1.A. The field of complex numbers

A complex number z is expressed by $x + iy$ where (x, y) is a point in $\mathbf{R}^2$. This identifies the complex plane $\mathbf{C}$ with $\mathbf{R}^2$. When $z = x + iy$ we set

$$\mathfrak{Re}(z) = x \quad : \mathfrak{Im}(z) = y$$

and refer to x as the real part and y as the imaginary part of z. The sum of two complex numbers is defined by

(i) $$z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$$

Complex multiplication is defined by:

(ii) $$(x_1 + iy_1)(x_2 + iy_2) = (x_1x_1 - y_1y_2) + i(x_1y_2 + ix_2y_1)$$

One verifies that the product satisfies the associative law. If $z = x + iy$ its multiplicative inverse becomes

(*) $$z^{-1} = \frac{x - iy}{x^2 + y^2}\,.$$

1.1 Conjugation and absolute value. If $z = x + iy$ its complex conjugate is $x - iy$ and denoted by $\bar{z}$. The absolute value of z is defined as $\sqrt{x^2 + y^2}$ and denoted by $|z|$. The map $z \mapsto \bar{z}$ corresponds to reflection of plane vectors with respect to the x-axis and (*) gives

(**) $$z^{-1} = \frac{\bar{z}}{|z|^2}$$

1.2. The complex argument. In $\mathbf{R}^2$ we have polar coordinates (r, ϕ). If z is non-zero we write:

(1.2) $$z = r \cdot \cos\phi + i \cdot r \cdot \sin\phi \quad : \quad r = |z|\,.$$

The angle ϕ is denoted by $\arg(z)$ and called the argument of z. Since trigonometric functions are periodic, $\arg(z)$ is determined up to an integer multiple of 2π. Specific choices of $\arg(z)$ appear in different situations. As an example we consider the upper half-plane $\mathfrak{Im}(z) > 0$ where one usually takes $0 < \phi < \pi$ for $\arg(z)$. In the right half plane $\mathfrak{Re}(z) > 0$ one takes $-\pi/2 < \phi < \pi/2$. Another case occurs when we consider the polar representation of complex numbers z outside the *negative* real axis $(-\infty, 0]$. Then every z has a unique polar representation in (1.2) with $-\pi < \phi < \pi$.

1.3. The complex number $e^{i\phi}$. This is complex number has absolute value one and argument ϕ. Thus

(1.3) $$e^{i\phi} = \cos\phi + i \cdot r\sin\phi\,,$$

where e as *Neper's constant* defined by

$$e = \lim_{n\to\infty} (1 + \frac{1}{n})^n$$

The notation (1.3) comes from the Taylor series expansions of the sine- and the cosine functions. Recall from *Calculus* that

(i) $$\sin\phi = \sum_{\nu=0}^{\infty} (-1)^\nu \cdot \frac{\phi^{2\nu+1}}{(2\nu+1)!} \quad : \quad \cos\phi = \sum_{\nu=0}^{\infty} (-1)^\nu \cdot \frac{\phi^{2\nu}}{(2\nu!)}$$

Adding these series and using that $i^2 = -1$ which gives $i^4 = 1$ and so on, we get:

(ii) $$\cos\phi + i \cdot \sin\phi = \sum_{\nu=0}^{\infty} \frac{i\phi)^\nu}{\nu\,!}$$

The last series resembles the series of the real exponential function from *Calculus*:

(iii) $$e^x = \sum_{\nu=0}^{\infty} \frac{x^\nu}{\nu\,!} \quad : \quad x \in \mathbf{R}$$

1.4 Addition formula for arg(z). From Euclidian geometry one has addition formulas for the sine-and the cosine functions:

$$\sin(\phi_1+\phi_2)=\sin(\phi_1)\cos(\phi_2)+\sin(\phi_2)\cos(\phi_1) \tag{1}$$

$$\cos(\phi_1+\phi_2)=\cos(\phi_1)\cos(\phi_2)-\sin(\phi_1)\sin(\phi_2) \tag{2}$$

