Pacific Journal of Mathematics

INVERSION INVARIANT ADDITIVE SUBGROUPS OF DIVISION RINGS

DANIEL GOLDSTEIN, ROBERT M. GURALNICK,
LANCE SMALL AND EFIM ZELMANOV

Volume 227 No. 2 October 2006

PACIFIC JOURNAL OF MATHEMATICS
Vol. 227, No. 2, 2006

INVERSION INVARIANT ADDITIVE SUBGROUPS OF DIVISION RINGS

DANIEL GOLDSTEIN, ROBERT M. GURALNICK,
LANCE SMALL AND EFIM ZELMANOV

We characterize the inversion invariant additive subgroups of any field, and, more generally, those of a division ring (apart from division rings of characteristic 2). We also show how a classical identity of Hua provides a bridge between this problem and Jordan algebras.

Answering a question of Dan Mauldin, we characterize in this note the inversion invariant additive subgroups of a field. We show in Section 2 that aside from the case of imperfect fields of characteristic 2, a nonzero subgroup that is inversion invariant is either a subfield or the set of trace-zero elements in a subfield with respect to an automorphism of order 2. A key ingredient in the proof is a simple, classical identity of Hua, through which we can bring to bear known results about Jordan algebras and Jordan triple systems. We also solve in Section 1 the same problem for division rings of characteristic not 2.

1. Division rings

We characterize pairs $T \subseteq D$, where D is a division ring of characteristic $\neq 2$; T is an additive of subgroup of D; for an arbitrary nonzero element of $t \in T$ the inverse t^{-1} again lies in T, and T generates D as a ring.

Example 1. $T = D$.

Example 2. Let $\sigma : D \to D$ be an involution of a division ring D (an additive map such that $\sigma(\sigma(a)) = a$ and $\sigma(ab) = \sigma(b)\sigma(a)$ for arbitrary elements a, b in D). Then $T = H(D, \sigma) = \{a \in D \mid \sigma(a) = a\}$ is inversion invariant. The additive subgroup $H(D, \sigma)$ generates D unless D is a quaternion algebra over its center and σ is a quaternionic involution; see [Herstein 1976].

MSC2000: 17C10, 17A35, 12E99.

Keywords: Jordan algebra, Clifford algebra, Jordan triple system.

Guralnick was supported by the National Science Foundation grant DMS 0140578, and Zelmanov was supported by NSF grant DMS 0350399.

Example 3. The additive group of skew symmetric elements

$$S(D,\sigma)=\{a\in D\mid \sigma(a)=-a\}$$

is also inversion invariant. It generates D unless D is a field and $\sigma=\mathrm{Id}$.

Example 4. Let σ, τ be two commuting involutions of a division ring D, and set $T=H(D,\sigma)\cap S(D,\tau)$. The subgroup T is inversion invariant.

Example 5. Let g be an automorphism of a division ring D of order 2. Then $T=S(D,g)=\{a\in D\mid g(a)=-a\}$ is inversion invariant and generates D.

Finally, we will describe somewhat special pairs which we will refer to as Clifford pairs.

Let V be a vector space over a field F with a quadratic form $q:V\to F$ such that the Clifford algebra $C=C(V,q)$ is a division ring. Let $J=F\cdot 1+V\subseteq C$ and let $0\neq x\in C$ be an element such that $xJx=J$. Then

$$\text{(i)}\qquad T=xJ\subset C$$

is inversion invariant and generates C.

Now suppose that the space V is finite dimensional over F and $\dim_F V=n$ is even. Choose an orthogonal basis $v_1,\dots,v_n$ of V. Let $0\neq x\in C$ be an element such that $x(J+Fv_1\cdots v_n)x=J+Fv_1\cdots v_n$. Then

$$\text{(ii)}\qquad T=x(J+Fv_1\cdots v_n)\subset C$$

is inversion invariant.

Let $\langle T\rangle_{\text{even}}$, $\langle T\rangle_{\text{odd}}$ be the additive subgroups of C generated by products of elements of T of even and odd lengths, respectively.

In the pairs of types (i) and (ii)

$$\langle T\rangle_{\text{even}}=\langle T\rangle_{\text{odd}}.$$

This does not always have to be the case. Let D be a $\mathbb{Z}/2\mathbb{Z}$-graded division ring, $D=D_0+D_1$, whose even part D_0 is isomorphic to the Clifford algebra C of a quadratic form $q:V\to F$. Suppose $x\in D_1$ satisfies $xJx=J$. Then

$$\text{(iii)}\qquad T=xJ\subset D_1\subset D$$

is inversion invariant and generates D.

