R. Loos: Computing in Algebraic Extensions. In: Buchberger, Collins, Loos (eds.): Symbolic and Algebraic Computation. Springer, Wien, 1983

3. Resultant Calculus

Let $A = \sum_{i=0}^{m} a_i x^i$ and $B = \sum_{i=0}^{n} b_i x^i$ be two polynomials over a commutative ring R with identity. The Sylvester matrix of A and B is the $m+n$ by $m+n$ matrix

$$M = \begin{pmatrix} a_m & a_{m-1} & \cdots & & a_0 & & \\ & a_m & a_{m-1} & \cdots & & a_0 & \\ & & \cdots\cdots\cdots & & & & \\ & & & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\ & b_n & \cdots & & & b_0 & \\ & & \cdots\cdots\cdots & & & & \\ & & & b_n & \cdots & & b_0 \end{pmatrix}.$$

The upper part of M consists of n rows of elements of A, the lower part of m rows of elements of B, where all entries not shown are zero. The *resultant* of A and B is defined by

$$\operatorname{res}(A, B) = \det(M).$$

Clearly the resultant is an element of R and we have

$$\operatorname{res}(A, B) = (-1)^{mn} \operatorname{res}(B, A), \tag{1}$$

$$\operatorname{res}(aA, B) = a^n \operatorname{res}(A, B), \qquad a \in R. \tag{2}$$

By definition

$$\operatorname{res}(a, B) = a^n, \qquad a \in R,$$

$$\operatorname{res}(a, b) = 1, \qquad a, b \in R. \tag{3}$$

With m indeterminates α_i, $1 \leqslant i \leqslant m$, we construct

$$A_m(x) = \prod_{i=1}^{m} (x - \alpha_i) = \sum_{i=0}^{m} a_i^{(m)} x^i.$$

Clearly, we will be interested mainly in the case where the roots of $A_m(x)$ are substituted for the indeterminates α_i. But all resultant relations in this section will be derived without the assumption of the existence of roots, thus with the weaker assumption that the α_i are indeterminates. The coefficients a_i are related to the indeterminates α_i by

$$\begin{aligned} a_m^{(m)} &= s_m = 1, \\ -a_{m-1}^{(m)} &= s_{m-1} = \alpha_1 + \cdots + \alpha_m, \\ a_{m-2}^{(m)} &= s_{m-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{m-1}\alpha_m, \\ &\cdots \\ (-1)^m a_0^{(m)} &= s_0 = \alpha_1\alpha_2 \cdots \alpha_m, \end{aligned}$$

where the s_i are the elementary symmetrical polynomials.

The coefficients $a_i^{(m)}$ are linear in α_m. Let us define $A_{m-1}(x) = A_m(x)/(x - \alpha_m)$. Between the coefficients of A_m and A_{m-1} considered as polynomials in the α_i's the relation

$$a_{i-1}^{(m-1)}(\alpha_1, \ldots, \alpha_{m-1}) = a_i^{(m)}(\alpha_1, \ldots, \alpha_{m-1}, 0), \qquad 1 \leqslant i \leqslant m \tag{4}$$

holds.

We are now ready to prove the

Lemma. *Let $B(x)$ be a polynomial over an integral domain R, $\deg(B) > 0$, and let $m > 1$ be an integer. With m indeterminates α_i let $A_m(x) = \prod_{i=1}^{m}(x - \alpha_i)$ and $A_{m-1}(x) = A_m(x)/(x - \alpha_m)$. Then*

$$\operatorname{res}(A_m, B) = B(\alpha_m)\operatorname{res}(A_{m-1}, B).$$

Proof. For $1 \leqslant i < m + n$ add to the last column of the Sylvester matrix M of A_m and B α_m^{m+n-i} times the ith column. For the resulting matrix M_1 we have $\det(M_1) = \det(M)$ and the elements of the last column from top to bottom are $\alpha_m^{n-1}A_m(\alpha_m), \ldots, \alpha_m^0 A_m(\alpha_m), \alpha_m^{m-1}B(\alpha_m), \ldots, \alpha_m^0 B(\alpha_m)$. Since $A_m(\alpha_m) = 0$ we take the factor $B(\alpha_m)$ out of the last column resulting in a matrix M_2 with the last column $0, \ldots, 0, \alpha_m^{m-1}, \ldots, \alpha_m^0$ and

$$\operatorname{res}(A_m, B) = \det(M) = \det(M_1) = B(\alpha_m)\det(M_2). \tag{5}$$

