GENERALIZED TWISTED FIELDS

A. A. ALBERT
1. Introduction. Consider a finite field $\mathbb{F}$. If $V$ is any automorphism of $\mathbb{F}$ we define $\mathbb{F}_V$ to be the fixed field of $K$ under $V$. Let $S$ and $T$ be any automorphism of $\mathbb{F}$ and define $F$ to be the fixed field $F = \mathbb{F}_S = \mathbb{F}_T$ under both $S$ and $T$. Then $\mathbb{F}$ is the field of $q = p^n$ elements, where $p$ is the characteristic of $\mathbb{F}$, and $\mathbb{F}$ is a field of degree $n$ over $\mathbb{F}_s$. We shall assume that

$$n > 2, \quad q > 2.$$  

Then the period of a primitive element of $\mathbb{F}$ is $q^n - 1$ and there always exist elements $c$ in $\mathbb{F}$ such that $c \neq k^{s-1}$ for any element $k$ of $\mathbb{F}$. Indeed we could always select $c$ to be a primitive element of $\mathbb{F}$.

Define a product $(x, y)$ on the additive abelian group $\mathbb{F}$, in terms of the product $xy$ of the field $\mathbb{F}$, by

$$(3) \quad (x, y) = xA_y + yB_x = xy - c(xT)(yS),$$

for $c$ in $\mathbb{F}$. Then

$$(4) \quad A_y = R_y - TR_{c(yS)} = R_x - SR_{c(xT)}.$$

where the transformation $R_y = R[y]$ is defined for all $y$ in $\mathbb{F}$ by the product $xy = xR_y$ of $\mathbb{F}$. Then the condition that $(x, y) \neq 0$ for all $xy \neq 0$ is equivalent to the property that

$$(5) \quad c \neq \frac{x}{xT} \frac{y}{yS},$$

for any nonzero $x$ and $y$ of $\mathbb{F}$. But the definition of a generating automorphism $U$ of $\mathbb{F}$ over $\mathbb{F}$ by $xU = x^2$ implies that

$$(6) \quad S = U^\beta, \quad T = U^\gamma.$$  

We shall assume that $S \neq I, T \neq I$, so that

$$0 < \beta < n, \quad 0 < \gamma < n.$$  

Then $xy[(xS)(yT)]^{-1} = z^{s-1}$, where

$$(8) \quad 1 - q^\beta = (q - 1)^s, \quad 1 - q^\gamma = (q - 1)^s, \quad z = x^by^c.$$
Thus the condition that \( c \neq k^{a-1} \) is sufficient to insure the property that 
\( (x, y) \neq 0 \) whenever \( xy \neq 0 \).

For every \( c \) satisfying (5) we can define a division ring \( \mathbb{D} = \mathbb{D}(\mathbb{R}, S, T, c) \), with unity quantity \( f = e - c \), where \( e \) is the unity quantity of \( \mathbb{R} \). It is the same additive group as \( K \) and we define the
product \( x \cdot y \) of \( D \) by

\[
(9) \quad xA_e \cdot yB_e = (x, y).
\]

These rings may be seen to generalize the twisted fields defined in an earlier paper.¹

We shall show that \( \mathbb{D} \) is isomorphic to \( \mathbb{K} \) if and only if \( S = T \). Indeed we shall derive the following result.

**Theorem 1.** Let \( S \neq I \), \( T \neq I \), \( S \neq T \). Then the right nucleus of 
\( \mathbb{D}(\mathbb{R}, S, T, c) \) is \( f\mathbb{K}_s \) and the left nucleus of \( \mathbb{D}(\mathbb{R}, S, T, c) \) is \( f\mathbb{K}_r \). If \( \mathcal{L} \) is the set of all elements \( g \) of \( \mathbb{R} \) such that \( gS = gT \) then \( gA_e = gB_e \) and 
\( \mathcal{L}A_e = \mathcal{L}B_e \) is the middle nucleus of \( \mathbb{D} \).

