ON THE FUNDAMENTAL THEOREM OF ALGEBRA

HANS ZASSENHAUS, Ohio State University

Introduction. In the year 1799 C. F. Gauss [4] gave the first formal proof of the theorem that every nonconstant polynomial with real coefficients can be factored into a product of linear factors and quadratic factors. A constructive proof based on arguments of a purely algebraic nature and on assumptions about the real number field that were stated in purely algebraic terms (though the proof of these assumptions would require analytic methods) was first given by O. Perron [6]. In this paper Perron's method is further developed towards an algorithmic routine for solving algebraic equations with complex coefficients.

1. Really closed fields. The real number field has the following properties:

1.1. The negative of a nonsquare is a square.

1.2. The sum of squares is zero only if each summand is zero.

1.3. An algebraic equation of odd degree has a real solution.

The first two properties derive from the existence of an algebraic ordering of the real number field and a square root of every positive real number.

The last property follows from an application of the intermediate-value theorem of analysis to a polynomial: $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ of odd degree n with real coefficients, in view of the inequalities:

$$1.4 \qquad f\left(1+\sum_{i=1}^{n}|a_i|\right)>0>f\left(-\left(1+\sum_{i=1}^{n}|a_i|\right)\right)\cdot$$

Fields with the properties 1.1, 1.2, 1.3 are said to be *really closed.* E.g. the real number field is really closed. For a really closed field F an algebraic ordering is given by the rule:

1.5 The element a of F is greater than the element b of F if and only if the difference element $a-b$ is a nonzero square element of F. This implies the positivity concept:

1.6 An element of F is positive if and only if it is a nonzero square element of F.

In order to deduce the ordering properties of F from 1.5 we have to verify the positivity rules:

1.7 The negative of any nonpositive nonzero element is positive.

1.8 The sum and product of two positive elements are positive.

Indeed, if a is non positive and nonzero, then a is a non square of F. It follows from 1.1 that $-a$ is a square element of F so that $-a$ is positive.

If a and b are positive elements of F then the equations

$$a=\xi^2, \qquad b=\eta^2$$

are solvable by non zero elements ξ, η of F. From 1.2 it follows that $a+b$ does not vanish. If there would hold an equation: $-(a+b)=\zeta^2$ in F then

$$\xi^2+\eta^2+\zeta^2=0$$

would hold contrary to 1.2.

Thus $a+b$ is a square element of F so that the sum of two positive elements of F always is positive. Since,

$$ab = \xi^2\eta^2 = (\xi\eta)^2 \neq 0$$

the product of two positive elements is positive.

Clearly, for any really closed field only one positivity concept exists.

2. Ordered division rings. (See [1], [2], [3], [5], [7]). For a unital ring D with positivity concept satisfying 1.7, 1.8 we define an algebraic ordering by declaring the relation

$$a > b \text{ (or: } b < a)$$

to mean that the difference of the elements a, b of D is positive.

This definition implies the rules customarily demanded of an algebraic ordering relation:

2.1 (trichotomy). For any two elements a, b of R, there holds one and only one of the three relations:

$$a > b, \qquad a = b, \qquad b > a.$$

2.2 (transitivity). If $a>b$, $b>c$ then $a>c$.

2.3 If $a>b$, $c>d$ then $a+c>b+d$ and $ac+bd>ad+bc$.

Conversely, if $a>$relation is defined in D which satisfies 2.1, 2.3 then the relation $a>0$ defines a positivity concept satisfying 1.7 and 1.8, from which the $>$relation can be derived as was done above.

The derived relation:

$$a \geqq b \text{ (or: } b \leqq a)$$

meaning that either a is greater than b or a is equal to b (or: not $a<b$) and the functions:

$$\operatorname{sign} a = \begin{cases} 1 & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -1 & \text{if } a < 0 \end{cases}$$

$$|a| = a \cdot \operatorname{sign} a = (\operatorname{sign} a) \cdot a$$

satisfy the basic rules:

$$a \geqq a, \qquad a \geqq b \text{ and } b \geqq a \Rightarrow a = b, \qquad a \geqq b \text{ and } b \geqq c \Rightarrow a \geqq c,$$

$$a \geqq b \text{ and } c \geqq d \Rightarrow a + c \geqq b + d, \qquad ab + cd \geqq ad + cb$$

$$\operatorname{sign}(ab) = \operatorname{sign} a \cdot \operatorname{sign} b$$

$$|a| \cdot \operatorname{sign} a = (\operatorname{sign} a) \cdot |a| = a$$

$$|a| = |-a| \geqq 0, \qquad |a| = 0 \Leftrightarrow a = 0,$$

$$|a+b| \leqq |a| + |b|, \qquad |a-b| \geqq ||a| - |b||, \qquad |ab| = |a| \cdot |b|.$$

The positive elements of an ordered division ring D form a half-ring H (according to [8], p. 95, a halfring is a nonempty subset of a ring that is closed under addition and multiplication,) with the following properties:

2.4. The halfring H contains the square of every non zero element of the subdivision ring D_H generated by H.

2.5. The halfring H is a maximal subhalfring of D not containing the zero element of D.

Conversely, every halfring H of D satisfying 2.4 and 2.5 is associated with a positivity concept of D_H satisfying 1.7, 1.8.

