Division in Associative $D$-Algebra

Aleks Kleyn

Abstract. From the symmetry between definitions of left and right divisors in associative $D$-algebra $A$, the possibility to define quotient as $A \otimes A$-number follows. In the paper, I considered division and division with remainder. I considered also definition of prime $A$-number.

Contents

1. Preface ................................................................. 1
2. Conventions ............................................................ 2
3. Geometry of Quotients ............................................... 3
4. Division in $D$-Algebra .............................................. 4
5. Division with Remainder ............................................ 5
6. Highest Common Factor ............................................. 9
7. Prime $A$-number .................................................... 9
8. References ............................................................ 10
9. Index ........................................................................ 11
10. Special Symbols and Notations .................................. 12

1. Preface

Let $D$ be commutative ring. Let $D$-algebra $A$ be associative.

Definition 1.1. $A$-number $a$ is left divisor of $A$-number $b$, if there exists $A$-number $c$ such that

\[(1.1) \quad ac = b \]

Definition 1.2. $A$-number $a$ is right divisor of $A$-number $b$, if there exists $A$-number $c$ such that

\[(1.2) \quad ca = b \]
It is evident that there is symmetry between definitions 1.1 and 1.2. The difference between left and right divisors is also evident since the product is noncommutative. However we can consider a definition generalizing definitions 1.1 and 1.2.

We may consider quotient of $b$ divided by $a$ as tuple of numbers $c$, $d$ such that
\[ cad = b \]

However we may consider division from another point of view.

Equations (1.1), (1.2) are examples of linear maps of $D$-algebra $A$. For commutative product, the equation (1.1) is only definition of linear map. For noncommutative product, $A \otimes A$-number generates linear map of $D$-algebra $A$. For instance, the tensor $c \otimes d$ is $A \otimes A$-number. Thus, we get the following definition.

**Definition 1.3.** $A$-number $a$ is divisor of $A$-number $b$, if there exists $A \otimes A$-number $c$ such that
\[ c \circ a = b \]

$A \otimes A$-number $c$ is called quotient of $A$-number $b$ divided by $A$-number $a$. □

In the paper [2], I considered equation
\[ c \circ x = b \]

In this paper, I consider equation
\[ x \circ a = b \]

$D$-algebra $A$ is called division algebra, if for any $A$-number $a \neq 0$ there exists $A$-number $a^{-1}$.

2. Conventions

**Convention 2.1.** Element of $D$-algebra $A$ is called $A$-number. For instance, complex number is also called $C$-number, and quaternion is called $H$-number. □

**Convention 2.2.** Let $A$ be $\Omega_1$-algebra. Let $B$ be $\Omega_2$-algebra. Notation
\[ A \rightarrow B \]

means that there is representation of $\Omega_1$-algebra $A$ in $\Omega_2$-algebra $B$. □

---

1Here somebody can argue that division is the inverse operation of multiplication. If product is commutative, then it follows from expression
\[ ca = b \]

that

- $c$ is factor; the product of $c$ and $a$ is equal to $b$.
- $c$ is quotient of $b$ divided by $a$.

Thus, for commutative product, definitions of factor and quotient coincide. For noncommutative product, we distinguish right and left divisors; therefore, we distinguish left and right quotient.

2Since the map
\[ a \rightarrow cad \]

is bilinear, then, according to the theorem [3]-3.6.4, we may consider the map
\[ a \rightarrow (c \otimes d) \circ a \]

instead of the map (1.3)
Convention 2.3. Let $A$ be associative $D$-algebra. The representation

$$\begin{align*}A \otimes A & \xrightarrow{f} A \\ f(p) : a \to p \circ a\end{align*}$$

of $D$-module $A \otimes A$ generates the set of linear maps. This representation generates product $\circ$ in $D$-module $A \otimes A$ according to rule

$$(p \circ q) \circ a = p \circ (q \circ a)$$

Without a doubt, the reader may have questions, comments, objections. I will appreciate any response.

3. Geometry of Quotients

Theorem 3.1. Let real field $R$ be subfield of the center $Z(D)$ of the ring $D$. Then, for any $A$-numbers $a, b$, the set of quotients is convex.

Proof. Let $A \otimes A$-number $c$ be quotient of $A$-number $b$ divided by $A$-number $a$

$$c \circ a = b$$  \hspace{1cm} (3.1)

Let $A \otimes A$-number $d$ be quotient of $A$-number $b$ divided by $A$-number $a$

$$d \circ a = b$$  \hspace{1cm} (3.2)

Then, for any $t \in R$, $0 \leq t \leq 1$, from (3.1), (3.2), it follows that

$$(tc + (1-t)d) \circ a = (tc) \circ a + ((1-t)d) \circ a$$

$$= t(c \circ a) + (1-t)(d \circ a) = tb + (1-t)b = b$$

Therefore, $A \otimes A$-number $tc + (1-t)d$ is quotient of $A$-number $b$ divided by $A$-number $a$.

Theorem 3.2. Let $A \otimes A$-numbers $c, d$ be quotients of $A$-number $b$ divided by $A$-number $a$

$$c \circ a = b$$  \hspace{1cm} (3.3)

$$d \circ a = b$$  \hspace{1cm} (3.4)

Then $A \otimes A$-number $c - d$ is quotient of $A$-number $0$ divided by $A$-number $a$

$$c \circ a - d \circ a = 0$$  \hspace{1cm} (3.5)

Proof. From (3.3), (3.4), it follows that

$$(c - d) \circ a = c \circ a - d \circ a = b - b = 0$$  \hspace{1cm} (3.6)

From (3.6), it follows that $A$-number $c - d$ is quotient of $A$-number $0$ divided by $A$-number $a$.