The result above implies that \( f\mathbb{K}_s \) is the center of \( \mathbb{D}(\mathbb{R}, S, T, c) \). Since it is known² that isotopic rings have isomorphic right (left and middle) nuclei, our results imply that the (generalized) twisted fields 
\( \mathbb{D}(\mathbb{R}, S, T, c) \) are new whenever the group generated by either \( S \) or \( T \) is not the group generated by \( S \) and \( T \). In this case our new twisted fields define new finite non-Desarguesian projective planes.³

2. The fundamental equation. Consider the equation

\[
(9) \quad A_x A_e^{-1} A_y = A_z,
\]

for \( x, y \) and \( z \) in \( \mathbb{K} \). Assume that the degree of \( \mathbb{K} \) over \( \mathbb{K}_T \) is \( m \), where we shall now assume that

\[
(10) \quad m > 2.
\]

¹ For earlier definitions of twisted fields see the case \( c = -1 \) in *On nonassociative division algebras*, Trans. Amer. Math. Soc. 72 (1952), 296-309 and the general case in *Finite noncommutative division algebras*, Proc. Amer. Math. Soc. 9 (1958), 928-932. In those papers we defined a product \( [x, y] = x(yT) - cy(xT) \) so that \( (x, y) = [x, yT^{-1}] = xy - c(yS)(xT) \) is the product (3) with \( S = T^{-1} \).

² This result was originally given for loops by R. H. Bruck. It is easy to show that, if \( \mathbb{D} \) and \( \mathbb{D}_0 \) are isotopic rings with isotopy defined by the relation \( QR_xP = R_y^{-1}QR_z \), then the mapping \( x \to (xz)^P \) induces an isomorphism of the right nucleus \( \mathbb{D} \) onto that of \( \mathbb{D}_0 \), and the mapping \( x \to (xz)^P \) induces an isomorphism of the middle nucleus of \( \mathbb{D} \) onto that of \( \mathbb{D}_0 \).

³ Two finite projective planes \( \mathcal{M}(\mathbb{D}) \) and \( \mathcal{M}(\mathbb{D}_0) \) coordinatized by division rings \( \mathbb{D} \) and \( \mathbb{D}_0 \) respectively are known to be isomorphic if and only if \( \mathbb{D} \) and \( \mathbb{D}_0 \) are isotopic. See the author's *Finite division algebras and finite planes*, Proceedings of Symposia in Applied Mathematics; vol. 10, pp. 53-70.
Then the norm in $\mathfrak{K}$ over $\mathfrak{K}_r$ of any element $k$ of $\mathfrak{K}$ is
\begin{equation}
\nu(k) = k(kT) \cdots (kT^{m-1}),
\end{equation}
and $\nu(k)$ is in $\mathfrak{K}_r$, that is,
\begin{equation}
\nu(k) = [\nu(k)]T
\end{equation}
for every $k$ of $\mathfrak{K}$. Thus
\begin{equation}
I - (TR_c)^m = I - R_{\nu(c)} = R_d,
\end{equation}
where
\begin{equation}
d = e - \nu(e) = dT.
\end{equation}
Now
\begin{equation}
A_e = I - TR_c, \quad B_e = I - SR_c,
\end{equation}
and we obtain
\begin{equation}
A_e[I + TR_c + (TR_c)^3 + \cdots + (TR_c)^{m-1}] = R_d,
\end{equation}
so that
\begin{equation}
I + TR_c + (TR_c)^3 + \cdots + (TR_c)^{m-1} = A_e^{-1}R_d.
\end{equation}
Our definition (4) implies that
\begin{equation}
R_xA_y = A_yR_x, \quad R_yB_x = B_xR_y,
\end{equation}
for every $x$ and $y$ of $K$, providing that
\begin{equation}
a = aT, \quad b = bS.
\end{equation}
In particular, $R_dA_y = A_yR_d$, and so (9) is equivalent to
\begin{equation}
A_e[I + (TR_c) + (TR_c)^3 + \cdots + (TR_c)^{m-1}]A_y = A_sR_d.
\end{equation}

