On Multiplicative Properties of the Algebra of Test-Functions

by

A. Uhlmann

Theoretisch-Physikalisches Institut der Karl-Marx-Universität, Leipzig.
Abstract

An analogue of Euclid's algorithm is valid in the algebra of test-functions $R$ for quantum fields. From this a number of conclusions may be derived.

For instance: The intersection of any two main right ideals $aR$ and $bR$ is a right ideal $dR$. $aR + bR$ is a main right ideal iff $d \neq 0$. The prime factor decomposition is non-unique generally. However, there is a function $a \rightarrow \lfloor a \rfloor$ with $\lfloor ab \rfloor = \lfloor a \rfloor + \lfloor b \rfloor$ and $\lfloor a \rfloor = 1$ iff $a$ is prime. There are "large" semi-groups with unique prime factor decomposition.
0. Introduction.

Let us denote by $R$ the algebra of test functions (see 1)\textsuperscript{2} and below) for scalar hermitian fields\textsuperscript{3}. A scalar hermitian quantum field may be considered as a symmetric representation

$$A: \quad a \mapsto A(a), \quad a \in R \quad (0-1)$$

by unbounded operators in a Hilbert space. Now it is straightforward, that in its domain of definition the operator

$$A(a + 1) \quad \text{with} \quad a = a^* \quad (0-2)$$

is bounded from the below by one. If the operator $A(a)$ turns out to be essentially self-adjoint, the inverse of (0-2) is well defined and can be extended to a bounded operator.

More generally let us denote by $N$ the set of all the elements $b$ of $R$ with the property: In every symmetric representation (0-1) the operator $A(b)$ is in its domain of definition bounded from the below by a real number larger than zero.

The set $N$ is multiplicatively closed in $R$ and one can construct a canonical extension $\overline{R}$ of $R$ such, that every element of $N$ is invertible. Therefore the finite sums

$$\sum b^{-1} \quad \text{with} \quad b \in N \cap N^* \quad (0-3)$$

constitute a symmetric subalgebra of this extension $\overline{R}$ and we may try to consider such an algebra of test functions for Haag–Araki fields.

However, the aim of this paper is not to achieve such constructions (a paper on this subject is under preparation), but rather to give same results on the multiplicative structure of the elements of $R$.

These results shall be used in the constructions mentioned above.

1. Definition of $R$.

We denote by $S_n$ the linear space of test functions for the tempered distributions of $n$ space–time points. $S_0$ denotes the ring of
complex numbers. Further we consider "functions" over the non-
negative integers, the values of which for the integer $n$ is in
$S_n$,

$$a: \quad n \rightarrow a(n) = a(n;x_1,x_2,\ldots,x_n) \in S_n \quad (1-1)$$

and with $a(n) = 0$ for all but a finite set of integers.

The picture $a(n)$ of $a$ under the map $(1-1)$ is called the
$n$th component of $a$. If not all components of $a$ are zero, there
is an integer $n$ with $a(n) \neq 0$ and $a(m) = 0$ for all $m$
larger than $n$. Then the integer $n$ is the degree of $a$ and it
will be denoted by the symbol $|a|$. The component $a(n)$ with
$n = |a|$ will be called the highest component of $a$. Sometimes
it is convenient to define $|a| = -\infty$ iff $a(n) = 0$ for all
integers.

$R$ becomes a symmetric algebra by the definitions

$$(a + b)(n) = a(n) + b(n), \quad (\lambda a)(n) = \lambda \cdot a(n) \quad (1-2)$$

$$(ab)(n) = \sum_{i=0}^{n} a(i;x_1,\ldots,x_i)b(n-i;x_{i+1},\ldots,x_n) \quad (1-3)$$

$${a^*}(n;x_1,\ldots,x_n) = a(n;x_n,x_{n-1},\ldots,x_1) \quad (1-4)$$

(The bar denotes complex conjugation.) We denote the unit element
of $R$ by $e$. It is defined by $e(0) = 1$, $e(n) = 0$ for $n > 0$.

We mention that there is a natural topology for $R$ (see 1, 2).

From the definition of the degree we conclude

$$|ab| = |a| + |b| \quad (1-5)$$

$$|a + b| \leq \max (|a|, |b|). \quad (1-6)$$

If one knows $|a| \neq |b|$ then the equality sign holds in $(1-6)$.

