2.4. Prove that if $\cos\alpha$ and $\cos\beta$ are constructible then so are $\cos(\alpha+\beta)$ and $\cos(\alpha-\beta)$.

2.5. Determine those integers k for which $\cos k^\circ = \cos(k\pi/180)$ is constructible.

2.6. Prove that if $\alpha+\beta+\gamma=\pi$ then

$$1-(\cos^2\alpha+\cos^2\beta+\cos^2\gamma)-2\cos\alpha\cos\beta\cos\gamma=0.$$

2.7. Let Δ be a triangle and let O denote the centre of the circumscribed circle of Δ. Suppose that the distances between O and the sides of Δ are 1, 2 and 3. Prove that the triangle Δ cannot be constructed using ruler and compass. (H)

3. Constructible regular polygons

The exact characterization of the constructible regular polygons was given by C. F. Gauss in a celebrated theorem proved in 1801. Gauss' theorem is rather surprising in that it gives a purely number theoretic answer to a purely geometric problem.

The numbers $F_i=2^{2^i}+1$ $(i=0,1,\ldots)$ are called *Fermat numbers*. The first five Fermat numbers, corresponding to $i=0,1,2,3,4$ are 3, 5, 17, 257 and 65537. Each of these numbers is prime. Based on this "evidence" Pierre Fermat conjectured (about 1640) that the numbers F_i are prime for every i. Fermat's conjecture was disproved by L. Euler in 1732: Euler discovered that 641 divides F_5 and thus F_5 is composite. The prime factorization of F_6 was found in 1880; it turned out that 274177 divides F_6. In 1970 it was shown that F_7 is the product of two primes consisting of 17 and 22 decimal digits, respectively. By now it is known that F_i is composite for every $5\leqslant i\leqslant 23$. Several other Fermat numbers were also examined, but no Fermat primes were found after F_4.

Gauss' theorem states that *the regular n-gon is constructible if and only if $n=2^k p_1\ldots p_m$, where $p_1,\ldots,p_m$ are different Fermat primes.*

Since 3 and 5 are Fermat primes, this implies that for $n=3,4,5,6,8$ and 10 the regular n-gon is constructible (this was known already by Euclid). On the other hand, 7 is not a Fermat prime, and thus the regular 7-gon is not constructible (as we proved in the previous section). Also, the prime factorization of 9 contains a power of an odd prime, therefore the regular 9-gon is not constructible either.

In this section we sketch the proof of the "only if" part of Gauss' theorem. The proof is based on the notions of algebraic number and degree.

The set of polynomials with rational coefficients will be denoted by $\mathbf{Q}[x]$. A complex number α is said to be *algebraic* if it is the root of a nonzero polynomial $p\in\mathbf{Q}[x]$. Among the degrees of all nonzero polynomials $f\in\mathbf{Q}[x]$ satisfying $f(\alpha)=0$ there is a minimal one. This minimal degree is called the *degree of the number* α.

For example, every rational number is algebraic of degree 1. The number $\sqrt{2}$ is algebraic of degree 2. The number $\sqrt[3]{2}$ is algebraic of degree 3 (prove it!).

The proof of Gauss' theorem is based on the following statement: *if a number is constructible then it is algebraic, and its degree is a power of* 2.

We shall prove this in the next section; for the time being let us take it for granted. We show that if p is an odd prime and if the regular p-gon is constructible then p must be a Fermat prime. Let $t=2\cos\frac{2\pi}{p}$. Then t is constructible and thus t is algebraic and its degree is a power of 2. Since $t=\varepsilon+\varepsilon^{-1}$ where $\varepsilon=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$, it follows that the degree of ε is also a power of 2 (the proof of this is also postponed to the next section; see Exercise 4.7). Now ε is a root of

$$\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\ldots+1,$$

and hence the degree of ε is at most $p-1$. It can be shown that the degree of ε is *exactly* $p-1$ (we omit the proof). Thus $p-1=2^j$ for some j, and $p=2^j+1$. Now, j must be a power of 2. Indeed, suppose that $d>1$ is an odd divisor of j. If $j=de$ and $2^e=a$ then

$$p=2^j+1=2^{de}+1=a^d+1=(a+1)(a^{d-1}-a^{d-2}+\ldots-d+1)$$

which is impossible, since p is prime. Hence $j=2^i$, and $p=2^{2^i}+1=F_i$ is a Fermat prime.

Next we show that if p is an odd prime then the regular p^2-gon is never constructible. Indeed, otherwise the degree of the algebraic number $t=2\cos\frac{2\pi}{p^2}$ would be a power of 2. Then the degree of

$$\eta=\cos\frac{2\pi}{p^2}+i\sin\frac{2\pi}{p^2}$$

would be a power of 2, as well. However, η is a root of

$$\frac{x^{p^2}-1}{x^p-1}=x^{p(p-1)}+x^{p(p-2)}+\ldots+1,$$

and it can be shown that the degree of η is exactly $p(p-1)$. Since $p(p-1)$ cannot be a power of 2, this is a contradiction.