Indeed, for any two non zero elements u, v of D we have the identity:

2.6 $$uvu^{-1}v^{-1} = (uv)^2(v^{-1}u^{-1}v)^2(v^{-1})^2$$

so that

2.7 $$uvu^{-1}v^{-1} \in H \quad \text{if } 0 \neq u \in D_H,\ 0 \neq v \in D_H.$$

Thus $uh=h(h^{-1}u\ hu^{-1})u\in Hu$ if $0\neq u\in D_H$, $h\in H$; hence $hu\in uH$, $uH\subseteq Hu$. Similarly $Hu\subseteq uH$; hence $uH=Hu(u\in D_H)$.

For h of H we have

$$H = h^{-1}hH \subseteq h^{-1}H, \qquad h^{-1} = h^{-1}1^2 \in h^{-1}H,$$
$$h^{-1}H + h^{-1}H \subseteq h^{-1}H,$$
$$h^{-1}Hh^{-1}H = h^{-1}(Hh^{-1})H = h^{-1}h^{-1}HH \subseteq H \subseteq h^{-1}H,$$

hence $h^{-1}H$ is a halfring of D_H containing H, but not zero. Since $h^{-1}H$ contains every non zero square element of $D_H=D_{h^{-1}H}$ it follows from the maximal property of H that $h^{-1}H=H$, hence $h^{-1}\in H$.

If the non zero element c of D_H is not contained in H then $-c$ belongs to H. Indeed,

$$c = c\cdot 1^2 \in cH \subseteq \hat{H} = H\cup cH \cup (H + cH)$$
$$(H + cH) + (H + cH) \subseteq H + cH$$
$$HcH = cHH \subseteq cH,$$
$$cHcH = c(Hc)H = c(cH)H = c^2HH \subseteq H$$
$$(H + cH)(H + cH) \subseteq H + cH.$$

Hence, $\hat{H}$ is a halfring of D_H properly containing H, so $\hat{H}$ contains zero because of the maximal property of H.

There are elements h_1, h_2 of H for which $h_1+ch_2=0$. Hence,

$$-c = h_1h_2^{-1} \in HH = H.$$

THEOREM 1. *A division ring D can be algebraically ordered if and only if the sum of finitely many finite products of square elements is zero only if all summands are zero.* (What happens if one makes the weaker assumption that the sum of finitely many squares can be zero only in the trivial way?)

Proof. That the condition is necessary was shown above. Let it be satisfied.

The set H_0 of all sums of finitely many finite products of non zero square elements of D does not contain zero. H_0 is a halfring. By Zorn's lemma [9] H_0 is contained in a maximal halfring H of D not containing zero. Hence, $2=1^2+1^2 \in H_0 \subseteq H$, $2 \neq 0$.

Since for any element u of D we have $u=\frac{1}{2}((u+1)^2-u^2) \in D_H$ it follows that $D_H=D$ and D has indeed the algebraic ordering which is given by

2.8. $a>b$ if and only if $a-b$ is in H.

THEOREM 2. *If the field F is algebraically ordered and if F is contained in an algebraically closed field extension Ω, then there is a really closed subfield Φ of Ω such that*

2.9. *every positive element of F is a square element of Φ.*

2.10. *Ω is algebraic over Φ.*

Proof. By Zorn's lemma [9] there is a maximal halfring H of Ω containing all positive elements of F and every non zero square element of the subfield Φ generated by H, but not zero.

We have shown above that the given ordering of F can be extended to an algebraic ordering of the field Φ such that H is the halfring of the positive elements.

If there were an element ξ of Ω that would not be algebraic over Φ then the halfring formed by the sums of finitely many nonzero square elements of $\Phi(\xi)$ with coefficients in H would be larger than H and it would contain all nonzero square elements of $\Phi(\xi)$. Because of the maximal property of H it would contain zero; hence there would be an equation.

$$0=\sum_{i=1}^{n} h_i\left(\frac{P_i(\xi)}{N(\xi)}\right)^2 \quad (h_i \in H)$$

where $N(x)$, $P_1(x)$, $\cdots$, $P_n(x)$ are non zero polynomials of $\Phi[x]$. Let m be the maximum degree of the polynomials $P_1(x)$, $\cdots$, $P_n(x)$ and let a_i be the coefficient of x^m in $P_i(x)$. Then

$$0=\sum_{i=1}^{n} h_i P_i(\xi)^2=\sum_{i=1}^{n} h_i P_i(x)^2=\sum_{i=1}^{n} h_i a_i^2,$$

contrary to the construction of H. Hence Ω is algebraic over Φ.