Remark 3.3. This point in the paper is interesting since it is easy to make mistake here and this mistake can be proved as a theorem. After we proved theorems 3.1, 3.2, the following question arises. If the difference of two quotients of $A$-number $b$ divided by $A$-number $a$ is quotient of $A$-number $0$ divided by $A$-number $a$, then what is the structure of the set of quotient $A$-number $0$ divided by any $A$-number? Or, equivalently, what is the structure of the set of quotients of $A$-number $b$ divided by $A$-number $a$?

Initially I wanted to prove the following statement.
Let $A$-number $a$ be neither a left nor right zero divisor. Then the quotient of $A$-number $0$ divided by $A$-number $a$ has either the form $0ac$, or the form $ca0$.

The proof is very simple. Since $c \neq 0$ in the expression $cad$, then $d = 0$.

When I decided to write down the quotient as $c \otimes 0 + 0 \otimes d$ I asked myself whether I was right. Indeed, according to theorems \[1\]-13.2.2, \[5\]-9.2.2, there exists nontrivial representation of zero tensor.

\[ \square \]

4. Division in $D$-Algebra

**Theorem 4.1.** Let $D$-algebra $A$ be division algebra. Then, for any $A$-numbers $a$, $b$, there exist $A$-numbers $c$, $d$ such that

$$ cad = b $$

**Proof.** To prove the theorem it suffices to put

$$ c = ba^{-1} \quad d = c $$

or

$$ c = e \quad d = a^{-1}b $$

\[ \square \]

**Theorem 4.2.** Let $A$-number $a$ divide $A$-number $b$. Let $A$-number $b$ divide $A$-number $c$. Then $A$-number $a$ divides $A$-number $c$.

**Proof.** According to the definition 1.3, since $A$-number $a$ divides $A$-number $b$, then there exists $A \otimes A$-number $p$ such that

$$ (4.1) \quad b = p \circ a $$

According to the definition 1.3, since $A$-number $b$ divides $A$-number $c$, then there exists $A \otimes A$-number $q$ such that

$$ (4.2) \quad c = q \circ b $$

From equations (4.1), (4.2), it follows that

$$ (4.3) \quad c = q \circ (p \circ a) = (q \circ p) \circ a $$

According to the definition 1.3, from the equation (4.3), it follows that $A$-number $a$ divides $A$-number $c$.

\[ \square \]

**Theorem 4.3.** Let $A$-number $a$ divide $A$-number $b$. Let $A$-number $a$ divide $A$-number $c$. Then $A$-number $a$ divides $A$-number $b + c$.

**Proof.** According to the definition 1.3, since $A$-number $a$ divides $A$-number $b$, then there exists $A \otimes A$-number $p$ such that

$$ (4.4) \quad b = p \circ a $$

According to the definition 1.3, since $A$-number $a$ divides $A$-number $c$, then there exists $A \otimes A$-number $q$ such that

$$ (4.5) \quad c = q \circ a $$

From equations (4.4), (4.5), it follows that

$$ (4.6) \quad b + c = p \circ a + q \circ a = (p + q) \circ a $$
According to the definition 1.3, from the equation (4.6), it follows that A-number $a$ divides A-number $b + c$. 

**Theorem 4.4.** Let A-number $a$ divide A-number $b$. Let $c$ be $A \otimes A$-number. Then A-number $a$ divides A-number $c \circ b$.

**Proof.** According to the definition 1.3, since A-number $a$ divides A-number $b$, then there exists $A \otimes A$-number $p$ such that

(4.7) \quad b = p \circ a

From the equation (4.7), it follows that

(4.8) \quad c \circ b = c \circ (p \circ a) = (c \circ p) \circ a

According to the definition 1.3, from the equation (4.8), it follows that A-number $a$ divides A-number $c \circ b$. 

5. Division with Remainder

**Definition 5.1.** Let division in the D-algebra $A$ is not always defined. A-number $a$ divides A-number $b$ with remainder, if the following equation is true

(5.1) \quad c \circ a + f = b

$A \otimes A$-number $c$ is called quotient of A-number $b$ divided by A-number $a$. A-number $f$ is called remainder of the division of A-number $b$ by A-number $a$.

**Theorem 5.2.** For any A-numbers $a$, $b$, there exist quotient and remainder of the division of A-number $b$ by A-number $a$.

**Proof.** To prove the theorem, it is enough to assume that

\begin{align*}
  c &= a \otimes a \\
  f &= b - (a \otimes a) \circ a = b - aaa
\end{align*}

From the theorem 5.2, it follows that, for given A-numbers $a$, $b$, a representation (5.1) is not unique. If we divide with remainder A-number $f$ by A-number $a$, then we get

(5.2) \quad c' \circ a + f' = f

From (5.1), (5.2), it follows that

(5.3) \quad c \circ a + c' \circ a + f' = (c + c') \circ a + f' = b

How can we compare representations (5.1), (5.3), when order is not defined in D-algebra $A$?

Therefore, the set of remainders of the division of A-number $b$ by A-number $a$ has form

(5.4) \quad A\{b, a\} = \{ f \in A : f = b - c \circ a, c \in A \otimes A \}

If $0 \in A\{b, a\}$, then choice of remainder and corresponding quotient is evident. In general, a choice of a representative of the set $A\{b, a\}$ depends on properties of the algebra. In the algebra $N$ of integers, we choose the smallest positive number. In the algebra $A[x]$ of polynomials, we choose polynomial which has the power less then
power of divisor. If there is norm in algebra $A$, (for instance, the algebra of integer quaternions), then we can chose $A$-number with the smallest norm as remainder.

**Theorem 5.3.** Since

\[(5.5)\]  
$A\{b, a\} \cap A\{c, a\} \neq \emptyset$

then

5.3.1: $A$-number $a$ divides $A$-number $b - c$ without remainder.