If $\dim_F V=n$ is even, let $v_1,\dots,v_n$ be an orthogonal basis of V. If $0\neq x\in D_1$ satisfies $x(J+Fv_1\cdots v_n)x=J+Fv_1\cdots v_n$, then

$$\text{(iv)}\qquad T=x(J+Fv_1\cdots v_n)\subset D_1\subset D$$

is inversion invariant and generates D. In the pairs of types (iii) and (iv)

$$\langle T\rangle_{\text{even}} \cap \langle T\rangle_{\text{odd}} = 0.$$

Theorem 1.1. *If T is an inversion invariant additive subgroup of a division ring D, the characteristic of D is not 2, and T generates D, then $T \subseteq D$ is a pair of one of the types described in Examples 1–5 or of one of the Clifford types (i)–(iv).*

The key observation is an elementary identity of L. K. Hua [Jacobson 1980, Exercise 9, page 92].

Lemma 1.2 (Hua's Identity). *Let R be a ring with elements $a, b \in R$ such that a, b and $ab - 1$ are invertible. Then*

$$\big((a - b^{-1})^{-1} - a^{-1}\big)^{-1} = aba - a.$$

Corollary 1.3. *If T is an inversion invariant additive subgroup of a division ring D then for arbitrary elements $a, b \in T$ we have $aba \in T$.*

We will need a few definitions from the theory of Jordan systems.

A (not necessarily associative) ring J is called a Jordan ring if it satisfies

(J1) $$xy = yx,$$

(J2) $$(x^2y)x = x^2(yx),$$

for all x and y in J.

Example 6. If R is an associative ring then the additive group of R with the new multiplication $x \cdot y = xy + yx$ is a Jordan ring which is denoted $R^{(+)}$.

Example 7. If $\sigma : R \to R$ is an involution, then $H(R, \sigma) = \{a \in R \mid \sigma(a) = a\}$ is a Jordan subring of $R^{(+)}$.

Example 8. Let V be a vector space over a field F, $q : V \to F$ a quadratic form, and let $C = C(V, q)$ be the Clifford algebra. The space $J = F \cdot 1 + V$ is a Jordan subalgebra of $C^{(+)}$, which is called the Jordan algebra of the quadratic form q.

A Jordan ring J is said to be *special* if it is embeddable into $R^{(+)}$, where R is an associative ring. If R is generated by J then R is an associative enveloping ring of R.

Clearly, Examples 6, 7, and 8 are special. A Jordan ring that is not special is called exceptional.

Theorem 1.4. *A simple Jordan ring of characteristic $\neq 2$ is either isomorphic to $R^{(+)}$, where R is a simple associative ring, or to $H(R, \sigma)$, where R is a simple associative ring with an involution σ, or to a Jordan algebra of a nondegenerate quadratic form or is an exceptional 27-dimensional algebra over its center (called an Albert algebra).*

Simple (quadratic) Jordan algebras of characteristic 2 were classified in [McCrimmon and Zelmanov 1988].

Let T be an additive group equipped with group endomorphisms $P(x)$ for each x in T. We assume that the map from x to $P(x)$ is quadratic; that is, $P(nx) = n^2 P(x)$ and the map $P(x_1 + x_2) - P(x_1) - P(x_2)$ is bilinear in x_1 and x_2.

In other words, the product $P(x)y$ is quadratic in x and linear in y. We write

$$\{x, y, z\} = P(x+z)y - P(x)y - P(z)y.$$

We say that T is a Jordan triple system if it satisfies the identities

$$\text{(JT1)} \qquad \{z, P(x)y, y\} = \{z, x, P(y)x\},$$

$$\text{(JT2)} \qquad P(P(x)y)z = P(x)P(y)P(x)z,$$

$$\text{(JT3)} \qquad \{P(x)z, y, x\} = P(x)\{z, x, y\}$$

and all their linearizations (i.e., identities of lower degree coming from bilinearity: these are superfluous if we are working over a field F of at least four elements).

Example 9. If R is an associative ring then the additive group of R with a product $P(x)y = xyx$ is a Jordan triple system which we will also denote by $R^{(+)}$.