Since (1) and (2) are very essential results in complex analysis we recall the proof. Let Δ be a triangle with angles α,β,γ where and A,B,C denote the opposed sides and consider the case when both α and β are $<\pi/2$. Now $\sin\gamma=\sin(\pi-\alpha-\beta)=\sin(\alpha+\beta)$ and the sine-theorem in euclidian geometry gives:

$$\frac{\sin\alpha}{A}=\frac{\sin\beta}{B}=\frac{\sin\gamma}{C} \tag{i}$$

Draw the normal line from the corner where the angle which hits the opposed side at a point whose distance to the α-corner is x. So then $C-x$ is the distance to the β-corner. Looking at a figure the reader can recognize that

$$\cos\alpha=\frac{x}{B}\quad \cos\beta=\frac{C-x}{A}\implies A\cdot\cos\beta+B\cdot\cos\alpha+=C \tag{ii}$$

Together with (i) we get

$$\sin(\alpha+\beta)=\frac{C}{A}\sin\alpha=\sin\alpha\cdot\cos\beta+\sin\alpha\cdot\frac{B}{A}\cos\alpha$$

Finally, the first equality in (i) gives $\sin\alpha\cdot\frac{B}{A}\cos\alpha=\sin\beta\cdot\cos\alpha$ and the requested addition formula for the sine-function follows. A similar proof gives the addition formula for the cosine-function.

Next, the construction of complex multiplication and (1.3) yields the equality

$$r_1\cdot e^{\phi_1}\cdot r_2\cdot e^{\phi_2}=r_1r_2\cdot e^{\phi_1+\phi_2}$$

for all pairs of positive numbers r_1,r_2 and a pair of ϕ-angles. So when complex arguments are identified up to integer multiples of 2π we get:

$$\arg(z_1)+\arg(z_2)=\arg(z_1z_2) \tag{3}$$

for each pair of non-zero complex numbers. By an induction over k the following hold for every k-tuple of complex numbers:

$$\sum_{\nu=1}^{\nu=k}\arg(z_\nu)=\arg(\prod_{\nu=1}^{\nu=k}z_\nu)\,. \tag{*}$$

We refer to (*) as the addition formula for the argument function. It plays a fundamental role in complex analysis.

1.5 Associated matrices. Let $z=a+ib$ be a complex number. Identifying $\mathbf{C}$ with $\mathbf{R}^2$ the complex multiplication with z yields a linear operator represented by a matrix. More precisely, the euclidian basis vectors e_1,e_2 correspond to the complex numbers 1 and i. Since $z\cdot i=ia-b$ the 2×2-matrix M_z associated to multiplication with z becomes

$$M_z=\begin{pmatrix}a & -b\\ b & a\end{pmatrix}$$

Notice that the determinant of M_z is a^2+b^2 and the inversion formula (*) from 1.1 corresponds to the matrix identity

$$M_z^{-1}=\frac{1}{a^2+b^2}\cdot\begin{pmatrix}a & b\\ -b & a\end{pmatrix}$$

1.6 A polynomial approximation. With $0\leq\phi\leq 2\pi$ we consider the ϕ-polynomials

$$P_n(\phi)=\big(1+\frac{i\phi}{n}\big)^n \tag{i}$$

Notice that

$$\arg(1+\frac{i\phi}{n}) = \frac{\phi}{n}$$

The addition formula (*) in 1.4 therefore gives

$$\arg(P_n(\phi)) = \phi$$

for every n. Next, regarding absolute values we have

$$|1+\frac{i\phi}{n}|^2 = 1+\frac{\phi^2}{n^2} \implies |(P_n(\phi)|^2 = \big(1+\frac{\phi^2}{n^2}\big)^n$$

Recall from calculus that $\log(1+t) \leq t$ for each real $t > 0$. With $0 \leq \phi \leq 2\pi$ it follows that

$$\log|P_n(\phi)|^2 \leq \frac{\phi^2}{n} \leq \frac{4\pi^2}{n}$$

It follows that

$$\lim_{n\to\infty} |P_n(\phi)| = 1$$

holds uniformly on $[0, 2\pi]$ and the reader may also notice that Neper's limit formula for e entails that