Now suppose that the regular n-gon is constructible. If d is a divisor of n then the regular d-gon is also constructible, since a suitable subset of the vertices of the n-gon forms a regular d-gon. This implies that if p is an odd prime divisor of n then the regular p-gon is constructible and thus p must be a Fermat prime. Also, n cannot have a divisor of the form p^2 where p is an odd prime, since the regular p^2-gon is not constructible. Therefore the prime decomposition of n must be of the form $n=2^k p_1\ldots p_m$, where $p_1,\ldots,p_m$ are different Fermat primes. This concludes the proof of the "only if" part of Gauss' theorem.

Exercises

3.1. Prove that for $i\geqslant 2$, F_i is not the sum of two primes.

3.2. Prove that for every $i\geqslant 2$ the last digit of F_i is 7.

3.3. Prove that if $F_i=p^m$ where p is a prime then $m=1$.

3.4. Determine those primes that are smaller than 10^6 and can be written in the form n^n+1 where n is a positive integer.

3.5. Prove that $2^{2^i}+3$ is composite for infinitely many i. (H)

3.6. Prove that $\sqrt{2}+\sqrt{3}$ is an algebraic number of degree 4.

3.7. Prove that if α is an algebraic number of degree n then (each value of) $\sqrt{\alpha}$ is an algebraic number of degree at most $2n$. Is it true that the degree of $\sqrt{\alpha}$ is exactly $2n$?

3.8. Prove that if α is an algebraic number of degree n then α^2 is an algebraic number of degree at most n. Is it true that the degree of α^2 is exactly n?

4. Some basic facts on linear spaces and fields

An expression of the form $c_1x_1+\ldots+c_nx_n$ is called a *linear combination* of the numbers $x_1,\ldots,x_n$ with coefficients $c_1,\ldots,c_n$.

Let $F\subset\mathbf{C}$ be a field. The set $V\subset\mathbf{C}$ is called a *linear space (or vector space) over F,* if every linear combination of elements of V with coefficients from F belongs to V.

A subset $G\subset V$ is said to be a *generating system of V,* if every element of V can be obtained as a linear combination of elements of G with coefficients from F.

The elements of a subset $H\subset V$ are said to be *linearly independent,* if whenever $x_1,\ldots,x_n$ are different elements of H, $t_1,\ldots,t_n\in F$ and $t_1x_1+\ldots+t_nx_n=0$, then necessarily $t_1=\ldots=t_n=0$.

As an illustration of these notions consider the set $V=\mathbf{Q}(\sqrt{2})$. It is clear that V is a linear space over $\mathbf{Q}$. Each of the sets $\{1,2,\sqrt{2}+5\}$, $\{1+\sqrt{2},1-3\sqrt{2}\}$, $\{1,\sqrt{2}\}$ is a generating system of V. In every linear space any one-element set consisting of a nonzero number is linearly independent. In $\mathbf{Q}(\sqrt{2})$ the set $\{1,\sqrt{2}\}$ consists of linearly independent elements, while $\{1,2,\sqrt{2}+5\}$ does not.

The following basic fact is sometimes called the fundamental theorem of linear algebra. We shall accept it without proof.

In every linear space, the cardinality of any generating system is not less than the cardinality of any set of linearly independent elements.

If a set is a generating system and, at the same time, it consists of linearly independent elements, then it is called a *basis.* It is easy to see that a set B is a basis of the linear space V over F if and only if every element of V can be written uniquely as the linear combination of elements of B with coefficients from F.

One can prove that *every linear space has a basis.* Moreover, *every set of linearly independent elements is contained in a basis.* It follows from the fundamental theorem that *in every linear space V the cardinality of any two bases is the same.* This common cardinality is called the *dimension* of the linear space V. The space is called *finite dimensional* if its dimension is finite (that is, if it has a finite basis).

Let F be a field. A field K is called an *extension of F* if $F\subset K$. In this case K is a linear space over F (why?). The dimension of this linear space is called the *degree* of the extension $F\subset K$ and is denoted by $[K:F]$. The extension $F\subset K$ is called *finite* if $[K:F]$ is finite.

For example, let $a\in F$ be a positive real number such that $\sqrt{a}\notin F$. Let $K=F(\sqrt{a})$. Then the set $\{1,\sqrt{a}\}$ is a generating system of K and consists of linearly independent elements. Therefore it is a basis, and thus the dimension of K over F is two. In other words, $F(\sqrt{a})$ is a finite extension of F and $[F(\sqrt{a}):F]=2$.