Any Jordan triple system T gives rise to a family of Jordan rings $T^{(a)}$, the a-homotopes, by fixing the middle element: $x \cdot y = \{x, a, y\}$.

A Jordan triple system T is called special if it is embeddable into $R^{(+)}$, where R is an associative ring, $T \subseteq R^{(+)}$. If the ring R is generated by T then we say R is an associative enveloping algebra of T. An associative enveloping algebra R of T is said to be *tight* if $T \cap I \neq (0)$ for any nonzero ideal I of R.

Let G be the ideal of the free Jordan triple system constructed in [Zelmanov 1984]. The identities from G distinguish triples of Clifford type assuming that the characteristic $\neq 2, 3$. Similar ideals for characteristics 2 and 3 were constructed in [D'Amour and McCrimmon 2000].

Proposition 1.5 [Zelmanov 1984]. *Let T be a simple special Jordan triple system such that $G(T) \neq (0)$. Then T is isomorphic to one of the triples $R^{(+)}$; $H(R, \sigma) = \{a \in R \mid \sigma(a) = a\}$; $S(R, \sigma) = \{a \in R \mid \sigma(a) = -a\}$; $H(R, \sigma) \cap S(R, \tau)$; $S(R, g)$, where R is a simple associative ring; σ, τ are involutions, $\sigma\tau = \tau\sigma$; g is an automorphism of order* 2.

Moreover, the ring R is in some sense unique.

Proposition 1.6 [Zelmanov 1984]. *Let T_1, T_2 be simple Jordan triple systems, such that $G(T_i) \neq (0)$. Let $T_i \subseteq R_i$ be their tight associative enveloping algebras. Then any isomorphism $T_1 \to T_2$ can be extended to an isomorphism or anti-isomorphism $R_1 \to R_2$.*

Proposition 1.7 [Zelmanov 1984]. *Let T be a simple special Jordan triple system such that $G(T) = (0)$. Then T is isomorphic to a mutation or a polarization of a Jordan triple system of a quadratic form. In particular, an arbitrary homotope $T^{(a)}$ is the Jordan algebra of a quadratic form.*

Proof of Theorem 1.1. Let $T \subseteq D$ be an inversion invariant additive subgroup that generates D. By the corollary to Hua's identity, T is a Jordan subtriple of $D^{(+)}$ and D is a tight associative enveloping algebra of T. If $G(T) \neq (0)$, Propositions 1.5 and 1.6 imply that $T \subseteq D$ is one of the types in Examples 1–5.

Suppose now that $G(T) = (0)$. Choose an arbitrary nonzero element $x \in T$. Then $J = x^{-1}T$ is a unital Jordan subalgebra of $D^{(+)}$. Indeed if $a, b, \in T$ then $(x^{-1}a)(x^{-1}b)+(x^{-1}b)(x^{-1}a)=x^{-1}(ax^{-1}b+bx^{-1}a)\in x^{-1}T=J$. By Proposition 1.7, J is isomorphic to the Jordan algebra of a symmetric nondegenerate bilinear form, $J = F\cdot 1 + V$, where F is a subfield of D, V is an F-space; $vw + wv = q(v, w)1$; $v, w, \in V$ and $q(v, w) \in F$.

Case 1. *J generates D and the dimension* $\dim_F V$ *is either infinite or even.* In this case the only associative enveloping algebra of J is the Clifford algebra $C(V, q)$ (see [Jacobson 1968]). Hence $D \cong C(V, q)$, $T = xJ$ and $T \subseteq D$ is a pair of type (i).

Case 2. *J generates D and the dimension* $\dim_F V$ *is odd.* Choose an orthogonal basis $v_1, \dots, v_{n+1}$ of V. Then the element $z = v_1 \cdots v_{n+1}$ lies in the center of the Clifford algebra $C(V, q)$, where $z^2 = \pm q(v_1)\cdots q(v_{n+1})$ depending on whether or not n is divisible by 4. If z^2 is not the square of an element of F then $C(V, q)$ is simple. In this case, $D \cong C(V, q)$ and $T \subseteq D$ is again a pair of type (i).

Suppose now that $z^2 = \alpha^2$, $\alpha \in F$. Then $z = \alpha$ or $-\alpha$ in D and $v_{n+1} \in Fv_1 \cdots v_n$. Let $V' = \sum_{i=1}^{n} Fv_i$. We have $D \cong C(V', q)$, $J = F \cdot 1 + V' + Fv_1 \cdots v_n$, and $T = xJ \subseteq D$ is a pair of type (ii).