For the set of elements with $a(m) = 0$ if $m \neq n$ the map $(1-1)$
is an isomorphism onto $S_n$. Therefore we may identify $S_n$ with a
subset of $R$. In doing so we refer the elements of $S_n$ sometimes
as "homogeneous elements of degree $n"$.

An element $a$ of $R$ is said to be prime iff its degree is larger
than zero and no decomposition

$$a = a_1a_2 \text{ with } |a_1| > 0 \quad (1-7)$$
exists\(^4\). (The first condition excludes the zero of \(R\) and the invertible elements of \(R\) from being prime.)

If the degree of an element \(a\) is larger than zero, there always exists by virtue of (1-5) at least one decomposition
\[
a = p_1 p_2 \cdots p_n
\]
(1-8)

with prime elements \(p_i\) and clearly the number \(n\) has to be not larger than the degree of \(a\).

(Obviously all elements of the first degree are prime elements.)

Definition of \([a]\):

If \(|a| > 0\) the following natural number: There exists a decomposition \(a = p_1 p_2 \cdots p_n\) with \([a] = n\) and \(p_i\), \(i = 1, 2, \ldots, n\) prime. Further, if \(a = q_1 q_2 \cdots q_m\) denotes another decomposition of \(a\) in prime elements, it is \(m \leq n = [a]\).

It is always
\[
|a| \geq [a]
\]
(1-9)

and the prime elements are characterized by \([a] = 1\).

Furthermore one has
\[
[a \ b] \geq [a] + [b]
\]
(1-10)

Later on we shall see that the equality sign always holds in (1-10).

On the other hand let us mention that for some elements the prime factor decomposition is essentially non-unique. \(\forall\) see this denote by \(u\) and \(t\) two homogeneous elements of the first degree with \(u \neq t u\) and consider the decomposition
\[
(a + t u) = (a + u t) u.
\]
(1-11)
The right as well as the left side of equation (1-11) is a product of prime factors. However, the two prime factors \(a + tu\) and \(a + uf\) are not equivalent.

\([a]\) we denote by \([a]\)
2. Homogeneous elements.

The results of this paper are almost trivial for homogeneous elements of $R$. However, these elements do not belong to the class mentioned in the introduction.

**Lemma 1**: Let be $a \in R$ homogeneous and consider two prime factor decompositions

$$a = p_1p_2 \cdots p_n = q_1 \cdots q_m.$$  \hspace{1cm} (2-1)

Then we have $n = m$ and there are complex numbers

$$\lambda_i; \text{ with } p_i = \lambda_i q_i, \quad i = 1, \ldots, n.$$  

Furthermore the prime elements $p_i$ are homogeneous ones.

**Proof**: Let use first mention that the component of lowest degree of the product of two non-zero elements equals the product of the lowest components of its factors. The same is true for the component of highest degree. Hence the product of two elements turns out to be homogeneous if and only if its factors are homogeneous ones.

Because there are no zero divisors in $R$ (as may be seen from (1-5) for instance) the statement is simply proved by induction, provided we know $p_1 = \lambda_1 q_1$ for every homogeneous element $a$.

Rewrite (2-1) into $p_1 b_1 = q_1 b_2$ and assume $/p_1/ \geq /q_2/ = s$, $/a/ = n$.

Now we choose points $\beta_1, \ldots, \beta_{n-s}$ such that the function $b_2$ is different from zero on the point $(\beta_1, \ldots, \beta_{n-s})$ of the product of $n-s$ Minkowski spaces. It follows

$$p_1(x_1, \ldots, x_r) b_1(n-x, \beta_{r+1}, \ldots, \beta_n) = q_1(s; x_1, \ldots, x_s) b_2(n-s; x_{s+1}, \ldots, x_r, \beta_{r+1}, \ldots, \beta_n).$$

Because of our assumption on the $\beta$'s, the last factor on the right hand side of this equation is not the zero of $R$. Therefore $p_1$ is not prime if $r \neq s$. But from $r = s$ the last factors of the right hand as well as of the left hand side are non-vanishing constants. Hence we have the desired equation $p_1 = \lambda_1 q_1$. 

Induction with respect to the degree or with respect to the number \( [a] \) now proves Lemma 1.

