Anzahl der Lösungen $(x^2, y^2)$ von (3) mit $x, y \in GF(q)^*$

$$\text{für} \quad -1 \notin K^2 \quad : \frac{1}{4}(p^e - e - 2), \qquad\qquad \text{für} \quad -1 \in K^{*2} : \frac{1}{4}(p^e - e).$$

Die Überprüfung dieser Ergebnisse, die Auffindung der Lösungsanzahlen für die Gleichung $x^2 - y^2 = 0$ sowie die Untersuchung für Galois-Felder gerader Ordnung überlassen wir dem Leser.

Herbert Zeitler, Math. Institut der Universität Bayreuth, Bayreuth

LITERATURVERZEICHNIS

1  L.E. Dickson: Linear Groups. Leipzig 1901.
2  G.H. Hardy und E.M. Wright: Einführung in die Zahlentheorie. München 1958.
3  K. Radbruch: Algebraische Strukturen und elementare Zahlentheorie (Mathematik S II). Freiburg 1975.

# Linear operators satisfying the chain rule

In computational calculus the derivative is treated as a formal operator satisfying certain functional relationships. This leads to the question of which properties of the derivative characterize that operator on the elementary functions, i.e., the rational, logarithmic, exponential, trigonometric and inverse trigonometric functions. In this note we will show that, provided we rule out trivial cases, any operator, which acts on a suitable collection of functions containing the elementary functions and which is both linear and satisfies the chain rule formula must agree with the derivative on the elementary functions.

We begin by describing the functions on which our operators act. If $f$ and $g$ are two real-valued functions with domains contained in $R$, the real numbers, and $c \in R$, let $f + g$, $fg$, $cf$, $f \circ g$, $f/g$ denote the usual pointwise operations of addition, multiplication, scalar multiplication, composition, and division, each defined on its natural domain (the largest set on which the resulting formula makes sense). Let $F$ denote any set of real-valued functions with non-empty domains contained in $R$ satisfying the following properties.

1. $F$ is closed under addition, multiplication and scalar multiplication.

2. If $f$ and $g$ are in $F$, then $f \circ g$ and $f/g$ are also in $F$ whenever their natural domains are non-empty.

3. $i(x) \equiv x$ and $u(x) \equiv 1$ are in $F$. Observe that any such $F$ is an algebra of real-valued functions which contains the rational functions. In what follows we shall use the facts that for all $f \in F$, $f \circ i \in F$; and if we set $t(x) = x + r$, with $r \in R$, $f \circ t \in F$.

A *chain rule operator* on $F$ is a linear operator, $D$, on $F$ such that if $f \circ g \in F$ and $(Df) \circ g \in F$, then $D(f \circ g) = ((Df) \circ g)(Dg)$. Any linear operator, $P$, on $F$ which satisfies $P(fg) = (Pf)g + f(Pg)$ is called a *derivation*. The derivative on $F_1$, the set of all functions whose domains consist of all but a finite number of points of $R$ and which are differentiable on their domains, is both a chain rule operator and a derivation, as is the zero operator defined by $(0f)(x) = 0$ on $F_2$, the set of all real-valued function whose domains are contained in $R$. The example $D = 2(d/dx)$ on $F_1$ shows that not every derivation is a chain rule operator. We shall prove, however,

**Theorem.** *Any chain rule operator on $F$ is a derivation on $F$.*

In order to prove this theorem and to understand its consequences we need the following computational formulas. Let $s$ denote the function $s(x) = x^2$.

**Lemma.** *If $D$ is a chain rule operator which is not the zero operator:*
*a) $Di = u$,   b) $Du = 0$,   c) $Ds = ki$ for some $k \in R$.*

Proof:
a) Since $f \circ i = f$, the chain rule implies: (1) $Df = (Df)(Di)$ for all $f \in F$. Setting $f = i$ in (1) yields $Di = (Di)^2$ so that $(Di)(x) = 1$ provided $(Di)(x) \neq 0$. Thus we need only show that for any $r \in R$, $(Di)(r) \neq 0$. Since $D$ is not the zero operator, (1) implies that there must exist some $a \in R$ such that $(Di)(a) \neq 0$. Set $t(x) = x + a - r$ and $t^{-1}(x) = x - a + r$. Then $t, t^{-1} \in F$, $i = t \circ t^{-1}$ and $Di = ((Dt) \circ t^{-1})(Dt^{-1})$. Evaluating this at $x = a$ yields $0 \neq (Di)(a) = (Dt)(r)(Dt^{-1})(a)$. Thus, $(Dt)(r) \neq 0$, so setting $f = t$ in (1) and evaluating at $x = r$ gives $(Di)(r) \neq 0$.
b) For any $c \in R$, $u \circ (ci) = u$ implies that $Du = ((Du) \circ (ci)) cu$. Set $c = 0$.
c) Applying the chain rule to $s \circ (ci) = c^2 s$, yields (2) $c^2 Ds = ((Ds) \circ (ci)) cu$. Evaluating (2) at $x = 1$ shows, $c(Ds)(1) = (Ds)(c)$ provided $c \neq 0$. This proves the result with $k = (Ds)(1)$, if the argument of $Ds$ is not 0. To complete the proof, note that setting $c = 2$ in (2) and evaluating at $x = 0$ shows $4(Ds)(0) = 2(Ds)(0)$ so $(Ds)(0) = 0 = k0$.