Case 3. *The subring $\langle J\rangle$ of D generated by J is not equal to D and the dimension* $\dim_F V$ *is infinite or even.* Then $D = D_0 + D_1$, where $D_0 = \langle J\rangle$, $D_1 = x\langle J\rangle$ is a $\mathbb{Z}/2\mathbb{Z}$-grading. As above, $D_0 \cong C(V, q)$ and the pair $T \subseteq D$ is of type (iii).

Case 4. *$\langle J\rangle \neq D$ and* $\dim_F V$ *is odd.* Choose an orthogonal basis $v_1, \dots, v_{n+1}$ of V. Set $V' = \sum_{i=1}^{n} Fv_i$ and $z = v_1 \cdots v_{n+1}$. If z^2 is not equal to the square of an element of F then $\langle J\rangle \cong C(V, q)$ and $T \subset D$ is of type (i).

Otherwise, $v_{n+1} \in Fv_1 \cdots v_n$ lies in D and $T = x(F \cdot 1 + V' + Fv_1 \cdots v_n) \subseteq D_1 \subseteq D$ is a pair of type (iv). This finishes the proof of the proposition. □

2. Fields

In this section, we classify the inversion invariant additive subgroups of fields. Of course this result is included in the main theorem from the previous section as long as the characteristic is not 2. We include the proof for all characteristics.

Let K be a field. Write k for the prime subfield of K. Let V be an inversion invariant additive subgroup of K. Since $V \subseteq k(V)$, there is no harm in assuming that $K = k(V)$. If the characteristic p of the field L is positive, write

$$L^p = \{x^p \mid x \in L\}$$

for the subfield consisting of p-th powers of elements of L.

Our main result for the commutative case is:

Theorem 2.1 (Commutative Theorem). *Let K be a field of characteristic $p \geq 0$. Let V be a nonzero subset of K that is a subgroup under addition. Let k be the prime field of K and assume that $K = k(V)$. Then V is closed under inversion if and only if one of the following holds*:

(1) *$p \neq 2$ and either $V = K$ or there is an automorphism σ of K of order 2 such that $V = \{x \in K \mid \sigma(x) = -x\}$;*

(2) *$p = 2$ and V is a K^2-module.*

It is straightforward to verify that the possibilities mentioned in the theorem are inversion invariant. In particular, if K has characteristic 2, then $(aK^2)^{-1} = a^{-1}K^2 = a(a^{-2}K^2) = aK^2$ and so any K^2-submodule of K is inversion invariant.

Corollary 2.2. *Let K be a field of characteristic $p \geq 0$. Assume that $1 \in V$ and that either $p \neq 2$ or that the field generated by V is perfect* (*in particular*, *if K is contained in the algebraic closure of the field of size* 2). *Then V is inversion invariant if and only if V is a subfield of K.*

The remainder of this section is devoted to the proof of Theorem 2.1.

Lemma 2.3. *Let K be a field and V an additive subgroup of K closed under inversion. Let $0 \neq a \in V$. Then $a^3 \in V$ and $a^2V = V$.*

Proof. We saw in the corollary to Hua's identity that if a, b in V, then $aba \in V$. Taking $b = a$, we conclude that $a^3 \in V$. We also have $a^2V \subseteq V$. We get equality by multiplying by a^{-1}. □

Let K be a field and V a nonzero additive subgroup of K closed under inversion. Let V_2 be the set of all products xy with $x, y \in V$.

We have the following lemma.

Lemma 2.4. *Assume that $p \neq 2$. Let $0 \neq a \in V$. Then*

$$(1)\ \ V_2 = Va; \qquad (2)\ \ V_2a = V; \qquad (3)\ \ Va^2 = V.$$

Proof. We have already seen that $a^2V \subseteq V$. Thus, $2ab = (a+b)^2 - a^2 - b^2$ also sends V back to itself for any $a, b \in V$. Since the characteristic of K is not 2, the identity $v/2 = 1/(1/v + 1/v)$ for nonzero v shows that $(1/2)V \subseteq V$. Hence $abV \subseteq 2abV \subseteq V$. If $a \neq 0$, then using a^{-1} instead of a gives $Vb \subseteq Va$.

Hence $V_2 \subseteq Va$ since b was arbitrary in V. The reverse inclusion follows from the definition of V_2. This proves (1).