Next we consider some consequences of lemma 1. Assume

\[
\begin{align*}
a \cdot b &= b \cdot a \\
(2-2)
\end{align*}
\]

for two homogeneous elements of \( R \). If neither \( a \) nor \( b \) is the zero and if \( |a| \geq |b| \), then there is an homogeneous element \( c \) with

\[
\begin{align*}
a &= b \cdot c \\
|c| &= |a| - |b| \\
(2-3)
\end{align*}
\]

Namely, because of lemma 1, the prime factor decomposition of \( b \) coincides with the beginning of the prime factor decomposition of \( a \).

We may use this information for a further study of the relation (2-2). Assume \( |a| > 0 \) for the homogeneous element \( a \).

Define the set

\[
N = \{ b \in R : \quad ab = ba, \quad |b| > 0 \} \\
(2-4)
\]

Denote by \( d \) an element of \( N \) having the smallest degree of all elements of \( N \). Then the assertion is

\[
N = \{ b \in R : \quad b = \lambda d^s, \quad \lambda \text{ constant} \} \\
(2-5)
\]

Proof: First we have \( a = d^r c \) by the argument leading from (2-2) to (2-3). If \( b \in N \) we therefore have \( dcb = bdc \). Because the degree of \( b \) is not smaller than that of \( d \), we conclude equal well \( b = d^f \) for the arbitrary element \( b \) of \( N \).

For given \( b \in N \) we define \( r \) to be the largest natural number for which an equation \( b = d^r \) \( g \) is valid. The elements \( b \) and \( d \) commute with \( a \) and hence

\[
d^r (g \cdot a - a \cdot g) = 0.
\]

Therefore \( g \) commutes with \( a \). Hence \( |g| = 0 \), because otherwise \( g \in N \) and there should exist a decomposition \( g = d \cdot h \) and this contradicts the choice of the number \( r \). But \( |g| = 0 \) indicates
that \( g \) is a constant.

As a first application we prove:

**Theorem 1:**

Every two commuting elements of \( R \) are algebraically dependent.

**Proof:** Assume

\[
 a_1 a_2 = a_2 a_1, \quad /a_1/ = n, \quad /a_2/ = m, \quad n \geq m \quad (2-6)
\]

Without loss of generality we may assume \( m > 0 \). From (2-6) it follows that the highest components of the elements under consideration are commuting too. Hence there is an homogeneous element \( h \) with

\[
 a_1(n) = \lambda_1 h^s_1, \quad a_2(m) = \lambda_2 h^s_2.
\]

Now we consider two independent free variables \( \xi, \eta \). The number of linear independent polynomials of the form

\[
 \sum \alpha_{i_k} \xi^i \eta^k; \quad i + k \leq r \quad (2-7)
\]

equals

\[
 (r+1)(r+2)/2.
\]

Now we estimate the number of linear independent elements of \( R \) of the form

\[
 \sum \alpha_{i_k} a_1^i a_2^k; \quad i + k \leq r. \quad (2-8)
\]

The degree of such an element does not exceed \( r n_0 \). Every element (2-8) commutes with \( a_1 \) and \( a_2 \) and therefore the highest component of such an element is of the form \( \lambda h^s \) with \( r n \geq /h/s \).

Hence there are at most

\[
 1 + r n_0, \quad \text{with} \quad n_0 = n /h^{-1},
\]

linear independent elements of the form (2-8). Evidently, for sufficient large \( r \), the number \( (r+1)(r+2)/2 \) is larger than
1 + r n_q. Hence there is a polynomial (2-7), not vanishing identically, with
\[ \sum x_{1k} a_1^k a_2^k = 0. \]

3. The Euclidian algorithm.

In this section we shall establish an analogue to Euclid's algorithm for the naturals. We start with

**Lemma 2:** Consider any two elements \( a \) and \( b \) with \( b \neq 0 \). Then there is at most one element \( t \) satisfying
\[ |a - bt| < |b| \]  \hspace{1cm} (3-1)

To prove this we assume \( |a - bu| < |b| \). From this and (3-1) we conclude \( |(a - bt) - (bu - a)| < |b| \). Therefore \( |b| + |u - t| < |b| \). Because \( b \) is different from the zero, the number \( |b| \) is finite. Therefore \( |u - t| < 0 \) and hence \( u = t \).