Let us consider both sides of (5) as polynomials in α_m. Since M has n rows of coefficients of $A(\alpha_m)$, which are at most linear in α_m, the left-hand side is of degree n or less in α_m. On the right-hand side the factor $B(\alpha_m)$ is already of degree n. Since R is an integral domain $\det(M_2)$ is of degree 0 in α_m. Taking $\det(M_2)$ at $\alpha_m = 0$ the last column becomes now $0, \ldots, 0, 0, \ldots, 1$ and the coefficients of A_m are transformed into the coefficients of A_{m-1} according to (4). Expansion of $\det(M_2)|_{\alpha_m = 0}$ with respect to the last column results in the $m + n - 1$ by $m + n - 1$ matrix with $\det(M_3) = \det(M_2) = \operatorname{res}(A_{m-1}, B)$ which together with (2) proves the lemma. ■

Theorem 1 immediately follows, which represents the resultant as symmetrical polynomial in the indeterminates α_i [14].

Theorem 1. *Let $A(x) = a_m \prod_{i=1}^{m}(x - \alpha_i)$ and $B(x) = b_n \prod_{i=1}^{n}(x - \beta_i)$ be polynomials over an integral domain R with indeterminates $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$. Then*

$$\operatorname{res}(A, B) = (-1)^{mn} b_n^m \prod_{i=1}^{n} A(\beta_i), \tag{6}$$

$$\operatorname{res}(A, B) = a_m^n \prod_{i=1}^{m} B(\alpha_i), \tag{7}$$

$$\operatorname{res}(A, B) = a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j). \tag{8}$$

Proof. The theorem holds for $m = 0$ or $n = 0$ with the convention $\prod_{i=k}^{l} f_i = 1$, for $l < k$. Eq. (6) follows from (7) by (1), also (8) follows from (7) immediately. We prove (7) by induction on m. $\operatorname{res}(A_1, B) = B(\alpha_1)$, where $A_1(x) = x - \alpha_1$, follows from the expansion of the determinant with respect to the last row. Now by (2),

$\operatorname{res}(A, B) = a_m^n \operatorname{res}(A_m, B)$ and an inductive application of the Lemma results in (7). ■

We state now some resultant relations in which the indeterminates α_i do not occur.

Theorem 2. *Let $A(x)$ and $B(x)$ be polynomials of positive degree over a commutative ring R with identity. Then there exist polynomials $S(x)$ and $T(x)$ over R with* $\deg(S) < \deg(B)$ *and* $\deg(T) < \deg(A)$ *such that*

$$AS + BT = \operatorname{res}(A, B). \tag{9}$$

Theorem 2 is a special instance of (1) in the chapter on polynomial remainder sequences.

Theorem 3. *Let A, B_1 and B_2 be polynomials over an integral domain. Then*

$$\operatorname{res}(A, B_1 B_2) = \operatorname{res}(A, B_1) \operatorname{res}(A, B_2). \tag{10}$$

Proof.

$$\operatorname{res}(A, B_1 B_2) = a_m^{n_1 + n_2} \prod_{i=1}^{m} (B_1(\alpha_i) B_2(\alpha_i)) = \operatorname{res}(A, B_1) \operatorname{res}(A, B_2). \quad ■$$

Theorem 4. *Let A, B, Q be polynomials over an integral domain and let* $\deg(A) = m$, $\operatorname{lc}(A) = a_m$, $\deg(B) = n$, $\deg(AQ + B) = l$. *Then*

$$\operatorname{res}(A, AQ + B) = a_m^{l-n} \operatorname{res}(A, B). \tag{11}$$

Proof. Again we use (7).

$$\operatorname{res}(A, B) = a_m^n \prod_{i=1}^{m} B(\alpha_i) = a_m^n \prod_{i=1}^{m} (A(\alpha_i) Q(\alpha_i) + B(\alpha_i)) = a_m^{n-l} \operatorname{res}(A, AQ + B). \quad ■$$

Theorem 3 may be used to increase the efficiency of the resultant calculation whenever a factorization of one of the polynomials is known. For example by (10) $\operatorname{res}(A, x^k B) = \operatorname{res}(A, B) \prod_{l=1}^{k} \operatorname{res}(A, x)$ and by (6)

$$\operatorname{res}(A, x) = (-1)^m A(0) = (-1)^m a_0.$$

Therefore

$$\operatorname{res}(A, x^k B) = (-1)^{mk} a_0^k \operatorname{res}(A, B). \tag{12}$$

Let $\deg(A) - \deg(B) = k \geqslant 0$. Then Eq. (12) together with (1) shows also that there is no loss of generality in the assumption that the polynomials of the resultant are of a specific degree as we stated in the chapter on polynomial remainder sequences.