It is well known that distinct automorphisms of any field $\mathfrak{K}$ are linearly independent in the field of right multiplications of $\mathfrak{K}$. Thus we can equate the coefficients of the distinct powers of $T$ in the equation (20). The right member of (20) is $R_{\nu(d)} - TR_{\nu(d)\nu(S)}$ and so does not contain the term in $T^{m-1}$ when $m > 2$. It follows that
\begin{equation}
R_x[(TR_c)^{m-1}R_y - (TR_c)^{m-2}(TR_c)R_{yS}]
- TR_{c(xS)}[(TR_c)^{m-2}R_y - (TR_c)^{m-3}(TR_c)R_{yS}] = 0.
\end{equation}
This equation is equivalent to
\begin{equation}
xT^{m-1}(y - yS) = xST^{m-2}(y - yS),
\end{equation}
and so to the relation
\[(x - x_{ST^{-1}})T^{n-1})(y - yS) = 0.\]
By symmetry we have the following result.

**Lemma 1.** Let \(T\) have period \(m > 2\). Then the equation \(A_xA_y^{-1}A_y = A_x\) holds for some \(x, y, z\) in \(\mathcal{S}\) only if \(y = yS\) or \(x = x_{ST^{-1}}\). If \(S\) has period \(m_o > 2\) the equation \(B_yB_x^{-1}B_x = B_x\) holds for some \(x, y, z\) in \(\mathcal{S}\) only if \(x = xT\) or \(y = yST^{-1}\).

3. **The nuclei.** The ring \(\mathcal{D} = \mathcal{D}(\mathcal{S}, S, T, c)\) has its product defined by
\[(24) \quad x \cdot y = xR_y^{(c)} = yL_y^{(c)},\]
where
\[(25) \quad R_y^{(c)} = A_y^{-1}A_y, \quad L_y^{(c)} = B_y^{-1}B_y.\]
When \(S = T\) our formula (3) becomes \((x, y) = xy - c[(xy)S] = xy(I - SR_e).\) But then the ring \(\mathcal{D}_e\), defined by the product \((x, y),\) is isotopic to the field \(\mathcal{S}\). Since \(\mathcal{D} = \mathcal{D}(\mathcal{S}, S, S, c)\) is isotopic to \(\mathcal{D}_e\), it is isotopic to \(\mathcal{S}\), and it is well known that \(\mathcal{D}\) is then also isomorphic to \(\mathcal{S}\). Assume henceforth that
\[(26) \quad S \neq T.\]

The right nucleus of \(\mathcal{D}\) is the set \(\mathcal{N}_p\) of all elements \(z_p\) in \(\mathcal{S}\) such that
\[(27) \quad (x \cdot y) \cdot z_p = x \cdot (y \cdot z_p),\]
for every \(x\) and \(y\) of \(\mathcal{S}\). Suppose that \(b = bS\) so that
\[(28) \quad A_b = R_b - TR_{e(bS)} = (I - TR)_b R_b, \quad A_x^{-1}A_b = R_b.\]
By (18) we know that \(R_bB_x = B_xR_b\), and so \(R_b(B_x^{-1}B_x) = (B_x^{-1}B_x)R_b\) for every \(x\) of \(\mathcal{S}\). By (25) this implies that the transformation
\[(29) \quad R_b = A_x^{-1}A_b = R_{bB_x}^{(c)}\]
commutes with every \(L_x^{(e)}\). However, (27) is equivalent to
\[(30) \quad L_x^{(e)}R_x^{(e)} = R_x^{(e)}L_x^{(e)}.\]
Thus \(bB_x = b(I - SR_e) = b(e - c) = bf\) is in \(\mathcal{N}_p\). We have proved that the right nucleus of \(\mathcal{D} = \mathcal{D}(\mathcal{S}, S, T, c)\) contains the field \(f\mathcal{S}\), a subring of \(\mathcal{D}\) isomorphic to \(\mathcal{S}\).

