Mathematics. — *On the fundamental theorem of algebra.* (First communication.) By J. G. VAN DER CORPUT.

(Communicated at the meeting of June 29, 1946.)

§ 1. *Introduction* [1].

There exist several versions of the fundamental theorem of algebra. One of these versions is as follows:

If Ω be the field of the real numbers, then any polynomial

$$F(X) = f_0 + f_1 X + \ldots + f_\mu X^\mu$$

of degree $\mu \geq 1$, the coefficients of which belong to Ω and the highest coefficient of which is equal to 1, possesses exactly μ roots $x_1, \ldots, x_\mu$, belonging to the field $\Omega(i)$, where $i = \sqrt{-1}$; in other words it is possible to write $F(X)$ in the form

$$F(X) = (X - x_1)\ (X - x_2) \ldots (X - x_\mu),$$

where $x_\varrho = a_\varrho + ib_\varrho$ $(\varrho = 1, \ldots, \mu)$ and a_ϱ and b_ϱ denote elements of Ω.

It is not possible to give a purely algebraic proof of this theorem, because this proposition involves the notion of real numbers and therefore the notion of a limit, which does not belong to algebra. It is not appropriate to call the theorem in this form the fundamental theorem of algebra, because by far the greatest part of algebra does not require the theorem in this form at all. The simplest proof of the theorem in this form is given by J. E. LITTLEWOOD [2], who uses the fact (belonging to analysis), that a continuous function ≥ 0, given on a bounded closed set, assumes at one point of this set at least a minimum value.

Now the second version that may justly be called the fundamental theorem of algebra:

If Ω be an arbitrary commutative field, then to any polynomial $F(X)$ of degree $\mu \geq 1$, the coefficients of which belong to Ω and the highest coefficient of which is equal to the unit element e of Ω, corresponds a commutative field Ω_1, containing all elements of Ω, such that $F(X)$ possesses exactly μ roots, all belonging to Ω_1.

The proof of this theorem is purely algebraic. Here $\sqrt{2}$ is a symbol, for which addition, subtraction, multiplication and division are defined in such a manner, that the usual rules remain valid and that the square of this symbol equals 2.

---

[1]) Lecture given at the Manchester University, May 28th 1946.

[2]) J. E. LITTLEWOOD, Mathematical notes (14): "Every polynomial has a root". J. London Math. Soc. **16**, 95—98 (1941).

The arguments, applied in this part of mathematics, do not permit us to distinguish between $\sqrt{2}$ and $-\sqrt{2}$. Any rational relation with rational coefficients, involving $\sqrt{2}$, remains valid if $\sqrt{2}$ is replaced by $-\sqrt{2}$. On this fact, suitably generalised, is based the whole Galois theory.

In this theory we suppose that it is always possible to decide, whether a given polynomial $F(X)$, the coefficients of which belong to the given commutative field Ω, is reducible or not. The polynomial $F(X)$ of degree μ is called reducible (with respect to Ω), if it is possible to write $F(X)$ as a product $F_1(X).\ F_2(X)$ of two polynomials of degree $< \mu$, the coefficients of which belong to Ω. There are many fields, f.i. the field of the rational numbers, which satisfy this condition, but there are exceptions. And even if it is theoretically possible, then the calculations are so long, that practically nobody gets through them. Nevertheless this investigation is often necessary, even for the very simplest problem.

Let α be a root of $F(X)$, so that α is an element of Ω_1. Consider a polynomial

$$G(X) = g_0 + g_1 X + \ldots + g_\nu X^\nu,$$

of degree $\nu \geqq 1$, the coefficients of which belong to Ω (and therefore to Ω_1) and the highest coefficient of which is the unit element of Ω (and therefore also of Ω_1). According to the fundamental theorem of algebra, applied with Ω_1 instead of Ω, there exists a commutative extension Ω_2 of Ω, such that $G(X)$ possesses exactly ν roots, all belonging to Ω_2. If β be a root of $G(X)$, then what do we know about $\alpha + \beta$ and $\alpha\beta$? We can construct in the following manner two polynomials $U(X)$ and $V(X)$, both of degree $\mu\nu$, such that $\alpha + \beta$ is a root of $U(X)$ and $\alpha\beta$ is a root of $V(X)$. The products