For every element u of H the equation $u=\xi^2$ is solvable in Ω. If ξ would not belong to Φ then the elements $a+b\xi$ with a, b contained in Φ such that $a\geqq 0$, $b\geqq 0$, $a+b>0$ forms a halfring $\overline{H}$ of Ω larger than H; it would be contained in the halfring $\overline{H}\,\overline{H}^{-1}$ containing all square elements of $\Phi(\xi)$, but not zero, which is a contradiction. (It is clear that $\overline{H}$ is a halfring larger than H, not containing zero and that $\overline{H}\,\overline{H}^{-1}$ has the same properties. Moreover, if a, $b \in \Phi$, $a\geqq 0$, $b<0$, $a^2>b^2u$, then both $-bu+a\xi$ and $(a+b\xi)(-bu+a\xi)=(a^2-b^2u)\xi$ belong to $\overline{H}$; hence $a+b\xi$ belongs to $\overline{H}\,\overline{H}^{-1}$. Now, if c, $d \in \Phi$ and $c+d\xi\neq 0$, then $(c+d\xi)^2\neq 0$, then $(c+d\xi)^2=a+b\xi$ when $a=c^2+d^2u\in H$, and $b=2cd$, $a^2-b^2u=(c^2-d^2u)^2>0$ so that indeed $(c+d\xi)^2$ belongs to $\overline{H}\,\overline{H}^{-1}$.) Hence every element of H is a square element of Φ and 1.1, 1.2 are satisfied by Φ.

If there were a polynomial $f(x)$ of odd degree with coefficients in Φ for which the equation

$$2.11 \qquad -1 \equiv \sum_{i=1}^{s} f_i(x)^2\ (f(x))$$

could be solved by polynomials $f_1(x), \cdots, f_s(x)$ with coefficients in Φ, then we could find among these $f(x)$ one of minimal degree $2n+1$. Upon substitution of the least remainders with regard to division by $f(x)$ it would follow that a relation 2.11 would obtain in which the maximum degree k of the polynomials $f_1(x), \cdots, f_s(x)$ would be not greater than $2n$.

Moreover, since Φ has an algebraic ordering we conclude that $n>0$ and that the coefficient of x^{2k} in

$$\sum_{i=1}^{s} f_i(x)^2$$

does not vanish, therefore the polynomial $1+\sum_{i=1}^{s} f_i(x)^2=f(x)g(x)$ is of degree $2k$ and consequently the polynomial $g(x)$ is of odd degree less than $2n+1$. But this is impossible in view of the congruence:

$$-1 = \sum_{i=1}^{s} f_i(x)^2\ (g(x))$$

and the minimal property of $f(x)$.

Hence, for a polynomial $f(x)$ of odd degree over Φ a relation of the form 2.11 never holds. On the other hand there must be a polynomial $g(x)$ of odd degree among the irreducible divisors of $f(x)$ in $\Phi[x]$. Since Ω is algebraically closed, there is a root ξ of $g(x)$ in Ω. As was shown above, no sum of square elements of the extension field $\Phi(\xi)$ can be equal to -1. This implies that the sums of finitely many nonzero square elements of $\Phi(\xi)$ form a halfring $\overline{H}$ containing H as well as all nonzero square elements of $\Phi(\xi)$. Because of the maximal property of H we conclude that $\overline{H}$ coincides with H, $\Phi(\xi)=\Phi$, $\xi\in\Phi$, Φ is really closed.

3. The ring extensions associated with an equation. Suppose that the polynomial

3.1. $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ with coefficients $a_0=1, a_1, a_2, \cdots, a_n$ in the commutative unital ring v has the root ξ in v then

$$f(x) = f(x) - f(\xi) = \sum_{h=0}^{n} a_{n-h}(x^h - \xi^h)$$

$$= (x-\xi)\sum_{h=1}^{n} a_{n-h}\left(\sum_{j=0}^{h-1} \xi^{h-j-1}x^j\right)$$

$$= (x - \xi)\frac{f}{x - \xi}(x)$$

where

3.2 $$\frac{f}{x - \xi}(x) = \sum_{j=0}^{n-1}\left(\sum_{h=0}^{n-1-j} a_{n-j-h-1}\xi^h\right)x^j.$$

Hence every root of the polynomial 3.2 is also a root of $f(x)$. Moreover, if v is an integral domain then every root of $f(x)$ that is not equal to ξ is also a root of 3.2. And if for some polynomial $g(x)$ of degree $n-1$ over v the equation $f(x) = (x-\xi)g(x)$ holds then $g(x) = f(x)/(x-\xi)$. This is because the equation for $g(x)$ allows us to determine recursively the coefficients of $g(x)$.

The preceding remarks motivate the following formal construction.