The left nucleus \(\mathcal{N}_\lambda\) of \(\mathcal{D}\) consists of all \(z_\lambda\) such that
\[(31) \quad (z_\lambda \cdot y) \cdot x = z_\lambda \cdot (y \cdot x)\]
for all \( x \) and \( y \) of \( \mathfrak{R} \). This equation is equivalent to

\[
L_x^{(c)} R_x^{(c)} = R_x^{(c)} L_x^{(c)}
\]

for every \( x \) of \( \mathfrak{R} \). If \( a = aT \) then \( B_a = (I - SR_c)R_a \), \( B^{-1}B_a = R_a = L_x^{(c)} \) commutes with every \( A_y \) and every \( R_x^{(c)} \), and we see that the left nucleus of \( \mathcal{D}(\mathfrak{R}, S, T, c) \) contains the field \( f\mathfrak{R}_r \) isomorphic to \( \mathfrak{R}_r \).

The middle nucleus of \( \mathcal{D} = \mathcal{D}(\mathfrak{R}, S, T, c) \) is the set \( \mathcal{N}_\mu \) of all \( z_\mu \) of \( \mathfrak{R} \) such that

\[
(x \cdot z_\mu) \cdot y = x \cdot (z_\mu \cdot y)
\]

for every \( x \) and \( y \) of \( \mathfrak{R} \). This equation is equivalent to

\[
R_z^{(c)} R_y^{(c)} = R_z^{(c)} R_y^{(c)}
\]

where \( z = z_\mu \). However, we can observe that the assumption that

\[
R_z^{(c)} R_y^{(c)} = R_z^{(c)}
\]

for some \( v \) in \( \mathfrak{R} \), implies that \((f \cdot z) \cdot y = f \cdot v = v = z \cdot y \). Hence (34) holds for every \( y \) in \( \mathfrak{R} \) if and only if

\[
A_y A_{e'} A_v = A_v,
\]

for every \( y \) of \( \mathfrak{R} \), where \( v \) is in \( \mathfrak{R} \) and

\[
gB_e = z = z_\mu.
\]

If \( gS = gT \) then \( A_g = R_g - TR_{c(gS)} = R_g - TR_{c(gT)} = R_g - R_g TR_c = R_g A_s \). Then (36) becomes

\[
R_g A_y = R_g (R_g - TR_{c(\cdot gS)}) = R_g v - TR_{c(gSgT)} = A_y v.
\]

Hence \( gB_e = g(I - SR_c) = g - (gS)c = g - (gT)c = gA_s \), and \( \mathfrak{R}_\mu \) contains the field of all elements \( gB_e \) for \( gS = gT \).

We are now able to derive the converse of these results. We first observe that (27) is equivalent to

\[
R_y^{(c)} R_z^{(c)} = R_z^{(c)} R_y^{(c)}
\]

for every \( y \) of \( \mathfrak{R} \), where \( z = z_\mu \). This equation is equivalent to

\[
A_y A_{e'} A_u = A_u,
\]

where \( z = uB_e \). If the period of \( T \) is \( m > 2 \) we use Lemma 1 to see that, if we take \( y \neq yST^{-1} \), then \( u = uS \), \( z = uB_e = fu \). The stated choice of \( y \) is always possible since we assuming that \( S \neq T \) and so some element of \( \mathfrak{R} \) is not left fixed by \( ST^{-1} \). Thus \( \mathfrak{R} = f\mathfrak{R}_g \). Similarly, if the period of \( S \) is not two then \( \mathfrak{R}_\lambda = f\mathfrak{R}_r \). Assume that one of \( S \) and \( T \) has period two.
The automorphisms $S$ and $T$ cannot both have period two. For the group $G$ of automorphisms of $\mathcal{F}$ is a cyclic group and has a unique subgroup $\xi$ of order two. This group contains $I$ and only one other automorphism. If $S$ and $T$ both had period two we would have $S = T$ and so $m = n = 2$, contrary to hypothesis. Thus we may assume that one of $S$ and $T$ has period two. There is clearly no loss of generality if we assume that $T$ has period two, so that the period of $S$ is at least three. By the argument already given we have $R_\lambda = f R_T$. We are then led to study (40) as holding for all elements $y$ of $\mathcal{F}$, where $z_p = uB_e$. Now