We are now in a position to prove our theorem. If $D$ is the zero operator the result is immediate. Otherwise, computing both sides of $D(s \circ (f + g)) = D(s \circ f + 2fg + s \circ g)$ separately using the chain rule and the lemma yields: $D(fg) = (k/2)(f(Dg) + (Df)g)$, where $k$ is the constant appearing in the lemma. Finally, using the fact that $ui = i$, $1 = D(ui) = (k/2)(u(Di) + (Du)i) = k/2$. Therefore, $k = 2$.

Several observations follow almost immediately from the theorem. First, note that at the end of the proof of the theorem we established that $Ds = 2i$ (since $k = 2$). Also, $i \in F$ implies $r = 1/i$, with domain $R - \{0\}$, is in $F$ and applying the product rule to $ri$ shows $Dr = -1/s$. This, combined with the product and chain rules, gives a quotient rule for chain rule operators. In addition, we can obtain a formula for $Df^{-1}$ by applying $D$ to the identity $i = f \circ f^{-1}$. We summarize these results as:

**Corollary 1.** *If $D$ is a chain rule operator on $F$, then*

*a)* $D(f/g) = \dfrac{(Df)g - f(Dg)}{s \circ g}$ *whenever $f/g \in F$,*

*b)* $(Df^{-1})(f(x)) = 1/(Df)(x)$ *provided* $(Df)(x) \neq 0$.

It is convenient to call chain rule operators other than the zero operator, non-trivial chain rule operators. The example

$$Df = \lim_{h \to 0+} \frac{f(x+h) - f(x)}{h}$$

provides a familiar operator other than the derivative which is a non-trivial chain rule operator.

Finally, we characterize the action of chain rule operators on elementary functions, as promised in the first paragraph.

**Corollary 2.** *Suppose $F$ contains all the elementary functions and $D$ is a non-trivial chain-rule operator such that if $f \in F$ is differentiable at $x \in R$, then $x$ is in the domain of $Df$. Then $De = de/dx$ whenever $e$ is an elementary function.*

Proof: A straightforward induction argument using the theorem and the lemma shows that $dp/dx = Dp$ for any polynomial $p$. Corollary 1, part a, and this result imply that $dr/dx = Dr$ for any rational function $r$. Next we compute $D\exp$, $D\sin$ and $D\cos$. Applying $D$ to both sides of the identity $\exp(x+y) = \exp(x)\exp(y)$, considering $x$ as a variable and $y$ as an arbitrary constant yields $(D\exp)(y) = (D\exp)(0)\exp(y)$. Similarly, applying $D$ to the identities for $\sin(x+y)$ and $\cos(x+y)$ shows $(D\sin)(y) = (D\sin)(0)\cos(y) + \sin(y)(D\cos)(0)$ and $(D\cos)(y) = (D\cos)(0)\cos(y) - (D\sin)(0)\sin(y)$. Furthermore, applying $D$ to the identity $\sin^2(x) + \cos^2(x) = 1$ and evaluating at $x = 0$ gives $(D\cos)(0) = 0$. We have shown $(D\sin)(y) = (D\sin)(0)\cos(y)$, $(D\cos)(y) = -(D\sin)(0)\sin(y)$. To see that $(D\exp)(0) = 1$, use Taylor's theorem to write $\exp(x) = 1 + x + E(x)$ where $E(x) = Z(x)x^2$. Then $E$ and $Z$ are in $F$. Moreover $Z(x)$ is differentiable at $0$ (cf. [1], p. 125), thus $(DZ)(0) \in R$. Now $(DE)(x) = (DZ)(x)x^2 + 2xZ(x)$, so that $(DE)(0) = 0$. Thus $(D\exp)(0) = 1 + (DE)(0) = 1$. A similar argument shows $(D\sin)(0) = 1$. The remainder of the proof follows by straightforward calculations using these results, Corollary 1 and the definitions of the logarithmic, trigonometric and inverse trigonometric functions in terms of the exponential, sine and cosine functions.

Richard L. Rubin, Florida International University, Miami, Florida

REFERENCE

1  W. Fulks: Advanced Calculus. Wiley, 1978.