5.3.2: $A\{b, a\} = A\{c, a\}$

**Proof.** From the statement (5.5), it follows that there exists $A$-number

\[(5.6)\]  
d $\in A\{b, a\} \cap A\{c, a\}$

From the statement (5.6) and from the definition (5.4), it follows that there exist $A \otimes A$-numbers $f$, $g$ such that

\[(5.7)\]  
b = f \circ a + d\]

\[(5.8)\]  
c = g \circ a + d\]

From equations (5.7), (5.8), it follows that

\[(5.9)\]  
b - c = f \circ a - g \circ a = (f - g) \circ a\]

The statement 5.3.1 follows from the equation (5.9).

Let $m \in A\{b, a\}$. From the definition (5.4), it follows that there exist $A \otimes A$-number $n$ such that

\[(5.10)\]  
b = n \circ a + m\]

From equations (5.7), (5.10), it follows that

\[(5.11)\]  
f \circ a + d = n \circ a + m\]

From the equation (5.11), it follows that

\[(5.12)\]  
d = n \circ a - f \circ a + m = (n - f) \circ a + m\]

From equations (5.8), (5.12), it follows that

\[(5.13)\]  
c = g \circ a + (n - f) \circ a + m = (g + n - f) \circ a + m\]

From the definition (5.4) and the equation (5.13), it follows that there exist $m \in A\{c, a\}$. Therefore,

\[(5.14)\]  
A\{b, a\} \subseteq A\{c, a\}\]

The same way, we prove the statement

\[(5.15)\]  
A\{c, a\} \subseteq A\{b, a\}\]

The statement 5.3.2 follows from statements (5.14), (5.15).

From the theorem 5.3, it follows that, for given $A$-number $a$, the family of sets $A\{b, a\}$ generates equivalence mod $a$.

**Definition 5.4.** We define canonical remainder $b \mod a$ of the division of $A$-number $b$ by $A$-number $a$ as selected element of the set $A\{b, a\}$. The representation $c \circ a + (b \mod a) = b$ of division with remainder is called canonical.
At first glance, the choice of $A$-number $b \mod a$ is arbitrary. However we can define the natural constrains of the arbitrary choice.

**Theorem 5.5.** If we define sum on the set $A/\mod a$ according to the rule

$$b \mod a + c \mod a = (b + c) \mod a$$

then the set $A/\mod a$ is Abelian group.

**Proof.** According to the definition 5.4, there exist $A \otimes A$-numbers $p, q$ such that

$$b = p \circ a + b \mod a$$
$$c = q \circ a + c \mod a$$

From (5.17), it follows that

$$b + c = p \circ a + b \mod a + q \circ a + c \mod a$$
$$= (p + q) \circ a + b \mod a + c \mod a$$

From equations (5.4), (5.18), it follows that

$$b \mod a + c \mod a \in A\{b + c, a\}$$

From the statement (5.19) and from the definition 5.4, it follows that sum (5.16) is well defined.

We verify commutativity of the sum (5.16) directly. □

**Theorem 5.6.** The representation

$$D \longrightarrow A/\mod a$$

of ring $D$ in Abelian group $A/\mod a$ defined by the equation

$$d(b \mod a) = (db) \mod a$$

generates $D$-module $A/\mod a$.

**Proof.** According to the definition 5.4, there exist $A \otimes A$-number $p$ such that

$$b = p \circ a + b \mod a$$

From (5.21), it follows that

$$db = d(p \circ a) + d(b \mod a) = (dp) \circ a + d(b \mod a)$$

From equations (5.4), (5.22), it follows that

$$d(b \mod a) \in A\{db, a\}$$

From the statement (5.23) and from the definition 5.4, it follows that representation (5.20) is well defined. □

**Theorem 5.7.** If we define product in $D$-module $A/\mod a$ according to the rule

$$b \mod a)(c \mod a) = (bc) \mod a$$

then $D$-module $A/\mod a$ is $D$-algebra.
Proof. According to the definition 5.4, there exist $A \otimes A$-numbers $p, q$ such that
\begin{align*}
  b &= p \circ a + b \mod a \\
  c &= q \circ a + c \mod a
\end{align*}
From (5.25), it follows that
\begin{align*}
  bc &= (p \circ a + b \mod a)(q \circ a + c \mod a) \\
  &= (p \circ a)(q \circ a + c \mod a) + (b \mod a)(q \circ a + c \mod a) \\
  &= ((1 \otimes b) \circ p) \circ a + ((b \mod a) \otimes 1) \circ q \circ a + (b \mod a)(c \mod a)
\end{align*}
From equations (5.4), (5.26), it follows that
\begin{equation}
  (b \mod a)(c \mod a) \in A\{bc, a\}
\end{equation}
From the statement (5.27) and from the definition 5.4, it follows that product (5.24) is well defined.