\begin{equation}
A_e = I - TR_e, \quad A_e(I + TR_e) = R_d, \quad d = e - c(cT) = dT.
\end{equation}

But then (40) becomes

\begin{equation}
[R_y - TR_{c(yS)}](I + TR_e)[R_y - TR_{c(uS)}] = R_{vd} - TR_{vd(yS)}.
\end{equation}

This yields the equations

\begin{align}
y[u - c(cT)(uS)] - (yST)[c(cT)](u - uS) &= vd, \\
yT(u - uS) - yS[u - (uS)c(cT)] &= -d(vS).
\end{align}

Hence

\begin{align*}
d(yS)[uS - (cS)(cST)(uS^2)] - yS^2T(cS)(cST)(uS - uS^2)d &= vS(dS)d \\
&= (dS)yS[u - (uS)c(cT)] - yT(u - uS)(dS).\end{align*}

Since this holds for all $y$ we have the transformation equation

\begin{equation}
SR[d(uS) - d(cS)(cST)uS^2] - S^2TR[d(cS)(cST)(uS - uS^2)] \\
= SR[dSu - (dS)(uS)c(cT)] - TR[(u - uS)dS].
\end{equation}

Since $S^2 \neq I$ and $T \neq S$, $S^2T$ we know that the coefficient of $S^2T$ is zero. Thus $(u - uS)dS = 0$ and $u = uS$ as desired. This shows that $R_\lambda = f R_\xi$.

The middle nucleus condition (36) implies that $gS = gT$ if $T$ does not have period two. When $T$ does have period two but $S$ does not have period two the analogous property

\begin{equation}
L_{z^e}^{(c)} = L_{z}^{(c)}L_{z}^{(c)}
\end{equation}

is equivalent to

\begin{equation}
B_zB_z^{-1}B_z = B_z,
\end{equation}

and we see again that $gS = gT$. This completes our proof of the theorem stated in the introduction.
4. Commutativity. It is known\(^4\) that \(\mathfrak{D} = (\mathfrak{F}, S, S^{-1}, c)\) is commutative if and only if \(c = -1\). There remains the case where \(S \neq I, T \neq I, ST \neq I, S \neq T\).

Any \(\mathfrak{D}(\mathfrak{F}, S, T, c)\) is commutative if and only if \(R_x^{(c)} = L_x^{(c)}\) for every \(x\) of \(\mathfrak{F}\). Assume first that \(\mathfrak{F}_S \neq \mathfrak{F}_T\). There is clearly no loss of generality if we assume that there is an element \(b\) in \(\mathfrak{F}_S\) and not in \(\mathfrak{F}_T\), since the roles of \(S\) and \(T\) can be interchanged when \(\mathfrak{D}(\mathfrak{F}, S, T, c)\) is commutative. Thus we have \(b = bS \neq bT\). By (28) we know that \(A_b = A_e R_b\) and so we have \(R_b^{(c)} = R_b\). Then \(L_b^{(c)} = B_b^{-1} B'_y = R_b\), where \(y = (bf)A_e^{-1}\). It follows that

\[
B_y = R_y - SR_c(yT) = B_e R_b = (I - SR_c) R_b. \quad (49)
\]

Then \(R_y = R_b\), \(y = b\), \(c(yT) = c(bT) = cb\), and \(b = bT\) contrary to hypothesis.