$$\Pi(X - Y_\varrho - Z_\sigma) \quad \text{and} \quad \Pi(X - Y_\varrho Z_\sigma), \quad . \quad . \quad . \quad . \quad . \quad (1)$$

where ϱ runs over $1, 2, \ldots, \mu$ and σ over $1, 2, \ldots, \nu$ and where

$$X, Y_1, \ldots, Y_\mu, Z_1, \ldots, Z_\nu$$

denote indeterminates, are integral rational symmetrical functions of the indeterminates $Y_1, \ldots, Y_\mu$ and also of the indeterminates $Z_1, \ldots, Z_\nu$. Hence these products may be written as integral rational functions of X, the elementary symmetrical functions of $Y_1, \ldots, Y_\mu$, and the elementary symmetrical functions of $Z_1, \ldots, Z_\nu$. If we replace the elementary symmetrical functions $\Sigma Y_1,\ \Sigma Y_1 Y_2, \ldots, Y_1 Y_2 \ldots Y_\mu$ successively by

$$-f_{\mu-1}, f_{\mu-2}, \ldots, (-1)^\mu f_0$$

and similarly the elementary symmetrical functions

$$\Sigma Z_1, \Sigma Z_1 Z_2, \ldots, Z_1 Z_2, \ldots, Z_\nu$$

successively by $-g_{\nu-1}, g_{\nu-2}, \ldots, (-1)^{\nu} g_0$, then the products in question transform into polynomials

$$U(X, f_0, \ldots, f_{\mu-1}, g_0, \ldots, g_{\nu-1}) \text{ and } V(X, f_0, \ldots, f_{\mu-1}, g_0, \ldots, g_{\nu-1})$$

in the X, f_ϱ en g_σ ($\varrho = 0, \ldots, \mu-1$; $\sigma = 0, \ldots, \nu-1$).

These polynomials, both of degree $\mu\nu$ in X, and both uniquely determined by the polynomials $F(X)$ and $G(X)$, will be denoted by $F(X) \dotplus G(X)$ and $F(X) \times G(X)$. It is easy to see that $\alpha + \beta$ is a root of the first and $\alpha\beta$ is a root of the second polynomial.

For instance, if

$$F(X) = X^2 - 2 \text{ and } G(X) = X^2 - 2X - 1,$$

then we find

$$F(X) \dotplus G(X) = (X-1)^2 (X^2 - 2X - 7)$$
$$F(X) \times G(X) = (X^2 + 4X + 2)\ (X^2 - 4X - 2).$$

This example shows, that the properties of $\alpha + \beta$ are not completely determined by the fact, that $\alpha + \beta$ is a root of $F(X) \dotplus G(X)$, for $\alpha + \beta$ may be equal to 1, or $\alpha + \beta$ may be a root of $X^2 - 2X - 7$, and the roots of the last polynomial do not have the same proporties as the number 1.

To find the properties of $\alpha + \beta$ we must decompose $F(X) \dotplus G(X)$ into irreducible factors (generally a tiresome problem) and then we must know which of these factors has $\alpha + \beta$ as a root.

To a third polynomial $H(X)$ corresponds a commutative extension Ω_3 of Ω, containing the roots of $F(X)$, $G(X)$ and $H(X)$, and so we can go on.

If the number of elements of the given commutative field is enumerable, then we find in this manner after an infinite number of steps a commutative extension Ω'' of Ω, containing all roots of each polynomial, whose coefficients belong to Ω.

The last features of this theory, on which I draw the attention, is that it is not possible to distinguish here beween real and non-real roots, and that we may not say, that $\sqrt{2}$ is situated between 1 and 2; in fact if that were the case, then $-\sqrt{2}$ would be negative, and, as we have said, it is impossible in this theory to distinguish between $\sqrt{2}$ and $-\sqrt{2}$. It is therefore impossible to approximate $\sqrt{2}$ by rational numbers.

Let us now consider a third version of the fundamental theorem of algebra. Let Ω be a commutative Archimedeanly ordered field, i.e. I assume that it is possible for any couple of elements a and b to decide whether $a = b$, $a > b$ or $a < b$; furthermore an arbitrary element a being given, a natural number ν can be found, such that a is less than the sum of ν terms, each of which is equal to the unit-element e of the field.