$$\lim_{n\to\infty} P_n(\phi) = e^{i\phi}$$

Remark. The function $\phi \mapsto e^{i\phi}$ is 2π-periodic which entails that

$$\lim_{n\to\infty} (1+\frac{2\pi i}{n})^n = 1$$

It is instructive to check this limit formula numerically with a computer for some relatively large values of n. Notice also that the periodicity gives the following limit formula for every integer k:

$$\lim_{n\to\infty} \big(1+\frac{(2k+1)\pi i}{n}\big)^n = -1$$

1.7 Complex numbers and geometry. Many results in euclidian geometry can be proved in a neat fashion by complex numbers. Let us give an example. Consider a triangle Δ with sides of length a, b, c. Let α be the angle at the corner p point opposed to the side of length a. Then

$$(*) \qquad \cos\alpha = \frac{b^2+c^2-a^2}{2bc}$$

To prove this we may without loss of generality assume that the corner point p is the origin and the two other corner points of Δ are represented by a pair of complex vectors z and w. Here

$$a^2 = |z-w|^2 \quad : |z|^2 = b^2 \quad : |w|^2 = c^2$$

The formula (*) is invariant under dilation with z replaced by rz and w by rw for some r, and also under a rotation. So without loss of generality we can take $w = 1$ and $z = x+iy$ with $x > 0$. In this case a figure - or rather the definition of the cosine-function gives

$$\cos\alpha = \frac{x}{|z|}$$

So (*) amounts to prove the equation

$$(i) \qquad \frac{x}{|z|} = \frac{|z|^2+1-|1-z|^2}{2|z|}$$

Above $|z|$ is cancelled and we have

$$|z|^2+1-|1-z|^2 = x^2+y^2+1-(y^2+(1-x)^2) = 2x$$

which gives (i) and (*) follows. This illustrates how complex numbers provide an efficient tool to establish geometric formulas.

Exercise. Let Δ be a triangle with corner points at the origin, $(1,0)$ and $z_0 = x_0+iy_0$ where $|z| \leq \sqrt{2}$ and both x_0 and y_0 are positive. The line ℓ passing $(1,0)$ which is $\perp$ to the vector z_0 consists of complex numbers of the form $1+\mathbf{R}\cdot iz_0$ where we use that the vectors z_0 and $i\cdot z_0$

are $\perp$ to each other. The normal from the corner point z_0 stays on the line $\{x = x_0\}$ and to get the intersection point of ℓ and this normal we seek a real number a such that

$$x_0 = 1 + ai(x_0 + iy_0) \implies a = \frac{1 - x_0}{y_0} \tag{i}$$

Hence the intersection point becomes $(x_0 + iy_*$ where (i) gives

$$y_* = x_0 \cdot \frac{1 - x_0}{y_0} \tag{ii}$$

Next, we draw the line from the origin passing (x_0, y_*) and it turns out that it is $\perp$ to the vector $1 - z_0$. This amounts to show that there exists a *real* number b such that

$$x_0 + iy_* = bi(1 - z_0) = by_0 + ib(1 - x_0) \tag{iii}$$

But this is clear from (ii) which shows that (iii) holds with $b = \frac{x_0}{y_0}$. So these complex computations verify the wellknown fact that the three normals intersect at a point.

B. The fundamental theorem of algebra.

Introduction. The proof of Theorem B.2 below was given by Cauchy in 1815 based upon the analytic result that the absolute value of a complex-valued continuous function on a compact disc achieves its minimum some point. In the article [Weierstrass] from 1868 Weierstrass gave another proof. Here follows a citation from the introduction in [ibid]: *Obgleich wir gegenwärtig von dem in Rede stehenden Fundamentaltheoreme der Algebra eine Reihe strengen Beweise besitzen, so dürfte doch die Mitteilung der nachstehenden Begründung desselben, deren Eigenthümlichkeit hauptsächlich darin besteht, dass sie ohne Heranziehung von Hilfsmitteln und begriffen die der Algebra fremd sind, rein arithmetisch durchgeführt wird, vielen Mathematikern nicht unwillkommen sein.* So Weierstrass points out that in spite of the already known existence proofs, a procedure which is not too remote from algebra derives the fundamental theorem of algebra by arithematical methods, a fact that might be appreciated by many mathematicians. The merit in [ibid] is that it gives a method to get numerical approximations of roots to a polynomial