**Theorem 2:** Let us assume for the four elements \( a, b, p, q \) of \( R \) the relation
\[ a p = q b, \quad |a| \geq |q| \]  \hspace{1cm} (3-2)

There exists an element \( t \) satisfying
\[ |a - qt| < |q| \]
\[ |b - tp| < |p| \]  \hspace{1cm} (3-3)

**Proof:** Let us abbreviate \( |a| = n, |b| = m, |p| = r, |q| = s \).

It is \( n + r = m + s \). We have to show the existence of an element \( t \) satisfying for all \( k \) with \( 0 \leq k \leq n - s \) the equation
\[ a(n-k) = \sum_{j=0}^{\infty} q(s-j) t(n-s-k+j) \]  \hspace{1cm} (3-4)

\[ b(m-k) = \sum_{j=0}^{\infty} t(m-r-k+j) p(r-j) \]  \hspace{1cm} (3-5)

Here we assume, that i.e. \( p(1) = 0 \) if \( i \) becomes negative.
The proof proceeds by complete induction.

First step: Assume \( k = 0 \). Then we have

\[
a(n) \ p(r) = q(s) \ b(m) . \tag{3-6}
\]

Because only homogeneous elements are involved here, there is an element \( t(n-s) \) with

\[
a(n) = q(s) \ t(n-s) \tag{3-7}
\]

and inserting in the equation (3-6) we find

\[
b(m) = t(m-r) \ p(r) , \ n-s = m-r . \tag{3-8}
\]

Hence the equations (3-4) and (3-5) are valid for \( k = 0 \).

Second step: We now assume that our assertion is correct for all numbers \( k \) with \( 0 \leq k < 1 \leq n - s = m - r \) and for the homogeneous elements \( t(n-s-k) \). We then consider

\[
(a \ p)(n+r-1) = (q \ b)(m+s-1) \tag{3-9}
\]

and rewrite both sides of this equation as following:

\[
(ap)(n+r-1) = a(n-1)p(r) + \sum_{j=1}^{\infty} a(n-1+j)p(r-j) \tag{3-10}
\]

\[
= a(n-1)p(r) + \sum_{j=1}^{\infty} \sum_{l=0}^{\infty} q(s-l)t(n-s+l-1+j) p(r-j)
\]

and

\[
(qb)(m+s-1) = q(s)b(m-1) + \sum_{j=1}^{\infty} \sum_{l=0}^{\infty} q(s-j)t(m-r+j+l-1) p(r-1)
\]

The left hand sides of (3-10) and (3-11) are equal and the right hand sides would be identical if the index \( l \) only runs over \( l = 1, 2, \ldots \). Therefore we have to have the equation

\[
q(s)b(m-1) + \sum_{j=1}^{\infty} q(s-j)t(m-r+j+l-1) p(r) = \tag{3-12}
\]

\[
a(n-1)p(r) + \sum_{j=1}^{\infty} q(s) t(n-s+j-1) p(r-j)
\]

or

\[
q(s) \left[ \begin{array}{c}
b(m-1) - \sum_{j=1}^{\infty} t(n-s+j-1) p(r-j) \\
a(n-1) - \sum_{j=1}^{\infty} q(s-j)t(m-r+j-1)
\end{array} \right] = \tag{3-13}
\]

\[
p(r)
\]
Now \( q(s) \) is different from the zero and the number \( n-1 \) is not smaller than the number \( s \). Hence there exists an homogeneous element \( t(n-1-s) \) with

\[
a(n-1) - \sum_{j=1}^{\infty} q(s-j)t(m-r+j-1) = q(s)t(n-1-s) \quad (3-14)
\]

Inserting this into (3-13) and remembering that \( p(r) \) is not the zero we get

\[
b(m-1) - \sum_{j=1}^{\infty} t(n-s+j-1)p(r-j) = t(n-1-s)p(r) \quad (3-15)
\]

But the equations (3-14) and (3-15) are identical with (3-4) and (3-5) for \( i = k \). This completes the proof.

Remark: As one can see, it is not necessary for the proof to consider the equality \( (ap)(j) = (qb)(j) \) for \( j < r+s \). Hence the conclusion of theorem 2 is valid if only

\[
|ap - qb| < |a| + |p|, \quad |a| \geq |q| \quad (3-16)
\]

is satisfied. The equation \( |a| + |p| = |q| + |b| \) is a consequence of (3-16).

4. Right main ideals

The set of all elements \( ab, b \in R \) with fixed \( a \) constitutes a main right ideal of \( R \) that shall be called \( aR \).