In a purely algebraic manner I will show that it is possible to construct in one step a commutative Archimedeanly ordered extension Ω' of Ω with the following property:

Any polynomial of degree $\mu \geqq 1$, *the coefficients of which belong to* Ω *and the highest coefficient of which equals the unit element* e *of* Ω, *possesses exactly* μ *roots, all belonging to a third field* $\Omega'(i)$, *where* $\Omega'(i)$ *denotes the field, formed by adjoining to* Ω' *the number* $i = \sqrt{-e}$.

If Ω is the field of the rational numbers, then Ω' is the field of the real algebraic numbers. If Ω is the field of the real algebraic numbers, then Ω' is identical with Ω. If we take for Ω the field of the real numbers, we depart from algebra because then we want the notion of limits. Every real number belongs in this case to Ω', since Ω' is an extension of Ω. Conversely each element of Ω' can be approximated [3]) by elements of Ω', i.e. by real numbers and is therefore a real number itself. Hence Ω' is identical with Ω.

Now some remarks about the proof. By an interval Φ we mean the set of elements x of the given ordered field Ω, satisfying the inequalities $a \leqq x \leqq b$, where a and b are elements of Ω with $a \leqq b$. The elements a and b may coincide; in that case the interval consists of only one point.

By the characteristic divisor $F^*(X)$ of $F(X)$ we mean the quotient

$$F^*(X) = \frac{F(X)}{\left(F, \frac{dF}{dX}\right)},$$

where $\left(F, \frac{dF}{dX}\right)$ denotes the greatest common divisor of the polynomial $F(X)$ and its derivative $\frac{dF(X)}{dX}$; if we put the highest coefficient of this greatest common divisor equal to the unit element of Ω, this divisor is uniquely determined.

I say that the polynomial $F(X)$, the coefficients of which belong to Ω, changes sign in the interval Φ, if Φ contains two elements u and v of Ω, satisfying the inequalities

$$F^*(v) \leqq 0 \leqq F^*(u);$$

if u and v coincide, we have $F^*(u) = 0$, hence $F(u) = 0$ [4]).

---

[3]) As will appear presently, each element γ of Ω' has the form (Γ, C), where C denotes a polynomial and Γ an interval, which may be taken arbitrarily small. The endpoints of Γ, which belong to Ω, give an arbitrarily precise approximation of γ.

[4]) If the polynomial $F(X)$ and the interval Φ are given, it is possible to decide in a finite number of steps, whether Φ contains two elements u and v which satisfy the above named inequalities. In fact by § 3 the interval Φ can be divided into a finite number of subintervals, such that throughout each of these subintervals the polynomial $F^*(X)$ has either a fixed sign or is an increasing or a decreasing function of X. If $F^*(X)$ has the same sign in the endpoints of all these subintervals, then $F^*(X)$ has a fixed sign in the interval Φ. Otherwise Φ contains two elements u and v, which satisfy the above named inequalities; in fact one of the subintervals in question has the property that $F^*(X)$ takes a value $\geqq 0$ at one endpoint and a value $\leqq 0$ at the other endpoint.

I say, that $F(X)$ changes sign in Φ more than once, if Φ contains three elements, u, v and w of Ω, with $u < v < w$, such that either

$$F^*(u) \leqq 0, \quad F^*(v) \geqq 0, \quad F^*(w) \leqq 0$$

or

$$F^*(u) \geqq 0, \quad F^*(v) \leqq 0, \quad F^*(w) \geqq 0.$$

Now the main point:

Let us consider couples (Γ, C), where $C = C(X)$ denotes a polynomial in Ω with highest coefficient $= e$, that changes sign only once in the interval Γ. If Γ contains only one point w, then the polynomial $C(X)$ vanishes at that point w; in this case we identify (Γ, C) with that point w. The set Ω' formed by couples (Γ, C) is therefore an extension of the given field Ω.

We write $(\Gamma, C) = (\triangle, D)$ if and only if the greatest common divisor of $C(X)$ and $D(X)$ changes sign in the common part $(\Gamma, \triangle)$ of the intervals Γ and $\triangle$; in that case this greatest common divisor changes sign only once in $(\Gamma, \triangle)$, as I will show in § 2.