(*) $\qquad P(z) = z^n + c_{n-1}z^{n-1} + \ldots + c_1 z + c_0 \quad : \quad c_0, \ldots, c_{n-1}$ are complex numbers

of some degree $n \geq 2$. To begin with Weierstrass made the observation that the fundamental theorem of algebra amounts to show that for an arbitrary n-tuple $c_0, c_1, \ldots, c_{n-1}$ expressing P by (*) there exists a unique unordered n-tuple of complex numbers $\alpha_1, \ldots, \alpha_n$ such that

$$P(z) = \prod_{\nu=1}^{\nu=n} (z - \alpha_\nu)$$

In other words the mapping of unordered n-tuples of α-numbers to their associated symmetric polynomials is injective and the range is equal to all ordered complex n-tuples $c_0, c_1, \ldots, c_{n-1}$. Or equivalently, for each n-tuple of complex numbers $w_1, \ldots, w_n$ there exists a unique unordered n-tuple $\{\alpha_\nu\}$ such that

$$\sum_{\nu=1}^{\nu=n} \alpha_\nu^k = w_k \quad : 1 \leq k \leq n$$

Above the polynomial $P(z)$ in (*) has simple zeros if and only if the ideal generated by $P(z)$ and its derivative $P'(z)$ is equal to $\mathbf{C}[z]$, i.e. there exists a unique pair of polynomials A, B such that

(i) $$1 = A(z)P(z) + B(z)P'(z)$$

where $\deg A \leq n-2$. The existence of such a pair A, B is equivalent to the existence of a solution of a linear system of equations in $2n-1$ many indeterminates corresponding to coefficients of A and B. Cramer's rule gives a criterion for the existence of a solution which expressed by an algebraic equation

$$\mathcal{D}_n(c_0, \ldots, c_{n-1}) = 0$$

where $\mathcal{D}_n$ is a polynomial in n variables with integer coefficients. We leave it as an exercise to find $\mathcal{D}_n$, if necessary a text-book in algebra can be consulted. Starting with an n-tuple $\{c_\nu\}$ where the (i) has a solution, Weierstrass demonstrates that that for each $\epsilon > 0$ there exists a finite number of arithmetical operations which give an unordered n-tuple of complex numbers $a_1, \ldots, a_n$ determined by the given c-coefficients such that if

$$Q(z) = \prod_{\nu=1}^{\nu=n} (z - a_\nu) = z^n + \sum c_\nu^* z^\nu$$

then $|c_\nu - c_\nu^*| < \epsilon$ for each $0 \leq \nu \leq n-1$. Next, starting with a sufficiently small ϵ Weierstrass proved that the roots of the Q-polynomial approximate the true roots of P by recursive formulas. More precisely, set

$$a_\nu^{(1)} = a_\nu - \frac{P(a_\nu)}{\prod_{j \neq \nu}(a_\nu - a_j)}$$

Inductively we put:

$$a_\nu^{(k+1)} = a_\nu - \frac{P(a_\nu^{(k)})}{\prod_{j \neq \nu}(a_\nu^{(k)} - a_j^{k)})}$$

Then it is proved in [ibid] that the true roots of P are given by

$$a_\nu^* = \lim_{k\to\infty} a_\nu^{(k)}$$

Moreover, the rate of convergence is rapid in the sense that there is a constant C which depends on P and the choice of ϵ such that

$$|a_\nu^* - a_\nu^{(k)}| \leq C \cdot 2^{-k} \quad \text{for every} \quad 1 \leq \nu \leq n$$

Weierstrass' constructions can be implemented into a computer which leads to to approximations of zeros polynomials with high accuracy. So readers interested in numerical investigations should consult the rich material in [Weierstrass].

Cauchy's proof. Here we admit the existence of extremal values taken by continuous functions on compact sets. Let $P(z)$ be given in (*). If P has a zero α one gets a factorisation

$$P(z) = (z-\alpha)(z^{n-1} + d_{n-2}z^{n-2} + \ldots + d_1 z + d_0)$$

where the d-coefficients are found by algebraic identities. One has for example

$$d_{n-2} = c_{n-1} - \alpha \quad : \quad d_{n-3} = c_{n-2} - \alpha d_{n-2}$$

and so on. If the factor polynomial of degree $n-1$ also has a complex root we can continue and conclude

Proposition. *Assume that every polynomial $P(z)$ has at least one complex root. Then it has a factorisation*

$$P(z) = \prod_{\nu=1}^{\nu=k} (z - \alpha_\nu)$$

Here k is the degree of P and $\alpha_1, \ldots, \alpha_k$ is a k-tuple of complex numbers where repetitions occur when P has multiple roots.