Taking a^{-1} for a gives (2), and (3) follows from (1) and (2). □

We now complete the proof in characteristic not 2.

Theorem 2.5. *Let K be a field of characteristic not 2 with V a nontrivial additive subgroup of K closed under inversion. Then*

(1) *V_2 is a field.*

(2) *The ring R generated by V (over $\mathbb{Z}$) is a field.*

(3) *Either $R = V = V_2$ or $[R : V_2] = 2$.*

Proof. We have $V_2 = Va$ for any nonzero $a \in V$. Fix such an a. Thus, $V_2 V_2 = VaVa = VVa^2 = VV = V_2$. Hence V_2 is a subgroup under addition and closed under multiplication. Since it also closed under inverses, it follows that V_2 is a field. This proves (1).

Let $R = \mathbb{Z}[V]$ be the ring generated by V. Since $V_2 V = V$ and $VV = V_2$, we see that $R = V + V_2$. Thus, R is a field (since it is algebraic over the field V_2 and is contained in the field K). This proves (2).

We have already seen that $R = V + V_2$ and that V and V_2 are each one-dimensional modules over the field V_2. So either the sum is direct and $[R : V_2] = 2$, or $R = V = V_2$. □

This gives the main result for fields of characteristic not 2 — for either V itself is a field or the ring R generated by V is a field and $[R : V_2] = 2$. We see that $V = aV_2$ with $a^2 \in V_2$, whence V is the -1 eigenspace of a nontrivial automorphism of R/V_2.

It remains to prove Theorem 2.1 in the case that the field K has characteristic 2.

We have $a^2 b \in V$ whenever a, b in V. It follows that V is a $k[V^2]$ module. Set $J = k[V^2]$. So $Ja^{-1} \subseteq V$ if $0 \neq a \in V$. Therefore $J^{-1}a \subseteq V$ since V is inversion invariant.

This shows that V is in fact a module over $k(V^2) = K^2$ and completes the proof of Theorem 2.1. Also note that since V is a K^2-module, the same is true for the ring R generated by V, whence this ring is a field.

Remark 2.6. From the arguments above, it follows that if T is a nonzero additive subgroup of a division ring D that is closed under inversion and either the characteristic is not 2 or D is a field, then the ring generated by T (over $\mathbb{Z}$) is a division ring.

References

[D'Amour and McCrimmon 2000] A. D'Amour and K. McCrimmon, "The structure of quadratic Jordan systems of Clifford type", *J. Algebra* **234** (2000), 31–89. MR 2001k:17050 Zbl 0982.17015

[Herstein 1976] I. N. Herstein, *Rings with involution*, University of Chicago Press, Chicago, 1976. MR 56 #406 Zbl 0343.16011

[Jacobson 1968] N. Jacobson, *Structure and representations of Jordan algebras*, AMS Colloquium Publications **39**, Amer. Math. Soc., Providence, RI, 1968. MR 40 #4330 Zbl 0218.17010

[Jacobson 1980] N. Jacobson, *Basic algebra*, vol. 2, Freeman, San Francisco, 1980. MR 81g:00001 Zbl 0441.16001

[McCrimmon and Zelmanov 1988] K. McCrimmon and E. Zelmanov, "The structure of strongly prime quadratic Jordan algebras", *Adv. in Math.* **69**:2 (1988), 133–222. MR 89k:17052 Zbl 0656.17015

[Zelmanov 1984] E. I. Zelmanov, "Prime Jordan triple systems, II", *Sibirsk. Mat. Zh.* **25**:5 (1984), 50–61. In Russian; translated in *Siberian Math. J.* **25**:5 (1984), 726–735. MR 87d:17022 Zbl 0562.17007

Received January 13, 2005.

DANIEL GOLDSTEIN
CENTER FOR COMMUNICATIONS RESEARCH
SAN DIEGO, CA 92121-1969
UNITED STATES

dgoldste@ccrwest.org

ROBERT M. GURALNICK
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTHERN CALIFORNIA
3620 S. VERMONT AVE.
LOS ANGELES, CA 90089-2532
UNITED STATES

guralnic@usc.edu

LANCE SMALL
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA SAN DIEGO
LA JOLLA, CA 92093-0112
UNITED STATES

lwsmall@ucsd.edu

EFIM ZELMANOV
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA SAN DIEGO
LA JOLLA, CA 92093-0112
UNITED STATES

ezelmano@euclid.ucsd.edu