Let us denote by $v[\xi; f]$ the v-module with basis $1, \xi, \cdots, \xi^{n-1}$ over v. The rule

3.3 $$\begin{gathered} \xi_\tau(1) = \xi \\ \xi_\tau(\xi^i) = \xi^{i+1} \quad (0 < i < n-1) \\ \xi_\tau(\xi^{n-1}) = -a_1\xi^{n-1} - a_2\xi^{n-2} - \cdots - a_n 1 \\ \xi_\tau\left(\sum_{j=0}^{n-1} b_j\xi^j\right) = \sum_{j=0}^{n-1} b_j\xi_\tau(\xi^j) \quad (b_j \in v,\ 0 \leqq j < n) \end{gathered}$$

establishes a v-endomorphism ξ_τ of $v[\xi; f]$ satisfying the equation:

3.4 $$f(\xi_\tau) = 0$$

which is an equation for ξ_τ over v of minimal degree.

We define a multiplication on $v[\xi; f]$ by the rule:

$$\left(\sum_{h=0}^{n-1} k_h\xi^h\right)\eta = \sum_{h=0}^{n-1} k_h\xi_\tau^h(\eta)(\eta \in v[\xi; f])$$

which turns the v-module $v[\xi; f]$ into a commutative unital ring extension of v when the mapping $b \rightarrow b1 + 0\xi^1 + \cdots + 0\xi^{n-1}(b \in v)$ provides the embedding isomorphism of v into $v[\xi; f]$. The unit element of v also is the unit element of $v[\xi; f]$. Together with

$$\xi = 01 + 1\xi^1 + 0\xi^2 + \cdots + 0\xi^{n-1}$$

the ring v generates the v-ring $v[\xi; f]$ with v-basis $1, \xi, \xi^2, \cdots, \xi^{n-1}$ such that $f(\xi) = 0$. If in a commutative unital ring extension v^* of v for some element η of v the equation $f(\eta) = 0$ holds, then the mapping

$$\sum_{j=0}^{n-1} b_j\xi^j \rightarrow \sum_{j=0}^{n-1} b_j\eta^j(b_j \in v; 0 \leqq j < n)$$

provides a v-homomorphism of $v[\xi; f]$ into v^*.

Extending the preceding construction we define the commutative unital ring extension $v[\xi_1, \cdots, \xi_n; f]$ of v with $n!$ basis elements

$$\xi_1^{\nu_1}\xi_2^{\nu_2}\cdots\xi_n^{\nu_n} \quad (0 \leqq \nu_j < n - j; j=1, 2, \cdots, n)$$

over v as follows:

3.5 $$v[\xi_1, \cdots, \xi_n; f] = (v[\xi_1; f])[\xi_2, \cdots, \xi_n; f/(x - \xi_1)].$$

It follows that in $v[\xi_1, \cdots, \xi_n; f]$ there holds the factorization:

3.6 $$f(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_n)$$

of $f(x)$ into n linear factors.

THEOREM. 3 *The $n!$ permutations of the n distinct roots $\xi_1, \xi_2, \cdots, \xi_n$ of f determine automorphisms of $v[\xi_1, \cdots, \xi_n; f]$ such that the automorphism induced by the permutation π maps the polynomial expression $P(\xi_1, \xi_2, \cdots, \xi_n)$ on $P(\pi\xi_1, \cdots, \pi\xi_n)$ for any polynomial $P(x_1, \cdots, x_n)$. These $n!$ automorphisms form a group γ_n such that every element of v is fixed by every member of γ_n. The elements of v are the only elements of the ring $v[\xi_1, \cdots, \xi_n; f]$ that are fixed by γ_n.*

Proof. This is clear if $n=1$. Apply induction over n. Let $n>1$. The subset $\bar{v}$ of all elements of the ring extension that are fixed by γ_n is a subring containing v. Because of 3.5 and the induction assumption it follows that $\bar{v}$ is contained in $v[\xi_1]$. Applying a permutation automorphism interchanging ξ_1, ξ_2 to an element of $v[\xi_1]$ that is not contained in v, we obtain an element of $v[\xi_1]$ $[\xi_2]$ which is not contained in $v[\xi_1]$. Hence the theorem.

COROLLARY. (Theorem on symmetric functions.) *Let $R=v[x_1, x_2, \cdots, x_n]$ be the polynomial ring in n commuting independent variables $x_1, x_2, \cdots, x_n$ over v.* Let $s_i = \sum x_{\alpha_1}x_{\alpha_2} \cdots x_{\alpha_i} | 1 \leqq \alpha_1 < \cdots < \alpha_i \leqq n$ *be the i-th basic symmetric function $(1 \leqq i \leqq n)$. Then every polynomial in $x_1, x_2, \cdots, x_n$ over v that is fixed by all variable permutations (symmetric polynomial in $x_1, x_2, \cdots, x_n$) is equal to a polynomial in $s_1, s_2, \cdots, s_n$ over v.*

Proof. We note that, for the polynomial $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n$,

3.7 $$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n),$$

3.8 $$f(x_i) = 0 \quad (1 \leqq i \leqq n).$$

If v coincides with the rational integer ring $\mathbf{Z}$, then R is an integral domain. Hence