We have shown that if \(\mathfrak{D}(\mathfrak{F}, S, T, c)\) is commutative the automorphisms \(S\) and \(T\) have the same fixed fields, that is, \(b = bS\) if and only if \(b = bT\), \(b\) is in \(\mathfrak{F}_S\). Thus \(S\) and \(T\) both generate the cyclic automorphism group \(\mathfrak{G}\) of order \(n\) of \(\mathfrak{F}\) over \(\mathfrak{F}_S\), and \(S\) is a power of \(T\). Since \(T^{-1} = T^{n-1} \neq S\) there exists an integer \(r\) such that

\[
0 < r < n - 1, \quad S = T^r. \quad (50)
\]

We now use the fact that \(R_x^{(c)} = L_x^{(c)}\) for every \(x\) of \(K\) to see that \(A_e^{-1} A_x = B_e^{-1} B'_y\) for every \(x\) of \(\mathfrak{F}\), where \(y = xB_eA_e^{-1}\). Also \((TR_c)^n = (SR_c)^n = R_{v(c)}\), and our condition becomes

\[
[I + TR_c + (TR_c)^2 + \cdots + (TR_c)^{n-1}] [R_x - TR_c(xS)] = [I + SR_c + (SR_c)^2 + \cdots + (SR_c)^{n-1}] [R_y - SR_c(yT)], \quad (51)
\]

where we have used the fact that \(d = e - \nu(c) = dT = dS\). Compute the constant term to obtain the equation

\[
R_x - (TR_c)^n R_{xS} = R_y - (SR_c)^n R_{yT}. \quad (52)
\]

This is equivalent to the relation \(x - [\nu(c)](xS) = y - [\nu(c)]yT\) for every \(x\) of \(K\), where \(y = xB_eA_e^{-1}\). Thus (52) is equivalent to

\[
I - SR_{v(c)} = B_e A_e^{-1} [I - TR_{v(c)}], \quad (53)
\]

We also compute the term in \(T^r\) in (51). Since \(r < n - 1\) the left member of this term is \((TR_c)^r R_x - (TR_c)^r R_{xS}\), which is equal to \(R_x R_{gT}(R_x - R_{xS})\), where \(g = (cT)(cT)^2 \cdots (cT)^{r-1}\). The right member is the term in \(S\), and this is \(SR_c(R_y - R_{yT})\). Hence \((x - xS)g = y - yT\), a result equivalent to

\(^4\) See footnote 1.
(54) \[(I - S)R_g = B_eA_e^{-1}(I - T).\]

Since the transformations \(I - T\) and \(I - TR_{\nu(c)}\) commute we may use (53) to obtain

(55) \[(I - S)R_g[I - TR_{\nu(c)}] = [I - SR_{\nu(c)}](I - T).\]

By (48) we may equate coefficients of \(I, S, T\) and \(ST\), respectively. The constant term yields \(g = e\). The term in \(S\) then yields \(\nu(c) = e\) which is impossible when \(S\) and \(T\) generate the same group and \(D = D(\mathbb{K}, S, T, c)\) is a division algebra.

We have proved the following result.

**Theorem 2.** Let \(D = D(\mathbb{K}, S, T, c)\) be a division algebra defined for \(S \neq I, T \neq I, S \neq T\). Then \(D\) is commutative if and only if \(ST = I\) and \(c = -1\).
PACIFIC JOURNAL OF MATHEMATICS

EDITORS
RALPH S. PHILLIPS
Stanford University
Stanford, California

F. H. BROWNELL
University of Washington
Seattle 5, Washington

A. L. WHITEMAN
University of Southern California
Los Angeles 7, California

L. J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS
E. F. BECKENBACH
D. DERRY
T. M. CHERRY
M. OHTSUKA
H. L. ROYDEN
E. SPANIER
E. G. STRAUS
F. WOLF

SUPPORTING INSTITUTIONS
UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON

* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
HUGHES AIRCRAFT COMPANY
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Reprinted 1966 in the United States of America