Hence the fundamental theorem of algebra follows if we have proved:

B.1 Theorem *Every polynomial $P(z)$ has at least one root.*

Remark. The proof below relies upon the fact that absolute values of complex polynomials cannot achieve local minima. Consider as an example some integer $k \geq 2$ and the function

$$g(z) = |1 + z^k|^2$$

Here $g(0) = 1$ but $z = 0$ is not a minimum for with a small $\epsilon > 0$ we can take $z = \epsilon \cdot e^{\pi i/k}$ which gives $z^k = \epsilon^k$ and hence

$$g(\epsilon \cdot e^{\pi i/k}) = (1 - \epsilon^k)^2 < 1$$

Notice the contrast to arbitrary real polynomials where a minimum can occur. For example, the polynomial $g(x,y) = 1 + x^4 + x^2y^2 + y^4$ has a minimum at the origin and no zeros in the (x,y)-plane.

Proof of Theorem B.1: We are given $P(z)$ as in (*) above and put $M = |c_0| + \ldots + |c_{k-1}|$. If $|z| \geq 1$ the triangle inequality gives

(i) $$|P(z)| \geq |z|^k - M \cdot |z|^{k-1} \geq |z| - M$$

With $R = M + 2 \cdot |c_0|$ it follows that

(ii) $$|z| \geq R \implies |P(z)| \geq R - M \geq 2 \cdot |c_0| = 2 \cdot |P(0)|$$

Next, the restriction of $P(z)$ to the closed disc $|z| \leq R$ is a continuous function and therefore the absolute value takes a minimum at some point z_0 which in particular gives $|P(z_0)| \leq |P(0)|$. Hence (ii) implies that we have a global minimum, i.e.

(iii) $$|P(z_0)| \leq |P(z)|$$

hold for all z. To show that (iii) entails $P(z_0) = 0$ we argue by contradiction, i.e suppose that $P(z_0) \neq 0$ and with a new variable ζ we get the polynomial

$$P(z_0 + \zeta) = P(z_0) + d_m\zeta^m + d_{m+1}\zeta^{m+1} + \ldots + d_k\zeta^k \tag{iv}$$

where $1 \leq m \leq k$ and $d_m \neq 0$. We find real numbers α, β such that

$$P(z_0) = |P(z_0)|e^{i\alpha} \quad \text{and} \quad d_m = |d_m|e^{i\beta} \tag{v}$$

Next, with $\epsilon > 0$ we set

$$\zeta = \epsilon \cdot e^{i\cdot \frac{\pi+\alpha-\beta}{m}} \tag{vi}$$

Since $e^{i\pi} = -1$ this choice of ζ together with (v) gives

$$P(z_0) + d_m\zeta^m = (1 - |d_m| \cdot \epsilon^m)P(z_0) \tag{vi}$$

Put $M^* = |d_{m+1}| + |d_{m+2}| + \ldots |d_k|$. When $\epsilon < 1$ the triangle inequality gives

$$|d_{m+1}\zeta^{m+1} + d_{m+2}\zeta^{m+2} + \ldots d_k z^k| \leq M \cdot \epsilon^{m+1} \tag{vii}$$

Together with (vii) another application of the triangle inequality gives:

$$|P(z_0 + \epsilon \cdot e^{i\cdot \frac{\pi+\alpha-\beta}{m}})| \leq |P(z_0)|(1 - |d_m|\epsilon^m| + M \cdot \epsilon^{m+1} =$$

$$|P(z_0)| - \epsilon^m\big(|d_m| \cdot |P(z_0)| - M \cdot \epsilon\big) \tag{viii}$$

Now we can take

$$0 < \epsilon < \frac{|d_m| \cdot |P(z_0)|}{M}$$

and then (viii) gives a strict inequality

$$|P(z_0 + \zeta)| < |P(z_0)|$$

This contradicts that z_0 gave a minimum for the absolute value of P and the proof is finished.