3.9 $$\frac{f(x_2)}{x - x_1} = 0.$$

Using the homomorphism of $Z[x_1, x_2, \cdots, x_n]$ into R which sends 1 into 1, x_i into $x_i (1 \leqq i \leqq n)$ we find that 3.9 always holds. By induction over n we conclude that there is a homomorphic mapping ψ of the ring extension $T = S[\xi_1 \cdots, \xi_n; f]$ over the subring S of R generated by v and $s_1, s_2, \cdots, s_n$ which maps ξ_i onto x_i. Clearly T is generated by v and $\xi_1, \xi_2, \cdots, \xi_n$, hence there is a homomorphism σ of R onto T over v mapping x_i onto $\xi_i (1 \leqq i \leqq n)$. We have $\sigma\psi = 1_T$, $\psi\sigma = 1_R$, hence σ, ψ are isomorphisms over v. Now the corollary follows from Theorem 3.

Let $\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_n$ be another set of n independent commuting variables over v and let $\bar{f}(x) = x^n - \bar{s}_1 x^{n-1} + \bar{s}_2 x^{n-2} - \cdots + (-1)^n \bar{s}_n$.

There is a homomorphism ϕ of the ring extension $\overline{T} = \overline{S}[\bar{\xi}_1, \cdots, \bar{\xi}_n; \bar{f}]$ of $\overline{S} = v[\bar{s}_1, \cdots, \bar{s}_n]$ onto T over v which maps $\bar{\xi}_i$ onto $\xi_i (1 \leqq i \leqq n)$ and hence $\bar{s}_i$ onto s_i. On the other hand, there is a homomorphism κ of R onto $\overline{T}$ over v mapping x_i onto $\bar{\xi}_i (1 \leqq i \leqq n)$ and we have: $\kappa\psi\phi = 1_{\overline{T}}$, $\phi\kappa\psi = 1_T$ therefore ϕ, $\kappa\psi$ are isomorphisms over v. It follows that the homomorphic mapping of $\overline{S}$ onto S over v which maps $\bar{s}_i$ onto $s_i (1 \leqq i \leqq n)$is an isomorphism. In other words the basic symmetric functions are independent over v.

From the theorem on symmetric functions it follows that the coefficients of the polynomials

$$S_j(f)(x) = \prod_{1 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_j \leq n} (x - (\xi_{\alpha_1} + \xi_{\alpha_2} + \cdots + \xi_{\alpha_j}))$$

of degree $\binom{n}{j}$ are in v. Moreover, if v is an integral domain in which the factorization $f(x) = \prod_{j=1}^{n} (x - \eta_j)$ obtains then the mapping of ξ_j onto $\eta_j (1 \leqq j \leqq n)$ can be extended in precisely one way to a homomorphism of $v[\xi_1, \cdots, \xi_n; f]$ onto v over v, and the equations $S_j(f)(\eta_{\gamma_1} + \cdots + \eta_{\gamma_j}) = 0$ hold whenever $1 \leqq \gamma_1 < \gamma_2 < \cdots < \gamma_j \leqq n$.

Assume that v is a field and that $S_2(f)$ has the root ξ in v. Let $d(x)$ be the greatest common divisor of the polynomials $f(x)$ and $f(\xi - x)$ in $v[x]$ with leading coefficient 1.

There holds an equation $d(x) = A(x)f(x) + B(x)f(\xi - x)$ with polynomials $A(x)$, $B(x)$ in $v[x]$. Hence in $v[\xi_1, \cdots, \xi_n; f]$:

$$d(x) = A(x)f(x) + B(x)f(\xi_1 + \xi_2 - x) + (\xi - \xi_1 - \xi_2)g(x, \xi_1 + \xi_2)$$

where $g(x, y)$ is a polynomial in two variables x, y over v. Upon substitution of ξ_2: $d(\xi_2) = (\xi - \xi_1 - \xi_2)g(\xi_2, \xi_1 + \xi_2)$.

If $d(x)$ would be a nonzero constant then $d(x) = 1 = d(\xi_2)$, hence $\xi - \xi_1 - \xi_2$ would be invertible in $v[\xi_1, \cdots, \xi_n; f]$. The same would apply to $\xi - \xi_i - \xi_k$ $(1 \leqq i < k \leqq n)$ and hence to the product.

But this product is equal to $S_2(f)(\xi)$ which is zero, a contradiction. Hence, $d(x)$ is not constant.

4. The fundamental theorem of algebra.

THEOREM 4. *Let F be a really closed field. The field extension E formed by the symbols $a + bi$ $(a, b \in F)$ with the operational rules*

4.1
$$\begin{gathered} a + bi = c + di \Leftrightarrow a = c,\, b = d \\ (a + bi) + (c + di) = (a + c) + (b + d)i \\ (a + bi)(c + di) = (ac - bd) + (ad + bc)i \\ (a, b, c, d \in F) \end{gathered}$$

is algebraically closed.