**Theorem 5.8.** Let
\begin{align*}
  p \circ b + q &= a \\
  t \circ c + s &= b
\end{align*}
be canonical representation of division with remainder of $A$-number $a$ by $A$-number $b$. Let
\begin{align*}
  t \circ c + s &= b
\end{align*}
be canonical representation of division with remainder of $A$-number $b$ by $A$-number $c$.
5.8.1: Let
\begin{equation}
  u \circ c + v = p \circ s + q
\end{equation}
be canonical representation of division with remainder of $A$-number $p \circ s + q$ by $A$-number $c$.
5.8.2: Then the canonical representation of division with remainder of $A$-number $a$ by $A$-number $c$ has form
\begin{equation}
  (p \circ t + u) \circ c + v = a
\end{equation}
Proof. From equations (5.28), (5.29), it follows that
\begin{equation}
  a = p \circ (t \circ c + s) + q = p \circ t \circ c + p \circ s + q
\end{equation}
The equation (5.32) is representation of division with remainder of $A$-number $a$ by $A$-number $c$. From equations (5.30), (5.32), it follows that
\begin{equation}
  a = p \circ t \circ c + u \circ c + v
\end{equation}
The equation (5.31) follows from the equation (5.33). From the statement 5.8.1 and from the definition 5.4, it follows that
\begin{equation}
  v = (p \circ s + q) \mod c
\end{equation}
From equations (5.4), (5.31), it follows that
\begin{equation}
  v \in A\{a, c\}
From the statement (5.35) and from the definition 5.4, it follows that
\[ v = a \mod c \]
The statement 5.8.2 follows from the statement (5.36) and from the definition 5.4. □

6. Highest Common Factor

**Definition 6.1.** A-number \( c \) is called common factor of A-numbers \( a \) and \( b \), if A-number \( c \) divides each of A-numbers \( a \) and \( b \). If A-numbers \( a \) and \( b \) are not unit divisors and any common factor of A-numbers \( a \) and \( b \) is not unit divisor, then A-numbers \( a \) and \( b \) are called relatively prime. □

**Definition 6.2.** A-number \( c \) is called highest common factor of A-numbers \( a \) and \( b \), if A-number \( c \) is common factor of A-numbers \( a \) and \( b \) and any common factor \( d \) of A-numbers \( a \) and \( b \) divides A-number \( c \). □

7. Prime A-number

**Definition 7.1.** Let A-number \( b \) be not unit divisor of D-algebra \( A \). A-number \( b \) is called prime, if any divisor \( a \) of A-number \( b \) satisfies one of the following conditions.

7.1.1: A-number \( a \) is unit divisor.
7.1.2: Quotient of A-number \( b \) divided by A-number \( a \) is unit divisor of D-algebra \( A \otimes A \).

**Theorem 7.2.** Let D-algebra \( A \) is division algebra. Let \( A[x] \) be algebra of polynomials over D-algebra \( A \). Polynomial of power 1 is prime \( A[x] \)-number.

**Proof.** Let \( p \) be polynomial of power 1. Let \( q \) be polynomial. Let
\[ p = (r_1 \otimes r_2) \circ q = r_1 q r_2 \]
be canonical representation of division with remainder of polynomial \( p \) over polynomial \( q \). Here \( r_1, r_2 \) are polynomials. According to the theorems [4]-5.9, [6]-20,
\[ \deg r_1 + \deg q + \deg r_2 = \deg p = 1 \]
From the equation (7.2), it follows that only one polynomial \( q, r_1, r_2 \) has power 1, and other two polynomials are A-numbers.

- Since the polynomial \( q \) is A-number, then the polynomial \( q \) is unit divisor and satisfies the condition 7.1.1.
- Since \( q \) is polynomial of power 1, then, according to the theorems [4]-6.10,
\[ p = r \circ q \]
where \( r \) is \( A \otimes A \)-number. Since \( p \) and \( q \) are polynomials of power 1, then, according to the theorems [6]-28, [4]-6.10,
\[ q = r' \circ p + s \]
where \( r' \) is \( A \otimes A \)-number and \( s \) is A-number. From equations (7.3), (7.4), it follows that
\[ p = r \circ r' \circ p + r \circ s \]
From the equation \((7.5)\), it follows that
\[
(7.6) \quad r \circ r' = 1 \otimes 1 \quad r \circ s = 0
\]
From the equation \((7.6)\), it follows that \(A \otimes A\)-number \(r\) is unit divisor and \(s = 0\). Therefore, the polynomial \(q\) satisfies the condition 7.1.2.

According to the definition 7.1, the polynomial \(p\) is prime \(A[x]\)-number. □

8. References

[1] Aleks Kleyn, Lectures on Linear Algebra over Division Ring, eprint arXiv:math.GM/0701238 (2010)
[2] Aleks Kleyn, Linear Equation in Finite Dimensional Algebra, eprint arXiv:0912.4061 (2010)
[3] Aleks Kleyn, Linear Maps of Free Algebra, eprint arXiv:1003.1544 (2010)
[4] Aleks Kleyn, Polynomial over Associative \(D\)-Algebra, eprint arXiv:1302.7204 (2013)
[5] Aleks Kleyn.
Linear Algebra over Division Ring: Vector Space.
CreateSpace, 2014; ISBN-13: 978-1499324006
[6] Aleks Kleyn, Polynomial over Associative \(D\)-Algebra.
Clifford Analysis, Clifford Algebras and their applications, Vol 2, Issue 2, pages 97 - 115, 2013
9. INDEX

A-number 2

canonical remainder of the division 6
canonical representation of division with remainder 6
common factor 9

division algebra 2
division with remainder 5
division without remainder 6

highest common factor 9

prime A-number 9

quotient 2, 5

relatively prime A-numbers 9
remainder of the division 5
10. Special Symbols and Notations

\[ b \mod a \quad \text{canonical remainder of the division} \]
Деление в ассоциативной $D$-алгебре

Александр Клейн

Аннотация. Из симметрии между определениями левого и правого делителей в ассоциативной $D$-алгебре $A$ следует возможность определять частное как $A \otimes A$-число. В статье рассмотрены деление и деление с остатком. Я рассмотрел также понятие простого $A$-числа.

Содержание

1. Предисловие .................. 1
2. Соглашения .................... 2
3. Геометрия частных .................. 3
4. Деление в $D$-алгебре ................. 4
5. Деление с остатком .................. 5
6. Наибольший общий делитель ............. 9
7. Простое $A$-число .................. 9
8. Список литературы .................. 10
9. Предметный указатель ..................... 11
10. Специальные символы и обозначения .................. 12

1. Предисловие

Пусть $D$ - коммутативное кольцо. Мы будем предполагать, что $D$-алгебра $A$ ассоциативна.

