Chr. Nelius: Kryptographie (SS 2011)

9. Aufgabe: Beweise: $V_A^{-1} \circ V_G = V_U^{-1} \circ V_A$.

Die Abbildung $V_A:\mathfrak{a}\longrightarrow\mathfrak{A}$ verwandelt einen Kleinbuchstaben in den entsprechenden Großbuchstaben, und $V_A^{-1}:\mathfrak{A}\longrightarrow\mathfrak{a}$ verwandelt einen Großbuchstaben in den entsprechenden Kleinbuchstaben.

 $V_A^{-1} \circ V_G$ und $V_U^{-1} \circ V_A$ sind beides Abbildungen $\mathfrak{a} \longrightarrow \mathfrak{a}$.

a	a	b	c	d	е	f	g	h	i	j	k	1	m	n	О	р	q	r	s	t	u	v	w	x	у	z
$V_G \downarrow$																										
\mathfrak{A}	G	Н	Ι	J	K	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	X	Y	Z	A	В	С	D	Ε	F
$V_A^{-1} \downarrow$																										
a	g	h	i	j	k	1	m	n	О	р	q	r	s	t	u	V	W	X	У	Z	a	b	С	d	е	f
a	a	b	c	d	е	f	g	h	i	j	k	1	m	n	О	p	q	r	S	t	u	v	W	X	у	Z
$V_U \downarrow$																										
A	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	Ν	О	Р	Q	R	S	Т
a	a	b	с	d	е	f	g	h	i	j	k	1	m	n	О	р	q	r	S	t	u	v	W	х	у	z
$V_A \downarrow$																										
\mathfrak{A}	A	В	С	D	Е	F	G	Н	Ι	J	K	L	Μ	Ν	О	Р	Q	R	S	Т	U	V	W	X	Y	Z
$V_U^{-1} \downarrow$																										
α	g	h	i	j	k	1	m	n	О	р	q	r	s	t	u	V	W	x	У	Z	a	b	С	d	е	f

Aus den Tabellen kann man

$$(V_A^{-1} \circ V_G)(\alpha) = (V_U^{-1} \circ V_A)(\alpha)$$
 für alle $\alpha \in \mathfrak{a}$

ablesen, so dass

$$V_A^{-1} \circ V_G = V_U^{-1} \circ V_A$$

folgt.