Theorem 3

For any two elements \( a_1 \) and \( a_2 \) of \( R \) there is an element \( d \in R \) with

\[
a_1 R \cap a_2 R = dR \quad (4-1)
\]

If \( d \) is not the zero of \( R \), there exists an element \( a \) of \( R \) with

\[
a_1 R + a_2 R = aR \quad (4-2)
\]

In the latter case we have

\[
|d| + |a| = |a_1| + |a_2| \quad (4-3)
\]
Proof: Define

\[ J = a_1 R + a_2 R, \quad s = |a_1| + |a_2| . \quad (4-4) \]

The theorem is valid, if \( J \) consists only of the zero of \( R \), because in this case we have \( d = 0 \). Now we assume, that at least one element different from the zero is contained in \( J \) and proceed with the aid of complete induction with respect to \( s \).

If \( s = 0 \), the theorem is true and we may choose \( a = d = e \).

We now assume, that the assertion is correct for all \( s < n \) and we consider the case with \( s = n \). Let be \( d \in J \) an element different from the zero of \( R \). There are elements \( b_1, b_2 \) with

\[ d = a_1 b_2 = a_2 b_1 \quad (4-5) \]

and because of theorem 2 there is an element \( t \) of \( R \) satisfying

\[ |a_1 - a_2 t| < |a_2|; \quad |b_1 - tb_2| < |b_2| \]

and hence \( |a_1 - a_2 t| + |a_2| < n \).

If \( a_1 = a_2 t \), we can choose \( d = a_1 \) and \( a = a_2 \) and the assertion is true. If \( a_1 \neq a_2 t \), we find

\[(a_1 - a_2 t) b_2 = a_2 (b_1 - t b_2) \neq 0 \]

and therefore the right ideal

\[ J_1 = (a_1 - a_2 t) R \cap a_2 R \]

does not consist of the zero only and we are in the domain of our induction assumptions.

Therefore there are elements \( d_1 \) and \( a \) with

\[ J_1 = d_1 R \quad \text{and} \quad (a_1 - a_2 t) R + a_2 R = a R \quad (4-6) \]

and with

\[ |d_1| + |a| = |a_2| + |a_1 - a_2 t| \quad (4-7) \]

Because of (4-6) we are allowed to write

\[ a_1 R + a_2 R = a R . \]
Next we consider the equation

\[(a_1 - a_2 t) \circ_2 = a_2 \circ_1 = d_1\]  \hspace{1cm} (4-8)

which follows from the first equation of (4-6). Hence we may write

\[d = a_1 \circ_2 = a_2 (\circ_1 + a_2 t) \in J.\]  \hspace{1cm} (4-9)

From (4-7) and (4-8) it follows that

\[- \dot{d} = \dot{a}_1 + \dot{a}_2 = \dot{a}_1 + \dot{a}_2 - \dot{a}_1 - \dot{a}_2 t = - \dot{a}_1 + \dot{a}_2 - \dot{d}\]

is valid. Now we prove \(J = d R\) and to this purpose it is sufficient to show \(\tilde{d} \in d R\), for \(\tilde{d}\) has been chosen as an arbitrary element of \(J\), different from the zero. Now we have

\[\frac{(a_1 - a_2 t) b_2}{d} = d_1 b = (a_1 - a_2 t) c_2 b\]

because the right-hand side of the last equation is in \(J\) and because of equ. (4-8). Hence \(b_2 = c_2 b\) and

\[\tilde{d} = a_1 b_2 = a_1 \circ_2 b = d b \in d R.\]

Remark: One can explicitly construct the element \(a\) of the theorem with the help of the "Euclidean algorithm": There are elements \(a_3, \ldots, a_n = a\) and elements \(t_1, \ldots, t_{n-2}\) with

\[a_k = a_{k+1} t_k + a_{k+2}, \hspace{0.5cm} k=1, \ldots, n-2\]  \hspace{1cm} (4-10)

and

\[\frac{a_1}{a_2} > \frac{a_2}{a_3} > \cdots > \frac{a_{k+1}}{a_{k+2}}, \hspace{0.5cm} k=2, \ldots, n-1.\]  \hspace{1cm} (4-11)

Because of lemma 2, the elements \(t_k\) and \(a_j\) are uniquely determined by \(a_1\) and \(a_2\). To construct the element \(d\) one has to consider the elements

\[b_n = a_n; \hspace{0.5cm} b_k = t_k b_{k+1} + b_{k+2}, \hspace{0.5cm} k=1, \ldots, n-2\]  \hspace{1cm} (4-12)

Then it follows

\[d = a_1 b_2 = a_2 b_1\]  \hspace{1cm} (4-13)

Now we come to the following
Lemma 3: Let \( p \) be a prime and \( b \) an arbitrary element of \( R \). It exists an element \( q \) with \( bR \cap pR = bq_R \).