The notion of $F(\sqrt{a})$ can be generalized as follows. Let F be a field and let α be an arbitrary complex number. If a field K contains both F and α then K must also contain every number of the form

$$\frac{a_n\alpha^n+\ldots+a_1\alpha+a_0}{b_k\alpha^k+\ldots+b_1\alpha+b_0}\qquad(a_0,\ldots,a_n,b_0,\ldots,b_k\in F).\tag{1}$$

It is clear that the set of numbers listed in (1) forms a field and therefore it is the smallest field that contains both F and α. We shall denote this field by $F(\alpha)$. Note that this notation is in accordance with the earlier definition of $F(\sqrt{a})$. That is, if $a\in F$ is a positive real number and $\alpha=\sqrt{a}$ then the field $F(\sqrt{a})$ coincides with the new notion of $F(\alpha)$. The fact that $[\mathbf{Q}(\sqrt{2}):\mathbf{Q}]=2$ is a special case of the following theorem.

If α is algebraic then $\mathbf{Q}(\alpha)$ is a finite extension of $\mathbf{Q}$, and $[\mathbf{Q}(\alpha):\mathbf{Q}]$ equals the degree of α.

Proof. Let n denote the degree of α, and put

$$F=\{r_{n-1}\alpha^{n-1}+\ldots+r_1\alpha+r_0:r_i\in\mathbf{Q}\ (i=0,\ldots,n-1)\}.$$

Then F is a linear space over $\mathbf{Q}$, and the set $\{1,\alpha,\ldots,\alpha^{n-1}\}$ is a generating system of F. These elements are linearly independent over $\mathbf{Q}$, since otherwise there would be a polynomial $q\in\mathbf{Q}[x]$ of degree $\leqslant n-1$ such that $q(\alpha)=0$. This, however, would contradict the fact that the degree of α is n. Therefore F has a basis of n elements; that is, the dimension of F is n.

It is clear that $F\subset\mathbf{Q}(\alpha)$. We shall prove that F is a field. Since $\mathbf{Q}(\alpha)$ is the smallest field containing α, this will prove $\mathbf{Q}(\alpha)=F$ and $[\mathbf{Q}(\alpha):\mathbf{Q}]=n$.

Obviously, the sum and difference of elements of F also belong to F. In order to prove that the product of two elements of F also belongs to F it is enough to show that $\alpha^k\in F$ for every $k=0,1,\ldots$. We shall prove this by induction on k. The statement is obviously true if $k\leqslant n-1$. Let $k\geqslant n$, and suppose that $1,\alpha,\ldots,\alpha^{k-1}\in F$. Let $p(x)=x^n+c_{n-1}x^{n-1}+\ldots+c_1x+c_0$ be a polynomial with rational coefficients such that $p(\alpha)=0$. Then $\alpha^{k-n}p(\alpha)=0$, and thus

$$\alpha^k=-c_{n-1}\alpha^{k-1}-\ldots-c_1\alpha^{k-n+1}-c_0\alpha^{k-n}.$$

Since $\alpha^i\in F$ for every $i<k$, it follows that the right hand side belongs to F. Thus $\alpha^k\in F$ for every k, and hence F is closed under multiplication.

Finally, we have to prove that if $\beta \in F$ and $\beta \neq 0$ then $1/\beta \in F$. Every element of F is of the form $f(\alpha)$, where $f \in \mathbf{Q}[x]$ and the degree of f is less than n. (Recall that $\mathbf{Q}[x]$ denotes the set of polynomials with rational coefficients.) Let $\deg f$ denote the degree of the polynomial f. We have to show that if $f \in \mathbf{Q}[x]$, $\deg f < n$, and $f(\alpha) \neq 0$, then $1/f(\alpha) \in F$. We shall prove this statement by induction on $\deg f$. If $\deg f = 0$ then f is a non-zero rational constant, and thus $1/f(\alpha) \in \mathbf{Q} \subset F$.

Suppose that $\deg f = k$ where $0 < k < n$, and that the statement is true for every polynomial $g \in \mathbf{Q}[x]$ of degree $< k$. Applying the division algorithm to the polynomials p and f we obtain that $p = q \cdot f + r$, where $q, r \in \mathbf{Q}[x]$ and $\deg r < k$. Since $\deg p = n > k$, we have $q \neq 0$. Also, $k > 0$ implies $\deg q < n$. Therefore $q(\alpha) \neq 0$, since otherwise the degree of α would be less than n.

We have $r(\alpha) = p(\alpha) - q(\alpha) \cdot f(\alpha) = -q(\alpha) \cdot f(\alpha) \neq 0$. Then, by the induction hypothesis, $1/r(\alpha) \in F$. Since F is closed under multiplication, this gives

$$1/f(\alpha) = -q(\alpha) \cdot (1/r(\alpha)) \in F,$$

and the proof is complete.