Определение 1.1. $A$-число $a$ называется левым делителем $A$-числа $b$, если существует $A$-число $c$ такое, что

\[ ac = b \]

Определение 1.2. $A$-число $a$ называется правым делителем $A$-числа $b$, если существует $A$-число $c$ такое, что

\[ ca = b \]
Симметрия между определениями 1.1 и 1.2 очевидна. Также как очевидно различие между левым и правым делителями в связи с некоммутативностью произведения. Однако мы можем рассмотреть определение, обобщающее определения 1.1 и 1.2.

Мы можем рассматривать частное от деления $b$ на $a$ как пару чисел $c, d$ таких, что

$$cad = b$$

Однако мы можем рассмотреть операцию деления с другой точки зрения.

Равенства (1.1), (1.2) являются примерами линейных отображений $D$-алгебры $A$. В коммутативном случае равенство (1.1) является единственным определением линейного отображения. В некоммутативном случае, линейное отображение $D$-алгебры $A$ порождается $A \otimes A$-числом. Например, тензор $c \otimes d$ является $A \otimes A$-числом. Таким образом, мы получаем следующее определение.

Определение 1.3. $A$-число $a$ называется делителем $A$-числа $b$, если существует $A \otimes A$-число $c$ такое, что

$$c \circ a = b$$

$A \otimes A$-число $c$ называется частным от деления $A$-числа $b$ на $A$-число $a$. 

В статье [2] я рассмотрел уравнение

$$c \circ x = b$$

В этой статье я рассматривал уравнение

$$x \circ a = b$$

$D$-алгебра $A$ называется алгеброй с делением, если для любого $A$-числа $a \neq 0$ существует $A$-число $a^{-1}$.

2. Соглашения

Соглашение 2.1. Элемент $D$-алгебры $A$ называется $A$-числом. Например, комплексное число также называется $C$-числом, а кватернйон называется $H$-числом.

1 Здесь можно возразить, что деление - это операция, обратная умножению. В коммутативном случае, из выражения

$$ca = b$$

следует, что

- $c$ является множителем, произведение $c$ и $a$ равно $b$.
- $c$ является частным деления $b$ на $a$.

Таким образом, в коммутативном случае определения множителя и частного совпадают. В некоммутативном случае, мы различаем правый и левый делители; следовательно, мы различаем левое и правое частное.

2 Так как отображение

$$(1.3) \quad a \rightarrow cad$$

бilinearное, то, согласно теореме [3]-3.6.4, мы можем рассматривать отображение

$$a \rightarrow (c \otimes d) \circ a$$

вместо отображения (1.3).
Соглашение 2.2. Пусть $A$ - $\Omega_1$-алгебра. Пусть $B$ - $\Omega_2$-алгебра. Запись $A \rightarrow B$ означает, что определено представление $\Omega_1$-алгебры $A$ в $\Omega_2$-алгебре $B$.

Соглашение 2.3. Пусть $A$ ассоциативная $D$-алгебра. Представление $A \otimes A \rightarrow A$ порождает множество линейных отображений. Это представление порождает произведение $\circ$ в $D$-модуле $A \otimes A$ согласно правилу

$$(p \circ q) \circ a = p \circ (q \circ a)$$

Без сомнения, у читателя могут быть вопросы, замечания, возражения. Я буду признателен любому отзыву.

3. Геометрия частных

Теорема 3.1. Пусть поле действительных чисел $R$ является подполем центра $Z(D)$ кольца $D$. Тогда для любых $A$-чисел $a$, $b$ множество частных выпукло.

Доказательство. Пусть $A \otimes A$-число $c$ является частным от деления $A$-числа $b$ на $A$-число $a$

(3.1) $$c \circ a = b$$

Пусть $A \otimes A$-число $d$ является частным от деления $A$-числа $b$ на $A$-число $a$

(3.2) $$d \circ a = b$$

Тогда для любого $t \in R$, $0 \leq t \leq 1$, из (3.1), (3.2) следует, что

$$(tc + (1 - t)d) \circ a = (tc) \circ a + ((1 - t)d) \circ a = t(c \circ a) + (1 - t)(d \circ a) = tb + (1 - t)b = b$$

Следовательно, $A \otimes A$-число $tc + (1 - t)d$ является частным от деления $A$-числа $b$ на $A$-число $a$.

Теорема 3.2. Пусть $A \otimes A$-числа $c$, $d$ являются частными от деления $A$-числа $b$ на $A$-число $a$

(3.3) $$c \circ a = b$$

(3.4) $$d \circ a = b$$

Тогда $A \otimes A$-число $c - d$ является частным от деления $A$-числа $0$ на $A$-число $a$

(3.5) $$(c - d) \circ a = 0$$

Доказательство. Из (3.3), (3.4) следует, что

(3.6) $$(c - d) \circ a = c \circ a - d \circ a = b - b = 0$$

Из (3.6) следует, что $A$-число $c - d$ является частным от деления $A$-числа $0$ на $A$-число $a$. □
Замечание 3.3. Это место в статье очень интересно тем, что здесь очень легко совершить ошибку, которую легко доказать как теорему. После доказательства теорем 3.1, 3.2, естественно возникает следующий вопрос. Если разность двух частных от деления $A$-числа $b$ на $A$-число $a$ является частным от деления $A$-числа $0$ на $A$-число $a$, то какова структура множества частных от деления $A$-числа $0$? Или, что тоже самое, какова структура множества частных от деления $A$-числа $b$ на $A$-число $a$?

