Pacific Journal of Mathematics

GENERALIZED TWISTED FIELDS

A. A. Albert

Vol. 11, No. 1 November 1961

GENERALIZED TWISTED FIELDS

A. A. ALBERT

1. Introduction. Consider a finite field $\mathfrak{K}$. If V is any automorphism of $\mathfrak{K}$ we define $\mathfrak{K}_V$ to be the *fixed field* of K under V. Let S and T be any automorphism of $\mathfrak{K}$ and define F to be the fixed field

$$(1) \qquad \mathfrak{F} = \mathfrak{F}_q = (\mathfrak{K}_S)_T = (\mathfrak{K}_T)_S ,$$

under both S and T. Then $\mathfrak{F}$ is the field of $q = p^\alpha$ elements, where p is the characteristic of $\mathfrak{K}$, and $\mathfrak{K}$ is a field of degree n over $\mathfrak{F}$. We shall assume that

$$(2) \qquad n > 2 , \qquad q > 2 .$$

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

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

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

for c in $\mathfrak{K}$. Then

$$(4) \qquad A_y = R_y - TR_{c(yS)} , \qquad B_x = R_x - SR_{c(xT)} ,$$

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

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

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

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

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

$$(7) \qquad 0 < \beta < n , \qquad 0 < \gamma < n .$$

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

$$(8) \qquad 1 - q^\beta = (q-1)^\delta,\ 1 - q^\gamma = (q-1)^\varepsilon,\ z = x^\delta y^\varepsilon .$$

Received April 25, 1960. This paper was supported in part by an Esso Educational Foundation Grant and by NSF Grant G-9504.

Thus the condition that $c \neq k^{q-1}$ 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 $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, S, T, c)$, with unity quantity $f = e - c$, where e is the unity quantity of $\mathfrak{K}$. It is the same additive group as K and we define the product $x \cdot y$ of D by

$$(9) \qquad xA_e \cdot yB_e = (x, y) .$$

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

We shall show that $\mathfrak{D}$ is isomorphic to $\mathfrak{K}$ 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 $\mathfrak{D}(\mathfrak{K}, S, T, c)$ is $f\mathfrak{K}_S$ and the left nucleus of $\mathfrak{D}(\mathfrak{K}, S, T, c)$ is $f\mathfrak{K}_T$. If $\mathfrak{L}$ is the set of all elements g of $\mathfrak{K}$ such that $gS = gT$ then $gA_e = gB_e$ and $\mathfrak{L}A_e = \mathfrak{L}B_e$ is the middle nucleus of $\mathfrak{D}$.*

The result above implies that $f\mathfrak{F}$ is the center of $\mathfrak{D}(\mathfrak{K}, S, T, c)$. Since it is known[2] that isotopic rings have isomorphic right (left and middle) nuclei, our results imply that the (generalized) twisted fields $\mathfrak{D}(\mathfrak{K}, S, T, c)$ 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

$$(9) \qquad A_x A_e^{-1} A_y = A_z ,$$

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

$$(10) \qquad m > 2 .$$

[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 $\mathfrak{D}$ and $\mathfrak{D}_0$ are isotopic rings with isotopy defined by the relation $QR_{xP} = R_x^{(c)} QR_z$, then the mapping $x \rightarrow (zx)P^{-1}$ induces an isomorphism of the right nucleus $\mathfrak{D}$ onto that of $\mathfrak{D}_0$, and the mapping $x \rightarrow (xz)P^{-1}$ induces an isomorphism of the middle nucleus of $\mathfrak{D}$ onto that of $\mathfrak{D}_0$.

[3] Two finite projective planes $\mathfrak{M}(\mathfrak{D})$ and $\mathfrak{M}(\mathfrak{D}_0)$ coordinatized by division rings $\mathfrak{D}$ and $\mathfrak{D}_0$ respectively are known to be isomorphic if and only if $\mathfrak{D}$ and $\mathfrak{D}_0$ 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 $\mathfrak{K}_T$ of any element k of $\mathfrak{K}$ is

$$\nu(k) = k(kT)\cdots(kT^{m-1}) , \tag{11}$$

and $\nu(k)$ is in $\mathfrak{K}_T$, that is,

$$\nu(k) = [\nu(k)]T \tag{12}$$

for every k of $\mathfrak{K}$. Thus

$$I - (TR_c)^m = I - R_{\nu(e)} = R_d , \tag{13}$$

where

$$d = e - \nu(c) = dT . \tag{14}$$

Now

$$A_e = I - TR_c , \qquad B_e = I - SR_c , \tag{15}$$

and we obtain

$$A_e[I + TR_c + (TR_c)^2 + \cdots + (TR_c)^{m-1}] = R_d , \tag{16}$$

so that

$$I + TR_c + (TR_c)^2 + \cdots + (TR_c)^{m-1} = A_e^{-1}R_d . \tag{17}$$

Our definition (4) implies that

$$R_aA_y = A_yR_a , \qquad R_bB_x = B_xR_b \tag{18}$$

for every x and y of K, providing that

$$a = aT , \qquad b = bS . \tag{19}$$

In particular, $R_dA_y = A_yR_d$, and so (9) is equivalent to

$$A_x[I + (TR_c) + (TR_c)^2 + \cdots + (TR_c)^{m-1}]A_y = A_zR_d . \tag{20}$$

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 $R_{zd} - TR_{cd(zS)}$ and so does not contain the term in T^{m-1} when $m > 2$. It follows that