Theorem 4 suggests an alternative way to calculate the value of the resultant. Moreover, it provides a proof of the next theorem, sometimes called the standard theorem on resultants [9], which follows immediately from (8), without any reference to the indeterminates α_i and β_i in (8).

Theorem 5. *Let A and B be non-zero polynomials over an integral domain R. Then* $\operatorname{res}(A, B) = 0$ *if and only if* $\deg(\gcd(A, B)) > 0$.

Proof. The theorem holds if A or B is constant. Assume $\deg(A) \geqslant \deg(B) > 0$. Working over the quotient field Q of R let $A = P_1$, $B = P_2$, $P_i = Q_i P_{i+1} + P_{i+2}$, $1 \leqslant i \leqslant k-2$, $k \geqslant 3$, be a polynomial remainder sequence, thus

$$\deg(P_1) \geqslant \deg(P_2) > \cdots > \deg(P_k) \geqslant 0, \qquad P_{k+1} = 0.$$

Let $n_i = \deg(P_i)$ and set $A = P_{i+1}$, $B = P_{i+2}$ and $Q = Q_i$ in (11). Using also (1) we obtain

$$\operatorname{res}(P_i, P_{i+1}) = (-1)^{n_i n_{i+1}} \operatorname{lc}(P_{i+1})^{n_i - n_{i+2}} \operatorname{res}(P_{i+1}, P_{i+2}), \tag{13}$$

or

$$\operatorname{res}(P_1, P_2) = \operatorname{res}(P_{k-1}, P_k) \prod_{i=i}^{k-2} (-1)^{n_i n_{i+1}} \operatorname{lc}(P_{i+1})^{n_i - n_{i+2}}, \tag{14}$$

where lc denotes the leading coefficient.

If $\deg(P_k) = \deg(\gcd(A, B)) = 0$ then $\operatorname{res}(P_{k-1}, P_k) = \operatorname{lc}(P_k)^{n_{k-1}} \neq 0$ by (3). Otherwise we apply (11) again and since $P_{k+1} = 0$ the resultant vanishes. ■

In [5] efficient algorithms for resultant calculation are given which are finally based on Eq. (14). They are superior to an evaluation of the determinant of the Sylvester matrix. In fact, the maximum computing time to calculate the resultant of two r-variate polynomials of maximal degree n and maximal seminorm d is $O(n^{2r+1}L(d) + n^{2r}L(d)^2)$.

4. Arithmetic in the Field K of All Algebraic Numbers over $\mathbb{Q}$

First we consider arithmetical operations on algebraic numbers. The following theorem gives the arithmetic in the field K of all algebraic numbers over $\mathbb{Q}$:

Theorem 6 (Loos 1973). *Let $A(x) = a_m \prod_{i=1}^{m} (x - \alpha_i)$ and $B(x) = b_n \prod_{j=1}^{n} (x - \beta_j)$ be polynomials of positive degree over an integral domain R with roots $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ respectively. Then the polynomial*

$$r(x) = (-1)^{mn} g a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - \gamma_{ij})$$

has the $m \cdot n$ roots, not necessarily distinct, such that

(a) $r(x) = \operatorname{res}(A(x-y), B(y))$, $\gamma_{ij} = \alpha_i + \beta_j$, $g = 1$,

(b) $r(x) = \operatorname{res}(A(x+y), B(y))$, $\gamma_{ij} = \alpha_i - \beta_j$, $g = 1$,

(c) $r(x) = \operatorname{res}(y^m A(x/y), B(y))$, $\gamma_{ij} = \alpha_i \beta_j$, $g = 1$,

(d) $r(x) = \operatorname{res}(A(xy), B(y))$, $\gamma_{ij} = \alpha_i / \beta_j$, $B(0) \neq 0$, $g = (-1)^{mn} B(0)^m / b_n^m$.