Вначале я хотел доказать следующее утверждение.

Пусть $A$-число $a$ не является ни левым, ни правым делителем нуля. Тогда частное от деления $A$-числа $0$ на $A$-число $a$ имеет либо вид $0a$, либо вид $ca0$. Докажательство очень просто. Если $c \neq 0$ в выражении $cad$, то $d = 0$.

Когда я решил записать частное в виде

$$c \otimes 0 + 0 \otimes d$$

я подумал прав ли я. Действительно, согласно теоремам [1]-13.2.2, [5]-9.2.2, существует нетривиальная запись нулевого тензора. □

4. ДЕЛЕНИЕ В $D$-АЛГЕБРЕ

Теорема 4.1. Если $D$-алгебра $A$ является алгеброй с делением, то для любых $A$-чисел $a$, $b$ существуют $A$-числа $c$, $d$ такие, что

$$cad = b$$

Доказательство. Для доказательства теоремы достаточно положить

$$c = ba^{-1} \quad d = e$$

или

$$c = e \quad d = a^{-1}b$$

□

Теорема 4.2. Пусть $A$-число $a$ делит $A$-число $b$. Пусть $A$-число $b$ делит $A$-число $c$. Тогда $A$-число $a$ делит $A$-число $c$.

Доказательство. Согласно определению 1.3, так как $A$-число $a$ делит $A$-число $b$, то существует $A \otimes A$-число $p$ такое, что

(4.1)\[ b = p \circ a \]

Согласно определению 1.3, так как $A$-число $b$ делит $A$-число $c$, то существует $A \otimes A$-число $q$ такое, что

(4.2)\[ c = q \circ b \]

Из равенств (4.1), (4.2) следует, что

(4.3)\[ c = q \circ (p \circ a) = (q \circ p) \circ a \]

Согласно определению 1.3, из равенства (4.3) следует, что $A$-число $a$ делит $A$-число $c$. □

Теорема 4.3. Пусть $A$-число $a$ делит $A$-число $b$. Пусть $A$-число $a$ делит $A$-число $c$. Тогда $A$-число $a$ делит $A$-число $b + c$. 4
Доказательство. Согласно определению 1.3, так как $A$-число $a$ делит $A$-число $b$, то существует $A \otimes A$-число $p$ такое, что
\begin{equation}
    b = p \circ a
\end{equation}
Согласно определению 1.3, так как $A$-число $a$ делит $A$-число $c$, то существует $A \otimes A$-число $q$ такое, что
\begin{equation}
    c = q \circ a
\end{equation}
Из равенств (4.4), (4.5) следует, что
\begin{equation}
    b + c = p \circ a + q \circ a = (p + q) \circ a
\end{equation}
Согласно определению 1.3, из равенства (4.6) следует, что $A$-число $a$ делит $A$-число $b + c$. \hfill \Box

Теорема 4.4. Пусть $A$-число $a$ делит $A$-число $b$. Пусть $c$ является $A \otimes A$-числом. Тогда $A$-число $a$ делит $A$-число $c \circ b$.

Доказательство. Согласно определению 1.3, так как $A$-число $a$ делит $A$-число $b$, то существует $A \otimes A$-число $p$ такое, что
\begin{equation}
    b = p \circ a
\end{equation}
Из равенств (4.7) следует, что
\begin{equation}
    c \circ b = c \circ (p \circ a) = (c \circ p) \circ a
\end{equation}
Согласно определению 1.3, из равенства (4.8) следует, что $A$-число $a$ делит $A$-число $c \circ b$. \hfill \Box

5. Деление с остатком

Определение 5.1. Пусть деление в $D$-алгебре $A$ не всегда определено. $A$-число $a$ делит $A$-число $b$ с остатком, если следующее равенство верно
\begin{equation}
    c \circ a + f = b
\end{equation}
$A \otimes A$-число $c$ называется частным от деления $A$-числа $b$ на $A$-число $a$. $A$-число $d$ называется остатком от деления $A$-числа $b$ на $A$-число $a$. \hfill \Box

Теорема 5.2. Для любых $A$-чисел $a$, $b$, существует частное и остаток от деления $A$-числа $b$ на $A$-число $a$.

Доказательство. Для доказательства теоремы достаточно положить
\begin{align*}
    c &= a \otimes a \\
    f &= b - (a \otimes a) \circ a = b - aaa
\end{align*}
Из теоремы 5.2 следует, что для заданных $A$-чисел $a$, $b$ представление (5.1) определено не однозначно. Если мы поделим с остатком $A$-число $f$ на $A$-число $a$, то мы получим
\begin{equation}
    c' \circ a + f' = f
\end{equation}
Из (5.1), (5.2) следует, что
\begin{equation}
    c \circ a + c' \circ a + f' = (c + c') \circ a + f' = b
\end{equation}
Как мы можем сравнить представления (5.1), (5.3), если отношение порядка не определено в $D$-алгебре $A$?

Следовательно, множество остатков от деления $A$-числа $b$ на $A$-число $a$ имеет вид

\begin{equation}
A\{b, a\} = \{ f \in A : f = b - c \circ a, c \in A \otimes A \}
\end{equation}

Если $0 \in A\{b, a\}$, то выбор остатка и соответствующего частного очевиден. Вообще говоря, выбор представителя множества $A\{b, a\}$ зависит от свойств алгебры. В алгебре $\mathbb{N}$ целых чисел мы выбираем наименьшее положительное число. В алгебре $A[x]$ многочленов мы выбираем многочлен степени меньше степени делителя. Если в алгебре $A$ определена норма (например, алгебра целых кватернионов), то в качестве остатка мы можем выбрать $A$-число с наименьшей нормой.