Proof by residue calculus. Later Cauchy gave other proofs using reside theory in his famous text-books devoted to analytic functions. For if the polynomial $P(z)$ in (*) has no complex zeros then $P^{-1}(z)$ is an entire function and taking the complex derivative $P*(z)$ it follows that the complex line integrals

$$\int_{|z|=R} \frac{P'(z)}{P(z)}\, dz = 0$$

for all R. When the line integral is evaluated in polar coordinates it becomes

$$\int_0^{2\pi} \frac{n + (n-1)c_{n-1}R^{-1}e^{-i\theta} + \ldots c_1R^{-n-1}e^{-i(n-1)\theta}}{1 + c_{n-1}R^{-1}e^{-i\theta} + \ldots + c_0R^{-n}e^{-in\theta}}\, d\theta$$

Passing to the limit as $R \to +\infty$ the last integral converges to n which gives the contradiction. Cauchy concluded that P must have at least one zero and actually residue calculus immediately entails that the number of zeros counting multiplicities is equal to the degree of the polynomial.

Remark. If the degree of $P(z)$ is ≤ 4 one can find the roots by *Cardano's formula*. See § B.3 for an example. But as soon as the degree is ≥ 5 it is in general not possible to find the zeros of a polynomial by roots and radicals even if the coefficients are integers. This was proved by Niels Henrik Abel in 1823 whose article [Ab:1] published in the first volume of Crelle's Journal contains pioneering results about algebraic field extensions. Abel used these new discoveries to prove that the general algebraic equation of degree ≥ 5 cannot be solved by roots and radicals by investigating a system of 120 linear equations expressed by the coefficients of a polynomial in degree ≥ 5. An example from Abel's work where a Cardano solution fails is the equation

$$z^5 + z + 1 = 0$$

For an account about Abel's contributions the reader should consult articles from *The Abel Legacy* published in 2004 on the occasion of the first Abel Prize. After Abel's decease in 1829, Everiste Galois constructed a group to every polynomial which as an alternative to Abel's criterium also can be used to decide when zeros of a polynomial can be found by roots and radicals. This leads

to *Galois theory* which brings the theory about field extensions together with group theory and has become a central topic in algebra.

An algebraic problem. Consider a pair of polynomials

$$p(z) = z^n + a_1 z^{n-1} + \ldots + a_{n-1}z + a_n$$
$$q(z) = z^n + b_1 z^{n-1} + \ldots + b_{n-1}z + b_n$$

where $\{a_\nu\}$ and $\{b_\nu\}$ are rational numbers. Both polynomials are assumed to be irreducible in the unique factorization domain $Q[z]$ which entails that the roots of p and q are simple. By the fundamental theorem of algebra we can write

$$p(z) = \prod (z - \alpha_j) \quad \text{and} \quad q(z) = \prod (z - \beta_j)$$

Each root α_j of p generates a field $K = Q[\alpha_j]$ which as a vector space of Q has dimension n and a basis is given by $1, \alpha_j, \ldots, \alpha_j^{n-1}$. In fact, this holds since $p(z)$ was irreducible and we remark that the field K is isomorphic to the field $\frac{Q[z]}{(p)}$ where (p) denotes the pirnicipal ideal generated by p in the polynomial ring $Q[z]$. Similar conclusions hold for the roots of q. Now one may ask when there exists a pair of roots α_j, β_ν for p and q respectively, such that the fields $K[\alpha_j]$ and $K[\beta_\nu]$ are equal. By elementary field theory the necessary and sufficient condition for the equality $K[\alpha_j] = K[\beta_\nu]$ is that

(i) $$\beta_\nu = q_0 + q_1 \cdot \alpha_j + \ldots + q_{n-1}\alpha_j^{n-1}$$

holds for some n-tuple $\{q_\nu\}$ of rational numbers. The problem is to find equations satisfied by the pair of n-tuples $\{a_j\}$ and $\{b_k\}$ which appear as coefficients of the two polynomials in order that (i) holds for some pair of roots. This is a problem in algebraic elimination theory and solved as follows: Let $\lambda, \xi_0, \ldots, \xi_{n-1}$ be $n+1$ many new variables and set

$$S(\lambda, \xi_0, \ldots, \xi_{n-1}) = \prod_{j=1}^{j=n} \big(\lambda - (\xi_0 + \xi_1\alpha_j + \ldots + \xi_{n-1}\alpha_j^{n-1})\big)$$