Proof. The proof is based on relation (6) in all four cases.

(a)
$$\operatorname{res}(A(x-y), B(y)) = (-1)^{mn} b_n^m \prod_{j=1}^{n} A(x - \beta_j)$$
$$= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - (\alpha_i + \beta_j)).$$

(b) $$\operatorname{res}(A(x+y), B(y)) = (-1)^{mn} b_n^m \prod_{j=1}^{n} A(x+\beta_j)$$
$$= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - (\alpha_i - \beta_j)).$$

(c) $$\operatorname{res}(y^m A(x(y), B(y)) = (-1)^{mn} b_n^m \prod_{j=1}^{n} \beta_j^m A(x/\beta_j)$$
$$= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - \alpha_i \beta_j).$$

(d) $$\operatorname{res}(A(xy), B(y)) = (-1)^{mn} b_n^m \prod_{j=1}^{n} A(x\beta_j)$$
$$= (-1)^{mn} a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x\beta_j - \alpha_i)$$
$$= (-1)^{mn} a_m^n \prod_{i=1}^{m} b_n \left(\prod_{j=1}^{n} \beta_j \right) \prod_{j=1}^{n} (x - \alpha_i/\beta_j)$$
$$= (-1)^{mn} a_m^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - \alpha_i/\beta_j) \quad \text{mit} \quad b_0 \neq 0. \ \blacksquare$$

Theorem 6 constructs explicit polynomials and we see that, except in case (d) the polynomial $r(x)$, to within a sign, is monic if A and B are. We have therefore

Corollary 1. *All algebraic integers over R form a ring.*

We denote the ring by R_∞.

Corollary 2. *All algebraic numbers over R form a field.*

We denote the field by K, where Q is the quotient field of R.

Since the degree of $r(x)$ is $m \cdot n$, the resultants are linear in the particular case the given polynomials are. We conclude that the rational numbers over R form a subfield Q of K and that R forms a subring of R_∞. We convince ourselves that R_∞ is an integral domain by considering Theorem 6, case (c) with $A(0) = 0$, $r(0) = \operatorname{res}(y^m A(0), B(y))$. By (1), (2), (3) and (12), we find $r(0) = A(0)^n b_n^m$. Since R has no zero divisors the same holds for R_∞.

Theorem 6 is the base of Algorithm 1. Obviously, it is sufficient to consider only addition and multiplication of algebraic numbers. For if the number α is defined by the polynomial $A(x)$, then the polynomial $A(-x)$ defines $-\alpha$ and $x^m A(1/x)$, $m = \deg(A)$, defines $1/\alpha$ if $\alpha \neq 0$.

Algorithm 1 (Algebraic number arithmetic).

Input: Let R be an Archimedian ordered integral domain. α, β are algebraic numbers represented by two isolating intervals I, J having endpoints in Q and by two defining polynomials A and B of positive degree over R.

Output: An isolating interval K and a defining primitive squarefree polynomial $C(x)$ representing $\gamma = \alpha + \beta$ (or $\gamma = \alpha * \beta$ for multiplication).

(1) [Resultant]
$r(x) = \operatorname{res}(A(x - y), B(y))$
($r(x) = \operatorname{res}(y^m A(x/y), B(y))$ for multiplication).

(2) [Squarefree factorization] $r(x) = D_1(x)D_2(x)^2 \cdots D_f(x)^f$.

(3) [Root isolation] Generate isolating intervals or rectangles $I_{11}, \ldots, I_{1g_1}, \ldots, I_{fg_f}$ such that every root of D_i is contained in exactly one I_{ij} and $I_{ij} \cap I_{kl} = \emptyset$, $1 \leqslant i, k \leqslant f$, $1 \leqslant j \leqslant g_i$, $1 \leqslant l \leqslant g_k$, $(i,j) \neq (k,l)$.

(4) [Interval arithmetic] Set $K = I + J$ ($I * J$ for multiplication) using exact interval arithmetic over Q.