If \( /q/ > 0 \), then \( q \) is a prime element.

Proof: The existence of the element \( q \) is provided by theorem 3. Let us assume \( q = q_1q_2 \). We have

\[
bq_1R \cap pR \supseteq bq_1q_2R = bR \cap pR \supseteq bq_1R \cap pR
\]  

(4-14)

Hence

\[
bq_1R \cap pR = bR \cap pR = bq_1q_2R.
\]

If this ideal is not the zero ideal, we can write

\[
bq_1 + pR = aR
\]  

(4-15)

by theorem 3. Because \( p \) is a prime element we can choose either \( a = p \) or \( a = e \). If \( a = p \) we conclude via

\[
bq_1 \in pR \quad \text{that} \quad bq_1R \subseteq bq_1q_2R \quad \text{is valid. Hence} \quad /q_2/ = 0.
\]

If \( a = e \) we have \( bR + pR = R \) also. From this and (4-15) we find with the aid of the degree relation (4-3)

\[
/bq_1/ + /p/ = /b/ + /p/
\]

and this means \( /q_1/ = 0 \). Thus in every decomposition

\[
q = q_1q_2 \quad \text{at least one factor is of the first degree, i.e.} \quad q
\]

is prime if its degree is larger than zero.

Next we prove

Theorem 4: It is always

\[
[a] + [b] = [ab]
\]  

(4-16)

and every prime factor decomposition

of an element \( a \neq 0 \) consists of exact \([a]\)

prime factors.

To prove this, we mention first that it is sufficient to consider the second assertion of the theorem. We use induction with respect to the degree of \( a \). If \( /a/ = 1 \) we conclude at once that

\[
[a] = 1
\]

and hence \( a \) is prime. Let us now assume the assertion is correct for all elements with degree less than \( n \). If
\[ a = p_1 \cdots p_r = q_1 \cdots q_s, \quad \sqrt[\alpha]{a} = n \]

We may distinguish two possibilities: If \( p_1R = q_1R \) we may assume \( p_1 = q_1 \). By the assumption of our induction we then have \( r = s \).

Now, if \( p_1R \neq p_2R \) we can use theorem 3 and lemma 3 to show the existence of two prime elements \( p \) and \( q \) with

\[ p_1p = q_1q. \]

With a certain \( b \) we have

\[ a = p_1pb = q_1qb \]

or

\[ pb = p_2 \cdots p_r \quad \text{and} \quad qb = q_2 \cdots q_s. \]

We see that we can use the assumption of our induction for \( pb \) and \( qb \) and for \( b \). Therefore \( \left[ pb \right] = \left[ b \right] + 1 = \left[ qb \right] \) and \( r = s \).

5. Strongly prime elements

Definition:

An element \( p \) of \( R \) is called \( rs \)-prime ("strongly prime from the right"), iff \( a \notin pR \) and \( b \notin pR \) always implies \( ab \notin pR \).

\( p \) is called \( ls \)-prime, iff \( a \notin Rp \) and \( b \notin Rp \) always implies \( ab \notin Rp \).

We call \( p \) \( s \)-prime, iff it is \( rs \)-prime as well as \( ls \)-prime.

Remark:

If \( p \) is \( rs \)-prime, then it is prime. If the degrees of \( a \) and \( b \) are larger than zero and if \( p = ab \), then neither \( a \) nor \( b \) is contained in \( pR \). The same applies for \( ls \)-prime elements.

We mention a simple consequence: If a product \( a_1a_2 \cdots a_n \) is contained in \( pR \) with \( rs \)-prime element \( p \), it follows that at least one of the factors \( a_1 \) is contained in \( pR \).

The existence of \( s \)-prime elements is given by the following lemmata.
Lemma 4: The element $p$ is rs-prime if it satisfies the following condition: If $|p| \leq |a|$ and $pR \cap aR$ does not contain of the zero only, then either $pR = aR$ or $aR = R$.