**Теорема 5.3.** Если

\begin{equation}
A\{b, a\} \cap A\{c, a\} \neq \emptyset
\end{equation}

то

5.3.1: $A$-число $a$ делит $A$-число $b - c$ без остатка.

5.3.2: $A\{b, a\} = A\{c, a\}$

**Доказательство.** Из утверждения (5.5) следует, что существует $A$-число

\begin{equation}
d \in A\{b, a\} \cap A\{c, a\}
\end{equation}

Из утверждения (5.6) и определения (5.4) следует, что существуют $A \otimes A$-числа $f, g$ такие, что

\begin{align}
b &= f \circ a + d \\
c &= g \circ a + d
\end{align}

Из равенств (5.7), (5.8) следует, что

\begin{equation}
b - c = f \circ a - g \circ a = (f - g) \circ a
\end{equation}

Утверждение 5.3.1 является следствием равенства (5.9).

Пусть $m \in A\{b, a\}$. Из определения (5.4) следует, что существует $A \otimes A$-число $n$ такие, что

\begin{equation}
b = n \circ a + m
\end{equation}

Из равенств (5.7), (5.10) следует, что

\begin{equation}
f \circ a + d = n \circ a + m
\end{equation}

Из равенства (5.11) следует, что

\begin{equation}
d = n \circ a - f \circ a + m = (n - f) \circ a + m
\end{equation}

Из равенств (5.8), (5.12) следует, что

\begin{equation}
c = g \circ a + (n - f) \circ a + m = (g + n - f) \circ a + m
\end{equation}

Из определения (5.4) и равенства (5.13) следует, что существует $m \in A\{c, a\}$.

Следовательно,

\begin{equation}
A\{b, a\} \subseteq A\{c, a\}
\end{equation}
Аналогичным образом мы доказываем утверждение
(5.15) \[ A\{c, a\} \subseteq A\{b, a\} \]
Утверждение 5.3.2 является следствием утверждений (5.14), (5.15).  

Из теоремы 5.3 следует, что для данного \( A \)-числа \( a \) семейство множеств \( A\{b, a\} \) порождает отношение эквивалентности \( \text{mod } a \).

Определение 5.4. Определим каноническое частное \( b \mod a \) от деления \( A \)-числа \( b \) на \( A \)-число \( a \) как выбранный элемент множества \( A\{b, a\} \). Представление
\[ c \circ a + (b \mod a) = b \]
dеления с остатком называется каноническим.

На первый взгляд, выбор \( A \)-числа \( b \mod a \) произволен. Однако мы можем определить естественные границы этого произвола.

Теорема 5.5. Если мы определим сложение на множестве \( A/\text{mod } a \) согласно правилу
(5.16) \[ b \mod a + c \mod a = (b + c) \mod a \]
то множество \( A/\text{mod } a \) является абелевой группой.

Доказательство. Согласно определению 5.4, существуют \( A \otimes A \)-числа \( p, q \) такие, что
(5.17) \[ b = p \circ a + b \mod a \]
\[ c = q \circ a + c \mod a \]
Из (5.17) следует, что
(5.18) \[ b + c = p \circ a + b \mod a + q \circ a + c \mod a \]
\[ = (p + q) \circ a + b \mod a + c \mod a \]
Из равенств (5.4), (5.18) следует, что
(5.19) \[ b \mod a + c \mod a \in A\{b + c, a\} \]
Из утверждения (5.19) и определения 5.4 следует корректность определения (5.16) суммы.

Коммутативность суммы (5.16) доказывается непосредственной проверкой.  

Теорема 5.6. Представление
\[ D \twoheadrightarrow A/\text{mod } a \]
кольца \( D \) в абелевой группе \( A/\text{mod } a \) определённое равенством
(5.20) \[ d(b \mod a) = (db) \mod a \]
порождает \( D \)-модуль \( A/\text{mod } a \).
Доказательство. Согласно определению 5.4, существует $A \otimes A$-число $p$ такое, что
\begin{equation}
(5.21) \quad b = p \circ a + b \mod a
\end{equation}
Из (5.21) следует, что
\begin{equation}
(5.22) \quad db = d(p \circ a) + d(b \mod a) = (dp) \circ a + d(b \mod a)
\end{equation}
Из равенств (5.4), (5.22) следует, что
\begin{equation}
(5.23) \quad d(b \mod a) \in A\{db, a\}
\end{equation}
Из утверждения (5.23) и определения 5.4 следует корректность определения (5.20) представления.

Teorema 5.7. Если мы определим умножение в $D$-модуле $A/ \mod a$ согласно правилу
\begin{equation}
(5.24) \quad (b \mod a)(c \mod a) = (bc) \mod a
\end{equation}
то $D$-модуль $A/ \mod a$ является $D$-алгеброй.

Доказательство. Согласно определению 5.4, существуют $A \otimes A$-числа $p$, $q$ такие, что
\begin{equation}
(5.25) \quad b = p \circ a + b \mod a \quad c = q \circ a + c \mod a
\end{equation}
Из (5.25) следует, что
\begin{equation}
bc = (p \circ a + b \mod a)(q \circ a + c \mod a)
= (p \circ a)(q \circ a + c \mod a) + (b \mod a)(q \circ a + c \mod a)
= (p \circ a)b + (b \mod a)(q \circ a) + (b \mod a)(c \mod a)
= ((1 \otimes b) \circ p) \circ a + ((b \mod a) \otimes 1) \circ q \circ a + (b \mod a)(c \mod a)
\end{equation}
Из равенств (5.4), (5.26) следует, что
\begin{equation}
(5.27) \quad (b \mod a)(c \mod a) \in A\{bc, a\}
\end{equation}
Из утверждения (5.27) и определения 5.4 следует корректность определения (5.24) произведения.