(5) [Refinement] If there is more than one I_{ij} such that $K \cap I_{ij} \neq 0$, bisect I and J and go back to step (4). Otherwise, return K and $C(x) = D_i(x)$. ■

Note that the computing time of the algorithm is a polynomial function of the degrees and seminorms of α and β. In practical implementation it may be preferable to replace in step 2 the squarefree factorization by a complete factorization, which would give the algorithm an exponential maximum computing time.*

The effectiveness of step (3) depends essentially on a non-algebraic property of the underlying ring R, its Archimedean order. A ring is *Archimedean ordered* if there exists for every element A a natural number (i.e. a multiple of the identity of the ring) N such that $N - A > 0$. Let us for example take the non-Archimedean ordered ring of polynomials over the rationals, $\mathbb{Q}[x]$, where an element is called positive if the leading coefficient is positive. Thus the element x is greater than any rational number and there is no assurance that an interval or rectangle containing x can be made arbitrarily small by bisection. It is still possible to count the zeros in intervals over non-Archimedean rings by Sturm's theorem, but root isolation requires Archimedean order.

The loop in step (4) and step (5) is only executed a finite number of times, since by Theorem 6 exactly one isolating interval contains the sum $\alpha + \beta$ (or the product $\alpha * \beta$) and bisection decreases the length of the interval K, computed by exact interval arithmetic, under any bound. Therefore, the input assumption of the Archimedean order enforces the termination of the algorithm.

The proof of the theorem is based on the relation (6) which in turn follows immediately from Lemma 1. We will show, using the equivalent relation (7), how similar constructions of defining polynomials for algebraic numbers can be established. If α is defined by A, we consider the norm $N_\alpha = \operatorname{res}_\alpha(A(\alpha), \cdot)$ as a polynomial operator with indeterminate α. In order to compute any function $g(\alpha)$ composed finally by ring operations on α only, we have to apply the operator N_α to $x = g(\alpha)$ yielding

$$N_\alpha(x - g(\alpha)) = \operatorname{res}_\alpha(A(\alpha), x - g(\alpha)) = a_m^n \prod_{i=1}^{m} (x - g(\alpha_i))$$

which shows that $N_\alpha(x - g(\alpha))$ is a polynomial having $g(\alpha)$ as root. By iteration, the method can be extended to any polynomial function of several algebraic numbers. Let α, β be defined by A and B respectively. In order to compute, say $f(\alpha, \beta) = \alpha + \beta$, we form

$$\begin{aligned} N_\alpha(N_\beta(x - f(\alpha, \beta))) &= \operatorname{res}_\alpha(A(\alpha), \operatorname{res}_\beta(B(\beta), x - (\alpha + \beta))) \\ &= \operatorname{res}_\alpha\left(A(\alpha), b_n \prod_{i=1}^{n} (x - (\alpha + \beta_j))\right) \\ &= a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x - (\alpha_i + \beta_j)) \end{aligned}$$

which is up to a sign the defining polynomial of Theorem 6, (a). In fact, the method can still be further generalized. All that is required is that the relation $x = f(\alpha, \beta)$ may be transformed into a polynomial relation, say $F(x, \alpha, \beta)$. The following theorem gives an application. Let us consider fractional powers of algebraic numbers. Since the reciprocal of an algebraic number can be computed trivially we restrict ourselves to positive exponents.

Theorem 7 (Fractional powers of algebraic numbers). *Let A be a polynomial of positive degree m over an integral domain R with roots $\alpha_1, \ldots, \alpha_m$. Let p, q be positive integers. Then*

$$r(x) = \operatorname{res}(A(y), x^q - y^p)$$

has the roots $\alpha_i^{p/q}$, $i = 1, \ldots, m$.

Proof.

$$r(x) = a_m^p \prod_{i=1}^{m} (x^q - \alpha_i^p). \quad \blacksquare$$

We can base on Theorem 7 an algorithm for the computation of fractional powers of algebraic numbers, which would be quite similar to Algorithm 1.

Another application of our algebraic number calculus allows a transformation of the algebraic number representation in $\mathbb{Q}(\alpha)$ as a polynomial $\beta = B(\alpha)$ to a defining polynomial for β. We get $N_\alpha(x - B(\alpha))$ as defining polynomial for β.

Theorem 8. *Let α be an algebraic number over R and A its defining polynomial of degree $m > 0$. Let $\beta = \sum_{x=0}^{m-1} b_i \alpha^i = B(\alpha)$, where $b_i \in Q$, $\deg(B) = n < m$. Then β is algebraic over R and a root of*

$$r(x) = \operatorname{res}(x - B(y), A(y)).$$

If α is an algebraic integer then so is β, provided $b_i \in R$.