Proof. The field property of E is shown in the customary manner. The zero element of E is the symbol $0+0i$, the unit element of E is the symbol $1+0i$, the inverse of $a+bi$ is the symbol

$$\frac{a}{a^2 + b^2} + \left(\frac{-b}{a^2 + b^2}\right)i$$

provided not both of the elements a, b of F are zero. The mapping of a onto $a+0i$ provides an embedding isomorphism of F into E such that upon identification of a and $a+0i$ the field F becomes a subfield of E. The symbol $0+1i$ generates the quadratic extension E over F. Since $a+bi=(a+0i)+(b+0i)$ $(0+1i)$, we are entitled to denote the symbol $0+1i$ by i, so that $a+bi$ is the actual sum of the element a of F and the product of the element b of F by i. The element i is a root of the irreducible quadratic equation:

4.2 $$i^2 + 1 = 0$$

over F the other root being $-i$. Hence the complex conjugate mapping:

4.3 $$a + bi \rightarrow \overline{a + bi} = a - bi(a, b \in F)$$

establishes an involutoric automorphism of E over F. An element γ of E is in F if and only if its complex conjugate $\bar{\gamma}$ coincides with γ. The automorphism 4.3 is extended to an involutoric automorphism:

4.4 $$f(x) \rightarrow \bar{f}(x)$$

of $E[x]$ over $F[x]$ by setting

4.5 $$\bar{f}(x) = \bar{a}_0x^n + \bar{a}_1x^{n-1} + \cdots + \bar{a}_n$$

if

4.6 $$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n(a_0, a_1, \cdots, a_n \in E).$$

The polynomial 4.6 lies in $F[x]$ if it coincides with its complex conjugate polynomial $\bar{f}(x)$.

Let us further mention that for every element $a+bi$ of $E(a, b \in F)$ the equation

4.7 $$a + bi = (\xi + \eta i)^2(\xi, \eta \in F)$$

is solved in E by:

4.8
$$\xi = \left| \sqrt{1/2(a + \left| \sqrt{a^2 + b^2} \right|)} \right|$$
$$\eta = (\operatorname{sign} b) \cdot \left| \sqrt{1/2(-a + \left| \sqrt{a^2 + b^2} \right|)} \right|.$$

Our task is to find a root in E for every polynomial

4.9
$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$$

with coefficients $a_1, a_2, \cdots, a_n$ in E.

Let $n = 2^s n'$ when $0 \leqq s$, $n' \equiv 1(2)$.

If it would not always be possible to find a root in E for a given nonconstant polynomial, then there would be polynomials 4.9 with minimum value of s for which no root could be found in E and among those polynomials there would be a polynomial 4.9 with minimum value of n'.

If $s = 0$ and if all coefficients $a_1, a_2, \cdots, a_n$ are real then by assumption about F we can find a root of $f(x)$ in F, a contradiction.

If there is a root η of $S_2(f)$ in E then the greatest common divisor $d(x)$ of $f(x)$ and of $f(\eta - x)$ can be formed in $E[x]$. It is not constant as we have seen previously.

There holds an equation $f(x) = d(x)e(x)$ in $E[x]$ so that every root of $d(x)$ or $e(x)$ also is a root of $f(x)$. Since there is no root of $f(x)$ in E the same applies to the polynomials $d(x)$, $e(x)$. Because of the minimal property of $f(x)$ it follows that $d(x)$ has the same degree as $f(x)$ whereas $e(x)$ is a nonzero constant. In other words $f(x) = f(\eta - x)$ if $s > 0$. Or, setting $y = x - \eta/2$ we have

$$f(x) = g(y), \qquad g(y) = g(-y), \qquad g(y) = h(y^2), \qquad f(x) = h((x - \eta/2)^2)$$

when h is a polynomial of degree $n/2$ with coefficients in E.

It follows from this argument that $S_2(f)$ has no root in E if n is even. On the other hand, the degree of $S_2(f)$ is not divisible by 2^s, hence we can find a root of $S_2(f)(x)$ in E due to the minimal property of $f(x)$.

These arguments show that n is odd and that not all coefficients of $f(x)$ are real. But the degree of $f_1(x) = f(x)\bar{f}(x)$ is $2n$, the degree of $S_2(f_1)$ is the odd number $n(2n-1)$. Since $f_1(x)$ has real coefficients, also $S_2(f_1)$ has real coefficients. Therefore, $S_2(f_1)$ has a real root and by the argument given above $f_1(x)$ has a root ξ in E. Since $0 = f_1(\xi) = f(\xi)\bar{f}(\xi)$, but by assumption $0 \neq f(\xi)$ it follows that $0 = \bar{f}(\xi)$. Forming the complex conjugate of this equation we obtain $0 = f(\bar{\xi})$ so that $f(x)$ does have the root $\bar{\xi}$ in E which is a contradiction.

Thus we have established Theorem 4.