This is a *symmetric* expression in the n-tuple of roots of p and text-books in elementary algebra teaches that every symmetric polynomial of the roots can be expressed as a polynomial of the coefficients with integer coefficients. It follows that

(ii) $$S(\lambda, \xi_0, \ldots, \xi_{n-1}) = \sum_{j=0}^{j=n-1} \phi_j(a_1, \ldots, a_n, \xi_0, \ldots, \xi_{n-1}) \cdot \lambda^j$$

where $\{\phi_j\}$ are polynomials with integer coefficients of the two n-tuples $\{a_\nu\}$ and $\{\xi_\nu\}$ expressed by explicit interpolatation formulas. With these notations, (1) is satisfied for a pair of roots if and only if the λ-polynomial in (ii) has at least one root in common with q. To check if this holds one employs a determinant of a certain $2n \times 2n$-matrix whose elements are determined explicitly by the coefficients $\{b_\nu\}$ and the n-tuple $\phi_j(a, \xi)$. See Exercise § xx from § I:C for this. The conclusion is that there exists a polynomial of the ξ-variables

$$\mathcal{S}(\xi_0, \ldots, \xi_{n-1}) = \sum \rho_\gamma(a_\bullet, b_\bullet) \cdot \xi^\gamma$$

where $\{\rho_\gamma\}$ are polynomials of the $2n$-tuple formed by the coefficients of the given polynomials and $\gamma = (\gamma_0, \ldots \gamma_{n-1})$ are multi-indices expressing the monomials

$$\xi^\gamma = \xi_0^{\gamma_0} \cdots \xi_{n-1}^{\gamma_{n-1}}$$

Now (i) has a solution with rational numbers $\{q_\nu\}$ if and only if $\mathcal{S}(q_0, \ldots, q_{n-1}) = 0$. In other words, the necessary and sufficient condition to obtain (i) for a pair of roots is that the $\mathcal{S}$-polynomial of n variables has at least one zero in the n-dimensional ξ-space given by an n-tuple of rational numbers. Using terminology from algebraic geometry it means that the algebraic hypersurface $\{\mathcal{S} = 0\}$ contains at least one rational point. This example gives a glimpse of elimination theory where the problems consist in finding various algorithmic formulas. Concerning the specific problem above we remark that calculations which lead to equations in order that (i)

holds were carried out in work by Delannay and Tschebotarëw for polynomials of degree ≤ 4. The interested reader may consult the plenary talk by Tschebotarëw from the IMU-congress at Zürich in 1932 which describes the interplay between the problem above and Galois theory. It appears that a complete investigation for arbitrary large n remains unsettled.

B.2 Algebraic numbers. Of special interest are complex numbers which are *algebraic* over the field Q of rational numbers, i.e. complex numbers α which are roots to some polynomial whose coefficients are rational numbers. The set of all such complex numbers is a subfield of $\mathbf{C}$ denoted by A. Inside A there occur subfields generated by roots to a finite family of polynomials. These subfields are finite dimensional vector spaces over Q and called finite algebraic fields. Given such a field K one then gets a subring $\mathcal{D}(K)$ which consists of all $\alpha \in K$ such that α is a root of a monic polynomial with integer coefficients, i.e. α satisfies an equation

$$\alpha^m + c_{m-1}\alpha^{m-1} + \ldots + c_1\alpha + c_0 \quad : \quad c_0, \ldots, c_{m-1} \text{ are integers}$$