It is easy to show that this notion of equality is reflexive and symmetrical, i.e. we have $(\Gamma, C) = (\Gamma, C)$ and the relation $(\Gamma, C) = (\triangle, D)$ implies $(\triangle, D) = (\Gamma, C)$. In § 2 I show, that this notion of equality is also transitive, i.e. $(\Gamma, C) = (\triangle, D)$ and $(\triangle, D) = (\Lambda, L)$ implies $(\Gamma, C) = (\Lambda, L)$.

Now we have to define the sum of two couples (Γ, C) and $(\triangle, D)$. If u runs through the interval Γ and v runs through the interval $\triangle$, then $u + v$ runs through an interval which we denote by $\Gamma + \triangle$. In § 3 I show that the above defined polynomial $C(X) + D(X)$ changes sign in the interval $\Gamma + \triangle$. It is possible, that this polynomial changes sign in this interval more than once, but we can find a subinterval Γ_1 of Γ, in which $C(X)$ changes sign, and a subinterval $\triangle_1$ of $\triangle$, in which $D(X)$ changes sign, in such a manner that $C + D$ changes sign only once in the interval $\Gamma_1 + \triangle_1$. (This last condition is satisfied, if the subintervals Γ_1 and $\triangle_1$ are small enough.) In that case we have by definition

$$(\Gamma, C) = (\Gamma_1, C) \text{ and } (\triangle, D) = (\triangle_1, D).$$

In § 3 I will show, that then the couple $(\Gamma_1 + \triangle_1, C + D)$ is uniquely determined by the couples (Γ, C) and $(\triangle, D)$ (also independant of the choice of the subintervals Γ_1 and $\triangle_1$). I put:

$$(\Gamma, C) + (\triangle, D) = (\Gamma_1 + \triangle_1, C + D).$$

Let us consider the special case in which Γ consists of only one point u, and $\triangle$ of only one point v. Then $\Gamma_1 = \Gamma$ and $\triangle_1 = \triangle$, so that $\Gamma_1 + \triangle_1$ consists of the point $u + v$ only. The polynomial $C + D$, which changes sign in that interval, vanishes therefore at the point $u + v$ and we have:

$$(\Gamma, C) = u; \quad (\triangle, D) = v; \quad (\Gamma_1 + \triangle_1, C + D) = u + v.$$

Hence it appears, that the above definition of addition of two couples is allowed.

In a similar way we define the product of two couples. If u runs through the interval Γ and v through the interval $\triangle$, then uv runs through an interval, which we denote by $\Gamma \times \triangle$. The polynomial $C(X) \times D(X)$ changes sign in that interval, but perhaps more than once. It is possible to replace again Γ and $\triangle$ by subintervals Γ_1 and $\triangle_1$ with $(\Gamma, C) = (\Gamma_1, C)$ and $(\triangle, D) = (\triangle_1, D)$, such that $C \times D$ changes sign only once in the interval $\Gamma_1 \times \triangle_1$; then the couple $(\Gamma_1 \times \triangle_1, C \times D)$ is uniquely determined (also independent of the choice of the sub-intervals) and I put:

$$(\Gamma, C)\ (\triangle, D) = (\Gamma_1 \times \triangle_1, C \times D).$$

Similarly as above it is obvious, that this definition is allowed.

It is easy to show, as shall be done in § 4, that the couples (Γ, C) form a commutative field Ω'. It is therefore possible to calculate the value, which the polynomial $F(X)$ assumes, if we replace the indeterminate X by a couple (Φ, F). We find that F vanishes in that case; hence (Φ, F) is a root of the polynomial $F(X)$. Therefore I call Ω' the field of the real algebraic numbers with respect to the given field Ω.

