no solutions expressible in terms of rational operations and square roots. In view of Chapter 14, we may therefore conclude that problems **I**, **II** and **IV** cannot be solved using only ruler and compass constructions. In summary:

Theorem 15.4. *It is impossible to double a cube, to trisect an arbitrary angle or to draw a regular heptagon by ruler and compass constructions.*

We have seen that the Greeks were able to draw regular polygons with 3 or 5 sides, but not with 7 sides. The question arises, for which primes p is it possible to construct a regular p-gon using ruler and compass only? Carl Friedrich Gauss showed that this is possible whenever p is a prime of the form $2^n + 1$ and Wantzel proved the converse. Gauss was so pleased with his discovery that he wanted a regular 17-gon inscribed on his tombstone. His request was not carried out, but a regular 17-gon was inscribed on a monument to Gauss in Braunschweig, Germany.

Odd prime numbers of the form $2^n + 1$ are called 'Fermat primes', after Pierre de Fermat (1601–1665). It is easy to prove that $2^n + 1$ cannot be prime unless n has the form 2^k.