Proof: Assume $ab = pd$ but $a \notin pR$. If $aR \neq R$ then $|p| > |a|$ and there is an element $t$ with $|a - pt| < |p|$ and $(a - pt)b \in pR \cap (a-pt)R$. Obviously $a - pt \neq 0$, because otherwise $a \in pR$. Now the assertion of lemma 4 tells us $(a - pt)R = R$.

Hence

$$ab = (pt + \lambda e)b = pd \quad \text{with} \quad \lambda \neq 0$$

and therefore

$$b = pd - ptb \in pR.$$  

i.e. $b$ is contained in $pR$ and $p$ is rs-prime.

Lemma 5:

Under the assumptions $|a| = n$ and $a(n)$ is prime, the element $a$ of $R$ is s-prime.

Proof: First part: Assume $aR \cap bR \neq \{0\}$. It follows that there is an equation

$$a(n)c_1(s_1) = b(m)c_2(s_2), \quad |b| = m$$

with homogeneous elements $c_1(s_1)$. Namely there is an equation of the form $ac_1 = bc_2$ by assumption and for the $c_1(s_1)$ we take the highest components of the $c_1$.

Now assume $|a| > |b|$ it follows (lemma ...)

$$a(n) = b(m)t \quad \text{with} \quad |t| > 0$$

But $a(n)$ is a prime element and hence $|b(m)| = 0$ i.e.

$|b| = 0$. Now by virtue of lemma 4 the element $a$ is rs-prime.

Second part: The assumptions of our lemma apply with $a$ to $a^*$ also. Hence $a^*$ is rs-prime and $a = (a^*)^*\neq 0$ is ls-prime.

We conclude that $a$ is s-prime.
We now come to some questions of uniqueness of prime factor decompositions. We start with

**Lemma 6**: Assume \( a \notin pR \) and \( aR \cap pR \neq \{0\} \). If \( p \) turns out to be rs-prime, we have

\[
pR \cap aR = apR.
\]  
(5-1)

If \( aR = R \), the assertion is trivially valid. In the other case we have \( pR \cap aR = aqR \) with a certain prime \( q \) according to lemma 3. Now \( aq \in pR \), \( a \notin pR \) and \( p \) rs-prime. Hence by definition \( q \in pR \). But \( q \) is prime and therefore \( pR = qR \).

A simple consequence is the following:

**Lemma 7**: If both elements, \( p \) and \( q \), are rs-prime and if

\[
pR \cap qR \neq 0,
\]
we have \( pq = qp \).

Namely, from lemma 6 it follows \( pqR = qpR \) i.e.

\[
pq = \lambda \text{ qp with a complex number } \lambda.
\]
The last equation remains true for the highest components of \( p \) and \( q \) and because of lemma 1 we must have \( \lambda = 1 \).

Let us now consider two prime factor decompositions of an element:

\[
a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_n
\]  
(5-2)

(Because of theorem 4 the number of prime factors is always the same.) We shall call the two decompositions equivalent if and only if the following is true: 1) With suitable permutation of the numbers \( 1, \ldots, n \) we have

\[
p_i = \lambda; \quad q_{k_i}, \quad i = 1, \ldots, n
\]  
(5-3)

with some complex numbers \( \lambda; \). 2) If this permutation is not the identity permutation we can write it as a product of transpositions of the form

\[
\begin{align*}
\{ j \mapsto (j + 1) \} \quad \text{with} \quad q_j q_{j+1} &= q_{j+1} q_j
\end{align*}
\]  
(5-4)
An element of $R$ is said to have an essentially unique prime factor decomposition, iff every two of its prime factor decompositions are equivalent.

**Theorem 5:** If one of the prime factor decompositions of an element $a \in R$ consists of $s$-prime factors only, the the element has an essentially unique prime factor decomposition.

**Proof:** We prove the theorem by induction with respect to the length of an element. If $[a] = 1$, the assertion is trivial. Now let us consider an equation (5–2) under the assumptions that firstly our assertion is true for elements of length smaller than $n$ and that secondly the factors $P_1$ in (5–2) are $s$-prime ones. If $P_1R = q_1R$ we may devide by $P_1$ and the assumption of the induction establish the theorem for elements of length $n$. In the other case we conclude with the help of the definition of $s$-prime elements that $q_2 \cdots q_n \in P_1R$ and for $a$ is contained in $P_2R \cap q_1R$, there is an prime element $r_1$ with $q_1P_1 = P_1r_1$ (see lemma 6).