To give an example: If Φ is the interval with the endpoints 1 and 2 and if we put $F(X) = X^2 - 2$, then we have to show that $(\Phi, F)^2 = 2$. Here $F \times F = (X^2 - 4)^2$ and $\Phi \times \Phi$ is the interval Ψ with endpoints 1 and 4. If Ψ_1 consists of only the number 2, we have

$$(\Phi, F)^2 = (\Phi \times \Phi, (X^2-4)^2) = (\Psi, (X^2-4)^2) = (\Psi_1, (X^2-4)^2) = 2.$$

The proof of the formula $\sqrt{2}\sqrt{3} = \sqrt{6}$ proceeds as follows: If Φ is again the interval with endpoints 1 and 2, hence $\Psi = \Phi \times \Phi$ the interval with endpoints 1 and 4, we have

$$(\Phi, X^2 - 2)\ (\Phi, X^2 - 3) = (\Psi, (X^2 - 6)^2) = (\Psi, X^2 - 6).$$

In the field Ω', formed by the elements, which are real algebraic with respect to Ω, the element 0 is the couple (Π, P), where Π contains the element 0 of Ω and P is a polynomial, which vanishes in that point. In fact $(\Pi, P) = (\Pi_0, X)$ by definition, where Π_0 is the interval which consists of only the element 0; if (Π_0, X) is added to an arbitrary element $(\triangle, D)$, we get again $(\triangle, D)$, for $\triangle + \Pi_0 = \triangle$ and $D + X = D$.

To order the field Ω' it is sufficient to distinguish whether a couple $\gamma = (\Gamma, C)$, which is not equal to the element 0, is positive or negative. Since $\gamma \neq 0$, it is impossible that Γ contains the element 0 and that at the same time $C(0) = 0$. Hence only two cases are possible:

1°: $C(X)$ changes sign in the interval, formed by the elements $X \geqq 0$ of Γ; in this case we put γ positive.

2° $C(X)$ changes sign in the interval, formed by the elements $X \leqq 0$ of Γ; in that case we put γ negative.

It is obvious that the sign of (Γ, C) is independant of the choice of Γ and C i.e. if $(\Gamma, C) = (\triangle, D)$, then $(\triangle, D)$ is positive, 0 or negative according to whether (Γ, C) is positive, 0 or negative.

The two conditions imposed on an ordered field are satisfied here, viz.:

1°: For every couple γ one and only one of the relations $\gamma = 0$, $\gamma > 0$ and $\gamma < 0$ is valid. In fact, put $L(X) = (-1)^{\mu} C(-X)$, where μ denotes the degree of the polynomial $C(X)$. Be Λ the interval of the elements $-x$ of Ω, where x runs through the interval Γ. Then we have $-\gamma = (\Lambda, L)$, which means that $(\Gamma, C) + (\Lambda, L)$ is the element 0 of Ω'. It is obvious that, if γ is not equal to the element 0, only one of the couples (Γ, C) and (Λ, L) is positive.

2°: If $\gamma = (\Gamma, C)$ and $\delta = (\triangle, D)$ are positive, then also their sum and product are positive. In fact, we may suppose, that all elements both of Γ and $\triangle$ are $\geqq 0$, consequently also all elements of $\Gamma + \triangle$ and $\Gamma \times \triangle$.

In this manner we have ordered Ω'.

The axiom of ARCHIMEDES is valid, for to a given couple γ corresponds an element $c > \gamma$ of Ω and Ω being Archimedeanly ordered, a natural number ν exists, such that the sum of ν terms, each equal to the unit element of Ω, is greater than c, hence greater than γ.

By means of the arbitrary commutative Archimedeanly ordered field Ω we have constructed a new Archimedeanly ordered field Ω' consisting of the elements, which are real-algebraic with respect to Ω. Repeating our argument with Ω' in stead of Ω we find the commutative Archimedeanly ordered field, formed by the elements, which are real-algebraic with respect to Ω'. In order to prove that this new field is identical with Ω', it is sufficient to show, that an arbitrary element (Φ', F') of the new field belongs to Ω'; here Φ' denotes an interval, formed by elements of Ω'; the polynomial $F'(X)$ changes sign only once in the interval Φ' and the coefficients of this polynomial belong to Φ'. The coefficients of the polynomial F' belong to Ω' and therefore are real algebraic with respect to the original field Ω'. As we show in § 5 it is possible to construct a polynomial $F(X)$, not identically $= 0$, such that the coefficients of $F(X)$ belong to Ω and that $F'(X)$ is a divisor of $F(X)$. The polynomial $F(X)$ changes sign in Φ', but perhaps more than once; however it is possible to find a subinterval Φ'_1 of Φ', such that $F'(X)$ and $F(X)$ both change sign only once in Φ'_1. By definition we have