Proof. By Theorem 1, Eq. (6), $r(x) = (-1)^{mn} a_m^n \prod_{i=1}^{m} (x - B(\alpha_i))$. $\blacksquare$

Corollary 3. *If A of Theorem 8 is the minimal polynomial of α then B is uniquely determined.*

Proof. Suppose $\beta = B^*(\alpha)$, $\deg(B^*) < m$ and $B^* \neq B$. $B(\alpha) - B^*(\alpha) = \beta - \beta = 0$.

This is a polynomial, not identically vanishing, of degree $< m$, a contradiction to the minimal property $\deg(A) = m$. ■

Theorem 8 can be used to compute the sign of a real algebraic number differently from the approach in Section 1. Given $\beta = B(\alpha)$, we construct $r(x)$ from the theorem and compute $I_\beta = B(I_\alpha)$ by interval arithmetic such that I_β is isolating with respect to $r(x)$. The position of I_β in relation to 0 gives the sign of β. The position in relation to I_α, made disjoint from I_β, gives an algorithm for real algebraic number comparison.

Historical Note. The resultant $\mathrm{res}_y(A((x-y)/2), A((x+y)/2))$ was considered by Householder in [8] and stimulated our interest in resultants.

A special case of Theorem 6 is the resultant $\mathrm{res}_y(A(x+y), A(y))$, a polynomial having the roots $\alpha_i - \alpha_j$. The task of obtaining lower bounds on $\min_{i,j} |\alpha_i - \alpha_j|$ is reduced by it to the problem of a lower bound for the roots of $r(x)/x^m$. By this approach Collins [6] improved Cauchy's [4] lower bound for the minimum root separation.

5. Constructing Primitive Elements

The representation $\beta = B(\alpha)$ allows the construction of extensions of R and Q as shown by the next two theorems.

Theorem 9. *Let α be an algebraic integer over R and A its defining polynomial of degree $m > 1$. Then the set of all algebraic numbers represented by $\beta = \sum_{i=0}^{m-1} b_i \alpha^i = B(\alpha)$, where $b_i \in R$, forms a ring of algebraic integers.*

We call the ring a *simple extension of* R and denote it by $R[\alpha]$.

Proof. Since $C(x) = Q(x)A(x) + B(x)$, where $B = 0$ or $\deg(B) < m$, and $A(\alpha) = 0$ we have $B(\alpha) = C(\alpha)$. Hence, there is an isomorphism between $R[\alpha]$ and $R[x]/(A(x))$, the ring of residue classes of A. ■

Theorem 10. *Let α be an algebraic number over a field Q and A its defining polynomial of degree $m > 0$. Then the set of all algebraic numbers represented by $\beta = \sum_{i=0}^{m-1} b_i \alpha^i = B(\alpha)$, where $b_i \in Q$, forms a field.*

We call the field a *simple algebraic extension of* Q and denote it by $Q(\alpha)$.

Proof. We have to show that every non-zero element β of $Q(\alpha)$ has a multiplicative inverse. First, assume $\deg(\gcd(A(x), B(x))) = 0$. By Theorem 5, $\mathrm{res}(A, B) \neq 0$. Theorem 2 gives, for $x = \alpha$, $B(\alpha)T(\alpha) = \mathrm{res}(A, B)$ with $\deg(T) < m$. Therefore, $T(\alpha)/\mathrm{res}(A, B)$ is the inverse of $B(\alpha)$. Now, let $C(x) = \gcd(A, B)$, $\deg(C) > 0$, and $A = CA^*$. Clearly, $C(\alpha) \neq 0$, otherwise $\beta = B(\alpha) = 0$. Therefore, $A^*(\alpha) = 0$. Replace A by A^* and apply the first argument of the proof, observing that $\deg(\gcd(A^*, B)) = 0$. ■

Extensions $Q(\alpha)$ are called *separable*, if the defining polynomial for α is squarefree.

Clearly, $R \subseteq R[\alpha] \subset R_\infty$. Since R_∞ was shown to be an integral domain the same holds for $R[\alpha]$. Also $Q \subseteq Q(\alpha) \subset K$. All previous results remain valid with $R[\alpha]$ and $Q(\alpha)$ in place of R and Q respectively. In particular $R[\alpha][\beta]$ is a ring and $Q(\alpha)(\beta)$ a