This existence proof can be reformulated so as to yield an algorithm:

I. If $s = 0$, $f(x) \in F[x]$ then we know by assumption how to find a root of f in F.

II. If the algorithm is defined already for polynomials of odd degree less than $2n+1$ with coefficients in E and if $f(x)$ is a polynomial of degree $2n+1$ with coefficients in E, then solve $S_2(f\bar{f})(\eta) = 0$ as in I. Form $d(x)$ as above. If $[d] \equiv 1$ (2) then $[d] < 2n+1$; apply the algorithm to find a root of d in E.

It turns out to be a root of f too. If $[d]\equiv 0(2)$, then the algorithm can be applied to $e(x)=(f/d)(x)$ and provides a root of e which turns out to be also a root of f.

Thus, the algorithm is obtained for solving in E equations of odd degree over E.

III. If $s>0$ and if the algorithm is defined for solving in E equations with coefficients in E such that either the degree is not divisible by 2^s or it is smaller than the degree of f and not divisible by 2^{s+1}, then apply the algorithm to the equation $S_2(f)(\eta)=0$ and form $d(x)$ as above. Apply the algorithm to $d(x)$ in case $2^s \nmid [d]$ or $2^{s+1}\nmid [d]$ and $[d]<[f]$. Apply the algorithm to f/d in case $[d]<[f]$, $2^{s+1}\mid [d]$. In either case, a root of f is obtained. If $[d]=[f]$, then form h as above. Apply the algorithm to h, to find a root ξ of h. As above we obtain the root $\eta/2+\sqrt{\xi}$ of f for finding a root.

However, the degrees of the auxiliary equations involved may become very large. E.g. for $n=8$ we may find the degrees 8,

$$\binom{8}{2}=28,\qquad \binom{28}{2}=378,\qquad \binom{378}{2}=71253.$$

But let us note that the binomial coefficient

$$\binom{n}{2^i}=\frac{2^s n'\cdot(n-1)\cdots(n-2^i+1)}{2^i\cdot 1\cdots(2^i-1)}$$

is divisible by 2^{s-i}, but not divisible by 2^{s-i+1} for $i=0, 1, 2, \cdots s$. Hence the same arguments also apply to the auxiliary equations:

$$f(x)=0,\qquad S_2(f)(x)=0,\qquad S_4(f)(x)=0,\cdots, S_{2^{s-i}}(f)(x)=0,\cdots$$
$$S_{2^s}(f)(x)=0.$$

Note that polynomial $S_{2^{s-1}}(f)$ is symmetric about $-(1/2)a_1$ in case $n=2^s$. Hence in that case it is of the form $g(x+(1/2)a_1)^2$ where $g(x)$ is of odd degree.

In any event we obtain considerable economy; e.g. for $n=8$ we have to form and to solve equations of degrees 8, 28, 2, 35.

Assuming that there exists an algorithm for finding the real roots of a polynomial 4.9. with real coefficients we extend it as follows to an algorithm for finding all the roots of $f(x)$

(1) If $\gcd(f, df/dx)=d(x)$ is not constant, let $(f/d)(x)=e_0(x)$, $\gcd(e_0, (df/dx))=e_1(x)$ not constant, $(e_0/e_1)(x)=f_1(x)$, $\gcd(e_{j-1}, (d^jf/dx^j))=e_j(x)$ not constant, $(e_{j-1}/e_j)(x)=f_j(x)$

$$\gcd\left(e_j, \frac{d^{j+1}f}{dx^{j+1}}\right)=1,\quad (j>0).$$

Hence $f(x)=f_1(x)f_2(x)^2\cdots f_j(x)^jf_{j+1}(x)^{j+1}$ when $f_1(x), f_2(x), \cdots, f_j(x), f_{j+1}(x)$ are mutually prime, separable polynomials.

The task is now to find the roots of these polynomials.

(2) $\gcd(f, df/dx)=1$, $f(x)$ has the real roots $\alpha_1, \alpha_2, \cdots, \alpha_r$, $f(x)=(x-\alpha_1)$

$(x-\alpha_2)\cdots(x-\alpha_r)g(x)$, $g(x)$ is separable and has no real root. The task is to find the roots of $g(x)$.

(3) $f(x)$ is separable and has no real root.

Find the real roots of $S_2(f(x))$ say $\beta_1<\beta_2<\cdots<\beta_\rho$. Normally speaking each of the real roots β_j is simple and in this case we have $\gcd(f(x), f(\beta_j-x)) = (x-\beta_j/2)^2+\gamma_j^2$ where γ_j is positive.

In this case the roots of $f(x)$ are the $n=2\rho$ complex numbers

$$\beta_j/2 \pm i\gamma_j \quad (1 \leqq j \leqq \rho).$$

If the real roots β_j are not all simple, a more elaborate algorithm must be carried out.