$$(\Phi', F') = (\Phi'_1, F).$$

If the characteristic divisor of the polynomial $F(X)$ vanishes at one endpoint of Φ'_1, then (Φ'_1, F) is by definition equal to that endpoint, and therefore equal to an element of Ω'. Hence we may assume, that this characteristic divisor does not vanish at either of the endpoints of the interval. Then it is possible to find a subinterval Φ'_2 of Φ'_1, such that the endpoints a and b of Φ'_2 belong to Ω and that F changes sign only once in that interval Φ'_2. So we obtain

$$(\Phi', F') = (\Phi'_1, F) = (\Phi'_2, F).$$

Be Φ the interval formed by the elements of Ω, belonging to Φ'_2; hence

Φ is formed by the elements $\geqq a$ and $\leqq b$ of Ω. The couple (Φ, F) is an element $\geqq a$ and $\leqq b$ of Ω' and belongs consequently to Φ'_2. Moreover the polynomial $F(X)$ vanishes, if the indeterminate X is replaced by (Φ, F). By definition $(\Phi', F') = (\Phi'_2, F)$ is equal to the element (Φ, F) of Φ'_2, and this element belongs to Ω'.

Hence it is not possible to extend the field Ω' in the specified manner.

Now we pass to the third version of the fundamental theorem of algebra, which we state as follows:

Be Ω an arbitrary commutative Archimedeanly ordered field, Ω' the ordered commutative field, formed by the elements which are real-algebraic with respect to Ω. Then any polynomial of degree $\mu \geqq 1$, the coefficients of which belong to $\Omega'(i)$, and the highest coefficient of which is equal to e, possesses exactly μ roots and these roots belong to $\Omega'(i)$.

In order to give a proof we show first, that the polynomial $F(X)$ possesses at least one root, belonging to $\Omega'(i)$. Let us first consider the case $F(X) = X^2 - q$, where q denotes a positive element of Ω'. Then it is possible to find a positive element b of Ω', such that $b^2 > q$. If Φ denotes the interval with the endpoints 0 and b, formed by elements of Ω', then $X^2 - q$ changes sign only once in that interval; hence the couple $x_1 = (\Phi, X^2 - q)$ is a root of the polynomial $X^2 - q$. Consequently this polynomial possesses in Ω' the root x_1 and the polynomial $X^2 + q$ possesses in $\Omega'(i)$ the root $x_1 i$. Hence each quadratic polynomial $X^2 + pX + q$, with highest coefficient $= e$ and the coefficients of which belong to Ω', possesses at least one root, belonging to $\Omega'(i)$, for this polynomial is identical with

$$\left(X + \frac{p}{2}\right)^2 - \left(\frac{p^2}{4} - q\right).$$

Consider now the case that $F(X)$ is a polynomial of odd degree with coefficients, belonging to Ω'. Then it is possible to find two elements a and b of Ω', such that the polynomial changes sign in the interval with the endpoints a and b. Perhaps it changes sign more than once in that interval, but it is always possible to find a subinterval Φ, such that F changes sign only once in Φ. Hence the polynomial $F(X)$ possesses a root (Φ, F) belonging to Ω'.

So we have shown that each quadratic polynomial and also each polynomial of odd degree with coefficients belonging to Ω' possesses at least one root, belonging to $\Omega'(i)$. As GAUSS has shown in his second proof of the fundamental theorem of algebra, herefrom it follows, that each polynomial with highest coefficient equal to e and the coefficients of which belong to $\Omega'(i)$, possesses at least one root belonging to $\Omega'(i)$.

If x_1 is a root of $F(X)$, belonging to $\Omega'(i)$, the coefficients of $\frac{F(X)}{X - x_1}$ belong also to $\Omega'(i)$, so that the argument may be repeated with this quotient instead of $F(X)$. Continuing in this manner we find the number of roots to be equal to the degree of the polynomial.

In the last section (§ 6) I give a proof of the following lemma.