Teorema 5.8. Пусть
\begin{equation}
(5.28) \quad p \circ b + q = a
\end{equation}
является каноническим представлением деления с остатком $A$-числа $a$ на $A$-число $b$. Пусть
\begin{equation}
(5.29) \quad t \circ c + s = b
\end{equation}
является каноническим представлением деления с остатком $A$-числа $b$ на $A$-число $c$.

5.8.1: Пусть
\begin{equation}
(5.30) \quad u \circ c + v = p \circ s + q
\end{equation}
является каноническим представлением деления с остатком $A$-числа $p \circ s + q$ на $A$-число $c$. 
5.8.2: Тогда каноническое представление деления с остатком A-числа a на A-число с имеет вид
\[(p \circ t + u) \circ c + v = a\]

Доказательство. Из равенств (5.28), (5.29) следует, что
\[ a = p \circ (t \circ c + s) + q = p \circ t \circ c + p \circ s + q \]
Равенство (5.32) является представлением деления с остатком A-числа a на A-число c. Из равенств (5.30), (5.32) следует, что
\[ a = p \circ t \circ c + u \circ c + v \]
Равенство (5.31) является следствием равенства (5.33). Из утверждения 5.8.1 и определения 5.4 следует, что
\[ v = (p \circ s + q) \mod c \]
Из равенств (5.4), (5.31) следует, что
\[ v \in A\{a, c\} \]
Из утверждения (5.35) и определения 5.4 следует, что
\[ v = a \mod c \]
Утверждение 5.8.2 является следствием утверждения (5.36) и определения 5.4.

6. Наибольший общий делитель

Определение 6.1. A-число c называется общим делителем A-чисел a и b, если A-число c делит каждое из A-чисел a и b. Если A-числа a и b не являются делителями единицы и любой общий делитель A-чисел a и b не является делителем единицы, то A-числа a и b называются взаимно простыми.

Определение 6.2. A-число c называется наибольшим общим делителем A-чисел a и b, если A-число c является общим делителем A-чисел a и b и любой общий делитель d A-чисел a и b делит A-число c.

7. Простое A-число

Определение 7.1. Пусть A-число b не является делителем единицы D-алгебры A. A-число b называется простым, если любой делитель a A-числа b удовлетворяет одному из следующих условий.

7.1.1: A-число a является делителем единицы.
7.1.2: Частное от деления A-числа b на A-число a является делителем единицы D-алгебры A ⊗ A.

Теорема 7.2. Пусть D-алгебра A является алгеброй с делением. Рассмотрим алгебру многочленов A[x] над D-алгеброй A. Многочлен степени 1 является простым A[x]-числом.
Доказательство. Пусть \( p \) - многочлен степени 1. Пусть \( q \) - многочлен. Пусть
\[
p = (r_1 \otimes r_2) \circ q = r_1 q r_2
\]
каноническая форма деления с остатком многочлена \( p \) на многочлен \( q \). Здесь \( r_1, r_2 \) - многочлены. Согласно теоремам [4]-5.9, [6]-20,
\[
\text{deg} r_1 + \text{deg} q + \text{deg} r_2 = \text{deg} p = 1
\]
Из равенства (7.2) следует, что только один многочлен \( q, r_1, r_2 \) имеет степень 1, и остальные два многочлена являются \( A \)-числами.

• Если многочлен \( q \) является \( A \)-числом, то многочлен \( q \) является делителем единицы и удовлетворяет условию 7.1.1.
• Если степень многочлена \( q \) равна 1, то, согласно теоремам [4]-6.10, [6]-28,
\[
p = r \circ q
\]
где \( r \) является \( A \otimes A \)-числом. Так как \( p, q \) - многочлены степени 1, то, согласно теоремам [4]-6.10, [6]-28,
\[
q = r' \circ p + s
\]
где \( r' \) является \( A \otimes A \)-числом и \( s \) является \( A \)-числом. Из равенств (7.3), (7.4) следует, что
\[
p = r \circ r' \circ p + r \circ s
\]
Из равенства (7.5) следует, что
\[
r \circ r' = 1 \otimes 1 \quad r \circ s = 0
\]
Из равенства (7.6) следует, что \( A \otimes A \)-число \( r \) является делителем единицы и \( s = 0 \). Следовательно, многочлен \( q \) удовлетворяет условию 7.1.2.

Согласно определению 7.1, многочлен \( p \) является простым \( A[x] \)-числом. □

8. Список литературы

[1] Александр Клейн, Лекции по линейной алгебре над телом, eprint arXiv:math.GM/0701238 (2010)
[2] Александр Клейн, Линейное уравнение в конечномерной алгебре, eprint arXiv:0912.4061 (2010)
[3] Александр Клейн, Линейные отображения свободной алгебры, eprint arXiv:1003.1544 (2010)
[4] Александр Клейн, Многочлен над ассоциативной \( D \)-алгеброй, eprint arXiv:1302.7204 (2013)
[5] Александр Клейн. Линейная алгебра над телом: Векторное пространство. CreateSpace, 2014; ISBN-13: 978-1499323948
[6] Aleks Kleyn, Polynomial over Associative \( D \)-Algebra. Clifford Analysis, Clifford Algebras and their applications, Vol 2, Issue 2, pages 97 - 115, 2013
9. ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

- $A$-число 2
- алгебра с делением 2
- взаимно простые $A$-числа 9
- деление без остатка 6
- деление с остатком 5
- каноническое представление деления с остатком 7
- наибольший общий делитель 9
- общий делитель 9
- остаток от деления 5
- простое $A$-число 9
- частное от деления 2, 5
Специальные символы и обозначения

\[ b \mod a \] каноническое частное от деления 7