The ring $\mathcal{D}(K)$ is a Dedekind ring and enjoys nice properties which are exposed in text-books devoted to algebraic number fields. Analytic function theory is used to study approximations of algebraic numbers by rational numbers. Let ξ be a positive real number which satisfies an algebraic equation

$$\xi^n + c_{n-1}\xi^{n-1} + \ldots + c_1\xi + c_0 = 0$$

where $\{c_\nu\}$ are integers and the polynnomial $P(z) = z^n + \sum c_\nu z^\nu$ is irreducible in the unique factorisation domain $Q[z]$. In 1908 Thue proved a remarkable result in the article *Bemerkungen über gewisse Näherungsbrüche algebraishen Zahlen.* Namely, for every $\epsilon > 0$ the set of positive rational numbers $q = \frac{x}{y}$ such that

$$(*) \qquad \big|\xi - \frac{x}{y}\big| \leq \frac{1}{y^{\frac{n}{2}+1+\epsilon}}$$

is finite. Thue's result means that there are lower bounds for approximations of algebraic integers which are not rational numbers. In his thesis from 1921, Siegel proved that if ξ is as above then the set of rational numbers $\frac{x}{y}$ for which

$$(**) \qquad \big|\xi - \frac{x}{y}\big| \leq \frac{1}{y^{2\sqrt{n}}}$$

is finite. Notice that Sigel's result improves (*) as soon as $n \geq 16$. The proof of (**) is quite involved. The interested reader may consult Siegel's article *Über Näherungswerte algebraischen Zahlen*(Math. Zeitschrift 1921) for refined results about approximations of algebraic numbers by rationals. But let us give one of the minor steps from Siegel's impressive work.

An inequality by Siegel. Let $p(z) = z^n + c_{n-1}z^{n-1} + \ldots + c_1 z + c_0$ be a polynomial with integer coefficients. Suppose that $p(z)$ has a factorisation in the polynomial ring $Q[z]$:

$$p(z) = (k_0 z^m + \ldots + k_{m-1}z + k_m) \cdot q(z)$$

where $1 \leq m < n$ and $k_0, \ldots, k_m$ are integers with no common divisor ≥ 2 while $q(z)$ is a polynomial of degree $n - m$ in $Q[z]$. Set

$$\rho^* = \max\{|c_0|, \ldots, |c_n|\} \quad \text{and} \quad \rho_* = \max\{|k_0|, \ldots, |k_m|\}$$

Then one has the inequality

$$(*) \qquad \frac{\rho_*}{\rho^*} \leq (m+1)\cdots n$$

Proof. Consider first a polynomial $f(z) = a_0 z^k + \ldots + a_k$ of some degree $k \geq 1$ with arbitrary complex coefficients. Let $\lambda \neq 0$ be another complex numbers and set

$$g(z) = (z - \lambda)f(z) = d_0 z^{k+1} + \ldots + d_k z + d_{k+1}$$

Let $d^* = \max\{|d_\nu|\}$ and $c^* = \max\{|c_\nu\}$. Then one has the inequality

$$(1) \qquad \frac{a^*}{d^*} \leq k + 1$$

To prove (1) we notice that

$$a_\nu = d_0\lambda^\nu + d_1\lambda^{\nu-1} + \ldots + d_\nu \quad : \, 0 \leq \nu \leq k$$

If $|\lambda| \leq 1$ it follows that

$$|a_\nu| \leq |d_0| + |d_1| + + \ldots + |d_\nu| \leq (\nu+1) \cdot d^*$$

Since this holds for every ν we get $a^* \leq (k+1)d^*$ as requested. Next, if $|\lambda| > 1$ we rewrite (1) so that

$$(z - \frac{1}{\lambda})(a_k z^k + \cdots + a_0) = -\frac{1}{\lambda} \cdot (d_0 + \ldots + d_{k+1}z^{k+1})$$

Since $\frac{1}{\lambda}$ has absolute value ≤ 1 the previous case entails that

$$a^* \leq (k+1)\frac{d^*}{|\lambda|} \leq (k+1)d^*$$

and hence (1) also holds when $|\lambda| \geq 1$. To prove (*) we consider the factorisation

$$q(z) = k_0^{-1}(z - \lambda_1) \cdots (z - \lambda_{n-m})$$

Hence the polynomial $p(z)$ arises from $p_*(z) = k_0^{-1}(k_0 z^m + \cdots + k_m)$ via an $(n-m)$-fold application of the case above and from this the reader can deduce that

$$\frac{\rho_*}{\rho^*} \leq (m+1) \cdots n$$

which proves (*).