Now either $P_1R = q_2R$ or $q_2 \cdots q_n \in P_1R$ and there is an element $r_2$ with $q_2P_1 = P_1r_2$ by the same argument. Going further on this line we see: There is an integer $s$ with $P_1R = q_sR$, there are prime elements $r_1, \ldots, r_{s-1}$ with $q_kP_1 = P_1r_k$. Hence we may rewrite (5–2) as

$$P_1 \cdots P_n = q_1 \cdots q_{s-1}P_1q_{s+1} \cdots q_n \beta = P_1 \cdots r_{s-1}q_{s+1} \cdots q_n \beta$$

with complex constant $\beta$. Now, after deviding by $P_1$, we make use of our assumption and conclude that the elements $r_1, \ldots, r_{s-1}, q_{s+1}, \ldots, q_n$ are $s$-prime. Because $P_1R \cap Rr_k$ is not the zero ideal, we have by an obvious extension of lemma 7 to left main ideals.
\[ p_k r_k = r_k p_1 = q_k p_1, \quad r_k = q_k \] (5-5)

Equation (5-5) tells us: After some transpositions of the type (5-4) we are allowed to divide by \( p_1 \) and we may use the assumption of our induction a second time showing that \( p_2 \ldots p_n \) and \( q_2 \ldots q_{s-1} q_{s+1} \ldots q_n \) are equivalent decompositions. This proves our assertion by induction. The following theorem and lemma show that rs-prime elements have remarkable simple properties.

**Theorem 6:**

Assume \( p \) to be rs-prime. An element \( a \) commutes with \( p \) if and only if \( a \) is a polynomial in \( p \). If \( a \) is prime, this polynomial is of the first degree.

**Proof:** Take \( a \neq 0 \). Because of \[ [p, a] = 0 \] there are polynomials \( q_k(x) \) with

\[ p^n q_0(a) + p^{n-1} q_1(a) + \ldots + q_n(a) = 0 \] (5-6)

for a certain \( n \). We may assume \( q_n \not\equiv 0 \) (otherwise we divide by a power of \( p \)). Now we have

\[ q_n(a) \in pR \] (5-7)

and on the other hand there is a decomposition

\[ q_n(a) = \prod (a - \lambda_k) \] (5-8)

Thus, with a complex number \( \lambda \), we conclude

\[ a - \lambda e \in pR \] (5-9)

because \( p \) is rs-prime. Now we start an induction: There are elements \( a_1 \) and complex numbers \( \lambda \) with

\[ a - \lambda e = p a_1, \quad [p, a_1] = 0 \] (5-10)

\[ a_1 - \lambda_1 e = p a_2, \quad [p, a_2] = 0 \]

\[ \ldots \]

\[ a_s - \lambda_s e = p a_{s+1}, \quad [p, a_{s+1}] = 0 \]

and

\[ |a| > |a_1| > |a_2| > \ldots > |a_{s+1}| \] (5-11)
The procedure ends by arriving, for a certain $s$, at $a_{s+1} = 0$, $a_s \neq 0$. Hence the resolution of (5-10) shows, that $a$ is a polynomial in $p$. Because every prime polynomial with complex coefficients in one variable is linear in the variable the second part of the assertion is established too.

**Corollary:** Let $p$ be $rs$-prime. The set of all elements commuting with $p$ constitutes a maximal commutative subalgebra of $R$.

**Lemma 8:** Let be $p$ $rs$-prime and consider an arbitrary complex number $\beta$. The element $p - \beta e$ is a prime element.

For the proof we are allowed to choose $\beta = 1$ because with $p$ also its multiples have to be $rs$-prime. Now assume $p - e = ab$, a prime. We get $pa = a(ba + e)$. If $aR \neq pR$ we have $(ba + e) \in p$.

From $/ba + e/ = /p/$ we conclude $ba + e = \beta_1 p$. Therefore $pa = \beta_1$ and $\beta_1 = 1$. It follows that $a$ is a polynomial in $p$ (theorem 6). Because $a$ is prime, it has to be linear in $p$. Therefore $/p - e/ = /p/$ and hence $/b/ = 0$. If $aR = pR$, $a$ is prime trivially.
References:


(4) This concept is sometime denotes by "indecomposable" and the word "prime" is used in the sense of our "s-prime". In the proofs we have tried to use standard arguments of the theory of commutative rings.