Be $0 \leqq \lambda \leqq \mu$. Suppose that the polynomials $A(X) = a_0 + \ldots + a_\mu X^\mu$ and $B(X) = b_0 + \ldots + b_\mu X^\mu$, the coefficients of which belong to $\Omega'(i)$, satisfy the inequalities

$$\sum_{\varrho=0}^{\lambda} |a_\varrho| \geqq \frac{a}{u}; \quad \sum_{\varrho=\lambda}^{\mu} |a_\varrho| \geqq \frac{a}{u}; \quad \sum_{\varrho=0}^{\lambda} |b_\varrho| \geqq \frac{b}{u};$$

$$\sum_{\varrho=\lambda}^{\mu} |b_\varrho| \geqq \frac{b}{u}; \quad |b_\varrho - a_\varrho| \leqq a\, r^{\mu+1} \quad (\varrho = 0, \ldots, \mu);$$

here a denotes the sum $\neq 0$ of the absolute values of the coefficients of $A(X)$ and b the sum $\neq 0$ of the absolute values of the coefficients of $B(X)$, whereas u and r are positive elements of Ω.

1° Then Ω contains a positive element v depending only on μ and u with the following property:

$A(X)$ may be written in the form

$$A(X) = a'(X - x_1) \ldots (X - x_\lambda)(e - x_{\lambda+1} X) \ldots (e - x_\mu X), \quad . \quad . \quad (2)$$

where

$$|x^\varrho| \leqq v \ (\varrho = 1, \ldots, \mu) \text{ and } |a'| \leqq a\, v. \quad . \quad . \quad . \quad . \quad . \quad (3)$$

2° To any decomposition of $A(X)$ of the form (2), satisfying the inequalities (3), corresponds a decomposition of $B(X)$ of the form

$$B(X) = b'(X - y_1) \ldots (X - y_\lambda)\ (e - y_{\lambda+1} X) \ldots (e - y_\mu X),$$

such that

$$|y_\varrho - x_\varrho| < w\, r \ (\varrho = 1, \ldots, \mu) \text{ and } |b' - a'| < w\, a\, r,$$

where w depends only on μ, u and v.

The intuitionist does not object to the above arguments, since each consists of a finite number of steps. For instance, in the preceding lemma, it is possible to evaluate v in a finite number of steps, if μ and u are given. One has however to take into consideration that, according to the intuitionist, the set of the real numbers does not posses the property imposed on the field Ω, viz. that it is possible for any couple of elements a and b of Ω to decide in a finite number of steps, which of the three cases $a = b$, $a > b$ or $a < b$ occurs. Therefore it is in the intuitionistic mathematics not allowed to take for Ω the set of the real numbers. Nevertheless it is possible to give in a few lines a purely intuitionistic proof of the fundamental theorem of algebra. I prove even this theorem in the following stronger form, due to L. E. J. BROUWER [5]).

---

[5]) Compare: H. WEYL, Randbemerkingen zu Hauptproblemen der Mathematik, Mathematische Zeitschrift **19**, 131—150 (1924).

B. DE LOOR, Die hoofstelling van die algebra van intuïsionistiese standpunt, Dissertation Amsterdam, 1925, 63 p.

L. E. J. BROUWER and B. DE LOOR, Intuitionistischer Beweis des Fundamentalsatzes der Algebra, Proc. Kon. Akad. v. Wetensch., Amsterdam, **27**, 186—188 (1924). The same

The polynomial

$$F(X) = f_0 + \ldots + f_\mu X^\mu$$

with complex coefficients, where f_σ *and* f_τ $(0 \leqq \sigma \leqq \tau \leqq \mu)$ *are positively different from* 0, *may be written for any integer* $\lambda \geqq \sigma$ *and* $\leqq \tau$ *in the form*

$$F(X) = a(X - x_1) \ldots (X - x_\lambda)(1 - x_{\lambda+1} X) \ldots (1 - x_\mu X), \quad . \quad . \quad (4)$$

where a *is positively different from* 0.

If f_μ is positively different from 0, we may choose σ, τ and λ all equal to μ, so that then we get the decomposition

$$F(X) = f_\mu (X - x_1) \ldots (X - x_\mu).$$

For a proof we remark that f_σ and f_τ differ positively from 0; hence a positive rational number $u \geqq \mu + 1$ exists, such that

$$|f_\sigma| \geqq \frac{3f}{u} \text{ and } |f_\tau| \geqq \frac{3f}{u};$$

here f denotes the sum of the absolute values of the coefficients of $F(X)$ and is therefore positively different from 0.