Let B_0 be the set of all roots β_j and let $\mu_0(\beta_j)$ be the multiplicity of the root β_j of $S_2(f)(x)$. Denote by A_1 the set of all elements of B_0 that are not the arithmetic mean of two distinct elements of B_0. We find that gcd $(f(x), f(\beta-x)) = \phi_\beta(x) = \phi_\beta(\beta-x)$ is nonconstant for any β of A_1. Hence $\phi_\beta(x) = h_\beta((x-\beta/2)^2)$ where $\phi_\beta(x)$ has degree $2\mu_0(\beta)$ and h_β is a polynomial with half the degree of $\phi_\beta(x)$ such that all roots of h_β are negative, say, they are of the form: $-\gamma_{\beta_k}$ $(1 \leqq k \leqq \frac{1}{2}\mu_0(\beta))$ when γ_{β_k} is positive. Hence the roots of $\phi_\beta(x)$ are the $\mu_0(\beta)$ complex numbers $\beta/2 \pm \gamma_{\beta_k} i$. If the total number of these roots is n then the task is completed.

If the total number is less than n then we determine for each member γ of B_0 that is not contained in A_1 the number of times, say $\nu_0(\gamma)$ that $\gamma = \frac{1}{2}(\beta+\beta')$ $(\beta, \beta' \in A_1, \beta<\beta')$ and

$$\gamma_{\beta_k} = \gamma_{\beta'_{k'}}(1 \leqq k \leqq \mu_0(\beta)/2,\ 1 \leqq k' \leqq \mu_0(\beta')/2).$$

In view of the connection between f and $S_2(f)$ we find that $\mu_1(\gamma) = \mu_0(\gamma) - 2\nu_0(\gamma) \geqq 0$ when $\mu_1(\gamma)$ is not always zero.

Let us form the set B_1 of all γ's for which $\mu_1(\gamma)$ is positive.

We proceed as above, substituting B_1 for B_0, μ_1 for μ_0, A_2 for A_1 when A_2 is the subset of all members of B_1 that are not an arithmetic mean of two distinct members of B_1. In this way some further roots of $f(x)$ will be obtained. If not yet all of them are found, proceed as before until all n roots are constructed.

References

1. E. Artin, Kennzeichnung des Körpers der reellen algebraischen Zahlen, Abhg. Math. Sem. Univ. Hamburg, 3 (1924) 170–175.

2. E. Artin und O. Schreier, Algebraische Konstruktion reeller Körper, Abh. Math. Sem. Univ. Hamburg, 5 (1927) 85–99.

3. E. Artin und O. Schreier, Eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Univ. Hamburg, 5 (1927) 225–231.

4. Carl Friedrich Gauss, Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse, Inaugural dissertation, Göttingen, 1799.

5. Nathan Jacobson, Lectures in Abstract Algebra, Vol. III, Van Nostrand, Princeton, N. J., 1951.

6. Oskar Perron, Algebra, 3rd ed., Berlin, 1951.

7. Wolfgang Krull, Elementare und klassische Algebra vom modernen Standpunkt, Berlin 1963 (see last chapter).

8. Hans Zassenhaus, The Theory of Groups, 2nd ed., Chelsea, New York, 1958.

9. Max Zorn, A remark on a method in transfinite algebra, Bull. Amer. Math. Soc. 41 (1935) 667–670.

PSEUDOPOLYHEDRONS

J. R. GOTT, III, Mayme S. Waggener High School, Louisville, Kentucky

A regular generalized polyhedron may be defined as a network of congruent regular polygons connected vertex to vertex so that the number and arrangement of polygons around every vertex is the same. The five regular polyhedrons and the three regular tessellations are the familiar examples of regular generalized polyhedrons. In the regular polyhedrons the sum of the face angles around any vertex is less than 360°. In the regular tessellations the sum of the face angles around a vertex is equal to 360°. The regular polyhedrons approximate positively curved surfaces (spheres), while the regular tessellations approximate surfaces with 0 curvature (planes).

We may define a third group of regular generalized polyhedrons in such a way that they will share the properties of the regular polyhedrons and tessellations but will have the sum of the face angles around a vertex greater than 360°. I have called such a group of figures regular pseudopolyhedrons. I have chosen the name pseudopolyhedrons (or false polyhedrons) because while possessing many of the properties of polyhedrons they are in some aspects distinctly different. A similar convention was used in naming a specific negatively curved surface, the pseudosphere. The pseudosphere has similar properties to the sphere except that it is negatively, instead of positively, curved. By the same token it will be shown later that the pseudopolyhedrons possess similar properties to the polyhedrons except that they approximate negatively curved surfaces.

I have defined a regular pseudopolyhedron as follows:

A regular pseudopolyhedron is a network in space of congruent regular polygons fitted together vertex to vertex so that (1) every vertex is surrounded by the same number and arrangement of polygons; (2) the sum of the face angles around every vertex is greater than 360°; (3) just two polygons may meet at an edge; and (4) two polygons may share no more than one edge.

Except for condition (2), the definition is identical with that of the regular polyhedrons and the regular tessellations.

I have found seven regular pseudopolyhedrons which satisfy the conditions of this definition. These are diagrammed in Figures 1–7. Each is a repeating structure with an infinite number of faces. In the diagrams the structural form of each is presented. Each of the pseudopolyhedrons is a surface which divides