$$\begin{aligned} R_x[(TR_c)^{m-1}R_y - (TR_c)^{m-2}(TR_c)R_{yS}] \\ - TR_{c(xS)}[(TR_c)^{m-2}R_y - (TR_c)^{m-3}(TR_c)R_{yS}] = 0 . \end{aligned} \tag{21}$$

This equation is equivalent to

$$xT^{m-1}(y - yS) = xST^{m-2}(y - yS) , \tag{22}$$

and so to the relation

$$[(x - xST^{-1})T^{m-1}](y - yS) = 0 \; . \tag{23}$$

By symmetry we have the following result.

LEMMA 1. *Let T have period $m > 2$. Then the equation $A_x A_e^{-1} A_y = A_z$ holds for some x, y, z in $\mathfrak{K}$ only if $y = yS$ or $x = xST^{-1}$. If S has period $m_0 > 2$ the equation $B_y B_e^{-1} B_x = B_z$ holds for some x, y, z in $\mathfrak{K}$ only if $x = xT$ or $y = yST^{-1}$.*

3. The nuclei. The ring $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, S, T, c)$ has its product defined by

$$x \cdot y = xR_y^{(o)} = yL_y^{(c)}, \tag{24}$$

where

$$R_{yB_e}^{(c)} = A_e^{-1} A_y \; , \qquad L_{xA_e}^{(c)} = B_e^{-1} B_x \; . \tag{25}$$

When $S = T$ our formula (3) becomes $(x, y) = xy - c[(xy)S] = xy(I - SR_c)$. But then the ring $\mathfrak{D}_0$, defined by the product (x, y), is isotopic to the field $\mathfrak{K}$. Since $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, S, S, c)$ is isotopic to $\mathfrak{D}_0$ it is isotopic to $\mathfrak{K}$, and it is well known that $\mathfrak{D}$ is then also isomorphic to $\mathfrak{K}$. Assume henceforth that

$$S \neq T \; . \tag{26}$$

The right nucleus of $\mathfrak{D}$ is the set $\mathfrak{N}_\rho$ of all elements z_ρ in $\mathfrak{K}$ such that

$$(x \cdot y) \cdot z_\rho = x \cdot (y \cdot z_\rho) \; , \tag{27}$$

for every x and y of $\mathfrak{K}$. Suppose that $b = bS$ so that

$$A_b = R_b - TR_{c(bS)} = (I - TR_c)R_b, \; A_e^{-1} A_b = R_b \; . \tag{28}$$

By (18) we know that $R_b B_x = B_x R_b$, and so $R_b(B_e^{-1} B_x) = (B_e^{-1} B_x) R_b$ for every x of $\mathfrak{K}$. By (25) this implies that the transformation

$$R_b = A_e^{-1} A_b = R_{bB_e}^{(c)} \tag{29}$$

commutes with every $L_x^{(e)}$. However, (27) is equivalent to

$$L_x^{(c)} R_{z_\rho}^{(c)} = R_{z_\rho}^{(c)} L_x^{(c)} \; . \tag{30}$$

Thus $bB_e = b(I - SR_c) = b(e - c) = bf$ is in $\mathfrak{N}_\rho$. We have proved that the right nucleus of $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, S, T, c)$ *contains* the field $f\mathfrak{K}_S$, a subring of $\mathfrak{D}$ isomorphic to $\mathfrak{K}_S$.

The left nucleus $\mathfrak{N}_\lambda$ of $\mathfrak{D}$ consists of all z_λ such that

$$(z_\lambda \cdot y) \cdot x = z_\lambda \cdot (y \cdot x) \tag{31}$$

for all x and y of $\mathfrak{R}$. This equation is equivalent to

(32) $$L_{z_\lambda}^{(c)} R_x^{(c)} = R_x^{(c)} L_{z_\lambda}^{(c)}$$

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

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

(33) $$(x \cdot z_\mu) \cdot y = x \cdot (z_\mu \cdot y)$$

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

(34) $$R_z^{(c)} R_y^{(c)} = R_{z \cdot y}^{(c)} ,$$

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

(35) $$R_z^{(c)} R_y^{(c)} = R_v^{(c)} ,$$

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

(36) $$A_g A_e^{-1} A_y = A_v ,$$

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

(37) $$gB_e = z = z_\mu .$$

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

(38) $$R_g A_y = R_g(R_g - TR_{c(yS)}) = R_{gy} - TR_{c(ySgT)} = A_{gy} .$$

Hence $gB_e = g(I - SR_c) = g - (gS)c = g - (gT)c = gA_e$, and $\mathfrak{N}_\mu$ 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