The connection between algebraic numbers and finite extensions of $\mathbf{Q}$ is given by the following theorem: *a number is algebraic if and only if it is contained in a finite extension of* $\mathbf{Q}$.

The "only if" part is immediate from the previous theorem: if α is algebraic then α is contained in $\mathbf{Q}(\alpha)$ which is a finite extension of $\mathbf{Q}$. To prove the other direction, let F be a finite extension of $\mathbf{Q}$ with $[F : \mathbf{Q}] = n$. Then any system of linearly independent elements of F consists of at most n elements. Hence, for every $\alpha \in F$, the $n+1$ elements $1, \alpha, \ldots, \alpha^n$ cannot be linearly independent. This means that there are rational numbers $c_0, \ldots, c_n$ such that not all of them are zero and $c_n\alpha^n + \ldots + c_1\alpha + c_0 = 0$. Then α is algebraic, and this is what we wanted to show.

We shall need the following theorem on the multiplication of degrees.

If $F \subset K$ and $K \subset L$ are finite field extensions, then $F \subset L$ is also a finite extension and $[L : F] = [K : F] \cdot [L : K]$.

Indeed, let $[K : F] = n$ and let $\{a_1, \ldots, a_n\}$ be a basis of K over F. Let $[L : K] = m$ and $\{b_1, \ldots, b_m\}$ be a basis of L over K. Then it is easy to check that

$$\{a_i b_j : i = 1, \ldots, n,\ j = 1, \ldots, m\}$$

is a basis of L over F, and thus $[L : F] = nm$.

This theorem implies that *if K is a finite extension of* $\mathbf{Q}$ *then the degree of every element of K divides* $[K : \mathbf{Q}]$.

Indeed, let n be the degree of an element $\alpha \in K$. Then $\mathbf{Q}(\alpha) \subset K$ and $[\mathbf{Q}(\alpha) : \mathbf{Q}] = n$. Since $[K : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}] \cdot [K : \mathbf{Q}(\alpha)] = n \cdot [K : \mathbf{Q}(\alpha)]$, we can see that n is a divisor of $[K : \mathbf{Q}]$.

Now we turn to constructible numbers and constructions. We prove Gauss' result used in the previous section: *every constructible number is algebraic and its degree is a power of two.*

Let t be a constructible number. We proved that there is a sequence of fields $F_0 = \mathbf{Q} \subset \ldots \subset F_m$ such that $t \in F_m$, and for every $k = 1, \ldots, m$ there is a positive number $a_{k-1} \in F_{k-1}$ such that $F_k = F_{k-1}(\sqrt{a_{k-1}})$. Clearly, for every k the degree $[F_k : F_{k-1}]$ equals either 1 or 2 (it is 1 if $F_k = F_{k-1}$). Thus F_m is a finite extension of $\mathbf{Q}$ and its degree equals the product of the degrees $[F_k : F_{k-1}]$ $(k = 1, \ldots, m)$. Consequently, $[F_m : \mathbf{Q}]$ is a power of 2. Therefore $t \in F_m$ is algebraic, and also its degree, as a divisor of $[F_m : \mathbf{Q}]$, is a power of 2.

Exercises

4.1. Prove that 1, $\sqrt{2}$ and $\sqrt[3]{2}$ are linearly independent over $\mathbf{Q}$.

4.2. Prove that if $p_1, \ldots, p_n$ are distinct primes then 1, $\sqrt{p_1}, \ldots, \sqrt{p_n}$ are linearly independent over $\mathbf{Q}$. (H)

4.3. Let $a_1, \ldots, a_k$ be positive rational numbers. What is the necessary and sufficient condition of the linear independence of $\sqrt{a_1}, \ldots, \sqrt{a_k}$ over $\mathbf{Q}$? (H)

4.4. Let $F \subset K$ be fields and let $V \neq \{0\}$ be a linear space over K. Prove that if the dimension of V as a linear space over F is finite then K is a finite extension of F. Show that the dimension of V as a linear space over F equals the dimension of V as a linear space over K multiplied by $[K : F]$.

4.5. Let V be a finite dimensional linear space over $\mathbf{Q}$ such that $x, y \in V$ implies $xy \in V$. Prove that V is a field.

4.6. Let α be an algebraic number of degree n. Prove that the degree of α^2 is a divisor of n and the degree of $\sqrt{\alpha}$ is a divisor of $2n$.

4.7. Let t and ε be complex numbers such that $t = \varepsilon + \varepsilon^{-1}$. Prove that if t is an algebraic number of degree n then ε is also algebraic and its degree divides $2n$. If, in particular, n is a power of two then the degree of ε is also a power of two.