Consider a positively convergent series $r_1 + r_2 + \ldots$, consisting of positive, rational, decreasing numbers $r_\nu \leqq 1$, such that

$$\tfrac{1}{4} u r_\nu^{\mu+1} < 1.$$

To any natural number ν corresponds a polynomial

$$A_\nu(X) = a_{\nu 0} + \ldots + a_{\nu\mu} X^\mu$$

with rational complex coefficients, such that

$$|a_{\nu\varrho} - f_\varrho| < \frac{f}{4} r_\nu^{\mu+1} \qquad (\varrho = 0, \ldots, \mu).$$

Hence

$$\sum_{\varrho=0}^{\mu} |a_{\nu\varrho}| < \sum_{\varrho=0}^{\mu} |f_\varrho| + \tfrac{1}{4}(\mu+1) f r_\nu^{\mu+1} < 2f.$$

Moreover we obtain

$$\sum_{\varrho=0}^{\lambda} |a_{\nu\varrho}| \geqq |a_{\nu\sigma}| \geqq |f_\sigma| - \tfrac{1}{4} f r_\nu^{\mu+1} \geqq \frac{3f}{u} - \frac{f}{u} = \frac{2f}{u} > \frac{1}{u} \sum_{\varrho=0}^{\mu} |a_{\nu\varrho}|$$

---

paper in Dutch: Intuitionistisch bewijs van de hoofdstelling der algebra, Verslag Kon. Akad. v. Wetensch., Amsterdam, **33**, 82—84 (1924).

L. E. J. BROUWER, Intuitionistische Ergänzung des Fundamentalsatzes der Algebra, Proc. Kon. Akad. v. Wetensch., Amsterdam, **27**, 631—634 (1924). The same paper in Dutch: Intuitionistische aanvulling van de hoofdstelling der algebra, Versl. Kon. Akad. v. Wetensch., Amsterdam, **33**, 459—462 (1924).

and similarly

$$\sum_{=\lambda}^{\mu} | a_{\nu\varrho} | > \frac{1}{u} \sum_{\varrho=0}^{\mu} | a_{\nu\varrho} |.$$

Finally we get, from $r_{\nu+1} < r_\nu$,

$$| a_{\nu+1,\varrho} - a_{\nu\varrho} | < \tfrac{1}{2} f r_\nu^{\mu+1} < r_\nu^{\mu+1} \sum_{\varrho=0}^{\mu} | a_{\nu\varrho} |.$$

Hence it appears that the conditions of the lemma are satisfied with $A(X) = A_\nu(X)$, with $B(X) = A_{\nu+1}(X)$ and with $r = r_\nu$. Consequently we may write $A_1(X)$ in the form

$$A_1(X) = a_1'(X - x_{11}) \ldots (X - x_{1\lambda})(1 - x_{1,\lambda+1} X) \ldots (1 - x_{1\mu} X).$$

To this form corresponds a decomposition of $A_2(X)$

$$A_2(X) = a_2'(X - x_{21}) \ldots (X - x_{2\lambda})(1 - x_{2,\lambda+1} X) \ldots (1 - x_{2\mu} X),$$

such that

$$| x_{2\varrho} - x_{1\varrho} | < w r_1 \ , \ | a_2' - a_1' | < w r_1 \sum_{\varrho=0}^{\mu} | a_{1\varrho} | < 2 w r_1 f,$$

where w denotes a positive rational number depending only on μ and u. Continuing in this way we find for $A_\nu(X)$ $(\nu = 1, 2, \ldots)$ the decomposition

$$A_\nu(X) = a_\nu'(X - x_{\nu 1}) \ldots (X - x_{\nu\lambda})(1 - x_{\nu,\lambda+1} X) \ldots (1 - x_{\nu\mu} X), \qquad (5)$$

such that

$$| x_{\nu+1,\varrho} - x_{\nu\varrho} | < w r_\nu \text{ and } | a'_{\nu+1} - a'_\nu | < 2 w r_\nu f.$$

Since the series $r_1 + r_2 + \ldots$ is positively convergent, the numbers $x_{\nu 1}, \ldots x_{\nu\mu}, a'_\nu$ tend positively to limits $x_1, \ldots, x_\mu, a$, so that (5) gives (4) by a passage to the limit.