(39) $$R_y^{(c)} R_z^{(c)} = R_{y \cdot z}^{(c)} ,$$

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

(40) $$A_y A_e^{-1} A_u = A_v ,$$

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 $\mathfrak{N} = f\mathfrak{R}_S$. Similarly, is the period of S is not two then $\mathfrak{N}_\lambda = f\mathfrak{R}_T$. 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 $\mathfrak{K}$ is a cyclic group and has a unique subgroup $\mathfrak{H}$ 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 $\mathfrak{N}_\lambda = f\mathfrak{K}_T$. We are then led to study (40) as holding for all elements y of $\mathfrak{K}$, where $z_\rho = uB_e$. Now

$$(41) \qquad A_e = I - TR_c,\ A_e(I + TR_c) = R_d,\ d = e - c(cT) = dT\,.$$

But then (40) becomes

$$(42) \qquad [R_y - TR_{c(yS)}](I + TR_c)[R_u - TR_{c(uS)}] = R_{vd} - TR_{cd(vS)}\,.$$

This yields the equations

$$(43) \qquad y[u - c(cT)(uS)] - (yST)[c(cT)](u - uS) = vd\,,$$

$$(44) \qquad yT(u - uS) - yS[u - (uS)c(cT)] = -d(vS)\,.$$

Hence

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

Since this holds for all y we have the transformation equation

$$(45) \qquad \begin{aligned} SR[d(uS) - d(cS)(cST)uS^2] - S^2TR[d(cS)(cST)(uS - uS^2)] \\ = SR[dSu - (dS)(uS)c(cT)] - TR[(u - uS)dS]\,. \end{aligned}$$

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 $\mathfrak{N}_\rho = f\mathfrak{K}_S$.

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

$$(46) \qquad L^{(c)}_{x\cdot z} = L^{(c)}_z L^{(c)}_x$$

is equivalent to

$$(47) \qquad B_g B_e^{-1} B_x = B_v\,,$$

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 $\mathfrak{D} = (\mathfrak{K}, S, S^{-1}, c)$ is commutative if and only if $c = -1$. There remains the case where

$$S \neq I,\ T \neq I,\ ST \neq I,\ S \neq T\ . \tag{48}$$

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

$$B_g = R_y - SR_{c(yT)} = B_e R_b = (I - SR_c)R_b\ . \tag{49}$$

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

We have shown that if $\mathfrak{D}(\mathfrak{K}, S, T, c)$ 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 $\mathfrak{F}$. Thus S and T both generate the cyclic automorphism group $\mathfrak{G}$ of order n of $\mathfrak{K}$ over $\mathfrak{F}$, and S is a power of T. Since $T^{-1} = T^{n-1} \neq S$ there exists an integer r such that

$$0 < r < n - 1,\ S = T^r\ . \tag{50}$$

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 $\mathfrak{K}$, where $y = xB_e A_e^{-1}$. Also $(TR_c)^n = (SR_c)^n = R_{\nu(c)}$, and our condition becomes

$$\begin{aligned}[I + TR_c + (TR_c)^2 + \cdots + (TR_c)^{n-1}][R_x - TR_{c(xS)}]\\ = [I + SR_c + (SR_c)^2 + \cdots + (SR_c)^{n-1}][R_y - SR_{c(yT)}]\ ,\end{aligned} \tag{51}$$

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

$$R_x - (TR_c)^n R_{xS} = R_y - (SR_c)_u R_{yT}\ . \tag{52}$$

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

$$I - SR_{\nu(c)} = B_e A_e^{-1}[I - TR_{\nu(c)}]\ . \tag{53}$$

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 $R^r R_{gc}(R_x - R_{xS})$, 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.

$$(54) \qquad (I - S)R_g = B_e A_e^{-1}(I - T) .$$

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

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

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 $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, S, T, c)$ is a division algebra.

We have proved the following result.

THEOREM 2. *Let $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, S, T, c)$ be a division algebra defined for $S \neq I$, $T \neq I$, $S \neq T$. Then $\mathfrak{D}$ is commutative if and only if $ST = I$ and $c = -1$.*

THE UNIVERSITY OF CHICAGO

PACIFIC JOURNAL OF MATHEMATICS

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

Reprinted 1966 in the United States of America

Pacific Journal of Mathematics
Vol. 11, No. 1 November, 1961